

抽象代数讲义 3.0

徐彬斌

2025 年 12 月 12 日

目录

第一部分 一些准备	9
第一章 一点历史	10
第二章 一些例子	13
2.1 基本概念	13
2.2 整数 $\mathbb{Z}$	15
2.2.1 整除	15
2.2.2 素数	16
2.2.3 同余	16
2.2.4 消去律	17
2.3 一个注记	17
第三章 集合	18
3.1 基本概念	18
3.2 集合之间的比较	18
3.3 集合的运算	19
第四章 关系	20
4.1 定义	20
4.2 映射	21
4.3 等价关系	27
4.4 (偏)序关系	34
4.4.1 定义	34
4.4.2 子集间的偏序关系	35
4.4.3 极大和最大	35
第五章 集合上的运算	37
第二部分 群理论	42
第六章 群	43
6.1 定义	43
6.2 子群及群的生成	51
6.3 陪集	59
6.4 正规子群	65
6.5 商群	73

第七章 群同态	77
7.1 定义	77
7.2 群同态基本定理	83
7.2.1 群同态基本定理	83
7.2.2 群同态与子群	85
7.3 给定群之间的同态	92
第八章 一些特殊的群	100
8.1 循环群	100
8.1.1 循环群的分类	100
8.1.2 循环群的子群	102
8.1.3 有限群中的循环群	103
8.2 对称群	105
8.3 交错群	117
第九章 群在集合上的作用	121
9.1 定义	121
9.2 群作用的轨道	123
9.3 群在自身上的共轭作用(伴随作用)	134
第十章 群的结构	140
10.1 Sylow 定理	140
10.2 Sylow 定理的应用	147
10.3 群的直积	151
10.4 群的半直积	154
10.5 群的短正合列	156
10.6 $\ast$ 群的合成列	160
10.6.1 群的极大正规子群	160
10.6.2 群的次正规列以及合成列	162
10.7 $\ast$ 可解群和幂零群	167
10.7.1 可解群	167
10.7.2 幂零群	177
第十一章 自由群	184
11.1 自由群的定义	184
11.2 自由群的泛性质	186
11.3 自由基	186
11.4 群的表达	188
11.5 群的表达的可视化	190
第十二章 群的构造	195
12.1 群的自由积 Free Product	195
12.2 群的融合自由积 Amalgamated Free Product	197
12.3 群的 HNN 扩张 HNN extension	198
12.4 群图	198
第三部分 环理论	200
第十三章 环	201
13.1 定义	201

13.2 环的乘法	205
13.2.1 交换环	205
13.2.2 么元	206
13.2.3 零因子	207
13.2.4 单位	210
13.3 环的特征	218
13.4 理想与商环	219
13.4.1 定义	219
13.4.2 理想的运算及生成	223
13.5 素理想与极大理想	224
第十四章 环同态	228
14.1 定义	228
14.2 环同态基本定理	230
14.2.1 环同态基本定理	230
14.2.2 环同态与子环	231
14.3 中国剩余定理	234
第十五章 一些特殊的整环	241
15.1 定义	241
15.2 唯一分解整环	248
15.2.1 定义	248
15.2.2 唯一分解的等价条件	253
15.3 主理想整环	260
15.4 欧几里得整环	262
第十六章 二次整数环	265
16.1 二次域	266
16.2 二次整数环	270
16.3 二次整数的分解	272
16.3.1 欧几里得环	272
16.3.2 元素的分解	274
16.4 理想的唯一分解	276
16.4.1 二次整数环中的理想	277
16.4.2 理想的唯一分解	283
16.4.3 刻画素理想	286
16.5 一些例子	292
16.5.1 $\mathcal{O}_{-1}$	292
16.5.2 $\mathcal{O}_{-2}$	294
16.5.3 $\mathcal{O}_{-3}$	296
第十七章 环上的一元多项式	298
17.1 实系数一元多项式环回顾	298
17.2 环上一元多项式	300
17.3 交换么环上一元多项式	307
17.4 整环上的多项式	316
17.5 UFD 上的多项式	324

第十八章 环上的多元多项式	330
18.1 $\mathbb{N}^n$	330
18.2 基本概念	332
18.3 交换幺环上的多元多项式	333
18.4 对称多项式	338
18.5 Hilbert 零点定理	344
 第四部分 模理论	 348
第十九章 模论基础	349
19.1 模	350
19.2 子模	355
19.3 商模	360
19.4 模同态	362
 第二十章 自由模	 367
20.1 模的直和	368
20.2 自由模的定义	369
 第二十一章 自由模之间的同态	 374
21.1 自由模间的同态及其矩阵表示	374
21.2 交换幺环上的矩阵	379
21.3 PID 上的矩阵	386
 第二十二章 主理想整环上的有限生成模	 395
22.1 主理想整环上的自由模	395
22.2 主理想整环上的扭模	397
22.3 主理想整环上的有限生成扭模	402
22.4 主理想整环上的有限生成模结构定理的应用	413
 第二十三章 模的张量积	 428
23.1 模的系数环的扩张	428
23.2 幺环上的模的张量积	436
23.3 交换幺环上的模的张量积	445
23.4 向量空间之间的张量积	450
 第二十四章 模的正合列	 455
24.1 模的扩张	455
24.2 模的正合列	456
24.3 投射模	462
24.4 入射模	469
24.5 平坦模	480
 第二十五章 模的子模链	 485
25.1 子模链	485
25.2 Artin 模和 Noether 模	495
25.3 Artin 环和 Noether 环	505

第五部分 域理论 512

第二十六章 域 513

26.1 基本概念	513
26.2 子域	514
26.2.1 定义	514
26.2.2 子域的生成	515
26.3 域的扩张	517
26.4 域同态	519

第二十七章 域的代数扩张 524

27.1 域上的代数元	524
27.2 域的代数扩张	531
27.3 分裂域	537
27.3.1 定义	537
27.3.2 分裂域之间的同态	540
27.3.3 例子	549
27.4 尺规作图	549
27.5 域的代数闭包	556
27.5.1 定义	557
27.5.2 域的代数闭包的存在性	558
27.5.3 域的代数闭包的唯一性	559
27.5.4 例子	561
27.6 域的正规扩张	562
27.7 域的可分扩张	570
27.7.1 可分扩张的定义及一些基本结论	570
27.7.2 不可分不可约多项式	576
27.7.3 Frobenius 同态	580
27.7.4 不可分多项式	584

第六部分 Galois 理论 588

第二十八章 Galois 扩张 589

28.1 域的自同构的不变子域	589
28.2 Galois 扩张的定义及其等价性质	592

第二十九章 Galois 基本定理 602

第三十章 多项式的 Galois 群 606

30.1 多项式的 Galois 群在根集上的作用	606
30.2 多项式的判别式	609
30.3 泛扩张	609
30.4 $\mathbb{Q}$ 上的五次以下多项式的 Galois 群的分类	610
30.4.1 一次多项式	611
30.4.2 二次多项式	611
30.4.3 三次多项式	611
30.4.4 四次多项式	614
30.5 Galois 反问题	617

第三十一章 *Galois 理论与几何 618

第三十二章 有限域	625
32.1 有限域的描述	625
32.2 有限域的同构群	626
第三十三章 本原元	633
33.1 本原元的定义	633
33.2 一个有限 Galois 扩张中如何找本原元	634
第三十四章 根式扩张	635
34.1 定义	635
34.2 分圆扩张	635
34.2.1 条件设定	635
34.2.2 分圆多项式	636
34.2.3 关于分圆多项式是否可约的讨论	638
34.2.4 U_n 的结构	641
34.2.5 可构造正多边形	643
34.3 循环扩张	646
34.4 Kummer 扩张	649
34.5 多项式的根式解	651
34.5.1 若 G_f 可解	651
34.5.2 若 f 是根式可解的	652
34.5.3 五次及以上多项式的可解性	654
第七部分 范畴论	655
第三十五章 范畴论基础	656
35.1 范畴	657
35.2 对偶	663
35.3 函子	667
35.4 自然变换	672
35.5 范畴的等价	682
第三十六章 函子的伴随	687
36.1 伴随	687
36.2 伴随变换与 Hom-函子	689
36.3 单位和余单位	691
36.4 自然变换的可视化	696
第三十七章 泛性质	704
37.1 泛性质	704
37.2 起点对象与终点对象	705
37.3 逗号范畴	707
第三十八章 函子的可表性	711
38.1 可表函子	711
38.2 Yoneda 引理	713
38.3 可表性与泛性质	716

第三十九章 极限和余极限	719
39.1 定义	719
39.2 例子	721
附录 A 同态基本定理	727
A.1 环同态的像与原像	727
A.2 集合之间的映射	728
A.3 群同态基本定理	731
A.4 环同态基本定理	733
A.5 例子	736
A.6 模同态基本定理	736
A.7 总结	738
附录 B 直积与直和	739
B.1 非空集合的笛卡尔积	739
B.2 群的直积与直和	740
B.3 环/模的直积与直和	741
附录 C 尝试在给定域之间的所有同态的集合上构造运算	742

该讲义是根据我于2022年秋期至今在南开大学数学科学学院教授的抽象代数 I, 抽象代数 II 以及 Galois 理论课程内容整理的. 在此基础上, 讲义也包括了一些课堂内容的延申. 感兴趣的同学可以有选择的阅读. 课程的教材为科学出版社出版的由邓少强, 朱富海编著的《抽象代数》. 课程内容准备的过程中也参考了其它文献资料. 详见讲义最后的参考文献列表. 讲义在准备过程中难免会有疏漏, 若阅读过程中发现错误, 欢迎指证.

特别感谢 2020 级和 2021 级参与课程的同学对讲义改进提供的建议和帮助.

第一部分

一些准备

第一章 一点历史

我们首先简要地回顾一下代数(主要是抽象代数)的发展. 本节主要的参考文献为[?book11]以及

<https://mathshistory.st-andrews.ac.uk/>

代数早期的发展就是解多项式方程的历史. 早在公元前1700年, 古巴比伦人就开始对线性方程和二次方程做系统的研究, 并已经找到了求根公式. 那时的很多数学问题多来自于几何和天文, 因此人们在考虑方程的时候一般都会设系数为正数. 当时并没有抽象的符号, 因此方程以及解多用文字叙述. 中国古代(大约公元前200年)和古印度(大约公元前600年)也都对线性方程和二次方程做了系统的研究. 这些研究已经允许负数存在, 此外在九章算术中, 已经有了用矩阵表示线性方程组, 通过矩阵变换消元解线性方程组的思想.

波斯数学家花刺子模 (Al-Khwarizmi) 写了一本书 "al-jabr w al-muqadalah". 其中 "al-jabr" 是把方程的一个负项移动到等号的另一边让其变为正项, 而 "al-muqadalah" 意思是消去方程两边相同的正项. 这些也正是花刺子模解二次方程中使用的方法. 这本书后来传入欧洲, 书名 "al-jabr" 也即后来英文 "algebra" 的来源. 而他的名字则是英文 "algorithm" 的来源.

三次方程和四次方程的求根公式由文艺复兴时期的意大利数学家 Ferro 和 Tartaglia 各自独立找到. 这些公式后由 Cardano 整理后记入其著作 "Ars Magna" 中. 现在的三次方程的求根公式被称为 Cardano 公式. 在得到三次求根公式之前, Cardano 的学生(助手) Ferrari 已经找到了可以将四次方程的求解问题转化为三次求解问题, 因此有了三次方程的公式, 四次方程的求根公式也就找到了. 需要指出的是, 这里所谓的求根公式是指对多项式方程的系数使用加减乘除以及根式得到多项式方程的解. 在此之前, 人们对多项式方程的近似解的研究已经得到了一定的成果.

另一个需要指出的是, 在使用 Cardano 公式时, 我们有时会遇到负数的平方根, 这在当时通常被认为没有意义的, 通常将其忽略. 例如, 使用 Cardano 公式研究了三次方程

$$x^3 = 15x + 4,$$

得到了一个根

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}.$$

意大利数学家 Bombelli 注意到 4 也是以上方程的根, 同时这个方程还有另外两个实根 $-2 \pm \sqrt{3}$. 在其著作 L'Algebra 中, 在尝试解释这个现象的过程中, Bombelli 引入了我们现在熟悉的复数的运算规则. 从而得到了

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}} = (2 + \sqrt{-1}) + (2 - \sqrt{-1}) = 4.$$

此外, 直到此时, 人们还没有开始在数学论证中使用数学符号. 例如 Cardano 关于三次方程的根式解的推到需要三页纸, 而使用符号, 我们仅用半页就可以将其写完. 在韦达 Viète 的著作 "Introduction à l'Art Analytique" 以及笛卡尔 Descartes 的著作 "La Géométrie" 中, 数学符号被正式引入数学论述中. 这大大简化了数学表达的复杂程度.

在解决四次方程的求解之后, 人们的目光自然就放在了一般的五次方程是否有求根公式的问题上. 1770 年, Lagrange 尝试使用根的置换的思想来求解五次方程, 但没有成功.

1779年, Ruffini 证明了五次及以上方程没有根式解. 不过他的证明有漏洞. 1824年, Abel 给出了第一个完整的证明. 现在这个定理被称为 Abel-Ruffini 定理. 另一方面, 我们注意到一些特殊形式的五次及以上方程(比如 $x^5 = 1$)还是有根式解的. 法国数学家 Galois 在前人工作的基础上建立了一套理论来研究这个问题, 给出了判定一个多项式是否有根式解的充要条件. 他的工作现在被称为 Galois 理论.

抽象群理论 在此之后, 抽象的群概念逐渐进入人们的视野. 抽象的群的概念的诞生有三个主要来源:

- (1) 18世纪在研究多项式方程的解的时候对置换(permutation)的研究 (Lagrange, Ruffini, Cauchy, Abel, Galois, Liouville, Jordan, Betti 等);
- (2) 18世纪数论中对模算数(modular arithmetic)的研究 (Euler, Gauss);
- (3) 19世纪初对非欧几何(non-Euclidean geometry)以及射影几何(projective geometry)的研究 (Monge, Carnot, Poncelet, Lambert, Gauss, Lobachevsky, Bolyai, Mobius 等), 在 1872 年, Klein 发表了 "A comparative review of recent researches in geometry" 提出群作用的角度来刻画几何的方法, 现在被称为 "Erlangen program".

Cayley 于 1854 年在其著作 "On the theory of groups, as depending on the symbolic equation $\theta^n = 1$ " 中第一次给出了抽象(有限)群的定义, 将其定义为

"一个由有限个符号构成的集合中任意两个元素的乘积以及任意一个元素乘以自己都仍在这个集合中, 这个乘积运算不一定满足交换律但一定满足结合率, 如果整个群乘以其中一个元素, 那么我们仍得到该群".

之后 Heinrich Weber 将抽象群的概念进一步发展, 他也给出了一个抽象群的定义. 不过这两个定义在现在看来都不完善. 第一个给出比较完善的抽象群的定义的是 von Dyck (Klein 的助手). 他的定义中最重要的一点就是提到了么元和逆元.

由抽象群概念的起源我们可以看出, 群的诞生与研究某个集合上的作用是紧密联系的, 例如, 置换群在根集上的作用, 射影变换在射影空间上的作用等等. 因此有时我们在介绍抽象群的两个元素做运算的时候也会用到"复合" (composition) 这个词. 例如, 两个射影变换的复合仍是射影变换.

在抽象群概念出现之后, 作为一个基础的代数结构, 抽象群理论在基础理论逐渐完善的同时也出现了不同的分支, 例如, 有限群理论, 李群理论, 拓扑群理论, 组合群论, 几何群论等. 此外, 群论也在其他领域有广泛的应用.

抽象环理论 整数环 $\mathbb{Z}$, 实系数多项式环 $\mathbb{R}[x]$, 以及实系数矩阵环 $\text{Mat}_n(\mathbb{R})$ 是环的三个最基本的例子. 这些例子也是代数数论, 代数几何, 不变量理论, 超复数等领域基本的例子. 对这些领域里一些问题的研究可以看作是抽象的环论的来源:

- (1) 代数数论对费马大定理, 二次互反律, 二元二次型, Kummer 理想数, 戴德金理想等的研究(Lamé, Kummer, Gauss, Dedekind 等)
- (2) 代数几何对代数曲线, 多项式环及其理想, 代数函数域等的研究(Riemann, Clebsch, Gordan, Brill, Noether, Dedekind, Weber, Hilbert, Lasker, Macauley 等)
- (3) 不变量理论 Invariant theory (Gauss, Hilbert, Gordan)
- (4) 超复数 hypercomplex number 如四元数, 八元数等(Hamilton, Cayley, Clifford, Grassmann 等)

其中前三个与交换环理论有关, 最后一个与非交换环理论有关.

Fraenkel 在其1914年的文章 "On zero divisors and decomposition of ring" 给出了第一个公理化的环的定义. 之后利用这个思想, Sono 添加了交换的条件给出了交换环的定义. Noether 和 Artin 的工作大力发展了抽象环理论.

抽象域理论 域论主要有以下三个来源:

- (1) Galois理论关于域的扩张的研究(Lagrange, Ruffini, Abel, Galois等)
- (2) 代数数论关于代数数域的研究(Dedekind, Kronecker等)
- (3) 代数几何关于代数函数域, 有理函数域的研究(Dedekind, Weber, Kronecker等)

抽象的域的定义第一次出现在 Weber 1893年的文章"General foundations of Galois's theory of equations". 这个文章的目标是给 Galois 理论一个抽象的表述. 之后, Weber, Veronese, Hensel, Steinitz, Artin 等都对抽象域理论的发展做出了重要贡献.

第二章 一些例子

由抽象代数的发展我们可以看出, 我们将见到的抽象的概念都源于对某些例子的研究. 另一方面, 抽象代数理论又可以被应用在更广泛的例子上来推动相关研究的发展. 因此, 例子在我们的课程中是非常重要的. 我们这里通过已经接触过的例子来大概的说明一些我们这门课的内容.

2.1 基本概念

我们在数学分析的课程中已经接触到了 $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ 以及 $\mathbb{R}$ (可能还有 $\mathbb{C}$?)等空间. 并研究了 $\mathbb{R}$ 上的取值在 $\mathbb{R}$ 中的函数. 在高等代数的课程中, 我们已经接触到了 $\mathbb{R}$ 上(可能还有 $\mathbb{C}$ 上?)的线性空间. 我们经常会考虑这些空间上的一些运算. 例如, 整数集合 $\mathbb{Z}$ 上的 $+$, $-$ 和 $\times$, 实数集合 $\mathbb{R}$ 上的 $+$, $-$, $\times$ 和 $\div$, 向量空间上的向量加法等. 这些运算将相应集合中的元素联系起来.

在抽象代数的课程中, 我们将会沿着这个思路来讨论更一般的情况. 我们通常面对的是某个非空集合以及在其上定义的某个或者某几个"运算". 这些"运算"将集合中的元素联系起来, 从而构成我们通常说的"代数结构". "代数结构"及其相关理论将是我们这门课讨论的主要对象.

例 2.1.1.

以下是附带一个"运算" $*$ 的集合 S 的例子:

S	自然数集 $\mathbb{N}$	3-维实向量空间 $\mathbb{R}^3$	$\mathbb{R}$ 的子集的集合 $\mathcal{P}(\mathbb{R})$
元素例子	0, 3	(1, 0, 0), (3, 2, 1)	$\{1, 2, 3\}$, $[0, 2]$, $2\mathbb{Z}$
$*$	自然数加法运算 $+$	向量加法运算 $+$	集合的并 $\cup$
例子	$2 + 3 = 5$	$(1, 2, 0) + (0, 3, 3) = (1, 5, 3)$	$[0, 1] \cup \{1\} = [0, 1]$

以下是带有两个不同"运算" $*_1$ 和 $*_2$ 的集合 S 的例子:

S	自然数集 $\mathbb{Z}$	{定义在 $\mathbb{R}$ 上在 $\mathbb{R}$ 中取值的函数}
元素例子	-10, 23	$f(x) = 3x, g(x) = \begin{cases} 0, & x \text{ 为有理数} \\ 2, & x \text{ 为无理数} \end{cases}$
$*_1$	加法运算 $+$	加法运算 $+$
例子	$5 + 3 = 8$	$(f + g)(x) = \begin{cases} 3x, & x \text{ 为有理数} \\ 3x + 2, & x \text{ 为无理数} \end{cases}$
$*_2$	乘法运算 $\times$	复合运算 $\circ$
例子	$4 \times 8 = 32$	$(f \circ g)(x) = \begin{cases} 0, & x \text{ 为有理数} \\ 6, & x \text{ 为无理数} \end{cases}$

当然不同的集合上的不同运算满足的性质也不同. 我们以 $(\mathbb{Z}, +, \times)$ 为例来大概的说明我们将关注的运算的性质. 我们用 a, b, c 记 $\mathbb{Z}$ 中的元素.

- (1) "加法幺元": 0 , 满足对任意 $a \in \mathbb{Z}$, 有 $0 + a = a + 0 = a$,
例如, $0 + 2 = 2 + 0 = 2$;
- (2) "加法逆元": 任取 $a \in \mathbb{Z}$, 存在 $-a$, 满足 $a + (-a) = 0$,
例如, $2 + (-2) = 0$;
- (3) "加法交换律": $a + b = b + a$,
例如, $2 + 3 = 3 + 2$;
- (4) "加法结合律": $(a + b) + c = a + (b + c)$,
例如, $(2 + 3) + 4 = 2 + (3 + 4)$;
- (5) "乘法幺元": 1 , 满足对任意 $a \in \mathbb{Z} \setminus \{0\}$, 有 $1 \times a = a \times 1 = a$,
例如, $1 \times 2 = 2 \times 1 = 2$;
- (6) "乘法交换律": $a \times b = b \times a$,
例如, $2 \times 3 = 3 \times 2$;
- (7) "乘法结合律": $(a \times b) \times c = a \times (b \times c)$,
例如, $(2 \times 3) \times 4 = 2 \times (3 \times 4)$;
- (8) "左分配律": $a \times (b + c) = a \times b + a \times c$,
例如, $2 \times (3 + 4) = 2 \times 3 + 2 \times 4$.
- (9) "右分配律": $(a + b) \times c = a \times c + b \times c$,
例如, $(2 + 3) \times 4 = 2 \times 4 + 3 \times 4$.

虽然以上这些性质我们在实际计算中经常使用, 看起来比较显然, 而这些抽象出来的性质就是"群"和"环"抽象概念的基础. 后边当我们介绍完"群"和"环"的定义之后, 我们就可以说

- $\mathbb{Z}$ 关于加法成一个"(交换)群";
- $\mathbb{Z}$ 关于乘法不是一个"群";
- $\mathbb{Z}$ 关于加法和乘法成一个"(交换)环".

我们注意到 $\mathbb{Z}$ 中的乘法运算与加法运算相比少了"存在逆元"这个性质. 我们可以将 $\mathbb{Z}$ 扩展为 $\mathbb{Q}$. 注意到 $\mathbb{Q}$ 上的加法和乘法也满足以上所有的性质, 并且 $\mathbb{Q}$ 中不等于 0 的元素都有乘法逆:

- 任取 $a, b \in \mathbb{Z}^*$, 则 $\frac{a}{b} \in \mathbb{Q} \setminus \{0\}$ 有乘法逆元 $\frac{b}{a} \in \mathbb{Q} \setminus \{0\}$:

$$\frac{a}{b} \times \frac{b}{a} = 1.$$

例如, $\frac{1}{2} \times 2 = 1$.

有了这个性质, 我们就有了一个"域": $\mathbb{Q}$.

注 2.1.2.

从前边介绍的例子, 我们可以看出, 这些条件并不是任意集合上的任意"运算"都可以满足的. 例如, 自然数 $\mathbb{N}$ 上的加法运算就没有"存在逆元"这个性质, 而 $\mathbb{R}$ 上所有函数的集合上的复合运算不具有交换的性质 (可以使用之前例子中的 f 和 g 计算 $g \circ f$, 并于 $f \circ g$ 作比较)

2.2 整数 $\mathbb{Z}$

在本课程的学习中, 整数将以两种身份出现. 第一种身份是我们所讲的理论的基本的例子, 例如, 群, 环, 整环, 唯一分解整环, 主理想整环, 欧几里得环等等. 正如大家在回顾代数发展历史的时候发现的那样, 我们有许多概念都是从对整数的研究抽象推广出来的. 第二种身份是作为证明一些结论的工具. 例如, Lagrange 定理, Sylow 定理, 有限交换群的结构定理的证明等等. 这里我们简要的回顾一下大家比较熟悉的与 $\mathbb{Z}$ 相关的一些定义和结论.

2.2.1 整除

定义 2.2.1 (整除, 因子)

任取 a 和 b 两个整数, 如果存在整数 c , 满足

$$b = ac,$$

我们就称 a **整除** b , 记作 $a \mid b$. 另一方面, 我们称 a 为 b 的一个**因子**.

从因子数目的角度考虑, 我们有以下一类特殊的整数:

定义 2.2.2 (素数, 合数)

记 p 为一个大于 1 的整数. 若 p 的正因子只有 1 和 p , 那么我们称 p 为一个**素数**. 若 p 有除了 1 和 p 以外的正因子, 我们称 p 为一个**合数**.

定义 2.2.3 (公因子, 最大公因子, 互素)

记 a 和 b 为两个非零整数. 如果一个整数 $c \in \mathbb{Z}$, 满足

$$c \mid a, c \mid b,$$

我们称 c 为 a 和 b 的**公因子**.

如果 d 为 a 和 b 的所有公因子中最大的一个, 我们称 d 为 a 和 b 的**最大公因子**, 记作 $d = \gcd(a, b)$.

若 $d = 1$, 我们称 a 和 b **互素**.

命题 2.2.4 (带余除法)

任取两个非零整数 a 和 b , 其中 $a > 0$, 则存在唯一的一对整数 p 和 r , 满足

$$b = pa + r,$$

其中 $0 \leq r < a$.

命题 2.2.5 (Bezout等式)

记 a 和 b 为不为零的整数, 并记 $d = \gcd(a, b)$. 则存在整数 u 和 v , 满足

$$d = ua + vb.$$

命题 2.2.6 (互素的一个充要条件)

记 a 和 b 为两个不为零的整数. 则 a 和 b 互素当且仅当存在整数 u 和 v , 满足

$$1 = ua + vb.$$

2.2.2 素数**定理 2.2.7 (算术基本定理)**

任意一个大于1的正整数 a , 都可以分解为 $n > 0$ 个素数的乘积:

$$a = p_1 \times \cdots \times p_n,$$

并且这种分解在相差一个重新排列的前提下是唯一的.

定理 2.2.8 (素数无限)

存在无穷多个素数.

2.2.3 同余

固定一个非零正整数 m . 任取整数 a 和 b . 考虑关于 m 的带余除法, 我们有唯一的整数 p, q, r, s , 满足

$$a = pm + r, \quad b = qm + s,$$

其中 $0 \leq r < m$ 且 $0 \leq s < m$.

定义 2.2.9 (同余)

如果 $r = s$, 我们称 a 和 b 模 m 同余, 记作

$$a \equiv b \pmod{m}.$$

从定义我们可以验证, a 和 b 模 m 同余, 当且仅当

$$m \mid a - b.$$

固定非零正整数 m , 利用模 m 同余, 我们可以将 $\mathbb{Z}$ 分解为一些不交集合的并集. 我们记 $m\mathbb{Z}$ 为所有被 m 整除的整数的集合, 则这个分解可以写为

$$\mathbb{Z} = m\mathbb{Z} \cup (m\mathbb{Z} + 1) \cup \cdots \cup (m\mathbb{Z} + (m - 1)).$$

命题 2.2.10

设 a 和 b 为两个整数. 则 a 和 b 模 m 同余, 当且仅当存在 $0 \leq j \leq m-1$, 满足

$$a \in m\mathbb{Z} + j, b \in m\mathbb{Z} + j.$$

我们下边考虑同余与 $\mathbb{Z}$ 上的加法和乘法的关系, 有以下结论

命题 2.2.11

设 m 为一个非零正整数. 设整数 a, a', b, b' 满足

$$a \equiv a' \pmod{m}, b \equiv b' \pmod{m},$$

则我们有

$$a + b \equiv a' + b' \pmod{m}, a \times b \equiv a' \times b' \pmod{m}.$$

注 2.2.12.

以上讨论为我们课程某些内容提供了基本的例子.

- (1) 同余构成了集合 $\mathbb{Z}$ 上的一个"等价关系", 同余的元素构成了一个"等价类".
- (2) 对任意 $0 \leq j \leq m-1$, 我们记 $\bar{j} = m\mathbb{Z} + j$, 则得到由同余等价关系所诱导的"商空间":

$$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} := \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}.$$

- (3) 考虑 $\mathbb{Z}$ 上的"环结构", 则 $m\mathbb{Z}$ 构成了 $\mathbb{Z}$ 的一个"理想".
- (4) 考虑同余与 $\mathbb{Z}$ 上加法和乘法运算的关系, 我们可以在 $\mathbb{Z}_m$ 上定义加法和乘法 ("等价类"之间的运算), 从而在 $\mathbb{Z}_m$ 上诱导一个"环结构". 我们将看到 $\mathbb{Z}_m$ 为 $\mathbb{Z}$ 的一个"商环".

2.2.4 消去律

我们在讨论整数的时候经常会使用以下结论.

命题 2.2.13 (消去律)

任取整数 a, b, c , 若 $ab = ac$, 且 $a \neq 0$, 则我们有 $b = c$.

注 2.2.14.

以上结论看起来平凡, 但当我们考虑一般的环的时候, 该结论并不是总成立.

2.3 一个注记

整数(更进一步数域)为我们将讨论的内容提供了例子, 但我们也应该注意, 并不是所有的例子都来自于数域. 有许多例子与数域中的例子相比, 有许多不同的性质.

第三章 集合

3.1 基本概念

集合并没有一个明确的定义. 笼统地讲集合就是一族有相同性质的物体的整体. 例如: 所有整数的集合, 所有实数域上的实数函数的集合等等. 我们称一个集合中的物体为集合的元素. 如果一个集合记为 A , a 是 A 中的元素, 我们通常记作

$$a \in A.$$

一个集合通常有以下两种表达方式:

- (i) 在大括号 $\{ \}$ 中列举出所有的包含在其中的元素. 例如: $\{1, 2, a, M\}$.
- (ii) 我们可以使用 $|$ 将在大括号 $\{ \}$ 中空间分为两部分, $|$ 前边写一个代表元, $|$ 后边写元素所满足的性质.

$$\{a \mid a \in \mathbb{R}, a^2 = 1\}.$$

我们有时也会使用 $:$ 代替 $|$. 例如,

$$\{a : a \in \mathbb{R}, a^2 = 1\}.$$

尽管没有明确的定义, 集合有一个要求就是任给一个物体, 我们需要能够明确地说明这个物体是否在这个集合中. 当我们使用第二种方法描述一个集合的时候, 我们需要给出一个明确可以用来判断是否满足的性质. 例如: " $\mathbb{R}$ 中像 3 一样的数字" 就不能作为 $|$ 后的部分来定义一个集合.

关于集合另外一个需要注意的地方就是不是所有的放在一起的物体都可以构成一个集合. 一个著名的例子就是所有集合的整体. 我们记其为 A . 假设 A 是一个集合, 那么我们可以给出一个性质就是 " $a \notin a$ ", 从而考虑所有不包含自己的集合, 将这些集合的整体记为 B . 此时我们遇到的一个问题就是 B 是否属于 B . 如果 B 不属于 B , 那么 B 不属于自己, 满足用来定义 B 的性质, 因此 B 应该属于 B . 而属于一个集合和不属于一个集合不能同时成立. 这就是著名的"罗素悖论".

注 3.1.1.

利用这个悖论, 我们还可以说明所有群的整体不构成一个集合.

3.2 集合之间的比较

设 A 和 B 都是集合, 它们之间的比较包含以下几种情况:

- (i) A 被 B 包含记作 $A \subset B$: 集合 A 中的元素都属于 B ($\forall a \in A, a \in B$);
- (ii) A 包含 B 记作 $A \supset B$: 集合 B 中的元素都属于 A ($\forall a \in B, a \in A$);

- (iii) A 和 B **相等** 记作 $A = B$: 两个集合包含相同的元素 $((A \subset B) \wedge (A \supset B))$;
 (iv) 以上都不满足.

我们可以用冒号后边的性质来验证这些关系. 这也是我们在证明中经常会用到的.

3.3 集合的运算

集合之间是可以运算的. 常用的运算有集合的并, 交, 补.
 任取集合 A 和 B , 我们定义

- (i) A 和 B 的**并集**记作 $A \cup B$ 为如下集合:

$$A \cup B := \{a \mid a \in A \text{ 或者 } a \in B\}.$$

- (ii) A 和 B 的**交集**记作 $A \cap B$ 为如下集合:

$$A \cap B := \{a \mid a \in A \text{ 并且 } a \in B\}.$$

- (iii) 若 $B \subset A$, 则 B 在 A 中的**补集**记作 B^c 为如下集合:

$$B^c := \{a \in A \mid a \notin B\}.$$

注 3.3.1.

补集右上角记号 c 来自于 complement 的首字母.

我们可以进一步将这些运算组合起来得到更复杂的集合间的运算. 利用这些运算的定义, 我们有如下关系:

命题 3.3.2

任取集合 A 以及其子集 B, C 和 D , 我们有

(i) $B \cap (C \cup D) = (B \cap C) \cup (B \cap D).$

(ii) $B \cup (C \cap D) = (B \cup C) \cap (B \cup D).$

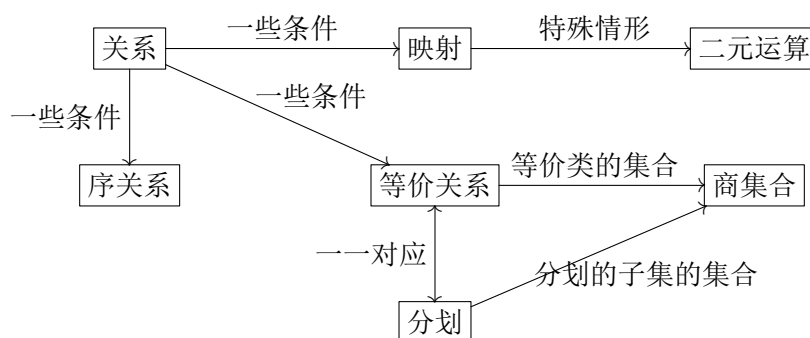
(iii) $(B \cap C)^c = B^c \cup C^c.$

(iv) $(B \cup C)^c = B^c \cap C^c.$

第四章 关系

本节主要介绍的概念有关系, 映射, 等价关系, 二元运算. 这些概念在抽象代数的学习中将会被经常用到, 是很多其他概念的基础. 例如: 一个群同态首先是一个映射; 商群首先是关于某个等价关系的商集合等等.

这些概念之间的关系如下:



注 4.0.1.

为了给之后严格化讨论做准备, 我们本节中多使用公理化的方法来介绍定义, 因此比较抽象, 建议通过多举各种各样的例子来帮助理解.

4.1 定义

在该讲义中, 除了特殊说明外, 我们考虑的集合均非空. 我们记 A 和 B 为两个集合, 并记 $A \times B$ 为 A 与 B 的笛卡尔积:

$$A \times B := \{(a, b) \mid a \in A, b \in B\}.$$

定义 4.1.1 (教材定义1.2.13(改))

集合 A 与 B 之间的一个**关系**是 $A \times B$ 的一个子集.

设 $\mathcal{R} \subset A \times B$ 为 A 与 B 的一个关系. 若 $(a, b) \in \mathcal{R}$, 我们称 a 和 b **$\mathcal{R}$ -相关**. 我们通常用 $a\mathcal{R}b$ 来表示 $(a, b) \in \mathcal{R}$.

例 4.1.2.

我们考虑以下集合:

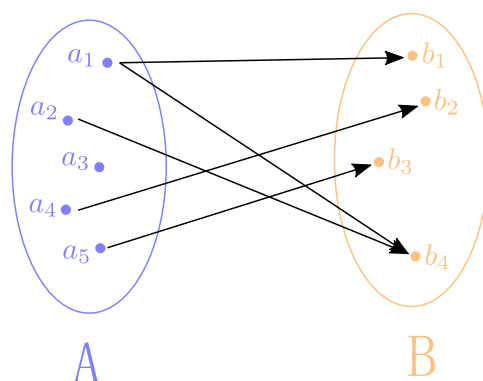
$$A = \{a_1, a_2, a_3, a_4, a_5\}, \quad B = \{b_1, b_2, b_3, b_4\}.$$

以下 $A \times B$ 的子集 $\mathcal{R}$ 给出 A 和 B 的一个关系

$$\mathcal{R} = \{(a_1, b_1), (a_1, b_4), (a_2, b_4), (a_4, b_2), (a_5, b_3)\}.$$

(参考以下示意图)

	b_1	b_2	b_3	b_4
a_1	(a_1, b_1)			(a_1, b_4)
a_2				(a_2, b_4)
a_3				
a_4		(a_4, b_2)		
a_5			(a_5, b_3)	



4.2 映射

设 $\mathcal{R} \subset A \times B$ 为 A 与 B 的一个关系.

定义 4.2.1

若关系 $\mathcal{R}$ 满足以下条件, 我们称关系 $\mathcal{R}$ 为一个从集合 A 到集合 B 的**映射**:

- 对于任意 $a \in A$, 存在唯一的 $b \in B$, 使得我们有 $a\mathcal{R}b$.

集合 A 被称为映射 $\mathcal{R}$ 的**定义域**.

注 4.2.2.

若 $\mathcal{R}$ 是一个从 A 到 B 的映射, 我们通常用 f, g, ϕ, ψ 等来记映射, 并使用记号类似 $f: A \rightarrow B$ 记 A 到 B 的映射. 此时, 若有 $a\mathcal{R}b$, 通常会记 $b = f(a)$.

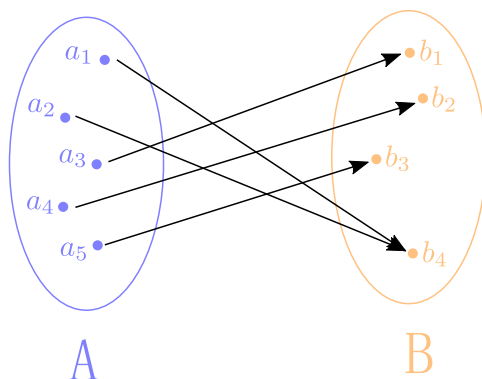
例 4.2.3.

我们考虑以下集合:

$$A = \{a_1, a_2, a_3, a_4, a_5\}, \quad B = \{b_1, b_2, b_3, b_4\},$$

以及关系

$$\mathcal{R} = \{(a_1, b_4), (a_2, b_4), (a_3, b_1), (a_4, b_2), (a_5, b_3)\}.$$



我们可以根据定义验证 $\mathcal{R}$ 为一个从 A 到 B 的映射:

$$\begin{aligned}\mathcal{R} : A &\rightarrow B, \\ a_1 &\mapsto b_4, \\ a_2 &\mapsto b_4, \\ a_3 &\mapsto b_1, \\ a_4 &\mapsto b_2, \\ a_5 &\mapsto b_3.\end{aligned}$$

思考 4.2.4

例子 4.1.2 中的关系是一个映射么? 为什么?

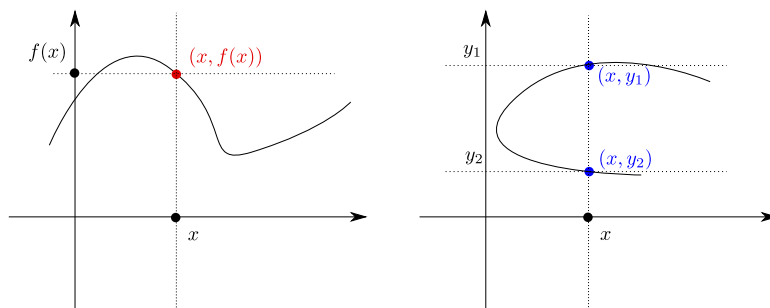
例 4.2.5.

数学分析中, 我们曾经接触过函数的概念. 这个实际上就是数集之间的映射.

记 f 是一个非空数集 $X \subset \mathbb{R}$ 到 $\mathbb{R}$ 的一个映射. 从关系的角度来看, 我们考虑一个数 $x \in X$ 以及其在 f 下的像 $y = f(x) \in \mathbb{R}$, 它们构成的数对 (x, y) 就是 $X \times \mathbb{R}$ 中的一个元素. 这些元素所构成的 $X \times \mathbb{R}$ 的一个子集就给出了 X 和 $\mathbb{R}$ 的一个关系. 我们仍记作 f .

在函数的定义中, 我们要求任取 X 中一个数 x , 都有唯一的一个 $y = f(x) \in \mathbb{R}$ 与之对应. 换句话说, 任取 $x \in X$, 首先要存在一个 $(x, y) \in f$, 其次这样的 y 是唯一的, 也就是说如果有 $(x, y_1) \in f$ 且 $(x, y_2) \in f$, 那么 $y_1 = y_2$.

我们可以考虑在平面 $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ 用画示意图的方法来表示一个函数. 通常横轴代表第一个 $\mathbb{R}$, 纵轴代表第二个 $\mathbb{R}$. 当我们给出一个函数图像的时候, 任给定义域 X 中的一个数 x (也即横轴上一个点), 考虑过这一点与纵轴平行的线. 那么这条线与函数图像有且仅有一个交点. 下边示意图中, 右侧的就不满足交点的唯一性.



注 4.2.6.

在后续的学习中, 我们会经常用到这个定义. 比如, 笼统地说, 两个"群"之间的"同态"是两个"群"之间满足某种条件的映射. 如果我们希望验证两个"群"之间的某种关系是一个"同态"的话, 我们首先就需要验证这个关系是一个映射, 然后再去验证其满足附加的条件. 而验证一个关系是一个映射, 我们就需要用到映射的定义.

设 A_1 为 A 的任意子集. 我们考虑 A 和 B 的一个关系 $\mathcal{R}$. 由此我们可以构造如下 $A \times B$ 的子集:

$$\mathcal{R}_1 := \{(a, b) \in \mathcal{R} \mid a \in A_1\}.$$

集合 $\mathcal{R}_1$ 是一个 A_1 和 B 的关系.

命题 4.2.7

若 $\mathcal{R}$ 为一个映射, 则 $\mathcal{R}_1$ 也为一个映射, 且满足

- 对于任意 $a \in A_1$, 我们有 $\mathcal{R}_1(a) = \mathcal{R}(a)$.

考虑如上定义的关系 $\mathcal{R}$ 和 $\mathcal{R}_1$. 设 $\mathcal{R}$ 为一个映射.

定义 4.2.8

我们称 $\mathcal{R}_1$ 为映射 $\mathcal{R}$ 在 A_1 上的**限制**.

定义 4.2.9

设 A_1 为 A 的任意子集. 我们称以下集合为 A_1 的 **$\mathcal{R}$ -像集**:

$$\mathcal{R}(A_1) := \{b \in B \mid \exists a \in A_1, b = \mathcal{R}(a)\}.$$

当 $A_1 = A$ 时, 我们也会使用记号 $\text{Im}(\mathcal{R})$ 来记 $\mathcal{R}(A)$.

例 4.2.10.

我们考虑以下集合:

$$A = \{a_1, a_2, a_3, a_4, a_5\}, \quad B = \{b_1, b_2, b_3, b_4\},$$

以及关系

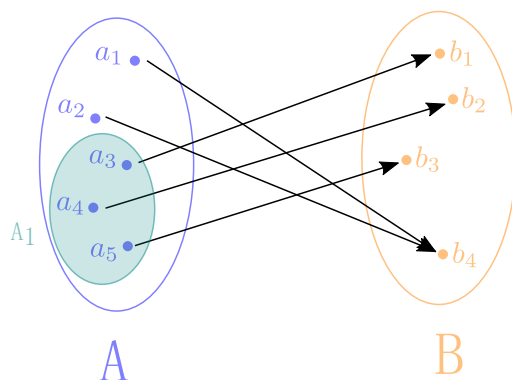
$$\mathcal{R} = \{(a_1, b_4), (a_2, b_4), (a_3, b_1), (a_4, b_2), (a_5, b_3)\}.$$

记

$$A_1 = \{a_3, a_4, a_5\} \subset A,$$

则有

$$\mathcal{R}_1 = \{(a_3, b_1), (a_4, b_2), (a_5, b_3)\}.$$



我们可以根据定义验证 $\mathcal{R}_1$ 为一个从 A_1 到 B 的映射:

$$\begin{aligned}\mathcal{R}_1 : A_1 &\rightarrow B, \\ a_3 &\mapsto b_1, \\ a_4 &\mapsto b_2, \\ a_5 &\mapsto b_3.\end{aligned}$$

这里映射 $\mathcal{R}$ 的像集为 $\text{Im}(\mathcal{R}) = B$, 映射 $\mathcal{R}_1$ 的像集为

$$\text{Im } \mathcal{R}_1 = \{b_1, b_2, b_3\} \subset B.$$

定义 4.2.11

我们称映射 $\mathcal{R}$ 为**单射**, 若其满足以下条件:

- 对于任意 $b \in \text{Im}(\mathcal{R})$, 存在唯一的 $a \in A$, 满足 $b = \mathcal{R}(a)$.

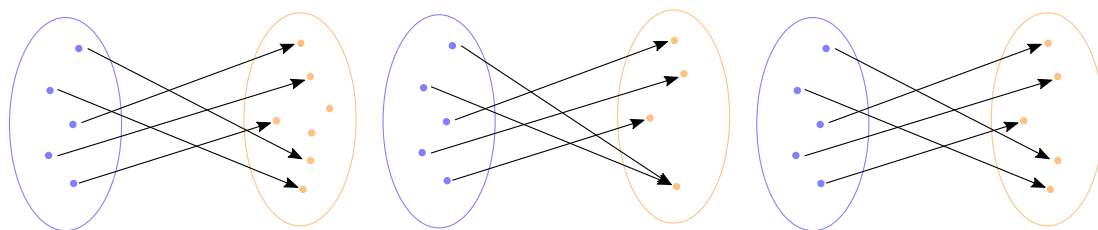
我们称映射 $\mathcal{R}$ 为**满射**, 若其满足以下条件:

- 对于任意 $b \in B$, 存在一个 $a \in A$, 满足 $b = \mathcal{R}(a)$.

若映射 $\mathcal{R}$ 既是单射又是满射, 我们称 $\mathcal{R}$ 为**双射**.

注 4.2.12.

粗略地讲, 单射要求 A 中两个不同的元素不能被送到同一个 B 中的元素; 满射要求 B 中每一个元素都是 A 中某个元素的像 (也即 $\text{Im}(\mathcal{R}) = B$). 下图是集合有限情形下, 单射, 满射, 双射的示意图:



若 $\mathcal{R}$ 为一个 A 和 B 的关系, 我们可以定义一个 B 和 A 的关系 $\mathcal{R}^{-1}$ 为如下 $B \times A$ 的子集:

$$\mathcal{R}^{-1} := \{(b, a) \in B \times A \mid a\mathcal{R}b\}.$$

命题 4.2.13

若 $\mathcal{R}$ 为一个双射, 则 $\mathcal{R}^{-1}$ 为一个从 B 到 A 的双射.

证明. 由于 $\mathcal{R}$ 为满射, 因此任取 $b \in B$, 存在 $a \in A$, 满足 $a\mathcal{R}b$. 所以任取 $b \in B$, 存在 $a \in A$, 满足 $b\mathcal{R}^{-1}a$.

任取 $b \in B$, 若存在 $a_1, a_2 \in A$, 满足 $b\mathcal{R}^{-1}a_1$ 以及 $b\mathcal{R}^{-1}a_2$, 那么我们有 $a_1\mathcal{R}b$ 以及 $a_2\mathcal{R}b$. 由于 $\mathcal{R}$ 为单射, 因此 $a_1 = a_2$.

以上两部分讨论证明了 $\mathcal{R}^{-1}$ 是一个映射.

最后, 由映射的定义, 对任意 $a \in A$, 都存在唯一的 $b \in B$, 满足 $a\mathcal{R}b$. 由 a 的任意性, 知 $\mathcal{R}^{-1}$ 为满射. 由 b 的唯一性知 $\mathcal{R}^{-1}$ 为单射. $\square$

思考 4.2.14

当 $\mathcal{R}$ 为一个映射, 但不是单射或满射时, 关系 $\mathcal{R}^{-1}$ 是一个映射么? 为什么?

定义 4.2.15

若 $\mathcal{R}$ 为一个双射, 我们称映射 $\mathcal{R}^{-1}$ 为 $\mathcal{R}$ 的逆映射.

例 4.2.16.

我们考虑以下集合:

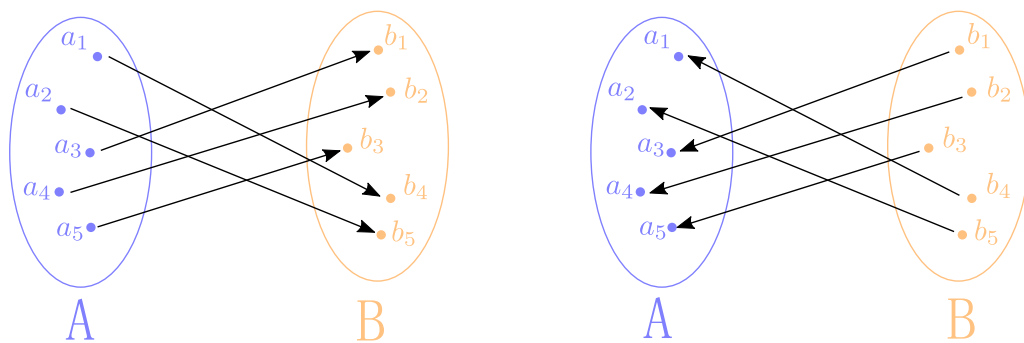
$$A = \{a_1, a_2, a_3, a_4, a_5\}, B = \{b_1, b_2, b_3, b_4\},$$

以及双射

$$\mathcal{R} = \{(a_1, b_4), (a_2, b_5), (a_3, b_1), (a_4, b_2), (a_5, b_3)\} = A \times B.$$

其逆映射 $\mathcal{R}$

$$\mathcal{R}^{-1} = \{(b_1, a_3), (b_2, a_4), (b_3, a_5), (b_4, a_1), (b_5, a_2)\} = B \times A,$$



注 4.2.17.

给定有限集 A 和 B , 我们可以比较 A 和 B 的大小, 也就是两个集合哪个元素个数比较多一

些. 有限集中元素个数就成为这个集的势. 我们可以进一步的将集的势推广到集合无穷的情形. 任取集合 A , 我们通常用 $|A|$ 来记 A 的势. 如果要比较两个无穷集合的大小, 那么数元素个数的方法就无法实现了.

我们的比较方式就是使用单射. 任取两个非空集合 A 和 B , 如果存在单射

$$f: A \rightarrow B,$$

我们就称 A 的势小于 B 的势, 记作 $|A| < |B|$.

如果进一步存在单射

$$g: B \rightarrow A,$$

那么就同时有 $|B| < |A|$. 两个结合起来, 我们就称 A 和 B 等势. 所以如果 A 和 B 两个集合之间存在双射, 那么它们的势相等. 如果是有限集, 那么就有它们的元素个数相等.

需要注意的是, 这里我们没有要求 g 是 f 的逆映射. 另一方面, 如果 $A \subset B$, 两个集合也是有可能等势的. 例如:

$$\begin{aligned} f: \mathbb{N} &\rightarrow 2\mathbb{N} & g: 2\mathbb{N} &\rightarrow \mathbb{N} \\ n &\mapsto 4n & k &\mapsto k+1 \end{aligned}$$

因此 $\mathbb{N}$ 和 $2\mathbb{N}$ 等势.

记 A, B 和 C 为三个集合. 设 $\mathcal{R}_1$ 为一个 A 与 B 的关系, $\mathcal{R}_2$ 为一个 B 与 C 的关系. 那么我们可以由此构造一个 A 与 C 的关系 $\mathcal{R}$:

$$\mathcal{R} := \{(a, c) \in A \times C \mid \exists b \in B, (a\mathcal{R}_1b) \wedge (b\mathcal{R}_2c)\}.$$

命题 4.2.18

若 $\mathcal{R}_1$ 和 $\mathcal{R}_2$ 都是映射, 那么 $\mathcal{R}$ 也是一个映射, 且满足

- 对任意 $a \in A$, 我们有 $\mathcal{R}(a) = \mathcal{R}_2(\mathcal{R}_1(a))$.

证明. 我们首先验证 $\mathcal{R}$ 满足映射的定义.

任取 $a \in A$, 由 $\mathcal{R}_1$ 为映射知, 存在唯一的 $b \in B$, 满足 $a\mathcal{R}_1b$. 由 $\mathcal{R}_2$ 为映射知, 存在唯一的 $c \in C$, 满足 $b\mathcal{R}_2c$. 因此 $a\mathcal{R}c$.

下证 c 是唯一的. 我们使用反证法, 若存在 $c' \in C$ 也满足 $a\mathcal{R}c'$, 则由 $\mathcal{R}$ 的定义, 存在 $b' \in B$, 同时满足 $a\mathcal{R}_1b'$ 以及 $b'\mathcal{R}_2c'$. 由于 $\mathcal{R}_1$ 是映射, 因此 $b = b'$. 由于 $\mathcal{R}_2$ 是映射, 因此 $c = c'$. 因此 c 是唯一满足 $a\mathcal{R}c$ 的 C 中元素.

综上所述, 关系 $\mathcal{R}$ 为从 A 到 C 的映射.

任取 $a \in A$, 由于 $a\mathcal{R}(\mathcal{R}(a))$, 因此存在 b 满足 $a\mathcal{R}_1b$ 以及 $b\mathcal{R}_2(\mathcal{R}(a))$, 即

$$b = \mathcal{R}_1(a), \quad \mathcal{R}(a) = \mathcal{R}_2(b),$$

因此, 我们有

$$\mathcal{R}(a) = \mathcal{R}_2(\mathcal{R}_1(a)).$$

□

定义 4.2.19

若 $\mathcal{R}_1$ 和 $\mathcal{R}_2$ 都是映射, 我们称映射 $\mathcal{R}$ 为映射 $\mathcal{R}_2$ 和 $\mathcal{R}_1$ 的复合, 并记做 $\mathcal{R} = \mathcal{R}_2 \circ \mathcal{R}_1$.

例 4.2.20.

我们考虑以下集合:

$$A = \{a_1, a_2, a_3, a_4, a_5\}, \quad B = \{b_1, b_2, b_3, b_4\}, \quad C = \{c_1, c_2, c_3, c_4, c_5, c_6\}$$

以及映射

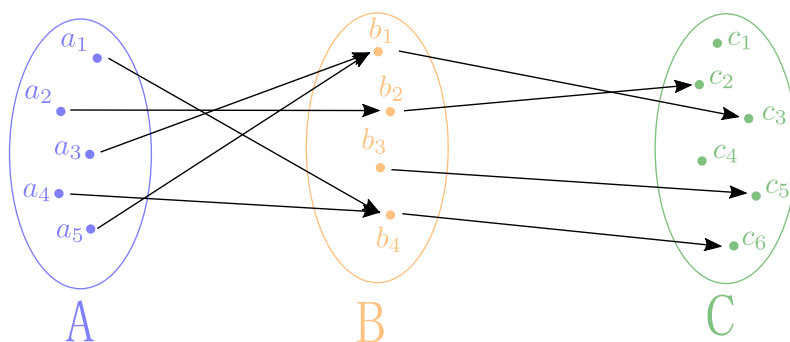
$$\mathcal{R}_1 = \{(a_1, b_4), (a_2, b_2), (a_3, b_1), (a_4, b_4), (a_5, b_1)\} \subset A \times B,$$

和映射

$$\mathcal{R}_2 = \{(b_1, c_3), (b_2, c_2), (b_3, c_5), (b_4, c_6)\} \subset B \times C.$$

则我们有映射地复合

$$\mathcal{R}_2 \circ \mathcal{R}_1 = \{(a_1, c_6), (a_2, c_2), (a_3, c_3), (a_4, c_6), (a_5, c_3)\} \subset A \times C.$$



4.3 等价关系

设 $\mathcal{R} \subset A \times B$ 为 A 与 B 的一个关系, 假设同时我们还有 $A = B$, 我们称 $\mathcal{R}$ 为 A 上的一个关系. 从集合的角度看, 关系 $\mathcal{R}$ 是 A 上有序点对的集合 $A \times A$ 的一个子集.

定义 4.3.1 (教材定义1.2.14)

我们称集合 A 上的一个关系 $\mathcal{R}$ 具有:

- (i) **自反性**, 若对于任意 $x \in A$, 我们有 $x\mathcal{R}x$,
(即 $(x, x) \in \mathcal{R}$);
- (ii) **传递性**, 若对于任意 $x, y, z \in A$, 我们有 $(x\mathcal{R}y) \wedge (y\mathcal{R}z) \implies x\mathcal{R}z$,
(即若 $(x, y), (y, z) \in \mathcal{R}$, 则有 $(x, z) \in \mathcal{R}$);
- (iii) **对称性**, 若对于任意 $x, y \in A$, 我们有 $x\mathcal{R}y \implies y\mathcal{R}x$,
(即若 $(x, y) \in \mathcal{R}$, 则 $(y, x) \in \mathcal{R}$).

定义 4.3.2

集合 A 上的一个关系 $\mathcal{R}$ 被称为是一个**等价关系**, 若其同时具有 (i) 自反性, (ii) 传递性以及 (iii) 对称性.

设 $\mathcal{R}$ 为集合 A 上的一个等价关系. 我们称元素 x 与 y **等价**, 若我们有 $x\mathcal{R}y$.

注 4.3.3.

我们通常会用记号 $\sim$ 来记一个等价关系.

注 4.3.4.

一个集合上的等价关系可以有很多种. 例如, 取

$$A = \{a_1, a_2, a_3\},$$

关系

$$\mathcal{R}_1 = \{(a_1, a_1), (a_2, a_2), (a_3, a_3)\},$$

以及

$$\mathcal{R}_2 = A \times A.$$

都给出 A 上的一个等价关系. 当集合上有更丰富的结构之后, 我们将更关注由这些结构给出的集合上的等价关系.

注 4.3.5.

我们定义集合 A 上的关系 $\mathcal{R}$ 具有

(iv) **反对称性**, 若对于任意 $x, y \in A$, 我们有 $(x\mathcal{R}y) \wedge (y\mathcal{R}x) \implies x = y$.

我们称关系 $\mathcal{R}$ 为一个**(偏)序关系**, 若其同时具有 (i) 自反性, (ii) 传递性以及 (iv) 反对称性.

如果对 A 中任意元素 $x \neq y$, 都有 $x\mathcal{R}y$ 或者 $y\mathcal{R}x$, 那么该偏序关系就是一个**全序关系**. 换句话说, 当我们的偏序关系中, 任意两个元素都是可以比较的, 我们就有了一个全序关系.

例 4.3.6.

我们先考虑一个熟悉的例子: 同余.

考虑集合 $\mathbb{Z}$. 我们定义 $\mathbb{Z}$ 上的关系如下:

$$m \sim n \Leftrightarrow 4 \mid m - n.$$

我们需要验证以上定义的关系确实是一个等价关系.

(i) 自反性, 任取 $m \in \mathbb{Z}$, 我们有 $m - m = 0$, 因此 $4 \mid m - m$, 我们有 $m \sim m$.

(ii) 传递性, 任取 $k, m, n \in \mathbb{Z}$, 满足 $k \sim m$ 以及 $m \sim n$, 由 $\sim$ 的定义, 我们知道

$$4 \mid k - m, \quad 4 \mid m - n.$$

因此存在 $p, q \in \mathbb{Z}$, 满足

$$k - m = 4p, \quad m - n = 4q.$$

因此

$$k - n = k - m + m - n = 4(p + q),$$

从而有 $4 \mid k - n$. 因此 $k \sim n$.

(iii) 对称性, 任取 $m, n \in \mathbb{Z}$, 满足 $m \sim n$, 由 $\sim$ 的定义, 我们有

$$4 \mid m - n,$$

因此存在整数 p , 满足 $m - n = 4p$. 取相反数可得

$$n - m = -4p = 4(-p).$$

从而有 $4 \mid n - m$. 因此 $n \sim m$.

例 4.3.7.

我们给一个抽象一点的例子. 考虑非空集合 A 和 B . 设

$$f: A \rightarrow B,$$

为一个映射.

我们定义 A 上的一个关系

$$a_1 \sim a_2 \Leftrightarrow f(a_1) = f(a_2).$$

下边验证 $\sim$ 是一个等价关系.

(i) 自反性, 任取 $a \in A$, 由 $f(a) = f(a)$, 我们有 $a \sim a$.

(ii) 传递性, 任取 $a_1, a_2, a_3 \in A$, 若 $a_1 \sim a_2$ 且 $a_2 \sim a_3$, 由 $\sim$ 的定义, 我们有

$$f(a_1) = f(a_2) = f(a_3).$$

因此 $a_1 \sim a_3$.

(iii) 对称性, 任取 $a_1, a_2 \in A$, 若 $a_1 \sim a_2$, 由 $\sim$ 的定义, 我们知道

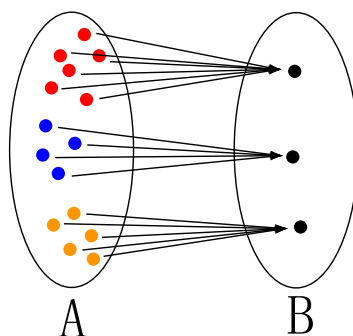
$$f(a_1) = f(a_2).$$

因此

$$f(a_2) = f(a_1),$$

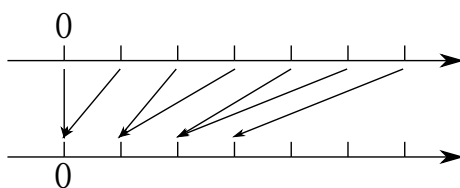
我们有 $a_2 \sim a_1$.

下边示意图中, 相同颜色代表的是有相同像的元素, 不同的颜色的元素有不同的像.



我们可以考虑一个更具体的例子.

$$\begin{aligned} \lfloor \cdot \rfloor : \mathbb{Z} &\rightarrow \mathbb{Z}, \\ n &\mapsto \left\lfloor \frac{n}{2} \right\rfloor. \end{aligned}$$



例 4.3.8.

我们再考虑一个几何的例子. 记 $\mathbb{E}$ 为平面. 我们可以将平面旋转或者平移. 为了更方便的描述这些作用, 我们可以选取一个点 O 作为原点, 来建立一个直角坐标系. 考虑坐标, 平面就可以和 $\mathbb{R}^2$ 等同起来.

任取 $P = (x, y)$, $\theta \in [0, 2\pi)$, 我们可以考虑将平面以 O 点为圆心逆时针旋转角度 $\theta \in \mathbb{R}$ (如果 $\theta < 0$, 则表示顺时针旋转), 记为 R_θ . 我们可以使用矩阵来表示这个作用:

$$R_\theta : \mathbb{R}^2 \rightarrow \mathbb{R}^2$$

$$\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

我们考虑以下 $\mathbb{R}^2$ 中的点之间的关系:

$$P \sim Q \Leftrightarrow \exists \theta \in \mathbb{R}, Q = R_\theta(P).$$

几何上看的话就是两个点之间相差一个绕着点 O 的旋转.

考虑旋转角度为 0, 我们有 $P \sim P$.

任给三个点 P, Q, T , 如果 $Q = R_\theta(P)$, $T = R_\eta(Q)$, 那么 $T = R_{\theta+\eta}(P)$. 换句话说, 先转角度 θ 在转角度 η 等同于直接转角度 $\theta + \eta$. 因此 $P \sim T$.

任给点 P, Q , 满足 $Q = R_\theta(P)$, 那么 $P = R_{-\theta}(Q)$. 因此 $\sim$ 满足对称性.

设 A 为一个集合, 并设 $\sim$ 为其上的一个等价关系.

定义 4.3.9 (教材定义1.2.15)

对于任意 $x \in A$, 我们称以下 A 的子集为 A 中的一个包含 x 的等价类:

$$\bar{x} := \{y \in A \mid x \sim y\}.$$

给定一个等价类 $\bar{x}$, 我们称其中的元素为其代表元.

注 4.3.10.

我们考虑之前介绍的等价关系例子中的对应的等价类.

例 4.3.6 中的包含 $m \in \mathbb{Z}$ 的等价类为模 4 的同余类 $4\mathbb{Z} + m$.

例 4.3.7 中包含 $x \in A$ 的等价类为原像集

$$f^{-1}(f(x)) := \{y \in A \mid f(y) = f(x)\}.$$

例 4.3.8 中包含一个点 P 的等价类为以点 O 为圆心的圆.

在以上的例子中我们注意到, 等价类似乎不依赖于代表元的选取, 并且不同的等价类两两不相交, 且并集为整个集合. 我们下边将证明这些观察都是正确的.

命题 4.3.11

设 $\sim$ 为 A 上的等价关系. 任取 $x, y \in A$, 满足 $x \sim y$, 我们有

$$\bar{x} = \bar{y}.$$

证明. 我们只需证明 $\bar{x} \subset \bar{y}$. 将 x 和 y 的角色互换重复该证明就可以得到另一个包含关系.

任取 $z \in \bar{x}$, 我们有 $z \sim x$. 由于 $x \sim y$, 因此由传递性, 我们知道 $z \sim y$, 从而有 $z \in \bar{y}$. 因此

$$\bar{x} \subset \bar{y}.$$

□

命题 4.3.12 (教材引理1.2.12(改))

取任意 $x, y \in A$, 我们有 $\bar{x} = \bar{y}$ 或 $\bar{x} \cap \bar{y} = \emptyset$. 进一步的, $\bar{x} = \bar{y}$ 当且仅当 $x \sim y$.

证明. 这个命题的证明主要使用的是等价关系的定义, 等价类的定义, 以及等价类的代表元的概念.

我们首先证明结论的第一部分. 设 $\bar{x} \cap \bar{y}$ 非空, 则存在

$$z \in \bar{x} \cap \bar{y}.$$

因此 $z \sim x$ 且 $z \sim y$. 由等价关系的传递性, 我们知道 $x \sim y$. 由之前的命题, 我们知道

$$\bar{x} = \bar{z} = \bar{y}.$$

因此, 我们有命题的第一部分.

我们继续证明命题的第二部分. 由之前的命题, 我们有若 $x \sim y$, 则 $\bar{x} = \bar{y}$. 反过来, 若 $\bar{x} = \bar{y}$, 我们有 $x \in \bar{y}$, 因此 $x \sim y$.

综上所述, 我们得到命题第二部分结论. □

定义 4.3.13 (教材定义1.2.17)

集合 A 中所有关于 $\sim$ 的等价类的空间

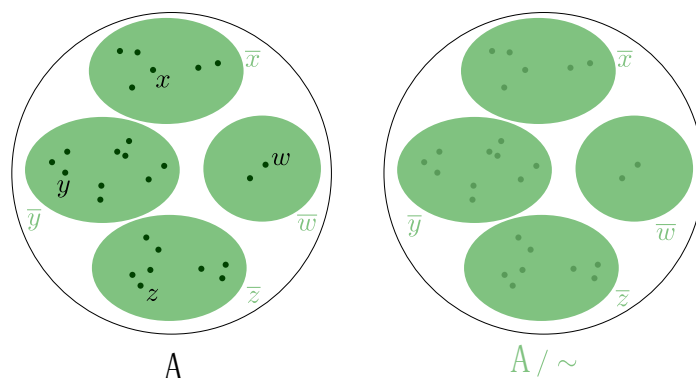
$$A/\sim := \{\bar{x} \mid x \in A\},$$

被称为 A 关于 $\sim$ 的商集合.

注 4.3.14.

在下边的示意图中, 左边表示原集合 A , 右边为商集

$$A/\sim = \{\bar{x}, \bar{y}, \bar{z}, \bar{w}\}.$$



定义 4.3.15

集合 A 的一个**分划**是一族 A 的非空子集 $\{A_\alpha\}_{\alpha \in I}$ 构成的集合 (I 为指标集), 满足

- (i) 任取不同的下标 $\alpha, \beta \in I$, 我们有 $A_\alpha \cap A_\beta = \emptyset$;
- (ii) $A = \bigcup_{\alpha \in I} A_\alpha$.

注 4.3.16.

当我们讨论多个同类型的物体时, 为了区分, 我们通常会给不同的物体做个标记. 例如, 我们考虑集合 A 中的 3 个元素的时候, 我们会用 x, y 和 z 来记不同的元素. 但是当我们考虑更多的元素的时候, 这样的记号就会比较复杂. 我们通常会使用一个非空集合作为指标集, 也就是下标的集合, 然后用下标来区分不同的元素. 例如, 我们要考虑 10 个 A 中的元素时, 我们可以记

$$x_1, x_2, \dots, x_{10}.$$

甚至更一般的, 我们考虑 A 中 $n \in \mathbb{N}^*$ 个元素的时候, 我们可以记 $x_1, \dots, x_n$.

以上讨论是关于有限多个物体. 我们当然可以考虑无穷多个物体. 分析中, 我们已经接触过, 不同的无穷集的大小(即集合的势)可能是不同的. 因此我们会将用一个符号来记所有的下标的集合. 例如, 我们在考虑 A 中的元素构成的子集时, 可以记

$$\{x_\alpha \mid \alpha \in I\}, \text{ 或者 } \{x_\alpha\}_{\alpha \in I}.$$

这里的 I 的势可以是有限, 可以是可数无穷, 或者更一般的势. 方便我们更灵活的讨论.

注 4.3.17.

记 A 为一个集合, 并记其幂集(A 的子集构成的集合)为:

$$\mathcal{P}(A) := \{A \text{ 的子集}\}.$$

例如, 若

$$A = \{0, 1, 2\},$$

则

$$\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}.$$

由集合分划的定义, 我们知道任意 A 的分划都是 $\mathcal{P}(A)$ 的子集

命题 4.3.12 告诉我们, 等价关系诱导 A 上的一个分划, 每个子集是一个等价类. 相反的, 我们也可以从一个分划 $\{A_\alpha\}_{\alpha \in I}$ 出发, 定义一个 A 上的等价关系:

- $x \sim y$, 当且仅当存在一个 $\alpha \in I$, 满足 $x \in A_\alpha$ 且 $y \in A_\alpha$.

命题 4.3.18 (教材定理1.2.16)

给定一个非空集合 A , 则 A 上的等价关系和 A 的分划一一对应. 更详细一些的表述如下: 以下两个集合之间存在一一对应

$$\{\mathcal{R} \subset A \times A \mid \mathcal{R} \text{ 是一个等价关系}\} \xleftrightarrow{1:1} \{A \subset \mathcal{P}(A) \mid A \text{ 是一个分划}\}$$

注 4.3.19.

我们考虑等价关系的时候, 作为一个关系, 我们将其看作是 $A \times A$ 的子集. 我们在定义等价关系的时候通常利用其他的工具, 不同方法定义出来的等价关系有可能是相同的. 例如, 我们可以考虑 A 上任意一个等价关系 $\sim$ 给出的一个分划, 然后利用分划在 A 上定义一个等价关系. 这两个等价关系是相同的.

设 $\{A_\alpha\}_{\alpha \in I}$ 为 A 的一个分划.

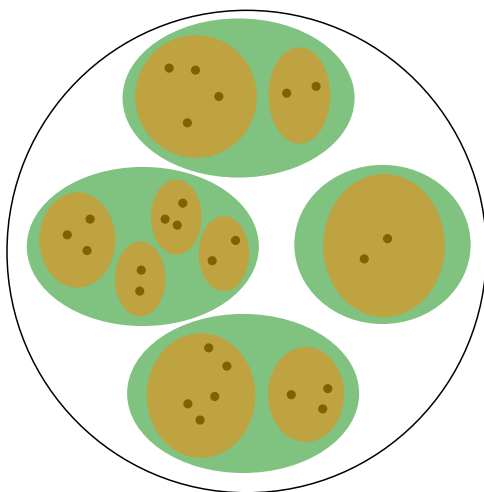
定义 4.3.20

我们称 A 的一个分划 $\{B_\beta\}_{\beta \in J}$ 比分划 $\{A_\alpha\}_{\alpha \in I}$ **更细**, 若我们有

- 对任意 $\beta \in J$, 存在 $\alpha \in I$, 满足 $B_\beta \subset A_\alpha$.

注 4.3.21.

换句话说, 分划 $\{B_\beta\}_{\beta \in J}$ 可以由先对 A 做分划 $\{A_\alpha\}_{\alpha \in I}$, 再对每一个 A_α 做分划得到的. 下边给出一个集合的两个分划的示意图. 其中**橙色**的分划比**绿色**的分划更细.



设 $\sim$ 为 A 上的一个等价关系.

定义 4.3.22 (教材定义1.2.18)

我们定义 A 到商空间 $A/\sim$ 的**自然映射**为:

$$\begin{aligned}\pi: A &\rightarrow A/\sim \\ x &\mapsto \pi(x) := \bar{x}.\end{aligned}$$

思考 4.3.23

验证自然映射的定义是良定义.

定理 4.3.24

设 $\sim$ 为 A 上的一个等价关系. 任取集合 B 以及映射 $f: A \rightarrow B$. 若 f 满足

- 对于 A 中任意两个等价元素 x 和 y , 我们都有 $f(x) = f(y)$,

那么, 我们可以找到唯一的一个映射 $\bar{f}: A/\sim \rightarrow B$, 使得 $f = \bar{f} \circ \pi$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \pi \downarrow & \nearrow \exists! \bar{f} & \\ A/\sim & & \end{array}$$

注 4.3.25.

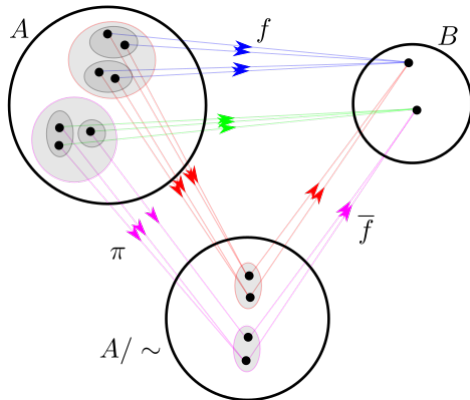
我们可以在 A 上定义另外一个等价关系:

- 我们称 $x \sim_B y$ 当且仅当 $f(x) = f(y)$.

也即, 两个元素等价当且仅当它们在 f 下的像相同. 定理中的条件可以被替换为下边这个,

- 对任意 A 中的元素 x 和 y , 若 $x \sim y$, 则 $x \sim_B y$.

从分划的角度看, 这意味着 $\sim$ 诱导的 A 的分划比 $\sim_B$ 诱导的 A 的分划更细.

**注 4.3.26.**

后边提到的(群, 环, 模等)同态基本定理都是这个定理在不同情形下的表述. 到时我们会从这个角度详细说明.

4.4 (偏)序关系

4.4.1 定义

在讨论自然数, 整数, 有理数, 实数的时候, 我们可以做的一件事情就是比大小. 记 $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ 或者 $\mathbb{R}$. 通常我们都是比较两个数的大小, 因此通过比较大小, 我们可以建立一个 A 上的关系. 进一步地, 我们会注意到这个关系满足以下几个条件:

- (i) 任取 $a \in A$, 我们有 $a \leq a$.

- (ii) 任取 $a, b \in A$, 若 $a \leq b$ 且 $b \leq a$, 我们有 $a = b$.
- (iii) 任取 $a, b, c \in A$, 若 $a \leq b$ 且 $b \leq c$, 我们有 $a \leq c$.
- (iv) 任取 $a, b \in A$, 则 $a < b$, $a = b$ 以及 $b < a$ 有且仅有一个成立.

我们可以将 (i), (ii) 和 (iii) 推广到对一般集合的讨论中, 就得到了偏序关系. 第 (iv) 点只是在告诉我们集合 A 中任意两个元素都可以比较. 下边我们给出一个严格的定义:

定义 4.4.1

任取非空集合 A , 记 $\preceq$ 为 A 上的一个关系. 如果 $\preceq$ 满足

- (i) (自反性) 任取 $a \in A$, 我们有 $a \preceq a$.
- (ii) (反对称性) 任取 $a, b \in A$, 若 $a \preceq b$ 且 $b \preceq a$, 我们有 $a = b$.
- (iii) (传递性) 任取 $a, b, c \in A$, 若 $a \preceq b$ 且 $b \preceq c$, 我们有 $a \preceq c$.

我们称 $\preceq$ 为 A 上的一个(偏)序关系.

任取 $a, b \in A$, 我们记 $a \prec b$, 若 a 和 b 满足:

$$a \preceq b \text{ 且 } a \neq b.$$

若 $\preceq$ 进一步满足 A 中任意两个元素可比较:

- (iv) 任取 $a, b \in A$, 则 $a \prec b$, $a = b$ 以及 $b \prec a$ 有且仅有一个成立.

我们称 $\prec$ 是 A 上的一个全序关系.

注 4.4.2.

我们有时也会使用 $\succ$ 或者 $\succeq$ 作为 $>$ 和 $\geq$ 的推广.

4.4.2 子集间的偏序关系

注意到以上包含关系可以被用来给出一个集合的所有子集构成的集合上的偏序关系. 任取 A 是一个集合, 我们考虑其所有子集构成的集合:

$$\mathcal{P}(A) := \{B \mid B \subset A\}.$$

我们称 $\mathcal{P}(A)$ 为 A 的幂集.

我们在 $\mathcal{P}(A)$ 上定义如下关系: 任取 A 的子集 B 和 C , 定义

$$B \preceq C \Leftrightarrow B \subset C.$$

通过直接验证, 这个关系满足自反性, 反对称性和传递性, 因此是一个偏序关系. 一般情况下, 一个集合中不是任意两个子集都可以比较. 因此通常这个偏序关系不是全序关系. ($\emptyset$ 和 $\{a\}$ 是两个例外)

当我们开始考虑的集合 A 有某个代数结构之后, 我们也会考虑 A 的具有此类代数结构的子集. 当然我们希望这类子集上的代数结构是在 A 上的结构限制下得到的. 我们可以将之前讨论的偏序关系 $\preceq$ 限制在这类子集上, 从而给出这类子集构成的集合上的一个偏序关系.

4.4.3 极大和最大

定义 4.4.3

记 A 是一个非空集合, $\preceq$ 是 A 上的一个序关系. 任取 $a \in A$, 我们称 a 为 A 关于 $\preceq$ 的**极大元**, 若任取 $b \in A$, 满足 $a \preceq b$, 都有 $a = b$.

注意到, $\preceq$ 是 A 的一个序关系, 但不一定 A 中所有元素之间都可以比较. 因此 A 中关于 $\preceq$ 的极大元不一定是唯一的.

例 4.4.4.

记 $A = \{a, b, c, d\}$. 考虑 A 的幂集 $\mathcal{P}(A)$. 我们可以把之前利用包含关系给出的偏序关系限制在

$$\Omega = \mathcal{P}(A) \setminus \{A\},$$

上. 我们可以直接验证 Ω 上有以下极大元:

$$\{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}.$$

定义 4.4.5

记 A 是一个非空集合, $\preceq$ 是 A 上的一个序关系. 记 $a \in A$, 满足任取 $b \in A$, 我们有 $b \preceq a$, 我们称 a 是 A 的**最大元**.

利用序关系的反对称性, 我们可以证明一个集合若存在最大元, 则其唯一.

例 4.4.6.

我们考虑 $\mathbb{N}$, 任取 $a, b \in \mathbb{N}$, 我们定义

$$a \preceq b \Leftrightarrow a \mid b.$$

我们可以直接验证 $\preceq$ 是 $\mathbb{N}$ 上的一个偏序关系, 不是全序关系. 另外, 0 为 $\mathbb{N}$ 的最大元.

类似地, 我们也可以定义一个非空集合关于某个偏序关系的极小元和最小元.

第五章 集合上的运算

设 A 为一个集合. 取 $n \in \mathbb{N}^*$. 我们记 A^n 为集合 A 与自己的笛卡尔积 n 次:

$$A^n = \underbrace{A \times \cdots \times A}_{n \text{ 个}}$$

定义 5.0.1

集合 A 上的一个 n -元运算是一个从 A^n 到 A 的映射.

注 5.0.2.

一个 A 上的 n -元运算就像一个 A 上的计算器, 输入是 A 中 n 个元素, 输出是一个 A 中的元素.

我们以下主要考虑 A 上的二元运算. 设 $*$: $A \times A \rightarrow A$ 为 A 上的一个二元运算.

定义 5.0.3 (教材定义1.1.2)

我们称二元运算 $*$ 满足

- (i) **结合率**, 若对于任意 $x, y, z \in A$, 我们有 $(x * y) * z = x * (y * z)$;
- (ii) **交换律**, 若对于任意 $x, y \in A$, 我们有 $x * y = y * x$.

例 5.0.4.

我们之前考虑的实数上的加法和乘法运算都满足这两个例子. 但在更一般的情况下, 这两个性质并不一定会被满足. 例如, 我们仍考虑实数集合, 并定义以下二元运算:

$$\begin{aligned} * : \mathbb{R} \times \mathbb{R} &\rightarrow \mathbb{R}, \\ (x, y) &\mapsto x * y := 2x + y \end{aligned}$$

下边我们通过直接计算来检验 $*$ 是否满足结合律和交换律. 首先考虑结合律, 设 $x, y, z \in \mathbb{R}$, 我们有

$$\begin{aligned} (x * y) * z & & x * (y * z) \\ = (2x + y) * z & & = x * (2y + z) \\ = 4x + 2y + z & & = 2x + 2y + z \end{aligned}$$

因此运算 $*$ 不满足结合律.

下边我们继续验证交换律

$$x * y = 2x + y \quad y * x = 2y + x$$

因此运算 $*$ 也不满足交换律.

注 5.0.5.

通过不断迭代二元运算 $*$, 对任意 $n \geq 2$, 对于任意 $x_1, \dots, x_n \in A$, 我们可以定义

$$*^{(n)}(x_1, \dots, x_n) := (\cdots((x_1 * x_2) * x_3) * \cdots * x_n).$$

我们可以验证 $*^{(n)}$ 为 A 上的一个 n -元运算. 给定 A 中任意 n 个元素, 我们通过在每一步中对第一个和第二个元素做 $*$ -运算, 最终得到这 n 个元素在 $*^{(n)}$ -运算下的值.

若 $*$ 满足结合律, 每次我们在做 $*$ -运算时, 就不必总考虑第一个和第二个元素. 我们只需每次挑相邻位置上的两个元素做 $*$ -运算就可以. 例如, 若 $*$ 满足结合律, 取 $n = 4$, 我们有

$$(((x_1 * x_2) * x_3) * x_4) = ((x_1 * x_2) * (x_3 * x_4)).$$

我们可以将其记作 $x_1 * x_2 * x_3 * x_4$.

若 $*$ 满足结合律的同时也满足交换律, 则我们有对于任意 $i_1, \dots, i_n \in \mathbb{N}$ 满足

$$\{i_1, \dots, i_n\} = \{1, \dots, n\},$$

我们都有

$$x_{i_1} * \cdots * x_{i_n} = x_1 * \cdots * x_n.$$

例如, 实数集 $\mathbb{R}$ 上的加法运算 $+$ 为一个满足结合律和交换律的二元运算, 取 $n = 4$, 我们有

$$1 + \sqrt{2} + \pi + (-1) = \sqrt{2} + \pi + 1 + (-1).$$

通过先计算 $1 + (-1)$, 我们可以简化运算.

思考 5.0.6

若 $*$ 仅满足交换律, 关于运算 $*^{(n)}$, 我们可以说什么?

定义 5.0.7

我们称 A 中的元素 x 和 y 关于 $*$ 交换, 若其满足 $x * y = y * x$.

例 5.0.8.

设 $k \in \mathbb{N}^*$. 考虑实数上的 k 阶方阵的集合 $\text{Mat}_k(\mathbb{R})$ 及其上的矩阵乘法运算. 我们考虑 n 个 k 阶方阵 $M_1, \dots, M_n$ 的乘积:

$$M_1 \cdots M_n.$$

由于矩阵乘法运算满足结合律, 我们计算时, 每一步可以挑选任意一对相邻的方阵来计算它们的乘积.

这个二元运算不满足交换律, 例如:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 2 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix} \quad \begin{bmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 0 & \frac{1}{2} \end{bmatrix}.$$

因此在做乘法的时候我们不能任意交换矩阵的顺序. 另一方面, 纯量矩阵

$$\begin{bmatrix} \lambda & 0 & \cdots & 0 \\ 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda \end{bmatrix} (\lambda \in \mathbb{R})$$

和任意矩阵关于这个运算交换, 例如,

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

定义 5.0.9 (教材定义1.1.4)

一个 A 中的元素 e , 被称为(关于运算 $*$ 的)

- (i) **左幺元**, 若对于任意 $x \in A$, 我们有 $e * x = x$;
- (ii) **右幺元**, 若对于任意 $x \in A$, 我们有 $x * e = x$;
- (iii) **幺元**, 若对于任意 $x \in A$, 我们有 $e * x = x * e = x$, 也即其同时是左幺元和右幺元.

例 5.0.10.

我们考虑 $\mathbb{R}$ 上的二元运算 $x * y := 2x + y$. 这里 0 是一个左幺元, 但不是右幺元, 因为任取 $x \neq 0$, 我们有

$$x * 0 = 2x \neq x.$$

命题 5.0.11

若二元运算 $*$ 满足交换律, 那么左幺元(如果存在的话)也是右幺元.

证明. 考虑集合 A 上的二元运算 $*$. 设 $*$ 满足交换律, 并由左幺元 $e \in A$. 任取 $x \in A$, 我们有

$$x * e = e * x = x.$$

因此 e 也是右幺元. □

定义 5.0.12 (教材定义1.1.10)

设 A 有关于运算 $*$ 的幺元 e . 我们称 A 中的元素 y 为 x (关于运算 $*$ 的)

- (i) **左逆元**, 若 $y * x = e$;
- (ii) **右逆元**, 若 $x * y = e$;
- (iii) **逆元**, 若 $y * x = x * y = e$, 也即其同时是左逆元和右逆元.

若一个元素 x 有逆元, 我们称之为**可逆元素**, 并将其逆元记为 x^{-1} .

例 5.0.13 (教材例1.1.7, 思考题1.1.11, 练习1.1.3).

我们可以考虑 $\mathbb{N}$ 上的取值在 $\mathbb{N}$ 中的映射的集合:

$$\mathcal{F}(\mathbb{N}, \mathbb{N}) := \{f : \mathbb{N} \rightarrow \mathbb{N} \text{ 为一个映射}\}.$$

考虑 $\mathcal{F}(\mathbb{N}, \mathbb{N})$ 上的复合运算. 考虑恒等映射:

$$\begin{aligned} \iota : \mathbb{N} &\rightarrow \mathbb{N}, \\ n &\mapsto n \end{aligned}$$

我们可以验证 ι 是 $\mathcal{F}(\mathbb{N}, \mathbb{N})$ 上的幺元. 我们考虑映射

$$\begin{aligned} f : \mathbb{N} &\rightarrow \mathbb{N} \\ n &\mapsto n + 1 \end{aligned}$$

以及映射

$$\begin{aligned} g : \mathbb{N} &\rightarrow \mathbb{N} \\ n &\mapsto \max\{0, n - 1\} \end{aligned}$$

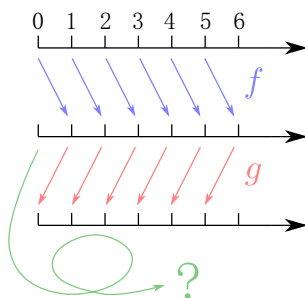
任取 $n \in \mathbb{N}$, 我们有

$$(g \circ f)(n) = g(f(n)) = g(n + 1) = n = \iota(n).$$

因此 $g \circ f = \iota$, g 为 f 左逆元. 注意到 f 没有右逆元. 注意到 ι 的值域有 0, 而对任意 $h \in \mathcal{F}(\mathbb{N}, \mathbb{N})$ 和任意 $n \in \mathbb{N}$, 我们有

$$(f \circ h)(n) \in \mathbb{N} \setminus \{0\}.$$

因此不存在 f 有右逆元.



思考 5.0.14 (习题1.1.3)

以上例子中的映射 f 的左逆元是否唯一? 为什么?

命题 5.0.15

- (i) 任取 $x \in A$, 若其逆元 x^{-1} 存在, 则 x 与 x^{-1} 关于运算 $*$ 交换.
- (ii) 若二元运算 $*$ 满足交换律, 那么对任意有左逆元的元素, 其左逆元也是其右逆元, 因此是其逆元.

考虑集合 A 及其上得二元运算 $*_A$ 和 B 及其上得二元运算 $*_B$.

定义 5.0.16

我们称一个映射 $\mathcal{R} : A \rightarrow B$ 为从 $(A, *_A)$ 到 $(B, *_B)$ 的**同态映射**, 若其满足以下条件:

- 对于任意 $x, y \in A$, 我们有 $\mathcal{R}(x *_A y) = \mathcal{R}(x) *_B \mathcal{R}(y)$.

若在此基础上, 映射 $\mathcal{R}$ 为双射, 我们称 $\mathcal{R}$ 为从 $(A, *_A)$ 到 $(B, *_B)$ 的**同构映射**. 此时, 我们称 $(A, *_A)$ 和 $(B, *_B)$ **同构**.

例 5.0.17.

我们令 $(A, *_A) = (\mathbb{R}, +)$, 以及 $(B, *_B) = (\mathbb{R}_{>0}, \cdot)$. 考虑指数映射

$$\mathcal{R} = \exp : \mathbb{R} \rightarrow \mathbb{R}_{>0},$$

则有任取 $x, y \in \mathbb{R}$,

$$\exp(x + y) = \exp x \cdot \exp y.$$

因此 $\exp$ 映射是一个同态. 另一方面, 该映射也是一个双射, 因此 $\exp$ 为 $(\mathbb{R}, +)$, 以及 $(\mathbb{R}_{>0}, \cdot)$ 之间的同构.

(后边当我们介绍完群的概念之后, 我们可以验证 $(\mathbb{R}, +)$ 和 $(\mathbb{R}_{>0}, \cdot)$ 都为群, 且 $\exp$ 为这两个群之间的群同构.)

命题 5.0.18

若 $\mathcal{R}$ 为一个从 $(A, *_A)$ 到 $(B, *_B)$ 的同构, 那么其逆映射 $\mathcal{R}^{-1}$ 为一个从 $(B, *_B)$ 到 $(A, *_A)$ 的同构.

设 A_1 为 A 的一个子集. 设 $*$ 为 A 上的一个运算.

定义 5.0.19

我们称 A_1 对 A 上的运算 $*$ **封闭**, 若其满足以下条件:

- 对任意 $a, b \in A_1$, 我们有 $a * b \in A_1$.

注 5.0.20.

换句话说, 映射

$$* : A \times A \rightarrow A,$$

在 $A_1 \times A_1 \subset A \times A$ 上的限制诱导了 A_1 上的一个二元运算.

例 5.0.21.

我们考虑整数集合 $\mathbb{Z}$, 及其上的加法运算. 以下 $\mathbb{Z}$ 的子集均对该运算封闭:

$$\mathbb{N}, \mathbb{N}^*, 2\mathbb{Z}.$$

相反, 以下 $\mathbb{Z}$ 的子集对加法运算不封闭

$$\{0, 1\}, 2\mathbb{Z} \cup \{1\}.$$

第二部分

群理论

第六章 群

6.1 定义

考虑一个集合 G , 设 $*$ 为 G 上的一个二元运算.

定义 6.1.1 (教材定义 1.1.14)

我们称二元组 $(G, *)$ 为一个**群**, 若其满足:

(i) 二元运算 $*$ 满足结合律, 即对于任意 $a, b, c \in G$, 我们有

$$(a * b) * c = a * (b * c);$$

(ii) 存在幺元, 即存在元素 $e \in G$, 对于任意 $a \in G$, 我们有

$$e * a = a * e = a;$$

(iii) 任意 $a \in G$ 都有逆元, 即对于任意 $a \in G$, 存在 $a^{-1} \in G$, 满足

$$a^{-1} * a = a * a^{-1} = e.$$

注 6.1.2.

记号 G 来自群的英文 Group (另一个常用记号 Γ 相当于希腊字母中的 G).

定义 6.1.3 (教材定义 1.1.4)

若二元组 $(G, *)$ 只满足群结构条件 (i), 我们称之为一个**半群**.

若一个半群结构 $(G, *)$ 同时也满足群结构条件 (ii), 我们称之为一个**幺半群**.

例 6.1.4.

所有整数的集合 $\mathbb{Z}$ 关于加法构成一个群.

所有非零自然数的集合 $\mathbb{N}^*$ 关于加法构成一个半群.

所有自然数的集合 $\mathbb{N}$ 关于加法构成一个幺半群.

思考 6.1.5

整数集 $\mathbb{Z}$ 关于乘法是一个群么? 为什么?

例 6.1.6.

我们称集合

$$A = \{1, 2, 3, 4, 5\},$$

到自己的双射为一个 A 上的一个**置换**. 集合 A 上所有置换构成的集合记为 $S(A)$.

由之前对双射以及映射的复合的讨论, 我们知道两个置换的复合仍是置换. 因此我们可以在 $S(A)$ 上定义复合运算. $S(A)$ 关于这个复合运算构成群.

更一般地, 任意集合上所有的双射构成的集合与其上的复合运算构成群.

例 6.1.7.

考虑 $\mathbb{R}$ 上所有取值在 $\mathbb{R}$ 中的函数的集合

$$\mathcal{F}(\mathbb{R}, \mathbb{R}) := \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ 为一个函数}\}.$$

我们可以在上边定义加法运算. 任取 f 和 g 两个函数, 我们定义:

$$\begin{aligned} f + g : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto f(x) + g(x). \end{aligned}$$

可以验证 $\mathcal{F}(\mathbb{R}, \mathbb{R})$ 关于加法运算构成一个群.

类似地, 我们可以定义函数之间地乘法. 任取 f 和 g 两个函数, 我们定义:

$$\begin{aligned} f \cdot g : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto f(x) \cdot g(x). \end{aligned}$$

可以验证 $\mathcal{F}(\mathbb{R}, \mathbb{R})$ 关于乘法运算构成一个幺半群.

此外我们还可以考虑复合运算. 任取 f 和 g 两个函数, 我们定义:

$$\begin{aligned} f \circ g : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto f(g(x)). \end{aligned}$$

可以验证 $\mathcal{F}(\mathbb{R}, \mathbb{R})$ 关于复合运算构成一个幺半群.

思考 6.1.8

为什么 $(\mathcal{F}(\mathbb{R}, \mathbb{R}), \cdot)$ 和 $(\mathcal{F}(\mathbb{R}, \mathbb{R}), \circ)$ 不是群? 它们的幺元是什么?

例 6.1.9 (教材例1.1.9).

任取集合 A , 我们可以在其幂集 $\mathcal{P}(A)$ 上定义二元运算 $\cup$ 和二元运算 $\cap$. 利用定义, 我们可以验证 $(\mathcal{P}(A), \cup)$ 和 $(\mathcal{P}(A), \cap)$ 都是幺半群. 例如, 取并集的运算满足下列性质:

(i) 任取 $A_1, A_2, A_3 \in \mathcal{P}(A)$, 我们有

$$(A_1 \cup A_2) \cup A_3 = A_1 \cup (A_2 \cup A_3).$$

(ii) 任取 $A_1 \in \mathcal{P}(A)$, 我们有

$$A_1 \cup \emptyset = \emptyset \cup A_1 = A_1.$$

(iii) 对任意 $A_1, A_2 \in \mathcal{P}(A)$, 设 $A_1 \neq \emptyset$, 则有

$$\emptyset \subsetneq A_1 \subset A_1 \cup A_2.$$

思考 6.1.10

$(\mathcal{P}(A), \cup)$ 和 $(\mathcal{P}(A), \cap)$ 的么元分别是什么? 是否存在集合 A , 使得 $(\mathcal{P}(A), \cup)$ 或 $(\mathcal{P}(A), \cap)$ 为群?

注 6.1.11.

若二元运算 $*$ 没有歧义, 我们通常将 $(G, *)$ 简记为 G . 为了记号简便, 在没有歧义的时候, 我们省略 $*$, 记 $ab = a * b$.

设 G 为一个群.

定义 6.1.12 (教材定义 1.1.14)

若 G 的群运算满足交换律, 即对于任意 $a, b \in G$, 我们有

$$ab = ba,$$

那么我们称 G 为一个**交换群**. 若群 G 不交换, 我们称之为一个**非交换群**.

注 6.1.13.

注意到单位元与所有元素都交换. 每个元素也都与其逆元交换. 这里的非交换的意思是存在至少一对元素 a 和 b , 满足 $ab \neq ba$.

例 6.1.14.

整数考虑加法运算 $(\mathbb{Z}, +)$ 是一个交换群.

非零实数集合考虑乘法运算 $(\mathbb{R}^*, \cdot)$ 是一个交换群

复数域上向量空间考虑向量加法运算 $(V, +)$ 是一个交换群.

例 6.1.15.

实数上二阶可逆矩阵集合考虑矩阵乘法 $GL(2, \mathbb{R})$ 是非交换群.

考虑 $\mathbb{R}$ 到自己的双射的集合

$$\{f: \mathbb{R} \rightarrow \mathbb{R} \text{ 为双射}\},$$

以及映射的复合运算. 这是一个非交换群. 例如, 我们考虑以下两个运算:

$$\begin{array}{ll} f: \mathbb{R} \rightarrow \mathbb{R} & g: \mathbb{R} \rightarrow \mathbb{R} \\ x \mapsto x + 1 & x \mapsto 2x \end{array}$$

任取 $x \in \mathbb{R}$, 我们有

$$\begin{aligned} (f \circ g)(x) &= f(g(x)) = f(2x) = 2x + 1, \\ (g \circ f)(x) &= g(f(x)) = g(x + 1) = 2x + 2. \end{aligned}$$

因此 $f \circ g \neq g \circ f$.

这个实际上是更一般的 n 维线性空间 $\mathbb{R}^n$ 上的仿射变换的特殊情形. f 的是平移的一个例子, g 是放缩的一个例子.

玩魔方的时候, 我们可以观察到(观察什么?), 魔方所有变化构成一个非交换群.

我们下边给出一些关于逆元和单位元的基本性质 (可以和线性空间的 0 向量以及向量的逆的性质做一个对比)

命题 6.1.16 (教材命题 1.1.13)

- (i) 群 G 的单位元唯一, 即若 e_1 和 e_2 都是 G 的单位元, 则有 $e_1 = e_2$.
- (ii) 群 G 中每个元素 $g \in G$ 的逆元唯一, 即若 h_1 和 h_2 都是 g 的逆元, 则有 $h_1 = h_2$.

证明. (练习)

□

定义 6.1.17 (教材定义 1.1.14)

记 G 为一个群. 如果 G 作为集合有限, 我们称 G 为一个**有限群**, 并将其势 $|G|$ 称为 G 的**阶**. 特别的, 如果 G 只有一个么元, 我们称 G 为**平凡群**.
如果 G 作为集合是一个无限集, 则称 G 是一个**无限群**.

有限群的群表

考虑一个有限群

$$G = \{a_1, \dots, a_n\}.$$

我们使用如下方式将 G 中元素两两相乘的结果列出 ((i, j) 位置上为 $a_i a_j$):

	a_1	$\cdots$	a_n
a_1	$a_1 a_1$	$\cdots$	$a_1 a_n$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n	$a_n a_1$	$\cdots$	$a_n a_n$

我们将这个表称为 G 的**群表**. 注意到, 我们得到了一个参数取值在 G 中的一个 $n \times n$ 方阵:

$$M(G) = \begin{bmatrix} a_1 a_1 & \cdots & a_1 a_n \\ \vdots & \ddots & \vdots \\ a_n a_1 & \cdots & a_n a_n \end{bmatrix}$$

命题 6.1.18

一个有限群 G 交换当且仅当 $M(G)$ 对称.

例 6.1.19.

我们考虑

$$G = \{\text{奇}, \text{偶}\},$$

如下定义 G 上的一个二元运算(记为 "+"):

$$\begin{aligned} \text{奇} + \text{奇} &= \text{偶} + \text{偶} = \text{偶}, \\ \text{偶} + \text{奇} &= \text{奇} + \text{偶} = \text{奇}. \end{aligned}$$

可以验证

- (i) 以上运算满足结合律. (例如, $(\text{奇} + \text{偶}) + \text{偶} = \text{奇} + \text{偶} = \text{奇} + (\text{偶} + \text{偶})$)
- (ii) "偶"为 G 关于加法运算的单位元.
- (iii) "偶" 的逆元为 "偶", "奇"的逆元为奇.
- (iv) 以上运算满足交换律.

因此 G 关于 "+" 构成一个交换群. 我们有如下群表

	偶	奇
偶	偶	奇
奇	奇	偶

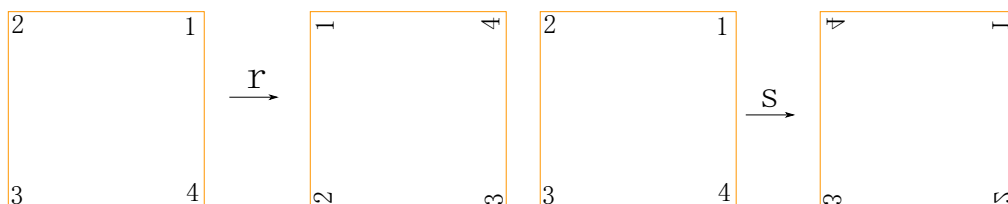
例 6.1.20.

我们考虑二面体群 D_4 (见练习). 我们记 r 和 s 为平面到自己的映射. 其中 r 为平面绕原点顺时针旋转 $\pi/2$, s 为平面沿着直线 $x = y$ 做反射. 这两个映射满足如下条件:

$$\begin{aligned} r^4 &= s^2 = id, \\ rs &= sr^3. \end{aligned}$$

(这里我们省略映射复合使用的 $\circ$.) 二面体群 D_4 为所有 s 和 r 可能的有限复合. 因此我们有

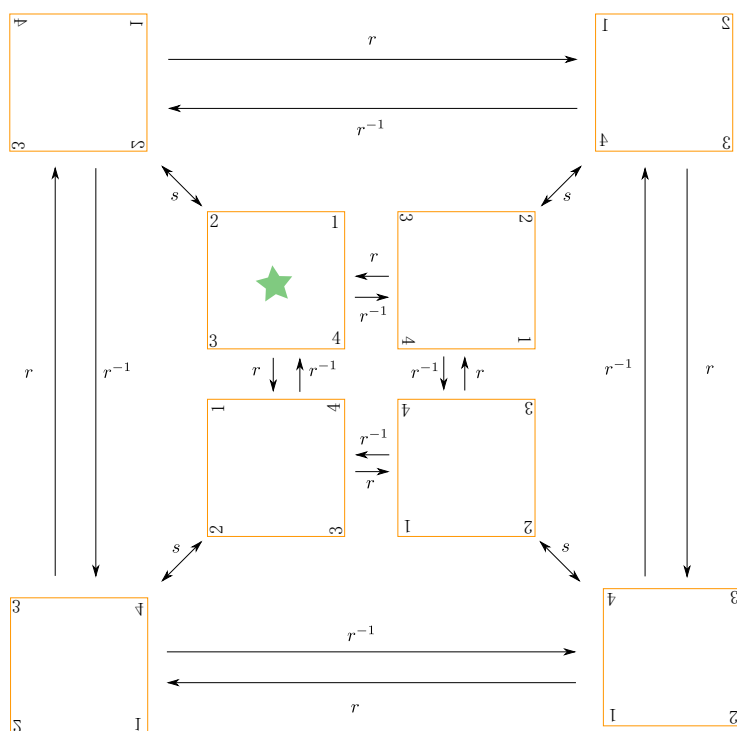
$$D_4 = \{id, r, r^2, r^3, s, rs, r^2s, r^3s\}$$



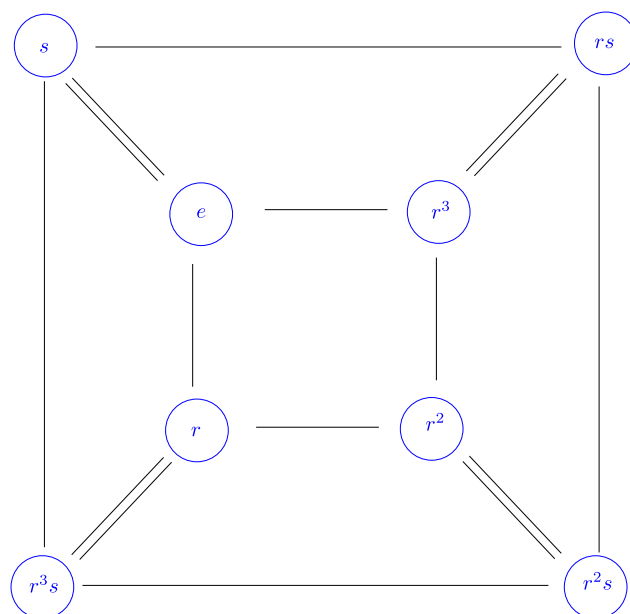
我们可以验证 D_4 关于映射的复合构成一个有限非交换群. 我们进一步有如下群表

	id	r	r^2	r^3	s	rs	r^2s	r^3s
id	id	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	id	rs	r^2s	r^3s	s
r^2	r^2	r^3	id	r	r^2s	r^3s	s	rs
r^3	r^3	id	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	id	r^3	r^2	r
rs	rs	s	r^3s	r^2s	r	id	r^3	r^2
r^2s	r^2s	rs	s	r^3s	r^2	r	id	r^3
r^3s	r^3s	r^2s	rs	s	r^3	r^2	r	id

由于这个群是一个正方形的对称群的一部分. 关于这个群的结构, 我们可以进一步通过观察这个群在正方形上的作用来了解.



如果我们将标星的看作起点, 那么其他的情形都可以唯一的对应一个群元素, 我们得到由"生成元" r 和 s 给出的 D_4 的 "Cayley 图":



Cayley 图中的点都是群的元素, 两个元素 u 和 v 由一条线相连, 当且仅当 vu^{-1} 是一个生成元. 这里 s 与 e 之间连了两条线是由于 s 是一个二阶元素. Cayley 图是将一个群图形化的方法, 可以反映群的很多信息, 比如其中任何一个路径都会给我们一个生成元构成的词. 当这个路径是一个回路的时候, 这个词等于幺元 e . 例如, 我们从 e 出发右乘 r 到达 r 点, 继续下去, 我们依次经过 r^2, r^3 , 然后右乘四次 r 后回到 e . 这代表 $r^4 = e$.

另一方面, Cayley 图也可以给我们一种利用几何工具研究群的方法. 例如, 我们可以令所有边的长度都是 1, 由此, 我们可以定义任意两个元素之间的距离. 这在构造是研究某些特殊类型的群(双曲群)的基本工具.

思考 6.1.21

如何从 D_4 的群表中看出 D_4 非交换?

我们注意到在这个群表中, 每一行都是 D_4 的元素的重新排列(对比第一行的顺序). 每一行都由 D_4 所有元素左乘相同的元素得到的. 类似地, 每一行都是 D_4 的元素的重新排列(对比第一列的顺序). 每一列都是由 D_4 所有的元素右乘相同的元素得到的. 我们考虑一般群 G , 并给出如下定义.

定义 6.1.22 (教材定义 1.4.9)

记 G 为一个群. 考虑群运算:

$$\begin{aligned} \cdot : G \times G &\rightarrow G \\ (a, b) &\mapsto ab \end{aligned}$$

在以上映射中固定左边的元素为一个群元素 $a \in G$, 我们得到了以下 a 的左平移映射:

$$\begin{aligned} L_a : G &\rightarrow G \\ b &\mapsto L_a(b) := ab \end{aligned}$$

同样地, 我们也可以定义 a 的右平移映射:

$$\begin{aligned} R_a : G &\rightarrow G \\ b &\mapsto R_a(b) := ba \end{aligned}$$

就如同我们看到的关于 D_4 中左平移映射和右平移映射那样, 我们有如下的关于一般群上这两个映射的性质:

命题 6.1.23 (教材注1.1.20)

任取群 G 的元素 a , 左平移映射 L_a 和右平移映射 R_a 都是双射(因此都给出了 G 中元素的置换).

证明. 记 $a \in G$. 我们将给出 L_a 是双射的证明, R_a 是双射的证明类似.

考虑 a 的左平移映射.

$$\begin{aligned} L_a : G &\rightarrow G \\ b &\mapsto L_a(b) := ab \end{aligned}$$

我们首先证明 L_a 是单射. 任取 G 中的元素 b 和 c , 若

$$L_a(b) = L_a(c),$$

那么我们有

$$ab = ac.$$

考虑 a 在 G 中的逆元 a^{-1} , 我们有

$$b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = c.$$

因此 L_a 为单射.

下证 L_a 为满射. 我们记 G 中的幺元为 e . 任取 $b \in G$, 我们有

$$b = eb = (aa^{-1})b = a(a^{-1}b) = L_a(a^{-1}b).$$

因此 b 在 L_a 的像中, L_a 为满射.

综上所述 L_a 为双射. □

定义 6.1.24

我们考虑 $(G, *)$ 为一个半群. 若 G 满足任取 $a, b, c \in G$, 有

$$ab = ac \implies b = c,$$

那么我们称 $(G, *)$ 满足**左消去律**. 若 G 满足任取 $a, b, c \in G$, 有

$$ba = ca \implies b = c,$$

那么我们称 $(G, *)$ 满足**右消去律**.

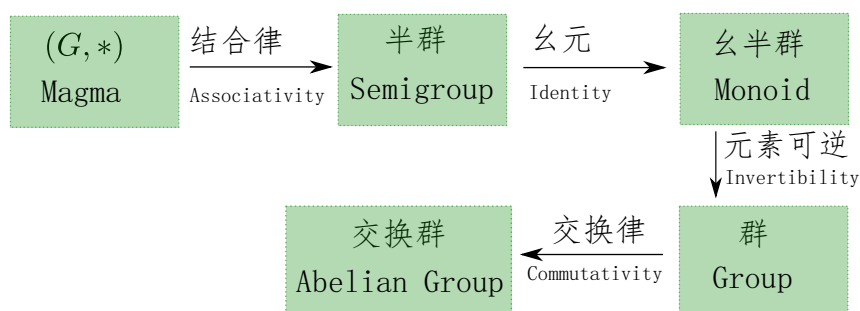
由左平移映射, 右平移映射以及元素交换的定义, 我们有以下命题 6.1.18 的等价叙述.

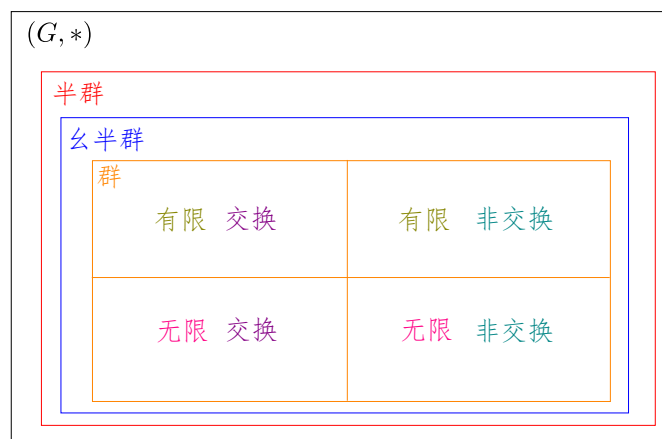
命题 6.1.25

设 G 为一个群. 任取 G 的元素 a , $L_a = R_a$ 当且仅当 a 与 G 中所有元素交换.

注 6.1.26.

最后我们给出之前介绍的一些概念之间的关系.





注 6.1.27.

教材中提到了一些关于半群的结论, 我们后边在学习环论的时候将会用到. 这里我们先跳过.

6.2 子群及群的生成

设 $H \subset G$ 为 G 的一个非空子集.

定义 6.2.1 (教材定理1.2.1)

若 H 对 G 的群运算封闭, 即任取 $g, g' \in H$, 我们有 $gg' \in H$, 且 H 关于 G 的群运算为一个群, 我们称 H 为 G 的一个**子群**. 我们通常记 $H < G$.

注 6.2.2.

我们可以由子群定义得到, 若 H 为 G 的一个子群, K 为 H 的一个子群, 那么 K 为 G 的一个子群; 若 H 和 K 都是 G 的子群, 且 $K \subset H$, 则 K 为 H 的子群.

例 6.2.3.

考虑 $\mathbb{C}$ 上的加法运算. 我们将 $\mathbb{C}$ 看作一个加法群, 则 $\{0\}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ 都是 $\mathbb{C}$ 的子群.

考虑 $\mathbb{C}$ 上的乘法运算. 我们将 $\mathbb{C}^*$ 看作一个乘法群, 则 $\{1\}$, $\mathbb{Q}^*$, $\mathbb{R}^*$ 都是 $\mathbb{C}^*$ 的子群.

例 6.2.4 (教材例1.2.6).

我们将 $\mathbb{Z}$ 看作一个加法群. 任取整数 m , 则

$$m\mathbb{Z} := \{mn \mid n \in \mathbb{Z}\},$$

为 $\mathbb{Z}$ 的一个子群.

实际上, 使用辗转相除, 我们可以证明其中的子群都是 $m\mathbb{Z}$ 的形式, 这里 m 为任意整数. (具体见练习)

例 6.2.5.

记 $n \in \mathbb{N}^*$. 我们考虑 $\mathbb{R}$ 上的 n -阶方阵的集合 $\text{Mat}_n(\mathbb{R})$. 该集合关于矩阵加法构成群. 以下

子集构成 $\text{Mat}_n(\mathbb{R})$ 的子群:

$H_1 := \{\text{上三角实矩阵}\};$

$H_2 := \{\text{下三角实矩阵}\};$

$$H_3 := \left\{ \begin{bmatrix} A_{r \times s} & O_{r \times (n-s)} \\ O_{(n-r) \times s} & B_{(n-r) \times (n-s)} \end{bmatrix} \mid \begin{array}{l} A_{r \times s} \in \text{Mat}_{r \times s}(\mathbb{R}), \\ B_{(n-r) \times (n-s)} \in \text{Mat}_{(n-r) \times (n-s)}(\mathbb{R}), \\ O_{r \times (n-s)} \text{ 和 } O_{(n-r) \times s} \text{ 为零矩阵} \end{array} \right\}, 1 \leq r, s \leq n-1$$

实际上, 在考虑矩阵加法群的时候, 我们也可以将其看成一个维数为 n^2 实线性空间. 从这个角度来看, 以上提到的子集都是这个线性空间的子空间.

例 6.2.6 (教材例1.2.4).

记 $n \in \mathbb{N}^*$. 我们考虑 $\mathbb{R}$ 上的 n -阶可逆方阵的集合 $\text{GL}(n, \mathbb{R})$. 该集合关于矩阵乘法构成群. 我们称之为**一般线性群**(General Linear group). 该群及其子群是李理论的研究对象的一部分. 以下是 $\text{GL}(n, \mathbb{R})$ 的一些子群:

(i) 特殊线性群 (Special Linear group):

$$\text{SL}(n, \mathbb{R}) := \{A \in \text{GL}(n, \mathbb{R}) \mid \det A = 1\},$$

(ii) 正交变换群 (Orthogonal group): 记 I_n 为 n -阶单位方阵,

$$\text{O}(n) := \{A \in \text{GL}(n, \mathbb{R}) \mid AA^t = I_n\},$$

(iii) 不定正交变换群 (Indefinite orthogonal group): 设 $p, q \in \mathbb{N}^*$, 满足 $p + q = n$, 记

$$I_{p,q} = \begin{bmatrix} I_p & \\ & -I_q \end{bmatrix}$$

我们记

$$\text{O}(p, q) := \{A \in \text{GL}(n, \mathbb{R}) \mid AI_{p,q}A^t = I_{p,q}\},$$

(iv) 辛变换群 (symplectic group): 设 $n = 2k$ 为偶数,

$$\text{Sp}(2k) := \left\{ A \in \text{GL}(n, \mathbb{R}) \mid A \begin{bmatrix} O_k & I_k \\ -I_k & O_k \end{bmatrix} A^t = \begin{bmatrix} O_k & I_k \\ -I_k & O_k \end{bmatrix} \right\}$$

从定义我们可以看出, 后边的几个群都是保持 $\mathbb{R}^n$ 上某些双线性型的矩阵构成的群. 这些双线性型通常与几何结构相关, 对应的保持这些双线性型的群代表了此类几何结构局部的对称性, 例如

$\text{O}(n)$	欧式几何
$\text{O}(n-1,1)$	双曲几何
$\text{O}(n-2,2)$	Anti-de Sitter 几何
$\text{O}(p,q)$	伪黎曼几何
$\text{Sp}(2k)$	辛几何

任给一个群 G , 则 $\{e\}$ 和 G 都是 G 的子群. 我们下边考虑一个非平凡的抽象的例子.

定义 6.2.7

设 G 为一个群. 我们称以下 G 的子集为 G 的**中心**:

$$Z(G) := \{a \in G \mid \forall b \in G, ab = ba\}.$$

命题 6.2.8

设 G 为一个群. 群 G 的中心 $Z(G)$ 为 G 的一个子群.

证明. 考虑 G 的幺元 e . 由幺元的定义, 我们知道 e 与 G 中所有元素交换, 因此 $e \in Z(G)$, $Z(G)$ 非空.

任取 $a, b \in Z(G)$, 任取 $c \in G$, 我们有

$$ac = ca, \quad bc = cb,$$

因此我们有

$$(ab)c = a(bc) = a(cb) = (ac)b = c(ab).$$

因此 $ab \in Z(G)$, 即 $Z(G)$ 对群运算封闭.

任取 $a, b, c \in Z(G) \subset G$, 由于群运算在 G 上满足结合律, 我们有

$$(ab)c = a(bc),$$

即群运算在 $Z(G)$ 也满足结合律.

任取 $a \in Z(G) \subset G$, 由于 $e \in G$ 为幺元, 因此

$$ae = ea = a.$$

e 为 $Z(G)$ 上群运算的单位元.

任取 $a \in Z(G)$, $b \in G$, 我们有

$$a^{-1}b = a^{-1}b(aa^{-1}) = a^{-1}(ba)a^{-1} = (a^{-1}a)ba^{-1} = ba^{-1}.$$

因此 $a^{-1} \in Z(G)$.

综上所述 $Z(G)$ 关于 G 上的群运算构成一个群, 也即 $Z(G)$ 为 G 的一个子群. $\square$

例 6.2.9.

记 $n \in \mathbb{N}^*$. 我们考虑 $\mathbb{R}$ 上的 n -阶可逆方阵群 $GL(n, \mathbb{R})$ (运算为矩阵乘法). 该矩阵群的中心由所有非零纯量矩阵构成:

$$Z(GL(n, \mathbb{R})) = \{\lambda I_n \mid \lambda \in \mathbb{R} \setminus \{0\}\}.$$

定理 6.2.10 (教材定理1.2.2, 习题 1.2.2)

(i) 群 G 的子集 H 为一个子群, 当且仅当任取 $a, b \in H$, 有

$$ab^{-1} \in H.$$

(ii) 记 $\{H_\alpha\}_{\alpha \in I}$ 为 G 中任意一族子群 (I 为指标集), 则

$$\bigcap_{\alpha \in I} H_\alpha,$$

为 G 的子群.

注 6.2.11.

这里"任意"有两个意思: 第一个是子群可以是任意一个, 第二个是所取的子群的数目, 也就是指标集的势可以是任意的(有限多个, 可数无限, 不可数无限等等).

以上结论 (i) 给了我们判定子群的一个简单的判别法.

证明. (i) 若 H 为 G 的子群, 则对任意 $a \in H$, 我们有 $a^{-1} \in H$, 由 H 对 G 的群运算封闭知, 任给 $a, b \in H$, 我们有 $ab^{-1} \in H$.

反过来, 假设对任意 $a, b \in H$, 我们有 $ab^{-1} \in H$. 由 H 非空知存在 $a \in H$. 因此我们首先取 $a = b$, 则有

$$e = aa^{-1} \in H.$$

因此 G 的幺元在 H 中也是 H 的幺元. 其次对任意 $a \in H$, 则有

$$a^{-1} = ea^{-1} \in H.$$

因此所有 H 中的元素的逆元也在 H 中. 最后, 任取 $a, b \in H$, 我们有

$$ab = a(b^{-1})^{-1} \in H.$$

因此 H 对 G 的群运算封闭. 由于 H 为 G 的子集, 因此群运算在 H 上也满足结合律. 综上所述, H 为 G 的子群.

(ii) 我们记

$$H = \bigcap_{\alpha \in I} H_{\alpha}.$$

由于对任意 α , H_{α} 为子群, 因此我们有 $e \in H_{\alpha}$ 对任意 α 成立. 因此由 H 的定义, $e \in H$, 集合 H 非空.

进一步任取 $a, b \in H$, 由 H 的定义, 对任意 α , 我们有

$$a, b \in H_{\alpha}.$$

又由于 H_{α} 为 G 的子群, 因此对任意 α , 我们有 $ab^{-1} \in H_{\alpha}$, 因此 $ab^{-1} \in H$. 由 (i), 我们知道 H 为子群.

□

注 6.2.12.

我们在证明 G 的某个子集为子群的时候, 由于子群首先要求是非空的, 因此我们首先需要验证所考虑的子集不是空集.

例 6.2.13.

考虑整数 $\mathbb{Z}$ 的子群. 记 $k \in \mathbb{N}^*$, $m_1, \dots, m_k$ 为 k 个两两不同的非零正整数, 则有

$$m_1\mathbb{Z} \cap \dots \cap m_k\mathbb{Z} = \text{lcm}(m_1, \dots, m_k)\mathbb{Z}.$$

如果我们取无穷多个两两不同的整数 $\{m_k\}_{k \in \mathbb{N}}$, 考虑所对应的子群的交, 则有:

$$\bigcap_{k \in \mathbb{N}} m_k\mathbb{Z} = \{0\}.$$

思考 6.2.14

两个子群的并集不一定是子群(可以与线性代数中两个子空间的并集不一定是子空间的结论比较). 为什么?

定义 6.2.15 (教材思考题1.2.9)

设 G 为一个群. 记 S 为 G 的一个非空子集. 我们称 G 中所有包含 S 的子群的交为 **由 S 生成的子群**, 记作 $\langle S \rangle$.

$$\langle S \rangle := \bigcap \{H \mid S \subset H < G\}.$$

我们记 S^{-1} 为 S 中元素的逆的集合:

$$S^{-1} := \{a^{-1} \mid a \in S\}.$$

下面我们给出 $\langle S \rangle$ 的另一种描述办法.

命题 6.2.16

$$\langle S \rangle = \{a_1 \cdots a_n \mid n \in \mathbb{N}^*, a_1, \dots, a_n \in S \cup S^{-1}\}.$$

证明. 我们记等式右边为

$$H = \{a_1 \cdots a_n \mid n \in \mathbb{N}^*, a_1, \dots, a_n \in S \cup S^{-1}\}.$$

首先证明 H 是一个子群.

任取 $c \in H$, 由 H 的定义, 存在 $a_1, \dots, a_n \in S \cup S^{-1}$, 满足

$$c = a_1 \cdots a_n.$$

另一方面, $a_1^{-1}, \dots, a_n^{-1} \in S \cup S^{-1}$, 因此

$$c^{-1} = a_n^{-1} \cdots a_1^{-1} \in H.$$

所以任取 H 的元素, 其逆元也在 H 中.

现在任取 $c, d \in H$, 我们有 $a_1, \dots, a_m, b_1, \dots, b_n \in S \cup S^{-1}$

$$c = a_1 \cdots a_m, \quad d = b_1 \cdots b_n.$$

由 H 的定义, 我们有

$$cd = a_1 \cdots a_m b_1 \cdots b_n \in H.$$

综上所述, 任取 $c, d \in H$, 我们有

$$cd^{-1} \in H.$$

因此 H 是 G 的一个子群.

下边我们证明二者作为集合相等. 由于 $S \subset H$, 因此我们有

$$\langle S \rangle \subset H.$$

另一方面, 任取子群 H' , 满足 $S \subset H'$, 则对任意 $a \in S$, $a^{-1} \in H'$. 因此 $S \cup S^{-1} \subset H'$.

由于 H' 对群运算封闭, 有归纳法我们可以得到, 任取 $S \cup S^{-1}$ 中的 $n \in \mathbb{N} \setminus \{0, 1\}$ 个元素 $a_1, \dots, a_n$, 我们有

$$a_1 \cdots a_n \in H',$$

也即任取 $c \in H$, 则有 $c \in H'$. 所以我们有 $H \subset H'$. 由于以上讨论对任意包含 S 的子集 H' 成立, 我们有

$$H \subset \langle S \rangle.$$

综上所述 $H = \langle S \rangle$. □

注 6.2.17.

我们这里将书上的思考题1.2.9中的叙述作为集合生成的子群的定义. 我们希望与之后讨论其他代数结构时要介绍的"子集生成的理想"(教材2.2节), "子集生成子模"(教材3.1节), "子集生成子域"(教材定义4.2.3)等的定义保持一致. 另一方面注意到子群的任意交仍是子群, 因此这个定义不需要纠结太多良好定义的问题.

两种定义方式反映了观察这个概念的两种不同的角度.

我们使用的定义反映出从整体上看 $\langle S \rangle$ 是 G 中包含 S 的"最小"的子群.

而书中的定义方式则更关注 S 生成的子群的内部结构, 更好的解释了为什么我们用"生成"这个词, 即给定一个集合 S , 如果我们考虑以 $S \cup S^{-1}$ 中的元素为输入的所有可能的有限次群运算, 将得到的结果收集起来就是 S 生成的子群. 这给出了这个群中的元素的一般形式.

如果 S 有限, 我们称群 $\langle S \rangle$ 有限生成. 第二种方法可以给我们一个枚举出所有 $\langle S \rangle$ 的元素的方法.

后边我们在讨论"子集生成的理想", "子集生成子模"以及"子集生成子域"也会从这两个角度来进行.

例 6.2.18.

我们考虑整数加群 $\mathbb{Z}$ 中的子集 $S = \{2\}$. 我们有

$$\langle 2 \rangle = \{m2 + n(-2) \mid m, n \in \mathbb{N}\}.$$

因此 $\{2\}$ 生成的子群就是 $2\mathbb{Z}$.

思考 6.2.19

我们考虑整数加群 $\mathbb{Z}$ 中的子集 $S = \{4, 6\}$. 由 S 生成的 $\mathbb{Z}$ 的子群是什么? 如果

$$S = \{n_1, \dots, n_k\},$$

是 k 个两两不同的整数的集合, 那么如何描述 S 生成的 $\mathbb{Z}$ 的子群?

定义 6.2.20

设 G 为一个群. 任取 G 的子群 H , 考虑 $\emptyset \neq S \subset H$, 若

$$\langle S \rangle = H,$$

则称 H 由 S 生成, 同时 S 为 H 的一组生成元.

特别的, 如果 G 的非空子集 S , 满足

$$\langle S \rangle = G,$$

我们称 G 由 S 生成, 且 S 是 G 的一组生成元.

注 6.2.21.

我们可以由 G 的子集 S 出发, 来生成 G 的子群 $\langle S \rangle$. 因此 $\langle S \rangle$ 是由 S 生成的, 而 S 是 $\langle S \rangle$ 的一组生成元.

我们也可以从 G 的子群 H 出发, 来寻找什么样的集合 $S \subset H$ 满足 $\langle S \rangle = H$. 这里要

特别指出的是, 一方面这样的集合 S 总是存在的, 例如 $S = H$ 就满足:

$$\langle H \rangle = H;$$

另一方面, 除了一些平凡的情况外(例如 $H = \{e\}$), 这样的 S 是不唯一的. 例如, 任取 H 中非幺元的元素 g , 记 $S = H \setminus \{g\}$ 就可以作为 H 的一组生成元.

当然这里举的例子都有些平凡, 更多的是为了说明理论上我们需要注意这些事情. 实际中, 我们通常希望考虑如何用更少的信息, 或者更有效的办法来生成一个群. 比如, 找到一个尽可能少的生成元组, 或者与其他结构相关的生成元组等等. (参考习题)

当然仅仅通过生成元, 我们只知道群的一部分信息, 我们还需要另一部分信息来完全确定群结构, 那就是生成元之间的关系. 我们后边在介绍完同态之后, 会介绍如何用生成元和关系来表示群. 特别地, 我们可以通过比较生成元和关系来确定两个群是否同构. 这在研究有限生成群的时候发挥了巨大作用.

我们考虑一种特殊情: 集合 S 只有一个元素.

定义 6.2.22

设 G 为一个群. 若群 G 中存在元素 a , 满足

$$G = \langle a \rangle,$$

我们称 G 为一个由 a 生成的**循环群**.

定义 6.2.23

设 G 为一个群. 任取群 G 中的元素 a , 我们称 $\langle a \rangle$ 为 G 的一个**循环子群**. 如果 $\langle a \rangle$ 有限, 我们称 a 为 G 的一个**有限阶元**, 并称 $|\langle a \rangle|$ 为 a 的**阶**, 记作:

$$o(a) = |\langle a \rangle|.$$

如果 $\langle a \rangle$ 无限, 我们称 a 为 G 的一个**无限阶元**.

例 6.2.24.

我们考虑整数加群 $\mathbb{Z}$. 考虑 $\mathbb{Z}$ 的幺元 1, 我们有

$$\mathbb{Z} = \langle 1 \rangle.$$

因此 $\mathbb{Z}$ 是一个循环群. 由于 $\mathbb{Z}$ 作为集合无限, 因此 1 是一个无限阶元. 任取 $m \in \mathbb{Z}$, 则 m 生成的 $\mathbb{Z}$ 的子群为 $m\mathbb{Z}$. 注意到 $m\mathbb{Z}$ 有限当且仅当 $m = 0$. 因此 $\mathbb{Z}$ 中有限阶元只有为 0, 且 $o(0) = 1$.

我们考虑 $S = \{p, q\} \subset \mathbb{Z}$, 满足 p 和 q 为两个互素的非零正整数, 则 S 生成 $\mathbb{Z}$. 通过例子我们可以看出一个群的生成元组不是唯一的, 并且生成元组的元素数目也不唯一.

例 6.2.25 (教材习题 1.2.13).

我们考虑 2 阶整系数矩阵集合 $\text{Mat}_2(\mathbb{Z})$ 的子集

$$\text{GL}(2, \mathbb{Z}) := \left\{ \begin{bmatrix} m & n \\ p & q \end{bmatrix} \mid |mq - np| = 1 \right\}.$$

这个集合关于矩阵乘法构成给一个群. 我们可以验证以下集合生成 $GL(2, \mathbb{Z})$:

$$S = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\}.$$

其中, 前两个矩阵生成了 $GL(2, \mathbb{Z})$ 中行列式为 1 的矩阵构成的子群 $SL(2, \mathbb{Z})$. (参考练习)

这两个矩阵生成 $SL(2, \mathbb{Z})$ 的过程和整数之间的辗转相除, 以及有理数的连分数展开有着紧密的联系.

例 6.2.26.

我们考虑 $GL(2, \mathbb{R})$ 的子群

$$SL(2, \mathbb{R}) := \left\{ M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \det M = ad - bc = 1 \right\}$$

任取实数 $t \in \mathbb{R}$, 矩阵

$$U_t = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$$

生成的循环子群为

$$\langle U_t \rangle = \left\{ \begin{bmatrix} 1 & nt \\ 0 & 1 \end{bmatrix} \middle| n \in \mathbb{Z} \right\}.$$

若 $t = 0$, 则 $\langle U_0 \rangle = \{e\}$, 为一阶循环群. 若 $t \neq 0$, 则 $\langle U_t \rangle$ 是一个无限阶的循环群.

任取正实数 $\lambda \in \mathbb{R}_{>0}$, 矩阵

$$D_\lambda = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix}$$

生成的循环子群为

$$\langle D_\lambda \rangle = \left\{ \begin{bmatrix} \lambda^n & 0 \\ 0 & \lambda^{-n} \end{bmatrix} \middle| n \in \mathbb{Z} \right\}.$$

若 $\lambda = 1$, 则 $\langle D_1 \rangle = \{e\}$, 为一阶循环群. 若 $\lambda \neq 1$, 则 $\langle D_\lambda \rangle$ 是一个无限阶的循环群.

任取实数 $\theta \in [0, 2\pi)$, 矩阵

$$R_\theta = \begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix}$$

生成的循环群为

$$\langle R_\theta \rangle = \left\{ \begin{bmatrix} \cos(n\theta) & \sin(n\theta) \\ -\sin(n\theta) & \cos(n\theta) \end{bmatrix} \middle| n \in \mathbb{Z} \right\}.$$

若 $\theta = u\pi$, 其中 $u \in \mathbb{Q}$, 则 $\langle R_\theta \rangle$ 为有限阶循环群. 若 $u \in \mathbb{R} \setminus \mathbb{Q}$, 则 $\langle R_\theta \rangle$ 为无限阶循环群.

以上三类矩阵是群 $SL(2, \mathbb{R})$ 三种基本的矩阵(也对应三种若当标准型). 我们可以证明, 任取 $M \in SL(2, \mathbb{R})$, 存在唯一的 t, λ 和 θ , 满足

$$M = R_\theta D_\lambda U_t.$$

换句话说, 如果我们记

$$\begin{aligned} K &= \left\{ R_\theta = \begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix} \middle| \theta \in [0, 2\pi) \right\} \\ A &= \left\{ D_\lambda = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} \middle| \lambda \in \mathbb{R}_{>0} \right\} \\ N &= \left\{ U_t = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \middle| t \in \mathbb{R} \right\} \end{aligned}$$

则有

$$\mathrm{SL}(2, \mathbb{R}) = KAN.$$

我们称其为 $\mathrm{SL}(2, \mathbb{R})$ 的 KAN 分解, 或者 Iwasawa 分解. 这里字母 K 代表 compact, A 代表 abelian, N 代表 Nilpotent. 注意到以上三个子群 K , A 和 N 不再是循环子群. 但是它们分别由 1 个参数决定, 我们通常称之为单参数子群.

6.3 陪集

定义 6.3.1 (教材定义 1.2.10)

设 G 为一个群. 任取 G 的一个子群 H , 以及 $a \in G$, 我们定义 H 关于 a 的左陪集为

$$aH := \{ab \in G \mid b \in H\},$$

H 关于 a 的右陪集为

$$Ha := \{ba \in G \mid b \in H\}.$$

以下我们将讨论陪集的性质. 我们将只给出关于左陪集的结论和证明. 关于右陪集的结论和证明与关于左陪集的情形相似.

命题 6.3.2

设 G 为一个群. 任取 G 的一个子群 H 以及一个元素 $a \in G$, 我们有

- (i) $aH = H$ 当且仅当 $a \in H$.
- (ii) aH 为一个子群当且仅当 $a \in H$;
- (iii) 若 $a \notin H$, 我们有 $aH \cap H = \emptyset$.

证明. (i) 若 $aH = H$, 考虑么元 $e \in H$, 我们有

$$a = ae \in aH = H.$$

反过来, 假设 $a \in H$, 任取 $b \in H$, 由于 H 关于群运算封闭, 我们有 $ab \in H$, 因此

$$aH \subset H.$$

另一方面, 任取 $b \in H$, 我们有

$$b = eb = (aa^{-1})b = a(a^{-1}b) \in aH.$$

因此 $H \subset aH$. 综上所述我们有

$$aH = H.$$

- (ii) 若 aH 为一个子群, 则有 $e \in aH$, 因此 $a \in H$.

反过来, 若 $a \in H$, 则由之前对左平移映射的讨论, 我们有 $aH = H$, 因此为一个子群.

- (iii) 我们使用反证法. 若 $a \notin H$, 假设存在 $b \in H \cap aH$, 则存在 $c \in H$, 满足 $ac = b$. 由于 H 为一个子群, 因此有 $c^{-1} \in H$, 且 H 对群运算封闭. 由此可得

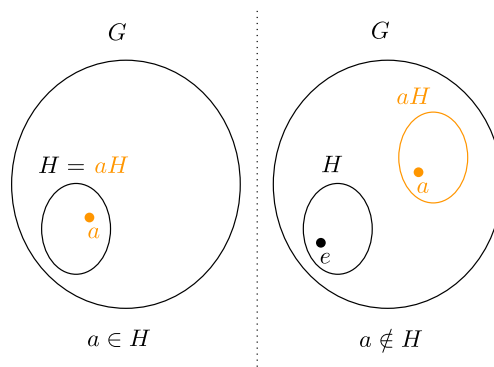
$$a = (ac)c^{-1} = bc^{-1} \in H,$$

与假设 $a \notin H$ 矛盾.

□

注 6.3.3.

我们用以下示意图来说明以上命题所说的陪集 H 和 aH 之间的关系:

**推论 6.3.4 (引理1.2.12)**

设 G 为一个群. 任取 G 的一个子群 H , 以及 G 的元素 a 和 b , 我们有 $aH = bH$ 或者 $aH \cap bH = \emptyset$.

进一步, 我们有 $aH = bH$ 当且仅当 $b^{-1}a \in H$.

证明. 考虑左平移映射 $L_{b^{-1}}$, 我们有

- $aH = bH$ 当且仅当 $b^{-1}aH = H$;
- $aH \cap bH = \emptyset$ 当且仅当 $(b^{-1}a)H \cap H = \emptyset$.

因此这个结论是之前命题的推论. □

例 6.3.5.

我们考虑整数加群 $G = \mathbb{Z}$, 以及其子群 $H = 3\mathbb{Z}$. 选取 $a = 2$, 则有 $3\mathbb{Z}$ 关于 2 的左陪集为:

$$2 + 3\mathbb{Z} = \{2 + 3n \mid n \in \mathbb{Z}\}.$$

我们进一步有:

$$(2 + 3\mathbb{Z}) \cap 3\mathbb{Z} = \emptyset.$$

(一个整数被 3 除, 不可能既余 0 又余 2.)

如果我们取 $a = 6$, 则有 $3\mathbb{Z}$ 关于 6 的左陪集为:

$$6 + 3\mathbb{Z} = \{6 + 3n \mid n \in \mathbb{Z}\}.$$

对任意 $m, n \in \mathbb{Z}$ 满足 $m - n = 2$, 我们有 $6 + 3n = 3m$, 因此有

$$(6 + 3\mathbb{Z}) = 3\mathbb{Z}.$$

注 6.3.6.

我们这里给出以上推论关于右陪集的版本:

任取群 G 的一个子群 H , 以及元素 a 和 b , 我们有 $Ha = Hb$ 或者 $Ha \cap Hb = \emptyset$. 进一步, 我们有 $Ha = Hb$ 当且仅当 $ab^{-1} \in H$.

命题 6.3.7

设 G 为一个群. 任取 G 的子群 H , 则 H 所有的左陪集构成 G 的一个划分, 即

- (i) $G = \bigcup \{aH \mid a \in G\}$;
- (ii) 任取 $a, b \in G$, 我们有 $aH \cap bH = \emptyset$ 或 $aH = bH$.

证明. 以上讨论中我们已经证明了第二点. 现在讨论第一点. 任取 $a \in G$, 我们有

$$aH \subset G.$$

因此我们有

$$\bigcup \{aH \mid a \in G\} \subset G.$$

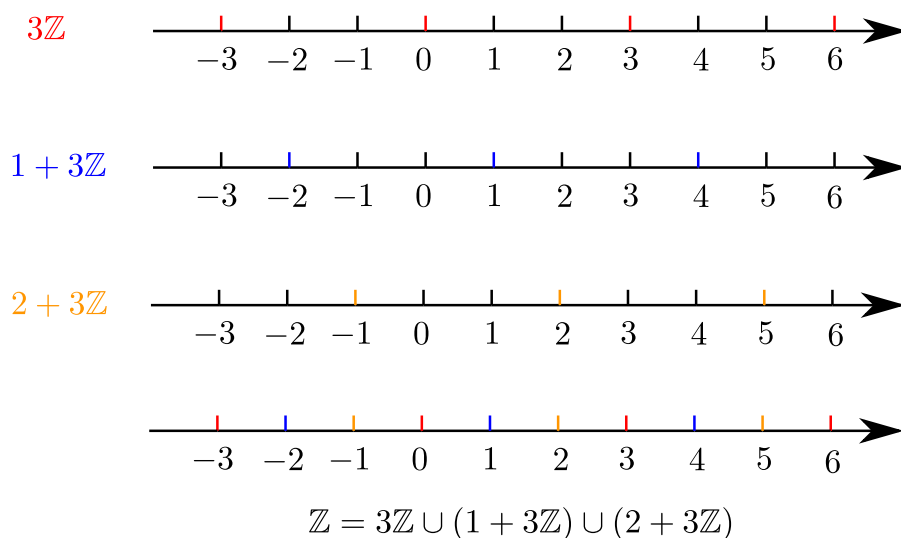
另一方面, 任取 $a \in G$, 由于幺元 $e \in H$, 因此 $a \in aH$. 我们继而有

$$G \subset \bigcup \{aH \mid a \in G\}.$$

因此我们得到

$$G = \bigcup \{aH \mid a \in G\}.$$

□

**注 6.3.8.**

我们从集合的角度来考虑, 将一个子群 H 左乘一个元素 a , 也可以被看作是将这个子集 H 在 G 中做了一个移动.

定理 6.3.9 (教材定理1.2.19)

设 G 为一个群. 任给 G 的子群 H , 以下定义了 G 中元素之间的一个等价关系:

$$a \sim b \Leftrightarrow a^{-1}b \in H.$$

证明. 我们需要验证 $\sim$, 满足自反性, 对称性, 传递性.

(自反性) 任取 $a \in G$, 我们有 $a^{-1}a = e \in H$, 因此 $a \sim a$.

(对称性) 任取 $a, b \in G$, 满足 $a \sim b$, 因此 $a^{-1}b \in H$. 我们有 $b^{-1}a = (a^{-1}b)^{-1} \in H$. 因此 $b \sim a$.

(传递性) 任取 $a, b, c \in G$, 满足 $a \sim b$, 且 $b \sim c$, 因此有 $a^{-1}b, b^{-1}c \in H$. 我们有

$$a^{-1}c = a^{-1}(bb^{-1})c = (a^{-1}b)(b^{-1}c) \in H.$$

因此 $a \sim c$. □

定义 6.3.10

设 G 为一个群. 任给 G 的子群 H , 我们记 G 对 H 的左陪集空间为如下集合:

$$G/H := \{aH \mid a \in G\}.$$

类似地, 我们记 G 对 H 的右陪集空间为如下集合:

$$H \backslash G := \{Ha \mid a \in G\}.$$

命题 6.3.11

设 G 为一个群. 任给 G 子群 H , 以下定义一个双射:

$$\begin{aligned} \phi : G/H &\rightarrow H \backslash G \\ aH &\mapsto Ha^{-1} \end{aligned}$$

证明. 我们首先证明, 任取 $a, b \in G$,

$$aH = bH \Leftrightarrow Ha^{-1} = Hb^{-1}.$$

这可以由以下一系列的等价关系得到:

$$aH = bH \Leftrightarrow b^{-1}a \in H \Leftrightarrow Ha^{-1} = Hb^{-1}.$$

最后一个等价参考注 6.3.6.

由这一系列的等价关系, 我们有以下结论:

- (i) 由于 $\phi(aH)$ 不依赖于 a 的选取, 映射 ϕ 是良定义的;
- (ii) 我们可以使用类似的方法构造映射

$$\begin{aligned} \psi : H \backslash G &\rightarrow G/H \\ Ha &\mapsto a^{-1}H \end{aligned}$$

并证明这个映射是良定义的.

- (iii) 通过 ϕ 和 ψ 的定义, 我们可以验证任取 $g \in G$, 我们有

$$(\psi \circ \phi)(aH) = \psi(Ha^{-1}) = aH, (\phi \circ \psi)(Ha) = \phi(a^{-1}H) = Ha.$$

因此 ϕ 是双射. □

注 6.3.12.

形式上定义如下的对应

$$\begin{aligned}\phi' : G/H &\rightarrow H \backslash G \\ aH &\mapsto Ha\end{aligned}$$

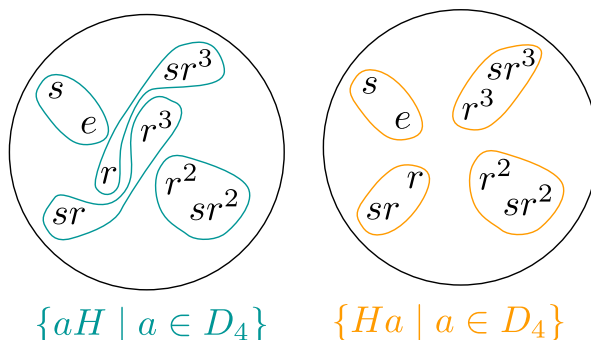
一般的情形下不是一个映射. 我们可以考虑下边的例子.

令 $G = D_4$. 我们记

$$H = \langle s \rangle = \{id, s\}.$$

我们列出每个 D_4 元素对应的左陪集和右陪集:

a	id	r	r^2	r^3	s	rs	r^2s	r^3s
aH	$\{id, s\}$	$\{r, rs\}$	$\{r^2, r^2s\}$	$\{r^3, r^3s\}$	$\{s, id\}$	$\{rs, r\}$	$\{r^2s, r^2\}$	$\{r^3s, r^3\}$
Ha	$\{id, s\}$	$\{r, r^3s\}$	$\{r^2, r^2s\}$	$\{r^3, rs\}$	$\{s, id\}$	$\{rs, r^3\}$	$\{r^2s, r^2\}$	$\{r^3s, r\}$



我们观察到

$$rH = \{r, rs\} = rsH,$$

另一方面, 从上表我们也可以看出

$$Hr = \{r, r^3s\} \neq \{rs, r^3\} = H(rs).$$

因此 ϕ' 不是一个映射.

我们马上会讲到"正规子群". 对于群 G 的一个"正规子群" H , 以上定义的 ϕ' 是一个映射.

注 6.3.13.

我们这里也列出以上例子在 ϕ 映射下左陪集和右陪集的对应关系:

gH	$(id)H = \{id, s\}$	$rH = \{r, rs\}$	$r^2H = \{r^2, r^2s\}$	$r^3H = \{r^3, r^3s\}$
$\phi(gH)$	$H(id) = \{id, s\}$	$Hr^{-1} = \{r^3, rs\}$	$Hr^{-2} = \{r^2, r^2s\}$	$Hr^{-3} = \{r, r^3s\}$
gH	$sH = \{s, id\}$	$(rs)H = \{rs, r\}$	$(r^2s)H = \{r^2s, r^2\}$	$(r^3s)H = \{r^3s, r^3\}$
$\phi(gH)$	$Hs = \{s, id\}$	$H(rs)^{-1} = \{rs, r^3\}$	$H(r^2s)^{-1} = \{r^2s, r^2\}$	$H(r^3s)^{-1} = \{r^3s, r\}$

实际上, $\phi(aH)$ 可以理解为以下集合

$$\phi(aH) = (aH)^{-1} = \{(ab)^{-1} \mid b \in H\} = \{b^{-1}a^{-1} \mid b \in H\} = Ha^{-1}.$$

推论 6.3.14

设 G 为一个群. 任给 G 的一个子群 H , H 的左陪集空间和右陪集空间等势:

$$|G/H| = |H \backslash G|.$$

证明. 考虑集合等势的定义, 该结论是命题 6.3.11 的直接推论. $\square$

定义 6.3.15

设 G 为一个群. 任给 G 的子群 H , 我们定义 H 在 G 中的**指数**为

$$[G : H] := |G/H| = |H \backslash G|.$$

如果 G 为有限群, 则 H 为有限集, 且 G/H 和 $H \backslash G$ 也为有限集. 利用之前对一个给定元素 $a \in G$ 诱导的 G 的左平移映射和右平移映射的性质, 我们可以得到以下结论:

引理 6.3.16

任取有限群 G 的一个子群 H 和一个元素 a , 我们有 $|H| = |aH|$.

证明. 由于 a 诱导的左乘映射 L_a 是双射, 因此有

$$|H| = |L_a(H)| = |aH|.$$

$\square$

综合以上所有结论, 我们得到以下定理:

定理 6.3.17 (教材定理1.2.22: Lagrange 定理)

设 G 为有限群, H 为 G 的一个子群, 则有

$$|G| = [G : H] \cdot |H|.$$

证明. 考虑 G 中由 H 的左陪集给出的划分. 设 $k = [G : H]$, 设 $a_1, \dots, a_k \in G$, 满足集合 G 可以写为以下不交并:

$$G = a_1H \cup \dots \cup a_kH.$$

因此

$$|G| = |a_1H| + \dots + |a_kH| = k|H| = [G : H]|H|.$$

$\square$

推论 6.3.18

设 G 为一个有限群. 任取 G 的子群 H , 我们有 H 的阶整除 G 的阶, 即

$$|H| \mid |G|.$$

特别地, 任取 $a \in G$, 我们有

$$o(a) = |\langle a \rangle| \mid |G|.$$

推论 6.3.19

若群 G 的阶为素数 p , 则 G 为一个循环群.

证明. 由于

$$|G| > 1,$$

因此 G 中有非幺元 a . ($a \neq e$).

由于 a 的阶整除 G 且非 1, 因此 a 的阶为 p . 因此我们有

$$|G| \geq |\langle a \rangle| = p = |G|.$$

因此 $G = \langle a \rangle$, 即 a 为 G 的生成元, G 为一个循环群. $\square$

思考 6.3.20 (教材思考题 1.2.24)

任取 $|G|$ 的一个因子 $m \in \mathbb{N}^*$, 一定存在一个元素 $a \in G$, 满足 $o(a) = m$ 么?

推论 6.3.21 (教材推论 1.2.23)

设 G 为一个有限群, H 为 G 的子群, K 为 H 的子群, 则有

$$[G : K] = [G : H][H : K].$$

证明. 由 Lagrange 定理, 我们知道

$$[G : K] = \frac{|G|}{|K|} = \frac{[G : H]|H|}{|K|} = \frac{[G : H][H : K]|K|}{|K|} = [G : H][H : K].$$

$\square$

6.4 正规子群

上节我们看到了 gH 和 Hg 在没有任何条件假设的前提下, 没有理由相同. 我们上节举了一个二面体群 D_4 的 s 生成的子群的例子. 但我们也看到了, 在我们考虑 $\mathbb{Z}$ 的子群的陪集的时候, 任取 $m, n \in \mathbb{Z}$,

$$m + n\mathbb{Z} = n\mathbb{Z} + m,$$

总是成立的. 如果我们进一步地考虑 G 是一个交换群, 那么 $aH = Ha$ 也是一个必须满足的结论. 那么我们可能会问, 只有满足交换条件, 我们才可以有 $aH = Ha$ 么? 或者我们可以有更一般的情况也可能发生呢? 此外, 我们还可以问一个更一般的问题, 那就是在什么条件下, H 的左陪集给出的 G 的划分和右陪集给出的 G 的划分相同呢? 相同之后, 这样的分划有什么性质?

命题 6.4.1

设 G 为一个群. 任取 H 为 G 的一个子群, $a, b \in G$, 若 $aH = Hb$, 则有 $aH = bH$.

证明. 由于 $aH = Hb$, 我们有

$$b = eb = be \in bH \cap aH.$$

因为 H 的左陪集给出 G 的一个划分, 因此 $aH = bH$. $\square$

推论 6.4.2

任取 G 的子群 H , 若 H 的左陪集给出的 G 的划分与 H 的右陪集给出的 G 的划分相同, 那么任取 $a \in G$, 我们有

$$aH = Ha.$$

定义 6.4.3

设 G 为一个群. 任取 G 的两个元素 a 和 b , 我们称元素 aba^{-1} 为元素 b 关于 a 的**共轭**.

任取 G 的一个子群 H . 任取 G 的元素 a . 我们称以下集合为 H 关于 a 的**共轭**:

$$aHa^{-1} := \{aba^{-1} \mid b \in H\}.$$

命题 6.4.4

设 G 为一个群. 任取 G 的子群 H 和 G 的元素 a , 我们有 aHa^{-1} 是 G 的一个子群.

证明. 由于 H 非空, 因此 aHa^{-1} 非空.

我们只需要验证任取 aHa^{-1} 中两个元素 b 和 b' , 我们有 $bb'^{-1} \in aHa^{-1}$.

任取 $c, c' \in H$, 设 $b = aka^{-1}$, $b' = ac'a^{-1}$. 我们有

$$bb'^{-1} = (aka^{-1})(ac'a^{-1})^{-1} = (aka^{-1})(ac'^{-1}a^{-1}) = acc'^{-1}a^{-1}.$$

因为 H 是一个子群, 因此 $cc'^{-1} \in H$. 由 aHa^{-1} 的定义, 我们有 $bb'^{-1} \in aHa^{-1}$. □

定义 6.4.5 (教材定义 1.3.1 改)

我们称 G 的一个子群 H 为 G 的一个**正规子群**, 若其满足条件:

- 任取 $a \in G$, 我们都有 $aHa^{-1} = H$.

通常我们记作 $H \triangleleft G$.

注 6.4.6.

我们可以由定义验证, 任意群 G 都有 $\{e\}$ 和 G 两个正规子群. 此外注意到一个交换群 G 的任意子群都满足以上提到的性质, 因此一个交换群的任意子群都是正规子群. 而当 G 非交换的时候, 情况会比较复杂.

若一个群 G 的正规子群只有 $\{e\}$ 和 G , 我们称 G 为一个**单群**.

例 6.4.7.

我们考虑 $\mathbb{Z}$ 作为加法群的子群. 任取 $m \in \mathbb{Z}^*$, 考虑子群 $m\mathbb{Z}$. 任取 $k, n \in \mathbb{Z}$, 我们有

$$k + nm + (-k) = nm$$

因此有

$$k + m\mathbb{Z} + (-k) = m\mathbb{Z}.$$

子群 $m\mathbb{Z}$ 是 $\mathbb{Z}$ 的正规子群.

例 6.4.8.

注意到以上讨论中, 我们只用到了 $\mathbb{Z}$ 上的加法满足交换律. 更确切的说是 $\mathbb{Z}$ 中元素与 $m\mathbb{Z}$ 中的元素交换. 如果我们找到 G 的一个子群 H , 满足 G 中元素和 H 中元素交换, 则 H 也是 G 的正规子群.

例如, 任给交换群 G , 则 G 的所有子群都是正规子群. 任给群 G , 则 G 的中心 $Z(G)$ 为 G 的正规子群.

例 6.4.9.

我们之前讨论过 D_4 的一个子群 $\langle s \rangle = \{e, s\}$. 由之前的讨论, 我们知道

$$rsr^{-1} = rsr^3 = sr^6 = sr^2 \notin H_s.$$

因此

$$r\langle s \rangle r^{-1} \neq H_s.$$

由定义, 我们有 $\langle s \rangle$ 不是 D_4 的正规子群.

另一方面, 考虑 $\langle r \rangle = \{e, r, r^2, r^3\}$. 任取 $r^j \in \langle r \rangle$, 我们考虑

$$sr^j s = ssr^{3j} = r^{3j} \in \langle r \rangle.$$

因此有 $s\langle r \rangle s = \langle r \rangle$. 由于 r 与 $\langle r \rangle$ 交换, 并且 $\{r, s\}$ 生成 D_4 , 我们知道 $\langle r \rangle$ 是 D_4 的一个正规子群.

注意到以上例子中, 我们验证 $\langle r \rangle$ 正规的时候并没有对所有 D_4 的元素验证定义中的等式. 为了说明这个, 我们注意到共轭运算利用到了元素的求逆. 我们知道取逆满足以下性质:

引理 6.4.10

设 G 为一个群, 任取 $a, b \in G$, 我们有 $(ab)^{-1} = b^{-1}a^{-1}$.

证明. 元素 $(ab)^{-1}$ 为 ab 的逆. 另一方面, 我们考虑元素 $b^{-1}a^{-1}$, 满足

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e.$$

因此 $b^{-1}a^{-1}$ 也是 ab 的逆元. 由逆元的唯一性我们知道

$$(ab)^{-1} = b^{-1}a^{-1}.$$

□

利用这个性质, 我们可以验证共轭满足

引理 6.4.11

设 G 为一个群, H 为 G 的一个子群. 任取 $a, b \in G$, 我们有

$$(ab)H(ab)^{-1} = a(bHb^{-1})a^{-1}.$$

注 6.4.12.

当我们利用定义验证一个子群 H 是正规子群的时候, 如果整个群 G 是由 S 生成的, 我们只需要对 S 中的元素验证正规子群的定义即可.

我们下边给出子群正规的一些等价条件.

定理 6.4.13 (教材定理 1.3.5 扩)

记 G 为一个群, H 为 G 的一个子群. 以下叙述等价:

- (i) $H \triangleleft G$;
- (ii) 任取 $a \in G$, 有 $aH = Ha$;
- (iii) H 的左陪集给出 G 的划分与 H 的右陪集给出的 G 的划分相同;
- (iv) 任取 $a, b \in G$, 我们有 $(aH)(bH) = (ab)H$.
- (v) 任取 $a \in G$ 以及 $b \in H$, 我们有 $aba^{-1} \in H$.

注 6.4.14.

当群 G 交换的时候, G 的任意子群都满足以上所有条件.

注 6.4.15.

记号 $(aH)(bH)$ 表示以下集合

$$(aH)(bH) := \{(ax)(by) \in G \mid x, y \in H\}.$$

证明. 我们之前已经讨论过 (iii) 和 (ii) 等价的结论. 下边我们将按照

$$(i) \implies (ii) \implies (iv) \implies (v) \implies (i)$$

的顺序证明.

(i) $\implies$ (ii) 由正规子群的定义, 我们有任取 $a \in G$,

$$aHa^{-1} = H.$$

任取 $b \in H$, 我们有

$$ab = (aba^{-1})a \in Ha.$$

因此 $aH \subset Ha$. 另一方面,

$$ba = a(a^{-1}ba) \in aH.$$

因此 $Ha \subset aH$. 综上所述, $aH = Ha$.

(ii) $\implies$ (iv) 任取 $a, b \in G$ 以及 $c, d \in H$, 我们考虑 $(ac)(bd)$. 由于 $bH = Hb$, 存在 $c' \in H$, 满足

$$cb = bc'.$$

因此我们有

$$(ac)(bd) = a(cb)d = (ab)(c'd) \in (ab)H.$$

因此 $(aH)(bH) \subset (ab)H$.

反过来, 任取 $a, b \in G$ 以及 $c \in H$, 由于 $bH = Hb$, 我们有 $c' \in H$, 满足

$$bc = c'b.$$

因此我们有

$$abc = (ac')(be) \in (aH)(bH).$$

因此 $(ab)H \subset (aH)(bH)$. 综上所述我们有 $(aH)(bH) = (ab)H$.

(iv) $\implies$ (v) 任取 $a \in G$, 由假设我们有

$$(eH)(a^{-1}H) = (ea^{-1})H = a^{-1}H.$$

任取 $b \in H$, 我们有 $c \in H$, 满足

$$(eb)a^{-1}b = a^{-1}c'.$$

因此有

$$aba^{-1} = c'b^{-1} \in H.$$

(v) $\implies$ (i) 任取 $a \in G$ 以及 $b \in H$, 由假设, 我们有

$$aba^{-1} \in H.$$

因此 $aHa^{-1} \subset H$.

反过来, 任取 $a \in G$ 以及 $b \in H$, 我们有

$$b = (aa^{-1})b(aa^{-1}) = a(a^{-1}ba)a^{-1}.$$

由假设, 存在 $c \in H$, 满足 $c = a^{-1}ba$. 因此

$$b = aca^{-1} \in aHa^{-1}.$$

因此 $H \subset aHa^{-1}$. 综上所述, 对任意 $a \in G$, 我们有

$$aHa^{-1} = H.$$

□

注 6.4.16.

这里注意到以上提到的每一项的侧重点都有不同.

(ii) 和 (iii) 讨论的是正规子群对应的陪集的特殊性质, 特别地, 当一个子群为正规子群时, 我们将不再区分左右陪集, 而统称陪集.

(iv) 则描述了左陪集空间上的一个二元运算. 在接下去的部分我们将进一步讨论这个二元运算, 并引入商群的概念. 这里要强调的是, 由这些等价关系, 我们可以看出, 我们对一个子群的左陪集空间可以定义这样的二元运算当且仅当这个子群是正规子群.

(v) 是我们在证明某些子群是正规子群的时候会使用的一个方法.

注 6.4.17.

记号 N 来自正规子群 Normal subgroup 首字母.

任取 G 的两个子群 H 和 K , 两个集合的乘积

$$HK := \{ax \in G \mid a \in H, x \in K\}.$$

一般情况下, 我们不一定有 $HK \subset G$ 是 G 的一个子群.

例 6.4.18.

我们考虑 $GL(2, \mathbb{R})$ 的子群

$$A = \left\{ \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} \mid \lambda \in \mathbb{R}_{>0} \right\},$$

$$U = \left\{ \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \mid t \in \mathbb{R} \right\}.$$

因此

$$AU = \left\{ \begin{bmatrix} \lambda & \lambda t \\ 0 & \lambda^{-1} \end{bmatrix} \mid \lambda \in \mathbb{R}_{>0}, t \in \mathbb{R} \right\}.$$

我们考虑 $a, b \in \mathbb{R}_{>0}$. 任取 $t \in \mathbb{R}$, 则有

$$\begin{bmatrix} a & at \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} b & bt \\ 0 & b^{-1} \end{bmatrix} = \begin{bmatrix} ab & (ab + ab^{-1})t \\ 0 & (ab)^{-1} \end{bmatrix}.$$

令

$$t' = \frac{ab + ab^{-1}}{ab} t,$$

我们有

$$\begin{bmatrix} ab & (ab + ab^{-1})t \\ 0 & (ab)^{-1} \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & (ab)^{-1} \end{bmatrix} \begin{bmatrix} 1 & t' \\ 0 & 1 \end{bmatrix} \in AU.$$

因此 AU 对群运算封闭. 实际上 AU 是上对角线为正, 行列式为 1 的上三角矩阵构成的群

例 6.4.19.

我们考虑 $\{1, 2, 3\}$ 集合上的置换(集合上的双射). 记

$$\begin{array}{ccc} \sigma : \{1, 2, 3\} \rightarrow \{1, 2, 3\}, & \tau : \{1, 2, 3\} \rightarrow \{1, 2, 3\}, \\ 1 \mapsto 2 & 1 \mapsto 1 \\ 2 \mapsto 1 & 2 \mapsto 3 \\ 3 \mapsto 3 & 3 \mapsto 2 \end{array},$$

因此

$$\begin{array}{ccc} \tau\sigma : \{1, 2, 3\} \rightarrow \{1, 2, 3\}, & \sigma\tau : \{1, 2, 3\} \rightarrow \{1, 2, 3\}, \\ 1 \mapsto 3 & 1 \mapsto 2 \\ 2 \mapsto 1 & 2 \mapsto 3 \\ 3 \mapsto 2 & 3 \mapsto 1 \end{array},$$

注意到 σ 和 τ 都是 2 阶元. 我们令

$$H = \{e, \sigma\}, \quad K = \{e, \tau\},$$

则有

$$HK = \{e, \sigma, \tau, \sigma\tau\}, \quad KH = \{e, \tau, \sigma, \tau\sigma\}.$$

由之前的讨论知 $\sigma\tau \neq \tau\sigma$, 因此 $HK \neq KH$.

命题 6.4.20

考虑群 G 的两个子群 H 和 K , 集合 $HK < G$ 当且仅当 $HK = KH$.

证明. 首先证明若 $HK = KH$, 则 HK 是 G 的一个子群.

任取 $a \in H, x \in K$, 我们有

$$(ax)^{-1} = x^{-1}a^{-1} \in KH = HK.$$

另一方面, 任取 $a, b \in H, x, y \in K$, 我们考虑

$$(ax)(by)^{-1} = axy^{-1}b^{-1}.$$

注意到 $xy^{-1}b^{-1} \in KH = HK$, 因此存在 $\tilde{b} \in H, \tilde{z} \in K$, 满足

$$xy^{-1}b^{-1} = \tilde{b}\tilde{z}.$$

因此

$$(ax)(by) = (a\tilde{b})\tilde{z} \in HK.$$

因此 HK 是 G 的一个子群.

下边证明另一个方向的推导.

由于 $e \in HK$, 如果 $HK \in G$ 是一个子群, 则 HK 进一步满足对运算封闭和任意元素都可逆这两个条件. 下边利用这两个条件(特别是逆元存在的条件)来自证明 $HK \subset KH$, 且 $KH \subset HK$.

任取 $a \in H, x \in K$, 我们有 $(xa)^{-1} = a^{-1}x^{-1} \in HK$. 由于 $HK < G$, 我们有

$$xa = (a^{-1}x^{-1})^{-1} \in HK.$$

因此 $KH \subset HK$.

任取 $a \in H, x \in K$, 我们有 $ax \in HK$. 由于 $HK < G$, 因此 $(ax)^{-1} \in HK$. 由 HK 的构造, 存在 $b \in H$, 以及 $y \in K$, 满足

$$(ax)^{-1} = by,$$

因此 $ax = y^{-1}b^{-1} \in KH$. 所以 $HK \subset KH$. □

如果我们进一步有 H 和 K 有限, 我们还可以计算 HK 的大小.

命题 6.4.21

设 G 为一个群, H 和 K 为 G 的两个有限子群. 我们有以下群的阶的关系:

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

证明. 考虑群运算的限制, 我们可以构造一个 $H \times K$ 到 HK 的映射:

$$\begin{aligned} \phi: H \times K &\rightarrow HK \\ (a, x) &\mapsto ax \end{aligned}$$

注意到这个映射是满射. 我们下边考虑每个 HK 的元素的像集. 任取 $u \in HK$, 我们记

$$\phi^{-1}(u) = \{(a, x) \in H \times K \mid ax = u\}.$$

下边证明 $|\phi^{-1}(u)| = |H \cap K|$. (我们主要的策略就是证明 $\phi^{-1}(u)$ 中任意两对元素之间的差别可以对应到唯一的一个 $H \cap K$ 中的元素)

任取 $a, b \in H, x, y \in K$, 假设 $ax = by = u$, 我们有

$$v = a^{-1}b = xy^{-1}.$$

注意到等式左边属于 H , 右边属于 K . 因此这是一个 $H \cap K$ 中的元素. 因此, 我们有

$$u = by = a(vv^{-1})x = a(a^{-1}b)(yx^{-1})x.$$

因此, 通过考虑所有 $\phi^{-1}(u)$ 中的元素与 (a, x) 的差别, 我们构造了一个映射

$$\begin{aligned} \psi_{(a,x)} : \phi^{-1}(u) &\mapsto H \cap K. \\ (b, y) &\mapsto v \end{aligned}$$

由于 $b = av$, $y = v^{-1}x$, 因此以上映射是一个单射(群运算是个映射). 下证以上映射是一个满射. 任取 $v \in H \cap K$, 我们记

$$(b, y) = (av, v^{-1}x).$$

注意到 $\phi(b, y) = by = avv^{-1}x = ax = u$. 因此 $(b, y) \in \phi^{-1}(u)$. 因此以上映射 ψ 是一个双射.

由于 ϕ 是满射, 我们有

$$|H||K| = |H \times K| = \sum_{u \in HK} |\phi^{-1}(u)| = |HK||H \cap K|.$$

因此

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

□

我们介绍两个后边会经常用到的与正规子群相关的结论.

命题 6.4.22

设 G 为一个群, N 为 G 的一个正规子群. 任取 G 的子群 H , 则

- (i) $HN = NH$;
- (ii) HN 为 G 的一个子群, 且 $N \triangleleft HN$.

证明. (i) 由于 $N \triangleleft G$, 任取 $a \in G$, 我们有 $aN = Na$. 因此

$$HN = \{ax \mid a \in H, x \in N\} = \bigcup_{a \in H} aN = \bigcup_{a \in H} Na = \{xa \mid a \in H, x \in N\} = NH.$$

(ii) 任取 $a \in H, x \in N$, 我们有 $a^{-1} \in H, x^{-1} \in N$, 因此

$$ax \in HN, \quad (ax)^{-1} = x^{-1}a^{-1} \in NH = HN.$$

由 $N \triangleleft G$, 任取 $a, b \in H, x, y \in N$, 存在 $x' \in N$, 满足

$$(ax)(by) = (ab)(x'y) \in HN.$$

由以上两点, 任取 $a, b \in H, x, y \in N$, 我们有

$$(ax)(by)^{-1} \in HN,$$

因此 HN 是 G 的一个子群. (也可以由之前的命题直接推出)

由于 $e \in H$, 因此 $N = eN \subset HN$. 另一方面, 由于 $N \triangleleft G$, 任取 $a \in H \subset G, x \in N$, 我们有

$$axa^{-1} \in N,$$

因此 N 为 HN 的正规子群.

□

思考 6.4.23 (教材习题 1.2.16)

设 G 为一个群. 任取 G 的两个子群 H 和 K , 两个集合的乘积 HK 是否总是 G 的子群? 若不是, 请举出一个反例.

命题 6.4.24

设 G 为一个群, N 为 G 的一个正规子群. 任取 G 的子群 H , 则 $N \cap H$ 为 H 的正规子群.

证明. 由之前关于子群的讨论, 我们知道子群的任意交仍是子群. 因此 $N \cap H$ 为 G 的子群, 也是 H 的子群.

下证 $N \cap H$ 为 H 的正规子群. 任取 $a \in N \cap H \subset N$, $b \in H \subset G$, 由于 $N \triangleleft G$, 因此

$$bab^{-1} \in N,$$

右由于 $bab^{-1} \in H$, 因此我们有

$$bab^{-1} \in N \cap H.$$

因此 $N \cap H$ 为 H 的正规子群. □

6.5 商群

设 G 为一个群, N 为 G 的一个正规子群. 下边我们将围绕着定理 6.4.13 中 (iv) 给出的二元运算进行讨论.

我们考虑 N 的陪集空间 G/N 上的二元运算:

$$\begin{aligned} \cdot : G/N \times G/N &\rightarrow G/N \\ (aN, bN) &\mapsto (ab)N \end{aligned}$$

定理 6.5.1 (教材定理 1.3.6)

陪集空间 G/N 关于二元运算 $\cdot$ 构成为一个群.

证明. 任取 $a, b, c \in G$, 我们由 G 中运算的结合律可得:

$$\begin{aligned} &((aN)(bN))(cN) \\ &= ((ab)N)(cN) \\ &= ((ab)c)N \\ &= (a(bc))N \\ &= (aN)((bc)N) \\ &= (aN)((bN)(cN)) \end{aligned}$$

注意到对任意 $a \in G$

$$(aN)(eN) = (ae)N = aN = (ea)N = (eN)(aN).$$

因此该二元运算有么元 $N = eN$.

任取 $a \in G$, 我们有

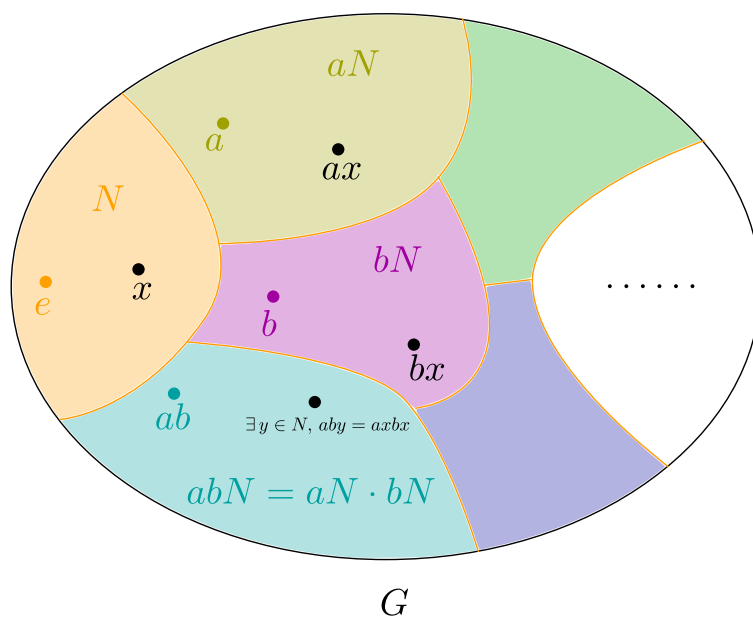
$$(aN)(a^{-1}N) = (aa^{-1})N = N = (a^{-1}a)N = (a^{-1}N)(aN).$$

因此 aN 有逆元 $a^{-1}N$.

综上所述, G/N 关于以上定义的 $\cdot$ 构成一个群. $\square$

注 6.5.2.

下边是一个正规子群 N 的陪集运算的示意图:



定义 6.5.3 (教材定理 1.3.6)

设 G 为一个群, N 为 G 的一个正规子群, 则群 G/N 被称为 G 关于 N 的**商群**.

例 6.5.4.

我们首先考虑整数加法群 $\mathbb{Z}$. 考虑 $\mathbb{Z}$ 的子群 $6\mathbb{Z}$. 由于 $\mathbb{Z}$ 是一个交换群, 因此 $6\mathbb{Z}$ 是 $\mathbb{Z}$ 的一个正规子群. 我们有

$$\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z} := \{6\mathbb{Z}, 1+6\mathbb{Z}, 2+6\mathbb{Z}, 3+6\mathbb{Z}, 4+6\mathbb{Z}, 5+6\mathbb{Z}\}.$$

利用命题 2.2.11, 我们知道任取 $m, n \in \mathbb{Z}$, 有

$$(m+6\mathbb{Z}) + (n+6\mathbb{Z}) = (m+n)+6\mathbb{Z}.$$

设 $n=0$, 则有

$$(m+6\mathbb{Z}) + 6\mathbb{Z} = m+6\mathbb{Z}.$$

此外, 我们可以验证以下关系

$$\begin{aligned} (1+6\mathbb{Z}) + (5+6\mathbb{Z}) &= (1+6\mathbb{Z}) + ((-1)+6\mathbb{Z}) = (1+(-1))+6\mathbb{Z} = 6\mathbb{Z}, \\ (2+6\mathbb{Z}) + (4+6\mathbb{Z}) &= (2+6\mathbb{Z}) + ((-2)+6\mathbb{Z}) = (2+(-2))+6\mathbb{Z} = 6\mathbb{Z}, \\ (3+6\mathbb{Z}) + (3+6\mathbb{Z}) &= (3+6\mathbb{Z}) + ((-3)+6\mathbb{Z}) = (3+(-3))+6\mathbb{Z} = 6\mathbb{Z}. \end{aligned}$$

这里我们要注意的, 以上的运算中的等号都是集合相等的意思. 商群里边的每个元素都是之前群的一个子集.

例 6.5.5.

我们考虑一个非交换群的例子: 二面体群 D_4 . 通过我们之前在陪集部分的讨论, 我们已经知道了 s 生成的子群 $\langle s \rangle$ 不是一个正规子群, 而 r 生成的子群:

$$\langle r \rangle = \{id, r, r^2, r^3\}.$$

是 D_4 的一个正规子群.

我们实际上也可以从 D_4 在 $\mathbb{R}^2$ 的作用看出来这个结论. 考虑顶点在

$$v_1 = (1, 1), v_2 = (-1, 1), v_3 = (-1, -1), v_4 = (1, -1),$$

的正方形, 注意到 v_1, v_2, v_3, v_4 在这个正方形边界上沿着逆时针顺序排列. 任取 $\langle r \rangle$ 中元素 r^j 作用之后, 顶点的像

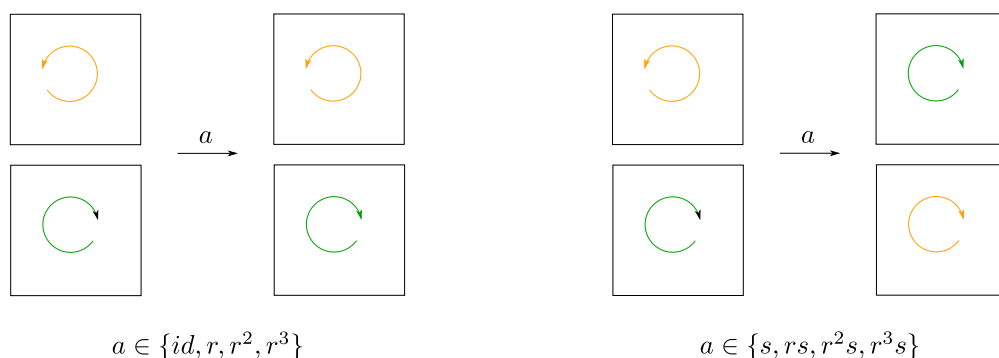
$$r^j(v_1), r^j(v_2), r^j(v_3), r^j(v_4),$$

的在边界上的排列仍是逆时针. 考虑 $D_4 \setminus \langle r \rangle$ 中的元素 $r^j s$ 作用之后, 顶点的像

$$r^j s(v_1), r^j s(v_2), r^j s(v_3), r^j s(v_4),$$

的在边界上的排列是顺时针的. 因此, 任取 $a \in D_4$, $x \in \langle r \rangle$, 则 $a^{-1}, xa^{-1}, axa^{-1}$ 作用在 v_1, v_2, v_3, v_4 上之后排列的顺序总是满足以下两种中的一种:

- (i) 逆时针-顺时针-顺时针-逆时针;
- (ii) 逆时针-逆时针-逆时针-逆时针.



由于 $\langle r \rangle$ 包含了所有使 v_1, v_2, v_3, v_4 的像逆时针排列的元素, 因此 $axa^{-1} \in \langle r \rangle$. 我们考虑 H 对应的商群:

$$D_4 / \langle r \rangle := \{\langle r \rangle, s\langle r \rangle\}.$$

我们有

$$(s\langle r \rangle)(s\langle r \rangle) = s^2\langle r \rangle = \langle r \rangle.$$

我们先在考虑一个群和它的商群之间的关系. 记 G 为一个群, $N \triangleleft G$. 记 G/N 为其商群. 由陪集的定义, 我们有如下映射

$$\begin{aligned} \pi : G &\rightarrow G/N \\ a &\mapsto aN \end{aligned}$$

由定理 6.4.13 第 (iv) 点, 我们可以进一步将其改写为:

命题 6.5.6

任取 $a, b \in G$, 我们有

$$\pi(ab) = \pi(a)\pi(b).$$

我们后边介绍完群同态之后, 就可以看出, 这个命题实际上在说映射 π 是一个从 G 到 G/N 的同态映射.

定义 6.5.7 (教材定义 1.3.11)

任取群 G 和它的正规子群 N , 映射

$$\begin{aligned}\pi : G &\rightarrow G/N \\ a &\mapsto aN\end{aligned}$$

被称作群 G 到商群 G/N 的**自然同态**.

注 6.5.8.

定理 6.3.9 告诉我们, 从等价关系的角度来看, G/N 中也是一个等价关系的等价类集合. 在后续讨论中, 我们有时也会使用等价类的记号来记陪集: $\bar{a} = aN$.

第七章 群同态

考虑 D_4 中由 r 生成的子群

$$\langle r \rangle = \{id, r, r^2, r^3\},$$

以及 $\mathbb{Z}_4$. 考虑下边的映射:

$$\begin{aligned}\phi: \langle r \rangle &\rightarrow \mathbb{Z}_4 \\ id &\mapsto 0 + 4\mathbb{Z} \\ r &\mapsto 1 + 4\mathbb{Z} \\ r^2 &\mapsto 2 + 4\mathbb{Z} \\ r^3 &\mapsto 3 + 4\mathbb{Z}\end{aligned}$$

我们注意到首先映射 ϕ 是一个双射, 其次 ϕ 还满足以下条件:

$$\phi(r^i \cdot r^j) = (i + j) + 4\mathbb{Z} = (i + 4\mathbb{Z}) + (j + 4\mathbb{Z}) = \phi(r^i) + \phi(r^j).$$

因此, 虽然 $\langle r \rangle$ 包含的元素是平面的角度为 $\pi/4$ 的倍数的旋转映射和 $\mathbb{Z}_4$ 包含的是整数关于 4 的所有同余等价类, 但是从一个带二元运算的集合的角度来看, 二者没有本质区别. 这时当我们研究与二元运算相关的性质的时候, 二者是相同的. 例如, 二者都是交换群, 二者都包含两个 4 阶元素, 一个 2 阶元素等等.

我们在研究群的过程中会遇到两个群看起来不一样, 但其代数结构可能是相似甚至相同的. 这种相似性就是通过群同态或者群同构来描述的. 这是本节以及下节关心的主要对象. 我们首先给出群同态以及群同构的定义.

7.1 定义

定义 7.1.1 (教材定义 1.4.1)

设 $(G, *)$ 和 $(H, \diamond)$ 为两个群. 设

$$\phi: G \rightarrow H$$

为一个从 G 到 H 的映射. 映射 ϕ 被称为一个**群同态**, 若 ϕ 满足对于任意 $a, b \in G$, 我们有

$$\phi(a * b) = \phi(a) \diamond \phi(b).$$

若同态 ϕ 是单射(满射, 双射), 我们称之为**单同态**(**满同态**, **群同构**).

特别地, 若有 $G = H$, 我们称群同态(群同构) ϕ 为群 G 的一个**自同态**(**自同构**).

注 7.1.2.

我们利用 ϕ 定义如下映射:

$$\begin{aligned}D_\phi: G \times G &\rightarrow H \times H \\ (a, b) &\mapsto (\phi(a), \phi(b))\end{aligned}$$

以上定义中的条件也可以用交换图表示:

$$\begin{array}{ccc}
 G \times G & \xrightarrow{*} & G \\
 D_\phi \downarrow & & \downarrow \phi \\
 H \times H & \xrightarrow{\diamond} & H
 \end{array}
 \qquad
 \begin{array}{ccc}
 (a, b) & \xrightarrow{*} & a * b \\
 D_\phi \downarrow & & \downarrow \phi \\
 (\phi(a), \phi(b)) & \xrightarrow{\diamond} & \phi(a) \diamond \phi(b)
 \end{array}$$

注 7.1.3.

以上为了清楚的介绍同态的概念, 我们使用不同的记号来记不同群的运算. 以下为了简化记号, 我们将不再标明不同群的群运算.

定义 7.1.4

任给两个群 G 和 H , 若存在一个群同构:

$$\phi: G \rightarrow H,$$

我们称 G 和 H **同构**, 记作 $G \cong H$.

例 7.1.5.

任何群 G 都满足 $G \cong G$. 我们考虑 G 上的恒等映射:

$$\begin{aligned}
 id: G &\rightarrow G \\
 a &\mapsto a
 \end{aligned}$$

这是一个群 G 的自同构.

例 7.1.6 (教材例 1.4.4).

我们考虑 $(\mathbb{R}, +)$ 和 $(\mathbb{R}_{>0}, \cdot)$, 则指数映射

$$\begin{aligned}
 \exp: \mathbb{R} &\rightarrow \mathbb{R}_{>0} \\
 x &\mapsto \exp x
 \end{aligned}$$

是一个群同构.

例 7.1.7 (教材例 1.4.5).

设 V 和 W 是两个 $\mathbb{R}$ 上的线性空间. 我们可以考虑向量加法将 V 和 W 看作交换群. 设

$$\phi: V \rightarrow W,$$

为一个线性变换, 则由线性变换的定义, 我们知道 ϕ 是一个群同态.

注 7.1.8.

正如本节开始的时候讨论的一样, 同构的群结构具有相同的代数性质. 因此, 当我们只关系代数性质的时候, 通常会在"群同构意义下"考虑问题. 另一方面, 群的分类也是群论中研究的重要问题之一.

以下关于群同态的结论, 可以与线性代数中关于线性映射的结论做一个对比.

命题 7.1.9

若 ϕ 为一个从 G 到 H 的群同态, 则

(i) 记 e_G 和 e_H 分别为群 G 和 H 的幺元, 我们有 $\phi(e_G) = e_H$;

(ii) 对于任意 $a \in G$, 我们有 $\phi(a^{-1}) = (\phi(a))^{-1}$.

证明. (i) 我们考虑

$$\phi(e_G) = \phi(e_G e_G) = \phi(e_G) \phi(e_G).$$

利用消去律, 我们有 $\phi(e_G) = e_H$.

(ii) 任取 $a \in G$, 我们有

$$e_H = \phi(e_G) = \phi(a a^{-1}) = \phi(a) \phi(a^{-1}).$$

由逆元的唯一性 (H 中),

$$(\phi(a))^{-1} = \phi(a^{-1}).$$

□

命题 7.1.10 (教材命题 1.4.3)

(i) 设 G 和 H 为两个群. 设存在群同态:

$$\phi : G \rightarrow H.$$

则任取 G 的子群 K , $\phi|_K$ 为一个 K 到 H 的群同态.

(ii) 设 G, H 和 K 为三个群. 若

$$\phi : G \rightarrow H, \quad \psi : H \rightarrow K,$$

为两个群同态, 则复合映射

$$\psi \circ \phi : G \rightarrow K,$$

也是群同态.

(iii) 若

$$\phi : G \rightarrow H,$$

为一个群同构, 则 ϕ 有逆映射

$$\phi^{-1} : H \rightarrow G,$$

且 ϕ^{-1} 是一个从 H 到 G 的群同构.

证明. (i) 由 K 为子群, 我们有任取 $a, b \in K$, $ab \in K$. 由映射在子集上的限制的定, 我们有

$$\phi|_K(ab) = \phi(ab) = \phi(a)\phi(b) = \phi|_K(a)\phi|_K(b).$$

因此 $\phi|_K$ 是 K 到 H 的群同态.

(ii) 任取 $a, b \in G$, 由映射复合的定义可得:

$$\begin{aligned} (\psi \circ \phi)(ab) &= \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) \\ &= \psi(\phi(a))\psi(\phi(b)) = (\psi \circ \phi)(a)(\psi \circ \phi)(b). \end{aligned}$$

其中第二个等号和第三个等号分别使用了 ϕ 是群同态以及 ψ 是群同态的条件. 因此 $\psi \circ \phi$ 是一个群同态.

$$\begin{array}{ccc} G & \xrightarrow{\psi \circ \phi} & K \\ & \searrow \phi & \nearrow \psi \\ & H & \end{array}$$

(iii) 由于 ϕ 为一个双射, 因此其逆映射 ϕ^{-1} 也是一个双射. 我们只需要验证 ϕ^{-1} 是一个群同态即可. 任取 $x, y \in H$, 由于 ϕ 为同构, 因此存在 $a, b \in G$, 满足

$$\phi(a) = x, \quad \phi(b) = y, \quad \phi(ab) = xy.$$

因此由 ϕ^{-1} 的定义我们有

$$\phi^{-1}(x) = a, \quad \phi^{-1}(y) = b, \quad \phi^{-1}(xy) = ab = \phi^{-1}(x)\phi^{-1}(y).$$

因此 ϕ^{-1} 为一个群同构.

$$G \xrightleftharpoons[\phi^{-1}]{\phi} H$$

□

定义 7.1.11 (教材定义 1.4.11)

设 G 和 H 为两个群, 并设

$$\phi: G \rightarrow H,$$

为一个群同态. 我们称以下集合为 ϕ 的核:

$$\ker \phi := \{a \in G \mid \phi(a) = e_H \in H\} \subset G.$$

我们称以下集合为 ϕ 的像:

$$\operatorname{Im} \phi := \{x \in H \mid \exists a \in G, \phi(a) = x\} \subset H.$$

命题 7.1.12 (教材引理 1.4.12, 1.4.13)

我们沿用以上定义中的记号.

- (i) $\ker \phi$ 是 G 的一个正规子群.
- (ii) 同态 ϕ 的像集 $\phi(G)$ 为 H 的一个子群.
- (iii) ϕ 为单同态当且仅当 $\ker \phi = \{e_G\}$.

证明. (i) 我们有 $e_G \in \ker \phi$. 因此 $\ker \phi$ 非空.

其次任取 $a, b \in \ker \phi$, 我们有

$$\phi(ab^{-1}) = \phi(a)(\phi(b))^{-1} = e_H e_H^{-1} = e_H.$$

因此 $ab^{-1} \in \ker \phi$. 因此 $\ker \phi$ 为 G 的一个子群.

下证 $\ker \phi$ 是一个正规子群. 任取 $a \in G, b \in \ker \phi$, 我们有

$$\phi(aba^{-1}) = \phi(a)\phi(b)\phi(b)^{-1} = \phi(a)e_H\phi(a)^{-1} = e_H.$$

因此 $aba^{-1} \in \ker \phi$. 所以 $\ker \phi$ 为 G 的一个正规子群.

(ii) 注意到 $e_H \in \phi(G)$. 任取 $x, y \in \phi(G)$, 存在 $a, b \in G$, 满足

$$\phi(a) = x, \quad \phi(b) = y.$$

因此

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(G).$$

由定理 6.2.10 可知, $\phi(G)$ 为 H 的一个子群.

(iii) 我们假设 ϕ 为单同态. 由于

$$e_H = \phi(e_G) \in \phi(G).$$

由于 ϕ 是单射, 任取 $a \in G$, 满足 $\phi(a) = e_H$, 我们有 $a = e_G$. 因此 $\ker \phi = \{e_G\}$.

反过来, 设 $\ker \phi = \{e_G\}$. 任取 $a, b \in G$, 满足 $\phi(a) = \phi(b)$, 我们有

$$\phi(ab^{-1}) = \phi(a)(\phi(b))^{-1} = e_H.$$

因此 $ab^{-1} \in \ker \phi$, 即 $ab^{-1} = e_G$. 因此 $a = b$. 由单射定义知, ϕ 为单射.

□

例 7.1.13.

设 G 为一个群, 记 N 为 G 的一个正规子群. 我们考虑自然同态:

$$\pi : G \rightarrow G/N.$$

商群 G/N 的么元是 N .

任取 $a \in G$, 由命题 6.3.2 中陪集的性质, 我们知道

$$aN = N \Leftrightarrow a \in N.$$

因此

$$\ker \pi = N.$$

例 7.1.14.

考虑二面体群 D_4 中的元素 r 生成的子群

$$H = \{id, r, r^2, r^3\}.$$

我们可以定义映射

$$\begin{aligned} \phi : \mathbb{Z} &\rightarrow H \\ n &\mapsto r^n \end{aligned}$$

这是一个同态映射, 并且

$$\ker \phi = 4\mathbb{N}.$$

例 7.1.15.

下边是以上例子的推广. 设 G 为一个群, a 为 G 中的元素. 我们设 a 的阶为 k , 则存在以下群同态:

$$\begin{aligned}\phi: \mathbb{Z} &\rightarrow \langle a \rangle \\ n &\mapsto a^n\end{aligned}$$

由于 a 的阶为 k , 因此 $a^k = e$. 因此我们有

$$\ker \phi = k\mathbb{Z}.$$

例 7.1.16.

设 $n \in \mathbb{N}^*$. 我们考虑 $\mathbb{R}$ 上的一般线性群 $\mathrm{GL}(n, \mathbb{R})$. 考虑矩阵的行列式, 由于 $\mathrm{GL}(n, \mathbb{R})$ 中的矩阵行列式都非零, 我们有如下映射:

$$\begin{aligned}\det: \mathrm{GL}(n, \mathbb{R}) &\rightarrow \mathbb{R}^* \\ A &\mapsto \det A\end{aligned}$$

我们考虑 $\mathbb{R}^*$ 关于乘法构成的群. 由行列式的性质, 任给 $A, B \in \mathrm{GL}(n, \mathbb{R})$, 我们有

$$\det(AB) = \det A \det B.$$

因此 $\det$ 是一个群同态.

作为乘法群 $\mathbb{R}^*$ 的么元是 1. 因此

$$\ker \det = \{A \in \mathrm{GL}(n, \mathbb{R}) \mid \det A = 1\} = \mathrm{SL}(n, \mathbb{R}).$$

为特殊线性群.

例 7.1.17.

设 G 为一个群. 我们考虑 G 上所有到自己的双射:

$$S_G := \{f: G \rightarrow G \text{ 为双射}\}.$$

我们使用映射的复合可以在 S_G 上定义一个二元运算. 映射的复合满足结合律. 考虑恒等映射

$$\begin{aligned}id: G &\rightarrow G \\ a &\mapsto a\end{aligned}$$

和任意 $f \in S_G$, 我们有

$$id \circ f = f \circ id = f.$$

最后任意 G 上的双射都有逆映射也是双射, 并且二者复合就是 G 上的恒等映射. 综上所述, 映射复合运算在 S_G 给出了一个群结构. (注意这个构造对任意非空集合都成立.)

考虑 G 上的左平移映射, 我们证明 G 的任意元素给出的左平移映射都是 G 上的双射. 因此我们可以构造以下映射:

$$\begin{aligned}\phi: G &\rightarrow S_G, \\ a &\mapsto L_a.\end{aligned}$$

注意到任给 $a, b \in G$, 考虑对应的左平移映射 L_a 和 L_b , 任给 $c \in G$, 我们有

$$(L_a \circ L_b)(c) = L_a(L_b(c)) = L_a(bc) = a(bc) = (ab)c = L_{ab}(c).$$

因此, 我们有 $L_{ab} = L_a \circ L_b$. 映射 ϕ 是一个群同态.

任取 $a \in G$, 若对任意 $b \in G$, 都有

$$L_a(b) = b,$$

则 $a = e$. 因此 $\ker \phi = \{e\}$, ϕ 是一个单射. 因此我们有同构

$$G \cong \text{Im}(\phi) < S_G.$$

我们可以将其表述为以下定理.

定理 7.1.18 (教材定理 1.4.10: Cayley 定理)

任何群 G 都和 G 的对称群 S_G 的一个子群同构.

实际上, 群元素的左平移映射给出了群 G 在 G (作为集合) 上的一个作用. 这是群在几何上的作用的一个基本的例子. 我们后边会详细介绍群作用的概念.

思考 7.1.19

我们可以使用右平移映射来进行以上讨论么? 为什么?

7.2 群同态基本定理

我们回顾前一节中提到的例子. 考虑同态映射

$$\begin{aligned} \phi: \mathbb{Z} &\rightarrow D_4 \\ n &\mapsto r^n \end{aligned}$$

我们知道这个映射的核是

$$\ker \phi = 4\mathbb{N}.$$

它的像是

$$\text{Im} \phi = \{id, r, r^2, r^3\}.$$

注意到

$$\mathbb{Z} / \ker \phi = \mathbb{Z} / 4\mathbb{Z}.$$

另一方面, 我们之前曾讨论过

$$\mathbb{Z} / 4\mathbb{Z} \cong \{id, r, r^2, r^3\}.$$

7.2.1 群同态基本定理

实际上我们看到的是以下的一般结论的在具体例子上的应用(或者体现).

命题 7.2.1 (教材定理 1.4.19: 群同态基本定理)

设 G 和 H 是两个群. 设

$$\phi: G \rightarrow H,$$

为一个群同态, 则我们有群同构:

$$G / \ker \phi \cong \text{Im} \phi.$$

注 7.2.2.

我们在高等代数中学习过维数定理: 任取 $\mathbb{R}$ 上的有限维线性空间 V 和 W , 设

$$L: V \rightarrow W,$$

为一个线性映射, 那么我们有

$$\dim V = \dim \ker L + \dim \operatorname{Im} L.$$

维数相等则线性空间同构, 因此作为线性空间

$$V / \ker L \cong \operatorname{Im} L.$$

如果将它们看作关于向量加法的群, 则由线性映射的定义, 这也是一一个群同构. (要注意的是向量空间之间的关于向量加法的群同态映射不一定是线性映射)

证明. 以下证明是构造性的, 即我们将构造出来一个 $G / \ker \phi$ 和 $\operatorname{Im} \phi$ 之间的同构.

1. 任取 $a \in G$, 我们考虑它在 ϕ 下的像 $\phi(a) \in H$. 我们定义:

$$\begin{aligned} \bar{\phi}: G / \ker \phi &\rightarrow H, \\ a \ker \phi &\mapsto \phi(a). \end{aligned}$$

我们首先证明 $\bar{\phi}$ 是一个映射. 我们需要验证 $\bar{\phi}(a \ker \phi)$ 不依赖于 $a \ker \phi$ 的代表元的选取, 即任取 $b \in \ker \phi$, 我们有

$$\bar{\phi}(a \ker \phi) = \phi(b).$$

注意到存在 $c \in \ker \phi$, 满足 $b = ac$, 因此

$$\phi(b) = \phi(ac) = \phi(a)\phi(c) = \phi(a) = \bar{\phi}(a \ker \phi).$$

因此 $\bar{\phi}$ 是一个映射.

2. 我们下边证明 $\bar{\phi}$ 是一个群同态. 任取 $a, b \in G$, 我们有

$$\bar{\phi}((a \ker \phi)(b \ker \phi)) = \bar{\phi}((ab) \ker \phi) = \phi(ab) = \phi(a)\phi(b) = \bar{\phi}(a \ker \phi)\bar{\phi}(b \ker \phi).$$

因此 $\bar{\phi}$ 是一个群同构.

3. 我们最后证明 $\bar{\phi}$ 给出 $G / \ker \phi$ 和 $\operatorname{Im} \phi$ 之间的双射. 任取 $a, b \in G$, 若

$$\bar{\phi}(a \ker \phi) = \bar{\phi}(b \ker \phi),$$

我们有

$$\phi(a) = \phi(b),$$

因此

$$e_H = \phi(a)^{-1}\phi(b) = \phi(a^{-1}b).$$

这说明 $a^{-1}b \in \ker \phi$. 因此我们有 $a \ker \phi = b \ker \phi$, $\bar{\phi}$ 为单射.

另一方面, 任取 $x \in \operatorname{Im} \phi$, 由像集的定义, 我们知道存在 $a \in G$, 满足

$$\phi(a) = x.$$

因此我们有

$$\bar{\phi}(a \ker \phi) = x,$$

映射 $\bar{\phi}$ 为满射.

综上所述 $\bar{\phi}$ 给出 $G / \ker \phi$ 和 $\operatorname{Im} \phi$ 之间的同构. □

注 7.2.3.

考虑以上定义的映射 $\bar{\phi}$, 我们可以得到以下交换图:

$$\begin{array}{ccc} G & \xrightarrow{\phi} & H \\ \pi \downarrow & \nearrow \bar{\phi} & \\ G/\ker \phi & & \end{array}$$

注 7.2.4.

这个定理也被称为第一群同构定理.

以下是群同态基本定义的一个直接推论

推论 7.2.5

设 G 和 H 为两个群. 设存在满同态

$$\phi : G \rightarrow H,$$

那么我们有

$$G/\ker \phi \cong H.$$

注 7.2.6.

笼统地说, 如果存在一个从 G 到 H 的群满同态, 我们就可以在同构意义下将 H 看作是 G 的一个商群.

例 7.2.7.

设 G 为循环群, a 为生成元, 因此 $G = \langle a \rangle$. 我们有满同态

$$\begin{aligned} \phi : \mathbb{Z} &\rightarrow \langle a \rangle \\ n &\mapsto a^n \end{aligned}$$

由之前的讨论知, 若 $o(a) = m$, 则 $\ker \phi = m\mathbb{Z}$. 因此

$$G \cong \mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}.$$

注意到若整数 $|m| \neq |n|$, 则 $\mathbb{Z}_m \not\cong \mathbb{Z}_n$, 因此我们实际上在同构意义下给所有循环群一个分类.

7.2.2 群同态与子群

我们下面讨论一个 G 到 H 的群同态在 G 的子群和 H 的子群之间建立怎样的联系

命题 7.2.8

设 G 和 H 为两个群. 设存在群同态

$$\phi : G \rightarrow H.$$

(i) 任取 G 的子群 K , 则 K 的像 $\phi(K)$ 为 H 的一个子群.

(ii) 任取 H 的子群 L , 则 L 的原像

$$\phi^{-1}(L) := \{a \in G \mid \phi(a) \in L\},$$

是 G 的一个子群, 且 $\ker \phi < \phi^{-1}(L)$.

证明. (i) 由定理 7.1.10 (i) 和命题 7.1.12 (ii) 可得结论.

(ii) 任取 H 的子群 L , 我们有

$$e_H \in L.$$

由于

$$\phi(e_G) = e_H,$$

我们有

$$e_G \in \phi^{-1}(L).$$

因此 $\phi^{-1}(L)$ 非空.

下边我们证明 $\phi^{-1}(L)$ 为一个子群.

(a) 我们首先证明任取 $a \in \phi^{-1}(L)$, 我们有 $a^{-1} \in \phi^{-1}(L)$.

任取 $a \in \phi^{-1}(L)$, 则存在 $x \in L$, 满足

$$\phi(a) = x.$$

考虑元素的逆, 我们有

$$\phi(a^{-1}) = x^{-1} \in L,$$

因此 $a^{-1} \in \phi^{-1}(L)$.

(b) 任取 $a, b \in \phi^{-1}(L)$, 我们有 $x, y \in L$, 满足

$$\phi(a) = x, \phi(b) = y.$$

由同态的定义以及 L 为子群, 我们有

$$\phi(ab) = \phi(a)\phi(b) = xy \in L,$$

因此 $ab \in \phi^{-1}(L)$.

因此任取 $a, b \in \phi^{-1}(L)$, 我们有 $ab^{-1} \in \phi^{-1}(L)$. 由定理 6.2.10, 我们有 $\phi^{-1}(L)$ 为 G 的一个子群.

由于 $e_H \in L$, 我们有 $\ker \phi < \phi^{-1}(L)$.

□

命题 7.2.9

设 G 和 H 为两个群. 设存在群同态

$$\phi: G \rightarrow H.$$

我们有

- (i) 任取 H 的正规子群 M , 其逆像 $\phi^{-1}(M)$ 为 G 的正规子群;
- (ii) 设 ϕ 为满同态, 任取 G 的正规子群 N , 满足 $N \triangleleft G$, 则 $\phi(N)$ 为 H 的正规子群.

证明. (i) 任取 $a \in \phi^{-1}(M)$, 存在 $x \in M$, 满足 $\phi(a) = x$. 任取 $b \in G$, 我们有

$$\phi(bab^{-1}) = \phi(b)x(\phi(b))^{-1}.$$

由于 $M \triangleleft H$, 我们有 $\phi(b)x(\phi(b))^{-1} \in M$, 因此 $bab^{-1} \in \phi^{-1}(M)$. 由定义知 $\phi^{-1}(M)$ 是 G 的正规子群.

- (ii) 由于 ϕ 是一个群同态, 因此 $\phi(N)$ 为 H 的一个子群. 我们下边需要证明这个子群是正规的. 任取 $x \in \phi(N)$, 存在 $a \in N$, 满足

$$\phi(a) = x.$$

任取 $y \in H$, 由于 ϕ 为满射, 因此存在 $b \in G$, 满足

$$\phi(b) = y.$$

我们有

$$yxy^{-1} = \phi(b)\phi(a)\phi(b)^{-1} = \phi(bab^{-1}).$$

由于 $N \triangleleft G$, 我们有 $bab^{-1} \in N$, 因此 $yxy^{-1} \in \phi(N)$.

综上所述 $\phi(N) \triangleleft H$.

□

思考 7.2.10

若在上述命题中, 我们不要求同态 ϕ 是一个满射, 那么以上命题还成立么? 成立的话, 请给出证明; 不成立的话, 请给出反例.

命题 7.2.11 (教材定理 1.4.23)

设 G 和 H 为两个群. 设存在群同态

$$\phi: G \rightarrow H.$$

任取 G 的子群 K , 我们有

- (i) $\phi(K) = \phi(K \ker \phi)$;
- (ii) $K \ker \phi = \phi^{-1}(\phi(K))$.

证明. (i) 由 $e_G \in \ker \phi$, 我们有

$$K \subset K \ker \phi,$$

因此

$$\phi(K) \subset \phi(K \ker \phi).$$

另一方面, 任取 $a \in K \ker \phi$, 存在 $b \in K, x \in \ker \phi$, 满足 $a = bx$, 继而有

$$\phi(a) = \phi(bx) = \phi(b)\phi(x) = \phi(b).$$

因此

$$\phi(K \ker \phi) \subset \phi(K).$$

综上所述, 我们有 $\phi(K \ker \phi) = \phi(K)$.

(ii) 由 (i), 我们有

$$K \ker \phi \subset \phi^{-1}(\phi(K)).$$

另一方面, 任取 $a \in \phi^{-1}(\phi(K))$, 存在一个 $b \in K$, 满足

$$\phi(a) = \phi(b).$$

因此

$$\phi(b^{-1}a) = \phi(b)^{-1}\phi(a) = e_H,$$

由此可得 $b^{-1}a \in \ker \phi$. 我们可以将 a 写为

$$a = (bb^{-1})a = b(b^{-1}a) \in K \ker \phi.$$

因此

$$\phi^{-1}(\phi(K)) \subset K \ker \phi.$$

综上所述, 我们有

$$K \ker \phi = \phi^{-1}(\phi(K)).$$

□

从以上证明的结论, 我们可以得到以下结论.

定理 7.2.12 (教材定理 1.4.21)

设 G 和 H 为两个群. 设存在满同态

$$\phi: G \rightarrow H.$$

我们有如下结论:

(i) ϕ 诱导以下 G 的包含 $\ker \phi$ 的子群集和 H 的子群集之间的映射:

$$\phi: \{K \mid \ker \phi < K < G\} \rightarrow \{L \mid L < H\}.$$

并且该映射是一个双射.

(ii) ϕ 诱导以下 G 的包含 $\ker \phi$ 的正规子群集和 H 的正规子群集之间的映射:

$$\phi: \{K \mid \ker \phi < K \triangleleft G\} \rightarrow \{L \mid L \triangleleft H\}.$$

并且该映射是一个双射.

(iii) 任取 $K \triangleleft G$, 且 $\ker \phi < K$, 我们有

$$G/K \cong H/\phi(K).$$

证明. (i) 由命题 7.2.8, 定理叙述中的映射是良定义的. 并且我们可以定义以下映射:

$$\begin{aligned}\phi^{-1} : \{L \mid L < H\} &\rightarrow \{K \mid \ker \phi < K < G\} \\ L &\mapsto \phi^{-1}(L)\end{aligned}$$

我们注意到若 $K < G$, 满足 $\ker \phi < K$, 则有

$$K = K \ker \phi.$$

因此由命题 7.2.11 (ii), 我们有

$$\phi^{-1} \circ \phi : \{K \mid \ker \phi < K < G\} \rightarrow \{K \mid \ker \phi < K < G\},$$

是恒等映射. 因此 ϕ 是单射. 另一方面, 任取 $L < H$, 我们总有 $\phi(\phi^{-1}(L))$, 因此

$$\phi \circ \phi^{-1} : \{L \mid L < H\} \rightarrow \{L \mid L < H\},$$

是恒等映射. 因此 ϕ 是满射. 综上所述, ϕ 是双射.

(ii) 利用命题 7.2.9, 证明与 (i) 类似.

(iii) 由于 K 是 G 的一个正规子群, 因此 $\phi(K)$ 是 H 的正规子群. 我们考虑同态映射的复合

$$\begin{array}{ccc} G & \xrightarrow{\pi \circ \phi} & H/\phi(K) \\ & \searrow \phi & \nearrow \pi \\ & H & \end{array}$$

任取 $a \in G$, 若

$$(\pi \circ \phi)(a) = \pi(\phi(K)) = \phi(K),$$

我们有

$$\phi(aK) = \phi(a)\phi(K) = \phi(K).$$

因此由 (ii), 我们有

$$a \in \phi^{-1}(\phi(aK)) = \phi^{-1}(\phi(K)) = K.$$

因此

$$\ker(\pi \circ \phi) = K.$$

由于 ϕ 和 π 都是满射, 因此 $\pi \circ \phi$ 也是满射. 利用群同态基本定理的推论, 我们有

$$G/K \cong H/\pi(K).$$

□

注 7.2.13.

(iii) 的证明过程是我们经常会用到的, 通常为了证明一个商群 G/N 和某个群 H 同构, 我们首先构造 G 到 H 的满同态, 然后证明这个同态的核是 N , 利用同态基本定理, 我们就得到了所求的同构.

我们下边考虑以上定理在一个特殊情况下的应用.

推论 7.2.14 (教材推论 1.4.22)

设 G 为一个群, N 为 G 的一个正规子群. 记

$$\pi: G \rightarrow G/N,$$

为自然同态. 我们有如下结论:

(i) π 诱导以下 G 的包含 N 的子群集和 G/N 的子群集之间的映射:

$$\pi: \{K \mid N < K < G\} \rightarrow \{L \mid L < G/N\}.$$

并且该映射是一个双射.

(ii) π 诱导以下 G 的包含 N 的正规子群集和 G/N 的正规子群集之间的映射:

$$\pi: \{K \mid N < K \triangleleft G\} \rightarrow \{L \mid L \triangleleft G/N\}.$$

并且该映射是一个双射.

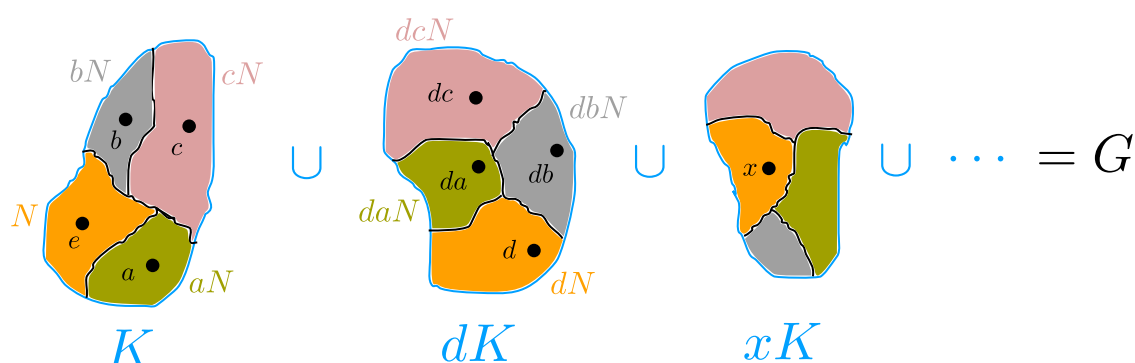
(iii) 任取 $K \triangleleft G$, 且 $N < K$, 我们有

$$G/K \cong (G/N)/(K/N).$$

证明. 将定理中的 H 替换为 G/N , ϕ 替换为自然同态 π . 注意到 $\ker \pi = N$, 因此我们有以上推论. $\square$

注 7.2.15.

这个推论也被称为第三群同构定理. 以下是在以上定理中 (iii) 的条件下, G 关于 N 的陪集划分和关于 K 的陪集划分的关系的示意图:

**定理 7.2.16 (教材定理 1.4.23)**

设 G 为一个群, N 为 G 的一个正规子群. 任取 G 的一个群 H , 我们有群同构:

$$HN/N \cong H/(H \cap N).$$

证明. 群 H 是 HN 的一个子群. 我们考虑 H 到 HN 的嵌入映射:

$$\begin{aligned} j: H &\rightarrow HN \\ a &\mapsto a \end{aligned}$$

这是一个群同态.

由命题 6.4.24, 由于 $N \triangleleft G$, 因此有 $N = N \cap HN \triangleleft HN$. 我们考虑自然同态:

$$\begin{aligned} \pi: HN &\rightarrow HN/N \\ a &\mapsto aN \end{aligned}$$

我们考虑同态的复合

$$\begin{array}{ccc} H & \xrightarrow{\pi \circ j} & HN/N \\ & \searrow j & \nearrow \pi \\ & HN & \end{array}$$

以下我们将证明

- (i) $\pi \circ j$ 为满同态;
 - (ii) $\ker(\pi \circ j) = H \cap N$.
- (i) 任取 $a \in HN$, 存在 $b \in H, c \in N$, 满足 $a = bc$. 因此我们有

$$aN = bcN = bN = (\pi \circ j)(b).$$

因此, $\pi \circ j$ 为满同态.

- (ii) 任取 $a \in H$, 满足 $(\pi \circ j)(a) = N$, 我们有 $a \in N$, 因此 $a \in H \cap N$. 由此可得

$$\ker(\pi \circ j) \subset H \cap N.$$

另一方面, 任取 $a \in H \cap N$, 由 $\pi \circ j$ 的定义, 我们有 $(\pi \circ j)(a) = N$, 因此

$$H \cap N \subset \ker(\pi \circ j).$$

由以上两个关系我们有

$$\ker(\pi \circ j) = H \cap N.$$

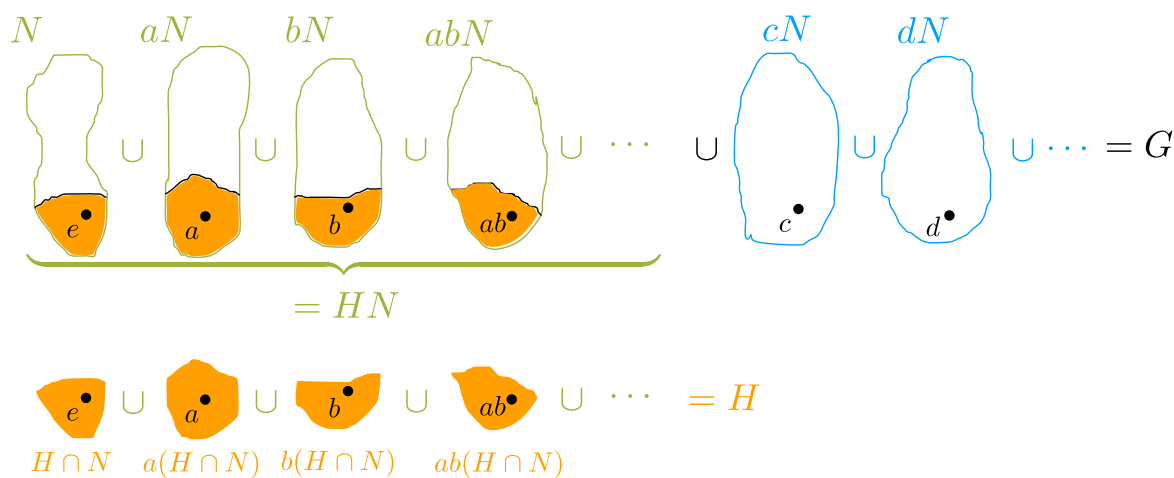
综合以上所得, 由群同态基本定理, 我们有群同构

$$HN/N \cong H/(H \cap N).$$

□

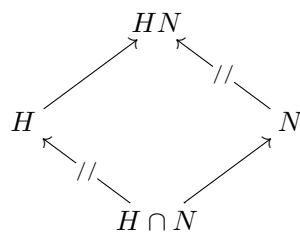
注 7.2.17.

这个定理也被成为第二群同构定理. 以下我们给出这个定理涉及的 HN 关于 N 的陪集分解, 以及 H 关于 $H \cap N$ 的陪集分解的关系的示意图:



注 7.2.18.

这个定理还有一个名字叫钻石定理, 因为我们可以将所涉及的 G 的子群的关系表示如下图:



以上定理讨论的是画斜线的两个包含关系之间的关系

注 7.2.19.

关于同态基本定理更一般的讨论可以参考讲义最后的附录 A.

7.3 给定群之间的同态

我们之前对群同态这个概念有了一定的了解. 本节我们考虑的问题是, 如果给定两个群 G 和 H , 那么从 G 到 H 的同态映射有多少? 这些同态映射构成的集合是否也有某种代数结构?

我们首先介绍以下记号:

定义 7.3.1

设 G 和 H 为两个群. 我们记所有从 G 到 H 的群构成的同态的集合为

$$\text{Hom}(G, H) := \{\phi : G \rightarrow H \mid \phi \text{ 为群同态}\}.$$

任给两个群之间都至少有一个平凡的群同态:

$$\begin{aligned} \phi_e : G &\rightarrow H, \\ a &\mapsto e_H. \end{aligned}$$

因此我们有

命题 7.3.2

任取群 G 和 H , 集合 $\text{Hom}(G, H)$ 非空.

同态的乘积

下边我们固定群 G 和 H , 记 $\phi, \psi \in \text{Hom}(G, H)$. 我们可以构造如下映射:

$$\begin{aligned}\phi \cdot \psi : G &\rightarrow H \\ a &\mapsto \phi(a)\psi(a)\end{aligned}$$

一般情况下这个映射 $\phi \cdot \psi$ 不是一个同态. 要理解这点, 我们任取 $a, b \in G$, 考虑

$$\begin{aligned}(\phi \cdot \psi)(ab) &= \phi(ab)\psi(ab) = \phi(a)\phi(b)\psi(a)\psi(b). \\ (\phi \cdot \psi)(a)(\phi \cdot \psi)(b) &= \phi(a)\psi(a)\phi(b)\psi(b).\end{aligned}$$

因此对 $a, b \in G$, 满足群同态的条件

$$(\phi \cdot \psi)(ab) = (\phi \cdot \psi)(a)(\phi \cdot \psi)(b),$$

当且仅当 $\psi(a)\phi(b) = \phi(b)\psi(a)$.

如果 H 是一个交换群, 则以上条件自然满足. 实际上我们还会得到一个更强的结论.

命题 7.3.3

任取群 G 和交换群 H , 以下映射

$$\begin{aligned}\cdot : \text{Hom}(G, H) \times \text{Hom}(G, H) &\rightarrow \text{Hom}(G, H) \\ (\phi, \psi) &\mapsto \phi \cdot \psi\end{aligned}$$

给出 $\text{Hom}(G, H)$ 上一个交换群结构.

证明. 由 H 交换以及之前的讨论知, 以上映射是良定义的, 给出 $\text{Hom}(G, H)$ 一个二元运算.

由 H 中运算满足结合律, 我们得到以上定义的 $\text{Hom}(G, H)$ 上的运算满足结合律. 因此以上运算给出了 $\text{Hom}(G, H)$ 的一个半群结构.

注意到

$$\begin{aligned}\phi_e : G &\rightarrow H \\ a &\mapsto e_H\end{aligned}$$

属于 $\text{Hom}(G, H)$.

任取 $\phi \in \text{Hom}(G, H)$, 任取 $a \in G$, 我们有

$$(\phi \cdot \phi_e)(a) = \phi(a)e_H = \phi(a) = e_H\phi(a) = (\phi_e \cdot \phi)(a).$$

因此 ϕ_e 是 $\text{Hom}(G, H)$ 上的幺元.

最后我们还需要证明 $\text{Hom}(G, H)$ 中每个元素都有逆元. 为此, 我们先证明一下引理:

引理 7.3.4

设 H 为一个交换群. 则取逆的映射:

$$\begin{aligned}\text{Inv} : H &\rightarrow H \\ x &\mapsto x^{-1}.\end{aligned}$$

是一个群同构.

引理 7.3.4 的证明. 任取 $x, y \in H$, 我们有

$$(xy)^{-1} = y^{-1}x^{-1}.$$

由于 H 交换, 因此我们有

$$\text{Inv}(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \text{Inv}(x)\text{Inv}(y).$$

因此 Inv 是一个群同态.

由逆元的唯一性可知, Inv 是一个双射. 因此 Inv 是一个群同构. $\square$

任取 $\phi \in \text{Hom}(G, H)$, 我们考虑 $\text{Inv} \circ \phi$. 由命题 7.1.10 我们知道 $\text{Inv} \circ \phi \in \text{Hom}(G, H)$. 进一步, 对任意 $a \in G$, 我们有

$$\begin{aligned}(\phi \cdot (\text{Inv} \circ \phi))(a) &= \phi(a)(\text{Inv} \circ \phi)(a) = \phi(a)(\phi(a))^{-1} = e_H = \phi_e(a), \\ ((\text{Inv} \circ \phi) \cdot \phi)(a) &= (\text{Inv} \circ \phi)(a)\phi(a) = (\phi(a))^{-1}\phi(a) = e_H = \phi_e(a).\end{aligned}$$

因此 $\text{Inv} \circ \phi$ 是 ϕ 关于 $\cdot$ 运算的逆. 综上所述, 我们有 $\text{Hom}(G, H)$ 关于 $\cdot$ 运算构成群.

最后由 H 中群运算的交换性, 我们有 $\text{Hom}(G, H)$ 上的 $\cdot$ 的交换性. 因此 $\text{Hom}(G, H)$ 关于 $\cdot$ 是一个交换群. $\square$

例 7.3.5.

在线性代数中, 我们知道任给 $\mathbb{R}$ 上两个有限维线性空间 V 和 W , 任给两个 V 到 W 的线性变换 ϕ 和 ψ , 我们可以定义线性变换的和

$$\begin{aligned}\phi + \psi : V &\rightarrow W \\ \vec{v} &\mapsto \phi(\vec{v}) + \psi(\vec{v})\end{aligned}$$

利用定义, 我们可以验证这也是 V 到 W 的线性变换. 我们考虑所有的 V 到 W 的线性变换的集合 $L(V, W)$, 则 $L(V, W)$ 关于这个求和运算构成交换群. (实际上 $L(V, W)$ 是一个 $\dim V \times \dim W$ 维的 $\mathbb{R}$ -线性空间, 但此处我们只关心群结构.)

这里要注意的是, 线性空间作线性映射只是其作为群的同态的一部分

$$L(V, W) < \text{Hom}(V, W).$$

例如我们考虑 $\mathbb{R}$ 到 $\mathbb{R}$ 的线性映射, 只有 $f(x) = \lambda x$ 这种类型 ($\lambda \in \mathbb{R}$). 但是 $\mathbb{R}$ 也是 $\mathbb{Q}$ 线性空间, 我们也可以考虑 $\mathbb{R}$ 上的 $\mathbb{Q}$ 线性变换, 从群的角度这仍是 $\mathbb{R}$ 上的群同态, 但是不一定仍保持 $\mathbb{R}$ 的线性结构.

注 7.3.6.

虽然在命题中我们没有给 G 设任何条件, 但是群同态基本定理实际上给出了一定的限制. 对任意群同态

$$\phi : G \rightarrow H,$$

我们有

$$G/\ker(\phi) \cong \text{Im}(\phi).$$

由之前作业 05 中对换位子群的讨论(教材1.8节), 我们知道这个同态的核必须包含 $[G, G]$.

同态的复合

我们之前已经讨论过, 如果两个群同态的复合是良定义的, 那么这个复合也是一个群同态. 注意到若 $H \not\subseteq G$, 我们无法用映射复合给出 $\text{Hom}(G, H)$ 上一个运算. 因此本节我们考虑 $G = H$ 的情形, 我们将讨论一个给定群 G 上的自同态.

定义 7.3.7

任取群 G , 我们记 G 的自同态的集合为:

$$\text{End}(G) := \{\phi : G \rightarrow G \mid \phi \text{ 为 } G \text{ 的自同态}\}.$$

注意到 G 的自己的映射的复合仍是 G 到自己的映射. 之前的命题 7.1.10 告诉我们这个结论可以推广到群同态映射, 即 G 的自同态的复合仍是自同态, 因此定义了 G 上的一个二元运算.

命题 7.3.8

集合 $\text{End}(G)$ 关于群同态的复合运算构成一个幺半群.

证明. 我们首先验证这个运算满足结合律.

任取 $\phi, \psi, \eta \in \text{End}(G)$, 由映射复合的定义, 任取 $a \in G$, 我们有

$$((\phi \circ \psi) \circ \eta)(a) = (\phi \circ \psi)(\eta(a)) = \phi(\psi(\eta(a))) = \phi((\psi \circ \eta)(a)) = (\phi \circ (\psi \circ \eta))(a).$$

因此运算 $\circ$ 满足结合律, $\text{End}(G)$ 为一个半群.

下证 $\text{End}(G)$ 存在幺元. 我们考虑 G 上的恒等同态:

$$\begin{aligned} \iota : G &\rightarrow G, \\ a &\mapsto a. \end{aligned}$$

任取 $\phi \in \text{End}(G)$, 任取 $a \in G$, 我们有

$$(\phi \circ \iota)(a) = \phi(\iota(a)) = \phi(a) = \iota(\phi(a)) = (\iota \circ \phi)(a).$$

因此 ι 是 $\text{End}(G)$ 关于运算 $\circ$ 的幺元. □

思考 7.3.9

举一个 $\text{End}(G)$ 不是群的例子. 运算 $\circ$ 交换么? 为什么?

引理 7.3.10

设 G 为一个幺半群, 记 e 为其幺元. 则 G 中的可逆元素构成的集合

$$U(G) := \{a \in G \mid \exists b, ab = ba = e\},$$

关于 G 的运算构成群.

证明. 由幺元的定义知 $e \in U(G)$, 因此 $U(G)$ 非空.

我们下边证明 $U(G)$ 关于 G 的运算封闭, 即任取可逆元 $a, b \in U(G)$, 我们有 ab 也可逆. 我们记 a^{-1} 和 b^{-1} 分别为 a 和 b 的逆元, 由于 G 为半群, 因此运算满足结合律, 我们有

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} = aa^{-1} = e. \\ (b^{-1}a^{-1})(ab) &= b^{-1}(aa^{-1})b = b^{-1}b = e.\end{aligned}$$

因此 ab 也是可逆元, $U(G)$ 关于 G 的运算封闭.

最后若元素 $a \in G$ 可逆, 则 $a^{-1} \in G$ 也可逆. 因此任意元素 $a \in U(G)$ 在 $U(G)$ 中有逆元.

综上所述, $U(G)$ 为一个群. $\square$

引理 7.3.11

设 G 为一个群, 任取 $\phi \in \text{End}(G)$, 则 ϕ 关于运算 $\circ$ 可逆当且仅当 ϕ 是 G 的自同构.

证明. 由命题 7.1.10, 若 ϕ 是 G 的自同构, 则 ϕ^{-1} 也是 G 的自同构. 另一方面, 设 $\phi \in \text{End}(G)$, 且存在 $\psi \in \text{End}(G)$, 满足

$$\phi \circ \psi = \psi \circ \phi = \iota,$$

则 ϕ 为双射, 因此 ϕ 为 G 的自同构. $\square$

我们有如下定义

定义 7.3.12

我们记 G 的自同构的集合为:

$$\text{Aut}(G) := \{\phi : G \rightarrow G \mid \phi \text{ 为 } G \text{ 的自同构}\}.$$

称之为 G 的自同构群.

我们首先介绍 $\text{Aut}(G)$ 中一类特殊的元素.

命题 7.3.13 (教材命题 1.4.7)

设 G 为群. 任取 $a \in G$, 映射

$$\begin{aligned}\text{Ad}_a : G &\rightarrow G, \\ b &\mapsto aba^{-1}.\end{aligned}$$

是一个 G 的自同构.

证明. 任取 $b, c \in G$, 我们有

$$\text{Ad}_a(bc) = a(bc)a^{-1} = (aba^{-1})(aca^{-1}) = \text{Ad}_a(b)\text{Ad}_a(c).$$

因此 Ad_a 是 G 的一个自同态.

任取 $b \in G$, 满足 $\text{Ad}_a(b) = aba^{-1} = e$, 我们有

$$b = a^{-1}(aba^{-1})a = a^{-1}ea = e.$$

因此 $\ker(\text{Ad}_a) = \{e\}$, Ad_a 为单同态.

最后, 任取 $b \in G$, 我们有

$$b = a(a^{-1}ba)a^{-1} = \text{Ad}_a(a^{-1}ba).$$

因此 Ad_a 为满同态.

综上所述 Ad_a 为 G 的自同构. □

定义 7.3.14 (教材命题 1.4.7)

设 G 为群. 任取 $a \in G$, 我们称 G 的自同构 Ad_a 为由 a 给出的 G 的**内自同构**.

我们可以从两个不同的角度来看内自同构的特殊性. 一是当我们考虑的群 G 可以"作用"在某个空间上的时候, 内自同构的"作用"在"某种意义"上是平凡的. 我们从以下两个例子来说明这句话的意思.

例 7.3.15.

记 V 为 $\mathbb{R}$ 上的 n 为线性空间, 并记 $L(V)$. 当我们选取 V 上的一组基 $\mathcal{B}$ 之后, 任取 $\vec{v} \in V$, 我们记 $\vec{v}$ 在 $\mathcal{B}$ 下的坐标为 $[\vec{v}]_{\mathcal{B}} \in \mathbb{R}^n$.

任取 $T \in L(V)$, 存在唯一的一个 n -阶方阵 $[T]_{\mathcal{B}} \in \text{Mat}_n(\mathbb{R})$, 满足对任意 $\vec{v} \in V$, 有

$$[T(\vec{v})]_{\mathcal{B}} = [T]_{\mathcal{B}}[\vec{v}]_{\mathcal{B}}.$$

我们称 $[T]_{\mathcal{B}}$ 为 T 在基底 $\mathcal{B}$ 下的矩阵表示.

若 T 为线性空间 V 的一个自同构, 则 $\mathcal{C} = T(\mathcal{B})$ 也是 V 的一组基, 我们记坐标变换矩阵为 $P_{\mathcal{C}, \mathcal{B}}$, 任给 $\vec{v} \in V$, 我们有

$$[\vec{v}]_{\mathcal{C}} = P_{\mathcal{C}, \mathcal{B}}[\vec{v}]_{\mathcal{B}}.$$

我们可以验证 $P_{\mathcal{C}, \mathcal{B}} = [T]_{\mathcal{B}}^{-1}$.

任给 V 上的一个线性变换 S , 则 S 在 $\mathcal{C}$ 下的矩阵表示和在 $\mathcal{B}$ 下的矩阵表示的关系为:

$$[S]_{\mathcal{C}} = P_{\mathcal{C}, \mathcal{B}}[S]_{\mathcal{B}}P_{\mathcal{C}, \mathcal{B}}^{-1} = [T]_{\mathcal{B}}^{-1}[S]_{\mathcal{B}}[T]_{\mathcal{B}}.$$

这可以由以下交换图表示:

$$\begin{array}{ccc} (V, \mathcal{B}) & \xrightarrow{[S]_{\mathcal{B}}} & (V, \mathcal{B}) \\ \uparrow P_{\mathcal{C}, \mathcal{B}}^{-1} & & \downarrow P_{\mathcal{C}, \mathcal{B}} \\ (V, \mathcal{C}) & \xrightarrow{[S]_{\mathcal{C}}} & (V, \mathcal{C}) \end{array}$$

我们考虑 V 上的线性自同构集合 $\text{GL}(V)$. 利用类似于之前证明 G 上双射的集合 S_G 在复合运算下是一个群的方法, 我们可以证明 $\text{GL}(V)$ 在复合运算下是一个群. 任取 $T \in \text{GL}(V)$, 我们记 Ad_T 为 T 给出的 $\text{GL}(V)$ 的自同构:

$$\begin{aligned} \text{Ad}_T : \text{GL}(V) &\rightarrow \text{GL}(V) \\ S &\mapsto TST^{-1} \end{aligned}$$

任取 V 的基底 $\mathcal{B}$, 我们仍记 $\mathcal{C} = T(\mathcal{B})$.

由之前的讨论, 我们可以看出 S 在 $\mathcal{B}$ 下的矩阵表示 $[S]_{\mathcal{B}}$ 与 $\text{Ad}_T(S)$ 在 $\mathcal{C}$ 下的矩阵表示相同:

$$[\text{Ad}_T(S)]_{\mathcal{C}} = [T]_{\mathcal{B}}^{-1}[TST^{-1}]_{\mathcal{B}}[T]_{\mathcal{B}} = [S]_{\mathcal{B}}.$$

并且以上关系对任意 $S \in \text{GL}(V)$ 都成立.

例 7.3.16.

我们可以再考虑一个更几何一点的例子. 考虑 $\mathbb{R}^2$ 上关于欧式度量的保定向等距变换群. 这里边的元素是平面的平移, 旋转以及它们的复合.

为了具体描述这些变换, 我们考虑 $\mathbb{R}^2$ 上的标准正交基下的坐标. 平面的平移是可以有一个向量决定. 我们可以考虑 $\mathbb{R}^2$ 上的一个向量 $\vec{v}$, 则

$$T_{\vec{v}} : \mathbb{R}^2 \rightarrow \mathbb{R}^2 \\ (x, y) \mapsto (x, y) + \vec{v}$$

另一方面, 以原点为对称中心顺时针旋转 $\theta \in [0, 2\pi)$ 角度的旋转由以下线性变换给出:

$$R_\theta = \begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix}$$

那么我们该如何描述对称中心不在原点的旋转呢? 这里就用到了内自同构的作用.

如果我们希望将平面以 (x, y) 为对称中心顺时针旋转 $\theta \in [0, \theta)$, 我们记 $\vec{v} = (x, y)$, 则所求的旋转就是

$$R = T_{\vec{v}} \circ R_\theta \circ T_{\vec{v}}^{-1}.$$

笼统地说, 如果我们固定平面上一个参照物(直角坐标系), 从在平面上的作用来说, 以上两个旋转是不同的. 但是如果相对各自的对称中心, 两个旋转是相同的.

命题 7.3.17 (教材命题 1.4.7)

设 G 为一个群. 记 $\text{Inn}(G)$ 为 G 的所有内自同构的集合. 则 $\text{Inn}(G)$ 构成 $\text{Aut}(G)$ 的一个正规子群.

证明. 我们已经证明了内自同构的存在性. 因此 $\text{Inn}(G)$ 非空.

任取 $a, b \in G$, 我们考虑对应的内自同构 Ad_a 和 Ad_b . 任取 $c \in G$, 我们有

$$(\text{Ad}_a \circ \text{Ad}_b)(c) = \text{Ad}_a(\text{Ad}_b(c)) = \text{Ad}_a(bcb^{-1}) = a(bcb^{-1})a^{-1} = (ab)c(ab)^{-1} = \text{Ad}_{ab}(c).$$

因此 $\text{Inn}(G)$ 关于 $\text{Aut}(G)$ 上的群作用封闭.

任取 $a \in G$, 考虑内自同构 Ad_a 和 $\text{Ad}_{a^{-1}}$. 由之前的讨论, 我们有

$$\text{Ad}_{a^{-1}} \circ \text{Ad}_a = \text{Ad}_{a^{-1}a} = \text{Ad}_e = id = \text{Ad}_{aa^{-1}} = \text{Ad}_a \circ \text{Ad}_{a^{-1}}.$$

因此

$$(\text{Ad}_a)^{-1} = \text{Ad}_{a^{-1}} \in \text{Inn}(G).$$

任取 $a, b \in G$, 我们有

$$\text{Ad}_a \circ (\text{Ad}_b)^{-1} = \text{Ad}_{ab^{-1}} \in \text{Inn}(G).$$

因此 $\text{Inn}(G)$ 是 $\text{Aut}(G)$ 的一个子群.

最后我们证明这是一个正规子群. 任取 $\phi \in \text{Aut}(G)$, 任取 $a \in G$, 我们考虑 G 的自同构 $\phi \circ \text{Ad}_a \circ \phi^{-1}$. 任取 $b \in G$, 我们有

$$\begin{aligned} & (\phi \circ \text{Ad}_a \circ \phi^{-1})(b) \\ &= (\phi \circ \text{Ad}_a)(\phi^{-1}(b)) \\ &= \phi(a\phi^{-1}(b)a^{-1}) \\ &= \phi(a)b(\phi(a))^{-1} \\ &= \text{Ad}_{\phi(a)}(b) \end{aligned}$$

因此 $\phi \circ \text{Ad}_a \circ \phi^{-1} \in \text{Inn}(G)$, $\text{Inn}(G)$ 为 $\text{Aut}(G)$ 的正规子群. □

命题 7.3.18

若 G 为一个交换群, 则有

$$\text{Inn}(G) = \{id\}.$$

定义 7.3.19 (教材命题 1.4.7)

设 G 为一个群. 我们称商群

$$\text{Out}(G) := \text{Aut}(G)/\text{Inn}(G),$$

为 G 的**外自同构群**.

注 7.3.20.

这里要注意的是, 按照定义 "外自同构" 是同构的等价类. 例如, 在我们之前考虑的 $\mathbb{R}^2$ 关于欧式度量的保定向等距变换群中, 任给 $\theta \in [0, 2\pi)$, 任给一点 $(x, y) \in \mathbb{R}^2$, 让平面绕该点顺时针旋转 θ 角度的变换记为 $R(x, y)$, 则以下等距变换群的子集构成一个外自同构群的元素:

$$\{R(x, y) \mid (x, y) \in \mathbb{R}^2\}.$$

另一个可以看出内自同构群的特殊性的角度更多来自对有限生成群的研究中. 详细内容可以参考附录 ?? 中关于群的表达以及群的 Cayley 图的介绍.

第八章 一些特殊的群

在本章中, 我们将介绍一些比较基本的, 常见的群.

8.1 循环群

我们之前已经介绍过这个概念. 除了平凡群 $\{e\}$ 外, 循环群是最基本的群. 我们在任何群中都可以看到它的身影.

考虑一个群 G . 任取 $a \in G$, 我们记

$$a^n = \begin{cases} \underbrace{a \cdots a}_{n \uparrow} & n \in \mathbb{Z}_{>0} \\ e & n = 0 \\ \underbrace{a^{-1} \cdots a^{-1}}_{n \uparrow} & n \in \mathbb{Z}_{<0} \end{cases}$$

8.1.1 循环群的分类

我们可以利用定义直接验证一下结论.

命题 8.1.1

任取群 G 和其中的元素 a , 以上定义的映射

$$\begin{aligned} \phi_a : \mathbb{Z} &\rightarrow G \\ n &\mapsto a^n \end{aligned}$$

是一个群同态.

由我们之前对 $\mathbb{Z}$ 的子群的讨论知, 存在 $k \in \mathbb{N}$, 满足

$$\ker \phi_a = k\mathbb{Z}.$$

注 8.1.2.

我们抽代二讲模的时候也会将 $\ker \phi_a$ 记为 $\text{ann}(a)$.

我们进一步有以下观察

命题 8.1.3

沿用以上记号, 设 $k \in \mathbb{N}$, 满足

$$\ker \phi_a = k\mathbb{Z}.$$

任取 $i, j \in \mathbb{Z}$, 则有 $i - j \in k\mathbb{Z}$, 当且仅当

$$a^i = a^j.$$

证明. 若 $i - j \in k\mathbb{Z} = \ker \phi_a$, 我们有

$$\phi_a(i - j) = a^{i-j} = e.$$

两边同时右乘 a^j 可得,

$$a^i = a^j.$$

反过来, 如果 $a^i = a^j$, 则有

$$a^{i-j} = e,$$

因此 $i - j \in \ker \phi_a = k\mathbb{Z}$. □

沿用以上记号, 我们有以下推论

推论 8.1.4

- (i) 元素 a 为有限阶元素当且仅当 $k > 0$.
- (ii) 若 $k > 0$, 则元素 a 的阶为 k .

利用群同态基本定理, 沿用以上记号, 我们有

推论 8.1.5 (教材定理 1.5.5)

- (i) 若 $k > 0$, 我们有 $\langle a \rangle \cong \mathbb{Z}_k$.
- (ii) 若 $k = 0$, 我们有 $\langle a \rangle \cong \mathbb{Z}$.

由此我们看出一个元素生成的循环群总是与 $\mathbb{Z}$ 或者 $\mathbb{Z}$ 的某个非平凡商群同构.

引理 8.1.6

任取 G, H 和 K 为群, 若有

$$G \cong H, \quad H \cong K,$$

则有

$$G \cong K.$$

证明. 由条件存在群同构

$$\phi: G \rightarrow H, \quad \psi: H \rightarrow K.$$

注意到双射的复合仍是双射, 群同态的复合仍是群同态, 因此

$$\psi \circ \phi : G \rightarrow K,$$

是一个群同构. 因此 $G \cong K$. □

注 8.1.7.

群之间的同构似乎给出了群之间的一个等价关系. 但这里有一个与罗素悖论相关的问题就是, 所有群放在一个不构成一个集合. 因此不满足我们关于几何上等价关系的定义. 但是我们确实有以下结论:

- (i) 任取群 G , 有 $G \cong G$,
- (ii) 任取群 G 和 H , 若 $G \cong H$, 则 $H \cong G$,
- (iii) 任取群 G, H 和 K , 若 $G \cong H$ 且 $H \cong K$, 则 $G \cong K$.

命题 8.1.8 (教材定理 1.5.5)

两个循环群同构当且仅当它们生成元有相同的阶.

8.1.2 循环群的子群

我们首先证明以下引理.

引理 8.1.9

任取群 G 及其循环子群 H , 设 N 为 G 的一个正规子群, 则 HN/N 为 G/N 中的循环子群.

证明. 由于 H 为 G 的循环子群, 因此存在 $a \in G$, 满足

$$H = \langle a \rangle = \{a^j \mid j \in \mathbb{Z}\}.$$

另一方面, 我们有

$$HN/N = \{aN \mid a \in H\} = \{a^j N \mid j \in \mathbb{Z}\}.$$

任取 $i, j \in \mathbb{Z}$, 由于 $N \triangleleft G$, 我们有

$$(a^i N)(a^j N) = a^{i+j} N.$$

因此 HN/N 由 aN 生成, 即

$$HN/N = \langle aN \rangle.$$

□

引理 8.1.10

设 G 为一个循环群, H 为一个群, 设 $\phi : G \rightarrow H$ 为一个群同态, 则 $\phi(G)$ 是一个循环群.

证明. 设 a 为 G 的生成元, 则 $\phi(a)$ 为 $\phi(G)$ 的生成元. □

命题 8.1.11 (教材引理 1.5.7)

循环群 $\langle a \rangle$ 的任意子群都是循环群.

证明. 如果 a 为无限阶元素, 则

$$\langle a \rangle \cong \mathbb{Z}.$$

因此 $\langle a \rangle$ 的子群与 $\mathbb{Z}$ 的子群存在一一对应. 由于 $\mathbb{Z}$ 的子群都是 $k\mathbb{Z}$ 的形式(满足 $k \in \mathbb{N}$), 为循环群(由 k 生成), 因此 $\langle a \rangle$ 的子群都是由某个 a^k 生成的循环群.

如果 a 为有限阶元素, 则存在 $k \in \mathbb{N}^*$, 满足

$$\langle a \rangle \cong \mathbb{Z}_k = \mathbb{Z}/k\mathbb{Z}.$$

因此 $\langle a \rangle$ 的子群与 $\mathbb{Z}_k$ 的子群存在一一对应. 另一方面, 由同态基本定理, 商群 $\mathbb{Z}_k$ 的子群与 $\mathbb{Z}$ 中包含 $k\mathbb{Z}$ 的子群有一一对应, 作为 $\mathbb{Z}$ 的子群仍是循环群. 由以上引理, 我们知道 $\mathbb{Z}_k$ 的子群都是循环群. 因此 $\langle a \rangle$ 所有的子群都是循环群. $\square$

8.1.3 有限群中的循环群

这里我们主要关注有限群 G 中的循环群 $\langle a \rangle$ ($a \in G$). 因此 $\langle a \rangle$ 也是有限群, 其生成元 a 为有限阶. 我们将主要研究 G 的阶, a 的阶, 以及 $\langle a \rangle$ 的子群的阶之间的关系. 这里我们将使用的主要工具有两个: Lagrange 定理以及整数的素数分解.

我们首先给出 Lagrange 定理的关于有限群中的循环子群情形下的叙述.

命题 8.1.12

设 G 为一个有限群. 任取 $a \in G$, 我们有

$$o(a) = |\langle a \rangle| \mid |G|.$$

注 8.1.13.

以上命题说明, G 中元素的阶整除 G 的阶, 即任取 $m \in \mathbb{N}^*$, 若存在 $a \in G$, 满足 $m = o(a)$, 则

$$m \mid |G|.$$

但是反过来并不正确, 即任取 $m \in \mathbb{N}^*$, 若 $m \mid |G|$, 我们**并不能**说一定存在 $a \in G$, 满足

$$o(a) = m.$$

思考 8.1.14 (教材思考题 1.5.6)

考虑二面体群 D_4 . 给出 D_4 中所有元素的阶. D_4 中是否存在 8-阶元素?

我们下边考虑一个特殊情况: G 本身是一个有限循环群, 即存在 $a \in G$, 满足

$$G = \langle a \rangle.$$

定理 8.1.15 (教材定理 1.5.8, 1.5.9)

- (i) 任取 $b \in G$, 我们有

$$o(b) \mid o(a).$$
- (ii) 任取 $m \in \mathbb{N}^*$, 若 $m \mid |G|$, 则存在 $b \in G$, 满足 $o(b) = m$.
- (iii) 任取群 H , 满足 $|H|$ 为一个素数, 则 H 是一个循环单群.
- (iv) 任取群 H , 若 H 是交换单群, 则 H 是一个素数阶循环单群.

证明. (i) 由 Lagrange 定理, 我们有

$$o(b) = |\langle b \rangle| \mid |\langle a \rangle| = o(a).$$

(ii) 设 $n = |G| = o(a)$, 因此我们有

$$G = \{e, a, \dots, a^{n-1}\}.$$

设 $m \in \mathbb{N}^*$, 我们记 $j = n/m$. 令 $b = a^j$. 下证

$$o(b) = m.$$

我们使用反证法. 若 $o(b) < m$, 我们有

$$e = b^{o(b)} = a^{j \cdot o(b)}.$$

因此 $o(a) \mid j \cdot o(b) < jm = n$. 矛盾.

(iii) 任取 H 中的非单位元 b , 我们有

$$1 < |\langle b \rangle| \mid |H|,$$

因为 $|H|$ 是一个素数, 因此

$$|\langle b \rangle| = |H|.$$

因此 $\langle b \rangle = H$. 因此 H 的子群只有 $\{e\}$ 和 H , H 为单群.

(iv) 任取 H 中的非单位元 b , 我们有

$$1 < |\langle b \rangle| \mid |H|,$$

由于 H 为交换群, 因此任意子群都是 H 的正规子群. 由于 H 为单群, H 中没有不同于 $\{e\}$ 和 H 的子群. 由于 b 非幺元, 因此我们有

$$\langle b \rangle = H,$$

即 H 为循环群. 若 $o(b) > 1$ 不是素数, 则存在 $1 < j < o(b)$, 且 $j \mid o(b)$. 我们考虑 b^j 生成的子群为 H 的子群, 则有

$$1 < o(b^j) = \frac{o(b)}{j} < o(b).$$

因此

$$\{e\} \subsetneq \langle b^j \rangle \subsetneq H.$$

这与 H 没有非平凡子群矛盾. 因此 $o(b)$ 为素数.

□

8.2 对称群

对称群中的元素通常被称作置换. 这是一个我们将常会遇到的与某些物体的对称性相关的概念. 我们考虑下边几个例子.

例 8.2.1.

第一个例子是正三角形的对称性. 为了方便叙述, 我们将借助平面上的复坐标.

我们考虑顶点在单位圆上的正三角形. 设其中一个顶点为 $z_0 = 1 \in \mathbb{C}$, 则另外两个顶点为 $z_1 \exp 2\pi/3$ 和 $z_2 \exp(4\pi/3)$. 我们可以将这个三角形绕原点顺时针旋转 120° . 所得的三角形与原三角形重合. 在此过程中, 我们将顶点 (z_0, z_1, z_2) 分别送到 (z_1, z_2, z_0) . 类似地如果逆时针旋转 120° , 我们将顶点 (z_0, z_1, z_2) 分别送到 (z_2, z_0, z_1) . 我们也可以考虑将平面沿着实轴做一个反射. 此时, 我们将顶点 (z_0, z_1, z_2) 送到了 (z_0, z_2, z_1) .

如果我们称将 (z_0, z_1, z_2) 送到 $(z_{j_0}, z_{j_1}, z_{j_2})$, 满足

$$\{j_0, j_1, j_2\} = \{0, 1, 2\},$$

为这三个顶点的一个置换的话(注意到我们所得的三角形总是和原三角形重合), 我们之前每个操作都给出了顶点集合的一个置换. 并且如果我们连续进行两个操作, 所得的仍是顶点集合的一个置换. 另外, 我们注意到每一个置换都是可逆的. 如果我们顺时针旋转 120° , 在逆时针旋转 120° , 我们就回到了初始位置. 当然根据置换的定义, 如果我们什么也不做, 每个顶点都对应到自己, 这也是一个置换.

联系到之前群的定义, 我们看出, 上边的讨论实际上告诉我们, 正三角形的顶点的置换构成一个群.

例 8.2.2.

第二个例子, 我们考虑三维空间中的一个正四面体. 我们记四个顶点分别为 a, b, c 和 d . 我们考虑其中一个面, 例如由顶点 a, b 和 c 决定的面, 则这是一个正三角形. 由之前的讨论, 我们知道正三角形有一个关于其中心的三阶的旋转对称. 我们记正三角形的中心为 O , 然后考虑三维空间中过 O 和顶点 d 的直线, 如果我们将正四面体绕着这个直线旋转 120° , 那么所得的正四面体和原正四面体重合, 我们将正四面体的四个顶点 (a, b, c, d) 送到了 (b, c, a, d) 或者 (c, a, b, d) (取决于我们绕直线 Od 旋转的时候的方向的选择).

另一方面, 我们可以考虑正四面体的一组对边 ab 和 cd , 我们记 p 和 q 分别为 ab 和 cd 的中点. 考虑三维空间中的直线 pq . 我们可以考虑将正四面体绕着直线 pq 旋转 180° . 类似于前一种情况, 所得的正四面体和原正四面体重合, 我们将正四面体的四个顶点 (a, b, c, d) 送到了 (b, a, d, c) .

类似于之前的例子, 我们可以验证由以上所有几何对称性给出的顶点的置换构成一个群.

例 8.2.3.

我们考虑整数 $\mathbb{Z}$ 集合, 这个集合也有对称性. 我们考虑 $\mathbb{Z}$ 大于 0 的部分和小于 0 的部分, 并分别记作 $\mathbb{Z}_{>0}$ 和 $\mathbb{Z}_{<0}$. 如果我们考虑 $\mathbb{Z}$ 到自身的映射: $n \mapsto -n$, 我们将 $\mathbb{Z}_{>0}$ 和 $\mathbb{Z}_{<0}$ 做了一个对换. 如果我们再进行一次这个过程, $\mathbb{Z}_{>0}$ 和 $\mathbb{Z}_{<0}$ 就回到了初始的位置.

例 8.2.4.

在这个例子中, 我们考虑实系数多项式. 我们假设 $f(x)$ 是一个次数为 5 的首项系数为 1 的实系数, 并在实数中有 5 个根 $\{x_1, x_2, x_3, x_4, x_5\}$, 我们知道 $f(x)$ 有如下分解:

$$f(x) = x^5 + ax^4 + bx^3 + cx^2 + dx + e = (x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5).$$

由韦达定理, 我们知道

$$\begin{cases} -a = \sum_{j=1}^5 x_j \\ b = \sum_{1 \leq j_1 < j_2 \leq 5} x_{j_1} x_{j_2} \\ -c = \sum_{1 \leq j_1 < j_2 < j_3 \leq 5} x_{j_1} x_{j_2} x_{j_3} \\ d = \sum_{1 \leq j_1 < j_2 < j_3 < j_4 \leq 5} x_{j_1} x_{j_2} x_{j_3} x_{j_4} \\ -e = x_1 x_2 x_3 x_4 x_5 \end{cases}$$

如果我们考虑 $(y_1, y_2, y_3, y_4, y_5) = (x_2, x_1, x_3, x_4, x_5)$, 我们有

$$(x - y_1)(x - y_2)(x - y_3)(x - y_4)(x - y_5) = (x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5) = f(x).$$

更一般地, 我们可以将五个根按照任意顺序排列, 所得多项式仍是 $f(x)$. 这是 Lagrange, Abel, Galois 等人在研究五次方程是否有根式解时用到的根的对称性.

我们之前学习的内容中也有以下抽象的例子.

例 8.2.5.

设 G 为一个有限群, ϕ 为 G 的一个自同构, 那么 ϕ 是对 G 中元素做了一个置换 (重新排列将 $a \in G$ 送到 $\phi(a)$). 因此一个群的自同构群在这个意义上反映出了该群的对称性.

例 8.2.6.

设 G 为一个有限群, 任取 $a \in G$, 我们考虑 a 的左平移映射 L_a . 则 L_a 也是群 G 中元素的置换. 关于这个映射, 我们将在后续关于群作用的章节中做进一步讨论.

实际上, 当我们排除掉以上例子中的几何背景或者代数背景等之后, 我们所做的就是将按照一定顺序排列的元素做了一个重新排列, 这样的重新排列就是我们所谓的置换. 更严格的定义如下:

定义 8.2.7

设 $n \in \mathbb{N}^*$. 我们考虑集合 $\{1, 2, \dots, n\}$. 一个 n -元置换是一个双射

$$\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}.$$

我们记所有 n -元置换的集合为

$$S_n := \{\sigma \mid \sigma \text{ 为一个 } n\text{-元置换}\},$$

称之为 n -元对称群.

命题 8.2.8

任取非零自然数 n , n -元对称群 S_n 是一个阶为 $n!$ 的有限群.

证明. 确定一个映射, 我们只需要确定每一个自然数 $k \in \{1, \dots, n\}$ 的像即可.

记 $\sigma \in S_n$, 我们考虑 1 的像. 注意到 $\sigma(1)$ 有 n 中选择. 我们确定

$$\sigma(1) = i_1 \in \{1, \dots, n\}.$$

然后考虑 $\sigma(2)$. 注意到 σ 是双射, 因此

$$\sigma(2) \in \{1, \dots, n\} \setminus \{i_1\},$$

有 $n-1$ 种可能. 我们对 $\sigma(3), \dots, \sigma(n)$ 的像重复以上讨论, 可得 σ 有 $n!$ 种不同选择. 因此 $|S_n| = n!$. $\square$

推论 8.2.9

任取非零自然数 n , 考虑 n -元对称群 S_n . 任意 $\sigma \in S_n$ 都是有限阶元素.

注 8.2.10.

群 S_n 包含了 n 个元素集合所有可能的对称性. 我们之前举得例子中, 由于在置换的过程中我们需要保持一些其他的结构, 我们得到的通常是 S_n 的子群. 例如在本节第二个例子中, 当我们考虑正四面体的对称性的时候, 我们无法将 (a, b, c, d) 送到 (b, a, c, d) . 因此这个置换就不在正四面体的对称群中. 倒数第二个例子中, 一个群由自同构给出的对称性需要保持群的代数结构. 例如, G 中互逆的两个元素 a 和 b 在 G 同构下的像仍需要是互逆的. 因此一般情况下, $\text{Aut}(G)$ 是 S_n (设 $|G| = n$) 的一个真子群.

思考 8.2.11

设 G 为一个 n 阶有限群. 什么样的群 G , 满足 $\text{Aut}(G) = \{id\}$? 什么样的群 G , 满足 $\text{Out}(G) = \{id\}$?

以上例子告诉我们对称群是一类非常基本同时也是非常重要的群. 下边我们希望进一步对对称群的结构进行更深入的了解. 为了方便讨论, 我们首先给出一些记号和定义.

设 n 为一个非零自然数. 任取 $\sigma \in S_n$, 由定义我们知道 σ 是一个 $\{1, \dots, n\}$ 到自己的双射. 我们通常使用 $2 \times n$ 矩阵的方法, 将 1 到 n 每个自然数与其在 σ 下的相对应起来:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix},$$

或者我们设 $i_k = \sigma(k)$, 并将该矩阵记为

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}.$$

我们下边考虑 σ 及其生成的 S_n 中的循环子群. 由之前的讨论我们知道这是一个有限子群.

定义 8.2.12

记 $\sigma \in S_n$. 任取 $i \in \{1, \dots, n\}$, 存在 $k \in \mathbb{N}^*$, 满足

$$\sigma^k(i) = i.$$

我们称集合

$$O_\sigma(i) = \{i, \sigma(i), \dots, \sigma^{k-1}(i)\},$$

为 i 在 σ 下的**轨道**.

引理 8.2.13

任取 $i, j \in \{1, \dots, n\}$, 若 $j \in O_\sigma(i)$, 则

$$O_\sigma(j) = O_\sigma(i).$$

命题 8.2.14

任取非零自然数 n , 考虑 n -元对称群 S_n . 任取 $\sigma \in S_n$, 则以下给出 $\{1, \dots, n\}$ 上的一个等价关系:

- 任取 $i, j \in \{1, \dots, n\}$, 定义 $i \sim j$ 当且仅当 $O_\sigma(i) = O_\sigma(j)$.

因此通过考虑 σ 的轨道, 我们得到 $\{1, \dots, n\}$ 的一个划分.

任取 $\sigma \in S_n, i \in \{1, \dots, n\}$, 我们考虑轨道 $O_\sigma(i)$. 为方便讨论, 我们记

$$j_1 = \sigma(i), \dots, j_{k-1} = \sigma^{k-1}(i), j_k = i.$$

这些元素之间满足以下关系:

$$j_1 \xrightarrow{\sigma} j_2 \xrightarrow{\sigma} \cdots \xrightarrow{\sigma} j_{k-1} \xrightarrow{\sigma} j_k$$

σ

定义 8.2.15 (教材定义 1.6.1, 1.6.2)

任取 $1 \leq k \leq n$, 设 $\tau \in S_n$, 我们称 τ 为一个**长度为 k 的轮换**, 若存在 $\{1, \dots, n\}$ 中两两不同的 k 个元素 $j_1, \dots, j_k$, 满足

$$\tau(j_1) = j_2, \tau(j_2) = j_3, \dots, \tau(j_k) = j_1.$$

我们通常将记作 $(j_1 j_2 \cdots j_k)$.

如果 $(j_1 j_2 \cdots j_k)$ 和 $(l_1 l_2 \cdots l_m)$ 为两个轮换, 且满足

$$\{j_1, \dots, j_k\} \cap \{l_1, \dots, l_m\} = \emptyset,$$

我们称轮换 $(j_1 j_2 \cdots j_k)$ 和 $(l_1 l_2 \cdots l_m)$ **不相交**.

我们称一个长度为 2 的轮换为**对换**(transposition).

注 8.2.16.

这里需要说明的是一个轮换的记号并不是唯一的. 我们通常考虑

$$(j_1 j_2 \cdots j_{k-1} j_k) = (j_2 j_3 \cdots j_k j_1) = \cdots = (j_k j_1 \cdots j_{k-2} j_{k-1})$$

例如:

$$(1524) = (5241) = (2415) = (4152).$$

注 8.2.17.

注意区别轮换的符号和有限数列的符号. 例如

$$(i_1 i_2 \cdots i_k)$$

是一个 k 轮换, 而

$$(i_1, i_2, \dots, i_k)$$

是一个 k 个元素的序列.

引理 8.2.18

任取非零自然数 n , 考虑 n -元对称群 S_n . 任取 $\sigma \in S_n$, 并任取 $i \in \{1, \dots, n\}$, 则 $\sigma|_{O_\sigma(i)}$ 是一个长度为 $|O_\sigma(i)|$ 的轮换.

引理 8.2.19 (教材命题 1.6.3)

记 n 为一个非零自然数, 考虑 n -元对称群 S_n . 设 $\tau, \eta \in S_n$ 为两个不相交的轮换, 则两个元素交换:

$$\tau\eta = \eta\tau.$$

定理 8.2.20 (教材定理 1.6.4)

任取非零自然数 n , 考虑 n -元对称群 S_n . 任意 $\sigma \in S_n$, 都可以表示为 s 个不相交的轮换的乘积

$$\sigma = (j_{11} \cdots j_{1k_1}) \cdots (j_{s1} \cdots j_{sk_s}),$$

满足 $k_1 + \cdots + k_s = n$, 或等价地

$$\{j_{11}, \dots, j_{sk_s}\} = \{1, \dots, n\}.$$

证明. 我们考虑将 σ 诱导的 $\{1, \dots, n\}$ 上的划分. 由之前的引理, σ 在每个轨道上的作用是一个轮换, 另外任意两个不同的轨道的交际为空. 因此由划分的性质我们得到命题中的结论. $\square$

例 8.2.21.

我们考虑 S_6 . 记 σ 为以下元素:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 2 & 1 & 3 \end{pmatrix}$$

σ 有两个轨道

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 2 & 1 & 3 \end{pmatrix}.$$

我们可以将 σ 写为

$$\sigma = (1425)(36).$$

注 8.2.22.

当我们将 $\sigma \in S_n$ 写为不相交轮换的乘积时, 如果一个轮换的长度为 1, 那么所对应的元素被 σ 固定. 我们通常会省略长度为 1 的轮换.

例如: 在 S_6 中, 如果有

$$\sigma = (154)(26)(3),$$

我们通常会记作

$$\sigma = (154)(26).$$

引理 8.2.23

记 n 为一个非零自然数, 考虑 n -元对称群 S_n . 设 $k \in \{1, \dots, n\}$, $\tau \in S_n$ 为一个 k -轮换, 则 τ 的阶为 k :

$$o(\tau) = k.$$

命题 8.2.24

记 n 为一个非零自然数, 考虑 n -元对称群 S_n . 任取 $\sigma \in S_n$, 若其可以写为如下轮换的乘积

$$\sigma = (j_{11} \cdots j_{1k_1}) \cdots (j_{s1} \cdots j_{sk_s}),$$

其中, $s \in \mathbb{N}^*$ 且 $k_1, \dots, k_s \in \mathbb{N}^*$, 则

$$o(\sigma) = \text{lcm}(k_1, \dots, k_s).$$

思考 8.2.25 (教材思考题 1.6.6)

设 p 为一个素数. 在群 S_p 中有多少个 p -阶元素? 分别是什么?

我们还可以将轮换作进一步的分解成为对换的乘积. 通过直接计算, 我们可以证明以下引理:

引理 8.2.26 (教材引理 1.6.7)

设 n 为一个非零自然数. 任取

$$\{i_1, \dots, i_k\} \subset \{1, \dots, n\},$$

为一个 k 个元素的子集. 我们有

$$(i_1 \cdots i_k) = (i_1 i_k) \cdots (i_1 i_3)(i_1 i_2).$$

命题 8.2.27 (教材命题 1.6.8)

记 n 为一个非零自然数, 考虑 n -元对称群 S_n . 任取 $\sigma \in S_n$, 我们可以将其写为对换的乘积.

注 8.2.28.

我们约定 id 为 0 个对换的乘积.

由这个命题出发, 我们自然会有一个疑问就是, 任给一个置换 σ , 其被分解为对换的方式是否唯一? 当然我们首先要说明唯一是什么意思. 我们所谓的唯一是指两种分解方式相差的仅仅是可交换元素的不同排序. 我们考虑下边的例子.

例 8.2.29.

我们首先考虑 S_3 中的元素. 比较 (12) 和 (23) , 考虑之前我们对群共轭作用的讨论, 我们有以下关系

$$(12) = (13)(23)(13).$$

另一方面, 我们考虑 5-轮换 (12345) . 该轮换有以下分解方法:

$$(12345) = (15)(14)(13)(12) = (21)(32)(43)(54).$$

利用以上的例子, 我们可以将同一个置换按照不同方法分解为对换的乘积. 虽然写法不唯一, 但是我们观察到不同方法用到的对换的个数的奇偶性相同. 实际上我们可以证明以下结论:

命题 8.2.30

记 n 为一个非零自然数, 考虑 n -元对称群 S_n . 任取 $\sigma \in S_n$, 若其既可以写为 k 个对换的乘积, 又可以写为 l 个对换的乘积, 那么 k 和 l 的奇偶性相同.

我们将给出两个证明. 一个是使用的是对换的性质不断的调整对换的位置来证明, 另一个使用的是线性代数方法将置换对应到矩阵, 利用行列式的性质来证明.

证明一. 我们首先证明对换的一些性质.

引理 8.2.31

任取 a, b, c, d 表示 4 个不同的数字, 我们有

- (i) $(ab)(cd) = (cd)(ab);$
- (ii) $(ac) = (ab)(bc)(ab);$
- (iii) $(ab)(ac) = (ab)(ab)(bc)(ab) = (bc)(ab);$
- (iv) $(ab)(ac) = (ac)(bc)(ac)(ac) = (ac)(bc);$
- (v) $(ab)(ab) = 1.$

引理 8.2.32

设 n 为非零自然数, 考虑 S_n . 么元 id 任意的分解为对换的写法中, 对换的个数都是偶数.

引理 8.2.32 的证明. 我们假设 id 有如下分解:

$$id = (i_1 i_2)(i_3 i_4) \cdots (i_{2k-1} i_{2k}).$$

这里不在一个对换中的两个数字可能相同. 我们记

$$\tilde{i}_1 := \max\{i_1, \dots, i_{2k}\}.$$

利用之前对换的性质, 我们可以将所有包含 $\tilde{i}$ 的对换放在最开始的位置:

$$(\tilde{i}_1 \tilde{i}_2)(\tilde{i}_1 \tilde{i}_3) \cdots (\tilde{i}_1 \tilde{i}_l) \cdots.$$

这是我们有以下两种情况

- (i) 如果存在两个 $(\tilde{i}_1 \tilde{i}_2)$ 并且 $\tilde{i}_3 = \tilde{i}_2$, 利用对换的性质, 我们可以将前两项消掉. 由于去掉两项, 因此剩下的对换个数与之前对换个数的奇偶性相同. 我们继续对剩下的对换个数的奇偶性进行讨论.
- (ii) 如果存在两个 $(\tilde{i}_1 \tilde{i}_2)$ 并且 $\tilde{i}_3 \neq \tilde{i}_2$, 我们假设 $\tilde{i}_s$ 是从 $\tilde{i}_3$ 到 $\tilde{i}_l$ 中第一个等于 $\tilde{i}_2$ 元素, 那么我们有

$$(\tilde{i}_1 \tilde{i}_2)(\tilde{i}_1 \tilde{i}_3) \cdots (\tilde{i}_1 \tilde{i}_{s-1})(\tilde{i}_1 \tilde{i}_s) = (\tilde{i}_2 \tilde{i}_3) \cdots (\tilde{i}_2 \tilde{i}_{s-1}).$$

同样的, 对换个数减少 2, 因此奇偶性不变, 我们对剩下的对换个数的奇偶性进行讨论. 注意到此时排在最左边的对换已经不包含 $\tilde{i}_1$, 因此, 我们重复第一步, 利用对换的性质将包含 $\tilde{i}_1$ 的对换换至最左边.

我们重复以上讨论, 注意到每经过一次这样的讨论, 如果从第二个对换开始, 存在与第一个对换相同的对换, 我们都可以将对换的个数减少 2 个. 由于对换的总数有限, 因此经过有限次之后, 有两种可能:

- (i) 剩下的所有对换都不包含 $\tilde{i}_1$;
- (ii) 仍有包含 $\tilde{i}_1$ 的对换在最左边, 并且从第二个对换开始, 不存在与第一个对换相同的对换.

如果第一种情况发生, 我们就考虑剩下的数字中最大的, 重复以上讨论. 如果是第二种情况, 如果第二个对换仍包含 $\tilde{i}_1$, 我们就对除第一项之外所有包含 $\tilde{i}_1$ 的对换重复以上讨论. 经过有限次后, 我们有两种可能情况

- (i) 剩下的所有对换都不包含 $\tilde{i}_1$;
- (ii) 所有包含 $\tilde{i}_1$ 的对换

$$(\tilde{i}_1 \tilde{j}_1) \cdots (\tilde{i}_1 \tilde{j}_t),$$

中 $\tilde{j}_1, \dots, \tilde{j}_t$ 两两不同.

因此我们有

$$id = (\tilde{j}_t \tilde{j}_{t-1} \cdots \tilde{j}_1 \tilde{i}_1) \sigma'.$$

其中 σ' 为一些不包含 $\tilde{i}_1$ 的对换的乘积. 注意到左边满足 $id(\tilde{i}_1) = \tilde{i}_1$, 而右边则是 $\tilde{j}_t \neq \tilde{i}_1$. 因此不可能发生.

综上所述, 通过以上过程, 我们剩下的对换中将不包含 $\tilde{i}_1$, 且与最初的对换个数有相同的奇偶性. 我们对剩下的对换中涉及的最大的数进行相同的讨论, 由于所有对换涉及的数字在 $\{1, \dots, n\}$ 中是有限个, 因此经过有限步后, 所得对换个数是 0. 因此用任何方法将 id 写为对换的乘积后, 所得对换的个数为偶数. $\square$

现在任取一个元素 $\sigma \in S_n$, 我们设 σ 有以下两种分解为对换的方式:

$$\sigma = (i_1 i_2) \cdots (i_{2k-1} i_{2k}) = (j_1 j_2) \cdots (j_{2l-1} j_{2l}).$$

那么我们有

$$id = \sigma \sigma^{-1} = (i_1 i_2) \cdots (i_{2k-1} i_{2k}) (j_{2l-1} j_{2l}) \cdots (j_1 j_2).$$

因此 id 的分解有 $k+l$ 个对换. 由于 id 的分解总是偶数个对换, 因此 $k+l$ 为偶数, 也即 k 和 l 的奇偶性相同. $\square$

证明二. 我们将借助矩阵行列式来证明.

我们考虑 n -维实线性空间 $\mathbb{R}^n$, 考虑标准正交基 $\mathcal{B}$

$$\vec{e}_1 = (1, 0, 0, \dots, 0)$$

$$\vec{e}_2 = (0, 1, 0, \dots, 0)$$

$$\dots$$

$$\vec{e}_n = (0, 0, 0, \dots, 1)$$

任给 $\sigma \in S_n$, 任取 $i \in \{1, \dots, n\}$, 我们考虑 σ 在基底 $\mathcal{B}$ 上的作用

$$\sigma(\vec{e}_i) = \vec{e}_{\sigma(i)}.$$

这个作用可以扩展为 $\mathbb{R}^n$ 上的一个线性映射. 我们记该线性映射在标准正交基下的矩阵为

$$A_\sigma = (a_{ij})_{n \times n},$$

满足

$$a_{ji} = \begin{cases} 1 & \text{若 } j = \sigma(i) \\ 0 & \text{若 } j \neq \sigma(i) \end{cases}$$

(我们考虑 $\mathbb{R}^n$ 中元素为列向量). 由行列式的计算公式, 我们由 $\det A_\sigma = 1$ 或者 -1 .

我们考虑映射

$$\Phi: S_n \rightarrow \text{GL}(n, \mathbb{R})$$

$$\sigma \mapsto A_\sigma$$

通过直接计算, 我们可以证明这是一个群同态. 特别地, 我们有任取 $\sigma, \tau \in S_n$,

$$A_{\sigma\tau} = A_\sigma A_\tau.$$

我们记 E_{ij} 只有 (i, j) 位置为 1, 其他位置为 0 的 n -阶方阵. 则对换 (ij) 可以表达为矩阵

$$A_{(ij)} = I_n - E_{ii} - E_{jj} + E_{ij} + E_{ji}.$$

注意到 $\det A_{(ij)} = -1$.

任取 $\sigma \in S_n$, 若我们可以将其分解为对换的乘积

$$A_\sigma = A_{(i_1 i_2)} \cdots A_{(i_{2k-1} i_{2k})},$$

考虑行列式, 我们有

$$\det A_\sigma = \det(A_{(i_1 i_2)} \cdots A_{(i_{2k-1} i_{2k})}) = \det A_{(i_1 i_2)} \cdots \det A_{(i_{2k-1} i_{2k})} = (-1)^k.$$

由于 A_σ 的行列式值唯一, 当我们将 σ 的分解为对换时, 不同分解方法的对换个数必须有相同的奇偶性. $\square$

定义 8.2.33

设 n 为一个非零自然数. 任取 $\sigma \in S_n$, 我们称 σ 为一个**奇置换**, 若当我们将其分解为对换的乘积时, 对换的个数为奇数; 我们称 σ 为一个**偶置换**, 若当我们将其分解为对换的乘积时, 对换的个数为偶数.

考虑 S_n 上的群结构, 我们有以下命题:

引理 8.2.34

设 n 为一个非零自然数. 群 S_n 中的奇置换与奇置换的乘积为偶置换, 奇置换与偶置换的乘积为奇置换, 偶置换与偶置换的乘积为偶置换.

集合 $\{1, -1\}$ 对乘法运算构成群. 考虑奇置换和偶置换, 我们可以定义以下映射

$$\text{sgn} : S_n \rightarrow \{1, -1\},$$

满足

$$\text{sgn}(\sigma) := \begin{cases} 1 & \text{若 } \sigma \text{ 为偶置换} \\ -1 & \text{若 } \sigma \text{ 为奇置换} \end{cases}$$

以上引理告诉我们

命题 8.2.35

映射 sgn 为一个群同态.

定义 8.2.36

设 n 为非零自然数. 任取 $\sigma \in S_n$, 我们称 $\text{sgn}(\sigma)$ 为置换 σ 的**符号**.

我们要介绍的关于置换的最后一个概念是逆序数.

定义 8.2.37

设 n 为非零自然数, 任取

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \in S_n,$$

我们定义 σ 的逆序数为以下值

$$\rho(\sigma) := \#\{(i, j) \in \mathbb{N}^2 \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\}.$$

命题 8.2.38

设 n 为非零自然数. 任取 $\sigma \in S_n$, 则

- (i) $\rho(\sigma) \geq 0$;
- (ii) σ 为幺元当且仅当 $\rho(\sigma) = 0$.

证明. 根据定义 $\rho(\sigma)$ 是一个有限集的子集的势, 因此总是大于等于 0 的. 我们将主要证明第二点.

如果 $\sigma = id$, 则定义中的集合

$$\{(i, j) \in \mathbb{N}^2 \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\} = \emptyset,$$

因此 $\rho(id) = 0$.

我们下证若 $\sigma \neq id$, 则以上集合非空. 设 $\sigma \neq id$. 我们考虑

$$i_0 := \min\{i \mid \sigma(i) \neq i\}.$$

注意到因为 $\sigma \neq id$, 集合

$$\{i \mid \sigma(i) \neq i\} \neq \emptyset,$$

因此 i_0 存在. 由于对任意 $j < i_0$ (如果 j 存在), 我们有 $\sigma(j) = j$, 因此若 $\sigma(i_0) \neq i_0$, 那么我们有

$$\sigma(i_0) > i_0.$$

另一方面, 由于 σ 为有限阶元素, 因此存在 $k > 0$ 使得 $\sigma^k(i_0) = i_0$. 我们记

$$j_0 = \sigma^{k-1}(i_0),$$

注意到 σ 固定所有比 i_0 小的自然数. 因此 $j_0 > i_0$. 另一方面, 我们有

$$\sigma(j_0) = i_0 < \sigma(i_0).$$

因此

$$(i_0, j_0) \in \{(i, j) \in \mathbb{N}^2 \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\}.$$

从而我们有 $\rho(\sigma) \neq 0$. □

我们在使用置换定义行列式的时候已经遇到了这个概念. 这里我们给出逆序数与之前讨论的几个概念之间的关系.

命题 8.2.39

设 n 为非零自然数. 任取 $\sigma \in S_n$, 我们有

- (i) 任意 σ 有由 $\rho(\sigma)$ 个对换构成的分解.
- (ii) $\text{sgn}(\sigma) = 1$ 当且仅当 $\rho(\sigma)$ 为偶数.

证明. (i) 任取 $i \in \{1, \dots, n\}$, 我们记

$$U_i = \{(i, j) \in \mathbb{N}^2 \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\}$$

因此集合

$$U = \{(i, j) \in \mathbb{N}^2 \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\} = U_1 \cup \cdots \cup U_n.$$

为不交并.

我们首先考虑 U_1 中的元素, 也即第一个位置是 1 的元素. 设 $\sigma(1) = i_k$, 若 $k = 1$, 则 $U_1 = \emptyset$. 如果 $k > 1$, 则以上集合中第一个位置是 1 的元素有

$$U_1 = \{(1, i_1), \dots, (1, i_{k-1})\}.$$

通过进行以下置换

$$\sigma_1 = (1i_1) \cdots (1i_{k-1}),$$

我们将 1 移动到第一个位置. 我们记

$$\sigma_1 \sigma = \begin{pmatrix} 1 & 2 & \cdots & k & k+1 & \cdots & n \\ 1 & i_1 & \cdots & i_{k-1} & i_{k+1} & \cdots & i_n \end{pmatrix}$$

我们下边考虑集合 U_2 . 由于 1 此时在第一个位置, 我们通过 $|U_2|$ 个对换的乘积可以将 2 移动到第二个位置上而不改变 $U_3 \cup \cdots \cup U_n$ 中的元素. 我们记这个元素为 σ_2 .

我们依次对 $U_3, \dots, U_n$ 重复以上操作, 将所使用的对换的乘积分别记为 $\sigma_3, \dots, \sigma_n$. 最终我们将 $(i_1, \dots, i_n)$ 重新排列为 $(1, 2, \dots, n)$. 因此

$$\sigma^{-1} = \sigma_n \cdots \sigma_1.$$

注意到在构造过程中, σ_i 可以写为 U_i 个对换的乘积. 因此 σ^{-1} 可以写为

$$|U| = |U_1| + |U_2| + \cdots + |U_n|,$$

个对换的乘积, 也即 σ 可以写为 $\rho(\sigma) = |U|$ 个对换的乘积.

□

注 8.2.40.

注意到 $\rho(\sigma)$ 不一定是 σ 对换分解最小的对换数目. 例如

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

注意到其逆序数为 3 (这里 $\sigma(1) > \sigma(3)$, $\sigma(2) > \sigma(3)$ 以及 $\sigma(1) > \sigma(2)$). 但实际上 $\sigma = (13)$.

另一方面, 考虑有限序列 $(\sigma(1), \dots, \sigma(n))$, 我们希望仅利用对相邻两个位置上的元素做对换, 来将这个序列重排为 $(1, \dots, n)$, 那么以上构造说明 $\rho(\sigma)$ 是需要的最小的数目. 注意到交换 $\sigma(i)$ 和 $\sigma(i+1)$ 对逆序数的影响是或者 +1 或者 -1, 而以上构造中, 每一步都是 -1. 因此是最小数目.

思考 8.2.41

设 $n \in \mathbb{N}^*$, 任取 $\sigma \in S_n$, 如何实现 σ 的最小个数的对换分解?

注 8.2.42.

我们知道 S_n 可以由对换生成. 以上问题实际上在问, 任给一个 σ , 生成 σ 最少要用多少生成元?

8.3 交错群

我们首先考虑 4×4 的数字华容道的游戏. 我们考虑以下问题:

- (i) 将 15 个数字取出打乱再放入盒子中, 是否一定可以将这 15 个数字按照顺序排列在盒子中?
- (ii) 不实际操作, 我们可否从初始状态就能看出所给的情形是否可解?
- (iii) 是否可以在按顺序排列的初始状态下, 经过有限次步骤将 14 和 15 互换?

实际上这个问题和我们下边要讨论的交错群有这紧密的联系. 我们首先给出交错群的概念.

之前我们已经了解了一个对称群中的元素可以分为奇置换和偶置换两种. 我们还定义了符号同态映射

$$\text{sgn} : S_n \rightarrow \{1, -1\}.$$

注意到以上同态的核为所有的偶置换. 所有偶置换构成 S_n 的一个子群.

定义 8.3.1

设 n 为非零自然数. 对称群 S_n 中所有偶置换构成的群被称为 n -元交错群, 记为 A_n .

由之前对同态映射的核的讨论, 我们有如下结论:

命题 8.3.2

设 n 为非零自然数. 则 n -元交错群是 n -元对称群的正规子群, 即 $A_n \triangleleft S_n$.

证明. 我们也可以直接证明这个结论. 注意到任意奇置换的逆也是奇置换, 任意偶置换的逆也是偶置换. 因此任取 $\sigma \in A_n$ 以及 $\tau \in S_n$, 我们有 $\tau\sigma\tau^{-1}$ 为偶置换. 因此 $\tau\sigma\tau^{-1} \in A_n$. $\square$

其次, 我们考虑 A_n 在 S_n 中的陪集. 我们考虑 $(12) \in S_n$.

命题 8.3.3

设 n 为非零自然数且 $n > 1$, 则 S_n 有以下划分

$$S_n = A_n \cup (12)A_n.$$

证明. 由于奇置换与偶置换的乘积为奇置换. 因此我们有

$$A_n \cap (12)A_n = \emptyset.$$

由于两个奇置换的乘积为偶置换, 任取 $\tau \in S_n$, 若 τ 为偶置换, 则 $\tau \in A_n$, 若 τ 为奇置换, 我们有

$$\tau = (12)((12)\tau) \in (12)A_n.$$

因此命题得证. $\square$

我们进一步有

命题 8.3.4

设 n 为一个非零自然数且 $n > 1$. 则 n -元交错群 A_n 满足

$$|A_n| = \frac{n!}{2}.$$

证明. 注意到 $L_{(12)}$ 为一个左平移映射, 因此是一个双射. 由于 S_n 为有限群, 考虑 S_n 关于 A_n 的陪集分解, 我们有

$$n! = |S_n| = |A_n| + |(12)A_n| = 2|A_n|.$$

由此命题得证. □

类似于对 S_n 的讨论, A_n 也是可以由特殊的轮换生成.

命题 8.3.5

设 n 为大于 3 的非零自然数, 则 A_n 由 S_n 中的 3-轮换生成.

证明. 我们先考虑两个对换 (ab) 和 (cd) .

(i) 如果 $\{a, b\} = \{c, d\}$, 则 $(ab)(cd) = e$;

(ii) 如果 $\#\{a, b\} \cap \{c, d\} = 1$, 不妨设 $a = c$, 则有 $(ab)(ad) = (adb)$.

(iii) 如果 $\{a, b\} \cap \{c, d\} = \emptyset$, 则有

$$(ab)(cd) = (ab)(ac)(ac)(cd) = (acb)(cda).$$

由于 A_n 中的置换都可以写为偶数个对换的乘积, 我们可以将相邻的两个配对, 用以上放些改写为三轮换的乘积. 因此我们有以上命题. □

注 8.3.6.

如果考虑华容道中的情况, 我们可以先考虑 2×2 的情况, 注意到, 在经过有限步操作后, 将右下角空出, 我们所得的总是起始的 123 的一个三轮换. 我们可以将这个观察推广到 4×4 的情形, 或者更一般的情形. 因此通过移动方块得到的排序总是起始的 $(1, 2, \dots, 15)$ 的一个偶置换. 实际上, 我们可以进一步证明, 我们可以实现所有的偶置换. 因此如果我们将方块取随机重排之后, 会有 50% 的机会不能复原到 $(1, 2, \dots, 15)$.

本节最后一部分用来证明以下命题.

命题 8.3.7

任取自然数 $n \geq 5$, 交错群 A_n 是一个单群.

设自然数 $n \geq 4$. 我们记

$$B = \{(ij)(kl) \mid 1 \leq i, j, k, l \leq n \text{ 且两两不等}\},$$

并记

$$T = \{(ijk) \mid 1 \leq i, j, k \leq n \text{ 且两两不等}\}.$$

引理 8.3.8

任取 $n \geq 4$, n 元交错群 A_n 可以由 $B \cup T$ 生成.

引理 8.3.9

任取 $n \geq 4$, B 中任意两个元素之间都共轭, T 中任意两个元素之间都共轭.

引理 8.3.10

任取 $n \geq 5$, B 生成的 S_n 的子群中包含 T 中的元素; 另一方面 T 生成的 S_n 的子群也包含 B 中的元素.

推论 8.3.11

任取 $n \geq 5$, n 元交错群 A_n 的正规子群只有 $\{id\}$ 和 A_n . (A_n 为单群)

证明. 我们只需证明任给 A_n 的非 $\{id\}$ 正规子群 N , 我们总有

$$N \cap B \neq \emptyset.$$

我们对 n 使用归纳法证明以上命题对 $n \geq 4$ 均成立. 当 $n = 4$ 时, A_4 的非平凡正规子群是四元群 V 的子群, 因此结论成立.

我们假设结论对 $n - 1 \geq 4$ 成立, 下边考虑 A_n . 设 $N \triangleleft A_n$ 为一个非平凡子群. 注意到任给 N 中的一个元素 σ , 存在 n 的一个分划: $k_1 + k_2 + \cdots + k_s = n$, 元素 σ 可以写成

$$\sigma = \sigma_1 \cdots \sigma_s,$$

其中对任意 $1 \leq i \leq s$, σ_i 是一个 k_i 轮换, 并且任给 $1 \leq i \neq j \leq s$, σ_i 和 σ_j 涉及的数字的集合不交.

若 σ_i 都是对换, 不妨设

$$\sigma = (12)(34) \cdots.$$

我们考虑

$$\tau = (123)\sigma(132) \in N.$$

则有

$$(13)(24) = \tau\sigma \in N.$$

结论成立.

若 σ 在 $\{1, \dots, n\}$ 中有不动点, 也即存在 $k_i = 1$, 我们可以将其看作一个 A_{n-1} 中的元素. 由归纳假设, 结论成立. 下设 σ 在 A_n 中没有不动点, 且包含长度大于 2 的轮换, 不妨设为

$$\sigma_1 = (12 \dots l),$$

任取 $3 < d \leq n$. 记

$$\sigma' = (2\sigma(d))(1d)\sigma(1d)(2\sigma(d)).$$

则有

$$\sigma'(d) = \sigma(d), \quad \sigma'^{-1}(3) \neq \sigma^{-1}(3).$$

因此 $\sigma'^{-1}\sigma$ 为一个固定 d 的非平凡元素. 我们可以使用共轭变换使 $d = n$, 以上证明说明 $N \cap A_{n-1}$ 中有非平凡元素. 注意到

$$N \cap A_{n-1} \triangleleft A_{n-1}.$$

由归纳假设我们有 $(N \cap A_{n-1}) \cap B \neq \emptyset$. 因此 $N \cap B \neq \emptyset$, 结论对 A_n 成立.

由之前的引理, 我们有

$$N = A_n.$$

□

注 8.3.12.

注意这里说 A_n ($n \geq 5$) 是单群的时候, 我们考虑的是关于 A_n 里的元素的共轭, 不是关于 S_n 里的元素的共轭.

推论 8.3.13

设自然数 $n \geq 5$. 任取 $N \triangleleft S_n$, 若 $N \neq \{e\}$ 且 $N \neq S_n$, 则 $N = A_n$.

证明. 任取 S_n 中的正规子群 N , 我们考虑 $N \cap A_n$. 欲证明这个子群包含非平凡元素.

任取 $\sigma \in N \setminus \{e\}$, 由于 $N \triangleleft S_n$, 因此我们有 $[\sigma]$ 即 σ 的共轭类在 N 中. 注意到 $|[\sigma]| = 1$ 当且仅当 $\sigma \in Z(S_5) = \{e\}$, 因此我们有 $\tau \in [\sigma]$ 且 $\tau \neq \sigma$. 考虑 $\tau\sigma \in N$, 由于 τ 和 σ 共轭因此有相同的奇偶性. 由此可得 $\tau\sigma \in A_n$.

综上所述, 我们有 $N \cap A_n \neq \{e\}$. 注意到 $N \cap A_n \triangleleft A_n$, 由 A_n 为单群知 $N \cap A_n = A_n$. 因此我们有

$$A_n < N < S_n.$$

考虑群的指数有

$$2 = [S_n : A_n] = [S_n : N][N : A_n].$$

因此 $[S_n : N] = 2$ 或者 $[N : A_n] = 2$, 也即 $[N : A_n] = 1$ 或者 $[S_n : N] = 1$. 因此有 $N = A_n$ 或者 $N = S_n$. 由假设 $N \neq S_n$, 我们有 $N = A_n$. □

第九章 群在集合上的作用

我们在之前的部分已经见过一些群作用的例子. 例如, 对称群的元素交换一个坐标系基底中的元素, 或者交换一个四面体的顶点, 或者交换多项式的根等等. 本节我们将在更一般的意义上研究一个群在一个集合上的作用.

9.1 定义

我们这里给出"一个群作用在一个非空集合上"的定义.

定义 9.1.1 (教材定义 1.9.1)

设 X 为一个非空集合, G 是一个群. 我们称映射

$$\begin{aligned} f : G \times X &\rightarrow X \\ (a, x) &\mapsto f(a, x) \text{ (简记为 } a.x \text{ 或 } ax) \end{aligned}$$

为 G 在 X 上的(左)作用, 若 f 满足以下条件:

- (i) 任取 $x \in X$, 有 $e.x = x$;
- (ii) 任给 $a, b \in G$, 任取 $x \in X$, 有 $(ab).x = a.(b.x)$.

我们注意到, 任取 $a \in G$, 我们可以定义映射:

$$\begin{aligned} f_a : X &\rightarrow X \\ x &\mapsto f(a, x) = a.x \end{aligned}$$

由 (ii), 任取 $a, b \in G$, 我们有

$$f_{ab} = f_a \circ f_b.$$

引理 9.1.2

设群 G 作用在非空集合 X 上, 任取 $a \in G$, 映射 f_a 为 X 到自己的双射. 我们进一步有

$$f_{a^{-1}} = (f_a)^{-1}.$$

证明. 由 G 在 X 上的作用的定义, 任取 $a \in G$, 我们有

$$f_{a^{-1}} \circ f_a = f_a \circ f_{a^{-1}} = f_e = id.$$

因此 f_a 既是单射又是满射. 因此 f_a 是双射, 且

$$f_{a^{-1}} = (f_a)^{-1}.$$

□

我们之前在讨论群的左平移的时候曾经考虑过一个集合上所有双射的集合在复合作用下是一个群. 由群在集合上的作用的定义我们有以下结论.

命题 9.1.3

设群 G 作用在一个非空集合 X 上. 映射

$$\begin{aligned}\phi : G &\rightarrow S_X \\ a &\mapsto f_a\end{aligned}$$

是一个群同态.

注 9.1.4.

这里我们定义的群作用通常也称为群的左作用. 如果任给 $a, b \in G$, 我们有

$$f_{ab} = f_b \circ f_a,$$

那么我们称这个作用是一个右作用. 对应的 G 到 S_X 的映射是一个群的"反同态". 除了特殊说明外, 本章我们只考虑左作用.

定理 9.1.5 (教材定理 1.9.2)

记 G 为一个群, X 为一个非空集合. 任意群同态

$$\phi : G \rightarrow S_X,$$

定义一个群 G 在 X 上的作用. 另一方面, 若 ϕ 和 ψ 都是 G 到 S_X 的同态, 则 ϕ 和 ψ 定义的作用相同当且仅当 $\phi = \psi$.

证明. 我们记 $\text{Hom}(G, S_X)$ 为所有 G 到 S_X 的同态的集合. 任取 $\phi \in \text{Hom}(G, S_X)$, 我们可以定义

$$\begin{aligned}f : G \times X &\rightarrow X \\ (a, x) &\mapsto a.x := (\phi(a))(x).\end{aligned}$$

由计算得, 任取 $x \in X$ 和 $a, b \in G$

$$(i) \quad e.x = (\phi(e))(x) = id(x) = x;$$

$$(ii) \quad ab.x = (\phi(ab))(x) = (\phi(a) \circ \phi(b))(x) = (\phi(a))((\phi(b))(x)) = a.(b.x).$$

因此 f 是一个 G 在 X 上的作用.

设 $\phi, \psi \in \text{Hom}(G, S_X)$. 我们分别记 f 和 g 为 ϕ 和 ψ 诱导的 G 在 X 上的作用.

若 $\phi = \psi$, 则任取 $a \in G, x \in X$, 我们有

$$f(a, x) = \phi(a)(x) = \psi(a)(x) = g(a, x).$$

因此 $f = g$, 二者给出得 G 在 X 上的作用相同.

另一方面, 若 $f = g$, 则任取 $a \in G$, 任取 $x \in X$,

$$\phi(a)(x) = f(a, x) = g(a, x) = \psi(a)(x).$$

因此对任意 $a \in G$, $\phi(a) = \psi(a)$. 由此可得 $\phi = \psi$. $\square$

注 9.1.6.

有以上定理可知, G 在 X 上的作用和 $\text{Hom}(G, S_X)$ 中的元素是一一对应的. 因此给定一个群 G 和一个非空集合 X , G 在 X 上的作用不一定唯一.

例 9.1.7.

我们考虑二面体群 D_4 . 我们仍使用之前的约定, 即考虑的正方形的四个顶点分别在 $(1, 1)$, $(-1, 1)$, $(-1, -1)$ 和 $(1, -1)$. 令

$$X = \{(1, 1), (-1, 1), (-1, -1), (1, -1)\},$$

考虑 D_4 对平面上点的移动, 我们有 D_4 在 X 上的作用.

例 9.1.8.

任取集合 X . 令 G 为 X 到自己的双射的群 S_X , 则 G 作用在 X 上. 由定义, 对称群 S_n 作用在 $\{1, \dots, n\}$.

例 9.1.9.

记 G 为一个群, 任取 $a \in G$, 则由 a 给出的左平移 L_a 是一个 G 在 G 上的作用. 考虑右平移, 任取 $a, b \in G$, 我们有

$$R_{ab} = R_b \circ R_a.$$

因此 $a \mapsto R_a$ 是一个群的反同态. 另一方面, 取逆的映射 $a \mapsto a^{-1}$ 是 G 到 G 的反同态, 我们考虑以下映射的复合

$$a \mapsto a^{-1} \mapsto R_{a^{-1}},$$

这个映射诱导了 G 在 G 上的一个作用. 我们可以如下验证: 任取 $a, b, c \in G$, 我们有

$$(ab).c = R_{(ab)^{-1}}(c) = R_{b^{-1}a^{-1}}(c) = cb^{-1}a^{-1} = (R_{a^{-1}} \circ R_{b^{-1}})(c) = a.(b.c).$$

任取 $a \in G$, 之前我们也介绍过共轭作用: $a \mapsto \text{Ad}_a$. 这个也给出 G 在 G 上的作用.

例 9.1.10.

设 G 为一个群, H 为 G 的子群. 任取 $a, b \in G$, 我们考虑 $a(bH) = (ab)H$. 这个关系给出了 G 在 H 的左陪集集合 G/H 上的作用.

例 9.1.11.

设 n 为非零自然数. 我们考虑 n 维实线性空间 V , 以及 V 上线性自同构群 $\text{GL}(V)$, 则利用线性映射在线性空间上的作用 $\text{GL}(V)$ 作用在 V 上.

9.2 群作用的轨道

在介绍完定义之后, 我们开始进一步的研究一个给定的群在集合上的作用的性质, 其中一个重要的概念就是作用的轨道. 我们之前在讨论对称群的时候已经介绍过轨道的概念(见定义 8.2.12).

群作用轨道的定义

定义 9.2.1

设群 G 在非空集合 X 上有一个作用, 任取 $x \in X$, 我们记

$$G.x := \{a.x \in X \mid a \in G\}.$$

并称该集合为 x 在 G 作用下的**轨道**, 也称之为过 x 的 G -轨道.

例 9.2.2.

我们考虑二面体群 D_4 作用在 $\mathbb{R}^2$ 上, 则任取 $(x, y) \in \mathbb{R}^2$, 其在 D_4 作用下的轨道是

$$D_4.(x, y) = \{(x, y), (-y, x), (-x, -y), (y, -x)\}.$$

例 9.2.3.

我们考虑 2 阶特殊正交群

$$\mathrm{SO}(2) := \left\{ \begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix} \mid \theta \in [0, 2\pi) \right\}.$$

群 $\mathrm{SO}(2)$ 在平面上的作用是将平面绕原点旋转. 因此 $\mathbb{R}^2$ 中点 (x, y) 的轨道是

$$\mathrm{SO}(2).(x, y) = \{(w, z) \in \mathbb{R}^2 \mid w^2 + z^2 = x^2 + y^2\}.$$

为一个半径为 $x^2 + y^2$ 圆心在原点的圆.

例 9.2.4.

设 n 为非零自然数. 我们考虑对称群 S_n 在集合 $\{1, \dots, n\}$ 上的作用. 注意到 S_n 包含所有的对换 (ij) , 因此任取 $k \in \{1, \dots, n\}$, 它的轨道为

$$S_n.k = \{1, \dots, n\}.$$

可递作用

注意到以上例子中, 有的例子中一个点的轨道是全集, 有的则不是.

定义 9.2.5 (教材定义 1.9.7)

设群 G 在非空集合 X 上有一个作用. 我们称这个作用是**可递的**(transitive), 若对任意 $x, y \in X$, 存在 $a \in G$, 满足

$$a.x = y.$$

我们称这个作用是**有效的**(faithful, 也有称**忠实的**), 若 $a \in G$, 满足对任意 $x \in X$, $a.x = x$, 则有 $a = e$.

考虑群作用的定义, 我们可以给出作用可递的一个充要条件.

命题 9.2.6

设群 G 在非空集合 X 上有一个作用. 以下两个条件等价:

- (i) G 在 X 上的作用可递.
- (ii) 存在 $x \in X$, 满足 $G.x = X$.

证明. 若 G 在 X 上作用可递, 我们选取并固定 $x \in X$, 由可递的定义, 对任意 $y \in X$, 存在 $a \in G$, 满足

$$y = a.x \in G.x.$$

因此 $X \subset G.x$, 从而有 $X = G.x$.

另一方面, 设存在 $x \in X$, 使得 $G.x = X$. 任取 $y, z \in X$, 存在 $a, b \in G$, 满足

$$y = a.x, \quad z = b.x.$$

因此

$$y = a.x = a.(b^{-1}.z) = (ab^{-1}).z.$$

因此 G 在 X 上作用可递. □

例 9.2.7.

我们考虑群 $SO(2)$. 该群可以作用在 $\mathbb{R}^2$ 上, 之前的讨论说明这个作用不是可递的. 另一方面, 我们也可以令 X 为以原点为圆心的单位圆, $SO(2)$ 在这个 X 上的作用是可递的.

例 9.2.8.

设 G 为一个群, H 为 G 的一个子群. 我们考虑 G 在 H 的左陪集上的作用. 这个作用是可递的. 因为任取 $a \in G$, 我们有

$$a.H = aH.$$

因此 $G.H = G/H$.

 X 关于 G 作用的分解

如同之前在关于对称群的部分讨论的一样, G 在 X 上的作用的轨道给出了 X 上的一个划分.

命题 9.2.9

设群 G 在非空集合 X 上有一个作用. 任取 $x, y \in X$, 以下两个叙述等价:

- (i) x 和 y 属于同一个 G -轨道;
- (ii) $G.x = G.y$.

证明. 任取 $x, y \in X$, 设存在 $z \in X$, 满足 $x, y \in G.z$, 则存在 $a, b \in G$, 满足

$$x = a.z, \quad y = b.z.$$

因此

$$y = (ab^{-1}).x, \quad x = (ba^{-1}).y$$

由第一个, 任取 $x' \in G.x$, 存在 $a' \in G$, 满足 $x' = a'.x$. 因此

$$x' = a'.((ba^{-1}).y) = (a'ba^{-1}).y \in G.y.$$

所有我们有 $G.x \subset G.y$. 同理我们有 $G.y \subset G.x$. 因此 $G.x = G.y$.

反过来, 若 $G.x = G.y$, 由于 $x \in G.x$ 且 $y \in G.y = G.x$, 因此 x 和 y 属于同一个 G -轨道. $\square$

推论 9.2.10

设群 G 在非空集合 X 上有一个作用, 则任取 $x, y \in X$,

- 或者 $G.x = G.y$;
- 或者 $G.x \cap G.y = \emptyset$.

证明. 设 $G.x \cap G.y \neq \emptyset$, 则存在 $z \in G.x \cap G.y$, $a, b \in G$, 满足

$$z = a.x = b.y.$$

因此 $x = a^{-1}.z \in G.z$, 且 $y = b^{-1}.z \in G.z$. 由以上命题知 $G.x = G.y$. $\square$

推论 9.2.11

设群 G 在非空集合 X 上有一个作用, 则以下给出了 X 上的一个等价关系:

- 任取 $x, y \in X$, 我们定义 $x \sim y$ 当且仅当 $G.x = G.y$.

进一步地, 包含 $x \in X$ 的等价类就是 $G.x$.

稳定化子

考虑 G 作用在一个非空集合 X 上. 任取 $a \in G$ 和 $x \in X$, 一种特殊的情况就是 $a.x = x$. 我们可以考虑 G 中哪些元素固定 x , 这就是稳定化子的概念.

定义 9.2.12

设群 G 在非空集合 X 上有一个作用. 任取 $x \in X$, 我们考虑 G 的子集:

$$G_x := \{a \in G \mid a.x = x\}.$$

我们称 G_x 为 x 的**稳定化子**(stabilizer/迷向子群 isotropy subgroup). 若 $x \in X$ 满足 $G_x = G$, 我们称 x 为 G -作用的**不动点**. 我们记 G 在 X 上作用的不动点的集合为

$$\text{Fix}(G) := \{x \in X \mid G_x = G\}.$$

我们先来看一些例子.

例 9.2.13.

我们考虑二面体群 D_4 . 我们仍考虑以下平面上的点构成的集合.

$$X = \{(1, 1), (-1, 1), (-1, -1), (1, -1)\},$$

考虑 D_4 在 X 上的作用. 注意到固定 $(1,1)$ 的除了 id 之外就是反射 s . 因此 $(1,1)$ 的稳定化子就是

$$\{id, s\}.$$

例 9.2.14.

设 n 为一个大于 1 的自然数. 我们考虑对称群 S_n 在 $\{1, \dots, n\}$ 上的作用. 任取

$$k \in \{1, \dots, n\},$$

则 k 的稳定化子是所有其他 $n-1$ 个数字

$$\{1, \dots, k-1, k+1, \dots, n\},$$

的所有置换, 因此同构于 S_{n-1} .

例 9.2.15.

设 n 为一个非零自然数. 我们考虑矩阵群 $GL(n, \mathbb{R})$ 在 $\mathbb{R}^n$ 上的作用. 任取非零向量 $\vec{v} \in \mathbb{R}^n$, 则 $\vec{v}$ 的稳定化子为

$$\{A \in GL(n, \mathbb{R}) \mid A(\vec{v}) = \vec{v}\}.$$

我们考虑特征值和特征向量的概念就可以看出, 一个可逆矩阵 A 属于以上子群当且仅当 $\vec{v}$ 是 A 的关于特征值 1 的特征向量.

命题 9.2.16

考虑群 G 作用在一个非空集合 X 上. 任取 $x \in X$, 集合

$$G_x := \{a \in G \mid a.x = x\},$$

为 G 的一个子群.

证明. 注意到 e 在 X 上的作用是恒等映射, 也即任取 $x \in X$, 我们有 $e.x = id(x) = x$. 因此 $e \in G_x$, 集合 G_x 非空.

设 $a \in G_x$, 我们有 $a.x = x$. 由群作用的定义, 我们有

$$a^{-1}.x = a^{-1}.(a.x) = (a^{-1}a).x = x.$$

因此 $a^{-1} \in G_x$.

设 $a, b \in G_x$, 由定义我们有

$$a.x = x, \quad b.x = x,$$

因此

$$(ab).x = a.(b.x) = a.x = x.$$

因此 $ab \in G_x$.

由以上结论可得, G_x 非空, 且任取 $a, b \in G_x$, 我们有 $ab^{-1} \in G_x$, 因此 G_x 为 G 的一个子群. $\square$

群 G 在 X 上的作用可以诱导一个 G 在 X 的子集的集合 $\mathcal{P}(X)$ 上的作用. 考虑这个作用, 我们也可以定义 X 的子集的稳定化子.

定义 9.2.17

设群 G 作用在一个非空集合 X 上, 任取 X 的非空子集 Y , 我们称以下集合

$$G_Y := \{a \in G \mid a.Y = Y\},$$

为 Y 的**稳定化子**.

注 9.2.18.

集合 G_Y 是 G 的一个子群的证明与之前类似, 我们这里就不再重复.

注 9.2.19.

这里我们是将 Y 作为 X 的幂集中的元素来看, 因此任给 $a \in G$, 我们只考虑 $a.Y = Y$ 作为集合的等式是否成立. 但是 a 有可能会对 Y 中的元素进行置换. 如果我们希望固定所有 Y 中的元素, 我们将称之为**点态稳定化子**:

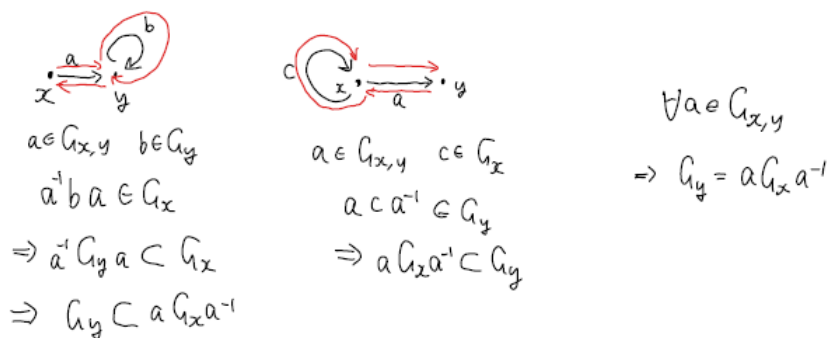
$$G_Y^{pw} = \{a \in G \mid \forall x \in Y, a.x = x\} = \bigcap_{x \in Y} G_x.$$

我们下边给出稳定化子的一个性质:

命题 9.2.20

设群 G 作用在非空集合 X 上. 任取 $x \in X$, 对任意 $y \in G.x$, 存在 $a \in G$, 满足

$$G_y = aG_xa^{-1}.$$



$a \in G_{x,y} \quad b \in G_y$
 $a^{-1}ba \in G_x$
 $\Rightarrow a^{-1}G_ya \subset G_x$
 $\Rightarrow G_y \subset aG_xa^{-1}$

$a \in G_{x,y} \quad c \in G_x$
 $aca^{-1} \in G_y$
 $\Rightarrow aG_xa^{-1} \subset G_y$

$\forall a \in G_{x,y}$
 $\Rightarrow G_y = aG_xa^{-1}$

证明. 任取 $y \in G.x$, 则存在 $a \in G$, 满足

$$y = a.x.$$

因此任取 $b \in G_x$, 我们有

$$(aba^{-1}).y = a.(b.(a^{-1}.y)) = a.(b.x) = a.x = y.$$

因此我们有 $aG_xa^{-1} \subset G_y$.

另一方面, 任取 $c \in G_y$, 类似于以上讨论, 我们有

$$(a^{-1}ca).x = x.$$

因此 $c \in aG_xa^{-1}$, 从而有 $G_y \subset aG_xa^{-1}$.

综上所述, 我们有 $G_y = aG_xa^{-1}$. □

例 9.2.21.

考虑之前讨论的例子 7.3.16. 我们可以考虑 $\mathbb{R}^2$ 上欧式度量的保定向的等距变换群可以作用在 $\mathbb{R}^2$ 的所有的圆构成的集合上. 我们注意到每个圆在这个作用下的轨道是所有有相同半径的圆.

我们考虑以原点为圆心的半径为 1 的圆. 注意到这个圆的稳定化子是 $SO(2)$. 这是因为我们目前考虑的是圆构成的子集, 虽然 $SO(2)$ 旋转了圆, 但是作为集合, 这个圆并没有变.

如果我们考虑另一个在这个轨道中的圆是圆心在 $\vec{v} = (1, 0)$ 半径为 1 的圆, 则其稳定化子为

$$T_{\vec{v}} \circ SO(2) \circ T_{\vec{v}}^{-1}.$$

我们下边考虑一个类似的问题: 任取 $x, y \in X$, 所有将 x 送到 y 的 G 的元素构成的集合是怎样的?

注意到 $x = y$ 的情况就是我们之前讨论的稳定化子. 下边假设 $x \neq y$. 我们发现如果 $a, b \in G$ 都将 x 送到 y , 则 $b^{-1}a \in G_x$. 我们记

$$G_{x,y} := \{a \in G \mid a.x = y\}.$$

以上讨论告诉我们以下结论.

命题 9.2.22

设群 G 作用在非空集合 X 上. 任取 $x \in X$, 任取 $a \in G$ 记 $y = a.x$, 则

$$G_{x,y} = aG_x.$$

即 $G_{x,y}$ 是 G_x 的一个左陪集.

Handwritten diagrams illustrating the proof of Proposition 9.2.22. The first diagram shows a mapping from x to y via element b , and then y to y via element a , resulting in a mapping from x to y via element ab . The second diagram shows a mapping from x to y via element a , and then y to x via element b , resulting in a mapping from x to x via element ba . The third diagram shows a mapping from x to y via element a , and then y to y via element b , resulting in a mapping from x to y via element ab . The fourth diagram shows a mapping from x to y via element a , and then y to x via element b , resulting in a mapping from x to x via element ba . The fifth diagram shows a mapping from x to y via element a , and then y to y via element b , resulting in a mapping from x to y via element ab . The sixth diagram shows a mapping from x to y via element a , and then y to x via element b , resulting in a mapping from x to x via element ba . The seventh diagram shows a mapping from x to y via element a , and then y to y via element b , resulting in a mapping from x to y via element ab . The eighth diagram shows a mapping from x to y via element a , and then y to x via element b , resulting in a mapping from x to x via element ba . The ninth diagram shows a mapping from x to y via element a , and then y to y via element b , resulting in a mapping from x to y via element ab . The tenth diagram shows a mapping from x to y via element a , and then y to x via element b , resulting in a mapping from x to x via element ba .

证明. 以上讨论告诉我们, $G_{x,y} \subset aG_x$. 另一方面, 任取 $c \in G_x$, 我们有

$$(ac).x = a.(c.x) = a.x = y.$$

因此 $ac \in G_{x,y}$, 我们进而有 $aG_x \subset G_{x,y}$.

综上所述, 我们有 $G_{x,y} = aG_x$. □

推论 9.2.23

我们沿用以上记号. 存在双射:

$$\begin{aligned}\Phi: G.x &\rightarrow \{aG_x \mid a \in G\} \\ a.x &\mapsto aG_x\end{aligned}$$

证明. 之前的命题说明以上映射定义是良好的. 任取 $a, b \in G$, 由之前的命题, 我们知道

$$aG_x = G_{x,a.x}, \quad bG_x = G_{x,b.x}.$$

若 $a.x \neq b.x$, 则 $G_{x,a.x} \neq G_{x,b.x}$, 因此 $aG_x \neq bG_x$, 映射 Φ 是单射. 另一方面, 任取左陪集 aG_x , 我们总有 $a \in aG_x$. 我们有 $a.x \in G.x$, 满足 $\Phi(a.x) = aG_x$. 因此 Φ 是满射. $\square$

等价作用

如同我们之前关于 $SO(2)$ 的作用的讨论, 一个群 G 可以作用在不同的集合上. 另一个比较简单的例子就是对称群的作用. 我们可以取 4 个数字 $\{1, 2, 3, 4\}$, 也可以取 $\{3, 5, 7, 9\}$. 对称群 S_4 都可以作用在上边. 但是这两个作用似乎"在某种意义上"是相同的(等价的). 我们下边将尝试比较同一个群在不同集合上的作用, 并给出等价作用的定义.

定义 9.2.24 (教材定义 1.9.13)

设群 G 分别作用在非空集合 X 和非空集合 Y 上. 设存在双射

$$f: X \rightarrow Y,$$

满足任取 $x \in X$ 以及 $a \in G$, 我们有

$$a.f(x) = f(a.x),$$

那么我们称 G 在 X 上的作用和在 Y 上的作用**等价**.

注 9.2.25.

从映射的角度, 以上条件在讲以下交换图:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ a \downarrow & & \downarrow a \\ X & \xrightarrow{f} & Y \end{array}$$

对任意 $a \in G$ 都成立.

我们考虑 G 在轨道 $Y = G.x \subset X$ 上的作用.

命题 9.2.26 (教材定理 1.9.14)

设存在群 G 作用在非空集合 X . 任取 $x \in X$, 则 G 在 G/G_x 上的作用与 G 在 $G.x$ 上的作用等价.

例 9.2.27.

我们借用以下例子来说明该定理的叙述.

考虑 $G = S_3$ 在 $X = \{1, 2, 3\}$ 上的置换给出的作用. 注意到 G 在 X 上的作用是可递的, 因此任取 $i \in X$, 我们有 $G.i = X$.

下边考虑 $x = 1$, 因此有

$$G.1 = \{1, 2, 3\}.$$

另一方面我们考虑

$$G = \{e, (12), (13), (23), (123), (132)\}.$$

注意到

$$G_1 = \{e, (23)\}.$$

考虑 G_1 的左陪集

$$\begin{aligned} eG_1 &= (23)G_1, \\ (12)G_1 &= (123)G_1, \\ (13)G_1 &= (132)G_1. \end{aligned}$$

以及左陪集空间

$$G/G_1 = \{eG_1, (12)G_1, (13)G_1\}.$$

我们定义 $G.1$ 到 G/G_1 的映射如下

$$\begin{aligned} f : G.1 &\rightarrow G/G_1, \\ 1 &\mapsto eG_1, \\ 2 &\mapsto (12)G_1, \\ 3 &\mapsto (13)G_1. \end{aligned}$$

考虑 $G = S_3$ 在 $G.1$ 上的置换作用和在 G/G_1 上的左乘作用. 令 $\sigma = (12) \in G$, 我们有

$$\begin{aligned} (12).1 &= 2 & (12).(eG_1) &= (12)G_1 \\ (12).2 &= 1 & (12).((12)G_1) &= (12)(12)G_1 = eG_1 \\ (12).3 &= 3 & (12).((13)G_1) &= (12)(13)G_1 = (132)G_1 = (13)G_1 \end{aligned}$$

一下是 σ 作用的示意图

$$\begin{array}{ccc} 1 & \xrightarrow{f} & eG_1 \\ \sigma \uparrow & & \downarrow \sigma \\ 2 & \xrightarrow{f} & (12)G_1 \end{array}$$

$$\begin{array}{ccc} 3 & \xrightarrow{f} & (13)G_1 \\ \sigma \curvearrowright & & \curvearrowright \sigma \end{array}$$

因此我们有 $\sigma \circ f = f \circ \sigma$. 类似地, 我们可以验证任意 $\tau \in S_3$ 都满足 $\tau \circ f = f \circ \tau$. 因此 S_3 在 $G.1$ 和 G/G_1 上的作用等价.

注 9.2.28.

如果群 G 在 X 上有一个作用, 则这个作用可以诱导一个 G 在一些 G -轨道的并集上的作用, 更详细地说, 就是任取 $Y \subset X$, G 在 X 上的作用给出一个 G 在

$$X_1 = \bigcup \{G.x \mid x \in Y\},$$

上的作用. 如果映射

$$f: G \times X \rightarrow X$$

给出了 G 在 X 上的作用, 那么由 X_1 的构造, 我们有 f 在 $G \times X_1$ 上的限制的像在 X_1 中, 且满足群作用的条件, 因此

$$f_1: G \times X_1 \rightarrow X_1$$

给出了 G 在 X_1 上的作用.

实际上如果我们考虑 G 在 G 上的共轭作用(伴随作用), 则之前习题中所说正规子群是一些共轭类的并就是以上叙述的一个特例. 注意到任给 G 的一个正规子群 N , G 在 G 上的共轭作用可以诱导出 G 在 N 上的一个作用.

有限群在有限集上的作用

我们自这部分将主要考虑有限群在有限集合上的作用. 设有限群 G 作用在有限集合 X 上.

我们记

$$X/G := \{G.x \mid x \in X\},$$

为所有 G 轨道的空间. 任取 $x \in X$, 我们考虑 G -轨道 $G.x$. 由 G 在 $G.x$ 上的作用和 G 在 $G/G.x$ 上的作用等价, 我们有以下关于轨道大小的公式.

推论 9.2.29 (教材推论 1.9.15)

沿用以上记号, 我们有

$$|G.x| = |G/G.x| = [G : G_x] = \frac{|G|}{|G_x|}.$$

我们考虑 X 关于 G -轨道的分解, 可以进一步用以上公式来描述集合 X 的大小.

推论 9.2.30

沿用之前的记号, 我们有

$$|X| = \sum_{G.x \in X/G} \frac{|G|}{|G_x|}.$$

注 9.2.31.

由于 G -作用的不动点个数通常会包含特殊信息, 我们也会将上式写为

$$|X| = |\text{Fix}_G| + \sum_{G.x \in X/G, |G_x| > 1} \frac{|G|}{|G_x|}.$$

我们这里给出以上结论的一个应用.

推论 9.2.32 (教材命题 1.10.3)

设群 G 作用在非空集合 X 上. 若存在素数 p , 使得 $|G| = p^l$, 其中 l 为非零自然数, 则

$$|X| \equiv |\text{Fix}_G| \pmod{p}.$$

定义 9.2.33

设群 G 作用在非空集合 X 上. 任取 $a \in G$, 若 $x \in X$, 满足 $a.x = x$, 我们称 x 为 a 的一个**不动点**. 我们记 a 的不动点集为

$$X^a := \{x \in X \mid a.x = x\}.$$

当 X 和 G 有限的时候, G -作用的轨道的个数以及 G 的每个元素的不动点集的大小之间有如下关系.

命题 9.2.34 (教材习题 1.9.20 Burnside 引理)

设有限群 G 作用在一个有限非空集合 X 上. 则

$$|X/G| = \frac{1}{|G|} \sum_{a \in G} |X^a|.$$

证明. 我们考虑 $G \times X$ 的子集:

$$D = \{(a, x) \in G \times X \mid a.x = x\}.$$

则有

$$\sum_{a \in G} |X^a| = |D|.$$

另一方面, 我们也有

$$\sum_{x \in X} |G_x| = |D|$$

任取 $x \in X$, 我们可以将 G 分解为一些子集的不交并:

$$G = \bigcup_{y \in G_x} \{a \in G \mid a.x = y\}.$$

这个实际上就是 G 关于 G_x 的左陪集分解, 轨道 $G.x$ 中每个元素对应一个 G_x 的左陪集.

注意到任取 $a \in G$, 我们有

$$|G_x| = |aG_x|,$$

因此

$$|G_x| = \frac{|G|}{|G.x|}$$

综合以上信息, 我们有

$$\sum_{a \in G} |X^a| = |D| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|G.x|} = |G| \sum_{G.x \in X/G} \sum_{y \in G.x} \frac{1}{|G.x|} = |G| \sum_{G.x \in X/G} 1.$$

因此, 我们有

$$|X/G| = \frac{1}{|G|} \sum_{a \in G} |X^a|.$$

□

9.3 群在自身上的共轭作用(伴随作用)

本节我们将讨论一个群在自身上的共轭作用(伴随作用).

伴随同态

我们首先回忆共轭作用的定义. 任取群 G , 任取 $a \in G$, 我们可以定义以下映射:

$$\begin{aligned} \text{Ad}_a : G &\rightarrow G, \\ b &\mapsto aba^{-1}. \end{aligned}$$

注意到不同于左平移和右平移仅仅是双射, a 诱导的伴随映射还是 G 的群同构. 利用以上定义, 我们得到如下 G 到 $\text{Aut}(G)$ 的同态映射:

$$\begin{aligned} \text{Ad} : G &\rightarrow \text{Aut}(G), \\ a &\mapsto \text{Ad}_a. \end{aligned}$$

根据我们之前对群 G 的自同构群 $\text{Aut}(G)$ 的讨论, 同态 Ad 的像为 G 的内自同构群:

$$\text{Ad}(G) = \text{Inn}(G).$$

任取 $a \in \ker \text{Ad}$, 我们有 $\text{Ad}_a = \text{id} \in \text{Aut}(G)$, 即任取 $b \in G$

$$aba^{-1} = \text{Ad}_a(b) = \text{id}(b) = b.$$

因此等价地, 我们任取 $b \in G$, 有

$$ab = ba,$$

即 a 与 b 交换. 由之前的我们给出的群的中心定义, 我们知道

$$a \in Z(G) := \{c \in G \mid \forall b \in G, cb = bc\}.$$

另一方面, 任取 $a \in Z(G)$, 我们考虑伴随作用的定义可以直接验证, 任取 $b \in G$,

$$\text{Ad}_a(b) = aba^{-1} = baa^{-1} = b.$$

因此 $a \in \ker \text{Ad}$. 以上讨论实际上给出了以下结论的证明.

命题 9.3.1

任给群 G , 我们有 $\ker \text{Ad} = Z(G)$.

共轭作用的轨道: 共轭类

我们回顾以下定义. 任取 $a, b \in G$, 若存在 $c \in G$, 使得 $a = cbc^{-1}$, 那么我们称 a 和 b 共轭. 我们首先从等价关系的角度来看共轭作用.

命题 9.3.2

设 G 为一个群. 以下关系给出 G 上元素的等价关系:

- 任取 $a, b \in G$, 我们定义 $a \sim b$ 当且仅当 a 和 b 共轭.

证明. 我们将依次检验自反性, 对称性和传递性.

(自反性) 任取 $a \in G$, 由幺元 e 与所有元素交换, 我们有 $ea a^{-1} = a$, 因此 $a \sim a$.

(对称性) 任取 $a, b \in G$, 设 $a \sim b$ 共轭, 由定义, 存在 $c \in G$, 满足

$$a = cbc^{-1}.$$

因此我们有关系

$$b = c^{-1}ac.$$

由定义, 我们有 b 和 a 共轭. 我们有 $b \sim a$.

(传递性) 任取 $a, b, c \in G$, 我们假设 $a \sim b$ 且 $b \sim c$, 由定义, 存在 $x, y \in G$, 满足

$$a = xbx^{-1}, \quad b = ycy^{-1}.$$

因此我们有

$$a = xbx^{-1} = x(ycy^{-1})x^{-1} = (xy)c(xy)^{-1}.$$

因此 $a \sim c$.

综上所述, 命题中的定义的关系给出 G 上的等价关系. □

定义 9.3.3

设 G 为一个群. 任取 $a \in G$, 我们称以下集合为 a 的**共轭类**:

$$[a] := \{b \in G \mid a \sim b\}.$$

我们考虑等价关系 $\sim$ 的定义, 可以将等价类 $[a]$ 重写为:

$$[a] := \{b \in G \mid a \sim b\} = \{b \in G \mid \exists c \in G, b = cac^{-1}\} = \{\text{Ad}_c(a) \mid c \in G\}.$$

命题 9.3.4

考虑群 G 在 G 上的共轭作用. 任取 $a \in G$, 则 a 的轨道为 a 的共轭类:

$$G.a = \text{Ad}(G)(a) = [a].$$

稳定化子和中心化子

任取 $a \in G$, 我们考虑 a 的稳定化子:

$$G_a := \{b \in G \mid \text{Ad}_b(a) = a\}.$$

由共轭作用的定义, 我们有

命题 9.3.5

考虑群 G 在 G 上的共轭作用. 任取 $a, b \in G$, 以下两个叙述等价:

- (i) a 和 b 交换: $ab = ba$;
- (ii) $b \in G_a$.

定义 9.3.6

设 G 为一个群. 任取 $a \in G$, 集合

$$Z_G(a) := \{b \in G \mid ab = ba\},$$

为 a 在 G 中的**中心化子**(centralizer).

命题 9.3.7

设 G 为一个群. 任取 $a \in G$, a 的中心化子为 G 的一个子群.

证明. 注意到 G 的幺元 e 与 G 所有的元素交换, 因此 $e \in Z_G(a)$, $Z_G(a)$ 非空.

任取 $b \in Z_G(a)$, 由定义 $ab = ba$, 等价地我们有

$$b^{-1}a = ab^{-1}.$$

因此 $b^{-1} \in Z_G(a)$.

任取 $b, c \in Z_G(a)$, 我们有

$$ab = ba, \quad ac = ca.$$

我们考虑以下计算:

$$a(bc) = (ab)c = (ba)c = b(ac) = b(ca) = (bc)a.$$

因此 $bc \in Z_G(a)$.

因此 $Z_G(a)$ 是 G 的一个子群. □

由以上讨论, 我们有

推论 9.3.8

考虑群 G 在 G 上的共轭作用. 任取 $a \in G$, 则 a 的稳定子群和 a 在 G 中的中心化子相同:

$$G_a = Z_G(a).$$

注 9.3.9.

以上讨论可以认为是从群作用的角度来解释一个元素的中心化子.

利用之前 x 的 G -轨道大小与稳定化子 G_x 的左陪集空间大小的关系, 以及上边我们对中心化子和稳定化子的关系的讨论, 我们有

命题 9.3.10

设 G 为一个有限群. 任取 $a \in G$, 我们有

$$|[a]| = [G : Z_G(a)].$$

我们可以进一步的定义 G 的子集的在 G 中的中心化子和关于 G 的共轭作用的稳定子群. 由于讨论与以上类似, 我们略去具体过程, 只给出结论.

定义 9.3.11

设 G 为一个群. 任取 G 的非空子集 S , 我们称以下集合:

$$Z_G(S) := \{b \in G \mid \forall a \in S, ab = ba\},$$

为集合 S 在 G 中的**中心化子**.

命题 9.3.12

设 G 为一个群. 任取 G 的非空子集 S , 则 S 的中心化子 $Z_G(S)$ 为 G 的一个子群.

命题 9.3.13

设 G 为一个群. 任取 G 的非空子集 S , 则 S 的中心化子与 S 关于共轭作用的**点态稳定化子**相同.

正规化子

当我们考虑一个 G 的一个非空子集 S , 我们也可以适当的将要求放宽, 考虑 $a \in G$, 满足

$$\text{Ad}_a(S) = S.$$

这里的等号是集合相等, 即 Ad_a 将 S 送到 S , 但是有可能将 S 中的元素重新排列. 注意到如果 $a \in Z_G(S)$, 则 a 满足以上要求, 但是由于我们不要求点态固定, 因此满足以上要求的 a 构成的 G 的子集可能会更大.

定义 9.3.14

设 G 为一个群. 任取 G 的一个非空子集 S , 我们称集合

$$N_G(S) := \{a \in G \mid \text{Ad}_a(S) = S\},$$

为 S 的**正规化子**.

例 9.3.15.

由定义我们看出, 如果我们考虑的 G 在 G 上的作用是由共轭给出的, 则有 $N_G(S) = G_S$.

例 9.3.16.

由以上定义, 如果 S 只有一个元素 a , 那么 $N_G(a) = Z_G(a)$. 但是当我们考虑的 S 有更多元素的时候, 这两个集合就不同了. 如果 S 是 G 的一个正规子群, 那么 $N_G(S) = G$.

例 9.3.17.

设 $G = D_4$, 取 $S = \{e, s\}$, 则

$$N_{D_4}(S) = \{e, s, r^2, r^2s\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

由正规子群的定义, 我们有以下结论.

命题 9.3.18

设 G 为群. 任取 G 的子群 H , 我们有 $H \triangleleft N_G(H)$.

我们记 G 中所有共轭类的集合为:

$$[G] = \{[a] \mid a \in G\}.$$

以下结果是命题 9.2.30 在当前情况下的表述. 我们通常称之为**类方程**(class equation).

定理 9.3.19 (类方程)

设 G 为一个有限群. 记 $Z(G)$ 为 G 的中心, 我们有

$$|G| = |Z(G)| + \sum_{[a] \in [G], |[a]| > 1} [G : N_G(a)].$$

注 9.3.20.

注意到求和的第二部分的每一项中 $N_G(a)$ 的选取是依赖于共轭类 $[a]$ 中代表元 a 的选取. 如果我们选择另一个代表元 $b \in [a]$, 因此有 $c \in G$,

$$b = cac^{-1}.$$

因此 $N_G(b) = cN_G(a)c^{-1}$, 我们继而有

$$[G : N_G(a)] = [G : N_G(b)]$$

因此这个数值是不依赖 $[a]$ 中代表元的选取.

推论 9.3.21

设 G 为一个阶为 p^l 的群, 其中 p 为素数, l 为非零自然数. 则 G 的中心非平凡, 即 $Z(G) \neq \{e\}$.

证明. 由类方程

$$|G| = |Z(G)| + \sum_{[a] \in [G], |[a]| > 1} [G : N_G(a)],$$

我们注意到 $p \mid |G|$, 且对任意 $[a]$, 我们有 $p \mid [G : N_G(a)]$. 因此

$$p \mid |Z(G)|.$$

由于 $e \in Z(G)$, 因此 $Z(G) = kp$, 其中 k 为非零自然数. □

推论 9.3.22

设 G 为一个阶为 p^2 的群, 其中 p 为素数. 则 G 为交换群.

证明. 由之前的推论知, $Z(G) \neq \{e\}$. 由于 $Z(G)$ 为 G 的子群. 因此 $|Z(G)| = p$ 或 p^2 .

若 $|Z(G)| = p^2$, 则 G 为交换群.

若 $|Z(G)| = p$, 由推论 6.3.19, 我们知道 $Z(G)$ 为 p -阶循环群. 设 $a \in Z(G)$ 为生成元. 注意到 $Z(G) \triangleleft G$, 我们有商群

$$G/Z(G).$$

由于

$$|G/Z(G)| = |G|/|Z(G)| = p.$$

由推论 6.3.19, 我们知道 $G/Z(G)$ 是 p -阶循环群. 设 $b \in G$ 满足 $bZ(G)$ 为 $G/Z(G)$ 的生成元.

考虑 G 的关于 $Z(G)$ 的左陪集分解, 我们有

$$G = \bigcup_{i=0}^{p-1} b^i Z(G).$$

因此 G 中所有元素都可以写为 $b^i a^j$ 的形式, 其中 $i, j \in \mathbb{Z}$.

任取 $b^i a^j$ 和 $b^s a^t$, 我们考虑

$$(b^i a^j)(b^s a^t) = b^i (a^j b^s) a^t = b^{i+s} a^{j+t} = b^s (b^i a^t) a^j = (b^s a^t)(b^i a^j).$$

因此 G 是交换群, 即 $G = Z(G)$, 这与 $|Z(G)| = p$ 矛盾.

因此 $Z(G) = p^2$, 即 G 为交换群. □

注 9.3.23.

教材例 3.5.3 告诉我们若 G 的阶为 p^2 , 其中 p 为素数, 则 $G \cong \mathbb{Z}_{p^2}$ 或者 $\mathbb{Z}_p \times \mathbb{Z}_p$.

第十章 群的结构

研究整数时,我们会使用素数分解这个工具;研究多项式的时候,我们会考虑多项式分解.我们也希望使用类似的想法来研究群的结构,并用这个方法对群进行分类.例如我们希望尝试回答

- (i) 在同构意义下,阶为 60 的群有哪几种?
- (ii) 在同构意义下,有限单群有哪些不同的种类?

等等.

10.1 Sylow 定理

本节中我们将主要关注有限群及其子群.特别地,我们希望通过对一个有限群的阶作为整数进行研究,从而了解该群是否具有某些阶的子群.

设 G 为一个有限群.由 Lagrange 定理我们知道,任取 G 的子群 H ,我们总有

$$|H| \mid |G|.$$

如果单纯从整数的分解的角度看,我们最终可以将一个整数分解为一系列素数的乘积.那么我们是否对任意 $m \mid |G|$,我们都有可以找到一个子群 H ,满足 $|H| = m$? 这个问题被称为 Lagrange 逆问题.以下例子告诉我们,并不是所有的群都满足这个性质.我们通常称满足这个性质的群为 CLT (Converse of Lagrange Theorem) 群.注意到循环群就是其中的一种.

例 10.1.1.

考虑之前作业中的习题.我们有 A_5 没有指数为 2, 3 和 4 的子群.因此也就没有 12, 8 和 6 阶子群.

本节我们将关注 m 为素数的幂方的情形.我们首先考虑简单的情形.

定理 10.1.2 (Cauchy 定理(交换群情形))

设 n 为一个大于 1 的自然数, G 为一个阶为 n 的交换群,则任取素数 $p \mid n$, 我们可以在 G 中找到一个 p -阶子群.

证明. 我们总是考虑被 p 整除的自然数 n .

设 $n = pm$, 其中 m 为一个非零自然数.我们对 m 的素数分解因子个数(计算重数)使用归纳法来证明.

若 m 的素因子个数为 0, 则 $m = 1$, 因此 $|G| = p$. 定理得证.

设定理对素因子个数小于等于 $k \in \mathbb{N}^*$ 的自然数 m 都成立, 我们考虑 m 的素因子个数为 $k + 1$. 由于 $n > 1$, 且幺元唯一, 因此存在非幺元元素 $a \in G$.

我们考虑 a 生成的 G 的子群 $\langle a \rangle$. 若 $p \mid o(a)$, 则存在 $l \in \mathbb{N}^*$, 满足

$$pl = o(a).$$

我们考虑 a^l 生成的 $\langle a \rangle$ 的子群, 也是 G 的子群. 注意到 $\langle a^l \rangle$ 是一个 p -阶子群.

下边假设 $\langle a \rangle$ 是 G 的一个非平凡的真子群, 且 $p \nmid o(a)$. 我们考虑商群 $G/\langle a \rangle$. 该群仍是交换群, 且阶为

$$|G/\langle a \rangle| = |G|/|\langle a \rangle| < |G|,$$

由于 $p \mid |G|$ 且 $p \nmid |\langle a \rangle|$, 因此

$$p \mid |G/\langle a \rangle|.$$

由归纳假设, 我们知道 $G/\langle a \rangle$ 有一个 p 阶子群. 由推论 6.3.19, 我们知道该子群是一个 p 阶循环群.

因此存在 $b \in G$, 满足在 $G/\langle a \rangle$ 中有,

$$o(b\langle a \rangle) = p.$$

因此 $b^p \in \langle a \rangle$, 即存在 $l \in \mathbb{N}^*$, 满足

$$b^p = a^l.$$

我们有

$$(b^{o(a)})^p = (b^p)^{o(a)} = (a^l)^{o(a)} = e.$$

因此元素 $b^{o(a)}$ 的阶整除 p 为 1 或者 p .

设 $b^{o(a)}$ 的阶为 1, 则 $b^{o(a)} = e$, 因此 b 的阶整除 $o(a)$. 由

$$p = o(b\langle a \rangle) \mid o(b), \quad o(b) \mid o(a),$$

得 $p \mid o(a)$, 与 $p \nmid o(a)$ 矛盾. 因此 G 中元素 $b^{o(a)}$ 生成的子群为 p 阶. □

以上结论也可以被推广到更一般的情形.

定理 10.1.3 (定理 1.10.1 Cauchy 定理(一般情形))

设 n 为一个大于 1 的自然数, G 为一个阶为 n 的有限群, 则任取素数 $p \mid n$, 我们可以在 G 中找到一个 p -阶子群.

注 10.1.4.

这里用到的是交换群这个条件的地方是, 交换群的任意子群都是正规子群, 因此 $G/\langle a \rangle$ 是一个群.

一般的群是不具有这个性质的, 因此我们需要使用其他办法来证明. 我们使用的主要工具是注 9.2.31.

证明. 我们考虑以下集合

$$X = \{(a_1, \dots, a_p) \in \underbrace{G \times \cdots \times G}_{p \text{ 次}} \mid a_1 \cdots a_p = e \in G\} \subset \underbrace{G \times \cdots \times G}_{p \text{ 次}}.$$

我们注意到对称群 S_p 中的 p 轮换 $\sigma = (12 \cdots p)$ 生成的子群

$$H = \langle \sigma \rangle,$$

可以作用在 X 上:

$$\begin{aligned} f: H \times X &\rightarrow X, \\ (\sigma^k, (a_1, \dots, a_p)) &\mapsto (a_{\sigma^k(1)}, \dots, a_{\sigma^k(p)}). \end{aligned}$$

由注 9.2.31, 我们有

$$|X| = |\text{Fix}_H| + \sum_{H \cdot x \in X/H, |H \cdot x| > 1} \frac{|H|}{|H_x|}.$$

注意到 $|H| = p$, 由于 $H_x < H$, 且 $H_x \neq H$, 因此 $H_x = \{e\}$. 我们有

$$|X| = |\text{Fix}_H| + \sum_{H \cdot x \in X/H, |H \cdot x| > 1} p.$$

另一方面, 注意到任取 X 中的元素 $(a_1, \dots, a_p)$, 若我们取定 $a_1, \dots, a_{p-1}$, 则

$$a_p = (a_1 \cdots a_{p-1})^{-1},$$

也就确定了.

因此 $|X| = |G|^{p-1}$. 特别地, 我们有

$$p \mid |X|.$$

因此

$$p \mid |\text{Fix}_H|.$$

注意到 $(e, \dots, e) \in \text{Fix}_H$, 因此 $|\text{Fix}_H| = kp$, 其中 $k \in \mathbb{N}^*$.

最后我们研究 Fix_H 中的元素. 若 $(a_1, \dots, a_p) \in \text{Fix}_H$, 则对任意 $k \in \mathbb{N}$, 我们有

$$(a_1, \dots, a_p) = (a_{\sigma^k(1)}, \dots, a_{\sigma^k(p)}).$$

因此存在 $a \in G$, 满足 $a_1 = \cdots = a_p = a$. 由于 $|\text{Fix}_H| > 1$, 由以上讨论, 存在非单位 p -阶元素 a . 因此 $\langle a \rangle$ 为 G 的一个 p -阶子群. $\square$

定理 10.1.5 (教材定理 1.10.5 Sylow 第一定理)

记 G 为一个有限群. 设 G 的阶为 $n = p^l m$, 其中 p 为素数, $l, m \in \mathbb{N}$, 满足 $\gcd(p, m) = 1$. 则任取自然数 $0 \leq k \leq l$, G 中有阶为 p^k 的子群.

注 10.1.6.

Sylow 定理有多种不同的证明. 但这些证明都用到了群作用, 只是考虑的作用是不同的. 例如, 教材中考虑的是群 G 在某个群 H 的左陪集空间 G/H 上的左乘作用; Dummit & Foote 以及 Jacobson 的证明考虑的是群 G 在 G 上的共轭作用; Artin 的证明考虑的是群 G 在 G 所有大小为 p^l 的子集的集合上的左乘作用.

教材中的证明思路是, 既然可以由 Cauchy 定理得到一个 p 阶子群, 我们可不可以由这个 p 阶子群出发构造一个包含这个 p 阶子群的 p^2 阶的子群呢? 如果可以的话, 我们能不能继续从这个 p^2 阶的子群构造一个包含它的 p^3 阶子群? 等等.

这里就涉及到如果构造一个更大的群的问题. 可以使用方法比如添加元素然后生成, 或者使用群同态基本定理 (当然还会有其他的方法). 教材中使用的是后者. 但要使用同态基本定理就需要考虑正规子群. 而一般的 p 阶群 H 不一定是 G 的正规子群. 因此我们就考虑 H 的正规化子 $N_G(H)$. 这是包含 H 为正规子群的最大的 G 的子群.

另一方面, 商群 $N_G(H)/H$ 作为陪集空间 G/H 的子集, 是 H 在 G/H 上通过左平移作用的不动点的集合. 利用轨道分解, 以及轨道元素个数与其中一个元素的稳定子群 (迷向子

群)的指数的关系, 我们可以证明 $|N_G(H)/H|$ 被 p 整除. 然后由同态基本定理, 我们就得到了所求的 p^2 阶子群.

这个证明还有另外一个推论. 注意到这个构造对任意 p^k 阶子群 ($0 \leq k < l$) 都可以使用, 因此作为推论, 我们也证明了任意 p^k 阶子群都在一个 p^l 阶子群中, 也就是 Sylow 第二定理的一部分结论.

证明. 我们将使用归纳法对 G 的阶进行归纳来证明: 设 G 的阶为 $n = p^l m$, 其中 $l \in \mathbb{N}$, p, m 非零自然数, 且 p 为素数, $\gcd(p, m) = 1$. 则任取自然数 $k \leq l$, G 中有阶为 p^k 的子群.

若 $|G| = 1$, 则 $k = l = 0$, 我们考虑 $\{e\}$ 即满足条件.

下设结论对 $1 \leq |G| = i < n$ 都成立, 我们考虑 $|G| = n$ 的情形. 若 $l = 0$, 则 $0 \leq k \leq l$. 因此 $k = 0$. 我们总有 1 阶子群 $\{e\}$. 我们下设 $l \geq k > 0$. 我们按照 $|Z(G)|$ 是否可以被 p 整出来分类.

- (i) 若 $p \mid |Z(G)|$, 则 $Z(G)$ 有一个 p 阶子群 P . 由于 $P < Z(G)$, 我们有 $P \triangleleft G$. 考虑 G/P , 这是一个阶比 G 小的群. 由归纳假设结论对 G/P 成立. 记 $\bar{H}$ 为 G/P 的一个 p^{k-1} 阶子群. 若 π 为自然同态

$$\pi : G \rightarrow G/P,$$

我们考虑 $H < G$, 满足

$$H = \pi^{-1}(\bar{H}).$$

因此 $P < H$, 且 $H/P = \bar{H}$. 因此我们有

$$|H| = |H/P||P| = p^k.$$

结论成立.

- (ii) 若 $p \nmid |Z(G)|$, 我们考虑类方程

$$|G| = |Z(G)| + \sum_{[a] \in [G], |[a]| > 1} [G : N_G(a)].$$

由于 $p \mid G$ 且 $p \nmid |Z(G)|$, 因此存在 $[a] \in [G]$, 满足 $|[a]| > 1$, 且

$$p \nmid [G : N_G(a)] = \frac{|G|}{|N_G(a)|}.$$

因此 $p^l \mid |N_G(a)|$. 由归纳假设, 结论对 $N_G(a)$ 成立. 因此对任意 $0 < k \leq l$, 群 $N_G(a)$ 包含一个 p^k 阶子群.

□

定义 10.1.7 (教材定义 1.10.6)

记 G 为一个群. 设 G 的阶为 $n = p^l m$, 其中 p, l, m 非零自然数, 且 p 为素数, $\gcd(p, m) = 1$.

- (i) 若 $\{e\} \neq H < G$, 满足 $|H| = p^k$, 其中自然数 k 满足 $k \leq l$, 我们称 H 为 G 的一个 **p -子群**.
- (ii) 若 $\{e\} \neq H < G$, 满足 $|H| = p^l$, 我们称 H 为 G 的一个 **Sylow p -子群**.

注 10.1.8.

Sylow 第一定理保证了以上定义子群总是存在的.

在证明 Sylow 第二和第三定理的时候, 我们需要以下两个引理:

引理 10.1.9

记 G 为一个群. 设 G 的阶为 $n = p^l m$, 其中 p, l, m 非零自然数, 且 p 为素数, $\gcd(p, m) = 1$. 设 P 为 G 的一个 Sylow p -子群.

任取 $a \in G$, 若 $o(a) \mid p^l$, 且 $aPa^{-1} = P$, 则 $a \in P$.

证明. 设 $a \in G$, 满足 $o(a) \mid p^l$. 我们记 $H = \langle a \rangle$. 若 $aPa^{-1} = P$, 我们考虑 a 和 P 生成的 G 的子群 K . 注意到

$$K = \{a^j b \mid j \in \mathbb{Z}, b \in P\} = HP.$$

由群同态基本定理, 我们知道

$$|K| = \frac{|H||P|}{|H \cap P|} = p^l \frac{|H|}{|H \cap P|}.$$

由于 $|H| \mid p^l$, 因此若

$$H \neq H \cap P,$$

我们有

$$p^{l+1} \mid |K|,$$

这与 G 的阶满足的条件矛盾.

因此 $H = H \cap P$, 也即 $H \subset P$ ($a \in P$). □

引理 10.1.10

记 G 为一个群. 设 G 的阶为 $n = p^l m$, 其中 p, l, m 非零自然数, 且 p 为素数, $\gcd(p, m) = 1$. 设 P 为 G 的一个 Sylow p -子群, H 为 G 的一个 p -子群, 则有

$$H \cap P = H \cap N_G(P) (= N_H(P)).$$

证明. 注意到 $P < N_G(P)$, 因此我们总有

$$H \cap P \subset H \cap N_G(P).$$

以下我们主要证明另一个方向的包含关系.

任取 $a \in H$, 由于 H 为 p -子群, 因此 $o(a) \mid |H| \mid p^l$. 因此若 $a \in N_G(P)$, 由前一个引理, 我们知道 $a \in P$, 因此我们有

$$H \cap N_G(P) \subset H \cap P.$$

综上所述, 我们有

$$H \cap N_G(P) = H \cap P.$$

□

定理 10.1.11 (教材定理 1.10.8 Sylow 第二定理)

记 G 为一个群. 设 G 的阶为 $n = p^l m$, 其中 p, l, m 非零自然数, 且 p 为素数, $\gcd(p, m) = 1$. 我们有以下结论:

- (i) 任意 G 的 p -子群都是 G 的某个 Sylow p -子群的子群.
- (ii) G 的任意两个 Sylow p -子群互相共轭, 即若 H_1 和 H_2 都是 G 的 Sylow p -子群, 则存在 $a \in G$, 满足

$$H_2 = aH_1a^{-1}.$$

证明. 由 Sylow 第一定理, 我们知道 G 中有 Sylow p -子群. 设 $P < G$ 为一个 Sylow p -子群. 我们记

$$[P] = \{P_1, \dots, P_s\}$$

为 P 在共轭作用下的轨道, 即 $[P]$ 为 G 中所有与 P 共轭的子群构成的集合.

任取 $H < G$, 满足 $|H| = p^k$, 其中自然数 k 满足 $0 \leq k \leq l$.

我们考虑 H 在 $[P]$ 上的共轭作用, 并记 $[P]$ 的轨道分解为

$$[P] = O_1 \cup \dots \cup O_t.$$

在对 $[P]$ 的元素做一个重排之后, 我们设对任意 $1 \leq i \leq t$, 有 $P_i \in O_i$. 由之前在讨论共轭作用是, 对轨道大小和正规化子之间的关系讨论, 以及两个技术性引理, 我们知道

$$|O_i| = [H : N_H(P_i)] = [H : (H \cap N_G(P_i))] = [H : H \cap P_i].$$

因此我们有以下两个结论:

- (i) 若 $|O_i| = 1$ (即 P_i 为 H 作用的不动点), 则

$$H = H \cap P_i.$$

因此我们有 $H < P_i$.

- (ii) 若 $|O_i| > 1$, 由于 $|O_i| \mid |H| \mid p^l$, 因此 $p \mid |O_i|$.

我们假设 H 不被包含在任意的 P_i 中, 则对任意 $i = 1, \dots, t$, 都有

$$p \mid |O_i|.$$

因此

$$p \mid |O_1| + |O_2| + \dots + |O_t| = |[P]|.$$

另一方面, 我们考虑

$$|[P]| = [G : N_G(P)],$$

由于 $P < N_G(P)$, 因此

$$p \nmid |[P]|,$$

矛盾.

因此存在 P_i , 满足 $|O_i| = [H : N_H(P_i)] = 1$, 即有 $H < P_i$.

我们现在考虑 (ii). 取 H 为 G 的任意一个 Sylow p -子群. 设 P 为任意 G 的 Sylow p -子群. 考虑所有与 P 共轭的子群构成的集合.

重复以上讨论, 我们知道存在一个与 P 共轭的 Sylow p -子群 P' 包含 H . 由于

$$|P'| = |H|,$$

我们有 $P' = H$, 结论得证. □

注 10.1.12.

教材中的证明使用了 H 在 G/P 上的左平移作用. 我们知道 $|P| = p^l$ 以及 $|G| = p^l m$, 因此 $|G/P| = m$, 且 $p \nmid |G/P|$.

注意到 H 通过左平移作用在 G/P , 由于 $H = p^k$, 利用轨道分解, 我们有

$$|\text{Fix}_H| \equiv |G/P| \pmod{p}.$$

由于 $p \nmid |G/P|$, 因此 $\text{Fix}_H \neq \emptyset$, 存在 $aP \in \text{Fix}_H$, 满足任取 $b \in H$, 有

$$b.aP = aP.$$

因此

$$b(aPa^{-1}) = aPa^{-1}.$$

注意到以上是两个 aPa^{-1} 的陪集相同, 因此 $b \in aPa^{-1}$. 由于以上讨论对任意 $b \in H$ 都成立, 因此 $H < aPa^{-1}$.

如果 $|H| = p^l$, 即 H 为一个 Sylow p -子群, 则有 $H = aPa^{-1}$. 换句话说 $P = a^{-1}Ha$. 以上讨论最开始, 我们是任取的 Sylow p -子群 P , 因此以上讨论告诉我们, 所有 Sylow p -子群都共轭于 H , 因此所有 Sylow p -子群两两共轭.

定理 10.1.13 (Sylow 第三定理)

记 G 为一个群. 设 G 的阶为 $n = p^l m$, 其中 p, l, m 非零自然数, 且 p 为素数, $\gcd(p, m) = 1$. 则群 G 中 Sylow p -子群的个数 n_p 满足以下条件

$$n_p \equiv 1 \pmod{p}.$$

证明. 设 P 为 G 的一个 Sylow p -子群. 我们记

$$[P] := \{P_1 = P, P_2, \dots, P_s\},$$

为所有 Sylow p -子群的集合.

我们下边的证明与 Sylow 第二定理的证明类似. 我们取 $H = P$. 考虑 P 在 $[P]$ 上的共轭作用. 我们记 $[P]$ 的轨道分解如下:

$$[P] = O_1 \cup \dots \cup O_t.$$

不妨设对任意 $1 \leq i \leq t \leq s$, O_i 为 P_i 的轨道. 因此 O_1 为 P 的轨道, 我们有 $|O_1| = 1$.

任取 $i > 1$, 我们有

$$N_P(P_i) = P \cap P_i.$$

由于 $P \neq P_i$, 我们有

$$|O_i| = [P : P \cap P_i] > 1.$$

因此

$$p \mid |O_i|.$$

综上所述, 我们有

$$(n_p = |[P]|) \equiv |O_1| (= 1) \pmod{p}.$$

□

以下是 Sylow 第三定理结合正规子群的定义的一个直接推论:

推论 10.1.14

记 G 为一个群. 设 G 的阶为 $n = p^l m$, 其中 p, l, m 非零自然数, 且 p 为素数, $\gcd(p, m) = 1$. 设 P 为 G 的一个 Sylow p -子群, 沿用以上定理中的记号, 我们有以下两个叙述等价:

- (i) $P \triangleleft G$;
- (ii) $n_p = 1$.

注 10.1.15.

综上所述, 群 G 的阶如果可以写为 $p^l m$ 满足条件如前, 则 G 的 Sylow p -子群的个数 n_p 满足以下两个条件:

- $n_p \mid m$,
- $n_p \equiv 1 \pmod{p}$.

这两个条件可以用来判断一个群中是否有正规 Sylow 子群. 例如, 考虑 $|G| = 12$, 我们有 $12 = 2^3 \times 3$, 因此 G 中有 Sylow 3 子群和 Sylow 2-子群. 我们记 n_3 和 n_2 分别为二者个数, 则有以下关系:

$$\begin{cases} n_3 \equiv 1 \pmod{3} \\ n_3 \mid 4 \end{cases}, \quad \begin{cases} n_2 \equiv 1 \pmod{2} \\ n_2 \mid 3 \end{cases}$$

由这两个条件知

$$n_3 = 1 \text{ 或者 } 4, \quad n_2 = 1 \text{ 或者 } 3.$$

若 $n_3 = 1$, 则 Sylow 3-子群为一个正规子群. 否则 $n_3 = 4$, 由于每一个 3 阶群都是循环群, 这些 Sylow 3-子群中的非幺元共有 8 个, 均为 3 阶元素. 注意到 Sylow 2-子群是一个 4 阶群, 且元素的阶都是 2 的幂次. 因此除了幺元和 3 阶元素外, 其他元素都在一个 Sylow 2 子群内. 所以 $n_2 = 1$, 该 Sylow 2-子群是一个正规子群.

10.2 Sylow 定理的应用

对一类结构的分类通常是我们对此类结构认知的一部分, 有助于我们进一步深入的研究此类结构 (比如, 某个维数拓扑流形的分类, 某个拓扑流形上的度量结构的分类,); 另一方面, 群这个基本的概念出现在许多领域的研究中, 例如我们之前讨论的很多群都是有一定几何, 代数或者数论的背景, 对相应问题的研究也会涉及对相应的群结构的研究. Sylow 定理是对有限群的结构研究的一个重要的工具.

例 10.2.1 (阶为素数 p 的幂方的群).

我们首先考虑一个平凡的例子. 设群 G 的阶为素数 p 的幂方 p^l , 其中 $l \in \mathbb{N}^*$. 此时 G 只有 Sylow p -子群, 就是 G 子自己. 阶为 p^l 只有 G , 我们有 $n_p = 1$, 因此群 G 总是 G 中的一个正规子群. 当然, 另一方面我们知道任意 G 都是 G 的一个(平凡的)正规子群.

当 $l = 1$ 时, 我们知道 G 是一个循环群, 同构于 $\mathbb{Z}_p$.

当 $l = 2$ 时, 我们之前证明了 G 是交换的. 我们实际上可以进一步证明 G 总是同构于以下两个群之一: $\mathbb{Z}_{p^2}$ 和 $\mathbb{Z}_p \times \mathbb{Z}_p$.

当 $l > 2$ 时, 情况就更复杂了. 特别地, 此时我们并不一定有 G 是交换的. 例如 $p = 2$, $l = 3$, 我们有二面体群 D_4 , 并非是交换群.

例 10.2.2 (阶为两个素数乘积 pq 的群).

记 p 和 q 为两个不同的素数. 我们不妨设 $p > q$.

设 G 为一个阶为 pq 的群. 我们知道 G 中有 Sylow p -子群和 Sylow q -子群, 并且均是循环群.

我们设 P 为 G 的一个 Sylow p -子群. 我们设 a 为 P 的生成元. 我们考虑 P 在 G 共轭作用下的轨道

$$O_P = \{P_1 = P, P_2, \dots, P_k\}.$$

利用轨道和正规化子的关系, 我们有

$$n_p = |O_P| = [G : N_G(P)] \mid [G : P] = q.$$

由于 q 为素数, 因此 $|O_P|$ 为 1 或者 q .

由 Sylow 第三定理, 我们知道

$$n_p \equiv 1 \pmod{p},$$

因此存在整数 $k \in \mathbb{Z}$, 满足

$$n_p = 1 + kp.$$

若 $n_p = q$, 则 k 无解. 这是因为若 $k < 0$, 则 $n_p < 0$, 若 $k = 0$, 则 $n_p = 1$, 若 $k > 0$, 则 $q = 1 + p > p$ 与 $p > q$ 矛盾.

因此 $n_p = 1$, 由 Sylow 第三定理, 我们有 P 为 G 的正规子群.

下边我们将进一步讨论 G 的构造, 来得到 G 的同构类型.

我们考虑 G/P , 则

$$|G/P| = \frac{|G|}{|P|} = q.$$

因此 G/P 是一个阶为 q 的循环群. 记 $b \in G$, 满足

$$G/P = \{P, bP, \dots, b^{q-1}P\}.$$

我们记

$$H = \langle b \rangle.$$

由于 $P \triangleleft G$, 我们有

$$G = HP = \{b^i a^j \mid i, j \in \mathbb{Z}\}.$$

我们有

$$b^q = a^j.$$

下边我们分两种情况来讨论:

(i) 若 $j \neq 0$, 则有

$$o(b^q) = p.$$

因此 b 的阶为 pq . 另一方面 $|G| = pq$. 因此我们有

$$G = \langle b \rangle \cong \mathbb{Z}_{pq}.$$

(ii) 若 $j = 0$, 我们有 $o(b) = q$. 注意到

$$\langle b \rangle \cong \mathbb{Z}_q.$$

我们目前有两个群各自同构于 $\mathbb{Z}_p$ 和 $\mathbb{Z}_q$. 我们也知道

$$G = HP.$$

由于我们将 G 的元素都表达为 $b^i a^j$. 目前我们还缺少的信息是, 任取 $b^i a^j$ 以及 $b^s a^t$, 它们的乘积对应哪个元素

$$b^i a^j b^s a^t = b^? a^?.$$

这个问题可以进一步简化为

$$bab^{-1} = a^?.$$

因此我们考虑同构映射

$$\text{Ad}_b : P \rightarrow P$$

由于 $P \cong \mathbb{Z}_p$, 因此

$$\text{Aut}(\mathbb{Z}_p) = \mathbb{Z}_p^*.$$

其中 $\mathbb{Z}_p^*$ 为 $\mathbb{Z}_p$ 中所有非零元关于乘法构成的群.

注意到若 $\text{Ad}_b = id$, 则 a 和 b , 则元素 ab 的阶为 pq , 从而有 $G \cong \mathbb{Z}_{pq}$. 若 $\text{Ad}_b \neq id$, 则

$$\text{Ad}(H) < \text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^*.$$

因此

$$|\text{Ad}(H)| = q \mid p-1 = |\mathbb{Z}_p^*|.$$

另一方面, 我们会问是不是, 若 $q \mid p-1$, 就一定会存在非平凡的 Ad_b . 这个问题的答案是肯定的. 我们后边会证明 $\mathbb{Z}_p^*$ 为一个循环群. 因此任取 $p-1$ 的因子 m , $\mathbb{Z}_p^*$ 都有阶为 m 的循环子群. 因此存在 H 到这个子群的同构.

由于此时 $\text{Ad}_b \neq id$, 因此

$$bab^{-1} \neq a,$$

群 G 不是交换群.

另一方面, 由于素数阶循环群的性质, $\mathbb{Z}_q$ 每个非零元素都是 $\mathbb{Z}_q$ 的生成元. 因此以上构造的 Ad 在共轭意义下是唯一的, 进一步我们有以上构造的非交换的 pq 阶群在同构意义下是唯一的.

注 10.2.3.

我们后边会看到以上过程实际上是将 G 写为 H 和 P 的半直积:

$$G = P \rtimes_{\text{Ad}} H.$$

注 10.2.4.

关于更一般的情形, 我们有 Schur-Zassenhaus 定理. 见附录 ??.

例 10.2.5 (4-阶对称群 S_4).

我们首先考虑群 S_4 的阶的素数分解

$$|S_4| = 4! = 24 = 2^3 \cdot 3.$$

由 Sylow 第一定理, S_4 中有 3 阶的 Sylow 3-子群和 8 阶的 Sylow 2-子群.

我们首先考虑 Sylow 2-子群. 任取 S_4 的一个 Sylow 2-子群 P , 由 Sylow 第二定理, 我们知道 S_4 所有的 Sylow 2-子群都与 P 共轭. 我们考虑 P 在 S_4 的共轭作用下的轨道 O , 由之前轨道和正规化子之间的关系, 我们有

$$|O| = [S_4 : N_{S_4}(P)] \mid [S_4 : P] = 3.$$

因此 $|O| = 1$ 或者 3, 即 S_4 有 1 个或者 3 个 Sylow 2-子群.

注意到二面体群 D_4 作为正方形的对称群可以看作是正方形的四个顶点的置换构成的群. 我们记正方形的四个顶点为 a, b, c 和 d . 通过将 $\{a, b, c, d\}$ 与 $\{1, 2, 3, 4\}$ 对应起来, 我们可以得到有 S_4 中与 D_4 同构的子群. 注意到 D_4 阶为 8, 因此我们得到的 S_4 的子群就是 S_4 的 Sylow 2-子群. 注意到 $\{a, b, c, d\}$ 和 $\{1, 2, 3, 4\}$ 之间不同的对应可以给出同样的 S_4 的子群 (例如, $(a, b, c, d) = (1, 2, 3, 4)$ 和 $(a, b, c, d) = (2, 3, 4, 1)$ 给出的是同一个 S_4 的子群). 以下对应给出 D_4 在 S_4 中三种不同嵌入

$$\begin{aligned}(a, b, c, d) &= (1, 2, 3, 4), \\(a, b, c, d) &= (2, 1, 3, 4), \\(a, b, c, d) &= (4, 2, 3, 1).\end{aligned}$$

所得的 S_4 的 Sylow 2-子群为

$$\begin{aligned}&\{e, (1234), (13)(24), (1432), (12)(34), (14)(23), (13)(24)\}, \\&\{e, (2134), (23)(14), (2431), (12)(34), (24)(13), (23)(14)\}, \\&\{e, (4231), (43)(21), (4132), (24)(13), (14)(23), (43)(21)\}.\end{aligned}$$

类似地, S_4 中的 Sylow 3-子群的个数 n_3 整除 $[S_4 : Q] = 8$, 这里 Q 是一个 Sylow 3-子群. 注意到 Q 是一个循环群. 我们记 Q 的生成元为 σ , 考虑将其分解为不交的轮换的乘积, 则 σ 是一个长度为 3 的轮换. 注意到在 S_4 中, 长度为 3 的轮换有 8 个:

$$(123), (132), (124), (142), (134), (143), (234), (243),$$

分别属于 4 个 S_4 的子群:

$$\langle (123) \rangle, \langle (124) \rangle, \langle (134) \rangle, \langle (234) \rangle.$$

我们可以通过几何的方法来描述 S_4 的 Sylow 子群. 通过将正四面体的顶点与 $\{1, 2, 3, 4\}$ 对应, 我们可以将 S_4 等同于正四面体的所有的对称, 一个 Sylow 2 子群所包含的是保持一对对边的正四面体的所有的对称. 记四个顶点为 a, b, c, d , 我们考虑对边 ab 和 cd . 这样的对称有三种:

- (i) 绕着 ab 和 cd 的公共垂线 L_1 将正四面体旋转 180° , 将每个边的顶点对换.
- (ii) 绕着 ac 和 bc 的公共垂线 L_2 将正四面体旋转 180° , 将两个边对换.
- (iii) 考虑关于过 ab 和 L_1 的平面的对称, 这样我们交换 c 和 d , 同时保持 a 和 b .

我们共有三组对边分别对应三个 Sylow 2-子群. 注意到当我们通过正四面体的对称 σ 将一组对边送到另一组对边的位置, 我们就可以将两组对边对应的 Sylow 2-子群不妨记作 P_1 和 P_2 对应起来, 二者满足

$$P_1 = \sigma P_2 \sigma^{-1}.$$

另一方面, 我们任取一个顶点, 例如 a , 我们考虑其他三个顶点的旋转, 则得到了 Sylow 3-子群. 由于我们有 4 个顶点, 因此有 4 个 Sylow 3-子群. 类似于之前的讨论, 我们知道所有 Sylow 3-子群相互共轭.

例 10.2.6 (有限交换群).

我们设 G 是一个阶为正整数 m 的交换群. 设 $m > 1$, 且有素数分解:

$$m = p_1^{n_1} \cdots p_k^{n_k}.$$

其中 $p_1, \dots, p_k$ 为两两不同的素数.

由 Sylow 定理, 我们知道对任意 p_i , G 有阶为 $p_i^{n_i}$ 的子群记做 G_i .

注意到 G_i 中元素的阶都整除 $p_i^{n_i}$, 因此任取 $i \neq j$, 我们有

$$G_i \cap G_j = \{e\}.$$

我们有群的内直积

$$G_i G_j = G_i \times G_j.$$

利用归纳法, 我们有

$$\prod_{i=1}^k G_i < G.$$

另一方面

$$\left| \prod_{i=1}^k G_i \right| = p_1^{n_1} \cdots p_k^{n_k} = |G|.$$

因此

$$G = \prod_{i=1}^k G_i.$$

因此, 为了确定 G 的结构, 我们只需要知道 G_i 的结构即可. 实际上一个阶为 p^l 的交换群总是同构于

$$\mathbb{Z}_{p^{l_1}} \times \cdots \times \mathbb{Z}_{p^{l_s}},$$

满足 $l_1 \leq \cdots \leq l_s$, 且 $l_1 + \cdots + l_s = l$. 利用这个结论, 我们就可以将 G 写为一系列 $\mathbb{Z}_{p_i^{l_j}}$ 的直积.

我们在学习完模之后, 给出有限交换群的完全分类(有限交换群结构定理)及其证明.

10.3 群的直积

记 H 和 K 为两个群. 我们从集合角度来考虑以下的笛卡尔积

$$H \times K := \{(a, x) \mid a \in H, x \in K\}.$$

我们可以使用 H 和 K 上的二元运算在这个集合上定义一个二元运算:

$$\begin{aligned} \cdot : (H \times K) \times (H \times K) &\rightarrow H \times K, \\ ((a, x), (b, y)) &\mapsto (ab, xy). \end{aligned}$$

通过直接计算, 我们有以下结论:

- (i) 以上定义的 $H \times K$ 上的二元运算满足结合律;
- (ii) 元素 $(e_H, e_K) \in H \times K$ 为幺元;
- (iii) 任取元素 $(a, x) \in H \times K$, 有逆元 (a^{-1}, x^{-1}) .

因此 $H \times K$ 是一个群.

定义 10.3.1 (教材习题 1.3.3)

任取群 H 和 K , 我们称群 $H \times K$ 为 H 和 K 的(外)直积. 记作 $H \otimes_e K$ (区别于集合的笛卡尔积).

注 10.3.2.

我们可能也听到过直和这个名词. 在考虑有限多个群的时候, 这两个概念是相同的. 只有当我们考虑无穷多个群的笛卡尔积的时候, 这两个概念才有区别, 详细解释请参考附录 B.

注 10.3.3.

记号 $\otimes_e$ 的下标是为了说明这是外直积 (external direct product), 与后边的内直积 (internal direct product) (将记作 $\otimes_i$) 区分.

考虑群 H 和 K , 我们记 $G = H \otimes_e H$. 通过考虑第一个分量以及第二个分量, 我们可以构造群 H 和 K 到 G 的单射:

$$\begin{aligned} j_H : H &\rightarrow G & j_K : K &\rightarrow G \\ a &\mapsto (a, e_K) & x &\mapsto (e_H, x) \end{aligned}$$

通过直接计算, 我们可以验证 j_H 和 j_K 都是群单同态. 我们记

$$N_H = \text{Im}(j_H), \quad N_K = \text{Im}(j_K).$$

我们可以通过之验证得到以下结论.

命题 10.3.4 (教材引理 1.7.7)

我们沿用以上记号 G, H, K, N_H 和 N_K , 有以下结论:

- (i) $H \cong N_H$ 且 $K \cong N_K$.
- (ii) 任取 $a \in H$ 和 $x \in K$, 我们有

$$(a, e_K)(e_H, x) = (e_H, x)(a, e_K).$$

- (iii) $N_H \triangleleft G$ 且 $N_K \triangleleft G$.
- (iv) $N_H \cap N_K = \{(e_H, e_K)\}$.
- (v) $G = N_H N_K$.

从以上讨论, 我们看出外直积的结构诱导出 G 上的一个分解. 反过来, 我们也可以从群 G 的子群出发, 来研究 G 是否存在类似的分解.

定义 10.3.5

设 G 为一个群, N_1 和 N_2 为 G 的两个子群. 假设 N_1 和 N_2 满足以下条件:

- (i) $N_1 \triangleleft G$ 且 $N_2 \triangleleft G$;
- (ii) $N_1 \cap N_2 = \{e\}$;
- (iii) $G = N_1 N_2$.

我们称 G 为 N_1 和 N_2 的(内)直积. 我们记作 $G = N_1 \otimes_i N_2$.

我们首先证明如果 G 是 N_1 和 N_2 的内直和, 那么 N_1 的元素和 N_2 的元素互相交换.

命题 10.3.6 (教材引理 1.7.7)

设 G 为一个群. 设 N_1 和 N_2 为 G 的两个正规子群, 满足 $G = N_1 \otimes_i N_2$, 则任取 $a \in N_1, x \in N_2$, 我们有

$$ax = xa.$$

证明. 我们首先考虑 N_2 为正规子群, 且 $ax \in aN_2$, 因此存在元素 $y \in N_2$, 满足

$$ax = ya = x(x^{-1}y)a.$$

其中 $x^{-1}y \in N_2$.

另一方面 N_1 为正规子群, 且 $ax \in N_1x$, 因此存在 $b \in N_1$, 满足

$$ax = xb = x(ba^{-1})a.$$

其中 $ba^{-1} \in N_1$.

由以上两个等式以及消去律, 我们有

$$x^{-1}y = ba^{-1} \in N_1 \cap N_2.$$

因此 $x^{-1}y = ba^{-1} = e$, 从而有

$$ax = xa.$$

□

注意到 N_1 和 N_2 都是群, 也可以定义外直和. 以上命题告诉我们这两个群的内直积和外直积同构.

命题 10.3.7

设 G 为一个群. 设 N_1 和 N_2 为 G 的两个正规子群, 满足 $G = N_1 \otimes_i N_2$, 则映射

$$\begin{aligned} \phi : N_1 \otimes_e N_2 &\rightarrow N_1 \otimes_i N_2, \\ (a, x) &\mapsto ax \end{aligned}$$

是一个群同构.

证明. 注意到以上映射是乘法运算在 $N_1 \times N_2$ 上的限制. 任取 $a, b \in N_1$ 和 $x, y \in N_2$, 我们有

$$\phi((a, x)(b, y)) = \phi((ab, xy)) = (ab)(xy) = a(bx)d = (ax)(by) = \phi((a, b))\phi((c, d)).$$

第三个等号是因为上一个命题中, 我们证明了 N_1 中的元素和 N_2 中的元素交换.

由此, 我们知道以上映射是一个群同态. 我们需要证明这是一个双射, 即可证命题.

首先证明这是一个单射. 任取 $a, b \in N_1$ 和 $x, y \in N_2$, 我们考虑 (a, x) 和 (b, y) . 若

$$\phi((a, x)) = ax = by = \phi((b, y)),$$

我们有

$$N_1 \ni b^{-1}a = yx^{-1} \in N_2.$$

因此以上元素在 $N_1 \cap N_2 = \{e\}$ 中为单位元 e . 所以我们有 $a = b$ 和 $x = y$, 同态 ϕ 是单射.

另一方面, 任取 $ax \in N_1N_2$, 我们总有 $(a, x) \in N_1 \times N_2$, 满足

$$\phi(a, x) = ax.$$

因此 ϕ 是满射. 综上所述, ϕ 为 N_1 和 N_2 的内外直和之间的同构.

□

在我们研究某些群的时候(例如交换群), 我们可以将其分解为一些子群的直积, 方便我们对群的结构进行研究. 特别地, 我们有以下结论.

命题 10.3.8 (教材定理 1.7.8)

任取群 H_1, H_2, K_1 和 K_2 , 若 $H_1 \cong H_2$, 且 $K_1 \cong K_2$, 则

$$H_1 \otimes_e K_1 \cong H_2 \otimes_e K_2.$$

证明. (练习, 直接构造同构)

□

注 10.3.9.

我们将使用 $\otimes$ 表示内直积和外直积. 具体意义参考语境.

10.4 群的半直积

将一个群写为两个正规子群的直积是一种比较特殊的分解, 要求群具有较好的性质. 我们可以将直积的概念做一定的推广, 从而方便我们研究更一般的群. 这就是我们本节要介绍的半直积的概念.

设 G 为一个群. 我们希望将其写为子群的乘积. 注意到任取 G 的两个子群 H 和 K , 集合 HK 可能不是 G 的子群. 不过, 如果其中一个是 G 的正规子群的话, 这就不再是个问题了.

我们可以仿照直积的定义给出以下定义:

定义 10.4.1

设 G 为一个群, 设 N 和 H 为 G 的子群, 满足

- (i) $N \triangleleft G$;
- (ii) $N \cap H = \{e\}$;
- (iii) $G = NH$.

我们称 G 为 N 和 H 的**半直积**. 我们记 $G = N \rtimes H$.

然而与直积不同的是, 仅仅知道 N 和 H 的结构, 我们并不能确定 G 的结构. 更详细地说, 我们假设 G_1 和 G_2 是两个群, 并且 G_i 中存在正规子群 N_i 和子群 H_i , 使得 G_i 是 N_i 和 H_i 的半直积(按照以上定义). 条件 $N_1 \cong N_2$ 以及 $H_1 \cong H_2$, 不能保证 $G_1 \cong G_2$. 我们可以考虑下边这个例子:

例 10.4.2.

我们考虑群

$$G_1 = \mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

我们记

$$N_1 = \{\bar{0}, \bar{2}, \bar{4}\} \cong \mathbb{Z}_3, \quad H_1 = \{\bar{0}, \bar{3}\} \cong \mathbb{Z}_2.$$

注意到 G_1 是交换群, 因此 N 和 H 都是 G_1 的正规子群. 我们可以直接验证 G_1 按照以上定义是 N 和 H 的半直积.

另一方面, 我们可以考虑三元对称群

$$G_2 = S_3 = \{e, (12), (23), (13), (123), (132)\}.$$

我们记

$$N_2 = \{e, (123), (132)\} \cong \mathbb{Z}_3, \quad H_2 = \{e, (12)\} \cong \mathbb{Z}_2.$$

我们可以直接验证按照以上定义 G_2 是 N_2 和 H_2 的半直积.

注意到 G_1 是交换群, 而 G_2 不是交换群.

我们注意到如果 G 是正规子群 N 和子群 H 的半直积, 由于 N 是 G 的正规子群, 任取 $a \in N, x \in H$, 存在 $b \in N$, 满足

$$xa = bx,$$

我们可以将其重写为

$$xax^{-1} = b.$$

因此任意 $x \in H$ 都通过共轭作用给出 N 的一个群自同构. 由之前关于共轭作用的讨论, 我们有群同态:

$$\begin{aligned} \phi : H &\rightarrow \text{Aut}(N), \\ x &\mapsto (a \mapsto xax^{-1}). \end{aligned}$$

在之前的例子中 N_1 和 N_2 都同构于 $\mathbb{Z}_3$, H_1 和 H_2 都同构于 $\mathbb{Z}_2$, 那么我们有

$$\begin{aligned} \phi_1 : \mathbb{Z}_2 &\rightarrow \text{Aut}(\mathbb{Z}_3) \\ \bar{0} &\mapsto (\bar{0} \mapsto \bar{0}, \bar{1} \mapsto \bar{1}, \bar{2} \mapsto \bar{2}) \\ \bar{1} &\mapsto (\bar{0} \mapsto \bar{0}, \bar{1} \mapsto \bar{1}, \bar{2} \mapsto \bar{2}) \end{aligned}$$

以及

$$\begin{aligned} \phi_2 : \mathbb{Z}_2 &\rightarrow \text{Aut}(\mathbb{Z}_3) \\ \bar{0} &\mapsto (\bar{0} \mapsto \bar{0}, \bar{1} \mapsto \bar{1}, \bar{2} \mapsto \bar{2}) \\ \bar{1} &\mapsto (\bar{0} \mapsto \bar{0}, \bar{1} \mapsto \bar{2}, \bar{2} \mapsto \bar{1}) \end{aligned}$$

因此为了从 N 和 H 的结构出发确定 G 结构, 我们还需要了解 H 在 N 上通过共轭给出的作用.

利用这些观察, 我们可以如下任意两个群的半直积.

定义 10.4.3

设 N 和 H 为两个群, 记同态

$$\begin{aligned} \phi : H &\rightarrow \text{Aut}(N), \\ x &\mapsto \phi_x \end{aligned}$$

为 H 在 N 上的作用. 我们定义 N 和 H 的半直积为集合 $N \times H$ 带有以下群运算:

$$\begin{aligned} * : (N \times H) \times (N \times H) &\rightarrow N \times H \\ ((a, x), (b, y)) &\mapsto (a\phi_x(b), xy). \end{aligned}$$

并记作 $N \rtimes_{\phi} H$.

注 10.4.4.

任取 $(a, x), (b, y), (c, z) \in N \rtimes_{\phi} H$, 我们验证该运算满足结合律:

$$\begin{aligned}
 & (a, x) * ((b, y) * (c, z)) \\
 &= (a, x) * (b\phi_y(c), yz) \\
 &= (a\phi_x(b\phi_y(c)), x(yz)) \\
 &= (a\phi_x(b)(\phi_x \circ \phi_y)(c), (xy)z) \\
 &= ((a\phi_x(b))\phi_{xy}(c), (xy)z) \\
 &= ((a, x) * (b, y)) * (c, z)
 \end{aligned}$$

命题 10.4.5

任取群 N_1, N_2, H_1 和 H_2 , 设存在群同态

$$\begin{aligned}
 \phi &: N_1 \rightarrow N_2 \\
 \psi &: H_1 \rightarrow H_2 \\
 \rho &: H_1 \rightarrow \text{Aut}(N_1) \\
 \eta &: H_2 \rightarrow \text{Aut}(N_2)
 \end{aligned}$$

满足

- ϕ 和 ψ 为群同构;
- 任取 $x \in H_1, \eta_{\psi(x)} = \phi \circ \rho_x \circ \phi^{-1}$.

则

$$N_1 \rtimes_{\rho} H_1 \cong N_2 \rtimes_{\eta} H_2.$$

注 10.4.6.

关于半直积的记号, 如果乘积群是已知的, 我们可以省略 ϕ , 直接记 $G = H \rtimes K$. 我们也可将正规子群记在右边, 从而有 $G = K \rtimes H$.

10.5 群的短正合列

我们任取一个群满同态

$$\phi: G \rightarrow H,$$

记 $N = \ker \phi$. 由同态基本定理, 我们知道 $H \cong G/N$. 我们可以考虑下图

$$N \xrightarrow{j} G \xrightarrow{\phi} H.$$

其中 j 为 N 到 G 的嵌入同态. 由 N 的构造, 我们知道 j 为单同态, ϕ 为满同态, 且 $\text{Im } j = \ker \phi$.

我们进一步考虑如下特殊的情况. 设 H 和 K 为两个群, 考虑它们的直积 $G = H \times K$. 由之前关于群的直积的讨论, 我们可以将 H 和 K 看作是 G 的子群, 考虑嵌入映射:

$$\begin{aligned}
 j_H: H &\rightarrow H \times K & j_K: K &\rightarrow H \times K \\
 a &\mapsto (a, e_K) & a &\mapsto (e_H, a)
 \end{aligned}$$

二者均为单同态.

另一方面, 二者都是 G 的正规子群, 因此我们有

$$\pi_H : G \longrightarrow G/K \xrightarrow{\cong} H, \quad \pi_K : G \longrightarrow G/H \xrightarrow{\cong} K$$

考虑 H, K 和 G 的关系, 我们有下图:

$$H \xrightarrow{j_H} G \xrightarrow{\pi_K} K.$$

我们注意到 j_H 为单射, π_K 为满射, 且 $\text{Im } j_H = \ker \pi_K$. 最后一个条件可以给出以下结果:

$$\begin{aligned} \pi_K \circ j_H : H &\rightarrow K \\ a &\mapsto e_K \end{aligned}$$

为一个平凡映射. 实际上以上过程对 $G = H \rtimes K$ 也成立.

反过来, 我们可以问如果对群 G, H 和 K , 我们有同态 ϕ 和 ψ :

$$H \xrightarrow{\phi} G \xrightarrow{\psi} K.$$

满足 ϕ 为单射, ψ 为满射, 且 $\text{Im } \phi = \ker \psi$, 我们是否可以说 $G \cong H \rtimes K$?

本节我们将简要的讨论以上问题. 我们首先给以上情形一个名字.

定义 10.5.1

设 G, H 和 K 为群, 且存在同态 ϕ 和 ψ :

$$H \xrightarrow{\phi} G \xrightarrow{\psi} K.$$

满足 $\text{Im } \phi = \ker \psi$, 我们称以上序列在 G 处**正合**. 如果我们进一步有 ϕ 为单射, ψ 为满射, 记 1 为只有一个元素的群, 则我们可以将以上序列延长:

$$1 \longrightarrow H \xrightarrow{\phi} G \xrightarrow{\psi} K \longrightarrow 1.$$

满足该序列在 H, G 和 K 处正合, 那么我们称这个序列为一个**短正合列**. 此时, 我们称 G 为 K 过 H 的**扩张**. 如果我们进一步有 $\phi(H) < Z(G)$, 则称这个 G 为 K 的**中心扩张**.

注 10.5.2.

回顾一下, $Z(G)$ 为 G 的中心:

$$Z(G) = \{a \in G \mid \forall b \in G, ab = ba\}.$$

注 10.5.3.

由同态基本定理, 我们有 $K \cong G/H$.

注 10.5.4.

由之前的讨论, 我们知道若 $G = H \rtimes K$, G 是 K 过 H 的扩张.

注 10.5.5.

对应于短正合列, 我们也有长正合列这个概念. 设 $(G_i)_{i \in \mathbb{Z}}$ 为一列群. 我们假设对任意 $i \in \mathbb{Z}$, 存在一个群同态:

$$\phi_i : G_i \rightarrow G_{i+1},$$

满足

$$\ker \phi_{i+1} = \text{Im } \phi_i,$$

即以下序列

$$\cdots \xrightarrow{\phi_{i-2}} G_{i-1} \xrightarrow{\phi_{i-1}} G_i \xrightarrow{\phi_i} G_{i+1} \xrightarrow{\phi_{i+1}} \cdots,$$

在每个 G_i 处都正合, 我们称这个序列为长正合列. 我们在交换代数, 同调代数, 代数拓扑等领域中经常会遇到这样的序列.

定义 10.5.6 (教材定义 1.7.4)

设群 G, H 和 K , 满足以下短正合列:

$$1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1.$$

若存在同态

$$\phi : K \rightarrow \text{Aut}(H),$$

使得 $G \cong H \rtimes_{\phi} K$, 我们称以上短正合列**分裂**.

由直积和半直积的构造, 我们知道分裂的短正合列是存在的. 那么有没有不分裂的短正合列呢? 我们考虑以下例子.

例 10.5.7.

我们令 G 为加法群 $\mathbb{Z}_9$, H 为加法群 $\mathbb{Z}_3$, K 为加法群 $\mathbb{Z}_3$. 考虑 $\mathbb{Z}_9$ 中的子群

$$N = \{\bar{0}, \bar{3}, \bar{6}\},$$

我们有 $N \cong H$. 另一方面, $G/N \cong K$.

因此我们有短正合列

$$1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1.$$

但是不存在 $\phi : \mathbb{Z}_3 \rightarrow \text{Aut}(\mathbb{Z}_3)$, 满足 $\mathbb{Z}_9 \cong \mathbb{Z}_3 \rtimes_{\phi} \mathbb{Z}_3$.

为了证明这个断言, 我们先看一下 $\mathbb{Z}_3$ 加法群的自同构有哪些. 注意到一个自同构总是将幺元送到幺元, 因此任取

$$\psi : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3,$$

为一个群同构, 我们有

$$\begin{cases} \phi(\bar{1}) = \bar{1} \\ \phi(\bar{2}) = \bar{2} \end{cases} \quad \text{或者} \quad \begin{cases} \phi(\bar{1}) = \bar{2} \\ \phi(\bar{2}) = \bar{1} \end{cases}$$

因此 $\text{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$. 我们考虑 $\mathbb{Z}_3$ 到 $\mathbb{Z}_2$ 的同态映射. 注意到 $\mathbb{Z}_3$ 中元素的阶为 1 或者 3, 而 $\mathbb{Z}_2$ 中元素的阶为 1 或者 2. 回顾一个关于同态映射的结论. 若 $\eta : A \rightarrow B$ 为一个群同态, 任取 $a \in A$, 则

$$o(\eta(a)) \mid o(a).$$

因此 $\mathbb{Z}_3$ 到 $\mathbb{Z}_2$ 的同态映射只有平凡映射, 即所有元素都送到幺元也即 $\text{Aut}(\mathbb{Z}_3)$ 中的 id 映射. 因此我们有

$$\mathbb{Z}_3 \rtimes_{\phi} \mathbb{Z}_3 = \mathbb{Z}_3 \times \mathbb{Z}_3.$$

因此如果我们考虑的正合列分裂, 那么我们应该有 $\mathbb{Z}_9 \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. 但这是不正确的. 我们注意到 $\mathbb{Z}_9$ 中有 9 阶元素, 而 $\mathbb{Z}_3 \times \mathbb{Z}_3$ 中元素的阶最多为 3.

综上所述, 我们考虑的短正合列不分裂.

以上例子也告诉我们, 任给群 H 和 K , K 过 H 的扩张不一定唯一.

定理 10.5.8 (教材定理 1.7.2)

设 G 为 K 过 H 的扩张:

$$1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1$$

记 G' 为一个群, 则存在群同态 f , α' 和 β' 满足以下交换图

$$\begin{array}{ccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K \longrightarrow 1 \\ & & \downarrow id_H & & \downarrow f & & \downarrow id_K \\ 1 & \longrightarrow & H & \xrightarrow{\alpha'} & G' & \xrightarrow{\beta'} & K \longrightarrow 1 \end{array}$$

其中 α' 为单同态, β' 为满同态, 且 $\text{Im } \alpha' = \ker \beta'$ 当且仅当 $G \cong G'$.

证明. $\Leftarrow$ 设存在群同构

$$f: G \rightarrow G',$$

我们考虑 $\alpha' = f \circ \alpha$ 和 $\beta' = f^{-1} \circ \beta$ 即满足条件.

$\Rightarrow$ 下设存在单同态 α' 和满同态 β' 满足以上交换图, 下证 f 为群同构.

注意到 $\alpha' = f \circ \alpha$ 为一个单同态, $\beta' = f \circ \beta$ 为一个满同态. 我们希望证明 f 既是单射又是满射.

- 先证明 f 是一个单射, 即证明 $\ker f = \{e\}$. 任取 $a \in \ker f$, 我们有

$$f(a) = e' \in G',$$

因此

$$\beta(a) = (\beta' \circ f)(a) = e_K,$$

由于 G 是 K 过 H 的扩张 (交换图第一行为短正合列), 我们有

$$a \in \ker \beta = \text{Im } \alpha,$$

因此存在 $u \in H$, 满足

$$\alpha(u) = a \in G,$$

进而有

$$\alpha'(u) = (f \circ \alpha)(u) = f(a) = e'.$$

由于 α' 为单射, 我们有 $u = e$, 因此 $a = e$, 从而有 $\ker f = \{e\}$.

(我们讨论的同态的顺序为 β' , $\beta = \beta' \circ f$, α , $\alpha' = f \circ \alpha$, 注意这些同态在交换图上的位置.)

• 下证 f 为满射. 任取 $a' \in G'$, 我们有 $\beta'(a') \in K$. 由于 β' 为满射, 因此存在 $a \in G$, 满足

$$\beta(a) = \beta'(a').$$

另一方面, 由交换图我们有

$$\beta(a) = (\beta' \circ f)(a) = \beta'(f(a)).$$

因此 $b' = a'f(a)^{-1} \in \ker \beta'$. 由于 $\text{Im } \alpha' = \ker \beta'$, 因此存在 $u \in H$, 满足

$$f(\alpha(u)) = (f \circ \alpha)(u) = \alpha'(u) = b = a'f(a)^{-1}.$$

因此

$$f(\alpha(u)a) = f(\alpha(u))f(a) = a',$$

因此 $a' \in \text{Im } f$.

(我们讨论的同态的顺序为 β' , $\beta = \beta' \circ f$, $\alpha' = f \circ \alpha$, α 注意这些同态在交换图上的位置.) $\square$

10.6 *群的合成列

10.6.1 群的极大正规子群

如前文所述, 设 N 为群 G 的正规子群, 我们考虑群同态基本定理, 则得到短正合列:

$$1 \longrightarrow N \xrightarrow{j} G \xrightarrow{\pi} G/N \longrightarrow 1.$$

一方面 G/N 是 G 关于 N 的商群, 另一方面, 由群扩张的定义, 我们也可以将 G 看作是 G/N 关于 N 的扩张. 通过研究 N 和 G/N , 我们可以了解 G 的一些信息.

一个群 G 中可能有不同的正规子群, 那么有没有一个典则(即在某种意义上唯一)的选法呢?

我们首先考虑之前介绍过的一个概念.

定义 10.6.1

一个群 G 被称为**单群**, 若其没有除了 $\{e\}$ 和 G 之外的正规子群.

命题 10.6.2

设 G 为一个交换群. 则 G 为单群当且仅当 $G \cong \mathbb{Z}_p$.

证明. 由于 G 交换, 因此 G 的任意子群都是 G 的正规子群.

利用 Cauchy 定理可得, 任取 G 的阶的素因子 p , G 中有一个 p -阶子群. 因此 G 为一个单群当且仅当 G 的阶为素数, 这也等价于存在素数 $p \in \mathbb{Z}$, 使得 $G \cong \mathbb{Z}_p$. $\square$

如果我们希望通过正规子群研究 G 的话, 就只能选择 $N = \{e\}$ 或者 $N = G$, 而这些都是平凡的情况.

在继续讨论一般情况之前, 我们先给出以下定义:

定义 10.6.3

设 G 为一个群. 我们称 G 的一个正规子群 N 为 G 的**极大正规子群**, 若其满足任取 G 的正规子群 M , 满足 $N \triangleleft M \triangleleft G$, 则 $M = N$ 或者 $M = G$.

例 10.6.4.

我们首先考虑一个平凡的例子. 如果 G 是一个单群, 那么 G 的极大正规子群就是 $\{e\}$.

例 10.6.5.

令 G 为整数加法群 $\mathbb{Z}$, 则极大正规子群是 $p\mathbb{Z}$, 其中 p 为一个素数. 从这个例子我们发现, 极大正规子群有可能是不唯一的.

命题 10.6.6

令 G 为一个群, 设 N 为 G 的一个正规子群. 以下两个叙述等价:

- (i) N 为 G 的极大正规子群.
- (ii) 商群 G/N 为单群.

证明. 由群同态基本定理, 我们有 G/N 中的正规子群和 G 中包含 N 的正规子群之间的一一对应. 正规子群 N 为极大的, 当且仅当包含 N 的 G 的正规子群只有 G 和 N , 等价地有 G/N 中的正规子群只有幺元 eN 和 G/N , 即 G/N 为单群. $\square$

例 10.6.7.

令 G 为加法群 $\mathbb{Q}$, 由于 $\mathbb{Q}$ 交换. 我们假设存在 $N \triangleleft \mathbb{Q}$ 是一个极大子群, 则 $\mathbb{Q}/N$ 同构于 $\mathbb{Z}_p$, 其中 p 为某个素数.

另一方面, 任取 $\mathbb{Q}$ 的元素 $a \neq 0$, 对任意 $n \in \mathbb{Z}^*$, 我们有 $a/n \in \mathbb{Q}$. 因此若

$$G/N = \{N, aN, 2aN, \dots, (p-1)aN\}.$$

我们也应该有

$$\frac{a}{2}N \in G/N,$$

因此

$$G/N = \left\{ N, \frac{a}{2}N, \dots, \frac{(2p+1)a}{2}N \right\}.$$

注意到任取 $\{0, \dots, p-1\}$ 中 $i \neq j$, 我们有

$$\frac{(i-j)a}{2} \notin N.$$

否则, 若

$$\frac{(i-j)a}{2} \in N.$$

因此 $(i-j)a \in N$. 另一方面, 由于 $i-j \in \mathbb{Z}$, 且 $0 < |i-j| < p-1$, 因此 $(i-j)aN \neq N$, 即 $(i-j)a \notin N$. 矛盾.

例 10.6.8.

以上例子说明极大正规子群并不一定总是存在. 类似地, 我们也可以考虑极小正规子群, 我们也有极小正规子群不一定存在的结论.

例 10.6.9.

涉及极大元素的存在性的问题, 我们总会考虑使用 Zorn 引理. 我们可以尝试使用 Zorn 引理来证明一个群总有极大正规子群(当然一定会失败, 因为命题是不正确的), 看看哪里出了问题.

10.6.2 群的次正规列以及合成列

设 G 为一个群, N 为一个极大正规子群, 我们可以进一步讨论 N 的极大正规子群, 以及 N 的极大正规子群的极大正规子群等等. 如果我们可以通过有限步得到 $\{e\}$, 即如果记第 i 步得到的群为 G_i , 有以下序列:

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k = \{e\},$$

满足 G_i/G_{i+1} 为单群, 利用单群的性质, 我们可以得到 G 的一些信息. 这种类型的分解(包括后边可解群以及幂零群涉及得子群序列)也使得我们在证明一些结论时可以使用归纳法.

但在这个过程中, 我们会遇到两个问题. 一个是每一步极大正规子群是否存在性的问题, 另一个就是在每步都可以进行的情况下, 有限步是否终止的问题, 因此以上分解并不一定被任意群满足. 我们本节将主要考虑满足以上条件的群, 并证明以上子群列一旦存在, 则在"某种意义上"是唯一的, 也即 Jordan-Hölder 定理.

我们首先介绍一些概念.

定义 10.6.10

任取一个群 G , 如果存在 $t \in \mathbb{N}^*$, 存在 G 的子群下降列

$$G_0 = G > G_1 > \cdots > G_t = \{e\},$$

满足对任意 $0 \leq i \leq t-1$, 有

$$G_i \triangleright G_{i+1},$$

我们称以上序列为 G 的一个**次正规序列**. 如果我们进一步有对于任意 $0 \leq i \leq t-1$, $G_{i+1} \subsetneq G_i$, 则称这个次正规序列是**无重复的**. 此时, 我们称 t 为该次正规序列的**长度**.

注 10.6.11.

这里我们没有要求 G_{i+1} 是 G_i 的极大正规子群. 注意到, 按照这个定义, 任意群 G 都有一个平凡的次正规序列

$$G \triangleright \{e\}.$$

注 10.6.12.

在介绍正规子群的概念的时候, 我们提到这个概念没有传递性, 即若 $K \triangleleft H$, $H \triangleleft G$, 我们不一定有 $K \triangleleft G$. 例如我们考虑 4 阶交错群

$$A_4 = \{e, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}.$$

我们一般称

$$V = \{e, (12)(34), (13)(24), (14)(23)\}.$$

为 Klein 4 元群. 注意到 $V \triangleleft A_4$, 且

$$V \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

我们考虑 $K = \{e, (12)(34)\}$, 则 $K \triangleleft V$ 但 K 不是 A_4 的正规子群.

在以上次正规序列的定义中, 我们只要求 G_{i+1} 是 G_i 的正规子群, 并没有要求 G_{i+1} 是 G 的正规子群.

定义 10.6.13

任取群 G 以及非零自然数 t , 设 $(G_i)_{i=0}^t$ 为一个次正规序列. 若对任意 $0 \leq i \leq t$, 我们有

$$G_i \triangleleft G,$$

我们称 $(G_i)_{i=0}^t$ 为一个**正规序列**.

我们可以添加一些子群来改变一个正规序列.

定义 10.6.14

任取群 G , 设 G 的一个子群序列 $(G_i)_{i=0}^t$ 为 G 的一个次正规序列. 若有 $0 \leq i \leq t-1$, 以及 $N < G$, 使得

$$G_0 = G > G_1 > \cdots > G_i > N > G_{i+1} > \cdots > G_t,$$

为 G 的次正规序列, 我们称其为 $(G_i)_{i=0}^t$ 的**一步加细**.

进一步地, 我们定义从 $(G_i)_{i=0}^t$ 出发, 经过有限次一步加细得到次正规序列为 $(G_i)_{i=0}^t$ 的**加细**.

注 10.6.15.

我们并没有要求 G_i 严格包含 G_{i+1} , 因此不方便利用集合包含:

$$\{G_0, \dots, G_t\} \subset \{H_0, \dots, H_s\},$$

来给出定义.

任取群 G , 设存在以下次正规列:

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_t = \{e\},$$

我们有以下一系列的短正合列:

$$\begin{aligned} 1 &\rightarrow G_1 \rightarrow G_0 \rightarrow G_0/G_1 \rightarrow 1 \\ 1 &\rightarrow G_2 \rightarrow G_1 \rightarrow G_1/G_2 \rightarrow 1 \\ &\dots \\ 1 &\rightarrow G_{t-1} \rightarrow G_{t-2} \rightarrow G_{t-2}/G_{t-1} \rightarrow 1 \\ 1 &\rightarrow 1 = G_t \rightarrow G_{t-1} \rightarrow G_{t-1} \rightarrow 1 \end{aligned}$$

因此由之前关于群扩张的讨论, G 可以看作是由 $G_{t-1}, G_{t-2}/G_{t-1}, \dots, G_0/G_1$ 构造出来的. 因此研究这些群的性质可以帮助我们了解 G 的结构. 这些群的性质更特殊, 群 G 的性质也更特殊. 另一方面, 我们希望用这样的信息来给一些特殊类型的群 G 进行分类, 但是一个这里有一个问题就是这类分解的(在某种意义下的)唯一性.

定义 10.6.16

任取群 G , 以及非零自然数 t . 设 G 的一个子群递降序列

$$G_0 = G > G_1 > \cdots > G_t = \{e\},$$

满足对任意 $0 \leq i \leq t-1$, 有

- (i) $G_{i+1} \triangleleft G_i$,
- (ii) G_i/G_{i+1} 是一个单群,

我们称 $(G_i)_{i=0}^t$ 为一个**合成列**.

如果该合成列进一步满足对任意 $0 \leq i \leq t$, $G_i \triangleleft G$, 我们称该合成列为一个**主序列**.

注 10.6.17.

由本节开始的讨论, 我们知道对于一般的群, 合成列并不一定存在.

命题 10.6.18

设 G 为一个有限群, 则 G 有一个合成列.

证明. 设 G 为一个有限群. 如果 $G = \{e\}$, 则我们可以直接验证 $\{e\}$ 为一个合成列, 因此结论成立. 我们下设 $G \neq \{e\}$.

我们考虑 G 的所有的正规真子群的集合:

$$\{N \mid N \triangleleft G, N \neq G\}.$$

由于 $\{e\}$ 在里边, 因此以上集合非空.

注意到任意一个正规真子群的阶都严格小于 $|G|$. 由于群的阶为非零自然数, 因此 G 的正规子群的阶最多只有 $|G| - 1$ 种可能. 我们记 G_1 为 G 的一个正规真子群, 满足

$$|G_1| := \max\{|N| \mid N \triangleleft G, N \neq G\}.$$

因此 G_1 为 G 的一个极大正规子群. 否则, 存在 G 的一个正规子群 G'_1 , 满足

$$G_1 \subsetneq G'_1 \subsetneq G,$$

这与 G_1 的阶满足的条件矛盾.

我们对 G_1 重复以上讨论可以得到 G_2 . 注意到 G 的阶有限, 并且对任意 i , 我们有

$$|G_{i+1}| < |G_i|,$$

因此存在一个自然数 $k > 0$, 使得 $G_k = \{e\}$. 由此我们得到一个合成列. □

注 10.6.19.

在以上证明中, 第一步得到的 G_1 可能有多种选择, 理论上这些选择可能不是同构的. 然而, 下边我们将证明的结论告诉我们, 当 G 有合成列是, 整个合成列在同构意义下是唯一的.

定理 10.6.20 (Jordan-Hölder 定理)

设 G 为一个群, 并设 G 有两个无重复的长度分别为 s 和 t 的合成列:

$$\begin{aligned} G &= G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = \{e\}, \\ G &= H_0 \triangleright H_1 \triangleright \cdots \triangleright H_n = \{e\} \end{aligned}$$

则有 $m = n$ 存, 且在一个 $\sigma \in S_m$, 满足对任意 $0 \leq i \leq m-1$, 我们有

$$G_i/G_{i+1} \cong H_{\sigma(i)}/H_{\sigma(i)+1}.$$

注 10.6.21.

注意这里是 $H_{\sigma(i)+1}$ 不是 $H_{\sigma(i+1)}$.

注 10.6.22.

这里要注意的是, 这个定理关注的是每一步涉及的两个群之间的商群. 我们考虑

$$G = \mathbb{Z}_6 = \mathbb{Z}_2 \times \mathbb{Z}_3.$$

这个群有以下两个合成列:

$$\begin{aligned} \mathbb{Z}_6 &\triangleright \mathbb{Z}_3 \triangleright \{e\}, \\ \mathbb{Z}_6 &\triangleright \mathbb{Z}_2 \triangleright \{e\} \end{aligned}$$

我们看到中间位置上的群相互之间并不同构, 但是我们有

$$\begin{aligned} G_0/G_1 &\cong \mathbb{Z}_2, & G_1/G_2 &\cong \mathbb{Z}_3 \\ H_0/H_1 &\cong \mathbb{Z}_3, & H_1/H_2 &\cong \mathbb{Z}_2 \end{aligned}$$

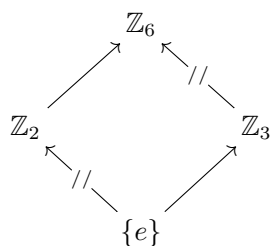
注意到我们取 $\sigma \in S_3$ 满足

$$0 \mapsto 1, 1 \mapsto 0, 2 \mapsto 2,$$

就可以得到

$$G_0/G_1 \cong H_{\sigma(0)}/H_{\sigma(0)+1}, G_1/G_2 = H_{\sigma(1)}/H_{\sigma(1)+1}.$$

我们可以考虑以下示意图

**注 10.6.23.**

Jordan 介绍了正合列和主序列的概念, 并证明了一个群的两个不同的正合列的长度相同. Hölder 证明了在相差一个置换的前提下, 一个的两个正合列给出的对应的商群同构.

Jordan-Hölder 定理的证明. 以下对任意 $0 \leq i \leq n-1$, 我们将找出 $0 \leq j \leq m-1$, 满足

$$H_i/H_{i+1} \cong G_j/G_{j+1}.$$

我们首先回顾一个关于正规子群的结果. 设 $N_1 \triangleleft N_2$, 任取 $A < G$, 我们有

$$(A \cap N_1) \triangleleft (A \cap N_2),$$

因此我们考虑 H_i 与 $(G_k)_{0 \leq l \leq m}$ 中的群的交集:

$$K_l = H_i \cap G_l,$$

因此我们有一个 H_i 子群的次正规列递降列

$$H_i = K_0 \triangleright K_1 \triangleright K_2 \triangleright \cdots \triangleright K_m = \{e\}.$$

注意到 $H_{i+1} \triangleleft H_i$, 我们有

$$H_i = K_0 H_{i+1} > K_1 H_{i+1} > K_2 H_{i+1} > \cdots > K_m H_{i+1} = H_{i+1}.$$

注意到 K_1 和 H_{i+1} 都是 $H_i = K_0$ 的正规子群, 因此

$$H_i \triangleright K_1 H_{i+1} > H_{i+1}.$$

由于 H_i/H_{i+1} 是一个单群, 因此 $K_1 H_{i+1} = H_i$ 或者 $K_1 H_{i+1} = H_{i+1}$.

假设 $K_1 H_{i+1} = H_i$, 我们对 $K_2 H_{i+1}$ 重复以上讨论, 如此往复. 由于 $K_m H_{i+1} = H_{i+1}$, 存在一个下标 $1 \leq j \leq m-1$, 满足

$$\begin{aligned} (G_j \cap H_i) H_{i+1} &= K_j H_{i+1} = H_i \\ (G_{j+1} \cap H_i) H_{i+1} &= K_{j+1} H_{i+1} = H_{i+1} \end{aligned}$$

所以上构造的序列可记为

$$H_i = K_0 H_{i+1} = K_1 H_{i+1} = \cdots = K_j H_{i+1} \triangleright K_{j+1} H_{i+1} = \cdots = K_m H_{i+1} = H_{i+1}$$

任取 $N \triangleleft G$, $A < G$, 我们有 $A \cap N \triangleleft A$, 且

$$A/(A \cap N) \cong AN/N.$$

令 $G = H_i$, $A = G_j \cap H_i$, $N = H_{i+1} = G_{j+1} \cap H_i$, 我们有

$$\begin{aligned} & H_i/H_{i+1} \\ & \cong (G_j \cap H_i) H_{i+1} / (G_{j+1} \cap H_i) H_{i+1} \\ & \cong (G_j \cap H_i) / (G_j \cap H_i) \cap (G_{j+1} \cap H_i) H_{i+1} \\ & \cong (G_j \cap H_i) / (G_j \cap H_i \cap G_{j+1} H_{i+1}) \end{aligned}$$

我们可以将 H_i 的角色和 G_j 的角色调换一下. 考虑 G_j 与 $(H_l)_{0 \leq l \leq n}$ 中的群的交集:

$$L_l = G_j \cap H_l,$$

因此我们有一个 G_j 子群的次正规列递降列

$$G_j = L_0 \triangleright L_1 \triangleright L_2 \triangleright \cdots \triangleright L_n = \{e\}.$$

注意到 $G_{j+1} \triangleleft G_j$, 我们有

$$G_j = L_0 G_{j+1} > L_1 G_{j+1} > L_2 G_{j+1} > \cdots > L_m G_{j+1} = G_{j+1}.$$

由于 G_j/G_{j+1} 为单群, 重复之前的讨论, 我们可以找到 $1 \leq s \leq n-1$, 满足

$$G_j = L_0 G_{j+1} = L_1 G_{j+1} = \cdots = L_s G_{j+1} \triangleright L_{s+1} G_{j+1} = \cdots = L_n G_{j+1} = G_{j+1}.$$

注意到

$$\begin{aligned} & (G_j \cap H_l) G_{j+1} / (H_{l+1} \cap G_j) G_{j+1} \\ & \cong (G_j \cap H_l) / (G_j \cap H_l) \cap (H_{l+1} \cap G_j) G_{j+1} \\ & \cong (G_j \cap H_l) / (G_j \cap H_l \cap G_{j+1} H_{l+1}), \end{aligned}$$

要确定 s , 我们只需要考虑商群 $(G_j \cap H_l) / (G_j \cap H_l \cap G_{j+1} H_{l+1})$ 非平凡时对应的 l 即为 s 的值. 之前的讨论也说明这样的 l 是唯一的. 考虑之前关于 H_i/H_{i+1} 的讨论, 我们知道 $s = i$, 并且我们进一步有

$$G_j/G_{j+1} \cong (G_j \cap H_i) / (G_j \cap H_i \cap G_{j+1} H_{i+1}) \cong H_i/H_{i+1}.$$

注意到以上给出了 $(H_i/H_{i+1})_{1 \leq i \leq n}$ 和 $(G_j/G_{j+1})_{1 \leq j \leq m}$ 之间的一个一一对应, 因此我们得到定理. $\square$

注 10.6.24.

证明中用到了 Zassenhaus Lemma (见习题). 我们也可以使用归纳法来证明这个定理.

注 10.6.25.

由 Jordan-Hölder 定理出发, 我们可以考虑利用单群对有限群进行分类问题. 这部分被称为 Hölder Program 的研究关心两个问题:

- (i) 将所有有限单群进行分类.
- (ii) 找到所有将单群放在一起构造任意其他有限群的方法.

注 10.6.26.

实际上以上想法出现在很多领域的研究中. 通常当某种结构非常复杂时, 我们会考虑将其分解为同类型的简单容易研究的结构, 然后研究如何将这些简单的结构粘起来. 我们熟知的三角剖分就是一个例子(研究流形的拓扑结构或者几何结构).

10.7 *可解群和幂零群

上节我们讨论了合成列这种特殊的次正规序列. 本节我们讨论另一种特殊情形的次正规序列, 即商群 G_i/G_{i+1} 为交换群的情形.

10.7.1 可解群

可解群起源于 Galois 对多项式方程是否有根式可解(即可解)问题的研究, 这也是可解群名字中可解的来源. 在 Galois 理论中, 我们将看到 $\mathbb{Q}$ 上一个多项式方程有根式解当且仅当该多项式的 Galois 群为一个可解群. 本节中我们讲给出可解群的定义和一些性质. 我们将在下学期 Galois 理论中详细讨论以上提到的多项式方程可解的充要条件.

换位子群

可解群的定义会涉及使用商群 G/H 为交换群的条件. 为了得到交换的商群, 我们需要至少将 G 中非交换的部分商掉, 而这部分信息就包含在 G 的换位子群中.

记 G 为一个群.

定义 10.7.1 (教材定义 1.8.1)

任取 $a, b \in G$, 我们定义 a 和 b 的换位子为:

$$[a, b] := a^{-1}b^{-1}ab.$$

定义 10.7.2 (教材定义 1.8.1)

我们定义 G 的**换位子群**为 G 中元素的换位子生成的群:

$$[G, G] := \langle [a, b] \mid a, b \in G \rangle.$$

注 10.7.3.

注意到 G 中两个元素 a 和 b 交换, 即

$$ab = ba,$$

当且仅当 a 和 b 的换位子平凡, 即

$$[a, b] = e.$$

所以某种意义上, 换位子群告诉了我们群 G 与不交换相关的"信息".

我们首先考虑以下两个与换位子群相关的命题.

命题 10.7.4

任取群 G , 则换位子群 $[G, G]$ 为 G 的正规子群.

证明. 任取 $a, b, c \in G$, 我们有以下运算:

$$\begin{aligned} & c[a, b]c^{-1} \\ &= c(a^{-1}b^{-1}ab)c^{-1} \\ &= (ca^{-1}c^{-1})(cb^{-1}c^{-1})(cac^{-1})(cbc^{-1}) \\ &= [cac^{-1}, cbc^{-1}] \in [G, G]. \end{aligned}$$

由于 G 中元素的换位子生成 $[G, G]$, 并且任给元素 $g_1, \dots, g_k \in G$, 有

$$c(g_1 \cdots g_k)c^{-1} = (cg_1c^{-1}) \cdots (cg_kc^{-1}),$$

我们有

$$[G, G] \triangleleft G.$$

□

由以上命题我们可以定义商群 $G/[G, G]$. 利用换位子群的定义以及正规子群的性质, 我们有一下结论.

命题 10.7.5

商群 $G/[G, G]$ 交换.

证明. 任取 $a, b \in G$, 利用正规子群的性质, 我们有以下计算:

$$\begin{aligned}
 & a[G, G]b[G, G] \\
 &= ab[G, G] \\
 &= ab[b, a][G, G] \\
 &= abb^{-1}a^{-1}ba[G, G] \\
 &= ba[G, G] \\
 &= b[G, G]a[G, G].
 \end{aligned}$$

□

任取 G 的一个正规子群 H , 利用换位子群, 我们可以得到商群 G/H 交换的一个充要条件.

命题 10.7.6

记 $H \triangleleft G$ 为一个正规子群, 则 G/H 交换当且仅当 $[G, G] \triangleleft H$.

证明. 证明 $[G, G] \triangleleft H$ 的充分性, 我们回顾推论 7.2.14 中的结论:

任取 G 的两个正规子群 H_1 和 H_2 , 满足 $H_1 \triangleleft H_2$, 则有

$$G/H_2 \cong (G/H_1)/(H_2/H_1).$$

因此若 $[G, G] \triangleleft H$, 我们有 G/H 同构于 $G/[G, G]$ 的一个商群, 因此也是交换群.

下证 $[G, G] \triangleleft H$ 的必要性. 任取 $a, b \in G$, 我们有

$$abH = aHbH = bHaH = baH.$$

因此

$$[a, b]H = H.$$

由之前关于陪集的讨论(命题 6.3.2), 以上关系等价于 $[a, b] \in H$. 由于 H 包含 G 中所有的换位子, 我们有

$$[G, G] \subset H.$$

利用命题 6.4.24 中的结论, 我们有 $[G, G] \triangleleft H$.

□

可解群的定义

我们归纳定义以下 G 的子群. 令 $G^{(0)} = G$. 任取 $k \in \mathbb{N}^*$, 定义

$$G^{(k)} := [G^{(k-1)}, G^{(k-1)}].$$

定义 10.7.7 (教材定义 1.8.7)

我们称群 G 为一个**可解群**, 若存在 $k \in \mathbb{N}^*$, 满足

$$G^{(k)} = \{e\},$$

其中 e 为 G 的幺元.

任取群 G , 我们都可以定义换位子群. 因此任给群 G , 我们都可以定义由换位子群给出的次正规列.

定义 10.7.8 (教材定义 1.8.6)

记 G 为一个群, 我们称以下次正规序列

$$G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots,$$

为 G 的**导出列**(derived series).

由定义, 我们有以下结论.

命题 10.7.9

设 G 为一个群. 以下两个叙述等价:

- (i) 群 G 可解.
- (ii) 群 G 的导出列中除了至多有限多项外都是 $\{e\}$.

由之前对换位子群的讨论, 如果一个群可解, 则我们可以得到一个次正规列, 满足相邻两个群之间的商群是交换的. 下边的结论告诉我们, 这个结论反过来也是正确的.

命题 10.7.10

设 G 为一个群. 以下两个叙述等价:

- (i) 群 G 可解.
- (ii) 存在 $n \in \mathbb{N}^*$, 以及群 G 有一个有限子群递降列:

$$G = G_0 > G_1 \cdots > \{e\} = G_n,$$

满足

- (a) 对任意 $1 \leq i \leq n$, $G_{i-1} \triangleright G_i$;
- (b) 对任意 $1 \leq i \leq n$, G_{i-1}/G_i 交换.

证明. (i) $\implies$ (ii)

若 G 是可解群, 则存在 $k \in \mathbb{N}^*$, 满足

$$\{e\} = G^{(k)} \triangleleft \cdots \triangleleft G^{(1)} \triangleleft G^{(0)} = G.$$

对任意 $1 \leq i \leq k$, 我们有

$$G^{(i)} = [G^{(i-1)}, G^{(i-1)}],$$

由换位子群的性质可得 $G^{(i-1)}/G^{(i)}$ 是一个交换群. 所以 G 满足 (ii) 中条件.

(ii) $\implies$ (i)

假设 G 满足 (ii) 中条件, 则存在 G 的一个次正规子群有限列:

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{e\}.$$

满足对任意 $1 \leq i \leq n$, 有 G_{i-1}/G_i 为一个交换群. 我们对 n 使用归纳法.

当 $n = 1$ 时, 我们有 G 交换, 因此 $G^{(1)} = \{e\}$. 结论成立.

下边假设 $m > 1$ 且结论对 $n = m - 1$ 成立. 因此由归纳假设, 我们有 $k \in \mathbb{N}^*$, 满足

$$G = G_0 \triangleright G_1 = G_1^{(0)} \triangleright G_1^{(1)} \triangleright \cdots \triangleright G_1^{(k)} = \{e\}.$$

由于 G/G_1 交换, 由换位子群的性质, 我们有

$$G \triangleright G_1 \triangleright G^{(1)}.$$

由于 $G_1/G^{(1)} < G/G^{(1)}$, 因此也是交换群. 由此可得

$$G_1 \triangleright G^{(1)} \triangleright G_1^{(1)}.$$

利用类似的方法, 我们可以证明对任意 $1 \leq i \leq k$, 我们有

$$G_1^{(i-1)} \triangleright G^{(i)} \triangleright G_1^{(i)}.$$

由于 $G_1^{(k)} = \{e\}$, 因此 $G^{(k+1)} = \{e\}$. 群 G 为可解群. □

由此我们得到另一种定义可解群的方法.

定义 10.7.11

若一个群 G 满足以上命题中的条件 (ii), 我们称之为**可解群**.

注 10.7.12.

考虑之前 G 与其次正规列给出的一系列的商群的关系, 若 G 可解, 则 G 可以看作是由一系列的交换群的扩张得到的.

当群 G 有限时, 我们考虑有限交换群的结构定理, 可以得到以下结论.

命题 10.7.13

设 G 为一个有限群. 以下两个叙述等价:

(i) 群 G 可解.

(ii) 存在非零自然数 n , 以及 G 的一个次正规子群有限列:

$$G = G_0 \triangleright \cdots \triangleright G_n = \{e\}.$$

满足对任意 $1 \leq i \leq n$, 商群 G_{i-1}/G_i 是一个有限循环群.

注 10.7.14.

当群 G 有限的时候, 我们也会用以上命题中的条件 (ii) 作为 G 可解的定义.

注 10.7.15.

若有限群 G 满足条件 (ii), 由商群的性质, 以及循环群的性质, 我们可以将该次正规列加细使得序列中相邻两个群之间的商群为一个素数阶的循环群.

例 10.7.16.

考虑 3 元置换群 S_3 , 注意到 $A_3 \triangleleft S_3$, 且 $[S_3 : A_3] = 2$, 因此 S_3/A_3 为一个 2 阶循环群. 由于 A_3 为一个 3 阶循环群, 因此我们有如下次正规子群列:

$$\{id\} \triangleleft A_3 \triangleleft S_3,$$

满足可解群的定义.

例 10.7.17.

考虑 4 元置换群 S_4 . 注意到 $A_4 \triangleleft S_4$, 且 $[S_4 : A_4] = 2$, 因此 S_4/A_4 为一个 2 阶循环群. 考虑 A_4 中的 Klein 4 元群 V , 商群 A_4/V 为一个 3 阶循环群. 考虑 V 中的子群 $G_3 = \{id, (12)(34)\}$, 则有 V/G_3 为一个 2 阶循环群. 因此, 我们有如下次正规子群列

$$\{id\} \triangleleft G_3 \triangleleft V \triangleleft A_4 \triangleleft S_4.$$

导出列是正规序列

以上对可解群 G 的讨论中涉及的 G 的子群列都是次正规序列. 这里我们将进一步说明这些次正规序列实际上也是正规序列. 我们首先证明以下引理:

引理 10.7.18

设 G 为一个群, H 为 G 的一个正规子群, 则有

$$[H, H] \triangleleft G$$

证明. 任取 $a \in G$, 以及 $b, c \in H$, 我们考虑

$$\begin{aligned} & a[b, c]a^{-1} \\ &= a(b^{-1}c^{-1}bc)a^{-1} \\ &= (ab^{-1}a^{-1})(ac^{-1}a^{-1})(aba^{-1})(aca^{-1}) \\ &= (aba^{-1})^{-1}(aca^{-1})^{-1}(aba^{-1})(aca^{-1}) \\ &= [(aba^{-1}), (aca^{-1})] \end{aligned}$$

由于 $H \triangleleft G$, 因此 aba^{-1} 和 aca^{-1} 都属于 H . 因此

$$a[b, c]a^{-1} \in [H, H].$$

由正规子群的定义知

$$[H, H] \triangleleft G.$$

□

推论 10.7.19

任意群 G 的导出列是正规列.

证明. 我们使用归纳法.

考虑以上引理, 取 $H = G$, 我们知 $G^{(1)} \triangleleft G$.

设 $G^{(k)} \triangleleft G$, 考虑以上引理令 $H = G^{(k)}$, 则有

$$G^{(k+1)} \triangleleft G.$$

因此结论得证. □

注 10.7.20.

若 G 为可解群, 任取 G 中满足可解群定义中条件的次正规列并不总是正规列. 例如

$$S_4 \triangleright A_4 \triangleright V \triangleright G_3 \triangleright \{id\},$$

其中 G_3 并不是 S_4 的正规子群.

可解群的性质

由此, 我们可以得到关于可解群的以下结论.

定理 10.7.21

- (i) 可解群的任意子群也是可解群;
- (ii) 设 G 为一个群, $H \triangleleft G$ 为一个正规子群. 则 G 可解当且仅当 H 可解且 G/H 可解.

我们将利用不同定义给出两个证明.

证明一(使用换位子群). (i) 若 G 可解, 则存在 $k \in \mathbb{N}^*$, 满足

$$G^{(k)} = \{e\}.$$

任取 A 为 G 的子群, 对任意 $i \in \mathbb{N}$,

$$A^{(i)} < G^{(i)}.$$

因此 $A^{(k)} = \{e\}$, A 可解.

(ii) 记 H 为 G 的一个正规子群, 若 G 可解, 则由 (i) 我们有 H 可解. 另一方面, 考虑自然同态:

$$\pi : G \rightarrow G/H,$$

对任意 $i \in \mathbb{N}$, 我们有

$$(G/H)^{(i)} = (\pi(G))^{(i)} = \pi(G^{(i)}).$$

因此 G/H 可解.

现在假设 H 和 G/H 可解. 预证 G 可解.

由 G/H 可解, 存在一个 $k \in \mathbb{N}^*$, 满足

$$\pi(G^{(k)}) = (G/H)^{(k)} = \{\bar{e}\}.$$

因此 $G^{(k)} < H$. 由 H 可解, 我们知 $G^{(k)}$ 可解, 因此 G 可解. □

证明二(不使用换位子群). (i) 若 G 可解, 则存在 $k \in \mathbb{N}^*$, 以及 G 的一个次正规子群列:

$$\{e\} = G_k \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G,$$

满足对任意 $1 \leq i \leq k$, G_{i-1}/G_i 交换.

设 A 为 G 的一个子群, 我们记

$$A_i = A \cap G_i.$$

因此我们有子群列

$$\{e\} = A_k \triangleleft \cdots \triangleleft A_1 \triangleleft A_0 = A.$$

我们需要证明以下两点:

- 对任意 $1 \leq i \leq k$, $A_i \triangleleft A_{i-1}$;
- 对任意 $1 \leq i \leq k$, A_{i-1}/A_i 交换.

注意到对任意 $1 \leq i \leq k$, 任取

$$a \in A_{i-1} = A \cap G_{i-1}, \quad b \in A_i = A \cap G_i,$$

则

- 由于 $a \in A$ 和 $b \in A$, 有 $aba^{-1} \in A$;
- 由于 $a \in G_{i-1}$ 和 $b \in G_i$, 且 $G_i \triangleleft G_{i-1}$, 有 $aba^{-1} \in G_i$.

因此 $aba^{-1} \in A_i$. 我们有

$$A_i \triangleleft A_{i-1}.$$

其次考虑

$$A_i = A \cap G_i = (A \cap G_{i-1}) \cap G_i = A_{i-1} \cap G_i.$$

我们有

$$A_{i-1}/A_i \cong A_{i-1}G_i/G_i \triangleleft G_{i-1}/G_i.$$

因此 A_{i-1}/A_i 同构于一个交换群的子群, 也是交换群. 从而我们有 A 可解.

(ii) 我们首先假设 G 可解, 则存在 $k \in \mathbb{N}^*$, 以及 G 的一个次正规子群列:

$$\{e\} = G_k \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G,$$

满足对任意 $1 \leq i \leq k$, G_{i-1}/G_i 交换.

设 $H \triangleleft G$, 则由 (i), H 可解. 下证 G/H 可解. 对任意 $1 \leq i \leq k$, 我们记

$$\overline{G}_i = G_i H / H \cong G_i / (G_i \cap H).$$

因此我们有 G/H 的一个子群列:

$$\{e\} = \overline{G}_k \triangleleft \cdots \triangleleft \overline{G}_1 \triangleleft \overline{G}_0 = G/H.$$

我们需要证明以下两点:

- 对任意 $1 \leq i \leq k$, $\overline{G}_i \triangleleft \overline{G}_{i-1}$;
- 对任意 $1 \leq i \leq k$, $\overline{G}_{i-1}/\overline{G}_i$ 交换.

注意到 $H \triangleleft G$, 因此任取 $A < G$, 我们有

$$AH = \{ah \mid a \in A, h \in H\}.$$

由此可得

$$AH/H = \{aH \mid a \in H\}.$$

任取 $a \in G_{i-1}$ 和 $b \in G_i$, 我们有

$$(aH)(bH)(a^{-1}H) = aba^{-1}H.$$

由于 $G_i \triangleleft G_{i-1}$, 我们有 $aba^{-1} \in G_i$, 因此

$$(aH)(bH)(a^{-1}H) = aba^{-1}H \in G_iH.$$

由此我们可得

$$\overline{G}_i \triangleleft \overline{G}_{i-1}.$$

我们考虑两个自然同态:

$$\begin{aligned}\pi_1 : G_{i-1} &\rightarrow G_{i-1}/(G_{i-1} \cap H) \\ \pi_2 : G_{i-1}H/H &\rightarrow (G_{i-1}H/H)/(G_iH/H)\end{aligned}$$

以及群同构

$$\phi : G_{i-1}/(G_{i-1} \cap H) \rightarrow G_{i-1}H/H$$

记 $\psi = \pi_2 \circ \phi \circ \pi_1$. 因此 ψ 是一个满射.

任取 $a \in G_{i-1}$, 我们有 $\phi(a) = \tilde{e}$ 为 $(G_{i-1}H/H)/(G_iH/H)$ 中的单位元, 当且仅当

$$\phi \circ \pi_1(a) \in (G_iH/H);$$

当且仅当

$$\pi_1(a) \in G_i(G_{i-1} \cap H),$$

当且仅当

$$a \in G_{i-1} \cap G_iH.$$

因此

$$\overline{G}_{i-1}/\overline{G}_i \cong G_{i-1}/(G_{i-1} \cap G_iH) \cong (G_{i-1}/G_i)/((G_{i-1} \cap G_iH)/G_i).$$

最后的群是一个交换群的商群, 因此也是交换的. 由此我们证明了第二点, 从而得到 G/H 也是可解的.

下边证明另一个方向. 我们假设 H 和 G/H 可解. 由 H 可解, 我们有一个次正规子群列

$$\{e\} = H_k \triangleleft \cdots \triangleleft H_0 = H,$$

满足对任意 $1 \leq i \leq k$, 有 H_{i-1}/H_i 交换.

由 G/H 可解, 我们有一个次正规子群列

$$\{\bar{e}\} = \overline{G}_l \triangleleft \cdots \triangleleft \overline{G}_0 = G/H,$$

满足对任意 $1 \leq i \leq l$, 有 $\overline{G}_{i-1}/\overline{G}_i$ 交换. 我们考虑自然同态

$$\pi : G \rightarrow G/H.$$

记 $G_i = \pi^{-1}(\overline{G}_i)$, 则对任意 $1 \leq i \leq l$, 有

- $H \triangleleft G_i$;

- $G_i \triangleleft G_{i-1}$.

因此我们有次正规子群列:

$$\{e\} \triangleleft H_k \triangleleft \cdots \triangleleft H_0 = H = G_l \triangleleft \cdots \triangleleft G_0 = G.$$

由

$$G_{i-1}/G_i \cong (G_{i-1}/H)/(G_i/H),$$

知 G_{i-1}/G_i 交换. 因此 G 可解. $\square$

我们考虑交错群 A_n . 之前我们证明了当 $n \geq 5$ 时, n -阶交错群 A_n 为单群. 由可解群的定义, 我们知道

命题 10.7.22

设自然数 $n \geq 5$, 则 n -阶交错群 A_n 不可解.

以上介绍的可解群的性质告诉我们

推论 10.7.23

设自然数 $n \geq 5$, 则 n -阶对称群 S_n 不可解.

注 10.7.24.

因此 n 次方程, 当 $n \geq 5$ 时没有根式(通)解.

有限可解群

命题 10.7.25

任取素数 p , 任意有限 p 群是一个可解群.

定理 10.7.26 (Burnside)

任取素数 p 和 q , 以及非零自然数 a 和 b , 若 G 为一个阶为 $p^a q^b$ 的群, 则 G 可解.

定理 10.7.27 (Philip Hall)

设有限群 G 的阶为 n , 若任取素数 $p \mid n$, 记 $n = p^k m$, 满足 $\gcd(p, m) = 1$, 群 G 中都有阶为 m 的子群, 则 G 可解.

定理 10.7.28 (Feit-Thompson)

所有奇数阶的有限群都是可解群.

定理 10.7.29 (Thompson)

设有限群 G 中任意两个元素 a 和 b 生成的子群都是可解群, 那么 G 可解.

10.7.2 幂零群**幂零群的定义**

记 G 为一个群, 我们考虑 G 的中心 $Z(G)$. 我们之前证明

$$Z(G) \triangleleft G.$$

进一步考虑商群 $G/Z(G)$, 我们也可以研究该群的中心:

$$Z(G/Z(G)) := \{aZ(G) \mid \forall b \in G, aZ(G)bZ(G) = bZ(G)aZ(G)\}.$$

我们记

$$Z^2(G) := \{a \in G \mid aZ(G) \in Z(G/Z(G))\}.$$

由以上定义知, 任取 $a \in G, aZ(G) \in Z(G/Z(G))$ 当且仅当对任意 $b \in G$, 我们有

$$[a, b] \in Z(G).$$

进一步, 以上条件等价于任取 $b, c \in G$, 我们有

$$[[a, b], c] = e \in G.$$

因此, 我们有

$$Z^2(G) = \{a \in G \mid \forall b \in G, [a, b] \in Z(G)\}.$$

我们可以继续考虑商群

$$(G/Z(G))/Z(G/Z(G)).$$

及其中心

$$Z((G/Z(G))/Z(G/Z(G))) := \{aZ(G)(G/Z(G)) \mid \forall bZ(G) \in G/Z(G), [aZ(G), bZ(G)] \in Z(G/Z(G))\}.$$

(这个表达比较复杂, 我们可以考虑将以上讨论中的 G 替换为 $G/Z(G)$). 我们可以进一步计算

$$[aZ(G), bZ(G)] = [a, b]Z(G) \in Z(G/Z(G)).$$

因此, 任取 $c \in G$, 我们有

$$[a, b]Z(G)cZ(G) = cZ(G)[a, b]Z(G),$$

因此

$$[[a, b], c] \in Z(G),$$

或等价地任取 $b, c, d \in G$, 我们有

$$[[[a, b], c], d] = e \in G.$$

与 $Z^2(G)$ 的讨论中的表达式比较, 我们有任取 $a \in G$,

$$aZ(G)(G/Z(G)) \in Z((G/Z(G))/Z(G/Z(G))),$$

当且仅当对任意 $b \in G$, 我们有

$$[a, b] \in Z^2(G).$$

我们定义

$$Z^3(G) := \{a \in G \mid \forall b \in G, [a, b] \in Z^2(G)\}.$$

我们可以继续重复以上讨论, 对任意 $k \in \mathbb{N}^*$, 归纳定义

$$Z^{k+1}(G) := \{a \in G \mid \forall b \in G, [a, b] \in Z^k(G)\}.$$

由定义, 我们可以直接验证以上构造的 G 的子群 $(Z^k(G))_{k \in \mathbb{N}^*}$, 满足以下关系:

$$\{e\} \subset Z(G) \subset Z^2(G) \subset \cdots.$$

我们约定 $Z^0(G) = \{e\}$.

定义 10.7.30

以上序列被称为 G 的**上升中心序列**.

定义 10.7.31

任给群 G , 若 G 的上升中心列中存在 $k \in \mathbb{N}$, 满足

$$Z^k(G) = G,$$

我们称 G 为一个**幂零群**. 此时, 最小的满足

$$Z^k(G) = G,$$

的自然数 k 称为 G 的**幂零类**.

注 10.7.32.

利用定义, 我们先观察幂零类比较小的群 G 的性质:

- (i) G 的幂零类为 0 当且仅当 $G = \{e\}$.
- (ii) G 的幂零类为 1 当且仅当 G 为非平凡交换群.
- (iii) G 的幂零类为 2 当且仅当 $G/Z(G)$ 交换, 我们称此类群为**亚交换群** (metabelian group).

设 G 为一个群, $Z(G)$ 为 G 的中心. 我们有以下短正合列:

$$1 \rightarrow Z(G) \rightarrow G \rightarrow G/Z(G) \rightarrow 1.$$

因此 G 是 $G/Z(G)$ 的中心扩张.

我们下一步考虑对 $Z^2(G)$ 做类似地的讨论. 我们首先证明以下引理

引理 10.7.33

群 $Z^2(G)$ 为 G 的正规子群, 且

$$G/Z^2(G) \cong (G/Z(G))/Z(G/Z(G)).$$

证明. 由群同态基本定理. 自然同态

$$\pi: G \rightarrow G/Z(G),$$

给出了 G 中包含 $Z(G)$ 的正规子群与 $G/Z(G)$ 中正规子群的双射. 由之前关于 $Z^2(G)$ 的讨论, 我们知道

$$\pi^{-1}(Z(G/Z(G))) = Z^2(G),$$

因此 $Z^2(G)$ 是 G 的正规子群, 且

$$G/Z^2(G) \cong (G/Z(G))/Z(G/Z(G)).$$

□

因此我们有以下短正合列:

$$1 \rightarrow Z^2(G)/Z(G) \rightarrow G/Z(G) \rightarrow G/Z^2(G) \rightarrow 1.$$

群 $G/Z(G)$ 是 $G/Z^2(G)$ 的中心扩张.

任给一个群 H , 我们都可以考虑 H 到商群 $H/Z(H)$ 的自然同态. 为了避免叙述过于复杂, 对任意群 H , 我们都用 π 来记这个自然同态. 考虑 G 的上升中心列中的群 $Z^i(G)$ 的定义, 我们有:

引理 10.7.34

记 $k \in \mathbb{N} \setminus \{0\}$. 设 G 为一个幂零类为 k 的幂零群, 则任取 $0 \leq i \leq k$, 我们有

$$\ker \pi^i = Z^i(G).$$

这里 π^i 是对一个群取 i 次关于其中心的商群.

利用这个引理, 重复以上讨论, 我们可以证明以下命题

命题 10.7.35

记 $k \in \mathbb{N} \setminus \{0\}$. 设 G 为一个幂零类为 k 的幂零群, 则任取 $0 \leq i \leq k-1$, 我们有以下短正合列

$$1 \rightarrow Z^{i+1}(G)/Z^i(G) \rightarrow G/Z^i(G) \rightarrow G/Z^{i+1}(G) \rightarrow 1.$$

且

$$Z^{i+1}(G)/Z^i(G) \cong Z(G/Z^i(G)).$$

注 10.7.36.

由以上命题知 $G/Z^i(G)$ 是 $G/Z^{i+1}(G)$ 关于 $Z^{i+1}(G)/Z^i(G)$ 的中心扩张. 因此 G 是 e 依次过

$$Z^k(G)/Z^{k-1}(G), Z^{k-1}(G)/Z^{k-2}(G), \dots, Z^2(G)/Z(G), Z(G),$$

中心扩张得到的. 详细一点, 我们有

- $\{e\} = G/Z^k(G)$ 过 $Z^k(G)/Z^{k-1}(G)$ 的中心扩张是 $G/Z^{k-1}(G)$,
- $G/Z^{k-1}(G)$ 过 $Z^{k-1}(G)/Z^{k-2}(G)$ 的中心扩张是 $G/Z^{k-2}(G)$,
- $\dots$,
- $G/Z(G)$ 过 $Z(G)/Z^0(G) = Z(G)$ 的中心扩张是 G .

这里群相等都是在同构意义下.

设 G 为一个群. 我们考虑 G 的上升中心序列

$$\{e\} \triangleleft Z(G) \triangleleft Z^2(G) \triangleleft \dots$$

引理 10.7.37

对任意 $i \in \mathbb{N}$, 任取 $a \in (G)$, 我们有 $a \in Z^i(G)$, 当且仅当对任意 $b_1, \dots, b_i \in G$,

$$[\dots [[a, b_1], b_2], \dots, b_i] = e.$$

命题 10.7.38

设 G 为一个非平凡群. 群 G 为幂零群, 当且仅当存在 $l \in \mathbb{N} \setminus \{0, 1\}$, 对任意 $a_1, \dots, a_l \in G$, 我们有

$$[\dots [[a_1, a_2], a_3], \dots, a_l] = e.$$

证明. 注意到 G 为幂零群, 当且仅当存在 $k \in \mathbb{N}^*$, 满足 $G = Z^k(G)$. 另一方面, 任取 $a \in G$, 我们有 $a \in Z^k(G)$ 当且仅当对任意 $b_1, \dots, b_k \in G$, 满足

$$[\dots [[a, b_1], b_2], \dots, b_k] = e.$$

令 $l = k + 1$, 命题得证. □

以上命题启发我们也可以使用换位子来给出幂零群的一个等价定义. 我们归纳定义如下—列 G 的子群:

$$\begin{aligned} G^0 &= G \\ G^1 &= [G, G] \\ G^2 &= [G, G^1] \\ &\dots \\ G^{k+1} &= [G, G^k] \\ &\dots \end{aligned}$$

由定义看出, 这些群满足如下包含关系:

$$G^0 > G^1 > \dots > G^k > \dots$$

定义 10.7.39

以上序列被称为 G 的**下降中心序列**.

利用之前的讨论, 我们有幂零群的另一个定义.

定义 10.7.40

若群 G 的下降中心序列中, 存在 $k \in \mathbb{N}$, 满足 $G^k = \{e\}$, 则 G 为**幂零群**.

我们将这个定义与可解群的定义比较, 可得如下直接的推论.

推论 10.7.41

若群 G 是幂零群, 则 G 为可解群.

注 10.7.42.

我们将之前讨论过的特殊的群的概念放在一起做一个比较:

$$\text{循环群} \subset \text{交换群} \subset \text{幂零群} \subset \text{可解群} \subset \text{群}.$$

注 10.7.43.

任给一个群 G , 以及元素 $a \in G$, 我们可以定义 a 在 G 上如下的作用

$$\begin{aligned} \text{ad}_a : G &\rightarrow G \\ b &\mapsto [a, b] \end{aligned}$$

若 G 是一个幂零群, 则存在 $k \in \mathbb{N}^*$, 满足

$$(\text{ad}_a)^k = \iota,$$

这里 ι 是将 G 中所有元素都送到 e 的映射.

命题 10.7.44

设 k 为一个非零自然数. 设 G 为一个幂零类为 k 的幂零群. 则 k 是最小的令 $Z^k(G) = G$ 的自然数, 也是最小的令 $G^k = \{e\}$ 的自然数. 我们进一步有对任意 $0 \leq i \leq k-1$,

$$Z^i(G) < G^{k-i-1} < Z^{i+1}(G).$$

证明. 使用定义直接验证即可. □

注 10.7.45.

例如 $i = 0$, 我们有

$$\{e\} < G^{k-1} < Z(G).$$

第二个包含关系可以使用中心的定义, 以及幂零群的幂零类的定义直接验证.

例 10.7.46.

我们考虑对角线上元素都为 1 的实系数上三角矩阵群

$$G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| a, b, c \in \mathbb{R} \right\}.$$

任取两个元素

$$A_1 = \begin{bmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{bmatrix}$$

它们的逆分别为

$$A_1^{-1} = \begin{bmatrix} 1 & -a_1 & -b_1 + a_1 c_1 \\ 0 & 1 & -c_1 \\ 0 & 0 & 1 \end{bmatrix}, \quad A_2^{-1} = \begin{bmatrix} 1 & -a_2 & -b_2 + a_2 c_2 \\ 0 & 1 & -c_2 \\ 0 & 0 & 1 \end{bmatrix}$$

我们计算它们的换位子

$$\begin{aligned} & [A_1, A_2] \\ &= \begin{bmatrix} 1 & -a_1 & -b_1 + a_1 c_1 \\ 0 & 1 & -c_1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -a_2 & -b_2 + a_2 c_2 \\ 0 & 1 & -c_2 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & -a_1 - a_2 & -b_1 - b_2 + a_1 c_1 + a_2 c_2 + a_1 c_2 \\ 0 & 1 & -c_1 - c_2 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a_1 + a_2 & b_1 + b_2 + a_1 c_2 \\ 0 & 1 & c_1 + c_2 \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & a_1 c_1 + a_2 c_2 - (a_1 + a_2)(c_1 + c_2) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & -a_1 c_2 - a_2 c_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{aligned}$$

因此

$$G^1 = [G, G] = \left\{ \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \middle| a \in \mathbb{R} \right\}.$$

我们可以直接计算验证, $[G, G] = Z(G)$. 因此 $G^2 = \{e\}$, 群 G 为幂零群.

另一方面, $G/Z(G)$ 交换, 因此 $Z^2(G) = G$.

我们使用类似于关于导出列是正规列的证明, 也可以得到以下结果.

命题 10.7.47

任给一个群 G , 其下降中心序列是一个正规列.

幂零群的性质

命题 10.7.48

令 G 为一个幂零群. 任取 G 的子群 H , 以及 G 的正规子群 N , 则

- (i) H 为幂零群.
- (ii) G/N 为幂零群.

与可解群不同的是, G/N 和 N 都是幂零群不一定可以有 G 是幂零群. 这个结论只在 $N < Z(G)$ 时成立. 我们有以下结果:

命题 10.7.49

记 G 为一个群, N 为 G 的中心的一个正规子群, 若 G/N 是一个幂零类为 m 的幂零群, 则 G 是一个幂零类小于等于 $m+1$ 的幂零群.

推论 10.7.50

任取素数 p , 任意 p 群 G 都是幂零群.

有限幂零群

定理 10.7.51

令 G 为一个有限群. 以下叙述等价:

- (i) G 是一个幂零群.
- (ii) G 的所有真子群 H 都是其正规化子的真子群:

$$H \subsetneq N_G(H) := \{a \in G \mid aHa^{-1} = H\}.$$

- (iii) G 中所有 Sylow 子群都是正规子群.
- (iv) G 是其 Sylow 子群的直积.

第十一章 自由群

我们将从群的生成的角度来考虑群. 本节中我们将只讨论有限生成的自由群. 记 G 是一个有限生成群, 并称呼 G 的运算为乘积. 记 $n \in \mathbb{N}^*$. 设

$$\{a_1, \dots, a_n\} \subset G,$$

为 G 的一个生成元集, 即

$$G = \{b_1 \cdots b_m \mid m \in \mathbb{N}^*, b_1, \dots, b_m \in \{a_1^{\pm 1}, \dots, a_n^{\pm 1}\}\}.$$

这里只说明 G 的所有元素可以表达为

$$\{a_1^{\pm 1}, \dots, a_n^{\pm 1}\},$$

中的元素的有限乘积. 我们并没有关系这种表达是否是唯一的. 以下是一个很简单的例子:

$$a_1 = a_1 a_2 a_2^{-1}.$$

这里表达不唯一的原因是元素 a_2 和 a_2^{-1} 有一个"关系":

$$a_2 a_2^{-1} = e,$$

也即么元的表达不唯一.

当然以上给出的元素之间的关系在每个群中都会出现的, 这是逆元的定义. 取一个一般的群, 我们可能有其他的关系出现. 例如, 任取奇素数 p , 考虑乘法群 $\mathbb{Z}_p^*$, 由 Lagrange 定理, 我们有

$$\overline{2}^{p-1} = \overline{1}.$$

而 $a^{p-1} = e$ 并不是每个群中的元素都会满足的. 另一个大家熟悉的例子就是交换群. 记 G 为一个交换群, 任取 $a, b \in G$, 我们有 $ab = ba$. 但这个并不是任意一个群都满足的. 通过以上讨论, 我们可以考虑以下两个问题:

- (i) 如果我们确定生成元的数目, 并且只要求一些必要的关系, 比如: 么元 e 与任意元素交换, 任意元素与其逆交换, 且相乘得到么元, 这样得到的群是不是唯一的?
- (ii) 如果 G 和 H 是由相同数目的生成元生成的, 通过研究生成元之间的关系, 我们是否可以得到 G 和 H 之间的关系? 例如, 是否存在一个从 G 到 H 的满同态等等.

11.1 自由群的定义

我们首先考虑第一个问题. 实际上这个问题的答案是肯定的, 如果我们考虑 $n \in \mathbb{N}^*$ 个元素生成的群, 且元素之间的关系只有群定义要求的关系, 则得到的群在同构意义下是唯一的, 被称为 n -元自由群. 我们下边给出更详细的说明.

记 $n \in \mathbb{N}^*$. 记

$$A = \{a_1, \dots, a_n\},$$

为 n 个字符的集合. 考虑另一个集合

$$A^{-1} = \{a_1^{-1}, \dots, a_n^{-1}\}.$$

任取 $k \in \mathbb{N}^*$, 我们称

$$a_{i_1}^{\epsilon_1} \cdots a_{i_k}^{\epsilon_k},$$

为一个**词**, 其中对任意 $1 \leq j \leq k$, $\epsilon_j \in \{1, -1\}$.

我们称一个词

$$a_{i_1}^{\epsilon_1} \cdots a_{i_k}^{\epsilon_k},$$

是**不可约的**, 若任取 $1 \leq j \leq k-1$, 我们有

$$a_{i_j}^{-\epsilon_j} \neq a_{i_{j+1}}^{\epsilon_{j+1}}.$$

我们记

$$F_n = \{e\} \cup \{\text{不可约词}\},$$

其中 e 为**空词**不同于任意一个不可约词, 且不可约词两两不同.

注 11.1.1.

如果觉得词的定义比较怪, 我们也可以考虑 $\{e\} \cup A \cup A^{-1}$ 中元素的无穷序列, 每个词都是一个序列

$$(a_{i_1}^{\epsilon_{i_1}}, a_{i_2}^{\epsilon_{i_2}}, \dots, a_{i_k}^{\epsilon_{i_k}}, e, e, \dots),$$

不可约词就是相邻两个位置上的元素如果不是 e 需要满足

$$a_{i_j}^{-\epsilon_{i_j}} \neq a_{i_{j+1}}^{\epsilon_{i_{j+1}}}.$$

空词就是

$$(e, e, \dots).$$

这样当我们考虑 F_n 是 $\{e\} \cup A \cup A^{-1}$ 中元素的无穷序列的集合的子集时, 比较每个位置上的元素, 我们就有两个不同的不可约词是不同的元素.

我们下边在 F_n 上定义一个运算. 该运算共分两步. 任取 $w_1, w_2 \in F_n$, 首先我们把 w_2 接在 w_1 后边构成一个新的词. 第二步, 我们将 $w_1 w_2$ 化简, 即在词 $w_1 w_2$ 中, 相邻两个字母若是 $a_i a_i^{-1}$ 或 $a_i^{-1} a_i$, 我们就将其去掉, 这个过程可能需要重复多次. 若最后没有字母剩下, 我们记

$$w_1 w_2 = e,$$

否则, 我们得到一个不可约词 w . 定义 $w_1 w_2 = w$.

例 11.1.2.

考虑 $n = 5$, 记

$$w_1 = a_1 a_3 a_2 a_4, \quad w_2 = a_4^{-1} a_2^{-1} a_3 a_5,$$

则

$$a_1 a_3 a_2 \textcolor{red}{a_4 a_4^{-1}} a_2^{-1} a_3 a_5 \longrightarrow a_1 a_3 \textcolor{red}{a_2 a_2^{-1}} a_3 a_5 \longrightarrow a_1 a_3 a_3 a_5$$

我们定义

$$w_1 w_2 = a_1 a_3 a_3 a_5.$$

定义 11.1.3

集合 F_n 关于以上运算构成的群被称为由 $A = \{a_1, \dots, a_n\}$ 生成的 n -元自由群. 我们称 n 为 F_n 的阶.

注 11.1.4.

有时人们为了将其与 $\mathbb{Z}^n$ 区分称 F_n 为 n -元非交换自由群.

11.2 自由群的泛性质

我们沿用之前的记号. 自由群 F_n 的另一种定义方法是利用其泛性质达到的. 具体叙述如下:

定理 11.2.1

任取一个群 G , 记其中 n 个元素 $u_1, \dots, u_n$ (可以重复) 生成的子群为 H , 则存在唯一的一个群满同态

$$\phi : F_n \rightarrow H,$$

满足任取 $1 \leq i \leq n$, 都有 $\phi(a_i) = u_i$.

证明. 我们只需要验证 ϕ 是一个映射. 这是由 $a_1, \dots, a_n$ 的不可约词两两不同来保证的. $\square$

换句话说, 任意群中 n 个元素生成的子群都可以看作是 F_n 的一个商群. 我们有如下交换图

$$\begin{array}{ccc} F_n & \xrightarrow{\phi} & H \\ \pi \downarrow & \nearrow \bar{\phi} & \\ F_n / \ker \phi & & \end{array}$$

其中 $\bar{\phi}$ 是一个群同构.

注 11.2.2.

这里实际上和教材中自由模的定义一样, 我们也可以使用泛性质来定义自由群. 不过由于是用性质给出的定义, 我们需要说明这样的群确实存在, 即满足泛性质的群的集合不是空集. 而第一节构造出来的群就说明确实存在满足以上泛性质的群.

11.3 自由基

我们沿用之前的记号, 考虑

$$A' = \{a_1 a_2, a_2, \dots, a_n\} \subset F_n.$$

注意到

$$a_1 = (a_1 a_2) a_2^{-1} \in \langle A' \rangle.$$

因此

$$F_n = \langle A' \rangle.$$

这里注意到如果我们记

$$b_1 = a_1 a_2, b_2 = a_2, \dots, b_n = a_n,$$

为新的字母, 重复之前利用不可约词构造群, 我们可以得到一个群 F . 利用以上 $b_1, \dots, b_n$ 和 $a_1, \dots, a_n$ 的关系, 我们可以构造一个群同态

$$\psi : F \rightarrow F_n.$$

注意到这是一个满同态 ($a_1 = \psi(b_1 b_2^{-1})$). 另一方面, 利用 F_n 的泛性质, 我们有

$$\phi : F_n \rightarrow F,$$

满足任取 $1 \leq i \leq n$, 有 $\phi(a_i) = b_i$.

注意到任取 $1 \leq i \leq n$, 有 $\phi \circ \psi(b_i) = b_i$. 因此 ψ 为单同态. 综上所述 ψ 同构.

因此我们有 A' 生成 F_n , 并且 $b_1, \dots, b_n$ 构成的不可约词两两不同.

定义 11.3.1

记 $nm \in \mathbb{N}^*$. 任取 F_n 中 m 个元素 $c_1, \dots, c_m$, 满足

- $F_n = \langle c_1, \dots, c_m \rangle$,
- $c_1, \dots, c_m$ 的不可约词是 F_n 中的非幺元,

我们称 $\{c_1, \dots, c_m\}$ 为 F_n 的一组**自由基**.

例 11.3.2.

之前讨论过的 A 和 A' 都是 F_n 的一组自由基.

一个自然的问题就是 F_n 中自由基中元素的个数是不是总是 n .

定理 11.3.3

记 X 为 F_n 的一个自由基, 则有 $|X| = n$.

证明. 我们可以考虑 F_n 到 $\mathbb{Z}_2$ 的同态. 我们考虑自由基 $\{a_1, \dots, a_n\}$, 则任取

$$\phi : F_n \rightarrow \mathbb{Z}_2,$$

都由

$$\phi(a_1), \dots, \phi(a_n) \in \mathbb{Z}_2,$$

的取值决定. 另一方面, 利用泛性质, 我们知道任取 $u_1, \dots, u_n \in \mathbb{Z}_2$, 都有一个群同态

$$\phi : F_n \rightarrow \mathbb{Z}_2,$$

满足

$$\phi(a_1) = u_1, \dots, \phi(a_n) = u_n.$$

因此 F_n 到 $\mathbb{Z}_2$ 的群同态的集合满足

$$|\text{Hom}(F_n, \mathbb{Z}_2)| = 2^n.$$

任取 X 为 F_n 的自由基, 考虑 X 中元素生成的自由群 F_X , 有自由基的性质我们知道 F_X 和 F_n 同构. 重复以上讨论, 我们有

$$|\text{Hom}(F_n, \mathbb{Z}_2)| = |\text{Hom}(F_X, \mathbb{Z}_2)| = 2^{|X|}.$$

因此 $|X| = n$. □

11.4 群的表达

我们考虑 F_n 的泛性质. 任取群 G 中的 n 个元素 $u_1, \dots, u_n$, 考虑群同态

$$\phi: F_n \rightarrow H = \langle u_1, \dots, u_n \rangle,$$

满足任取 $1 \leq i \leq n$, 都有 $\phi(a_i) = u_i$. 由群同态基本定理我们有

$$\begin{array}{ccc} F_n & \xrightarrow{\phi} & H \\ \pi \downarrow & \nearrow \bar{\phi} & \\ F_n / \ker \phi & & \end{array}$$

其中 $\bar{\phi}$ 是一个群同构. 任意非幺元 $w \in \ker \phi$ 都是一个不可约词

$$w = a_{i_1}^{\epsilon_1} \cdots a_{i_k}^{\epsilon_k}.$$

因此在 H 中, 我们有

$$u_{i_1}^{\epsilon_1} \cdots u_{i_k}^{\epsilon_k} = e_G.$$

因此我们可以将群 H 看作是现有 $u_1, \dots, u_n$ 自由生成, 然后商掉一个包含某些 $u_1, \dots, u_n$ 不可约词的正规子群得到的. 详细一点地说, 我们首先将 $u_1, \dots, u_n$ 看做是字母, 考虑 H_n 为通过考虑这个字母的不可约词构成的群. 我们考虑群同态

$$\psi: F_n \rightarrow H_n,$$

满足任取 $1 \leq i \leq n$, 都有 $\psi(a_i) = u_i$, 则 ψ 是一个同构. 我们考虑 $\psi(\ker \phi) = N \triangleleft H_n$. 通过之前的讨论, 我们有

$$H \cong F_n / N.$$

正规闭包

我们可以通过比较生成元和生成关系 (n 以及 N) 来比较两个群是否同构. 当我们试图比较 F_n 中两个子群 N_1 和 N_2 的时候, 我们并不需要比较所有元素, 而只需要去看其中的"生成元"即可. 但是这里注意到我们想要比较的群都是 F_n 的正规子群, 因此我们这里需要考虑的是一个集合的正规闭包 (生成的正规子群).

设 G 为一个群.

定义 11.4.1

任取非空子集 $S \subset G$, 我们称

$$\langle\langle S \rangle\rangle := \bigcap \{N \triangleleft G \mid S \subset N\},$$

为 S 生成的正规子群, 或者是 S 的正规闭包.

注 11.4.2.

注意到任取 $N_1, N_2 \triangleleft G$, 我们有 $N_1 \cap N_2 \triangleleft G$. 这个结论对任意多个 G 的正规子群也成立. 因此以上定义良好.

之前我们讨论过集合生成的子群两种理解方式, 这里我们也可以从另一个角度来理解正规闭包. 任取 $a \in G$, 我们记 $[a]$ 为 a 在 G 中的共轭类. 任取 G 的非空子集 S , 我们记

$$[S] := \cup\{[a] \mid a \in S\}.$$

命题 11.4.3

任取 G 的非空子集 S , 则 S 的正规闭包满足

$$\langle\langle S \rangle\rangle = \{a_1 \cdots a_k \mid k \in \mathbb{N}^*, a_1, \dots, a_k \in [S] \cup [S^{-1}]\}.$$

注 11.4.4.

换句话说, $\langle\langle S \rangle\rangle$ 可以看作是 S 中的元素的共轭类的并集生成的 G 的子群. 以上命题的证明过程和关于子群生成的讨论中类似结论的证明相似.

记 $R \subset N$ 为一组正规生成 N 的元素, 即

$$N = \langle\langle R \rangle\rangle.$$

我们将 $u_1, \dots, u_n$ 看作符号, 将这些符号生成的 n -元自由群记作 $F(u_1, \dots, u_n)$. 任取 N 中的元素 w , 我们记 $w(u_1, \dots, u_n)$ 为将 $a_1, \dots, a_n$ 替换为 $u_1, \dots, u_n$ 得到的 $F(u_1, \dots, u_n)$ 中的词, 我们可以记

$$H = \langle u_1, \dots, u_n \mid R(u_1, \dots, u_n) \rangle = F(u_1, \dots, u_n) / \langle\langle R(u_1, \dots, u_n) \rangle\rangle,$$

称之为 H 的一个**表达**. 若进一步有 $|R| < \infty$, 我们称之为 H 的一个**有限表达**.

例 11.4.5.

四元数群 Q_8 有如下表达

$$Q_8 = \langle a, b \mid a^4, b^4, a^2b^2, abab^{-1} \rangle.$$

这个例子告诉我们群的表达不唯一.

例 11.4.6.

3-元置换群 S_3 有如下表达

$$S_3 = \langle a, b \mid a^2, b^3, abab \rangle.$$

例 11.4.7.

正四边形的二面体群 D_4 有如下表达

$$D_4 = \langle r, s \mid r^4, s^2, sr sr \rangle.$$

例 11.4.8.

二阶交换自由群 $\mathbb{Z}^2$ 有如下表达

$$\mathbb{Z}^2 = \langle a, b \mid aba^{-1}b^{-1} \rangle.$$

11.5 群的表达的可视化

当从生成的角度来考虑群的时候, 我们可以利用 Cayley 图将群可视化, 从而方便对其结构的研究.

记 G 为一个群, 非空不含幺元的子集 S 为 G 的一组生成元. 我们通常要求 S 关于求逆运算对称, 即 $S = S^{-1}$.

定义 11.5.1

群 G 关于生成元集 S 的 Cayley 图是一个图 $\Gamma(G, S) = (V, E)$, 其中

- 点集 $V = G$ 是 G 中的元素,
- 任取 $w, w' \in G$, 存在一个边连接 w 和 w' 当且仅当 $w' = ws$, 其中 $s \in S$.

一个边连接两个点的条件实际上反映的就是生成的过程. 任取 G 的一个元素 w , 我们都可以将其写成 S 中有限多个元素的乘积

$$w = a_1 \cdots a_k.$$

我们考虑写的过程, 则有

$$e \text{ --- } a_1 \text{ --- } a_1 a_2 \text{ --- } a_1 a_2 a_3 \text{ --- } \cdots \text{ --- } (a_1 a_2 \cdots a_k).$$

因此 w 的一种写法就可以给出 $\Gamma(G, S)$ 的一个从幺元 e 出发的道路. 当这个写法是 S 中元素作为字符的不可约词的时候, 这个道路是"最简的"(作为一个图, 没有度 (valence) 为 1 的点).

我们这里给出几个例子.

例 11.5.2.

令 $G = \mathbb{Z}_2$, 记 $S = \{-1\}$, 则有

$$1 \text{ --- } -1$$

注意到 -1 的逆就是 -1 . 有时我们观察 Cayley 图的时候会看到双线, 此时反映的是所乘元素为 2 阶. 有时如果所有生成元都是 2 阶, 我们会用单线连接.

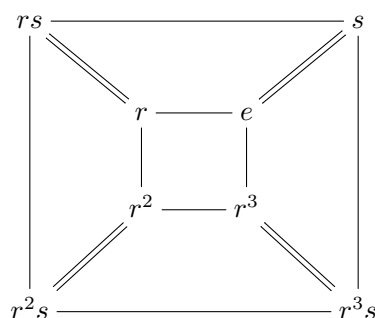
例 11.5.3.

令 $G = D_4$. 记平面上正方形四个顶点分别为

$$v_1 = (1, 1), v_2 = (-1, 1), v_3 = (-1, -1), v_4 = (1, -1).$$

记 s 为固定过 v_1 和 v_3 的直线的平面的反射, r 为将 (v_1, v_2, v_3, v_4) 送到 (v_2, v_3, v_4, v_1) 的平面的旋转.

记 $S = \{s, r, r^{-1} = r^3\}$, 则有

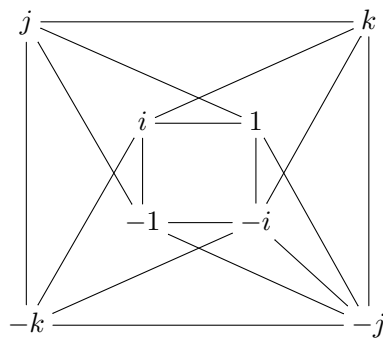


例 11.5.4.

令 $G = Q_8$. 考虑生成元组

$$S = \{\pm i, \pm j\},$$

则有



我们下边假设 G 由 n 个元素生成, 且

$$S = \{a_1^\pm, \dots, a_n^\pm\}.$$

当 w 有多种写法的时候, 我们就会有多种道路来连接 e 和 w . 如果是两个不同的写法, 则通过将两个道路合并, 我们可以在 $\Gamma(G, S)$ 上找到一个回路, 也即 e 的一个非平凡写法. 这个回路对应的 $a_1, \dots, a_n$ 的不可约词就在满同态

$$\phi: F_n \rightarrow G,$$

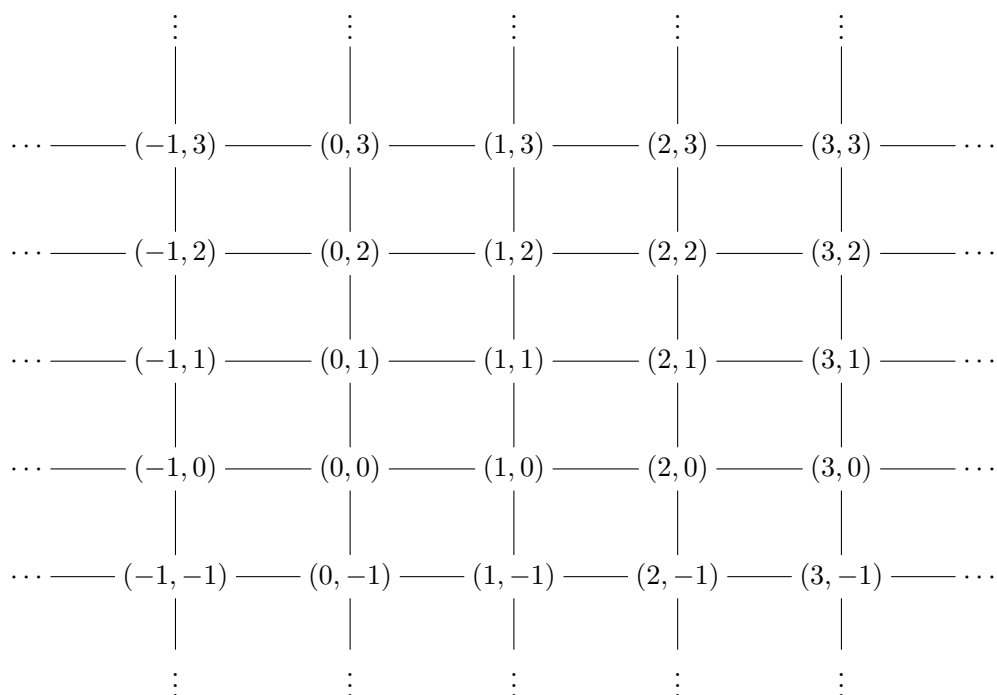
的核中.

 $\mathbb{Z}^2$ 的 Cayley 图

我们下边以 $\mathbb{Z}^2$ 为一个例子来说明. 我们考虑

$$S = \{(1, 0), (-1, 0), (0, 1), (0, -1)\},$$

则 $\mathbb{Z}^2$ 关于这组生成元的 Cayley 图如下



注意到这是一个无限图. 考虑之前 $\mathbb{Z}^2$ 的表达. 我们考虑自由群

$$F_2 = \langle a, b \rangle.$$

考虑群同态

$$\phi : F_2 \rightarrow \mathbb{Z}^2,$$

满足

$$\phi(a) = (1, 0), \phi(b) = (0, 1).$$

我们希望借助上图来说明

$$\ker \phi = N(aba^{-1}b^{-1}).$$

注意到任取 $w \in F_2$, 我们可以将其写为 a, b, a^{-1}, b^{-1} 的词,

$$w = w(a, b).$$

我们进一步有 $w \in \ker \phi$ 当且仅当

$$w((1, 0), (0, 1)) = (0, 0),$$

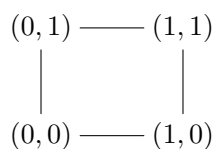
也即 $w(a, b)$ 所对应的从 e 出发的道路是一个回路.

当我们说

$$\ker \phi = N(aba^{-1}b^{-1}),$$

我们将看到所有的回路都可以分解成 $aba^{-1}b^{-1}$ 及其共轭对应的回路的"和".

首先考虑 $aba^{-1}b^{-1}$ 对应的回路



注意到这个关系说明生成元之间交换, 因此 $\mathbb{Z}^2$ 是一个交换群.

注意到在 $\mathbb{Z}^2$ 中任意一个回路所包含的区域都可以分解为如下类型的小正方形

$$\begin{array}{ccc} (p, q+1) & \text{---} & (p+1, q+1) \\ | & & | \\ (p, q) & \text{---} & (p+1, q) \end{array}$$

实际上这种小正方形对应的正是 $aba^{-1}b^{-1}$ 共轭所对应的回路. 例如我们可以考虑如下的回路

$$\begin{array}{ccc} (p, q+1) & \text{---} & (p+1, q+1) \\ | & & | \\ (p, q) & \text{---} & (p+1, q) \\ | & & \\ \vdots & & \\ | & & \\ (0, 0) & \text{---} \cdots \text{---} & (p, 0) \end{array}$$

即

$$w = (a^p b^q) aba^{-1} b^{-1} (b^{-q} a^{-p}).$$

这里我们可能会注意到, 在构造这样的共轭元素的时候, 我们只需要找到一个道路连接 $(0, 0)$ 和 (p, q) 即可, 因此构造这样回路的方法并不唯一. 利用这个方法, 我们就可以将任意一个回路分成一些 $aba^{-1}b^{-1}$ 的共轭类中元素的乘积. 例如我们考虑以下回路

$$\begin{array}{ccc} (0, 2) & \text{---} & (1, 2) \\ | & & | \\ (0, 1) & & (1, 1) \\ | & & | \\ (0, 0) & \text{---} & (1, 0) \end{array}$$

如果我们考虑沿逆时针方向走一圈, 所对应的元素是

$$abba^{-1}b^{-1}b^{-1}.$$

通过在中途回到 $(0, 0)$ 再出发, 我们可以将以上回路分成两段

$$\begin{array}{ccc} (0, 1) & \text{---} & (1, 1) \\ | & & | \\ (0, 0) & \text{---} & (1, 0) \end{array} \quad \begin{array}{ccc} (0, 2) & \text{---} & (1, 2) \\ | & & | \\ (0, 1) & \text{---} & (1, 1) \\ | & & \\ & & (0, 0) \end{array}$$

分别对应的 F_2 中不可约词是 $aba^{-1}b^{-1}$ 和 $baba^{-1}b^{-1}b^{-1}$.

因此我们有

$$abba^{-1}b^{-1}b^{-1} = (aba^{-1}b^{-1})(baba^{-1}b^{-1}b^{-1}).$$

注 11.5.5.

Cayley 图的一个用途就是可以帮我们在 G 上定义一个距离. 我们可以设每个边的长度为 1, G 是一个连通图, 任意两个元素之间都有道路相连, 我们考虑所有道路长度的最小值就是两个元素之间的距离. 如果两个元素之间的距离很大, 就说明相对于这组生成元, 这两个元素"很不同". 这样我们就可以从几何的角度来考虑群, 从而可以利用一些几何中的结论来研究群, 这就进入了几何群论的领域.

第十二章 群的构造

课程中我们已经介绍了群的直积和半直积, 用来从已有的群构造出新的群. 在这个附录中, 我们介绍另外几种从已有的群出发构造新的群的方法.

12.1 群的自由积 Free Product

在前一个附录中, 我们讨论了自由群, 也即生成元之间除了必要的群定义给出的关系外没有任何其他关系的群. 我们利用"元素之间没有关系"这个概念来构造群的自由积. 笼统地说, 我们想用两个群生成一个新的群, 两个群的并集可以看作是新群的生成元集, 不同群中的元素之间没有关系. 在对自由群的讨论中, 我们使用了两种方法来说明"元素之间没有关系"这件事. 一种是考虑不可约词, 另一种就是考虑泛性质. 这里我们也可以使用类似的方法定义两个群的自由积.

记 G 和 H 为两个群, 且都非平凡群 $\{e\}$. 我们将 $G \cup H$ 中的非幺元看作是字母, 任取 $k \in \mathbb{N}^*$, 称如下形式的元素

$$\begin{aligned} g_1 h_1 \cdots g_k h_k, \\ g_1 h_1 \cdots h_{k-1} g_k, \\ h_1 g_1 \cdots h_k g_k, \\ h_1 g_1 \cdots g_{k-1} h_k. \end{aligned}$$

为一个词.

我们记

$$G * H := \{e\} \cup \{\text{词}\}.$$

和定义自由群中的运算一样, 我们分两步定义: 任取 $w_1, w_2 \in G * H$, 且不同于 e , 我们首先将两个词拼接起来的到一个 G 和 H 中元素构成的序列, 如果 w_1 作为词的最后一个字母与 w_2 作为词的最后一个字母属于不同的群 (不都在 G 中或者不都在 H 中), 则所得的就是 $w_1 w_2$ 对应的词, 否则我们不妨设

$$w_1 = g_1 h_1 \cdots g_k h_k, \quad w_2 = h'_1 g'_1 \cdots h'_k g'_k.$$

我们考虑

$$g_1 h_1 \cdots g_k h_k h'_1 g'_1 \cdots h'_k g'_k.$$

若 $h_k h'_1 = e_H$, 我们将其消掉得到

$$g_1 h_1 \cdots h_{k-1} g_k g'_1 h'_2 \cdots h'_k g'_k$$

若 $g_k g'_1 = e_G$, 我们将其消掉得到

$$g_1 h_1 \cdots h_{k-1} h'_2 \cdots h'_k g'_k$$

重复以上过程.

若最终没有元素剩下, 我们就记

$$w_1 w_2 = e,$$

同时我们可以验证根据以上规则, 有

$$w_2 w_1 = e.$$

若不是所有元素都被消掉, 则剩下的元素给出一个词 w , 我们定义

$$w_1 w_2 = w.$$

此外, e 与其它词 w 的运算规则为

$$ew = we = w.$$

命题 12.1.1

集合 $G * H$ 关于以上定义的运算构成群.

定义 12.1.2

群 $G * H$ 被称为 G 和 H 的**自由积**.

注 12.1.3.

我们有 $H * G = G * H$. 我们可以将 G 和 H 看作 $G * H$ 的子群.

注 12.1.4.

利用以上构造, 我们可以得到任意多个群的自由积.

考虑前一个附录中讨论的概念自由群. 取 $A = \{a\}$, 记

$$F(a) = \{a^n \mid n \in \mathbb{Z}\},$$

为 a 生成的自由群.

记任取 $n \in \mathbb{N} \setminus \{0, 1\}$, 我们记

$$A = \{a_1, \dots, a_n\}$$

生成的自由群为 F_n .

命题 12.1.5

沿用以上记号, 我们有

$$F_n = F(a_1) * \dots * F(a_n).$$

群的自由积具有某种泛性质. 我们仍考虑两个群的自由积. 记 G 和 H 为两个群.

12.3 群的 HNN 扩张 HNN extension

这类构造群的方法由 Graham Higman, Bernhard Neumann, and Hanna Neumann, 在1949年的一篇文章 Embedding Theorems of Groups 中介绍的, HNN 是三位作者的姓的首字母.

之前的构造都是从多个群出发来构造一个群. 这里我们希望做的是在一个群 G 内部, 通过向群中添加一个元素 t 把 G 中的两个子群联系起来, 从而得到一个新的群. 具体的操作如下.

任取 H 和 G 为两个群, 设存在两个群的同态

$$\phi_1 : H \rightarrow G, \quad \phi_2 : H \rightarrow G.$$

我们记 t 为一个字符, 考虑 t 生成的自由群为 $F(t)$, 我们考虑自由积 $G * F(t)$. 在其中我们考虑

$$S = \{t\phi_1(a)t^{-1}\phi_2(a)^{-1} \mid a \in H\}.$$

定义 12.3.1

群 G 通过 ϕ_1 和 ϕ_2 关于 H 的 HNN 扩张为以下商群

$$G * F(t) / \langle\langle S \rangle\rangle.$$

我们通常记作 ${}^*_H G$.

12.4 群图

我们已经介绍了几种不同的构造新的群的方法. 实际操作中, 我们可以将这些操作混合起来, 从几个群出发来构造一个新的群出来. 在某些较好的情况下, 在同构意义下, 这些构造先后顺序是可以互换的. 例如, 我们考虑 G_1, G_2 和 G_3 三个群, 我们考虑 G_1 和 G_2 的自由群得到

$$G_1 * G_2,$$

然后设 $G_1 * G_2$ 和 G_3 可以通过

$$\phi : H \rightarrow G_1 * G_2, \quad \psi : H \rightarrow G_3,$$

做关于 H 的融合自由积得到

$$(G_1 * G_2) {}^*_H G_3.$$

假设 $\phi(H) < G_2$, 我们可以考虑有融合自由积

$$G_2 {}^*_H G_3,$$

在考虑其与 G_1 的自由群得到

$$G_1 * (G_2 {}^*_H G_3),$$

命题 12.4.1

沿用以上记号, 我们有群同构

$$(G_1 * G_2) *_H G_3 \cong G_1 * (G_2 *_H G_3).$$

我们将所得的群记作

$$G_1 * G_2 *_H G_3$$

我们可以用以下图来表示以上构造

$$G_1 \text{ --- } G_2 \xrightarrow{H} G_3.$$

由以上观察, 我们给出如下群图的定义

定义 12.4.2

群图 (graph of groups) 是一个二元组 $(\mathbb{G}, \Gamma)$, 其中 $\Gamma = (V, E)$ 是一个图, 并且

- (i) 对任意 $v \in V$, 我们给一个群 G_v ,
- (ii) 对任意 $e \in E$, 我们给一个群 G_e ,
- (iii) 若 v 是 e 的一个端点, 则存在一个群单同态 $\phi_e : G_e \rightarrow G_v$,
- (iv) $\mathbb{G} = \{G_v \mid v \in V\} \cup \{G_e \mid e \in E\}$.

我们可以从一个群图出发得到一个群. 具体操作如下, 若 v_1 和 v_2 ($v_1 \neq v_2$) 为边 e 的两个端点, 我们通过 ϕ_e 给出的 G_e 到 G_{v_1} 和 G_{v_2} 的嵌入做 G_{v_1} 和 G_{v_2} 关于 G_e 融合自由积

$$G_{v_1} *_H G_{v_2}.$$

若存在一个点 v 有一个回路 e (即两个端点都是 v), 则考虑利用 ϕ_e 给出的 G_e 到 G_v 的两个嵌入做 G_v 关于 G_e 的 HNN 扩张

$$*_H G_v.$$

由此, 我们可以从一个群图 $(\mathbb{G}, \Gamma)$ 得到一个群 G .

第三部分

环理论

第十三章 环

在群理论的部分, 我们考虑的是一个集合上的某一个运算的性质. 很多时候, 一个集合上可能会有不止一个运算, 除了每个运算子集的类型之外, 我们也会去关系两个运算之间的联系. 例如, 我们通常考虑的整数集合 $\mathbb{Z}$ 上就可以定义加法 "+" 和乘法 " $\times$ " 两种运算. 我们除了注意到 $(\mathbb{Z}, +)$ 构成一个交换群, $(\mathbb{Z}, \times)$ 构成一个幺半群以外, 还注意到二者之间满足分配律: 任取 $a, b, c \in \mathbb{Z}$, 我们有

$$a \times (b + c) = a \times b + a \times c.$$

这里的三元组 $(\mathbb{Z}, +, \times)$ 就构成了环的一个最基本的例子. 在这一部分里, 我们将考虑带有两个运算的集合, 除了这些运算满足一些条件外, 两个运算之间也需要满足"分配律". 我们将研究这类三元组构成的代数结构的性质.

13.1 定义

我们首先给出环的定义. 记 R 为一个集合. 我们假设其上有两个二元运算 $*$ 和 $\bullet$. 通常我们将其记作三元组 $(R, *, \bullet)$.

定义 13.1.1 (教材定义 2.1.1)

我们称一个三元组 $(R, *, \bullet)$ 为一个环, 若其满足以下条件:

- (i) $(R, *)$ 为一个交换群;
- (ii) $(R, \bullet)$ 为一个半群;
- (iii) $\bullet$ 满足对 $*$ 的左分配律, 也即对于任意 $a, b, c \in R$, 我们有

$$a \bullet (b * c) = (a \bullet b) * (a \bullet c).$$

- (iv) $\bullet$ 满足对 $*$ 的右分配律, 也即对于任意 $a, b, c \in R$, 我们有

$$(b * c) \bullet a = (b * a) \bullet (c * a).$$

注 13.1.2.

这里符号 R 是"环"的英语"ring"的首字母."环"在法语中称为 anneau, 因此在一些法语文献中, 也经常会见到用 A 来作为环的符号.

例 13.1.3.

对于一般的集合上的两个二元运算, 左分配律和右分配律不一定同时被满足.

- 1) 例如, 我们可以考虑实数上的多项式函数的空间 $\mathbb{R}[x]$. 对于运算 $*$, 我们定义: 任取 $p, q \in$

$\mathbb{R}[x]$, 我们有

$$p * q := p + q.$$

我们可以验证 $(\mathbb{R}[x], +)$ 是一个交换群. 么元是 $p \equiv 0$.

2) 对于运算 $\bullet$, 我们定义: 任取 $p, q \in \mathbb{R}[x]$, 我们有

$$p \bullet q := p \circ q.$$

这里我们不再使用多项式相乘作为运算 $\bullet$, 而是考虑函数的复合. 我们可以验证 $(\mathbb{R}[x], \circ)$ 是一个半群. 注意这个群是有么元 $p(x) = x$, 所以是一个么半群.

3) 我们考虑分配律, 可以验证: 对于所有的 $p_1, p_2, q \in \mathbb{R}[x]$, 我们有

$$(p_1 + p_2) \circ q = (p_1 \circ q) + (p_2 \circ q).$$

因此运算 $\circ$ 满足对运算 $+$ 右分配律.

4) 另一方面, 取 $p_1 = p_2 = x + 1, q = x^2$, 我们可以验证:

$$(q \circ (p_1 + p_2))(x) = (2(x + 1))^2 = 4(x + 1)^2,$$

而

$$((q \circ p_1) + (q \circ p_2))(x) = 2(x + 1)^2.$$

因此, 我们有 $q \circ (p_1 + p_2) \neq (q \circ p_1) + (q \circ p_2)$, 运算 $\circ$ 不满足对 $+$ 左分配律. 因此 $(\mathbb{R}[x], +, \circ)$ 不是一个环.

注 13.1.4.

当运算 $*$ 和 $\bullet$ 没有歧义的时候, 我们会将环 $(R, *, \bullet)$ 简记为 R .

环的一个经典的例子就是整数环 $(\mathbb{Z}, +, \cdot)$. 我们借用其中的术语, 对于任意的环 $(R, *, \bullet)$, 我们称运算 $*$ 为环 R 的**加法**, 运算 $\bullet$ 为环 R 的**乘法**. 对于一个环 $(R, *, \bullet)$, 通常我们称群 $(R, *)$ 的么元为**零元**.

为了简化记号, 我们借用熟悉的记号, 将加法运算记作 $a + b$, 乘法运算记作 ab . 我们将零元记作 0 . 对于任意的元素 $a \in R$, 我们记其逆元为 $-a$. 我们使用以下记号, 对于任意环 R 中的元素 a , 对于任意非零自然数 $n \in \mathbb{N}^*$:

$$na = \underbrace{a + \cdots + a}_{n\text{次}},$$

$$a^n = \underbrace{a \cdots a}_{n\text{次}}.$$

任取 $a \in R$, 我们通常用 $-a$ 来记 a 关于加法的逆.

这里我们给出一些环的例子.

例 13.1.5.

最基本的例子就是整数环 $\mathbb{Z}$. 我们后边会讨论到的环的性质有很多都来自于对这个环的研究.

例 13.1.6.

实数域上的多项式环 $\mathbb{R}[x]$. 多项式这个概念是我们在数学课程学习中经常会遇到.

$$\mathbb{R}[x] := \left\{ \sum_{n \in \mathbb{N}} a_n x^n \mid \forall n \in \mathbb{N}, a_n \in \mathbb{R}, \text{ 且集合 } \{n \in \mathbb{N} \mid a_n \neq 0\} \text{ 有限} \right\}.$$

这里 x 是一个形式变量. 我们定义其上的加法和乘法如下: 任取 $\mathbb{R}[x]$ 中多项式

$$f(x) = \sum_{n \in \mathbb{N}} a_n x^n, \quad g(x) = \sum_{n \in \mathbb{N}} b_n x^n,$$

我们定义加法和乘法分别为:

$$f(x) + g(x) := \sum_{n \in \mathbb{N}} (a_n + b_n) x^n$$

$$f(x)g(x) := \sum_{n \in \mathbb{N}} \left(\sum_{\substack{i, j \in \mathbb{N} \\ i+j=n}} a_i b_j \right) x^n$$

例 13.1.7.

以上例子还可以扩展到一个更一般的情形: 形式幂级数(formal power series)环. 我们记

$$\mathbb{R}[[x]] := \left\{ \sum_{n \in \mathbb{N}} a_n x^n \mid \forall n \in \mathbb{N}, a_n \in \mathbb{R} \right\},$$

使用以上给出的加法和乘法就得到了形式幂级数环.

例 13.1.8.

任取非零自然数 n , 考虑实数域上的 n 阶方阵的集合 $\text{Mat}_n(\mathbb{R})$. 这个集合和矩阵加法运算(对应位置相加)以及矩阵乘法运算一起构成一个环.

例 13.1.9.

整数模 5 的同余类: $\mathbb{Z}_5$. 我们知道同余关系满足以下性质, 任取 $a, b \in \mathbb{Z}$, 我们有

$$\overline{a+b} = \overline{a} + \overline{b} \pmod{5}$$

$$\overline{a \times b} = \overline{a} \times \overline{b} \pmod{5}$$

这也给出了 $\mathbb{Z}_5$ 上的加法和乘法运算. 集合 $\mathbb{Z}_5$ 和以上定义的加法和乘法构成了一个环.

例 13.1.10.

记 S 为一个集合, $\mathcal{P}(S)$ 为 S 的幂集, 也即 S 所有子集的集合. 我们如下定义 $\mathcal{P}(S)$ 上的加法和乘法:

$$+ : \mathcal{P}(S) \times \mathcal{P}(S) \rightarrow \mathcal{P}(S) \quad \cdot : \mathcal{P}(S) \times \mathcal{P}(S) \rightarrow \mathcal{P}(S)$$

$$(A, B) \mapsto (A \cap B^c) \cup (A^c \cap B) \quad (A, B) \mapsto A \cap B$$

可以验证 $\mathcal{P}(S)$ 关于以上加法和乘法构成环.

注 13.1.11.

这里要注意的是空集 $\emptyset$ 的幂集 $\mathcal{P}(\emptyset)$ 非空:

$$\mathcal{P}(\emptyset) = \{\emptyset\}.$$

引理 13.1.12

设 R 为一个环. 任取 $a, b \in R$, 我们有

- (i) $a0 = 0a = 0$;
- (ii) $a(-b) = (-a)b = -(ab)$;
- (iii) $(-a)(-b) = ab$;
- (iv) 任取 $n \in \mathbb{N}$, $n(ab) = (na)b = a(nb)$.

证明. (练习)

□

注 13.1.13.

我们记 R 中的所有非零元素的集合为 R^* .

子环

我们记 A 为 R 的一个子集.

定义 13.1.14 (教材定义 2.2.1)

我们称 A 为 R 的一个**子环**, 若其对 R 上的加法和乘法封闭, 并满足环定义中的条件.

命题 13.1.15 (教材命题 2.2.5)

若 A 对 R 中加法成群, 且对乘法封闭, 则 A 为 R 的一个子环.

例 13.1.16.

我们考虑整数环 $\mathbb{Z}$. 之前我们知道任取整数 $m \in \mathbb{Z}$, 我们有 $m\mathbb{Z}$ 关于加法为一个子群. 我们可以直接验证 $m\mathbb{Z}$ 关于乘法封闭. 因此 $m\mathbb{Z}$ 是 $\mathbb{Z}$ 的一个子环.

例 13.1.17.

我们可以考虑以下包含关系:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

每一个包含关系前一个都是后一个的子环.

例 13.1.18.

考虑实系数多项式环 $\mathbb{R}[x]$. 任给一个非零多项式

$$f(x) = \sum_{n \in \mathbb{N}} a_n x^n \in \mathbb{R}[x],$$

我们定义 f 的次数

$$\deg f := \max\{n \in \mathbb{N} \mid a_n \neq 0\}.$$

考虑所有偶数次多项式的集合构成 $\mathbb{R}[x]$ 的一个子环.

例 13.1.19.

取 $n \in \mathbb{N}^*$, 考虑 n 阶实矩阵环 $\text{Mat}_n(\mathbb{R})$. 这个环的加法是矩阵加法. 注意到特殊线性群 $\text{GL}(n, \mathbb{R})$ 是关于乘法成群, 但是关于加法不封闭, 因此不是加法群. 由此知 $\text{GL}(n, \mathbb{R})$ 不是一个子环. 另一方面, 所有上三角矩阵构成的集合关于矩阵加法和乘法构成子环.

我们记 S 为 R 的一个子集.

定义 13.1.20

我们称所有包含 S 的子环的交为 **由 S 生成的子环**. 我们记作 $A(S)$.

$$A(S) := \bigcap \{R' \mid R' \text{ 为 } R \text{ 的子环, 且 } S \subset R'\},$$

注 13.1.21.

由此定义, 我们知道 $A(S)$ 是包含 S 的最小的子环.

以下引理保证了集合生成的子环的定义中的条件是有意义的.

引理 13.1.22

记 R 为一个环. 任意一族 R 的子环的交仍是子环.

证明. (练习)

□

我们记 $-S$ 为 S 中所有元素的加法逆元的集合. 回顾之前讨论群的生成的时候我们知道, 讨论一个集合 S 生成的群的时候, 我们考虑集合 $S \cup (-S)$ 中的元素. 将任取其中的元素以任意次序做有限次群的运算得到的元素放在一起就是 S 生成的群. 这里 S 生成的子环也可以从这个角度理解. 我们有以下命题.

命题 13.1.23

任给 R 的子集 S , 由 S 生成的子环可以表示为一下集合:

$$A(S) = \{a_{11} \cdots a_{1n_1} + \cdots + a_{m1} \cdots a_{mn_m} \mid m \in \mathbb{N}^*, n_1, \dots, n_m \in \mathbb{N}^*, a_{ij} \in S \cup (-S)\}.$$

证明. (练习, 类似于群的情形)

□

13.2 环的乘法

我们在定义环的时候只是要求有两个运算, 其中的加法运算给出一个交换群结构. 我们仅要求乘法运算给出一个半群结构, 也就是仅仅满足结合律. 通过考虑满足不同性质的乘法结构, 我们介绍一些满足性质的特殊的环结构. 这其中很多性质都来自于对整数环的性质的观察.

13.2.1 交换环

设 R 为一个环.

定义 13.2.1

我们称环 R 为一个**交换环**, 若其乘法运算满足交换律, 即

- 对任意 R 中元素 a 和 b , 我们有 $ab = ba$.

注 13.2.2.

当环交换时, 乘法对加法的左分配律和右分配律等价, 我们称之为乘法对加法的分配律.

例 13.2.3.

复数域上的乘法交换, 因此之前讨论的复数域中的环例如 $\mathbb{Z}$, $\mathbb{Q}$ 等等都是交换环.

例 13.2.4.

利用 $\mathbb{R}$ 上乘法的交换以及 $\mathbb{R}[x]$ 上乘法的定义, 我们可以证明 $\mathbb{R}[x]$ 是一个交换环.

例 13.2.5.

设 n 为一个大于 1 的自然数. 我们知道 $\mathbb{R}$ 上的 n 阶方阵关于矩阵乘法不交换. 环 $\text{Mat}_n(\mathbb{R})$ 不是一个交换环.

13.2.2 幺元**定义 13.2.6**

我们称环 R 为一个**幺环**, 若 R 有乘法幺元, 也即

- 存在 $e \in R$, 满足对任意 $a \in R$, 有 $ea = ae = a$.

注 13.2.7.

我们称乘法的幺元为环的**幺元**, 并借用 $\mathbb{Z}$ 的记号, 将其记为 1.

例 13.2.8.

讨论子环的时候, 关于幺元会出现一些特殊的情况: A 为 R 的一个子环, 可能会存在 $a \in R$, a 在 A 中是幺元, 但是在 R 中不是幺元. 例如, 我们考虑 $R = \mathbb{Z} \times \mathbb{Z}$ 上对应项相加给出的加法, 以及对应项相乘给出的乘法, 则

$$A = \mathbb{Z} \times \{0\},$$

是 R 的一个子环. 考虑 $(1, 0) \in A$. 当我们只考虑 A , 则该元素是幺元, 但是

$$(1, 0)(0, 1) = (0, 0),$$

因此不是 R 的幺元. 实际上 R 有幺元 $(1, 1)$.

命题 13.2.9

么环 R 包含至少两个元素, 当且仅当 $0 \neq 1$.

注 13.2.10.

考虑环 $R = \{0\}$, 我们可以验证 R 也满足么环的定义, 此时么元与零元相同. 在以后的章节中, 若无特殊说明, 我们考虑的么环中总满足么元与零元不同.

注 13.2.11.

在阅读文献的时候要注意, 有的文献在讨论环的时候总是假设么元是存在的. 有的文献中会使用 "ring"(有么元) 和 "rng"(无么元) 来区分两种情况. 我们的课程中不假设一个环中总有么元, 当一个环有么元的时候, 我们会使用"么环".

13.2.3 零因子

在研究整数环的时候, 一个我们经常会用到的操作就是"消去". 任取 $a, b, c \in \mathbb{Z}$, 满足 $a \neq 0$, 若

$$ab = ac,$$

我们有 $b = c$.

我们知道 $a \neq \pm 1$ 的时候关于乘法是不可逆的, 因此这里使用的并不是群里边通常使用的同时左乘 a 的逆 (因为不一定存在). 我们实际上是考虑分配律

$$a(b - c) = 0.$$

我们知道整数环满足以下性质:

- 两个整数相乘为 0 当且仅当其中一个为 0

由于我们假设 $a \neq 0$, 因此 $b - c = 0$, 进而有 $b = c$.

而对一般的环, 以上提到的性质并不一定总是成立. 因此, 我们引入零因子的概念.

定义 13.2.12 (教材定义 2.1.6)

我们称一个非零元素 $a \in R^*$ 为一个**左零因子**, 若其满足

- 存在一个非零元 $b \in R^*$, 使得 $ab = 0$.

我们称一个非零元素 $a \in R^*$ 为一个**右零因子**, 若其满足

- 存在一个非零元 $b \in R^*$, 使得 $ba = 0$.

注 13.2.13.

我们将左零因子和右零因子统称为**零因子**. 若环 R 交换, 左零因子也是右零因子.

思考 13.2.14

若一个环 R 有左零因子, 那么 R 是不是一定有右零因子?

我们首先给一些零因子的例子.

例 13.2.15.

我们考虑实数上的 2 阶矩阵构成的环 $\text{Mat}_2(\mathbb{R})$. 这个环的零元是零矩阵:

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

取

$$A = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

则有

$$AB = BA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

因此 A 和 B 都既是左零因子又是右零因子.

例 13.2.16.

我们考虑模 6 的同余类构成的环 $\mathbb{Z}_6$.

考虑

$$\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}.$$

由于 $\mathbb{Z}_6$ 中的乘法交换, 因此 $\bar{2}$ 和 $\bar{3}$ 都是 $\mathbb{Z}_6$ 的左零因子和右零因子.

思考 13.2.17

如果是 $\mathbb{Z}_5$ 呢? 是否有零因子?

例 13.2.18.

以上例子中的零因子都既是左零因子又是右零因子, 但并不是总是这样. 我们这里给出一个只是左零因子和只是右零因子的例子.

考虑线性空间

$$\mathbb{R}^{\oplus \mathbb{N}} := \{x = (x_0, x_1, \dots) \mid \forall i \in \mathbb{N}, x_i \in \mathbb{R}, \#\{i \mid x_i \neq 0\} < \infty\}.$$

可数个线性空间 $\mathbb{R}$ 的直和(注意与直积的区别).

我们考虑 $\mathbb{R}^{\oplus \mathbb{N}}$ 上的线性映射的集合, 记为 $L(\mathbb{R}^{\oplus \mathbb{N}})$. 任取 $f, g \in L(\mathbb{R}^{\oplus \mathbb{N}})$, 定义

$$\begin{aligned} (f + g)(x) &:= (f(x)_0 + g(x)_0, f(x)_1 + g(x)_1, \dots), \\ (f * g)(x) &:= (f \circ g)(x). \end{aligned}$$

我们可以直接验证 $L(\mathbb{R}^{\oplus \mathbb{N}})$ 关于以上定义加法运算成群, 零元为零映射 $\mathbf{0}$. 关于以上定义的乘法运算成一个幺半群, 幺元为恒等映射 $\mathbf{1}$.

下边考虑映射 $f, g \in L(\mathbb{R}^{\oplus \mathbb{N}})$, 满足对任意 $x \in \mathbb{R}^{\oplus \mathbb{N}}$, 有

$$\begin{aligned} f(x) &= (x_1, x_2, \dots), \\ g(x) &= (0, x_0, x_1, \dots). \end{aligned}$$

另取 $p \in L(\mathbb{R}^{\oplus \mathbb{N}})$,

$$p(x) = (x_0, 0, 0, \dots).$$

可以验证

$$f \circ g = \mathbf{1}.$$

为恒等映射, 因此任取 $h \in L(\mathbb{R}^{\oplus \mathbb{N}})$, 如果

$$h \circ f = \mathbf{0},$$

则有

$$\mathbf{0} = (h \circ f) \circ g = h \circ (f \circ g) = h.$$

因此 f 不是右零因子. 下证 f 是左零因子. 任取 $\underline{x} \in \mathbb{R}^{\oplus \mathbb{N}}$,

$$(f \circ p)(\underline{x}) = f((x_0, 0, \dots)) = (0, 0, \dots) = \mathbf{0}(\underline{x}),$$

因此 $f \circ p = \mathbf{0}$. 由此可得 f 是一个左零因子. 类似地讨论可以证明 g 是一个右零因子, 但不是左零因子.

定义 13.2.19 (教材定义 2.1.8)

我们称一个环 R 为**无零因子环**, 若 R 中没有零因子.

例 13.2.20.

整数环 $\mathbb{Z}$ 是一个无零因子环.

例 13.2.21.

实系数多项式环 $\mathbb{R}[x]$ 是一个无零因子环.

例 13.2.22.

一个非交换的无零因子环的例子可以如下构造. 我们考虑实系数二元多项式环 $\mathbb{R}[x, y]$ 要求 x 和 y 不交换.

命题 13.2.23

若 R 为一个无零因子环, 那么 $(R^*, \cdot)$ 为一个半群.

证明. 若 R 无零因子, 则任取 $a, b \in R^*$, 我们有 $ab \neq 0$, 因此 R^* 对乘法封闭. 由于 R 对乘法构成半群, 因此 R 上乘法满足结合律. 所以 R^* 上乘法满足结合律, 构成半群. $\square$

推论 13.2.24

若 R 为一个无零因子环, 则任取 $a, b \in R$, 若 $ab = 0$, 则 $a = 0$ 或 $b = 0$.

证明. 若 R 为一个无零因子环, 任取 $a, b \in R^*$, 则有 $ab \in R^*$, 即 $ab \neq 0$. 因此若 $ab = 0$, 则 $a = 0$ 或 $b = 0$. $\square$

推论 13.2.25 (教材命题 2.1.7)

记 R 为一个无零因子环. 任取 $a, b, c \in R$, 且 $a \neq 0$,

(i) 若 $ab = ac$, 则有 $b = c$.

(ii) 若 $ba = ca$, 则有 $b = c$.

证明. 任取 $a, b, c \in R$, 满足 $a \neq 0$, 若

$$ab = ac,$$

由左分配律, 我们有

$$a(b - c) = 0,$$

由于 $a \neq 0$, 因此 $b - c = 0$, 所以有 $b = c$.

考虑右分配律, 第二个结论的证明类似, 这里略去. □

定义 13.2.26 (教材定义 2.1.6)

记 R 为一个环.

若任取元素 $a, b, c \in R$, 满足 $a \neq 0$, 且 $ab = ac$, 都有 $b = c$, 我们称 R 满足**左消去律**.

若任取元素 $a, b, c \in R$, 满足 $a \neq 0$, 且 $ba = ca$, 都有 $b = c$, 我们称 R 满足**右消去律**.

注 13.2.27.

以上推论告诉我们如果一个环 R 是无零因子环, 则 R 同时满足左消去律和右消去律. 实际上反过来也是对的.

命题 13.2.28 (教材命题 2.1.7)

记 R 为一个环. 若 R 同时满足左消去律和右消去律, 当且仅当 R 为无零因子环.

证明. (练习) □

13.2.4 单位**定义 13.2.29**

设 R 为一个幺环. 我们称元素 $a \in R$ **可逆**, 若其关于乘法 $\cdot$ 的逆元存在. 我们将 a 的逆元记为 a^{-1} .

注 13.2.30.

环 R 关于加法成群, 因此所有元素都关于加法可逆. 我们这里约定"可逆"是指关于乘法可逆.

引理 13.2.31

记 R 为一个幺环. 若元素 $a \in R$ 可逆, 那么 $a \neq 0$.

证明. 设 $a \in R$ 可逆, 记 a^{-1} 为其逆元.

任取 $b \in R$, 我们有 $0 \cdot b = b \cdot 0 = 0$, 因此若 $a = 0$, 则有

$$1 = aa^{-1} = 0 \cdot a^{-1} = 0,$$

矛盾. □

命题 13.2.32

记 R 为一个幺环. 若元素 $a \in R$ 可逆, 那么 a 不是零因子.

证明. 任取 $a \in R$, 设 a 可逆, 则存在 a^{-1} , 满足 $aa^{-1} = a^{-1}a = 1$.

任取 $b \in R$, 若 $ba = 0$, 我们有

$$0 = (ba)a^{-1} = b(aa^{-1}) = b.$$

因此, $b = 0$. 由此可得 a 不是右零因子. 类似地, 我们可以证明 a 也不是左零因子. □

注 13.2.33.

任给幺环 R , 幺元 1 不是零因子.

例 13.2.34.

可逆元素不是零因子, 但是反过来不一定正确. 我们考虑整数环 $\mathbb{Z}$. 任取 $m \neq 0$ 或 1 , 则有 m 不是零因子, 且 m 不可逆.

定义 13.2.35 (教材定义 2.2.19)

记 R 为一个幺环. 我们称 R 中的任一可逆元素为 R 的一个**单位**. 我们记 U 为 R 中所有单位的集合.

命题 13.2.36

记 R 为一个幺环, U 为 R 中所有单位的集合, 则 $(U, \cdot)$ 为一个群.

证明. 注意到 $1 \in U$, 因此 $U \neq \emptyset$.

任取 $a, b \in U$, 我们有 a^{-1} 和 b^{-1} 分别为 a 和 b 的逆元. 考虑

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = 1.$$

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = 1.$$

因此 ab 可逆, 且有 $(ab)^{-1} = b^{-1}a^{-1}$. 因此 U 对乘法运算封闭.

由于 R 上的乘法满足结合律, 因此 U 上乘法满足结合律. 由 1 的性质知 $1 \in U$ 为单位元.

任取 $a \in U$, 由

$$aa^{-1} = a^{-1}a = 1,$$

知

$$a = (a^{-1})^{-1},$$

即 $a^{-1} \in U$.

综上所述 U 为一个群. □

定义 13.2.37 (教材定义 2.2.19)

记 R 为一个幺环. 我们称 U 为 R 的**单位群**.

例 13.2.38.

考虑整数环 $\mathbb{Z}$, 其中的可逆元素只有 ± 1 . 因此 $\mathbb{Z}$ 中的单位群 $U = \{1, -1\}$ (关于乘法运算).

例 13.2.39.

考虑整数模 12 的同余类构成的环 $\mathbb{Z}_{12}$. 任给 $m \in \mathbb{Z}$, $\overline{m} \in \mathbb{Z}_{12}$ 可逆当且仅当 $\gcd(m, 12) = 1$. 因此 $\mathbb{Z}_{12}$ 的单位群为

$$U_{12} = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

例 13.2.40.

考虑整数模 5 的同余类构成的环 $\mathbb{Z}_5$. 由于 5 为素数, 我们有 $\mathbb{Z}_5$ 的单位群为:

$$U_5 = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \mathbb{Z}_5^* \cong \mathbb{Z}_4.$$

思考 13.2.41

任取 $n \in \mathbb{N} \setminus \{0, 1\}$, 记 U_n 为 $\mathbb{Z}_n$ 中的单位群. 什么时候 U_n 是一个循环群?

例 13.2.42.

考虑实数域上的 2 阶方阵环 $\text{Mat}_2(\mathbb{R})$, 其单位群为 $\text{GL}(2, \mathbb{R})$.

定义 13.2.43 (教材定义 2.2.20)

我们称一个环 R 为一个**整环**, 若其为一个不包含零因子的交换幺环.

定义 13.2.44 (教材定义 2.2.20)

我们称环 R 为一个**除环**或**体**, 若 R 中非零元素的集合对乘法构成一个群, 也即环 R 还满足

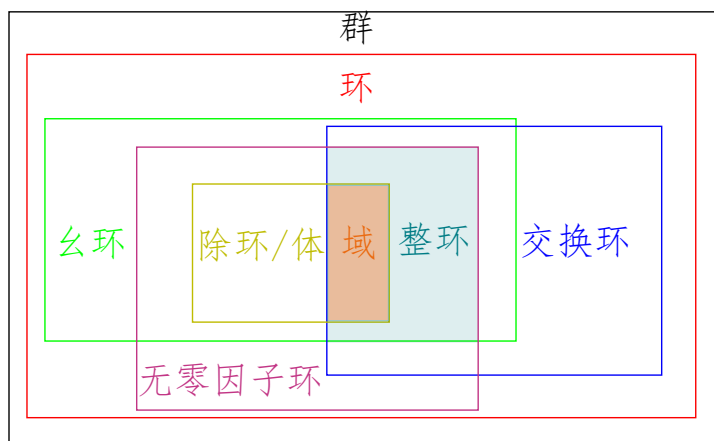
- R 是一个幺环;
- $U = R^*$, 即所有非零元素都可逆.

定义 13.2.45 (教材定义 2.2.20)

我们称环 R 为一个**域**, 若 $(R^*, \cdot)$ 是一个交换群, 即环 R 满足

- R 是一个幺环;
- $U = R^*$, 即所有非零元素都可逆;
- 任取 $a, b \in R$, 都有 $ab = ba$.

下图为之前介绍的一些概念之间的包含关系示意图.

**思考 13.2.46**

尝试为图中每个部分找一个例子.

注 13.2.47.

我们可以考虑 $\mathbb{R}$ 上两个变量 x 和 y 的多项式的集合, 并假设两个变量不交换 $xy \neq yx$. 我们考虑由单项式 x 和 y 生成的理想(定义见下章), 是一个没有幺元, 没有零因子, 且不交换的环.

若我们假设两个变量交换也即 $xy = yx$, 那么由 x 和 y 生成的理想是一个没有幺元, 没有零因子的交换环.

***交换群的自同态环**

我们取 $(M, +)$ 为一个交换群, 群 M 到自己的群同态映射被称为 M 的**自同态**. 我们考虑 M 上所有的自同态的集合 $\text{End}(M)$. 任取 $\phi, \psi \in \text{End}(M)$, 我们定义映射 $\phi + \psi : M \rightarrow M$,

满足

$$(\phi + \psi)(x) = \phi(x) + \psi(x),$$

对于任意 $x \in M$ 都成立. 由此我们可以定义 $\text{End}(M)$ 上一个二元算子:

$$+ : \text{End}(M) \times \text{End}(M) \rightarrow \text{End}(M)$$

$$(\phi, \psi) \mapsto \phi + \psi.$$

命题 13.2.48

二元组 $(\text{End}(M), +)$ 为一个交换群.

证明. 1) 我们首先需要验证该二元算子是良定义, 也即两个群同态的和也是一个同态.

由于 M 交换, 对于任意 $x, y \in M$, 任意 $\phi, \psi \in \text{End}(M)$, 我们有如下运算:

$$\begin{aligned} (\phi + \psi)(x + y) &= \phi(x + y) + \psi(x + y) && \cdots && \text{End}(M) \text{ 中 } + \text{ 的定义} \\ &= (\phi(x) + \phi(y)) + (\psi(x) + \psi(y)) && \cdots && \text{End}(M) \text{ 中 } + \text{ 的定义} \\ &= (\phi(x) + \psi(x)) + (\phi(y) + \psi(y)) && \cdots && M \text{ 中 } + \text{ 的交换律/结合律} \\ &= (\phi + \psi)(x) + (\phi + \psi)(y) && \cdots && \text{End}(M) \text{ 中 } + \text{ 的定义} \end{aligned}$$

2) 我们需要验证交换群定义中的条件:

a) (结合律) 对任意 $\phi, \psi, \rho \in \text{End}(M)$, 对任意 $x \in M$, 我们有

$$\begin{aligned} ((\phi + \psi) + \rho)(x) &= (\phi + \psi)(x) + \rho(x) && \cdots && \text{End}(M) \text{ 中 } + \text{ 的定义} \\ &= (\phi(x) + \psi(x)) + \rho(x) && \cdots && \text{End}(M) \text{ 中 } + \text{ 的定义} \\ &= \phi(x) + (\psi(x) + \rho(x)) && \cdots && M \text{ 中 } + \text{ 的结合律} \\ &= (\phi + (\psi + \rho))(x) && \cdots && \text{End}(M) \text{ 中 } + \text{ 的定义} \end{aligned}$$

因此 $(\phi + \psi) + \rho = \phi + (\psi + \rho)$.

b) (交换律) 任取 $\phi, \psi \in \text{End}(M)$, 对任意 $x \in M$,

$$\begin{aligned} (\phi + \psi)(x) &= \phi(x) + \psi(x) && \cdots && \text{End}(M) \text{ 中 } + \text{ 的定义} \\ &= \psi(x) + \phi(x) && \cdots && M \text{ 中 } + \text{ 的交换律} \\ &= (\psi + \phi)(x) && \cdots && \text{End}(M) \text{ 中 } + \text{ 的定义} \end{aligned}$$

因此 $\phi + \psi = \psi + \phi$.

c) (幺元) 我们考虑同态(验证作为练习):

$$\begin{aligned} o : M &\rightarrow M \\ x &\mapsto 0. \end{aligned}$$

对任意 $\phi \in \text{End}(M)$, 任意 $x \in M$, 我们有

$$\begin{aligned} (\phi + \iota)(x) &= \phi(x) + o(x) && \cdots && \text{End}(M) \text{ 中 } + \text{ 的定义} \\ &= \phi(x) + 0 && \cdots && o \text{ 的定义} \\ &= \phi(x) && \cdots && M \text{ 中 } \text{幺元} \text{ 的性质} \end{aligned}$$

因此 $\phi + o = o + \phi = \phi$

d) (逆元) 对于任意 $\phi \in \text{End}(M)$, 我们考虑同态(验证作为练习):

$$\begin{aligned} -\phi : M &\rightarrow M \\ x &\mapsto -(\phi(x)). \end{aligned}$$

任取 $x \in M$, 我们有

$$\begin{aligned} (\phi + (-\phi))(x) &= \phi(x) + (-\phi)(x) && \cdots \text{End}(M) \text{ 中 } + \text{ 的定义} \\ &= \phi(x) + (-(\phi(x))) && \cdots -\phi \text{ 的定义} \\ &= 0 && \cdots M \text{ 中逆元的性质} \end{aligned}$$

因此 $\phi + (-\phi) = o$.

□

注 13.2.49.

我们先验证交换律, 可以简化验证么元和逆元存在性的步骤.

思考 13.2.50

若群 M 不交换, 我们是否可以有以上结论? 若可以, 为什么? 若不可以, 哪里出问题?

我们定义 $\text{End}(M)$ 上的乘法为映射的复合:

$$\begin{aligned} \circ : \text{End}(M) \times \text{End}(M) &\rightarrow \text{End}(M) \\ (\phi, \psi) &\mapsto \phi \circ \psi \end{aligned}$$

由映射复合的性质, 我们知道 $(\text{End}(M), \circ)$ 为一个半群. 我们考虑恒等同态

$$\begin{aligned} \iota : M &\rightarrow M \\ x &\mapsto x. \end{aligned}$$

命题 13.2.51

自同态 ι 为半群 $(\text{End}(M), \circ)$ 的么元.

命题 13.2.52

任给 $\phi, \psi, \rho \in \text{End}(M)$, 我们有

$$(i) \quad \rho \circ (\phi + \psi) = \rho \circ \phi + \rho \circ \psi;$$

$$(ii) \quad (\phi + \psi) \circ \rho = \phi \circ \rho + \psi \circ \rho.$$

推论 13.2.53

任给交换群 M , 三元组 $(\text{End}(M), +, \circ)$ 为一个么环.

我们称么环 $(\text{End}(M), +, \circ)$ 为交换群 M 的**自同态环**, 简记为 $\text{End}(M)$.

***整环上的分式域**

我们首先回顾由整环诱导的分式域的概念. 设 R 为一个整环. 我们集合

$$\tilde{\mathcal{F}}(R) = R \times R^* := \{(a, b) \mid a \in R, b \in R^*\}.$$

换言之, 我们考虑 R 上的有序的元素对, 满足元素对的第二个位置上的元素非零. 由此类元素对构成的集合就是 $R \times R^*$. 我们可以在这个集合上定义加法和乘法运算: 任给 $\tilde{\mathcal{F}}(R)$ 中元素 (a, b) 和 (c, d) , 我们定义

$$(a, b) + (c, d) = (ad + bc, bd), \quad (a, b)(c, d) = (ac, bd).$$

命题 13.2.54

以上定义的加法和乘法是良定义.

证明. 我们只需验证 $bd \neq 0$. 由于 R 为一个整环, 因此无零因子. 由条件, $b, d \in R^*$, 因此非零. 由此, 我们得到 $bd \neq 0$. $\square$

我们考虑 $\tilde{\mathcal{F}}(R)$ 中的等价关系:

- $(a, b) \sim (c, d)$ 当且仅当 $ad = bc$.

并记其对应的商空间为 $\mathcal{F}(R) = \tilde{\mathcal{F}}(R) / \sim$. 我们首先验证一下结论. 任取 $\tilde{\mathcal{F}}(R)$ 中的元素 (a, b) 和 (c, d) , 我们有

命题 13.2.55

- (i) $\overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc, bd)}$.
- (ii) $\overline{(a, b)} \overline{(b, c)} = \overline{(ac, bd)}$.

命题 13.2.56

三元组 $(\mathcal{F}(R), +, \cdot)$ 为一个域.

证明. (练习) $\square$

定义 13.2.57

我们称域 $\mathcal{F}(R)$ 为整环 R 的分式域.

思考 13.2.58

若我们不模掉以上定义的等价关系而直接考虑 $\tilde{\mathcal{F}}$, 会出现什么问题?

例 13.2.59.

我们可以考虑一个经典的例子就是整数环 $\mathbb{Z}$ 以及其分式域 $\mathbb{Q}$, 也即有理数域. 我们知道每个有理数都可以写为分母不为零的两个整数的商. 但这种写法不唯一. 例如, 我们有

$$\frac{m}{n} = \frac{km}{kn}.$$

我们以上定义的等价关系就是为了避免这个情况的出现. 特别地, 我们有若

$$\frac{m}{n} = \frac{k}{l}$$

当且仅当 $ml = kn$.

命题 13.2.60

- (i) $\mathcal{F}(R)$ 的零元为 $\overline{(0, 1)}$.
- (ii) $\mathcal{F}(R)$ 的幺元为 $\overline{(1, 1)}$.
- (iii) 任取 R 中的非零元 a , 我们有 $\overline{(a, 1)}^{-1} = \overline{(1, a)}$.

我们考虑映射

$$\begin{aligned} \phi : R &\rightarrow \mathcal{F}(R) \\ a &\mapsto \overline{(a, 1)} \end{aligned}$$

命题 13.2.61

映射 ϕ 是一个环单同态. 因此 R 与 $\phi(R)$ 作为环同构.

命题 13.2.62

整环 R 的分式域 $\mathcal{F}(R)$ 可以有如下表示:

$$\mathcal{F}(R) = \{\overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} \mid a \in R, b \in R^*\}.$$

注 13.2.63.

以上构造是从一个环 R 开始构造一个同构意义下包含 R 的域. 任给一个 $b \in R^*$, 我们在该域中考虑逆元 b^{-1} .

若一开始我们考虑 R 包含在一个域 E 中, 我们可以直接使用 b 在 E 中的乘法逆元来构造如下 E 的子域

$$\{ab^{-1} \mid a \in R, b \in R^*\}.$$

这与使用等价类构造的 R 的分式域同构. 以下由于我们总是在域中考虑问题, 因此我们将直接使用域中逆元, 并仍称构造的域为 R 的分式域.

推论 13.2.64

设 R 为域 E 里的一个整环. 则 $\mathcal{F}(R)$ 为 E 中包含 R 的最小的子域.

证明. 包含 R 的子域必须包含 R 中所有元素以及它们的逆以及这些元素之间的乘积. 由以上 R 的分式域的表达式, 我们得到这个推论. $\square$

注 13.2.65.

另一个需要说明的是, 以上两种从整环 R 构造其分式域的过程中, 我们并没有用到整环的所有性质, 而仅仅使用了 R 为一个无零因子交换环. 因此我们也可以使用以上构造对任意一个无零因子交换环来构造分式域. 例如, 我们可以考虑从 $2\mathbb{Z}$ 通过构造 $2\mathbb{Z} \times 2\mathbb{Z}$ 中等价类的办法来构造分式域 $\mathcal{F}(2\mathbb{Z})$, 我们可以验证 $\mathcal{F}(2\mathbb{Z}) = \mathbb{Q}$.

13.3 环的特征

记 R 为一个环. 任取 $a \in R$, 我们考虑

$$\{na \mid n \in \mathbb{Z}\},$$

这是 R 中由 a 生成的加法循环子群. 由循环子群的分类, 我们知道这个子群或者同构于 $\mathbb{Z}$ 或者同构于某个 $\mathbb{Z}_m$, 其中 $m \in \mathbb{N}^*$.

我们考虑整数环 $\mathbb{Z}$, 任取 $m \in \mathbb{Z}$, 若 $m = 0$, 则 m 生成的加法子群为 $\{0\}$, 否则就是 $m\mathbb{Z} \cong \mathbb{Z}$.

另一方面, 任取 $m \in \mathbb{N}^*$, 考虑 $\mathbb{Z}_m$, 我们知道所有 $\mathbb{Z}_m$ 中的元素 $\bar{d}$ 都满足

$$m\bar{d} = \bar{0}.$$

因此 $\bar{d}$ 生成的加法子群的阶整除 m .

注意到环 $\mathbb{Z}$ 中所有非零元素的阶都是无穷, 而环 $\mathbb{Z}_m$ 中所有非零元素的阶都是有限的. 这个现象对没有零因子的环也是成立的.

命题 13.3.1

设 R 为无零因子环, 则 R 中所有非零元素的阶相等, 若其有限, 则为一个素数.

证明. 我们首先证明 R^* 中所有元素关于加法的阶相同. 任取 $a, b \in R^*$, 任取 $n \in \mathbb{N}^*$, 利用分配律, 我们有

$$(na)b = n(ab) = a(nb).$$

由于 R 为无零因子环, 因此 $na = 0$ 当且仅当 $nb = 0$. 我们有 a 和 b 的阶相同.

下设所有非零元素的阶为 $n \in \mathbb{N}^*$ 有限. 由于所有元素非零, 1 阶元素只有零元素, 因此 $n > 1$. 任取 $k, m \in \mathbb{N}^*$, 满足 $n = km$, 由分配律, 任取 $a, b \in R^*$, 我们有

$$0 = n(ab) = km(ab) = (ka)(mb).$$

由于 R 无零因子, 因此 $ka = 0$ 或者 $mb = 0$. 由于 $0 < k \leq n$ 且 $0 < m \leq n$, 我们有 $k = n$ 或者 $m = n$. 因此 n 为素数. $\square$

例 13.3.2.

若环有零因子, 考虑加法运算, 则可能同时有有限阶和无限阶元素. 例如: $\mathbb{Z} \times \mathbb{Z}_2$ 上定义加法和乘法分别为:

$$(k, \bar{l}) + (m, \bar{n}) = (k + m, \overline{l + n}), \quad (k, \bar{l}) \cdot (m, \bar{n}) = (k \cdot m, \overline{l \cdot n}).$$

注意到

$$(1, \bar{0}) \cdot (0, \bar{1}) = (0, \bar{0}).$$

因此这个环有零因子.

另一方面, 任取 $m \in \mathbb{Z}^*$, $(m, \bar{0})$ 的加法阶无限, 而 $(0, \bar{m})$ 的阶为 1 或者 2.

定义 13.3.3

设 R 为一个无零因子环. 若 R 中非零元素的阶有限, 记为 n , 则称 n 为 R 的**特征**. 若 R 中非零元素的阶无限, 则定义 R 的特征为 0. 我们记 R 的特征为 $\text{Ch}(R)$.

注 13.3.4.

在定义特征时, 有的教材或讲义中要求环为一个交换的幺环. 特征被定义为幺元 1 的阶. 在此定义中, 我们并不要求环无零因子. 在此情况下, 有可能出现特征为合数的情形. 例如, 我们考虑环 $\mathbb{Z}/8\mathbb{Z}$.

在环 $\mathbb{Z}/8\mathbb{Z}$ 中, 元素 $\bar{1}$ 的阶为 8. 我们可以观察到, 不同元素的阶可能不同. 若元素不是零因子, 则其阶也为 8. 若其为零因子, 那么阶会整除 8. 例如, 我们观察到 $\bar{2} \cdot \bar{4} = \bar{0}$. 因此 $\bar{2}$ 和 $\bar{4}$ 均为零因子. 而我们可以验证 $\bar{2}$ 的阶为 4, $\bar{4}$ 的阶为 2. 另一方面, 元素 $\bar{3}$ 不是零因子, 其阶为 8.

特别的, 当 R 为整环时, 该方法定义的特征与之前我们定义的非零因子环的特征等价. 此时我们有幺元 1 的阶为 0 或者一个素数, 且所有非零元素的阶与 1 的阶相同.

记 R 为一个特征为素数 p 的无零因子环. 考虑二项式展开, 我们可以验证

$$(a + b)^p = a^p + b^p.$$

这实际上给出了 R 到自己的一个"环同态", 被称为 Frobenius 同态. 我们会在后边的部分讨论这个同态.

13.4 理想与商环

13.4.1 定义

设 R 为一个环. 由定义, 我们知道 R 关于加法构成一个交换群. 交换群的任意子群都是正规子群, 因此任取 R 的子环 A , 我们都有 R/A 为一个商群. 当我们考虑乘法的时候, 由于我们并没有给乘法太多限制, 因此, R 中的乘法并不一定可以给出 R/A 上一个乘法运算. 更具体一点, 任取 $a, b \in R$, 利用分配律, 我们有

$$(a + A)(b + A) = ab + aA + Ab + AA.$$

一般地, 我们不一定有 $aA + Ab \subset A$. 例如: 我们考虑 2 阶实方阵环 $R = \text{Mat}_2(\mathbb{R})$, 考虑上三角方阵给出的子环 A , 则有

$$R/A := \left\{ \begin{bmatrix} 0 & 0 \\ t & 0 \end{bmatrix} + A \mid t \in \mathbb{R} \right\}.$$

我们考虑

$$\left(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + A\right) \left(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + A\right) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} A + A \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + AA.$$

考虑 A 中的矩阵

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

则有

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in \left(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + A\right) \left(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + A\right)$$

因此

$$\left(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + A\right) \left(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + A\right) \not\subseteq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + A.$$

因此我们需要子环 A 满足一些特殊性质来使得 R 上的乘法运算可以诱导 R/A 上的一个乘法运算.

定义 13.4.1 (教材定义 2.2.7)

我们称 R 的一个子环 A 为 R 的一个**左理想**, 若我们有:

- $(RA \subset A)$ 任取 $r \in R$, 任取 $a \in A$, 我们有 $ra \in A$.

类似地, 我们称 R 的一个子环 A 为 R 的一个**右理想**, 若我们有:

- $(AR \subset A)$ 任取 $r \in R$, 任取 $a \in A$, 我们有 $ar \in A$.

若 A 同时是 R 的左理想和右理想, 我们称 A 为 R 的**双边理想**. 若(左,右,双边)理想 $A \neq R$, 我们称 A 为**真(左,右,双边)理想**.

注 13.4.2.

我们通常使用 I 来记一个理想. 这是来自于其英文 ideal 首字母.

注 13.4.3.

如无特殊注明, 我们之后将通常考虑双边理想, 我们将其简称**理想**.

我们来看几个理想的例子.

例 13.4.4.

根据定义, 我们有两个平凡的例子. 任取环 R , 其子环 $\{0\}$ 和 R 都是 R 的理想. 这个例子告诉我们理想总是存在的.

例 13.4.5.

考虑整数环 $\mathbb{Z}$, 我们知道任意 $\mathbb{Z}$ 的加法子群都是形如 $m\mathbb{Z}$ 的子群, 其中 $m \in \mathbb{Z}$. 另一方面, 由于 $m\mathbb{Z}$ 对乘法封闭, 因此是 $\mathbb{Z}$ 的子环.

任取 $k, l \in \mathbb{Z}$, 我们有

$$l(mk) = (mk)l = m(kl) \in m\mathbb{Z}.$$

因此任取 $m \in \mathbb{Z}$, 子环 $m\mathbb{Z}$ 是环 $\mathbb{Z}$ 的理想.

例 13.4.6.

考虑有理数域 $\mathbb{Q}$ 中的理想. 我们发现由于任意非零元素都可逆, 如果 $\mathbb{Q}$ 的一个理想 A 中有非零元素, 那么 A 就包含 1, 因此 $A = \mathbb{Q}$. 实际上, 我们会证明一个交换幺环 R 为域当且仅当其只有平凡理想 $\{0\}$ 和 R .

例 13.4.7.

考虑实系数多项式环 $\mathbb{R}[x]$. 任取 $f(x) \in \mathbb{R}[x]$, 我们考虑

$$\mathbb{R}[x]f(x) := \{g(x)f(x) \mid g(x) \in \mathbb{R}[x]\}.$$

我们可以直接验证这是 $\mathbb{R}[x]$ 的一个理想.

例 13.4.8.

考虑 $[0, 1]$ 上的实函数的集合 $R = \mathcal{F}([0, 1], \mathbb{R})$. 这个集合关于以下加法运算 "+" 和乘法运算 "." 成环:

$$\begin{aligned} + : R \times R &\rightarrow R & \cdot : R \times R &\rightarrow R \\ (f, g) &\mapsto (f + g : x \mapsto f(x) + g(x)). & (f, g) &\mapsto (f \cdot g : x \mapsto f(x)g(x)) \end{aligned}$$

我们记

$$A = \{f \in R \mid \forall x \in [0, 1/2], f(x) = 0\},$$

可以验证 A 是 R 的一个理想.

我们考虑 R 中的一个理想 I . 任取元素 $a, b \in R$, 我们有

$$(a + I)(b + I) = ab + aI + Ib + II \subset ab + I.$$

这里还有一个问题需要验证就是以上的运算是否依赖于代表元, 即我们需要证明以下引理:

引理 13.4.9

记 R 为一个环, $I \subset R$ 为一个理想. 任取 $a_1, a_2, b_1, b_2 \in R$, 若 $a_1 - a_2 \in I$ 且 $b_1 - b_2 \in I$, 则有

$$a_1b_1 + I = a_2b_2 + I.$$

证明. 我们记 $c = a_1 - a_2 \in I$, $d = b_1 - b_2 \in I$.

考虑以下计算

$$\begin{aligned} &a_1b_1 + I \\ &= (a_2 + c)(b_2 + d) + I \\ &= a_2b_2 + cb_2 + a_2d + I \\ &= a_2b_2 + I. \end{aligned}$$

最后一个等号是由于 I 为理想且 $c, d \in I$. □

将以上讨论综合在一起, 我们有以下定理.

定理 13.4.10 (教材定理 2.2.16)

记 R 为一个环, $I \subset R$ 为一个理想, 则集合

$$R/I := \{a + I \mid a \in R\},$$

以及以下加法运算 "+" 和乘法运算 "·"

$$\begin{aligned} + : R/I \times R/I &\rightarrow R/I & \cdot : R/I \times R/I &\rightarrow R/I \\ (a + I, b + I) &\mapsto (a + b) + I & (a + I, b + I) &\mapsto (a \cdot b) + I \end{aligned}$$

构成一个环.

定义 13.4.11 (教材定理 2.2.16)

记 R 为一个环, $I \subset R$ 为一个理想. 我们称环 R/I 为 R 关于理想 I 的**商环**.

例 13.4.12.

任取 $m \in \mathbb{N} \setminus \{0, 1\}$, 则整数模 m 同余类环 $\mathbb{Z}_m$ 是 $\mathbb{Z}$ 关于其理想 $m\mathbb{Z}$ 的商环.

例 13.4.13.

域 $\mathbb{C}$ 可以看作是 $\mathbb{R}[x]$ 关于理想 $\mathbb{R}[x](x^2 + 1)$ 的商环.

类似于群到商群的自然同态, 我们也可以定义环到其商环的自然同态.

定义 13.4.14

记 R 为一个环, $I \subset R$ 为 R 的理想. 我们称映射:

$$\begin{aligned} \pi : R &\rightarrow R/I \\ a &\mapsto a + I \end{aligned}$$

为环 R 到商环 R/I 的**自然同态**.

当我们介绍完环的同态之后, 我们可以验证环到商环的自然同态是一个环同态. 类似于群同态, 自然同态会保留环的一些性质.

命题 13.4.15

- 1) 若环 R 交换, 那么环 R/I 交换;
- 2) 若环 R 为幺环, 那么环 R/I 也为幺环.

证明. (练习, 直接验证即可.)

□

注 13.4.16.

若 $I = R$, 则 $R/I = \{0\}$, 仍是一个幺环 (见注 13.2.10).

由理想的定义, 我们可以直接验证以下结论.

命题 13.4.17

设 R 为一个环, A 为 R 的一个子环, I 为 R 的一个理想, 则 $A \cap I$ 为 A 的理想.

13.4.2 理想的运算及生成

理想之间也可以做运算, 从而得到新的理想:

命题 13.4.18

记 R 为一个环.

(i) 理想的任意交都是理想, 即任取 R 的一组理想 $\{I_\alpha\}_{\alpha \in \Omega}$, 我们有

$$\bigcap_{\alpha \in \Omega} I_\alpha$$

是 R 的理想.

(ii) 理想的和是理想, 即任取 R 的理想 I 和 J , 则

$$I + J := \{a + b \in R \mid a \in I, b \in J\}.$$

是 R 的一个理想.

证明. (练习, 直接验证定义条件.)

□

类似于集合生成的子环, 我们可以定义集合生成的理想.

定义 13.4.19

记 R 为一个环, $S \subset R$ 为一个非空子集. 我们称 R 中所有包含 S 的理想的交为 **由 S 生成的理想**. 我们记作 $\langle S \rangle$.

$$\langle S \rangle := \bigcap \{I \mid I \text{ 为 } R \text{ 的理想, 且 } S \subset I\}.$$

类似于集合生成的子群, $\langle S \rangle$ 是包含 S 的最小的理想. 我们记 S 中所有元素的加法逆元集合为 $-S$. 我们也有另一种方法来描述 $\langle S \rangle$.

命题 13.4.20 (教材习题 2.2.2)

任给环 R 中的子集 S , 由 S 生成的理想可以被表示为以下集合:

$$\begin{aligned} \langle S \rangle = \left\{ \sum_{i=1}^p x_i a_i y_i + \sum_{j=1}^q u_j b_j + \sum_{k=1}^r c_k v_k + \sum_{l=1}^t n_l d_l \mid p, q, r, t \in \mathbb{N}^*, n_1, \dots, n_t \in \mathbb{Z}, \right. \\ \left. x_1, \dots, x_p, y_1, \dots, y_p, u_1, \dots, u_q, v_1, \dots, v_r \in R, \right. \\ \left. a_1, \dots, a_p, b_1, \dots, b_q, c_1, \dots, c_r, d_1, \dots, d_t \in S \cup (-S) \right\}. \end{aligned}$$

推论 13.4.21

若 R 为一个交换幺环, 任取 $S \subset R$ 为一个非空集合, 则

$$\langle S \rangle = \{x_1 a_1 + \cdots + x_k a_k \mid k \in \mathbb{N}^*, x_1, \dots, x_k \in R, a_1, \dots, a_k \in S\}.$$

定义 13.4.22

当 $S = \{a\}$ 时, 我们称 $\langle S \rangle$ 为由元素 a 生成的**主理想**(principle ideal), 并记为 $\langle a \rangle$. 我们称 a 为主理想 $\langle a \rangle$ 的**生成元**.

思考 13.4.23

比较一下集合生成的理想和集合生成的子环之间的区别.

13.5 素理想与极大理想

考虑整数环 $\mathbb{Z}$, 任取一个素数 p 有以下两个性质:

- 任取一个整数 $n \in \mathbb{Z}$, 则有 $\gcd(n, p) = p$ 或者 1 .
- 任取整数 $a, b \in \mathbb{Z}$, 若 $p \mid ab$, 则有 $p \mid a$ 或者 $p \mid b$.

我们可以从整数环 $\mathbb{Z}$ 的理想的角来考虑以上的两个性质. 考虑 $p\mathbb{Z}$ 是 $\mathbb{Z}$ 的一个理想, 以上两点翻译为理想的语言就是:

- $p\mathbb{Z}$ 具有极大性质, 即任取一个包含 $p\mathbb{Z}$ 的 $\mathbb{Z}$ 的理想 I , 我们有 $I = \mathbb{Z}$ 或者 $I = p\mathbb{Z}$.
- 任取整数 a 和 b 如果 $ab \in p\mathbb{Z}$, 那么有 $a \in p\mathbb{Z}$ 或者 $b \in p\mathbb{Z}$.

本节我们将这两个性质推广到对一般的环的理想的讨论中.

定义 13.5.1 (教材定义 2.6.9)

我们称环 R 的一个真理想 I 为 R 的**极大理想**, 若其满足:

- 对于任意 R 的真理想 J , 若 $I \subset J$, 则我们有 $I = J$.

定义 13.5.2 (教材定义 2.6.1)

我们称环 R 中的真理想 I 为一个**素理想**, 若其满足

- 任取 $a, b \in R$, 若 $ab \in I$, 我们有 $a \in I$ 或 $b \in I$.

例 13.5.3.

考虑整数环 $\mathbb{Z}$, 则任取 $n \in \mathbb{N}$, 我们有理想 $n\mathbb{Z}$. 若有自然数 m 和 k , 满足 $n = mk$, $m > 1$, 且 $k > 1$, 则

$$n\mathbb{Z} \subsetneq m\mathbb{Z} \subsetneq \mathbb{Z},$$

因此 $n\mathbb{Z}$ 不是一个极大理想.

另一方面, 我们有 $mk = n \in n\mathbb{Z}$, 但是 $m \notin n\mathbb{Z}$ 且 $k \notin m\mathbb{Z}$, 因此 $n\mathbb{Z}$ 不是素理想. 实际上 $m\mathbb{Z}$ 是一个极大理想当且仅当 $m\mathbb{Z}$ 是一个素理想当且仅当 m 是一个素数.

例 13.5.4.

我们考虑 $\mathbb{R}$ 上多项式环 $\mathbb{R}[x]$. 考虑理想 $\langle x \rangle$, 这是一个素理想. 任取 $\mathbb{R}[x]$ 中多项式

$$f(x) = a_0 + a_1x + \cdots + a_mx^m, \quad g(x) = b_0 + b_1x + \cdots + b_nx^n,$$

注意到若 $a_0 \neq 0$ 且 $b_0 \neq 0$, 则

$$f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots$$

不能写成 $xh(x)$ 的形式. 所以若 $f(x)g(x) \in \langle x \rangle$, 则有 $a_0 = 0$ 或者 $b_0 = 0$, 也即 $f(x) \in \langle x \rangle$ 或者 $g(x) \in \langle x \rangle$.

下边考虑 $\langle x \rangle$ 是否是极大理想. 任取 $f(x) \notin \langle x \rangle$, 记

$$f(x) = a_0 + \cdots + a_nx^n,$$

有 $a_0 \neq 0$. 因此 $a_0 \in \langle f(x), x \rangle$, 从而有 $1 \in \langle f(x), x \rangle$. 所以

$$\langle f(x), x \rangle = \mathbb{R}[x].$$

以上讨论告诉我们, 向 $\langle x \rangle$ 中添加任意的新的多项式所生成的理想都是整个环 $\mathbb{R}[x]$, 因此 $\langle x \rangle$ 为极大理想.

虽然以上例子中, 我们得到的理想同时是素理想和极大理想, 但是二者并不相同. 一个是素理想但不是极大理想的例子就是 $\mathbb{Z}[x]$ 中的理想 $\langle x \rangle$. 我们将在后续课程中详细讨论环上多项式.

我们注意到以上两个定义都需要是真理想. 下边是一个简单但是常用的引理.

引理 13.5.5

记 R 为一个交换幺环. 若 I 为 R 的一个真理想, 那么 $1 \notin I$.

证明. 由理想的定义, 我们有 $RI = I$. 因此, 若 $1 \in I$, 我们有

$$R = R\{1\} \subset RI = I.$$

因此, I 不是一个真理想. □

我们进而有如下推论:

推论 13.5.6

取一个交换幺环 R . 若 I 为 R 的一个真理想, 那么我们有:

- 若 $a \in U$ 为一个单位, 那么 $a \notin I$.

证明. 由于我们有 $RI = I$, 因此若 $a \in I$ 可逆, 那么我们有 $a^{-1}a = 1 \in I$. 而这与 I 为真理想矛盾. □

我们回顾一个交换幺环是域当且仅当 $U = R^*$. 因此我们有一下推论.

推论 13.5.7

考虑一个交换幺环 R . 我们有 R 为一个域当且仅当 R 中只有 $\{0\}$ 和 R 两个理想.

证明. 若 R 为一个域, 那么 $R \setminus \{0\}$ 中所有元素关于 $\cdot$ 运算可逆. 因此, 若理想 I 包含一个非零元 1 , 则 $1 \in I$. 因此 $I = R$. 因此 R 中只有 $\{0\}$ 和 R 两个理想.

反之, 我们假设 R 中只有 $\{0\}$ 和 R 两个理想. 取 R 中一个非零元素 a , 则 Ra 为 a 生成的 R 一个理想. 由于 $Ra \neq \{0\}$, 因此我们有 $Ra = R$, 因此存在元素 $b \in R$ 满足 $ba = 1$. 因此 a 可逆.

因此 $R \setminus \{0\}$ 关于 $\cdot$ 构成一个交换群. 因此 R 为一个域. $\square$

记 R 为一个环. 任给 R 的一个理想 I , 记 R/I 为其对应的商环. 我们可以通过研究 R/I 的性质得到 I 为极大理想或者素理想的判定方法.

命题 13.5.8 (教材定理 2.6.5)

考虑一个交换幺环 R , R 中的理想 I 为素理想, 当且仅当环 R/I 为整环.

证明. 商环 R/I 为一个整环, 当且仅当任取 $a, b \in R$ 满足,

$$(a + I)(b + I) = I,$$

有 $a + I = I$ 或者 $b + I = I$. 注意到

$$ab + I = (a + I)(b + I)$$

因此以上条件等价于若 $ab \in I$, 则有 $a \in I$ 或 $b \in I$. 即 I 是素理想. $\square$

考虑 $I = \{0\}$, 以上命题的一个直接推论如下.

推论 13.5.9 (教材推论 2.6.6)

记 R 为一个交换幺环. 环 R 为整环当且仅当 $\{0\}$ 为 R 的素理想.

命题 13.5.10

设 I 为交换幺环 R 的一个真理想. 那么我们有

- I 为极大理想, 当且仅当 R/I 为一个域.

证明. 由之前的命题我们知道, 环 R/I 为一个域当且仅当 R/I 中的理想只有 $\{0\}$ 和 R/I . 因此, 我们只需证明以下等价命题:

- 理想 I 极大当且仅当 R/I 中的理想只有 $\{0\}$ 和 R/I .

设 $\bar{J}$ 为 R/I 的一个理想. 我们记其关于自然映射 π 下的原像 $J := \pi^{-1}(\bar{J})$. 集合 J 满足以下性质:

- (i) $I \subset J$;

- (ii) J 为一个理想.
- (iii) $J = I$ 当且仅当 $\bar{J} = \{\bar{0}\}$;
- (iv) $J = R$ 当且仅当 $\bar{J} = R/I$.

因此 R/I 中存在不同与 $\{\bar{0}\}$ 和 R/I 的理想 $\bar{J}$, 当且仅当其原像 J 为 R 中包含 I 的真理想. 由于极大理想的定义, 我们得出, 理想 I 极大当且仅当 R/I 中的理想只有 $\{\bar{0}\}$ 和 R/I . $\square$

推论 13.5.11

考虑一个交换幺环 R . 若 I 为 R 的一个极大理想, 那么 I 也是 R 的素理想.

证明. 若 I 为 R 的极大理想, 那么 R/I 为一个域, 因此为一个整环. 因此由命题 13.5.8, I 为 R 的一个素理想. $\square$

注 13.5.12.

我们再给出一个比较直接的证明.

取 $a, b \in R^*$. 我们假设 $ab \in I$.

若 $a \notin I$, 那么, 我们考虑由 a 生成的主理想 $\langle a \rangle$. 我们有 $\langle a \rangle + I$ 为 R 的一个真包含 I 的理想. 因此

$$1 \in R = \langle a \rangle + I.$$

因此存在 $x \in R$ 和 $a' \in I$, 使得 $xa + a' = 1$, 那么我们考虑

$$(xa)b + a'b = x(ab) + a'b = b.$$

由于我们有 $ab \in I$ 以及 $a' \in I$, 我们可以得到 $b \in I$.

类似地, 若 $b \notin I$, 我们可以得到 $a \in I$. 因此, 我们知道对于任意 $ab \in I$, 我们必有 $a \in I$ 或 $b \in I$.

第十四章 环同态

14.1 定义

我们考虑环 R 和 R' . 记 $\phi: R \rightarrow R'$ 为一个从集合 R 到集合 R' 的映射. 为避免记号过于复杂, 在 R 的运算和 R' 的运算中我们都使用 $+$ 和 $\cdot$.

定义 14.1.1

映射 ϕ 被称为从环 R 到 R' 的**环同态映射(环同态)**, 若其满足以下条件:

- (i) 对于任意 $a, b \in R$, 我们有 $\phi(a + b) = \phi(a) + \phi(b)$;
- (ii) 对于任意 $a, b \in R$, 我们有 $\phi(ab) = \phi(a)\phi(b)$.

若同态 ϕ 为单射, 我们称其为**单同态**; 若其为满射, 我们称之为**满同态**; 若其为双射, 我们称之为**同构**.

注 14.1.2.

换句话说, 一个 R 到 R' 环同态是一个 R 到 R' 的映射, 既是关于加法群结构的同态也是关于乘法半群结构同态.

例 14.1.3.

设 I 为环 R 的一个理想. 自然映射 $\pi: R \rightarrow R/I$ 为一个满同态.

例 14.1.4.

我们考虑实数上的多项式环 $\mathbb{R}[x]$. 考虑其理想 $I = \langle x^2 + 1 \rangle$. 注意到任取 $f(x) \in \mathbb{R}[x]$, 我们考虑 $\mathbb{R}[x]$ 上的带余除法, 有

$$f(x) = p(x)(x^2 + 1) + r(x).$$

我们知道 $r(x) = a + bx$, 其中 $a, b \in \mathbb{R}$. 因此 $f(x) + I = r(x) + I$.

我们可以定义映射:

$$\begin{aligned}\phi: \mathbb{R}[x]/I &\rightarrow \mathbb{C} \\ a + bx + I &\mapsto a + bi\end{aligned}$$

可以验证这是一个环同构.

我们下边在给出一个特征为素数 p 的整环特有的自同态.

命题 14.1.5 (教材命题2.1.12)

若 R 为一个特征为素数 p 的整环, 则存在一个如下定义的同态映射:

$$\begin{aligned}\phi : R &\rightarrow R \\ a &\mapsto a^p\end{aligned}$$

证明. 使用二项式展开, 我们可以验证:

$$(a+b)^p = a^p + \sum_{j=1}^{p-1} C_p^j (a^{p-j} b^j) + b^p.$$

由于对于任意 $j \in \{1, \dots, p-1\}$, 我们有 $p \mid C_p^j$, 我们有 $(a+b)^p = a^p + b^p$. 另一方面, 由于环 R 交换, 我们有 $a^p b^p = (ab)^p$. 因此 ϕ 是一个同态. $\square$

注 14.1.6.

该同态被称为整环 R 上的 **Frobenius 同态**. 实际上, 任取交换幺环 R , 满足幺元 1 的阶为素数, 我们都可以定义此类同态. 其中素数的要求是必须的, 我们在证明中用到了如下结论:

- 对于任意 $j \in \{1, \dots, p-1\}$, 我们有 $p \mid C_p^j$.

当 p 不是素数是, 这个结论不对. 例如, $p = 12$, 那么

$$12 \nmid C_{12}^2 = (12 \cdot 11)/(2 \cdot 1) = 66.$$

考虑加法结构, 我们定义环同态的核如下:

定义 14.1.7

同态 ϕ 的核被定义为以下集合:

$$\ker \phi := \{a \in R \mid \phi(a) = 0' \in R'\},$$

这里 $0'$ 为环 R' 的零元.

我们沿用之前的记号用 $\text{Im } \phi$ 或 $\phi(R)$ 来记映射 ϕ 的像.

我们之前关于群同态的结论仍然成立.

命题 14.1.8

一个环同态 $\phi : R \rightarrow R'$ 为单同态当且仅当 $\ker \phi = \{0\}$.

命题 14.1.9

若 $\phi : R \rightarrow R'$ 为一个环同态, 那么

- (i) $\ker \phi$ 为 R 的理想;
- (ii) $\text{Im } \phi$ 为 R' 的一个子环 (不一定是理想).

进一步, 我们可以直接验证以下结论.

命题 14.1.10

设 I 为环 R 的一个理想. 我们考虑自然同态

$$\pi : R \rightarrow R/I,$$

则 $\ker \pi = I$.

14.2 环同态基本定理

类似于对群的讨论, 我们也有环同态基本定理.

14.2.1 环同态基本定理

关于本节部分结论的详细讨论可以参考附录 A. 我们首先考虑如下结论.

定理 14.2.1

设 I 为环 R 的一个理想. 任取环 R' 以及环同态 $\phi : R \rightarrow R'$, 若 $I \subset \ker \phi$, 则我们有唯一的环同态 $\bar{\phi} : R/I \rightarrow R'$, 满足以下交换图:

$$\begin{array}{ccc} R & \xrightarrow{\phi} & R' \\ \pi \downarrow & \nearrow \exists! \bar{\phi} & \\ R/I & & \end{array}$$

特别地, 我们有

$$\ker \bar{\phi} = \ker \phi / I.$$

证明. (见附录 A)

□

作为以上结论的推论, 我们有以下环同态基本定理

定理 14.2.2 (环第一同态基本定理)

设 R 和 R' 为两个环. 设

$$\phi : R \rightarrow R',$$

为一个环同态, 则我们有环同构:

$$R / \ker \phi \cong \operatorname{Im} \phi.$$

推论 14.2.3 (教材定理2.4.5 (1))

设 R 和 R' 为两个环. 设

$$\phi: R \rightarrow R',$$

为一个环满同态, 则我们有环同构:

$$R/\ker \phi \cong R'.$$

注 14.2.4.

换句话说, 若存在环 R 到环 R' 的满同态, 在同构意义下, 我们可以把 R' 看作是 R 的一个商环.

14.2.2 环同态与子环

我们下边讨论一个从 R 到 R' 的环同态是如何联系 R 的子环(理想)和 R' 的子环(理想).

命题 14.2.5

设 R 和 R' 为两个环. 设存在环同态

$$\phi: R \rightarrow R'.$$

- (i) 任取 R 的子环 A , 我们有 $\phi(A)$ 为 R' 的子环.
- (ii) 任取 R 的理想 I , 我们有 $\phi(I)$ 为 $\phi(R)$ 的理想.
- (iii) 任取 R' 的子环 B , 我们有 $\phi^{-1}(B)$ 为 R 的子环, 且 $\ker \phi \subset \phi^{-1}(B)$.
- (iv) 任取 R' 的理想 J , 我们有 $\phi^{-1}(J)$ 为 R 的理想, 且 $\ker \phi \subset \phi^{-1}(J)$.

证明. (练习)

□

命题 14.2.6

设 R 和 R' 为两个环. 设存在环同态

$$\phi: R \rightarrow R'$$

任取 R 的子环 A , 则有

- (i) $\phi(A) = \phi(A + \ker \phi)$;
- (ii) $A + \ker \phi = \phi^{-1}(\phi(A))$.

注 14.2.7.

这里要注意的是任取两个子环的和不一定是子环. 例如, 我们考虑 $\mathbb{R}$ 上的二元多项式环 $\mathbb{R}[x, y]$. 注意到 $\mathbb{R}[x]$ 和 $\mathbb{R}[y]$ 都可以看作是 $\mathbb{R}[x, y]$ 的子环. 但是 $\mathbb{R}[x] + \mathbb{R}[y]$ 不是 $\mathbb{R}[x, y]$

的子环. 子环需要对加法和乘法封闭. 我们这里有一个加法子群, 但是对乘法不封闭, 例如 $x \in \mathbb{R}[x]$, $y \in \mathbb{R}[y]$, 但是 $xy \notin \mathbb{R}[x] + \mathbb{R}[y]$.

另一方面, 记 R 为一个环, 任取子环 A 和理想 I , 我们有 $A + I$ 仍旧是 R 的子环. 我们只需验证 $A + I$ 对乘法封闭. 任取 $a, b \in A$ 以及 $x, y \in I$, 我们考虑

$$(a + x)(b + y) = ab + ay + xb + xy.$$

由于 I 是理想, 因此 $ay, xb \in I$, 所以我们有

$$(a + x)(b + y) \in A + I.$$

在以上命题中, $\ker \phi$ 是 R 的一个理想, 所以 $A + \ker \phi$ 仍是子环.

证明. (练习)

□

类似的结论对理想也成立.

命题 14.2.8

设 R 和 R' 为两个环. 设存在环同态

$$\phi : R \rightarrow R'$$

任取 R 的理想 I , 则有

- (i) $\phi(I) = \phi(I + \ker \phi)$;
- (ii) $I + \ker \phi = \phi^{-1}(\phi(I))$.

综合以上结论, 我们有下边的定理.

定理 14.2.9 (教材定理 2.4.5)

设 R 和 R' 为两个环. 设存在满同态:

$$\phi : R \rightarrow R'.$$

我们有如下结论:

- (i) ϕ 诱导以下 R 中包含 $\ker \phi$ 的子环的集合与 R' 中的子环的集合间的双射:

$$\phi : \{A \mid A \text{ 为 } R \text{ 的子环, 且 } \ker \phi \subset A\} \rightarrow \{B \mid B \text{ 为 } R' \text{ 的子环}\}$$

- (ii) ϕ 诱导以下 R 中包含 $\ker \phi$ 的理想的集合与 R' 中的理想的集合间的双射:

$$\phi : \{I \mid I \text{ 为 } R \text{ 的理想, 且 } \ker \phi \subset I\} \rightarrow \{J \mid J \text{ 为 } R' \text{ 的理想}\}$$

- (iii) 任取 R 的理想 I , 满足 $\ker \phi \subset I$, 我们有

$$R/I \cong R'/\phi(I).$$

证明. (练习)

□

我们下边考虑以上定理在环到商环自然同态这种特殊情形下的应用.

推论 14.2.10

设 R 为一个环 $I \subset R$ 为一个理想. 考虑自然同态:

$$\pi: R \rightarrow R/I.$$

我们有如下结论:

(i) π 诱导以下 R 中包含 I 的子环的集合与 R/I 中的子环的集合间的双射:

$$\pi: \{A \mid A \text{ 为 } R \text{ 的子环, 且 } I \subset A\} \rightarrow \{B \mid B \text{ 为 } R/I \text{ 的子环}\}$$

(ii) π 诱导以下 R 中包含 I 的理想的集合与 R/I 中的理想的集合间的双射:

$$\pi: \{J \mid J \text{ 为 } R \text{ 的理想, 且 } I \subset J\} \rightarrow \{L \mid L \text{ 为 } R/I \text{ 的理想}\}$$

(iii) 任取 R 的理想 J , 满足 $I \subset J$, 我们有

$$R/J \cong (R/I)/(J/I).$$

注 14.2.11.

(i) 和 (ii) 被称为环第四同构定理. (iii) 被称为环第三同构定理.

环同态基本定理有以下推论.

推论 14.2.12 (教材推论 2.4.8)

设 R 为一个环. 任取 R 的两个理想 I 和 J , 我们有

$$(I + J)/I \cong J/(I \cap J).$$

证明. 由命题 13.4.17, 我们知道 $I \cap J$ 为 J 的一个理想.

我们定义如下映射

$$\begin{aligned} \phi: I + J &\rightarrow J/(I \cap J) \\ a + x &\mapsto x + I \cap J \end{aligned}$$

我们首先验证以上定义良好. 设 $a, b \in I, x, y \in J$, 满足

$$a + x = b + y,$$

则有

$$a - b = y - x \in I \cap J.$$

因此

$$x + I \cap J = y + I \cap J.$$

下边证明这是一个环同态. 任取 $a, b \in I$, 以及 $x, y \in J$, 我们有

$$\begin{aligned} & \phi((a+x) + (b+y)) \\ &= \phi((a+b) + (x+y)) \\ &= (x+y) + I \cap J \\ &= x + I \cap J + y + I \cap J \\ &= \phi(a+x) + \phi(b+y) \end{aligned}$$

以及

$$\begin{aligned} & \phi((a+x)(b+y)) \\ &= \phi(ab + ay + xb + xy) \\ &= xy + I \cap J \\ &= (x + I \cap J)(y + I \cap J) \\ &= \phi(a+x)\phi(b+y) \end{aligned}$$

这里用到了 I 和 J 都是理想, 因此 $ay, xb \in I \cap J \subset I$. 因此 ϕ 为一个环同态. 我们下边确定 $\ker \phi$.

任取 $a \in I$ 以及 $x \in J$, 满足 $\phi(a+x) = I \cap J$, 则有 $x \in I \cap J$. 因此 $a+x \in I$. 由此可得

$$\ker \phi \subset I.$$

另一方面, 任给 $a \in I$, 我们有 $a = a + 0$, 进而有

$$\phi(a) = I \cap J,$$

因此 $a \in \ker \phi$. 由此可得

$$I \subset \ker \phi.$$

综上所述 $\ker \phi = I$. 由环同态基本定理, 我们有

$$I + J/I \cong J/(I \cap J).$$

□

注 14.2.13.

这个推论通常被称为环第二同构定理.

14.3 中国剩余定理

任取环 R 和 R' , 我们可以定义二者的直积 $R \times R'$ 如下. 我们考虑集合 $R \times R'$, 并定义加法和乘法为

$$\begin{aligned} + : (R \times R') \times (R \times R') &\rightarrow R \times R' & \cdot : (R \times R') \times (R \times R') &\rightarrow R \times R' \\ ((a, x), (b, y)) &\mapsto (a+b, x+y) & ((a, x), (b, y)) &\mapsto (ab, xy) \end{aligned}$$

记 R 为一个环, 任取 R 的两个理想 I 和 J , 我们考虑

$$IJ := \left\{ \sum_{i=1}^n a_i b_i \mid n \in \mathbb{N}^*, a_1, \dots, a_n \in I, b_1, \dots, b_n \in J \right\}.$$

设 R 为一个交换幺环.

定义 14.3.1

环 R 中的理想 I 和 J 被称为**互素的**, 若其满足 $I + J = R$.

注 14.3.2.

我们考虑 $\mathbb{Z}$ 中的理想 $p\mathbb{Z}$ 和 $q\mathbb{Z}$. 若 p 和 q 互素, 我们可以在 $p\mathbb{Z} + q\mathbb{Z}$ 中通过辗转相除的到 1. 若一个幺环中的理想包含 1, 那么这个理想就是整个环. 因此 $p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}$.

命题 14.3.3

设 R 为一个交换幺环. 任取 R 的两个理想 I 和 J , 我们有

$$IJ \subset I \cap J.$$

若进一步有 $I + J = R$, 则有

$$IJ = I \cap J.$$

证明. 任取 $a \in I, b \in J$, 由于 I 是理想因此 $ab \in I$. 同时, 由于 J 也是理想, 我们有 $ab \in J$. 因此 $ab \in I \cap J$. 因此, 我们有

$$IJ \subset I \cap J.$$

下边假设 $I + J = R$, 因此存在 $a \in I$ 以及 $b \in J$, 满足 $a + b = 1$. 任取 $c \in I \cap J$, 我们有

$$c = c \cdot 1 = c(a + b) = ca + cb.$$

注意到 $ca, cb \in IJ$, 因此 $ca + cb \in IJ$, 由此可得

$$I \cap J \subset IJ.$$

结合之前证明的结论, 此时有

$$IJ = I \cap J.$$

□

例 14.3.4.

我们首先给出一个例子说明确实存在 IJ 是 $I \cap J$ 的一个真子集.

考虑整数环 $\mathbb{Z}$ 的理想 $4\mathbb{Z}$ 和 $6\mathbb{Z}$. 注意到 $\gcd(4, 6) = 2$. 我们考虑

$$12 \in 4\mathbb{Z} \cap 6\mathbb{Z},$$

注意到任取 $m \in 4\mathbb{Z}, n \in 6\mathbb{Z}$, 我们有 $k, l \in \mathbb{Z}$ 满足

$$m = 4k, n = 6l,$$

因此

$$24\mathbb{Z} = (4\mathbb{Z})(6\mathbb{Z}),$$

但是 $12 \notin 24\mathbb{Z}$, 所以 $12 \notin (4\mathbb{Z})(6\mathbb{Z})$.

例 14.3.5.

注意到最后 $I + J = R$ 可以保证 $IJ = I \cap J$, 但 $I + J = R$ 并不是 $IJ = I \cap J$ 的必要条件. 我们考虑环 $\mathbb{Z}_6$. 记

$$I = J = \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}.$$

注意到

$$I \cap J = \langle \bar{2} \rangle.$$

另一方面, 我们有 $\bar{2} \cdot \bar{4} = \bar{2}$, $\bar{4} \cdot \bar{4} = \bar{4}$, 因此

$$IJ = \langle \bar{2} \rangle.$$

所以我们有 $IJ = I \cap J$. 但是 $I + J = \langle \bar{2} \rangle \neq \mathbb{Z}_6$.

推论 14.3.6

设 R 为一个交换幺环. 设 $k > 1$ 为一个非零自然数, 任取 R 的两两互素的理想 $I_1, \dots, I_k$, 我们有

$$I_1 \cdots I_k = I_1 \cap \cdots \cap I_k.$$

证明. 我们使用归纳法. 之前的命题已经证明了结论对 $k = 2$ 成立.

假设结论对小于 $k > 2$ 的情形都成立, 我们考虑 I_1 和

$$J_1 = I_2 \cap \cdots \cap I_k.$$

由归纳假设, 我们有

$$J_1 = I_2 \cdots I_k.$$

若我们可以证明 I_1 和 J_1 互素即可完成证明.

注意到任取 $i \neq j$, 我们有 $I_i + I_j = R$, 因此令 $i = 1$, 对任意 $j \neq i$, 存在 $a_j \in I_1$ 以及 $x_j \in I_i$, 满足

$$a_j + x_j = 1.$$

我们考虑

$$\begin{aligned} 1 &= (a_2 + x_2) \cdots (a_k + x_k) \\ &= \Sigma + x_2 \cdots x_k \end{aligned}$$

注意到 $\Sigma \in I_1$, $x_2 \cdots x_k \in J_1$, 因此右边属于 $I_1 + J_1$. 由此可得 $I_1 + J_1 = R$, 即 I_1 和 J_1 互素. $\square$

定理 14.3.7 (中国剩余定理)

设 R 为一个交换幺环. 设 k 为非零自然数, 任取 R 中 k 个理想 $I_1, \dots, I_k$. 并记 $\pi_1, \dots, \pi_k$ 为相应的自然映射, 则如下定义的映射是一个同态:

$$\begin{aligned}\phi: R &\rightarrow R/I_1 \times \cdots \times R/I_k; \\ a &\mapsto (\pi_1(a), \dots, \pi_k(a)).\end{aligned}$$

满足

$$\ker \phi = \bigcap_{j=1}^k I_j.$$

若进一步有 $I_1, \dots, I_k$ 两两互素, 则有 ϕ 为满射, 且

$$R/(I_1 \cdots I_k) = R/(\bigcap_{j=1}^k I_j) \cong R/I_1 \times \cdots \times R/I_k.$$

证明. 由 $\pi_1, \dots, \pi_k$ 的良好定义可得 ϕ 是一个映射.

任取 $a, b \in R$, 我们有

$$\begin{aligned}\phi(a+b) &= (\pi_1(a+b), \dots, \pi_k(a+b)) \\ &= (\pi_1(a) + \pi_1(b), \dots, \pi_k(a) + \pi_k(b)) \\ &= (\pi_1(a), \dots, \pi_k(a)) + (\pi_1(b), \dots, \pi_k(b)) \\ &= \phi(a) + \phi(b)\end{aligned}$$

以及

$$\begin{aligned}\phi(ab) &= (\pi_1(ab), \dots, \pi_k(ab)) \\ &= (\pi_1(a)\pi_1(b), \dots, \pi_k(a)\pi_k(b)) \\ &= (\pi_1(a), \dots, \pi_k(a))(\pi_1(b), \dots, \pi_k(b)) \\ &= \phi(a)\phi(b)\end{aligned}$$

因此 ϕ 是一个同态.

任取 $a \in R$, $a \in \ker \phi$ 当且仅当

$$\phi(a) = (a + I_1, \dots, a + I_k) = (I_1, \dots, I_k).$$

即

$$a \in \bigcap_{j=1}^k I_j.$$

因此

$$\ker \phi = \bigcap_{j=1}^k I_j.$$

下边假设 $I_1, \dots, I_k$ 两两互素. 由之前的推论知

$$I_1 \cdots I_k = I_1 \cap \cdots \cap I_k.$$

我们有

$$R/I_1 \cdots I_k = R/I_1 \cap \cdots \cap I_k.$$

最后还需证明此时 ϕ 是一个满射, 即任取

$$(a_1 + I_1, \dots, a_k + I_k) \in R/I_1 \times \cdots \times R/I_k,$$

存在一个 $a \in R$, 满足

$$\phi(a) = (a_1 + I_1, \dots, a_k + I_k).$$

我们可以先考虑 $k = 2$ 的情形. 由于 $I_1 + I_2 = R$, 因此存在 $x \in I_1$ 和 $y \in I_2$, 满足

$$x + y = 1.$$

任取 $a_1, a_2 \in R$, 我们有

$$\begin{aligned} a_1 + I_1 &= a_1x + a_1y + I_1 = a_1y + I_1 \\ a_2 + I_2 &= a_2x + a_2y + I_2 = a_2x + I_2 \end{aligned}$$

因此取

$$a = a_1y + a_2x,$$

则有

$$\begin{aligned} a + I_1 &= a_1y + a_2x + I_1 = a_1y + I_1 = a_1 + I_1 \\ a + I_2 &= a_1y + a_2x + I_2 = a_2x + I_2 = a_2 + I_2 \end{aligned}$$

因此我们证明了当 $k = 2$, 同态 ϕ 为满射.

下边考虑一般情形. 我们使用之前命题证明中的方法. 注意到 $I_1, \dots, I_k$ 两两互素, 任取 I_j , 对任意 $1 \leq i \leq k$ 且 $i \neq j$, 我们记 $b_{ij} \in I_j$, $x_{ij} \in I_i$, 满足对任意 $1 \leq i \leq k$ 且 $i \neq j$, 有

$$b_{ij} + x_{ij} = 1.$$

我们考虑

$$\begin{aligned} 1 &= \prod_{\substack{1 \leq i \leq k \\ i \neq j}} (b_{ij} + x_{ij}) \\ &= \Sigma_j + \prod_{\substack{1 \leq i \leq k \\ i \neq j}} x_{ij}. \end{aligned}$$

对任意 $1 \leq j \leq k$, 我们有

$$a_j + I_j = a_j \Sigma_j + a_j \prod_{\substack{1 \leq i \leq k \\ i \neq j}} x_{ij} + I_j = a_j \prod_{\substack{1 \leq i \leq k \\ i \neq j}} x_{ij} + I_j.$$

我们记

$$a = \sum_{j=1}^k \left(a_j \prod_{\substack{1 \leq i \leq k \\ i \neq j}} x_{ij} \right),$$

即满足

$$\phi(a) = (a_1 + I_1, \dots, a_k + I_k).$$

□

当我们考虑 $R = \mathbb{Z}$ 时, 就得到了我们常见的关于整数同余的中国剩余定理:

推论 14.3.8

设 k 为大于 0 的自然数. 任取大于 1 且两两互素的自然数 $n_1, \dots, n_k$, 我们有

$$\mathbb{Z}_{n_1 \cdots n_k} \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}.$$

换句话说, 任取整数 $y_1, \dots, y_k$, 以下关于整数的方程组在模 $n = n_1 \cdots n_k$ 的意义下有唯一解:

$$\begin{cases} x \equiv y_1 \pmod{n_1} \\ \dots \\ x \equiv y_k \pmod{n_k} \end{cases}$$

注 14.3.9.

推论中关于模方程组的结论包含了两层意思: 一是该方程组有解; 二是解唯一.

例 14.3.10 (韩信点兵).

有一个自然数在 1000 到 1100 之间满足

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

我们希望求出 x . 使用以上证明中的方法. 我们有

$$\begin{aligned} I_1 &= 3\mathbb{Z} : 6 + (-5) = 1, -6 + 7 = 1 \\ I_2 &= 5\mathbb{Z} : 6 + (-5) = 1, 15 + (-14) = 1 \\ I_3 &= 7\mathbb{Z} : -6 + 7 = 1, 15 + (-14) = 1 \end{aligned}$$

这里有

$$\begin{aligned} I_1 &= 3\mathbb{Z} : a_1 = 2, x_{21} = -5, x_{31} = 7 \\ I_2 &= 5\mathbb{Z} : a_2 = 4, x_{12} = 6, x_{32} = -14 \\ I_3 &= 7\mathbb{Z} : a_3 = 3, x_{13} = -6, x_{23} = 15 \end{aligned}$$

因此我们有

$$x \equiv 2 \times (-5) \times 7 + 4 \times 6 \times (-14) + 3 \times (-6) \times 15 = -592 \pmod{3 \times 5 \times 7 = 105}.$$

因此所求的值满足

$$1000 \leq -592 + 105k \leq 1100$$

因此

$$15 < k < 17.$$

因此 $x = -592 + 16 \times 105 = 1004$.

由以上推论, 我们也可以考虑涉及的环中的单位的对应:

推论 14.3.11

设 k 为大于 0 的自然数. 任取大于 1 且两两互素的自然数 $n_1, \dots, n_k$, 我们有

$$U_{n_1 \cdots n_k} \cong U_{n_1} \times \cdots \times U_{n_k},$$

其中对任意 $n \in \mathbb{Z}$, 我们记 U_n 为 $\mathbb{Z}_n$ 的单位群.

第十五章 一些特殊的整环

整数环 $\mathbb{Z}$ 中一个重要的概念就是"整除". 任给一个大于 1 的正整数, 我们可以将其分解为一些素数的乘积, 并且这个分解是唯一的.

整数环 $\mathbb{Z}$ 上可以做的另一件事就是带余除法. 利用辗转相除, 我们可以证明 Bezout 等式. 任取 $m, n \in \mathbb{N}^*$, 记 $d = \gcd(m, n)$, 则存在 $p, q \in \mathbb{Z}$, 满足

$$pm + qn = d.$$

这里 d 是 m 和 n 的最大公约数.

在这一部分, 我们希望将以上概念推广到对一般整环的研究中.

15.1 定义

整除和相伴

我们首先如下推广整除的概念.

定义 15.1.1 (教材定义 2.5.1, 2.5.2, 2.5.3)

设 R 为一个交换幺环. 任给 $a, b \in R$, 若我们可以找到元素 $c \in R$, 使得 $ac = b$, 我们就称 a 整除 b , 记作 $a \mid b$. 此时, 我们称 a 为 b 的**因子**. 若我们还有 $b \nmid a$, 则称 a 为 b 的**真因子**.

任给 $a, b \in R^*$, 若 $a \mid b$, 且 $b \mid a$, 那么我们称元素 a 和元素 b **相伴**, 记作 $a \sim b$.

注 15.1.2.

教材上考虑的是整环, 实际上我们可以在交换幺环讨论.

例 15.1.3.

任取 $m \in \mathbb{Z}^*$, 我们有 $m \sim -m$.

例 15.1.4.

考虑实数上的多项式环 $\mathbb{R}[x]$. 令

$$f(x) = x^2 + 3x + 2, \quad g(x) = x + 1.$$

令

$$h(x) = x + 2$$

我们有

$$f(x) = g(x)h(x).$$

因此

$$g(x) \mid f(x),$$

由此可得 $g(x)$ 是 $f(x)$ 的因子. 另一方面, 注意到 f 的次数是 2, 而 g 的次数是 1, 因此 $f(x) \nmid g(x)$. 所以 $g(x)$ 是 $f(x)$ 的真因子. 因此 $g(x)$ 和 $f(x)$ 不相伴.

注意到, $f(x) = f(x) \cdot 1$, 因此 $f(x)$ 也是 $f(x)$ 的因子. 但是 $f(x)$ 不是 $f(x)$ 的真因子. 我们这里有 $f(x)$ 与 $f(x)$ 相伴.

我们还可以进一步考虑以下关系

$$f(x) = \frac{1}{2} \cdot (2f(x)),$$

因此 $2f(x) \mid f(x)$. 另一方面, 我们有

$$2f(x) = 2 \cdot f(x),$$

因此 $f(x) \mid 2f(x)$. 所以 $2f(x)$ 也和 $f(x)$ 相伴.

注 15.1.5.

注意到两个非零自然数相伴当且仅当它们相等. 以上例子告诉我们"相伴"可以看作是"相等"的某种推广.

命题 15.1.6

记 R 为一个整环. 记 U 为 R 的单位群. 任取两个相伴的元素 $a, b \in R^*$, 则存在 $u \in U$, 满足

$$a = ub.$$

证明. 任取 $a, b \in R$, 若 $a \sim b$, 则有 $a \mid b$ 且 $b \mid a$. 因此存在 $u, v \in R$, 满足

$$a = ub, \quad b = va.$$

由以上两个等式知

$$b = uvb,$$

由于 R 为整环, 没有零因子, 因此利用消去律, 我们有

$$1 = uv,$$

因此 $u, v \in U$. 我们有

$$a = ub.$$

□

注 15.1.7.

以上命题告诉我们, 若 R 是一个整环, 则 $a, b \in R^*$ 相伴当且仅当存在 $u \in U$, 满足

$$a = ub.$$

后边当我们考虑整环的时候, 与整除相关的概念通常是在相差一个单位的前提下(相伴的意义下)讨论的.

思考 15.1.8

若 R 为交换幺环, 则以上结论还成立么?

例 15.1.9.

以下例子来自 Kaplansky. 这个例子告诉我们在一般的交换幺环中, 相伴的元素不一定是相差一个单位.

我们考虑 $R = C[0, 3]$ 为区间 $[0, 3]$ 上的连续实函数的集合. 任取 $f, g \in C[0, 3]$, 我们定义加法和乘法分别为

$$(f + g)(x) := f(x) + g(x), \quad (f \cdot g)(x) = f(x) \cdot g(x).$$

注意到零元 $\mathbf{0}$ 为值取 0 的常值函数, 幺元 $\mathbf{1}$ 为值取 1 的常值函数. 注意到这个环并不是整环.

下边取

$$f(x) = \begin{cases} 1-x, & x \in [0, 1] \\ 0, & x \in [1, 2] \\ x-2, & x \in [2, 3] \end{cases} \quad g(x) = \begin{cases} 1-x, & x \in [0, 1] \\ 0, & x \in [1, 2] \\ 2-x, & x \in [2, 3] \end{cases}$$

注意到两个函数在 $[0, 1]$ 上相同, 在 $[2, 3]$ 互为相反数. 我们可以构造一个函数在 $[0, 1]$ 上取 1, 在 $[2, 3]$ 上取 -1 . 要保证连续性, 我们需要其在 $[1, 2]$ 上取值"连接" 1 和 -1 . 注意到 f 和 g 在 $[1, 2]$ 上取值为 0, 因此我们可以考虑以下函数

$$t(x) = \begin{cases} 1 & x \in [0, 1] \\ 3-2x & x \in [1, 2] \\ -1 & x \in [2, 3] \end{cases}$$

因此

$$f(x) = t(x)g(x), \quad g(x) = t(x)f(x).$$

即有

$$f(x) \sim g(x).$$

另一方面, $t(3/2) = 0$, 因此 $t(x)$ 不可逆.

实际上任取 $t(x) \in C[0, 3]$, 满足

$$f(x) = t(x)g(x).$$

由中值定理, 存在 $x \in [1, 2]$, 满足 $t(x) = 0$, 因此不存在 $C[0, 3]$ 中的单位 $u(x)$, 满足 $f(x) = u(x)g(x)$.

最大公因子

当 we 有多个环元素的时候, 可以考虑它们的公共的因子.

定义 15.1.10

记 R 为一个交换幺环. 任给 $a, b \in R^*$, 若 $d \in R$ 满足

$$d \mid a, \quad d \mid b,$$

我们称 d 为 a 和 b 的**公因子**.

若 a 和 b 的公因子 d 进一步满足, 对任意 $c \in R$, 满足 $c \mid a$, 且 $c \mid b$, 都有 $c \mid d$, 我们称 d 为 a 和 b 的**最大公因子**, 记作 $\gcd(a, b)$.

关于最大公因子的进一步讨论参考附录??.

例 15.1.11.

考虑实数上的多项式环 $\mathbb{R}[x]$. 任取两个多项式 $f(x), g(x) \in \mathbb{R}[x]$, 我们可以对它们做辗转相除得到二者的最大公因子.

需要指出的是, 我们可以在环上讨论多项式. 但是只有当环是一个域的时候, 我们才可以在其上利用辗转相除来得到最大公因子. (我们后边会证明只有环 R 上的多项式环才是欧几里得整环当且仅当这个环 R 是一个域)

例 15.1.12.

对一般的环, 最大公因子并不总是存在. 我们考虑

$$\mathbb{Z}[\sqrt{-3}] := \{m + n\sqrt{-3} \mid m, n \in \mathbb{Z}\}.$$

令

$$a = 4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}), \quad b = 2(1 + \sqrt{-3}).$$

注意到 2 和 $1 + \sqrt{-3}$ 都是 a 和 b 的极大公因子. 但是二者不是相伴的.

要弄明白这点, 我们可以考虑 $\mathbb{Z}[\sqrt{-3}]$ 上的函数:

$$N(m + n\sqrt{-3}) = m^2 + 3n^2.$$

注意到任取

$$c = k + l\sqrt{-3}, \quad d = m + n\sqrt{-3},$$

我们有

$$cd = (km - 3ln) + (kn + lm)\sqrt{-3}.$$

直接计算验证:

$$N(cd) = (km - 3ln)^2 + 3(kn + lm)^2 = (k^2 + 3l^2)(m^2 + 3n^2) = N(c)N(d).$$

注意到 $\mathbb{Z}[\sqrt{-3}]$ 上所有元素在 N 下的像都是正整数, 因此若 $c, d \in \mathbb{Z}[\sqrt{-3}]$ 满足

$$cd = 1,$$

则有

$$N(c) = N(d) = 1.$$

所以 $c, d \in \{1, -1\}$.

若存在 $u \in \mathbb{Z}[\sqrt{-3}]$, 满足

$$2u = 1 + \sqrt{-3},$$

则有 $N(u) = 1$, 矛盾. 因此 $2 \nmid 1 + \sqrt{-3}$, 也即二者不相伴.

素元素和不可约元素

在 $\mathbb{Z}$ 中, 任取素数 p , 都满足以下性质:

- (i) 任取整数 $m, n \in \mathbb{Z}$, 若 $p \mid mn$, 则有 $p \mid m$ 或者 $p \mid n$.
- (ii) 任取整数 k 满足 $k \mid p$, 则有 $k = \pm 1$ 或者 $\pm p$.

我们想把以上讨论推广到对一般的交换环的讨论中. 我们先考虑以下两个例子

例 15.1.13.

我们考虑例子15.1.12中关于环 $\mathbb{Z}[\sqrt{-3}]$ 的讨论, 我们有

$$1 + \sqrt{-3} \mid 2 \cdot 2,$$

但是

$$1 + \sqrt{-3} \nmid 2.$$

另一方面, 任取 $a \in \mathbb{Z}[\sqrt{-3}]$, 满足

$$a \mid 1 + \sqrt{-3},$$

我们有

$$N(a) \mid N(1 + \sqrt{-3}) = 4.$$

因此

$$N(a) \in \{1, 2, 4\}.$$

设 $a = u + v\sqrt{-3}$, 其中 $u, v \in \mathbb{Z}$, 我们有

$$N(a) = u^2 + 3v^2.$$

因此 $N(a) \neq 2$. 若 $N(a) = 4$, 则有 $(|u|, |v|) = (2, 0)$ 或者 $(1, 1)$. 注意到

$$2 \nmid 1 + \sqrt{-3}.$$

综上所述, 我们有 $a \in \{1, -1, 1 + \sqrt{-3}, -1 - \sqrt{-3}\}$.

因此, 这里 $1 + \sqrt{-3}$ 满足条件 ii 但是不满足条件 i.

由之前的讨论知

$$2 \nmid 1 + \sqrt{-3} \text{ 且 } 2 \nmid 1 - \sqrt{-3},$$

但是

$$2 \mid (1 + \sqrt{-3})(1 - \sqrt{-3}) = 4.$$

因此 2 不满足 ii. 另一方面, 利用以上对 $1 + \sqrt{-3}$ 的讨论, 我们可以证明, 任取 $a \in \mathbb{Z}[\sqrt{-3}]$, 满足 $a \mid 2$, 都有

$$a \in \{\pm 1, \pm 2\}.$$

所以 2 满足 i.

定义 15.1.14

记 R 为一个交换幺环. 任取元素 $p \in R^* \setminus U$, 我们称 p 为**素元素**, 若任取 $a, b \in R$, 若 $p \mid ab$, 则有

$$p \mid a \text{ 或 } p \mid b.$$

注 15.1.15.

我们考虑整数环 $\mathbb{Z}$. 若 $m \in \mathbb{Z}$ 为一个素元素, 则存在素数 p , 满足 $m = p$ 或者 $m = -p$.

定义 15.1.16

记 R 为一个交换幺环. 任取元素 $a \in R^* \setminus U$, 我们称 a **不可约的**, 若任取 $b, c \in R^*$, 满足 $a = bc$,

$$b \in U \text{ 或 } c \in U.$$

若 a 不满足这个条件, 我们称之为**可约的**.

定义 15.1.17

记 R 为一个交换幺环. 记 $a \in R^*$, 任取 $b \in R^*$,

(i) 若 b 满足 $b \mid a$, 但 $a \nmid b$, 我们称 b 为 a 的**真因子**.

(ii) 若 $b \in U$ 或者 $b \sim a$, 则称 b 为 a 的**平凡因子**.

注 15.1.18.

一个元素不可约实际上是说当我们试图将一个元素分解为一些元素乘积的时候, 所分解出来的部分要么是可逆的, 要么与该元素相伴, 因此都是平凡的.

从之前的例子可以看出, 对一般的交换幺环, 素元素的条件和可约元素的条件相互之间没有推出关系. 当我们考虑整环的时候有如下命题.

命题 15.1.19

设 R 为一个整环, 若元素 $p \in R$ 为一个素元素, 那么 p 是不可约的.

证明. 设 $a, b \in R$, 满足 $p = ab$, 则 $p \mid a$ 或者 $a \mid b$.

不失一般性地, 我们设 $p \mid a$, 则存在 $u \in R$, 满足

$$a = pu.$$

因此我们有

$$p = bup.$$

由于 R 没有零因子, 因此有右消去律.

$$1 = bu.$$

由此可得 $b, u \in U$, 所以 p 不可约. □

从理想的角度再看整除

记 R 为一个交换幺环. 任取 $a \in R$, 由元素 a 生成的主理想记作 $\langle a \rangle$.

引理 15.1.20

记 $b \in R$. 我们有 $a \mid b$ 当且仅当 $b \in \langle a \rangle$.

证明. 若 $b \in \langle a \rangle$, 则存在 $x \in R$, 满足 $b = ax$, 因此 $a \mid b$.

若 $a \mid b$, 因此存在 $x \in R$, 满足 $b = ax \in \langle a \rangle$. □

我们可以验证以下结论.

命题 15.1.21

任取元素 $a, b \in R^*$, 我们有 $a \mid b$ 当且仅当 $\langle b \rangle \subset \langle a \rangle$;

证明. 假设 $a \mid b$, 则存在 $c \in R$, 满足

$$b = ac \in \langle a \rangle.$$

任取 $x \in R$, 我们有

$$bx = xca \in \langle a \rangle$$

因此

$$\langle b \rangle \subset \langle a \rangle.$$

反过来假设

$$\langle b \rangle \subset \langle a \rangle,$$

我们有

$$b \in \langle a \rangle,$$

由引理 15.1.20 得 $a \mid b$. □

推论 15.1.22

- 1) 任取元素 $a, b \in R^*$, 我们有 $a \sim b$ 当且仅当 $\langle b \rangle = \langle a \rangle$;
- 2) 任取元素 $a \in R^*$, 我们有 $a \sim 1$ 当且仅当 $\langle a \rangle = R$.

证明. 1) 若 $a \sim b$, 则有 $a \mid b$ 且 $b \mid a$, 由命题 15.1.21 我们有

$$\langle b \rangle \subset \langle a \rangle \text{ 且 } \langle a \rangle \subset \langle b \rangle.$$

因此我们有

$$\langle b \rangle = \langle a \rangle.$$

2) 若 $b = 1$, 则

$$\langle 1 \rangle = R \cdot 1 = R.$$

由 1) 的结论知若 $1 \sim a$, 我们有

$$\langle a \rangle = R.$$

□

命题 15.1.23

记 R 为一个交换幺环. 元素 $a \in R^*$ 为一个素元素, 当且仅当 $\langle a \rangle$ 为一个素理想.

证明. 设 $\langle a \rangle$ 是一个素理想. 任取 $b, c \in R$ 满足 $a \mid bc$, 由引理 15.1.20 有

$$bc \in \langle a \rangle.$$

由于 $\langle a \rangle$ 为素理想, 我们有

$$b \in \langle a \rangle \text{ 或者 } c \in \langle a \rangle.$$

因此由引理 15.1.20, 我们有

$$a \mid b \text{ 或者 } a \mid c.$$

因此 a 是一个素元素.

反过来设 a 为一个素元素. 任取 $b, c \in R$, 满足 $bc \in \langle a \rangle$, 由引理 15.1.20, 我们有

$$a \mid bc.$$

由于 a 为一个素元素, 我们有

$$a \mid b \text{ 或者 } a \mid c.$$

因此

$$b \in \langle a \rangle \text{ 或者 } c \in \langle a \rangle.$$

由此可知 $\langle a \rangle$ 为一个素理想. □

15.2 唯一分解整环

15.2.1 定义

任取一个非零非幺元的整数 $m \in \mathbb{Z}$, 在相差一个正负号的前提下, 我们可以将其写为有限多个素数的乘积, 在不考虑顺序的情况下, 这些素数是唯一的. 我们将对这个性质的讨论推广到对一般的整环的讨论中. 本节我们将主要关心什么样的整环里的也有这样的性质.

由于本节开始我们只考虑整环 Integral Domain, 我们以下将使用记号 D 来代表环.

定义 15.2.1

一个整环 D 是一个**唯一分解整环**(unique factorization domain), 若其满足

(i) 任意元素 $a \in D^* \setminus U$ 都可以写成有限多个不可约元素的乘积, 即

• 任取 D 中的元素 $a \in D^* \setminus U$, 存在不可约元素 $p_1, \dots, p_m$, 使得

$$a = p_1 \cdots p_m,$$

(ii) 这样的分解在相伴意义下是唯一, 即:

• 若存在不可约元素 $p_1, \dots, p_m, q_1, \dots, q_n$, 满足

$$a = p_1 \cdots p_m = q_1 \cdots q_n,$$

那么我们有 $m = n$, 且存在一个置换 $\sigma \in S_m$, 使得 $p_i \sim q_{\sigma(i)}$.

注 15.2.2.

我们定义乘法是二元运算, 由归纳法可以考虑任意有限多个元素的乘积, 而通常我们也只考虑有限多个元素的乘积. 当然这里的元素个数可以是任意大. 因此第一个条件的重点不在有限上, 而在所有元素都不可约. 一般的整环中, 不一定所有的元素都可以写成不可约元素的乘积.

若 D 为一个环不满足第一个条件, 则存在一个元素 $a \in R^* \setminus U$, 任取 a 的分解

$$a = p_1 \cdots p_k,$$

存在某个 $1 \leq j \leq k$, 元素 p_j 可约.

注 15.2.3.

定义中的条件有两个, (i) 是说任意 D 中的非零非幺元都可以写为有限多个不可约元素的乘积, (ii) 是说这种写法(在某种意义上)是唯一的. 下边我们给出一些不满足这些条件的例子.

注意这个定义和书上的定义使用的条件有所不同, 但是与书上的定义等价. (参考 15.2.14.)

注 15.2.4.

需要注意的是关于 UFD 的讨论通常会在相伴的意义下进行, 有时讨论的过程所希望表达的意思比较简单, 但是详细叙述起来, 由于相伴的存在, 会比较复杂.

例 15.2.5.

考虑整环 $D = \mathbb{Z}[\sqrt{-3}]$. 利用函数

$$\begin{aligned} N : \mathbb{Z}[\sqrt{-3}] &\rightarrow \mathbb{N} \\ m + n\sqrt{-3} &\mapsto m^2 + 3n^2 \end{aligned}$$

我们可以验证 $\mathbb{Z}[\sqrt{-3}]$ 满足有限分解条件, 但是不满足唯一性. 以下是一个反例:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

例 15.2.6.

考虑整环 $D = \mathbb{Z} + x\mathbb{Q}[x]$. 注意到 0 次多项式是 $\mathbb{Z}$, 因此任取次数大于 0 的多项式

$$f(x) \in \mathbb{Z} + x\mathbb{Q}[x],$$

我们不再有

$$2f(x) \sim f(x).$$

例如我们有 $x \mid 2x$, 但是 $2x \nmid x$.

类似地讨论告诉我们, 任取 D 中 0 次项系数为 0 的非零多项式, 都不是不可约多项式. 另一方面, 任意两个 0 次项不为 0 的 D 中的多项式的乘积的 0 次项也不为 0. 因此我们考虑 x 可以将其写为:

$$x = 2 \cdot \frac{x}{2} = 2 \cdot 3 \cdot \frac{x}{3!} = 2^n \cdot \frac{x}{2^n}.$$

不满足有限分解的性质.

我们希望将一个非单位元素的不可约元素分解写为类似于素数分解的形式, 即一些两两互素的素数的幂次的乘积, 但是两个相伴的元素不一定相等. 因此我们需要引入一个单位来帮助我们.

引理 15.2.7

记 D 为一个 UFD. 任取 $a \in D^* \setminus U$, 存在非零自然数 k , 以及两两不相伴的不可约元素 $p_1, \dots, p_k$ 和单位 $u \in U$, 满足

$$a = up_1^{m_1} \cdots p_k^{m_k},$$

其中 $m_1, \dots, m_k \in \mathbb{N}^*$.

进一步地, 若 a 有两种不同的写法

$$a = up_1^{m_1} \cdots p_k^{m_k} = vq_1^{n_1} \cdots q_l^{n_l},$$

则有 $k = l$, 且存在 $\sigma \in S_k$, 满足

$$\begin{aligned} p_1 &\sim q_{\sigma(1)}, \dots, p_k \sim q_{\sigma(k)} \\ m_1 &= n_1, \dots, m_k = n_k. \end{aligned}$$

证明. 由于 D 为一个 UFD, 因此任给 $a \in D^* \setminus U$, 存在非零自然数 n 以及不可约元素 $p_1, \dots, p_n$, 满足

$$a = p_1 \cdots p_n.$$

考虑 $p_1, \dots, p_n$ 之间是否相伴, 存在非零自然数 k , 使得 a 可以重写为

$$a = (p_{11} \cdots p_{1m_1}) \cdots (p_{k1} \cdots p_{km_k}),$$

其中对任意 $1 \leq i \neq j \leq k$, 我们有

$$p_{i1} \not\sim p_{j1},$$

且对任意 $1 \leq i \leq k$, 以及 $1 \leq j \leq m_i$, 我们有

$$p_{i1} \sim p_{im_i}.$$

则对任意 $1 \leq i \leq k$, 存在 $u_{i2}, \dots, u_{im_i}$, 满足

$$p_{i2} = u_{i2}p_{i1}, \dots, p_{im_i} = u_{im_i}p_{i1}.$$

将其代入 a 的表达式, 我们有

$$a = \left(\prod_{i=1}^k \prod_{j=2}^{m_i} u_{ij} \right) p_{11}^{m_1} \cdots p_{k1}^{m_k}.$$

令

$$u = \left(\prod_{i=1}^k \prod_{j=2}^{m_i} u_{ij} \right)$$

$$p_1 = p_{11}$$

$$\dots$$

$$p_k = p_{k1}$$

即得命题第一部分的结论.

若 $a \in D^* \setminus U$ 有两种以上形式的不可约分解

$$a = p_1 \cdots p_m = q_1 \cdots q_n,$$

我们可以将两种写法分别按照相伴元素进行分类得到

$$a = (p_{11} \cdots p_{1m_1}) \cdots (p_{k1} \cdots p_{km_k}) = (q_{11} \cdots q_{1n_1}) \cdots (q_{l1} \cdots q_{ln_l}).$$

由于 D 为 UFD, 因此对任意 p_{i1} , 存在 q_{j1} 满足 $p_{i1} \sim q_{j1}$. 下证 $m_i = n_j$. 否则, 我们不妨设 $m_j > n_j$.

由于 D 为 UFD, 存在 $\sigma \in S_m$, 满足 $p_i \sim q_{\sigma(i)}$. 对 $q_1, \dots, q_n$ 重新排列, 我们不妨设

$$p_{i1} \sim q_{j1}, \dots, p_{in_j} \sim q_{jn_j}.$$

此外, 存在 $p_{i(n_j+1)} \sim q_{st}$, 其中 $s \neq j$, 所以 $q_{st} \sim q_{j1}$. 但是 $p_{i(n_j+1)} \sim p_{i1} \sim p_{j1}$, 矛盾. 因此对任意 $1 \leq i \leq k$, 存在唯一的 $1 \leq j \leq l$, 满足 $m_i = n_j$.

又由于

$$\sim_{i=1}^k m_i = m = n = \sum_{j=1}^l n_l,$$

因此 $k = l$.

□

注 15.2.8.

考虑整数环 $\mathbb{Z}$, 任取 $n \in \mathbb{Z} \setminus \{0, \pm 1\}$, 存在非零自然数 k , 两两互素的素数 $p_1, \dots, p_k$, 以及 $\epsilon \in \{1, -1\}$, 满足

$$n = \epsilon p_1^{m_1} \cdots p_k^{m_k},$$

其中 $m_1, \dots, m_k \in \mathbb{N}^*$.

注 15.2.9.

考虑实数上的多项式环 $\mathbb{C}[x]$, 任取次数大于 0 的多项式 $f(x) \in \mathbb{C}[x]$, 存在非零自然数 k , 以及复数 $z_1, \dots, z_k$ 以及非零复数 $z \in \mathbb{C}^*$, 满足

$$f(x) = z(x - z_1)^{m_1} \cdots (x - z_k)^{m_k}.$$

其中 $m_1, \dots, m_k \in \mathbb{N}^*$.

任取 $n \in \mathbb{N} \setminus \{0, 1\}$, 我们在尝试利用因子分解来寻找 n 的素数分解.

如果 n 是素数, 那么 $n = n$ 就是 n 的素数分解; 否则, 我们可以将 n 写成两个大于 1 的自然数的乘积 $n = n_1 n_2$, 若 n_1 和 n_2 都是素数, 则我们已经得到了 n 的素数分解; 否则, n_1 或者 n_2 不是素数, 因此我们可以继续将其分解. 注意到每一步新的得到的自然数总是比之前的小, 所以这个过程在进行有限步之后会停下来, 此时我们就得到了 n 的素数分解.

对于一个一般的 n , 这样的过程可能不止一种. 比如

$$12 = 3 \times 4 = 2 \times 6,$$

但是不管, 我们进行哪一种分解, 总是在有限步终止.

我们可以将这个讨论推广到对一般的整环的研究中. 记 D 为一个整环, 任取 D 中一个非零元非单位的元素 a , 我们可以考虑对 a 做因子分解, 尝试将其写为不可约元素的乘积. 类似于对自然数的讨论, 若 a 已经是不可约的, 则目标已经完成; 否则, 我们可以将其写为两个非单位真因子的乘积 $a = bc$. 考虑 b 和 c 是否都是不可约元素, 若是则目标已经完成; 否则, 我们可以进一步将 b 或者 c 分解为两个非单位真因子的乘积. 如此重复, 我们称这个过程为 a 的真因子分解. 这个过程可能有限, 可能无限(参考例子 15.2.6).

定义 15.2.10

记 D 为一个整环. 若任取非零非单位元素 $a \in D$ 的任意因子分解总是在有限步终止, 则称 D 满足**有限分解条件**.

在考虑一个非零非单位的元素进行因子分解的过程中, 我们会得到一系列元素满足后一个是前一个的真因子. 我们给出如下定义.

定义 15.2.11

记 D 为一个整环. 记 $N > 0$ 为一个自然数, $(a_0, \dots, a_N)$ 为 D^* 中的一列元素, 满足任取 $0 \leq n \leq N-1$, 我们有 a_{n+1} 是 a_n 的真因子. 这样的序列被称为 D 中的一个**有限真因子链**.

记 $(a_n)_{n \in \mathbb{N}}$ 为 D^* 中的一列元素, 满足任取 $n \in \mathbb{N}$, 我们有 a_{n+1} 是 a_n 的真因子. 这样的序列被称为 D 中的一个**无限真因子链**.

定义 15.2.12

记 D 为一个整环. 若 D 中所有的真因子链都有限, 我们称 D 满足**因子链条件**.

命题 15.2.13

记 D 为一个整环, 若 D 满足有限分解条件, 当且仅当 D 满足因子链条件.

证明. 我们证明 D 不满足有限分解条件, 当且仅当 D 不满足因子链条件.

若 D 不满足有限分解条件, 则存在一个非零非单位元素 a , 及其一系列因子分解

$$\begin{aligned} a &= a_0 b_0 \\ &= a_1 b_0 b_0 \\ &= \dots \\ &= a_n b_0 \cdots b_n \\ &= \dots \end{aligned}$$

其中 a_0 是 a 的真因子, 且对任意 $n \in \mathbb{N}$, a_{n+1} 是 a_n 的一个真因子. 由此, 我们可以得到一个无限真因子列

$$(a, a_0, a_1, \dots).$$

因此 D 不满足因子链条件.

反过来, 设 D 不满足因子链条件, 则存在一个无限真因子链

$$(a_0, a_1, \dots)$$

注意到对任意 $n \in \mathbb{N}$, 存在非零非单位元素 $b_{n+1} \in R$, 满足

$$a_n = a_{n+1} b_{n+1}.$$

因此我们有 a_0 的如下因子分解

$$\begin{aligned} a_0 &= a_1 b_1 \\ &= a_2 b_1 b_1 \\ &= \cdots \\ &= a_n b_1 \cdots b_n \\ &= \cdots \end{aligned}$$

这个过程不会停止. 因此 D 不满足有限分解条件. $\square$

注 15.2.14.

注意到我们使用的 UFD 的定义中的第一个条件是存在一个有限不可约分解, 而教材中的第一个条件是所有的因子分解都是有限的. 后者是一个比前者更强的结论, 从逻辑上讲二者是不同的. 但是在加上唯一性条件之后二者等价. 这是由于 UFD 中不可约因子是素因子, 加上我们可以使用消去律, 因此存在一个有限不可约分解, 那么所有的因子分解都必须有限. 我们将在下一节中详细讨论.

15.2.2 唯一分解的等价条件

素条件与公因子条件

我们这里在引入另外两个来自整数环的性质. 注意到在 $\mathbb{Z}$ 中一个素元素总是形如 p 或者 $-p$, 其中 p 为素数. 另一方面, 整数环中的素元素也是不可约元素. 在之前对素元素和不可约元素的讨论中, 我们知道在一个整环中一个素元素总是不可约的, 但是反过来却不一定. 我们引入如下条件:

定义 15.2.15

记 D 为一个整环. 若 D 中不可约元素也是素元素, 我们称 D 满足**素条件**.

整数环的另外一个性质是最大公因子的存在性, 即任取 $m, n \in \mathbb{Z}$, 它们的最大公因子 $\gcd(m, n)$ 总是存在的. 之前关于最大公因子的讨论中, 我们知道这个性质不是所有整环都满足的.

定义 15.2.16

记 D 为一个整环. 若 D 中任意两个元素的最大公因子都存在, 我们称 D 满足**公因子条件**.

我们将证明这一个 UFD 总是满足这两个条件.

不可约分解与整除

记 D 为一个 UFD. 通过将所有元素唯一的写成不可约元素的乘积, 我们可以证明 D 满足素条件和公因子条件. 我们首先讨论一下在一个 UFD 中不可约元素分解与整除之间的关系. 在这部分中, 我们将在相伴的意义下讨论问题, 所以我们将只考虑 D 中的非单位元素.

引理 15.2.17

记 D 为一个 UFD. 任给 $b \in D^* \setminus U$, 记 b 的不可约元素分解为

$$b = vp_1^{j_1} \cdots p_m^{j_m},$$

其中 $v \in U$, $p_1, \dots, p_m$ 为两两不相伴的不可约元素, $j_1, \dots, j_m \in \mathbb{N}^*$, 任取 $a \in D^* \setminus U$, 则以下两个叙述等价

- (i) $a \mid b$.
- (ii) 存在非零自然数 $k \leq m$, $u \in U$ 为单位, $i_1, \dots, i_k \in \mathbb{N}^*$ 满足 $i_1 \leq j_1, \dots, i_k \leq j_k$, 使得

$$a = up_1^{i_1} \cdots p_k^{i_k}.$$

证明. • (ii) $\implies$ (i): 直接验证即可. 任取 $a, b \in D^*$, 若 a 和 b 的不可约元素分解满足以上条件, 则可取

$$x = vu^{-1}p_1^{j_1-i_1} \cdots p_k^{j_k-i_k}.$$

则有

$$ax = b.$$

- 下边证明**必要性**. 我们记 b 的不可约分解为

$$b = vp_1^{j_1} \cdots p_m^{j_m}$$

其中 $p_1, \dots, p_m$ 是两两不相伴的不可约元素, $j_1, \dots, j_m \in \mathbb{N}^*$, $v \in U$ 为单位.

若 $a \mid b$, 则存在 $x \in D$, 满足

$$ax = b.$$

若 x 为单位, 则 a 有如下不可约因子分解

$$a = xvp_1^{i_1} \cdots p_m^{i_m}$$

令 $u = xv$ 即得到所需表达式.

下边考虑 x 非单位的情形. 我们考虑 a 和 x 的不可约元素分解

$$\begin{aligned} a &= u_0 q_1^{i_1} \cdots q_k^{i_k} \\ x &= w_0 r_1^{l_1} \cdots r_n^{l_n} \end{aligned}$$

因此

$$ax = u_0 w_0 q_1^{i_1} \cdots q_k^{i_k} r_1^{l_1} \cdots r_n^{l_n}.$$

为 ax 的不可约元素分解.

若 $r_1, \dots, r_n$ 中有与 $q_1, \dots, q_k$ 中的元素相伴的, 通过改变 w_0 我们可以假设相等, 并记

$$ax = u' q_1^{s_1} \cdots q_t^{s_t},$$

其中 $k \leq t \leq k+n$. $s_1, \dots, s_t \in \mathbb{N}^*$, 且 $s_1 \geq j_1, \dots, s_k \geq j_k$.

由于 $ax = b$, 我们有

$$u' q_1^{s_1} \cdots q_t^{s_t} = vp_1^{j_1} \cdots p_m^{j_m} = b.$$

由 b 的不可约元素分解的唯一性, 我们有 $t = m$, 且在一个置换的前提下, 我们有

$$q_1 \sim p_1, \dots, q_m \sim p_m,$$

以及

$$s_1 = j_1, \dots, s_m = j_m.$$

我们取单位 $u_1, \dots, u_m \in R$, 满足

$$q_1 = u_1 p_1, \dots, q_m = u_m p_m.$$

因此

$$a = (u' u_1^{i_1} \cdots u_k^{i_k}) p_1^{i_1} \cdots p_k^{i_k}$$

注意到

$$u = u' u_1^{i_1} \cdots u_k^{i_k},$$

为一个单位. 因此我们有命题中的分解. □

推论 15.2.18

记 D 为一个 UFD. 任给 $b \in D^* \setminus U$, 记 b 的不可约元素分解为

$$b = v p_1^{j_1} \cdots p_m^{j_m},$$

其中 $v \in U$, $p_1, \dots, p_m$ 为两两不相伴的不可约元素, $j_1, \dots, j_m \in \mathbb{N}^*$, 任取 $a \in R^* \setminus U$, 则以下两个叙述等价

- (i) $a \mid b$ 且 a 不可约.
- (ii) 存在非零自然数 $1 \leq k \leq m$, $a \sim p_k$.

证明. (练习) □

我们首先证明一个 UFD 总是满足公因子条件.

命题 15.2.19

记 D 为一个 UFD. 任给 $a, b \in D^*$, 它们的最大公因子 $\gcd(a, b)$ 总存在.

证明. 任取 $a, b \in D^*$, 若 a 或者 b 是单位, 不失一般性地是可以设 $a \in U$, 则任取 a 和 b 的公因子 c , 由于 $c \mid a$, 我们有 $c \in U$. 另一方面, 任意两个单位之间相伴, 因此 $\gcd(a, b) = 1$.

下设 a 和 b 都是非单位的非零元素. 我们记 a 和 b 的不可约元素分解为

$$\begin{aligned} a &= v p_1^{i_1} \cdots p_m^{i_m} \\ b &= w q_1^{j_1} \cdots q_n^{j_n} \end{aligned}$$

其中 $p_1, \dots, p_m$ 为两两不相伴的不可约元素, $q_1, \dots, q_n$ 为两两不相伴的不可约元素, $v, w \in U$, 且 $i_1, \dots, i_m, j_1, \dots, j_n \in \mathbb{N}^*$.

若 $p_1, \dots, p_m, q_1, \dots, q_n$ 两两不相伴, 设 c 为 a 和 b 的公因子, 若 c 不为单位, 则由引理 15.2.17, 我们有

$$c = u_a p_1^{s_1} \cdots p_r^{s_r} = u_b q_1^{\tilde{s}_1} \cdots q_t^{\tilde{s}_t}.$$

但这与 c 的不可约分解的唯一性矛盾. 因此 c 为一个单位. 由于单位之间相伴, 因此 $\gcd(a, b) = 1$.

对每一个 $1 \leq k \leq m$, 若存 $1 \leq l \leq n$, 有 $p_k \sim q_l$, 则在相差一个单位的前提下, 我们可以假设 $q_l = p_k$. 我们对 $q_1, \dots, q_n$ 都做如上操作, 在对 $p_1, \dots, p_m$ 和 $q_1, \dots, q_n$ 分别重排后, 存在 $1 \leq s \leq \min\{m, n\}$, 满足

$$p_1 = q_1, \dots, p_s = q_s.$$

若 c 为 a 和 b 的公因子, 我们断言 c 的不可约因子在

$$\{p_1, \dots, p_s\},$$

中. 否则, 若 c 的不可约分解中包含 p_i ($i > s$) 或 q_i ($i > s$), 我们不妨前者成立, 由于 p_i 不和

$$\{p_1, \dots, p_s, q_{s+1}, \dots, q_n\},$$

中的任意元素相伴, 由引理 15.2.17, 我们得到 c 的两个不可约分解, 其中一个包含一个不可约元素不与另一个分解中的任意不可约元素相伴, 这与 UFD 的定义矛盾.

任取 $1 \leq k \leq s$, 我们记 $l_k = \min\{i_k, j_k\}$, 记

$$d = p_1^{l_1} \cdots p_s^{l_s},$$

我们断言 $d = \gcd(a, b)$.

由引理 15.2.17, 我们知道 d 为 a 和 b 的公因子, 由以上讨论, 任取 c 为 a 和 b 的公因子, 我们有

$$c = up_1^{t_1} \cdots p_s^{t_s},$$

其中 $u \in U$, 且 $0 \leq t_1 \leq l_1, \dots, 0 \leq t_s \leq l_s$, 由引理 15.2.17 知 $c \mid d$, 因此断言得证. $\square$

命题 15.2.20

设 D 为一个 UFD. 若元素 a 不可约, 则 a 为一个素元素.

证明. 任取 $a \in D$ 为一个不可约元素, 任取 $b, c \in D^*$, 满足 $a \mid bc$. 若 $b \in U$ 或者 $c \in U$, 则 $a \mid c$ 或者 $a \mid b$.

下设 $b, c \in D^* \setminus U$, 记其不可约元素分解为

$$b = vp_1^{i_1} \cdots p_m^{i_m}$$

$$c = wq_1^{j_1} \cdots q_n^{j_n}$$

其中 $p_1, \dots, p_m$ 为两两不相伴的不可约元素, $q_1, \dots, q_n$ 为两两不相伴的不可约元素, $v, w \in U$, 且 $i_1, \dots, i_m, j_1, \dots, j_n \in \mathbb{N}^*$.

因此 bc 的不可约元素分解为

$$bc = vp_1^{i_1} \cdots p_m^{i_m} wq_1^{j_1} \cdots q_n^{j_n}$$

若 $a \mid bc$, 由于 a 不可约, 由推论 15.2.18, 存在

$$p \in \{p_1, \dots, p_m, q_1, \dots, q_n\} = \{p_1, \dots, p_m\} \cup \{q_1, \dots, q_n\}.$$

满足

$$a \sim p.$$

注意到

$$p \in \{p_1, \dots, p_m\} \text{ 或者 } p \in \{q_1, \dots, q_n\},$$

因此

$$p \mid b \text{ 或者 } p \mid c.$$

因此

$$a \mid b \text{ 或者 } a \mid c.$$

所以 a 为一个素元素. □

我们下边证明若整环 D 满足所有非零非单位元素都有不可约分解, 以及以上两个条件中的任意一个, 则 D 为一个 UFD.

命题 15.2.21

记 D 为一个整环. 设 D 满足任意非零非单位元素都有不可约分解, 以及公因子条件, 则 D 为 UFD.

证明. 任取 $a \in D^* \setminus U$, 设其有以下两种分解:

$$a = p_1 \cdots p_s = q_1 \cdots q_t,$$

其中 $s, t \in \mathbb{N}^*$, $p_1, \dots, p_s, q_1, \dots, q_t \in R$ 均为不可约元素.

因此有

$$p_1 \mid q_1 \cdots q_t.$$

我们将证明以下引理

引理 15.2.22

记 D 为一个满足公因子条件的整环. 设自然数 $t \geq 1$. 任取 D 中的不可约元素 $p, q_1, \dots, q_t$, 满足

$$p \mid q_1 \cdots q_t,$$

则存在 $1 \leq j \leq t$, 满足

$$p \sim q_j.$$

引理 15.2.22 的证明. (证明思路是例 15.1.12 的构造的推广.)

我们使用归纳法.

当 $t = 1$ 时, 由不可约元素的定义知道 $p \sim p_1$.

下边设 $t > 1$, 假设结论对任意 $1, \dots, t-1$ 的情形都成, 我们设

$$p \mid q_1 \cdots q_t.$$

我们考虑元素 pq_1 . 记

$$d = \gcd(pq_1, q_1 \cdots q_t).$$

注意到 q_1 为 pq_1 和 $q_1 \cdots q_t$ 两个元素的公因子, 因此存在 $d_1 \in R$, 满足

$$d = d_1 q_1.$$

由于 D 为整环, 由消去律, 我们有

$$d_1 \mid p, \quad d_1 \mid q_2 \cdots q_t.$$

由于 p 不可约, 因此 $d_1 \in U$ 或者 $d_1 \sim p$. 若 $d_1 \in U$, 则

$$q_1 \sim d.$$

注意到

$$p \mid pd_1 \text{ 且 } p \mid p_1 \cdots p_t,$$

因此 $p \mid d \sim q_1$. 所以 $p \sim q_1$.

若 $d_1 \sim p$ 不可约, 由于

$$d_1 \mid q_2 \cdots q_t,$$

由归纳假设, 存在 $2 \leq j \leq t$, 满足 $d_1 \sim q_j$. 因此

$$p \sim q_j.$$

矛盾.

综上所述, 引理的结论成立. □

回到命题的证明. 由于

$$a = p_1 \cdots p_s = q_1 \cdots q_t.$$

我们使用归纳法来证明 $s = t$, 且存在一个 t -置换 σ , 满足对任意 $1 \leq j \leq t$, 有

$$p_{\sigma(i)} \sim q_i.$$

注意到 $p_1 \mid q_1 \cdots q_t$. 若 $t = 1$, 由引理 15.2.22 我们有 $p_1 \sim q_1$. 若 $s > t = 1$, 利用消去律由

$$p_1 \cdots p_s = q_1,$$

可得

$$p_2 \cdots p_s \sim 1,$$

这与 $p_2, \dots, p_s$ 不可约(进而不可逆) 矛盾. 因此 $s = t$.

下设 $t > 1$, 且对任意 $1 \leq j \leq t-1$, 结论都成立. 假设

$$a = q_1 \cdots q_t.$$

利用引理 15.2.22, 存在 $1 \leq j \leq t$, 满足

$$p_1 \sim q_j.$$

不妨设 $j = 1$. 若 $s = 1$, 则由之前的讨论知矛盾. 因此 $s > 1$, 利用消去律, 我们有

$$p_2 \cdots p_s = uq_2 \cdots q_t.$$

其中 $u \in U$.

我们记 $q'_2 = uq_2$ (因此 $q'_2 \sim q_2$), 对任意 $3 \leq j \leq t$ (若存在), 记 $q'_j = q_j$. 由归纳假设,

$$s-1 = t-1,$$

且存在 $\sigma \in S_{\{2, \dots, t\}}$, 对任意 $2 \leq j \leq t$, 有

$$p_{\sigma(j)} \sim q'_j \sim q_j.$$

注意到 $\sigma \in S_t$, 因此结论成立. 由此可得 D 为 UFD. □

注 15.2.23.

我们可以使用类似于以上证明的方法来证明 UFD 的任意非零非单位元素的任意因子分解总是有限的.

命题 15.2.24

记 D 为一个整环. 设 D 满足有限分解条件, 以及素条件, 则 D 为一个 UFD.

证明. 设 p 为 D 的一个素元素. 任取 $a, b \in D$, 满足 $p \mid ab$, 则有

$$p \mid a \text{ 或者 } p \mid b.$$

下边使用归纳法证明任取 $k \in \mathbb{N}^*$, 以及 $a_1, \dots, a_k \in D$, 满足 $p \mid a_1 \cdots a_k$, 则存在 $1 \leq i \leq k$, 有

$$p \mid a_i.$$

当 $k = 1$ 时, 我们有 $p \mid a_1$, 结论成立.

下设 $k > 1$, 且结论对 $1 \leq j < k$ 的情形都成立. 设 $a_1, \dots, a_k \in R$, 满足

$$p \mid a_1 \cdots a_k,$$

因此

$$p \mid (a_1 \cdots a_{k-1})a_k,$$

由于 p 是一个素元素, 因此

$$p \mid a_1 \cdots a_{k-1} \text{ 或者 } p \mid a_k.$$

若 $p \mid a_k$, 结论成立. 否则

$$p \mid a_1 \cdots a_{k-1}.$$

由归纳假设知, 存在 $1 \leq i \leq k-1$, 满足

$$p \mid a_i.$$

设 D 为整环, 满足有限分解条件以及素条件, 要证明 D 为一个 UFD, 只需证明不可约分解的唯一性即可.

任取 $a \in D^* \setminus U$, 设存在 $s, t \in \mathbb{N}^*$, 以及 $p_1, \dots, p_s, q_1, \dots, q_t \in D$ 为不可约元素满足

$$a = p_1 \cdots p_s = q_1 \cdots q_t.$$

注意到 p_1 为素元素, 且整除 $q_1 \cdots q_t$, 因此存在 $1 \leq j \leq t$, 满足 $p_1 \mid q_j$. 由于 p_1 和 q_j 都是不可约元素, 因此 $p_1 \sim q_j$. 不妨设 $j = 1$. 由消去律, 我们有

$$p_2 \cdots p_s = u q_2 \cdots q_t.$$

重复之前的讨论. 若 $s > t$, 我们有

$$p_{t+1} \cdots p_s \in U,$$

矛盾. 类似地, $s < t$ 也不可能成立. 因此 $s = t$, 且存在 $\sigma \in S_t$, 满足对任意 $1 \leq i \leq t$, 有

$$p_s \sim q_{\sigma(i)}.$$

所以 D 为 UFD. □

15.3 主理想整环

回忆 $\mathbb{Z}$ 作为环的理想都形如 $m\mathbb{Z}$, 即 $\mathbb{Z}$ 的理想均为主理想. 本节我们考虑将其推广到对一般整环的讨论中.

定义 15.3.1

一个环 D 被称为一个**主理想整环**(Principal Ideal Domain), 若其为整环, 且其中任意理想均为主理想. 我们将简称 PID.

以下, 我们假设 D 为一个 PID.

命题 15.3.2

若元素 a 不可约, 任取元素 $b \in D^*$, 我们有

$$\langle a \rangle + \langle b \rangle = D,$$

或者

$$b \in \langle a \rangle.$$

证明. 由于 D 是一个 PID, 我们可以找到元素 $d \in D$, 满足 $\langle d \rangle = \langle a \rangle + \langle b \rangle$. 特别的我们有 $d \mid a$, 即有 $a = cd$ 和 $b = c'd$. 由于 a 不可约, 因此, 我们有 d 为单位, 或者 c 为单位.

若 d 为单位, 我们有 $\langle d \rangle = D$. 若 c 为单位, 我们有 $b = c^{-1}c'a$, 因此 $b \in \langle a \rangle$. $\square$

推论 15.3.3

设 D 为一个 PID. 若元素 a 不可约, 则 a 为一个素元素.

证明. 设 a 为一个不可约元素. 设 D^* 中元素 b 和 c , 满足 $a \mid bc$. 若 $a \nmid b$, 由于 a 不可约, 由命题 15.3.2, 我们有

$$\langle a \rangle + \langle b \rangle = D.$$

因此 $1 = sa + tb$. 我们进一步有 $c = sac + tbc$. 由于 $a \mid sac + tbc$, 因此 $a \mid c$.

若 $a \nmid c$, 我们用类似的方法可以得到 $a \mid b$. 结论得证. $\square$

推论 15.3.4

一个 PID 中的元素 a 不可约, 当且仅当理想 $\langle a \rangle$ 极大.

在继续介绍 PID 的性质前, 我们先介绍如下概念

定义 15.3.5

设 R 为一个环. 我们称其满足**左(右)理想的升链条件**, 若我们有

- 任取 $I_0, I_1, \dots$ 一列 R 中的左(右)理想, 满足条件

$$I_0 \subset I_1 \subset \dots,$$

我们都可以找到下标 $k \in \mathbb{N}$, 满足 $I_k = I_{k+1} = \dots$.

满足左(右)理想的升链条件的环 R 被称为**左(右)诺特环**. 若环 R 同时为左诺特环和右诺特环, 我们称之为**诺特环**.

注 15.3.6.

若 R 交换, 那么以上三个定义(左诺特环, 右诺特环, 诺特环)等价.
存在升链条件等价于环中所有理想有限生成. 我们将考虑 PID 的情形.

命题 15.3.7

若 D 为一个 PID, 那么 D 是一个诺特环.

证明. 设 $I_0, I_1, \dots$ 为 D 中的一列理想满足

$$I_0 \subset I_1 \subset \dots.$$

我们考虑 $\cup_{j=0}^{\infty} I_j$ 为一个 D 的理想. 由于 D 为一个 PID, 我们可以找到一个元素 d , 满足

$$\langle d \rangle = \cup_{j=0}^{\infty} I_j.$$

特别的, 我们有 $d \in \cup_{j=0}^{\infty} I_j$. 因此存在一个 k , 使得 $d \in I_k$. 由此, 我们知道 $I_k = \cup_{j=0}^{\infty} I_j$.

因此我们有 $I_k = I_{k+1} = \dots$. 所以 D 满足升链条件, D 为一个诺特环. $\square$

命题 15.3.8

若 D 为一个 PID, 那么任取 $a \in D^* \setminus U$, 我们可以找到有限多个不可约元素 $p_0, \dots, p_m$, 满足

$$a = p_0 \cdots p_m.$$

证明. 设 $a \in D^* \setminus U$. 若 a 不可约, 那么命题得证. 若 a 可约, 那么我们可以将其写为两个 $D^* \setminus U$ 中元素的乘积 $b_0 c_0$. 若 b_0 和 c_0 都不可约, 那么命题得证. 否则, 其中一个, 设为 b_0 , 可以写为两个 $D^* \setminus U$ 中元素的乘积 $b_1 c_1$. 重复以上过程, 在第 $n+1$ 步, 我们有

$$a = b_n c_n \cdots c_0.$$

我们考虑由元素 b_j 生成的理想. 由于关系 $b_j = b_{j+1} c_{j+1}$, 我们有 $\langle b_j \rangle \subset \langle b_{j+1} \rangle$.

由于 D 为诺特环, 因此存在 $k \in \mathbb{N}^*$, 满足 $\langle b_k \rangle = \langle b_{k+1} \rangle$. 因此, b_k 不可约, 以上过程在有限步结束. 因此, 元素 a 被写为有限多个不可约元素的乘积

$$a = b_k c_k \cdots c_0.$$

$\square$

由命题 15.3.8 和推论 15.3.3, 我们可以得到如下 PID 与 UFD 的关系:

定理 15.3.9

若整环 D 是 PID, 那么 D 是 UFD.

命题 15.3.10

任给 D^* 中元素 a 和 b , 令 $d = \gcd(a, b)$, 我们有

$$\langle a \rangle + \langle b \rangle = \langle d \rangle.$$

证明. 由于 d 是 a 和 b 的公因子, 因此我们有

$$\langle a \rangle \subset \langle d \rangle, \langle b \rangle \subset \langle d \rangle.$$

因此 $\langle a \rangle + \langle b \rangle \subset \langle d \rangle$.

由于 D 为 PID, 我们有元素 d' 满足

$$\langle a \rangle + \langle b \rangle = \langle d' \rangle.$$

特别地, 我们有 $d' \mid a$ 且 $d' \mid b$. 因此 d' 是 a 和 b 的公因子. 由于 d 是最大公因子, 我们有 $d' \mid d$, 因此我们有

$$\langle d \rangle \subset \langle d' \rangle = \langle a \rangle + \langle b \rangle.$$

因此我们有 $\langle a \rangle + \langle b \rangle = \langle d \rangle$. □

推论 15.3.11

设 D 为一个 PID. 设 $a, b \in D^*$.

(i) 记 $d = \gcd(a, b)$, 则存在 $u, v \in D$, 满足

$$d = ua + vb.$$

(ii) 元素 a 和 b 互素当且仅当它们生成的主理想互素, 即

$$\langle a \rangle + \langle b \rangle = D.$$

15.4 欧几里得整环

在 $\mathbb{Z}$ 中我们可以做的另一件事情就是带余出发, 不断利用带余除法, 我们可以对两个非零整数做辗转相除从而得到二者的最大公约数. 这个操作也可以在多项式环 $\mathbb{R}[x]$ 中进行. 本节我们将其推广到对一般的整环的讨论中.

定义 15.4.1

我们称一个环 D 为**欧几里得整环**, 若其为一个整环且满足以下条件:

- 存在一个映射 $\delta: D^* \rightarrow \mathbb{N}$, 满足对于任意元素 $a \in D, b \in D^*$, 存在元素 $p, r \in D$, 满足: $a = pb + r$, 且有 $\delta(r) < \delta(b)$ 或 $r = 0$.

此时, 我们称 δ 为 D 的一个**欧几里得映射**.

注 15.4.2.

欧几里得整环的定义略微复杂, 简言之, 就是一个可以做辗转相除的环. 我们在整数环中做辗转相除时, 会要求余数 r 的绝对值小于 b 的绝对值. 在一般环中, 我们不能直接比较环中的元素, 而是需要借助欧几里得映射 δ .

另一个需要说明的是一般情况下, 对于一个欧几里得整环, 欧几里得映射并不是唯一的. 例如我们考虑整数环 $\mathbb{Z}$, 定义以下映射:

$$\delta: \mathbb{Z}^* \rightarrow \mathbb{N},$$

满足

$$\delta(n) = \begin{cases} n, & \text{若 } n > 0, \\ 2|n|, & \text{若 } n < 0. \end{cases}$$

我们可以验证 $\mathbb{Z}$ 关于以上新定义的映射 δ 也是满足欧几里得整环的定义. 以上定义的 δ 也是一个欧几里得映射.

设 D 为一个欧几里得整环, δ 为 D 的一个欧几里得映射. 我们记

$$\delta_{\min} = \min\{\delta(b) \mid b \in D^*\}.$$

命题 15.4.3

任取元素 $b \in D^*$, 若 $\delta(b) = \delta_{\min}$, 我们有 b 可逆.

证明. 我们取 $a = 1$, 由欧几里得整环的定义, 我们可以找到元素 $p, r \in D$, 满足

$$1 = pb + r,$$

满足 $0 \leq \delta(r) < \delta(b)$ 或者 $r = 0$.

由于 $\delta(b) = \delta_{\min}$, 我们找不到元素 r , 满足 $\delta(r) < \delta(b)$. 因此 $r = 0$. 所以 p 为 b 的逆元. $\square$

用以上证明方法来讨论 D 中的理想, 我们可以证明以下结论.

定理 15.4.4

若环 D 为一个欧几里得整环, 那么 D 是一个 PID.

证明. 设 I 为 D 的一个理想. 取元素 b 满足

$$\delta(b) = \min\{\delta(c) \mid c \in I \setminus \{0\}\}.$$

对于任意 $a \in I$, 由欧几里得整环的定义, 我们可以找到 p 和 r , 满足

$$a = pb + r.$$

虽然 p 不一定在 I 中, 但是 I 为理想, 因此 $pb \in I$, 由此我们有

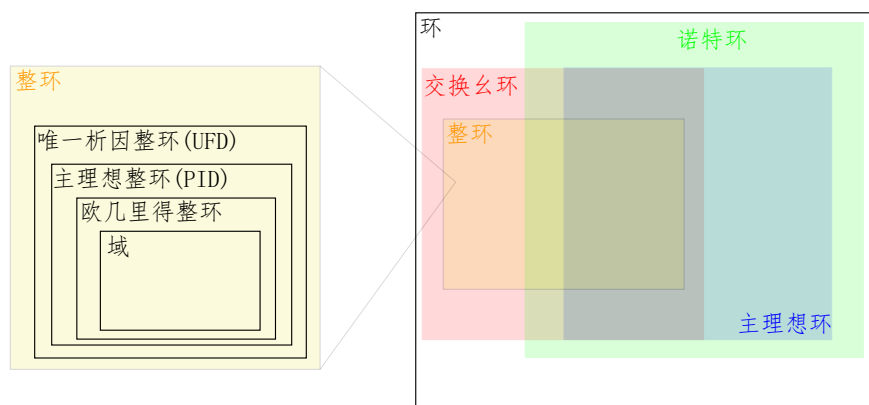
$$r = a - pb \in I.$$

由于 I 中没有非零元的 δ -值小于 $\delta(b)$, 因此我们有 $r = 0$. 因此 $b \mid a$, 对于任意 $a \in I$ 都成立. 因此 $I \subset \langle b \rangle$.

另一方面, 对于任意 $a \in I$, 我们有 $\langle a \rangle \subset I$. 因此我们有 $I = \langle b \rangle$.

因此, 整环 D 中任意理想都为主理想. 环 D 为一个 PID. □

各种特殊环之间的关系



第十六章 二次整数环

在十七世纪三十年代 (1630's), Fermat 在研究 Diophantus 的 "Arithmetica" 的时候, 在页面空白部分用拉丁语写道:

"Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere : cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet."

翻译过来就是

"立方数不能写成两个立方数的和, 四次方数不能写成两个四次方数的和, 这类结论对直到无穷的任意整数次方都成立. 我找到一个美妙的证明, 但是页面空白部分太小了, 写不下."

我们将其用现代语言写出来:

定理 16.0.1

当 $n > 2$ 的时候, 以下关于未知数 x, y 和 z 的方程

$$x^n + y^n = z^n,$$

没有整数解.

这个定理现在被称为著名的 Fermat great theorem/费马大定理, 也被称为 Fermat's last theorem.

实际上 Fermat 留下的工作基本都没有证明. 唯一的一个例外是下边的结论:

有理直角三角形的面积不可能是一个平方数.

利用这个结论, 我们可以证明费马大定理的 $n = 4$ 的情形.

证明. 假设方程 $x^4 + y^4 = z^4$ 存在整数解, 注意到 x^2, y^2 和 z^2 满足勾股定理. □

对费马大定理的证明持续了三百多年. 许多耳熟能详的名字, 比如 Euler, Legendre, Dirichlet, Lamé, Sophie Germain, Liouville, Kummer, etc.都出现在这段历史中. 直到 1994 年, Wiles 给出了一个完整的证明.

数学研究中, 对一个问题的研究的意义很多时候超越了问题本身. 对费马大定理的研究也不例外. 这段研究意义不仅仅在于证明了一个结论, 更重要的是在不断尝试的过程中, 大量新的研究工具和新的理论被建立发展起来. 这项研究也是交换环论发展的一个动力之一.

在最初的一些尝试中, 人们都会遇到这样一个问题. 对一个无平方因子数 $D \in \mathbb{Z}$, 当我们考虑形如 $a + b\sqrt{D}$ 其中 $a, b \in \mathbb{Z}$ 构成的集合的时候, 我们得到以下集合

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}.$$

注意到这样的一个集合对加法和乘法封闭, 并且关于加法构成交换群, 关于乘法构成交换半群. 用现代语言, 我们可以验证这是一个整环. 这个整环看起来和整数环很像, 于是一个直接的问题就是这样的环是不是也有一些元素具有类似于 $\mathbb{Z}$ 中的素数. 作为之前介绍的环论的例子和应用, 本章我们将对这类环做一个初步的介绍. 这也可以看作是代数数论的一个起点.

16.1 二次域

记 $D \in \mathbb{Z} \setminus \{0, \pm 1\}$.

定义 16.1.1

我们称 D 为一个**无平方因子数**, 若在相伴意义下, D 的素因子分解没有重复的素因子, 也即每个素因子在 D 的素因子分解中出现至多一次.

我们考虑复数域 $\mathbb{C}$ 的以下子集

$$\mathbb{Q}(\sqrt{D}) := \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}.$$

我们首先给出一个观察.

观察 16.1.2

我们有 $\sqrt{D} \notin \mathbb{Q}$.

证明. 否则, 存在 $m/n \in \mathbb{Q}$, 其中 $m \in \mathbb{Z}, n \in \mathbb{N}^*$, 满足

$$\sqrt{D} = \frac{m}{n}.$$

由此可得 $n^2 D = m^2$.

考虑 $a \in \mathbb{Z}$ 的素因子分解. 注意到所有 D 中出现的素因子在 $n^2 D$ 中出现奇数次, 在 m^2 中出现偶数次. 由于 $\mathbb{Z}$ 是 UFD, 因此矛盾. $\square$

利用这个观察, 我们有以下推论

推论 16.1.3

任取 $a + b\sqrt{D}, c + d\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, 我们有

$$a + b\sqrt{D} = c + d\sqrt{D}$$

当且仅当

$$a = c, \quad b = d.$$

注意到集合 $\mathbb{Q}(\sqrt{D})$ 关于复数加法和乘法封闭. 任取 $a + b\sqrt{D}, c + d\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, 我们有

$$\begin{aligned} (a + b\sqrt{D}) + (c + d\sqrt{D}) &= (a + b) + (c + d)\sqrt{D} \\ (a + b\sqrt{D}) \cdot (c + d\sqrt{D}) &= (ac + bdD) + (ad + bc)\sqrt{D} \end{aligned}$$

我们进一步可以验证 $\mathbb{Q}(\sqrt{D})$ 关于加法构成群. 考虑到复数加法和乘法得性质, 我们有 $\mathbb{Q}(\sqrt{D})$ 是一个整环.

任取 $a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})^*$, 我们定义

$$N(a + b\sqrt{D}) = a^2 - Db^2 \in \mathbb{Q}.$$

若

$$N(a + b\sqrt{D}) = 0,$$

则有

$$a^2 - Db^2 = 0,$$

因此

$$Db^2 = a^2.$$

考虑在 $\mathbb{Z}$ 中, a^2 不可约分解中素元素的个数, 我们有 $a = b = 0$. 因此我们有

$$(a + b\sqrt{D}) \cdot \frac{a - b\sqrt{D}}{a^2 - Db^2} = 1.$$

综上所述, 我们有以下结论.

命题 16.1.4

集合 $\mathbb{Q}(\sqrt{D})$ 关于复数的加法和乘法构成域.

定义 16.1.5

任取一个无平方因子数 $D \in \mathbb{Z}$, 我们称 $\mathbb{Q}(\sqrt{D})$ 为一个二次域.

注意到 $\sqrt{D}$ 为多项式 $x^2 - D \in \mathbb{Q}$ 在 $\mathbb{C}$ 中的根. 从这个角度, 我们可以使用 $\mathbb{Q}[x]$ 给出另一种二次域的描述.

我们首先讨论多项式 $x^2 - D$ 的性质.

命题 16.1.6

元素 $x^2 - D \in \mathbb{Q}[x]$ 不可约.

证明. 假设 $x^2 - D$ 可约, 则存在两个次数为 1 的多项式: $x - a, x - b \in \mathbb{Q}[x]$, 满足

$$x^2 - D = (x - a)(x - b).$$

展开后, 我们有 $a + b = 0$ 且 $ab = -D$. 因此 $a^2 = D$. 由此可得 $a \in \mathbb{Z}$. 由于 D 为一个无平方因子数, 我们得到矛盾.

因此 $x^2 - D$ 不可约. □

由于 $\mathbb{Q}$ 为域, 由定理我们有 $\mathbb{Q}[x]$ 为 PID.

推论 16.1.7

多项式 $x^2 - D \in \mathbb{Q}[x]$ 为一个素元素.

考虑元素的性质和其生成的主理想的性质之间的关系(命题 15.1.23, 推论 15.3.3 以及推论 15.3.4), 我们有以下结论

命题 16.1.8

环 $\mathbb{Q}[x]$ 的主理想 $\langle x^2 - D \rangle$ 是一个素理想, 也是一个极大理想.

推论 16.1.9

商环 $\mathbb{Q}[x]/\langle x^2 - D \rangle$ 为一个域.

下边要说明这个域实际上就是我们讨论的 $\mathbb{Q}(\sqrt{D})$.

命题 16.1.10

我们有以下环同构

$$\mathbb{Q}(\sqrt{D}) \cong \mathbb{Q}[x]/\langle x^2 - D \rangle.$$

证明. 我们考虑环同态

$$\begin{aligned} \varphi : \mathbb{Q}[x] &\rightarrow \mathbb{C}, \\ f(x) &\mapsto f(\sqrt{D}). \end{aligned}$$

注意到

$$\sqrt{D}^2 - D = 0,$$

因此

$$\langle x^2 - D \rangle \subset \ker \varphi.$$

另一方面, 任取 0 次多项式 $f(x) = a$, 我们有

$$f(\sqrt{D}) = a \neq 0.$$

因此 $\ker \varphi \neq \mathbb{Q}[x]$. 由于 $\ker \varphi$ 是一个非平凡理想, 由 $\langle x^2 - D \rangle$ 为一个极大理想, 我们有

$$\ker \varphi = \langle x^2 - D \rangle.$$

考虑 1 次多项式的像, 我们有

$$\mathbb{Q}(\sqrt{D}) \subset \text{Im } \varphi.$$

另一方面, 任取 $f(x) \in \mathbb{Q}[x]$, 我们考虑 $\mathbb{Q}[x]$ 中的带余除法, 可得

$$f(x) = (a + bx) + g(x)(x^2 - D).$$

因此

$$f(\sqrt{D}) = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D}).$$

因此有

$$\text{Im } \varphi \subset \mathbb{Q}(\sqrt{D}).$$

我们有 $\text{Im } \varphi = \mathbb{Q}(\sqrt{D})$.

利用环同态基本定理, 我们有环同构

$$\mathbb{Q}[x]/\langle x^2 - D \rangle \cong \mathbb{Q}(\sqrt{D}).$$

□

我们在后续讨论 $\mathbb{Z}[\sqrt{D}]$ 的时候会经常使用到下边这个定义.

定义 16.1.11

我们称如下映射

$$\begin{aligned} N : \mathbb{Q}(\sqrt{D}) &\rightarrow \mathbb{Q} \\ a + b\sqrt{D} &\mapsto a^2 - b^2D \end{aligned}$$

为 $\mathbb{Q}(\sqrt{D})$ 的**范数函数**.

注 16.1.12.

若 $D < 0$, 则 N 就是复数域上取模长平方的映射.

定义 16.1.13

任给元素 $\alpha = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, 我们称元素

$$\bar{\alpha} := a - b\sqrt{D},$$

为 α 在 $\mathbb{Q}(\sqrt{D})$ 的**共轭元**.

我们可以直接验证

命题 16.1.14

任取 $\alpha \in \mathbb{Q}(\sqrt{D})$, 我们有

$$N(\alpha) = \alpha\bar{\alpha}.$$

直接计算我们可以验证下边这个映射 N 的性质.

命题 16.1.15

任取 $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$, 我们有

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

证明. 任取 $a, b, c, d \in \mathbb{Q}$, 我们有如下计算

$$\begin{aligned} &N(a + b\sqrt{D})(c + d\sqrt{D}) \\ &= N(ac + bdD + (ad + bc)\sqrt{D}) \\ &= (ac + bdD)^2 - D(ad + bc)^2 \\ &= ((ac)^2 + 2abcdD + (bdD)^2 - (D(ad)^2 + 2abcdD + D(bc)^2)) \\ &= (a^2 - b^2D)c^2 - (a^2 - d^2D)d^2D \\ &= (a^2 - b^2D)(c^2 - d^2D) \\ &= N(a + b\sqrt{D})N(c + d\sqrt{D}). \end{aligned}$$

□

16.2 二次整数环

从代数的角度看, 整数环 $\mathbb{Z}$ 是 $\mathbb{Q}$ 的一个特殊的子环. 一方面 $\mathbb{Q}$ 是 $\mathbb{Z}$ 的分式域. 另一方面, 由之前的讨论我们知道 $\mathbb{Q}$ 中满足分式域是 $\mathbb{Q}$ 的子环并不是仅有 $\mathbb{Z}$. 例如 $2\mathbb{Z}$ 的分式域也是 $\mathbb{Q}$. 但是 $\mathbb{Z}$ 满足一个特殊的性质就是任取 $\mathbb{Z}$ 上首一多项式 $f(x)$, 如果 $f(x)$ 在 $\mathbb{Q}$ 中有根 α , 那么 $\alpha \in \mathbb{Z}$. 我们称这个性质为**整闭性**.

我们希望在任意的二次域 $\mathbb{Q}(\sqrt{D})$ 中也找到类似的子环. 如果这样的子环存在的话, 我们希望进一步研究这样的子环是不是像 $\mathbb{Z}$ 一样也是 Euclid 整环, 或者仅仅是满足 UFD 或者 PID 条件, 或者什么条件都不满足. 一种自然的定义二次域 $\mathbb{Q}(\sqrt{D})$ 中的整数的方法就是考虑 $\mathbb{Q}(\sqrt{D})$ 中的整系数的元素

$$\mathbb{Z}[\sqrt{D}] = \{m + n\sqrt{D} \mid m, n \in \mathbb{Z}\}.$$

如果我们考虑上边提到的整闭性的话, 对有的 D , $\mathbb{Z}[\sqrt{D}]$ 并不满足这个性质. 例如, 我们考虑以下多项式

$$f(x) = x^2 - x + \frac{1-D}{4} \in (\mathbb{Q}[\sqrt{D}])[x].$$

如果 D 满足

$$D \equiv 1 \pmod{4},$$

则 $f(x) \in \mathbb{Z}[x]$. 但是它的根是

$$\frac{-1 \pm \sqrt{D}}{2} \notin \mathbb{Z}.$$

另一方面, 我们考虑

$$\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] := \left\{m + n\frac{1+\sqrt{D}}{2} \mid m, n \in \mathbb{Z}\right\}$$

也构成 $\mathbb{Q}(\sqrt{D})$ 的子环. 此外这个子环是整闭的.

定义 16.2.1

我们定义二次域 $\mathbb{Q}(\sqrt{D})$ 的**二次整数环**为

$$\mathcal{O}_D := \begin{cases} \mathbb{Z}[\sqrt{D}], & \text{若 } D \equiv 2, 3 \pmod{4}, \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right], & \text{若 } D \equiv 1 \pmod{4}. \end{cases}$$

当 $D = -1$ 时, 我们称 $\mathbb{Z}[\sqrt{-1}]$ 为 **Gauss 整数环**.

我们考虑 $\mathbb{Q}(\sqrt{D})$ 的范数函数在其整数环上的限制则有以下观察.

观察 16.2.2

任意二次整数环 $\mathcal{O}_D$ 的元素的范数都是整数.

证明. 若 $D \equiv 2, 3 \pmod{4}$, 任取 $\alpha = m + n\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$, 其范数为

$$N(\alpha) = m^2 - Dn^2 \in \mathbb{Z}.$$

若 $D \equiv 1 \pmod{4}$, 任取 $\alpha = m + n\frac{1+\sqrt{D}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$, 其范数为

$$\begin{aligned} N(\alpha) &= \left(m + \frac{n}{2}\right)^2 - D\frac{n^2}{4} \\ &= m^2 + mn + n^2\frac{1-D}{4} \in \mathbb{Z}. \end{aligned}$$

□

利用这个观察, 范数函数的性质以及整数的性质, 我们可以得到对 $\mathcal{O}_D$ 中单位的描述.

命题 16.2.3

任意二次整数环 $\mathcal{O}_D$ 中的元素为单位当且仅当其范数为 1 或者 -1.

证明. 任取 $\alpha \in \mathcal{O}_D$, 若 α 为单位, 则存在 $\beta \in \mathcal{O}_D$, 满足

$$\alpha\beta = 1.$$

利用范数的性质我们有

$$N(\alpha)N(\beta) = N(\alpha\beta) = 1.$$

由于二次整数环元素的范数都是整数, 我们有

$$N(\alpha) \in \{\pm 1\}.$$

反过来, 任取 $\alpha \in \mathcal{O}_D$, 满足

$$N(\alpha) = 1.$$

由命题 16.1.14 中的关系, 我们有

$$\alpha\bar{\alpha} = 1.$$

若

$$N(\alpha) = -1.$$

我们有

$$\alpha(-\bar{\alpha}) = 1.$$

最后我们需要检查 $\bar{\alpha}$ 是否在 $\mathcal{O}_D$ 中. 若 $D \equiv 2, 3 \pmod{4}$, 那么考虑系数我们有 $\bar{\alpha} \in \mathcal{O}_D$.

若 $D \equiv 1 \pmod{4}$, 我们记

$$\alpha = m + n\frac{1+\sqrt{D}}{2},$$

则有

$$\bar{\alpha} = m + n\frac{1-\sqrt{D}}{2} = (m+n) - n\frac{1+\sqrt{D}}{2} \in \mathcal{O}_D.$$

□

例 16.2.4 ($n = -1$).

任取 $\alpha + m + n\sqrt{-1} \in \mathcal{O}_{-1} = \mathbb{Z}[\sqrt{-1}]$, α 为单位当且仅当

$$N(\alpha) = m^2 + n^2 = \pm 1.$$

因此 $\mathcal{O}_{-1}$ 的单位群为

$$\{1, -1, \sqrt{-1}, -\sqrt{-1}\}.$$

例 16.2.5 ($n = -3$).

任取 $\alpha = m + n\frac{1+\sqrt{-3}}{2} \in \mathcal{O}_{-3} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, α 为单位当且仅当

$$m^2 + mn + n^2 = 1.$$

因此 $\mathcal{O}_{-3}$ 的单位群为

$$\left\{1, -1, \frac{1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}\right\},$$

分别对应 (m, n) 的取值为

$$\{(1, 0), (-1, 0), (0, 1), (0, -1), (1, -1), (-1, 1)\}.$$

思考 16.2.6

计算其他 D 对应的二次整数环的单位.

另一方面, 我们也可以使用范数来讨论元素是否可约.

命题 16.2.7

任意二次整数环 $\mathcal{O}_D$ 中的范数为正负素数的元素都不可约.

证明. 记 $p \in \mathbb{N}$ 为一个素数. 设 $\alpha \in \mathcal{O}_D$ 满足

$$N(\alpha) = \pm p.$$

若存在 $\beta, \gamma \in \mathcal{O}_D$, 满足

$$\alpha = \beta\gamma,$$

我们有

$$N(\alpha) = N(\beta)N(\gamma).$$

由于 $\pm p$ 为 $\mathbb{Z}$ 的不可约元素, 因此我们有 $N(\beta) \in \{1, -1\}$ 或者 $N(\gamma) \in \{1, -1\}$. 因此 β 为单位或者 γ 为单位. 由此可得 α 不可约. $\square$

16.3 二次整数的分解

当我们将整数推广到二次整数之后, 一个自然的问题就是二次整数环的性质如何? 我们知道这是一个整环. 那么二次整数环是否也是欧几里得整环?

16.3.1 欧几里得环

任给一个二次整数环, 一个自然的可以用来作为欧几里得映射候选者的映射就是范数的绝对值. 如果一个二次整数环 $\mathcal{O}_D$ 关于范数绝对值映射为一个欧几里得环, 我们称其是**范数欧几里得的**.

我们首先考虑 $D = -1$ 的情形.

命题 16.3.1

Gauss 整数环是范数欧几里得环.

证明. 我们记 $i = \sqrt{-1}$. 任取 $a + bi, c + di \in \mathbb{Z}[i]^*$. 在 $\mathbb{Q}(i)$ 中, 我们考虑

$$\frac{a + bi}{c + di} = x + yi.$$

其中

$$\begin{cases} x = \frac{ac + bd}{c^2 + d^2} \\ y = \frac{ad - bc}{c^2 + d^2} \end{cases}.$$

我们将复平面看作欧氏平面, 考虑离 $x + yi$ 最近的 $\mathbb{Z}[i]$ 中的点, 记作 $q = s + ti$, 即

$$(s - x)^2 + (t - y)^2 = \min\{(m - x)^2 + (n - y)^2 \mid m, n \in \mathbb{Z}\}.$$

记 $r = a + bi - q(c + di)$. 下边证明 $r = 0$ 或者

$$N(r) < N(c + di).$$

我们可以从几何的角度来理解剩下的讨论. 注意到 q 的选择, 考虑 $\mathbb{Z}[i]$ 在 $\mathbb{C}$ 中的分布, 我们有

$$|s - x| \leq \frac{1}{2} \quad \text{且} \quad |t - y| \leq \frac{1}{2}.$$

因此

$$(s - x)^2 + (t - y)^2 \leq \frac{1}{2}.$$

等价地, 我们有

$$\frac{N(r)}{N(c + di)} \leq \frac{1}{2}.$$

因此结论成立. □

注 16.3.2.

如果将 $\mathbb{C}$ 等同于欧氏平面, 复数模长就是欧式距离, $\mathbb{Z}[i]$ 可以看作是当我们使用单位正方形做平面密铺的时候的顶点.

类似地, 当我们考虑 $D = -2$ 的时候, $\mathcal{O}_{-2}$ 中的点可以看作是我们使用斜边长为 1 的等腰直角三角形对平面做密铺的时候的所有顶点.

当我们考虑 $D = -3$ 的时候, $\mathcal{O}_{-3}$ 中的点可以看作是我们使用边长为 1 的正三角形做平面密铺的时候的所有顶点.

注 16.3.3.

关于 Gauss 整环是范数欧几里得环的证明可以用来证明结论对 $D = -7, -3, -2$ 和 2 也成立.

思考 16.3.4

证明 $\mathcal{O}_{-3}$ 是一个范数欧几里得环.

关于一般的 D , 我们有知道当 $D < 0$ 时, 二次整数环 $\mathcal{O}_D$ 为欧几里得环当且仅当为范数欧几里得环. 另一方面, $D < 0$ 时, 二次整数环 $\mathcal{O}_D$ 为范数欧几里得环只对

$$D = -1, -2, -3, -7, -11,$$

成立. 因此这部分研究对于 $D < 0$ 的情况是清楚的.

当 $D > 0$ 时, 二次整数环 $\mathcal{O}_D$ 为范数欧几里得环只对

$$D = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73,$$

成立. 但是 $D > 0$ 时, 二次整数环 $\mathcal{O}_D$ 可能关于其它映射称为欧几里得环. 已知的例子有 $\mathcal{O}_{14}$ 和 $\mathcal{O}_{69}$. 详细内容可以参考 [14, Chapter 8], [21], [12], [17]. 我们没钱还没有完整的对应的二次整数环为欧几里得环的 D 的列表.

16.3.2 元素的分解

我们知道许多二次整数环都不是欧几里得环. 那么这些环是否是一个 PID 或者 UFD? 如果我们从定义出发, 就会涉及到对元素分解的讨论.

考虑元素分解给出的范数的分解, 我们有以下结论

命题 16.3.5

任给一个二次整数环 $\mathcal{O}_D$, 任意其中的一个非零非单位的元素都有一个有限的不可约分解.

证明. 任取 $\alpha \in \mathcal{O}_D$, 我们将对 $|N(\alpha)|$ 进行归纳.

由之前关于范数的讨论, 我们知道若 $|N(\alpha)| = 0$, 则 $\alpha = 0$; 若 $|N(\alpha)| = 1$, 则 α 为单位. 因此若 α 非零非单位, 则 $|N(\alpha)| \geq 2$.

若 $|N(\alpha)| = 2$, 由于 2 为素数, 由命题 16.2.7 我们知道 α 不可约.

下设 $n > 2$, 结论对任意满足 $2 \leq |N(\alpha)| < n$ 的 α 都成立, 下设 $N(\alpha) = n$. 由于 $n > 1$, 因此 α 不是单位或零. 若 α 不可约, 则结论成立, 否则存在 $\beta, \gamma \in \mathcal{O}_D$, 满足

$$\alpha = \beta\gamma,$$

且 $N(\beta) < N(\alpha)$, $N(\gamma) < N(\alpha)$. 由归纳假设, β 和 γ 都有有限的不可约分解, 因此 α 也有有限的不可约分解. $\square$

由这个结论, 我们可以看出环 $\mathcal{O}_D$ 是不是 UFD 的关键是分解的唯一性是否成立.

要说明一些环不是 UFD, 只需要找到一些反例即可. 我们在之前关于 UFD 的讨论中已经左肋这部分的讨论. 当然 $\mathbb{Z}[-3]$ 不是二次整数环. 我们可以考虑 $D = -5$, 取 $\alpha = 9$, 则有

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

由于不存在范数为 ± 3 的元素, 这里 3, $2 + \sqrt{-5}$ 或者 $2 - \sqrt{-5}$ 都不可约, 相互之间也不相伴. 因此这是两种不同的不可约分解. 因此 $\mathbb{Z}[\sqrt{-5}]$ 不是唯一分解整环.

有一些情况下反例也相对容易寻找.

命题 16.3.6

任取大于 0 的奇的无平方因字数 n , 我们记 $D = -2n < 0$ 为无平方因字数, 则 $\mathcal{O}_D$ 不是 UFD.

证明. 这里考虑 D 的分解, 我们有

$$2n = -(\sqrt{2n})^2.$$

考虑 2, n 和 $\sqrt{2n}$ 三个元素.

元素 2 不可约. 否则存在 $a, b, c, d \in \mathbb{Z}$, 满足

$$4 = N(2) = (a^2 + 2nb^2)(c^2 + 2nd^2),$$

且 $a^2 + 2nb^2 = 2$. 注意到 (a, b) 没有整数解. 因此 2 不可约. 类似地, 我们可以证明 $\sqrt{2n}$ 不可约. 考虑元素的范数, 我们有 2 和 $\sqrt{2n}$ 不相伴, 因此元素 $2n$ 有两个不可约分解. 环 $\mathcal{O}_D$ 不是 UFD. $\square$

但是要用定义来直接证明某个 $\mathcal{O}_D$ 是 UFD 是比较困难的. 当然我们也可以使用 UFD 的等价条件. 例如, 我们可以尝试去讨论环素条件是不是满足, 但是这就需要去证明某个元素是素元素. 我们先来看两个证明元素为素元素的例子. 我们暂时忘掉二次整数环, 分别考虑 $\mathbb{Z}[\sqrt{-3}]$ 和 $\mathbb{Z}[\sqrt{5}]$.

例 16.3.7 ($\mathbb{Z}[\sqrt{-3}]$ 范数为素数的元素).

考虑 $\mathbb{Z}[\sqrt{-3}]$, 我们将证明任意范数为素数的元素都是素元素.

任取 $\alpha \in \mathbb{Z}[\sqrt{-3}]$, 满足 $N(\alpha)$ 为素数. 注意到

$$m^2 + 3n^2 = 2$$

没有整数解, 因此 $N(\alpha)$ 为奇素数. 由命题 16.2.7, 我们知道 α 是一个不可约元素. 下设 $\beta, \gamma \in \mathbb{Z}[\sqrt{-3}]$, 满足

$$\alpha \mid \beta\gamma.$$

我们希望证明 $\alpha \mid \beta$ 或者 $\alpha \mid \gamma$.

我们考虑二次整数环 $\mathcal{O}_{-3}$, 注意到 $\mathcal{O}_{-3}$ 为欧几里得环, 因此满足素条件. 因此在 $\mathcal{O}_{-3}$ 中, 有 $\alpha \mid \beta$ 或者 $\alpha \mid \gamma$.

不妨设 $\alpha \mid \beta$. 因此存在 $\eta \in \mathcal{O}_{-3}$, 满足

$$\alpha\eta = \beta.$$

我们记

$$\alpha = m + n\sqrt{-3}, \quad \eta = a + b\frac{1 + \sqrt{-3}}{2}.$$

因此

$$\beta = \left(ma + \frac{mb + 3nb}{2}\right) + \left(na + \frac{mb + nb}{2}\right)\sqrt{-3}.$$

如果 b 为偶数, 则 $\eta \in \mathbb{Z}[\sqrt{-3}]$, 因此 $\alpha \mid \beta$ 在 $\mathbb{Z}[\sqrt{-3}]$ 中成立.

如果 b 为奇数, 则由 $\beta \in \mathbb{Z}[\sqrt{-3}]$, 可得 m 和 n 有相同奇偶性. 考虑

$$N(\alpha) = m^2 + 3n^2,$$

因此

$$2 \mid N(\alpha),$$

与之前讨论 $N(\alpha)$ 应为奇素数矛盾.

综上所述, 我们有 $\alpha \mid \beta$ 在 $\mathbb{Z}[\sqrt{-3}]$ 中成立.

这里我们使用了 $\mathcal{O}_{-3}$ 是一个欧几里得环这个事实. 下边我们考虑另一种借助多项式环的证明方法.

例 16.3.8 ($3 + 2\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$).

我们将证明 $3 + 2\sqrt{5}$ 为 $\mathbb{Z}[\sqrt{5}]$ 的一个素元素. 我们计算其范数为

$$N(3 + 2\sqrt{5}) = 3^2 - 20 = -11.$$

我们将证明 $\langle 3 + 2\sqrt{5} \rangle$ 为 $\mathbb{Z}[\sqrt{5}]$ 的一个素理想.

注意到

$$\mathbb{Z}[\sqrt{5}] \cong \mathbb{Z}[x]/\langle x^2 - 5 \rangle.$$

因此我们有

$$\begin{aligned} & \mathbb{Z}[\sqrt{5}]/\langle 3 + 2\sqrt{5} \rangle \\ & \cong \mathbb{Z}[\sqrt{5}]/\langle 3 + 2\sqrt{5}, 11 \rangle \\ & \cong \mathbb{Z}[x]/\langle x^2 - 5, 3 + 2x, 11 \rangle \\ & \cong \mathbb{Z}_{11}[x]/\langle x^2 - 5, 3 + 2x \rangle \\ & \cong \mathbb{Z}_{11}[x]/\langle x^2 - 5, 7 + x \rangle \\ & \cong \mathbb{Z}_{11}[x]/\langle x + 7 \rangle \\ & \cong \mathbb{Z}_{11}. \end{aligned}$$

倒数第三个同构来自于在 $\mathbb{Z}_{11}[x]$ 中我们有 $3 = 14$, 且 2 可逆. 倒数第二个同构来自于

$$(x + 7)(x - 7) = x^2 - 49 = x^2 - 5 \in \mathbb{Z}_{11}[x].$$

由于 $\mathbb{Z}_{11}$ 为一个域, 商环 $\mathbb{Z}[\sqrt{5}]/\langle 3 + 2\sqrt{5} \rangle$ 为一个域, 因此 $\langle 3 + 2\sqrt{5} \rangle$ 为一个极大理想, 也是素理想. 因此 $3 + 2\sqrt{5}$ 为一个素元素.

我们注意到以上证明元素为一个素元素的方法也依赖于所在环以及所取元素的一些特殊的性质. 我们在下节将转换思路考虑理想的分解.

16.4 理想的唯一分解

我们将看到虽然元素的分解的情况似乎不时很清楚, 但是理想却满足唯一分解性. 在证明一般的结论之前我们先来重新研究一下之前为了说明 $\mathbb{Z}[\sqrt{-5}]$ 不是 UFD 而给出的分解不为一个的例子.

例 16.4.1.

我们考虑

$$9 = 3 \cdot 3 = (2 - \sqrt{-5})(2 + \sqrt{-5}).$$

下边我们将考虑以下一些 $\mathbb{Z}[\sqrt{-5}]$ 的理想

$$\langle 3 \rangle, \langle 3, 1 + \sqrt{-5} \rangle, \langle 3, 1 - \sqrt{-5} \rangle, \langle 2 + \sqrt{-5} \rangle, \langle 2 - \sqrt{-5} \rangle.$$

我们可以验证

$$\begin{aligned} \langle 3 \rangle &= \langle 3, 1 + \sqrt{-5} \rangle \langle 3, 1 - \sqrt{-5} \rangle, \\ \langle 2 + \sqrt{-5} \rangle &= \langle 3, 1 - \sqrt{-5} \rangle^2, \\ \langle 2 - \sqrt{-5} \rangle &= \langle 3, 1 + \sqrt{-5} \rangle^2. \end{aligned}$$

我们以第二个等式为例来讨论. 注意到

$$\langle 3, 1 - \sqrt{-5} \rangle^2 = \langle 9, 3 - 3\sqrt{-5}, -4 - 2\sqrt{-5} \rangle.$$

一方面, 我们有

$$2 + \sqrt{-5} = 9 + (-4 - 2\sqrt{-5}) - (3 - 3\sqrt{-5}).$$

因此我们有一个方向的包含关系

$$\langle 2 + \sqrt{-5} \rangle \subset \langle 3, 1 - \sqrt{-5} \rangle^2.$$

另一方面, 我们知道

$$\begin{aligned} 9 &= (2 + \sqrt{-5})(2 - \sqrt{-5})(2 + \sqrt{-5}) \in \langle 2 + \sqrt{-5} \rangle, \\ (-4 - 2\sqrt{-5}) &= (-2)(2 + \sqrt{-5}) \in \langle 2 + \sqrt{-5} \rangle. \end{aligned}$$

因此

$$3 - 3\sqrt{-5} \in \langle 2 + \sqrt{-5} \rangle,$$

由此可得

$$\langle 2 + \sqrt{-5} \rangle \supset \langle 3, 1 - \sqrt{-5} \rangle^2.$$

以上讨论告诉我们, 9 生成的理想有以下分解

$$\langle 9 \rangle = \langle 3, 1 + \sqrt{-5} \rangle^2 \langle 3, 1 - \sqrt{-5} \rangle^2.$$

注 16.4.2.

注意到当我们使用理想讨论之后, 之前出现的分解不唯一的情况似乎得到了解决. 我们将在接下来的部分来给出严格的讨论, 说明所谓的理想是在什么意义下有唯一分解. 实际上这正是 Kummer 在解决 $\mathcal{O}_D$ 缺少唯一分解的性质时, 引入的理想数 (ideal number) 的概念. 这也是理想 (ideal) 这个称呼的来源.

16.4.1 二次整数环中的理想

我们首先给出 $\mathcal{O}_D$ 中的理想的一般形式.

命题 16.4.3

任取二次整数环 $\mathcal{O}_D$ 及其中的一个理想 I , 存在整数 k, m, n , 满足

$$I = \left\langle k, m + n \frac{1 + \sqrt{D}}{2} \right\rangle.$$

证明. 我们考虑

$$I_0 = I \cap \mathbb{Z},$$

以及

$$I_1 = \left\{ t \in \mathbb{Z} \mid \exists s \in \mathbb{Z}, s + t \frac{1 + \sqrt{D}}{2} \in I \right\}$$

直接验证可得 I_0 和 I_1 都是 $\mathbb{Z}$ 的理想, 因此我们有整数 k 和 n , 满足

$$I_0 = k\mathbb{Z}, \quad I_1 = n\mathbb{Z}.$$

(这里 I_0 和 I_1 都在 I 中, 但都不是 $\mathcal{O}_D$ 的理想.)

记 $m \in \mathbb{Z}$, 满足

$$m + n \frac{1 + \sqrt{D}}{2} \in I.$$

下边证明

$$I = \left\langle k, m + n \frac{1 + \sqrt{D}}{2} \right\rangle.$$

注意到右边包含在左边里是平凡的, 我们只需要证明左边包含在右边即可, 这等价于证明任取 $\alpha \in D$ 都可以写成 k 和 $m + n \frac{1 + \sqrt{D}}{2}$ 的系数在 $\mathcal{O}_D$ 中的线性组合. 实际上我们只需要 $\mathbb{Z}$ -系数即可.

对任意 D , 我们都可以将 α 写为

$$a + b \frac{1 + \sqrt{D}}{2}$$

的形式, 其中 $a, b \in \mathbb{Z}$, 且这种写法唯一.

由于 $b \in I_1$, 存在 $q \in \mathbb{Z}$, 满足

$$b = qn.$$

我们考虑

$$a + b \frac{1 + \sqrt{D}}{2} = (a - qm) + q \left(m + n \frac{1 + \sqrt{D}}{2} \right).$$

注意到 $a - qm \in I$, 因此存在 $r \in \mathbb{Z}$, 满足

$$a - qm = kr.$$

因此

$$a + b \frac{1 + \sqrt{D}}{2} = kr + q \left(m + n \frac{1 + \sqrt{D}}{2} \right) \in \left\langle k, m + n \frac{1 + \sqrt{D}}{2} \right\rangle.$$

因此我们有

$$I \subset \left\langle k, m + n \frac{1 + \sqrt{D}}{2} \right\rangle.$$

□

有这个结论出发, 我们有以下推论.

推论 16.4.4

任取二次整数环 $\mathcal{O}_D$, 设 I 为其中一个非零理想, 则商环 $\mathcal{O}_D/I$ 有限.

证明. 若 $I \subset \mathcal{O}_D$ 为一个非零理想, 则任取 $\alpha \in I$, 我们有

$$N(\alpha) = \alpha \bar{\alpha} \in I.$$

因此 $I_0 = I \cap \mathbb{Z}$ 包含非零元素. 由于 I_0 为 $\mathbb{Z}$ 的理想, 因此我们有 $k \in \mathbb{Z}^*$, 满足

$$I_0 = k\mathbb{Z}.$$

利用环同态基本定理, 我们有

$$\mathcal{O}_D/I \cong (\mathcal{O}_D/\langle k \rangle)/(I/\langle k \rangle).$$

由于

$$\mathcal{O}_D/\langle k \rangle \cong \mathbb{Z}_k[x]/\langle x^2 - D \rangle,$$

因此是一个有限环. 由此可得 $\mathcal{O}_D/I$ 有限.

□

作为这个推论的特殊情况, 我们有以下结论.

推论 16.4.5

任取二次整数环 $\mathcal{O}_D$, 设 I 为其中一个非零理想, 如果 I 为一个素理想, 则 I 为一个极大理想.

证明. 理想 I 为素理想, 当且仅当 $\mathcal{O}_D/I$ 为一个整环. 另一方面, 由于有限整环为域, 且 $\mathcal{O}_D/I$ 为域当且仅当 I 为极大理想, 我们有以上结论. $\square$

利用这个结论, 我们可以得出如下关于 $\mathcal{O}_D$ 性质的结论.

命题 16.4.6

二次整数环 $\mathcal{O}_D$ 为 UFD 当且仅当其为 PID.

证明. 任意 PID 都是 UFD, 因此我们只需要证明另一个方向即可.

下边假设 $\mathcal{O}_D$ 为一个 UFD. 因此 $\mathcal{O}_D$ 满足素条件和公因子条件. 我们需要证明 $\mathcal{O}_D$ 的任意理想都是主理想.

任取 I 为 $\mathcal{O}_D$ 的理想, 由之前讨论知, 存在 $\alpha, \beta \in \mathcal{O}_D$, 满足

$$I = \langle \alpha, \beta \rangle.$$

若 $\alpha = 0$ 或者 $\beta = 0$, 则 I 为 β 生成的主理想或者 α 生成的主理想, 则结论成立.

若 α 为单位或者 β 为单位, 则 $I = \mathcal{O}_D$ 为 1 生成的主理想, 结论也成立.

下边假设 α 和 β 都是非零非单位元素. 我们要证明一个更强的结论

$$I = \langle \gcd(\alpha, \beta) \rangle = \langle \alpha \rangle + \langle \beta \rangle.$$

记 α 和 β 的不可约分解分别为

$$\alpha = \gamma_1 \cdots \gamma_m,$$

$$\beta = \eta_1 \cdots \eta_n.$$

我们首先考虑 $\gcd(\alpha, \beta) = 1$ 的情形, 即任取 γ_i 和 η_j , 我们有

$$\langle \gamma_i \rangle \neq \langle \eta_j \rangle.$$

由于任意 γ_i 和 η_j 都是素元素, 因此任意 $\langle \gamma_i \rangle$ 和 $\langle \eta_j \rangle$ 都是素理想, 由以上推论知均为极大理想. 所以任取 γ_i 和 η_j , 我们有

$$\langle \gamma_i \rangle + \langle \eta_j \rangle = \mathcal{O}_D = \langle 1 \rangle.$$

我们从 γ_1 和 η_1 开始, 考虑

$$\langle \gamma_1 \rangle + \langle \eta_1 \rangle = \mathcal{O}_D = \langle 1 \rangle.$$

同时乘以 γ_2 可得

$$\langle \gamma_2 \rangle = \langle \gamma_1 \gamma_2 \rangle + \langle \gamma_2 \eta_1 \rangle \subset \langle \gamma_1 \gamma_2 \rangle + \langle \eta_1 \rangle.$$

因此

$$\langle 1 \rangle = \langle \gamma_2 \rangle + \langle \eta_1 \rangle \subset \langle \gamma_1 \gamma_2 \rangle + \langle \eta_1 \rangle.$$

同时乘以 γ_3 可得

$$\langle \gamma_3 \rangle \subset \langle \gamma_1 \gamma_2 \gamma_3 \rangle + \langle \eta_1 \gamma_3 \rangle.$$

进而有

$$\langle 1 \rangle = \langle \gamma_3 \rangle + \langle \eta_1 \rangle \subset \langle \gamma_1 \gamma_2 \gamma_3 \rangle + \langle \eta_1 \rangle.$$

重复以上过程直到 γ_m , 我们可以证明

$$\langle 1 \rangle = \langle \alpha \rangle + \langle \eta_1 \rangle.$$

注意到以上讨论对任意 η_j 都成立. 因此我们可以对 η_j 's 重复以上过程. 首先都乘以 η_2 , 我们有

$$\langle \eta_2 \rangle \subset \langle \alpha \eta_2 \rangle + \langle \eta_1 \eta_2 \rangle \subset \langle \alpha \rangle + \langle \eta_1 \eta_2 \rangle.$$

因此

$$\langle 1 \rangle = \langle \alpha \rangle + \langle \eta_2 \rangle \subset \langle \alpha \rangle + \langle \eta_1 \eta_2 \rangle.$$

同时乘以 η_3 , 我们有

$$\langle \eta_3 \rangle \subset \langle \alpha \eta_3 \rangle + \langle \eta_1 \eta_2 \eta_3 \rangle,$$

因此有

$$\langle 1 \rangle = \langle \alpha \rangle + \langle \eta_3 \rangle \subset \langle \alpha \rangle + \langle \eta_1 \eta_2 \eta_3 \rangle.$$

重复以上过程直到 η_m , 我们有

$$\langle 1 \rangle = \langle \alpha \rangle + \langle \beta \rangle = I.$$

下边考虑一般情形, 设

$$d = \gcd(\alpha, \beta),$$

则有 $\alpha', \beta' \in \mathcal{O}_D$, 满足

$$\alpha = d\alpha' \quad \text{以及} \quad \beta = d\beta'.$$

特别地, 我们有 $\gcd(\alpha', \beta') = 1$, 且

$$I = \langle \alpha \rangle + \langle \beta \rangle = (\langle \alpha' \rangle + \langle \beta' \rangle)d.$$

由以上讨论我们有

$$\langle \alpha' \rangle + \langle \beta' \rangle = \langle 1 \rangle,$$

因此

$$I = \langle d \rangle.$$

□

注 16.4.7.

实际上我们之前的讨论验证了所有的二次整数环都是 Dedekind 整环, 即满足以下三个条件的整环

- (i) 诺特环 (所有理想有限生成);
- (ii) 满足整闭性;
- (iii) 所有素理想都是极大理想.

以上讨论对任意的 Dedekind 整环都成立, 即任取一个 Dedekind 整环 D , 则 D 为 UFD 当且仅当 D 为 PID.

我们之前讨论过 $\mathbb{Q}(\sqrt{D})$ 中元素的共轭元素. 这个概念也可以推广到理想上.

定义 16.4.8

若 I 为二次整数环 $\mathcal{O}_D$ 的理想, 我们定义其**共轭理想**为

$$\bar{I} := \{\bar{\alpha} \mid \alpha \in I\}.$$

注 16.4.9.

注意到 $\mathcal{O}_D$ 在取共轭下不变, 因此若 I 为由 α 和 β 生成的理想, 则 $\bar{I}$ 为由 $\bar{\alpha}$ 和 $\bar{\beta}$ 生成的理想.

命题 16.4.10

任取二次整数环 $\mathcal{O}_D$, 及其理想 I , 则理想 $I\bar{I}$ 为一个主理想.

证明. 记 $k, m, n \in \mathbb{Z}$ 满足

$$I = \left\langle k, m + n \frac{1 + \sqrt{D}}{2} \right\rangle,$$

其中 $k\mathbb{Z} = I \cap \mathbb{Z}$,

$$n\mathbb{Z} = \left\{ t \in \mathbb{Z} \mid \exists s \in \mathbb{Z}, s + t \frac{1 + \sqrt{D}}{2} \in I \right\}.$$

若 $k = 0$, 则 I 为主理想, $I\bar{I}$ 是主理想. 类似地, 若 $n = 0$, 则 $I\bar{I}$ 是主理想.

下设 $k \neq 0$ 且 $n \neq 0$. 我们有

$$I\bar{I} = \left\langle k^2, km + kn \frac{1 + \sqrt{D}}{2}, km + kn \frac{1 - \sqrt{D}}{2}, m^2 + mn + \frac{1 - D}{4} n^2 \right\rangle.$$

记

$$d = \gcd \left(k^2, 2km + kn, m^2 + mn + \frac{1 - D}{4} n^2 \right),$$

利用 $\mathbb{Z}$ 中的 Bezout 等式 d 可以写为三个整数的 $\mathbb{Z}$ -线性组合, 我们有

$$I\bar{I} \cap \mathbb{Z} = d\mathbb{Z}.$$

因此可得

$$J := \left\langle k^2, 2km + kn, m^2 + mn + \frac{1 - D}{4} n^2 \right\rangle = \langle d \rangle.$$

由

$$d^2 \mid k^2 \left(m^2 + mn + \frac{1 - D}{4} n^2 \right) = k^2 \left(\frac{(2m + n)^2}{4} - \frac{D}{4} n^2 \right)$$

可知

$$d^2 \mid 4d^2 \mid (k(2m + n))^2 - Dn^2k^2.$$

因此

$$d^2 \mid Dk^2n^2.$$

由于 D 无平方因子, 因此

$$d^2 \mid k^2n^2.$$

进而可得

$$d \mid kn \quad \text{且} \quad d \mid 2km.$$

下边对 D 分类. 若 $D \equiv 1 \pmod{4}$, 则 n 可以取奇数或者偶数.

若 d 为奇数, 则有 $d \mid km$. 我们有

$$d \mid km + kn \frac{1+\sqrt{D}}{2} \quad \text{且} \quad d \mid km + kn \frac{1-\sqrt{D}}{2},$$

下设 d 为偶数. 若 n 为奇数, 由 $d \mid kn$ 可知 d 素数分解中因子 2 的因子个数小于等于 k 中因子 2 的个数. 因此由 $d \mid 2km$ 可得 $d \mid km$. 我们有

$$d \mid km + kn \frac{1+\sqrt{D}}{2} \quad \text{且} \quad d \mid km + kn \frac{1-\sqrt{D}}{2},$$

若 n 为偶数, 考虑

$$4d^2 \mid (k(2m+n))^2 - Dn^2k^2.$$

由于 $d \mid 2km$, 因此 d 中因子 2 个数小于等于 $2km$ 中因子 2 的个数. 同理 d 中因子 2 个数小于等于 kn 中因子 2 的个数. 记 d 中因子 2 个数为 $l \in \mathbb{N}^*$, 则

$$4 \mid 4 \frac{d^2}{2^{2l}} \mid \frac{(k(2m+n))^2}{2^{2l}} - \frac{Dn^2k^2}{2^{2l}}.$$

由于 $D \equiv 1 \pmod{4}$, 我们有

$$4 \mid \frac{4k^2m^2}{2^{2l}} + \frac{4k^2mn}{2^{2l}}.$$

若 $2km$ 中因子 2 个数为 l , 则模 4 有 $\frac{4k^2m^2}{2^{2l}} \equiv 1$ 或者 3, 但是 $4k^2mn = 2(2km)kn$ 中因子 2 的个数多于 $2l$, 因此模 4 余 2, 矛盾. 因此

$$d \mid km.$$

我们有

$$d \mid km + kn \frac{1+\sqrt{D}}{2} \quad \text{且} \quad d \mid km + kn \frac{1-\sqrt{D}}{2},$$

考虑 $D \equiv 2, 3 \pmod{4}$, 则 n 必须为偶数.

若 d 为奇数, 则 $d \mid km$ 且 $d \mid kn/2$, 因此

$$d \mid km + kn \frac{1+\sqrt{D}}{2} \quad \text{且} \quad d \mid km + kn \frac{1-\sqrt{D}}{2},$$

若 d 为偶数, 仍记 d 中因子 2 的个数为 l . 重复上边的讨论可知

$$4 \mid \frac{(k(2m+n))^2}{2^{2l}} - \frac{Dn^2k^2}{2^{2l}}$$

若 $k(2m+n)$ 中因子 2 的个数为 l , 则 $\frac{(k(2m+n))^2}{2^{2l}}$ 模 4 余 1, 因此 $\frac{Dn^2k^2}{2^{2l}}$ 应该模 4 余 1, 但是 $\frac{n^2k^2}{2^{2l}}$ 模 4 余 1, 因此 D 模 4 余 1, 矛盾.

因此 $k(2m+n)$ 中因子 2 的个数严格多于 l , 因此 $\frac{(k(2m+n))^2}{2^{2l}}$ 被 4 整除. 由此可知 $\frac{Dn^2k^2}{2^{2l}}$ 被 4 整除. 但是 D 中没有平方因子, 因此 $4 \mid \frac{n^2k^2}{2^{2l}}$, 由此可知 kn 中因子 2 个数严格多于 l . 因此 $d \mid kn/2$, 且 $2mk$ 中因子 2 个数严格多于 l . 因此 $d \mid km$. 我们有

$$d \mid km + kn \frac{1+\sqrt{D}}{2} \quad \text{且} \quad d \mid km + kn \frac{1-\sqrt{D}}{2},$$

不管是哪种情况, 我们都可以得到

$$I\bar{I} = \langle d \rangle.$$

□

16.4.2 理想的唯一分解

考虑二次整数环 $\mathcal{O}_D$. 类似于元素的整除, 我们给出如下理想整除的定义.

定义 16.4.11

任取理想 I 和 J , 我们称 I **整除** J , 若存在理想 K , 满足 $J = IK$. 我们记作 $I \mid J$.

在 $\mathcal{O}_D$ 中, 理想的整除和包含之间有紧密的联系. 我们下边给出理想整除的一些性质.

命题 16.4.12

记 I, J 以及 K 为 $\mathcal{O}_D$ 的理想. 记 α, β 和 γ 为 $\mathcal{O}_D$ 中的元素. 我们有以下结论:

- 1) 若 $I \mid J$, 则 $J \subset I$.
- 2) $I \mid J$ 且 $J \mid I$ 当且仅当 $I = J$.
- 3) $\langle \alpha \rangle \mid I$ 当且仅当 $I \subset \langle \alpha \rangle$.
- 4) 若 $\langle \alpha \rangle I = \langle \alpha \rangle J$ 且 $\alpha \neq 0$, 则有 $I = J$.
- 5) 若 $IJ = IK$ 且 $I \neq \{0\}$, 则 $J = K$.
- 6) $I \mid J$ 当且仅当 $J \subset I$.

证明. 1) 若 $I \mid J$, 则有理想 L , 满足 $J = IL \subset I$.

2) 由 1) 若 $I \mid J$ 且 $J \mid I$, 我们有 $J \subset I$ 且 $I \subset J$, 因此 $I = J$. 反过来由于 $I = IR$, 若 $I = J$, 我们有 $I \mid J$ 且 $J \mid I$.

3) 直接验证可得结论对 $\alpha = 0$ 和 $I = \{0\}$ 成立.

我们下边假设 $\alpha \neq 0$. 由 1) 若 $\langle \alpha \rangle \mid I$, 则 $I \subset \langle \alpha \rangle$. 反过来, 记 $\beta, \gamma \in \mathcal{O}_D$, 满足 $I = \langle \beta, \gamma \rangle$. 若 $I \subset \langle \alpha \rangle$, 我们有

$$\alpha \mid \beta \quad \text{且} \quad \alpha \mid \gamma,$$

因此

$$I = \langle \alpha \rangle \left\langle \frac{\beta}{\alpha}, \frac{\gamma}{\alpha} \right\rangle.$$

我们有

$$\langle \alpha \rangle \mid I.$$

4) 任取 J 中的元素 β , 存在 $\gamma \in K$, 满足

$$\alpha\beta = \alpha\gamma.$$

由于 $\mathcal{O}_D$ 为整环, 且 $\alpha \neq 0$, 我们有 $\beta = \gamma$. 因此 $J \subset K$. 类似地, 我们可以证明 $K \subset J$. 因此 $J = K$.

5) 我们考虑等式

$$\bar{I}IJ = \bar{I}IK,$$

由之前的命题, 我们直到存在 $d \in \mathbb{Z}^*$, 满足

$$\bar{I}I = \langle d \rangle,$$

因此我们有

$$\langle d \rangle J = \langle d \rangle K.$$

由 4) 可知 $J = K$.

6) 由 1) 我们证明了一个方向. 下设 $J \subset I$, 则有

$$\bar{I}J \subset \bar{I}I,$$

由之前命题, 我们直到存在 $d \in \mathbb{Z}^*$, 满足

$$\langle d \rangle = \bar{I}I.$$

由 3) 可知

$$\bar{I}I \mid \bar{I}J,$$

即存在理想 L 满足

$$\bar{I}IL = \bar{I}J.$$

若 $J = \{0\}$, 则 $J = I\{0\}$, 因此 $I \mid J$.

若 $J \neq \{0\}$, 则由 5) 可知 $IL = J$, 因此 $I \mid J$. □

注 16.4.13.

以上性质反映了相比于一般的环, $\mathcal{O}_D$ 中理想的特殊的地方. 比如 6) 告诉我们, 如果有理想的包含, 就必有理想的整除. 这也是与 $\mathbb{Z}$ 中理想相似的地方.

我们回顾素理想的定义. 我们称一个理想 P 为素理想, 若任取 $\alpha, \beta \in \mathcal{O}_D$, 满足 $\alpha\beta \in P$ 都有 $\alpha \in P$ 或者 $\beta \in P$. 我们将考虑 $\mathcal{O}_D$ 中的非平凡理想的素理想分解. 这里首先介绍一个需要用到的工具.

由之前的命题我们知道任取理想 I , 我们考虑 $\bar{I}I$ 存在 $d \in \mathbb{N}$, 满足

$$\bar{I}I = \langle d \rangle.$$

定义 16.4.14

我们定义 I 的范数

$$N(I) := d \in \mathbb{N}.$$

由 d 的构造, 我们有以下一些观察.

观察 16.4.15

记 I 和 J 为 $\mathcal{O}_D$ 的理想.

- 1) $N(I) = 0$ 当且仅当 $I = \{0\}$;
- 2) $N(I) = 1$ 当且仅当 $I = \mathcal{O}_D$;
- 3) $N(IJ) = N(I)N(J)$.
- 4) $I \mid \langle N(I) \rangle$.

我们进而有以下推论.

推论 16.4.16

记 I 为 $\mathcal{O}_D$ 的一个理想. 若 $N(I)$ 为素数, 则 I 为素理想. 特别地, 若 $\alpha \in \mathcal{O}_D$ 满足 $N(\alpha)$ 为 $\mathbb{Z}$ 的一个素元素 (与素数相差至多一个符号), 那么主理想 $\langle \alpha \rangle$ 为一个素理想, 元素 α 为 $\mathcal{O}_D$ 的一个素元素.

证明. 我们之前证明在 $\mathcal{O}_D$ 中一个理想为素理想当且仅当是一个极大理想.

设 I 为一个范数为素数 p 的理想. 若 I 不是极大的, 则存在一个真理想 J , 满足

$$I \subsetneq J.$$

由之前的命题我们知道 $J \mid I$, 因此存在理想 K 满足 $I = JK$. 因此

$$N(I) = N(J)N(K).$$

注意到 $N(I)$ 为素数, 因此 $N(J) = 1$ 或者 $N(K) = 1$. 这等价于 $J = \mathcal{O}_D$ 或者 $K = \mathcal{O}_D$. 因此我们有 $J = \mathcal{O}_D$ 或者 $J = I$, 与 J 为一个真包含 I 的真理想矛盾. 因此 I 极大, 所以为素理想.

下边考虑 I 为主理想的情形. 设存在 $\alpha \in \mathcal{O}_D$, 满足

$$I = \langle \alpha \rangle,$$

则有

$$N(I) = |N(\alpha)| = |\alpha\bar{\alpha}|.$$

因此若 $N(\alpha)$ 为 $\mathbb{Z}$ 的一个素元素, 则 $N(I)$ 为一个素数, 因此 I 为素理想. 利用素元素与其生成的主理想之间的关系, 我们有 α 为 $\mathcal{O}_D$ 的一个素元素. $\square$

利用范数, 我们可以证明任何理想都有素理想分解.

命题 16.4.17

二次整数环 $\mathcal{O}_D$ 中任意非平凡理想 (不等于 $\{0\}$ 或者 $\mathcal{O}_D$) 都可以分解为有限多个素理想的乘积.

证明. 我们对理想的范数进行归纳.

若 $N(I) = 2$, 由于 2 为素数, 我们有 I 为素理想, 因此 $I = I$ 为其素理想分解.

下边假设 $n > 2$, 且结论对任意理想 I 满足 $N(I) < n$ 都成立. 考虑满足 $N(I) = n$ 的理想 I . 若 I 极大, 则 I 为素理想, 因此 $I = I$ 为其素理想分解.

若 I 不是极大的, 则存在真理想 J 满足

$$I \subsetneq J.$$

因此存在理想 K , 满足 $I = JK$. 我们进而有 $N(I) = N(J)N(K)$.

由于 J 为真包含 I 的真理想, 我们有

$$1 < N(J), N(K) < n.$$

由归纳假设, 我们知道 J 和 K 都有素理想分解, 因此它们分解的乘积就是 I 的素理想分解. $\square$

我们下边要证明这样的分解是唯一的. 类似于证明 UFD 的过程, 我们将需要一个类似于素条件的条件.

命题 16.4.18

记 P 为 $\mathcal{O}_D$ 的一个素理想, 并记 I 和 J 为 $\mathcal{O}_D$ 的理想. 若 $P \mid IJ$, 则有

$$P \mid I \quad \text{或者} \quad P \mid J.$$

证明. 由之前的讨论, 若 $P \mid IJ$, 我们有

$$IJ \subset P.$$

若 $I \not\subset P$ 且 $J \not\subset P$, 则存在 $x \in I \setminus P$ 且 $y \in J \setminus P$, 满足 $xy \in P$. 但是 P 为一个素理想, 因此必有 $x \in P$ 或者 $y \in P$. 矛盾. 因此我们有 $I \subset P$ 或者 $J \subset P$. 因此等价地, 我们有 $P \mid I$ 或者 $P \mid J$. $\square$

注 16.4.19.

实际上利用素理想的定义, 我们可以直接证明若 $P \subset IJ$, 则有 $P \subset I$ 或者 $P \subset J$. 这里用到 $\mathcal{O}_D$ 的地方是包含和整除等价.

定理 16.4.20

记 I 为 $\mathcal{O}_D$ 中一个非平凡的理想. 设 I 有以下两个素理想分解

$$I = P_1 \cdots P_m = Q_1 \cdots Q_n,$$

则 $m = n$, 且存在一个置换 $\sigma \in S_n$, 满足对任意 $1 \leq i \leq n$, 有

$$P_i = Q_{\sigma(i)}.$$

证明. 我们考虑 P_1 , 注意到

$$P_1 \mid Q_1 \cdots Q_n,$$

由之前命题, 存在 $1 \leq j \leq n$, 满足

$$P_1 \mid Q_j.$$

由于 P_1 和 Q_j 均为素理想, 因此均为极大理想(由定义一定是真理想). 我们有 $P_1 = Q_j$.

我们不妨设 $j = 1$, 由之前的命题, 我们可以使用消去律得到

$$P_2 \cdots P_m = Q_2 \cdots Q_n.$$

使用归纳法, 定理得证. $\square$

16.4.3 刻画素理想

之前的讨论告诉我们素理想在描述二次整数环的理想的过程中有着重要作用. 本节我们希望可以给出二次整数环的素理想一个刻画帮助我们确定给定 $\mathcal{O}_D$ 的素理想. 我们首先证明以下结论

命题 16.4.21

记 P 为 $\mathcal{O}_D$ 的一个素理想, 则 $N(P)$ 为一个素数或者其平方.

证明. 由于 P 为素理想, 因此 $N(P) \neq 0, 1$.

考虑嵌入同态

$$\varphi: \mathbb{Z} \rightarrow \mathcal{O}_D$$

我们有

$$\varphi^{-1}(P) = P \cap \mathbb{Z}.$$

由于 P 是 $\mathcal{O}_D$ 的理想, 因此 $P \cap \mathbb{Z}$ 也是 $\mathbb{Z}$ 的理想. 我们记 $d \in \mathbb{N}$ 为其生成元.

任取 $m, n \in \mathbb{Z}$, 满足 $\varphi(mn) \in P$, 我们有

$$\varphi(m)\varphi(n) \in P,$$

由于 P 为一个素理想, 因此有 $\varphi(m) \in P$ 或者 $\varphi(n) \in P$. 因此有 $m \in d\mathbb{Z}$ 或者 $n \in d\mathbb{Z}$. 即 $d\mathbb{Z}$ 为 $\mathbb{Z}$ 的一个素理想, 因此 d 为一个素数. 我们有

$$\langle d \rangle \subset P.$$

因此

$$N(P) \mid N(\langle d \rangle) = d^2.$$

所以 $N(P) = d$ 或者 d^2 . □

这个命题说明要研究 $\mathcal{O}_D$ 中的素理想, 我们需要对任意素数 $p \in \mathbb{Z}$ 研究其 $\mathcal{O}_D$ 生成的理想 $\langle p \rangle$ 的素理想分解. 若不能分解则说明 $\langle p \rangle$ 是一个素理想, 而 p 在 $\mathcal{O}_D$ 中也是一个素元素. 否则, 任取该理想存在一个素理想分解. 由于 $\langle p \rangle$ 的范数为 p^2 , 因此可以分解为两个素理想.

例 16.4.22.

我们给出一个素数可以分解的例子. 考虑 Gauss 整数环 $\mathbb{Z}[\sqrt{-1}]$, 我们有

$$2 = (1 + \sqrt{-1})(1 - \sqrt{-1}).$$

注意到

$$1 - \sqrt{-1} = (1 + \sqrt{-1}) - (1 + \sqrt{-1})^2,$$

因此我们有

$$\langle 2 \rangle = \langle 1 + \sqrt{-1} \rangle \langle 1 - \sqrt{-1} \rangle = \langle 1 + \sqrt{-1} \rangle^2.$$

注意到 $\sqrt{-1}$ 为 $x^2 + 1 \in \mathbb{Z}[x]$ 在 $\mathbb{C}$ 中的根. 实际上该多项式有两个根, 并且这两个根模 2 是相同的. 另一方面我们注意到 $x^2 + 1 \in \mathbb{Z}_2[x]$ 在 $\mathbb{Z}_2$ 中有重根 1. 以上讨论的结果说明 $\langle 2 \rangle$ 的素理想分解中也是一个素理想的平方. 这些观察之间的关系就是我们下边要介绍的 Dedekind-Kummer 分解定理.

定理 16.4.23

记 D 为一个无平方因子数. p 为一个素数. 我们考虑 $\mathbb{Z}[x]$ 中的多项式

$$f(x) = \begin{cases} x^2 - D, & D \equiv 2, 3 \pmod{4} \\ x^2 - x - \frac{D-1}{4}, & D \equiv 1 \pmod{4} \end{cases}$$

我们也将考虑其系数全部模 p 得到的 $\mathbb{Z}_p[x]$ 中的多项式, 仍记作 $f(x)$. 关于 $\mathcal{O}_D$ 中的理想 $\langle p \rangle$ 的素理想分解, 我们有以下结论:

- 1) 若 $f(x) \in \mathbb{Z}_p[x]$ 不可约, 则 $\langle p \rangle$ 为素理想;
- 2) 若 $f(x) \in \mathbb{Z}_p[x]$ 可约, 则 $f(x)$ 在 $\mathbb{Z}_p$ 中有两个根 (计算重根). 我们记 r_1 和 r_2 为 $f(x)$ 在 $\mathbb{Z}_p$ 中的根, 则 $\langle p \rangle$ 有以下素理想分解:

$$\langle p \rangle = \begin{cases} \langle p, \sqrt{D} - r_1 \rangle \langle p, \sqrt{D} - r_2 \rangle, & D \equiv 2, 3 \pmod{4} \\ \left\langle p, \frac{1 + \sqrt{D}}{2} - r_1 \right\rangle \left\langle p, \frac{1 + \sqrt{D}}{2} - r_2 \right\rangle, & D \equiv 1 \pmod{4} \end{cases}$$

证明. 关于有限域及其上多项式环的一般理论可以参考讲义后边 Galois 理论的部分.

我们仍旧使用多项式环来进行讨论. 注意到

$$\mathcal{O}_D \cong \mathbb{Z}[x] / \langle f(x) \rangle.$$

因此, 我们有商环的同构

$$\mathcal{O}_D / \langle p \rangle \cong \mathbb{Z}[x] / \langle p, f(x) \rangle.$$

由环同态基本定理, 我们有

$$\cong \mathbb{Z}[x] / \langle p, f(x) \rangle \cong \mathbb{Z}_p[x] / \langle f(x) \rangle.$$

若 $\langle p \rangle$ 为素理想, 则商环 $\mathcal{O}_D / \langle p \rangle$ 为整环. 注意到 $\mathbb{Z}_p[x] / \langle f(x) \rangle$ 为一个整环当且仅当 $f(x) \in \mathbb{Z}_p[x]$ 不可约. 因此, 若 $f(x) \in \mathbb{Z}_p[x]$ 不可约, 则 $\langle p \rangle$ 为一个素理想.

若 $f(x) \in \mathbb{Z}_p[x]$ 可约, 由于 $\mathbb{Z}_p$ 为域, 因此 0 次多项式都是单位, 我们有 $r_1, r_2 \in \mathbb{Z}_p$, 满足

$$f(x) = (x - r_1)(x - r_2) \in \mathbb{Z}_p[x].$$

因此

$$\langle f(x) \rangle = \langle x - r_1 \rangle \langle x - r_2 \rangle.$$

注意到 1 次多项式都是不可约多项式, 由中国剩余定理, 我们有

$$\mathbb{Z}_p[x] / \langle f(x) \rangle \cong \mathbb{Z}_p[x] / \langle x - r_1 \rangle \times \mathbb{Z}_p[x] / \langle x - r_2 \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

利用环同态基本定理, 我们有

$$\begin{aligned} & \mathbb{Z}_p \\ & \cong \mathbb{Z}_p[x] / \langle x - r_1 \rangle \\ & \cong (\mathbb{Z}_p[x] / \langle f(x) \rangle) / (\langle x - r_1 \rangle / \langle f(x) \rangle) \\ & \cong (\mathcal{O}_D / \langle p \rangle) / (\langle p, \omega - r_1 \rangle / \langle p \rangle) \\ & \cong \mathcal{O}_D / \langle p, \omega - r_1 \rangle. \end{aligned}$$

这里

$$\omega = \begin{cases} \sqrt{D} & D \equiv 2, 3 \pmod{4} \\ \frac{1 + \sqrt{D}}{4} & D \equiv 1 \pmod{4} \end{cases}.$$

同样的讨论对 $\langle p, \omega - r_1 \rangle$ 也成立.

因此我们有 $\langle p, \omega - r_1 \rangle$ 和 $\langle p, \omega - r_2 \rangle$ 都是 $\mathcal{O}_D$ 的素理想, 且满足

$$\langle p \rangle = \langle p, \omega - r_1 \rangle \langle p, \omega - r_2 \rangle.$$

□

例 16.4.24.

我们考虑 $D = -5$, 则有 $\mathcal{O}_D = \mathbb{Z}[\sqrt{-5}]$. 考虑 $p = 2, 3, 7, 11$.

1) 在 $\mathbb{Z}_2[x]$ 中, 我们有

$$x^2 + 5 = x^2 + 1 = (x + 1)(x + 1).$$

因此在 $\mathcal{O}_D$ 中, 我们有

$$\langle 2 \rangle = \langle 2, \sqrt{-5} + 1 \rangle \langle 2, \sqrt{-5} - 1 \rangle.$$

实际上我们考虑

$$2 \mid (\sqrt{-5} + 1)(\sqrt{-5} - 1) = -6,$$

就可以发现 2 不是素元素.

2) 在 $\mathbb{Z}_3[x]$ 中, 我们有

$$x^2 + 5 = x^2 - 1 = (x - 1)(x + 1).$$

因此在 $\mathcal{O}_D$ 中, 我们有

$$\langle 3 \rangle = \langle 3, \sqrt{-5} + 1 \rangle \langle 3, \sqrt{-5} - 1 \rangle.$$

实际上我们考虑

$$3 \mid (\sqrt{-5} + 1)(\sqrt{-5} - 1) = -6,$$

就可以发现 3 不是素元素.

3) 在 $\mathbb{Z}_7[x]$ 中, 我们有

$$x^2 + 5 = x^2 - 2 = x^2 - 9 = (x - 3)(x + 3).$$

因此在 $\mathcal{O}_D$ 中, 我们有

$$\langle 7 \rangle = \langle 7, \sqrt{-5} + 3 \rangle \langle 7, \sqrt{-5} - 3 \rangle.$$

实际上我们考虑

$$7 \mid (\sqrt{-5} + 3)(\sqrt{-5} - 3) = -14,$$

就可以发现 7 不是素元素.

4) 在 $\mathbb{Z}_{11}[x]$ 中, 直接带入验证发现 $x^2 + 5$ 在 $\mathbb{Z}_{11}$ 中无根, 因此 $x^2 + 5$ 不可约. 我们有 (11) 为 $\mathcal{O}_D$ 的一个素理想, 11 为 $\mathcal{O}_D$ 的一个素元素.

注意到在讨论的过程中, 我们实际上关心的是一个素数 p 模另一个素数 q 的同余类在 $\mathbb{Z}_q$ 是否是某个元素的平方.

定义 16.4.25

记 p 为一个奇素数. 任取不被 p 整除的整数 a , 我们称 a 为模 p 的二次剩余, 若方程

$$x^2 \equiv a \pmod{p},$$

可解.

我们通常使用 **Legendre 符号** 在表示一个整数是否是模一个素数的二次剩余: 任取 p 为一个奇素数, 以及不被 p 整除的整数 a , 我们记

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \exists n, n^2 \equiv a \pmod{p} \\ -1, & \nexists n, n^2 \equiv a \pmod{p} \end{cases}$$

若整数 a 满足 $p \mid a$, 我们约定

$$\left(\frac{a}{p}\right) = 0.$$

由定义, 任取整数 a 和 b , 若 $a \equiv b \pmod{p}$, 那么

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Euler 给出了一个计算 Legendre 符号的公式.

命题 16.4.26 (Euler)

记 p 为一个奇素数, 任取整数 a , 我们有

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

证明. 若 $p \mid a$, 直接验证可得结论成立.

下设 $p \nmid a$. 利用有限域的知识 (参考讲义 Galois 理论的部分) 我们知道 $\mathbb{Z}_p^*$ 是一个关于乘法的循环群. 因此存在整数 g , 满足其模 p 同余类 $\bar{g}$ 为乘法群 $\mathbb{Z}_p^*$ 的生成元. 因此 $\bar{g}$ 的阶为 $p-1$. 因此

$$\bar{g}^{\frac{p-1}{2}} = -1.$$

我们记 $i \in \{1, \dots, p-1\}$, 满足

$$\bar{a} = \bar{g}^i.$$

我们可以验证

$$\left(\frac{a}{p}\right) = (-1)^i.$$

若 a 为模 p 的二次剩余, 则存在 $b \in \mathbb{Z}$, 满足 $b^2 \equiv a \pmod{p}$. 我们记 $j \in \{1, \dots, p-1\}$, 满足

$$\bar{b} = \bar{g}^j.$$

因此

$$\bar{a} = \bar{g}^{2j}.$$

注意到 $i \equiv 2j \pmod{p-1}$. 由于 $p-1$ 为偶数, 所以 i 和 $2j$ 有相同的奇偶性.

反过来若 i 为偶数, 我们可以取整数 j , 满足 $2j = i$. 因此

$$\bar{a} = (\bar{g}^j)^2.$$

因此 $a \equiv g^i \pmod{p}$ 为模 p 的二次剩余.

另一方面, 我们有

$$\bar{a}^{\frac{p-1}{2}} = (\bar{g}^{\frac{p-1}{2}})^i = \overline{(-1)^i}.$$

因此我们有以上结论. □

作为一个直接的推论, 我们有

推论 16.4.27

任取奇素数 p 以及整数 a 和 b , 我们有

$$\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

证明. 由前一个命题, 我们有

$$\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}.$$

由于 p 为奇素数, 因此 $1 \not\equiv -1 \pmod{p}$, 我们有

$$\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

□

任取整数 $n \neq 0, \pm 1$, 我们将其写为

$$n = \epsilon p_1^{m_1} \cdots p_k^{m_k},$$

这里 $\epsilon \in \{1, -1\}$, $p_1, \dots, p_k$ 为两两不同的素数. 任取奇素数 p , 利用上边的推论, 我们就有

$$\left(\frac{n}{p}\right) = \left(\frac{\epsilon}{p}\right) \left(\frac{p_1}{p}\right)^{m_1} \cdots \left(\frac{p_k}{p}\right)^{m_k}.$$

当 $\epsilon = 1$ 的时候, 右边第一项为 1. 当 $\epsilon = -1$ 时, 我们考虑以下引理.

引理 16.4.28

任取奇素数 p , 我们有

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

因此要计算 $\left(\frac{n}{p}\right)$, 我们需要考虑任取两个素数 p 和 q , 如何计算 $\left(\frac{q}{p}\right)$. 二次互反律是一个重要工具. 作为一个猜想, Euler 首先给出了二次互反律. 之后 Gauss 首先给出了二次互反律的严格的证明. 这期间 Legendre 证明了一些特殊情形.

定理 16.4.29 (二次互反律)

1) 任取 p 和 q 两个不同的奇素数, 我们有以下关系

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right).$$

2) 任取奇素数 p , 我们有

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

16.5 一些例子

我们将使用上边的理论研究一些具体的例子. 我们将对 $D = -1, -2, -3$ 时, $\mathcal{O}_D$ 中的不可约元素做一个描述. 我们注意到当 $D = -1, -2$ 或者 -3 的时候, $\mathcal{O}_D$ 是欧几里得环, 因此所有的素元素都是不可约元素. 因此我们只需要描述所有的素元素即可.

16.5.1 $\mathcal{O}_{-1}$

当 $D = -1$ 时, 环 $\mathcal{O}_{-1} = \mathbb{Z}[\sqrt{-1}]$ 为 Gauss 整环. 此时任取 $m + n\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$, 其范数为

$$N(m + n\sqrt{-1}) = m^2 + n^2.$$

其中的单位为 $1, -1, \sqrt{-1}, -\sqrt{-1}$.

由之前的讨论, 我们考虑素数在 $\mathbb{Z}[\sqrt{-1}]$ 中的分解.

命题 16.5.1

所有素数在环 $\mathcal{O}_{-1}$ 的不可约分解如下:

- 1) $p = 2$ 时, 有不可约分解 $2 = (1 + i)(1 - i)$;
- 2) $p \equiv 3 \pmod{4}$ 时, p 为 $\mathbb{Z}[\sqrt{-1}]$ 的不可约元素.
- 3) $p \equiv 1 \pmod{4}$ 时, 存在 $m + n\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$, 使 p 有如下不可约分解

$$p = (m + n\sqrt{-1})(m - n\sqrt{-1}).$$

证明. 我们使用二次剩余来证明.

$p = 2$ 的情形直接验证即可. 下设 p 为一个奇素数. 由 Dedekind-Kummer 分解定理, 我们需要讨论

$$x^2 + 1 \in \mathbb{Z}_p[x]$$

的可约性. 注意到 $x^2 + 1$ 可约当且仅当其在 $\mathbb{Z}_p$ 中有根, 即 -1 为模 p 的二次剩余.

考虑之前给出的计算公式, 我们有

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

若 $p \equiv 1 \pmod{4}$, 则 $(-1)^{\frac{p-1}{2}} = 1$, 因此 $x^2 + 1 \in \mathbb{Z}_p[x]$ 可约, 即存在 $a \in \mathbb{Z}_p$, 满足

$$x^2 + 1 = (x + a)(x - a) \in \mathbb{Z}_p[x].$$

因此

$$\langle p \rangle = \langle p, a + \sqrt{-1} \rangle \langle p, a - \sqrt{-1} \rangle.$$

注意到 $\mathbb{Z}[\sqrt{-1}]$ 为一个欧几里得环, 因此存在 $m + n\sqrt{-1}$, 满足

$$\begin{aligned}\langle p, a + \sqrt{-1} \rangle &= \langle m + n\sqrt{-1} \rangle \\ \langle p, a - \sqrt{-1} \rangle &= \langle m - n\sqrt{-1} \rangle\end{aligned}$$

即

$$\langle p \rangle = \langle m + n\sqrt{-1} \rangle \langle m - n\sqrt{-1} \rangle.$$

在相差一个单位的前提下, 我们有

$$p = (m + n\sqrt{-1})(m - n\sqrt{-1}).$$

若 $p \equiv 3 \pmod{4}$, 则 $(-1)^{\frac{p-1}{2}} = -1$, 因此 $x^2 + 1 \in \mathbb{Z}_p[x]$ 不可约, 则由 Dedekind-Kummer 定理有 p 为一个不可约元素. $\square$

考虑元素范数的计算, 我们有以下推论.

推论 16.5.2

在相伴意义下, 环 $\mathcal{O}_{-1}$ 中的不可约元素有如下三类

- 1) $1 + \sqrt{-1}$ (范数为 2);
- 2) p (范数为 p^2 , 满足 $p \equiv 3 \pmod{4}$);
- 3) $m + n\sqrt{-1}, m - n\sqrt{-1}$ (范数为 p , 满足 $p \equiv 1 \pmod{4}$).

作为一个直接推论, 我们可以证明初等数论的 Fermat 关于素数的平方和定理.

定理 16.5.3 (Fermat 素数)

一个素数 p 可以写为两个非零自然数的平方和当且仅当 $p = 2$ 或者 $p \equiv 1 \pmod{4}$.

我们可以继续证明 Fermat 的关于一般自然数的平方和定理.

定理 16.5.4 (Fermat 整数)

任给一个大于 1 的整数 n , 记其素数分解

$$n = 2^k p_1^{l_1} \cdots p_s^{l_s} q_1^{m_1} \cdots q_t^{m_t},$$

其中 $p_1, \dots, p_s$ 为模 4 余 1 的两两不同的素数, $q_1, \dots, q_t$ 为模 4 余 3 的两两不同的素数, 则 n 可以写为两个非零自然数的平方和当且仅当 $m_1, \dots, m_t$ 均为偶数.

证明. 记 n 为一个大于 1 的自然数. 若存在非零自然数 k 和 m , 满足

$$n = k^2 + m^2,$$

则在 $\mathbb{Z}[\sqrt{-1}]$ 中有

$$n = (k + m\sqrt{-1})(k - m\sqrt{-1}).$$

因此 n 为平方和当且仅当 n 是 $\mathbb{Z}[\sqrt{-1}]$ 中某个元素的范数.

任取 $k + m\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$, 我们记其不可约分解为

$$k + m\sqrt{-1} = \alpha_1 \cdots \alpha_l.$$

因此

$$N(k + m\sqrt{-1}) = N(\alpha_1) \cdots N(\alpha_l).$$

由之前对不可约元素的刻画, 任取不可约元素 α , 我们有 $N(\alpha)$ 为 2, 模 4 余 1 的素数 p 或者模 4 余 3 的素数 p 的平方. 这就证明了结论的一个方向.

另一个方向的证明来自素数 p 在 $\mathbb{Z}[\sqrt{-1}]$ 中的分解. 我们考虑 n 的素数分解

$$n = 2^k p_1^{l_1} \cdots p_s^{l_s} q_1^{m_1} \cdots q_t^{m_t}.$$

对 2, 我们考虑 $\alpha = 1 + \sqrt{-1}$. 对任意 p_i , 我们有 $\beta_i = u_i + v_i\sqrt{-1}$. 考虑

$$k + m\sqrt{-1} = \alpha^k \beta_1^{l_1} \cdots \beta_s^{l_s} q_1^{\frac{m_1}{2}} \cdots q_t^{\frac{m_t}{2}},$$

则有

$$n = N(k + m\sqrt{-1}).$$

□

注 16.5.5.

注意到构造 $k + m\sqrt{-1}$ 时候, 我们只给出了一个可行的答案. 实际上, 如果具有如上素数分解的 n 可以写成平方和, 那么 (k, m) 的可能的选择共有 $4(l_1 + 1) \cdots (l_s + 1)$. 这是由于单位共有 4 个, 并且每个 β_i 也可以被替换为其共轭.

16.5.2 $\mathcal{O}_{-2}$

当 $D = -2$ 时, 环 $\mathcal{O}_{-1} = \mathbb{Z}[\sqrt{-2}]$ 为 Gauss 整环. 此时任取 $m + n\sqrt{-1} \in \mathbb{Z}[\sqrt{-2}]$, 其范数为

$$N(m + n\sqrt{-1}) = m^2 + 2n^2.$$

其中的单位为 1, -1.

由之前的讨论, 我们考虑素数在 $\mathbb{Z}[\sqrt{-2}]$ 中的分解.

命题 16.5.6

所有素数在环 $\mathbb{Z}[\sqrt{-2}]$ 中的不可约分解如下:

- 1) $p = 2$ 时, 有不可约分解 $2 = \sqrt{-2}(-\sqrt{-2})$;
- 2) $p \equiv 5, 7 \pmod{8}$ 时, p 为 $\mathbb{Z}[\sqrt{-2}]$ 的不可约元素.
- 3) $p \equiv 1, 3 \pmod{4}$ 时, 存在 $m + n\sqrt{-1} \in \mathbb{Z}[\sqrt{-2}]$, 使 p 有如下不可约分解

$$p = (m + n\sqrt{-1})(m - n\sqrt{-1}).$$

证明. $p = 2$ 的情形直接验证即可.

我们下边考虑 p 为一个奇素数的情形. 由 Dedekind-Kummer 分解定理, 我们需要讨论

$$x^2 + 2 \in \mathbb{Z}_2[x]$$

的可约性, 等价地, 我们需要知道 2 是否是模 p 的二次剩余.

由二次互反律结论的第二部分, 我们有

$$\left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p^2-1}{8}}.$$

注意到奇素数 p 满足 $\frac{p^2-1}{8}$ 为偶数, 当且仅当 $p \equiv 1, 7 \pmod{8}$. 另一方面, 奇素数 p 满足 $\frac{p-1}{2}$ 为偶数, 当且仅当 $p \equiv 1, 5 \pmod{8}$.

因此, 若 $p \equiv 1, 3 \pmod{8}$, 我们有

$$\left(\frac{-2}{p}\right) = 1,$$

即 -2 为 p 的二次剩余. 因此 $x^2 + 2 \in \mathbb{Z}_p[x]$ 可约. 若 $r \in \mathbb{Z}_p$ 为 $x^2 + 2$ 的一个根, 则有

$$x^2 + 2 = (x - r)(x + r) \in \mathbb{Z}_p[x].$$

因此在 $\mathbb{Z}[\sqrt{-2}]$ 中, 我们有

$$\langle p \rangle = \langle p, r - \sqrt{-2} \rangle \langle p, r + \sqrt{-2} \rangle.$$

由于 $\mathbb{Z}[\sqrt{-2}]$ 为一个欧几里得环, 我们有 $m + n\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ 满足

$$\langle p, r + \sqrt{-2} \rangle = \langle m + n\sqrt{-2} \rangle,$$

$$\langle p, r - \sqrt{-2} \rangle = \langle m - n\sqrt{-2} \rangle.$$

即

$$\langle p \rangle = \langle m + n\sqrt{-2} \rangle \langle m - n\sqrt{-2} \rangle.$$

在相差一个单位的前提下, 我们可以选取 $m + n\sqrt{-2}$, 满足

$$p = (m + n\sqrt{-2})(m - n\sqrt{-2}) = m^2 + 2n^2.$$

若 $p \equiv 5, 7 \pmod{8}$, 我们有

$$\left(\frac{-2}{p}\right) = -1,$$

因此 -2 不是模 p 的二次剩余. 由 Dedekind-Kummer 分解定理, 我们有 p 为 $\mathbb{Z}[\sqrt{-2}]$ 的一个不可约元素. $\square$

考虑元素的范数计算, 我们有以下推论.

推论 16.5.7

在相伴意义下, 环 $\mathbb{Z}[\sqrt{-2}]$ 中的不可约元素有如下三类

- 1) $\sqrt{-2}$ (范数为 2);
- 2) p (范数为 p^2 , 满足 $p \equiv 5, 7 \pmod{8}$);
- 3) $m + n\sqrt{-1}, m - n\sqrt{-1}$ (范数为 p , 满足 $p \equiv 1, 3 \pmod{8}$).

类似于之前的 Fermat 关于可以写为平方和的自然数的结论, 我们也可以讨论可以写为

$$m^2 + 2n^2$$

的自然数.

思考 16.5.8

使用类似于关于可以写为平方和的自然数的讨论, 给出自然数可以写为 $m^2 + 2n^2$ 的形式的一个充要条件, 并计算每个自然数有多少种不同的写法.

16.5.3 $\mathcal{O}_{-3}$

当 $D = -3$ 时, 环 $\mathcal{O}_{-3} = \mathbb{Z} \left[\frac{1+\sqrt{-3}}{2} \right]$ 为 Gauss 整环. 此时任取 $m+n\frac{1+\sqrt{-3}}{2} \in \mathbb{Z} \left[\frac{1+\sqrt{-3}}{2} \right]$, 其范数为

$$N \left(m + n \frac{1+\sqrt{-3}}{2} \right) = m^2 + mn + n^2.$$

其中的单位为 $1, -1, \frac{1+\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}$.

由之前的讨论, 我们考虑素数在 $\mathbb{Z} \left[\frac{1+\sqrt{-3}}{2} \right]$ 中的分解.

命题 16.5.9

所有素数在环 $\mathbb{Z} \left[\frac{1+\sqrt{-3}}{2} \right]$ 的不可约分解如下:

- 1) $p = 3$ 时, 有不可约分解 $3 = \sqrt{-3}\sqrt{-3}$;
- 2) $p \equiv 2 \pmod{3}$ 时, p 为 $\mathbb{Z} \left[\frac{1+\sqrt{-3}}{2} \right]$ 的不可约元素.
- 3) $p \equiv 1 \pmod{3}$ 时, 存在 $m+n\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$, 满足

$$p = (m+n\sqrt{-3})(m-n\sqrt{-3}).$$

证明. $p = 3$ 的情形直接验证即可.

任取素数 p , 由于 $-3 \equiv 1 \pmod{4}$, 我们需要考虑多项式

$$x^2 - x + 1 \in \mathbb{Z}_p[x]$$

是否可约.

若 $p = 2$, 则

$$x^2 + x + 1 \in \mathbb{Z}_2[x]$$

在 $\mathbb{Z}_2$ 中无根, 因此不可约. 所以 $2 \in \mathcal{O}_{-3}$ 为不可约元素, 也是素元素.

下边设 p 为一个大于 3 的素数. 注意到多项式 $x^2 + x + 1$ 在 $\mathbb{Z}_p[x]$ 中有根当且仅当 $\sqrt{-3} \in \mathbb{Z}_p$, 即

$$\left(\frac{-3}{p} \right) = 1.$$

计算 Legendre 符号有

$$\begin{aligned} & \left(\frac{-3}{p} \right) \\ &= \left(\frac{-1}{p} \right) \left(\frac{3}{p} \right) \\ &= (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} \left(\frac{p}{3} \right) \\ &= \left(\frac{p}{3} \right). \end{aligned}$$

若 $p \equiv 1 \pmod{3}$, 则 -3 是模 p 的二次剩余. 因此存在 $r \in \mathbb{Z}_p$ 为 $x^2 - x + 1 \in \mathbb{Z}_p[x]$ 的根. 我们有

$$x^2 - x + 1 = (x - r)(x + r - 1) \in \mathbb{Z}_p[x].$$

因此在 $\mathcal{O}_{-3}$ 中我们有理想的分解

$$\langle p \rangle = \left\langle p, \frac{1+\sqrt{-3}}{2} - r \right\rangle \left\langle p, \frac{1+\sqrt{-3}}{2} + r - 1 \right\rangle.$$

由于 $\mathcal{O}_{-3}$ 为一个欧几里得环, 我们有 $u + v\frac{1+\sqrt{-3}}{2}$, 满足

$$\begin{aligned}\left\langle p, \frac{1+\sqrt{-3}}{2} - r \right\rangle &= \left\langle u + v\frac{1+\sqrt{-3}}{2} \right\rangle \\ \left\langle p, \frac{1-\sqrt{-3}}{2} - r \right\rangle &= \left\langle u + v\frac{1-\sqrt{-3}}{2} \right\rangle\end{aligned}$$

即

$$\langle p \rangle = \left\langle u + v\frac{1+\sqrt{-3}}{2} \right\rangle \left\langle u + v\frac{1-\sqrt{-3}}{2} \right\rangle.$$

注意到

$$\begin{aligned}(u + v\frac{1+\sqrt{-3}}{2})\frac{1+\sqrt{-3}}{2} &\in \mathbb{Z}[\sqrt{-3}], \\ (u + v\frac{1-\sqrt{-3}}{2})\frac{1-\sqrt{-3}}{2} &\in \mathbb{Z}[\sqrt{-3}].\end{aligned}$$

因此在相差一个单位的前提下, 我们可以选取 $m + n\sqrt{-3}$, 满足

$$p = (m + n\sqrt{-3})(m - n\sqrt{-3}) = m^2 + 3n^2.$$

若 $p \equiv 2 \pmod{3}$, 则 -3 不是模 p 的二次剩余, 因此 $x^2 - x + 1 \in \mathbb{Z}_p[x]$ 不可约. 由 Dedekind-Kummer 分解定理可得 p 为 $\mathcal{O}_{-3}$ 的一个不可约元素. $\square$

考虑元素的范数计算, 我们有以下推论.

推论 16.5.10

在相伴意义下, 环 $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ 中的不可约元素有如下三类

- 1) $\sqrt{-3}$ (范数为 2);
- 2) p (范数为 p^2 , 满足 $p \equiv 2 \pmod{3}$);
- 3) $m + n\sqrt{-3}, m - n\sqrt{-3}$ (范数为 p , 满足 $p \equiv 1 \pmod{3}$).

考虑 $\mathcal{O}_{-3}$ 的元素的范数的形式, 任取 $\mathbb{Z}[\sqrt{-3}]$ 的元素, 其范数可以写为 $m^2 + 3n^2$ 的形式, 也可以写为 $u^2 + uv + v^2$ 的形式. 类似于之前的 Fermat 关于可以写为平方和的自然数的结论, 我们也可以讨论可以写为

$$m^2 + 3n^2$$

的自然数 (这等价于可以写为 $u^2 + uv + v^2$ 的形式).

思考 16.5.11

使用类似于关于可以写为平方和的自然数的讨论, 给出自然数可以写为 $m^2 + 3n^2$ 的形式的一个充要条件, 并计算每个自然数有多少种不同的写法.

第十七章 环上的一元多项式

17.1 实系数一元多项式环回顾

我们首先回顾实数 $\mathbb{R}$ 上的多项式的概念. 我们定义 $\mathbb{R}$ 上的一元多项式为如下形式的表达式

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

其中 $n \in \mathbb{N}$, $a_0, \dots, a_n \in \mathbb{R}$, x 是一个符号.

我们也可以将一个 $\mathbb{R}$ 上的一元多项式记为一个形式级数:

$$f(x) = \sum_{n \in \mathbb{N}} a_n x^n,$$

满足只存在有限多项的系数 $a_n \neq 0$.

对任意两个多项式:

$$f(x) = \sum_{n \in \mathbb{N}} a_n x^n, \quad g(x) = \sum_{n \in \mathbb{N}} b_n x^n,$$

我们定义 $f(x) = g(x)$ 当且仅当对于任意 $n \in \mathbb{N}$, 我们有 $a_n = b_n$. 此外, 我们定义它们的和为:

$$f(x) + g(x) = \sum_{n \in \mathbb{N}} (a_n + b_n) x^n,$$

它们之间的积为:

$$f(x)g(x) = \sum_{n \in \mathbb{N}} \left(\sum_{i=0}^n a_i b_{n-i} \right) x^n.$$

记 $\mathbb{R}[x]$ 为所有多项式的集合.

若 $f(x)$ 的第 m 项之后的各项系数都为 0, $g(x)$ 的第 n 项之后的各项系数都为 0, 设 $k > m + n$, 我们考虑 $f(x)g(x)$ 的第 k 项系数

$$\sum_{i=0}^k a_i b_{k-i} = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0.$$

由于每一项 $a_i b_{k-i}$ 中, 条件 $i > m$ 和 $k-i > n$ 总有至少一个成立, 因此 a_i 和 b_{k-i} 中至少有一个为 0. 因此 $f(x)g(x)$ 第 k 项系数为 0. 因此 $f(x)g(x)$ 仍只有有限多项系数非零.

例 17.1.1.

$$(a_0 + a_1x)(b_0 + b_1x) = a_0b_0 + (a_1b_0 + a_0b_1)x + a_1b_1x^2.$$

我们希望从代数的角度来观察 $\mathbb{R}[x]$.

观察 17.1.2 (i) $\mathbb{R}[x]$ 为一个交换幺环.

(ii) 零元 0 为零多项式, 即对于任意 $n \in \mathbb{N}$, $a_n = 0$.

(iii) 幺元为满足 $a_0 = 1$, 对于任意 $n > 0$, $a_n = 0$ 的多项式.

我们称之为域 $\mathbb{R}$ 上的**多项式环**. 类似的, 任给一个域 F , 我们可以定义 F 上的多项式.

多项式 ≠ 多项式函数

代数意义下的多项式的概念抽象自多项式函数, 但是两个概念是不同的. 当我们考虑函数的时候, 我们关心的是原像和像是如何对应的, 同一个对应可能会有多种表达式.

例如, 我们考虑

$$F = \mathbb{F}_2 = \{\bar{0}, \bar{1}\}.$$

域 $\mathbb{F}_2$ 上的加法和乘法运算表分别为

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

考虑多项式 $f(x) = x + x^2$. 我们将其看作是一个 $\mathbb{F}_2$ 上的函数, 则我们可以直接计算验证

$$f(\bar{0}) = \bar{0} + \bar{0}^2 = \bar{0},$$

$$f(\bar{1}) = \bar{1} + \bar{1}^2 = \bar{0}.$$

因此 $f(x)$ 是 $\mathbb{F}_2$ 上的零函数. 另一方面, 当我们将其看作是一个多项式, 那么 $f(x) \neq 0$, 因为它们有不同的系数.

进一步研究 $\mathbb{F}_2$ 上的多项式函数, 我们会发现里边只有有限多个:

$$\bar{0}, \bar{1}, x, \bar{1} + x.$$

而 $\mathbb{F}_2$ 上的多项式环 $\mathbb{F}_2[x]$ 有无穷多个元素.

实数多项式的数列表示

多项式的另一种描述办法可以帮助我们避免这个混淆. 我们将多项式 $f(x)$ 系数拿出来, 记为一个数列

$$f = (a_n)_{n \in \mathbb{N}} = (a_0, a_1, a_2 \dots).$$

由多项式定义我们知道这个数列里只有有限多项不为 0. 前边介绍的多项式加法和乘法可以翻译为: 对任意只有有限多项不为 0 的数列 $f = (a_n)_{n \in \mathbb{N}}$ 和 $g = (b_n)_{n \in \mathbb{N}}$ 我们定义它们的和以及乘积

$$f + g := (c_n)_{n \in \mathbb{N}}, \quad fg = (d_n)_{n \in \mathbb{N}},$$

满足对于任意 $n \in \mathbb{N}$,

$$c_n = a_n + b_n,$$

$$d_n = \sum_{i=0}^n a_i b_{n-i}.$$

注 17.1.3.

一个 $\mathbb{R}$ 中的数列可以看作是一个从 $\mathbb{N}$ 到 $\mathbb{R}$ 的映射. 我们在介绍多元多项式的时候也会使用这个观点.

17.2 环上一元多项式

我们可以将以上的构造推广到一般的环上. 设 R 为一个环.

定义 17.2.1

环 R 上的一个**多项式**为一个无穷序列

$$f = (a_n)_{n \in \mathbb{N}} = (a_0, a_1, a_2, \dots) \in R^{\mathbb{N}},$$

满足只存在**有限多项**不为 $0 \in R$.

我们首先定义环上多项式的加法和乘法. 任取 R 上的两个多项式

$$f = (a_n)_{n \in \mathbb{N}}, \quad g = (b_n)_{n \in \mathbb{N}},$$

我们定义它们的和以及乘积

$$f + g = (c_n)_{n \in \mathbb{N}}, \quad fg = (d_n)_{n \in \mathbb{N}},$$

满足对于任意 $n \in \mathbb{N}$,

$$c_n := a_n + b_n,$$

$$d_n := \sum_{i=0}^n a_i b_{n-i}.$$

注 17.2.2.

注意到以上的加法和乘法实际上可以定义在整个 $R^{\mathbb{N}}$ 上. 类似于对 $\mathbb{R}[x]$ 的讨论, 由 R 中零元的性质, 以上定义的加法和乘法保持 "有限多个位置非零" 这个性质, 即任意两个多项式的和以及乘积仍是多项式.

例 17.2.3.

乘积 fg 的前几项为:

$$\begin{aligned} d_0 &= a_0 b_0, \\ d_1 &= a_0 b_1 + a_1 b_0, \\ d_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0, \\ &\dots \end{aligned}$$

我们记 S 为环 R 上所有多项式的空间.

$$S := \{(a_0, a_1, \dots) \in R^{\mathbb{N}} \mid \#\{n \in \mathbb{N} \mid a_n \neq 0\} < \infty\} \subset R^{\mathbb{N}}.$$

命题 17.2.4

- (i) S 为一个环.
- (ii) S 的零元为零多项式, 即对于任意 $n \in \mathbb{N}$, $a_n = 0$.

证明. (直接按照定义验证.)

□

定义 17.2.5

环 S 被称作环 R 上的一元多项式环.

例 17.2.6.

我们考虑 $\mathbb{R}$ 上 2 阶上三角方阵构成的集合

$$T_2(\mathbb{R}) := \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{R} \right\}$$

我们可以验证 $T_2(\mathbb{R})$ 对矩阵乘法和加法运算封闭, 且对矩阵加法成群. 因此这是一个环. 其零元为零矩阵. 环 $T_2(\mathbb{R})$ 是一个幺环, 其幺元为单位阵. 该环有零因子. 其形式如下:

$$\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}.$$

一个一般的 $T_2(\mathbb{R})$ 上的多项式有如下形式:

$$\left(\begin{bmatrix} a_0 & b_0 \\ 0 & c_0 \end{bmatrix}, \dots, \begin{bmatrix} a_n & b_n \\ 0 & c_n \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \dots \right).$$

我们考虑两个多项式:

$$f = \left(\begin{bmatrix} a_0 & b_0 \\ 0 & c_0 \end{bmatrix}, \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \dots \right), g = \left(\begin{bmatrix} x_0 & y_0 \\ 0 & z_0 \end{bmatrix}, \begin{bmatrix} x_1 & y_1 \\ 0 & z_1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \dots \right)$$

则 fg 为如下多项式

$$\left(\begin{bmatrix} a_0 & b_0 \\ 0 & c_0 \end{bmatrix} \begin{bmatrix} x_0 & y_0 \\ 0 & z_0 \end{bmatrix}, \begin{bmatrix} a_0 & b_0 \\ 0 & c_0 \end{bmatrix} \begin{bmatrix} x_1 & y_1 \\ 0 & z_1 \end{bmatrix} + \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \begin{bmatrix} x_0 & y_0 \\ 0 & z_0 \end{bmatrix}, \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \begin{bmatrix} x_1 & y_1 \\ 0 & z_1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \dots \right).$$

类似地考虑 gf , 通过比较第 0 个位置上的元素, 我们可以构造 $fg \neq gf$ 的例子. 因此这个多项式环不交换.

另一方面, 这个多项式环含有幺元, 也有零因子. 例如, 若我们有

$$f = \left(\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \dots \right)$$

则 $f^2 = 0$. 因此 f 是多项式环的一个零因子.

我们观察到一般环上的多项式环 S 与实数域上的多项式环 $\mathbb{R}[x]$ 的一些区别是:

$\mathbb{R}[x]$	S
$\forall f, g \in \mathbb{R}[x], fg = gf$	$\exists? f, g \in S, fg \neq gf$
$\exists 1$	$\exists? 1$
$\forall f, g \in \mathbb{R}[x]^*, fg \neq 0$	$\exists? f, g \in S^*, fg = 0$

定义 17.2.7

设多项式 $f \in S$ 满足对于任意 $n > 0$, 都有 $a_n = 0$, 我们称 f 为一个常数多项式.

通过将环 R 中的元素对应到多项式环 S 中的常数多项式, 我们有了一个环 R 到多项式环 S 的嵌入映射定义如下:

$$\begin{aligned}\iota: R &\rightarrow S, \\ a &\mapsto (a, 0, 0, \dots)\end{aligned}$$

命题 17.2.8

映射 ι 是一个环的单同态.

因此我们有

$$R \cong \iota(R),$$

通常我们将 R 看作是 S 的一个子环.

我们记 $S^* := S \setminus \{0\}$.

定义 17.2.9

任取 $f = (a_n)_{n \in \mathbb{N}} \in S^*$, 存在 $n \in \mathbb{N}$, 满足 $a_n \neq 0$, 且对任意 $m \neq n$, $a_m = 0$, 我们称 f 为一个**单项式**.

定义 17.2.10

任给一个不为零的多项式

$$f = (a_n)_{n \in \mathbb{N}} \in S^*,$$

我们定义 f 的**次数**为其不为零的项的下标的最大值:

$$\deg f := \max\{n \in \mathbb{N} \mid a_n \neq 0\}.$$

我们约定 $0 \in S$ 的次数为 $-\infty$.

若 f 的次数为 $n \in \mathbb{N}$, 我们称 a_n 为其**首项系数**.

例 17.2.11.

对任意 $n \in \mathbb{N}$, 单项式 $(0, \dots, 0, \underset{n}{a}, 0, \dots)$ 的次数为 n . 非零常数多项式的次数为 0.

命题 17.2.12 (教材命题2.8.1)

任取 S 中两个非零多项式

$$f = (a_n)_{n \in \mathbb{N}}, \quad g = (b_n)_{n \in \mathbb{N}},$$

设 $\deg f = k$, $\deg g = m$, 我们有

- (i) 设 $k \neq m$, 则 $\deg(f + g) = \max\{\deg f, \deg g\}$.
- (ii) 设 $k = m$, 则 $\deg(f + g) \leq \max\{\deg f, \deg g\}$, 其中等号成立当且仅当 $a_k + b_m \neq 0$.
- (iii) $\deg fg \leq \deg f + \deg g$, 其中等号成立当且仅当 $a_k b_m \neq 0$.

证明. (利用多项式的次数的定义直接验证) □

例 17.2.13.

我们考虑系数在环 $\mathbb{Z}_4$ 中的多项式. 我们知道 $\mathbb{Z}_4$ 是一个含零因子的交换幺环. 其零因子为 $\bar{2}$. 我们考虑如下两个多项式:

$$\begin{aligned} f &= (\bar{1}, \bar{0}, \bar{2}, \bar{0}, \dots), \\ g &= (\bar{3}, \bar{2}, \bar{0}, \dots). \end{aligned}$$

我们有 $\deg f = 2, \deg g = 1$. 我们计算它们的乘积多项式的各项系数分别为:

$$\begin{aligned} c_0 &= \bar{1} \cdot \bar{3} = \bar{3} \\ c_1 &= \bar{1} \cdot \bar{2} + \bar{0} \cdot \bar{3} = \bar{2} \\ c_2 &= \bar{1} \cdot \bar{0} + \bar{0} \cdot \bar{2} + \bar{2} \cdot \bar{3} = \bar{2} \\ c_3 &= \bar{2} \cdot \bar{2} = \bar{0} \\ c_4 &= \bar{0} \\ &\dots \end{aligned}$$

因此 $\deg(fg) = 2 < 2 + 1 = \deg f + \deg g$.

由以上命题, 我们有以下推论

推论 17.2.14 (教材命题2.8.1)

- (i) 环 S 为一个幺环当且仅当 R 为一个幺环.
- (ii) 环 S 交换当且仅当 R 交换.
- (iii) 环 S 无零因子当且仅当 R 无零因子.
- (iv) 环 S 为一个整环当且仅当 R 是一个整环.

证明. (i) 若 R 有一个幺元 1 , 则我们可以考虑多项式

$$e = (1, 0, \dots).$$

任取 R 上的多项式

$$f = (a_0, a_1, \dots),$$

由公式我们计算 ef 和 fe , 得 $ef = fe = f$. 因此 e 为幺元.

假设 S 中有一个幺元, 记为

$$e = (e_0, e_1, e_2, \dots),$$

则 $e \in S^*$, 我们记 $n = \deg e$. 由幺元的性质, 任取多项式 f , 我们有 $ef = fe = f$.

任取 0 次非零多项式

$$f = (a_0, 0, 0, \dots),$$

我们计算 ef 和 fe 的第 0 个位置上的系数分别为 $e_0 a_0$ 和 $a_0 e_0$. 由于 $ef = fe = f$, 我们有

$$e_0 a_0 = a_0 e_0 = a_0 \in R.$$

由于 $a_0 \in R$ 可以任取, 因此我们有 e_0 为 R 的幺元.

(ii) 任取 R 中的元素 a , 我们有唯一的一个 0 次多项式

$$f_a = (a, 0, \dots).$$

若 S 交换, 则所有的零次多项式交换. 特别地, 任取 $a, b \in R$. 我们有 $f_a f_b = f_b f_a$. 我们考虑第 0 个位置上的系数有 $ab = ba$. 因此 R 交换.

现在假设 R 交换. 任取 S 中的两个多项式:

$$f = (a_0, a_1, \dots), g = (b_0, b_1, \dots),$$

我们考虑 fg 和 gf 的系数. 对任意 $n \in \mathbb{N}$, 两个多项式的第 n 个位置上的系数分别为

$$\sum_{i=1}^n a_i b_{n-i}, \sum_{i=1}^n b_{n-i} a_i$$

由于 R 交换, 我们有 $a_i b_{n-i} = b_{n-i} a_i$. 因此我们有对任意 $n \in \mathbb{N}$, fg 和 gf 第 n 个位置上系数相同. 因此 $fg = gf$. 由此我们得到 S 交换.

(iii) 假设 S 有零因子 f 和 g , 满足 $fg = 0$, 我们有

$$-\infty = \deg(fg) < \deg f + \deg g.$$

我们记 $\deg f = m, \deg g = n$. 由命题 17.2.12, 我们有首项系数乘积 $a_n b_m = 0 \in R$. 由于非零多项式首项系数非零, 因此 R 有零因子 a_m 和 b_n .

若 R 有零因子 a 和 b , 满足 $ab = 0$, 我们考虑 0 次多项式 f 和 g , 满足 $a_0 = a, b_0 = b$. 由于 $a, b \in R^*$, 我们有 $f, g \in S^*$. 另一方面, 我们有

$$fg = (ab, 0, \dots).$$

由于 $ab = 0$, 我们有 fg 所有位置上的系数都是 0. 因此 $fg = 0 \in S$. 因此 S 有零因子.

(iv) 以上三个结论合在一起可得 R 为整环当且仅当 S 为整环.

□

注 17.2.15.

记 R 为一个环. 若 $a \in R$, 满足对任意 $b \in R$, 有 $ab = ba = 0$, 我们并不能说明 $a = 0$. 比如

$$R = \left\{ \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} \middle| x \in \mathbb{R} \right\} \subset \text{Mat}_2(\mathbb{R})$$

以下我们列出一些 R 及其上的一元多项式环 S 之间的关系:

R	S
交换	交换
$\exists 1$	$\exists 1$
无零因子环	无零因子环
整环	整环

假设 R 为一个幺环. 我们令

$$x = (0, 1, 0, \dots) \in S,$$

任取 $n \in \mathbb{N}$ 以及 $a \in R$, 记

$$ax^n = (0, \dots, 0, \underset{n}{a}, 0, \dots)$$

命题 17.2.16

我们有如下结论

(i) 任取 $f \in S$, 我们有 $fx = xf$.

(ii) 对于任意 $a, b \in R$, 对于任意 $m, n \in \mathbb{N}$, 我们有

$$(ax^m)(bx^n) = (ab)x^{m+n} = (0, \dots, 0, \underset{m+n}{ab}, 0, \dots) \in S.$$

(iii) 任意多项式 $f = (a_n)_{n \in \mathbb{N}} \in S^*$ 可以唯一的被表示为如下形式:

$$f = a_0 + a_1x + \cdots + a_nx^n,$$

其中 $a_n \neq 0$.

证明. (i) 任取

$$f = (a_0, a_1, \dots) \in S,$$

我们直接计算

$$fx = (0, a_0, a_1, \dots) = xf.$$

(ii) (直接计算.)

(iii) 任取

$$f = (a_0, a_1, \dots, a_n, 0, \dots) \in S^*$$

设 $\deg f = n$, 我们有

$$f = a_0 + a_1x + \cdots + a_nx^n,$$

其中 $a_n \neq 0$.

若存在 $b_0, \dots, b_m \in R$, 且 $b_m \neq 0$, 满足

$$f = b_0 + \cdots + b_mx^m,$$

则

$$(a_0, a_1, \dots, a_n, 0, \dots) = f = (b_0, \dots, b_m, 0, \dots).$$

因此我们有 $m = n$ 且对任意 $i \in \{0, \dots, n\}$, 有 $a_i = b_i$. □

若 R 为幺环, 我们将使用 $R[x]$ 记 R 上的一元多项式环 S .

设 D 为一个整环, 我们希望知道:

D	$D[x]$
UFD	UFD ?
PID	PID ?
欧几里得整环	欧几里得整环 ?

思考 17.2.17

整数环 $\mathbb{Z}$ 为欧几里得环. 考虑 $\mathbb{Z}[x]$. 理想 $\langle 2, x \rangle$ 是主理想么?

引理 17.2.18

任给整环 D , 多项式 f 是 $D[x]$ 的单位, 当且仅当 f 是 D 中的单位.

证明. 注意到 $D \subset D[x]$ 幺元相同. 因此 D 的单位也是 $D[x]$ 的单位.

反过来, 由于 D 为整环, 我们有 $D[x]$ 为整环. 若 f 为 $D[x]$ 的单位, 则存在 $g \in D[x]$, 满足 $fg = 1$. 我们有

$$0 = \deg 1 = \deg(fg) = \deg f + \deg g.$$

因此 $\deg f = \deg g = 0$. 所以 $f, g \in D$. 引理得证. $\square$

命题 17.2.19

任给整环 D , 我们记 U 为其单位群. 我们有

- (i) 单项式 x 是 $D[x]$ 的一个不可约元素.
- (ii) 单项式 x 是 $D[x]$ 的一个素元素.
- (iii) $D[x]/\langle x \rangle \cong D$.
- (iv) 设存在 $a \in D^* \setminus U$ (即 a 非零且不可逆), 理想 $\langle a, x \rangle$ 不是主理想.

证明. (i) 设 $f, g \in D[x]$, 满足

$$x = fg.$$

由于 D 为整环, 我们有

$$\deg f + \deg g = \deg x = 1.$$

我们有 $\deg f = 0, \deg g = 1$ 或者 $\deg f = 1, \deg g = 0$. 不失一般性的, 我们假设 $\deg f = 0$ 且 $\deg g = 1$. 我们有:

$$f = a, \quad g = b_0 + b_1x$$

因此我们有 $x = ab_0 + ab_1x$. 由于多项式相等当且仅当系数相等, 我们有

$$ab_0 = 0, \quad ab_1 = 1.$$

因此 $f = a$ 为单位. 由此可知 x 不可约.

(ii) 任取 $h \in D[x]$, 满足第 0 项系数为 0, 我们记为

$$h = a_1x + a_2x^2 + \cdots + a_nx^n,$$

其中 $n \in \mathbb{N}^*$, 则有

$$h = x(a_1 + a_2x + \cdots + a_nx^{n-1}),$$

因此 $x \mid h$.

反过来, 若 $x \mid h$, 存在多项式

$$h_1 = b_0 + \cdots + b_mx^m \in D[x],$$

其中 $m \in \mathbb{N}$, 满足

$$h = xh_1 = b_0x + \cdots + b_mx^{m+1}.$$

因此 h 的第 0 项系数为 0.

设 $f, g \in D^*$, 满足 $x \mid fg$, 则存在多项式 $h \in D[x]$, 满足 $xh = fg$.

由于 xh 的第 0 项系数为 0, 因此 fg 的第 0 项系数为 0.

我们分别记 f 和 g 的第 0 项系数为 a_0 和 b_0 . 因此我们有 $a_0b_0 = 0$. 由于 D 为整环, 因此 $a_0 = 0$ 或者 $b_0 = 0$.

因此 $x \mid f$ 或者 $x \mid g$.

(iii) 由上可知, 由 x 生成的理想为所有第 0 项系数为 0 的多项式. 因此任给 R 中元素 $a \neq b$, 我们有

$$a + \langle x \rangle \neq b + \langle x \rangle.$$

因此

$$\phi : D \rightarrow D[x] \xrightarrow{\pi} D[x]/\langle x \rangle.$$

是一个单射.

另一方面, 任给 $D[x]/\langle x \rangle$ 中的非零元素 $f + \langle x \rangle$, 我们有 f 的第 0 项系数 a_0 不为 0. 因此是 $a_0 \in D$ 的像. 由此 ϕ 是一个满射. 所以 ϕ 是一个同构.

(iv) 我们考虑 $a \in D^* \setminus U$. 记 $I = \langle a, x \rangle$.

若存在多项式 f , 满足 $\langle f \rangle = I$, 则 $f \mid x$.

由于 x 不可约, 我们有 $f \in U$ 或者 $f \sim x$. 若 $f \sim x$, 则与 $f \mid a$ 矛盾, 因为 $\deg f > \deg a$. 因此 $f \in U$. 这样我们有 $I = D[x]$, 因此 $1 = ag + hx$.

由于 hx 的第 0 项系数为 0, 我们有 ag 的第 0 项系数为 1. 所以 $a \in U$. 矛盾. 命题得证. $\square$

推论 17.2.20

若 $D[x]$ 是 PID, 则 R 是一个域.

17.3 交换幺环上一元多项式

在这部分, 所有环均为交换幺环. 另外, 当我们讨论一个交换幺环包含另一个交换幺环为子环的时候, 我们总是假设两个环的幺元相同.

环 R 的自映射环

我们记 R 为一个交换幺环, 并记所有从 R 到自己的映射的集合为

$$\mathcal{F}(R) := \{\phi \in R \times R \mid \phi \text{ 为一个映射}\}.$$

任给 $\phi, \psi \in \mathcal{F}(R)$, 我们可以定义它们的和为

$$\begin{aligned} \phi + \psi : R &\rightarrow R, \\ a &\mapsto (\phi + \psi)(a) := \phi(a) + \psi(a). \end{aligned}$$

以及它们的乘积为

$$\begin{aligned} \phi\psi : R &\rightarrow R, \\ a &\mapsto (\phi\psi)(a) := \phi(a)\psi(a). \end{aligned}$$

命题 17.3.1

集合 $\mathcal{F}(R)$ 及其上的加法和乘法构成了一个交换幺环.

注 17.3.2.

我们此处考虑的是任意映射, 不要求一定是同态映射. 我们没有使用映射的复合来构造乘法. 实际上我们得到的是一个环的直积 $R^{\otimes R}$.

思考 17.3.3

所有 R 上的自同态映射的集合关于以上定义的加法和乘法封闭么?

命题 17.3.4

(i) 环 $\mathcal{F}(R)$ 的零元为:

$$\begin{aligned}\mathbb{0} : R &\rightarrow R, \\ a &\mapsto 0.\end{aligned}$$

(ii) 环 $\mathcal{F}(R)$ 的幺元为:

$$\begin{aligned}\mathbb{1} : R &\rightarrow R, \\ a &\mapsto 1.\end{aligned}$$

证明. (练习)

□

定义 17.3.5

我们称环 $\mathcal{F}(R)$ 为 R 的**自映射环**.

多项式函数

任给多项式

$$f = a_0 + \cdots + a_n x^n \in R[x],$$

我们可以构造一个多项式函数记做 ψ_f :

$$\begin{aligned}\psi_f : R &\rightarrow R \\ u &\mapsto \psi_f(u) := f(u) = a_0 + \cdots + a_n u^n\end{aligned}$$

从这个观点, 我们得到如下一个映射:

$$\begin{aligned}\Psi_R : R[x] &\rightarrow \mathcal{F}(R). \\ f &\mapsto \psi_f\end{aligned}$$

命题 17.3.6

映射 Ψ_R 是一个环同态.

证明. (练习)

□

思考 17.3.7

若环 R 不交换, Ψ_R 是否仍是良定义? 是否仍是同态?

提示: 多项式有 $(a_1x)(a_1x) = a_1^2x^2$, 我们是否有 $(a_1a)(a_1a) = a_1^2a^2$?

更一般的, 我们考虑 R_1 为一个包含 R 为子环的交换幺环. 则我们可以类似地定义环同态

$$\Psi_{R_1} : R[x] \rightarrow \mathcal{F}(R_1).$$

任给 R 为子环的交换幺环 R_1 , 同态 Ψ_{R_1} 的核不一定平凡. 也即可能存在非零多项式诱导一个零函数.

例 17.3.8.

例如我们之前介绍的 F_2 上的多项式. 我们考虑

$$\Psi_{\mathbb{F}_2} : \mathbb{F}_2[x] \rightarrow \mathcal{F}(\mathbb{F}_2).$$

多项式 $f = x + x^2$ 的像多项式函数 $\psi_f(u) = u + u^2$ 作为函数是一个零函数:

$$f(\bar{0}) = \bar{0} + \bar{0}^2 = \bar{0},$$

$$f(\bar{1}) = \bar{1} + \bar{1}^2 = \bar{0},$$

我们因此有 $f \in \ker \Psi_{\mathbb{F}_2}$.

引理 17.3.9 (教材引理2.8.6)

设 R 为一个交换幺环, 则存在交换幺环 $R_1 \supset R$, 有 Φ_{R_1} 是一个单同态, 也即任何 $R[x]$ 中两个不同的多项式作为 R_1 上的函数也不同.

证明. 我们考虑 $R_1 = R[x]$. 任取

$$f = a_0 + \cdots + a_n x^n \in R[x],$$

我们将其看作 $R[x]$ 上的映射:

$$\psi_f : R[x] \rightarrow R[x]$$

$$g \mapsto \psi_f(g) = a_0 + \cdots + a_n g^n.$$

若设 $g = x \in R[x]$. 则对任意 f , 我们有 $\psi_f(g) = f$. 因此任给 $f_1 \neq f_2$, 则 $\psi_{f_1}(g) \neq \psi_{f_2}(g)$. 因此两个函数不相同. □

例 17.3.10.

我们仍考虑 $R = \mathbb{F}_2$. 若我们考虑 $\mathbb{F}_2[x]$ 作为 $\mathbb{F}_2[x]$ 上的多项式函数, 则任取两个不同多项式给出的函数也不同.

注 17.3.11.

为了简化记号, 我们对多项式和多项式函数使用相同的记号 f .

代数元和超越元

我们考虑交换幺环 R_1 及环 $\mathcal{F}(R_1)$. 任给元素 $u \in R_1$, 我们可以构造一个映射:

$$\begin{aligned}\Phi_u : \mathcal{F}(R_1) &\rightarrow R_1, \\ \psi &\mapsto \psi(u).\end{aligned}$$

命题 17.3.12

映射 Φ_u 是一个环同态.

证明. (练习)

□

我们沿用以上记号, 考虑交换幺环 R_1 及其任意包含幺元的子环 R . 记 $R[x]$ 为 R 上的多项式环. 任给 $u \in R_1$, 则我们有 $\varphi_u = \Phi_u \circ \Psi_{R_1}$ 为一个从 $R[x]$ 到 R_1 的映射:

$$\begin{aligned}\varphi_u : R[x] &\xrightarrow{\Psi_{R_1}} \mathcal{F}(R_1) \xrightarrow{\Phi_u} R_1, \\ f &\longmapsto \psi_f \longmapsto \psi_f(u).\end{aligned}$$

推论 17.3.13

映射 φ_u 为一个环同态.

定义 17.3.14 (教材定义2.8.8)

任取 R_1 中的元素 u . 我们称 u 为 R 上的

- (i) **代数元**, 若 $\exists f \in R[x]^*, \varphi_u(f) = f(u) = 0$;
- (ii) **超越元**, 若 $\forall f \in R[x]^*, \varphi_u(f) = f(u) \neq 0$.

注 17.3.15.

我们可以将其重写为如下条件: R_1 中的元素 u 称为 R 上的

- (i) 代数元, 若存在 $n \in \mathbb{N}$ 以及 R 中不全为零的元素 $a_0, \dots, a_n$, 满足

$$\bullet \quad a_0 + a_1 u + \dots + a_n u^n = 0;$$

- (ii) 超越元, 若对任意 $n \in \mathbb{N}$ 以及任意 $a_0, \dots, a_n \in R$, 我们有

$$\bullet \quad a_0 + a_1 u + \dots + a_n u^n = 0 \text{ 当且仅当 } a_0 = \dots = a_n = 0.$$

从这个角度, 代数元和超越元的定义不需要事先定义 $R[x]$.

注 17.3.16.

从 R 上的多项式方程的角度看, R 上的代数元就是某个 R 上多项式的根.

命题 17.3.17

记 R 为交换幺环. 所有 R 中的元素都是 R 上的代数元.

证明. 对任意 $u \in R$, 我们取多项式 $f = u - x$. 则 $\varphi_u(f) = f(u) = u - u = 0$. $\square$

例 17.3.18.

环 R_1 中的关于 R 的代数元的集合可能严格包含 R . 例如, 我们取 $R = \mathbb{Q}$, $R_1 = \mathbb{R}$, 则 $\sqrt{2}$ 是 $\mathbb{Q}$ 上的代数元. 考虑 $x^2 - 2 \in \mathbb{Q}[x]$, 我们有

$$(\sqrt{2})^2 - 2 = 0.$$

我们仍考虑交换幺环 R_1 及其包含幺元的子环 R . 我们考虑之前定义的同态映射

$$\varphi_u : R[x] \rightarrow R_1.$$

由定义, 我们有

命题 17.3.19

- (i) 元素 $u \in R_1$ 为 R 上的代数元当且仅当 $\ker \varphi_u \neq \{0\}$.
- (ii) 元素 $u \in R_1$ 为 R 上的超越元当且仅当 $\ker \varphi_u = \{0\}$.

环的扩张

设 R_1 是包含交换幺环 R 的环. 任取 $u \in R_1$, 我们考虑 φ_u 的像集:

$$R[u] := \varphi_u(R[x]) = \{a_0 + a_1u + \cdots + a_nu^n \mid n \in \mathbb{N}, a_0, \dots, a_n \in R\} \subset R_1.$$

我们知道 $R[u]$ 是由 $R \cup \{u\}$ 生成的 R_1 的子环. 由环同态定理我们有如下推论.

推论 17.3.20 (教材命题2.8.9)

元素 a 为超越元当且仅当 φ_a 为从 $R[x]$ 到 $R[u]$ 的环同构.

推论 17.3.21

设元素 u 为 R 上的超越元. 任取 R 中的元素 $a_0, \dots, a_m, b_0, \dots, b_n$, 满足 $a_m, b_n \neq 0$, 若

$$a_0 + a_1u + \cdots + a_mu^m = b_0 + b_1u + \cdots + b_nu^n,$$

则 $m = n$, 且

$$\forall i \in \{0, \dots, n\}, a_i = b_i.$$

证明. 不失一般性的, 我们可以假设 $m \leq n$. 若 $m < n$, 我们可以添加系数为 0 的项, 将左边记为

$$a_0 + a_1u + \cdots + a_nu^n,$$

若存在 $k \in \{0, \dots, n\}$, 使得 $a_k \neq b_k$, 我们可以取两个式子的差

$$\sum_{i=0}^n (a_i - b_i) u^i = 0.$$

由假设, 我们知道 $a_k - b_k \neq 0$, 因此多项式

$$f = \sum_{i=0}^n (a_i - b_i) x^i,$$

非零. 由于

$$\varphi_u(f) = f(u) = 0,$$

由定义, 元素 u 为一个代数元. 矛盾. □

我们现在给出多项式环的另一种定义.

定义 17.3.22 (教材定义2.8.10)

设 R 为一个交换幺环, R_1 为一个包含 R 为子环的交换幺环. 我们称 R_1 为 R 上的**多项式环**, 若

- 存在元素 $u \in R_1$, 满足 $R_1 = R[u]$,
- 该元素 u 为 R 上超越元.

我们进一步称该超越元 u 为 R_1 在 R 上的**生成元**.

注 17.3.23.

该定义独立于之前的定义. 从这个角度我们主要关心的是一个环 R 在添加一个元素 u 后的扩张. 我们后边会看到, 当其在同构意义下是"最大"时, 就是多项式环.

思考 17.3.24 (教材思考题2.8.11)

举例说明多项式环的生成元不一定唯一.

定理 17.3.25 (教材定理2.8.12)

任意交换幺环上的多项式环(按照新的定义)一定存在, 且任意两个多项式环之间都同构.

证明. 我们考虑本章开始定义的环 S , 其中的元素为有限多个位置上不为 0 的 R 上的序列. 我们考虑 S 的子环:

$$\{(a, 0, \dots, 0, \dots) \mid a \in R\}.$$

该子环与 R 同构. 我们将其记为 R , 并仍记多项式 $(a, 0, \dots, 0, \dots)$ 为 a .

考虑元素 $x = (0, 1, 0, \dots, 0, \dots)$. 我们可以证明 x 是 R 上的超越元. 任取 $a_0, \dots, a_n \in R$, 我们有

$$a_0 + a_1 x + \dots + a_n x^n = (a_0, \dots, a_n, 0, \dots).$$

因此等式右边多项式为零多项式当且仅当

$$a_0 = \cdots = a_n = 0,$$

所以 u 为超越元. 由于任意多项式 $f \in S$ 都可以表达为

$$f = a_0 + \cdots + a_n x^n,$$

的形式, 因此 $R \cup \{x\}$ 生成 S , 即 $R[x] = S$. 由定义 S 是 R 上的多项式环, 且 x 为 $R[x]$ 的生成元.

若 $R_1 = R[u]$ 和 $R_2 = R[v]$ 都是 R 上的多项式环, 注意到 R 是 R_1 和 R_2 的子环, 我们可以考虑环同态

$$\varphi_u : R[x] \rightarrow R_1 \text{ 和 } \tilde{\varphi}_v : R[x] \rightarrow R_2,$$

由于 u 和 v 都是超越元, 由之前的讨论知, φ_u 和 $\tilde{\varphi}_v$ 都是环同构, 因此 $R_1 \cong R_2$. $\square$

例 17.3.26.

我们考虑 S . 记 $x = (0, 1, 0, \dots)$. 我们有 $x^2 = (0, 0, 1, 0, \dots)$. 我们可以验证 x^2 也是 R 上的超越元. 由此, 我们考虑 $R[x^2]$ 也是 R 上的多项式环. 但是 $R[x^2]$ 是 S 的一个真子环.

如下定理告诉我们, 若我们考虑环 R 的关于一个元素 u 的扩张 $R[u]$, 当 u 为超越元时, 这个扩张在同构意义下是"最大"的, 即任意 R 关于一个元素 v 的环扩张都可以看作是 $R[u]$ 的一个商环.

定理 17.3.27 (教材定理2.8.13)

设 R_1 为一个交换幺环, R 为其包含幺元的子环. 设 $u \in R_1$. 以下两个叙述等价:

- (i) $R[u]$ 是一个 R 上的多项式环, 也即 u 为 R 上的超越元;
- (ii) 任给交换幺环 R_2 , 同态 $\eta : R \rightarrow R_2$, 以及元素 $v \in R_2$, 存在 η 的一个扩充

$$\eta_1 : R[u] \rightarrow R_2,$$

满足 $\eta_1|_R = \eta$, 且 $\eta_1(u) = v$.

注 17.3.28.

由于 $R \cup \{u\}$ 生成 $R[u]$, 若扩充 η_1 存在, 则其唯一.

以上定理中 (ii) 说明存在 η_1 满足以下交换图:

$$\begin{array}{ccc} R & \xrightarrow{\eta} & R_2 \\ \downarrow \iota & \nearrow \exists! \eta_1 & \\ R[u] & & \end{array}$$

其中

$$\begin{aligned} \iota : R &\rightarrow R[u] \\ a &\mapsto a. \end{aligned}$$

定理 17.3.27 的证明. 若要证明命题中两个条件等价, 我们只需证明以下两个命题

1) 若 u 为一个超越元, 则对任意选取的 R_2, η 以及 v , 存在扩充 η_1 .

2) 若 u 为一个代数元, 则可以找到 R_2, η 以及 v , 使得扩充 η_1 不存在.

这两个命题分别对应 (i) $\implies$ (ii) 以及 (ii) $\implies$ (i).

(i) $\implies$ (ii): 我们考虑形式上定义 η_1 满足 $\eta_1|_R = \eta$, $\eta_1(u) = v$, 且保持加法与乘法运算. 由于 u 为一个超越元, 因此任取 $a_0, \dots, a_m, b_0, \dots, b_n \in R$, 满足 $a_m, b_n \neq 0$, 则

$$\sum_{i=0}^m a_i u^i = \sum_{i=0}^n b_i u^i,$$

当且仅当 $m = n$ 且

$$\forall i \in \{0, \dots, n\}, a_i = b_i.$$

因此对于任意 $R[u]$ 中的元素 α , 我们有唯一的表达式

$$\alpha = \sum_{i=0}^n a_i u^i,$$

其中 $a_n \neq 0$. 由此我们可以定义

$$\begin{aligned} \eta_1 : R[u] &\rightarrow R_2 \\ \sum_{i=0}^n a_i u^i = \alpha &\mapsto \eta_1(\alpha) := \sum_{i=0}^n \eta(a_i) v^i \end{aligned}$$

即为所求环同态.

(ii) $\implies$ (i): 我们可以取 $R_2 = R[x]$. 取 $v = x$. 令 $\eta = \iota : a \mapsto a$. 由于 u 为代数元, 因此存在 $n \in \mathbb{N}$, $a_0, \dots, a_n \in R$ 其中 $a_n \neq 0$, 满足:

$$a_0 + a_1 u + \dots + a_n u^n = 0.$$

假设存在环同态 η_1 , 则我们有

$$\begin{aligned} 0 &= \eta_1(0) \\ &= \eta_1(a_0 + a_1 u + \dots + a_n u^n) \\ &= \eta(a_0) + \eta(a_1)x + \dots + \eta(a_n)x^n \\ &= a_0 + a_1 x + \dots + a_n x^n \\ &\neq 0 \in R[x] \end{aligned}$$

矛盾. □

注 17.3.29.

考虑交换幺环 R_1 和 R_2 . 任意同态 $\phi : R_1 \rightarrow R_2$, 我们都可以将其扩充为 $\tilde{\phi} : R_1[x] \rightarrow R_2[x]$, 有 $\tilde{\phi}|_{R_1} = \phi$.

注 17.3.30.

以上命题实际是环同态基本定理 14.2.1 的一个特殊情形下的应用. 任给一个环 A 及其中一个固定的理想 I , 若我们希望对于任意 A 的理想 J 都有如下交换图:

$$\begin{array}{ccc} A & \xrightarrow{\pi_J} & A/J \\ \pi_I \downarrow & \nearrow \exists! \phi & \\ A/I & & \end{array}$$

则对任意 J , 我们都应有

$$I = \ker \pi_I \subset \ker \pi_J = J.$$

特别地, 我们取 $J = \{0\}$ 时, 有 $I \subset \{0\}$. 因此, 我们有 $I = \{0\}$.

考虑以上定理中的情形. 我们令 $A = R[x]$. 考虑同态 $\varphi_u : R[x] \rightarrow R[u]$. 令 $I = \ker \varphi_u$. 因此

$$R[u] \cong R[x]/I.$$

考虑同态

$$\bar{\varphi}_v : R[x] \rightarrow \eta(R)[x] \rightarrow \eta(R)[v].$$

令 $J = \ker \bar{\varphi}_v$. 因此

$$\eta(R)[v] \cong R[x]/J.$$

若 v 是 $\eta(R)$ 一个超越元, 我们有 $\bar{\varphi}_v$ 为单同态. 若同时 η 为一个单同态, 则 $J = \{0\}$. 由以上讨论, 若我们有以上交换图, 则 $I = \{0\}$. 因此元素 u 为超越元.

由此命题我们有以下两个推论:

推论 17.3.31 (教材推论2.8.14)

设 R_1 与 R_2 为交换幺环. 设 S_1 为 R_1 上的多项式环. 记 $u \in S_1$ 为一个生成元. 设交换幺环 S_2 为包含 R_1 的一个子环. 设 $v \in S_2$. 任意满同态 $T_0 : R_1 \rightarrow R_2$, 可以扩充为一个满同态:

$$T : R_1[u] \rightarrow R_2[v].$$

更进一步, T 为同构当且仅当 T_0 为同构, 且 v 为 R_2 上的超越元.

注 17.3.32.

我们尝试借助交换图来理解以上推论. 记 R, R_1 和 R_2 都是交换幺环.

首先任给一个 R , 我们有一个 R 到其多项式环的嵌入 ι , 将每个 $a \in R$ 送到 0 次多项式 $(a, 0, \dots)$.

然后, 我们由 R_1 到 R_2 的环同态 T_0 , 我们可以得到 $R_1[x]$ 到 $R_2[x]$ 的一个环同态记作 $\widetilde{T}_0$.

$$\begin{aligned} \widetilde{T}_0 : R_1[x] &\rightarrow R_2[x], \\ (a_0, a_1, \dots) &\mapsto (T_0(a_0), T_0(a_1), \dots). \end{aligned}$$

注意到 T_0 是一个环同构当且仅当 $\widetilde{T}_0$ 是一个环同构.

最后任取 $I \subset R$ 为一个理想, 我们有如下环同构

$$(R/I)[x] \cong R[x]/I[x].$$

将以上给部分放在一起, 并且考虑之前介绍的同态 φ_u 以及环同态基本定理, 我们可以

有以下交换图我们考虑如下交换图:

$$\begin{array}{ccccc}
 R_1 & \xrightarrow{T_0} & R_2 & & \\
 \downarrow \iota_1 & \searrow & \downarrow \iota_2 & \nearrow & \\
 & \overline{R_1} & & & \\
 & \downarrow \overline{\iota_1} & & & \\
 & \overline{R_1}[x] & & & \\
 \uparrow & \nearrow & \downarrow & \searrow & \\
 R_1[u] & \xrightarrow{\varphi_u^{-1}} & R_1[x] & \xrightarrow{\widetilde{T}_0} & R_2[x] & \xrightarrow{\varphi_v} & R_2[v] \\
 \cong \uparrow & & & & \downarrow & \nearrow & \\
 & & & & R_2[x]/\ker \varphi_v & &
 \end{array}$$

其中 $\iota_1, \iota_2, \overline{\iota_1}$ 均为环到其对应多项式环的嵌入, 记 $\overline{R_1} = R_1/\ker T_0$.
注意到

$$T = \varphi_v \circ \widetilde{T}_0 \circ \varphi_u^{-1}.$$

这里三个同态都是满射. 其中由于 u 为超越元, φ_u^{-1} 是一个环同构. 因此 T 是一个环同构当且仅当 $\widetilde{T}_0$ 和 φ_v 都是环同构. 另一方面, 我们有

- $\widetilde{T}_0$ 为环同构当且仅当 T_0 为环同构,
- φ_v 是一个环同构当且仅当 v 是 R_2 上的超越元.

因此我们有以上推论.

推论 17.3.33 (教材推论2.8.15)

设 R 是交换幺环, S_1 和 S_2 是 R 上的两个多项式环. 记 u 和 v 分别为 S_1 和 S_2 的生成元. 那么存在为一个从 S_1 到 S_2 的环同构 T , 满足 $T(u) = v$ 且 $T|_R$ 为恒等映射. (称 T 为一个 R -同构)

17.4 整环上的多项式

回顾: 若 $f \in R[x]$ 为一个 n -次多项式, 我们称 a_n 为 f 的首项系数. 设 f 和 g 分别为 R 上的次数为 n 和 m 的多项式, 且首项系数分别为 a_n 和 b_m , 则我们有 $\deg(fg) = \deg f + \deg g$ 当且仅当 $a_n b_m \neq 0$.

在本节中, 若无特殊注明, 我们考虑的环境均为整环.

记 D 是一个整环, 则其多项式环 $D[x]$ 也为整环. 我们有:

引理 17.4.1

任取 $f, g \in D[x]^*$, 我们有 $\deg(fg) = \deg f + \deg g$.

我们考虑 S 是 D 上的一个多项式环. 设 a 为一个生成元, 则 $S = D[a]$ 中的任意一个元素 y 都可以唯一的写为 $y = f(a)$, 这里 $f(x) \in D[x]$. 我们将 $f(x)$ 的次数和首项系数为 y 作为 a 的多项式的次数和首项系数. 我们记 y 关于 a 的次数为 $\deg_a y$.

注 17.4.2.

注意到以上定义的 y 的次数和首项系数都是关于 a 的, 即当我们将 S 考虑为 D 上的一元多项式环的时候, 似乎以上定义依赖于 a 的选择. 如果选取另一个生成元, 考虑将 y 表达为 b 的多项式, 我们会有疑问 y 关于 b 的次数和首项系数和之前关于 a 的相同么? 以下定理告诉我们, 如果 b 是另一个 S 在 D 上的生成元, 则有

$$\deg_a y = \deg_b y.$$

如果记 a_y 为 y 作为 a 的多项式的首项系数, b_y 为 y 作为 b 的多项式的首项系数, 则有 $a_y \sim b_y$, 二者相伴.

设 $S = D[a]$ 为 D 上的一个多项式环, 且 $a \in S$ 为一个生成元. 任取 $f(x) \in D[x]^*$, 我们得到 S 上的函数

$$\begin{aligned} \psi_f : S &\rightarrow S \\ b &\mapsto \psi_f(b) = f(b). \end{aligned}$$

定理 17.4.3 (教材定理2.9.1)

任取 $b \in S^*$ 和 $f(x) \in D[x]^*$, 满足 $\deg f = m$ 和 $\deg_a b = n$, 则

$$\deg_a f(b) = mn.$$

此外, b 为 S 在 D 上的生成元, 当且仅当 $b = a_0 + a_1 a$, 且 a_1 为 D 中的单位. (也即 b 为 a 的 1-次多项式, 且首项系数为 D 中的单位.)

我们首先来看一个引理.

引理 17.4.4

设 $g_1(a), \dots, g_k(a)$ 为 S 中 k 个多项式, 次数分别为 $n_1, \dots, n_k$. 则多项式

$$\deg_a (g_1(a) \cdots g_k(a)) = n_1 + \cdots + n_k.$$

证明. 任取 $f, g \in D[x]^*$, 由定义

$$\deg_a f(a)g(a) = \deg f(x)g(x).$$

由之前关于两个多项式乘积的次数的引理, 并对多项式个数做归纳, 引理得证. $\square$

定理 17.4.3 的证明. 由于 $b \in S^*$, 因此存在 $g(x) \in D[x]$, 满足 $b = g(a)$.

我们记

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m,$$

对于任意 $0 \leq j \leq m$, 若 $a_j \neq 0$, 利用引理可得

$$\deg_a a_j b^j = \deg_a a_j (g(a))^j = jn,$$

因此 $\deg_a f(b)$ 的次数为 nm .

若 b 为一个生成元, 则 $S = D[a] = D[b]$, 因此 a 可以写为 b 的多项式. 存在多项式 $f(x), g(x) \in D[x]^*$, 满足

$$a = f(b), \quad b = g(a).$$

因此, 我们有 $a = f(g(a))$. 我们记 $f(x)$ 和 $g(x)$ 的次数分别为 m 和 n .

由于 a 为 R 上的超越元, 由推论 17.3.21, 我们有两个关于 a 的多项式相等当且仅当各项系数相等. 因此, 作为必要条件, 我们有

$$\deg f(g(a)) = 1.$$

另一方面, 由命题的第一部分, 我们有 $\deg f(g(a)) = mn$. 因此 $m = n = 1$. 由此, 我们可以找到 R 中的元素 a_0, a_1, b_0, b_1 , 满足

$$\begin{aligned} a &= f(b) = b_0 + b_1 b \\ b &= g(a) = a_0 + a_1 a \end{aligned}$$

我们可以计算

$$\begin{aligned} a &= f(g(a)) \\ &= b_0 + b_1(a_0 + a_1 a) \\ &= (b_0 + b_1 a_0) + (b_1 a_1) a \end{aligned}$$

因此

$$\begin{cases} b_1 a_1 = 1 \\ b_0 + b_1 a_0 = 0 \end{cases}$$

因此 a_1 为一个单位, 且 $b_1 = a_1^{-1}$. 进一步, 我们有 $a_0 = -b_1^{-1} b_0$. 由此我们证明了, 若 b 为一个生成元, 则存在 D 中的元素

$$\begin{cases} a_0 = -b_1^{-1} b_0 \\ a_1 = b_1^{-1} \end{cases}$$

其中 b_0 和 b_1 是元素 a 写作 b 的多项式时的系数.

我们假设存在 $a_0, a_1 \in D$, 使得

$$b = a_0 + a_1 a = g(a),$$

其中 $a_1 \in U$. 我们有

$$a = -a_0 a_1^{-1} - a_1^{-1} b \in D[b].$$

由此可得 $D[a] \subset D[b]$. 另一方面 $D[b]$ 为 $D[a]$ 中由 $D \cup \{b\}$ 生成的子环, 因此我们有 $D[a] = D[b]$.

下边使用反证法证明 b 为 D 的超越元. 假设 b 为代数元, 则存在 $f(x) \in D[x]^*$, 使得 $f(b) = 0$.

考虑 $h(a) = f(a_0 + a_1 a)$ 为一个 a 的多项式. 我们有

$$\deg h = \deg_a h(a) = \deg f \geq 0.$$

因此 $h \in D[x]^*$. 由构造, 我们有 $h(a) = 0$. 因此 a 为 D 上的代数元, 这与 a 是一个生成元(超越元)矛盾. 因此 b 是一个超越元. $\square$

注 17.4.5.

由证明的最后一部分, 我们知道, 任取 $f \in D[x]^*$, 满足 $\deg f > 0$, 我们有 $f(a)$ 为 D 上的超越元.

利用我们在前一节证明的结论, 以及上边的命题, 我们有以下推论

推论 17.4.6 (教材推论2.9.3)

任意 $D[x]$ 上的同态映射 $\phi : D[x] \rightarrow D[x]$ 为一个 D -同构, 当且仅当存在一个单位 $\epsilon \in D$, 满足 $\phi(x) = \epsilon x + a$, 且 $\phi|_D = id$.

我们下边开始讨论 $D[x]$ 上的带余除法. 我们首先考虑 D 中的两个元素 a 和 b , 我们有如下观察:

观察 17.4.7 • 若 b 为一个单位, 则我们可以有 $a = (ab^{-1})b$.

- 若 b 不是一个单位, 则我们有 $ba = ab$.

我们进一步考虑 $D[x]$ 中的单项式.

观察 17.4.8

我们考虑 $ax^m, bx^n \in D[x]^*$. 我们假设 $m \geq n$. 则

- 若 b 为一个单位, 我们有 $ax^m = (ab^{-1}x^{m-n})bx^n$.
- 若 b 不是一个单位, 则我们有 $ba x^m = (ax^{m-n})bx^n$

因此, 我们有如下引理:

引理 17.4.9

任取单项式 ax^m 和 bx^n , 我们可以有多项式 $p(x)$ 和 $r(x)$ 满足

$$ba x^m = p(x)bx^n + r(x),$$

满足 $r(x)$ 的次数小于 m . 且这样的 $p(x)$ 和 $r(x)$ 是唯一的.

证明. 若 $n \leq m$, 可以取 $p(x) = ax^{m-n}$, $r(x) = 0$. 若 $n > m$, 我们可以取

$$p(x) = 0, \quad r(x) = ax^m.$$

若存在两对多项式 $(p_1(x), r_1(x))$ 以及 $(p_2(x), r_2(x))$, 我们有

$$(p_1(x) - q_1(x))g(x) + (r_1(x) - r_2(x)) = 0.$$

我们注意到若 $p_1(x) - q_1(x) \neq 0$, 由于 $R[x]$ 是一个整环, 没有零因子, 我们有

$$\begin{aligned} & \deg((p_1(x) - q_1(x))g(x) + (r_1(x) - r_2(x))) \\ &= \max\{\deg(p_1(x) - q_1(x))g(x), \deg(r_1(x) - r_2(x))\} \\ &= \deg(p_1(x) - q_1(x))g(x) && \text{引理17.2.12} \\ &= \deg(p_1(x) - q_1(x)) + \deg g(x) && \text{没有零因子} \\ &> -\infty \end{aligned}$$

因此, 矛盾. 则我们有 $p_1(x) = p_2(x)$, 进一步有 $r_1(x) = r_2(x)$. □

对于一般多项式, 我们可以不断的迭代以上引理, 得到以下定理

定理 17.4.10 (教材定理2.9.4)

任取 $f(x), g(x) \in D[x]^*$, 我们设 $\deg f = m, \deg g = n$, 并记多项式 g 的首项系数为 a , 以及记

$$k = \max\{m - n + 1, 0\},$$

则存在两个多项式 $p(x), r(x) \in D[x]$, 满足

$$a^k f(x) = p(x)g(x) + r(x),$$

其中 $0 \leq \deg r < \deg g$ 或者 $r(x) = 0$. 进一步地, 满足以上条件的多项式对 $(p(x), r(x))$ 是唯一的.

证明. 首先证明存在性. 任取 $n \in \mathbb{N}$, 我们考虑 $m < n$ 和 $m \geq n$ 两种情况.

若 $m < n$, 则我们取 $p(x) = 0$ 以及 $r(x) = f(x)$ 即满足要求.

若 $m \geq n$, 则我们对 m 做归纳. 记 f 的首项系数为 a_m .

首先考虑 $m = n$ 的情形, 此时 $m - n + 1 = 1$, 因此 $k = 1$. 考虑多项式

$$p(x) = a_m, \quad r(x) = af(x) - a_m g(x).$$

注意到 $r(x)$ 的次数至多为 m , 另一方面 $r(x)$ 的 m 次系数为 $aa_m - a_m a = 0$, 因此有 $0 \leq \deg r < \deg g$ 或者 $r(x) = 0$, 满足要求.

下设 $m > n$, 并设结论对小于 $\deg f < m$ 的情形都成立. 下设 $\deg f = m$, 考虑

$$q(x) = a_m x^{m-n},$$

则我们有

$$af(x) - q(x)g(x) = f_1(x).$$

由条件, 我们知道 $f_1(x)$ 是一个次数为 $m - 1$ 的多项式.

由归纳假设以及对 $m < n$ 的情形的讨论, 存在 $p_1(x)$ 和 $r_1(x)$ 满足

$$a^{k_1} f_1(x) = p_1(x)g(x) + r_1(x),$$

其中

$$k_1 = \max\{\deg f_1 - n + 1, 0\} \leq k - 1,$$

且 $0 \leq \deg r_1 < \deg g$ 或者 $r_1(x) = 0$.

考虑以上两式, 我们有

$$a^{k_1}(af(x) - q(x)g(x)) = p_1(x)g(x) + r_1(x).$$

我们可以将其整理为

$$a^{k_1+1}f(x) = (a^{k_1}q(x) + p_1(x))g(x) + r_1(x).$$

由于 $k_1 \leq k - 1$, 我们考虑以上等式两边都乘以 $a^{k-(k_1+1)}$, 则有

$$a^k f(x) = a^{k-(k_1+1)}(a^{k_1}q(x) + p_1(x))g(x) + a^{k-(k_1+1)}r_1(x).$$

因此我们有

$$\begin{aligned} p(x) &= a^{k-(k_1+1)}(a^{k_1}q(x) + p_1(x)) \\ r(x) &= a^{k-(k_1+1)}r_1(x) \end{aligned}$$

其中 $\deg r = \deg r_1 < \deg g$ 或者 $r_1 = r = 0$.

唯一性的证明与引理中的证明相同. 若存在两对多项式 $(p_1(x), r_1(x))$ 以及 $(p_2(x), r_2(x))$, 我们有

$$(p_1(x) - q_1(x))g(x) + (r_1(x) - r_2(x)) = 0.$$

我们注意到若 $p_1(x) - q_1(x) \neq 0$, 由于 $D[x]$ 是一个整环, 没有零因子, 我们有

$$\begin{aligned} & \deg((p_1(x) - q_1(x))g(x) + (r_1(x) - r_2(x))) \\ &= \max\{\deg(p_1(x) - q_1(x))g(x), \deg(r_1(x) - r_2(x))\} \\ &= \deg(p_1(x) - q_1(x))g(x) && \text{引理17.2.12} \\ &= \deg(p_1(x) - q_1(x)) + \deg g(x) && \text{没有零因子} \\ &> -\infty \end{aligned}$$

因此, 矛盾. 则我们有 $p_1(x) = p_2(x)$, 进一步有 $r_1(x) = r_2(x)$. □

思考 17.4.11

考虑一般交换幺环. 设其有零因子. 举一个例子使得不存在引理中的带余除法. 另举一个例子使得引理中的满足要求的两个多项式 $p(x)$ 和 $r(x)$ 不唯一.

这里应该注意, 之所以我们不能称 $D[x]$ 为一个欧几里得环, 是因为这里的带余除法是比较弱的一个版本. 特别地, 由于并非所有元素都是单位, 我们在做带余除法时, 必须在左侧也配一些元素. 但我们还是可以考虑如下问题:

- 若我们按这个较弱版本的带余除法做辗转相除, 会得到什么?

按照我们新的方式做辗转相除, 我们有

$$\begin{aligned} b_0^{k_0} f &= p_0 g + r_0 \\ b_1^{k_1} g &= p_1 r_0 + r_1 \\ b_2^{k_2} r_0 &= p_2 r_1 + r_2 \\ &\dots \\ b_{n-1}^{k_{n-1}} r_{n-3} &= p_{n-1} r_{n-2} + r_{n-1} \\ b_n^{k_n} r_{n-2} &= p_n r_{n-1} + r_n \end{aligned}$$

这里 b_i 为 r_{i-1} 的首项系数, $r_n = 0$. 因此, 我们有如下关系:

$$\begin{aligned} b_0^{k_0} \dots b_n^{k_n} f(x) &= q_f(x) r_{n-1}(x) \\ b_1^{k_1} \dots b_n^{k_n} g(x) &= q_g(x) r_{n-1}(x) \end{aligned}$$

由此, 我们可以得到如下命题:

命题 17.4.12

任给 $D[x]$ 中非零多项式 f 和 g , 存在一个非零多项式 r , 以及多项式 p 和 q , 满足

- $r = pf + qg$.
- $\deg r = \min\{\deg(uf + vg) \mid u, v \in D[x], uf + vg \neq 0\}$.

另外, 若存在多项式 r_1, p_1, q_1 满足条件则我们有零次多项式 $a, b \in D^*$, 满足 $ar_1 = br$.

注 17.4.13.

这是一个弱化版的 Bezout 等式.

证明. 由于次数是自然数, 且

$$\min\{\deg(uf + vg) \mid u, v \in D[x], uf + vg \neq 0\} \leq \max\{\deg f, \deg g\}.$$

因此, 存在 p 和 q 满足

$$\deg(pf + qr) = \min\{\deg(uf + vg) \mid u, v \in D[x], uf + vg \neq 0\}.$$

我们有多项式 r, p 和 q 的存在性. 我们下边主要证明命题的第二部分.

设存在 r_1 以及多项式 p_1 和 q_1 存在. 那么有

$$\begin{aligned} r &= pf + qg \\ r_1 &= p_1f + q_1g \end{aligned}$$

我们记 a 为 r 的首项系数. 注意到

$$\deg r = \min\{\deg(uf + vg) \mid u, v \in D[x], uf + vg \neq 0\} = \deg r_1$$

由定理 17.4.10, 我们可以找到多项式 q_2 和 r_2 , 满足

$$ar_1 = p_2r + r_2,$$

且 $0 \leq \deg r_2 < \deg r$ 或者 $r_2 = 0$. 由于

$$ar_1 - p_2r = a(p_1f + q_1g) - p_2(pf + qg) = (ap_1 - p_2p)f + (aq_1 - p_2q)g,$$

我们有 $r_2 = 0$, 即 $ar_1 = p_2r$. 注意到 $a \neq 0$ 且 $r_1 \neq 0$, 由

$$\deg(ar_1) = \deg a + \deg r_1 = \deg r_1 = \deg r = \deg(p_2r) = \deg p_2 + \deg r.$$

因此 $\deg p_2 = 0$. 因此 $p_2 = b \in D^*$, 命题得证. □

推论 17.4.14

对任意的多项式 $r = pf + qg$, 满足

$$\deg r = \min\{\deg(uf + vg) \mid u, v \in D[x], uf + vg \neq 0\},$$

存在 $b_f, b_g \in D^*$, 满足 $r \mid b_ff$, 且 $r \mid b_gg$.

例 17.4.15.

我们举一个抽象的例子来说明以上弱化版的辗转相除. 取 $f, g \in D[x]^*$, 且有

$$\begin{aligned} b_0^{k_0} f &= p_0g + r_0, \\ b_1^{k_1} g &= p_1r_0 + r_1, \\ b_2^{k_2} r_0 &= p_2r_1 + r_2, \\ b_3^{k_3} r_1 &= p_3r_2. \end{aligned}$$

其中

$$b_0, \dots, b_3 \in D^*, 0 \leq \deg r_2 < \deg r_1 < \deg r_0 < \deg g.$$

从上向下依次带入有

$$\begin{aligned} r_0 &= b_0^{k_0} f - p_0 g \\ r_1 &= b_1^{k_1} g - p_1 r_0 \\ &= b_1^{k_1} g - p_1 (b_0^{k_0} f - p_0 g) \\ &= (b_1^{k_1} + p_1 p_0) g - p_1 b_0^{k_0} f \\ r_2 &= b_2^{k_2} r_0 - p_2 r_1 \\ &= b_2^{k_2} (b_0^{k_0} f - p_0 g) - p_2 ((b_1^{k_1} + p_1 p_0) g - p_1 b_0^{k_0} f) \\ &= (b_2^{k_2} b_0^{k_0} + p_2 p_1 b_0^{k_0}) f + (b_2^{k_2} p_0 - p_2 (b_1^{k_1} + p_1 p_0)) g \end{aligned}$$

从下向上依次带入有

$$\begin{aligned} b_3^{k_3} r_1 &= p_3 r_2. \\ b_3^{k_3} b_2^{k_2} r_0 &= b_3^{k_3} p_2 r_1 + b_3^{k_3} r_2 \\ &= p_2 p_3 r_2 + b_3^{k_3} r_2 \\ &= (p_2 p_3 + b_3^{k_3}) r_2 \\ b_3^{k_3} b_2^{k_2} b_1^{k_1} g &= b_3^{k_3} b_2^{k_2} p_1 r_0 + b_3^{k_3} b_2^{k_2} r_1, \\ &= p_1 (p_2 p_3 + b_3^{k_3}) r_2 + b_2^{k_2} p_3 r_2 \\ &= (p_1 (p_2 p_3 + b_3^{k_3}) + b_2^{k_2} p_3) r_2 \\ b_3^{k_3} b_2^{k_2} b_1^{k_1} b_0^{k_0} f &= b_3^{k_3} b_2^{k_2} b_1^{k_1} p_0 g + b_3^{k_3} b_2^{k_2} b_1^{k_1} r_0 \\ &= p_0 (p_1 (p_2 p_3 + b_3^{k_3}) + b_2^{k_2} p_3) r_2 + b_1^{k_1} (p_2 p_3 + b_3^{k_3}) r_2 \\ &= (p_0 (p_1 (p_2 p_3 + b_3^{k_3}) + b_2^{k_2} p_3) + b_1^{k_1} (p_2 p_3 + b_3^{k_3})) r_2 \end{aligned}$$

因此有

$$\begin{aligned} r_2 &\mid b_3^{k_3} b_2^{k_2} b_1^{k_1} b_0^{k_0} f, \\ r_2 &\mid b_3^{k_3} b_2^{k_2} b_1^{k_1} g. \end{aligned}$$

推论 17.4.16

若 D 为一个域, 则多项式环 $D[x]$ 为一个欧几里得环.

证明. 域是特殊的整环, 任取 $f, g \in D[x]^*$, 记 f 和 g 的次数分别为 m 和 n , 利用定理 17.4.10, 我们有

$$a^k f = pg + r,$$

其中 a 为 g 的首项系数, $k = \max\{m - n + 1, 0\}$, 且有 $0 \leq \deg r < \deg g$ 或者 $r = 0$.

域中所有非零元素都是可逆的, 因此我们总有

$$f = a^{-k} pg + a^{-k} r,$$

其中 $0 \leq \deg a^{-k} r < \deg g$ 或者 $r = 0$.

考虑

$$\begin{aligned} \delta : D[x]^* &\rightarrow \mathbb{N}, \\ h &\mapsto \deg h, \end{aligned}$$

以上结论告诉我们 δ 是一个欧几里得函数, $D[x]$ 是一个欧几里得整环. □

综合之前的讨论, 考虑到欧几里得整环也是 PID, 我们有如下等价关系:

推论 17.4.17

任取环 D , 以下三个叙述等价:

- (i) D 为一个域;
- (ii) $D[x]$ 为一个 PID;
- (iii) $D[x]$ 为一个欧几里得整环.

17.5 UFD 上的多项式

设 D 为一个 UFD. 因此, 我们可以定义 D 中元素的最大公因子. 需要注意的是, 由于我们总是在相伴意义下讨论整除, 最大公因子在相伴意义下是良定义的, 且在此意义下是唯一的.

定义 17.5.1 (教材定义 2.9.6)

设 D 为一个 UFD, 任取 $f \in D[x]^*$, 我们称 f 为**本原多项式**, 若其所有系数互素, 即若记

$$f(x) = a_0 + \cdots + a_n x^n,$$

有

$$\gcd(a_0, \dots, a_n) = 1.$$

回顾: 1) $a_1, \dots, a_n$ **两两互素**是指

$$\forall i \neq j, \forall p \in D, (p|a_i) \wedge (p|a_j) \implies p \text{ 是一个单位}.$$

例如, 3, 20, 7, 11 两两互素.

2) $a_1, \dots, a_n$ **互素**是指

$$\forall p \in D, (\forall i, p|a_i) \implies p \text{ 是一个单位}.$$

例如, 2, 5, 10, 14 互素.

注 17.5.2.

有的文献中在定义本原多项式的时候仅考虑次数大于 0 的多项式, 此处我们沿用教材的处理, 也考虑 0 次多项式. 一个 0 次多项式为本原多项式当且仅当其为 $D[x]$ 的单位.

我们进一步考虑一个一般的多项式所有系数的最大公因子, 做如下定义.

定义 17.5.3 (教材定义2.9.6)

设 D 为一个 UFD, 任取一个多项式 $f \in D[x]^*$, 我们定义 f 的**容度** $c(f)$ 为其所有系数的最大公因子, 即若记

$$f(x) = a_0 + \cdots + a_n x^n,$$

则 f 的容度为

$$c(f) = \gcd(a_0, \dots, a_n).$$

注 17.5.4.

最大公因子是在相伴意义下是唯一的, 因此, 容度是在相伴意义下良定义的, 且是唯一的. 后边为方便书写, 我们使用 $c(f) = c(g)$ 来表示两个多项式容度相同. 需要注意的是这个等号是在相伴意义下定义的.

注 17.5.5.

考虑最大公因子的性质, 任取 $a \in D^*$ 以及 $f \in D[x]^*$, 我们有

$$c(af) = ac(f).$$

下边命题是以上定义的一个直接推论.

命题 17.5.6

设 D 为一个 UFD, 任取 $f \in D[x]^*$, 我们有

- (i) $c(f) \in U$ 当且仅当 f 为本原多项式.
- (ii) 若 $f \in D[x]$ 中不可约元素, 则 f 为本原多项式.

我们下边给出 Gauss 引理, 及其证明.

引理 17.5.7 (教材引理2.9.7)

设 D 为一个 UFD. 任给多项式 $f, g \in D[x]^*$, 我们有

$$c(fg) = c(f)c(g).$$

特别地, 我们有两个本原多项式的乘积仍是一个本原多项式.

证明. 我们记

$$\begin{aligned} f &= c(f)f_1, \\ g &= c(g)g_1, \\ fg &= c(fg)h. \end{aligned}$$

由于

$$fg = (c(f)f_1)(c(g)g_1) = (c(f)c(g))f_1g_1,$$

由容度的定义我们知道

$$c(f)c(g) | c(fg),$$

我们只需要证明

$$c(fg)|c(f)c(g).$$

由容度定义我们知道多项式 f_1 和 g_1 为本原多项式, 等价的我们有 $c(f_1)$ 和 $c(g_1)$ 都是单位. 因此其乘积也是单位.

另一方面, 我们有

$$c(fg) = c(f)c(g)c(f_1g_1).$$

由于 D 为整环, 利用消去律, 我们只需证明 $c(f_1g_1)|c(f_1)c(g_1)$, 即 $c(f_1g_1)$ 为一个单位.

我们使用反证法. 我们设 f 和 g 的次数分别为 m 和 n , 并记

$$f_1(x) = a_0 + \cdots + a_mx^m,$$

$$g_1(x) = b_0 + \cdots + b_nx^n.$$

假设 $c(f_1g_1)$ 不是单位, 因此存在一个不可约元素 $p \in D$ 整除 f_1g_1 的所有系数. 由于 f_1 和 g_1 都是本原多项式, 因此存在 $0 \leq s \leq m$ 以及 $0 \leq t \leq n$, 满足

$$s = \min\{i \in \{0, \dots, m\} \mid p \nmid a_i\},$$

$$t = \min\{i \in \{0, \dots, n\} \mid p \nmid b_i\}.$$

即 a_s 为 f_1 的系数中从 a_0 开始第一个不被 p 整除的系数, b_t 为 g_1 的系数中从 b_0 开始第一个不被 p 整除的系数. 我们考虑 f_1g_1 的第 $s+t$ 项的系数:

$$a_0b_{s+t} + a_1b_{s+t-1} + \cdots + a_{s-1}b_{t+1} + a_sb_t + a_{s+1}b_{t-1} + \cdots + a_{s+t}b_0.$$

我们注意到除了 a_sb_t 之外, 其他每一项都有 $S = \{a_0, \dots, a_{s-1}, b_0, \dots, b_{t-1}\}$ 中的元素. 由条件我们知道 p 整除 S 中的每一个元素. 由于 p 整除 f_1g_1 的所有系数, 我们有 $p|a_sb_t$.

由于 D 是一个 UFD, 因此所有的不可约元素也是素元素. 由 $p|a_sb_t$ 可得 $p|a_s$ 或 $p|b_t$, 这与 a_s 和 b_t 的选择矛盾.

因此, 我们有 f_1g_1 也是本原多项式. 引理得证. $\square$

引理 17.5.8 (教材引理2.9.8)

设 $f, g \in D[x]$, 其中 g 为一个本原多项式, 设 $b \in D^*$, 若 $g|bf$, 则 $g|f$.

证明. 若 $f = 0$, 则结论成立. 下设 $f \in D[x]^*$.

若

$$g \mid bf,$$

则存在多项式 $h \in D[x]^*$, 满足

$$hg = bf.$$

由 Gauss 引理, 我们有

$$c(h)c(g) = bc(f),$$

由于 $c(g)$ 是单位, 因此 $b \mid c(h)$, 我们进一步有 $b \mid h$. 因此存在多项式 $h_1 \in D[x]^*$,

$$h = bh_1,$$

由此可得

$$bh_1g = bf.$$

由于 D 是整环, 因此 $D[x]$ 也是整环. 利用消去律, 我们有

$$h_1g = f.$$

因此有 $g \mid f$. $\square$

定理 17.5.9 (教材定理2.9.9)

若 D 是一个 UFD, 那么 $D[x]$ 也是一个 UFD.

回顾: 一个整环 D 被称为 UFD, 若其满足以下条件: 任意 $a \in D^* \setminus U$ 可以被分解为有限多个不可约元素的乘积, 且该分解在相伴和相差一个重排的意义下唯一.

本节剩下的部分将用来给出定理 17.5.9 的证明. 我们将分别证明 $D[x]$ 满足素条件和满足有限分解条件.

引理 17.5.10

设 $\deg f = 0$. 则 f 在 $R[x]$ 中的不可约当且仅当 f 在 R 中的不可约.

证明. 在整环中, 任取 $g, h \in D[x]^*$, 我们有

$$\deg gh = \deg g + \deg h.$$

因此若 $g \mid f$, 则 $\deg g \leq \deg f$.

设 $g, h \in D[x]$, 满足 $f = gh$. 注意到

$$0 = \deg f = \deg g + \deg h.$$

因此

$$\deg g = \deg h = 0.$$

所以 $g, h \in D$. 由于 D 和 $D[x]$ 的单位群相同, g (相应的 h) 是 $D[x]$ 单位当且仅当 g (相应的 h) 是 D 的单位, 因此 f 在 $D[x]$ 中不可约当且仅当 f 在 D 中不可约. $\square$

下边我们证明 $D[x]$ 满足素条件.

引理 17.5.11

若多项式 $u \in D[x]$ 不可约, 则 u 为素元素.

证明. 设 $u \in D[x]^*$ 不可约. 任取 $v \in D[x]^*$, 由命题 17.4.12, 我们可以得到多项式 $r, p, q \in D[x]$, 满足

- $r = pu + qv$,
- $\deg r = \min\{\deg(\tilde{p}u + \tilde{q}v) \mid \tilde{p}, \tilde{q} \in R[x], \tilde{p}v + \tilde{q}w \neq 0\}$.

且存在 $b_u, b_v \in D^*$, 使得 $r \mid b_u u$, 且 $r \mid b_v v$.

记 w 为一个多项式. 我们假设 u 不可约, 且 $u \mid vw$. 则存在 u' 满足 $uu' = vw$. 考虑以上 $r, p, q \in D[x]$.

若 $q = 0$, 我们有 $u \mid r$, 因此

$$u \mid b_v v.$$

由于 u 不可约, 因此为本原多项式, 由之前引理, 我们有

$$u \mid v.$$

下设 $q \neq 0$, 我们有

$$\begin{aligned} quu' &= qvw \\ &= (r - pu)w \\ &= rw - puw \end{aligned}$$

因此 $u \mid rw$.

取本原多项式 $r_1 \in D[x]^*$, 满足

$$r = c(r)r_1,$$

由 $r \mid b_u u$, 可得

$$r_1 \mid u.$$

(同理可得 $r_1 \mid v$.) 因此存在 $s \in D[x]^*$, 满足

$$u = sr_1.$$

注意到 u 不可约, 因此是本原多项式. 所以 s 也是本原多项式. 另一方面, 考虑 $u \mid rw$, 我们有

$$sr_1 \mid c(r)r_1w.$$

利用消去律, 可得

$$s \mid c(r)w.$$

因此 $s \mid w$.

由于 u 不可约, 且 $u = sr_1$, 我们有 $r_1 \sim u$ 或 $s \sim u$.

若 $r_1 \sim u$, 由于 $r_1 \mid v$, 我们有

$$u \mid v.$$

若 $s \sim u$, 则有 $u \mid w$.

综上所述, 引理得证. □

引理 17.5.12

任意 $f \in D[x]^* \setminus U$ 都可以写为 $D[x]$ 中有限多个不可约元素的乘积.

证明. 任取多项式 $f \in D[x]^* \setminus U$, 则存在本原多项式 $g \in D[x]$, 满足

$$f = c(f)g.$$

若 $c(f)$ 为单位, 我们设 $f = g$. 否则, 由于 D 为 UFD, 因此 $c(f)$ 若不是单位, 则存在 $k > 0$ 个 D 中不可约元素 $p_1, \dots, p_k$, 满足

$$c(f) = p_1 \cdots p_k.$$

注意 D 中不可约元素也是 $D[x]$ 中不可约元素.

若 $\deg f = 0$, 则 $g \sim 1$, 我们不妨设 $f = c(f)$, 则 f 可以写为 $D[x]$ 中有限多个不可约元素的乘积.

下设 $\deg f > 0$, 因此 $\deg g > 0$. 我们只需证明 g 可以分解为有限多个 $D[x]$ 中不可约元素的乘积即可.

若 g 已经不可约, 则得证.

若 g 可约, 则存在 $g_0, g_1 \in D[x]^* \setminus U$, 满足

$$g = g_0 g_1.$$

我们进一步有

$$\deg g = \deg g_0 + \deg g_1,$$

$$\deg g > \deg g_0,$$

$$\deg g > \deg g_1.$$

注意到以上不等式是严格的. 这是由于 g 是一个本原多项式. 因此若 $g = g_0 g_1$, $\deg g_0 = 0$ 或者 $\deg g_1 = 0$, 我们有 $g_0 \in U$ 或 $g_1 \in U$, 这与 g_0 和 g_1 的条件矛盾.

注意到 g_0 和 g_1 都为本原多项式. 我们继续对 g_0 和 g_1 分别重复以上讨论, 并继续.

注意到以上讨论过程必然在有限步停止. 这是因为多项式的次数为自然数, 且每次分解都会让多项式次数降低至少 1.

最后我们需要说明以上过程停止的时候所得的多项式都是不可约的. 注意到我们每一步是对上一步得到的多项式分别讨论. 如果得到的某个多项式是不可约的, 我们停止. 如果不是不可约的, 我们继续分解, 得到的如果还需要分解, 最终我们回到一个 1 次多项式. 注意到 1 次多项式是本原的当且仅当是不可约的.

因此存在有限多个不可约次数大于 0 的多项式 $u_1, \dots, u_m$, 满足

$$g = u_1 \cdots u_m.$$

因此 g 满足有限分解条件.

综上所述, 我们有 f 可以分解为 $D[x]$ 中有限多个不可约元素的乘积:

$$f = p_1 \cdots p_k u_1 \cdots u_m.$$

□

以上我们分别证明 $D[x]$ 满足素条件和有限分解条件, 因此 $D[x]$ 是 UFD.

第十八章 环上的多元多项式

18.1 $\mathbb{N}^n$

我们先考虑 $\mathbb{R}$ 上的多项式. 类似于 $\mathbb{R}$ 上的一元多项式, $\mathbb{R}$ 上的多元多项式也可以写为有限多个单项式

$$ax_1^{i_1} \cdots x_n^{i_n},$$

的和.

在我们介绍和研究一元多项式 $\mathbb{R}[x]$ 的时候, 每个单项式都有一个次数是一个自然数 $n \in \mathbb{N}$. 自然数 $\mathbb{N}$ 上的加法幺半群结构以及序结构在我们将域上多项式的定义推广到环上多项式的定义, 以及后边换上多项式理论的研究中都发挥了重要的作用.

与一元多项式不同的是, 由于我们有了不止一个未知元, 我们需要多个自然数来描述不同未知元在同一个单项式中的次数, 来区别不同的单项式. 因此在介绍环上 n -元多项式之前, 我们首先介绍如何将 $\mathbb{N}$ 上的半群结构以及序结构推广到 $\mathbb{N}^n$.

我们考虑自然数 $\mathbb{N}$ 中 n 元组的集合:

$$\mathbb{N}^n := \{\underline{i} = (i_1, \dots, i_n) \mid i_1, \dots, i_n \in \mathbb{N}\} = \underbrace{\mathbb{N} \times \cdots \times \mathbb{N}}_{n \text{ 次}}.$$

任给 $\mathbb{N}^n$ 中两个元素 $\underline{i}$ 和 $\underline{j}$, 我们可以定义加法

$$\underline{i} + \underline{j} := (i_1 + j_1, \dots, i_n + j_n).$$

我们可以验证 $\mathbb{N}^n$ 关于这个加法成一个幺半群, 其幺元为 $(0, \dots, 0)$.

利用 $\mathbb{N}$ 上的序关系, 我们可以在集合 $\mathbb{N}^n$ 上定义一个**字典序**. 任取 $\underline{i} \neq \underline{j}$, 我们定义:

- $\underline{i} \prec \underline{j}$, 若存在一个 $k \in \{1, \dots, n\}$, 使得

$$\begin{cases} i_s = j_s, & \forall s < k \\ i_k < j_k \end{cases}$$

我们注意到, 若不存在以上条件中的 k , 则 $\underline{i}$ 和 $\underline{j}$ 在每个位置上都相同, 因此相等. 我们定义

- $\underline{i} \preceq \underline{j}$, 若我们有 $\underline{i} \prec \underline{j}$ 或 $\underline{i} = \underline{j}$,

并称 $\preceq$ 为 $\mathbb{N}^n$ 上的字典序关系.

我们可以验证 $\preceq$ 是一个全序关系, 也即 $\preceq$ 满足

- (i) 自反性: $\forall \underline{i}$, 有 $\underline{i} \preceq \underline{i}$;
- (ii) 传递性: 若 $\underline{i} \preceq \underline{j}$ 且 $\underline{j} \preceq \underline{k}$, 则有 $\underline{i} \preceq \underline{k}$;
- (iii) 反对称性: 若 $\underline{i} \preceq \underline{j}$ 且 $\underline{j} \preceq \underline{i}$, 则有 $\underline{i} = \underline{j}$,

因此为一个序关系, 且满足

(iv) 对任意 $\underline{i}$ 和 $\underline{j}$, 我们总有且仅有 $\underline{i} \prec \underline{j}$, $\underline{i} = \underline{j}$ 以及 $\underline{j} \prec \underline{i}$ 中的一个成立.

注 18.1.1.

当 $n = 1$ 时, $\mathbb{N}^n = \mathbb{N}$. 其上的字典序和 $\mathbb{N}$ 上的序关系相同.

这个序关系将帮助我们将多元多项式中的像排序, 并在之后的一些讨论中为我们提供便利. 需要注意的是, 我们在一元多项式的讨论中多次用到了以下结论.

命题 18.1.2

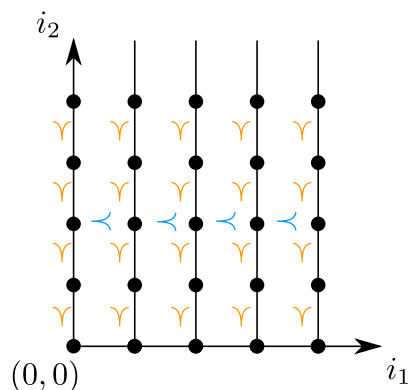
任给 $i \in \mathbb{N}$, 我们有:

$$\#\{j \in \mathbb{N} \mid j \leq i\} < \infty.$$

当 $n > 1$, $\mathbb{N}^n$ 不再具有以上性质.

例 18.1.3.

取 $n = 2$, 任取 $j \in \mathbb{N}$, 我们有 $(1, j) \preceq (2, 0)$.



不过我们有另外两个关于 $\mathbb{N}^n$ 的字典序关系的结论. 第一个结论如下.

命题 18.1.4

任取 $d \in \mathbb{N}$, 我们有

$$\#\{\underline{i} \in \mathbb{N}^n \mid i_1 \leq d, \dots, i_n \leq d\} < \infty.$$

要介绍另一个结论, 我们需要介绍以下记号:

$$\mathbb{N}_{\geq}^n := \{\underline{i} \in \mathbb{N}^n \mid i_1 \geq \dots \geq i_n\}.$$

第二个结论如下:

命题 18.1.5

任给 $\underline{i} \in \mathbb{N}_{\geq}^n$, 我们有:

$$\#\{\underline{j} \in \mathbb{N}_{\geq}^n \mid \underline{j} \preceq \underline{i}\} < \infty.$$

这两个结论将在我们之后的讨论中发挥作用.

18.2 基本概念

记 R 为一个环. 记 n 为一个正整数. 我们记 $R^{\mathbb{N}^n}$ 为从 $\mathbb{N}^n$ 到 R 的映射的集合.

定义 18.2.1 (教材定义 2.8.4)

我们称映射

$$f : \mathbb{N}^n \rightarrow R,$$

为一个 R 上的 n -元多项式, 若只有 $\mathbb{N}^n$ 中有限多个元素在 f 下的像不为 0, 即

$$\#\{\underline{i} \in \mathbb{N}^n \mid f(\underline{i}) \neq 0\} < \infty.$$

我们记 S 为 R 上所有 n -元多项式的集合.

我们如下定义 R 上 n -元多项式之间的加法和乘法. 任取多项式 $f, g \in S$, 我们定义

$$\begin{aligned} f + g : \mathbb{N}^n &\rightarrow R, \\ \underline{i} &\mapsto f(\underline{i}) + g(\underline{i}), \end{aligned}$$

$$\begin{aligned} fg : \mathbb{N}^n &\rightarrow R, \\ \underline{i} &\mapsto \sum_{\underline{j} + \underline{j}' = \underline{i}} f(\underline{j})g(\underline{j}'). \end{aligned}$$

命题 18.2.2

三元组 $(S, +, \cdot)$ 是一个环.

证明. (练习)

□

定义 18.2.3

以上构造的环 S 被称为 R 上的 n -元多项式环.

定义 18.2.4

设 $f \in S$. 我们称 f 为一个单项式, 若存在 $\underline{i} \in \mathbb{N}^n$, 满足

$$f(\underline{j}) \begin{cases} \neq 0, & \underline{j} = \underline{i} \\ = 0, & \underline{j} \neq \underline{i} \end{cases}$$

定义 18.2.5 (P.102)

设 $f \in S \setminus \{0\}$. 多项式 f 的**次数**为:

$$\deg f := \max\{i_1 + \cdots + i_n \mid \underline{i} \in \mathbb{N}^n, f(\underline{i}) \neq 0\}.$$

我们仍约定 $0 \in S$ 的次数为 $-\infty$. 我们称 $f(\underline{i})$ 为该**项的系数**.

定义 18.2.6

我们称 f 为一个**齐次多项式**, 若 f 是一些次数相同的单项式的和.

设 R 为一个幺环. 我们考虑 $\mathbb{N}^n$ 中如下元素

$$\begin{aligned} \underline{j}^{(1)} &= (1, 0, 0, \dots, 0, 0), \\ \underline{j}^{(2)} &= (0, 1, 0, \dots, 0, 0), \\ &\dots \\ \underline{j}^{(n)} &= (0, 0, 0, \dots, 0, 1). \end{aligned}$$

对任意 $1 \leq k \leq n$, 我们记 $x_k \in S$, 满足

$$x_k(\underline{i}) = \begin{cases} 1, & \underline{i} = \underline{j}^{(k)} \\ 0, & \underline{i} \neq \underline{j}^{(k)} \end{cases}$$

命题 18.2.7

任取 $i, j \in \{1, \dots, n\}$, $a \in R$, 我们有

$$ax_i = x_i a \text{ 和 } x_i x_j = x_j x_i.$$

换句话说, 任取 $i \in \{1, \dots, n\}$, x_i 与 S 中的所有元素交换(也即在 S 的中心 $Z(S)$ 里).

证明. (练习)

□

由此, 任给 $f \in S$, 我们可以将其唯一的记为

$$f = \sum_{\underline{i} \in \mathbb{N}^n} f(\underline{i}) x_1^{i_1} \cdots x_n^{i_n}.$$

通常我们将记 $a_{\underline{i}} = f(\underline{i})$. 我们使用记号 $R[x_1, \dots, x_n]$ 来记 R 上的 n 元多项式环.

18.3 交换幺环上的多元多项式

在本节中, 我们设 R 为一个交换幺环.

我们前边介绍过 R 上的一元多项式环. 假设 R 是一个交换幺环, 则 $R[x_1]$ 为一个交换幺环, 然后考虑其上的多项式环 $R[x_1][x_2]$ 也是交换幺环.

命题 18.3.1

记 R 为一个交换幺环. 存在环同构

$$\phi : R[x_1, x_2] \rightarrow R[x_1][x_2],$$

满足 $\phi|_R = id_R$, $\phi(x_1) = x_1$ 以及 $\phi(x_2) = x_2$.

证明. (练习)

□

考虑一个交换幺环 R , 我们之前证明过若 R 没有零因子, 则 $R[x_1]$ 没有零因子, 因此 $R[x_1][x_2]$ 也没有零因子.

推论 18.3.2 (教材思考题 2.8.16)

若 R 为整环, 则任取 $n \in \mathbb{N}^*$, 环 $R[x_1, \dots, x_n]$ 是整环.

证明. (练习)

□

注 18.3.3.

将 R 上的二元多项式环 $R[x_1, x_2]$ 看作是 R 的一元多项式环 $R[x_1]$ 的一元多项式环是我们常用的一种思想. 若我们有类似于

- R 有性质 P , 则 $R[x]$ 有性质 P .

的命题时, 由这个思想, 我们就可以使用归纳法证明对任意 $n \in \mathbb{N}^*$, 环 $R[x_1, \dots, x_n]$ 有性质 P .

设 R 为一个幺环, 我们有以下表格:

R	$R[x_1]$	$R[x_1][x_2] \cong R[x_1, x_2]$	$\cdots$	$R[x_1, \dots, x_n] \cong R[x_1, \dots, x_{n-1}][x_n]$
交换	交换	交换	$\cdots$	交换
无零因子	无零因子	无零因子	$\cdots$	无零因子
整环	整环	整环	$\cdots$	整环
UFD	UFD	UFD	$\cdots$	UFD
诺特环	诺特环	诺特环	$\cdots$	诺特环
域	PID	UFD	$\cdots$	UFD

环的扩张

设 R_1 为一个包含 R 的交换幺环, 且 R_1 和 R 有相同的幺元.

类似于一元多项式的情形, 我们也可以考虑 R 上多元多项式诱导的 R_1 上的映射. 任给 R 上的 n -元多项式

$$f = \sum_{\underline{i} \in \mathbb{N}^n} a_{\underline{i}} x_1^{i_1} \cdots x_n^{i_n},$$

我们定义:

$$\begin{aligned} \psi_f : R_1^n &\rightarrow R_1, \\ (b_1, \dots, b_n) &\mapsto \sum_{\underline{i} \in \mathbb{N}^n} a_{\underline{i}} b_1^{i_1} \cdots b_n^{i_n}. \end{aligned}$$

由此, 我们构造了

$$\begin{aligned}\Psi_{R_1} : R[x_1, \dots, x_n] &\rightarrow \mathcal{F}(R_1^n; R_1), \\ f &\mapsto \psi_f.\end{aligned}$$

环 R_1 上的加法和乘法诱导了 $\mathcal{F}(R_1^n; R_1)$ 上的加法和乘法. 在这两个运算下, $\mathcal{F}(R_1^n; R_1)$ 是一个交换幺环.

另一方面, 任给一个 R_1 中的 n -元组 $\underline{b} = (b_1, \dots, b_n)$, 我们可以考虑赋值映射:

$$\begin{aligned}\Phi_{\underline{b}} : \mathcal{F}(R_1^n; R_1) &\rightarrow R_1 \\ \psi &\mapsto \psi(\underline{b}).\end{aligned}$$

命题 18.3.4

映射 Ψ_{R_1} 和 $\Phi_{\underline{b}}$ 都是环同态.

证明. (练习)

□

推论 18.3.5

映射

$$\phi_{\underline{b}} := \Phi_{\underline{b}} \circ \Psi_{R_1},$$

是一个环同态.

证明. (练习)

□

我们记

$$R[b_1, \dots, b_n] = \text{Im } \phi_{\underline{b}}.$$

命题 18.3.6

- (i) 环 $R[b_1, \dots, b_n]$ 是 R_1 中包含 $R \cup \{b_1, \dots, b_n\}$ 最小的子环, 也即 R_1 中由 $R \cup \{b_1, \dots, b_n\}$ 生成的子环.
- (ii) $R[b_1, \dots, b_n] = R[b_1, \dots, b_{n-1}][b_n] = \cdots = R[b_1][b_2] \cdots [b_n]$.

证明. (练习)

□

定义 18.3.7 (教材定义 2.8.17)

我们称 R_1 上的 n 个元素 $b_1, \dots, b_n$ 在 R 上代数相关, 若存在 $f \in R[x_1, \dots, x_n]^*$, 满足

$$\phi_{\underline{b}}(f) = f(b_1, \dots, b_n) = 0.$$

若不存在这样的多项式 f , 我们称 $b_1, \dots, b_n$ 在 R 上代数无关.

注 18.3.8.

以上概念是对代数元, 超越元的推广.

命题 18.3.9

- (i) $b_1, \dots, b_n$ 是 R 上代数相关的, 当且仅当 $\ker \phi_{\underline{b}} \neq 0$.
(ii) $b_1, \dots, b_n$ 是 R 上代数无关的, 当且仅当 $\ker \phi_{\underline{b}} = 0$.

推论 18.3.10

$b_1, \dots, b_n$ 是 R 上代数无关的当且仅当 $R[b_1, \dots, b_n]$ 与 $R[x_1, \dots, x_n]$ 同构.

设 R_1 是一个交换幺环. 环 R 是 R_1 一个包含幺元的子环. 任取 R_1 中 n 个元素 $b_1, \dots, b_n$, 我们记

$$\begin{aligned} T_1 &= R[b_1] \\ T_2 &= T_1[b_2] \\ &\dots \\ T_n &= T_{n-1}[b_n] \end{aligned}$$

由之前一元多项式的内容我们知道, $T_1, \dots, T_n$ 均为 R_1 中的子环. 我们设 $T_0 = R$.

命题 18.3.11

元素 $b_1, \dots, b_n$ 代数无关当且仅当对任意 $0 < i \leq n$, 我们由元素 b_i 是 T_{i-1} 上的超越元.

证明. (练习)

□

类似于一元多项式的情形

定义 18.3.12 (教材定义 2.8.18)

任取 $n \in \mathbb{N} \setminus \{0, 1\}$, 我们称一个包含环 R 的交换幺环 R_1 为 R 上的 n -元多项式环, 若存在 R_1 中的 n 个元素 $b_1, \dots, b_n$, 满足

- (i) $R_1 = R[b_1, \dots, b_n]$,
(ii) $b_1, \dots, b_n$ 在 R 上代数无关.

此时, 我们称 $\{b_1, \dots, b_n\}$ 为 R_1 关于 R 的一个生成元集.

引理 18.3.13 (教材引理 2.8.19)

设 R_2 为包含 R 为子环的交换幺环. 取 R_2 中元素 $b_1, \dots, b_n$. 记

$$R_1 = R[b_1, \dots, b_{n-1}],$$

则 R_2 为 R 上生成元集为 $\{b_1, \dots, b_n\}$ 的多项式环当且仅当

- (i) R_1 是 R 上生成元集为 $\{b_1, \dots, b_{n-1}\}$ 的多项式环,
(ii) R_2 为 R_1 上的生成元为 b_n 一元多项式环.

证明. (练习)

□

定理 18.3.14 (教材定理 2.8.20)

设交换幺环 S 包含 R 为包含幺元的子环. 设 $b_1, \dots, b_n \in S$. 以下两个条件等价:

- (i) $R[b_1, \dots, b_n]$ 是一个 R 上的多项式环, 也即 $b_1, \dots, b_n$ 在 R 上的代数无关;
- (ii) 任给交换幺环 S_1 , 同态 $\eta: R \rightarrow S_1$, 以及元素 $c_1, \dots, c_n \in S_1$, 存在 η 的一个扩充

$$\eta_1: R[b_1, \dots, b_n] \rightarrow S_1,$$

满足 $\eta_1|_R = \eta$, 且对任意 $1 \leq i \leq n$, 有 $\eta_1(b_i) = c_i$.

若扩充 η_1 存在, 则其唯一.

证明. (练习)

□

使用以上定理中的记号, 我们有以下结论.

推论 18.3.15

若 η 为一个单同态, 且 $c_1, \dots, c_n$ 是 $\eta(R)$ 上的代数无关的, 则同态

$$\eta_1: R[b_1, \dots, b_n] \rightarrow \eta(R)[c_1, \dots, c_n],$$

为一个环同构.

证明. (练习)

□

推论 18.3.16 (教材推论 2.8.21)

设 R_1 和 R_2 是 R 上的 n -元多项式环. 设 $\{b_1, \dots, b_n\}$ 和 $\{c_1, \dots, c_n\}$ 分别是 R_1 和 R_2 在 R 上的生成元集. 那么存在唯一的从 R_1 到 R_2 的 R -同构, 满足 $T(b_i) = c_i$.

证明. (练习)

□

推论 18.3.17 (教材推论 2.8.22)

设 R_1 为 R 上的 n -元多项式. 设 $\{b_1, \dots, b_n\}$ 为 R_1 在 R 上的生成元集. 对于任意 $\sigma \in S_n$, 我们有唯一的从 R_1 到自己的 R -同构, 满足 $T(b_i) = b_{\sigma(i)}$.

证明. (练习)

□

注 18.3.18.

回顾: R 上的多项式环之间的 R -同构是指在当同构限制在 R 上时是恒等映射 id_R .

18.4 对称多项式

我们考虑交换幺环 R 上的多元多项式环 $R[x_1, \dots, x_n]$. 我们记 S_n 为 n -元置换群. 群 S_n 通过对 n 个自变量 $x_1, \dots, x_n$ 做置换, 在 $R[x_1, \dots, x_n]$ 上有如下定义的作用:

$$\sigma : R[x_1, \dots, x_n] \rightarrow R[x_1, \dots, x_n],$$

$$\sum_{\underline{i}} a_{\underline{i}} x_1^{i_1} \cdots x_n^{i_n} \mapsto \sum_{\underline{i}} a_{\underline{i}} x_{\sigma(1)}^{i_1} \cdots x_{\sigma(n)}^{i_n}.$$

由推论 18.3.17, σ 是一个环同构. 由此我们有了一个群同态

$$S_n \rightarrow \text{Aut}(R[x_1, \dots, x_n]).$$

这里 $\text{Aut}(R[x_1, \dots, x_n])$ 是 $R[x_1, \dots, x_n]$ 上的自同构群(群作用是复合).

定义 18.4.1 (教材定义 2.10.1)

一个多项式 $f \in R[x_1, \dots, x_n]$ 被称作是**对称多项式**, 若其为 S_n 在 $R[x_1, \dots, x_n]$ 的不动点, 也即

$$\forall \sigma \in S_n, \sigma.f = f.$$

例 18.4.2 (初等对称多项式, 教材例 2.10.2).

$$p_1 = x_1 + \cdots + x_n = \sum_i x_i$$

$$p_2 = x_1 x_2 + \cdots + x_{n-1} x_n = \sum_{i < j} x_i x_j$$

$$p_3 = x_1 x_2 x_3 + \cdots + x_{n-2} x_{n-1} x_n = \sum_{i < j < k} x_i x_j x_k$$

$$\dots$$

$$p_n = x_1 \cdots x_n$$

我们考虑所有对称多项式的集合

$$S[x_1, \dots, x_n] := \{f \in R[x_1, \dots, x_n] \mid f \text{ 为对称多项式}\}.$$

使用之前的记号 9.2.12, 我们有

$$S[x_1, \dots, x_n] = \text{Fix}(S_n).$$

任取 $\sigma \in S_n$, 我们记 σ 固定的多项式的集合为

$$\text{Fix}(\sigma) := \{f \in R[x_1, \dots, x_n] \mid \sigma.f = f\}.$$

由对称多项式的定义, 我们有如下命题.

命题 18.4.3

$$S[x_1, \dots, x_n] = \bigcap_{\sigma \in S_n} \text{Fix}(\sigma).$$

命题 18.4.4

任取 $\sigma \in S_n$, 我们有 $\text{Fix}(\sigma)$ 为 R 的一个子环.

证明. 由于 S_n 在 $R[x_1, \dots, x_n]$ 通过自同构作用, 因此任取 $f, g \in R[x_1, \dots, x_n]$, 都有

$$\sigma.(f - g) = \sigma.f - \sigma.g, \quad \sigma.(fg) = (\sigma.f)(\sigma.g).$$

因此任取 $f, g \in \text{Fix}(\sigma)$, 我们有

$$\begin{aligned} \sigma.(f - g) &= \sigma.f - \sigma.g = f - g \\ \sigma.(fg) &= (\sigma.f)(\sigma.g) = fg \end{aligned}$$

□

利用子环对交运算的封闭性, 我们有

推论 18.4.5

对称多项式集合 $S[x_1, \dots, x_n]$ 为 $R[x_1, \dots, x_n]$ 的一个子环.

我们将用本章的最后一部分来证明的如下定理:

定理 18.4.6 (对称多项式基本定理, 教材定理 2.10.3)

设 R 为一个交换幺环, 则 R 上的初等多项式 $p_1, \dots, p_n$ 在 R 上代数无关, 且

$$S[x_1, \dots, x_n] = R[p_1, \dots, p_n],$$

也即 R 上的对称多项式都可以写为初等对称多项式的多项式.

推论 18.4.7

初等多项式的集合 $\{p_1, \dots, p_n\}$ 构成 $S[x_1, \dots, x_n]$ 在 R 上的生成元集.

我们现在考虑 $R[x_1, \dots, x_n]$ 中的单项式. 我们记

$$\mathcal{M} := \{f \in R[x_1, \dots, x_n] \mid f \neq 0, \text{ 且 } f \text{ 为一个单项式}\}.$$

集合 $\mathbb{N}^n$ 上的字典序 $\preceq$ 诱导了 $\mathcal{M}$ 上的一个偏序:

- $ax_1^{i_1} \cdots x_n^{i_n} \prec bx_1^{j_1} \cdots x_n^{j_n}$ 若 $(i_1, \dots, i_n) \prec (j_1, \dots, j_n)$.

注 18.4.8.

我们将使用这个偏序来证明定理18.4.6. 大概的思路与之前研究一元多项式的带余除法时类似, 考虑将所有项按照一定顺序排列, 然后通过减去一些初等对称多项式的多项式来使它们消掉. 不同的在于, 由于我们考虑的是多元多项式, 因此可能有不同的单项式的次数相同, 我们无法直接使用次数来排序. 我们需要使用以上定义的偏序.

这里我们称之为偏序主要是我们无法比较两个只有系数不同的多单项式 (例如: ax_1 和 bx_1).

我们考虑 S_n 在集合 $\mathcal{M}$ 上的作用. 我们注意到任意两个 S_n -轨道是不相交的, 因此, 我们可以在 $\mathcal{M}$ 定义一个等价类关系:

- 两个 $\mathcal{M}$ 中的单项式等价当且仅当它们之间差一个 $\sigma \in S_n$ 作用.

任给非零单项式 $a_{\underline{i}} x_1^{i_1} \cdots x_n^{i_n}$, 我们记其等价类为

$$[ax_1^{i_1} \cdots x_n^{i_n}] := \{ax_{\sigma(1)}^{i_1} \cdots x_{\sigma(n)}^{i_n} = ax_1^{i_{\sigma^{-1}(1)}} \cdots x_n^{i_{\sigma^{-1}(n)}} \mid \sigma \in S_n\}.$$

我们注意到任给 $(i_1, \dots, i_n) \in \mathbb{N}^n$, 我们总是可以找到一个 $\eta \in S_n$, 满足

$$i_{\eta(1)} \geq i_{\eta(2)} \geq \cdots \geq i_{\eta(n)}.$$

更进一步的, 我们有 $(i_{\eta(1)}, \dots, i_{\eta(n)}) \in \mathbb{N}^n$ 是唯一的, 且满足任取 $\eta' \in S_n$, 我们有

- 或者 $(i_{\eta(1)}, \dots, i_{\eta(n)}) = (i_{\eta'(1)}, \dots, i_{\eta'(n)})$,
- 或者 $(i_{\eta(1)}, \dots, i_{\eta(n)}) \succ (i_{\eta'(1)}, \dots, i_{\eta'(n)})$.

换句话说, 任给 n 个自然数, 我们总是有唯一的办法将其从大到小排列. 注意 η 不一定是唯一的.

在一个等价类 $[ax_1^{i_1} \cdots x_n^{i_n}]$ 里, 存在为一个的一个单项式

$$ax_1^{i_{\eta(1)}} \cdots x_n^{i_{\eta(n)}},$$

满足

- (i) $i_{\eta(1)} \geq i_{\eta(2)} \geq \cdots \geq i_{\eta(n)}$,
- (ii) 在字典序关系下是极大的, 也即任取 $\sigma \in S_n$, 我们有

- 或者 $ax_1^{i_{\eta(1)}} \cdots x_n^{i_{\eta(n)}} = ax_1^{i_{\sigma(1)}} \cdots x_n^{i_{\sigma(n)}}$,
- 或者 $ax_1^{i_{\eta(1)}} \cdots x_n^{i_{\eta(n)}} \succ ax_1^{i_{\sigma(1)}} \cdots x_n^{i_{\sigma(n)}}$.

我们考虑集合

$$\mathbb{N}_{\geq}^n := \{(i_1, \dots, i_n) \in \mathbb{N}^n \mid i_1 \geq \cdots \geq i_n\}.$$

任给 $a \in R^*$ 和 $\underline{i} = (i_1, \dots, i_n) \in \mathbb{N}_{\geq}^n$, 我们有唯一的 $\mathcal{M}$ 中的等价类

$$[ax_1^{i_1} \cdots x_n^{i_n}].$$

我们考虑映射:

$$\begin{aligned} \Phi : R \times \mathbb{N}_{\geq}^n &\rightarrow \mathcal{M} / \sim \\ (a, i_1, \dots, i_n) &\mapsto [ax_1^{i_1} \cdots x_n^{i_n}] \end{aligned}$$

命题 18.4.9

映射 Φ 为双射.

任给 $\underline{i} \in \mathbb{N}_{\geq}^n$, 我们记其 S_n 轨道为 $S_n(\underline{i}) \subset \mathbb{N}^n$, 我们定义

$$f_{\underline{i}} := \sum_{\underline{j} \in S_n(\underline{i})} x_1^{j_1} \cdots x_n^{j_n}.$$

由其定义, 我们知道 $f_{\underline{i}}$ 是一个对称多项式.

例 18.4.10.

我们记 $e_k = (\underbrace{1, \dots, 1}_k, 0, \dots, 0) \in \mathbb{N}_n^{\geq}$. 考虑初等对称多项式, 则有

$$\begin{aligned} p_1 &= f_{e_1} \\ p_2 &= f_{e_2} \\ &\dots \\ p_n &= f_{e_n} \end{aligned}$$

以下引理将有助于我们理解一个对称多项式的结构, 特别地, 它将帮助我们证明定理18.4.6.

引理 18.4.11

任给一个对称多项式 $f \in R[x_1, \dots, x_n]$, 存在 $\mathbb{N}_n^{\geq}$ 中的 m 个元素 $i_1 \succ \dots \succ i_m$, 满足

$$f = a_1 f_{i_1} + \dots + a_m f_{i_m},$$

这里, $a_1, \dots, a_m \in R^*$.

证明. 由对称多项式的定义, 我们有对于任意 $\sigma \in S_n$,

$$\sigma.f = f.$$

因此多项式 $\sigma.f$ 和 f 有相同的项, 且对应项的系数相同. 特别的, 如果我们考虑 f 中的一项 $a_i x_1^{i_1} \dots x_n^{i_n}$, 则其像 $a_{\sigma(i)} x_{\sigma(1)}^{i_1} \dots x_{\sigma(n)}^{i_n}$ 必然在 $\sigma.f$ 中也即 f 中. 我们注意到 σ 并不改变系数, 因此 $a_i = a_{\sigma(i)}$.

不失一般性的, 我们可以假设 $i \in \mathbb{N}_n^{\geq}$. 以上讨论中的记号, 我们记

$$f_i = \sum_{j \in S_n(i)} x_1^{j_1} \dots x_n^{j_n}.$$

我们假设 f 中字典序最大的一项为 $a_i x_1^{i_1} \dots x_n^{i_n}$. 由 f 对称我们知道 $i \in \mathbb{N}_n^{\geq}$.

我们记 $i_1 = i$. 我们考虑 $g_1 = f - a_{i_1} f_{i_1}$. 由于 f 和 $a_{i_1} f_{i_1}$ 都是对称多项式, 我们有 g_1 也为对称多项式.

重复以上步骤, 我们找到 $a_{i_2} f_{i_2}$. 定义 $g_2 = g_1 - a_{i_2} f_{i_2}$. 类似的我们可以证明 g_2 也是对称多项式.

由此, 我们可以定义一系列的对称多项式 $g_3, g_4, \dots$. 我们记 $g_0 = f$.

我们注意到 g_{j+1} 的最大项按字典序严格小于 g_j 的最大项. 由命题 18.1.5, 我们只有有限多个 $j \in \mathbb{N}_n^{\geq}$, 满足 $i \succ j$. 因此, 以上归纳过程将在有限步停止. 引理得证. $\square$

下面我们开始证明定理18.4.6.

定理18.4.6的证明. 设 f 为一个对称多项式. 由引理可知, 我们可以将 f 写成

$$f = a_{i_1} f_{i_1} + \dots + a_{i_m} f_{i_m},$$

我们记 $i_1 = (i_{11}, \dots, i_{1n}) \in \mathbb{N}_n^{\geq}$, 也即 $i_{11} \geq \dots \geq i_{1n}$. 作为一个 n 元向量, 我们可以将 i_1 表示为 e_k 的线性组合:

$$i_1 = (i_{11} - i_{12})e_1 + (i_{12} - i_{13})e_2 + \dots + (i_{1(n-1)} - i_n)e_{n-1} + i_n e_n$$

我们记

$$h_1 = a_{\underline{i}_1} p_1^{i_{11}-i_{12}} p_2^{i_{12}-i_{13}} \cdots p_{n-1}^{i_{1(n-1)}-i_n} p_n^{i_n} \in R[p_1, \dots, p_n].$$

其最大项为 $a_{\underline{i}_1} x_1^{i_{11}} \cdots x_n^{i_{1n}}$. 因此由引理, 我们可以将 h_1 写为

$$h_1 = a_{\underline{i}_1} f_{\underline{i}_1} + b_{\underline{j}_2} f_{\underline{j}_2} + b_{\underline{j}_3} f_{\underline{j}_3} + \cdots + b_{\underline{j}_n} f_{\underline{j}_n}.$$

我们记 $g_1 = f - h_1$. 由以上讨论, 我们知道若将 g_1 写为按照引理写开, 最大项小于 $a_{\underline{i}_1} f_{\underline{i}_1}$ 也即 f 的最大项.

我们注意到 g_1 也是对称多项式. 我们重复以上过程可以找到 $h_2 \in R[p_1, \dots, p_n]$, 并定义 $g_2 = g_1 - h_2$, 且 g_2 的最大项严格小于 g_1 的最大项. 继续下去, 我们可以依次构造 $g_3, g_4, \dots$

注意到 g_{k+1} 的最大项总是小于 g_k , 另一方面, 由命题 18.1.5, 对于任意 $\underline{i} \in \mathbb{N}_n^\geq$, 我们只有有限多个 $\underline{j} \in \mathbb{N}_n^\geq$, 满足 $\underline{i} \succ \underline{j}$. 因此以上构造 g_k 的过程在有限步会停止. 也即存在一个 l 满足

$$\begin{aligned} f &= h_1 + g_1 \\ g_1 &= h_2 + g_2 \\ &\vdots \\ g_{l-2} &= h_{l-1} + g_{l-1} \\ g_{l-1} &= h_l. \end{aligned}$$

由此 $f = h_1 + \cdots + h_l \in R[p_1, \dots, p_n]$.

我们下边证明 $p_1, \dots, p_n$ 代数无关. 我们考虑任意 $f \in R[x_1, \dots, x_n]$. 若 $f(p_1, \dots, p_n) = 0$, 我们考虑 $f(x_1, \dots, x_n)$ 中字典序下最大的单项式, 记为

$$a_{\underline{i}} x_1^{i_1} \cdots x_n^{i_n}.$$

因此 $f(p_1, \dots, p_n)$ 在字典序下最大项的次数为

$$a_{\underline{i}} x_1^{i_1+\cdots+i_n} x_2^{i_2+\cdots+i_n} \cdots x_n^{i_n}.$$

由于 $f(p_1, \dots, p_n)$ 为对称多项式, 其他最高次项在字典序下都严格小于上述项. 因此 $a_{\underline{i}} = 0$, 矛盾. 因此 $p_1, \dots, p_n$ 在 R 上代数无关. $\square$

例 18.4.12.

我们考虑 $\mathbb{Z}[x_1, x_2, x_3]$ 整数上的三元多项式环. 任取非零多项式 $f \in \mathbb{Z}[x_1, x_2, x_3]$, 我们记

$$f(x_1, x_2, x_3) = \sum_{\underline{i} \in \mathbb{N}^3} a_{\underline{i}} x_1^{i_1} x_2^{i_2} x_3^{i_3},$$

并定义

$$\underline{i}_{\max}(f) := \{\underline{j} \in \mathbb{N}^3 \mid a_{\underline{j}} \neq 0\}$$

环 $\mathbb{Z}[x_1, x_2, x_3]$ 中得初等对称多项式为

$$\begin{aligned} p_1 &= x_1 + x_2 + x_3, \\ p_2 &= x_1 x_2 + x_1 x_3 + x_2 x_3, \\ p_3 &= x_1 x_2 x_3. \end{aligned}$$

取多项式

$$f(x_1, x_2, x_3) = x_1^3 x_2 + x_1^3 x_3 + x_2^3 x_3 + x_2^3 x_1 + x_3^3 x_1 + x_3^3 x_2 + 2x_1^2 x_2^2 + 2x_2^2 x_3^2 + 2x_1^2 x_3^2.$$

考虑 f 中系数非零项的次数向量, 我们有

$$D = \{(3, 1, 0), (3, 0, 1), (0, 3, 1), (1, 3, 0), (1, 0, 3), (0, 1, 3), (2, 2, 0), (2, 0, 2), (0, 2, 2)\}.$$

注意到其中有两个 S_3 轨道:

$$D = S_3 \cdot (3, 1, 0) \cup S_3 \cdot (2, 2, 0).$$

这两个轨道中, 我们寻找属于 $\mathbb{N}_{\geq}^3$ 的向量, 分别为 $(3, 1, 0)$ 以及 $(2, 2, 0)$. 按照字典序我们有

$$(3, 1, 0) \succ (2, 2, 0).$$

因此

$$i_{\max}(f) = (3, 1, 0).$$

注意到 f 中 $(3, 1, 0)$ -项对应的系数为 1, 我们考虑

$$g_1(x_1, x_2, x_3) = p_1^{d_1} p_2^{d_2} p_3^{d_3},$$

满足

$$i_{\max}(g) = (3, 1, 0).$$

因此有 d_1, d_2 和 d_3 的线性方程组

$$\begin{cases} d_1 + d_2 + d_3 = 3 \\ d_2 + d_3 = 1 \\ d_3 = 0 \end{cases}$$

因此 $(d_1, d_2, d_3) = (2, 1, 0)$, 即

$$\begin{aligned} g_1(x_1, x_2, x_3) &= p_1^2 p_2 \\ &= (x_1 + x_2 + x_3)^2 (x_1 x_2 + x_1 x - 3 + x_2 x_3) \\ &= (x_1^2 + x_2^2 + x_3^2 + 2x_1 x_2 + 2x_1 x_3 + 2x_2 x_3)(x_1 x_2 + x_1 x_3 + x_2 x_3) \\ &= \sum_{1 \leq i \neq j \leq 3} x_i^3 x_j + 2(x_1^2 x_2^2 + x_1^2 x_3^2 + x_2^2 x_3^2) + 5(x_1^2 x_2 x_3 + x_2^2 x_1 x_3 + x_3^2 x_1 x_2) \end{aligned}$$

我们考虑

$$\begin{aligned} f_1(x_1, x_2, x_3) &= f(x_1, x_2, x_3) - g_1(x_1, x_2, x_3) \\ &= 5(x_1^2 x_2 x_3 + x_2^2 x_1 x_3 + x_3^2 x_1 x_2). \end{aligned}$$

考虑 f_1 的各单项式的次数向量, 只有一个 S_3 轨道, 其中字典序下最大的次数向量为

$$i_{\max}(f_1) = (2, 1, 1).$$

注意到该项系数为 5

记

$$g_2(x_1, x_2, x_3) = 5p_1^{d_1} p_2^{d_2} p_3^{d_3}.$$

考虑 d_1, d_2 和 d_3 的线性方程组

$$\begin{cases} d_1 + d_2 + d_3 = 2 \\ d_2 + d_3 = 1 \\ d_3 = 1 \end{cases}$$

解得 $(d_1, d_2, d_3) = (1, 0, 1)$. 因此

$$\begin{aligned} g_2(x_1, x_2, x_3) &= 5p_1 p_3 \\ &= 5(x_1 + x_2 + x_3)x_1 x_2 x_3 \\ &= 5(x_1^2 x_2 x_3 + x_2^2 x_1 x_3 + x_3^2 x_1 x_2) \end{aligned}$$

因此 $g_2 = f_1$. 我们有

$$f - g_1 - g_2 = 0,$$

即

$$f = g_1 + g_2 = p_1^2 p_2 + 5p_1 p_3 \in \mathbb{Z}[p_1, p_2, p_3].$$

18.5 Hilbert 零点定理

代数与几何的关系可以回溯到代数思想出现的初期. 作为这种关系一个体现, Hilbert 零点定理构建了仿射空间中代数集与多元多项式的根理想之间的关系, 是代数几何中的一个基本定理. 由此我们可以将对一些仿射空间中的几何问题的研究转化为对多元多项式环的理想的讨论.

作为一个引子, 我们考虑以下来自线性代数的例子. 记 F 为一个域. 任取 $n \in \mathbb{N}^*$, 任取仿射空间 F^n 中的一个仿射子空间, 都存在一个以该仿射子空间为解集的方程组. 另一方面, 我们考虑 F 上的一个由 k 个 n -元线性方程构成的方程组:

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \cdots + a_{2n}x_n = b_2 \\ \cdots \\ a_{k1}x_1 + \cdots + a_{kn}x_n = b_n \end{cases} \quad (18.1)$$

若该方程组有解, 则解集为 F^n 的一个仿射子空间, 并且其维数为

$$n - \text{rank} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{pmatrix}.$$

此外, 方程组 18.1 有解当且仅当

$$\text{rank} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{pmatrix} = \text{rank} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} & b_n \end{pmatrix}.$$

我们尝试从 F 上的多元多项式环的角度对以上结论进行解读. 考虑域 F 上的 n -元多项式环 $F[x_1, \dots, x_n]$. 任给其中的一个 n -元多项式 f , 我们都可以给出以下赋值映射:

$$\begin{aligned} F^n &\rightarrow F, \\ (u_1, \dots, u_n) &\mapsto f(u_1, \dots, u_n). \end{aligned}$$

记多项式

$$\begin{aligned} f_1(x_1, \dots, x_n) &= a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n - b_1, \\ f_2(x_1, \dots, x_n) &= a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n - b_2, \\ &\cdots \\ f_k(x_1, \dots, x_n) &= a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n - b_k, \end{aligned}$$

则方程组 18.1 可以被重写为

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ f_2(x_1, \dots, x_n) = 0 \\ \cdots \\ f_k(x_1, \dots, x_n) = 0 \end{cases} \quad (18.2)$$

另记 $f_1, \dots, f_k$ 生成的理想为 $I = (f_1, \dots, f_k)$.

若方程组 18.2 的解集非空, 我们将其记为 P . 任取 $g \in I$, 由于 g 为 $f_1, \dots, f_k$ 的 $F[x_1, \dots, x_n]$ -线性组合, 因此任取 $(u_1, \dots, u_n) \in P$, 我们都有 $g(u_1, \dots, u_n) = 0$.

反过来, 任取 $g \in F[x_1, \dots, x_n]$, 满足 $g(P) = \{0\}$, 我们希望了解 g 和 I 的关系. 为此我们对方程组 18.2 使用 Gauss 消元. 不失一般性地, 我们设消元最终所得的线性方程组可以被记为

$$\begin{cases} x_1 & + a'_{l(l+1)}x_{l+1} + \cdots + a'_{1n}x_n - b'_1 = 0 \\ & x_2 & + a'_{l(l+1)}x_{l+1} + \cdots + a'_{2n}x_n - b'_2 = 0 \\ & & \cdots \\ & & x_l & + a'_{l(l+1)}x_{l+1} + \cdots + a'_{kn}x_n - b'_k = 0 \end{cases} \quad (18.3)$$

其中 $l \leq k$. 记方程组左边多项式为

$$\begin{aligned} \tilde{f}_1(x_1, \dots, x_n) &= x_1 & + a'_{l(l+1)}x_{l+1} + \cdots + a'_{1n}x_n - b'_1 \\ \tilde{f}_2(x_1, \dots, x_n) &= & x_2 & + a'_{l(l+1)}x_{l+1} + \cdots + a'_{2n}x_n - b'_2 \\ &\dots \\ \tilde{f}_l(x_1, \dots, x_n) &= & & x_l + a'_{l(l+1)}x_{l+1} + \cdots + a'_{kn}x_n - b'_k \end{aligned}$$

由于 Gauss 消元对方程组的改变是可逆的, 因此以上多项式 $\tilde{f}_1, \dots, \tilde{f}_l$ 生成的理想仍是 I .

考虑 $F[x_1, \dots, x_n] = F[x_{l+1}, \dots, x_n][x_l] \cdots [x_1]$, 我们可以利用 I 中的多项式把 g 中包含 $x_1, \dots, x_l$ 的项依次消掉, 从而得到一个变元 $x_{l+1}, \dots, x_n$ 的多项式

$$\tilde{g} \in F[x_{l+1}, \dots, x_n].$$

利用方程组 18.3, 我们可以得到方程组 18.2 的通解表达式. 其中变量 $x_{l+1}, \dots, x_n$ 可以被选作自由元取任意值, 也即 $\tilde{g}(F^{n-l}) = \{0\}$.

注意到我们总是可以将除了一个变元之外的其它变元赋值为 1 从而得到一个 F 上的一元多项式. 若进一步有 F 不是有限域, 则一元多项式在 F 上取值恒为 0 当且仅当该多项式是零多项式. 利用这个讨论, 我们可以进一步得到 $\tilde{g}$ 是一个零多项式, 从而有 $g \in I$.

如果方程组 18.2 无解, 则其经过 Gauss 消元之后得到的多项式组为

$$\begin{aligned} \tilde{f}_1(x_1, \dots, x_n) &= x_1 & + a'_{l(l+1)}x_{l+1} + \cdots + a'_{1n}x_n & - b'_1 \\ \tilde{f}_2(x_1, \dots, x_n) &= & x_2 & + a'_{l(l+1)}x_{l+1} + \cdots + a'_{2n}x_n & - b'_2 \\ &\dots \\ \tilde{f}_{l-1}(x_1, \dots, x_n) &= & & x_{l-1} + a'_{(l-1)l}x_l + \cdots + a'_{(l-1)n}x_n & - b'_{l-1} \\ \tilde{f}_l(x_1, \dots, x_n) &= & & & 1. \end{aligned}$$

其中 $l \leq k$. 因此 I 包含 1, 为平凡理想 R . 反过来 1 作为常数多项式给出的方程的解空间为空集, 所以 $I = R$ 时, 则解集 P 为空集.

我们总结一下从以上讨论中得到以下关于 $F[x_1, \dots, x_n]$ 的结论:

- 1) 仿射空间 F^n 中的仿射子空间与 $F[x_1, \dots, x_n]$ 中的 1 次多项式给出的线性方程组对应;
- 2) 一组 1 次多项式 $f_1, \dots, f_k$ 给出的方程组 (线性方程组) 有解当且仅当这些多项式生成的 R 的理想 I 不包含 1.
- 3) 设 F 不是有限域, 任取一组 1 次多项式 $f_1, \dots, f_k$ 给出的方程组, 设其有解并记其解空间为 P , 任取 $g \in F[x_1, \dots, x_n]$, 则 $g(P) = \{0\}$ 当且仅当 $g \in (f_1, \dots, f_k)$.

在这些结论中我们已经看到了 Hilbert 零点定理的影子.

Hilbert 零点定理考虑的是域上一般的多元多项式方程及其解集. 不过当我们考虑域上的多元多项式的时候, 一个多项式即便次数大于 0, 仍可能是无解的, 例如, 我们考虑实系数多项式方程

$$(x^2 + 1)(y^2 + 1) = 0,$$

其在 $\mathbb{R}^2$ 上的解空间为空集. 另一方面, 若我们考虑的域是代数封闭的, 则任意次数大于 0 的多元多项式方程的解集都非空. 为避免考虑解的存在性问题使讨论复杂化从而偏离我们的初衷, 本节将仅考虑代数闭域.

记 K 为一个代数闭域, n 为一个非零自然数. 我们考虑 K 上的 n 元多项式环 $K[x_1, \dots, x_n]$.

定义 18.5.1

任取一个多项式 $f \in K[x_1, \dots, x_n]$, 若仿射空间 K^n 中一个点 $(u_1, \dots, u_n)$ 满足

$$f(u_1, \dots, u_n) = 0,$$

我们称其为 f 的一个**解**. 我们记 $\text{Sol}(f)$ 为 f 所有的解构成的 K^n 的子集, 称之为多项式 f 的**解集**.

我们首先对多项式解的存在性做一个讨论.

定义 18.5.2

任取非空集合 $S \subset K[x_1, \dots, x_n]$, 我们称这些多项式在 K^n 中的解集的交集

$$V(S) := \bigcap_{f \in S} \text{Sol}(f)$$

为由 S 给出的**仿射簇**.

任取非空集合

$$S \subset K[x_1, \dots, x_n],$$

我们记其生成的 $K[x_1, \dots, x_n]$ 的理想为

$$I = (S).$$

由包含关系 $S \subset I$, 我们有 $V(I) \subset V(S)$.

另一方面, 由理想生成的定义, 任取 $f \in I$, 都有多项式 $f_1, \dots, f_k \in S$, 以及多项式 $g_1, \dots, g_k \in K[x_1, \dots, x_n]$, 满足

$$f = g_1 f_1 + \dots + g_k f_k.$$

因此任取 $(u_1, \dots, u_n) \in V(S)$, 我们都有

$$f(u_1, \dots, u_n) = 0.$$

由此可知 $V(S) \subset V(I)$. 综上所述, 我们有

$$V(I) = V(S).$$

注 18.5.3.

由于域 K 也是诺特环. 由 Hilbert 基定理可知环 $K[x_1, \dots, x_n]$ 也是诺特环. 因此在讨论 $K[x_1, \dots, x_n]$ 的理想的生成元集时, 我们总是可以不失一般性地假设该集合是有限的.

在之前关于线性方程组的讨论中, 我们看到一组 $K[x_1, \dots, x_n]$ 中的一次多项式的解集的交集为空集当且仅当这组多项式生成的理想中包含 1, 即所得理想为 $K[x_1, \dots, x_n]$. Hilbert 零点定理的弱形式告诉我们这个结论对 $K[x_1, \dots, x_n]$ 中一般的多项式也成立.

定理 18.5.4 (Hilbert 零点定理-弱形式)

记 n 为一个非零自然数. 任取代数闭域 K , 考虑其上的 n 元多项式环 $K[x_1, \dots, x_n]$. 任取其中的理想 $I \subset K[x_1, \dots, x_n]$, 则 $V(I) = \emptyset$, 当且仅当 $1 \in I$.

另一方面, 任给一个仿射簇 V , 我们可以考虑解集包含 V 的多项式构成的集合:

$$\mathcal{I}(V) := \{f \in K[x_1, \dots, x_n] \mid V \subset \text{Sol}(f)\}.$$

直接验证定义可知这是 $K[x_1, \dots, x_n]$ 的一个理想. 从其定义我们可以直接观察到 $I \subset \mathcal{I}(V)$. 同时, 我们也观察到由于域没有零因子, 任取 $a \in K$, 以及 $m \in \mathbb{N}^*$, 我们有 $a^m = 0$ 当且仅当 $a = 0$. 因此任取多项式 $f \in K[x_1, \dots, x_n]$, 我们有

$$\text{Sol}(f^m) = \text{Sol}(f).$$

因此我们进一步有 $\text{rad}I \subset \mathcal{I}(V)$. 这里 $\text{rad}I$ 为理想 I 的根理想

$$\text{rad}I := \{f \in K[x_1, \dots, x_n] \mid \exists m \in \mathbb{N}^*, f^m \in I\}.$$

那么一个自然的问题就是 $\text{rad}I$ 是 $\mathcal{I}(V)$ 的全部么? Hilbert 零点定理的强形式给了这个问题一个肯定的回答.

定理 18.5.5 (Hilbert 零点定理-强形式)

记 n 为一个非零自然数. 任取代数闭域 K , 考虑其上的 n 元多项式环 $K[x_1, \dots, x_n]$. 任取其中的理想 $I \subset K[x_1, \dots, x_n]$, 我们有

$$\mathcal{I}(V(I)) = \text{rad}I.$$

注 18.5.6.

尽管以上两个定理分别被称为 Hilbert 定理的弱形式和强形式, 但实际上二者是等价的. 对定理证明感兴趣的读者可以参考 [7].

第四部分

模理论

第十九章 模论基础

我们首先回顾一下域 F 上向量空间 V 这个概念. 我们将用 a, b, c 记域 F 中的元素, 用 $\mathbf{u}, \mathbf{v}, \mathbf{w}$ 记向量空间中的元素.

我们称 V 为 F -线性空间, 若我们有以下 V 加法运算和数乘运算:

$$\begin{aligned} + : V \times V &\rightarrow V & \cdot : F \times V &\rightarrow V \\ (\mathbf{u}, \mathbf{v}) &\mapsto \mathbf{u} + \mathbf{v} & (a, \mathbf{v}) &\mapsto a\mathbf{v} \end{aligned}$$

满足以下条件

$$(i) \quad \forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V, \quad (\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w});$$

$$(ii) \quad \exists \mathbf{0} \in V, \forall \mathbf{v} \in V, \quad \mathbf{0} + \mathbf{v} = \mathbf{v} + \mathbf{0} = \mathbf{v};$$

$$(iii) \quad \forall \mathbf{v} \in V, \exists -\mathbf{v} \in V, \quad \mathbf{v} + (-\mathbf{v}) = \mathbf{0};$$

$$(iv) \quad \forall \mathbf{u}, \mathbf{v} \in V, \quad \mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u};$$

$$(1) \quad \forall a \in F, \forall \mathbf{u}, \mathbf{v} \in V, \quad a(\mathbf{u} + \mathbf{v}) = (a\mathbf{u}) + (a\mathbf{v});$$

$$(2) \quad \forall a, b \in F, \forall \mathbf{v} \in V, \quad (a + b)\mathbf{v} = (a\mathbf{v}) + (b\mathbf{v});$$

$$(3) \quad \forall a, b \in F, \forall \mathbf{v} \in V, \quad (ab)\mathbf{v} = a(b\mathbf{v}).$$

$$(4) \quad \forall \mathbf{v} \in V, \quad 1\mathbf{v} = \mathbf{v};$$

注 19.0.1.

我们使用相同的记号来记域 F 上的和 V 上的加法(乘法)运算.

我们可以看到条件 (i), (ii), (iii), (iv) 在说 $(V, +)$ 是一个交换群. 我们考虑 V 作为加法群的自同态环 $\text{End}(V, +)$:

$$\text{End}(V, +) := \{\phi : V \rightarrow V \mid \phi \text{ 为群同态映射}\}.$$

(交换群的自同态环, 参考章节 ??).

取 $a \in F$, 我们考虑数乘运算限制在 $\{a\} \times V$ 上, 就得到一个映射:

$$\begin{aligned}\varphi_a: V &\rightarrow V \\ \mathbf{v} &\mapsto a\mathbf{v}.\end{aligned}$$

条件 (1) 说明映射 φ_a 是一个 V 到自己关于加法的群同态映射. 由此, 我们有了一个从 F 到 $\text{End}(V, +)$ 的映射:

$$\begin{aligned}\varphi: F &\rightarrow \text{End}(V, +) \\ a &\mapsto \varphi_a.\end{aligned}$$

条件 (2), (3), (4) 说明, 映射 Φ 是一个将幺元送到幺元的环同态.

例 19.0.2.

记 $n \in \mathbb{N}^*$. 考虑 n 维实向量空间 $\mathbb{R}^n$ 上所有线性映射构成的环. 我们可以将其看作是 $\mathbb{R}^n$ 作为加法群的自同态环的一个子环.

考虑纯量乘法, 我们有以下环同态:

$$\begin{aligned}\varphi: \mathbb{R} &\rightarrow \text{End}(\mathbb{R}^n, +, \cdot) \subset \text{End}(\mathbb{R}^n, +) \\ a &\mapsto \varphi_a.\end{aligned}$$

若选定 $\mathbb{R}^n$ 的一组基, 考虑线性映射的矩阵表示, 我们有:

$$\text{End}(\mathbb{R}^n, +, \cdot) \cong \text{Mat}_n(\mathbb{R}),$$

这里 $\text{Mat}_n(\mathbb{R})$ 为 n 阶方阵环. 任取任意 $a \in \mathbb{R}$, 其对应的群同态 φ_a 所对应的矩阵为纯量矩阵 aI_n , 其中 I_n 为 n 阶单位阵.

注 19.0.3.

在以上例子中, 我们考虑的是 $\mathbb{R}^n$ 作为线性空间的自同态. 如果考虑作为加法群的自同态, 这将是一个更大的集合. 例如, 我们考虑 $\mathbb{R}$ 作为线性空间的自同态环, 则同构于 $\mathbb{R}$. 而当我们考虑 $\mathbb{R}$ 作为一个加法群, 我们可以将 $\mathbb{R}$ 看作为一个 $\mathbb{Q}$ 上的线性空间, 它的维数是无穷维的, 而且是不可数的. 此时我们可以考虑 $\mathbb{R}$ 作为 $\mathbb{Q}$ 线性空间的 $\mathbb{Q}$ -线性映射. 这样的线性映射不一定是 $\mathbb{R}$ 上的连续映射.

我们注意到在这个定义中, 我们似乎并没有用到 F 是一个域的所有条件, 例如, 乘法运算交换, 任意非零元素都有乘法逆元. 由此, 我们可以考虑将 F 的条件弱化为一个幺环, 从而推广域上向量空间的概念. 这就是我们将要介绍的概念: 模. 实际上后续我们会发现, 在对线性空间的讨论中有一部分并没有用到域相较于一般幺环所具有的独特性质(交换, 元素可逆), 因此很多关于线性空间的结论对于模也成立.

另一方面, 我们也可以将交换群上的模结构给出了环在交换群上的作用. 就像我们可以通过群作用来研究群一样, 我们也可以通过以某个环作为系数的模的结构的研究来得到关于系数环的结构的结论.

19.1 模

定义及例子

设 R 为一个幺环. 我们记 M 为一个非空集合.

定义 19.1.1 (教材定义3.1.1)

我们称一个交换群 M 为一个**左 R -模**, 若我们有如下映射:

$$\begin{aligned}\Phi: R \times M &\rightarrow M \\ (a, x) &\mapsto ax,\end{aligned}$$

满足对任意 $a, b \in R$ 以及 $x, y \in M$ 都有:

- (1) $a(x + y) = (ax) + (ay)$;
- (2) $(a + b)x = (ax) + (bx)$;
- (3) $(ab)x = a(bx)$;
- (4) $1x = x$.

此时, 我们称 R 为模 M 的**系数环**, 称 Φ 为**纯量乘法映射**.

这里之所以称之为"左" R -模是因为在条件 3) 中, 我们要求

$$(ab)x = a(bx).$$

如果我们将 3) 换为条件 5)

$$5) (ab)x = b(ax),$$

我们称所得的结构为一个**右 R -模**.

定义 19.1.2

若交换群 M 既是一个左 R -模, 又是一个右 R -模, 那么我们称 M 为一个**双 R -模**.

注 19.1.3.

我们也可以从整体上考虑. 左模定义中纯量乘法所满足的条件实际上等价于存在一个 R 到 $\text{End}(M)$ 的一个将元送到元的环同态, 而右模定义中纯量乘法所满足的条件实际上等价于存在一个 R 到 $\text{End}(M)$ 的一个反同态(见定义 19.1.12).

注 19.1.4.

如果系数 R 交换, 则任意 R 上的左模也是右模.

我们来看一些例子.

例 19.1.5 (教材例3.1.2).

给定一个域 F , 我们可以将其看作一个环. 域 F 上的向量空间 V 是一个 F -模. 另一方面, 任给一个域 F , 若 M 是一个 F -模, 则 M 是一个 F 上的向量空间. 例如: $\mathbb{R}^2$ (关于 $\mathbb{R}$), $\mathbb{C}^2$ 关于 $\mathbb{C}$.

例 19.1.6.

我们考虑利用 n -阶实矩阵环 $\text{Mat}_n(\mathbb{R})$ 通过矩阵乘法给出向量空间 $\mathbb{R}^n$ 上的模结构. 我们记

$\mathbf{v} \in \mathbb{R}^n$, $A, B \in \text{Mat}_n(\mathbb{R})$. 若我们记 $\mathbf{v}$ 为一个列向量, 考虑左乘矩阵, 则有

$$(AB)(\mathbf{v}) = A(B(\mathbf{v})).$$

因此这种方式给出的是一个 $\mathbb{R}^n$ 上的左 $\text{Mat}_n(\mathbb{R})$ -模结构.

若我们记 $\mathbf{v}$ 为一个行向量, 考虑右乘矩阵则有:

$$(\mathbf{v})(AB) = ((\mathbf{v})A)B.$$

因此这种方式给出的是一个 $\mathbb{R}^n$ 上的右 $\text{Mat}_n(\mathbb{R})$ -模结构.

例 19.1.7 (教材例3.1.18).

给定一个交换群 M . 我们考虑其上的自同态环 $\text{End}(M)$. 群 M 可以看作是一个左 $\text{End}(M)$ -模. 例如: $\mathbb{Z}^2$ 的自同态环同构于矩阵群 $\text{Mat}_2(\mathbb{Z})$.

以下我们再给出一些更一般的例子.

例 19.1.8 (教材例3.1.3).

任意交换群 M 是一个 $\mathbb{Z}$ -模. 环 $\mathbb{Z}$ 在 M 上的作用如下: 对任意 $x \in M$, 任意 $n \in \mathbb{Z}$, 我们定义

$$nx = \begin{cases} \underbrace{x + \cdots + x}_n, & n > 0, \\ 0, & n = 0, \\ \underbrace{(-x) + \cdots + (-x)}_{-n}, & n < 0. \end{cases}$$

我们后边将考虑 M 为有限生成的情况, 并进一步给出有限生成交换群的分类.

例 19.1.9 (教材例3.1.4).

任给一个幺环 $(R, +, \cdot)$, 我们考虑交换群 $(R, +)$, 则利用幺环 R 中的乘法, 考虑左乘:

$$\begin{aligned} \cdot : R \times R &\rightarrow R, \\ (a, b) &\mapsto ab, \end{aligned}$$

其中 a 为环 R 中的元素, b 为群 R 中的元素, 我们可以将群 R 看作是一个左 R -模.

例 19.1.10.

任给一个幺环 R , 任给一个左(右)理想 I . 我们考虑交换群 $(I, +)$, 考虑环 R 中的乘法, 则通过将 R 中元素左(右)乘到 I 中的元素上, 群 I 可以看作是一个左(右) R -模. 例如: $\mathbb{R}[x]$ 中由 x 生成的理想 $\langle x \rangle$ 为一个 $\mathbb{R}[x]$ -模.

例 19.1.11 (教材例3.1.5).

我们考虑域 F 及其上的多项式环 $F[\lambda]$. 设 V 为一个 F 上的向量空间. 任给一个 V 上的线性变换 $\mathcal{A}$, 我们可以构造一个 $F[\lambda]$ 到 $\text{End}(V)$ 的环同态:

$$\begin{aligned} \psi_{\mathcal{A}} : F[\lambda] &\rightarrow \text{End}(V) \\ f(\lambda) &\mapsto f(\mathcal{A}). \end{aligned}$$

由此, 我们可以将 V 看作是一个 $F[\lambda]$ -模.

另一方面 $\psi_{\mathcal{A}}$ 为一个环同态, 我们记 $F[\mathcal{A}]$ 为其作用下的像. 因此 V 也可以被看作是 $F[\mathcal{A}]$ -模. 我们后边将仔细讨论这个例子, 来研究 V 上线性变换的标准型理论.

左模和右模之间的转化

取环 $(R, +, \cdot)$. 我们记 $(R', +', \cdot')$ 为另一个环, 且存在映射 $f: R' \rightarrow R$.

定义 19.1.12

我们称映射 f 为环 R' 到环 R 的**反同态**, 若其且满足以下条件:

- 1) 对任意 $a', b' \in R'$, 我们有 $f(a' +' b') = f(a') + f(b')$;
- 2) 对任意 $a', b' \in R'$, 我们有 $f(a' \cdot' b') = f(b') \cdot f(a')$.

若 f 还是双射, 我们称之为一个**反同构**.

给定一个交换群 M 和一个幺环 R . 假设存在一个环同态

$$\varphi: R \rightarrow \text{End}(M),$$

满足 $\varphi(1) = id_M$, 那么 M 是一个左 R -模. 使用不同的 R 到 $\text{End}(M)$ 的环同态, 我们可以在 M 上定义不同的左 R -模结构. 例如, 在之前的最后一个例子中, 我们如果选取不同的矩阵 $\mathcal{A}$, 则 V 作为 $F[\lambda]$ -模有不同的模结构.

类似地, 给定一个交换群 M 和一个幺环 R . 假设存在一个环反同态

$$\varphi: R \rightarrow \text{End}(M),$$

满足 $\varphi(1) = id_M$, 那么 M 是一个右 R -模. 由此, 我们可以看出, 使用不同的 R 到 $\text{End}(M)$ 的环反同态, 我们可以在 M 上定义不同的右 R -模结构.

例 19.1.13.

我们考虑 n -阶实矩阵环 $R = \text{Mat}_n(\mathbb{R})$. 我们记矩阵乘法为:

$$\Phi: \text{Mat}_n(\mathbb{R}) \times \text{Mat}_n(\mathbb{R}) \rightarrow \text{Mat}_n(\mathbb{R}).$$

我们考虑第一个位置上的 $\text{Mat}_n(\mathbb{R})$ 为环, 第二个位置上的 $\text{Mat}_n(\mathbb{R})$ 为群. 对于任意的矩阵 $A \in \text{Mat}_n(\mathbb{R})$, 我们可以定义如下映射:

$$\begin{aligned} \varphi_A^L: \text{Mat}_n(\mathbb{R}) &\rightarrow \text{Mat}_n(\mathbb{R}) \\ B &\mapsto \varphi_A^L(B) := AB. \end{aligned}$$

我们可以验证由这个定义, 我们得到一个从 $\text{Mat}_n(\mathbb{R})$ 到群自同态环 $\text{End}(\text{Mat}_n(\mathbb{R}))$ 的一个环同态. 群 $\text{Mat}_n(\mathbb{R})$ 是一个左 $\text{Mat}_n(\mathbb{R})$ -模.

类似地, 若我们考虑第二个位置上的 $\text{Mat}_n(\mathbb{R})$ 为环, 第一个位置上的 $\text{Mat}_n(\mathbb{R})$ 为群. 对于任意的矩阵 $A \in \text{Mat}_n(\mathbb{R})$, 我们可以定义如下映射:

$$\begin{aligned} \varphi_A^R: \text{Mat}_n(\mathbb{R}) &\rightarrow \text{Mat}_n(\mathbb{R}) \\ B &\mapsto (B)\varphi_A^R := BA. \end{aligned}$$

我们可以验证由这个定义, 我们得到一个从 $\text{Mat}_n(\mathbb{R})$ 到群自同态环 $\text{End}(\text{Mat}_n(\mathbb{R}))$ 的一个环反同态. 群 $\text{Mat}_n(\mathbb{R})$ 是一个右 $\text{Mat}_n(\mathbb{R})$ -模.

命题 19.1.14

设 ϕ 为环 R' 到环 R 的反同构. 若 M 是一个右 R -模, 则映射:

$$\begin{aligned}\Psi : R' \times M &\rightarrow M \\ (a', x) &\mapsto a'x := x\phi(a)\end{aligned}$$

给出一个左 R' -模结构.

证明. 证明留作练习. $\square$

以下我们将看到任取一个环, 我们都可以找到另一环与其反自同构. 我们考虑环 $(R, +, \cdot)$. 我们如下定义 R 上的一个新的运算:

$$\begin{aligned}\cdot' : R \times R &\rightarrow R \\ (a, b) &\mapsto a \cdot' b := b \cdot a.\end{aligned}$$

命题 19.1.15

三元组 $(R, +, \cdot')$ 是一个环.

证明. 证明留作练习. $\square$

定义 19.1.16

我们称环 $(R, +, \cdot')$ 为环 $(R, +, \cdot)$ 的**反转环** (opposite ring). 我们记环 R 的反转环为 R° .

命题 19.1.17

集合 R 上的恒等映射是一个从环 R 到 R° 反同构.

证明. 证明留作练习. $\square$

推论 19.1.18

任何右(左) R -模都是一个左(右) R° -模.

证明. 证明留作练习. $\square$

例 19.1.19.

我们仍考虑交换群 M 和其上的自同态集合. 若我们在定义对于任意 M 上的自同态 f 和 g , 对于任意 $x \in M$, 我们有

$$(f \circ' g)(x) = g(f(x)) = (g \circ f)(x).$$

我们可以验证, 三元组 $(\text{End}(M), +, \circ')$ 是一个幺环, 按照以上定义, 该环是 $\text{End}(M)$ 的反转环 $(\text{End}(M))^\circ$. 此时 M 是一个右 $(\text{End}(M))^\circ$ -模.

实际上, 我们可以考虑使用新的记号 $(x)f$, 将映射符号写在右边. 这样, 上边的运算复合可以写为:

$$(x)(f \circ' g) = ((x)f)g.$$

例 19.1.20.

我们考虑矩阵环 $\text{Mat}_n(\mathbb{R})$. 则其反转环 $\text{Mat}_n(\mathbb{R})^\circ$ 的乘法定义为: 对任意 $A, B \in \text{Mat}_n(\mathbb{R})$, 我们有 $A \cdot' B = B \cdot A$. 这是两个不同的环.

在本章剩余章节讨论中, 除非特别说明, 我们将只考虑左模, 并简称模.

一些关于模的简单的结论

类似于向量空间, 我们利用定义以及直接计算可以得到一些关于模的基本的结论.

命题 19.1.21 (教材116页)

设 R 为一个幺环, M 为一个 R -模.

- 1) 任取 $x \in M$, 我们有 $0_R x = 0_M$.
- 2) 任取 $a \in R$, 我们有 $a 0_M = 0_M$.
- 3) 任取 $a \in R, x \in M$, 我们有 $(-a)x = a(-x) = -(ax)$.
- 4) 任取 $a_1, \dots, a_n \in R, x_1, \dots, x_m \in M$, 我们有

$$\left(\sum_{i=1}^n a_i \right) \left(\sum_{j=1}^m x_j \right) = \sum_{i=1}^n \sum_{j=1}^m a_i x_j.$$

证明. 证明留作练习. □

19.2 子模

和之前介绍其他代数结构时一样, 一个模中对模运算封闭, 满足模定义子集构成一个同类型的子代数结构. 这就是我们将要介绍的概念: 子模.

定义及例子

设 R 为一个幺环, M 为一个 R -模.

定义 19.2.1 (教材定义 3.1.6)

任取 M 中非空子集 N , 我们称之为模 M 的**子模**, 若其在 M 的加法运算以及 R 与 M 的乘法运算下称为一个 R 模.

命题 19.2.2 (教材思考题 3.1.7)

模 M 中的非空子集 N 为一个子模当且仅当 N 满足以下两个条件:

- 1) 子集 N 为 M 的子群.
- 2) $(RN \subset N)$ 任取 $a \in R, x \in N$, 我们有 $ax \in N$.

例 19.2.3.

任取幺环 R 以及 R -模 M , 则 M 总有两个平凡子模 $\{0_M\}$ 和 M .

例 19.2.4.

当我们考虑域上的向量空间时, 子模就是我们熟悉的子空间..

例 19.2.5.

交换群 $\mathbb{Z}$ 作为 $\text{End}(\mathbb{Z})$ -模的子模有 $n\mathbb{Z}$.

要弄清楚这个结论, 我们首先观察到 $\mathbb{Z}$ 是一个由 1 生成的循环群. 因此要确定 $\mathbb{Z}$ 的一个自同构 f , 我们只需要确定 $f(1)$ 即可.

另一方面, 任取 $n \in \mathbb{N}$, 考虑子群 $n\mathbb{Z} < \mathbb{Z}$, 则 $n\mathbb{Z}$ 由 n 生成, 因此 $f(n\mathbb{Z}) < n\mathbb{Z}$ 当且仅当 $f(n) = nf(1) \in n\mathbb{Z}$.

利用这些我们可以看到任取 $n \in \mathbb{N}$, 任取 $f \in \text{End}(\mathbb{Z})$, 我们有

$$f(n\mathbb{Z}) \subset n\mathbb{Z}.$$

例 19.2.6.

考虑交换群 M . 任意 $N \subset M$ 关于 $\mathbb{Z}$ -模结构为一个子模当且仅当其关于群结构为一个子群.

例 19.2.7.

考虑幺环 R . 任意 $I \subset R$ 关于左(右) R -模结构为一个子模当且仅当其关于 R 的环结构为一个左(右)理想.

例 19.2.8.

记 V 为域 F 上的线性空间, $\mathcal{A}$ 为 V 上的线性变换. 考虑 $\mathcal{A}$ 诱导的 V 上的 $F[\lambda]$ -模结构. 则 V 作为 $F[\lambda]$ -模的子模是 $\mathcal{A}$ 在 V 上的不变子空间.

子模间的运算

正如我们在前边的例子中看到的, 一个模中的子模不一定唯一. 考虑子模之间做运算, 我们知道子模的有限和和任意交都是子模.

命题 19.2.9

记 R 为一个幺环, M 为一个 R -模.

- 1) 任取自然数 $k \in \mathbb{N}$, 若 $N_1, \dots, N_k$ 为模 M 的 k 个子模, 那么

$$N_1 + \dots + N_k := \{x_1 + \dots + x_k \mid x_1 \in N_1, \dots, x_k \in N_k\},$$

是 M 的一个子模.

- 2) 任取一个非空指标集 I , 我们考虑 M 的一些子集的集合 $\{N_\alpha\}_{\alpha \in I}$. 若对于任意 $\alpha \in I$, 我们有 N_α 为模 M 的子模, 那么 $\bigcap_{\alpha \in I} N_\alpha$ 是 M 的一个子模.

作为子模和的特殊情况, 我们介绍内直和的概念.

定义 19.2.10 (教材定义 3.1.9)

设 M 为一个 R -模. 设 $N_1, \dots, N_k$ 为 M 的 k 个子模. 我们称 $N = N_1 + \dots + N_k$ 为子模 $N_1, \dots, N_k$ 的**(内)直和**, 若 N 中的元素表示为 $N_1, \dots, N_k$ 元素的和方法唯一. 我们将其记作

$$N = N_1 \oplus \dots \oplus N_k.$$

注 19.2.11.

关于各种代数结构的直和以及直积的讨论, 请参考附录 B.

例 19.2.12.

考虑交换群

$$M = \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3,$$

上的 $\mathbb{Z}$ -模结构.

考虑其中的循环子模

$$N_1 = \mathbb{Z}(1, [0]_2, [0]_3),$$

$$N_2 = \mathbb{Z}(0, [1]_2, [0]_3),$$

$$N_3 = \mathbb{Z}(0, [0]_2, [1]_3),$$

则 M 可以写为以上三个循环模的直和:

$$M = N_1 \oplus N_2 \oplus N_3.$$

以下给出子模和为直和的等价条件.

定理 19.2.13 (教材定理 3.1.10)

设 M 为一个 R -模. 设 $N_1, \dots, N_k$ 为 M 的 k 个子模. 则以下叙述等价

- 1) $N_1 + \dots + N_k = N_1 \oplus \dots \oplus N_k$;
- 2) 若 $x_1 \in N_1, \dots, x_k \in N_k$, 满足 $x_1 + \dots + x_k = 0$, 则 $x_1 = \dots = x_k = 0$;
- 3) 对任意 $1 \leq i \leq k$, 我们有

$$N_i \cap \sum_{j \neq i} N_j = \{0\}.$$

证明. 证明留作练习. □

子模的生成

记 R 为一个幺环, M 为一个交换群. 我们考虑映射

$$\Phi : R \times M \rightarrow M,$$

给出的 M 上的模结构.

任给一个元素 $a \in R$, 其对应的纯量乘法给出一个群 M 的自同态映射

$$\begin{aligned} \varphi_a : M &\rightarrow M \\ x &\mapsto \varphi_a(x) = ax. \end{aligned}$$

类似的我们也可以考虑给定一个元素 $x \in M$, 我们可以定义以下映射:

$$\begin{aligned} \varphi_x : R &\rightarrow M \\ a &\mapsto \varphi_x(a) = ax. \end{aligned}$$

我们记映射 φ_x 的像集为

$$\text{Im } \varphi_x = Rx := \{ax \mid a \in R\},$$

通过直接验证定义, 我们可以得到如下结论.

命题 19.2.14

任取 $x \in M$, 同态 φ_x 的像 Rx 为 M 的一个子群.

证明. 证明留作练习. □

命题 19.2.15

任取 $x \in M$, 我们有

$$\ker \varphi_x := \{a \in R \mid ax = 0_M\},$$

是 R 的一个左理想.

证明. 任取 $a, b \in \ker \varphi_x$, 我们有

$$\varphi_x(a + (-b)) = (a + (-b))x = ax - bx = 0_M - 0_M = 0_M.$$

因此 $a + (-b) \in \ker \varphi_x$. 因此 $\ker \varphi_x$ 为 R 关于加法的一个子群.

任取 $a \in R$ 和 $b \in \ker \varphi_x$, 我们有

$$\varphi_x(ab) = (ab)x = a(bx) = a0_M = 0_M.$$

因此 $ab \in \ker \varphi_x$.

综上所述 $\ker \varphi_x$ 是 R 中的一个左理想. □

注 19.2.16.

类似地, 如果 M 为一个右 R -模, 则任取 $x \in M$, 核 $\ker \varphi_x$ 为一个右理想.

例 19.2.17.

我们考虑 $\mathbb{Z}_6$ 为一个 $\mathbb{Z}$ 模, 取 $a = 2$, 我们有

$$\begin{aligned}\varphi_2 : \mathbb{Z}_6 &\rightarrow \mathbb{Z}_6, \\ [m]_6 &\mapsto [m]_6.\end{aligned}$$

取 $x = [3]_6$, 我们有

$$\begin{aligned}\varphi_{[3]_6} : \mathbb{Z} &\rightarrow \mathbb{Z}_6, \\ n &\mapsto [3n]_6.\end{aligned}$$

可以证明 $\ker \varphi_{[3]_6} = 2\mathbb{Z}$, 为 $\mathbb{Z}$ 的一个理想..

命题 19.2.18

任取 $x \in M$, 映射 φ_x 的像 Rx 为 M 的一个子模.

证明. 证明留作练习. □

如果 M 的一个子模 N 包含 x , 由于 N 对纯量乘法封闭, 我们有 $Rx \subset N$. 因此 Rx 为最小的包含 x 的 M 的子模. 沿着这个思路, 考虑一般情形我们给出子模生成的概念.

定义 19.2.19

设 $S \subset M$ 为 M 的一个非空子集. 我们定义由子集 S 生成的模为所有包含 S 的子模的交, 即:

$$\langle S \rangle = \bigcap \{N \mid N \text{ 为 } M \text{ 的子模, 且 } S \subset N\}.$$

注 19.2.20.

笼统地说, $\langle S \rangle$ 是包含 S 最小的子模.

命题 19.2.21 (教材思考题 3.1.8)

设 S 为模 M 的一个非空子集. 我们有

$$\langle S \rangle = \{a_1x_1 + \cdots + a_kx_k \mid k \in \mathbb{N}^*, a_1, \dots, a_k \in R, x_1, \dots, x_k \in S\},$$

证明. 证明留作练习. □

定义 19.2.22

记 N 为模 M 中的一个子模, 若存在有限子集 $\{x_1, \dots, x_k\} \subset M$, 满足

$$N = \langle \{x_1, \dots, x_k\} \rangle = Rx_1 + \dots + Rx_k,$$

我们称 N 为 M 的一个**有限生成子模**. 集合 $\{x_1, \dots, x_k\}$ 被称为 N 的一个**生成元集**.

若进一步有 $M = N$, 我们称 M 为一个**有限生成模**.

例 19.2.23.

我们可以考虑幺环 R 上的多项式环 $R[x]$, 将其看作为一个 R 模. 所有次数小于等于 1 次多项式构成的集合 N 构成 $R[x]$ 的一个子模. 注意到

$$N = Rx + R.$$

例 19.2.24.

我们考虑以下交换群的直和

$$M = \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3.$$

任取其中的元素为 $(k, [m]_2, [n]_3)$, 我们可以将其写为

$$(k, [m]_2, [n]_3) = k(1, [0]_2, [0]_3) + m(0, [1]_2, [0]_3) + n(0, [0]_2, [1]_3)$$

因此

$$M = \mathbb{Z}(1, [0]_2, [0]_3) + \mathbb{Z}(0, [1]_2, [0]_3) + \mathbb{Z}(0, [0]_2, [1]_3),$$

为一个有限生成模.

定义 19.2.25

任取模 M 中的元素 x , 我们称 $\{x\}$ 生成的子模 Rx 为 M 的一个**循环子模**. 若存在 $x \in M$, 使得 $M = Rx$, 我们称 M 为一个**循环模**.

19.3 商模

记 R 为一个幺环. 记 M 为一个 R -模. 由于 M 是一个交换群, 其任意子群都是正规子群. 因此任取 M 的一个子群 N , 都有商群 M/N . 特别地, 商群 M/N 也是一个交换群. 对于任意元素 $x \in M$, 其在自然映射下的像为陪集 $x + N$. 接着一个自然的问题就是这里得到商群与 M 上的纯量乘法是否相容?

对于任意 $a \in R$, 我们仍记 φ_a 为 a 给出地纯量乘法映射. 我们希望定义映射:

$$\begin{aligned} \overline{\varphi_a} : M/N &\rightarrow M/N \\ x + N &\mapsto ax + N. \end{aligned}$$

要验证这个确实是映射, 我们需要 N 满足一些条件使得每个 $x + N$ 的像不依赖于这个陪集中代表元 x 的选取.

任取 $x, y \in M$, 由之前关于陪集的讨论, 我们有

$$x + N = y + N \Leftrightarrow x - y \in N.$$

考虑以上的构造, 任取 $a \in R$, 我们考虑 $ax + N$ 和 $ay + N$, 类似地有

$$ax + N = ay + N \Leftrightarrow a(x - y) = ax - ay \in N.$$

因此如果我们希望有

$$x + N = y + N \implies ax + N = ay + N,$$

则 N 需要满足任取 $a \in R$, 以及 $x \in N$, 有 $ax \in N$. 这也等价于要求子群 N 是 M 的子模.

注 19.3.1.

任给一个 R -模 M , 任取 N 为 M 的一个子群, 我们并不一定有 N 为 M 的子模. 例如我们有以下例子. 考虑 $\mathbb{Q}$ 为 $\mathbb{Q}$ -模. 取 $\mathbb{Q}$ 的加法子群 $\mathbb{Z}$, 注意到 $\mathbb{Q}1 = \mathbb{Q}$, 因此 $\mathbb{Z}$ 关于纯量乘法不封闭, 不是 $\mathbb{Q}$ 的子模.

我们总结如下.

命题 19.3.2

记 M 为一个 R -模. 任取 M 的子模 N , 任取 $a \in R$, 映射

$$\begin{aligned} \overline{\varphi}_a : M/N &\rightarrow M/N \\ x + N &\mapsto ax + N. \end{aligned}$$

定义良好, 且为 M/N 的自同态.

证明. 证明留作练习. □

沿用以上记号, 我们可以构造以下映射

$$\begin{aligned} \overline{\varphi} : R &\rightarrow \text{End}(M/N), \\ a &\mapsto \overline{\varphi}_a. \end{aligned}$$

命题 19.3.3

映射 $\overline{\varphi}$ 是一个环同态, 且将 $1 \in R$ 送到 M/N 上的恒等自同态.

证明. 证明留作练习. □

考虑如下映射:

$$\begin{aligned} \Phi : R \times M/N &\rightarrow M/N \\ (a, x + N) &\mapsto ax + N \end{aligned}$$

由之前对 ϕ_a 及 φ 的讨论, 我们有

推论 19.3.4

映射 Φ 给出商群 M/N 的一个 R -模结构.

证明. 证明留作练习. □

定义 19.3.5 (教材定理 3.1.13 中定义)

我们称以上构造的 R -模 M/N 为模 M 关于子模 N 的**商模**.

以下为一些商模的例子.

例 19.3.6.

设 V 为域 F 上的线性空间. 记 $W \subset V$ 为 V 的一个子空间. 则作为 F -模, 商空间 V/W 为 V 关于 W 的商模.

例 19.3.7.

设 R 为一个交换幺环. 记 I 为 R 的一个理想. 则从 R -模的角度看, 商环 R/I 可以看作是 R 关于 I 的商模.

例 19.3.8.

设 G 为一个交换群. 我们记 $H < G$ 为 G 的一个子群. 则从 $\mathbb{Z}$ -模的角度看, 商群 G/H 为模 G 关于子模 H 的商模.

19.4 模同态

记 R 为一个幺环.

模同态的定义

记 M 和 M' 为两个 R -模. 为了将两个模联系起来, 我们通常考虑使用二者之间与模结构相容的映射. 这就是模同态的概念. 我们首先给出模同态的定义.

定义 19.4.1 (教材定义 3.1.14)

我们称一个映射

$$f: M \rightarrow M'$$

为一个从模 M 到模 M' 的**模同态**, 若对任意 $a \in R$ 以及 $x, y \in M$, 都有

- 1) $f(x + y) = f(x) + f(y)$;
- 2) $f(ax) = af(x)$.

若进一步有映射 f 为单射(满射, 双射), 我们称 f 为一个**单同态**(**满同态**, **同构**).

注 19.4.2.

定义中第一个条件讲的是 f 与 M 和 M' 上的加法群结构相容; 而第二个条件讲的是 f 与 M 和 M' 上的 R -纯量乘法相容.

任给 $a \in R$, 记其在 M 和 M' 上给出的纯量乘法映射分别为 φ_a 和 ψ_a . 从映射的角度,

第二个条件是说对任意 $a \in R$, 我们都有如下交换图:

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ \varphi_a \downarrow & & \downarrow \psi_a \\ M & \xrightarrow{f} & M' \end{array}$$

以下是两个模同态的平凡例子.

例 19.4.3.

若我们考虑向量空间, 则以上定义给出向量空间之间的线性变换.

例 19.4.4.

记 G 和 G' 为两个交换群, 我们将其考虑为 $\mathbb{Z}$ -模. 任取 $f: G \rightarrow G'$ 为一个群同态, 则模同态定义中的第二个条件是自然满足的, 因此 f 也是二者间的 $\mathbb{Z}$ -模同态.

例 19.4.5.

若系数环 R 为一个交换环, 记 M 为一个 R -模, 则任取 $a \in R$ 以及 $x \in M$, 我们之前在章节 19.2 里定义的映射 φ_a 和 φ_x 都是模同态. 例如, 将 $\mathbb{Z}$ 看作 $\mathbb{Z}$ -模, 映射 $\varphi_2: n \mapsto 2n$ 为一个模同态.

定义 19.4.6

我们称模 M 到自身的模同态(模同构)为模 M 的**自同态(自同构)**.

定义 19.4.7

设 N 为 M 的一个子模, 我们称自然映射

$$\pi: M \rightarrow M/N$$

为模 M 到商模 M/N 的**自然同态**.

思考 19.4.8

验证自然映射是一个模同态.

模同态基本定理

模同态建立了相关模的元素之间的联系的时候, 也建立了相关模的子模之间的联系. 我们将通过模同态基本定理对这个联系进行描述.

记 M 和 M' 是两个 R -模, 并记

$$f: M \rightarrow M',$$

是一个模同态. 我们称集合

$$\ker f := \{x \in M \mid \phi(x) = 0'\},$$

为是模同态 f 的核. 我们仍用 $\text{Im } f$ 或 $f(M)$ 来记 f 的像.

命题 19.4.9 (教材命题3.1.16)

设 $f: M \rightarrow M'$ 是一个模同态. 我们有

- 1) $\ker f$ 为 M 的子模.
- 2) $\text{Im } f$ 为 M' 的子模.

证明. 证明留作练习. □

定理 19.4.10 (教材定理3.1.17)

设 M 和 M' 为 R -模. 假设 $f: M \rightarrow M'$ 为一个模满同态.

- (1) $M/\ker f \cong \text{Im } f$;
- (2) 存在 M 中包含 $\ker f$ 的子模与 M' 中子模的一一对应;
- (3) 若 $\ker f \subset N \subset M$ 为子模, 则有 $M/N \cong M'/f(N)$.

证明. 证明留作练习. □

模同态群

记 M 和 M' 为两个 R -模. 我们记

$$\text{Hom}(M, M') := \{f \mid f \text{ 为一个从 } M \text{ 到 } M' \text{ 的群同态}\}.$$

任取 $f, g \in \text{Hom}(M, M')$, 我们定义 $f + g$ 为一个从 M 到 M' 的映射, 满足对任意 $x \in M$, 我们有

$$(f + g)(x) = f(x) + g(x).$$

直接计算可验证 $f + g \in \text{Hom}(M, M')$. 由此, 我们可以定义 $\text{Hom}(M, M')$ 上的一个二元运算 $+$.

命题 19.4.11

二元组 $(\text{Hom}(M, M'), +)$ 为一个交换群.

证明. 由直接计算可得证明. 其中单位元为零同态; 任给 $f \in \text{Hom}(M, M')$, 其逆元为

$$\begin{aligned} -f: M &\rightarrow M', \\ x &\mapsto -f(x). \end{aligned}$$

□

我们考虑 $\text{Hom}(M, M')$ 的子集:

$$\text{Hom}_R(M, M') := \{\phi \in \text{Hom}(M, M') \mid \phi \text{ 为一个 } R\text{-模同态}\}.$$

命题 19.4.12

$\text{Hom}_R(M, M')$ 是 $\text{Hom}(M, M')$ 的一个子群.

我们回顾环 R 的中心的定义. 我们记以下 R 的子集为其中心:

$$Z(R) := \{a \in R \mid \forall b \in R, ab = ba\}.$$

集合 $Z(R)$ 为 R 的子环.

注 19.4.13.

对一般的幺环 R , 以下定义的纯量乘法并不一定能使其成为一个 R -模:

$$\begin{aligned} af : M &\rightarrow M' \\ x &\mapsto (af)(x) := a(f(x)). \end{aligned}$$

我们可以先假设存在这样的纯量乘法, 那么 af 也应该是一个 M 到 M' 的模同态. 因此, 我们应该有

$$(af)(bx) = b((af)(x)),$$

也即, 我们应该有 $ba f(x) = ab f(x)$. 由于 b 可以任取, 因此若我们希望 af 仍是一个模同态, 则任取 $a, b \in R$ 以及 $v \in \text{Im } f$, 都有

$$(ab - ba)v = 0'.$$

并不是任意环 R 上的模之间的任意同态都满足这个条件.

如果我们缩小考虑的范围, 令 $a \in Z(R)$, 则以上条件自然满足. 我们知道 $Z(R)$ 是 R 的一个子环. 因此 $\text{Hom}_R(M, M')$ 可以看作是一个 $Z(R)$ -模.

命题 19.4.14

$\text{Hom}_R(M, M')$ 为一个 $Z(R)$ -模.

证明. 证明留作练习. □

假设 $M = M'$. 我们考虑 M 的群自同态环 $\text{End}(M)$ (见章节 13.2.4). 由之前的讨论, 在构造模 M 时, 我们有一个环同态

$$\varphi : R \rightarrow \text{End}(M).$$

我们仍记 $\varphi(a) = \varphi_a$. 另外, 我们用如下记号记模 M 的自同态的集合:

$$\text{End}_R(M) := \{\phi \in \text{End}(M) \mid \phi \text{ 为模 } M \text{ 的自同态}\}.$$

由以上的讨论, 我们有如下关系:

命题 19.4.15

- 1) $\text{End}_R(M)$ 为 $\text{End}(M)$ 的一个子环;
- 2) 对任意 $a \in R$, 任意 $f \in \text{End}_R(M)$, 我们有 $\varphi_a \circ f = f \circ \varphi_a$.

例 19.4.16.

我们考虑 $\mathbb{R}$ 上的线性空间 $\mathbb{R}^n$. 作为 $\mathbb{R}$ -模, $\mathbb{R}^n$ 上的自同态环 $\text{End}_{\mathbb{R}}(\mathbb{R}^n)$ 是 $\mathbb{R}^n$ 上所有线性变换构成的环. 通过选取一组基, 我们可以将其等价于 n -阶方阵环. 任给 $a \in \mathbb{R}$, 其对应的 $\mathbb{R}^n$ 自同态的矩阵表示是一个纯量方阵 aI_n . 纯量方阵与所有 n -阶方阵交换.

定义 19.4.17

我们称 $\text{End}_R(M)$ 为模 M 的**自同态环**.

第二十章 自由模

通过选取一个基底, 一个域 F 上的有限维向量空间 V 可以被看作是有限多个一维向量子空间的直和:

$$V = (F\mathbf{v}_1) \oplus \cdots \oplus (F\mathbf{v}_n).$$

考虑当前基下的坐标, 我们可以得到一个 V 与

$$F^n = \underbrace{F \times \cdots \times F}_n.$$

的作为向量空间的同构. 我们可以利用维数对一个 F 上的线性空间分类. 从 F -模地角度看, 这个映射也是个 F -模同构.

记 R 为一个幺环. 记 M 为一个 R -模. 若 M 为有限生成的, 则存在 $n \in \mathbb{N}^*$ 以及 M 的 n 个元素

$$\{x_1, \dots, x_n\},$$

使得我们有

$$M = Rx_1 + \cdots + Rx_n.$$

我们也希望对 M 做类似的研究, 来看看关于 M 是否也有类似于向量空间的结论. 例如, 是否可以将 M 写为一些子模的直和, 是否也存在 $k \in \mathbb{N}^*$, 使我们有 $M \cong R^k$ 等等.

不过由于 R 为任取的幺环, 可能有不同于域的性质, 例如 R 可能不交换, 有零因子或者有不可逆的元素, R 中的理想可能不再仅仅只有 $\{0\}$ 和 R 两个等等. 这些因素都会对以上提到的研究产生影响. 因此对一般幺环 R 上的有限生成模的类似的研究结果会相对更复杂一些. 幸运的是, 我们确实可以将系数环为域这个条件做一定的放松 (例如系数环是 PID), 使得以上对向量空间的结论在一定程度上更一般的模上成立.

考虑上边提到的有限生成模 M . 注意到通过将 $(a_1, \dots, a_n)$ 送到 $a_1x_1 + \cdots + a_nx_n$, 我们可以构造一个从 R^n 到 M 的映射, 记为 f . 因此我们可以考虑以下问题:

- 1) R^n 上有模结构么?
- 2) 如果 R^n 是一个 R -模, 那么以上构造的 R^n 到 M 的映射 f 是一个模同态么?

本章我们将看到, 以上两个问题的答案都是肯定的. 我们称同构于 R^n 的模为(有限秩)自由模. 自由模在对模的研究中有着重要作用. 注意到在以上例子中 f 是满射, 利用模同态基本定理, 任意 R 上的有限生成模 M 都可以看作是类似于 R^n 的模的商模. 对 R^n 以及 $\ker f$ 的研究就能帮助我们了解 M 的结构.

我们在本章中介绍自由模的概念, 在之后的两章中, 我们将主要考虑 PID 上的自由模, 并利用这类模对 PID 上有限生成模进行研究, 从而得到 PID 上有限生成模结构定理. 作为该定理的应用, 我们将给出有限交换群的分类和线性变换的标准型.

需要说明的是, 对于不是有限生成的模, 我们也可以利用自由模从生成的角度来研究. 但受限于篇幅, 我们暂时仅关注有限生成模.

20.1 模的直和

设 R 为一个幺环. 设 $M_1, \dots, M_n$ 为 n 个 R -模. 我们考虑它们的直积(笛卡尔积):

$$M_1 \times \cdots \times M_n := \{\underline{x} = (x_1, \dots, x_n) \mid x_1 \in M_1, \dots, x_n \in M_n\}.$$

我们可以在其上定义加法以及与 R 的乘法. 任取 $\underline{x}$ 和 $\underline{y}$, 以及任意 $a \in R$, 我们定义

$$\begin{aligned}\underline{x} + \underline{y} &= (x_1 + y_1, \dots, x_n + y_n) \\ a\underline{x} &= (ax_1, \dots, ax_n)\end{aligned}$$

由此我们可以验证 $M_1 \times \cdots \times M_n$ 是一个 R -模. 我们称之为 $M_1, \dots, M_n$ 的(外)直和.

在本节讨论中, 我们暂时使用 $\oplus_e$ 来表示外直和 (external direct sum), 而用 $\oplus_i$ 来表示内直和 (internal direct sum).

注 20.1.1.

类似于我们在学习多项式环时所讨论的, 我们也可以考虑无穷多个模的直积和直和. 类似地, 作为集合, 直积考虑笛卡尔积中所有的元素, 而直和就意味着我们只考虑直积空间中那些只在有限多个位置上不为 0 的元素. 两个概念在只有在我们考虑有限多个模的情况下相同.

对任意 $1 \leq j \leq n$, 我们考虑以下映射:

$$\begin{aligned}\iota_j : M_j &\rightarrow M_1 \oplus_e \cdots \oplus_e M_n \\ x &\mapsto (0, \dots, 0, x, 0, \dots, 0)\end{aligned}$$

我们记其像为

$$\text{Im } \iota_j = M'_j = \{0\} \oplus_e \cdots \oplus_e \{0\} \oplus_e M_j \oplus_e \{0\} \oplus_e \cdots \oplus_e \{0\}.$$

命题 20.1.2 (教材命题3.1.12)

我们有以下结论:

- 1) 对任意 j , 映射 ι_j 是一个模之间的单同态, 我们有 $M_j \cong M'_j$.
- 2) $M_1 \oplus_e \cdots \oplus_e M_n$ 可以写为以下(内)直和:

$$M_1 \oplus_e \cdots \oplus_e M_n = M'_1 \oplus_i \cdots \oplus_i M'_n.$$

证明. 证明留作练习. □

注 20.1.3.

我们使用这些模构造了一个新的空间并在其上构造了模结构, 因此我们称之为外直和. 相对的, 由于一个模的子模之间已经有了良定义的运算, 且直和空间已经存在, 我们通常称之为(内)直和. 以上命题告诉我们, 通过同构映射 ι_j , 我们可以将外直和转化为内直和.

当我们讨论一个模的子模时, 我们既可以讨论子模的外直和, 也可以讨论子模的和. 设 M 为一个 R 模, 设 N_1 和 N_2 为 M 的两个子模. 我们可以考虑如下两个 R -模:

$$N_1 \oplus_e N_2, \quad N_1 + N_2.$$

我们要特别注意这两个模是不同的 R -模的子模:

- 模 $N_1 \oplus_e N_2$ 为 N_1 和 N_2 的外直和. 这是外直和 $M \oplus_e M$ 的一个子模而不是 M 的子模.
- 模 $N_1 + N_2$ 为 M 的子模. 在目前的条件下, 我们并不清楚 $N_1 + N_2$ 是不是内直和.

这两个模之间有一个自然的模同态:

$$\begin{aligned} f : N_1 \oplus_e N_2 &\rightarrow N_1 + N_2, \\ (x_1, x_2) &\mapsto x_1 + x_2. \end{aligned}$$

命题 20.1.4

模同态 f 为一个同构, 当且仅当 $N_1 + N_2$ 为内直和, 即当且仅当 $N_1 \cap N_2 = \{0\}$.

例 20.1.5.

我们考虑 $\mathbb{Z}$ 为一个 $\mathbb{Z}$ -模. 我们记 $N_1 = 2\mathbb{Z}$, $N_2 = 3\mathbb{Z}$. 我们可以验证

$$6\mathbb{Z} = 2\mathbb{Z} \cap 3\mathbb{Z}$$

以及

$$f(6, -6) = 0.$$

通过进一步直接验证, 我们有

$$\ker f = \{(6n, -6n) \mid n \in \mathbb{Z}\} = \mathbb{Z}(6, -6) \subset 2\mathbb{Z} \oplus_e 3\mathbb{Z}.$$

在之后的讨论中, 我们统一使用记号 $\oplus$. 若有歧义时, 我们会明确说明是内直和还是外直和.

20.2 自由模的定义

设 R 为一个幺环. 我们考虑 n 个 R 作为 R -模的直和:

$$R^n = \underbrace{R \oplus \cdots \oplus R}_n.$$

记其中的元素为

$$\underline{x} = (x_1, \dots, x_n) \in R^n.$$

为方便叙述, 我们记 ent_i 为以下映射:

$$\begin{aligned} \text{ent}_i : R^n &\rightarrow R \\ \underline{x} &\mapsto x_i \end{aligned}$$

对任意 $j \in \{1, \dots, n\}$ 我们记

$$\underline{e}_j = (0, \dots, 0, \underset{j}{1}, 0, \dots, 0).$$

我们有如下的观察:

观察 20.2.1

任取 R^n 中的元素 $\underline{x}$, 我们可以将其写为 $\underline{e}_1, \dots, \underline{e}_n$ 的 R -线性组合:

$$\underline{x} = x_1 \underline{e}_1 + \dots + x_n \underline{e}_n.$$

且

$$\underline{x} = 0,$$

当且仅当对任意 j , 我们有 $x_j = 0$.

简单地说就是我们可以将 R^n 中的元素写为 $\underline{e}_1, \dots, \underline{e}_n$ 的 R -线性组合, 且这种写法唯一.

证明. (练习)

□

定义 20.2.2 (教材定义 3.3.1)

设 R 为一个幺环, M 为一个 R 模. 我们称 M 为一个**秩为 n 的自由模**, 若 M 中存在 n 个元素 $u_1, \dots, u_n$, 使得对任意 R -模 N , 以及 N 中任意的 n 个元素 $v_1, \dots, v_n$, 我们有**唯一**的模同态:

$$\phi: M \rightarrow N,$$

满足对任意 $1 \leq j \leq n$, 我们有 $\phi(u_j) = v_j$. 我们进一步称 $\{u_1, \dots, u_n\}$ 为 M 的一组**基**.

注 20.2.3.

这里我们使用"泛性质"来定义自由模, 简单地说, 一个秩为 n 的 R 上自由模就是一个当我们试图用 n 个元素生成一个 R 模可能得到的"最大"的 R 模. 这里最大指的是存在一个从这个模到任意 n 个元素生成的 R 模的模同态.

从自由模定义出发, 我们可以直接验证这个概念被模同构保持:

命题 20.2.4 (教材命题 3.3.2)

设 R 为一个幺环. 设 M_1 和 M_2 为 R -模, 并设 M_1 为一个秩为 n 的自由模, 且

$$\{u_1, \dots, u_n\},$$

为 M_1 的一组基. 若存在

$$\phi: M_1 \rightarrow M_2,$$

为模同构, 则 M_2 也是 R 上自由模, 且

$$\{\phi(u_1), \dots, \phi(u_n)\},$$

为 M_2 的一组基.

我们也可以从另一个角度来说明秩为 n 的自由模是可以用 n 个元素生成的"最大"的模. 在我们尝试使用一些元素来生成一个代数结构的过程中, 我们都会遇到一个问题就是所使用的生成元之间是否有关系. 在我们讨论模的时候, 我们通常关心的是 " R -线性关系". 因此, 从生成的角度来说, R 上自由模就是由一组 " R -线性无关" 的元素生成的模. 具体来说, 我们有

定理 20.2.5 (教材定理 3.3.6)

设 R 为一个幺环, M 为一个 R -模. 设 $n \in \mathbb{N}^*$, 记 $u_1, \dots, u_n \in M$. 则 M 为自由模且 $\{u_1, \dots, u_n\}$ 为 M 的一组基当且仅当

(i) 任取 $u \in M$, 我们可以将其写为 $u_1, \dots, u_n$ 的 R -线性组合:

$$u = x_1 u_1 + \cdots + x_n u_n.$$

(ii) $x_1 u_1 + \cdots + x_n u_n = 0$ 当且仅当对任意 j , 我们有 $x_j = 0$.

注 20.2.6.

换言之, 第一个条件意味着 $M = Ru_1 + \cdots + Ru_n$, 第二个条件意味着对任意元素 $u \in R$, 以上表示为 $u_1, \dots, u_n$ 的 R -线性组合的方法唯一. 我们仍使用线性代数中的术语, 称满足第二个条件的 $u_1, \dots, u_n$ 是 R -线性无关的. 若元素 $u_1, \dots, u_n$ 不满足第二个条件, 我们称之为 R -线性相关.

注 20.2.7.

设 M 为一个自由模, 我们记

$$\mathcal{B} = \{u_1, \dots, u_n\},$$

为 M 的一组基. 对任意 $u \in M$, 考虑其在基 $\mathcal{B}$ 下的表示:

$$u = x_1 u_1 + \cdots + x_n u_n.$$

以上定理告诉我们这样的表达是唯一的. 我们称

$$[u]_{\mathcal{B}} = (x_1, \dots, x_n) \in R^n,$$

为 u 的在基 $\mathcal{B}$ 下的坐标.

我们先考虑 M 为一个循环模的情况.

设 $M = Ru$. 我们总有模同态

$$\phi_u : R \rightarrow Ru$$

$$x \mapsto xu.$$

之前我们证明过 $\ker \phi_u$ 是 R 的一个子模. 因此由模同态定理, 我们有 M 与 R 的一个商模同构.

注意到 $\{u\}$ 为 M 的一组基当且仅当 $\{u\}$ 线性无关, 也即任取 $a \in R$, 有

$$au \neq 0,$$

这等价于

$$\ker \phi_u = \{0\},$$

即 ϕ_u 是一个同构.

若 $\ker \phi_u = \{0\}$, 考虑任意模 N , 任取 $v \in N$, 我们考虑同态

$$\psi_v : R \rightarrow N,$$

$$a \mapsto av.$$

则 $\psi_v \circ \phi_u^{-1}$ 为一个从 M 到 N 的模同态, 将 u 送到 v .

另一方面, 如果我们暂时不知道 $\ker \phi_u$, 但是知道 $M = Ru$ 满足教材定义 3.3.1, 我们可以选取 $N = R$ 和 $v = 1$, 由定义 3.3.1, 我们知道存在唯一的一个模同态

$$\phi: M \rightarrow R,$$

满足 $\phi(u) = 1$.

我们考虑复合同态 $\phi \circ \phi_u$. 注意到这是一个从 R 到 R 的同态, 并且将 1 送到 1. 因此

$$id_R = \phi \circ \phi_u.$$

是 R 上的恒等映射. 因此 ϕ_u 是一个单射. 另一方面, ϕ_u 是一个满同态, 因此 ϕ_u 是同构, 我们有

$$\ker \phi_u = \{0\}.$$

教材定理 3.3.6 的证明. $\implies$ (i) 我们考虑

$$N = Ru_1 + \cdots + Ru_n.$$

若 M 是一个 R -自由模, 由定义我们有模满同态:

$$\xi: M \rightarrow N,$$

满足对任意 $1 \leq i \leq n$, $\xi(u_i) = u_i$.

另一方面, 我们有嵌入同态:

$$\eta: N \rightarrow M,$$

满足对任意 $u \in N$, $\eta(u) = u$.

因此

$$\eta \circ \xi: M \rightarrow M,$$

将 u_i 送到 u_i .

另一方面, 我们有 M 上的恒等同态映射 id_M 也满足这个性质. 由于 M 为一个自由模, 由定义中的模同态的唯一性, 我们有

$$\eta \circ \xi = id_M.$$

因此 ξ 为单射, η 为满射. 因此

$$M = N = Ru_1 + \cdots + Ru_n.$$

(ii) 由自由模的定义, 存在唯一的一个模同态:

$$\phi: M \rightarrow R^n,$$

满足对任意 $1 \leq i \leq n$, $\phi(u_i) = e_i$.

由于 $\{e_1, \dots, e_n\}$ 线性无关, 因此 $\{u_1, \dots, u_n\}$ 线性无关.

$\implies$ 假设 M 中可以由一组线性无关元素 $\{u_1, \dots, u_n\}$ 生成. 任给一个模 N 及其中的元素 $v_1, \dots, v_n$, 我们考虑同态映射

$$\phi: M \rightarrow N$$

满足对任意 $u \in M$,

$$\phi(a_1 u_1 + \cdots + a_n u_n) = a_1 v_1 + \cdots + a_n v_n.$$

首先证明该映射定义合理. 任取 $u \in M$, 由 (i) 我们可以将 u 写为 $u_1, \dots, u_n$ 的线性组合, 由 (ii) 这种写法唯一. 因此 ϕ 定义合理. 特别地, 我们有对任意 $1 \leq i \leq n$, $\phi(u_i) = v_i$.

由于 M 由 $u_1, \dots, u_n$ 生成, 因此 ϕ 由 $\phi(u_1), \dots, \phi(u_n)$ 决定. 因此 ϕ 唯一. $\square$

注 20.2.8.

我们这里希望说明的是如果一个代数结构 M 由 n 个元素生成, 那么 M 为"最大"的当且仅当这些生成元素之间有最少的关系(关于模结构就是"线性无关").

推论 20.2.9 (教材推论 3.3.7)

任取 $n \in \mathbb{N}^*$, 么环 R 上的模 M 为秩为 n 的自由模当且仅当 $M \cong R^n$.

证明. 证明留作练习. □

注 20.2.10.

需要注意的是, 我们目前还不清楚一个自由模的秩是否唯一. 实际上, 我们可以构造出秩不唯一的例子. 在下章介绍完环上的矩阵之后, 以及自由模之间的同态映射在固定基下的矩阵表示后, 我们将证明当 R 为交换么环时, R 上自由模的秩唯一.

推论 20.2.11

任取 $m, n \in \mathbb{N}^*$, 设 M 和 N 分别为秩为 m 和 n 的自由模, 则 $M \oplus N$ 也是自由模, 且秩为 $m + n$.

证明. 证明留作练习. □

第二十一章 自由模之间的同态

由前边几节的讨论, 利用坐标, 我们可以将对 R -自由模的讨论可以转化为对模 R^n 的讨论. 当我们考虑自由模 R^m 到 R^n 的模同态时, 矩阵是一个重要的工具. 本节我们将利用 R 上的矩阵及其性质, 对自由模之间的同态进行讨论.

21.1 自由模间的同态及其矩阵表示

设 R 为一个幺环. 任取非零自然数 m 和 n , 我们考虑 M 和 N 为秩分别为 m 和 n 的自由模. 记

$$\mathcal{B} = \{u_1, \dots, u_m\},$$

为 M 的一组基, 并记

$$\mathcal{C} = \{v_1, \dots, v_n\},$$

为 N 的一组基. 任取一个模同态

$$\varphi: M \rightarrow N,$$

我们考虑将 $\varphi(u_1), \dots, \varphi(u_m)$ 表达为 $v_1, \dots, v_n$ 的 R -线性组合, 则有:

$$\begin{aligned}\varphi(u_1) &= a_{11}v_1 + \dots + a_{1n}v_n, \\ \varphi(u_2) &= a_{21}v_1 + \dots + a_{2n}v_n, \\ &\dots \\ \varphi(u_m) &= a_{m1}v_1 + \dots + a_{mn}v_n,\end{aligned}$$

其中对任意 i, j , 有 $a_{ij} \in R$. 将以上表达式中的系数按照一定顺序排列, 我们可以引入矩阵来帮助讨论 φ 的性质.

定义 21.1.1

任取非零自然数 k 和 l , 环 R 上的 $k \times l$ 矩阵是一个映射

$$B: \{1, \dots, k\} \times \{1, \dots, l\} \rightarrow R.$$

通常我们记 $B(i, j) = b_{ij}$, 并将 B 写作 k 行 l 列的阵列形式:

$$B = (b_{ij})_{k \times l} = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1l} \\ b_{21} & b_{22} & \dots & b_{2l} \\ \dots & \dots & \dots & \dots \\ b_{k1} & b_{k2} & \dots & b_{kl} \end{bmatrix}$$

我们记 $R^{k \times l}$ 为 R 上所有 $k \times l$ 矩阵的集合.

考虑 $\varphi(u_1), \dots, \varphi(u_m)$ 的关于基底 $\mathcal{C}$ 的表达式中的坐标, 我们有以下定义.

定义 21.1.2

沿用之前的记号, 我们称矩阵

$$A_\varphi = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \in R^{m \times n},$$

是 φ 关于 $(M, \mathcal{B})$ 和 $(N, \mathcal{C})$ 的**矩阵表示**.

注 21.1.3.

若 $M = N$, 且 $\mathcal{B} = \mathcal{C}$, 我们称以上矩阵 A_φ 为 φ 在 $(M, \mathcal{B})$ 下的矩阵表示.

由此, 我们可以定义一个从 $\text{Hom}_R(M, N)$ 到 $R^{m \times n}(R)$ 的映射:

$$\begin{aligned} \Phi : \text{Hom}_R(M, N) &\rightarrow R^{m \times n}(R), \\ \varphi &\mapsto A_\varphi. \end{aligned}$$

由于 $\mathcal{B}$ 为 M 的一组基, 因此任意从 M 出发的同态都由 $u_1, \dots, u_m$ 的像唯一确定. 另一方面, 任取任取一个矩阵 $A \in R^{m \times n}$, 我们都有 N 中的元素:

$$\begin{aligned} v'_1 &= a_{11}v_1 + \cdots + a_{1n}v_n, \\ v'_2 &= a_{21}v_1 + \cdots + a_{2n}v_n, \\ &\cdots \\ v'_m &= a_{m1}v_1 + \cdots + a_{mn}v_n. \end{aligned}$$

利用自由模的泛性质, 我们有唯一的一个模同态

$$\varphi : M \rightarrow N,$$

满足对任意 $1 \leq i \leq m$, 我们有 $\varphi(u_i) = v'_i$. 因此我们有以下结论.

命题 21.1.4

映射 Φ 是一个双射.

记 $Z(R)$ 为 R 的中心. 考虑 $\text{Hom}_R(M, N)$ 上的 $Z(R)$ -模结构 (见命题 19.4.14), 则 Φ 诱导出 $R^{m \times n}$ 上的一个 $Z(R)$ -模结构. 任取同态 $\eta, \zeta \in \text{Hom}_R(M, N)$, 以及 $a \in Z(R)$, 我们定义

$$\begin{aligned} A_\eta + A_\zeta &:= A_{\eta+\zeta}, \\ aA_\eta &:= A_{a\eta}. \end{aligned}$$

考虑矩阵的具体表达式, 以上给出的加法和纯量乘法给出以下运算. 任取 R 上的矩阵 $B = (b_{ij})_{m \times n}$ 和 $C = (c_{ij})_{m \times n}$ 以及 $a \in R$, 我们定义

$$\begin{aligned} B + C &:= (b_{ij} + c_{ij})_{m \times n}, \\ aB &:= (ab_{ij})_{m \times n}. \end{aligned}$$

考虑 $R^{m \times n}$ 的这个由 Φ 诱导的 $Z(R)$ -模结构, 映射 Φ 自然为一个 $Z(R)$ -模同构.

注 21.1.5.

虽然 $R^{m \times n}$ 上的这个 $Z(R)$ -模结构是由 $\text{Hom}_R(M, N)$ 上的 $Z(R)$ -模结构诱导出的, 但 $R^{m \times n}$ 的 $Z(R)$ -模结构可以扩展为一个 R -模结构. 由定义可知所得的 R -模就是 $m \times n$ 个 R 作为 R -模的直和.

思考 21.1.6

以上注记中提到的 $R^{m \times n}$ 上的 $Z(R)$ -模结构总是可以扩展为 R -模结构, 而 $\text{Hom}_R(M, N)$ 上的 $Z(R)$ -模结构不一定可以扩展为 R -模结构. 二者矛盾么? 为什么?

定理 21.1.7 (教材定理3.2.1)

若 R 为一个交换幺环, 那么

- 1) $\text{Hom}_R(M, N)$ 是一个 R -模.
- 2) $\Phi : \text{Hom}_R(M, N) \rightarrow R^{m \times n}$ 为一个模同构.

证明. 我们已经在前一章讨论过 1). 关于 2), 注意到若 R 交换, 则 $Z(R) = R$, 我们可得结论. $\square$

推论 21.1.8

设 R 为一个交换幺环.

- 1) 模 $\text{Hom}_R(M, N)$ 为一个秩为 $m \times n$ 的自由模.
- 2) 模 $\text{End}_R(M)$ 与 $R^{n \times n}$ 同构.

下边对本节开始提到的同态 φ 做进一步的讨论. 沿用之前的记号. 任取 $u \in M$, 存在 $x_1, \dots, x_m \in R$, 有

$$u = x_1 u_1 + \cdots + x_m u_m.$$

元素 u 在同态 φ 下的像有以下表达:

$$\begin{aligned} \varphi(u) &= x_1 \varphi(u_1) + \cdots + x_m \varphi(u_m) \\ &= \sum_{i=1}^m \sum_{j=1}^n (x_i a_{ij}) v_j \\ &= \sum_{j=1}^n y_j v_j \\ &= v. \end{aligned}$$

由于 $\mathcal{C}$ 为 N 的一个基, 因此我们有

$$\begin{aligned} y_1 &= x_1 a_{11} + \cdots + x_m a_{m1}, \\ y_2 &= x_1 a_{12} + \cdots + x_m a_{m2}, \\ &\dots \\ y_n &= x_1 a_{1n} + \cdots + x_m a_{mn}. \end{aligned}$$

我们定义

$$R^{1 \times k} \times R^{k \times 1} \rightarrow R$$

$$\left([b_1 \ \cdots \ b_k], \begin{bmatrix} c_1 \\ \vdots \\ c_k \end{bmatrix} \right) \mapsto [b_1 \ \cdots \ b_k] \begin{bmatrix} c_1 \\ \vdots \\ c_k \end{bmatrix} = \sum_{i=1}^k b_i c_i.$$

利用这个定义, 之前的关系可以重写为

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_m \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} = \begin{bmatrix} y_1 & y_2 & \cdots & y_n \end{bmatrix}$$

例 21.1.9.

我们考虑自由模 R^m 的自然基

$$\begin{aligned} \underline{e}_1 &= \overbrace{(1, 0, 0, \dots, 0)}^m \\ \underline{e}_2 &= (0, 1, 0, \dots, 0) \\ &\vdots \\ \underline{e}_m &= (0, 0, 0, \dots, 1) \end{aligned}$$

以及自由模 R^n 的自然基

$$\begin{aligned} \underline{f}_1 &= \overbrace{(1, 0, 0, \dots, 0)}^n \\ \underline{f}_2 &= (0, 1, 0, \dots, 0) \\ &\vdots \\ \underline{f}_m &= (0, 0, 0, \dots, 1) \end{aligned}$$

设 φ 为 R^m 到 R^n 的模同态. 则我们有

$$\begin{aligned} \varphi(\underline{e}_1) &= a_{11}\underline{f}_1 + \cdots + a_{1n}\underline{f}_n \\ \varphi(\underline{e}_2) &= a_{21}\underline{f}_1 + \cdots + a_{2n}\underline{f}_n \\ &\vdots \\ \varphi(\underline{e}_m) &= a_{m1}\underline{f}_1 + \cdots + a_{mn}\underline{f}_n \end{aligned}$$

任取 R^m 中的元素 $\underline{x} = x_1\underline{e}_1 + \cdots + x_n\underline{e}_n$, 我们有

$$\begin{aligned} \varphi(\underline{x}) &= x_1\varphi(\underline{e}_1) + \cdots + x_n\varphi(\underline{e}_n) \\ &= \sum_{i=1}^m x_i a_{i1}\underline{f}_1 + \cdots + \sum_{i=1}^m x_i a_{in}\underline{f}_n \\ &= y_1\underline{f}_1 + \cdots + y_n\underline{f}_n = \underline{y} \end{aligned}$$

我们关注坐标则有:

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_m \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} = \begin{bmatrix} y_1 & y_2 & \cdots & y_n \end{bmatrix}$$

由此同态 φ 关于 R^m 的基 $\{e_1, \dots, e_m\}$ 以及 R^n 的基 $\{f_1, \dots, f_n\}$ 的矩阵为:

$$A_\varphi = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}.$$

记 k 为一个非零自然数, 并记 N' 为一个 R 上秩为 k 自由模. 记

$$\mathcal{D} := \{w_1, \dots, w_k\},$$

为 N' 的一组基. 记

$$\psi : N \rightarrow N'$$

为一个模同态. 因此 $\psi \circ \varphi$ 给出一个 M 到 N' 的模同态. 我们记

$$B_\psi = (b_{ij})_{n \times k} \quad \text{和} \quad C_{\psi \circ \varphi} = (c_{ij})_{m \times k}$$

分别为 ψ 关于 $(N, \mathcal{C})$ 和 $(N', \mathcal{D})$ 的矩阵表示和 $\psi \circ \varphi$ 关于 $(M, \mathcal{B})$ 和 $(N', \mathcal{D})$ 的矩阵表示.

任取 $1 \leq i \leq m$, 我们有

$$\begin{aligned} & (\psi \circ \varphi)(u_i) \\ &= \psi(\varphi(u_i)) \\ &= \psi\left(\sum_{j=1}^n a_{ij} v_j\right) \\ &= \sum_{j=1}^n a_{ij} \psi(v_j) \\ &= \sum_{j=1}^n a_{ij} \left(\sum_{l=1}^k b_{jl} w_l\right) \\ &= \sum_{l=1}^k \left(\sum_{j=1}^n a_{ij} b_{jl}\right) w_l. \end{aligned}$$

因此我们有

$$C_{\psi \circ \varphi} = (c_{il})_{m \times k} = \left(\sum_{j=1}^n a_{ij} b_{jl}\right)_{m \times k}.$$

由此, 取 m, n, k 三个非零自然数, 我们可以定义 R 上的矩阵乘法如下:

$$\begin{aligned} & R^{m \times n} \times R^{n \times k} \rightarrow R^{m \times k}, \\ & ((a_{ij})_{m \times n}, (b_{jl})_{n \times k}) \mapsto \left(\sum_{j=1}^n a_{ij} b_{jl}\right)_{m \times k}. \end{aligned}$$

注 21.1.10.

我们仍可以定义转置. 但是由于 R 不一定交换性, 关系 $(AB)^t = B^t A^t$ 不一定成立.

特别地, 若 $m = n = k$, 我们有幺环 $(\text{End}_R(M), +, \circ)$. 考虑 M 的基 $\mathcal{B}$ 以及同态在 $(M, \mathcal{B})$ 下的矩阵表示所给出的双射

$$\Phi : \text{End}_R(M) \rightarrow R^{m \times m}.$$

以上讨论告诉了我们 $\text{End}_R(M)$ 的复合运算通过 Φ 在 $R^{m \times m}$ 诱导出的乘法运算是如何进行的.

命题 21.1.11

考虑以上定义加法和乘法, 矩阵空间 $R^{m \times m}$ 构成了一个幺环, 并且 Φ 为一个幺环的同构.

注 21.1.12.

当 $n > 1$ 时, 不管 R 是否交换, 若存在 $a, b \in R$, 满足 $ab \neq 0$, 则环 $R^{n \times n}$ 不交换. 例如

$$\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & ba \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ b & 0 \end{bmatrix} \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}$$

我们称一个 $n \times n$ 矩阵为 n 阶方阵.

21.2 交换幺环上的矩阵

设 R 为一个交换幺环.

定义 21.2.1

记 $n \in \mathbb{N}^*$. 任取 $A \in R^{n \times n}$, 方阵 A 的行列式定义为以下 R 的元素:

$$\det A := \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

这里 $\text{sgn} : S_n \rightarrow \{-1, 1\}$ 为 n -元置换的符号.

回顾: n -元置换群元素 σ 的符号为 $(-1)^{\rho(\sigma)}$. 这里 $\rho(\sigma) \in \mathbb{N}$ 为 σ 的逆序数. 另一方面, 我们也可以考虑将 σ 写为对换的复合. 一个置换写成对换的复合的方法不唯一, 但是不同写法中对换的数目有相同的奇偶性. 如果 σ 写成对换复合中有奇数个对换, 我们称之为奇置换; 如果有偶数个对换, 我们称之为偶置换. 奇置换的符号为 -1 , 偶置换的符号为 1 .

定义 21.2.2

记 $n \in \mathbb{N} \setminus \{0, 1\}$. 任取 $A \in R^{n \times n}$. 矩阵 A 的 a_{ij} 的**余子式**为矩阵 A 去掉第 i 行和第 j 列之后的 $n-1$ 阶方阵的行列式:

$$M_{ij} := \det \begin{bmatrix} a_{11} & \cdots & a_{1(j-1)} & a_{1(j+1)} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{(i-1)1} & \cdots & a_{(i-1)(j-1)} & a_{(i-1)(j+1)} & \cdots & a_{(i-1)n} \\ a_{(i+1)1} & \cdots & a_{(i+1)(j-1)} & a_{(i+1)(j+1)} & \cdots & a_{(i+1)n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{n(j-1)} & a_{n(j+1)} & \cdots & a_{nn} \end{bmatrix}$$

矩阵 A 的 a_{ij} 的**代数余子式** 为 $A_{ij} = (-1)^{i+j} M_{ij}$.

记 $n \in \mathbb{N} \setminus \{0, 1\}$, 类似于我们在线性代数中见到的域上的方阵行列式的性质, 交换幺环 R 上的 n 阶方阵的行列式也有如下性质:

- 1) 交换矩阵的两行, 则其行列式乘以 (-1) .
- 2) 交换矩阵的两列, 则其行列式乘以 (-1) .
- 3) 将矩阵一行乘以一个系数加到另一行不改变行列式.
- 4) 将矩阵一列乘以一个系数加到另一列不改变行列式.
- 5) (列展开) 对任意 $j \in \llbracket 1, n \rrbracket$, 我们有

$$\det A = \sum_{i=1}^n a_{ij} A_{ij}.$$

- 6) (行展开) 对任意 $i \in \llbracket 1, n \rrbracket$, 我们有

$$\det A = \sum_{j=1}^n a_{ij} A_{ij}.$$

- 7) 任取两个 n 阶方阵 A 和 B , 我们有

$$\det(AB) = \det A \det B$$

注 21.2.3.

这些性质的证明主要涉及交换幺环运算的性质, 特别是交换幺环中乘法满足交换律, 以及乘法和加法有分配律.

定义 21.2.4

我们称如下矩阵为 A 的**代数余子式矩阵**为

$$\text{Cof}(A) = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{bmatrix}$$

其转置被称为 A 的**伴随矩阵**:

$$A^* = \begin{bmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{bmatrix}$$

我们考虑矩阵行列式关于列展开和行展开的公式, 可以得到以下命题

命题 21.2.5

记 $n \in \mathbb{N} \setminus \{0, 1\}$. 设 R 为一个交换幺环, 任取 $A \in R^{n \times n}$, 我们有

$$AA^* = A^*A = (\det A)I_n.$$

之前我们已经讨论过, 通过考虑矩阵加法和乘法, $R^{n \times n}$ 有一个环结构.

定义 21.2.6

我们称一个 n 阶方阵 $A \in R^{n \times n}$ **可逆**, 若存在一个矩阵 $B \in R^{n \times n}$ 满足

$$AB = BA = I_n,$$

即 A 关于矩阵乘法有逆元.

以上命题有如下推论.

推论 21.2.7

记 $n \in \mathbb{N} \setminus \{0, 1\}$. 设 R 为一个交换幺环, 任取 $A \in R^{n \times n}$, 我们有

- 1) A 可逆当且仅当 $\det A$ 为 R 中的单位.
- 2) 若 A 可逆, 则有

$$A^{-1} = (\det A)^{-1}A^*.$$

自由模的秩

在线性代数的学习中, 我们知道任给一个有限维向量空间, 所有的基底有相同的势. 例如, 若一个 F -线性空间 V 有一个基 $\{u_1, \dots, u_n\}$, 则任给 V 的另一组基 $\{v_1, \dots, v_n\}$, 我们有 $n = m$. 由此, 我们可以定义线性空间的维数. 交换幺环上的有限生成模也有类似的性质.

定理 21.2.8 (教材定理3.3.8)

设 R 为一个交换幺环, M 为一个 R -自由模. 设 $\mathcal{B} = \{u_1, \dots, u_m\}$ 和 $\mathcal{C} = \{v_1, \dots, v_n\}$ 都是 M 的基. 则我们有 $m = n$.

证明. 我们考虑 φ 为 M 上的恒等映射. 考虑 φ 关于 $(M, \mathcal{B})$ 和 $(M, \mathcal{C})$ 的矩阵 $A = (a_{ij})_{n \times m} \in R^{n \times m}(R)$, 以及关于 $(M, \mathcal{C})$ 和 $(M, \mathcal{B})$ 的矩阵 $B = (b_{ij})_{m \times n} \in R^{m \times n}(R)$. 因此我们有 $AB = I_n$ 以及 $BA = I_m$.

设 $m \neq n$. 不失一般性的, 我们可以假设 $m < n$. 我们可以通过添加 0 的方式, 将矩阵 A 和 B 扩充为 n -阶方阵:

$$\tilde{A} = \begin{bmatrix} A & 0 \end{bmatrix}, \tilde{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}$$

可以验证 $\tilde{A}\tilde{B} = AB = I_n$. 但是, $\det \tilde{A} = \det \tilde{B} = 0$ 与 $\det I_n = 1$ 矛盾. 因此我们有 $m = n$. $\square$

因此交换幺环上的模的秩唯一.

推论 21.2.9

设 R 为一个交换幺环. 任给 $m, n \in \mathbb{N}^*$, 我们有 $R^m \cong R^n$ 当且仅当 $m = n$.

矩阵表示与坐标

为了方便讨论, 我们将使用如下方法来记线性变换的矩阵表示在坐标上的作用.

记 R 为一个交换幺环. 设 M 为 R 的自由模, 且 $r(M) = m \in \mathbb{N}^*$. 设

$$\mathcal{B} = \{u_1, \dots, u_m\} \subset M,$$

为 M 的一组基. 任取 $u \in M$, 存在 $x_1, \dots, x_m \in R$, 满足

$$u = x_1 u_1 + \dots + x_m u_m.$$

我们用 R -列向量记

$$[u]_{\mathcal{B}} = \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix} \in R^m,$$

为 u 在基底 $\mathcal{B}$ 下的坐标.

记 N 为另一个 R 自由模, 且 $r(N) = n \in \mathbb{N}^*$. 记

$$\mathcal{C} = \{v_1, \dots, v_n\} \subset N,$$

为 N 的一组基. 我们类似的用 R -列向量 $[v]_{\mathcal{C}}$ 来记 $v \in N$ 在基 $\mathcal{C}$ 下的坐标.

任取 M 到 N 的模同态 φ , 我们考虑之前定义的 φ 在 M 的基底 $\mathcal{B}$ 和 N 的基底 $\mathcal{C}$ 下的矩阵表示. 为方便讨论, 我们从现在开始用 A_{φ} 记这个矩阵的转置, 则有

$$A_{\varphi} : (M, \mathcal{B}) \rightarrow (N, \mathcal{C}),$$

$$[u]_{\mathcal{B}} \mapsto A_{\varphi}[u]_{\mathcal{B}} = [\varphi(u)]_{\mathcal{C}}.$$

坐标变换

我们继续考虑模 M 和 N , 任取一个模同态

$$\varphi: M \rightarrow N,$$

为了方便研究它, 我们希望寻找 M 的基底和 N 的基底使得 φ 在这些基底下的矩阵表示相对简单一些. 这个寻找的过程就涉及到在 M (以及 N) 中不断尝试改变基底, 因此涉及到 M (以及 N) 中的坐标变换.

我们记 $\mathcal{B}$ 和 $\mathcal{B}'$ 为 M 的两组基. 由之前的讨论, 我们知道这两组基涉及到的元素数目相同, 都等于 M 的秩. 我们考虑 M 到自己的恒等同态

$$\begin{aligned} \text{id}: M &\rightarrow M \\ u &\mapsto u \end{aligned}$$

我们记 id 在基底 $\mathcal{B}$ 和 $\mathcal{B}'$ 下的矩阵表示为 $P_{\mathcal{B}', \mathcal{B}}$, 则对任意 $u \in M$, 有

$$P_{\mathcal{B}', \mathcal{B}}[u]_{\mathcal{B}} = [u]_{\mathcal{B}'}.$$

以下我们介绍矩阵 $P_{\mathcal{B}', \mathcal{B}}$ 与 $\mathcal{B}$ 和 $\mathcal{B}'$ 的具体关系. 我们记

$$\mathcal{B} = \{u_1, \dots, u_m\}.$$

以及

$$\mathcal{B}' = \{u'_1, \dots, u'_m\}.$$

我们有

$$P_{\mathcal{B}', \mathcal{B}} = [[u_1]_{\mathcal{B}'} \cdots [u_m]_{\mathcal{B}'}],$$

即基 $\mathcal{B}$ 中的元素 $u_1, \dots, u_m$ 关于 $\mathcal{B}'$ 的坐标构成 $P_{\mathcal{B}', \mathcal{B}}$ 的列向量.

定义 21.2.10

我们称矩阵 $P_{\mathcal{B}', \mathcal{B}}$ 为 M 上从关于基底 $\mathcal{B}$ 的坐标到关于基底 $\mathcal{B}'$ 的坐标变换矩阵.

我们可以验证一下坐标变换矩阵和坐标之间的关系. 考虑 u_1 在 $\mathcal{B}$ 下的坐标

$$[u_1]_{\mathcal{B}} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

则我们有

$$\begin{aligned} &P_{\mathcal{B}', \mathcal{B}}[u_1]_{\mathcal{B}} \\ &= [[u_1]_{\mathcal{B}'} \cdots [u_m]_{\mathcal{B}'}] \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \\ &= [u_1]_{\mathcal{B}'}. \end{aligned}$$

命题 21.2.11

模 M 上的有序基的集合与 $R^{m \times m}$ 上的可逆矩阵之间存在一个双射.

证明. 我们首先在 M 选定一个基底 $\mathcal{B}$. 然后考虑其它基底中的元素在 $\mathcal{B}$ 下的坐标, 可以定义如下映射:

$$F: \{\mathcal{B}' \in M^m \mid \mathcal{B}' \text{ 为 } M \text{ 的一组基}\} \rightarrow R^{m \times m}$$

$$\mathcal{B}' \mapsto F(\mathcal{B}') := P_{\mathcal{B}', \mathcal{B}}$$

为了验证这个映射是双射, 我们需要验证以下两点:

- 1) 对任意 $\mathcal{B}'$, 矩阵 $P_{\mathcal{B}', \mathcal{B}}$ 可逆.
- 2) $F(\mathcal{B}') = F(\mathcal{B}'')$ 当且仅当 $\mathcal{B}' = \mathcal{B}''$.
- 3) 任取可逆矩阵 $A \in R^{m \times m}$, 都有 $\mathcal{B}'$ 满足 $P_{\mathcal{B}', \mathcal{B}} = A$.

我们仍使用之前的记号, 记

$$\mathcal{B} = \{u_1, \dots, u_m\}.$$

以及

$$\mathcal{B}' = \{u'_1, \dots, u'_m\}.$$

注意到任取 $u \in M$, 我们有

$$(P_{\mathcal{B}, \mathcal{B}'} P_{\mathcal{B}', \mathcal{B}})[u]_{\mathcal{B}} = P_{\mathcal{B}, \mathcal{B}'}[u]_{\mathcal{B}'} = [u]_{\mathcal{B}}.$$

当我们取 $u = u_1$ 时, 有

$$(P_{\mathcal{B}, \mathcal{B}'} P_{\mathcal{B}', \mathcal{B}}) \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

我们对 $u_2, \dots, u_m$ 做类似的讨论则有

$$P_{\mathcal{B}, \mathcal{B}'} P_{\mathcal{B}', \mathcal{B}} = I_n.$$

类似地, 我们有

$$P_{\mathcal{B}', \mathcal{B}} P_{\mathcal{B}, \mathcal{B}'} = I_n.$$

因此 $P_{\mathcal{B}, \mathcal{B}'}$ 可逆, 且

$$P_{\mathcal{B}', \mathcal{B}} = P_{\mathcal{B}, \mathcal{B}'}^{-1}.$$

下边另取基底 $\mathcal{B}''$, 我们记

$$\mathcal{B}'' = \{u''_1, \dots, u''_m\},$$

注意到

$$P_{\mathcal{B}, \mathcal{B}'} = [[u'_1]_{\mathcal{B}} \cdots [u'_m]_{\mathcal{B}}].$$

$$P_{\mathcal{B}, \mathcal{B}''} = [[u''_1]_{\mathcal{B}} \cdots [u''_m]_{\mathcal{B}}].$$

若

$$P_{\mathcal{B}, \mathcal{B}'} = F(\mathcal{B}')^{-1} = F(\mathcal{B}'')^{-1} = P_{\mathcal{B}, \mathcal{B}''},$$

考虑对应列相等, 由于坐标决定元素, 我们有

$$u'_1 = u''_1, \dots, u'_m = u''_m.$$

因此

$$\mathcal{B}' = \mathcal{B}''.$$

最后任取可逆矩阵 A , 记其逆为

$$A^{-1} = (a_{ij})_{m \times m} \in R^{m \times m},$$

我们考虑

$$\begin{aligned} u'_1 &= a_{11}u_1 + \cdots + a_{m1}u_m, \\ &\cdots \\ u'_m &= a_{1m}u_1 + \cdots + a_{mm}u_m, \end{aligned}$$

并记

$$\mathcal{B}' = \{u'_1, \dots, u'_m\}.$$

由于 A 可逆, 基 $\mathcal{B}$ 的元素 $u_1, \dots, u_m$ 都在 $\mathcal{B}'$ 中元素生成 M 的子模中, 因此 $\mathcal{B}'$ 中元素构成 M 的一组生成元. 下证这些元素是 R 线性无关的.

任取 R 中元素 $b_1, \dots, b'_m$, 满足

$$b_1u'_1 + \cdots + b'_mu'_m = 0,$$

我们有

$$0 = \sum_{i=1}^m \left(\sum_{j=1}^m b_j a_{ij} \right) u_i.$$

由于 $u_1, \dots, u_m$ 构成一组基, 对任意 $1 \leq i \leq m$, 我们有

$$\sum_{j=1}^m b_j a_{ij} = 0.$$

将单位阵的第一列换为以下列向量

$$\begin{bmatrix} b_1 \\ \vdots \\ b'_m \end{bmatrix}$$

并记所的矩阵为 B . 由以上关系知矩阵

$$A^{-1}B = C,$$

的第一列系数全为 0. 我们左乘 A 得到

$$B = AC.$$

由于 C 第一列全为 0, 我们有 AC 的第一列也全为 0, 因此 B 的第一列也全为 0. 所以有

$$b_1 = \cdots = b'_m = 0.$$

因此 $\mathcal{B}'$ 中元素 R -线性无关. 综上所述 $\mathcal{B}'$ 为 M 的一组基.

注意到任取 $1 \leq i \leq m$, 元素 u'_i 在 $\mathcal{B}$ 下的坐标为

$$[u'_i]_{\mathcal{B}} = \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix}.$$

因此

$$P_{\mathcal{B}, \mathcal{B}'} = A^{-1}.$$

由之前的讨论可知

$$P_{\mathcal{B}', \mathcal{B}} = P_{\mathcal{B}, \mathcal{B}'}^{-1} = A.$$

因此 F 为满射. □

设 M 是一个阶为 m 的 R 上自由模, N 为一个阶为 n 的 R 上自由模, 记 $\mathcal{B}$ 和 $\mathcal{B}'$ 为 M 的两组基底, $\mathcal{C}$ 和 $\mathcal{C}'$ 为 N 的两组基底, 记

$$\varphi: M \rightarrow N,$$

为一个模同态, 且 A 为 φ 在基底 $\mathcal{B}$ 和 $\mathcal{C}$ 下的坐标表示:

$$\begin{aligned} A: (M, \mathcal{B}) &\rightarrow (N, \mathcal{C}), \\ [u]_{\mathcal{B}} &\mapsto [\varphi(u)]_{\mathcal{C}}. \end{aligned}$$

设

$$P = P_{\mathcal{B}, \mathcal{B}'}, Q = Q_{\mathcal{C}', \mathcal{C}},$$

则有

$$B[u]_{\mathcal{B}'} = (QAP)[u]_{\mathcal{B}'} = (QA)[u]_{\mathcal{B}} = Q[\varphi(u)]_{\mathcal{C}} = [\varphi(u)]_{\mathcal{C}'},$$

即所得矩阵 B 是模同态 φ 在基底 $\mathcal{B}'$ 和 $\mathcal{C}'$ 下的矩阵表示.

$$\begin{array}{ccc} (M, \mathcal{B}) & \xrightarrow{A} & (N, \mathcal{C}) \\ P \uparrow & & \downarrow Q \\ (M, \mathcal{B}') & \xrightarrow{B} & (N, \mathcal{C}') \end{array}$$

定义 21.2.12

任取矩阵 $A, B \in R^{n \times m}$, 我们称 A 与 B 等价, 若存在可逆矩阵 $P \in R^{m \times m}$ 和 $Q \in R^{n \times n}$ 满足使得 $B = QAP$.

因此, 从这个角度看, 相互等价的矩阵可以看作是同一个模同态在不同基底下的不同的矩阵表示.

21.3 PID 上的矩阵

在上一节的最后, 我们看到理论上我们可以通过坐标变换来简化一个模同态的矩阵表示. 我们首先考虑一个特别的例子. 令 $R = \mathbb{R}$, 我们知道通过左乘和右乘初等方阵, 我们可以将任意 $m \times n$ 非零实矩阵 A 转化为如下形式:

$$\Omega(A) := \begin{bmatrix} I_r & O_{r \times (n-r)} \\ O_{(m-r) \times r} & O_{(m-r) \times (n-r)} \end{bmatrix}$$

其中 $O_{k \times l}$ 为 $k \times l$ 零矩阵. 我们称 $\Omega(A)$ 为 A 的**标准型**, 并称 r 为 A 的秩.

当我们开始讨论环的时候, 由于环缺少域的一些性质, 当我们试图做同样的事情的时候, 我们会有疑问: 是否还能够达到同样的目标呢?

在本节中, 我们将说明, 当 R 为一个 PID 的时候, 虽然操作过程会复杂一些, 并且需要用到一些利用 PID 的特殊性质, 我们可以基本达到类似的目标 (结论略有不同). 以下我们记 D 为一个 PID.

初等矩阵

首先注意到之前一些针对域上矩阵的操作此时仍可以使用. 我们首先回顾初等矩阵的概念.

我们考虑 n -阶方阵. 任取 $1 \leq i, j \leq n$, 我们记 $E_{ij} = (e_{kl})_{n \times n}$, 满足

$$e_{kl} = \begin{cases} 1, & (k, l) = (i, j) \\ 0, & (k, l) \neq (i, j) \end{cases}$$

对任意 $i \neq j$, 我们定义

$$\begin{aligned} T_{ij}(a) &:= I_n + aE_{ij}, \quad a \in D \\ S_{ij} &:= I_n - E_{ii} - E_{jj} + E_{ij} + E_{ji} \\ K_i(a) &:= I_n + (a - 1)E_{ii}, \quad a \in U \end{aligned}$$

在乘法可以定义的情况下, 我们有如下观察.

观察 21.3.1 (i) 若对一个矩阵左乘 $T_{ij}(a)$, 我们将第 j 行乘以 a 加到第 i 行上. 若我们对一个矩阵右乘 T_{ij} , 则我们将第 i 列乘以 a 加到第 j 列.

(ii) 若对一个矩阵左乘 S_{ij} , 我们交换第 i 行和第 j 行. 若我们对一个矩阵右乘 S_{ij} , 则我们交换第 i 列和第 j 列.

(iii) 若对一个矩阵左乘 $K_i(a)$, 我们将第 i 行乘以 a . 若对一个矩阵右乘 $K_i(a)$, 则我们将第 i 列乘以 a . 注意此时我们要求 a 是一个单位.

定义 21.3.2

我们称矩阵 $T_{ij}(a)$, S_{ij} 和 $K_i(a)$ 为 n 阶**初等方阵**.

由定义我们有如下命题:

命题 21.3.3

初等方阵都可逆.

PID 上的特殊操作

我们首先回顾一下关于 PID 的一些结论. 主理想整环是一个满足任意理想均为主理想的整环, 也即任意一个理想都是一个元素生成的理想.

对 D 中任意两个非零元素 a 和 b , 它们的最大公因子总是存在的, 记为

$$d = \gcd(a, b).$$

进一步, 我们可以证明

$$\langle d \rangle = \langle a \rangle + \langle b \rangle.$$

因此存在 $p, q \in D$, 满足

$$d = ap + bq.$$

我们记 $a = a'd$, $b = b'd$, 则可得 $1 = a'p + b'q$. 因此以下矩阵

$$\begin{bmatrix} p & -b' \\ q & a' \end{bmatrix}$$

的行列式可逆, 也等价于矩阵为可逆矩阵. 另一方面, 我们有

$$\begin{bmatrix} a & b \end{bmatrix} \begin{bmatrix} p & -b' \\ q & a' \end{bmatrix} = \begin{bmatrix} d & 0 \end{bmatrix}$$

PID 上矩阵的标准型(一): 存在性

下边我们希望在 D 是一个主理想环的时候重复以上讨论来定义任意 A 的标准型和秩. 特别地, 我们希望证明以下结论:

定理 21.3.4

设 $m, n \in \mathbb{N}^*$, 记 D 是一个 PID. 任取非零矩阵 $A \in D^{m \times n}$, 则存在

$$r \leq \min\{m, n\},$$

以及

$$d_1, \dots, d_r \in D^*,$$

满足

- 1) 若 $r > 1$, 则对任意 $1 \leq i \leq r-1$, 我们有 $d_i \mid d_{i+1}$;
- 2) A 等价于如下矩阵:

$$\Omega(A) = \begin{bmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & d_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}_{m \times n}.$$

定义 21.3.5

我们称 $\Omega(A)$ 为 A 的**标准型**, 并称 r 为 A 的**秩**, 记为 $r(A)$.

我们使用 D 上的 "消元法" 来证明这个定理. 注意到, 此时我们并没有所有元素都可逆这个条件. 我们在考虑非单位元相消的时候需要使用之前关于主理想整环的讨论.

在消元的过程中, 我们需要进行不只一步的运算. 我们需要一个指标来告诉我们消元的进展. 由于 D 是一个主理想环, 因此也是一个 UFD. 特别地, 任意 D 的非单位非零元素都可以写为有限多个不可约元素的乘积. 我们定义:

$$L: D^* \setminus U \rightarrow \mathbb{N}$$

$$x \mapsto L(x) := \text{考虑重数的前提下, } x \text{ 的不可约分解的因子个数.}$$

例 21.3.6.

设 $x \in D^* \setminus U$ 的一个不可约分解为 $p_1^{n_1} \cdots p_k^{n_k}$, 则 $L(x) = n_1 + \cdots + n_k$.

定义 21.3.7

我们称 $L(x)$ 为 x 的长度.

我们约定 D 中单位的长度为 0, 将长度映射扩展到 D^* , 并仍用 L 作为记号. 下边我们开始证明定理.

注 21.3.8.

这个程序与书上介绍的有所不同.

证明. 设 A 为一个 D 上 $m \times n$ 的矩阵. 我们按照以下规则进行消元. 为方便区分, 我们使用 $T_{ij}(a)$, S_{ij} 和 $K_i(a)$ 记 m 阶初等方阵, 使用 $T'_{ij}(a)$, S'_{ij} 和 $K'_i(a)$ 来记 n 阶初等方阵.

- (1) 找到 A 的一个非零元素, 利用 S_{ij} 和 S'_{ij} 将其换至 $(1, 1)$ 位置.
- (2) 由于 $a_{11} \neq 0$, 观察第一列剩下的元素是否为 0, 若都是 0, 进行 (4), 若不都是 0, 进行 (3).
- (3) 观察 $a_{21}, \dots, a_{m1}$. 设 a_{k1} 为第一个不为 0 的元素, 我们记 $b_k = \gcd(a_{11}, a_{k1})$, 若 $a_{11} \mid a_{k1}$, 利用初等矩阵将 a_{k1} 变为 0, 否则记

$$\begin{aligned} a_{11} &= a_{11}b_k \\ a_{k1} &= a'_{k1}b_k \\ 1 &= a'_{11}p_k + a'_{11}p_k \end{aligned}$$

我们将 m 阶单位阵中的 $(1, 1), (1, k), (k, 1), (k, k)$ 位置上的元素分别替换为 $p_k, q_k, -a'_{k1}, a'_{11}$, 得到矩阵 J_{k1} . 并记 $B_1 = J_{k1}A$, 来令 $(k, 1)$ 位置上元素变为 0. 并对 B_1 重复步骤 (3). 若所有元素均为 0, 则进行步骤 (4).

- (4) 观察 $a_{12}, \dots, a_{1m}$. 设 a_{1k} 为第一个不为 0 的元素, 我们记 $b_k = \gcd(a_{11}, a_{1k})$, 若 $a_{11} \mid a_{1k}$, 利用初等矩阵将 a_{1k} 变为 0, 否则并记

$$\begin{aligned} a_{11} &= a_{11}b_k \\ a_{1k} &= a'_{1k}b_k \\ 1 &= a'_{11}p_k + a'_{11}p_k \end{aligned}$$

我们将 m 阶单位阵中的 $(1, 1), (1, k), (k, 1), (k, k)$ 位置上的元素分别替换为 $p_k, -a'_{1k}, q_k, a'_{11}$, 得到矩阵 J_{1k} . 并记 $B_1 = AJ_{k1}$, 并对 B_1 重复步骤 (4). 若第一列和第一行除了 a_{11} 之外都为 0, 进入 (5). 否则进行步骤 (2).

- (5) 观察不在第一行和第一列中的元素, 若存在不被 $(1, 1)$ 位置上的元素整除的元素, 则进行 (6), 否则进行 (7).
- (6) 设 (i, j) 满足 $i \neq 1$ 且 $j \neq 1$, 且 $a_{11} \nmid a_{ij}$. 利用 $T_{j1}(1)$ 将第 j 列加到第 1 列. 进行 (3).
- (7) 此时 a_{11} 为矩阵中所有元素的最大公约数. 且第一行和第一列除了 a_{11} 外均为 0. 我们考虑矩阵中去掉第一行和第一列的子矩阵. 若该子矩阵不存在或者为零矩阵, 程序终止, 否则对该子矩阵运行 (1).

这中间有多个循环, 我们需要说明这些循环会终止. 这是因为如果不终止, 则 $(1, 1)$ 位置上的元素的长度会持续下降, 由于长度是一个自然数, 如果不在大于 0 的时候终止, 我们得到 $(1, 1)$ 位置上的元素长度为 0, 因此是一个单位, 整除所有元素. 因此有限步后循环需要终止. 最终, 我们得到了所需要的形式. $\square$

PID 上矩阵的标准型(二): 唯一性

我们注意到在寻找矩阵标准型的过程中, 特别是消元的过程中, 我们做了一些选择. 例如, 如果 $(1, 1)$ 位置为 0, 我们把哪个非零元送到 $(1, 1)$ 位置, 消元的时候我们可以先考虑行再考虑列, 也可以先考虑列在考虑行, 实际上仔细考虑证明过程, 我们也可以混合起来考虑. 所以我们会有一个很自然的疑问: 所得的标准型是否依赖于以上操作过程中所作的选择, 即一个矩阵的标准型是否是唯一的?

在本节最后的部分, 我们将证明 PID 上矩阵的标准型是唯一的. 具体叙述如下:

定理 21.3.9 (教材定理 3.2.6)

给定矩阵 A , 其标准型在相伴意义下唯一. 也即若 A 有以下两个标准型

$$\begin{bmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & d_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}_{m \times n}, \quad \begin{bmatrix} d'_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d'_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & d'_s & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}_{m \times n}.$$

满足我们有 $r = s$, 且对任意 $1 \leq i \leq r$, $d_i \sim d'_i$.

定义 21.3.10

矩阵 A 的标准型中的元素 $d_1, \dots, d_r$ 被称为 A 的**不变因子**.

注 21.3.11.

由以上定理, 我们知道不变因子是在相伴意义下良定义的.

该定理可以看作是以下讨论的一个推论. 我们首先给出一些定义. 设 A 为 D 上一个 $m \times n$ 矩阵.

定义 21.3.12

任取 $1 \leq k \leq m$, 和 $1 \leq l \leq n$, 我们考虑其中的行 $i_1 < \cdots < i_k$ 和列 $j_1 < \cdots < j_l$. 将这些行列相交位置上元素拿出来构成的矩阵被称为 A 的一个 $k \times l$ **子矩阵**, 也即如下矩阵

$$\begin{bmatrix} a_{i_1 j_1} & a_{i_1 j_2} & \cdots & a_{i_1 j_l} \\ a_{i_2 j_1} & a_{i_2 j_2} & \cdots & a_{i_2 j_l} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i_k j_1} & a_{i_k j_2} & \cdots & a_{i_k j_l} \end{bmatrix}_{k \times l}$$

定义 21.3.13

任取 $k \leq \min\{m, n\}$, 矩阵 A 的一个 k **阶子式** 为 A 的一个 $k \times k$ 子矩阵的行列式. 若该子矩阵的元素来自于行 $i_1 < \cdots < i_k$ 和列 $j_1 < \cdots < j_k$ 相交位置上的元素, 则我们记该 k -阶子式为

$$A \begin{pmatrix} i_1 \cdots i_k \\ j_1 \cdots j_k \end{pmatrix}.$$

定理 21.3.14 (Binet-Cauchy定理)

设 B 为 D 上的一个 $n \times s$ 矩阵, 并记 $C = AB$. 则

$$C \begin{pmatrix} i_1 \cdots i_k \\ j_1 \cdots j_k \end{pmatrix} = \sum_{s_1 < \cdots < s_k} A \begin{pmatrix} i_1 \cdots i_k \\ s_1 \cdots s_k \end{pmatrix} B \begin{pmatrix} s_1 \cdots s_k \\ j_1 \cdots j_k \end{pmatrix}.$$

证明. 注意到 D 上方阵的行列式也满足, 若方阵里有两行相同, 则行列式为 0. 利用这个观察, 我们将 $C \begin{pmatrix} i_1 \cdots i_k \\ j_1 \cdots j_k \end{pmatrix}$ 展开得到. $\square$

注 21.3.15.

若 $k = 1$, 则以上定理中的等式就是矩阵的乘法运算公式

$$c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}.$$

注 21.3.16.

我们注意到若 $1 \leq k \leq \min\{m, n\} - 1$, 且所有 k -阶子式均为 0, 则由行列式的计算方法, 我们有 A 的所有 $k+1$ 阶子式也均为 0. 我们称 A 的**秩**为

$$r := \max\{k \in \llbracket 1, \min\{m, n\} \rrbracket \mid \text{存在一个非零 } k \text{ 阶子式}\}.$$

我们将看到这个定义方法与前文给出的等价. 由于 D 是一个主理想整环, 我们可以讨论最大公因子.

定义 21.3.17

任取 $1 \leq k \leq r$, 我们称 A 的 k 阶行列式因子, 为其所有 k 阶子式的最大公因子, 记作 $\Delta_k(A)$.

注 21.3.18.

这个定义是在相伴意义下是合理的.

定理 21.3.19

记 $m, n \in \mathbb{N}^*$, 且 D 为一个 PID. 任取非零矩阵 $A, B \in D^{m \times n}$, 若 A 和 B 等价, 则

$$r(A) = r(B),$$

且对任意 $1 \leq k \leq r(A)$, 我们有

$$\Delta_k(A) \sim \Delta_k(B).$$

证明. 若矩阵 A 与 B 等价, 则存在可逆矩阵 $P \in D^{m \times m}$, $Q \in D^{n \times n}$, 使得

$$A = PBQ.$$

若 B 为零矩阵, 则由矩阵乘法可得 A 为零矩阵. 由于 P 和 Q 可逆, 我们有

$$B = P^{-1}AQ^{-1},$$

因此若 A 为零矩阵, 则 B 为零矩阵. 因此结论对 $r(A) = 0$ 的情形成立.

下设 A 和 B 非零. 我们记 $B_1 = PB$. 由定理 21.3.14, 我们知道

$$r(B_1) \leq r(B)$$

且对任意 $1 \leq k \leq r(B_1)$, 有

$$\Delta_k(B) \mid \Delta_k(B_1)$$

另一方面, 由于 P 可逆, 我们有 $B = P^{-1}B_1$. 因此同理有

$$r(B) \leq r(B_1)$$

且对任意 $1 \leq k \leq r(B)$, 有

$$\Delta_k(B_1) \mid \Delta_k(B)$$

因此有

$$r(B) = r(B_1),$$

且对任意 $1 \leq k \leq r(B)$, 有

$$\Delta_k(B) \sim \Delta_k(B_1).$$

对 A 和 B_1 做相同的讨论, 我们有

$$r(A) = r(B_1),$$

且对任意 $1 \leq k \leq r(A)$, 有

$$\Delta_k(A) \sim \Delta_k(B_1).$$

将以上所得结论放在一起, 我们有

$$r(A) = r(B),$$

且对任意 $1 \leq k \leq r(A)$ 有

$$\Delta_k(A) \sim \Delta_k(B).$$

□

引理 21.3.20

若 $\min\{m, n\} > 1$, 对任意 $1 \leq k \leq \min\{m, n\} - 1$, 我们有 $\Delta_k(A) \mid \Delta_{k+1}(A)$.

证明. 由使用行展开或列展开的方式计算行列式, 我们可以得到 $\Delta_k(A)$ 整除所有的 $k+1$ 阶子式. 由 $\Delta_{k+1}(A)$ 的极大性, 我们知道 $\Delta_k(A) \mid \Delta_{k+1}(A)$. □

定理 21.3.9 的证明. 设 A 等价于如下两个矩阵:

$$\begin{bmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & d_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}_{m \times n}, \quad \begin{bmatrix} d'_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d'_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & d'_s & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}_{m \times n}.$$

这两个矩阵的秩分别为 r 和 s . 由行列式因子的定义以及标准型的定义, 我们有

$$\begin{aligned} \Delta_1(A) &= d_1 = d'_1, \\ \Delta_2(A) &= d_1 d_2 = d'_1 d'_2, \\ &\dots \\ \Delta_r(A) &= d_1 \cdots d_r = d'_1 \cdots d'_r, \end{aligned}$$

等号是在相伴意义下成立. 因此, 我们有对任意 $1 \leq k \leq r$, 使得 $d_k \sim d'_k$, 且有 $d_k \Delta_k(A) = \Delta_{k+1}(A)$. □

对任意矩阵 $A \in D^{m \times m}$, 对任意 $1 \leq k \leq r(A)$, 我们记 $\Delta_k(A)$ 生成的 D 中的主理想为

$$I_k(A) := \langle \Delta_k(A) \rangle.$$

由以上讨论我们有如下推论:

推论 21.3.21

(i) 对任意矩阵 $A \in D^{m \times n}$, 若 $r(A) > 1$, 则对任意 $1 \leq k \leq r(A) - 1$, 我们有

$$I_k(A) \supset I_{k+1}(A).$$

(ii) 对任意矩阵 $A \in D^{m \times n}$, 对任意 $1 \leq k \leq r(A)$, 我们有

$$I_k(A^t) = I_k(A).$$

(iii) 对任意矩阵 $A \in D^{m \times n}$, $B \in D^{n \times s}$, 对任意 $1 \leq k \leq r(AB)$, 我们有

$$I_k(AB) \subset I_k(A) \cap I_k(B).$$

(iv) 对任意矩阵 $A, B \in D^{m \times n}$, 设 A 与 B 等价, 则对任意 $1 \leq k \leq r(A)$, 我们有

$$I_k(A) = I_k(B).$$

第二十二章 主理想整环上的有限生成模

我们首先回顾有限生成模的定义. 设 M 为一个 R -模. 取子集 $S \subset M$. 我们称 S 生成 M , 若我们有

$$\langle S \rangle = M.$$

若更进一步, 我们有 S 为一个有限集

$$S = \{x_1, \dots, x_n\},$$

则称 M 为一个有限生成模, 并称 $x_1, \dots, x_n$ 为 M 的一组生成元. 此时, 我们有

$$M = Rx_1 + \cdots + Rx_n.$$

我们将在本节讨论主理想整环上的有限生成模的性质. 特别的我们希望对这类模的结构做一个分类. 在本节的最后, 我们将给出这个分类结果的两个应用, 分别对应有有限生成交换群的分类以及向量空间上的线性变换的基本型描述两个问题.

在本节中, 若无特殊说明, 环 R 为一个主理想整环, 记为 D .

22.1 主理想整环上的自由模

设 M 为一个秩为 m 的 D -自由模.

定理 22.1.1

任意 M 的子模 N 也是一个自由模, 且其秩 n 满足 $0 \leq n \leq m$.

证明. 我们对 M 的秩使用归纳法. 设 M 的秩为 0. 则 $N = \{0\}$, 定理成立.

设定理对秩为 $m-1$ 的自由模的子模成立. 我们设 M 秩为 m . 设 $\{u_1, \dots, u_m\}$ 为 M 的一组基. 任取 M 的子模 N , 则其中元素 u 均可写为如下形式:

$$u = x_1 u_1 + \cdots + x_m u_m.$$

我们将 N 中所有元素的第一个坐标收集起来得到 D 的一个子集:

$$I_1 := \{x \in D \mid \exists u \in N, u = xu_1 + x_2 u_2 + \cdots + x_m u_m\}.$$

由于 N 为 M 的子模, 我们有 I_1 为 D 的一个理想, 因此存在一个元素 a_1 满足 $I_1 = \langle a_1 \rangle$. 特别地存在 N 中的元素 v_1 , 满足其第一个坐标为 a_1 :

$$v_1 = a_1 u_1 + x_2 u_2 + \cdots + x_m u_m.$$

我们记 M_1 为由 $u_2, \dots, u_m$ 生成的子模:

$$M_1 = Du_2 + \cdots + Du_m.$$

我们记 $N_1 = N \cap M_1$ 也是 M 的子模.

若 $a_1 = 0$, 我们有 $N = N_1 \subset M_1$. 由于 M_1 的秩为 $m-1$, 由归纳假设, N 是一个自由模且秩 n 满足 $1 \leq n \leq m-1 < m$.

若 $a_1 \neq 0$, 由于 D 为整环, 我们有 $bv_1 = 0$ 当且仅当 $b = 0$, 因此我们有

$$1) \ Dv_1 \cong D.$$

$$2) \ N = Dv_1 \oplus N_1.$$

由于 Dv_1 和 N_1 均为自由模, 因此 N 为自由模, 且满足

$$1 \leq r(N) = 1 + r(N_1) \leq m-1+1 = m.$$

因此, 定理得证. □

思考 22.1.2

构造一个自由模与其一个真子模秩相同的例子, 并考虑类似的例子为什么不存在于对线性空间的讨论中?

定理 22.1.3

设 M 和 N 为两个 D -自由模, 并设 $r(M) = m, r(N) = n$. 对任意的模同态

$$\varphi: M \rightarrow N,$$

存在 M 的一组基 $\mathcal{B} = \{u_1, \dots, u_m\}$ 和 N 的一组基 $\mathcal{C} = \{v_1, \dots, v_n\}$, 以及 D 中的元素 $d_1, \dots, d_r$, 满足

- 1) 若 $r > 1$, 则对任意 $1 \leq i \leq r-1, d_i \mid d_{i+1}$;
- 2) 对任意 $1 \leq i \leq r, \varphi(u_i) = d_i v_i$;
- 3) 若 $r < m$, 则对任意 $r < i \leq m, \varphi(u_i) = 0$.

证明. 任取 M 的一组基 $\mathcal{B}'$ 和 N 的一组基 $\mathcal{C}'$, 并记 A 为 φ 关于这两组基的矩阵. 因此 $A \in D^{n \times m}$. 由定理 21.3.4, 我们知道存在可逆矩阵 $P \in D^{m \times m}$ 以及 $Q \in D^{n \times n}$, 使得 QAP 为 A 的标准型.

我们记 $\mathcal{B} = \{u_1, \dots, u_m\}, \mathcal{C} = \{v_1, \dots, v_n\}$, 满足

$$[[u_1]_{\mathcal{B}'} \cdots [u_m]_{\mathcal{B}'}] = P, [[v_1]_{\mathcal{C}'} \cdots [v_n]_{\mathcal{C}'}] = Q^{-1},$$

即为满足定理要求的基底.

$$\begin{array}{ccc} (M, \mathcal{B}') & \xrightarrow{A} & (N, \mathcal{C}') \\ \uparrow P & & \downarrow Q \\ (M, \mathcal{B}) & \xrightarrow{QAP} & (N, \mathcal{C}) \end{array}$$

□

我们仍使用以上记号.

推论 22.1.4

模同态 φ 的像可以写为以下直和:

$$\varphi(M) = D(d_1 v_1) \oplus \cdots \oplus D(d_r v_r).$$

集合 $\{d_1 v_1, \dots, d_r v_r\}$ 构成 $\varphi(M)$ 的一组基.

推论 22.1.5

设 N 为 M 的一个非零子模, 我们可以找到 M 的一个基 $\{u_1, \dots, u_m\}$, 以及元素非零元素 $d_1, \dots, d_r \in D$, 满足

1) 对任意 $1 \leq i \leq r-1$, $d_i \mid d_{i+1}$;

2) $N = D(d_1 u_1) \oplus \cdots \oplus D(d_r u_r)$.

这里 $r = r(N)$.

证明. 我们考虑嵌入 N 到 M 的嵌入映射. 这是一个自由模之间的同态. 利用定理 22.1.3 及其推论, 我们得到以上结论. $\square$

22.2 主理想整环上的扭模

设 M 为一个交换幺环 R 上的模.

定义 22.2.1

设 $u \in M$, 我们定义其**零化子**为以下 R 的子集:

$$\text{ann}(u) := \{a \in R \mid au = 0\}.$$

如前文讨论, u 的零化子也可以看作是模同态:

$$\begin{aligned} \varphi_u : R &\rightarrow M \\ a &\mapsto au \end{aligned}$$

的核 $\ker \varphi_u$. 因此 $\text{ann}(u)$ 从模的角度看是 R 的子模, 从环的角度看是 R 的理想.

定义 22.2.2 (教材定义 3.4.4)

设 $u \in M^*$. 若 $\text{ann}(u) = \{0\}$, 我们称 u 为 M 的**自由元**. 若 $\text{ann}(u) \neq \{0\}$, 我们称 u 为 M 的**扭元**.

若 M 中没有扭元, 我们称 M 为一个**无扭模**. 若 M 所有元素都是扭元, 我们称 M 为一个**扭模**.

注 22.2.3.

自由模不一定是无扭模, 例如 $\mathbb{Z}_4$ 作为 $\mathbb{Z}_4$ -模是自由模, 但是有扭元 $\bar{2}$. 无扭模不一定是自由模, 例如 $\mathbb{Q}$ 作为一个 $\mathbb{Z}$ 模. 它不是自由模, 但是没有扭元.

设 D 为一个主理想整环, M 为一个 D -模.

定理 22.2.4 (教材定理 3.4.5)

若 M 是有限生成的, 则存在元素 $v_1, \dots, v_s \in M$, 使得 M 可以如下写为循环模的直和:

$$M = Dv_1 \oplus \cdots \oplus Dv_s,$$

并满足 $\text{ann}(v_1) \supset \text{ann}(v_2) \supset \cdots \supset \text{ann}(v_s)$.

证明. 设 M 为 $n \in \mathbb{N}^*$ 个元素生成的模:

$$M = Du_1 + \cdots + Du_n.$$

不妨设 $u_1, \dots, u_n$ 都不为 0. 考虑模满同态

$$\begin{aligned} \varphi: D^n &\rightarrow M, \\ (x_1, \dots, x_n) &\mapsto x_1u_1 + \cdots + x_nu_n, \end{aligned}$$

并记同态 φ 的核 $K = \ker \varphi$ 为 D^n 的子模.

若 $K = \{0\}$, 则 φ 为一个模同构, 因此 M 为一个自由模, 且 $\{u_1, \dots, u_n\}$ 为 M 的一组基. 特别地, $u_1, \dots, u_n$ 都是 M 上的自由元, 因此令

$$v_1 = u_1, \dots, v_n = u_n,$$

我们有

$$\text{ann}(v_1) = \cdots = \text{ann}(v_n) = \{0\}.$$

定理在此情况下成立.

下边假设 $K \neq \{0\}$. 由推论 22.1.5, 我们知道存在 D^n 一组基

$$\{\underline{x}_1, \dots, \underline{x}_n\}$$

以及 $r \in \mathbb{N}^*$, $d_1, \dots, d_r \in D^*$, 满足

- 1) 若 $r > 1$, 则对任意 $1 \leq i \leq r-1$, $d_i \mid d_{i+1}$;
- 2) $K = D(d_1\underline{x}_1) \oplus \cdots \oplus D(d_r\underline{x}_r)$.

由模同态定理我们知道 M 与商模 D^n/K 同构. 以下我们将研究 D^n/K 的结构.

$$\begin{array}{ccc} D^n & \xrightarrow{\varphi} & M \\ \pi \downarrow & \nearrow \bar{\varphi} & \\ D^n/K & & \end{array}$$

回顾: 设 M_1, M_2 为 M 的子模, 且 $M_1 + M_2 = M_1 \oplus M_2$. 设 $N_1 \subset M_1$, $N_2 \subset M_2$ 为子模, 则有 $(M_1 \oplus M_2)/(N_1 \oplus N_2) \cong (M_1/N_1) \oplus (M_2/N_2)$.

注意到 $D^n = D\underline{x}_1 \oplus \cdots \oplus D\underline{x}_n$. 同时

$$K = D(d_1\underline{x}_1) \oplus \cdots \oplus D(d_r\underline{x}_r) \oplus \{0\} \oplus \cdots \oplus \{0\}.$$

由于对任意 $1 \leq i \leq r$, $D(d_i\underline{x}_i) \subset D\underline{x}_i$, 且 $\{0\} \subset D\underline{x}_j$ 对任意 $1 \leq j \leq n$ 都成立, 我们有

$$M \cong D^n/K \cong D(\underline{x}_1 + Dd_1\underline{x}_1) \oplus \cdots \oplus D(\underline{x}_r + Dd_r\underline{x}_r) \oplus D\underline{x}_{r+1} \oplus \cdots \oplus D\underline{x}_n =: N.$$

任取 $1 \leq i \leq r$, 任取 $a \in D$, 满足

$$a(\underline{x}_i + Dd_i\underline{x}_i) = \underline{0} + Dd_i\underline{x}_i,$$

我们有

$$a\underline{x}_i \in Dd_i\underline{x}_i.$$

因此存在 $b \in D$, 满足

$$a\underline{x}_i = bd_i\underline{x}_i.$$

由于 $\underline{x}_i$ 为基元素, 特别地是一个自由元, 因此 $a = bd_i$, 即 $a \in \langle d_i \rangle$. 另一方面, 任取 $a \in D$, 我们有

$$ad_i\underline{x}_i + Dd_i\underline{x}_i = Dd_i\underline{x}_i.$$

因此

$$\text{ann}(\underline{x}_i + Dd_i\underline{x}_i) = \langle d_i \rangle.$$

此外, 我们还注意到以下命题等价:

- 1) $D(\underline{x}_i + Dd_i\underline{x}_i) = \{0\}$;
- 2) $\underline{x}_i \in K$;
- 3) d_i 为一个单位.

若 $d_1, \dots, d_r \in U$, 则

$$M \cong N = D\underline{x}_{r+1} \oplus \dots \oplus D\underline{x}_n,$$

为自由模. 我们记以上同构为

$$\varphi: M \rightarrow N,$$

记

$$v_1 = \varphi^{-1}(\underline{x}_{r+1})$$

...

$$v_{n-r} = \varphi^{-1}(\underline{x}_n)$$

即满足定理要求.

下设存在 $d_i \notin U$, 由于 $d_i \mid d_{i+1}$, 若 d_i 为一个单位, 那么对于任意 $j \leq i$, 我们有 d_j 也是一个单位.

记 t 为最小的满足 d_t 非单位下标. 我们记 M 到 N 的同构为 φ , 并记

$$v_1 = \varphi^{-1}(\underline{x}_t + Dd_t\underline{x}_t, 0, \dots, 0)$$

...

$$v_{r-t+1} = \varphi^{-1}(0, \dots, 0, \underline{x}_r + Dd_r\underline{x}_r, 0, \dots, 0)$$

$$v_{r-t+2} = \varphi^{-1}(0, \dots, 0, \underline{x}_{r+1}, 0, \dots, 0)$$

...

$$v_{n-t+1} = \varphi^{-1}(0, \dots, 0, \underline{x}_n)$$

由于

$$\langle d_t \rangle \supset \dots \supset \langle d_r \rangle \supset \{0\} = \dots = \{0\}$$

因此定理得证.

□

推论 22.2.5 (教材推论 3.4.6)

主理想环上的有限生成无扭模必为自由模.

注 22.2.6.

虽然 $\mathbb{Q}$ 是无扭模, 且不是自由模, 但这并不是以上推论的反例, 因为 $\mathbb{Q}$ 作为 $\mathbb{Z}$ 模不是有限生成的.

设 M 为一个有限生成模并有定理中的分解:

$$M = Dv_1 \oplus \cdots \oplus Dv_s.$$

我们记 $\text{ann}(v_i) = \langle d_i \rangle$. 由定理, 我们可以将 M 写成两个部分的直和:

$$M = \left(\bigoplus_{i=1}^k Dv_i \right) \oplus \left(\bigoplus_{i=k+1}^s Dv_i \right).$$

我们记第一部分为 M^T , 第二部分为 M^F . 我们注意形式上看这个分解是依赖于生成元的选取的.

命题 22.2.7

模 M^T 为一个由 k 个元素生成的扭模, 模 M^F 为一个秩为 $s - k$ 的自由模.

证明. 任取 $u \in M^T$, 存在 $x_1, \dots, x_k \in D$, 满足

$$u = x_1 v_1 + \cdots + x_k v_k.$$

注意到

$$\text{ann}(v_1) \supset \text{ann}(v_2) \supset \cdots \supset \text{ann}(v_k) \supsetneq \{0\}.$$

任取 $a \in \text{ann}(v_k)^*$, 我们有

$$au = x_1(av_1) + \cdots + x_k(av_k) = 0.$$

因此 M^T 为扭模.

注意到 M^F 为 $s - k$ 个秩为 1 的自由模的直和, 因此是秩为 $s - k$ 的自由模. $\square$

我们考虑 M 中所有扭元的集合:

$$\text{Tor}(M) := \{u \in M \mid \exists a \in D^*, au = 0\}.$$

命题 22.2.8

- 1) $\text{Tor}(M)$ 是 M 的一个子模.
- 2) 任取 M 的如上文定理中的分解, 我们有
 - (a) $M^T = \text{Tor}(M)$.
 - (b) $M^F \cong M/\text{Tor}(M)$.

证明. 任取 $u, v \in \text{Tor}(M)$, 存在 $a, b \in D^*$, 满足 $au = bv = 0$. 因此我们有 $ab \in D^*$, 且

$$ab(u - v) = b(au) - a(bv) = 0.$$

因此 $\text{Tor}(M)$ 为 M 的一个子群.

任取 $c \in D$, 我们有

$$a(cu) = c(au) = 0.$$

因此 $cu \in \text{Tor}(M)$, 所以 $\text{Tor}(M)$ 为 M 的子模.

之前已经证明了 M^T 为一个扭模. 因此

$$M^T \subset \text{Tor}(M).$$

下边证明另一个方向也成立. 任取 $u \in \text{Tor}(M)$, 由于

$$M = M^T \oplus M^F,$$

因此存在 $u_1 \in M^T, u_2 \in M^F$, 满足

$$u = u_1 + u_2.$$

由之前对 M^T 的讨论, 我们取 $a \in \text{ann}(d_k)^*$, 则有

$$au = au_1 + au_2 = au_2.$$

注意到若 $u_2 \neq 0$, 则 u_2 为自由元, 因此任取 $b \in D^*$, $bu \neq 0$.

假设 $u_2 \neq 0$, 若存在 $c \in D^*$, 满足 $cu = 0$, 我们有

$$0 = a(cu) = (ca)u = (ca)u_2.$$

注意到 $a, c \in D^*$, 因此 $ac \in D^*$, 进一步有 $acu_2 \neq 0$, 矛盾, 因此 u 为自由元.

由于 $u \in \text{Tor}(M)$, 因此 $u_2 = 0$, 即 $u \in M^T$. 由此可得

$$\text{Tor}(M) \subset M^T.$$

综上所述我们有

$$\text{Tor}(M) = M^T.$$

利用莫同态基本定理, 我们有

$$M^F \cong M/\text{Tor}(M).$$

□

以上证明说明一个扭元和一个自由元的和是自由元. 由以上命题, 我们有 M^T 是不依赖于分解的, 但是 M^F 的选取不唯一. 比如我们可以将 $v_{k+1}, \dots, v_s$ 都加上一个扭元 v_1 , 得到 $w_{k+1}, \dots, w_s$. 我们仍有

$$M = \left(\bigoplus_{i=1}^k Dv_i \right) \oplus \left(\bigoplus_{i=k+1}^s Dw_i \right).$$

另一方面, 任给 M 的如定理中的分解, 其自由模的部分在同构意义下是相同的 (都同构于 $M/\text{Tor}(M)$), 因此有相同的秩. 我们可以利用这个观察来如下定义模 M 的秩.

定义 22.2.9

任取分解 $M = M^T \oplus M^F$, 我们将 M^F 作为自由模的秩称为模 M 的秩

注 22.2.10.

我们可以将 M 的秩理解为其自由模部分的"大小". 由定理 22.2.4 的证明,

$$r(M) = r(D^n) - r(K).$$

22.3 主理想整环上的有限生成扭模

在定理 22.2.4 中, 我们看到对一个有限生成扭模 M , 我们可以找到一个分解

$$M = Dy_1 \oplus \cdots \oplus Dy_s,$$

满足 $\text{ann}(y_1) \supset \cdots \supset \text{ann}(y_s) \supsetneq \{0\}$.

记 $\text{ann}(y_i) = \langle d_i \rangle$, 我们有 $d_i \mid d_{i+1}$. 本节中, 我们希望研究此类分解在某种意义下的唯一性. 特别地, 我们希望研究元素 $d_1, \dots, d_s$ 在相伴意义下是否是唯一的.

注 22.3.1.

这里我们可能会有如下疑问. 不变因子来自于莫同态基本定理的应用, 即我们有

$$M \cong D^n/K,$$

利用 K 到 D^n 的嵌入来得到 $d_1, \dots, d_n$. 由于自由模之间同态映射的标准中的不变因子是唯一的, 似乎我们已经有了 M 的不变因子的唯一性. 但这里有一个问题, 若我们有另一个 D^n 的子模 L , 满足

$$M \cong D^n/L,$$

我们还不知道

$$D^n/K \cong D^n/L,$$

是否可以给出 $K \cong L$?

注意这个结论在一般情况下是不对的, 即若 M 为一个模, N_1 和 N_2 为 M 的两个子模满足

$$M/N_1 \cong M/N_2,$$

我们并不能说 $N_1 \cong N_2$. 例如考虑作为 $\mathbb{Z}$ 模的交换群 $M = \mathbb{Z}_4 \times \mathbb{Z}_2$, 我们记

$$\begin{aligned} N_1 &= \mathbb{Z}_4 \times \{\bar{0}\}, \\ N_2 &= (2\mathbb{Z}_4) \times \mathbb{Z}_2 \end{aligned}$$

注意到

$$M/N_1 \cong \mathbb{Z}_2 \cong M/N_2.$$

但是 N_1 是循环群, 而 N_2 不是循环群, 二者作为 $\mathbb{Z}$ -模是不同构的. (两个模之间的模同构映射首先是一个群同构映射)

即便是我们考虑自由模, 也可以构造出反例. 例如: 考虑

$$M = D^{\oplus \mathbb{N}}, N_1 = \{0\}, N_2 = D \oplus \{0\} \oplus \cdots$$

则

$$M \cong M/N_1 \cong M/N_2.$$

注意到我们考虑的情形中, $M = D^n$ 是一个秩有限的自由模.

我们回顾线性代数中的情形发现, 这个问题在讨论线性空间的时候是平凡的, 即若 V 为一个维数为 $n \in \mathbb{N}^*$ 的域 F 上的线性空间, W_1 和 W_2 为 V 中两个子空间, 满足

$$V/W_1 \cong V/W_2,$$

则有

$$W_1 \cong W_2.$$

教材中的思路就是将所考虑的 D 上自由模问题转化为某个域上线性空间中的问题来讨论. 具体操作来自于以下的观察.

注意到一个交换幺环关于一个极大理想的商环是一个域. 在之前的讨论中若 $u \in M$ 满足

$$\text{ann}(u) = \langle d \rangle,$$

则 Du 也可以看作是 D/Dd 上的模. 因此若 d 为一个不可约元素, 我们就有 D/Dp 为一个域. Du 可以看作是 D/D_p 上的线性空间. (比如: $\mathbb{Z}/3\mathbb{Z}$ 是一个域.)

PID 上有限生成模的 p -分支分解

以上分析涉及一个问题就是我们是否可以将 M 分解为一些零化子是由不可约元素 p 或者 p^k 生成的元素生成的循环群的直和. 以下引理可以帮助我们解决这个问题.

引理 22.3.2

设 $u \in M$, 且存在 D 中两个元素 a 和 b , 满足 $\text{ann}(u) = \langle ab \rangle$. 设 a 和 b 互素, 则子模 Du 有如下分解:

$$Du = D(au) \oplus D(bu),$$

并且 $\text{ann}(au) = \langle b \rangle$, $\text{ann}(bu) = \langle a \rangle$.

证明. 我们首先证明

$$Du = D(au) + D(bu).$$

由于 $D(au) \subset Du$, $D(bu) \subset Du$, 因此我们有

$$D(au) + D(bu) \subset Du.$$

由于 $1 \sim \text{gcd}(a, b)$, 存在 $p, q \in D$, 满足 $1 = pa + qb$. 因此

$$u = 1 \cdot u = (pa + qb)u = p(au) + q(bu) \in D(au) + D(bu),$$

因此

$$Du \subset D(au) + D(bu).$$

综上所述, 我们有

$$Du = D(au) + D(bu).$$

下边证明

$$D(au) + D(bu) = D(au) \oplus D(bu).$$

任取 $v \in D(au) \cap D(bu)$, 注意到 $(ab)v = 0$, 因此

$$av = bv = 0.$$

因此

$$v = 1 \cdot v = p(av) + q(bv) = 0.$$

因此

$$D(au) \cap D(bu) = \{0\},$$

等价地, 我们有

$$D(au) + D(bu) = D(au) \oplus D(bu).$$

最后关于两个元素 au 和 bu 的零化子结论的证明相似, 我们只给出证明 $\text{ann}(au) = \langle b \rangle$ 的证明.

任取 $c \in D^*$, 若存在 $d \in D$, 满足 $c = bd$, 则

$$c(au) = d(abu) = 0.$$

因此

$$c \in \text{ann}(u),$$

我们可得

$$\langle b \rangle \subset \text{ann}(u).$$

反过来, 任取 $c \in \text{ann}(au)$, 我们有

$$c(au) = 0,$$

因此

$$ac \in \text{ann}(u) = \langle ab \rangle$$

所以我们有 $ab \mid ac$. 由于 $a \neq 0$, 由 D 中消去律, 我们有 $b \mid c$. 因此

$$\text{ann}(au) \subset \langle b \rangle.$$

综上所述

$$\text{ann}(au) = \langle b \rangle.$$

□

由于 PID 中元素都有唯一的不可约分解, 因此我们有

推论 22.3.3

设 $u \in M$ 有零化子 $\text{ann}(u) = \langle d \rangle$, 其中 $d \in D^*$ 并有不可约因子分解

$$d = p_1^{k_1} \cdots p_m^{k_m},$$

其中 $p_1, \dots, p_m$ 为两两不相伴的不可约元素, $k_1, \dots, k_m \in \mathbb{N}^*$, 那么 M 的子模 Du 有分解:

$$Du = \bigoplus_{i=1}^m D \left(\prod_{\substack{j=1 \\ j \neq i}}^m p_j^{k_j} u \right).$$

进一步的, 任取 $1 \leq i \leq m$, 我们有

$$\text{ann} \left(\prod_{\substack{j=1 \\ j \neq i}}^m p_j^{k_j} u \right) = \langle p_i^{k_i} \rangle.$$

证明. (练习)

□

定义 22.3.4 (教材定义 3.4.8)

任给不可约元素 $p \in D$, 我们定义如下 M 中的子集为其 p -分支:

$$M_p := \{u \in M \mid \exists k \in \mathbb{N}^*, p^k u = 0\}.$$

若我们有 $M = M_p$, 则称 M 为一个 p -模.

注 22.3.5.

任取 p 不可约, 任取 M 为一个 D 模, M_p 都是良定义的. 区别只在于是不是等于 $\{0\}$.

引理 22.3.6

任给 D 中不可约元素 p , 如下两个叙述等价:

- 1) $u \in M_p$.
- 2) $\exists k \in \mathbb{N}, \text{ann}(u) = \langle p^k \rangle$.

注 22.3.7.

我们这里约定 $p^0 = 1$.

证明. (ii) $\implies$ (i) 由零化子的定义立得.

下边假设 $u \in M_p$, 因此存在 $l \in \mathbb{N}^*$, 满足

$$p^l u = 0.$$

我们记 $d \in D^*$, 满足

$$\text{ann}(u) = \langle d \rangle,$$

因此

$$d \mid p^l.$$

由于 p 不可约, 我们有

$$0 \leq k \leq l,$$

满足

$$\text{ann}(u) = \langle p^k \rangle.$$

□

注 22.3.8.

这里特别说明的是, $u = 0$ 当且仅当 $\text{ann}(u) = D = \langle 1 \rangle$.

扭模中关于不相伴的不可约元素的 p -分支有如下关系:

引理 22.3.9

记 M 为一个扭模, 任取两个 D 中的不可约元素 p 和 q , 假设 $\gcd(p, q) = 1$, 则

$$M_p \cap M_q = \{0\}.$$

证明. 任取 $u \in M_p \cap M_q$, 由之前的引理, 存在 $k, l \in \mathbb{N}$, 满足

$$\text{ann}(u) = \langle p^k \rangle = \langle q^l \rangle.$$

若 $k = 0$, 则 $\text{ann}(u) = D$, 因此 $l = 0$. 同理我们也有若 $l = 0$, 则 $k = 0$. 由之前注记, 我们知道此种情况发生当且仅当 $u = 0$.

若 $u \neq 0$, 则有 $k \neq 0$ 且 $l \neq 0$, 因此

$$q^l \mid p^k,$$

所以 $q \mid p^k$. 由于 q 为不可约元素, 也是素元素, 因此 $q \mid p$.

由于 q 和 p 都是不可约元素, 因此我们有 p 与 q 相伴, 与题设矛盾.

综上所述我们有

$$M_p \cap M_q = \{0\}.$$

□

之前的推论 22.3.3 告诉我们任给 M 中的一个扭元, 我们都可以将其唯一的写成一些 p 分支中元素的和. 我们使用推论 22.3.3 中的记号, 可以如下描述这个联系:

引理 22.3.10

$$D \left(\prod_{\substack{j=1 \\ j \neq i}}^m p_j^{k_j} y \right) = Dy \cap M_{p_i}.$$

证明. (练习)

□

注意到 D 上相伴给出了元素之间的等价关系, 任给元素 $a \in D$, 我们记 $[a]$ 为 D 中关于相伴关系的等价类, 并记

$$[D] := \{[a] \mid a \in D\}.$$

考虑 D 中的不可约元素, 我们记

$$[D]_{irr} := \{[p] \mid p \in D, p \text{ 不可约}\}.$$

命题 22.3.11

任意 D 上的有限生成扭模 M 存在以下分解

$$M = \bigoplus_{[p] \in [D]_{irr}} M_p.$$

注 22.3.12.

此结论对不是有限生成的扭模也成立.

由于 M 为有限生成扭模, 因此由定理 22.2.4, 我们可以找到一个分解

$$M = Du_1 \oplus \cdots \oplus Du_s,$$

满足

$$D \supsetneq \text{ann}(u_1) \supset \cdots \supset \text{ann}(u_s) \supsetneq \{0\}.$$

对任意 $1 \leq i \leq s$, 我们记

$$\text{ann}(u_i) = \langle d_i \rangle,$$

并设 d_s 有不可约分解

$$d_s = p_1^{n_{s1}} \cdots p_k^{n_{sk}}$$

由 $d_1, \dots, d_s$ 的关系, 我们有 $d_1, \dots, d_{s-1}$ 的分解:

$$d_1 = \epsilon_1 p_1^{n_{11}} \cdots p_k^{n_{1k}}$$

...

$$d_{s-1} = \epsilon_{s-1} p_1^{n_{(s-1)1}} \cdots p_k^{n_{(s-1)k}}$$

这里 $\epsilon_1, \dots, \epsilon_s$ 为单位, $n_{ij} \in \mathbb{N}$, 且满足对任意 $1 \leq j \leq k$, 我们有

$$n_{1j} \leq \cdots \leq n_{sj}.$$

对任意 $1 \leq i \leq s, 1 \leq j \leq k$, 我们记

$$u_{ij} = \prod_{\substack{l=1 \\ l \neq j}}^k p_l^{n_{il}} u_i$$

因此 $Du_{ij} = Du_i \cap M_{p_j}$.

定理 22.3.13 (教材定理 3.4.9)

任给一个非零的有限生成扭模 M , 存在一组两两不相伴的不可约元素

$$\{p_1, \dots, p_s\},$$

满足

$$M = M_{p_1} \oplus \cdots \oplus M_{p_s}.$$

且每一个分支都非零.

若存在另一组两两不相伴的不可约元素

$$\{q_1, \dots, q_t\},$$

使得

$$M = M_{q_1} \oplus \cdots \oplus M_{q_t},$$

且每一个分支都非零, 则我们有 $s = t$, 且在一个置换的前提下, $p_i \sim q_i$.

证明. 满足命题条件的一组两两不相伴不可约元素的存在性由命题之前的讨论保证. 我们下边将主要讨论唯一性.

任取 $z \in M_{q_1}$, 我们可以将其表示为 $z = y_1 + \cdots + y_s$, 满足 $\text{ann}(y_i) = \langle p_i^{k_i} \rangle$. 我们考虑

$$0 = q_1^{l_1} z = q_1^{l_1} y_1 + \cdots + q_1^{l_1} y_s$$

因此若 $y_i \neq 0$, 我们有 $q_1^{l_1} \mid p_i^{k_i}$. 因此 $\{q_1, \dots, q_t\} \subset \{p_1, \dots, p_s\}$. 类似地, 我们可以得到另一个方向的包含. 所以两个集合相等. $\square$

注 22.3.14.

以上证明也说明了任取 D 中不可约元素 p , 满足与 p_i 都不相伴, 则 $M_p = \{0\}$.

注 22.3.15.

到这里, 我们将 M 分解为有限多个 p -分支中的循环子模的直和, 并且证明了这样的分解是唯一的. 下边我们将利用这个结论来证明有限生成扭模的不变因子的唯一性. 过程共分两步, 第一步我们在 p -模中考虑这个问题, 第二步我们再考虑一般的有限生成扭模.

PID 上的有限生成 p -模分解的唯一性

设 p 为 D 的一个不可约元素, 我们首先考虑 M 为一个有限生成 p -模的情形. 由定理 22.2.4, 我们有如下命题.

命题 22.3.16

存在 $u_1, \dots, u_l \in M_p$, $k_1 \leq \dots \leq k_l \in \mathbb{N}^*$, 使得

$$M = Du_1 \oplus \dots \oplus Du_l.$$

且任取 $1 \leq i \leq l$, 我们有 $\text{ann}(u_i) = \langle p^{k_i} \rangle$.

定理 22.3.17

若 M 存在两个分解:

$$M = Du_1 \oplus \dots \oplus Du_s = Dv_1 \oplus \dots \oplus Dv_t,$$

我们有 $s = t$, 且对任意 $1 \leq i \leq s$, 有 $k_i = k'_i$.

证明. 不妨设 $s \leq t$. 我们对 $s \in \mathbb{N}^*$ 使用归纳法来证明.

设 $M = Du_1$. 我们考虑最小的 $n \in \mathbb{N}^*$, 满足 $p^n M = 0$. 即

$$\text{ann}(M) = \langle p^n \rangle.$$

注意到 $n = k_1 = k'_t$. 若 $t = 1$, 命题成立. 因此下设 $t > 1$, 我们将导出矛盾.

我们记

$$u_1 = \sum_{i=1}^t x_i v_i$$

若对任意 $1 \leq i \leq t$, 都有 $p \mid x_i$, 由 n 的定义, 我们知道

$$p^{n-1} u_1 = 0,$$

与 $n = k_1$ 矛盾.

另一方面, 由于 $p^{n-1} u_1 \neq 0$, 因此存在满足 $\text{ann}(v_j) = \langle p^n \rangle$ 的 v_j , 其系数 $x_j \neq 0$. 我们不妨设 $p \nmid x_t$, 由于 p 不可约, 则存在 $a, b \in D$ 满足

$$ap^n + bx_t = \gcd(p^n, x_t) = 1.$$

我们有

$$bu_1 + ap^n v_t = \sum_{i=1}^{t-1} bx_i v_i + (bx_t + ap^n) v_t.$$

因此, 我们有

$$v_t = bu_1 - \sum_{i=1}^{t-1} bx_i v_i.$$

因此

$$M = Du_1 + (Dv_1 \oplus \dots \oplus Dv_{t-1})$$

另一方面, 我们设

$$yu_1 + y_1v_1 + \cdots + y_{t-1}v_{t-1} = 0,$$

有

$$y \left(\sum_{i=1}^{t-1} x_i v_i + x_t v_t \right) + y_1 v_1 + \cdots + y_{t-1} v_{t-1} = 0.$$

因此 $(yx_t)v_t = 0$, 即 $p^n \mid yx_t$.

由于 $p \nmid x_t$, 因此 $p^n \mid y$, 从而得 $yu_1 = 0$ 以及

$$y_1v_1 + \cdots + y_{t-1}v_{t-1} = 0.$$

考虑直和 $Dv_1 \oplus \cdots \oplus Dv_{t-1}$, 可知对任意 $1 \leq i \leq t-1$, 有 $y_i v_i = 0$. 由此可知

$$M = Du_1 \oplus Dv_1 \oplus \cdots \oplus Dv_{t-1}.$$

因此我们有

$$\{0\} \cong M/Du_1 \cong Dv_1 \oplus \cdots \oplus Dv_{t-1}$$

这与 $t > 1$ 矛盾. 因此命题在 $s = 1$ 时成立.

我们假设结论对 M 可以表为至多 $s-1$ 个循环模的直和时, 结论成立. 我们考虑 s 个情况.

我们考虑最小的 $n \in \mathbb{N}$, 满足 $p^n M = 0$. 注意到 $n = k_s = k'_t$.

我们记

$$u_s = \sum_{i=1}^t x_i v_i.$$

同前文讨论, 我们可以设 $p \nmid x_t$, 则存在 $a, b \in D$ 满足

$$ap^n + bx_t = \gcd(p^n, x_t) = 1.$$

我们有

$$bu_s + ap^n v_t = \sum_{i=1}^{t-1} bx_i v_i + (bx_t + ap^n) v_t.$$

因此, 我们有

$$v_t = bu_s - \sum_{i=1}^{t-1} bx_i v_i.$$

因此

$$M = Du_s + (Dv_1 \oplus \cdots \oplus Dv_{t-1})$$

另一方面, 我们设 $yu_1 + y_1v_1 + \cdots + y_{t-1}v_{t-1} = 0$, 有

$$y \left(\sum_{i=1}^{t-1} x_i v_i + x_t v_t \right) + y_1 v_1 + \cdots + y_{t-1} v_{t-1} = 0.$$

因此 $(yx_t)v_t = 0$, 即 $p^n \mid yx_t$.

由于 $p \nmid x_t$, 因此 $p^n \mid y$, 从而得 $yu_s = 0$ 以及

$$y_1v_1 + \cdots + y_{t-1}v_{t-1} = 0.$$

考虑直和 $Dv_1 \oplus \cdots \oplus Dv_{t-1}$, 可知对任意 $1 \leq i \leq t-1$, 有 $y_i v_i = 0$. 由此可知

$$M = Du_s \oplus Dv_1 \oplus \cdots \oplus Dv_{t-1}.$$

因此我们有

$$Du_1 \oplus \cdots \oplus Du_{s-1} \cong M/Du_s \cong Dv_1 \oplus \cdots \oplus Dv_{t-1}$$

由归纳法得证. □

我们下边再给出教材中构造线性空间的利用维数讨论给出的证明 (包含在定理 3.4.10 的证明中).

教材中的定理 22.3.17 的证明. 任取 $k \in \mathbb{N}$, 我们定义

$$p^k M := \{p^k u \mid u \in M\}.$$

考虑 M 的分解, 我们有

$$\begin{aligned} M &= D(p^k u_1) \oplus \cdots \oplus D(p^k u_s) \\ &= D(p^k v_1) \oplus \cdots \oplus D(p^k v_t). \end{aligned}$$

考虑

$$n := \min\{l \in \mathbb{N} \mid p^l M = \{0\}\}$$

由条件知 n 存在, 且满足

$$n = k_s = k'_t.$$

因此我们有

$$M \supset pM \supset p^2 M \supset \cdots \supset p^{n-1} M \supsetneq p^n M = \{0\}.$$

任取 $0 \leq k \leq n-1$, 我们记

$$N_k := p^k M / p^{k+1} M.$$

注意到 N_k 可以看作一个 D/Dp 模. 由于 p 是一个不可约元素, 因此 D/Dp 是一个域, 因此 N_k 是一个 D/Dp 上的线性空间. 由于 M 是有限生成 D 模, 因此 N_k 是一个有限维线性空间, 并由如下分解

$$\begin{aligned} N_k &\cong D(p^k u_1)/D(p^{k+1} u_1) \oplus \cdots \oplus D(p^k u_s)/D(p^{k+1} u_s) \\ &\cong D(p^k v_1)/D(p^{k+1} v_1) \oplus \cdots \oplus D(p^k v_t)/D(p^{k+1} v_t). \end{aligned}$$

因此 N_k 的维数为其中不为 $\{0\}$ 的分支的数目. 因此我们有

$$\begin{aligned} \dim N_k &= \#\{i \mid k_i > k\} \\ &= \#\{i \mid k'_i > k\} \end{aligned}$$

注意到 $\dim N_k$ 不依赖于 M 的分解. 因此对任意 $k \in \mathbb{N}$,

$$k_1 \leq \cdots \leq k_s$$

和

$$k'_1 \leq \cdots \leq k'_t$$

满足

$$\#\{i \mid k_i > k\} = \#\{i \mid k'_i > k\}.$$

所以我们有 $s = t$, 且对任意 $1 \leq i \leq t$, 都有

$$k_i = k'_i.$$

□

PID 上一般有限生成扭模分解的唯一性

在证明了 D 上 p -模关于其不变因子的分解的唯一性之后, 我们将利用以上结果来讨论一般的有限生成扭模的分解的唯一性. 下设 M 为一个有限生成扭模. 我们考虑分解

$$\begin{aligned} M &= \bigoplus_{i=1}^s \left(\bigoplus_{j=1}^k Du_i \cap M_{p_j} \right) \\ &= \bigoplus_{j=1}^k \bigoplus_{i=1}^s Du_{ij} \end{aligned}$$

我们记 $\text{ann}(u_{ij}) = \langle p_j^{n_{ij}} \rangle$.

定义 22.3.18 (教材定理 3.4.11)

D 中的元素 $d_1, \dots, d_s$ 被称为 M 的**不变因子**; $p_1^{n_{11}}, \dots, p_k^{n_{sk}}$ 中不为 1 的元素被称为 M 的**初等因子**.

注 22.3.19.

若 M 为一个 p -模, 则其不变因子和初等因子相同. 换句话说, 将 M 每个 p -分支作为 p -模的不变因子收集起来就是 M 的所有的初等因子.

定理 22.3.20 (教材定理 3.4.11)

设 M 有两种分解

$$M = Du_1 \oplus \cdots \oplus Du_s = Dv_1 \oplus \cdots \oplus Dv_t$$

则我们有 $s = t$, 且不变因子满足对任意 $1 \leq i \leq s$, 都有 $d_i \sim d'_i$.

证明. 我们可以将 M 重写为

$$\begin{aligned} M &= \bigoplus_{i=1}^s \left(\bigoplus_{j=1}^k Du_i \cap M_{p_j} \right) & M &= \bigoplus_{i=1}^t \left(\bigoplus_{j=1}^l Dv_i \cap M_{p'_j} \right) \\ &= \bigoplus_{j=1}^k \left(\bigoplus_{i=1}^s Du_i \cap M_{p_j} \right) & &= \bigoplus_{j=1}^l \left(\bigoplus_{i=1}^t Dv_i \cap M_{p'_j} \right) \\ &= \bigoplus_{j=1}^k M_{p_j} & &= \bigoplus_{j=1}^l M_{p'_j} \end{aligned}$$

以上两种分解, 每个都给出了一个组初等因子, 由之前讨论的 p -分支分解的唯一性, 以及 p -模分解的不变因子的唯一性, 我们得到 M 分解的初等因子的唯一性.

我们进一步考虑初等因子和不变因子之间由以上分解得到的关系, 我们从初等因子出发构造不变因子的方法唯一(见证明后的注记), 因此不变因子唯一, 即 $s = t$, 且

$$d_1 \sim d'_1, \dots, d_s \sim d'_s.$$

□

注 22.3.21.

这里详细的说明一下如何从初等因子得到不变因子. 假设我们有如下初等因子

$$\begin{aligned} & p_1^{n_{11}}, \dots, p_1^{n_{1k_1}} \\ & \dots \\ & p_r^{n_{r1}}, \dots, p_r^{n_{rk_r}} \end{aligned}$$

其中 $p_1, \dots, p_s$ 为两两不相伴的不可约元素, 且所有的次数满足

$$\begin{aligned} & 0 < n_{11} \leq \dots \leq n_{1k_1} \\ & \dots \\ & 0 < n_{r1} \leq \dots \leq n_{rk_r} \end{aligned}$$

假设一共有 s 个不变因子, 我们从 d_s 开始构造. 令每行次数最大项相乘即得 d_s :

$$d_s = p_1^{n_{1k_1}} \dots p_r^{n_{rk_r}},$$

将出现在 d_s 中的初等因子删除, 考虑剩下的每行中次数最大项相乘即得 d_{s-1} :

$$d_{s-1} = p_1^{n_{1(k_1-1)}} \dots p_r^{n_{r(k_r-1)}}$$

因此进行下去可得所有不变因子. 例如, 若初等因子是

$$\begin{aligned} & p_1^2, p_1^5, \\ & p_2^3, p_2^3, p_2^4, \\ & p_3, p_3^2, \\ & p_4^3 \end{aligned}$$

则不变因子为

$$\begin{aligned} d_s &= p_1^5 p_2^4 p_3^2 p_4^3, \\ d_{s-1} &= p_1^2 p_2^3 p_3, \\ d_{s-2} &= p_2^3. \end{aligned}$$

注意到在此情况下 $s = 3$, 整理得

$$\begin{aligned} d_1 &= p_2^3, \\ d_2 &= p_1^2 p_2^3 p_3, \\ d_3 &= p_1^5 p_2^4 p_3^2 p_4^3. \end{aligned}$$

推论 22.3.22

D 上的有限生成模 M 的秩唯一, 且在相伴意义下, 其不变因子和初等因子唯一. 此外, 不变因子和初等因子相互决定.

推论 22.3.23 (推论 3.4.12)

我们记 M_1 和 M_2 为 D 上两个有限生成模. 以下叙述等价

- 1) $M_1 \cong M_2$;
- 2) M_1 和 M_2 有相同的秩和不变因子;
- 3) M_1 和 M_2 有相同的秩和初等因子.

22.4 主理想整环上的有限生成模结构定理的应用

有限生成交换群的分类

任给一个交换群 G , 我们可以将其看成一个 $\mathbb{Z}$ -模. 我们用加法记 G 中的运算. 由于 $\mathbb{Z}$ 为主理想整环, 我们有 G 关于不变因子的分解:

定理 22.4.1

存在 G 中元素 $u_1, \dots, u_s \in G^*$, 满足

$$G = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_s,$$

且

$$\text{ann}(u_1) \supset \cdots \supset \text{ann}(u_s).$$

我们考虑模同态

$$\varphi_{u_1} : \mathbb{Z} \rightarrow \mathbb{Z}u_1,$$

则存在一个整数 $d_1 \in \mathbb{Z} \setminus \{1, -1\}$, 有

$$\ker \varphi_{u_1} = \text{ann}(u_1) = \langle d_1 \rangle.$$

由模同态基本定理我们有

$$\mathbb{Z}_{d_1} = \mathbb{Z}/\langle d_1 \rangle \cong \mathbb{Z}u_1.$$

因此我们有如下推论.

推论 22.4.2

设 G 为一个有限生成的既有扭元又有自由元的交换群, 则存在自然数 $r \in \mathbb{N}^*$ 以及 $d_1, \dots, d_k \in \mathbb{N} \setminus \{0, 1\}$, 满足

$$G \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \uparrow} \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_k},$$

且对任意 $1 \leq i \leq k-1$, $d_i \mid d_{i+1}$.

我们也可以考虑 G 关于初等因子的分解:

推论 22.4.3

设 G 为一个有限生成的交换群. 那么存在自然数 $r, s_1, \dots, s_k \in \mathbb{N}^*$, 以及素数 $p_1 \leq \cdots \leq p_k$, 满足

$$G \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_r \oplus \mathbb{Z}_{p_1^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{s_k}}.$$

注 22.4.4.

我们之前曾经证明过任取自然数 $n \in \mathbb{N} \setminus \{0, 1\}$, 假设存在两个大于 1 的自然数 a 和 b , 满足 $\gcd(a, b) = 1$, 则

$$\mathbb{Z}_m \cong \mathbb{Z}_a \oplus \mathbb{Z}_b.$$

这个也可以看作是之前引理 22.3.2 的一个特例.

作为该定理的一个应用, 我们有如下结果

定理 22.4.5

设 $n = p_1^{m_1} \cdots p_k^{m_k}$ 为其素数分解. 在同构的前提下, 阶为 n 的有限交换群的个数为:

$$\prod_{i=1}^k \rho(m_i),$$

这里 $\rho(m_i)$ 是 m_i 的划分的个数.

证明. 设 G 为一个交换群, 满足 $|G| = n$. 对任意 $1 \leq i \leq k$, 我们记 G_i 为 G 的 Sylow p_i -子群.

我们考虑 G 的子群

$$G_1 + \cdots + G_k.$$

注意到任取 $1 \leq i \leq k$, 我们有

$$G_i \cap (G_1 + \cdots + \widehat{G_i} + \cdots + G_k) = \{e\},$$

这时由于 Lagrange 定理告诉我们群中元素的阶要整除群的阶, 因此以上交集集中的元素既要整除 $p_i^{m_i}$ (G_i 的阶), 又要整除

$$p_1^{m_1} \cdots \widehat{p_i^{m_i}} \cdots p_k^{m_k},$$

的一个因子 ($G_1 + \cdots + \widehat{G_i} + \cdots + G_k$ 的阶), 注意到

$$\gcd(p_i^{m_i}, p_1^{m_1} \cdots \widehat{p_i^{m_i}} \cdots p_k^{m_k}) = 1,$$

因此这个交集集中的元素的阶必须为 1, 也即是么元. 因此

$$G_1 + \cdots + G_k = G_1 \oplus \cdots \oplus G_k.$$

考虑到

$$|G_1 \oplus \cdots \oplus G_k| = n = |G|,$$

我们有

$$G = G_1 \oplus \cdots \oplus G_k.$$

下边证明对任意 p_i , 阶为 $p_i^{m_i}$ 的群在同构意义下有 $\rho(m_i)$ 即可. 注意到

$$\rho(m_i) = \#\{(n_1, \dots, n_r) \in \mathbb{N}^* \mid r \in \mathbb{N}^*, 0 < n_1 \leq \cdots \leq n_r, n_1 + \cdots + n_r = m_i\}.$$

利用 p 模关于不变因子(初等因子)分解的唯一性, 我们有以下结论

- 1) 任取阶为 $p_i^{m_i}$ 的交换群, 考虑不变因子中 p_i 的次数, 我们得到一个 m_i 的划分;
- 2) 两个阶为 $p_i^{m_i}$ 的交换群同构当且仅当给出的 m_i 的划分相同.

因此, 我们只需要证明任给 m_i 的划分 $(n_1, \dots, n_r)$, 我们都有一个阶为 $p_i^{m_i}$ 的交换群, 其给出的 m_i 的划分为 $(n_1, \dots, n_r)$. 实际上我们可以构造这样的交换群:

$$\mathbb{Z}_{p_i^{n_1}} \oplus \cdots \mathbb{Z}_{p_i^{n_r}}$$

因此阶为 $p_i^{m_i}$ 的交换群在同构意义下共有 $\rho(m_i)$ 种, 考虑之前 G 可以写为 Sylow 子群的直和, 阶为 n 的交换群在同构意义下共有

$$\prod_{i=1}^k \rho(m_i),$$

种.

□

例 22.4.6.

考虑 $n = 72$. 我们首先给出 n 的素数分解

$$n = 2^3 \times 3^2.$$

考虑 3 的划分共有如下三种

$$3 = 1 + 2 = 1 + 1 + 1,$$

另一方面 2 的划分共有两种

$$2 = 1 + 1.$$

因此我们有如下所有阶为 72 的交换群的列表

	2 的划分	3 的划分
$\mathbb{Z}_9 \oplus \mathbb{Z}_8$	2	3
$\mathbb{Z}_9 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$	2	1 + 2
$\mathbb{Z}_9 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	2	1 + 1 + 1
$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_8$	1 + 1	3
$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$	1 + 1	1 + 2
$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	1 + 1	1 + 1 + 1

例 22.4.7.

记 G 为一个阶为 p^2 的群, 其中 p 为素数. 我们首先证明这样的 G 都是交换群. 考虑 G 在 G 上的伴随作用, 我们有

$$p \mid |Z(G)|,$$

即 G 的中心 $Z(G)$ 的阶被 p 整除. 因此有 $|Z(G)| = p$ 或者 $|Z(G)| = p^2$.

若 $|Z(G)| = p^2$, 则 $G = Z(G)$, 即 G 交换. 若 $|Z(G)| = p$, 我们知道 $Z(G) \triangleleft G$, 因此考虑商群

$$G/Z(G),$$

我们有

$$|G/Z(G)| = p.$$

注意到阶为 p 的群都同构于循环群 $\mathbb{Z}_p$, 因此存在 $a, b \in G$, 满足

$$Z(G) = \langle a \rangle, \quad G/Z(G) = \langle bZ(G) \rangle,$$

因此

$$G = \{b^i a^j \mid i, j \in \mathbb{Z}\}.$$

由于 a 为中心元, 因此 $ab = ba$, 所以 G 的生成元交换, 因此 G 是交换群与 $|Z(G)| = p$ 矛盾. 综上所述 G 是一个交换群.

我们考虑 2 的划分, 则有 G 同构于 $\mathbb{Z}_{p^2}$ 或者 $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

向量空间上的线性变换的标准型

设 V 为域 F 上的 n -维向量空间, 其中 $n \in \mathbb{N}^*$. 我们记 $F[\lambda]$ 为 F 上的多项式环, $\text{End}(V)$ 为 V 上所有线性变换的集合. 我们知道 $F[\lambda]$ 为一个主理想整环, $\text{End}(V)$ 也是一个 F -线性空间, 维数为 n^2 . 此外考虑 V 上线性变换之间的加法和复合给出了 $\text{End}(V)$ 上一个幺环结构, 其中幺元为 Id_V (将所有向量 $v \in V$ 送到 v), 零元为 $\mathbf{0}$ (将所有向量送到零向量).

我们考虑 V 上的一个线性变换 $\mathcal{A}$. 任取多项式

$$f(\lambda) = a_0 + a_1 \lambda + \cdots + a_m \lambda^m \in F[\lambda],$$

我们考虑

$$f(\mathcal{A}) := a_0 Id_V + a_1 \mathcal{A} + \cdots + a_m \underbrace{\mathcal{A} \circ \cdots \circ \mathcal{A}}_{m\text{次}}.$$

另一方面线性变换的复合还是线性变换, 因此我们有 $f(\mathcal{A})$ 也是 V 上的一个线性变换. 对任意 $m \in \mathbb{N}^*$, 我们记

$$\mathcal{A}^m = \underbrace{\mathcal{A} \circ \cdots \circ \mathcal{A}}_{m\text{次}}.$$

注 22.4.8.

以上过程实际构造了如下映射

$$\begin{aligned} \Psi_{\mathcal{A}} : F[\lambda] &\rightarrow \text{End}(V), \\ f(\lambda) &\mapsto f(\mathcal{A}). \end{aligned}$$

注意到 $F[\lambda]$ 作为多项式环有一个环结构, 此外考虑加法和 F 纯量乘法还有一个 F -模结构. 另一方面, $\text{End}(V)$ 关于线性映射的加法和复合构成一个环, 同时如上所说也有一个 F -模结构. 如上定义的 $\Psi_{\mathcal{A}}$ 既是一个环同态也是一个模同态.

不过考虑哪种结构的同态, 我们考虑 $\Psi_{\mathcal{A}}$ 的核

$$\ker \Psi_{\mathcal{A}} := \{f(\lambda) \mid f(\mathcal{A}) = \mathbb{O}\}.$$

注意到

$$\ker \Psi_{\mathcal{A}} \subset F[\lambda],$$

是一个理想 (作为 $F[\lambda]$ -模(或者 F -模)是一个子模). 由于 $F[\lambda]$ 是一个 PID, 存在

$$d(\lambda) \in F[\lambda],$$

满足

$$\ker \Psi_{\mathcal{A}} = \langle d(\lambda) \rangle.$$

这里 $d(\lambda)$ 就是 $\mathcal{A}$ 的极小多项式.

我们考虑如下 V 上的 $F[\lambda]$ -模结构:

$$\begin{aligned} \Phi_{\mathcal{A}} : F[\lambda] \times V &\rightarrow V \\ (f(\lambda), u) &\mapsto f(\mathcal{A})(u) \end{aligned}$$

思考 22.4.9

比较 $\mathcal{A} = \mathbb{O}$ 时, $\Phi_{\mathcal{A}}$ 给出的 V 上的 $F[\lambda]$ -模结构和 V 上的 F -模结构.

命题 22.4.10

V 是一个 $F(\lambda)$ 上的扭模.

证明. 考虑 $\text{End}(V)$, 这是一个 n^2 维的 F -线性空间, 因此以下线性变换线性相关:

$$Id_V, \mathcal{A}, \mathcal{A}^2, \dots, \mathcal{A}^{n^2}.$$

因此存在一个非零多项式 $f(\lambda) \in F[\lambda]$, 满足 $f(\mathcal{A}) = \mathbb{O}$. 因此任给 $u \in V$, 存在非零多项式 $f(\lambda)$, 满足 $f(\lambda)u = 0$, V 为扭模. $\square$

注 22.4.11.

注意到 V 作为 F 模是自由模.

命题 22.4.12

V 为有限生成 $F[\lambda]$ -模.

证明. 由于 V 为一个 n -维 F -线性空间. 设

$$\{v_1, \dots, v_n\},$$

为 V 的一组基(作为 F -线性空间). 因此我们有

$$V = Fv_1 + \dots + Fv_n.$$

另一方面, 由模结构的定义我们有 $Fv_i \subset F[\lambda]v_i$, 因此我们有

$$V = F[\lambda]v_1 + \dots + F[\lambda]v_n.$$

因此 V 为 $F[\lambda]$ 上有限生成模. □

注 22.4.13.

注意在下边的讨论中, 我们时常需要同时考虑 V 上的 F -模结构和 $F[\lambda]$ -模结构.

因此我们可以对 V 作为有限生成 $F[\lambda]$ -扭模使用结构定理得到以下结论:

命题 22.4.14

线性空间 V 有如下分解

$$V = F[\lambda]u_1 \oplus \dots \oplus F[\lambda]u_s,$$

满足 $\text{ann}(u_1) \supset \text{ann}(u_2) \supset \dots \supset \text{ann}(u_s) \supsetneq \{0\}$.

思考 22.4.15

以上命题在 $\mathcal{A} = \mathbb{O}$ 时给出 V 怎样的分解?

对任意 $1 \leq i \leq s$, 我们记

$$d_i(\lambda) \in F[\lambda] \setminus F,$$

满足

$$\text{ann}(u_i) = \langle d_i(\lambda) \rangle.$$

若 $s > 1$, 则对任意 $1 \leq i \leq s-1$, 我们有

$$d_i(\lambda) \mid d_{i+1}(\lambda).$$

由于 F 为域, 我们可以取 $d_i(\lambda)$ 为首一多项式.

任取 $u \in V$, $f(\lambda) \in F[\lambda]$, 我们有

$$\mathcal{A}(f(\lambda)u) = \mathcal{A}(f(\mathcal{A})(u)) = (\lambda f(\lambda))u \in F[\lambda]u.$$

因此我们有如下引理:

引理 22.4.16

任取 $u \in V$, 子空间 $F[\lambda]u \subset V$ 为 $\mathcal{A}$ 的不变子空间.

注 22.4.17.

回顾: 任取线性空间 V 的子空间 W , 若 W 满足

$$\mathcal{A}(W) \subset W,$$

我们称 W 为 $\mathcal{A}$ 的一个不变子空间.

另一方面, 任取 $u \in V^*$, 我们记

$$f(\lambda) = a_0 + \cdots + a_m \lambda^m \in F[\lambda],$$

满足

$$\text{ann}(u) = \langle f(\lambda) \rangle,$$

则我们有如下引理:

引理 22.4.18

集合

$$\mathcal{B} = \{u, \lambda u, \dots, \lambda^{m-1}u\}$$

子空间 $F[\lambda]u$ 的一组 F -基 (作为 F 线性空间).

证明. 任取多项式 $g(\lambda) \in F[\lambda]$, 我们考虑带余除法

$$g(\lambda) = p(\lambda)f(\lambda) + r(\lambda).$$

满足 $\deg r(\lambda) < m$ 或者 $r(\lambda) = 0$. 因此

$$g(\lambda)u = r(\lambda)u.$$

由此, 我们有

$$F[\lambda]u = Fu + F(\lambda u) + \cdots + F(\lambda^{m-1}u).$$

另一方面, 设存在 $b_0, \dots, b_{m-1} \in F$, 满足

$$b_0 u + \cdots + b_{m-1} \lambda^{m-1} u = 0,$$

记

$$g(\lambda) = b_0 + \cdots + b_{m-1} \lambda^{m-1},$$

则 $g(\lambda)u = 0$, 因此

$$g(\lambda) \in \text{ann}(u) = \langle f(\lambda) \rangle.$$

注意到 $g(\lambda)u = 0$ 当且仅当

$$f(\lambda) \mid g(\lambda),$$

若 $g(\lambda)$ 非零, 则有 $\deg g(\lambda) \geq \deg f(\lambda)$, 矛盾.

由 $g(\lambda) = 0$, 我们有

$$b_0 = \cdots = b_{m-1} = 0,$$

因此 $\mathcal{B}$ 中向量 F -线性无关, 引理得证. □

因此任取 $1 \leq i \leq s$, $F[\lambda]u_i$ 是 $\mathcal{A}$ 的一个不变子空间. 我们记

$$d_i(\lambda) = a_0 + a_1\lambda + \cdots + a_{m_i-1}\lambda^{m_i-1} + \lambda_i^m,$$

并考虑 $F[\lambda]u_i$ 的基底

$$\mathcal{B}_i = \{u_i, \lambda u_i, \dots, \lambda^{m_i-1}u_i\}.$$

我们考虑 $\mathcal{A}$ 在 $F[\lambda]u_i$ 上的限制, 记为 $\mathcal{A}_i$. 由以上讨论, 我们有 $\mathcal{A}_i$ 在 $\mathcal{B}_i$ 下的矩阵为

$$B_i = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & -a_{m_i-3} \\ 0 & 0 & 0 & \cdots & 1 & 0 & -a_{m_i-2} \\ 0 & 0 & 0 & \cdots & 0 & 1 & -a_{m_i-1} \end{bmatrix} \quad (22.1)$$

定理 22.4.19 (定理 3.6.2)

设 V 为 F 上的有限维线性空间. 记 $\mathcal{A}$ 为 V 上的线性变换. 则存在 V 上的一组基

$$\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_s,$$

使得 $\mathcal{A}$ 在这组基下的矩阵表示为准对角矩阵

$$\begin{bmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_s \end{bmatrix}$$

B_i 为形如 (22.1) 的矩阵.

我们称这个矩阵为 $\mathcal{A}$ 的有理标准型.

推论 22.4.20

线性空间 V 作为 $F[\lambda]$ -模的不变因子的次数满足

$$\deg d_1(\lambda) + \cdots + \deg d_s(\lambda) = \dim_F V.$$

我们下边考虑 V 按照初等因子分解. 假设 F 为一个特征为 0 的代数闭域. 因此 $F[\lambda]$ 中的首一不可约元素形如 $\lambda - a$, 这里 $a \in F$.

命题 22.4.21

线性空间有如下分解

$$V = F[\lambda]w_1 \oplus \cdots \oplus F[\lambda]w_t,$$

满足 $\text{ann}(w_1) = \langle (\lambda - b_1)^{n_1} \rangle, \dots, \text{ann}(w_t) = \langle (\lambda - b_t)^{n_t} \rangle$.

我们重复以前的讨论可得, 任取 $1 \leq i \leq t$, $F[\lambda]w_i$ 是 $\mathcal{A}$ 的一个不变子空间. 我们下边将证明

引理 22.4.22

集合

$$\mathcal{C}_i = \{w_i, (\lambda - b_i)w_i, \dots, (\lambda - b_i)^{n_i-1}w_i\}$$

子空间 $F[\lambda]w_i$ 的一组 F -基 (作为 F 线性空间).

证明. 我们重复之前的证明知道

$$\{w_i, \lambda w_i, \dots, \lambda^{n_i-1}w_i\},$$

为 $F[\lambda]w_i$ 的一组基. 我们使用归纳法证明这组元素表示为 $\mathcal{C}_i$ 中元素的线性组合. 我们考虑 $\lambda^k w_i$, 其中 $0 \leq k \leq n_i - 1$, 对 k 做归纳. 首先 $k = 0$ 时, 由于 $w_i \in \mathcal{C}_i$, 我们有

$$w_i = w_i.$$

若 $k = 1$, 我们有

$$\lambda w_i = (\lambda - b_i)w_i + b_i w_i.$$

因此 $n_i = 1, 2$, 则结论得证. 下边假设 $n_i > 2$, 并假设结论对任意 $0 \leq k \leq n_i - 2$ 成立, 下边考虑 $1 \leq k \leq n_i - 1$, 考虑

$$\lambda^k w_i = (\lambda - b_i)^k w_i - \sum_{j=0}^{k-1} C_k^j (-b_j)^{k-j} \lambda^j w_i,$$

注意到等式右边第二个求和项是 $w_i, \dots, \lambda^{k-1}w_i$ 的 F 线性组合, 因此可以表示为 $\mathcal{C}_i$ 中元素的 F -线性组合, 又 $(\lambda - b_i)^k w_i \in \mathcal{C}_i$, 因此 $\lambda^k w_i$ 也可以被表达为 $\mathcal{C}_i$ 中元素的 F -线性组合. 因此

$$F[\lambda]w_i = Fw_i + F(\lambda - b_i)w_i + \dots + F(\lambda - b_i)^{n_i-1}w_i.$$

另一方面, 由于

$$|\{w_i, \lambda w_i, \dots, \lambda^{n_i-1}w_i\}| = n_i,$$

我们有

$$\dim_F F[\lambda]w_i = n_i,$$

而 $\mathcal{C}_i$ 有 n_i 个元素, 因此为 $F[\lambda]w_i$ 的一组基. □

我们考虑 $\mathcal{A}$ 在 $F[\lambda]w_i$ 上的限制, 记为 $\mathcal{A}'_i$. 由以上讨论, 我们有 $\mathcal{A}'_i$ 在 $\mathcal{C}_i$ 下的矩阵为

$$J_i = \begin{bmatrix} b_i & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & b_i & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & b_i & \cdots & 0 & 0 & \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & b_i & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & b_i & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & b_i \end{bmatrix}$$

我们称这样的矩阵为一个 **Jordan 块**.

定理 22.4.23 (定理 3.6.3)

设 V 为 F 上的有限维线性空间. 记 $\mathcal{A}$ 为 V 上的线性变换. 则存在 V 上的一组基

$$\mathcal{C} = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_t,$$

使得 $\mathcal{A}$ 在这组基下的矩阵为准对角矩阵

$$\begin{bmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_t \end{bmatrix}$$

其中 J_i 为 Jordan 块.

我们称这个矩阵为 $\mathcal{A}$ 的 **Jordan 标准型**.

若域 F 不是代数封闭的, 则有可能存在次数大于 1 的不可约多项式. 设

$$p(\lambda) = a_0 + a_1\lambda + \cdots + a_m\lambda^m \in F[\lambda],$$

为一个不可约多项式. 我们假设 $u \in V^*$ 的零化子满足

$$\text{ann}(u) = \langle p(\lambda)^k \rangle,$$

其中 $k \in \mathbb{N}^*$.

我们可以考虑以下 $F[\lambda]u$ 中的元素构成 F -基:

$$\{u, \lambda u, \dots, \lambda^{m-1}u, p(\lambda)u, \lambda p(\lambda)u, \dots, \lambda^{m-1}p(\lambda)u, p(\lambda)^2u, \dots, p(\lambda)^{k-1}u\}.$$

则 V 上的线性变换 $\mathcal{A}$ 限制在 $F[\lambda]u$ 上得到的 $F[\lambda]u$ 上的线性变换在以上基下的矩阵表示为:

$$\begin{bmatrix} B & & & & \\ E_{1m} & B & & & \\ & E_{1m} & B & & \\ & & \ddots & \ddots & \\ & & & E_{1m} & B \\ & & & & E_{1m} & B \end{bmatrix}_{mk \times mk}$$

其中

$$B = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & -a_{m-2} \\ 0 & 0 & \cdots & 1 & -a_{m-1} \end{bmatrix}_{m \times m} \quad E = \begin{bmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \end{bmatrix}_{m \times m}$$

计算 V 的不变因子

我们仍考虑 F 上的 $n \in \mathbb{N}^*$ 维线性空间 V . 记

$$\mathcal{B} = \{v_1, \dots, v_n\},$$

为 V 作为 F -线性空间的一组基. 记 $\mathcal{A}$ 为 V 上的线性变换, 我们记

$$A = (a_{ij})_{n \times n},$$

为 $\mathcal{A}$ 在 $\mathcal{B}$ 下的矩阵表示.

注 22.4.24.

回顾: (F -线性空间) 我们考虑 $\mathcal{B}$ 中元素在 $\mathcal{A}$ 下的像:

$$\mathcal{A}(v_i) = a_{1i}v_1 + \cdots + a_{ni}v_n.$$

因此我们有

$$A = [\mathcal{A}]_{\mathcal{B}} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

为 $\mathcal{A}$ 在 $\mathcal{B}$ 下的矩阵表示. 该矩阵将每个向量 v 在 $\mathcal{B}$ 下的坐标 $[v]_{\mathcal{B}}$ (列向量) 送到 $\mathcal{A}(v)$ 在 $\mathcal{B}$ 下的坐标 $[\mathcal{A}(v)]_{\mathcal{B}}$ (列向量).

考虑由 $\mathcal{A}$ 给出 V 上的 $F[\lambda]$ -模结构. 注意到

$$V = F[\lambda]v_1 + \cdots + F[\lambda]v_n.$$

设

$$\{\underline{x}_1, \dots, \underline{x}_n\},$$

为 $F[\lambda]^n$ 作为 $F[\lambda]$ -模的一组基. 记满同态

$$\varphi : F[\lambda]^n \rightarrow V,$$

满足对任意 $1 \leq i \leq n$, 有

$$\varphi(\underline{x}_i) = v_i.$$

我们记 $K = \ker \varphi$. 由模同态基本定理, 我们有 $F[\lambda]$ -模同构:

$$F[\lambda]^n / K \cong V.$$

注 22.4.25.

我们在对一般的 PID 上有限生成模的讨论中曾得到如下结果:

记 D 为一个 PID, 任取 D 模 M , 设存在模满同态

$$\psi : D^n \rightarrow M,$$

其中 $n \in \mathbb{N}^*$, 则

$$n = r(\ker \psi) + r(M).$$

注意到作为 $F[\lambda]$ -模, V 为扭模, 因此 $r(K) = n$.

对任意 $1 \leq i \leq n$, 我们定义

$$\underline{y}_i = \lambda \underline{x}_i - \sum_{j=1}^n a_{ji} \underline{x}_j,$$

或者说

$$\begin{bmatrix} \underline{y}_1 & \cdots & \underline{y}_n \end{bmatrix} = \begin{bmatrix} \underline{x}_1 & \cdots & \underline{x}_n \end{bmatrix} (\lambda I_n - A) = \begin{bmatrix} \underline{x}_1 & \cdots & \underline{x}_n \end{bmatrix} \begin{bmatrix} \lambda - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \lambda - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & \lambda - a_{nn} \end{bmatrix}$$

定理 22.4.26 (定理 3.6.1)

$\{\underline{y}_1, \dots, \underline{y}_n\}$ 构成 K 作为 $F[\lambda]$ -自由模的一组基.

证明. 我们要说明以下三件事情:

- 1) $\{\underline{y}_1, \dots, \underline{y}_n\} \subset K$;
- 2) $\{\underline{y}_1, \dots, \underline{y}_n\}$ 可以 $F[\lambda]$ -生成 K ;
- 3) $\{\underline{y}_1, \dots, \underline{y}_n\}$ 是 $F[\lambda]$ -线性无关的.

1) 对任意 $1 \leq i \leq n$, 我们有如下计算:

$$\begin{aligned} \varphi(\underline{y}_i) &= \lambda \varphi(\underline{x}_i) - \sum_{j=1}^n a_{ji} \varphi(\underline{x}_j) \\ &= \lambda v_i - \sum_{j=1}^n a_{ji} v_j \\ &= \mathcal{A}(v_i) - \sum_{j=1}^n a_{ji} v_j = 0 \in V. \end{aligned}$$

因此 $\underline{y}_i \in K$.

2) 为了证明 $\underline{y}_1, \dots, \underline{y}_n$ 是 K 的一组生成元(作为 $F[\lambda]$ -模), 我们只需证明任取 $\underline{x} \in K$, 存在

$$f_1(\lambda), \dots, f_n(\lambda) \in F[\lambda],$$

满足

$$\underline{x} = f_1(\lambda) \underline{y}_1 + \cdots + f_n(\lambda) \underline{y}_n.$$

注意到 $\underline{x}_1, \dots, \underline{x}_n$ 为 $F[\lambda]^n$ 的一组基, 我们有

$$\underline{x} = g_1(\lambda) \underline{x}_1 + \cdots + g_n(\lambda) \underline{x}_n,$$

其中

$$g_1(\lambda), \dots, g_n(\lambda) \in F[\lambda].$$

若对任意 $1 \leq i \leq n$, 有 $g_i(\lambda) = b_i \in F$, 则有

$$0 = \varphi(\underline{x}) = b_1 v_1 + \cdots + b_n v_n.$$

由于 $\{v_1, \dots, v_n\}$ 为 V 的一组 F -基, 因此

$$b_1 = \cdots = b_n = 0,$$

我们有

$$\underline{x} = 0.$$

令

$$f_1(\lambda) = \cdots = f_n(\lambda) = 0,$$

即满足要求.

下边假设存在 $1 \leq i \leq n$, $\deg g_i(\lambda) > 0$. 我们将在 $\underline{x}$ 的表达式中逐渐尝试加入 $\underline{y}_1, \dots, \underline{y}_n$, 并使得 $\underline{x}_1, \dots, \underline{x}_n$ 的系数多项式的次数最大值下降.

注意到

$$\lambda \underline{x}_1 = \underline{y}_1 + \sum_{j=1}^n a_{j1} \underline{x}_j,$$

我们记

$$g_1(\lambda) = b_{01} + h_1(\lambda)\lambda.$$

因此

$$\begin{aligned} g_1(\lambda) \underline{x}_1 &= (b_{01} + h_1(\lambda)\lambda) \underline{x}_1 \\ &= b_{01} \underline{x}_1 + h_1(\lambda)(\underline{y}_1 + \sum_{j=1}^n a_{j1} \underline{x}_j) \\ &= (b_{01} + h_1(\lambda)a_{11}) \underline{x}_1 + \sum_{j=2}^n (a_{j1} h_1(\lambda)) \underline{x}_j + h_1(\lambda) \underline{y}_1 \end{aligned}$$

对任意 $g_i(\lambda)$ 做如上操作, 我们有

$$\underline{x} = (h_1(\lambda) \underline{y}_1 + \cdots + h_n(\lambda) \underline{y}_n) + \sum_{j=1}^n (b_{0j} + \sum_{i=1}^n h_i(\lambda) a_{ji}) \underline{x}_j.$$

我们观察以上表达式中 $\underline{x}_1, \dots, \underline{x}_n$ 的系数多项式的次数最大值, 有

$$\begin{aligned} &\max\{\deg(b_{0j} + \sum_{i=1}^n h_i(\lambda) a_{ji}), \dots, \deg(b_{0j} + \sum_{i=1}^n h_i(\lambda) a_{ji})\} \\ &\leq \max\{\deg h_1(\lambda), \dots, \deg h_n(\lambda)\} \\ &\leq \max\{\deg g_1(\lambda), \dots, \deg g_n(\lambda)\} - 1. \end{aligned}$$

我们下边考虑

$$\underline{x}' = \underline{x} - (h_1(\lambda) \underline{y}_1 + \cdots + h_n(\lambda) \underline{y}_n),$$

表达为

$$\{\underline{x}_1, \dots, \underline{x}_n\},$$

的线性组合的表达式

$$\underline{x}' = \sum_{j=1}^n (b_{0j} + \sum_{i=1}^n h_i(\lambda) a_{ji}) \underline{x}_j.$$

注意到 $\underline{x}' \in K$.

如果 $\underline{x}'$ 在

$$\{\underline{x}_1, \dots, \underline{x}_n\},$$

下的坐标都在 F 中, 则由第一种情况的证明知, $\underline{x}' = 0$, 我们有

$$\underline{x} = h_1(\lambda) \underline{y}_1 + \cdots + h_n(\lambda) \underline{y}_n.$$

否则, 我们重复以上过程得到 $\underline{x}''$, 并且其在基

$$\{\underline{x}_1, \dots, \underline{x}_n\},$$

下的坐标多项式次数最大值严格小于 $\underline{x}'$ 的坐标多项式的次数最大值.

不断重复以上过程, 注意到多项式的次数是有限, 且是自然数, 因此经过有限次之后, 以上过程终止, 存在多项式 $f_1(\lambda), \dots, f_n(\lambda) \in F[\lambda]$, 满足

$$\underline{x} - \sum_{i=1}^n f_i(\lambda) \underline{y}_i = \sum_{i=1}^n b_i \underline{x}_i,$$

对任意 $1 \leq i \leq n$, $b_i \in F$. 重复第一种情况的证明, 我们有

$$b_1 = \dots = b_n = 0.$$

因此

$$\underline{x} = \sum_{i=1}^n f_i(\lambda) \underline{y}_i.$$

3) 我们假设有 $l_1(\lambda), \dots, l_n(\lambda) \in F[\lambda]$, 满足

$$l_1(\lambda) \underline{y}_1 + \dots + l_n(\lambda) \underline{y}_n = 0$$

考虑 $\underline{y}_1, \dots, \underline{y}_n$ 在基底 $\underline{x}_1, \dots, \underline{x}_n$ 下的表达式, 我们将上式左边表达为 $\underline{x}_1, \dots, \underline{x}_n$ 的线性组合, 则有

$$\begin{cases} l_1(\lambda) \lambda = a_{11} l_1(\lambda) + \dots + a_{n1} l_n(\lambda) \\ \dots \\ l_n(\lambda) \lambda = a_{1n} l_1(\lambda) + \dots + a_{nn} l_n(\lambda) \end{cases}$$

注意到若 $l_1(\lambda), \dots, l_n(\lambda)$ 不全为 0, 等号左边的多项式的次数的最大值比等号右边多项式次数的最大值大 1, 矛盾. 因此 $\{\underline{y}_1, \dots, \underline{y}_n\}$ 是 $F[\lambda]$ -线性无关的. $\square$

我们记

$$\mathcal{C}_K = \{\underline{y}_1, \dots, \underline{y}_n\}, \quad \mathcal{C} = \{\underline{x}_1, \dots, \underline{x}_n\}$$

注意到 K 到 $F[\lambda]^n$ 的嵌入同态

$$\iota: K \rightarrow F[\lambda]^n,$$

在 $\mathcal{C}_K$ 和 $\mathcal{C}$ 下的矩阵表示为 $\lambda I_n - A$

$$\lambda I_n - A: (K, \mathcal{C}_K) \rightarrow (F[\lambda]^n, \mathcal{C}),$$

因此 V 作为 $F[\lambda]$ -模的不变因子就是 $\lambda I_n - A$ 的非单位的不变因子. 具体地说, 注意到 V 是一个扭模, 注意到作为 $F[\lambda]$ -模, 我们有如下秩的关系

$$r(F[\lambda]^n) - r(K) = r(V) = 0,$$

因此 $r(K) = n$, 即 K 为一个秩为 n 的 $F[\lambda]$ -自由模. 这个由定理 3.6.1 的结论也可以得到 (我们找到了一个 n 个元素的基). 因此 $\lambda I_n - A$ 有 n 个不变因子, 即其标准型 D 在 $0 < s < n$ 时为,

$$D = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & d_1(\lambda) & & \\ & & & & \ddots & \\ & & & & & d_s(\lambda) \end{bmatrix}_{n \times n}$$

在 $s = n$ 时为

$$D = \begin{bmatrix} d_1(\lambda) & & \\ & \ddots & \\ & & d_s(\lambda) \end{bmatrix}_{n \times n}.$$

其中

$$d_1(\lambda) \mid \cdots \mid d_s(\lambda).$$

另一方面, 由于 $\lambda I_n - A$ 与 D 等价, 即存在 $F[\lambda]$ 上的可逆 n 阶方阵 P 和 Q , 满足

$$\lambda I_n - A = PDQ,$$

因此

$$\det(\lambda I_n - A) = \det P \det D \det Q.$$

注意到 $F[\lambda]$ 上方阵可逆当且仅当方阵的行列式在 $F[\lambda]$ 中可逆, 即为 $F[\lambda]$ 中的单位 ($F[\lambda]$ 的单位群为 $U = F^*$), 因此

$$\det(\lambda I_n - A) \sim \det D = d_1(\lambda) \cdots d_s(\lambda),$$

即二者在 F 中相伴.

综上所述, 我们可以通过将 $\lambda I_n - A$ 化为标准型来找到 V 的不变因子, 也可以直接计算 $\lambda I_n - A$ 的行列式因子, 通过行列式因子与不变因子的关系来得到 V 的不变因子.

Cayley-Hamilton 定理

记 $d_1(\lambda), \dots, d_s(\lambda)$ 为 V 作为 $F[\lambda]$ -模的不变因子 (设为首一), 则我们有

$$\det(\lambda I_n - A) = d_1(\lambda) \cdots d_s(\lambda).$$

注意到右边多项式零化 V , 即 $d_1(A) \cdots d_s(A)$ 是零线性映射 (将所有向量送到零向量), 且

$$\text{ann}(V) = \langle d_s(\lambda) \rangle.$$

取定 $V = F^n$, 考虑任意 $A \in F^{n \times n}$ 为 F 上 n 阶方阵, 将 F^n 中元素记为列向量, 左乘 A 给出 F^n 上一个线性映射:

$$\begin{aligned} L_A : F^n &\rightarrow F^n, \\ u &\mapsto Au, \end{aligned}$$

且 $L_A = 0$ 当且仅当 $A = O_{n \times n}$ 为零矩阵. 以上讨论可以帮助我们证明 Cayley-Hamilton 定理:

定理 22.4.27 (Cayley-Hamilton 定理)

记 F 为一个域, 任取 F 上 $n \in \mathbb{N}^*$ 阶方阵 A , 考虑 F 上多项式

$$f(\lambda) = \det(\lambda I_n - A),$$

我们有

$$f(A) = O_{n \times n}.$$

证明. 我们考虑 F^n 的 F -基

$$\{e_1, \dots, e_n\},$$

其中对任意 $1 \leq i \leq n$, 有

$$e_i = (0, \dots, 0, \underset{i}{1}, 0, \dots, 0)^t,$$

则左乘 A 给出的线性变换在这组基下的矩阵表示就是 A , 利用之前的讨论即得结论. $\square$

注 22.4.28.

我们来看一下在这个证明过程中我们都经历了什么. 我们的出发点实际上是一个观察: V 上的线性映射空间 $\text{End}(V)$ 是一个有限维的 F -线性空间, 同时也是一个环(关于复合运算封闭). 利用这两点, 我们就可以得到 $f(\lambda) \in F[\lambda]^*$, 满足

$$f(\mathcal{A}) = \mathbb{O}.$$

另一方面由于 V 是有限维 F -线性空间, 放在一起我们有 V 是一个有限生成的 $F[\lambda]$ -扭模.

由之前关于 PID 上的有限生成模结构定理, 我们得到 V 的一个关于不变因子的分解. 在寻找这些不变因子的过程中, 我们首先注意到 V 同构于为 $F[\lambda]^n$ 关于某个子模 K 的商模, 而 V 的不变因子正是 K 到 $F[\lambda]^n$ 的嵌入同态的非单位的不变因子. 在构造这个同构的过程中, 我们选取 V 的一组 F -基 $\mathcal{B}$, 以及 $F[\lambda]^n$ 的一组 $F[\lambda]$ -基 $\mathcal{C}$, 由此, 我们得到 K 和所研究的线性变换 $\mathcal{A}$ 在 $\mathcal{B}$ 下的矩阵表示 A .

在研究 K 到 $F[\lambda]^n$ 的嵌入的过程中, 我们注意到如果

$$\mathcal{C} = \{\underline{x}_1, \dots, \underline{x}_n\},$$

则

$$[\underline{x}_1, \dots, \underline{x}_n](\lambda I_n - A)$$

给出 K 的一组基, 因此矩阵

$$\lambda I_n - A,$$

是 K 到 $F[\lambda]^n$ 的嵌入同态在某些基下的矩阵表示. 由此, 我们将 $\lambda I_n - A$ 与 V 作为 $F[\lambda]$ -模的不变因子联系起来. (注意 φ 依赖于 $\mathcal{B}$ 和 $\mathcal{C}$, 因此 $K = \ker \varphi$ 也依赖于 $\mathcal{B}$ 和 $\mathcal{C}$.)

由于 V 是扭模, 因此 $\lambda I_n - A$ 化为标准型之后, 对角线上没有 0 (否则 V 有自由元的部分), 所以 $\det(\lambda I_n - A)$ 相伴于所有不变因子的乘积 (在 $F[\lambda]$ 中), 而不变因子的乘积零化 V , 因此 $f(\lambda) = \det(\lambda I_n - A)$ 零化 V , 即

$$f(\mathcal{A})(V) = \{0\}.$$

因此

$$f(\mathcal{A}) = \mathbb{O}.$$

注意到以上都是线性变换, 我们考虑线性变换在 $\mathcal{B}$ 下的矩阵表示, 则有

$$f(A) = [f(\mathcal{A})]_{\mathcal{B}} = O_{n \times n}.$$

以上讨论是对任取 V 的线性映射 $\mathcal{A}$ 成立. 注意到通过考虑 V 中元素在 $\mathcal{B}$ 下的坐标, 我们有 $\text{End}(V)$ 和 $F^{n \times n}$ 之间的双射, 因此任取 A 我们都可以找到一个 $\mathcal{A}$ 满足 $[\mathcal{A}]_{\mathcal{B}} = A$. 所以我们得到了以上 Cayley-Hamilton 定理. (这里也可以看出定理叙述的矩阵之间的关系, 实际上是线性变换之间的关系在任取一组基下的矩阵体现.)

注 22.4.29.

任取 $A, B \in F^{n \times n}$, 考虑 A 和 B 左乘给出的线性变换 L_A 和 L_B , 则有

$$L_B \circ L_A = L_{BA}.$$

注 22.4.30.

考虑 $\lambda I_n - A$ 的非单位不变因子 $d_1(\lambda) \mid \cdots \mid d_s(\lambda)$ (首一), 我们有

$$f(\lambda) = d_1(\lambda) \cdots d_s(\lambda),$$

为 A 的特征多项式, 且 $d_s(\lambda)$ 为 A 的极小多项式.

第二十三章 模的张量积

从本章开始, 在以下三章中我们将研究幺环上的模的结构. 我们一方面将考虑如何从已有的模构造出新的模, 并且研究在某些情况下已有的模的性质是如何影响新构造的模的性质的; 另一方面, 我们也考虑如何从一个模出发, 通过研究其子模或者子模序列的性质来得到整个模的性质. 在本章中我们将讨论模的张量积.

23.1 模的系数环的扩张

记 S 为一个幺环, R 为 S 的一个包含幺元的子环. 记 M 为一个交换群. 设映射

$$\varphi : S \times M \rightarrow M$$

给出 M 一个左 S -模结构. 通过考虑 φ 在 $R \times M$ 上的限制, 我们可以给出 M 的一个左 R -模结构. 类似地, 通过对系数进行限制, 我们也可以从 M 上的一个右 S -模结构得到一个右 R -模结构.

反过来, 任给一个左 R -模 M , 我们可以考虑是否可以将该左 R -模结构扩展为一个左 S -模结构. 这个操作并不总是可行的. 例如 $\mathbb{Z}$ 是一个 $\mathbb{Z}$ -模, 但是上边没有 $\mathbb{Q}$ -模结构. 因此, 如果我们希望有这样的一个 S -模结构, 就需要考虑在 M 的基础上构造一个新的空间.

我们首先考虑如果这样的空间存在的话, 它需要满足什么条件. 记这个空间为 N . 首先这需要一个左 S -模, 因此是一个交换群, 并且需要满足左模的定义. 如果对任意 $s \in S$ 以及 $u \in M$, 我们都可以定义元素 $su \in N$. 并且任取 $s, t \in S, u, v \in M$, 我们有

$$\begin{aligned}(s+t)u &= su + tu, \\ s(u+v) &= su + sv, \\ (st)u &= s(tu), \\ 1u &= u,\end{aligned}$$

其中 $1 \in S$ 为幺元. 注意到任取 $s \in S, r \in R$, 以及 $u \in M$, 此时我们有 $ru \in M$, 最后一个条件可以写为

$$(sr)u = s(ru).$$

我们可以先考虑用 S 的元素和 M 的元素可以构造的最大的交换群, 然后商掉由上边所列的关系生成的正规子群来得到这样的一个交换群. 具体的构造过程如下.

考虑 $S \times M$ 生成的自由交换群, 记作

$$\mathbb{Z}^{\oplus S \times M} := \{f : S \times M \rightarrow \mathbb{Z} \mid f \text{ 在至多有限多个 } S \times M \text{ 的元素上取值非 } 0\}.$$

注 23.1.1.

这里 $\mathbb{Z}^{\oplus S \times M}$ 和 $S \oplus M$ 不同. 集合 $S \times M$ 给出 $\mathbb{Z}^{\oplus S \times M}$ 一个生成元组, 其中的元素除了满足交换的关系外没有其它的关系. 而在 $S \oplus M$ 中, 我们有加法运算.

在以下的讨论中, 我们记 $\mathbb{Z}^{S \times M}$ 中的元素为

$$\sum_{i=1}^n m_i(s_i, u_i),$$

其中 $n \in \mathbb{N}^*$, $m_1, \dots, m_n \in \mathbb{Z}$, $(s_1, u_1), \dots, (s_n, u_n) \in S \times M$. 记 H 为其中由以下形式的元素生成的子群

$$\begin{aligned} (s+t, u) - (s, u) - (t, u), \\ (s, u+v) - (s, u) - (s, v), \\ (sr, u) - (s, ru), \end{aligned}$$

其中 $s, t \in S, r \in R, u, v \in M$. 我们记 H 对应的商群为

$$S \otimes_R M := \mathbb{Z}^{\oplus S \times M} / H,$$

并记 $\mathbb{Z}^{S \times M}$ 到 $S \otimes_R M$ 的自然同态为 π .

定义 23.1.2

我们称商群 $S \otimes_R M$ 为环 S 和左 R -模 M 过环 R 的**张量积**, 并称其中的元素称为**张量**.

任取 $(s, u) \in \mathbb{Z}^{\oplus S \times M}$, 我们及其对应的商群的元素为 $s \otimes_R u$, 并称此类元素为**简单张量**.

注 23.1.3.

简单张量构成张量积 $S \otimes_R M$ 作为群的生成元. 之后我们会通过具体的例子来说明不是所有的张量都可以表达为简单张量.

由其构造, 我们可以验证 $S \otimes_R M$ 中有如下运算. 任取 $s, t \in S, r \in R$ 以及 $u, v \in M$, 我们有

$$\begin{aligned} (s+t) \otimes_R u &= s \otimes_R u + t \otimes_R u, \\ s \otimes_R (u+v) &= s \otimes_R u + s \otimes_R v, \\ sr \otimes_R u &= s \otimes_R ru, \\ 0_S \otimes_R u &= s \otimes_R 0_M = 0_S \otimes_R 0_M. \end{aligned}$$

考虑 S 上的乘法运算, 我们也可以验证以下映射给出了 $S \otimes_R M$ 上的一个自然的左 S -模结构:

$$\begin{aligned} \Phi : S \times (S \otimes_R M) &\rightarrow S \otimes_R M, \\ \left(s, \sum_{i=1}^n s_i \otimes_R u_i \right) &\mapsto \sum_{i=1}^n (ss_i) \otimes_R u_i. \end{aligned}$$

命题 23.1.4

由 Φ 给出的 $S \otimes_R M$ 上的左模结构定义良好.

证明. 我们首先验证 Φ 为一个映射, 即 Φ 的定义不依赖于 $S \otimes_R M$ 中元素的代表元的选取.

任给 $s \in S$, 任取 $(t, u) \in S \times M$, 我们将其送到 $t \otimes_R u \in S \otimes_R M$, 由自由交换群的泛性质, 我们有以下群同态:

$$\begin{aligned} \tilde{\varphi}_s: \mathbb{Z}^{S \times M} &\rightarrow S \otimes_R M, \\ \sum_{i=1}^n m_i(s_i, u_i) &\mapsto \sum_{i=1}^n m_i(ss_i) \otimes_R u_i. \end{aligned}$$

我们考虑 H 的生成元在 $\tilde{\varphi}$ 下的像. 任取 $t, t_1, t_2 \in S, r \in R, u, u_1, u_2 \in M$, 我们有

$$\begin{aligned} (st_1 + st_2, u) - (st_1, u) - (st_2, u) &\in H, \\ (st, u_1 + u_2) - (st, u_1) - (st, u_2) &\in H, \\ (s(tr), u) - (st, ru) &\in H, \end{aligned}$$

因此 $\tilde{\varphi}_s(H) = \{0\} < S \otimes_R M$, 进而有 $H < \ker \tilde{\varphi}_s$. 由此存在群同态 φ_s 满足以下交换图

$$\begin{array}{ccc} \mathbb{Z}^{S \times M} & \xrightarrow{\tilde{\varphi}_s} & S \otimes_R M \\ \pi \downarrow & \nearrow \varphi_s & \\ S \otimes_R M & & \end{array}$$

因此任取 $s \in S, \alpha \in S \otimes_R M$, 我们有

$$\Phi(s, \alpha) = \varphi_s(\alpha).$$

由此可得 Φ 作为映射定义良好.

下边验证 Φ 给出了 $S \otimes_R M$ 上的一个左 S -模结构. 由于对任意 $s \in S$, 都有 φ_s 为一个群同态, 又由于简单张量生成 $S \otimes_R M$, 我们只需考虑简单张量即可.

任取 $s, s_1, s_2 \in S$ 以及 $t \otimes_R u, t_1 \otimes_R v_1, t_2 \otimes_R v_2 \in S \otimes_R M$, 我们依次验证

$$\begin{aligned} (s_1 + s_2)(t \otimes_R u) &= (s_1 s_2)(t \otimes_R u) \\ &= ((s_1 + s_2)t) \otimes_R u = (s_1 s_2)t \otimes_R u \\ &= (s_1 t + s_2 t) \otimes_R u = s_1(s_2 t) \otimes_R u \\ &= s_1 t \otimes_R u + s_2 t \otimes_R u, &= s_1((s_2 t) \otimes_R u), \\ s(t_1 \otimes_R v_1 + t_2 \otimes_R v_2) &= st_1 \otimes_R v_1 + st_2 \otimes_R v_2 \\ 1(t \otimes_R u) &= t \otimes_R u. \end{aligned}$$

□

注 23.1.5.

我们称左 S -模 $S \otimes_R M$ 是由左 R -模系数扩张得到的. 由于 R 为 S 的子环, 因此 $S \otimes_R M$ 也是一个左 R -模.

我们考虑一个平凡的例子. 考虑环 R 为一个左 R -模, 则我们有 $S \otimes_R R$. 注意到任给 $(s, r) \in S \oplus R$, 我们有

$$s \otimes_R r = sr \otimes_R 1.$$

因此任给 $S \otimes_R R$ 中的元素

$$\sum_{i=1}^n s_i \otimes_R r_i,$$

我们有

$$\sum_{i=1}^n s_i \otimes_R r_i = \sum_{i=1}^n s_i r_i \otimes_R 1 = \left(\sum_{i=1}^n s_i r_i \right) \otimes_R 1.$$

到这里, 我们似乎看到 S 和 $S \otimes_R R$ 之间有一个同构. 但是要说明这点就需要说明任取 $s \in S^*$, 我们有

$$s \otimes_R 1 \neq 0 \in S \otimes_R R.$$

类似地, 我们也可以考虑 M 到 $S \otimes_R M$ 的自然映射

$$\begin{aligned} \iota_M : M &\rightarrow S \otimes_R M, \\ u &\mapsto 1 \otimes_R u. \end{aligned}$$

我们可以证明这个映射是一个 R -模同态. 接着我们会有一个自然的问题: 这个同态是一个同构么? 或者从 R -模的角度, 我们是不是总是可以把 M 看作是 $S \otimes_R M$ 的一个子模.

这个问题的答案是不一定. 我们可以考虑 $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_3$. 注意到任取 $m \in \mathbb{Z}$, 我们有

$$1 \otimes_{\mathbb{Z}} [m]_3 = \frac{1}{3} \otimes_{\mathbb{Z}} [3m]_3 = \frac{1}{3} \otimes_{\mathbb{Z}} [0]_3 = 0.$$

另一方面, 若我们取 $M = R$, 则有

$$\begin{aligned} \iota_R : R &\rightarrow S \otimes_R R, \\ r &\mapsto 1 \otimes_R r. \end{aligned}$$

这个似乎是一个单射. 综合这些观察, 我们需要找到一些方法来判断一个张量是否为 0. 然而, 这个工作在一般情况下是比较复杂的.

我们下边介绍一个对这部分讨论非常有用的一个工具. 我们通常称之为张量积的泛性质. 我们这里给出的是这个性质在系数扩张这个特殊情况下的叙述.

定理 23.1.6 (模系数扩张的泛性质)

记 S 为一个幺环以及 R 为 S 的一个包含幺元的子环. 记 M 为一个左 R -模, N 为一个左 S -模.

- 1) 任给左 R -模同态 $\varphi : M \rightarrow N$, 存在唯一的一个左 S -模同态

$$\Phi : S \otimes_R M \rightarrow N,$$

满足 $\varphi = \Phi \circ \iota_M$;

- 2) 任给左 S -模同态 $\Phi : S \otimes_R M \rightarrow N$, 则 $\varphi = \Phi \circ \iota_M$ 为一个 M 到 N 的 R -模同态.

注 23.1.7.

我们也可以用 1) 来定义 $S \otimes_R M$, 即定义其为满足泛性质的左 S -模. 由于泛性质, 这样的模在同构意义下唯一. 当然如果使用这个定义, 我们仍需要之前的构造来说明满足泛性质的左 S -模是存在的.

证明. 1) 设 $\varphi : M \rightarrow N$ 为一个左 R -模同态. 任取 $(s, u) \in S \times M$, 我们将其送到 $s\varphi(u) \in N$, 利用自由交换群的泛性质, 我们有群同态:

$$\begin{aligned} \tilde{\Phi} : \mathbb{Z}^{S \times M} &\rightarrow N, \\ \sum_{i=1}^n m_i(s_i, u_i) &\mapsto \sum_{i=1}^n m_i s_i \varphi(u_i). \end{aligned}$$

任取 $s, s_1, s_2 \in S, r \in R, u, u_1, u_2 \in M$, 以及 $v, v_1, v_2 \in N$, 我们有

$$\begin{aligned} \tilde{\Phi}(s_1 + s_2, u) &= (s_1 + s_2)\varphi(u) = s_1\varphi(u) + s_2\varphi(u) = \tilde{\Phi}(s_1, u) + \tilde{\Phi}(s_2, u), \\ \tilde{\Phi}(s, u_1 + u_2) &= s\varphi(u_1 + u_2) = s\varphi(u_1) + s\varphi(u_2) = \tilde{\Phi}(s, u_1) + \tilde{\Phi}(s, u_2), \\ \tilde{\Phi}(sr, u) &= sr\varphi(u) = s\varphi(ru) = \tilde{\Phi}(s, ru). \end{aligned}$$

因此 $\ker \pi < \ker \tilde{\Phi}$. 利用群同态基本定理, 我们有群同态

$$\begin{aligned} \Phi : S \otimes_R M &\rightarrow N, \\ \sum_{i=1}^n s_i \otimes_R u_i &\mapsto \sum_{i=1}^n s_i \varphi(u_i). \end{aligned}$$

任取 $s \in S$ 以及 $\sum_{i=1}^n s_i \otimes_R u_i \in S \otimes_R M$, 我们有

$$\Phi \left(s \sum_{i=1}^n s_i \otimes_R u_i \right) = \Phi \left(\sum_{i=1}^n s s_i \otimes_R u_i \right) = \sum_{i=1}^n s s_i \varphi(u_i) = s \left(\sum_{i=1}^n s_i \varphi(u_i) \right) = s \Phi \left(\sum_{i=1}^n s_i \otimes_R u_i \right).$$

因此 Φ 是一个左 S -模同态.

我们继续验证 $\varphi = \Phi \circ \iota_M$. 任取 $u \in M$, 我们有

$$(\Phi \circ \iota_M)(u) = \Phi(1 \otimes_R u) = 1\varphi(u) = \varphi(u),$$

因此等式成立.

最后证明 Φ 的唯一性. 注意到作为左 S -模, $\iota_M(M)$ 是 $S \otimes_R M$ 的生成元集. 因此任何一个从 $S \otimes_R M$ 出发的模同态都有 $\iota_M(M)$ 中元素的像决定. 由于任取满足条件的 Φ , 我们都有

$$\Phi \circ \iota_M = \varphi,$$

因此 Φ 唯一.

2) 由于 R 为 S 的子环, 因此通过限制系数, 任意左 S -模也是左 R -模, 同时任意左 S -模同态也是左 R -左同态. 考虑同态映射的复合仍是同态, 若存在左 S -模同态 $\Phi : S \otimes_R M \rightarrow N$, 由于 ι_M 为一个左 R -模同态, 我们有复合

$$\varphi := \Phi \circ \iota_M : M \rightarrow N,$$

为一个左 R -模同态. □

利用泛性质, 我们可以证明以下 S 和 $S \otimes_R R$ 的关系.

推论 23.1.8

我们有左 S -模同构 $S \cong S \otimes_R R$.

证明. 我们考虑 R 到 S 的嵌入映射

$$\begin{aligned} \varphi : R &\rightarrow S, \\ r &\mapsto r. \end{aligned}$$

这是一个左 R -模同态.

考虑定理 23.1.6 的证明中的构造, 我们知道存在左 S -模同态

$$\begin{aligned}\Phi : S \otimes_R R &\mapsto S, \\ \sum_{i=1}^n s_i \otimes_R r_i &\mapsto \sum_{i=1}^n s_i r_i,\end{aligned}$$

满足 $\varphi = \Phi \circ \iota_R$, 其中 ι_R 定义为

$$\begin{aligned}\iota_R : R &\mapsto S \otimes_R R, \\ r &\mapsto 1 \otimes_R r.\end{aligned}$$

由之前的讨论知道任取 $S \otimes R$ 的元素 $\sum_{i=1}^n s_i \otimes_R r_i$, 我们有

$$\sum_{i=1}^n s_i \otimes_R r_i = \left(\sum_{i=1}^n s_i r_i \right) \otimes_R 1.$$

因此我们有

$$S \otimes_R R = \{s \otimes_R 1 \mid s \in S\}.$$

由 Φ 的定义, 任取 $s \in S$, 我们有

$$\Phi(s \otimes_R 1) = s.$$

另一方面, 我们有左 S -模同态

$$\begin{aligned}\iota_S : S &\rightarrow S \otimes_R R, \\ s &\mapsto s \otimes_R 1.\end{aligned}$$

利用 Φ 和 ι_S 的定义, 我们可以得到复合 $\Phi \circ \iota_S$ 和 $\iota_S \circ \Phi$ 分别为 S 和 $S \otimes_R R$ 上的恒等映射. 因此 Φ 和 ι_S 均为左 S -模同构. 由此可得作为左 S -模, 我们有 $S \cong S \otimes_R R$. $\square$

我们可以进一步得到 $S \otimes_R R$ 中判断一个元素为 0 的等价条件.

推论 23.1.9

任取 $s \in S$, 元素 $s \otimes_R 1$ 为零张量当且仅当 $s = 0$.

使用类似的证明, 我们还可以考虑 S 和 R -自由模的张量积, 并得到类似的结论.

推论 23.1.10

任取 $n \in \mathbb{N}^*$, 我们有左 S -模同构 $S \otimes_R R^n \cong S^n$.

证明. 我们的证明与推论 23.1.8 的证明类似. 我们记 R^n 中的元素为

$$\underline{r} = (r_1, \dots, r_n) \in R^n,$$

记 S^n 中的元素为

$$\underline{s} = (s_1, \dots, s_n) \in S^n.$$

考虑 R^n 到 S^n 的自然嵌入:

$$\begin{aligned}\varphi : R^n &\rightarrow S^n, \\ \underline{r} &\mapsto \underline{r}.\end{aligned}$$

这是一个左 R -模同态.

考虑定理 23.1.6 的证明中的构造, 我们知道存在左 S -模同态

$$\begin{aligned}\Phi : S \otimes_R R^n &\mapsto S^n, \\ \sum_{i=1}^n s_i \otimes_R \underline{r}_i &\mapsto \sum_{i=1}^n s_i \underline{r}_i,\end{aligned}$$

满足 $\varphi = \Phi \circ \iota_{R^n}$, 其中 ι_{R^n} 定义为

$$\begin{aligned}\iota_{R^n} : R^n &\mapsto S \otimes_R R^n, \\ \underline{r} &\mapsto 1 \otimes_R \underline{r}.\end{aligned}$$

任取 $1 \leq i \leq n$, 我们记 $\underline{e}_i \in R^n$ 为第 i 个位置为 1, 其余位置为 0 的元素. 因此 $S \otimes_R R^n$ 中的简单张量有以下分解: 任取 $s \in S, \underline{r} = (r_1, \dots, r_n) \in R^n$,

$$\begin{aligned}s \otimes_R \underline{r} &= \sum_{i=1}^n s \otimes_R r_i \underline{e}_i \\ &= \sum_{i=1}^n sr_i \otimes_R \underline{e}_i.\end{aligned}$$

由 Φ 的定义, 任取 $s_1, \dots, s_n \in S$, 我们有

$$\Phi \left(\sum_{i=1}^n s_i \otimes_R \underline{e}_i \right) = (s_1, \dots, s_n) \in S^n.$$

另一方面, 我们可以定义一下映射

$$\begin{aligned}\Psi : S^n &\rightarrow S \otimes_R R^n, \\ (s_1, \dots, s_n) &\mapsto \sum_{i=1}^n s_i \otimes_R \underline{e}_i.\end{aligned}$$

直接计算可以验证 Ψ 是一个左 S -模. 利用 Φ 和 Ψ 的定义, 我们有 $\Phi \circ \Psi$ 和 $\Psi \circ \Phi$ 分别为 S^n 和 $S \otimes_R R^n$ 上的恒等映射. 因此 Φ 和 Ψ 均为 S -模同构. 作为左 S -模, 我们有 $S^n \cong S \otimes_R R^n$. $\square$

我们使用定理 23.1.6 来对 M 和 $S \otimes_R M$ 之间的关系做一个讨论.

推论 23.1.11

任取 M 到 $S \otimes_R M$ 的左 R -模同态 φ , 都存在一个左 S -模满同态

$$\psi : M / \ker \iota_M \rightarrow \operatorname{Im} \varphi,$$

即任意 φ 的像 $\operatorname{Im} \varphi$ 可以看作是 $M / \ker \iota_M$ 的商模.

注 23.1.12.

换句话说 $M / \ker \iota_M$ 是通过模同态将 M 送到 $S \otimes_R M$ 可以得到的最大的 $S \otimes_R M$ 的子模.

证明. 设 φ 为一个从 M 到 $S \otimes_R M$ 的左 R -模同态, 由定理 23.1.6, 存在一个左 S -模同态 Φ , 使得以下交换图成立

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & S \otimes_R M \\ & \searrow \iota_M & \uparrow \Phi \\ & & S \otimes_R M \end{array}$$

另一方面, 我们考虑对 ι_M 使用模同态基本定理, 则以上交换图可以扩展为

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & S \otimes_R M \\ \text{pr} \downarrow & \searrow \iota_M & \uparrow \Phi \\ M / \ker \iota_M & \xrightarrow{\iota_M} & S \otimes_R M \end{array}$$

其中 pr 为自然同态. 我们取 $\psi = \Phi \circ \overline{\iota_M}$ 即可. $\square$

注 23.1.13.

当我们做张量积 $S \otimes_R M$ 的时候, 有可能会有塌缩. 一个典型的例子就是 $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_n = \{0\}$. 以上推论说明如果这种情况发生了, 不存在任何 M 到 $S \otimes_R M$ 左 R -模单同态. 等价地, 我们也可以说 $S \otimes_R M$ 没有与 M 同构的左 R -模.

我们考虑几个具体的例子.

例 23.1.14 (有限生成的自由交换群).

记 G 为一个有限生成的交换群. 我们将其看作左 $\mathbb{Z}$ -模. 由 PID 上有限生成模的研究, 我们有

$$G \cong \mathbb{Z}^r \oplus \text{Tor}(G).$$

这里 r 为 G 作为 $\mathbb{Z}$ -模的秩, $\text{Tor}(G)$ 为 G 作为 $\mathbb{Z}$ -模的扭元部分.

由张量积的性质, 我们有

$$\mathbb{Q} \otimes_{\mathbb{Z}} G \cong (\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^r) + (\mathbb{Q} \otimes_{\mathbb{Z}} \text{Tor}(G)) = (\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^r) + \{0\} \cong \mathbb{Q}^r.$$

其中最后一个同构来自于以下观察: 任取 $n \in \mathbb{N} \setminus \{0, 1\}$, 我们有

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_n = \{0\}.$$

例 23.1.15 (实向量空间的复化).

考虑实向量空间 $\mathbb{R}^n$, 其中 $n \in \mathbb{N}^*$, 我们有

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \cong \mathbb{C}^n.$$

我们也可以将其看作实向量空间. 注意到其复维数为 n , 实维数为 $2n$. 若 $e_1, \dots, e_n$ 为 $\mathbb{R}^n$ 的一组基, 则

$$1 \otimes_{\mathbb{R}} e_1, \dots, 1 \otimes_{\mathbb{R}} e_n,$$

为 $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n$ 作为复向量空间的一组基. 同时

$$1 \otimes_{\mathbb{R}} e_1, i \otimes_{\mathbb{R}} e_1, \dots, 1 \otimes_{\mathbb{R}} e_n, i \otimes_{\mathbb{R}} e_n,$$

构成 $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n$ 作为实向量空间的一组基.

23.2 幺环上的模的张量积

在本节, 我们将把之前在扩张系数中张量积的构造推广到一般的情形.

记 R 为一个幺环. 任取一个右 R -模 M 和一个左 R -模 N , 我们考虑 $M \times N$ 生成的自由交换群

$$\mathbb{Z}^{M \times N} := \{f : M \times N \rightarrow \mathbb{Z} \mid f \text{ 在至多有限多个 } M \times N \text{ 的元素上取值非零}\}.$$

为方便讨论, 我们记其中元素为

$$\sum_{i=1}^n m_i(u_i, v_i),$$

其中 $n \in \mathbb{N}^*$, $m_1, \dots, m_n \in \mathbb{Z}$, $u_1, \dots, u_n \in M$, $v_1, \dots, v_n \in N$.

记 H 为 $\mathbb{Z}^{M \times N}$ 中由以下形式的元素生成的子群:

$$\begin{aligned} (u_1 + u_2, v) - (u_1, v) - (u_2, v), \\ (u, v_1 + v_2) - (u, v_1) - (u, v_2), \\ (ur, v) - (u, rv), \end{aligned}$$

其中 $u, u_1, u_2 \in M$, $v, v_1, v_2 \in N$, $r \in R$.

定义 23.2.1

我们定义右 R -模 M 和左 R -模 N 过 R 的**张量积**为以下商群

$$M \otimes_R N := \mathbb{Z}^{M \times N} / H,$$

并称其中的元素称为**张量**. 任取 $(u, v) \in M \times N$, 我们记其对应的商群的元素为 $u \otimes_R v$, 并称此类元素为**简单张量**.

注 23.2.2.

我们仍记 $\mathbb{Z}^{M \times N}$ 到 $M \otimes_R N$ 的自然同态为 π .

由其构造, 我们可以验证 $M \otimes_R N$ 中有如下运算. 任取 $u, u_1, u_2 \in M$, $r \in R$ 以及 $v, v_1, v_2 \in N$, 我们有

$$\begin{aligned} (u_1 + u_2) \otimes_R v &= u_1 \otimes_R v + u_2 \otimes_R v, \\ u \otimes_R (v_1 + v_2) &= u \otimes_R v_1 + u \otimes_R v_2, \\ ur \otimes_R v &= u \otimes_R rv, \\ 0_M \otimes_R v &= u \otimes_R 0_N = 0_M \otimes_R 0_N. \end{aligned}$$

在刚看到这个定义的时候我们可能立即会有两个疑问. 待我们分析完就会发现这两个疑问都和 R 的交换性相关.

第一个是关于张量积这个定义, 我们首先可能会问为什么是一个右模和左模的配合. 我们可以假设 M 和 N 都是左 R -模, 并将 H 的生成元最后一类元素改为

$$(ru, v) - (u, rv),$$

则任取 $u \in M$, $v \in N$ 以及 $s, r \in R$, 我们有

$$(rs)u \otimes_R v = su \otimes_R rv = u \otimes_R (sr)v = (sr)u \otimes_R v.$$

进而有

$$(rs - sr)u \otimes_R v = 0.$$

如果 R 交换, 则以上关系自然满足. 在一般情况下, 这样定义出来的可以看作是商环 $R/[R, R]$ 上的模的张量积. 这里 $[R, R]$ 为 R 中所有形如 $rs - sr$ 的元素生成的理想. 而 R 中与非交换有关的信息都丢失了.

第二个疑问是关于 R -模结构. 考虑到 M 和 N 都是 R -模, 一个自然的问题就是 $M \otimes_R N$ 上是否有 R -模结构. 我们仍旧对简单张量进行讨论. 任取 $r \in R, (u, v) \in M \times N$, 我们可以仿照之前的方法来定义模结构, 由于 M 此时为右 R -模, 因此我们定义

$$r(u \otimes_R v) := ur \otimes_R v = u \otimes_R rv.$$

这样看似没有问题, 但是如果任取元素 $s \in R$, 我们会观察到

$$u(sr) \otimes_R v = r(us \otimes_R v) = r(u \otimes_R sv) = ur \otimes_R sv = urs \otimes v.$$

因此对任意 $s, r \in R, u \in M$ 以及 $v \in N$, 我们应该有

$$(sr - rs)(u \otimes_r v) = 0.$$

如果 R 交换, 则以上关系自然满足. 因此 R 所有非交换的信息丢失了.

我们这里首先考虑一般情形, 后续我们会对 R 交换的情形做单独讨论.

张量积的泛性质

我们首先介绍张量积的泛性质. 注意到此时我们的张量积上暂时只有交换群结构, 因此所有的结果暂时都是关于群结构的.

定义 23.2.3

任取 G 为一个交换群, 设存在映射

$$\varphi: M \times N \rightarrow G,$$

满足对任意 $u, u_1, u_2 \in M, v, v_1, v_2 \in N$ 以及 $r \in R$ 都有

$$\varphi(u, v_1 + v_2) = \varphi(u, v_1) + \varphi(u, v_2)$$

$$\varphi(u_1 + u_2, v) = \varphi(u_1, v) + \varphi(u_2, v)$$

$$\varphi(ur, v) = \varphi(u, rv)$$

我们称这样的映射是 **R -平衡的**或者**中间 R -线性的**.

注 23.2.4.

我们考虑映射

$$\iota: M \times N \rightarrow M \otimes_R N,$$

$$(u, v) \mapsto u \otimes_R v.$$

直接计算我们可以验证 ι 是一个 R -平衡映射. 我们可以将 $M \times N$ 看作是 $\mathbb{Z}^{M \times N}$ 的一个子集, 则有 $\iota = \pi|_{M \times N}$.

定理 23.2.5 (模的张量积的泛性质)

记 R 为一个幺环, M 一个右 R -模, N 为一个左 R -模. 任给一个交换群 G , 则

- 1) 任给 R -平衡映射 $\varphi: M \times N \rightarrow G$, 存在唯一的一个群同态

$$\Phi: M \otimes_R N \rightarrow G,$$

满足 $\varphi = \Phi \circ \iota$;

- 2) 任给群同态 $\Phi: M \otimes_R N \rightarrow G$, 则 $\varphi = \Phi \circ \iota$ 为一个 $M \times N$ 到 G 的 R -平衡映射.

注 23.2.6.

我们也可以用 1) 来定义 $M \otimes_R N$, 即定义其为满足泛性质的交换群. 由于泛性质, 这样的交换群在同构意义下唯一. 当然如果使用这个定义, 我们仍需要之前的构造来说明满足泛性质的交换群是存在的.

证明. 1) 设 $\varphi: M \times N \rightarrow G$ 为一个 R -平衡映射. 利用自由交换群的泛性质, 我们有群同态:

$$\begin{aligned} \tilde{\Phi}: \mathbb{Z}^{M \times N} &\rightarrow G, \\ \sum_{i=1}^n m_i(u_i, v_i) &\mapsto \sum_{i=1}^n m_i \varphi(u_i, v_i). \end{aligned}$$

由于 φ 为 R -平衡映射, 我们有如下计算: 任取 $u, u_1, u_2 \in M, v, v_1, v_2 \in N$ 以及 $r \in R$, 我们有

$$\begin{aligned} \tilde{\Phi}((u_1 + u_2, v) - (u_1, v) - (u_2, v)) &= \varphi(u_1 + u_2, v) - \varphi(u_1, v) - \varphi(u_2, v) = 0_G, \\ \tilde{\Phi}((u, v_1 + v_2) - (u, v_1) - (u, v_2)) &= \varphi(u, v_1 + v_2) - \varphi(u, v_1) - \varphi(u, v_2) = 0_G, \\ \tilde{\Phi}(u, rv) - (ur, v)) &= \varphi(u, rv) - \varphi(ur, v) = 0_G. \end{aligned}$$

因此 $H \subset \ker \tilde{\Phi}$. 由群同态基本定理, 我们有以下交换图:

$$\begin{array}{ccc} \mathbb{Z}^{M \times N} & \xrightarrow{\tilde{\Phi}} & G \\ \pi \downarrow & \nearrow \Phi & \\ M \otimes_R N & & \end{array}$$

要证明 Φ 的唯一性, 注意到简单张量构成 $M \otimes_R N$ 的一组生成元, 因此 Φ 由 $\text{Im } \iota$ 中元素的像决定. 注意到任取满足条件的 Φ , 任取 $(u, v) \in M \times N$, 我们有

$$\Phi(u \otimes_R v) = \varphi(u, v),$$

所以 Φ 唯一.

2) 任取群同态 $\Phi: M \otimes_R N \rightarrow G$, 由于 ι 为 R -平衡映射, 我们有 $\varphi = \Phi \circ \iota$ 也是 R -平衡映射. $\square$

注 23.2.7.

以上定理告诉我们 $M \times N$ 到 G 的 R -平衡映射和 $M \otimes_R N$ 到 G 的同态映射有一一对应的关系. 特别地, 任意从 $M \times N$ 出发的 R -平衡映射都有过 $M \otimes_R N$ 的分解.

注 23.2.8.

任取交换群 G , 以及 R -平衡映射 $\varphi: M \times N \rightarrow G$, 我们考虑 $L = \langle \text{Im } \varphi \rangle$. 张量积的泛性质告诉我们 $M \otimes_R N$ 是通过这种办法得到的群中最大的那个. 这里"最大"的意思是指其它可能得到的群都可以看作是张量积的商群.

注 23.2.9.

张量积的泛性质的一个用途是可以被用来判断某些张量是否为零张量. 我们仍考虑张量积 $M \otimes_R N$, 考虑其中的简单张量. 具体来说, 取 $u \otimes_R v \in M \otimes_R N$, 若存在 G , 以及一个 R -平衡映射 $\varphi: M \times N \rightarrow G$ 满足 $\varphi(u, v) \neq 0_G$, 则 $u \otimes_R v$ 不是零张量.

我们首先回顾以下关于模的系数扩张的讨论. 记 S 为一个幺环, R 为 S 的包含幺元的子环. 任取左 R -模 M , 我们使用 S 为一个右 R -模这个条件构造了张量积 $S \otimes_R M$, 然后使用 S 为一个左 S -模的条件构造了 $S \otimes_R M$ 上的一个左 S -模结构. 在证明 $S \otimes_R M$ 为一个左 S -模的过程中, 我们并没有用到 S 和 R 的关系.

回到对一般的张量积的讨论, 任取左 R -模 M 和右 R -模 N , 由之前的讨论, 我们构造张量积 $M \otimes_R N$. 如果 M 和 N 有更多的结构的时候, 它们的张量积也会有更多的结构.

记 M 为一个交换群. 任取幺环 S 和 R , 设存在映射

$$\begin{aligned} \Phi: S \times M \times R &\rightarrow M, \\ (s, u, r) &\mapsto v. \end{aligned}$$

任给 $s \in S$ 和 $r \in R$, 我们可以定义

$$\begin{aligned} {}_s\Phi: M \times R &\rightarrow M, & \Phi_r: S \times M &\rightarrow M, \\ (u, r) &\mapsto \Phi(s, u, r), & (s, u) &\mapsto \Phi(s, u, r). \end{aligned}$$

定义 23.2.10

记 M 为一个交换群. 记 S 和 R 为幺环, 若存在映射

$$\begin{aligned} \Phi: S \times M \times R &\rightarrow M, \\ (x, u, y) &\mapsto v, \end{aligned}$$

满足对任意 $s \in S$ 和 $r \in R$, 映射 Φ_r 和 ${}_s\Phi$ 分别给出 M 上的一个左 S -模结构和一个右 R -模结构, 我们称 Φ 给出 M 上一个 (S, R) -**双模结构**.

注 23.2.11.

以上定义说明任取 $s \in S$, $u \in M$ 和 $r \in R$, 我们有 $(su)r = s(ur)$.

命题 23.2.12

记 S, R 和 T 为三个幺环.

- 1) 设 M 为一个 (S, R) -双模, N 为一个左 R -模, 则我们有映射

$$\begin{aligned} S \times (M \otimes_R N) &\rightarrow M \otimes_R N, \\ (s, u \otimes_R v) &\mapsto su \otimes_R v, \end{aligned}$$

给出张量积 $M \otimes_R N$ 上一个左 S -模结构.

- 2) 设 M 为一个右 R -模, N 为一个 (R, T) -双模, 则我们有映射

$$\begin{aligned} (M \otimes_R N) \times T &\rightarrow M \otimes_R N, \\ (u \otimes_R v, t) &\mapsto u \otimes_R vt, \end{aligned}$$

给出张量积 $M \otimes_R N$ 上一个右 T -模结构.

- 3) 设 M 为一个 (S, R) -双模, N 为一个 (R, T) -双模, 则我们有映射

$$\begin{aligned} S \times (M \otimes_R N) \times T &\rightarrow M \otimes_R N, \\ (s, u \otimes_R v, t) &\mapsto su \otimes_R vt, \end{aligned}$$

给出张量积 $M \otimes_R N$ 上一个 (S, T) -双模结构.

证明. 证明类似于命题 23.1.4 的证明. 留作练习. $\square$

张量积的结合性

当一个张量积有模结构之后, 我们可以构造其与其它模的张量积. 记 S 和 R 为幺环, 设 K 为一个右 S -模, M 为一个 (S, R) -双模, N 为一个左 R -模. 我们可以构造 $K \otimes_S (M \otimes_R N)$ 和 $(K \otimes_S M) \otimes_R N$ 两个张量积. 一个自然的问题就是不同的顺序的到的张量积是否在某种意义下唯一. 以下结论回答了这个问题.

命题 23.2.13

沿用以上记号, 则我们有映射

$$\begin{aligned} \Phi : K \otimes_S (M \otimes_R N) &\rightarrow (K \otimes_S M) \otimes_R N \\ w \otimes_S (u \otimes_R v) &\mapsto (w \otimes_S u) \otimes_R v \end{aligned}$$

给出 $K \otimes_S (M \otimes_R N)$ 和 $(K \otimes_S M) \otimes_R N$ 之间的群同构.

注 23.2.14.

考虑到两个张量积的构造, 将 $w \otimes_S (u \otimes_R v)$ 和 $(w \otimes_S u) \otimes_R v$ 对应起来是一个很自然的想法. 我们这里说明这样的对应确实给出了一个群同构. 我们称这个同构为 $K \otimes_S (M \otimes_R N)$ 到 $(K \otimes_S M) \otimes_R N$ 的**自然同构**. 我们并没有排除其它群同构存在的可能性.

证明. 我们考虑映射

$$\begin{aligned}\psi : K \times M \times N &\rightarrow (K \otimes_S M) \otimes_R N, \\ (w, u, v) &\mapsto (w \otimes_S u) \otimes_R v.\end{aligned}$$

任取 $w \in K$, 我们定义映射

$$\begin{aligned}\psi_w : M \times N &\rightarrow (K \otimes_S M) \otimes_R N, \\ (u, v) &\mapsto (w \otimes_S u) \otimes_R v.\end{aligned}$$

任取 $u, u_1, u_2 \in M, v, v_1, v_2 \in N$ 以及 $r \in R$, 有

$$\begin{aligned}\psi_w(u_1 + u_2, v) &= (w \otimes_S (u_1 + u_2)) \otimes_R v \\ &= (w \otimes_S u_1 + w \otimes_S u_2) \otimes_R v \\ &= (w \otimes_S u_1) \otimes_R v + (w \otimes_S u_2) \otimes_R v \\ &= \psi_w(u_1, v) + \psi_w(u_2, v), \\ \psi_w(u, v_1 + v_2) &= (w \otimes_S u) \otimes_R (v_1 + v_2) \\ &= (w \otimes_S u) \otimes_R v_1 + (w \otimes_S u) \otimes_R v_2 \\ &= \psi_w(u, v_1) + \psi_w(u, v_2), \\ \psi_w(ur, v) &= (w \otimes_S ur) \otimes_R v \\ &= (w \otimes_S u)r \otimes_R v \\ &= (w \otimes_S u) \otimes_R rv \\ &= \psi_w(u, rv).\end{aligned}$$

因此 ψ_w 是 R -平衡映射, 利用张量积的泛性质, 我们可以得到一个群同态

$$\begin{aligned}\Psi_w : M \otimes_R N &\rightarrow (K \otimes_S M) \otimes_R N, \\ u \otimes_R v &\mapsto (w \otimes_S u) \otimes_R v.\end{aligned}$$

由此可得以下映射定义良好

$$\begin{aligned}\varphi : K \times (M \otimes_R N) &\rightarrow (K \otimes_S M) \otimes_R N, \\ (w, u \otimes_R v) &\mapsto \Psi_w(u \otimes_R v) = (w \otimes_S u) \otimes_R v.\end{aligned}$$

我们下边验证 φ 是一个 S -平衡映射. 由于对任意 $w \in K, \Psi_w$ 都是群同态, 我们只需考虑 $M \otimes_R N$ 种的简单张量即可.

任取 $w, w_1, w_2 \in K, u, u_1, u_2 \in M, v, v_1, v_2 \in N$ 以及 $s \in S$, 我们有

$$\begin{aligned}\varphi(w_1 + w_2, u \otimes_R v) &= ((w_1 + w_2) \otimes_S u) \otimes_R v \\ &= (w_1 \otimes_S u + w_2 \otimes_S u) \otimes_R v \\ &= w_1 \otimes_S u \otimes_R v + (w_2 \otimes_S u) \otimes_R v \\ &= \varphi(w_1, u \otimes_R v) + \varphi(w_2, u \otimes_R v), \\ \varphi(w, u_1 \otimes_R v_1 + u_1 \otimes_R v_2) &= \Psi_w(u_1 \otimes_R v_1 + u_1 \otimes_R v_2) \\ &= \Psi_w(u_1 \otimes_R v_1) + \Psi_w(u_1 \otimes_R v_2) \\ &= \varphi(w, u_1 \otimes_R v_1) + \varphi(w, u_1 \otimes_R v_2), \\ \varphi(ws, u \otimes_R v) &= (ws \otimes_S u) \otimes_R v \\ &= (w \otimes_S su) \otimes_R v \\ &= \varphi(w, su \otimes_R v) \\ &= \varphi(w, s(u \otimes_R v)).\end{aligned}$$

因此 φ 是一个 S -平衡映射, 利用张量积的泛性质, 我们有群同态

$$\begin{aligned}\Phi : K \otimes_S (M \otimes_R N) &\rightarrow (K \otimes_S M) \otimes_R N, \\ w \otimes_S (u \otimes_R v) &\mapsto (w \otimes_S u) \otimes_R v.\end{aligned}$$

类似地, 我们可以证明存在群同态

$$\begin{aligned}\Theta : (K \otimes_S M) \otimes_R N &\rightarrow K \otimes_S (M \otimes_R N), \\ (w \otimes_S u) \otimes_R v &\mapsto w \otimes_S (u \otimes_R v).\end{aligned}$$

我们考虑 $\Phi \circ \Theta$ 和 $\Theta \circ \Phi$. 由 Φ 和 Θ 的定义我们可以直接验证两个复合分别为 $K \otimes_S (M \otimes_R N)$ 和 $(K \otimes_S M) \otimes_R N$ 上的恒等同构. 因此 Φ 和 Θ 都是群同构. $\square$

如果 K 或 N 上有双模结构, 则以上群同构也与对应的模结构相容, 因此是一个模同构.

推论 23.2.15

沿用以上记号, 记 T 为一个幺环.

- 1) 若 K 为一个 (T, S) -双模, 则以上群同构 Φ 是一个左 T -模同构;
- 2) 若 N 为一个 (R, T) -双模, 则以上群同构 Φ 是一个右 T -模同构.

证明. 我们将证明 1). 2) 的证明类似.

由于 K 为一个 (T, S) -双模, 由命题 23.2.12, 张量积 $K \otimes_S (M \otimes_R N)$, $K \otimes_S M$ 和 $(K \otimes_S M) \otimes_R N$ 均为左 T -模.

任取 $t \in T$, 任取 $w \in K$, $u \in M$ 以及 $v \in N$, 沿用之前的记号, 我们有

$$\begin{aligned}
 & \Phi(t(w \otimes_S (u \otimes_R v))) \\
 &= \Phi(tw \otimes_S (u \otimes_R v)) \\
 &= (tw \otimes_S u) \otimes_R v \\
 &= t(w \otimes_S u) \otimes_R v \\
 &= t((w \otimes_S u) \otimes_R v) \\
 &= t\Phi(w \otimes_S (u \otimes_R v)).
 \end{aligned}$$

□

注 23.2.16.

以上结论可以推广到对多个模的张量积的讨论.

张量积与直和

我们下边考虑张量积与直和之间的关系.

记 R 为一个幺环. 记 M, K 均为右 R -模, L, N 均为左 R -模. 我们有以下结论

命题 23.2.17

我们有以下群同构

$$\begin{aligned}
 M \otimes_R (L \oplus N) &\cong (M \otimes_R L) \oplus (M \otimes_R N), \\
 (M \oplus K) \otimes_R N &\cong (M \otimes_R N) \oplus (K \otimes_R N).
 \end{aligned}$$

证明. 我们将证明第一个关系. 第二个关系的证明类似.

我们考虑映射

$$\begin{aligned}
 \varphi: M \times (L \oplus N) &\rightarrow (M \otimes_R L) \oplus (M \otimes_R N) \\
 (u, (w, v)) &\mapsto (u \otimes_R w, u \otimes_R v)
 \end{aligned}$$

我们可以直接验证该映射为 R -平衡的. 任取 $r \in R$, $u, u_1, u_2 \in M$, $w, w_1, w_2 \in L$, 以及 $v, v_1, v_2 \in N$, 我们有

$$\begin{aligned}
 & \varphi(u_1 + u_2, (w, v)) & \varphi(u, (w_1 + w_2, v_1 + v_2)) \\
 &= ((u_1 + u_2) \otimes_R w, (u_1 + u_2) \otimes_R v) &= (u \otimes_R (w_1 + w_2), u \otimes_R (v_1 + v_2)) \\
 &= (u_1 \otimes_R w, u_1 \otimes_R v) + (u_2 \otimes_R w, u_2 \otimes_R v) &= (u \otimes_R w_1, u \otimes_R v_1) + (u \otimes_R w_2, u \otimes_R v_2) \\
 &= \varphi(u_1, (w, v)) + \varphi(u_2, (w, v)), &= \varphi(u, (w_1, v_1)) + \varphi(u, (w_2, v_2)),
 \end{aligned}$$

$$\begin{aligned}
& \varphi(ur, (w, v)) \\
&= (ur \otimes_R w, ur \otimes_R v) \\
&= (u \otimes_R rw, u \otimes_R rv) \\
&= \varphi(u, (rw, rv)).
\end{aligned}$$

由张量积的泛性质我们有群同态

$$\begin{aligned}
\Phi : M \otimes_R (L \oplus N) &\rightarrow (M \otimes_R L) \oplus (M \otimes_R N), \\
\sum_{i=1}^n u_i \otimes_R (w_i, v_i) &\mapsto \left(\sum_{i=1}^n u_i \otimes_R w_i, \sum_{i=1}^n u_i \otimes_R v_i \right).
\end{aligned}$$

由定义我们可以直接验证 Φ 为满同态. 若要证 Φ 为一个群同构, 我们只需证明 Φ 为一个单同态即可.

考虑内外直和之间的关系, 我们有群同构

$$M \otimes_R L \cong M \otimes_R (L \oplus \{0_N\}),$$

以及

$$M \otimes_R N \cong M \otimes_R (\{0_L\} \oplus N).$$

因此若

$$\Phi \left(\sum_{i=1}^n u_i \otimes_R (w_i, v_i) \right) = 0_{(M \otimes_R L) \oplus (M \otimes_R N)},$$

我们有

$$\sum_{i=1}^n u_i \otimes_R w_i = 0_{M \otimes_R L} \quad \text{且} \quad \sum_{i=1}^n u_i \otimes_R v_i = 0_{M \otimes_R N}.$$

进而有

$$\begin{aligned}
& \sum_{i=1}^n u_i \otimes_R (w_i, v_i) \\
&= \sum_{i=1}^n u_i \otimes_R (w_i, 0_N) + \sum_{i=1}^n u_i \otimes_R (0_L, v_i) \\
&= 0_{M \otimes_R (L \oplus N)}.
\end{aligned}$$

因此 $\ker \Phi = \{0_{M \otimes_R (L \oplus N)}\}$, 我们有 Φ 为单同态. 综上所述, 同态 Φ 为群同构. $\square$

推论 23.2.18

沿用以上记号, 记 T 为一个么环.

- 1) 若 M, M_1, M_2 均为 (T, R) -双模, 则以上群同构也是左 T -模同构;
- 2) 若 N, N_1, N_2 均为 (R, T) -双模, 则以上群同构也是右 T -模同构.

证明. 我们将证明 1). 2) 的证明类似.

任取 $t \in T$, 以及 $\sum_{i=1}^n u_i \otimes_R (w_i, v_i) \in M \otimes_R (L \oplus N)$, 我们有

$$\begin{aligned} & \Phi \left(t \left(\sum_{i=1}^n u_i \otimes_R (w_i, v_i) \right) \right) \\ &= \Phi \left(\sum_{i=1}^n t u_i \otimes_R (w_i, v_i) \right) \\ &= \left(\sum_{i=1}^n t u_i \otimes_R w_i, \sum_{i=1}^n t u_i \otimes_R v_i \right) \\ &= t \left(\sum_{i=1}^n u_i \otimes_R w_i, \sum_{i=1}^n u_i \otimes_R v_i \right) \\ &= t \Phi \left(\sum_{i=1}^n u_i \otimes_R (w_i, v_i) \right). \end{aligned}$$

因此 Φ 为左 t -模同构. □

推论 23.2.19

任取 $m, n \in \mathbb{N}^*$, 我们有以下 R -模同构

$$R^m \otimes_R R^n \cong R^{mn}.$$

证明. 由 23.1.8, 我们有 R -模同构 $R \otimes_R R \cong R$.

任取 $m, n \in \mathbb{N}^*$, 利用以上结论以及归纳法, 我们有 R -模同构

$$R^m \otimes_R R^n \cong (R \otimes R^n)^m \cong (R \otimes_R R)^{mn} \cong R^{mn}.$$

□

模同态的张量积

我们下边讨论模同态及其诱导的张量积之间的同态.

记 R 为一个幺环. 记 M, M' 为两个右 R -模, N, N' 为两个左 R -模. 记

$$f: M \rightarrow M' \quad \text{和} \quad g: N \rightarrow N',$$

为两个 R -模同态.

命题 23.2.20

沿用以上记号, 我们有以下群同态

$$\begin{aligned} f \otimes g: M \otimes_R N &\rightarrow M' \otimes_R N', \\ \sum_{i=1}^n u_i \otimes_R v_i &\mapsto \sum_{i=1}^n f(u_i) \otimes_R g(v_i). \end{aligned}$$

证明. 我们考虑映射

$$\begin{aligned} \Phi: M \times N &\rightarrow M' \otimes_R N', \\ (u, v) &\mapsto f(u) \otimes_R g(v). \end{aligned}$$

由于 f 和 g 为模同态, Φ 为 R -平衡映射. 由张量积的泛性质, 我们有群同态:

$$f \otimes g : M \otimes_R N \rightarrow M' \otimes_R N',$$

满足任取简单张量 $u \otimes_R v \in M \otimes_R N$, 我们有

$$(f \otimes g)(u \otimes_R v) = f(u) \otimes_R g(v).$$

由于 $f \otimes g$ 为群同态, 因此任取 $\sum_{i=1}^n u_i \otimes_R v_i \in M \otimes_R N$, 我们有

$$(f \otimes g) \left(\sum_{i=1}^n u_i \otimes_R v_i \right) = \sum_{i=1}^n f(u_i) \otimes_R g(v_i).$$

□

定义 23.2.21

我们称 $f \otimes g$ 为模同态 f 和 g 的**张量积**.

推论 23.2.22

沿用以上记号, 记 T 为一个么环.

- 1) 若 M 和 M' 均为 (T, R) -双模, 且 f 同时也为左 T -模同态, 则 $f \otimes g$ 也是左 T -模同态;
- 2) 若 N 和 N' 均为 (R, T) -双模, 且 g 同时也为右 T -模同态, 则 $f \otimes g$ 也是右 T -模同态.

证明. 证明与推论 23.2.18 的证明类似, 留作练习. □

沿用之前的记号, 设进一步有右 R -模 M'' 和左 R -模 N'' , 以及模同态

$$f' : M' \rightarrow M'' \quad \text{和} \quad g' : N' \rightarrow N'',$$

我们可以考虑映射的复合, 则有以下关系.

命题 23.2.23

沿用以上记号, 我们有

$$(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g).$$

证明. 二者均为相同的群之间的同态, 且在简单张量上的取值相同. 由于简单张量生成张量积, 因此二者相等. □

23.3 交换么环上的模的张量积

在之前介绍模的张量积的定义的时候, 我们看到交换么环上的模的张量积具有非交换么环上的模的张量积所不具有的性质. 我们将在本节中讨论交换么环上的模的张量积. 需要注

意的是由于考虑的问题不同, 交换环和非交换环的发展相互之间有一定的独立性, 所涉及的张量积理论发展的动机也有一定的区别. 在某种意义上本节内容也可以独立于前一节介绍的一般模上的张量积理论来学习.

促进对交换幺环上的模的张量积的一个契机就是对多线性映射的研究. 考虑到线性代数广泛的应用, 多线性映射出现在众多数学领域的研究种. 我们将在介绍完一般理论后着重讨论以下与向量空间相关的一些初步的结论. 在后续交换环理论介绍的章节中, 我们还将看到更多张量积的应用.

"左(右)模即右(左)模"

我们首先回顾一个交换幺环上的模的特点. 记 R 为一个交换幺环, M 为一个交换群. 设存在映射

$$\begin{aligned}\Phi: R \times M &\rightarrow M, \\ (r, u) &\mapsto ru.\end{aligned}$$

若 Φ 给出 M 上一个左模结构, 则根据定义任取 $s, r \in R$ 以及 $u, v \in M$, 我们有

$$\begin{aligned}(s+r)u &= su + ru, \\ s(u+v) &= su + sv, \\ (sr)u &= s(ru), \\ 1u &= u.\end{aligned}$$

由于 R 交换, 第三个关系也可以给出以下关系

$$(sr)u = (rs)u = r(su).$$

因此 Φ 实际上也给出了 M 上一个右 R -模结构. 这个区别于一般的幺环上的模的性质使得当我们讨论交换幺环上的模的张量积的时候可以得到一些更强的结论.

在之后的讨论中, 形式上我们将使用左模记号, 但我们不再区分左右, 而仅仅称 R -模. 为方便讨论, 我们这里重新给出张量积的构造.

记 R 为一个交换幺环, M 和 N 为 R -模. 我们考虑以 $M \times N$ 中元素为生成元生成的交换自由群:

$$\mathbb{Z}^{M \otimes N} := \{f: M \times N \rightarrow \mathbb{Z} \mid f \text{ 仅在有限多个 } M \times N \text{ 的元素上取值非零}\}.$$

我们仍记 $\mathbb{Z}^{M \otimes N}$ 中的元素为

$$\sum_{i=1}^n m_i(u_i, v_i),$$

其中有 $n \in \mathbb{N}^*$, $m_1, \dots, m_n \in \mathbb{Z}$, $u_1, \dots, u_n \in M$ 以及 $v_1, \dots, v_n \in N$.

我们记 H 为其中由以下形式的元素生成的子群:

$$\begin{aligned}(u_1 + u_2, v) - (u_1, v) - (u_2, v), \\ (u, v_1 + v_2) - (u, v_1) - (u, v_2), \\ (ru, v) - (u, rv),\end{aligned}$$

其中 $u, u_1, u_2 \in M$, $v, v_1, v_2 \in N$, 以及 $r \in R$. 则 M 和 N 的张量积定义为商群

$$M \otimes_R N := \mathbb{Z}^{M \otimes N} / H.$$

其中的元素被称为张量. 任取 $u \in M$, $v \in N$, 我们称张量 $u \otimes_R v$ 为简单张量.

考虑以上的 H 的生成元, 在张量积 $M \otimes_R N$ 中我们有

$$\begin{aligned}(u_1 + u_2) \otimes_R v &= u_1 \otimes_R v + u_2 \otimes_R v, \\ u \otimes_R (v_1 + v_2) &= u \otimes_R v_1 + u \otimes_R v_2, \\ ru \otimes_R v &= u \otimes_R rv, \\ 0_M \otimes_R v &= u \otimes_R 0_N = 0_{M \otimes_R N}.\end{aligned}$$

张量积上的 R -模结构

与一般的幺环上的张量积不同, 交换幺环上的模的张量积有一个自然的模结构(参考一般幺环上模的张量积定义后的讨论).

命题 23.3.1

记 R 为一个交换幺环. 记 M 和 N 为 R -模. 张量积 $M \otimes_R N$ 上有一个由以下映射给出的 R -模结构:

$$\begin{aligned} \Phi : R \times M \otimes_R N &\rightarrow M \otimes_R N, \\ \left(r, \sum_{i=1}^n u_i \otimes_R v_i \right) &\mapsto \sum_{i=1}^n r u_i \otimes_R v_i. \end{aligned}$$

证明. 证明与命题 23.1.4 的证明类似. 留作练习. □

 R -双线性映射与张量积的泛性质

考虑 $M \otimes_R N$ 上的 R -模结构, 任取 $u \in M, v \in N$ 以及 $r \in R$, 我们有

$$r(u \otimes_R v) = (ru) \otimes_R v = u \otimes_R (rv).$$

我们可以将其看作是以下映射的性质

$$\begin{aligned} \iota : M \times N &\rightarrow M \otimes_R N, \\ (u, v) &\mapsto u \otimes_R v. \end{aligned}$$

将其推广之后, 我们有以下定义

定义 23.3.2

记 K, M 和 N 为 R -模. 考虑映射

$$\varphi : M \times N \rightarrow K.$$

我们称 φ 为 R -**双线性的**, 若其满足以下条件: 任取 $u, u_1, u_2 \in M, v, v_1, v_2 \in N$ 以及 $r \in R$, 我们有

$$\begin{aligned} \varphi(u, v_1 + v_2) &= \varphi(u, v_1) + \varphi(u, v_2), \\ \varphi(u_1 + u_2, v) &= \varphi(u_1, v) + \varphi(u_2, v), \\ \varphi(ru, v) &= \varphi(u, rv) = r\varphi(u, v). \end{aligned}$$

我们有如下交换幺环上的张量积的泛性质.

定理 23.3.3 (关于双线性映射的张量积的泛性质)

记 R 为一个交换幺环. 记 K, M 和 N 为 R -模.

- 1) 任给 R -双线性映射 $\varphi: M \times N \rightarrow K$, 存在唯一的 R -模同态

$$\Phi: M \otimes_R N \rightarrow K,$$

满足 $\varphi = \Phi \circ \pi$.

- 2) 任给一个 R -模同态 $\Phi: M \otimes_R N \rightarrow K$, 则 $\varphi = \Phi \circ \pi$ 为一个 $M \times N$ 到 K 的 R -双线性映射.

注 23.3.4.

类似于之前的讨论, 这里 1) 也可以用来给出交换幺环上的模的张量积的定义, 即 M 和 N 的张量积是满足泛性质的 R -模. 以上定理给出了这样的结构在同构意义下的唯一性. 当然, 与之前类似, 我们仍需要之前的构造得到的 $M \otimes_R N$ 来说明这样定义出来的结构是存在的.

证明. 该定理的证明与定理 23.2.5 的证明类似, 留作练习. $\square$

注 23.3.5.

以上定理告诉我们 $M \times N$ 到 K 的 R -双线性映射和 $M \otimes_R N$ 到 K 的 R -模同态(或 R -线性映射)有一一对应的关系. 双线性在数学中是一个常见的现象. 例如, 我们考虑 $\mathbb{R}$ 上的函数空间 $\mathcal{F}(\mathbb{R})$, 则通过考虑一对 $\mathbb{R}$ 上的函数 f 和 g , 我们可以得到 $\mathbb{R} \times \mathbb{R}$ 上的函数: 任取 $(x, y) \in \mathbb{R}^2$, 有

$$(fg)(x, y) := f(x)g(y).$$

函数空间 $\mathcal{F}(\mathbb{R})$ 为 $\mathbb{R}$ -向量空间, 以上构造中, 任取 $r \in \mathbb{R}$, 我们有 $(rf)g = f(rg) = r(fg)$. 注意到 $\mathbb{R}^2$ 上的函数空间也是 $\mathbb{R}$ -向量空间. 因此, 我们这里从 $\mathbb{R}$ -双线性映射出发 (例如 $(f, g) \mapsto fg$), 希望得到一个 $\mathbb{R}$ -线性映射. 我们可以考虑 $\mathcal{F}(\mathbb{R}) \otimes_{\mathbb{R}} \mathcal{F}(\mathbb{R})$ 到 $\mathcal{F}(\mathbb{R}^2)$ 的映射 $(f \otimes_{\mathbb{R}} g) \mapsto fg$.

这类构造的一个在(量子)物理中的一个应用可以考虑 $\mathbb{R}$ 上的某个测度的分布函数, 我们可以通过两个测度的乘积得到 $\mathbb{R}^2$ 的一个测度的分布函数. 在下一节中我们会讨论来自线性代数中的一些与双线性相关的例子.

注意到当 R 交换之后, 我们可以同时定义 $M \otimes_R N$ 和 $N \otimes_R M$. 作为定理 23.3.3 的应用, 我们可以说明这两个张量积实际上同构.

推论 23.3.6

以下映射给出 R -模同构:

$$\begin{aligned} \Phi: M \otimes_R N &\rightarrow N \otimes_R M, \\ \sum_{i=1}^n u_i \otimes_R v_i &\mapsto \sum_{i=1}^n v_i \otimes_R u_i. \end{aligned}$$

注 23.3.7.

考虑到两个张量积的构造, 将 $u \otimes_R v$ 和 $v \otimes_R u$ 对应起来是一个很自然的想法. 我们这里说明这样的对应确实给出了 R -模同构. 我们称这个同构为 $M \otimes_R N$ 到 $N \otimes_R M$ 的**自然同构**. 我们并没有排除其它 R -模同构存在的可能性.

证明. 我们考虑映射

$$\begin{aligned}\varphi: M \times N &\rightarrow N \otimes_R M, \\ (u, v) &\mapsto v \otimes_R u.\end{aligned}$$

直接验证可得 φ 为一个 R -双线性映射. 因此存在 R -模同态

$$\begin{aligned}\Phi: M \otimes_R N &\rightarrow N \otimes_R M, \\ \sum_{i=1}^n u_i \otimes_R v_i &\mapsto \sum_{i=1}^n v_i \otimes_R u_i.\end{aligned}$$

类似地, 存在 R -模同态

$$\begin{aligned}\Psi: N \otimes_R M &\rightarrow M \otimes_R N, \\ \sum_{i=1}^n v_i \otimes_R u_i &\mapsto \sum_{i=1}^n u_i \otimes_R v_i.\end{aligned}$$

利用 Φ 和 Ψ 的定义, 我们可以直接验证 $\Phi \circ \Psi$ 和 $\Psi \circ \Phi$ 分别为 $N \otimes_R M$ 和 $M \otimes_R N$ 上的恒等映射, 因此 Φ 和 Ψ 均为 R -模同构. $\square$

张量积的结合律

我们可以将 R -双线性映射推广到 R -多重线性映射.

定义 23.3.8

记 $k \in \mathbb{N} \setminus \{0, 1\}$. 任给 k 个 R -模 $M_1, \dots, M_k$ 和 R -模 N , 我们称一个映射

$$\varphi: M_1 \times \cdots \times M_k \rightarrow N,$$

为一个 R - n -**重线性映射**, 若其满足任取 $u_1, v_1 \in M_1, \dots, u_k, v_k \in M_k$ 以及 $r \in R$, 对任意 $1 \leq i \leq k$

$$\begin{aligned}\varphi(u_1, \dots, u_i + v_i, \dots, u_k) &= \varphi(u_1, \dots, u_i, \dots, u_k) + \varphi(u_1, \dots, v_i, \dots, u_k), \\ \varphi(u_1, \dots, ru_i, \dots, u_k) &= r\varphi(u_1, \dots, u_i, \dots, u_k).\end{aligned}$$

我们可以将两个 R -模的张量积推广为 R -模的 n -重张量积. 记 $k \in \mathbb{N} \setminus \{0, 1\}$. 任给 k 个 R -模 $M_1, \dots, M_k$, 我们可以考虑张量积. 不同的取张量积的顺序给出不同的 R -模, 考虑命题 23.2.13 及其推论和推论 23.3.6, 得到的这些 R -模之间存在自然的模同构. 因此在模同构意义下, 我们可以将其记作

$$M_1 \otimes_R \cdots \otimes_R M_k.$$

注 23.3.9.

注意到任给两个 R -模, 我们可以取张量积, 得到的仍是 R -模. 我们可以考虑一个 R -模的集合 Ω . 若 Ω 对取张量积封闭. 命题 23.2.13 及其推论和推论 23.3.6 中给出的同构可以用来构造 Ω 上一个等价关系 $\sim$. 取张量积可以看作是 $\Omega/\sim$ 上一个二元运算. 而 $\sim$ 告诉我们这个运算满足结合律和交换律. 因此 $\Omega/\sim$ 为一个交换半群.

定义 23.3.10

我们称 $M_1 \otimes_R \cdots \otimes_R M_k$ 为 R -模 $M_1, \dots, M_k$ 的 n -重张量积.

交换幺环上的张量积的泛性质也可以推广到 n -重张量积的情形.

命题 23.3.11

记 $k \in \mathbb{N} \setminus \{0, 1\}$. 记 $M_1, \dots, M_k$ 和 N 为 R -模.

- 1) 任给 R - n -重线性映射 $\varphi: M \times \cdots \times M_k \rightarrow N$, 存在唯一的 R -模同态

$$\Phi: M \otimes_R \cdots \otimes_R M_k \rightarrow N,$$

满足 $\varphi = \Phi \circ \pi$.

- 2) 任给一个 R -模同态 $\Phi: M_1 \otimes_R \cdots \otimes_R M_k \rightarrow N$, 则 $\varphi = \Phi \circ \pi$ 为一个 $M \times \cdots \times M_k$ 到 N 的 R - n -重线性映射.

注 23.3.12.

以上定理告诉我们 $M \times \cdots \times M_k$ 到 N 的 R - n -重线性映射和 $M_1 \otimes_R \cdots \otimes_R M_k$ 到 N 的 R -模同态(或 R -线性映射)有一一对应的关系. 类似于张量积的情形, 我们也可以用这个泛性质来定义 n -重张量积.

23.4 向量空间之间的张量积

向量空间在数学中的黎曼几何, 物理中广义相对论等领域有着重要的作用. 如前文提到的, 在这些领域的研究中, 多重线性映射是一个常见的研究对象. 如果我们希望从此类映射中构造出一个线性映射, 就可以使用张量积这种构造. 我们可以将这些看作是最开始研究张量积的一个动机. 本节我们将讨论一些与向量空间相关的张量积的构造. 本节仅考虑过 $\mathbb{R}$ 的张量积, 我们将记号 $\otimes_{\mathbb{R}}$ 简化为 $\otimes$.

向量空间的张量积

在本节中, 我们只考虑实数域 $\mathbb{R}$ 上的有限维向量空间. 我们首先考虑 $\mathbb{R}^m$ 和 $\mathbb{R}^n$, 其中 $m, n \in \mathbb{N}$. 我们记其中的元素为列向量. 任取 $u \in \mathbb{R}^m$ 以及 $v \in \mathbb{R}^n$, 我们可以考虑以下矩阵乘法

$$uv^t \in \text{Mat}_{n \times m}(\mathbb{R}),$$

所得为一个阶为 $n \times m$ 的实矩阵. 注意到在这个计算过程中, 任取 $x \in \mathbb{R}$, 我们都有

$$(xu)v^t = u(xv^t) = x(uv^t).$$

因此我们有一个线性映射

$$\Phi: \mathbb{R}^m \otimes \mathbb{R}^n \mapsto \text{Mat}_{n \times m}(\mathbb{R}).$$

我们可以进一步直接验证 Φ 为双射, 因此为一个线性同构. 我们可以将 $\mathbb{R}^m \otimes \mathbb{R}^n$ 等同于 $\text{Mat}_{n \times m}(\mathbb{R})$. 实际上若我们将 $\text{Mat}_{n \times m}(\mathbb{R})$ 等同于 $\mathbb{R}^{nm}$, 利用推论 23.2.19, 我们也有以上同构. 考虑矩阵加法, 将实矩阵空间看作实向量空间, 则以上讨论也对实矩阵空间成立.

向量空间的双线性型

考虑 V 上的一个双线性型 φ , 即一个双线性映射

$$\varphi : V \times V \rightarrow \mathbb{R}.$$

定理 23.3.3 1) 告诉我们, 存在线性映射

$$\Phi : V \otimes V \rightarrow \mathbb{R},$$

满足任取 $u, v \in V$, 我们有

$$\Phi(u \otimes v) = \varphi(u, v).$$

定理 23.3.3 2) 则告诉我们, 任意一个 $V \otimes V$ 到 $\mathbb{R}$ 的线性映射, 都可以给我们一个 V 上的双线性型. 因此, 我们可以将 V 上的双线性型空间和线性映射的空间

$$\text{Hom}(V \otimes V, \mathbb{R})$$

等同起来.

向量空间之间的线性映射

考虑两个有限维线性空间 V 和 W , 记 $\text{Hom}(V, W)$ 为所有 V 到 W 的线性映射的集合, 其上也有一个 $\mathbb{R}$ -线性空间结构. 任取 $f \in \text{Hom}(V, W)$, 以及 $v \in V$, 任取 $r \in \mathbb{R}$, 我们有

$$(rf)(v) = f(rv) = r(f(v)).$$

如果取 V 的一组基底 $v_1, \dots, v_m$, 以及 W 的一组基底 $w_1, \dots, w_n$, 我们有 $\text{Hom}(V, W)$ 的一组基

$$\{f_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq n\},$$

其中对任意 $1 \leq i \leq m$ 以及 $1 \leq j \leq n$, 我们定义

$$f_{ij}(v_k) = \begin{cases} w_j, & k = i \\ 0_W, & k \neq i \end{cases}$$

我们考虑 V 的对偶空间 V^* 以及 $v_1, \dots, v_m$ 给出的 V^* 的对偶基 $v_1^*, \dots, v_m^*$, 则以上定义可以写为

$$f_{ij}(v_k) = (v_i^*(v_k))w_j.$$

由此, 任取 $v \in V$, 我们有如下表达

$$f(v) = \sum_{i=1}^m \sum_{j=1}^n r_{ij} f_{ij}(v) = \sum_{i=1}^m \sum_{j=1}^n r_{ij} (v_i^*(v))w_j.$$

反过来任取 $v^* \in V^*$ 与 $w \in W$, 我们可以构造以下映射

$$\begin{aligned} g_{(v^*, w)} : V &\rightarrow W, \\ u &\mapsto v^*(u)w. \end{aligned}$$

我们可以验证 $g \in \text{Hom}(V, W)$. 由此, 我们可以构造一个映射

$$\begin{aligned} \varphi : V^* \times W &\rightarrow \text{Hom}(V, W), \\ (v^*, w) &\mapsto g_{(v^*, w)}. \end{aligned}$$

直接计算我们可以验证 φ 为一个双线性映射. 由张量积的泛性质, 我们有线性映射

$$\Phi : V^* \otimes W \rightarrow \text{Hom}(V, W),$$

满足任取简单张量 $v^* \otimes w \in V^* \otimes W$, 我们有

$$\Phi(v^* \otimes w) = g_{(v^*, w)}.$$

之前关于 $\text{Hom}(V, W)$ 中映射的讨论说明这是一个满射.

以下简单张量集

$$\{v_i^* \otimes w_j \mid 1 \leq i \leq m, 1 \leq j \leq n\},$$

为 $V^* \otimes W$ 的一个生成元组.

任取张量 $\alpha \in \ker \Phi$, 我们记其为

$$\alpha = \sum_{i=1}^m \sum_{j=1}^n r_{ij} v_i^* \otimes w_j.$$

对任意 $v \in V$, 我们有

$$\sum_{i=1}^m \sum_{j=1}^n r_{ij} v_i^*(v) w_j = 0_W.$$

我们取 $v = v_1$, 则有

$$\sum_{j=1}^n r_{1j} w_j = 0,$$

因此对任意 $1 \leq j \leq n$, 我们有 $r_{1j} = 0$. 类似地, 我们可以证明对任意 $1 \leq i \leq m$ 以及 $1 \leq j \leq n$, 我们有 $r_{ij} = 0$. 因此 α 为零张量. 由此可得 Φ 为同构. 我们称之为 $\text{Hom}(V, W)$ 和 $V^* \otimes W$ 之间的**自然同构**.

以上也证明了

$$\{v_i^* \otimes w_j \mid 1 \leq i \leq m, 1 \leq j \leq n\},$$

为 $V^* \otimes W$ 的一组基.

张量与 Hom 之间的伴随

任取有限维向量空间 U 和 V , 使用张量积的泛性质, 我们可以证明(留作练习)以下向量空间的同构:

$$U^* \otimes V^* \cong (U \otimes V)^*.$$

结合之前讨论过的张量积的结合律, 我们有以下观察: 任取有限维向量空间 U, V 和 W , 我们有以下一系列自然的线性同构

$$\begin{aligned} & \text{Hom}(U \otimes V, W) \\ & \cong (U \otimes V)^* \otimes W \\ & \cong U^* \otimes V^* \otimes W \\ & \cong U^* \otimes \text{Hom}(V, W) \\ & \cong \text{Hom}(U, \text{Hom}(V, W)). \end{aligned}$$

如果我们固定向量空间 V , 任取向量空间 W ,

- 我们可以通过将其与 V 做张量积得到一个新的向量空间 $W \otimes V$;
- 我们也可以通过考虑 V 到 W 的线性映射得到一个新的向量空间 $\text{Hom}(V, W)$.

例 23.4.1.

作为一个应用, 我们考虑 V 上的双线性型空间. 由之前的讨论, 我们可以将其等同于

$$\text{Hom}(V \otimes V, \mathbb{R}).$$

利用上边的伴随性质, 我们有自然的线性同构

$$\operatorname{Hom}(V \otimes V, \mathbb{R}) = \operatorname{Hom}(V, V^*).$$

考虑具体的元素, 我们记 $\varphi \in \operatorname{Hom}(V \otimes V, \mathbb{R})$, 则任取 v , 我们考虑

$$\varphi(v \otimes \cdot) : V \rightarrow \mathbb{R},$$

就得到了一个 V 上的线性函数. 以上提到的伴随性质告诉我们, 这样得到的

$$\begin{aligned} \Phi : \operatorname{Hom}(V \otimes V, \mathbb{R}) &\rightarrow \operatorname{Hom}(V, V^*), \\ \varphi &\mapsto (v \mapsto \varphi(v \otimes \cdot)), \end{aligned}$$

是一个线性同构.

以上同构

$$\operatorname{Hom}(U \otimes V, W) \cong \operatorname{Hom}(W, \operatorname{Hom}(V, W)),$$

告诉我们这两种构造新的线性空间的方法之间有一种伴随的性质, 通常被称作张量积与 Hom 的伴随性. 实际上这个结论对更一般的模也成立.

定理 23.4.2

记 R 和 S 为幺环. 任取右 R -模 K , (R, S) -模 M 和左 S -模 N , 则我们有群同构

$$\operatorname{Hom}_S(K \otimes_R M, N) \cong \operatorname{Hom}_R(K, \operatorname{Hom}_S(M, N)).$$

证明. 任取右 S -模同态

$$\varphi : K \otimes_R M \rightarrow N,$$

考虑 K 在简单张量上的限制, 则任取 $w \in K$, 我们构造

$$\begin{aligned} \Phi_w : M &\rightarrow N, \\ u &\mapsto \varphi(w \otimes_R u). \end{aligned}$$

利用张量积 $\otimes_R$ 的性质以及 φ 为 S -同态的事实, 我们可以通过直接计算验证 Φ_w 为一个右 S -同态.

由此我们有以下映射

$$\begin{aligned} \Phi : K &\rightarrow \operatorname{Hom}_S(M, N), \\ w &\mapsto \Phi_w. \end{aligned}$$

我们首先说明 $\operatorname{Hom}_S(M, N)$ 上有一个由以下映射

$$\begin{aligned} F : R \times \operatorname{Hom}_S(M, N) &\rightarrow \operatorname{Hom}_S(M, N), \\ (r, \alpha) &\mapsto (u \mapsto \alpha(ru)), \end{aligned}$$

给出的右 R -模结构. 任取 $\alpha, \beta \in \operatorname{Hom}_S(M, N)$, $r, s \in R$ 以及 $u \in M$, 我们有

$$\begin{aligned} \alpha((r+s)u) &= \alpha(ru + su) = \alpha(ru) + \alpha(su), \\ (\alpha + \beta)(ru) &= \alpha(ru) + \beta(ru), \\ \alpha(rsu) &= \alpha(r(su)), \\ \alpha(1_R u) &= \alpha(u). \end{aligned}$$

因此映射 F 给出 $\text{Hom}_S(M, N)$ 上一个右 R -模结构.

任取 $w, w_1, w_2 \in K, u \in M$ 以及 $r \in R$, 我们有

$$\begin{aligned}\Phi_{w_1+w_2}(u) &= \varphi((w_1 + w_2) \otimes_R u) = \varphi(w_1 \otimes_R u) + \varphi(w_2 \otimes_R u) \\ \Phi_{rw}(u) &= \varphi(wr \otimes_R u) = \varphi(w \otimes_R ru) = \Phi_w(ru) = (r\Phi_w)(u).\end{aligned}$$

因此 Φ 给出一个右 R -模同态. 由此, 我们有了映射

$$\begin{aligned}\Psi : \text{Hom}_S(K \otimes_R M, N) &\rightarrow \text{Hom}_R(K, \text{Hom}_S(M, N)), \\ \varphi &\mapsto \Phi.\end{aligned}$$

任取 $\varphi, \varphi' \in \text{Hom}_S(K \otimes_R M, N)$, 任取 $w \in K$, 任取 $u \in M$, 我们有

$$\Psi(\varphi + \varphi')_w(u) = (\varphi + \varphi')(w \otimes_R u) = \varphi(w \otimes_R u) + \varphi'(w \otimes_R u) = \Psi(\varphi)_w(u) + \Psi(\varphi')_w(u).$$

因此映射 Ψ 为一个群同态.

最后我们证明 Ψ 为同构. 任取 $\varphi \in \ker \Psi$, 则有对任意 w , $\Psi(\varphi)(w)$ 为零映射. 特别地, 对任意 $u \in M$ 我们有

$$0_N = \Psi(\varphi)_w(u) = \varphi(w \otimes u) = 0_N.$$

因此 φ 在简单张量上取值为 0_N . 由于简单张量生成张量积 $K \otimes_R M$, 同态 φ 为零映射. 因此 Ψ 为单同态.

另一方面, 任取 $\Phi \in \text{Hom}_R(K, \text{Hom}_S(M, N))$, 我们考虑

$$\begin{aligned}\Theta : K \times M &\rightarrow N, \\ (w, u) &\mapsto \Phi_w(u).\end{aligned}$$

由于 Φ 是一个右 R -模同态, 任取 $w, w_1, w_2 \in K, u, u_1, u_2 \in M$ 以及 $r \in R$, 我们有

$$\begin{aligned}\Theta(w_1 + w_2, u) &= \Phi_{w_1+w_2}(u) = \Phi_{w_1}(u) + \Phi_{w_2}(u) = \Theta(w_1, u) + \Theta(w_2, u), \\ \Theta(w, u_1 + u_2) &= \Phi_w(u_1 + u_2) = \Phi_w(u_1) + \Phi_w(u_2) = \Theta(w, u_1) + \Theta(w, u_2), \\ \Theta(wr, u) &= \Phi_{wr}(u) = (r\Phi_w)(u) = \Phi_w(ru) = \Theta(w, ru) + \Theta(w_2, u).\end{aligned}$$

因此 Θ 为一个 R -平衡映射. 由张量积的泛性质, 我们有群同态

$$\theta : K \otimes_R M \rightarrow N,$$

满足任取简单张量 $w \otimes_R u \in K \otimes_R M$, 都有 $\theta(w \otimes_R u) = \Theta(w, u)$.

由于 M 和 N 都是右 S 模, 我们可以进一步验证 θ 为一个右 S -模同态. 任取 $s \in S$, 考虑简单张量 $w \otimes_R u \in K \otimes_R M$, 我们有

$$\theta(w \otimes_R us) = \Theta(w, us) = \Phi_w(us) = s\Phi_w(u) = s\Theta(w, u) = s\theta(w \otimes_R u).$$

由于简单张量生成张量积 $K \otimes_R M$, 我们有 $\theta \in \text{Hom}_S(K \otimes_R M, N)$.

综上所述我们有群同构

$$\text{Hom}_S(K \otimes_R M, N) \cong \text{Hom}_R(K, \text{Hom}_S(M, N)).$$

□

第二十四章 模的正合列

模的扩张是我们从已有的模出发来得到新的模的一种常用方法. 在本章中我们将对模的扩张进行讨论. 为了方便讨论, 如无特别说明, 所有讨论中出现的模均为左模. 对右模的讨论与之类似.

24.1 模的扩张

记 R 为一个幺环, M 和 N 为 R -模. 设存在一个模满同态

$$\varphi : M \rightarrow N.$$

我们记 $K = \ker \varphi$. 由模同态基本定理, 我们有

$$M/K \cong N.$$

我们可以考虑下图

$$K \xrightarrow{j} M \xrightarrow{\varphi} N.$$

其中 j 为 K 到 M 的嵌入同态, 因此为单同态. 由 K 的定义, 我们有

$$\operatorname{Im} j = \ker \varphi.$$

通过模同态基本定理, 我们可以将 N 看作是 M 的商模. 如果我们知道 M 的信息, 以及 K 的信息, 就可以确定 N 的结构.

另一方面, 当我们观察上边的序列的时候, 我们也会好奇如果我们知道了 K 和 N 的信息, 我们是否可以反过来得到 M 的模的所有信息?

我们来看一个特殊的情况. 设 K 和 N 为两个左 R -模, 考虑它们的直和 $M = K \oplus N$. 此时我们有以下嵌入同态:

$$\begin{aligned} j_K : K &\rightarrow K \oplus N, \\ w &\mapsto (w, 0_N). \end{aligned}$$

同时, 我们也有

$$\pi_N : M \xrightarrow{\pi} M/K \xrightarrow{\cong} N.$$

综合以上的信息, 我们有下图:

$$K \xrightarrow{j_K} M \xrightarrow{\pi_N} N.$$

我们注意到 j_K 为单射, π_N 为满射, 且 $\operatorname{Im} j_K = \ker \pi_N$. 由模的直和的定义, 我们知道在这种情况下, 模 K 和 N 的结构完全决定模 M 的结构.

另一方面, 我们之前研究群的扩张的时候也讨论过下边的例子. 考虑以下群同态

$$\begin{aligned} \varphi : \mathbb{Z}_9 &\rightarrow \mathbb{Z}_3, \\ [n]_9 &\mapsto [n]_3. \end{aligned}$$

直接计算, 我们可得

$$K = \ker \varphi = \{[3n]_9 \mid n \in \mathbb{Z}\}.$$

我们有以下群序列

$$K \xrightarrow{j} \mathbb{Z}_9 \xrightarrow{\varphi} \mathbb{Z}_3,$$

其中 j 为 K 到 $\mathbb{Z}_9$ 的嵌入同态. 我们可以将以上交换群看作 $\mathbb{Z}$ -模, 则以上群同态均为 $\mathbb{Z}$ -模同态. 注意到 j 为单同态, φ 为满同态, 且有 $\operatorname{Im} j = \ker \varphi$, 而模 $\mathbb{Z}_9$ 并不同构于

$$K \oplus \mathbb{Z}_3 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3.$$

定义 24.1.1

记 K 和 N 为两个 R -模. 若 M 有一个子模 M' , 满足

$$M' \cong K \quad \text{且} \quad M/M' \cong N,$$

我们称 M 为 N 过 K 的**扩张**.

以上的例子告诉我们, 给定 K 和 N , 模 N 过 K 的扩张不一定唯一. 要研究一个扩张的性质, 我们需要知道关于扩张更多的信息.

24.2 模的正合列

记 R 为一个幺环. 在讨论模的扩张的时候, 我们有两个模同态 j 和 φ 给出以下 R -模序列

$$K \xrightarrow{j} M \xrightarrow{\varphi} N,$$

并且满足 j 为单同态, φ 为满同态以及 $\ker \varphi = \operatorname{Im} j$.

定义 24.2.1

任给两个 R -模同态 φ 和 ψ 给出的序列

$$X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z,$$

若 $\ker \psi = \operatorname{Im} \varphi$, 我们称该序列在 Y 处**正合**.

若一系列 R -模同态

$$\cdots \xrightarrow{\varphi_{k+2}} X_{k+1} \xrightarrow{\varphi_{k+1}} X_k \xrightarrow{\varphi_k} X_{k-1} \xrightarrow{\varphi_{k-1}} \cdots,$$

在任意两个相邻模同态之间的模处正合, 我们称这是一个 R -模的**正合列**.

注 24.2.2.

在写序列的时候, 若同态映射无歧义, 我们也可以将其省略.

我们记 0 为零模. 任给一个 R -模 A , 都有唯一的一个从零模出发的同态

$$0 \rightarrow A,$$

以及唯一的一个送到零模的同态

$$A \rightarrow 0.$$

定义 24.2.3

若同态序列

$$0 \longrightarrow X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \longrightarrow 0,$$

正合, 我们称其为一个**短正合列**.

命题 24.2.4

记 X, Y 和 Z 为左 R -模.

1) 序列

$$0 \longrightarrow X \xrightarrow{\varphi} Y,$$

在 X 处正合当且仅当 φ 为单同态;

2) 序列

$$Y \xrightarrow{\psi} Z \longrightarrow 0,$$

在 Z 处正合当且仅当 ψ 为满同态.

证明. 1) 零模到 X 的唯一的同态的像是 $\{0_X\}$. 因此序列在 X 处正合等价于

$$\ker \varphi = \{0_X\},$$

进而等价于 φ 为单同态.

2) 任意模到零模的同态的核为整个模, 因此序列在 Z 处正合等价于

$$\operatorname{Im} \psi = Z,$$

进而等价于 ψ 为满同态. □

考虑模的扩张的定义, 我们有以下推论.

推论 24.2.5

以下序列

$$0 \longrightarrow X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \longrightarrow 0,$$

为短正合列当且仅当 φ 为单同态, ψ 为满同态, $\operatorname{Im} \varphi = \ker \psi$, 即 Y 为 Z 过 X 的扩张.

在之前的例子中, 我们看到给定模 Z 过 X 不一定唯一. 我们可以通过短正合列之间的同态来比较不同的扩张.

定义 24.2.6

我们记

$$0 \longrightarrow X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \longrightarrow 0,$$

和

$$0 \longrightarrow X' \xrightarrow{\varphi'} Y' \xrightarrow{\psi'} Z' \longrightarrow 0,$$

为两个短正合列. 我们称模同态三元组 (α, β, γ) 为这两个短正合列之间的**同态**, 若 α , β 和 γ , 满足以下交换图

$$\begin{array}{ccccccc} 0 & \longrightarrow & X & \xrightarrow{\varphi} & Y & \xrightarrow{\psi} & Z \longrightarrow 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\ 0 & \longrightarrow & X' & \xrightarrow{\varphi'} & Y' & \xrightarrow{\psi'} & Z' \longrightarrow 0. \end{array}$$

若进一步有 α , β 和 γ 均为模同构, 我们称 (α, β, γ) 为两个短正合列之间的**同构**, 并称这两个短正合列**同构**, 我们称扩张 Y 和 Y' **同构**.

若 (α, β, γ) 为同构, 且进一步有 $X = X'$, $Z = Z'$, $\alpha = \text{id}_X$ 以及 $\gamma = \text{id}_Z$, 我们称两个短正合列**等价**. 我们称扩张 Y 和 Y' **等价**.

注 24.2.7.

以下例子说明正合列的同构和等价是不同的. 任取素数 p , 我们考虑 $\mathbb{Z}$ -模 $\mathbb{Z}$ 和 $\mathbb{Z}_p$, 以及以下三个模同态

$$\begin{array}{lll} \varphi: \mathbb{Z} \rightarrow \mathbb{Z} & \psi: \mathbb{Z} \rightarrow \mathbb{Z}_p & \psi': \mathbb{Z} \rightarrow \mathbb{Z}_p \\ m \mapsto mp & m \mapsto [m]_p & m \mapsto [2m]_p \end{array}$$

则以下两个短正合列

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\varphi} \mathbb{Z} \xrightarrow{\psi} \mathbb{Z}_p \longrightarrow 0,$$

和

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\varphi} \mathbb{Z} \xrightarrow{\psi'} \mathbb{Z}_p \longrightarrow 0,$$

同构但是不等价.

实际上当我们考虑两个短正合列之间的同态 (α, β, γ) 的时候, 三个同态 α , β 和 γ 并不是相互独立的.

命题 24.2.8 (短五引理)

设 (α, β, γ) 为两个短正合列之间的同态:

$$\begin{array}{ccccccc} 0 & \longrightarrow & X & \xrightarrow{\varphi} & Y & \xrightarrow{\psi} & Z \longrightarrow 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\ 0 & \longrightarrow & X' & \xrightarrow{\varphi'} & Y' & \xrightarrow{\psi'} & Z' \longrightarrow 0 \end{array}$$

- 1) 若 α 和 γ 为单同态, 则 β 为单同态;
- 2) 若 α 和 γ 为满同态, 则 β 为满同态;
- 3) 若 α 和 γ 为同构, 则 β 为同构.

证明. 1) 任取 $y \in \ker \beta$, 利用交换图我们有

$$\gamma(\psi(y)) = \psi'(\beta(y)) = 0.$$

由于 γ 为单射, 因此 $\psi(y) = 0_Z$, 我们进而有 $y \in \ker \psi$. 由第一行的序列在 Y 正合, 存在 $x \in X$, 满足

$$\varphi(x) = y.$$

利用交换图我们有

$$\varphi'(\alpha(x)) = \beta(\varphi(x)) = 0_{Y'}.$$

考虑第二行正合列, 由于 φ' 为单射, 我们有 $\alpha(x) = 0_{X'}$. 由于 α 为单射, 因此 $x = 0_X$. 由上可得

$$y = \varphi(x) = 0_Y.$$

因此 $\ker \beta = \{0_Y\}$, 同态 β 为单射.

2) 任取 $y' \in Y'$, 我们考虑 $\psi'(y') \in Z'$. 由于 γ 为满射, 因此存在 $z \in Z$, 满足

$$\gamma(z) = \psi'(y').$$

考虑第一行短正合列, 我们有 ψ 为满同态, 因此存在 $y \in Y$, 满足

$$\psi(y) = z.$$

考虑同态的复合, 我们有

$$\psi'(\beta(y)) = \gamma(\psi(y)) = \psi'(y').$$

由于 ψ' 为模同态, 我们有

$$\psi'(\beta(y) - y') = 0_{Z'}.$$

第二行序列为短正合列, 因此存在 $x' \in X'$, 满足

$$\varphi'(x') = \beta(y) - y'.$$

由于 α 为满射, 因此存在 $x \in X$, 满足

$$\alpha(x) = x'.$$

因此

$$\beta(\varphi(x)) = \varphi'(\alpha(x)) = \beta(y) - y'.$$

由于 β 为模同态, 移项可得

$$y' = \beta(y - \varphi(x)) \in \text{Im } \beta.$$

因此 β 为满同态.

3) 这是 1) 和 2) 的直接推论. □

注 24.2.9.

我们在讨论群的扩张的时候也用短正合列来给出群的扩张. 注意到在证明的过程中, 我们只用到了模中的群运算, 并且没有用到交换律. 因此这里的短五引理对群的短正合列也成立.

分裂扩张/分裂短正合列

任给一个模我们总是可以用直和给出其过另一个模的扩张.

定义 24.2.10

我们称短正合列

$$0 \longrightarrow X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \longrightarrow 0.$$

分裂, 若该正合列等价于直和给出的短正合列, 即有以下正合列的同构 $(\text{id}_X, \beta, \text{id}_Z)$,

$$\begin{array}{ccccccc} 0 & \longrightarrow & X & \xrightarrow{\varphi} & Y & \xrightarrow{\psi} & Z \longrightarrow 0 \\ & & \downarrow \text{id}_X & & \downarrow \beta & & \downarrow \text{id}_Z \\ 0 & \longrightarrow & X & \xrightarrow{j_X} & X \oplus Z & \xrightarrow{\pi_Z} & Z \longrightarrow 0 \end{array}$$

此时我们称 Y 为 Z 过 X **分裂扩张**.

如果 Z 过 X 的扩张 Y 分裂, 使用定义中的记号, 我们可以在 Y 中找到分别同构于 X 和 Z 的子模 $\varphi(X)$ 和 $\beta^{-1}(\{0_X\} \oplus Z)$, 满足

$$Y = \varphi(X) \oplus \beta^{-1}(\{0_X\} \oplus Z).$$

考虑到 X 到 Y 的单同态, 我们不妨把 X 看作是 Y 的一个子模. 因此研究一个扩张 Y 是否分裂就与研究以下问题相关: 是否存在 Y 中的子模 K , 满足 $K \cong Z$ 且 $Y = X \oplus K$?

实际上回答这个问题和回答 Y 是否分裂这个问题是等价的. 我们使用短正合列来给出这个结论.

命题 24.2.11

短正合列:

$$0 \longrightarrow X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \longrightarrow 0.$$

分裂当且仅当存在模同态 $s: Z \rightarrow Y$, 满足 $\psi \circ s = \text{id}_Z$.

注 24.2.12.

注意到 $Y/X \cong Z$, 我们可以从几何的角度将 Y 看作是以 Z 为底的 X -纤维丛, 每个纤维都是 X 的一个陪集. 我们可以在每个纤维里边取一个代表元, 从而构造一个映射

$$s: Z \rightarrow Y,$$

一般情况下, 这样的 s 并不能保持模结构. 以上命题告诉我们 Y 分裂当且仅当我们可以取到一个是模同态的 s . 这样的 s 被称为一个**截面**.

证明. 不妨设 X 为 Y 的一个子模, 同态 φ 为嵌入同态. 因此 $X = \text{Im } \varphi = \ker \psi$.

设 Y 是 Z 过 X 的分裂扩张, 由之前的讨论, 存在一个 Y 的子模 K , 满足

$$Y = X \oplus K \quad \text{且} \quad K \cong Z.$$

我们考虑 ψ 限制在 K 上给出了 K 和 Z 的一个模同构. 我们考虑这个同构的逆映射即给出了一个截面映射.

反过来, 若存在截面映射

$$s: Z \rightarrow Y,$$

我们记 $K = s(Z)$. 由于 $\psi \circ s = \text{id}_Z$, 我们有 s 为单同态, 且 $Z \cong K$. 下证 $Y = X \oplus s(Z)$.

首先证明 $Y = X + K$. 任取 $u \in Y$, 我们考虑 $s(\psi(u)) \in Y$. 注意到

$$\psi(u) = \psi(s(\psi(u))) = (\psi \circ s)(\psi(u)).$$

因此

$$u - s(\psi(u)) \in X,$$

我们有

$$u = (u - s(\psi(u))) + s(\psi(u)) \in X + K.$$

下证 $X \cap K = \{0_Y\}$. 记 $u \in X \cap K$, 由于

$$u \in \text{Im } \varphi = \ker \psi,$$

因此

$$\psi(u) = 0_Z.$$

从而有

$$u = s(\psi(u)) = s(0_Z) = 0_Y.$$

综上所述 $Y = X \oplus K$.

由之前的讨论, 同态 s 给出 Z 到 K 的同构, 仍记做 s . 我们构造模同态

$$\begin{aligned} \beta: X \oplus K &\rightarrow X \oplus Z \\ u + v &\mapsto (u, s^{-1}(v)) \end{aligned}$$

直接验证可得 $(\text{id}_X, \beta, \text{id}_Z)$ 为正合列的同构. 因此所讨论的正合列分裂. $\square$

由以上讨论, 当 Y 为 Z 过 X 的分裂扩张的时候, 我们仍将 X 看作 Y 的子模, 则存在 Y 的子模 K , 满足

$$Y = X \oplus K.$$

由此我们还有另一个观察就是, 存在一个模同态

$$\begin{aligned} t: X \oplus K (= Y) &\rightarrow X, \\ u + v &\mapsto u, \end{aligned}$$

满足 $t \circ \varphi = \text{id}_X$. 因此我们可以将 X 看作是 Y 的商模.

注意到这些结论在一般情况下是不一定成立的. 比如, 作为 $\mathbb{Z}$ -模, $\mathbb{Z}$ 就不能看作是 $\mathbb{Q}$ 的商模. 即便是可以看作商模, 满足以上性质的同态 t 是不一定存在的. 例如, $\mathbb{Z}_9$ 的子模 $3\mathbb{Z}_9$. 虽然我们可以使用 $\mathbb{Z}_9$ 通过乘以 3 得到一个模同态, 但是这个同态和 $3\mathbb{Z}_9$ 到 $\mathbb{Z}_9$ 的嵌入同态的复合是零同态. 实际上存在这样的同态 t 也等价于扩张是分裂的.

命题 24.2.13

短正合列:

$$0 \longrightarrow X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \longrightarrow 0.$$

分裂当且仅当存在模同态 $t: Y \rightarrow X$, 满足 $t \circ \varphi = \text{id}_X$.

证明. 不妨设 X 为 Y 的子模, 同态 φ 为嵌入同态.

设 Y 是 Z 过 X 的分裂扩张, 由之前的讨论, 存在一个 Y 的子模 K , 满足

$$Y = X \oplus K \quad \text{且} \quad K \cong Z.$$

我们考虑模同态

$$\begin{aligned} t: X \oplus K (= Y) &\rightarrow X, \\ u + v &\mapsto u, \end{aligned}$$

即满足 $t \circ \varphi = \text{id}_X$.

设存在模同态

$$t: Y \rightarrow X$$

满足 $t \circ \varphi = \text{id}_X$. 由此可得 t 为一个满同态.

我们记 $\ker t = K$ 为 Y 的一个子模, 下证 $Y = X \oplus K$.

任取 $u \in Y$. 我们有 $t(u) \in X$, 考虑

$$t(u - \varphi(t(u))) = t(u) - (t \circ \varphi)(t(u)) = 0.$$

因此 $u - \varphi(t(u)) \in \ker t$, 我们有

$$u = (u - \varphi(t(u))) + \varphi(t(u)) \in X + K.$$

因此 $Y = X + K$.

任取 $u \in X \cap K$, 我们有 $t(u) = 0_Y \in X$, 因此 $\varphi(t(u)) = 0_Y$. 因此 $X \cap K = \{0_Y\}$, 我们有

$$Y = X \oplus K.$$

由此可知

$$K \cong Y/X \cong Z.$$

我们记该同构为 $f: K \rightarrow Z$, 定义模同态

$$\begin{aligned} \beta: X \oplus K (= Y) &\rightarrow X \oplus Z, \\ u + v &\mapsto (u, f(v)). \end{aligned}$$

直接计算可得 $(\text{id}_X, \beta, \text{id}_Z)$ 为正合列的同构. 因此所讨论的正合列分裂. $\square$

24.3 投射模

记 R 为幺环. 记 M 为一个 R -自由模, 记 $\mathcal{B} \subset M$ 为 M 的一组基, 则任给 R -模 N , 以及任意映射

$$f: \mathcal{B} \rightarrow N,$$

我们都可以将其扩张为一个模同态(仍记做 f)

$$f: M \rightarrow N.$$

考虑一个短正合列

$$0 \longrightarrow X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \longrightarrow 0.$$

若 Z 为一个自由模, 我们记 $\mathcal{B}$ 为 Z 的一组基. 由于 ψ 为满射, 因此任取 $v \in \mathcal{B}$, 我们可以取 $u \in Y$, 满足

$$\psi(u) = v.$$

将 v 送到 $u \in \psi^{-1}(v)$, 我们可以得到映射

$$s : \mathcal{B} \rightarrow Y.$$

由自由模的泛性质, 我们可以将其扩展为一个模同态(仍记做 s)

$$s : Z \rightarrow Y.$$

注意到任取 s 满足 $\psi \circ s = \text{id}_Z$, 因此为一个截面映射. 由命题 24.2.11, 以上短正合列分裂, 模 Y 为 Z 过 X 的分裂扩张. 因此 $Y \cong X \oplus Z$.

考虑这个性质, 我们可以将自由模的概念推广的到以下定义.

定义 24.3.1

我们称一个 R -模 P 为**投射模**, 若其扩张总是分裂的, 等价地若任意短正合列

$$0 \longrightarrow X \xrightarrow{\varphi} Y \xrightarrow{\psi} P \longrightarrow 0,$$

都是分裂的.

由定义, 我们首先有以下投射模和自由模之间的一个关系:

命题 24.3.2

记 P 为一个 R -模. 模 P 为一个投射模当且仅当存在 R -模 Q , 满足 $Q \oplus P$ 为 R 自由模.

证明. 设模 P 为一个投射模. 记 S 为 P 的一组生成元, 以及 $F = R^{\oplus S}$ 为一个自由模. 将 $u \in S$ 对应的 F 的生成元送到 $u \in P$, 则由自由模的泛性质, 这个映射可以扩展为一个满同态

$$\psi : F \rightarrow P.$$

由此可得 F 为 P 过 $\ker \psi$ 的扩张. 由投射模的定义, 令 $Q = \ker \psi$, 我们有

$$F \cong P \oplus Q.$$

下边证明另一个方向. 设存在一个模 Q , 满足 $F = P \oplus Q$ 为一个自由模. 考虑短正合列

$$0 \longrightarrow X \xrightarrow{\varphi} Y \xrightarrow{\psi} P \longrightarrow 0.$$

记 π_P 为 F 到 P 的投影同态

$$\begin{aligned} \pi_P : P \oplus Q (= F) &\rightarrow P, \\ (u, v) &\mapsto u. \end{aligned}$$

由于 ψ 为满射, 任给 $u \in P$, 我们可以取 $y_u \in Y$, 满足 $\psi(y_u) = u$. 我们记 $\mathcal{B}$ 为 F 的一组基. 任取 $(u, v) \in \mathcal{B}$, 定义映射

$$\begin{aligned}\tilde{s} : \mathcal{B} &\rightarrow Y, \\ (u, v) &\mapsto y_u.\end{aligned}$$

利用自由模的泛性质, 映射 $\tilde{s}$ 可以扩展为一个模同态(仍记做 $\tilde{s}$):

$$\tilde{s} : F \rightarrow Y,$$

满足 $\psi \circ \tilde{s} = \pi_P$. 注意到 $\pi_P|_P = \text{id}_P$. 我们考虑 $\tilde{s}$ 在 P 上的限制, 得到模同态

$$s := \tilde{s}|_P : P \rightarrow Y,$$

满足 $\psi \circ s = \text{id}_P$. 因此 s 为一个截面映射. 由命题 24.2.11 可得以上短正合列分裂.

综上所述, 由定义模 P 为投射模. □

注 24.3.3.

由对称性, 我们知道 Q 也是投射模.

注 24.3.4.

虽然从定义看来, 投射模是自由模的推广, 我们还需要一个是投射模但不是自由模的例子来说明这个推广是非平凡的. 我们考虑以下 $\mathbb{Z}_6$ -模同构

$$\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3.$$

我们可以从元素个数看出 $\mathbb{Z}_3$ 和 $\mathbb{Z}_2$ 都不是 $\mathbb{Z}_6$ 自由模. 但是由以上命题, 告诉我们 $\mathbb{Z}_2$ 和 $\mathbb{Z}_3$ 作为 $\mathbb{Z}_6$ -模都是投射模.

由之前关于 PID 上自由模的子模的讨论, 我们有以下推论.

推论 24.3.5

若 D 为一个 PID, 则任意 D 上的投射模都是自由模.

注 24.3.6.

这个命题也告诉我们一个投射模的子模不一定是投射模. 我们考虑 $\mathbb{Z}_9$ 作为 $\mathbb{Z}_9$ -模. 考虑子模 $M = 3\mathbb{Z}_9$, 之前的讨论告诉我们不存在另一个子模 Q , 使得 $\mathbb{Z}_9 \cong M \oplus Q$ 成立. 因此作为 $\mathbb{Z}_9$ -模, M 不是投射模.

考虑到自由模的直和仍是自由模, 以下是命题 24.3.2 的另一个直接的推论.

推论 24.3.7

任取投射模 P_1 和 P_2 , 都有模 $P_1 \oplus P_2$ 为投射模.

证明. 任取 P_1 和 P_2 均为投射模, 则由命题 24.3.2, 存在模 Q_1 和 Q_2 , 满足 $P_1 \oplus Q_1$ 和 $P_2 \oplus Q_2$ 都是自由模. 因此

$$(P_1 \oplus P_2) \oplus (Q_1 \oplus Q_2) \cong (P_1 \oplus Q_1) \oplus (P_2 \oplus Q_2)$$

也是自由模, 因此由命题 24.3.2, 直和 $P_1 \oplus P_2$ 为投射模. □

由推论23.2.19, 自由模的张量积仍是自由模. 考虑张量积对直和满足分配律, 若系数环为交换幺环, 则命题 24.3.2 有如推论.

推论 24.3.8

设 R 交换幺环. 任取投射模 P_1 和 P_2 , 都有 $P_1 \otimes_R P_2$ 为投射模.

证明. 任取 P_1 和 P_2 均为投射模, 则由命题 24.3.2, 存在模 Q_1 和 Q_2 , 满足 $P_1 \oplus Q_1$ 和 $P_2 \oplus Q_2$ 都是自由模. 因此

$$(P_1 \oplus Q_1) \otimes_R (P_2 \oplus Q_2) \cong (P_1 \otimes_R P_2) \oplus ((P_1 \otimes_R Q_2) \oplus (P_2 \otimes_R Q_1) \oplus (Q_1 \otimes_R Q_2)).$$

也是自由模, 因此由命题 24.3.2, 直和 $P_1 \otimes_R P_2$ 为投射模. $\square$

在以上证明中, 我们发现虽然投射模 P 不一定是自由模, 但是似乎可以借助自由模来具有某种程度上的泛性质. 这个性质具体表述如下.

命题 24.3.9

记 P 为一个 R -模. 模 P 为投射模当且仅当以条件成立: 对任意 R -模 M 和 N , 若存在同态 $f: P \rightarrow N$, 以及满同态 $g: M \rightarrow N$, 则有模同态 $h: P \rightarrow M$, 使得以下交换图成立:

$$\begin{array}{ccc} & P & \\ h \swarrow & \downarrow f & \\ M & \xrightarrow{g} & N \end{array}$$

注 24.3.10.

以上命题说明投射模满足某种提升性质. 由以上等价性, 我们可以用满足命题中的提升性质来定义投射模. 实际上这也是 Cartan 和 Eilenberg 在 1956 年于他们的名为 Homological Algebra 的书作为对自由模的推广引入投射模这个概念时使用的定义. 此类模的一个特殊性质是一个短正合列中的模在与之作张量积之后仍得到一个短正合列(见后续对平坦模的讨论).

证明. 若 P 为投射模, 由命题 24.3.2, 存在一个模 Q , 满足 $P \oplus Q$ 是一个自由模.

记 M 和 N 为模. 设存在模同态

$$\begin{array}{ccc} & P & \\ & \downarrow f & \\ M & \xrightarrow{g} & N \end{array}$$

设 g 是满同态. 我们考虑 F 到 P 的投影同态

$$\begin{aligned} \pi_P: P \oplus Q &\rightarrow P, \\ (u, v) &\mapsto u. \end{aligned}$$

我们记 $\mathcal{B}$ 为 $P \oplus Q$ 的一组基. 由于 g 为满同态, 任取 $(u, v) \in \mathcal{B}$, 我们取 $w_u \in M$, 满足

$$g(w_u) = f(u).$$

由此可以定义一个映射

$$\begin{aligned}\tilde{h} : \mathcal{B} &\rightarrow M, \\ (u, v) &\mapsto w_u.\end{aligned}$$

映射 $\tilde{h}$ 可以扩展为一个模同态(仍记作 $\tilde{h}$):

$$\tilde{h} : P \oplus Q \rightarrow M,$$

满足 $g \circ \tilde{h} = f \circ \pi_P$. 注意到 $\pi_P|_P = \text{id}_P$. 考虑同态 $\tilde{h}$ 限制在 P 上则有同态

$$h := \tilde{h}|_P : P \rightarrow M,$$

满足 $g \circ h = f \circ \text{id}_P = f$.

$$\begin{array}{ccc} & P \oplus Q & \\ & \downarrow \pi_P & \\ & P & \\ \tilde{h} \swarrow & & \downarrow f \\ M & \xrightarrow{g} & N \end{array}$$

我们下边证明另一个方向. 我们将使用定义来证明若 P 满足命题中的条件, 则 P 为投射模. 任取短正合列

$$0 \longrightarrow K \longrightarrow M \xrightarrow{g} P \longrightarrow 0.$$

取 $N = P$ 以及 $f = \text{id}_P$.

$$\begin{array}{ccccccc} & & & & P & & \\ & & & & \downarrow \text{id}_P & & \\ & & h \swarrow & & & & \\ 0 & \longrightarrow & K & \longrightarrow & M & \xrightarrow{g} & P \longrightarrow 0. \end{array}$$

由条件, 存在同态 $h : P \rightarrow M$, 满足

$$g \circ h = \text{id}_P.$$

因此 h 为一个截面映射. 因此该短正合列分裂. 由定义模 P 为投射模. □

任取模 M, N 和 P , 记 $g : M \rightarrow N$ 为一个模同态. 任给同态

$$h : P \rightarrow M,$$

通过复合, 我们有模同态 $f = g \circ h : P \rightarrow N$. 任取 $h_1, h_2 \in \text{Hom}(P, M)$, 我们有

$$g \circ (h_1 + h_2) = g \circ h_1 + g \circ h_2.$$

因此与 g 复合给出了以下群同态

$$\begin{aligned}\Phi_g : \text{Hom}(P, M) &\rightarrow \text{Hom}(P, N), \\ h &\mapsto f = g \circ h.\end{aligned}$$

命题 24.3.9 告诉我们当 P 为投射模, g 为满同态的时候, 我们有另一个方向的映射.

$$\begin{aligned}\Psi_g : \text{Hom}(P, N) &\rightarrow \text{Hom}(P, M), \\ f &\mapsto h.\end{aligned}$$

这里由于构造提升的时候的选择, 我们不能得到映射 Ψ_g 为一个群同态. 不过作为映射, 我们仍有 $\Phi_g \circ \Psi_g = \text{id}_{\text{Hom}(P, N)}$, 因此同态 Φ_g 为满同态, 而映射 Ψ_g 为单射.

另一方面, 任取模 K , 以及一个同态

$$g' : K \rightarrow M,$$

通过与 g' 复合, 我们有群同态

$$\Phi_{g'} : \text{Hom}(P, K) \rightarrow \text{Hom}(P, M).$$

如果我们进一步有 g' 为模的单同态, 则 $\Phi_{g'}$ 为群的单同态. 这是因为任取 $\alpha, \beta \in \text{Hom}(P, K)$, 如果 $\alpha \neq \beta$, 则存在 $w \in K$, 满足

$$\alpha(w) \neq \beta(w).$$

由于 g' 为单同态, 因此

$$(g' \circ \alpha)(w) = g'(\alpha(w)) \neq g'(\beta(w)) = (g' \circ \beta)(w).$$

因此 $g' \circ \alpha \neq g' \circ \beta$.

将以上讨论与模扩张结合, 我们发现当 P 为一个投射模的时候, 通过考虑从 P 出发的模同态群, 如果 M 为 N 过 K 的模的扩张, 则 $\text{Hom}(P, M)$ 为 $\text{Hom}(P, N)$ 过 $\text{Hom}(P, K)$ 的群的扩张. 实际上这也是投射模的等价定义之一.

命题 24.3.11

模 P 为投射模, 当且仅当其满足以下条件: 任给一个模的短正合列

$$0 \longrightarrow K \xrightarrow{g'} M \xrightarrow{g} N \longrightarrow 0,$$

我们都有一个群的短正合列

$$0 \longrightarrow \text{Hom}(P, K) \xrightarrow{\Phi_{g'}} \text{Hom}(P, M) \xrightarrow{\Phi_g} \text{Hom}(P, N) \longrightarrow 0.$$

证明. 我们首先证明充分性, 即若 P 为投射模, 则以上条件满足. 之前的讨论已经证明了 $\Phi_{g'}$ 为单射, Φ_g 为满射. 任取 $\alpha \in \text{Hom}(P, K)$, 由于 $\text{Im } g' = \ker g$, 我们有 $g \circ g'$ 为零同态, 因此

$$(\Phi_g \circ \Phi_{g'})(\alpha) = g \circ (g' \circ \alpha) = (g \circ g') \circ \alpha = 0.$$

由此可得 $\text{Im } \Phi_{g'} \subset \ker \Phi_g$.

任取 $\beta \in \ker \Phi_g$, 我们有 $g \circ \beta$ 为零映射, 即

$$\text{Im } \beta \in \ker g = \text{Im } g'.$$

我们考虑下图

$$\begin{array}{ccc} & P & \\ & \downarrow \beta & \\ K & \xrightarrow{g'} & \text{Im } g' \end{array}$$

注意到 g' 为一个到 $\text{Im } g'$ 的满同态, 由于 P 为投射模, 由命题 24.3.9, 存在同态 $\alpha \in \text{Hom}(P, K)$, 使得以下交换图成立

$$\begin{array}{ccc} & P & \\ \alpha \swarrow & \downarrow \beta & \\ K & \xrightarrow{g'} & \text{Im } g' \end{array}$$

因此

$$\beta = g' \circ \alpha = \Phi_{g'}(\alpha) \in \text{Im } \Phi_{g'}.$$

由此可得 $\ker \Phi_g \subset \text{Im } \Phi_{g'}$, 结合之前的结论, 我们进而有

$$\text{Im } \Phi_{g'} = \ker \Phi_g.$$

由此可得, 序列

$$0 \longrightarrow \text{Hom}(P, K) \xrightarrow{\Phi_{g'}} \text{Hom}(P, M) \xrightarrow{\Phi_g} \text{Hom}(P, N) \longrightarrow 0,$$

为正合列.

另一个方向是命题 24.3.9 的直接推论. □

在证明 $\text{Im } \Phi_{g'} = \ker \Phi_g$ 的时候, 我们实际上不需要使用 P 为投射模这个条件, 只需要

$$0 \longrightarrow K \xrightarrow{g'} M \xrightarrow{g} N \longrightarrow 0,$$

为短正合列即可.

任给 $\beta \in \ker \Phi_g$, 我们需要构造一个同态 $\alpha \in \text{Hom}(P, K)$, 满足 $g' \circ \alpha = \beta$.

由于 $\text{Im } (\beta) \subset \ker g = \text{Im } g'$, 因此任取 $u \in P$, 存在 $w \in K$, 满足

$$\beta(u) = g'(w).$$

由短正合列的定义, 我们有 g' 为单射, 因此这样的 w 唯一. 我们有一个良好定义的映射

$$\begin{aligned} \alpha : P &\rightarrow K, \\ u &\mapsto w. \end{aligned}$$

下边需要证明 α 为一个模同态. 任取 $u, u_1, u_2 \in P$, 记 $v = \beta(u), v_1 = \beta(u_1), v_2 = \beta(u_2) \in M$, 任取 $r \in R$, 由

$$\begin{aligned} \beta(u_1 + u_2) &= v_1 + v_2 = g'(w_1 + w_2) \\ \beta(ru) &= rv = g'(rw) \end{aligned}$$

因此

$$\begin{aligned} \alpha(u_1 + u_2) &= w_1 + w_2 = \alpha(u_1) + \alpha(u_2), \\ \alpha(ru) &= rv = r\alpha(u). \end{aligned}$$

至此我们验证了 α 为一个模同态. 因此我们有以下命题

命题 24.3.12

记 P 为一个模. 任给一个模的短正合列

$$0 \longrightarrow K \xrightarrow{g'} M \xrightarrow{g} N \longrightarrow 0,$$

我们都有一个群的正合列

$$0 \longrightarrow \text{Hom}(P, K) \xrightarrow{\Phi_{g'}} \text{Hom}(P, M) \xrightarrow{\Phi_g} \text{Hom}(P, N).$$

证明. 在之前关于 $\text{Hom}(P, K)$ 处和 $\text{Hom}(P, M)$ 处正合的讨论都对一般的模成立, 因此有以上结论. □

注 24.3.13.

注意到 $\text{Hom}(P, \cdot)$ 将 R -模 M 送到一个交换群 $\text{Hom}(P, M)$. 并且 R -模之间的模同态可以给出同态群之间的群同态. 当我们介绍完范畴的概念之后, 实际上 $\text{Hom}(P, \cdot)$ 给出的是从 R -模的范畴到交换群的范畴的一个协变函子.

命题 24.3.12 中的结论说明这个函子是**左正合**的. 而命题 24.3.11 告诉我们, 一个模 P 是投射模, 当且仅当其对应的 $\text{Hom}(P, \cdot)$ 函子是正合的.

利用张量积和 Hom 的伴随性质, 我们可以给出推论 24.3.8 的另一个证明.

推论 24.3.8 的另一个证明. 设 R 为交换幺环. 我们只需证明结论对两个投射模的张量积成立.

任取 R -投射模 P_1 和 P_2 , 任取短正合列,

$$0 \longrightarrow K \longrightarrow M \longrightarrow N \longrightarrow 0,$$

由命题 24.3.11, 我们有短正合列

$$0 \longrightarrow \text{Hom}(P_2, K) \longrightarrow \text{Hom}(P_2, M) \longrightarrow \text{Hom}(P_2, N) \longrightarrow 0.$$

再次利用命题 24.3.11, 我们有短正合列

$$0 \longrightarrow \text{Hom}(P_1, \text{Hom}(P_2, K)) \longrightarrow \text{Hom}(P_1, \text{Hom}(P_2, M)) \longrightarrow \text{Hom}(P_1, \text{Hom}(P_2, N)) \longrightarrow 0.$$

利用张量积和 Hom 的伴随性质, 我们有短正合列

$$0 \longrightarrow \text{Hom}(P_1 \otimes_R P_2, K) \longrightarrow \text{Hom}(P_1 \otimes_R P_2, M) \longrightarrow \text{Hom}(P_1 \otimes_R P_2, N) \longrightarrow 0.$$

由命题 24.3.11, 模 $P_1 \otimes_R P_2$ 为投射模. □

24.4 入射模

入射模(于 1940 年左右由 Reinhold Baer 引入)可以被看作是与投射模对偶(笼统地理解为将所有箭头反向)的概念. 此类模具有某种与 $\mathbb{Z}$ -模 $\mathbb{Q}$ 类似的性质, 即如果 $\mathbb{Q}$ 可以通过同态 ι 嵌入到某个 $\mathbb{Z}$ -模 M 中, 则 M 可以写为 $\iota(\mathbb{Q})$ 与另一个子模的直和. 需要注意的是相较于之前对投射模的讨论, 对入射模的讨论比较复杂, 并多次用到了 Zorn 引理来进行讨论. 此外所谓的对偶也不是处处都可以进行的.

类似于投射模, 入射模也有多种等价的定义, 我们将从与投射模的提升性质对偶的性质出发进行讨论.

定义 24.4.1

我们称一个模 Q 为**入射模**, 若任取模同态 $f: K \rightarrow Q$ 以及模单同态 $g: K \rightarrow M$, 存在一个模同态 $h: M \rightarrow Q$, 满足 $f = h \circ g$, 即我们有以下交换图

$$\begin{array}{ccc} K & \xrightarrow{g} & M \\ f \downarrow & \swarrow h & \\ Q & & \end{array}$$

类似于投射模的情形, 利用同态的复合, 我们可以从模的正合列出发构造模的同态群的正合列, 并由此得到入射模的一个等价定义. 需要注意的是这里方向是反过来的.

命题 24.4.2

模 Q 为投射模, 当且仅当其满足以下条件: 任给一个模的短正合列

$$0 \longrightarrow K \xrightarrow{g} M \xrightarrow{g'} N \longrightarrow 0,$$

我们都有一个群的短正合列

$$0 \longrightarrow \operatorname{Hom}(N, Q) \xrightarrow{\Phi_{g'}} \operatorname{Hom}(M, Q) \xrightarrow{\Phi_g} \operatorname{Hom}(K, Q) \longrightarrow 0.$$

证明. 设 Q 为入射模. 设我们有短正合列

$$0 \longrightarrow K \xrightarrow{g} M \xrightarrow{g'} N \longrightarrow 0.$$

考虑复合与 g 复合, 我们有群同态

$$\begin{aligned} \Phi_g : \operatorname{Hom}(M, Q) &\rightarrow \operatorname{Hom}(K, Q), \\ h &\mapsto h \circ g. \end{aligned}$$

由入射模的定义, 我们同时也有另一个方向的映射

$$\Psi_g : \operatorname{Hom}(K, Q) \rightarrow \operatorname{Hom}(M, Q).$$

这里对任意 $f \in \operatorname{Hom}(K, Q)$, 我们有 $f = \Psi_g(f) \circ g$. 考虑 Φ_g 和 Ψ_g 的定义, 我们有

$$\Phi_g \circ \Psi_g = \operatorname{id}_{\operatorname{Hom}(K, Q)}.$$

因此 Φ_g 为满同态. 我们有正合列

$$\operatorname{Hom}(M, Q) \xrightarrow{\Phi_g} \operatorname{Hom}(K, Q) \longrightarrow 0.$$

考虑与同态 g' 的复合, 我们有群同态

$$\begin{aligned} \Phi_{g'} : \operatorname{Hom}(N, Q) &\rightarrow \operatorname{Hom}(M, Q), \\ \alpha &\mapsto \alpha \circ g'. \end{aligned}$$

由于 $\ker g' = \operatorname{Im} g$, 我们有 $\operatorname{Im} \Phi_{g'} \subset \ker \Phi_g$. 另一方面, 任取 $h \in \ker \Phi_g$, 则有 $h \circ g$ 为零映射. 由于 g' 为满同态, 任取 $v \in N$, 我们取 $u_v \in g'^{-1}(v)$, 定义

$$\alpha(u) = h(v).$$

直接计算可以验证 α 为一个模同态. 由此可知 $h \in \operatorname{Im} \Phi_{g'}$. 因此我们同时也有 $\ker \Phi_g \subset \operatorname{Im} \Phi_{g'}$. 综上所述, 我们有

$$\operatorname{Im} \Phi_{g'} = \ker \Phi_g.$$

因此以上群的正合列可以延长为

$$\operatorname{Hom}(N, Q) \xrightarrow{\Phi_{g'}} \operatorname{Hom}(M, Q) \xrightarrow{\Phi_g} \operatorname{Hom}(K, Q) \longrightarrow 0.$$

任取 $\alpha, \beta \in \operatorname{Hom}(N, Q)$, 若 $\alpha \neq \beta$, 则存在 $v \in N$, 满足 $\alpha(v) \neq \beta(v)$. 由于 g' 为满同态, 因此存在 $v \in M$, 有 $g'(v) = u$. 由此我们可得

$$\Phi_{g'}(\alpha)(v) = (\alpha \circ g')(v) \neq (\beta \circ g')(v) = \Phi_{g'}(\beta)(v).$$

所以 $\Phi_{g'}(\alpha) \neq \beta_{g'}(\beta)$, 同态 $\Phi_{g'}$ 为单射.

综上所述, 我们有群的正合列

$$0 \longrightarrow \text{Hom}(N, Q) \xrightarrow{\Phi_{g'}} \text{Hom}(M, Q) \xrightarrow{\Phi_g} \text{Hom}(K, Q) \longrightarrow 0.$$

由于存在满群同态 Φ_g , 我们可以直接验证入射模定义的条件, 因此 Q 为入射模. $\square$

类似于对投射模的讨论, 观察以上证明, 我们发现以上群的正合列中有一部分是对任意模 Q 均成立的.

命题 24.4.3

记 Q 为一个模. 任给一个模的正合列

$$0 \longrightarrow K \xrightarrow{g} M \xrightarrow{g'} N \longrightarrow 0,$$

我们都有一个群的正合列

$$0 \longrightarrow \text{Hom}(N, Q) \xrightarrow{\Phi_{g'}} \text{Hom}(M, Q) \xrightarrow{\Phi_g} \text{Hom}(K, Q).$$

注 24.4.4.

类似于 $\text{Hom}(P, \cdot)$ 将 R -模 M 送到一个交换群 $\text{Hom}(P, M)$, 这里 $\text{Hom}(\cdot, Q)$ 将模 M 送到一个交换群 $\text{Hom}(M, Q)$, 并且 R -模之间的模同态可以给出同态群之间的群同态. 当我们介绍完范畴的概念之后, 实际上 $\text{Hom}(P, \cdot)$ 给出的是从 R -模的范畴到交换群的范畴的一个反变函子(箭头反向).

命题24.4.3 中的结论说明这个函子是**左正合**的. 而命题 24.4.2 告诉我们, 一个模 Q 是入射模, 当且仅当其对应的 $\text{Hom}(\cdot, Q)$ 函子是正合的.

若 Q 为入射模, 作为一个特殊的情形, 对任意单同态 $g: Q \rightarrow M$, 存在群同态 $h: M \rightarrow Q$, 满足以下交换图

$$\begin{array}{ccc} Q & \xrightarrow{g} & M \\ \text{id}_Q \downarrow & \swarrow h & \\ Q & & \end{array}$$

由命题 24.2.13, 我们有以下命题.

命题 24.4.5

若 Q 为入射模, 则任意短正合列

$$0 \longrightarrow Q \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \longrightarrow 0,$$

分裂.

注 24.4.6.

该命题的逆命题也成立. 因此任意以上形式的短正合列分裂是 Q 为入射模的等价条件, 也可

以用来作为入射模的定义. 在证明关于投射模的类似的结论的时候, 我们实际上说明了任何模都是投射模的商模. 作为对偶的情形, 我们就需要说明任意模都是入射模的子模. 这个结论是成立的, 但是证明比较复杂.

我们首先介绍一个用来检测一个模是否为入射模的判据.

命题 24.4.7 (Baer 判据)

模 Q 为一个入射模当且仅当任取 R 的左理想 I , 任意 I 到 Q 的模同态都可以延拓为 R 到 Q 的模同态.

证明. 若 Q 为入射模, 我们考虑 I 到 R 的嵌入同态 ι , 这是一个单同态. 由入射模的定义, 任意 I 到 Q 的模同态 f 都可以扩展为 R 到 Q 的模同态 h (即满足 $h \circ \iota = f$).

下边证明另一个方向. 我们仍记 $\iota: I \rightarrow R$ 为嵌入模同态. 设任给模同态 $f: I \rightarrow Q$, 都存在模同态 $h: R \rightarrow Q$, 满足 $h \circ \iota = f$.

我们下边考虑模单同态 $g: K \rightarrow M$. 不妨设 K 为 M 的子模, g 为嵌入同态. 下边要证明任给模同态 $\alpha: K \rightarrow Q$, 都存在模同态 $\beta: M \rightarrow Q$, 满足 $\beta \circ g = \alpha$. 我们考虑二元组 (M', α') 其中 M' 为包含 K 的 M 的子模, $\alpha': M' \rightarrow Q$ 为模同态, 满足 $\alpha' \circ g = \alpha$. 我们称之为 (K, α) 的扩张. 考虑集合

$$\Omega := \{(M', \alpha') \mid (M', \alpha') \text{ 为 } (K, \alpha) \text{ 的扩张}\}.$$

我们可以在 Ω 上定义一个偏序关系:

$$(M', \alpha') \preceq (M'', \alpha'') \Leftrightarrow M' \subset M'' \text{ 且 } \alpha''|_{M'} = \alpha'.$$

注意到 $(K, \alpha) \in \Omega$, 因此 Ω 非空. 由 Zorn 引理, 集合 Ω 中存在关于以上偏序关系的极大元 (M_0, α_0) .

若 $M_0 \neq M$, 任取 $u \in M \setminus M_0$, 我们定义

$$I := \{r \in R \mid ru \in M_0\}.$$

直接验证可得 I 为 R 的左理想. 我们定义

$$\begin{aligned} f: I &\rightarrow Q, \\ r &\mapsto \alpha_0(ru). \end{aligned}$$

直接验证可得 f 为模同态. 由条件 f 可以扩展为一个模同态 $h: R \rightarrow Q$, 满足 $h \circ \iota = f$.

下边考虑 M 的子模 $M_1 = M_0 + Ru$. 我们定义

$$\begin{aligned} \alpha_1: M_1 &\rightarrow Q, \\ v + ru &\mapsto \alpha_0(v) + h(r). \end{aligned}$$

首先验证以上定义良好. 若 $v_1 + r_1u = v_2 + r_2u$, 则有

$$(r_1 - r_2)u = v_2 - v_1 \in M_0.$$

因此 $r_1 - r_2 \in I$. 我们进而有

$$\begin{aligned} &h(r_1) - h(r_2) \\ &= h(r_1 - r_2) \\ &= f(r_1 - r_2) \\ &= \alpha_0((r_1 - r_2)u) \\ &= \alpha_0(v_2 - v_1) \\ &= \alpha_0(v_2) - \alpha_0(v_1). \end{aligned}$$

由此可得 $\alpha_1(v_1 + r_1 u) = \alpha_1(v_2 + r_2 u)$, 映射 α_1 定义良好. 直接验证定义可得 α_1 为模同态, 并且满足 $\alpha_1|_{M_0} = \alpha_0$. 因此 $(M_1, \alpha_1) \in \Omega$, 且

$$(M_0, \alpha_0) \prec (M_1, \alpha_1).$$

这与 (M_0, α_0) 为极大元矛盾. 因此 $M_0 = M$. 我们有如下交换图

$$\begin{array}{ccc} K & \xrightarrow{g} & M \\ \alpha \downarrow & \swarrow \alpha_0 & \\ Q & & \end{array}$$

综上所述 Q 为入射模. □

我们下边介绍这个命题在 R 为 PID 时的一个推论. 为此, 我们先介绍一个概念.

定义 24.4.8

我们称一个模 M **可除**, 若任取 $a \in R^*$, 映射

$$\begin{aligned} \Phi_a : M &\rightarrow M, \\ u &\mapsto au, \end{aligned}$$

为满射.

注 24.4.9.

记 $a \in R^*$. 条件 Φ_a 为满射并不一定给出 Φ_a 为单射. 我们可以考虑 $\mathbb{Z}$ -模 $\mathbb{Q}$. 任取 $p/q \in \mathbb{Q}$, 其中 $p \in \mathbb{Z}, q \in \mathbb{Z}^*$. 任取 $n \in \mathbb{Z}^*$, 任取 $p/q \in \mathbb{Q}$, 考虑 $p/nq \in \mathbb{Q}$, 我们有

$$n \frac{p}{nq} = \frac{p}{q}.$$

注意到此时 Φ_n 为双射.

下边考虑商模 $\mathbb{Q}/\mathbb{Z}$, 使用之前的记号, 任取 $p/q \in \mathbb{Q}$, 我们记 $[p/q]$ 为 p/q 在自然同态下的像. 任取 $n \in \mathbb{Z}^*$, 我们有

$$n \left[\frac{p}{q} \right] = \left[\frac{np}{q} \right].$$

由于左乘 n 和自然同态均为满射, 因此 $\mathbb{Q}/\mathbb{Z}$ 仍是可除模.

注意到任取 $k \in \mathbb{Z}$, 我们有

$$n \left[\frac{p + kq}{nq} \right] = \left[\frac{p}{nq} \right] = \left[\frac{p}{q} \right].$$

因此 $n \neq \pm 1$ 时, 则映射 Φ_n 不是单射.

利用直和的定义和类似于以上注记中对 $\mathbb{Q}$ 的讨论, 我们有如下观察.

观察 24.4.10

可除模的直和和商模都是可除模.

命题 24.4.7 有以下关于可除性的推论.

推论 24.4.11

若 R 无零因子, 则任何入射模都是可除的. 若 R 的任意左理想都是主理想, 则任意可除的 R -模都是入射模.

证明. 设 Q 为一个入射模. 任取 R 的左理想 I , 记 $\iota: I \rightarrow R$ 为嵌入同态. 由入射模的定义, 任给同态

$$f: I \rightarrow Q,$$

都可以扩张为一个

$$h: R \rightarrow Q.$$

我们需要证明任取 $r \in R^*$, 任取 $u \in M$, 存在 $v \in M$, 满足 $u = rv$.

我们考虑 I 为 $r \in R$ 生成的左理想 Rr . 记 $u \in M$. 定义映射

$$\begin{aligned} f: Rr &\rightarrow M, \\ sr &\mapsto su. \end{aligned}$$

由于 R 无零因子, 因此任取 $s, t \in R$ 以及 $r \in R$, 若 $sr = tr$, 则有 $s = t$. 因此映射 f 定义良好. 直接计算可以验证 f 为一个模同态. 由 Q 为一个入射模, 存在同态 f 的扩张

$$h: R \rightarrow M.$$

记 $v = h(1)$. 我们有

$$u = f(r) = h(r) = rh(1) = rv.$$

以上说明任取 $u \in M$, 存在 $v \in M$, 满足 $u = rv$. 因此映射

$$\begin{aligned} \Phi_r: M &\rightarrow M, \\ v &\mapsto rv. \end{aligned}$$

为满射. 从上所述 M 为可除模.

若 R 的任何左理想都是主理想, 则任取 R 的左理想 I , 存在 $r \in R$, 满足 $I = Rr$.

若 $I = \{0_R\}$ 为零理想, 则存在唯一的从 I 到 M 的模同态将 0_R 送到 0_M . 我们考虑 R 到 M 的零同态即为其扩张.

下设左理想 I 不是零理想, 则存在 $r \in R^*$, 满足 $I = Rr$. 任意 I 到 M 的模同态 f 都由 $f(r)$ 决定. 任取 $s \in R$, 我们有

$$f(sr) = sf(r).$$

由于 M 为可除模, 因此映射

$$\begin{aligned} \Phi_r: M &\rightarrow M, \\ v &\mapsto rv, \end{aligned}$$

为满射. 我们记 $w \in R$, 满足 $u = rw$.

注意到 R 为 R 自由模, 且 1_R 为 R 的基. 由自由模的泛性质, 我们可以定义以下同态 h :

$$\begin{aligned} h: R &\rightarrow M, \\ s &\mapsto sw. \end{aligned}$$

进一步地, 我们可以验证任取 $s \in R$ 都有

$$f(sr) = su = srw = srh(1_R) = h(sr).$$

因此 $f = h \circ \iota$, 其中 ι 为 I 到 R 的嵌入同态.

由 Baer 判据可知 M 为入射模. □

由此我们可以得到 PID 上模为入射模的一个等价条件.

推论 24.4.12

若 R 为 PID, 任取 R -模 M , 则 M 为入射模当且仅当 M 为可除模.

我们下边将通过一系列的引理来证明以下定理. 这个证明是由 B.Eckmann 和 A.Schöpf 给出的.

定理 24.4.13

任何模 Q 都可以嵌入到一个入射模中.

引理 24.4.14

任何 $\mathbb{Z}$ -模都可以嵌入到一个可除 $\mathbb{Z}$ -模中.

证明. 记 G 为一个交换群. 任意交换群都可以看作是自由交换群的商群. 设 F 为 X 生成的交换群, 以及 K 为 F 的子群, 满足

$$G \cong F/K.$$

不妨设 $G = F/K$.

我们考虑 X 生成的 $\mathbb{Q}$ -线性空间 V . 作为加法群 V 为加法群, 且在同构意义下, 群 F 可以看作是 V 的子群. 我们考虑 V/K , 则有 $G < V/K$.

在之前的注记中, 我们证明了 $\mathbb{Q}$ 为 $\mathbb{Z}$ 上可除模. 由观察 24.4.10, 我们有 V 为可除模, 进而有 V/K 为可除模. $\square$

推论 24.4.15

任何 $\mathbb{Z}$ -模都可以嵌入到一个入射 $\mathbb{Z}$ -模中.

证明. 由于 $\mathbb{Z}$ 为 PID, 因此 $\mathbb{Z}$ -模 M 可除当且仅当其为入射模. 由之前引理可得此推论. $\square$

命题 24.4.16

若 Q 为一个入射 $\mathbb{Z}$ -模, 则 $\text{Hom}_{\mathbb{Z}}(R, Q)$ 为一个入射 R -模.

证明. 任取 $f \in \text{Hom}_{\mathbb{Z}}(R, Q)$, 以及 $r \in R$, 我们定义

$$\begin{aligned} f_r &: R \rightarrow Q, \\ s &\mapsto f(sr). \end{aligned}$$

直接计算可以验证 f 为一个 $\mathbb{Z}$ -模同态. 由此, 我们可以得到如下映射

$$\begin{aligned} \Phi &: R \times \text{Hom}_{\mathbb{Z}}(R, Q) \rightarrow \text{Hom}_{\mathbb{Z}}(R, Q), \\ (r, f) &\mapsto f_r. \end{aligned}$$

任取 $r, s, t \in R$, $f, g, h \in \text{Hom}_{\mathbb{Z}}(R, Q)$, 我们有

$$\begin{aligned} f_{r+s}(t) &= f(t(r+s)) = f(tr) + f(ts) = f_r(t) + f_s(t), \\ (f+g)_r(t) &= (f+g)(tr) = f(tr) + g(tr) = f_r(t) + g_r(t), \\ f_{rs}(t) &= f(t(rs)) = f((tr)s) = (f_s)(tr) = (f_s)_r(t), \\ f_{1_R}(t) &= f(t). \end{aligned}$$

因此映射 Φ 给出了 $\text{Hom}_{\mathbb{Z}}(R, Q)$ 上一个左 R -模结构.

设存在 R -模单同态 $g: K \rightarrow M$, 不妨设 K 为 M 的子模, g 为嵌入同态. 设存在 R -模同态

$$f: K \rightarrow \text{Hom}_{\mathbb{Z}}(R, Q).$$

注意到任取 $w \in K$, 我们有 $\mathbb{Z}$ -模同态:

$$f(w): R \rightarrow Q,$$

由于 f 为 R -模同态, 任取 $s \in R$, 我们有

$$f(rw)(s) = f(w)(sr).$$

因此我们有如下 R -平衡映射

$$\begin{aligned} \varphi: R \times K &\rightarrow Q \\ (s, w) &\mapsto f(w)(s) \end{aligned}$$

由此我们得到一个群同态

$$\Phi: R \otimes_R K \rightarrow Q,$$

满足任取 $s \in R, w \in K$, 我们有 $\Phi(s \otimes_R w) = \varphi(s, w)$.

由于 K 为左 R -模, 因此我们有左 R -模同构 $R \otimes_R K \cong K$. 类似的, 我们有左 R -模同构 $R \otimes_R M$. 因此左 R -模单同态 g 诱导以下左 R -模单同态

$$\tilde{g}: R \otimes_R K \rightarrow R \otimes_R M,$$

满足任取 $s \in R$ 以及 $w \in K$, 我们有 $\tilde{g}(s \otimes_R w) = s \otimes_R g(w)$.

由于 Q 为 $\mathbb{Z}$ 上的入射模, 存在 $\mathbb{Z}$ -模同态

$$\Psi: R \otimes_R M \rightarrow Q,$$

满足 $\Phi = \Psi \circ \tilde{g}$.

由此任取 $s \in R$ 以及 $u \in M$, 我们可以定义

$$h(u)(s) = \Psi(s \otimes u).$$

因此

$$h(u): R \rightarrow Q,$$

为一个 $\mathbb{Z}$ -模同态. 我们进而有

$$\begin{aligned} h: M &\rightarrow \text{Hom}_{\mathbb{Z}}(R, Q), \\ u &\mapsto h(u). \end{aligned}$$

由 Ψ 为一个 $\mathbb{Z}$ -模同态, 以及张量积的性质, 我们有 h 为一个 $\mathbb{Z}$ -模同态. 要验证 h 为一个 R -模同态, 我们只需要验证任取 $u \in M$ 以及 $r, s \in R$, 我们有

$$h(ru)(s) = h(u)(sr).$$

这个是由于

$$h(ru)(s) = \Psi(s \otimes_R ru) = \Psi(sr \otimes_R u) = h(u)(sr).$$

综上所述 $\text{Hom}_{\mathbb{Z}}(R, Q)$ 为一个 R 上入射模. □

下边我们给出定理 24.4.13 的证明.

定理 24.4.13 的证明. 任给 R 模 M , 任给 R 到 M 的 R -模同态 f , 由于 1_R 为自由模 R 的基, 因此 f 由 $f(1_R)$ 确定. 由此我们可以构造以下 R -模同构

$$\begin{aligned}\mathrm{Hom}_R(R, M) &\rightarrow M, \\ f &\mapsto f(1).\end{aligned}$$

注意到 R -模同态也是 $\mathbb{Z}$ -模同态, 我们有以下包含关系

$$\mathrm{Hom}_R(R, M) \subset \mathrm{Hom}_{\mathbb{Z}}(R, M).$$

我们记 Q 为包含 M 的 $\mathbb{Z}$ 上入射模. 考虑与 M 到 Q 的嵌入同态复合, 我们有

$$j : \mathrm{Hom}_{\mathbb{Z}}(R, M) \rightarrow \mathrm{Hom}_{\mathbb{Z}}(R, Q).$$

因此存在一个从 M 到一个 R 上入射模 $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ 的嵌入. 我们可以进一步验证每个包含或者嵌入都是 R -模同态. 因此 R -模 M 可以嵌入一个 R 上入射模. $\square$

利用定理 24.4.13, 我们可以证明命题 24.4.5 的逆命题.

命题 24.4.17

记 Q 为一个模. 若任意短正合列

$$0 \longrightarrow Q \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \longrightarrow 0,$$

都分裂, 则 Q 为一个入射模.

证明. 记 Q 为一个模, 满足任意短正合列

$$0 \longrightarrow Q \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \longrightarrow 0,$$

都分裂.

由定理 24.4.13, 我们可以选 M 为包含 Q 的入射模. 任取模单同态 $g : K \rightarrow N$, 以及模同态 $f : K \rightarrow Q$, 我们考虑 φ 有下图:

$$\begin{array}{ccc} K & \xrightarrow{g} & N \\ f \downarrow & & \\ Q & & \\ \varphi \downarrow & & \\ M & & \end{array}$$

由于 M 为入射模, 因此存在模同态 $h_0 : N \rightarrow M$, 满足 $h_0 \circ g = \varphi \circ f$.

考虑短正合列, 由命题 24.2.13, 存在同态 $t : M \rightarrow Q$, 满足 $t \circ \varphi = \mathrm{id}_Q$.

因此我们考虑模同态 $h = t \circ h_0$, 则有

$$h \circ g = (t \circ h_0) \circ g = t \circ (h_0 \circ g) = t \circ (\varphi \circ f) = (t \circ \varphi) \circ f = f.$$

因此 Q 为入射模. 以上各映射满足以下交换图

$$\begin{array}{ccc}
 K & \xrightarrow{g} & N \\
 f \downarrow & \searrow h & \\
 Q & & \\
 \varphi \uparrow \downarrow t & \nearrow h_0 & \\
 M & &
 \end{array}$$

□

在证明了每个模都可以嵌入到一个入射模中之后, 一个自然的问题就是: 是否存在一个典范的入射模的选择? 我们将看到在同构意义下, 任给模 M , 都存在一个最小的包含 M 的入射模.

我们首先引入以下定义.

定义 24.4.18

我们称一个模同态 $\iota: K \rightarrow M$ 是**本质的**, 若任取 M 的子模 N , 都有

$$\{0_M\} \subsetneq N \cap \iota(K).$$

注 24.4.19.

作为平凡例子, 任意满同态都是本质的.

我们可以用本质的单同态来给出入射模的一种刻画.

命题 24.4.20

模 Q 为入射模当且仅当任意从 Q 出发的本质单同态都是同构.

证明. 设 Q 为一个入射模. 任取 $\iota: Q \rightarrow M$ 为一个本质的单同态, 我们有短正合列

$$0 \longrightarrow Q \xrightarrow{\iota} M \xrightarrow{\pi} M/\iota(Q) \longrightarrow 0,$$

其中 π 为自然同态. 由于 Q 为入射模, 以上短正合列分裂, 因此存在 M 的子模 $K \cong M/\iota(Q)$, 满足 $M = \iota(Q) \oplus K$. 由于 ι 是本质的, 因此 $K = \{0_M\}$. 由此可得 ι 为满同态. 由于 ι 也是单同态, 因此为同构.

反过来, 设模 Q 满足任意从 Q 出发的本质单同态都是同构, 我们将证明任意短正合列

$$0 \longrightarrow Q \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \longrightarrow 0,$$

都分裂.

我们考虑 Y 中与 Q 交集为零模的子模. 这类子模构成的集合 Ω 上存在由包含给出的偏序关系. 由 Zorn 引理知道, 集合 Ω 中存在一个极大元记作 M . 我们考虑 Y/M . 由于 $M \cap Q = \{0_Y\}$, 我们有 Q 到 Y/M 的嵌入同态, 记作 φ' . 下边证明这个嵌入是本质的. 否则存在一个元素 $y \in Y \setminus M$, 满足

$$\varphi'(Q) \cap R(y + M) = M.$$

因此

$$Q \cap (Ry + M) = \{0_Y\}.$$

由于 $M \subsetneq Ry + M$, 这与 M 极大矛盾. 因此 φ' 为本质的. 由假设, 我们有 φ' 为同构. 由此可得

$$Y = \varphi(Q) \oplus M.$$

由此可得存在一个 Y 到 Q 的同态 t , 满足 $t \circ \varphi = \text{id}_Q$. 由命题 24.2.13, 我们有以上短正合列分裂.

由命题 24.4.17 可得 Q 为入射模. □

命题 24.4.21

任给模 M , 都存在入射模 Q , 满足 M 可以通过本质单同态嵌入到 Q 中.

证明. 任取模 M , 由定理 24.4.13, 存在入射模 Q_0 以及单同态

$$\iota_0 : M \rightarrow Q_0.$$

考虑 Q_0 中任意包含 $\iota_0(M)$ 的子模 N , 我们可以通过限制 ι_0 的像集到 N 来得到一个模同态

$$\iota_N : M \rightarrow N.$$

考虑所有满足 ι_N 为本质同态的子模 N 构成的集合

$$\Omega := \{N \mid \iota_N \text{ 为本质同态}\}.$$

集合 Ω 上有由集合包含关系给出的偏序关系. 由 Zorn 引理知, 集合 Ω 中存在关于包含关系的极大元, 记作 Q .

我们将证明 Q 为入射模. 记 $j : Q \rightarrow Q_0$ 为恒等嵌入同态. 任取本质单同态 $g : Q \rightarrow N$, 由于 Q_0 为入射模, 由入射模的定义, 存在同态 $h : N \rightarrow Q_0$, 满足 $j = h \circ g$.

$$\begin{array}{ccc} Q & \xrightarrow{g} & N \\ j \downarrow & \swarrow h & \\ Q_0 & & \end{array}$$

记 $u \in \ker h \cap \text{Im } g$, 存在 $v \in Q$, 满足我们有 $(h \circ g)(v) = 0_{Q_0}$. 由于 $h \circ g = j$, 因此 $v = 0_{Q_0}$, $u = 0_N$. 所以 N 中有子模 $\ker h \oplus \text{Im } g$.

由于 g 是本质单同态, 因此 $\ker h = \{0_N\}$. 由此可得 h 为单同态. 记 $Q' = \text{Im } h \subset Q_0$.

由于 ι_Q 和 g 都是本质单同态, 因此

$$g \circ \iota_Q : M \rightarrow N,$$

也是本质单同态. 由此可得 $\iota_{Q'}$ 也是本质单同态, 从而有 $Q \subset Q' \in \Omega$. 由于 Q 极大, 因此 $Q' = Q$. 我们有 $\text{Im } h = Q$. 因此 h 为 Q 和 N 的同构.

由命题 24.4.20 可知 Q 为入射模. □

定义 24.4.22

任给模 M , 我们称命题 24.4.21 中给出地入射模为 M 的一个入射包.

我们下边证明任意模的入射包在同构意义下是唯一的.

命题 24.4.23

记 M 为一个模. 设存在本质的单同态 $\iota_1 : M \rightarrow Q_1$ 和 $\iota_2 : M \rightarrow Q_2$, 满足 Q_1 和 Q_2 都是入射模, 则存在模同构 $h : Q_1 \rightarrow Q_2$, 使得下图交换

$$\begin{array}{ccc} M & \xrightarrow{\iota_1} & Q_1 \\ \downarrow \iota_2 & \swarrow h & \\ & & Q_2 \end{array}$$

证明. 若 M , ι_1 和 ι_2 满足命题条件, 则由入射模的定义, 我们有同态

$$h : Q_1 \rightarrow Q_2,$$

满足以上交换图.

使用命题 24.4.21 的证明, 我们有 h_1 为单同态. 由于 ι_2 为本质的, 且 $\iota_2 = h \circ \iota_1$, 我们有 h 为本质的. 命题 24.4.20 告诉我们 h 为一个模同构. $\square$

24.5 平坦模

在本章的最后, 我们考虑模扩张和模的张量积之间的关系.

在前一节关于入射模的讨论中, 我们证明了任取 R -模 M , 我们有 $R \otimes_R M$ 同构于 M . 实际上使用张量积与直和之间的关系, 我们还可以得到以下结论.

命题 24.5.1

记 M 为一个左 R -模, 任取 $n \in \mathbb{N}^*$, 我们有模同构 $R^{\oplus n} \otimes_R M \cong M^{\oplus n}$.

另一方面, 任取 K 到 M 的同态 φ , 任取 $n \in \mathbb{N}^*$, 考虑同态的直和, 我们有以下同态

$$\begin{aligned} \varphi^{\oplus n} : K^{\oplus n} &\rightarrow M^{\oplus n}, \\ (w_1, \dots, w_n) &\mapsto (\varphi(w_1), \dots, \varphi(w_n)), \end{aligned}$$

并有以下关系

$$\begin{aligned} \text{Im}(\varphi^{\oplus n}) &= (\text{Im } \varphi)^{\oplus n}, \\ \ker(\varphi^{\oplus n}) &= (\ker \varphi)^{\oplus n}. \end{aligned}$$

利用这些观察, 我们有以下结论.

命题 24.5.2

任给短正合列

$$0 \longrightarrow K \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0,$$

任取 $n \in \mathbb{N}^*$, 我们有以下正合列

$$0 \longrightarrow R^{\oplus n} \otimes_R K \xrightarrow{\varphi^{\oplus n}} R^{\oplus n} \otimes_R M \xrightarrow{\psi^{\oplus n}} R^{\oplus n} \otimes_R N \longrightarrow 0,$$

考虑到投射模和自由模之间的关系, 我们有以下推论.

推论 24.5.3

记右 R -模 P 为一个投射模, 任给短正合列

$$0 \longrightarrow K \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0,$$

任取 $n \in \mathbb{N}^*$, 我们有以下正合列

$$0 \longrightarrow P \otimes_R K \xrightarrow{1_P \otimes \varphi} P \otimes_R M \xrightarrow{1_P \otimes \psi} P \otimes_R N \longrightarrow 0.$$

证明. 由命题 24.3.2, 存在模 Q , 满足 $F = P \oplus Q$ 为一个自由模. 为方便讨论, 我们将 P 和 Q 看作 F 的子模, 以上直和为内直和.

任取模同态 $f: X \rightarrow Y$, 我们考虑同态的张量积 $1_F \otimes f$, 则有同态

$$1_F \otimes f: F \otimes_R X \rightarrow F \otimes_R Y.$$

考虑张量积关于直和的分配律, 我们有

$$\begin{aligned} (P \oplus Q) \otimes_R X &= (P \otimes_R X) \oplus (Q \otimes_R X), \\ (P \oplus Q) \otimes_R Y &= (P \otimes_R Y) \oplus (Q \otimes_R Y). \end{aligned}$$

考虑 $1_F \otimes f$ 分别在 $P \otimes_R X$ 和 $Q \otimes_R X$ 上的限制, 考虑简单张量的像, 我们有

$$\begin{aligned} (1_F \otimes f)|_{P \otimes_R X} &= 1_P \otimes f, \\ (1_F \otimes f)|_{Q \otimes_R X} &= 1_Q \otimes f, \end{aligned}$$

且有 $\text{Im}(1_P \otimes f) \subset P \otimes_R Y$ 以及 $\text{Im}(1_Q \otimes f) \subset Q \otimes_R Y$.

因此若 f 为单同态, 则 $1_P \otimes f$ 为单同态. 若 f 为满同态, 则 $1_P \otimes f$ 为满同态. 若有另一个模同态

$$g: Y \rightarrow Z,$$

满足 $\text{Im } f = \ker g$, 则有 $\text{Im}(1_P \otimes f) = \ker(1_P \otimes g)$.

任给短正合列

$$0 \longrightarrow K \longrightarrow M \longrightarrow N \longrightarrow 0,$$

由命题 24.5.2, 我们有以下短正合列

$$0 \longrightarrow F \otimes_R K \xrightarrow{1_F \otimes \varphi} F \otimes_R M \xrightarrow{1_F \otimes \psi} F \otimes_R N \longrightarrow 0.$$

由证明开始的讨论, 我们进而有短正合列

$$0 \longrightarrow P \otimes_R K \xrightarrow{1_P \otimes \varphi} P \otimes_R M \xrightarrow{1_P \otimes \psi} P \otimes_R N \longrightarrow 0.$$

□

我们考虑具有类似相知的模, 其为平坦模.

定义 24.5.4

我们称一个右 R -模 F 为**平坦模**, 若对任意左 R -模短正合列

$$0 \longrightarrow K \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0,$$

我们都有以下正合列

$$0 \longrightarrow F \otimes_R K \xrightarrow{\varphi'} F \otimes_R M \xrightarrow{\psi'} F \otimes_R N \longrightarrow 0,$$

其中 $\varphi' = \text{id}_F \otimes \varphi$, $\psi' = \text{id}_F \otimes \psi$.

如果对一般的右模, 我们考虑类似的问题, 则会发现类似于对 $\text{Hom}(P, \cdot)$ 和 $\text{Hom}(\cdot, Q)$ 的讨论, 以上正合列的右半部分对任意模都成立.

命题 24.5.5

任取右 R -模 X , 任给短正合列

$$0 \longrightarrow K \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0,$$

任取 $n \in \mathbb{N}^*$, 我们有以下正合列

$$X \otimes_R K \xrightarrow{1_X \otimes \varphi} X \otimes_R M \xrightarrow{1_X \otimes \psi} X \otimes_R N \longrightarrow 0.$$

证明. 考虑短正合列

$$0 \longrightarrow K \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0.$$

由于简单张量生成张量积, 由于 ψ 为满同态, 因此

$$1_X \otimes \varphi : X \otimes_R M \rightarrow X \otimes_R N,$$

也是满同态.

注意到任取 $x \in X$, 都有 $x \otimes_R 0_N \in X \otimes_R N$ 为零张量, 因此任取 $x \in X$ 以及 $w \in K$, 我们有

$$((1_X \otimes \psi) \circ (1_X \otimes \varphi))(x \otimes_R w) = (1_X \otimes (\psi \circ \varphi))(x \otimes_R w) = x \otimes_R 0_N.$$

由此可得

$$\text{Im}(1_X \otimes \varphi) \subset \ker(1_X \otimes \psi).$$

下边考虑证明另一个方向的包含. 由群同态基本定理, 我们有以下群的满同态:

$$\overline{1_X \otimes \psi} : X \otimes_R M / \text{Im}(1_X \otimes \varphi) \rightarrow X \otimes_R N.$$

我们尝试构造逆映射. 任取简单张量 $x \otimes_R v \in X \otimes_R N$, 我们定义

$$g(x \otimes_R v) = x \otimes_R u + \text{Im}(1_X \otimes \varphi),$$

其中 $u \in M$, 满足 $\psi(u) = v$. 下边验证对任意 $x \otimes_R v$, $g(x \otimes_R v)$ 是唯一的. 任取 $u' \in M$, 满足 $\psi(u') = v$, 我们有 $\psi(u - u') = 0_N$. 因此 $u - u' \in \ker \psi$. 由于 $\text{Im} \varphi = \ker \psi$, 我们有 $w \in K$, 满足 $\varphi(w) = u - u'$. 因此对任意 $x \in X$, 我们有

$$x \otimes_R (u - u') \in \text{Im}(1_X \otimes \varphi).$$

由此可知 g 可以扩展为一个群同态

$$g : X \otimes_R N \rightarrow X \otimes_R M / \text{Im}(1_X \otimes \varphi),$$

并且满足 $g \circ \overline{1_X \otimes \psi}$ 为恒等映射. 因此 $\overline{1_X \otimes \psi}$ 为同构, 我们有

$$\text{Im}(1_X \otimes \varphi) = \ker(1_X \otimes \psi).$$

□

注 24.5.6.

平坦模是由 Serre 在引入的. 命题 24.5.5 告诉我们在对模取张量积的时候, 短正合列的右半部分的正合性是会被保持的. 类似于对 $\text{Hom}(P, \cdot)$ 和 $\text{Hom}(\cdot, Q)$ 的讨论, $F \otimes_R \cdot$ 可以被看作是一个从 R -模范畴到交换群范畴的右正合的协变函子.

因此一个右 R -模 F 为平坦模, 当且仅当其对应的函子 $F \otimes_R \cdot$ 也是左正合的. 从映射的角度看, 任给左 R -模的单同态 $\varphi : K \rightarrow M$, 则 $1_F \otimes \varphi : F \otimes_R K \rightarrow F \otimes_R M$ 是群的单同态.

作为一个特殊情形, 我们可以考虑模与其系数环及其理想和商环的张量积. 记 I 为 R 的一个理想. 我们考虑以下短正合列

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0.$$

若右模 M 为一个平坦模, 则我们有以下短正合列

$$0 \longrightarrow M \otimes_R I \longrightarrow M \otimes_R R \longrightarrow M \otimes_R R/I \longrightarrow 0.$$

这里 $M \otimes_R R \cong M$. 因此以上短正合列的前半部分告诉我们, 同态

$$\varphi : M \otimes_R I \rightarrow M,$$

为单同态. 这里同态 φ 满足对任意 $u \in M, r \in I$, 我们有

$$\varphi(u \otimes_R r) = ur.$$

命题 24.5.7

设 M 为一个平坦模. 任给一个 R 中不是右零因子的非零元 $r \in R$, 我们有对任意 $u \in M$, 若 $ur = 0$, 则 $u = 0$.

证明. 任取 $r \in R^*$, 我们设 r 不是右零因子, 即任取 $s \in R^*$, 都有 $rs \neq 0$.

右乘元素 r 诱导处下 R 上的左模同态:

$$\begin{aligned} \sigma_r : R &\rightarrow R, \\ s &\mapsto sr. \end{aligned}$$

我们有模同态

$$1_M \otimes \sigma_r : M \otimes_R R \rightarrow M \otimes_R R.$$

我们考虑右模同构

$$\begin{aligned} \varphi : M \otimes_R R &\rightarrow M, \\ u \otimes_R 1_R &\mapsto u. \end{aligned}$$

我们考虑复合

$$\psi = \varphi \circ (1_M \otimes \sigma_r) : M \otimes_R R \rightarrow M,$$

满足对任意 $u \in M$, 将 $u \otimes_R 1_R$ 送到 ur . 注意到若 $u \neq 0$, 则有 $u \otimes_R 1_R$ 不是零张量, 由于 ψ 为单射, 我们有 $ur \neq 0$. $\square$

注 24.5.8.

对于一般的环 R , 平坦模一定是无扭模, 但是无扭模不一定是平坦模. 我们这里将不对一般的结论做进一步的讨论, 感兴趣的同学可以参考

这里需要注意的是我们使用的无扭模的定义是关于无零因子环的. 如果直接使用这个定义, 则任给一个有零因子的环 R 上的非零模 M , 其中都是有扭元的. 任取 $a \in R^*$ 为一个右零因子, 则存在 $b \in R^*$, 满足 $ba = 0$. 现在任取 $u \in M^*$, 我们都有 $au = 0$ 或者 $b(au) = 0$. 因此无论如何都有扭元存在. 因此在讨论有零因子的环的时候, 我们通常会使用如下无扭模的定义: 任取左 R -模 M , 我们称 M 为一个无扭模, 若任取一个非右零因子元素 $a \in R^*$, 任取 $u \in M^*$, 都有 $au \neq 0$.

我们最后把之前讨论中提到的各种模的性质之间的关系总结一下, 对于任意环上的任意模, 我们都有

$$\text{自由模} \implies \text{投射模} \implies \text{平坦模} \implies \text{无扭模}.$$

第二十五章 模的子模链

类似于之前对群的结构的研究, 本章我们将通过对子模链的讨论来研究一个模的结构.

25.1 子模链

我们仍以左模为例进行讨论. 记 R 为一个幺环, M 为一个 R -模. 一个 M 的子模链就是 M 的一个子模序列构成关于包含关系的全序集.

定义 25.1.1

记 $n \in \mathbb{N}$, 我们称一个 M 的一个子模序列 $(N_i)_{i=0}^n$ 为一个 M 的(有限)子模链, 若对任意 $0 \leq i \leq n$, 都有 $N_i \subset N_{i+1}$. 我们称 n 为以上子模链的长度.

注 25.1.2.

零模只有唯一的子模, 因此对零模的子模链的讨论是平凡的. 在后边的讨论中, 除了特别指出的地方以外, 我们总是假设 M 不是零模.

定义 25.1.3

任给 M 的两个子模链 $(K_i)_{i=0}^m$ 和 $(L_i)_{i=0}^n$, 若前者可以看作是后者的子列, 我们称后者是前者的加细.

任给一个 M 的子模链, 我们都可以通过在链的两个相邻的模之间插入一个子模来构造该子模链的加细. 通过不断重复, 我们可以得到越来越长的子模链. 这样我们就有一个问题: 这样的操作是可以无限做下去的么? 更一般地, 模 M 中存在任意长的子模链么?

注意到我们总是可以在某个链中的子模 N_i 前后插入 N_i 来把子模链加细, 这样的操作可以无限重复下去, 但这种加细是平凡的, 我们并不能从中得到更多 M 的信息. 因此我们将考虑每一个包含关系都是严格的子模链, 并引入如下概念.

定义 25.1.4

记 R 为一个环, M 为一个 R -模. 模 M 的长度定义为以下量

$$l(M) := \sup\{k \in \mathbb{N} \mid \exists \{0\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_k = M\}.$$

若 $l(M) \notin \mathbb{N}$, 我们约定 $l(M) = \infty$, 并称 M 的长度无限.

注 25.1.5.

我们可以将模的长度看作是线性空间维数的推广. 从零向量出发, 每次添加一个与之前所选向量都线性无关的向量, 并考虑生成的子空间, 我们就有了一个子空间列. 线性空间维数有限当且仅当其作为模的长度有限.

注 25.1.6.

我们约定零模的长度为 0. 任意非零模中都至少有一个长度为 1 的子模链

$$\{0\} \subsetneq M.$$

命题 25.1.7

任取模 M , 模 M 的长度为 1 当且仅当 M 中没有除了 $\{0\}$ 和 M 之外的子模.

证明. 若 M 只有 $\{0\}$ 和 M 两个子模, 则 M 中有唯一的子模链,

$$\{0\} \subsetneq M,$$

因此长度为 1.

另一方面, 若 M 有不同于 $\{0\}$ 和 M 的子模 N , 则我们总有子模链

$$\{0\} \subsetneq N \subsetneq M,$$

因此 M 的长度无限或者至少为 2. □

从子模链的角度, 长度为 1 的模是最简单的.

定义 25.1.8

若非零模 M 只有 $\{0\}$ 和 M 两个子模, 我们称 M 为**单模**.

由于子模的交集也是子模, 以上定义给出下边的一个直接的推论.

推论 25.1.9

若模 M 中有一个子模 K 是单模, 则任取 M 的子模 L , 我们都有

$$L \cap K = \{0\} \quad \text{或者} \quad K \subset L.$$

下边考虑 M 中的一个一般的子模链

$$\{0\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_k = M.$$

若 N_1 为单模, 则我们不能在 N_0 和 N_1 之间插入新的子模来对以上子模链做加细.

下边考虑 N_1 和 N_2 之间. 我们可以通过考虑商模得到 M/N_1 的一个子模链

$$\{0\} = N_1/N_1 \subsetneq N_2/N_1 \subsetneq \cdots \subsetneq N_k/N_1 = M/N_1.$$

利用模同态基本定理, 我们知道, 存在 M 的子模 N , 满足

$$N_1 \subsetneq N \subsetneq N_2,$$

当且仅当存在 M/N_1 的子模 K , 满足

$$N_1/N_1 \subsetneq K \subsetneq N_2/N_1.$$

因此

$$N_1 \subsetneq N_2,$$

没有加细当且仅当 N_2/N_1 为单模. 重复以上讨论, 我们发现以上子模链不存在非平凡的加细当且仅当任取 $0 \leq i \leq k-1$, 都有 N_{i+1}/N_i 为单模, 这样的子模链被称为 M 的一个合成列.

定义 25.1.10

模 M 的一个子模链 $(N_i)_{i=0}^n$ ($n \in \mathbb{N}^*$) 被称为 M 的一个**合成列**, 若其满足以下条件:

- 1) $N_0 = \{0\}$;
- 2) $N_n = M$;
- 3) 任取 $0 \leq i < n$, 商模 N_{i+1}/N_i 为单模.

此时, 对任意 $0 \leq i \leq n-1$, 我们称商模 N_{i+1}/N_i 为该合成列的**因子**.

任给 M 的一个相邻子模都是真包含的子模链 $(N_i)_{i=0}^n$, 若我们不能通过将其加细得到一个合成列, 则说明 M 的长度为无穷. 反过来, 如果我们通过对其做非平凡加细, 得到一个合成列, 则此时非平凡的加细操作将不能继续进行下去, 且该合成列的子模个数给出 M 的长度的一个下界. 为了研究 M 的长度, 我们就需要更换加细的方法, 或者更换一个子模链来进行加细. 不过我们下边将进行的讨论告诉我们, 这样做是没有必要的. 当我们得到一个合成列的时候, 就已经得到了模的长度.

我们首先证明合成列的唯一性. 这里唯一性的证明和群论中合成列的唯一性的证明类似.

定理 25.1.11 (Jordan-Hölder 定理)

记 M 为一个模. 设 M 有两个合成列 $(K_i)_{i=0}^m$ 和 $(L_i)_{i=0}^n$, 其中 $m, n \in \mathbb{N}^*$, 则我们有 $m = n$, 且存在一个 $\sigma \in S_m$, 满足对任意 $1 \leq i \leq m$, 我们有

$$K_i/K_{i-1} \cong L_{\sigma(i)}/L_{\sigma(i)-1}.$$

证明. 任取 $0 < i \leq m$, 考虑

$$N_j := K_i \cap L_j,$$

可得一个 K_i 的一个子模列

$$\{0\} = N_0 \subset N_1 \subset \cdots \subset N_n = K_i.$$

考虑以上子模与 K_{i-1} 的和, 我们有

$$K_{i-1} = N_0 + K_{i-1} \subset N_1 + K_{i-1} \subset \cdots \subset N_n + K_{i-1} = K_i.$$

由于 K_i/K_{i-1} 为单模, 因此, 存在 $0 < j \leq n$, 满足

$$K_{i-1} = N_0 + K_{i-1} = \cdots = N_{j-1} + K_{i-1} \subsetneq N_j + K_{i-1} = \cdots = N_n + K_{i-1} = K_i.$$

因此, 我们有

$$\begin{aligned}
 & K_i/K_{i-1} \\
 &= (N_j + K_{i-1})/(N_{j-1} + K_{i-1}) \\
 &= (K_i \cap L_j + K_{i-1})/(K_i \cap L_{j-1} + K_{i-1}) \\
 &\cong K_i \cap L_j / (K_i \cap L_{j-1} + K_{i-1}) \cap K_{i-1} \\
 &= (K_i \cap L_j) / (L_{j-1} + K_{i-1}).
 \end{aligned}$$

由此我们可以得到一个从 $\{1, \dots, m\}$ 到 $\{1, \dots, n\}$ 的映射 φ .

我们对 L_j 重复以上操作可以, 则存在 $0 < k \leq m$, 满足

$$L_{j-1} = K_0 \cap L_j + L_{j-1} = \dots = K_{k-1} \cap L_j + L_{j-1} \subsetneq K_k \cap L_j + L_{j-1} = \dots = K_m \cap L_j + L_{j-1} = L_j.$$

由之前的讨论知, 当 $k = i$ 时, 商群

$$(K_k \cap L_j + L_{j-1}) / (K_{k-1} \cap L_j + L_{j-1}),$$

非平凡, 且同构于 L_j/L_{j-1} . 因此我们有

$$L_j/L_{j-1} \cong (K_i \cap L_j) / (L_{j-1} + K_{i-1}) \cong K_i/K_{i-1}.$$

由此我们可以得到一个从 $\{1, \dots, n\}$ 到 $\{1, \dots, m\}$ 的映射 ψ , 并且满足 $\psi \circ \varphi$ 为 $\{1, \dots, m\}$ 上恒等映射.

类似地, 从 L_j 出发从头重复以上讨论可以得到 $\varphi \circ \psi$ 为 $\{1, \dots, n\}$ 上的恒等映射. 因此 ψ 和 φ 都是双射, 我们有 $m = n$, 并且存在一个 $\sigma \in S_m$, 满足对任意 $1 \leq i \leq m$, 有

$$K_i/K_{i-1} \cong L_{\sigma(i)}/L_{\sigma(i)-1}.$$

□

我们将定理 25.1.11 中两个合成列满足的性质推广到对一般的子模链的讨论中.

定义 25.1.12

设 $(K_i)_{i=0}^m$ 和 $(L_i)_{i=0}^n$ 其中 $m, n \in \mathbb{N}^*$ 为模 M 中的两个子模链. 我们称二者等价若 $m = n$, 且存在 $\sigma \in S_m$, 满足对任意 $1 \leq i \leq m$, 我们有

$$K_i/K_{i-1} \cong L_{\sigma(i)}/L_{\sigma(i)-1}.$$

注 25.1.13.

在子模链等价的定义中, 我们并不要求一个子模链中相邻的子模的包含的是严格的.

注 25.1.14.

定理 25.1.11 给出了合成列在等价意义下的唯一性.

下边我们将说明合成列可以给出模的长度. 为此我们将证明以下定理.

定理 25.1.15 (Schreier 加细定理)

任意 M 的两个子模链都可以通过分别加细成为两个等价的子模链.

证明. 我们在证明定理 25.1.11 的时候所做的加细的操作就是 Schreier 加细定理的证明中将要做的.

任取 M 的两个子模链分别记作 $(K_i)_{i=0}^m$ 和 $(L_j)_{j=0}^n$, 其中 $m, n \in \mathbb{N}^*$. 不妨设我们有 $K_0 = L_0 = \{0\}$ 和 $K_m = L_n = M$.

我们首先描述对 $(K_i)_{i=0}^m$ 的加细操作. 任取 $1 \leq i \leq m$, 我们将 $K_i \subset K_{i+1}$ 加细为

$$K_{i-1} = K_{i-1,0} \subset \cdots \subset K_{i-1,n} \subset K_i.$$

其中对任意 $0 \leq j \leq n$, 我们定义

$$K_{i-1,j} := K_i \cap L_j + K_{i-1}.$$

直接计算得加细后的子模链共有 $mn + 1$ 个子模.

我们用相似的方法对任意 $1 \leq j \leq n$ 和 $0 \leq i \leq m$ 定义

$$L_{j-1,i} := L_j \cap K_i + L_{j-1},$$

并用这些子模来对另一个子模链 $(L_j)_{j=0}^n$ 做加细. 所得新的子模链也有 $mn + 1$ 个子模.

类似于我们在定理 25.1.11 的证明中所作的讨论, 对任意 $1 \leq i \leq m$ 和 $1 \leq j \leq n$, 我们有

$$\begin{aligned} & K_i \cap L_j + K_{i-1} / K_i \cap L_{j-1} + K_{i-1} \\ & \cong K_i \cap L_j / (K_i \cap L_{j-1} + K_{i-1}) \cap K_{i-1} \\ & = K_i \cap L_j / (L_{j-1} + K_{i-1}) \\ & \quad L_j \cap K_i / (L_j \cap K_{i-1} + L_{j-1}) L_{j-1} \\ & \cong L_j \cap K_i + L_{j-1} / L_j \cap K_{i-1} + L_{j-1}. \end{aligned}$$

因此我们有模同构

$$K_{i,j} / K_{i,j-1} \cong L_{j,i} / L_{j,i-1}.$$

由此可得所得的两个子模链的加细等价. □

由此可得以下推论.

推论 25.1.16

若模 M 中存在合成列, 则任意满足相邻子模之间为真包含的 M 的子模链都可以加细为一个合成列.

证明. 记 $(K_i)_{i=0}^m$ 为 M 的一个合成列, 其中 $m \in \mathbb{N}^*$. 任取 $n \in \mathbb{N}^*$ 以及 M 的子模链 $(L_j)_{j=0}^n$, 满足任意相邻的两个子模之间为真包含.

由 Schreier 加细定理 25.1.15 我们可以将两个子模链分别进行加细, 从而得到等价的子模链. 合成列 $(K_i)_{i=0}^m$ 的加细中相邻子模之间的商模或者为零模或者为单模, 因此 $(L_j)_{j=0}^n$ 的加细中相邻子模之间的商模或者为零模或者为单模, 因此包含一个合成列作为子列. 由于 $(L_j)_{j=0}^n$ 相邻子模之间为真包含, 该合成列包含整个 $(L_j)_{j=0}^n$ 作为子列. □

综合之前的讨论, 我们得到以下结论.

推论 25.1.17

模 M 中存在合成列, 当且仅当 M 的长度有限. 若 M 长度有限, 则其长度与其合成列的长度相等.

证明. 设 M 有合成列. Jordan-Hölder 定理 25.1.11 告诉我们 M 中所有合成列长度相等. Schrier 加细定理 25.1.15 及其推论告诉我们, 任取 M 中一个相邻子模严格包含的子模链, 其长度都小于等于 M 的合成列的长度. 因此 M 长度有限.

反过来, 设 M 长度有限, 任给 M 的一个相邻子模严格包含的子模列 $(N_i)_{i=0}^n$ 其中 $n \in \mathbb{N}^*$, 我们对其做非平凡的加细. 如果不存在合成列, 则在任意 $(N_i)_{i=0}^n$ 的非平凡加细中都存在一个位置相邻的两个模的商模不是单模, 利用模同态基本定理, 我们可以构造出 $(N_i)_{i=0}^n$ 的一个非平凡加细. 因此 M 的长度大于任意自然数, 与 M 长度有限矛盾. $\square$

有限长度模

我们下边讨论以下有限长度模的性质. 我们首先考虑一个模的子模和商模.

命题 25.1.18

设 M 为一个模. 记 N 为 M 的一个子模, 则模 M 长度有限当且仅当 N 和 M/N 的长度有限.

若 M 的长度有限, 则我们进一步有

$$l(M) = l(N) + l(M/N).$$

证明. 若 N 为 $\{0\}$ 或者 M , 则结论自然成立. 下设 N 为非平凡子模.

设 M 长度有限. 由于子模具有传递性, 任意 N 的子模链都是 M 的子模链. 因此 N 长度有限, 且有

$$l(N) + 1 \leq l(M).$$

记 M 到 M/N 的自然同态为 π . 任取 M/N 的一个相邻子模严格包含的子模链 $(L_i)_{i=0}^n$ 其中 $n \in \mathbb{N}$, 我们有 M 的子模链

$$(\pi^{-1}(L_i))_{i=0}^n,$$

并且该子模链也满足相邻子模的包含是严格的. 因此我们有

$$l(M/N) + 1 \leq l(M).$$

反过来, 设 N 和 M/N 的长度有限. 记 $(K_i)_{i=0}^m$ 和 $(L_j)_{j=0}^n$ 分别为 N 和 M/N 中的一个合成列. 则由模同态基本定理, 子模列

$$\{0\} = K_0 \subset K_1 \subset \cdots \subset K_m = N = \pi^{-1}(L_0) \subset \pi^{-1}(L_1) \subset \cdots \subset \pi^{-1}(L_n) = M$$

为 M 的合成列. 因此 M 长度有限, 且满足

$$l(M) = l(N) + l(M/N).$$

$\square$

推论 25.1.19

记 M 为一个长度有限的模, N 为模 M 的一个子模, 则 $N = M$ 当且仅当 $l(M) = l(N)$.

注 25.1.20.

在高等代数的学习中, 我们知道任给一个有限维的实数域上线性空间 V , 则 V 的一个子空间 W 等于 V 当且仅当 $\dim W = \dim V$.

推论 25.1.21

记 $\varphi: M \rightarrow N$ 为一个模同态. 若模 M 长度有限, 则 $\ker \varphi$ 和 $\operatorname{Im} \varphi$ 长度有限, 且满足

$$l(\ker \varphi) + l(\operatorname{Im} \varphi) = l(M).$$

注 25.1.22.

记 V 和 W 为两个有限维实线性空间. 任取线性映射 $L: V \rightarrow W$, 我们都有

$$\dim \ker L + \dim \operatorname{Im} L = \dim V.$$

考虑一般的模扩张, 我们有以下结论.

推论 25.1.23

考虑模的短正合列

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0,$$

则 M_2 长度有限当且仅当 M_1 和 M_3 长度有限. 若 M_2 长度有限, 我们进一步有

$$l(M_2) = l(M_1) + l(M_3).$$

作为特例, 平凡的模扩张给出的是模的直和. 使用归纳法, 我们有以下结论.

推论 25.1.24

记 $k \in \mathbb{N} \setminus \{0, 1\}$. 任意 k 个模 $M_1, \dots, M_k$ 的直和

$$M := \bigoplus_{i=1}^k M_i,$$

长度有限当且仅当对任意 $1 \leq i \leq k$ 都有模 M_i 长度有限.

若 M 长度有限, 我们进一步有

$$l(M) = \sum_{i=1}^k l(M_i).$$

反过来, 我们也可以考虑对一个模进行直和分解. 注意到长度有限的模的长度取值是在 $\mathbb{N}$ 中, 因此如果一个模 M 长度有限, 当我们将其写为子模的直和的时候, 是不能无限的分解下去的. 为了更详细的说明, 我们引入下边的定义.

定义 25.1.25

如果模 M 不能写成两个非零子模的直和, 我们就称模 M 为一个**不可分解模**.

推论 25.1.26

所有的单模都是不可分解模.

借助这个定义, 我们有以下关于长度有限模的结论.

定理 25.1.27 (Krull-Schmidt 定理)

若 M 为一个长度有限的模, 则 M 可以分解为有限多个不可分解模的直和, 并且这种直和分解在同构意义下是唯一的.

证明. 之前的讨论给出了存在性. 由于每个长度有限的非零模的长都至少为 1, 当我们将 M 写为非零子模的直和的时候, 最多只有 $l(M)$ 个分支. 如果达到 $l(M)$ 个分支, 则每个分支都是长度为 1 的子模, 因此为单模, 所以都是不可分解的.

要证明这种分解在同构意义下的唯一性, 我们介绍以下一些引理.

引理 25.1.28 (Fitting 引理)

如果 N 为一个长度有限模, 则任取 N 的模自同态 φ , 存在 $n \in \mathbb{N}^*$, 记 φ^n 为 φ 的 n 次迭代, 满足

$$N = \ker \varphi^n \oplus \operatorname{Im} \varphi^n.$$

证明. 我们考虑以下两个由 φ 诱导出的 N 的子模序列

$$\begin{aligned} \ker \varphi &\subset \ker \varphi^2 \subset \cdots, \\ \operatorname{Im} \varphi &\supset \operatorname{Im} \varphi^2 \supset \cdots. \end{aligned}$$

由于 N 的长度有限, 因此存在 $n \in \mathbb{N}^*$, 满足

$$\begin{aligned} \ker \varphi^n &= \cdots \ker \varphi^{n+1} = \cdots, \\ \operatorname{Im} \varphi^n &= \operatorname{Im} \varphi^{n+1} = \cdots. \end{aligned}$$

任取 $u \in N$, 由于 $\operatorname{Im} \varphi^{2n} = \operatorname{Im} \varphi^n$, 存在 $v \in N$, 满足

$$\varphi^n(u) = \varphi^{2n}(v).$$

由此可得

$$u = (u - \varphi^n(v)) + \varphi^n(v) \in \ker \varphi^n + \operatorname{Im} \varphi^n.$$

因此我们有

$$N = \ker \varphi^n + \operatorname{Im} \varphi^n.$$

任取 $u \in \ker \varphi^n \cap \operatorname{Im} \varphi^n$, 我们有 $v \in N$, 满足

$$u = \varphi^n(v).$$

由于 $\varphi^n(u) = 0$, 我们有 $\varphi^{2n}(v) = 0$, 即 $v \in \ker \varphi^{2n}$. 由于 $\ker \varphi^n = \ker \varphi^{2n}$, 我们有 $\varphi^n(v) = 0$, 即 $u = 0$.

综上所述我们有

$$N = \ker \varphi^n \oplus \operatorname{Im} \varphi^n.$$

□

将该引理用在 N 为不可分解模的情形, 我们有以下推论.

推论 25.1.29

若 N 为一个长度有限的不可分解模, 则任意 N 的自同态 φ 或者为幂零的或者为同构.

注 25.1.30.

这里我们称一个自同态为幂零的. 若其复合有限多次之后得到零同态.

证明. 由 Fitting 引理 25.1.28 可知, 存在 $n \in \mathbb{N}^*$, 满足

$$N = \ker \varphi^n \oplus \operatorname{Im} \varphi^n.$$

由于 N 不可分解, 我们有 $\ker \varphi^n = \{0\}$, $\operatorname{Im} \varphi^n = N$ 或者 $\ker \varphi^n = N$, $\operatorname{Im} \varphi^n = \{0\}$. 前者推出 φ 为同构, 后者推出 φ 为幂零的. $\square$

推论 25.1.31

若 N 为一个长度有限的不可分解模, 任意两个幂零的 N 的自同态的和仍是幂零的.

证明. 记 f 和 g 为两个 N 的幂零的同态. 设 $f + g$ 为可逆的. 我们不妨设 $f + g = \operatorname{id}_N$, 则有

$$g = \operatorname{id}_N - f.$$

注意到 $\operatorname{id}_N - f$ 有逆元

$$\operatorname{id}_N + f + f^2 + \cdots + f^k,$$

这里 $k \in \mathbb{N}^*$, 满足 f^k 为零同态. 因此 $\operatorname{id}_N - f$ 可逆, 但是 g 为幂零的, 因此不可逆, 矛盾. $\square$

我们下边回到定理的证明.

若 M 具有两个不可分解模的直和分解

$$M = K_1 \oplus \cdots \oplus K_m = L_1 \oplus \cdots \oplus L_n,$$

我们对 $m + n$ 进行归纳. 注意到 $m \geq 1$, $n \geq 1$ 且 $m + n \geq 2$. 当 $m + n = 2$ 时, 我们有 $m = n = 1$, 结论自然成立.

下设 $m + n = k > 2$, 且结论对 $2 \leq m + n < k$ 都成立. 任取下标 $1 \leq i \leq m$ 和 $1 \leq j \leq n$, 我们有投影同态和嵌入同态

$$\begin{aligned} \pi_i &: K_1 \oplus \cdots \oplus K_m \rightarrow K_i, \\ \iota_i &: K_i \rightarrow K_1 \oplus \cdots \oplus K_m, \\ \operatorname{pr}_j &: L_1 \oplus \cdots \oplus L_n \rightarrow L_j, \\ \operatorname{inj}_j &: L_j \rightarrow L_1 \oplus \cdots \oplus L_n. \end{aligned}$$

我们可以构造同态

$$\begin{aligned} \varphi_{ij} &= \operatorname{pr}_j \circ \iota_i : K_i \rightarrow L_j, \\ \psi_{ji} &= \pi_i \circ \operatorname{inj}_j : L_j \rightarrow K_i. \end{aligned}$$

我们考虑 $\eta_{ij} = \psi_{ji} \circ \varphi_{ij}$ 为一个 K_i 的自同态. 由之前的结论, 我们知道 η_{ij} 为幂零的或者是一个同构.

我们不妨设 $i = 1$. 注意到

$$\text{id}_1 = \sum_{j=1}^n \eta_{1j},$$

这里 id_1 为 K_1 上的恒等同态.

由于 id_1 可逆, 因此存在 η_{1j} 为同构. 不妨设 η_{11} 为同构. 因此 φ_{11} 为单射, ψ_{11} 为满射. 下证 φ_{11} 和 ψ_{11} 都是同构.

这两个同态给出了两个短正合列

$$0 \longrightarrow K_1 \xrightarrow{\varphi_{11}} L_1 \xrightarrow{\pi} L_1/\text{Im } \varphi_{11} \longrightarrow 0,$$

$$0 \longrightarrow \ker \varphi_{11} \xrightarrow{\iota} L_1 \xrightarrow{\psi_{11}} K_1 \longrightarrow 0,$$

其中 π 为自然同态, ι 为嵌入同态. 由于 η_{11} 为同构, 我们有

$$\begin{aligned} \psi_{11} \circ (\varphi_{11} \circ \eta_{11}^{-1}) &= \text{id}_1, \\ (\eta_{11}^{-1} \circ \psi_{11}) \circ \varphi_{11} &= \text{id}_1. \end{aligned}$$

由之前关于短正合列分裂的判据 (命题 24.2.11 和命题 24.2.13), 以上两个短正合列分裂, 由于 L_1 不可分解, 因此我们有 φ_{11} 也是满同态, ψ_{11} 也是单同态, 因此二者均为同构. 因此通过 φ_{11} 我们有 $K_1 \cong L_1$.

考虑模同态的直和的复合

$$\varphi = \left(\bigoplus_{j=2}^n \text{pr}_j \right) \circ \left(\bigoplus_{i=2}^m \iota_i \right) : K_2 \oplus \cdots \oplus K_m \rightarrow L_2 \oplus \cdots \oplus L_n.$$

下证 φ 为一个同构. 首先证明 φ 为一个单同态. 我们考虑

$$u \in K_2 \oplus \cdots \oplus K_m,$$

则有

$$\varphi(u) = \left(\bigoplus_{j=2}^n \text{pr}_j \right) (u).$$

若 $u \in \ker \varphi$, 则 $u \in L_1$. 所以我们有

$$\psi_{11}(u) = \pi_1(u) \in K_1.$$

由于

$$K_1 \cap (K_2 \oplus \cdots \oplus K_m) = \{0\},$$

因此 $\pi_1(u) = 0$. 由于 ψ_{11} 为模同构, 因此 $u = 0$. 由此可得 $\ker \varphi = \{0\}$, 同态 φ 为单射.

要证 φ , 我们考虑 $\text{Im } \varphi$ 的长度. 注意到 φ 为单射, 因此

$$l(\text{Im } \varphi) = l(K_2 \oplus \cdots \oplus K_m) = l(M) - l(K_1) = l(M) - l(L_1) = l(L_2 \oplus \cdots \oplus L_n).$$

所以我们有

$$\text{Im } \varphi = L_2 \oplus \cdots \oplus L_n,$$

即 φ 为满射. 由此可得 φ 为同构. 在相差一个同构的前提下, 我们不妨设

$$K_2 \oplus \cdots \oplus K_m = L_2 \oplus \cdots \oplus L_n.$$

利用归纳法结论得证. □

25.2 Artin 模和 Noether 模

本节我们将介绍 Artin 模和 Noether 模两个概念. 我们之前介绍过有限生成模的概念. 某种意义上, 这两个概念都是对有限生成的推广.

我们知道当系数环为 PID 的时候, 有限生成是一个被子模保持的很好的性质. 在之前的章节中, 我们证明了 PID 上的有限生成自由模的子模仍是有限生成的. 利用模同态基本定理, 我们知道这个结论对一般的 PID 上有限生成模也成立. 然而当我们考虑一般的幺环的时候, 就会有不一样的情况发生. 例如, 考虑幺环 R 为整数环 $\mathbb{Z}$ 上的无穷元多项式环 $\mathbb{Z}[x_1, x_2, \dots]$, 则 R 为由幺元 1 生成的 R -模. 此外, 任意 $I \subset R$ 为一个子模当且仅当 I 为 R 的理想. 我们考虑 R 中由 $\{x_1, x_2, \dots\}$ 生成的理想, 则该理想作为一个 R -模不是有限生成的.

下边我们换一种思路用子模链讨论模生成. 记 R 为一个幺环. 记 M 为一个 R -模. 为方便之后的讨论, 我们对之前子模链的概念做一定的扩展.

定义 25.2.1

记 $(N_k \mid k \in \mathbb{N})$ 为一个 M 的子模序列. 若有

$$N_0 \subset N_1 \subset N_2 \subset \cdots,$$

我们称该序列为一个 M 的**子模升链**. 类似地, 若有

$$N_0 \supset N_1 \supset N_2 \supset \cdots,$$

我们称该序列为一个 M 的**子模降链**.

任取模 M 的一组生成元 S , 任取 S 的一个元素, 从其生成的 M 的子模出发, 通过不断向其中添加 S 中的生成元来生成 M 的子模, 我们就得到了一个子模升链. 另一方面, 我们也可以从 M 出发, 通过不断去除 S 中的元素, 然后考虑剩下的元素生成的 M -子模, 我们就得到了一个 M 的子模降链. 特别地, 如果 S 有限, 则这样得到的子模升链或者降链从某一个时刻, 所构造出的子模就不再变化了.

定义 25.2.2

任取 M 的子模序列 $(N_k \mid k \in \mathbb{N})$, 若存在 $k_0 \in \mathbb{N}$, 满足对任意 $k > k_0$, 都有 $N_k = N_{k+1}$, 我们称该子模序列**最终稳定**.

由此我们定义模的升链条件和降链条件, 并进一步给出 Artin 模和 Noether 模的定义.

定义 25.2.3

若模 M 的任意的子模升链都是最终稳定的, 我们称模 M 满足**升链条件** (ACC), 并称 M 为一个 **Noether 模**.

若模 M 的任意的子模降链都是最终稳定的, 我们称模 M 满足**降链条件** (DCC), 并称 M 为一个 **Artin 模**.

注 25.2.4.

由定义以及模同态基本定理可知, 满足升(降)链条件被模同构保持.

记 M 为一个 R -模. 任意一族 M 的子模的和以及交仍是子模. 注意到任取 M 的一族子模 $(N_k \mid k \in \mathbb{N})$, 我们有

$$N_0 \subset N_0 + N_1 \subset \cdots,$$

以及

$$N_0 \supset N_0 \cap N_1 \supset \cdots.$$

因此由定义, 若 M 为一个 Noether 模, 则存在 $\mathbb{N}$ 的一个非空有限子集 J , 满足

$$\sum_{j \in J} N_j = \sum_{j \in \mathbb{N}} N_j.$$

类似地, 若 M 为一个 Artin 模, 则存在 $\mathbb{N}$ 的一个非空有限子集 J , 满足

$$\bigcap_{j \in J} N_j = \bigcap_{j \in \mathbb{N}} N_j.$$

我们首先来看一些例子.

例 25.2.5.

记 V 为一个维数为 $n \in \mathbb{N}^*$ 的实线性空间. 从模的角度这是一个 $\mathbb{R}$ -模. 模 V 的子模就是其子空间. 一个线性空间和其子空间相等当且仅当它们的维数相等. 因此 V 自然满足升链条件和降链条件, 即 V 同时是 Noether 模和 Artin 模.

例 25.2.6.

考虑整数环 $\mathbb{Z}$. 我们可以将其看作 $\mathbb{Z}$ -模. 此时, 我们知道 $\mathbb{Z}$ 的子模就是 $\mathbb{Z}$ 的理想. 由之前对 $\mathbb{Z}$ 的理想的讨论我们知道, 任取子模 $N \subset \mathbb{Z}$, 存在 $n \in \mathbb{Z}$, 满足

$$N = n\mathbb{Z}.$$

进一步地, 任取 $m, n \in \mathbb{Z}$, 我们有 $m\mathbb{Z} \subset n\mathbb{Z}$ 当且仅当 $n \mid m$. 因此任意模 $\mathbb{Z}$ 的一个子模升链都对应某个整数取因子, 然后取因子的因子, 不断重复下去. 考虑整数的唯一分解性质我们知道, 任意模 $\mathbb{Z}$ 的子模升链都是最终稳定的, 因此 $\mathbb{Z}$ 为一个 Noether 模.

另一方面, 任取素数 $p \in \mathbb{Z}$, 我们有子模降链

$$\mathbb{Z} \supsetneq p\mathbb{Z} \supsetneq p^2\mathbb{Z} \supsetneq \cdots.$$

注意到该序列不是最终稳定的, 因此 $\mathbb{Z}$ 不是 Artin 模.

例 25.2.7.

我们考虑 $\mathbb{Z}$ -模 $\mathbb{Q}$. 我们将构造一个没有有限生成元组的 $\mathbb{Z}$ 上 Artin 模. 注意到 $\mathbb{Z}$ 不是 Artin 模, 我们考虑商模 $\mathbb{Q}/\mathbb{Z}$.

任取素数 p , 我们可以考虑分母为 p 的某个次方的有理数构成的 $\mathbb{Q}$ 的子集

$$\mathbb{Z} \left[\frac{1}{p} \right] := \left\{ \frac{m}{p^n} \in \mathbb{Q} \mid m, n \in \mathbb{Z} \right\}.$$

这是 $\mathbb{Q}$ 关于加法的一个子群. 我们也可以将其看作是 $\mathbb{Z}[x]$ 通过赋值 $x = 1/p$ 所得的 $\mathbb{Q}$ 的子集, 或者环 $\mathbb{Z}$ 在 $\mathbb{Q}$ 中通过添加 $1/p$ 做环扩张得到的 $\mathbb{Q}$ 的子环.

我们称其对应的商群

$$\mathbb{Z}(p^\infty) := \mathbb{Z}[1/p]/\mathbb{Z},$$

为 Prüfer p -群. 任取其子模 N , 对任意 $u \in N$, 记 $k(u) \in \mathbb{N}$, 以及与 p 互素的整数 l , 满足

$$u = \frac{l}{p^{k(u)}} + \mathbb{Z} \in N,$$

则有

$$M_{k(u)} := \frac{1}{p^{k(u)}} \mathbb{Z}/\mathbb{Z} \subset N.$$

另一方面, 任取 $u, v \in N$, 我们考虑其对应的 $k(u), k(v) \in \mathbb{N}$. 若 $k(u) \leq k(v)$, 则有

$$M_{k(u)} \subset M_{k(v)}.$$

因此我们考虑

$$k := \max\{k(u) \in \mathbb{N} \mid u \in N\} \in \mathbb{N} \cup \{\infty\}.$$

若 $k = \infty$, 则有 $N = \mathbb{Z}(p^\infty)$; 否则, 则有 $N = M_k$. 由于 M_0 为零模, 因此 $\mathbb{Z}(p^\infty)$ 满足降链条件, 为一个 Artin 模.

另一方面, 我们有如下子模升链

$$M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots,$$

不是最终稳定的, 因此 $\mathbb{Z}(p^\infty)$ 不是 Noether 模.

以上两个例子说明 Noether 模和 Artin 模的概念是不同的. 最后我们给一个简单的但是抽象的既不是 Noether 模又不是 Artin 模的例子.

例 25.2.8.

我们记 $(N_k \mid k \in \mathbb{N})$ 为 M 的一族非零子模, 并满足

$$M = \bigoplus_{k \in \mathbb{N}} N_k.$$

我们可以构造升链

$$N_0 \subsetneq N_0 \oplus N_1 \subsetneq \cdots,$$

和降链

$$\bigoplus_{k \geq 0} N_k \supsetneq \bigoplus_{k \geq 1} N_k \supsetneq \cdots.$$

注意到这两个子模链都不是最终稳定的, 因此 M 既不是 Noether 模也不是 Artin 模.

我们下边将对这两类模的性质进行进一步的讨论.

Noether 模的性质

我们首先对有限生成与升链条件进行一个比较.

命题 25.2.9

记 M 为一个 R -模. 以下三个叙述等价:

- 1) 模 M 满足升链条件;
- 2) 模 M 的任意一族子模都有一个关于由包含给出的偏序关系的极大元;
- 3) 模 M 所有的子模都是有限生成的.

证明. 我们首先证明 1) 推出 2).

设模 M 满足升链条件. 记 Ω 为 M 的一族子模. 设 Ω 中不包含极大元, 即任取子模 $N \in \Omega$, 都存在一个子模 $N' \in \Omega$, 满足 $N \subsetneq N'$. 任取 $N \in \Omega$ 记作 N_0 . 由假设知存在 $N_1 \in \Omega$, 满足 $N_0 \subsetneq N_1$. 下设对 $k \in \mathbb{N}$, 已经构造了 N_k , 由假设知存在 $N_{k+1} \in \Omega$, 满足 $N_k \subsetneq N_{k+1}$. 由此我们构造了一个 M 的子模升链

$$(N_k \mid k \in \mathbb{N}),$$

满足任取 $k \in \mathbb{N}$, 都有 $N_k \subsetneq N_{k+1}$. 因此该子模链不是最终稳定的, 这与 M 满足升链条件矛盾. 因此我们有 2) 成立.

下边证明 2) 推出 3).

设 M 的任意一族子模都有一个极大元. 任取 M 的一个子模 N . 若 N 不是有限生成的, 则存在 N 的一个生成元组 S 包含无限多个元素. 任取 S 中的元素 u_0 , 考虑 u_0 生成的 M 的子模, 记为 N_0 . 由于 N 不是有限生成的, 存在 $u_1 \in S \setminus \{u_0\}$, 满足 $u_1 \notin N_0$. 我们记 $\{u_0, u_1\}$ 生成的子模为 N_1 .

若对 $k \in \mathbb{N}$, 我们已经找到元素 $u_0, \dots, u_k \in S$, 及其生成的子模 N_k . 由于 N 不是有限生成的, 存在

$$u_{k+1} \in S \setminus \{u_0, \dots, u_k\},$$

满足 $u_{k+1} \notin N_k$. 我们记 N_{k+1} 为

$$\{u_0, \dots, u_{k+1}\}.$$

生成的子模. 我们由此构造了一个 M 的子模升链

$$(N_k \mid k \in \mathbb{N}),$$

满足任取 $k \in \mathbb{N}$, 都有 $N_k \subsetneq N_{k+1}$. 因此这族子模 $\{N_k \mid k \in \mathbb{N}\}$ 没有极大元, 这与 2) 矛盾. 因此我们有 3) 成立.

最后我们证明 3) 推出 1).

设 M 所有的子模都是有限生成的. 任取 M 的一个子模升链

$$(N_k \mid k \in \mathbb{N}),$$

我们记

$$N = \bigcup_{k \in \mathbb{N}} N_k.$$

注意到 N 仍是子模. 由假设知, 子模 N 有限生成, 因此存在一个有限的生成元组记作 S . 我们记 S 中的元素为

$$u_0, \dots, u_n.$$

由于

$$S \subset N = \bigcup_{k \in \mathbb{N}} N_k.$$

因此任取 $0 \leq i \leq n$, 存在一个 $k_i \in \mathbb{N}$, 满足

$$u_i \in N_{k_i}.$$

记

$$m = \max\{k_0, \dots, k_n\},$$

则由升链的包含关系, 我们有

$$N = N_m.$$

由此可知, 任取 $k \geq m$, 我们有

$$N_{k+1} \subset N = N_m \subset N_k.$$

因此 $N_k = N_{k+1}$, 即该子模升链最终稳定. 由以上讨论知 M 满足升链条件. $\square$

注 25.2.10.

在之前对 PID 上的有限生成模的讨论中, 我们知道 PID 上有限生成模的子模都是有限生成的, 因此任意 PID 上的有限生成模都是 Noether 模. 特别地, 作为一个具体的例子, 当我们考虑线性空间的时候, 线性空间的维数就是其一组生成元的个数. 当线性空间的维数有限时, 我们知道其所有子空间的维数都是有限的. 从模的角度, 我们知道有限维线性空间所有的子空间都是有限生成的, 因此利用以上命题可知其为 Noether 模.

不同于有限生成这个性质不能被子模保持, 利用子模的传递性, 升链条件是可以被子模保持的.

命题 25.2.11

Noether 模的任意子模都是 Noether 模.

证明. 记 M 为一个 Noether 模. 由定义模 M 满足升链条件.

任取 M 的子模 N , 由于 N 的子模也是 M 的子模, 因此任意 N 的子模升链也是 M 的子模升链. 由于 M 满足升链条件, 模 N 也满足升链条件. $\square$

考虑商模, 利用模同态基本定理, 升链条件也可以被取商模保持.

命题 25.2.12

Noether 模的任意商模也是 Noether 模.

证明. 记 M 为一个 Noether 模. 任取 M 的子模 N , 考虑商模 M/N .

由模同态基本定理可知, 任取 M/N 的一个子模 K , 都存在 M 的一个包含 N 的子模 L , 满足

$$K = L/N.$$

任取 M/N 的一个子模升链

$$K_0 \subset K_1 \subset \cdots,$$

我们有对应的一个 M 的包含 N 的子模升链

$$L_0 \subset L_1 \subset \cdots,$$

满足对任意 $k \in \mathbb{N}$, 都有 $K_k = L_k/N$. 由于 M 为 Noether 模, 由定义 M 满足升链条件. 因此存在 $k_0 \in \mathbb{N}$, 对任意 $k \geq k_0$, 我们有

$$L_k = L_{k+1},$$

由此可知对任意 $k \geq k_0$, 都有

$$K_k = K_{k+1}.$$

由以上讨论, 我们知道 M/N 也满足升链条件, 因此也是 Noether 模. $\square$

任取模 M 及其子模 N , 我们也可以反过来问若 N 和 M/N 都是 Noether 模, 那么 M 是否是 Noether 模? 答案是肯定的.

命题 25.2.13

若模 M 的子模 N 和其对应的商模 M/N 都是 Noether 模, 则模 M 也是 Noether 模.

证明. 记模 M 到其子模 N 对应的商模的自然同态为 π . 我们给出一个利用有限生成进行讨论的证明.

任取 M 的子模 L , 由模同态基本定理, 我们有

$$L' := \pi^{-1}(\pi(L)) = L + N.$$

由于 M/N 为 Noether 模, 因此由命题 25.2.9 可得 $\pi(L)$ 有限生成, 即存在非零自然数 k , 以及元素 $u_1, \dots, u_k \in L$, 满足 $\pi(L)$ 由

$$u_1 + N, \dots, u_k + N,$$

生成. 因此任取 $u \in L$, 存在 $r_1, \dots, r_k \in R$, 满足

$$u + N = \sum_{i=1}^k r_i u_i + N.$$

注意到

$$u - \sum_{i=1}^k r_i u_i \in N \cap L.$$

由于 N 为 Noether 模, 由命题 25.2.9 可得 $L \cap N$ 有限生成. 记 $L \cap N$ 的一组有限生成元为 $v_1, \dots, v_l \in L \cap N$. 因此存在元素 $s_1, \dots, s_l \in R$, 满足

$$u - \sum_{i=1}^k r_i u_i = \sum_{j=1}^l s_j v_j.$$

因此我们有

$$u = \sum_{i=1}^k r_i u_i + \sum_{j=1}^l s_j v_j.$$

注意到 L 的元素 $u_1, \dots, u_k, v_1, \dots, v_l$ 的选取不依赖于 u , 且任意 L 的元素 u 都可以表达为这组元素的 R -线性组合, 因此这组元素构成 L 的一个生成元组, 我们有 L 是有限生成的.

由以上讨论可得, M 的任意子模都是有限生成的, 因此 M 是 Noether 模. $\square$

推论 25.2.14

记 M 为一个模, K 和 L 为 M 的子模. 设 M/K 和 M/L 都为 Noether 模, 则 $M/K \cap L$ 也是 Noether 模.

证明. 考虑模同构

$$K/K \cap L \cong K + L/L \subset M/L.$$

因此 $K/K \cap L$ 为 Noether 模. 进一步考虑模同构

$$M/K \cong (M/(K \cap L))/(K/(K \cap L)).$$

由于 M/K 是 Noether 模. 因此 $M/(K \cap L)$ 是 Noether 模. $\square$

我们可以使用短正合列来给出这个结论的一个一般的叙述.

推论 25.2.15

任取一个模的短正合列

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0,$$

若 M_1 和 M_3 都是 Noether 模, 则 M_2 也是 Noether 模.

使用模扩张的语言来讲即为任意 Noether 模过 Noether 模的扩张所得也是 Noether 模. 作为模扩张的一个平凡的情形, 我们有以下结论.

推论 25.2.16

若模 M 和 N 均为 Noether 模, 则其直和 $M \oplus N$ 也是 Noether 模. 更一般地, 任意有限多个 Noether 模的直和也是 Noether 模.

注 25.2.17.

如果我们考虑命题 25.2.13 可以发现以上推论对模的有限和也是成立的. 我们以两个模的和情形为例进行讨论. 设 M 和 N 均为模 K 的子模并且都是 Noether 模, 我们考虑 M 和 $M + N/M$. 利用模同态基本定理, 我们有

$$M + N/M \cong N/M \cap N.$$

因此 M 和 $M + N/M$ 都是 Noether 模. 由此可得 $M + N$ 也是 Noether 模.

Noether 模的自同态也有一些特殊的性质.

命题 25.2.18

设 M 为 Noether 模. 任取 f 为一个 M 到自己的模同态, 存在 $n \in \mathbb{N}^*$, 满足

$$\ker f^n \cap \operatorname{Im} f^n = \{0\}.$$

证明. 任取模同态

$$f: M \rightarrow M,$$

则 f 及其叠带的核自然满足一个包含关系

$$\ker f \subset \ker f^2 \subset \ker f^3 \subset \cdots.$$

由于 M 为 Noether 模, 因此存在 $n \in \mathbb{N}^*$, 满足

$$\ker f^n = \ker f^{n+1} = \cdots.$$

任取 $v \in \operatorname{Im} f^n$, 存在 $u \in M$, 满足

$$f^n(u) = v.$$

若同时有 $v \in \ker f^n$, 则有

$$f^{2n}(u) = f^n(v) = 0.$$

因此

$$u \in \ker f^{2n} = \ker f^n.$$

由此可得 $v = f^n(u) = 0$.

□

推论 25.2.19

任意 Noether 模到自己的满同态都是同构.

证明. 记 M 为一个 Noether 模. 设 $f \in \text{End}_R M$ 为一个满同态. 因此 f 所有的迭代都是满同态.

由之前的命题知存在 $n \in \mathbb{N}^*$, 满足

$$\ker f^n \cap \text{Im } f^n = \{0\}.$$

因此我们有 $\ker f^n = \{0\}$, 等价地, 我们有 f^n 为单同态. 因此 f 为单同态, 进而可知 f 为模同构. $\square$

注 25.2.20.

考虑域上有限维线性空间到自己的线性映射. 如果为满射, 则一定为线性同构.

Artin 模的性质

类似于升链条件与子模集合关于包含给出的偏序关系的极大元的存在性之间的关系, 我们有以下降链条件的等价条件.

命题 25.2.21

记 M 为一个 R -模. 以下两个叙述等价:

- 1) 模 M 满足降链条件;
- 2) 模 M 的任意一族子模都有一个关于包含给出的偏序关系的极小元.

证明. 证明讨论与之前类似, 留作练习. $\square$

接着我们对有限生成和降链条件进行一个比较. 不同于升链条件与有限生成的关系, 降链条件和有限生成之间并没有很明确的关系. 我们利用之前的两个例子进行说明.

一方面, 在之前的对 $\mathbb{Z}$ 作为 $\mathbb{Z}$ -模的讨论中, 我们看到 $\mathbb{Z}$ 不是 Artin 模. 但是 $\mathbb{Z}$ 的所有子模都是有限生成的. 因此有限生成不能保证降链条件.

另一方面, 我们考虑 $\mathbb{Z}$ -模 $\mathbb{Z}(p^\infty)$. 利用类似于 $\mathbb{Q}$ 不是有限生成的 $\mathbb{Z}$ -模的证明, 我们可以证明 $\mathbb{Z}(p^\infty)$ 不是有限生成的. 而我们之前也验证了 $\mathbb{Z}(p^\infty)$ 是一个 Artin 模. 因此满足降链条件也不能保证有限生成.

我们下边考虑降链条件与子模和商模的联系. 类似于 Noether 模的情形, 我们也有以下相似的结论.

命题 25.2.22

Artin 模的任意子模是 Artin 模. Artin 模的任意商模是 Artin 模.

证明. 证明与 Noether 模的情形类似. 留作练习. $\square$

与 Noether 模的情形类似, 我们也有另一个方向的结论.

命题 25.2.23

若模 M 的子模 N 和其对应的商模 M/N 都是 Artin 模, 则模 M 也是 Artin 模.

证明. 设模 M 有子模 N 及其对应的商模 M/N . 记 M 到 M/N 的自然同态为 π . 我们使用子模降链来进行讨论.

任意 M 的一个下子模降链

$$(N_k \mid k \in \mathbb{N})$$

给出 M/N 的一个子模降链

$$(\pi(N_k) \mid k \in \mathbb{N}),$$

以及 N 的一个子模降链

$$(N_k \cap N \mid k \in \mathbb{N}).$$

由于 N 和 M/N 都为 Artin 模, 存在 $k_0 \in \mathbb{N}$, 对任意 $k \geq k_0$, 我们有

$$N_k \cap N = N_{k+1} \cap N \quad \text{和} \quad \pi(N_k) = \pi(N_{k+1}).$$

此时我们有以下交换图

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N_k \cap N & \xrightarrow{j} & N_k & \xrightarrow{\pi} & \pi(N_k) & \longrightarrow & 0 \\ & & \downarrow \text{id} & & \downarrow \iota & & \downarrow \text{id} & & \\ 0 & \longrightarrow & N_{k+1} \cap N & \xrightarrow{j} & N_{k+1} & \xrightarrow{\pi} & \pi(N_{k+1}) & \longrightarrow & 0. \end{array}$$

这里 j 和 ι 均为包含给出的单同态. 注意到第一行和第二行均为短正合列. 由短五引理, 我们知道 ι 为同构, 因此为恒等映射. 由此对任意 $k > k_0$, 我们有 $N_k = N_{k+1}$.

由以上讨论, 我们知道 M 满足降链条件, 因此为 Artin 模. $\square$

注 25.2.24.

由于没有类似于 Noether 模的用有限生成来描述的等价定义, 我们这里证明与之前命题 25.2.13 的证明不同.

另一方面, 利用这个证明思路对升链进行讨论可以给出命题 25.2.13 的另一个证明.

推论 25.2.25

记 M 为一个模, K 和 L 为 M 的子模. 设 M/K 和 M/L 都为 Artin 模, 则 $M/(K \cap L)$ 也是 Artin 模.

证明. 证明与 Noether 模的情形类似, 留作练习. $\square$

我们可以使用短正合列来给出之前命题中的结论的一般的叙述.

推论 25.2.26

任取一个模的短正合列

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0,$$

若 M_1 和 M_3 都是 Artin 模, 则 M_2 也是 Artin 模.

使用模扩张的语言来讲即为任意 Artin 模过 Artin 模的扩张所得也是 Artin 模. 作为模扩张的一个特例, 我们有以下结论.

推论 25.2.27

若模 M 和 N 均为 Artin 模, 则其直和 $M \oplus N$ 也是 Artin 模. 更一般地, 任意有限多个 Artin 模的直和也是 Artin 模.

注 25.2.28.

类似于对 Noether 模的情形的讨论, 如果我们考虑命题 25.2.23 可以发现以上推论对模的有限和也是成立的, 即任取模 M , 其中任意有限个 Artin 子模的和也是 Artin 模.

我们下边考虑 Artin 模的自同态.

命题 25.2.29

设 M 为 Artin 模. 任取 f 为一个 M 到自己的模同态, 存在 $n \in \mathbb{N}^*$, 对任意 $k \geq n$, 都有

$$\operatorname{Im} f^k = \operatorname{Im} f^{k+1}.$$

证明. 任取模同态

$$f: M \rightarrow M,$$

则 f 及其迭代的核自然满足一个包含关系

$$\operatorname{Im} f \supset \operatorname{Im} f^2 \supset \operatorname{Im} f^3 \supset \cdots.$$

由于 M 为 Artin 模, 因此存在 $n \in \mathbb{N}^*$, 满足

$$\operatorname{Im} f^n = \operatorname{Im} f^{n+1} = \cdots.$$

□

推论 25.2.30

任意 Artin 模到自己的单同态都是同构.

证明. 记 M 为一个 Artin 模. 设 $f \in \operatorname{End}_R M$ 为一个单同态. 因此 f 所有的迭代都是单同态.

若 f 不是满同态, 则有

$$M \supsetneq f(M).$$

由于对任意 $k \in \mathbb{N}^*$, 同态 f^k 都是单射, 我们有

$$f^k(M) \supsetneq f^{k+1}(M).$$

这与之前命题矛盾. 因此我们有 f 为满同态, 继而可得 f 为同构.

□

注 25.2.31.

考虑域上有限维线性空间到自己的线性映射. 如果为单射, 则一定为线性同构.

25.3 Artin 环和 Noether 环

任何幺环 R 都有自然的左 R -模结构和右 R -模结构.

定义 25.3.1

若环 R 作为左(右) R -模为 Artin 模, 则称 R 为一个左(右) *Artin 环*.

若环 R 作为左(右) R -模为 Noether 模, 则称 R 为一个左(右) *Noether 环*.

注 25.3.2.

以下的讨论仍将以左模为例. 当我们将 R 看作左 R -模时, 则 $N \subset R$ 为一个子模当且仅当 N 为 R 的一个左理想.

我们来给出一些简单的例子.

例 25.3.3.

任意有限幺环既是 Noether 环, 又是 Artin 环. 例如, $\mathbb{Z}_m$, 这里 $m \in \mathbb{N} \setminus \{0, 1\}$.

例 25.3.4.

任意域 F 都只有两个理想 F 和 $\{0\}$. 因此任意域既是 Noether 环, 又是 Artin 环.

例 25.3.5.

任意 PID 都是 Noether 环, 但不一定是 Artin 环 (例如 $\mathbb{Z}$).

Noether 环

Emmy Noether 在其 1921 年的文章 [23] 中证明了关于交换环, 我们有 4) 推出 2). Noether 环这个称呼是由 Chevalley [11] 与 1943 年引入的.

由之前关于 Noether 模的讨论, 我们有以下关于 Noether 环的等价叙述:

命题 25.3.6

记 R 为一个环, 以下叙述等价:

- 1) 环 R 为 Noether 环;
- 2) 环 R 中的任意左理想升链都是最终稳定的;
- 3) 环 R 的任意一族左理想都有一个包含给出的偏序关系下的极大元;
- 4) 环 R 的任意左理想都是有限生成的.

任意环 R 到自己的环同态都给出一个模同态, 因此我们也有以下关于 Noether 环的自同态的结论.

命题 25.3.7

记 R 为一个 Noether 环. 任意 R 到自己的满环同态都是环同构.

在对 Noether 环的研究中, David Hilbert 做出了重要的工作. 下边将介绍其中的一个被称为 "Hilbert 基定理" 的结论. 利用这个工作, 我们可以构造更多的 Noether 环的例子. 我们给出关于左 Noether 环的版本.

定理 25.3.8 (Hilbert 基定理)

若环 R 为一个左 Noether 环, 则 $R[x]$ 也是一个左 Noether 环.

证明. 记 I 为 $R[x]$ 的一个左理想. 若 I 为零理想, 则可由零多项式生成, 结论成立.

下设 I 不是零理想. 记 f_0 为 I 中次数最低的一个非零多项式, 并记 J_0 为 f_0 生成的左理想.

记 f_1 为 $I \setminus J_0$ 中次数最低的非零多项式, 并记 J_1 为 $\{f_0, f_1\}$ 生成的左理想.

下设对 $k \in \mathbb{N}^*$, 我们得到了多项式 $f_0, \dots, f_k$, 并记 J_k 为

$$\{f_0, \dots, f_k\},$$

生成的左理想. 我们记 f_{k+1} 为 $I \setminus J_k$ 中次数最小的非零多项式.

若以上构造在某一步无法继续进行, 即存在 $k \in \mathbb{N}^*$, 满足 $I = J_k$, 则 I 有限生成. 否则, 我们得到 I 的一个无穷序列

$$f_0, f_1, \dots, f_k, \dots$$

由构造, 我们知道以上多项式序列的次数是一个递增数列.

记个以上多项式序列对应的首项系数序列为

$$u_0, u_1, \dots, u_k, \dots$$

并对任意 $k \in \mathbb{N}$, 记 L_k 为 $\{u_0, \dots, u_k\}$ 在 R 中生成的左理想. 由此我们得到一个左理想升链

$$L_0 \subset L_1 \subset L_2 \subset \dots$$

由于 R 为左 Noether 环, 因此存在 $k_0 \in \mathbb{N}$, 对任意 $k \geq k_0$, 我们有

$$L_k = L_{k+1}.$$

考虑 u_{k_0+1} , 由以上结论, 存在 $r_0, \dots, r_{k_0} \in R$, 满足

$$u_{k_0+1} = \sum_{i=0}^{k_0} r_i u_i.$$

记

$$g = \sum_{i=0}^{k_0} r_i X^{\deg f_{k_0+1} - \deg f_i} f_i.$$

以上讨论告诉我们 g 和 f_{k_0+1} 有相同的首项. 因此

$$\deg(f_{k_0+1} - g) < \deg f_{k_0+1}.$$

另一方面, $g \in J_{k_0}$, $f_{k_0+1} \notin J_{k_0}$, 因此我们有

$$f_{k_0+1} - g \notin J_{k_0}.$$

但是这与 f_{k_0+1} 为 $I \setminus J_{k_0}$ 中次数最低的多项式矛盾. 因此以上构造多项式序列的过程必然在有限步终止. 不妨记为第 k_0 步中止, 则左理想 I 由

$$\{f_0, \dots, f_{k_0}\}.$$

生成.

由此我们证明了所有 $R[x]$ 的左理想都是有限生成的, 因此 $R[x]$ 为左 Noether 环. $\square$

利用归纳法, 我们可以得到以下推论.

推论 25.3.9

若 R 为一个左 Noether 环, 则任给 $n \in \mathbb{N}^*$, 多元多项式环 $R[x_1, \dots, x_n]$ 也是左 Noether 环.

注 25.3.10.

任取 Noether 环 R , 我们也可以证明环 R 上的形式幂级数环 $R[[x]]$ 也是 Noether 环. 不过由于 $R[[x]]$ 中元素不一定具有首项, 因此以上证明方法不再适用. 不过我们可以考虑次数最低项, 利用类似于以上证明中的讨论, 我们可以证明 $R[[x]]$ 也是 Noether 环. 使用归纳法, 类似于多项式的情形, 我们可以证明对任意 $n \in \mathbb{N}^*$, 环 $R[[x_1, \dots, x_n]]$ 也是 Noether 环.

注 25.3.11.

我们知道 Noether 环的任意商环都是 Noether 环, 因此利用 Hilbert 基定理, 我们可以考虑多项式环关于其理想的商环来从一个 Noether 环出发构造出更多的 Noether 环.

例如 Gauss 整数环 $\mathbb{Z}[i]$ 与多项式环 $\mathbb{Z}[x]$ 商去 $x^2 + 1$ 生成的理想得到的商环同构. 由于 $\mathbb{Z}$ 为 Noether 环, 因此 $\mathbb{Z}[x]$ 为 Noether 环, 进而可得 $\mathbb{Z}[x]/\langle x^2 + 1 \rangle$ 也是 Noether 环. 因此 $\mathbb{Z}[i]$ 也是 Noether 环. 作为一个应用, 我们知道 $\mathbb{Z}[i]$ 中所有理想都是有限生成的.

更一般的任取 $D \in \mathbb{Z}$, 我们都有环同构

$$\mathbb{Z}[\sqrt{D}] \cong \mathbb{Z}[x]/\langle x^2 - D \rangle.$$

因此 $\mathbb{Z}[\sqrt{D}]$ 都是 Noether 环. 我们可以进一步考虑 $\mathbb{Z}[\sqrt{D_1}, \sqrt{D_2}]$, 其中 $D_1, D_2 \in \mathbb{Z}$. 考虑环同构

$$\mathbb{Z}[\sqrt{D_1}, \sqrt{D_2}] \cong \mathbb{Z}[x_1, x_2]/\langle x_1^2 - D_1, x_2^2 - D_2 \rangle.$$

由于 $\mathbb{Z}[x_1, x_2]$ 为 Noether 环, 因此 $\mathbb{Z}[\sqrt{D_1}, \sqrt{D_2}]$ 也是 Noether 环 (例如 $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$).

注 25.3.12.

关于交换的 Noether 环的研究是交换代数中的一个重要主题. 我们将在交换环论和代数几何介绍部分对交换的 Noether 环做进一步的讨论.

我们下边考虑 Noether 环上的模. 利用之前关于 Noether 模和 Noether 环的讨论, 我们有以下结论.

命题 25.3.13

若 R 为一个 Noether 环, 则秩有限的 R 上自由模为 Noether 模.

由于任意 R 上的模都可以看作是 R 上自由模的商模, 我们进一步有以下结论.

推论 25.3.14

若 R 为一个 Noether 环, 则 R -模 M 为 Noether 模当且仅当 M 为有限生成的.

证明. 若 M 为 Noether 模, 则由命题 25.2.9 可知 M 有限生成.

反过来, 若 M 有限生成, 则存在 $n \in \mathbb{N}^*$, 使得 M 同构于 R^n 的商模. 由于 R 为 Noether 环, 因此 R^n 为 Noether 模, 由之前的讨论知其商模也是 Noether 模. 因此 M 是 Noether 模. $\square$

注 25.3.15.

在系数环 R 为 Noether 环的情形下, 这个结论一方面给了我们判断一个 R -模是否是 Noether 模的方法, 另一方面也给了我们从已有的 Noether 模出发构造新的 Noether 模的方法.

Artin 环

Emil Artin 引入了使用理想降链条件来推广有限环以及域上有限维线性空间. Artin 环是以其名字命名的.

由之前关于 Artin 模的讨论, 我们有以下关于 Artin 环的等价叙述.

命题 25.3.16

记 R 为一个环, 以下叙述等价:

- 1) 环 R 为 Artin 环;
- 2) 环 R 中的任意左理想降链都是最终稳定的;
- 3) 环 R 的任意一族左理想都有一个包含给出的偏序关系下的极小元.

任意环 R 到自己的环同态都给出一个模同态, 因此关于 Artin 环的自同态, 我们有以下结论.

命题 25.3.17

记 R 为一个 Artin 环. 任意 R 到自己的环单同态都是同构.

我们下边讨论 Artin 环和 Noether 环的关系. 我们首先考虑 Noether 模和 Artin 模的定义, 有如下结论.

命题 25.3.18

记 R 为一个环, M 为一个 R -模. 模 M 的长度有限当且仅当 M 同时是 Noether 模和 Artin 模.

证明. 若 M 不是 Noether 模, 则存在 M 的一个子模升链

$$N_0 \subsetneq N_1 \subsetneq \cdots$$

特别地, 对任意 $k \in \mathbb{N}$, 我们有 $N_k \subsetneq M$, 否则由于 M 是所有子模的集合中的最大元, 序列最终稳定. 由于 $\{0\}$ 被包含在任意子模中, 因此不妨设 $N_0 = \{0\}$ 为零模.

对任意 $k \in \mathbb{N}^*$, 我们考虑前 $k-1$ 个子模, 并构造

$$\{0\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_{k-1} \subsetneq N'_k = M.$$

因此由定义, 模 M 的长度大于等于 k . 由 k 的任意性知 M 的长度无限.

类似地, 我们可以证明, 若 M 不是 Artin 模, 则 M 的长度无限. 由此我们证明了若 M 长度有限, 则 M 是一个 Noether 模和 Artin 模.

反过来, 若 M 既是 Noether 模, 也是 Artin 模. 考虑 M 中长度有限的子模的集合

$$\Omega = \{N \in \mathcal{P}(M) \mid N \text{ 为长度有限的 } M \text{ 的子模}\}.$$

由于零模总是有限长度的, 因此该集合非空. 由于 M 是 Noether 模, 因此 Ω 包含一个极大元, 记为 N' . 若 $N' = M$, 则结论得证. 否则, 模 N' 为模 M 的一个真子模. 我们考虑

$$\Lambda = \{L \in \mathcal{P}(M) \mid L \text{ 为 } M \text{ 的子模, 且 } N' \subsetneq L\}.$$

由于 M 包含 N , 因此 Λ 非空. 由于 M 为一个 Artin 模, 因此 Λ 有一个极小元, 记为 L' . 由极小性, 我们知道 L'/N' 为单模, 长度为 1. 因此模 L' 长度有限, 且严格包含 N . 但这与 N 的极大性矛盾. $\square$

考虑 Krull-Schmidt 定理 25.1.27, 我们有以下推论.

推论 25.3.19

若模 M 同时是 Noether 环和 Artin 环, 则 M 可以分解为有限多个不可分解模的直和, 并且这种直和分解在同构意义下是唯一的.

命题 25.3.20

记 R 为一个环, M 为一个 Artin R -模. 若存在一个自然数 n , 使得 M 可以写为长度小于等于 n 的子模的和, 则 M 长度有限.

证明. 我们记

$$\Omega = \{N \in \mathcal{P}(M) \mid N \text{ 为长度小于等于 } n \text{ 的 } M \text{ 的子模}\}$$

我们对 n 使用归纳法.

若 $n = 1$, 则 M 可以写为单模的和. 由单模的性质, 模 M 为这些单模的直和. 如果有无限多个单模, 我们不妨设

$$N_0, N_1, \dots$$

为两两不同的单模, 则我们可以构造

$$M \supsetneq M \setminus N_0 \supsetneq M \setminus (N_0 \oplus N_1) \supsetneq \dots$$

由于 M 为 Artin 模, 因此存在 $k \in \mathbb{N}$, 我们有

$$M = N_0 \oplus \dots \oplus N_k.$$

因此 M 长度有限.

下设 $n \geq 2$, 结论对任意 $1 \leq k < n$ 都成立. 任意 $N \in \Omega$, 取 $K(N) \subset N$ 为一个长度为 $l(N) - 1$ 的模. 记

$$M' = \sum_{N \in \Omega} K(N),$$

并考虑 M/M' . 注意到任取 $N \in \Omega$, 我们有

$$N + M'/M' \cong N/N \cap M' \cong (N/K(N))/(N \cap M'/K(N)).$$

由于 $N/K(N)$ 的长度为 1, 因此 $N + M'/M'$ 长度至多为 1. 因此 M/M' 为一些长度至多为 1 的子模的和. 由于 M 为 Artin 模, 因此 M' 和 M/M' 都是 Artin 模.

利用 $n = 1$ 的情形, 我们有 M/M' 的长度有限. 另一方面 M' 为长度至多为 $n - 1$ 的模的和, 由归纳假设也是长度有限的模. 因此 M 的长度有限. $\square$

命题 25.3.21

若 R 为一个 Artin 环, 则作为模 R 的长度有限.

证明. 考虑 R 中所有满足对应的商模长度有限的左理想构成的集合:

$$\Omega = \{I \in \mathcal{P}(R) \mid I \text{ 为左理想, 且商模 } R/I \text{ 长度有限}\}.$$

由于 R/R 为零模, 因此 $R \in \Omega$.

任取 $I \subset \Omega$, 由于 R/I 长度有限, 因此 R/I 既是 Noether 模又是 Artin 模. 任取 $I, J \in \Omega$, 我们有 $R/I \cap J$ 既是 Noether 模, 又是 Artin 模, 因此长度有限. 由此可得 $I \cap J \in \Omega$.

由于 R 为 Artin 环, 因此 Ω 中存在极小元. 以上讨论告诉我们, 该极小元是唯一的, 为最小元, 记为 K . 我们记 $n = l(R/K)$.

任取 $u \in R$, 其左零化子 $\text{ann}(u)$ 为一个 R 的左理想并且满足模同构

$$Ru \cong R/\text{ann}(u).$$

若 $R/\text{ann}(u)$ 长度有限, 则有 $K \subset \text{ann}(u)$, 因此有模同构

$$R/\text{ann}(u) \cong (R/K)/(\text{ann}(u)/K),$$

由此可得

$$l(Ru) = l(R/\text{ann}(u)) \leq l(R/K) = n.$$

记

$$S = \{u \in R \mid Ru \text{ 长度有限}\},$$

考虑左理想

$$L = \sum_{u \in S} Ru.$$

由命题 25.3.20 可知 L 的长度有限. 任取 R 的长度有限的左理想 I , 任取 $u \in I$, 都有 Ru 长度有限, 因此 $I \subset L$, 即所有长度有限的左理想都被包含在 L 中.

下证 $L = R$. 若不成立, 以下集合

$$\Lambda = \{I \in \mathcal{P}(R) \mid I \text{ 为 } R \text{ 的左理想, 并且满足 } L \subsetneq I\},$$

包含 R , 因此非空.

由于 R 为 Artin 环, 因此 Λ 存在极小元, 记为 N . 由 N 的极小性可得 $l(N/L) = 1$. 由于 L 长度有限, 因此 N 的长度有限. 但是由之前的讨论, 左理想 L 包含所有长度有限的左理想, 因此 $N \subset L$ 矛盾. 因此 $L = R$. $\square$

由命题我们有以下推论.

推论 25.3.22

任意 Artin 环都是 Noether 环.

注 25.3.23.

由命题 25.3.18, 环 R 长度有限当且仅当 R 为 Artin 环.

我们进一步考虑 Artin 环上的模, 有如下结论.

命题 25.3.24

记 R 为一个 Artin 环. 记 M 为一个 R -模. 以下叙述等价:

- 1) M 为 Artin 模;
- 2) M 有限生成;
- 3) M 长度有限;
- 4) M 为 Noether 模.

证明. 设 M 为有限生成, 则 M 为秩有限的 R 上自由模的商模, 因此 M 为 Artin 模.

设 M 为一个 Artin 模. 模 M 可以写为其元素生成的自由模的和. 任取 $u \in M$, 我们有

$$Ru \cong R/\text{ann}(u).$$

由于 R 为一个 Artin 环, 由命题 25.3.21 知其长度有限, 记为 n . 所以 $l(Ru) \leq n$. 由命题 25.3.20, 我们知道 M 长度有限.

设 M 长度有限. 由命题 25.3.18 可得, M 同时为 Noether 模和 Artin 模.

由推论 25.3.22 知 R 也是 Noether 环, 因此若 M 为 Noether 模, 则 M 有限生成. $\square$

最后我们考虑无零因子环.

命题 25.3.25

若 Artin 环 R , 则任意不是右零因子的元素都有左逆.

证明. 任取 R 中一个不是右零因子的元素 a , 我们考虑以下左理想降链

$$R \supset Ra \supset Ra^2 \supset \cdots.$$

由于 R 为 Artin 环, 因此存在 $k \in \mathbb{N}^*$, 满足

$$Ra^k = Ra^{k+1}.$$

因此存在 $s \in R$, 满足 $a^k = sa^{k+1}$. 考虑

$$(1 - sa)a^k = 0,$$

由于 a 不是右零因子, 我们有 $1 - sa$. 因此 a 有左逆. $\square$

推论 25.3.26

若 R 为一个 Artin 整环, 则 R 为域.

推论 25.3.27

若 R 为一个交换 Artin 环, 则 R 中所有素理想都是极大理想.

证明. 任取 R 的素理想 P , 我们有 R/P 为 Artin 整环. 由前一个推论知, R/P 为域. 因此 P 为一个极大理想. $\square$

第五部分

域理论

第二十六章 域

26.1 基本概念

记 F 为一个整环, 且 $0 \neq 1$. 我们以下不考虑 $F = \{0\}$ 的情况.

定义 26.1.1 (教材定义 4.1.1)

我们称一个整环 F 为一个域, 若其所有非零元素都可逆.

回顾: 我们称一个幺环 R 的任意可逆元素为 R 的一个单位. 我们记 U 为 R 的所有单位构成的子集. 则 U 关于幺环 R 的乘法构成一个群. 当 R 是一个域的时候, 我们看到 $U = R^*$ 任意非零元都是一个单位. 因此域 R 关于加法成交换群, 其非零元素构成的子集子集 R^* 关于乘法成交换群.

注 26.1.2.

在查阅资料的时候, 我们需要注意, 有的资料里域的定义仅仅要求 F 是一个幺环($0 \neq 1$) 且所有非零元素可逆, 也即教材中定义的体. 因此, 在那些资料里, 会出现交换域和非交换域的概念. 在本课程中, 我们定义的域总是交换的.

命题 26.1.3 (教材引理 4.1.2)

一个交换幺环 F 为一个域当且仅当 F 中的理想只有 $\{0\}$ 和 F .

证明. 设 I 为 F 的一个理想. 若 F 为一个域, 则 F 中所有非零元素都可逆, 因此若 $I \neq \{0\}$, 则 I 包含一个非零元素 a 且可逆. 因此我们有

$$F = F1 = Fa \subset FI \subset F.$$

因此 $I = F$.

另一方面, 若 F 只有 $\{0\}$ 和 F 两个理想. 我们任取一个非零元素 a , 考虑其生成的主理想 $\langle a \rangle$. 由于 $a \neq 0$, 我们有

$$\langle a \rangle = F.$$

特别的 $1 \in \langle a \rangle$. 因此 a 可逆. 由定义, 我们知道 F 为一个域. □

注 26.1.4.

一个交换幺环 F 为一个域当且仅当 $\{0\}$ 为其极大理想. 更一般的, 我们可以考虑任意交换

么环商掉其任意极大理想来得到一个域. 需要注意的是, 交换么环里总存在极大理想这个命题与选择公理以及 Zorn 引理相互等价.

在对环的讨论中, 我们引入了特征这个概念. 它在我们对域的研究中有着重要的用途. 我们首先回顾一下特征的定义. 记 F 为一个域. 我们考虑其么元 1 . 对任意 $n \in \mathbb{N}^*$, 记

$$n1 = \underbrace{1 + \cdots + 1}_n.$$

定义 26.1.5

我们定义域 F 的特征如下 $\text{Ch}(F)$:

- 若存在 $n \in \mathbb{N}^*$, 满足 $n1 = 0$, 则定义:

$$\text{Ch}(F) := \min\{n \in \mathbb{N}^* \mid n1 = 0\};$$

- 否则, 我们定义 $\text{Ch}(F) := 0$.

注 26.1.6.

之前关于无零因子环的特征的结论 (命题 13.3.1) 告诉我们一个域的特征若非零则为素数.

26.2 子域

26.2.1 定义

定义 26.2.1 (教材定义 4.1.10)

设 E 为一个域, F 为 E 的一个非空子集. 我们称 F 为一个 E 的一个子域, 若其在 E 的运算下是一个域.

作为域, 子域 F 需要有零元 0_F 和么元 1_F , 并且由我们的约定 $1_F \neq 0_F$. 为了区分, 我们暂时记 E 的零元和么元分别为 0_E 和 1_E . 由于 E 是整环, 我们有 $1_F = 1_E$. 实际上任取 $a \in F^*$, 我们有

$$a = 1_F a = 1_E a,$$

因此

$$(1_F - 1_E)a = 0,$$

由于 E 是整环, 我们有

$$1_F = 1_E.$$

因此任取 E 的子域 F , F 的零元和么元就分别是 E 的零元和么元.

当然一个域 E 要满足所有元素关于加法 $+$ 构成交换群, 所有非零元素关于乘法 $\cdot$ 构成交换群, 因此 E 的一个子集 F 如果关于 E 的运算构成域的话就需要关于加法 $+$ 构成子群, 所有非零元素关于乘法 $\cdot$ 构成子群. 从这个角度看, 我们也能得出 $1_E = 1_F$ 的结论, 另一方面, 这中看法也给了我们如下判定一个子集是子域的方法.

命题 26.2.2

设 E 为一个域. 其子集 F 为一个子域当且仅当 F 满足

- $F \cap E^* \neq \emptyset$;
- 任取 $a, b \in F$, 我们有 $a - b \in F$;
- 任取 $a, b \in F^*$, 我们有 $ab^{-1} \in F$.

证明. (练习)

□

和之前所有的代数结构一样, 任意多个子域的交仍是子域.

命题 26.2.3

设 $\mathcal{A}$ 为一个指标集, $\{F_\alpha\}_{\alpha \in \mathcal{A}}$ 为域 E 的一些子域的集合. 则 $\bigcap_{\alpha \in \mathcal{A}} F_\alpha$ 也是 E 的子域.

证明. (这里我们首先需要说明以上集合非空. 而这是由 E 的任意子域都包含 0 和 1 得到的, 具体证明留作练习)

□

26.2.2 子域的生成

设 E 为一个域, S 为 E 的一个非空子集, 且 $S \cap E^* \neq \emptyset$.

定义 26.2.4

我们称所有包含 S 的 E 的子域的交为由 S 生成的域:

$$C(S) = \bigcap \{F \mid S \subset F \subset E, F \text{ 为 } E \text{ 的子域}\}.$$

子集生成的子域也可以通过先生成环, 再考虑对应的分式域得到. (参考附录 13.2.4). 我们记 $A(S)$ 为 E 中由 S 生成的环, 也即 E 中包含 S 的最小的子环.

回顾: 由 S 生成的环可以有如下表达式

$$A(S) = \{a_{00} \cdots a_{0n_0} + \cdots + a_{m0} \cdots a_{mn_m} \mid m \in \mathbb{N}, n_0, \dots, n_m \in \mathbb{N}, a_{ij} \in S \cup (-S)\}.$$

注 26.2.5.

我们注意到这个环不一定是整环. 例如我们考虑 $2 \in \mathbb{Q}$, 则得到的环 $2\mathbb{Z}$. 不过这个并没有问题, 我们在附录 13.2.4 中讨论过分式域的定义可以推广到对一般的无零因子环中.

命题 26.2.6

域 E 中子集 S 生成的子域为 $A(S)$ 的分式域:

$$C(S) = \mathcal{F}(S) := \{ab^{-1} \mid a \in A(S), b \in A(S) \setminus \{0\}\}.$$

证明. 由 $\mathcal{F}(S)$ 的构造, 任意 E 中包含 S 的子域, $\mathcal{F}(S) \subset F$, 因此 $\mathcal{F}(S) \subset C(S)$. 另一方面, $\mathcal{F}(S)$ 为 E 中一个包含 S 的子域, 因此 $C(S) \subset \mathcal{F}(S)$. 因此 $C(S) = \mathcal{F}(S)$. $\square$

若 $S = \{a\}$, 则我们记 S 生成的域为 $C(a)$.

注 26.2.7.

环 $A(S)$ 是用加法, 乘法, 以及取加法逆构造的 E 的子环, 而 $\mathcal{F}(S)$ 为用加法, 乘法, 取加法逆以及乘法逆构造的 E 的子域. 由定义, 域也是环. $A(S)$ 为 E 作为环中包含 S 的最小的子环. $C(S)$ 为包含 S 的最小的域.

素域

定义 26.2.8

我们称一个域 F 为**素域**, 若 F 中的子域只有 F .

命题 26.2.9

任意域 E 中都包含唯一的一个子域为素域.

证明. 任给一个域 E , 我们考虑 E 中所有子域的交, 记为 F . 子域 F 为一个素域. 否则, 存在 F 的真子域 K . 由于 K 也是 E 的子域, 因此要包含 F . 矛盾.

这个子域在 E 中是唯一的. 否则, 假设 F_1 和 F_2 都是 E 的素域, 且不相等, 由于 $F_1 \cap F_2$ 为 F_1 的真子域, 矛盾. $\square$

注 26.2.10.

我们称之为 E 的**素域**.

命题 26.2.11

任给域 E , 其素域为 $C(1)$.

证明. 根据子域的定义, 任何子域都包含 1, 因此包含 $C(1)$. 此外 $C(1)$ 为一个子域, 因此 E 中所有子域的交就是 $C(1)$. $\square$

命题 26.2.12

- (1) $\text{Ch}(E) = p$ 当且仅当 E 的素域同构于 $\mathbb{Z}_p$;
- (2) $\text{Ch}(E) = 0$ 当且仅当 E 的素域同构于 $\mathbb{Q}$.

证明. 我们考虑 $\mathbb{Z}$ 到 E 的环同态:

$$\begin{aligned}\varphi: \mathbb{Z} &\rightarrow E, \\ n &\mapsto n \cdot 1_E.\end{aligned}$$

若存在一个素数 p , 满足 $\text{Ch}(E) = p$, 则我们有 $\ker \varphi = p\mathbb{Z}$. 因此由 1 生成的环 $A(1) \cong \mathbb{Z}/p\mathbb{Z}$. 因此由 1 生成的域 $C(1) \cong \mathbb{F}_p$.

若 $\text{Ch}(E) = 0$, 我们有 $\ker \varphi = \{0\}$, 因此 $A(1) \cong \mathbb{Z}$. 由此由 1 生成的域 $C(1) \cong \mathbb{Q}$. $\square$

26.3 域的扩张

设 E 为一个域.

定义 26.3.1 (教材定义 4.1.10)

若 F 为 E 的一个子域, 我们称 E 为 F 的一个**扩张**, 记作 E/F .

注 26.3.2.

回顾: 我们称 V 为 F -线性空间, 若我们有以下 V 加法运算和数乘运算:

$$\begin{aligned} + : V \times V &\rightarrow V & \cdot : F \times V &\rightarrow V \\ (\mathbf{u}, \mathbf{v}) &\mapsto \mathbf{u} + \mathbf{v} & (a, \mathbf{v}) &\mapsto a\mathbf{v} \end{aligned}$$

满足以下条件

$$(i) \quad \forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V, \quad (\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w});$$

$$(ii) \quad \exists \mathbf{0} \in V, \forall \mathbf{v} \in V, \quad \mathbf{0} + \mathbf{v} = \mathbf{v} + \mathbf{0} = \mathbf{v};$$

$$(iii) \quad \forall \mathbf{v} \in V, \exists -\mathbf{v} \in V, \quad \mathbf{v} + (-\mathbf{v}) = \mathbf{0};$$

$$(iv) \quad \forall \mathbf{u}, \mathbf{v} \in V, \quad \mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u};$$

$$(1) \quad \forall a \in F, \forall \mathbf{u}, \mathbf{v} \in V, \quad a(\mathbf{u} + \mathbf{v}) = (a\mathbf{u}) + (a\mathbf{v});$$

$$(2) \quad \forall \mathbf{v} \in V, \quad 1\mathbf{v} = \mathbf{v};$$

$$(3) \quad \forall a, b \in F, \forall \mathbf{v} \in V, \quad (a + b)\mathbf{v} = (a\mathbf{v}) + (b\mathbf{v});$$

$$(4) \quad \forall a, b \in F, \forall \mathbf{v} \in V, \quad (ab)\mathbf{v} = a(b\mathbf{v}).$$

定理 26.3.3 (教材定理 4.1.14)

若 E 为域 F 的扩张, 则 E 为 F 上的线性空间 (F -线性空间).

定义 26.3.4 (教材定义 4.1.15)

1) 我们称 E 作为 F -线性空间的维数为扩张 E/F 的**次数**, 记作

$$[E : F] := \dim_F E.$$

2) 若 $[E : F] < \infty$, 我们称 E 为 F 的**有限扩张**. 特别地, 若

$$[E : F] = n \in \mathbb{N},$$

我们称 E 为 F 的 n -**次扩张**. 此时 E 作为 F -线性空间的任意一组基被称为 E 的一组 F -**基**.

3) 若 $[E : F] = \infty$, 我们称 E 为 F 的**无限扩张**.

定理 26.3.5 (教材定理 4.1.16)

设域 E 为域 K 的有限扩张, K 为域 F 的有限扩张. 则 E 为 F 的有限扩张, 同时我们有如下关系:

$$[E : F] = [E : K][K : F].$$

证明. 我们设 $[E : K] = m$, $[K : F] = n$. 设 $\{\alpha_1, \dots, \alpha_m\}$ 为 E 的一组 K -基, $\{\beta_1, \dots, \beta_n\}$ 为 K 的一组 F -基.

任取 $\gamma \in E$, 存在 $a_1, \dots, a_m \in K$ 满足

$$\gamma = \sum_{i=1}^m a_i \alpha_i.$$

另一方面, 对任意 $i \in \{1, \dots, m\}$, 我们有 $b_{i1}, \dots, b_{in}$ 满足

$$a_i = \sum_{j=1}^n b_{ij} \beta_j.$$

因此, 我们有

$$\gamma = \sum_{i=1}^m \left(\sum_{j=1}^n b_{ij} \beta_j \right) \alpha_i = \sum_{i=1}^m \sum_{j=1}^n b_{ij} (\beta_j \alpha_i).$$

因此 $\{\alpha_i \beta_j \mid i \in \{1, \dots, m\}, j \in \{1, \dots, n\}\}$ 张成整个空间 E . 我们现在验证其线性无关. 对任意 i, j , 我们取 $c_{ij} \in F$, 使得

$$\sum_{i=1}^m \sum_{j=1}^n c_{ij} (\alpha_i \beta_j) = 0.$$

我们可以将其写为

$$\sum_{i=1}^m \left(\sum_{j=1}^n c_{ij} \beta_j \right) \alpha_i = 0.$$

由 $\alpha_1, \dots, \alpha_m$ 在 E 中 K -线性无关, 且对任意 i , 有 $\sum_{j=1}^n c_{ij} \beta_j \in K$, 因此我们有

$$\sum_{j=1}^n c_{ij} \beta_j = 0.$$

再由 $\beta_1, \dots, \beta_n$ 在 K 中 F -线性无关性, 我们有 $c_{ij} = 0$ 对任意 i, j 成立. 因此集合

$$\{\alpha_i \beta_j \mid i \in \{1, \dots, m\}, j \in \{1, \dots, n\}\},$$

为 E 的一组 F -基. 因此作为 F -线性空间, E 为 mn -维. 因此定理得证. $\square$

设 E 为 K 的一个扩张, K 为 F 的一个扩张.

定义 26.3.6

我们称 K 为扩张 E/F 的一个**中间域**, 并称扩张 K/F 为 E/F 的一个**子扩张**.

26.4 域同态

我们记 E 和 F 为两个域. 记 $\varphi: F \rightarrow E$ 为一个 F 到 E 的映射.

定义 26.4.1 (教材定义 4.1.4)

我们称映射 φ 为 F 到 E 的一个**域同态**, 若其满足以下条件:

- 任取 $a, b \in F$, 有 $\varphi(a + b) = \varphi(a) + \varphi(b)$;
- 任取 $a, b \in F$, 有 $\varphi(ab) = \varphi(a)\varphi(b)$;
- $\varphi(1_F) = 1_E$.

注 26.4.2.

由于域本身是一个所有非零元素构成一个乘法交换群的环, 而同态只要求与双方的二元运算相容, 因此, 域同态的定义与环同态的定义基本相同. 唯一附加的条件是需要将幺元送到幺元.

实际上这个条件是非常自然的. 任取域 F 和 E , 设

$$\varphi: F \rightarrow E,$$

为一个环同态. 我们下边讨论一下 1_F 被送到了哪里

注意到 $\varphi(F) \subset E$ 为一个子环(我们目前考虑环同态). 注意到 $\varphi(F)$ 为一个幺环, 任取 $\alpha \in \varphi(F)$, 存在 $a \in F$, 满足 $\varphi(a) = \alpha$, 注意到

$$\alpha\varphi(1_F) = \varphi(a1_F) = \varphi(a) = \alpha = \varphi(a) = \varphi(1_F a) = \varphi(1_F)\alpha,$$

因此 $\varphi(1_F)$ 为 $\varphi(F)$ 的幺元.

若 $\varphi(F) \neq \{0_E\}$, 任取 $\alpha \in \varphi(F)^*$, 我们有

$$\alpha = \alpha\varphi(1_F) = \alpha 1_E,$$

因此

$$(\varphi(1_F) - 1_E)\alpha = 0.$$

由于 E 无零因子, 因此我们有

$$\varphi(1_F) = 1_E.$$

也就是说, 如果 φ 是一个非平凡的从 F 到 E 的域同态 (即 $\varphi(F) \neq \{0_E\}$), 则一定有 $\varphi(1_F) = 1_E$.

注意到

$$\begin{aligned}\varphi : F &\rightarrow E, \\ a &\mapsto 0_E,\end{aligned}$$

也是环同态, 但是是"平凡的". 因此定义中的第三个条件等价于 φ 是一个非平凡的环同态.

与之前群同态和环同态的讨论不同, 我们先证明如下命题:

命题 26.4.3 (教材引理 4.1.9)

任何域同态都是单射.

证明. 设 $\varphi : F \rightarrow E$ 为一个域同态. 我们考虑其核 $\ker \varphi$. 从环的角度, 我们知道 $\ker \varphi$ 是 F 的一个理想. 由于 F 是一个域, 其理想只有 $\{0\}$ 和 F , 且 $\varphi(1_F) = 1_E$, 我们可以得出

$$\ker \varphi = \{0\}.$$

因此 φ 是一个单射. □

定义 26.4.4

设 $\varphi : F \rightarrow E$ 为一个域同态.

- 1) 我们称 φ 为一个**域同构**, 若其为满射.
- 2) 若 $F = E$, 我们称 φ 为域 E 的**自同态**. 若进一步还有 φ 为一个域同构, 我们称 φ 为域 E 的**自同构**.

设 E 和 F 为两个域. 我们记 $\text{Hom}(F, E)$ 为 F 到 E 的域同态的集合:

$$\text{Hom}(F, E) := \{\varphi : F \rightarrow E \text{ 为一个域同态}\}.$$

当 $F = E$, 我们记

$$\text{End}(E) := \text{Hom}(E, E),$$

为 E 的所有域自同态的集合, 并记

$$\text{Aut}(E) := \{\varphi : E \rightarrow E \text{ 为一个域同构}\},$$

为 $\text{End}(E)$ 中 E 所有的域自同构的集合.

命题 26.4.5 (教材注记 4.1.5)

任给域 E , 其域自同构集合 $\text{Aut}(E)$ 以及同构的复合运算构成一个群.

注 26.4.6.

考虑复合映射 $\text{End}(E)$ 是一个么半群.

定义 26.4.7 (教材注记 4.1.5)

记 E 为一个域, 我们称群 $\text{Aut}(E)$ 为 E 的**自同构群**.

下边这个命题是域同态除了单射之外的另一个特别的性质.

命题 26.4.8 (教材推论 4.1.13)

设 $\varphi: F \rightarrow E$ 为一个域同态. 则 φ 为 F 的素域到 E 的素域的域同构. 特别地, 若 F 和 E 都是素域 Π 的扩张, 则 φ 限制在 Π 是恒等映射.

推论 26.4.9

若域 F 和域 E 之间存在域同态映射, 则 $\text{Ch}(F) = \text{Ch}(E)$.

注 26.4.10.

以上命题的逆命题, 即若 $\text{Ch}F = \text{Ch}E$, 我们不一定有域同态

$$\varphi: F \rightarrow E.$$

一个例子就是 $E = F_0$ 为 F 的素域. 我们使用反证法来证明当 $F_0 \subsetneq F$ 时, 不存在 F 到 F_0 的同态.

假设存在 F 到 F_0 的同态, 记为 φ , 由之前的命题, 我们知道 $\varphi|_{F_0}$ 为 F_0 上的恒等映射, 由于

$$F_0 \subsetneq F,$$

我们有 φ 不是单射, 矛盾. 因此不存在从 F 到 F_0 的域同态 φ .

以上讨论一个简单的应用就是, 不存在从 $\mathbb{R}$ 到 $\mathbb{Q}$ 的域同态.

注 26.4.11.

前一个注记告诉我们不是任何两个域之间的都有同态, 即有可能有域 F 和 E , 使得

$$\text{Hom}(F, E) = \emptyset,$$

另一方面, 由于任何域上的恒等映射都是域同构, 因此任何域 E 都有自同构. 因此 E 的域自同构群 $\text{Aut}(E)$ 以及所有自同态幺半群 $\text{End}(E)$ 总是存在的.

 $\text{End}(E)$ 和 $\text{Aut}(E)$ 的关系

设 E/F 为一个域扩张, 我们记

$$\text{End}_F(E) := \{\varphi \in \text{End}(E) \mid \varphi|_F = \text{id}_F\}.$$

$$\text{Aut}_F(E) := \{\varphi \in \text{Aut}(E) \mid \varphi|_F = \text{id}_F\}.$$

命题 26.4.12

若 E/F 为一个有限域扩张, 则 $\text{End}_F(E) = \text{Aut}_F(E)$

证明. 任给一个 $\varphi \in \text{End}_F(E)$, 我们有 $\varphi(E)$ 为 E/F 的一个中间域. 使用扩张的次数的关系, 我们有

$$[E : \varphi(E)][\varphi(E) : F] = [E : F].$$

由于 φ 为单射且 $\varphi|_F = \text{id}_F$, 因此 $[\varphi(E) : F] = [E : F]$. 由此可得

$$[E : \varphi(E)] = 1,$$

这等价于

$$\varphi(E) = E$$

即 φ 为满射. 因此 φ 为同构. □

由于每个 E 的自同态在 E 的素域上的限制都是恒等映射, 因此我们有如下推论:

推论 26.4.13

若 E 为其素域的有限扩张, 我们有 $\text{End}(E) = \text{Aut}(E)$.

更进一步地, 当 E 是有限域的时候, E 一定是其素域的有限扩张, 因此我们有如下推论:

推论 26.4.14

若域 E 为一个有限域, 则有 $\text{End}(E) = \text{Aut}(E)$.

当并不是所有的域的自同态都是自同构. 我们下边给出两个 $\text{End}(E) \neq \text{Aut}(E)$ 的例子:

例 26.4.15.

设 p 为一个素数, $E = \mathbb{F}_p(t)$. 这是 $\mathbb{F}_p$ 上多项式环的分式域. 我们有 $\text{Ch}(E) = p$. 考虑以下与自同态:

$$\begin{aligned} \text{Fr} : \mathbb{F}_p(t) &\rightarrow \mathbb{F}_p(t) \\ f(t) &\mapsto (f(t))^p. \end{aligned}$$

我们可以验证 $t \notin \mathbb{F}_p$. 因此该自同态不是满射, 即不是自同构.

注意到该自同态限制在 $\mathbb{F}_p$ 上被称作 $\mathbb{F}_p$ 的 **Frobenius 同构**. 注意到这样的同态实际上在任意特征为 p 的域上都可以定义, 我们称之为 **Frobenius 同态**.

另一个例子来自于无限集合可以与自己的子集之间存在双射.

例 26.4.16.

我们考虑实数域上的如下无限元多项式环

$$\mathbb{R}[t_n \mid n \in \mathbb{N}],$$

考虑其分式域

$$E = \mathbb{R}(t_0, t_1, \dots),$$

注意到域 E 是由

$$\{t_n \mid n \in \mathbb{N}\},$$

生成的. 我们考虑 E 的自同态 φ , 满足对任意 $n \in \mathbb{N}$, 我们有

$$\varphi(t_n) = t_{n+1}.$$

注意到 $\varphi(E) = \mathbb{R}(t_1, t_2, \dots)$, 因此 $t_0 \notin \varphi(E)$, 即 φ 不是满射, 不是一个域同构.

第二十七章 域的代数扩张

从生成的角度看域扩张 E/F , 扩域 E 也可以看作是向 F 中添加了一些元素生成得到的. 一个自然的问题就是我们添加的元素是否和 F 中的元素有某种关系, 也即是否可以通过域运算得到 0. 因此我们需要研究一个添加的元素 α 是否是某个 F 上非零多项式的根. 这也就是我们之前讨论的代数元和超越元的概念.

27.1 域上的代数元

我们首先回顾一下域(作为环的一种)上代数元的概念. 设域 E 为域 F 的扩张. 任取 $\alpha \in E$, 我们考虑其诱导的 $F[x]$ 上的赋值映射:

$$\begin{aligned}\phi_\alpha : F[x] &\rightarrow E \\ f(x) &\mapsto f(\alpha)\end{aligned}$$

由多项式理论的学习我们知道 ϕ_α 为一个环同态, 其核为 $F[x]$ 的一个理想.

定义 27.1.1

任取 $f(x) \in \ker \phi_\alpha$, 我们称其为 α 的一个**零化多项式**, 即 $F[x]$ 中满足 $f(\alpha) = 0$ 的多项式.

回顾: 任取环 F , 以下三个叙述等价,

- (i) F 为一个域;
- (ii) $F[x]$ 为一个 PID;
- (iii) $F[x]$ 为一个欧几里得整环.

由以上回顾, 我们知道 $\ker \phi$ 是一个主理想. 因此我们有如下结论.

命题 27.1.2

设 $\alpha \in E$. 存在一个多项式 $f_\alpha(x) \in F[x]$, 满足

$$\ker \phi = \langle f_\alpha(x) \rangle.$$

并且 $f_\alpha(x)$ 在相伴意义下唯一.

注 27.1.3.

若 $\ker \phi_\alpha = \{0\}$, 则 $f_\alpha(x) = 0 \in F[x]$.

定义 27.1.4

记 E/F 为一个域扩张, $\alpha \in E$. 设 $f_\alpha(x) \in F[x]$, 满足

$$\ker \phi_\alpha = \langle f_\alpha(x) \rangle.$$

1) 若 $f_\alpha(x) \neq 0$ (即 $\ker \phi_\alpha \neq \{0\}$), 我们称 α 为 F 上的**代数元**, 此时:

(a) 我们称 $f_\alpha(x) \in F[x]$ 为 α 在 F 上的**最小多项式**, 也记作 $\text{Irr}(\alpha, F)$.

(b) 我们称 $\deg f_\alpha(x)$ 为 α 在 F 上的**次数**, 也记作 $\deg(\alpha, F)$.

2) 若 $f_\alpha = 0$, 也即 $\ker \phi_\alpha = \{0\}$, 我们称 α 为 F 上的**超越元**.

注 27.1.5.

任取 $f(x) \in F[x]^*$, 通过乘以首项系数的逆, $f(x)$ 总是和某个首一多项式相伴. 在后续的部分中, 我们经常可以通过考虑首一多项式来简化讨论. 例如, 我们说两个不可约多项式 $p(x)$ 和 $q(x)$ 相伴的时候, 通常我们不能得到相等. 但如果 $p(x)$ 和 $q(x)$ 是两个首一的不可约多项式, 那么就有 $p(x)$ 和 $q(x)$ 相伴当且仅当 $p(x) = q(x)$.

注 27.1.6.

任取 0 次多项式 $a \in F[x]^*$, 任取 $\alpha \in E$, 我们有

$$\phi_\alpha(a) = a.$$

因此 $a \in F[x]$ 不零化任意 $\alpha \in E$. 由此可知, 任意 F 上代数元 α 的次数满足

$$\deg(\alpha, F) = \deg f_\alpha(x) > 0.$$

注意到 F 中的元素都是 F 上的代数元. 任取 $a \in F$, 我们总有

$$x - a \in F[x],$$

零化 a . 实际上, 我们可以利用这个观察来刻画 F 中的元素.

引理 27.1.7

设 E/F 为一个域扩张. 设 $\alpha \in E$ 为 F 上的代数元. 以下两个叙述等价:

1) $\alpha \in F$;

2) $\deg(\alpha, F) = 1$.

证明. 若 $\alpha \in F$, 则 α 被 $x - \alpha \in F[x]$ 零化. 任取 $f(x) \in F[x]$, 考虑带余除法

$$f(x) = p(x)(x - \alpha) + r(x),$$

其中 $0 \leq \deg r(x) < 1$ 或者 $r(x) = 0$. 因此 $r(x) = a \in F$.

若 $f(\alpha) = 0$, 则 $r(\alpha) = a = 0$, 因此

$$x - a \mid f(x).$$

由此可得

$$f_\alpha(x) = x - \alpha.$$

进而有

$$\deg(\alpha, F) = \deg f_\alpha(x) = 1.$$

反过来设

$$\deg f_\alpha(x) = 1,$$

存在 $a \in F$, 满足

$$f_\alpha(x) = x - a \in F[x].$$

由

$$0 = f_\alpha(\alpha) = \alpha - a,$$

得 $\alpha = a \in F$. □

利用 E 中没有零因子, 我们还可以得到以下最小多项式的性质.

命题 27.1.8

记 E/F 为一个域扩张. 设 $\alpha \in E$ 为 F 上的代数元, 则其最小多项式 $f_\alpha(x) \in F[x]$ 不可约.

证明. 由题设, 我们有

$$\ker \phi_\alpha := \{f(x) \in F[x] \mid f(\alpha) = 0\} = \langle f_\alpha(x) \rangle.$$

因此任给 $f(x) \in F[x]$, 我们有 $f(\alpha) = 0$ 当且仅当

$$f_\alpha(x) \mid f(x).$$

下设存在 $g(x), h(x) \in F[x]$, 满足

$$f_\alpha(x) = g(x)h(x).$$

由 $f_\alpha(\alpha) = 0$ 可得

$$g(\alpha)h(\alpha) = 0,$$

由于 E 中没有零因子, 我们有

$$g(\alpha) = 0 \text{ 或者 } h(\alpha) = 0.$$

也即

$$f_\alpha(x) \mid g(x) \text{ 或者 } f_\alpha(x) \mid h(x).$$

不失一般性地, 我们以下设 $f_\alpha(x) \mid g(x)$.

下边比较 $\deg f_\alpha(x)$ 和 $\deg g(x)$. 由于 $f_\alpha(x) \neq 0$, 因此 $g(x) \neq 0$ 且 $h(x) \neq 0$, 因此我们有

$$\deg f_\alpha(x) = \deg g(x) + \deg h(x).$$

因此

$$\deg f_\alpha(x) \geq \deg g(x).$$

另一方面由于

$$f_\alpha(x) \mid g(x),$$

且由之前讨论知二者均非零多项式, 我们有

$$\deg f_\alpha(x) \leq \deg g(x).$$

综上所述我们有

$$\deg f_\alpha(x) = \deg g(x).$$

因此

$$\deg h(x) = 0,$$

即

$$h(x) = a \in F^*.$$

为单位. 因此 $f_\alpha(x)$ 不可约. □

这个结果有如下价格推论.

推论 27.1.9

记 E/F 为一个域扩张. 任取 $\alpha \in E$ 为 F 上的代数元, 设 $f(x) \in F[x]$ 为一个不可约多项式, 且 $f(\alpha) = 0$, 则

$$f(x) = f_\alpha(x) \in F[x],$$

即 $f(x)$ 为 α 在 F 上的最小多项式.

推论 27.1.10

记 E/F 为一个域扩张. 设 $\alpha \in E$ 为 F 上的代数元, 则 $\langle f_\alpha(x) \rangle$ 为一个极大理想.

证明. 由于 F 为一个域, 因此 $F[x]$ 为一个 PID. 利用推论 ??, 由于 $f_\alpha(x)$ 不可约, 我们有

$$\langle f_\alpha(x) \rangle \subset F[x],$$

为 $F[x]$ 的极大理想. □

推论 27.1.11

记 E/F 为一个域扩张. 设 $\alpha \in E$ 为 F 上的代数元, 则 $F[x]/\langle f_\alpha(x) \rangle$ 为一个域.

证明. 由于 $\langle f_\alpha(x) \rangle$ 为极大理想, 我们有商环

$$F[x]/\langle f_\alpha(x) \rangle,$$

为一个域. □

$\alpha \in E$ 在 F 上生成的域

之前提到 F 的扩域 E 可以看作是 F 和一些 E 中的元素生成的域. 作为一个基础的例子, 我们来看下 F 和一个元素 $\alpha \in E$ 生成的域的情况.

定义 27.1.12

记 E/F 为一个域扩张. 任取 $\alpha \in E$, 我们可以记

$$F(\alpha) := C(F \cup \{\alpha\}),$$

为 E 中由 $F \cup \{\alpha\}$ 生成的子域, 称之为 α 在 F 上生成的子域.

我们称 $F(\alpha)/F$ 为 F 的单扩张.

若 $\alpha \in E$ 为 F 上的代数元. 由环的同态定理, 我们可以得到一个环的单同态 $\overline{\phi_\alpha}$

$$\begin{array}{ccc} F[x] & \xrightarrow{\phi_\alpha} & E \\ \pi_\alpha \downarrow & \nearrow \exists! \overline{\phi_\alpha} & \\ F[x]/\langle f_\alpha \rangle & & \end{array}$$

由以上讨论可知 $\overline{\phi_\alpha}$ 也是一个域同态. 注意到

$$F[\alpha] = \text{Im } \phi_\alpha = \text{Im } \overline{\phi_\alpha}$$

因此 $F[\alpha]$ 为一个域. 此时我们有

$$F(\alpha) = F[\alpha].$$

例 27.1.13.

我们考虑 $E = \mathbb{R}$, $F = \mathbb{Q}$. 令 $\alpha = \sqrt{2}$ 为 $\mathbb{Q}$ 上的代数元. 其最小多项式为 $f_\alpha = x^2 - 2 \in \mathbb{Q}[x]$ 在 $\mathbb{Q}$ 上是不可约的(不可分解为非零次多项式的乘积). 因此商环

$$\mathbb{Q}[x]/\langle f_\alpha \rangle,$$

为一个域. 注意到在这个等价关系下, 所有次数为 2 的多项式都与某个次数最多为 1 的多项式等价. 使用归纳法, 我们可以证明任意次数大于 1 的多项式都与某个次数最多为 1 的多项式等价. 因此我们只需考虑每个等价类里次数最多为 1 的代表元.

考虑 $g = 1 + x$. 若我们希望找到 $\bar{g}$ 的逆元, 我们只需考虑一个次数不超过 1 的多项式 h , 满足 $hg = 1 + g_1 f_\alpha$. 特别地, 我们可以假设 $h = a + bx$.

$$\begin{aligned} gh &= (1+x)(a+bx) \\ &= a + (a+b)x + bx^2 \\ &= (a+2b) + (a+b)x + b(x^2-2). \end{aligned}$$

因此, 我们有以下线性方程组

$$\begin{cases} a + 2b = 1 \\ a + b = 0 \end{cases}$$

通过解方程, 我们得到 $a = -1$, $b = 1$. 因此 $(\bar{g})^{-1} = \overline{-1+x}$.

我们也可以用另一种方法来说明这个结论. 注意到

$$F[\alpha] \subset F(\alpha).$$

我们只需证明另一个方向的包含即可. 我们将证明以下结论:

命题 27.1.14

记 E/F 为一个域扩张. 设 $\alpha \in E$ 为 F 上的代数元, 则任取 $g(x) \in F[\alpha]$, 满足 $g(\alpha) \neq 0$, 存在多项式 $q(x) \in F[x]$, 满足

$$q(\alpha) = g(\alpha)^{-1}.$$

证明. 我们记 $f_\alpha(x) \in F[x]$ 为 α 在 F 上的最小多项式. 任取 $g(x) \in F[x]$, 若

$$g(\alpha) \neq 0,$$

则

$$g(x) \notin \langle f_\alpha(x) \rangle,$$

因此

$$f_\alpha(x) \nmid g(x).$$

由于 $f_\alpha(x)$ 不可约, 在 $F[x]$ 中我们有

$$\gcd(f_\alpha(x), g(x)) = 1.$$

利用 $F[x]$ 中的 Bezout 等式, 存在 $p(x), q(x) \in F[x]$, 满足

$$p(x)f_\alpha(x) + q(x)g(x) = 1.$$

考虑左右两边在 α 处的取值, 我们有

$$q(\alpha)g(\alpha) = 1.$$

因此

$$q(\alpha) = g(\alpha)^{-1}.$$

□

另一方面, 设 $\alpha \in E$ 为 F 上的超越元, 则我们有环同构 $F[x] \cong F[\alpha]$. 因此它们的分式域同构

$$F(x) \cong F(\alpha).$$

特别地, 我们有一个域同态

$$\psi : F(x) \rightarrow E,$$

满足 $\psi|_F = \text{id}_F$, 以及 $\psi(x) = \alpha$.

综上所述, 我们有以下定理

定理 27.1.15 (教材定理 4.2.13)

记 E/F 为一个域扩张, 任取 $\alpha \in E$, 我们有

$$F(\alpha) \cong \begin{cases} F[x]/\langle f_\alpha(x) \rangle & \alpha \text{ 为代数元} \\ F(x) & \alpha \text{ 为超越元} \end{cases}$$

定义 27.1.16

记 E/F 为一个域扩张. 任取 $\alpha \in E$,

1. 若 α 为 F 上的代数元, 我们称 $F(\alpha)/F$ 为一个**单代数扩张**;
2. 若 α 为 F 上的超越元, 我们称 $F(\alpha)/F$ 为一个**单超越扩张**.

记 E/F 为一个域扩张. 任取 $\alpha \in E$, 我们考虑单扩张 $F(\alpha)/F$

命题 27.1.17

设 $\alpha \in E$ 为 F 上的一个代数元, 则 $F(\alpha)$ 为 F 的一个有限扩张, 且

$$[F(\alpha) : F] = \deg(\alpha, F) = \deg f_\alpha(x).$$

证明. 设 $\deg f_\alpha(x) = m$, 记

$$f_\alpha(x) = a_0 + a_1x + \cdots + a_mx^m \in F[x].$$

任取 $g(x) \in F[x]$, 利用带余除法, 我们有 $p(x), r(x) \in F[x]$, 满足

$$g(x) = p(x)f_\alpha(x) + r(x),$$

其中 $0 \leq \deg r(x) < f_\alpha(x)$ 或者 $r(x) = 0$.

考虑两边在赋值映射 ϕ_α 下的像, 则有

$$g(\alpha) = r(\alpha).$$

因此

$$g(\alpha) \in F + F\alpha + \cdots + F\alpha^{m-1} \subset F[\alpha].$$

因此

$$F(\alpha) = F[\alpha] = F + F\alpha + \cdots + F\alpha^{m-1}.$$

下边只需证明作为 F -线性空间 $F(\alpha)$ 的元素,

$$\{1, \alpha, \dots, \alpha^{m-1}\}$$

是 F -线性无关的. 否则存在 $b_0, \dots, b_{m-1} \in F$ 不全为零, 满足

$$b_0 + b_1\alpha + \cdots + b_{m-1}\alpha^{m-1} = 0.$$

记

$$g(x) = b_0 + \cdots + b_{m-1}x^{m-1} \in F[x]^*,$$

则有 $g(\alpha) = 0$. 因此

$$f_\alpha(x) \mid g(x),$$

由 $g(x) \neq 0$, 有

$$m = \deg f_\alpha(x) \leq \deg g(x) \leq m-1,$$

矛盾.

综上所述, 以下元素

$$1, \alpha, \dots, \alpha^{m-1}$$

构成 $F(\alpha)$ 的一组 F -基, 因此有

$$\dim_F F(\alpha) = m = \deg f_\alpha(x).$$

□

27.2 域的代数扩张

定义 27.2.1 (教材定义 4.2.2)

记 E/F 为一个域扩张. 我们称 E 为 F 的**代数扩张**, 若任取 $\alpha \in E$, 元素 α 为 F 的代数元.

命题 27.2.2 (教材引理 4.2.1)

若 E 为 F 的一个有限次扩张, 则 E 为 F 的一个代数扩张.

证明. 我们设

$$\dim_F E = [E : F] = n \in \mathbb{N}^*,$$

任取 $\alpha \in E$, 考虑非零元素 $1, \alpha, \alpha^2, \dots, \alpha^n$. 这 $n+1$ 个非零元素必然 F -线性相关, 也即存在不全为 0 的 F 的 $n+1$ 个元素:

$$a_0, \dots, a_n,$$

满足

$$a_0 + a_1\alpha + \dots + a_n\alpha^n = 0.$$

这等价于存在

$$f(x) = a_0 + \dots + a_n x^n \in F[x]^*,$$

满足 $f(\alpha) = 0$. 因此 α 为 F 上的代数元. □

注 27.2.3.

特别地, 对任意 $\alpha \in E$, 我们有 $F(\alpha) \subset E$ 为一个 F -子空间, 因此

$$1 \leq [F(\alpha) : F] \leq [E, F] < \infty.$$

之前关于单扩张的讨论告诉我们, α 为一个代数元.

设 E/F 为一个域扩张.

定义 27.2.4 (教材定义 4.2.3)

任给 E 的非空子集 S , 我们称 $C(F \cup S)$ 为 S 在 F 上**生成的域**, 并将其记作 $F(S)$.

命题 27.2.5 (教材命题 4.2.4)

记 E/F 为一个域扩张. 任取域 E 的非空子集 S , 我们有:

$$F(S) = \bigcup \{F(S') \mid S' \subset S, S' \text{ 有限}\}.$$

证明. 任取 $\emptyset \neq S' \subset S$, 我们有

$$F \cup S' \subset F(S),$$

由集合生成的子域的定义, 我们进而有

$$F(S') \subset F(S).$$

因此我们有

$$F(S) \supset \bigcup \{F(S') \mid S' \subset S, S' \text{ 有限}\}.$$

下边证明另一个方向的包含. 注意到

$$S = \bigcup_{\alpha \in S} \{\alpha\}.$$

因此我们有

$$F \cup S \subset \bigcup_{\alpha \in S} F(\alpha) \subset \bigcup \{F(S') \mid S' \subset S, S' \text{ 有限}\}.$$

由集合生成的子域的定义, 我们有

$$F(S) \subset \bigcup \{F(S') \mid S' \subset S, S' \text{ 有限}\}.$$

综上所述, 我们有

$$F(S) = \bigcup \{F(S') \mid S' \subset S, S' \text{ 有限}\}.$$

□

注 27.2.6.

任取 E 的两个子域 F_1 和 F_2 , 集合 $F_1 \cup F_2$ 并不一定是一个子域. 例如, 我们考虑扩张

$$\mathbb{Q}(\sqrt{3}, \sqrt{2})/\mathbb{Q}.$$

集合

$$\mathbb{Q}(\sqrt{2}) \cup \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3}, \sqrt{2}),$$

不是一个子域. 注意到 $\sqrt{2} + \sqrt{3}$ 不在其中, 因为 $\sqrt{2} + \sqrt{3}$ 在 $\mathbb{Q}$ 上的次数是 4, 但是集合

$$\mathbb{Q}(\sqrt{2}) \cup \mathbb{Q}(\sqrt{3}),$$

中所有元素在 $\mathbb{Q}$ 上的次数至多为 2.

以上命题在 S 有限的时候是平凡的. 例如, 设 $S = \{\alpha_1, \alpha_2\}$, 以上命题的等式应被写为:

$$F(\alpha_1, \alpha_2) = F(\alpha_1) \cup F(\alpha_2) \cup F(\alpha_1, \alpha_2).$$

我们需要考虑所有的有限子集, 其中就有 S .

以上命题在 S 的势无穷的时候是非平凡的. 也即每个分式域中的元素只用到了 $F \cup S$ 中有限多个元素. 当然这个有限子集可以很大, 因此我们需要考虑所有的有限子集. 一个例子就是 F 上的无限元多项式环的分式域

$$F(t_n \mid n \in \mathbb{N}).$$

我们记 $S = \{t_n \mid n \in \mathbb{N}\}$, 则任意其中的元素都只涉及 S 中有限多个元素, 但是这有限多个元素的数目可以是任意大.

命题 27.2.7 (教材命题 4.2.4)

记 E/F 为一个域扩张. 记 S_1 和 S_2 为域 E 的两个非空子集, F 为域 E 的一个子域. 记 $S = S_1 \cup S_2$, 则我们有

$$F(S) = F(S_1)(S_2).$$

注 27.2.8.

这里的记号 $F(S_1)(S_2)$ 是指集合 S_2 在域 $F(S_1)$ 上生成的域.

证明. 注意到两个域都是 E 的子域. 我们只需验证两个域作为集合相等即可.

注意到

$$F \cup S_1 \subset F(S_1) \subset F(S_1)(S_2),$$

且

$$S_2 \subset F(S_1)(S_2),$$

因此

$$F \cup S = F \cup S_1 \cup S_2 \subset F(S_1)(S_2),$$

因此

$$F(S) \subset F(S_1)(S_2).$$

另一方面, 注意到

$$S_1 \subset S,$$

因此

$$F \cup S_1 \subset F(S),$$

进而有

$$F(S_1) \subset F(S).$$

又由于

$$S_2 \subset S \subset F(S),$$

因此

$$F(S_1) \cup S_2 \subset F(S),$$

由此可得

$$F(S_1)(S_2) \subset F(S).$$

综上所述, 我们有

$$F(S_1)(S_2) = F(S).$$

□

我们可以使用归纳法证明

推论 27.2.9 (教材推论 4.2.5)

记 E/F 为一个域扩张, 则任取 $\alpha_1, \dots, \alpha_n \in E$, 我们有

$$F(\alpha_1, \dots, \alpha_n) = F(\alpha_1) \cdots (\alpha_n).$$

注 27.2.10.

当我们扩张 F 至 $F(\alpha_1, \dots, \alpha_n)$, 我们可以分 n 次进行, 每次都考虑一个元素的扩张.

我们考虑命题 27.1.17 和 27.2.2, 则可得出以下推论.

推论 27.2.11 (教材推论 4.2.7)

记 E/F 为一个域扩张. 任取 $\alpha, \beta \in E$, 为 F 上的代数元, 则以下元素

$$\alpha + \beta, \alpha - \beta, \alpha\beta, \alpha\beta^{-1} (\beta \neq 0),$$

均为 F 上的代数元.

证明. 注意到

$$[F(\alpha, \beta) : F] = [F(\alpha)(\beta) : F(\alpha)][F(\alpha) : F].$$

由于 α 为 F 上的代数元, 因此

$$[F(\alpha) : F] < \infty.$$

由于 β 为 F 上的代数元, 因此也是 $F(\alpha)$ 上的代数元, 由此可得

$$[F(\alpha)(\beta) : F(\alpha)] < \infty.$$

因此

$$[F(\alpha, \beta) : F] < \infty.$$

由命题 27.2.2, 我们有 $F(\alpha, \beta)/F$ 为一个代数扩张.

由于

$$\alpha + \beta, \alpha - \beta, \alpha\beta, \alpha\beta^{-1} (\beta \neq 0),$$

都是 $F(\alpha, \beta)$ 中的元素, 由代数扩张的定义得到结论. □

总结以上讨论, 我们给出如下定理

定理 27.2.12 (教材定理 4.2.6)

记 E/F 为一个域扩张, $\alpha_1, \dots, \alpha_n \in E$. 我们考虑 $K = F(\alpha_1, \dots, \alpha_n)$. 以下三个叙述等价:

- (i) K 为 F 的代数扩张.
- (ii) $\alpha_1, \dots, \alpha_n$ 都为 F 上的代数元.
- (iii) K 为 F 的有限扩张.

证明. 我们考虑 $F(\alpha_1, \dots, \alpha_n) = F(\alpha_1) \cdots F(\alpha_n)$.

命题 27.2.2 证明了 (iii) $\implies$ (i).

由定义 (i) $\implies$ (ii).

要证明 (ii) $\implies$ (iii), 我们考虑域扩张列

$$F(\alpha_1, \dots, \alpha_n) / \cdots / F(\alpha_1, \alpha_2) / F(\alpha_1) / F,$$

考虑命题 27.1.17, 我们有

$$[F(\alpha_1, \dots, \alpha_n) : F] = [F(\alpha_1, \dots, \alpha_n) : F(\alpha_1, \dots, \alpha_{n-1})] \cdots [F(\alpha_1, \alpha_2) : F(\alpha_1)][F(\alpha_1) : F].$$

对任意 $1 \leq i \leq n$, 元素 α_i 为 F 上的代数元. 因此任取 $2 \leq i \leq n$, α_i 为 $F(\alpha_1, \dots, \alpha_{i-1})$ 上的代数元. 因此以上等式右边各扩张次数均有限. 由此可得

$$[K : F] < \infty.$$

□

注 27.2.13.

任给 E 中 F 的有限扩张 K , 设 $\beta_1, \dots, \beta_m$ 为 K 的一组 F -基, 我们有

$$K = F(\beta_1, \dots, \beta_m).$$

我们要注意的, K 在 F 上生成元的数目可以严格小于其维数. 例如, 记 $\xi_5 \in \mathbb{C}$ 为 5 次单位根, 其在 $\mathbb{Q}$ 上的最小多项式

$$\Phi_5(x) = 1 + x + x^2 + x^3 + x^4 \in \mathbb{Q}[x],$$

则

$$[\mathbb{Q}(\xi_5) : \mathbb{Q}] = 4.$$

利用命题 27.2.5, 我们可以得到以下推论

推论 27.2.14 (教材推论 4.2.9)

设非空子集 $S \subset E$ 的元素都为 F 上的代数元, 则 $F(S)$ 为一个代数扩张.

注 27.2.15.

此时, 集合 S 的势可以任意.

定理 27.2.16 (教材定理 4.2.10)

若 E 为 K 的一个代数扩张, K 为 F 的一个代数扩张, 则 E 为 F 的代数扩张.

注 27.2.17.

这个定理告诉我们代数扩张就有传递性.

证明. 我们知道 E 为 K 的有限扩张, 任取 $\alpha \in E$, 存在 K 中不全为零的元素 $a_0, \dots, a_n$, 满足

$$a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$$

我们考虑 $F(a_0, \dots, a_n)$. 以上条件告诉我们 α 在 $F(a_0, \dots, a_n)$ 上的次数小于等于 n .

$$[F(a_0, \dots, a_n, \alpha) : F(a_0, \dots, a_n)] \leq n.$$

另一方面, 由于 $a_0, \dots, a_n$ 都是 F 上的代数元, 由定理 27.2.12, 有

$$[F(a_0, \dots, a_n) : F] < \infty.$$

综合以上结论, 我们有

$$[F(a_0, \dots, a_n, \alpha) : F] = [F(a_0, \dots, a_n, \alpha) : F(a_0, \dots, a_n)][F(a_0, \dots, a_n) : F] < \infty.$$

由定理 27.2.12, 我们知道

$$F(a_0, \dots, a_n, \alpha)/F,$$

为代数扩张, 因此 α 为 F 上的代数元. $\square$

任给一个 F 的扩域 E , 其中可能同时包含 F 上的代数元和超越元. 我们可以记 $E_0 \subset E$ 为如下集合:

$$E_0 := \{\alpha \in E \mid \alpha \text{ 为 } F \text{ 上的代数元}\}.$$

我们可以直接验证 E_0 为一个域, 且包含 F .

定义 27.2.18

我们称 E_0 为 F 在 E 中的代数闭包.

注 27.2.19.

注意这个定义与后边一个域的代数闭包之间的区别.

若

$$E \setminus E_0 \neq \emptyset,$$

那么由 E_0 的定义, 任取 $\alpha \in E \setminus E_0$, 都有 α 为 F 上的超越元. 利用代数扩张的传递性, 我们得到如下定理:

定理 27.2.20 (教材定理 4.2.11)

任取域扩张 E/F , 我们记 E_0 为 F 在 E 中的代数闭包. 设 $E \setminus E_0$ 非空, 则任取

$$\alpha \in E \setminus E_0,$$

都有 α 为 E_0 上的超越元.

证明. 我们使用反证法. 设 $\alpha \in E \setminus E_0$ 为 E_0 上的代数元, 则有扩张 $E_0(\alpha)/E_0$ 为代数扩张, 由于 E_0/F 为代数扩张, 由代数扩张的传递性, 我们有

$$E_0(\alpha)/F,$$

为代数扩张. 因此 α 为 F 上的代数元, 这与 E_0 的定义矛盾. 因此 α 为 E_0 上的超越元. $\square$

与代数扩张类似的, 我们可以定义纯超越扩张.

定义 27.2.21

我们称一个 F 的扩张为**纯超越扩张**, 若所有 $E \setminus F$ 中的元素为 F 上的超越元.

例 27.2.22.

单超越扩张 $\mathbb{Q}(\pi)/\mathbb{Q}$ 为一个纯超越扩张.

27.3 分裂域

27.3.1 定义

由定义, 我们注意到代数元与域上多项式的根有着密切的关系. 我们考虑域 F 的代数扩张 E , 则 E 中每个元素都是 F 上的某个多项式的根. 反过来我们可以问, 是否 F 上的任取一个多项式 $f(x)$, 是否都在 E 中有根? 如果不能, 我们是否可以找到一个 F 的扩张 E 使得 $f(x)$ 在 E 中有根?

下边的命题给出了以上问题的一个肯定的回答.

命题 27.3.1 (教材引理 4.4.2 (Kronecker 构造))

设 F 为一个域, 任取 $f(x) \in F[x]$, 满足 $\deg f(x) > 0$, 则存在一个 F 的扩张 E , 使得 $f(x)$ 在 E 中有根.

证明. 这个域我们实际上已经遇到过了. 任给一个多项式 $f(x) \in F[x]$, 由于 $F[x]$ 是 PID, 我们可以将 $f(x)$ 写为 $F[x]$ 中不可约多项式的乘积:

$$f(x) = a f_1(x) \cdots f_n(x).$$

设 E/F 为一个域扩张, 记 $\alpha \in E$. 注意到

$$f(\alpha) = 0,$$

当且仅当存在 $1 \leq i \leq n$, 满足

$$f_i(\alpha) = 0.$$

因此, 我们只需要讨论 $f(x)$ 不可约的情形即可.

设 $f(x) \in F[x]$ 不可约, 由于 $F[x]$ 是 PID, 因此 $f(x)$ 生成的理想 $\langle f(x) \rangle$ 为极大理想, 我们有商环

$$E = F[x]/\langle f(x) \rangle,$$

为一个域. 我们将证明 $f(x)$ 在 E 中有根. 为了简化记号, 任取 $g(x) \in F[x]$, 我们记

$$\overline{g(x)} = g(x) + \langle f(x) \rangle.$$

我们考虑 E 中元素 $\bar{x}$. 任取 $n \in \mathbb{N}^*$, 我们有

$$\bar{x}^n = \overline{x^n}.$$

若我们记

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m,$$

则

$$\begin{aligned} f(\bar{x}) &= \overline{a_0} + \overline{a_1} \bar{x} + \cdots + \overline{a_m} \bar{x}^m \\ &= \overline{f(x)} \\ &= \bar{0} \in E \end{aligned}$$

因此 $f(x)$ 在 E 中有根 $\bar{x}$. □

下边一个是我们将会经常用到的引理.

引理 27.3.2

记 E 为 F 的一个扩张, $f(x) \in F[x]$ 为一个非零多项式. 若 $f(x)$ 在 E 中有根 α , 则我们在 $E[x]$ 中有如下因式分解:

$$f(x) = (x - \alpha)f_1(x).$$

证明. 若 $f(x)$ 在 E 上有根 α , 我们考虑 $x = x - \alpha + \alpha$. 则

$$\begin{aligned} f(x) &= f(x - \alpha + \alpha) \\ &= b_0 + b_1(x - \alpha) + \cdots + b_m(x - \alpha)^m. \end{aligned}$$

这里 $b_0, \dots, b_m \in E$.

由 $f(\alpha) = 0$, 我们有 $b_0 = 0$, 因此

$$\begin{aligned} f(x) &= (x - \alpha)(b_1 + \cdots + b_m(x - \alpha)^{m-1}) \\ &= (x - \alpha)f_1(x) \end{aligned}$$

这里 $f_1(x) \in E[x]$. □

由以上讨论, 我们得到如下定理

定理 27.3.3 (定理 4.4.4)

任给域 F 上的一个多项式 $f(x) \in F[x]$, 满足 $\deg f(x) = n > 0$, 则存在 F 的一个代数扩张 E , 满足 $\alpha_1, \dots, \alpha_n \in E$ 以及 $a \in F^*$, 满足

$$f = a(x - \alpha_1) \cdots (x - \alpha_n).$$

(即在 $E[x]$ 中可以分解为 1 次多项式的乘积.)

注 27.3.4.

这个定理的结论等价于存在代数扩张 E/F , 使得 $f(x)$ 在 E 上有 $\deg f(x)$ 个根 (计算重数).

证明. 我们对 f 的次数使用归纳法.

考虑 1 次多项式, 任给域 F , 我们取 $E = F$ 即满足要求.

假设以上结论对 $n \in \mathbb{N}^*$ 次多项式成立, 我们考虑多项式次数为 $n + 1$ 的情况. 任给 F 上的 $n + 1$ 次多项式 $f(x)$, 由命题 27.3.1, 我们可以找到域 K 使得 $f(x)$ 在 K 上有根 α_1 . 由引理 27.3.2, 我们可以将 $f(x)$ 写为

$$f(x) = (x - \alpha_1)f_1(x).$$

这里 $f_1(x) \in K[x]$ 且为 n 次多项式.

由归纳法假设, 定理结论对域 K 上的 n 次多项式成立, 因此我们可以找到一个 K 的代数扩张 E , 满足

$$f_1(x) = a(x - \alpha_2) \cdots (x - \alpha_{n+1}).$$

我们注意到 K/F 为代数扩张, E/K 为代数扩张, 因此 E/F 为代数扩张, 且在 $E[x]$ 中有

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{n+1}).$$

因此以上结论对 $n + 1$ 次多项式也成立. 由此定理得证. □

定义 27.3.5

任给域 F 非零多项式 $f(x) \in F[x]$, 设 $\deg f(x) = n > 0$. 我们称 $f(x)$ 在 F 的一个扩张 E 上**分裂**, 若在 $E[x]$ 中, 我们有

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n).$$

这里 $a \in F^*$, $\alpha_1, \dots, \alpha_n \in E$.

若我们进一步有 $E = F(\alpha_1, \dots, \alpha_n)$, 则称 E 为 $f(x) \in F[x]$ 的**分裂域**. 此时我们也称 E/F 为 $f(x) \in F[x]$ 的**分裂域扩张**.

例 27.3.6.

我们考虑一个特殊情况. 当 $f(x) \in F[x]$ 的次数为 1 的时候, 其分裂域为 F .

记 E/F 为一个域扩张, 且 $f(x) \in F[x] \setminus F$ 在 E 上分裂, 则在计算重数的情形下, $f(x)$ 在 E 中有 $\deg f(x)$ 个根. 如上记

$$\alpha_1, \dots, \alpha_n \in E,$$

为 $f(x)$ 的根, 则 $f(x)$ 的分裂域 $F(\alpha_1, \dots, \alpha_n)$ 是 E 使得 $f(x)$ 分裂的最小的 F 的扩张. 这个结论主要来自于以下引理:

引理 27.3.7

沿用以上记号, 考虑 E/F 的中间域 K (即 $E/K/F$), 满足 $f(x)$ 在 K 上分裂, 则有

$$\{\alpha_1, \dots, \alpha_n\} \subset K.$$

证明. 由条件 $f(x)$ 在 K 中分裂, 我们有 $\beta_1, \dots, \beta_n \in K$, 满足

$$f(x) = a(x - \beta_1) \cdots (x - \beta_n).$$

因此我们在 $E[x]$ 中有

$$a(x - \alpha_1) \cdots (x - \alpha_n) = f(x) = a(x - \beta_1) \cdots (x - \beta_n).$$

注意到域上的 1 次多项式都是不可约多项式, 因此以上给出了 $f(x)$ 在 $E[x]$ 中两个不可约分解. 由于 $E[x]$ 为 PID, 因此也是 UFD, 由 UFD 的定义, 在相差一个置换的前提下, 对任意 $1 \leq i \leq n$, 有

$$(x - \alpha_i) \sim (x - \beta_i)$$

注意到二者都是首一多项式, 因此我们有 $\alpha_i = \beta_i$. 因此我们有

$$\{\alpha_1, \dots, \alpha_n\} \subset K.$$

□

推论 27.3.8

记 E/F 为一个域扩张, 设多项式 $f(x) \in F[x] \setminus F$ 在 E 上分裂, 记 $\alpha_1, \dots, \alpha_n$ 为 $f(x)$ 在 E 中所有的根, 则有

$$F(\alpha_1, \dots, \alpha_n) = \bigcap \{K \subset E \mid K \text{ 为 } E/F \text{ 的中间域且 } f(x) \text{ 在 } K \text{ 上分裂}\}.$$

注 27.3.9.

若记 $f(x) = af_1(x)$, 则有 $f_1(x)$ 也是 F 上的与 $f(x)$ 次数相同的多项式, 且在 E 中与 $f(x)$ 有相同的根(每个根重数也相同), 域 E 也是 $f_1(x)$ 的分裂域. 因此我们通常可以考虑首一多项式.

注 27.3.10.

我们目前还没有证明分裂域的唯一性. 我们将在下节讨论完分裂域之间的同态之后证明分裂域在同构意义下是唯一的.

命题 27.3.11

若 E 为 F 上次数为 n 的多项式的分裂域, 则 E 为 F 的代数扩张, 且满足

$$[E : F] \leq n!.$$

证明. E 可以由 F 使用至多 n 次 Kronecker 构造得到. 注意到第 i -次的 Kronecker 构造使用的不可约多项式至多 $n - i + 1$ 次, 因此每次扩张的次数至多为 $n - i + 1$, 利用定理 26.3.5, 我们得到结论. $\square$

27.3.2 分裂域之间的同态

设 F 和 F' 为两个域. 我们假设存在域同构

$$\iota : F \rightarrow F'.$$

该同构诱导了两个域的多项式环的同构, 我们仍记做

$$\begin{aligned} \iota : F[x] &\rightarrow F'[x], \\ f(x) &\mapsto \iota(f)(x), \end{aligned}$$

其中若

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x],$$

则

$$\iota(f)(x) = \iota(a_0) + \iota(a_1)x + \cdots + \iota(a_n)x^n \in F'[x].$$

引理 27.3.12 (教材引理 4.4.10)

设 $f(x) \in F[x]$. 我们有 $f(x)$ 不可约当且仅当 $\iota(f)(x) \in F'[x]$ 不可约.

证明. 设存在 $g(x), h(x) \in F'[x]$, 满足

$$\iota(f)(x) = g(x)h(x),$$

我们考虑环同构

$$\iota^{-1} : F'[x] \rightarrow F[x],$$

则有

$$f(x) = \iota^{-1}(g)(x)\iota^{-1}(h)(x).$$

若 $f(x) \in F[x]$ 不可约, 则有

$$\iota^{-1}(g)(x) \in F^* \text{ 或者 } \iota^{-1}(h)(x) \in F^*,$$

这等价于

$$g(x) \in (F')^* \text{ 或者 } h(x) \in (F')^*,$$

因此 $\iota(f)(x) \in F'[x]$ 不可约.

将 F 与 F' 的位置互换, ι 和 ι^{-1} 的位置互换, 同样的证明给我们另一个方向的结论. $\square$

我们首先考虑域上的单代数扩张的情形. 仍考虑域同构

$$\iota: F \rightarrow F'.$$

定理 27.3.13

考虑 F 上的单代数扩张 $F(\alpha)$ 和 F' 的一个扩张 K . 记 f_α 为 α 的最小多项式. 则以下两个叙述等价.

(i) 存在一个域同态:

$$\tilde{\iota}: F(\alpha) \rightarrow K,$$

满足 $\tilde{\iota}|_F = \iota$;

(ii) 存在 $\beta \in K$, 满足 $\iota(f_\alpha)(\beta) = 0$.

注 27.3.14.

我们记 $j: F \rightarrow F(\alpha)$ 为嵌入映射, 即任取 $a \in F$, 有

$$j(a) = a \in F(\alpha),$$

则以上定理给出了 "存在一个映射

$$\tilde{\iota}: F(\alpha) \rightarrow K,$$

使得以下交换图存在" 的一个充要条件:

$$\begin{array}{ccc} F & \xrightarrow{\iota} & K \\ j \downarrow & \nearrow \exists \tilde{\iota} & \\ F(\alpha) & & \end{array}$$

证明. 我们记 α 在 F 上的最小多项式为

$$f_\alpha(x) = a_0 + \cdots + a_s x^s \in F[x].$$

充分性: 若存在 $\tilde{\iota}$, 令

$$\beta = \tilde{\iota}(\alpha) \in K,$$

则我们有

$$\begin{aligned} 0 &= \tilde{\iota}(f_\alpha(\alpha)) \\ &= \tilde{\iota}(a_0 + a_1 \alpha + \cdots + a_s \alpha^s) \\ &= \tilde{\iota}(a_0) + \tilde{\iota}(a_1) \tilde{\iota}(\alpha) + \cdots + \tilde{\iota}(a_s) (\tilde{\iota}(\alpha))^s \\ &= \iota(a_0) + \iota(a_1) \beta + \cdots + \iota(a_s) \beta^s \\ &= \iota(f_\alpha)(\beta). \end{aligned}$$

必要性: 假设存在 $\beta \in K$, 满足 $\iota(f_\alpha)(\beta) = 0$.

1, $\iota(f_\alpha)$ 不可约

由于 ι 是 $F[x]$ 和 $F'[x]$ 之间的同构, 因此 $h(x) \in F[x]$ 为不可约当且仅当 $\iota(h)(x) \in F'[x]$ 不可约. 我们有 $\iota(f_\alpha)(x)$ 不可约. 因此 $\iota(f_\alpha)(x)$ 是 β 的最小多项式.

2, $\tilde{\iota}$ 的存在性

由推论 27.1.11, 我们有 $F[x]/\langle f_\alpha(x) \rangle$ 和 $F'[x]/\langle \iota(f_\alpha)(x) \rangle$ 都为域. 考虑同态

$$\pi' \circ \iota : F[x] \rightarrow F'[x] \rightarrow F'[x]/\langle \iota(f_\alpha)(x) \rangle,$$

其中

$$\pi' : F'[x] \rightarrow F'[x]/\langle \iota(f_\alpha)(x) \rangle,$$

为自然同态.

任取 $g(x) \in F[x]$, 满足 $(\pi' \circ \iota)(g(x)) = \bar{0}$, 则有

$$\iota(f_\alpha)(x) \mid \iota(g)(x),$$

即存在 $q(x) \in F'[x]$, 满足

$$\iota(g)(x) = \iota(f_\alpha)(x)q(x),$$

因此

$$g(x) = f_\alpha(x)\iota^{-1}(q)(x),$$

由此可得

$$f_\alpha(x) \mid g(x).$$

所以我们有

$$\ker(\pi' \circ \iota) \subset \langle f_\alpha(x) \rangle.$$

反之任取

$$g(x) \in \langle f_\alpha(x) \rangle,$$

存在 $h(x) \in F[x]$, 满足

$$g(x) = f_\alpha(x)h(x),$$

因此

$$\pi'(\iota(g)(x)) = \pi'(\iota(f_\alpha)(x)\iota(h)(x)) = \pi'(\iota(f_\alpha)(x))\pi'(\iota(h)(x)) = \bar{0} \in F'[x]/\langle \iota(f_\alpha)(x) \rangle.$$

由此可知

$$\ker(\pi' \circ \iota) \supset \langle f_\alpha(x) \rangle.$$

综上所述

$$\ker(\pi' \circ \iota) = \langle f_\alpha(x) \rangle.$$

由于 $\pi' \circ \iota$ 是一个满同态, 由环同态定理, 我们有环同构 $\tilde{\iota}$, 满足如下交换图:

$$\begin{array}{ccc} F[x] & \xrightarrow{\iota} & F'[x] \\ \pi \downarrow & & \downarrow \pi' \\ F[x]/\langle f_\alpha(x) \rangle & \xrightarrow{\exists! \tilde{\iota}} & F'[x]/\langle \iota(f_\alpha)(x) \rangle \end{array}$$

注意到 $\tilde{\iota}$ 不是零映射, 因此 $\tilde{\iota}$ 是一个域同构.

因此我们有如下关系:

$$\begin{array}{ccccc} F[x] & \xrightarrow{\quad \iota \quad} & F'[x] & & \\ \pi \downarrow & & \downarrow \pi' & & \\ \tilde{\iota} : F(\alpha) & \xrightarrow{\quad \phi \quad} & F[x]/\langle f_\alpha(x) \rangle & \xrightarrow{\quad \exists! \tilde{\iota} \quad} & F'[x]/\langle \iota(f_\alpha)(x) \rangle \xrightarrow{\quad \psi \quad} F'(\beta) \subset K \end{array}$$

其中我们有 $\phi|_F = \text{id}_F$, 且 $\phi(\alpha) = \bar{x}$, 以及 $\psi|_{F'} = \text{id}_{F'}$, 且 $\psi(\bar{x}) = \beta$. 注意到 $\tilde{\iota}|_F = \iota$, 因此 $\tilde{\iota}|_F = \iota$ 满足要求. $\square$

注 27.3.15.

记 E/F 为一个域扩张, 记 K 为一个域, 设存在域同态,

$$\iota : F \rightarrow K,$$

以及域同态

$$\tilde{\iota} : E \rightarrow K,$$

满足 $\tilde{\iota}|_F = \iota$, 我们称 $\tilde{\iota}$ 为 ι 在 E 上的开拓.

以上证明实际上不依赖于 $\iota(f_\alpha)(x)$ 在 K 中的根的选取, 也即若 $\iota(f_\alpha)(x)$ 在 K 中有根, 则对任意 $\beta \in K$ 为 $\iota(f_\alpha)(x)$ 的根, 都有 ι 在 $F(\alpha)$ 上的开拓

$$\tilde{\iota} : F(\alpha) \rightarrow K,$$

满足

$$\tilde{\iota}(\alpha) = \beta.$$

这是因为, 任给 $\iota(f_\alpha)(x)$ 的根 $\beta \in K$, 我们都有

$$F'[x]/\langle \iota(f_\alpha)(x) \rangle \cong F'(\beta) \subset K.$$

另一方面, 注意到 $F(\alpha)$ 为 $F \cup \alpha$ 生成的域, 且 $\tilde{\iota}|_F = \iota$, 因此 $\tilde{\iota}$ 被 $\tilde{\iota}(\alpha)$ 决定, 即若存在两个 ι 在 $F(\alpha)$ 上的开拓 $\tilde{\iota}_1$ 和 $\tilde{\iota}_2$, 则 $\tilde{\iota}_1 = \tilde{\iota}_2$ 当且仅当 $\tilde{\iota}_1(\alpha) = \tilde{\iota}_2(\alpha)$. 由此, 我们得到以下推论.

推论 27.3.16

任给 F 的一个单代数扩张 $F(\alpha)$, 并记 $f_\alpha(x) \in F[x]$ 为 α 的最小多项式. 设 K 为 F' 的一个扩张. 记 $r \in \mathbb{N}$, 则以下两个叙述等价

1. $\iota(f_\alpha)(x) \in F'[x]$ 在 K 中有 r 个不同的根;
2. 存在 r 个不同的域同态

$$\tilde{\iota} : F(\alpha) \rightarrow K,$$

满足 $\tilde{\iota}|_F = \iota$.

利用以上关于 F 的单代数扩张的结论, 我们可以得到如下几个关于分裂域的结论. 仍考虑域同构

$$\iota : F \rightarrow F'.$$

定理 27.3.17

记 F 的扩张 E 为 $f(x) \in F[x] \setminus F$ 的分裂域. 另记 K/F' 为一个域扩张. 以下两个叙述等价:

1. 存在一个域同态

$$\tilde{\iota} : E \rightarrow K,$$

满足 $\tilde{\iota}|_F = \iota$;

2. $\iota(f)(x) \in F'[x]$ 在 K 中分裂.

证明. 设 $\deg f = n \in \mathbb{N}^*$, 由定义存在 $\alpha_1, \dots, \alpha_n \in E$, 满足

$$f = (x - \alpha_1) \cdots (x - \alpha_n),$$

以及

$$E = F(\alpha_1, \dots, \alpha_n).$$

充分性: 假设存在一个同态

$$\tilde{\iota} : E \rightarrow K,$$

满足 $\tilde{\iota}|_F = \iota$.

对任意 $1 \leq i \leq n$, 我们记 $\beta_i = \tilde{\iota}(\alpha_i)$. 由于 $f(x) \in F[x]$, 我们有

$$\begin{aligned} \iota(f)(x) &= \tilde{\iota}(f)(x) \\ &= \tilde{\iota}((x - \alpha_1) \cdots (x - \alpha_n)) \\ &= (x - \beta_1) \cdots (x - \beta_n) \in K[x]. \end{aligned}$$

因此 $\iota(f)(x)$ 在 K 中分裂.

必要性: 我们对 $f(x)$ 的次数归纳. 若 $\deg f(x) = 1$, 则 $E = F$. 因此 ι 即满足要求.

现在假设定理对 $n-1$ 次多项式成立, 设 $f(x) \in F[x]$ 为一个 n 次多项式. 我们考虑 α_1 在 F 上的最小多项式 $g(x)$. 因此 $f(x) = g(x)h(x)$.

由于 $\iota(f)(x)$ 在 K 上分裂, $\iota(g)(x)$ 也在 K 上分裂. 设 $\beta_1 \in K$ 为 $\iota(g)(x)$ 的一个根, 我们有域同态:

$$\iota_1 : F(\alpha_1) \rightarrow K.$$

满足 $\iota_1(\alpha_1) = \beta_1$, 且 $\iota_1|_F = \iota$.

在 $F(\alpha_1)[x]$ 中, 我们有

$$f(x) = (x - \alpha_1)f_1(x),$$

注意到在 $E[x]$ 中有

$$f_1(x) = (x - \alpha_2) \cdots (x - \alpha_n),$$

因此

$$E = F(\alpha_1)(\alpha_2, \dots, \alpha_n),$$

为 $f_1(x) \in F(\alpha_1)[x]$ 的分裂域.

令 $F_1 = F(\alpha_1)$, $F'_1 = F'(\beta_1)$. 由于 $F_1 \cong F'_1$, 且

$$\deg f_1(x) \leq n - 1,$$

因此我们可以对 E/F_1 , K/F'_1 和 $f_1(x)$ 使用归纳假设, 可得一个域同态

$$\tilde{\iota} : E \rightarrow K,$$

满足 $\tilde{\iota}|_{F(\alpha_1)} = \iota_1$. 因此

$$\tilde{\iota}|_F = \iota_1|_F = \iota.$$

□

注 27.3.18.

实际上从 ι 开拓到 $\tilde{\iota}$ 的过程可以看作是多次使用定理 27.3.13 的结果. 我们可以考虑如下交换图:

$$\begin{array}{ccc}
 F & \xrightarrow{\iota} & K \\
 j_0 \downarrow & \nearrow \iota_1 & \\
 F(\alpha_1) & \nearrow \iota_2 & \\
 j_1 \downarrow & & \\
 F(\alpha_1)(\alpha_2) & \nearrow \iota_n = \tilde{\iota} & \\
 j_2 \downarrow & & \\
 \vdots & & \\
 j_{n-1} \downarrow & & \\
 F(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) & &
 \end{array}$$

这里映射 $j_0, \dots, j_{n-1}$ 都是嵌入同态. 在归纳的过程中, 我们依次得到了同态

$$\iota_1, \dots, \iota_{n-1}, \iota_n = \tilde{\iota}.$$

我们现在开始证明分裂域在同构意义下的唯一性. 设 F 为一个域, $f(x) \in F[x]$ 为一个次数为 $n \in \mathbb{N}^*$ 的多项式. 设 E/F 和 E'/F 均为 $f(x)$ 的分裂域扩张.

推论 27.3.19

存在域同构 $\tilde{\iota}: E \rightarrow E'$, 满足 $\tilde{\iota}|_F = \text{id}_F$.

证明. 由于 E 和 E' 都是 $f(x) \in F[x]$ 的分裂域, 我们记 $f(x)$ 在 E 和 E' 中的根分别为

$$\alpha_1, \dots, \alpha_n \text{ 以及 } \beta_1, \dots, \beta_n.$$

由分裂域的定义, 我们有

$$E = F(\alpha_1, \dots, \alpha_n) \text{ 和 } E' = F(\beta_1, \dots, \beta_n).$$

考虑 $F' = F$, $\iota = \text{id}$, $K = E'$, 则由以上定理我们知道, 我们可以找到域同态:

$$\tilde{\iota}: E \rightarrow E',$$

满足 $\tilde{\iota}|_F = \text{id}_F$.

下边证明 $\tilde{\iota}$ 为域同构. 由于域同态总是单射, 我们只需要证明 $\tilde{\iota}$ 是满射. 我们考虑如下计算:

$$\begin{aligned}
 f(x) &= \tilde{\iota}(f) \\
 &= \tilde{\iota}((x - \alpha_1) \cdots (x - \alpha_n)) \\
 &= (x - \tilde{\iota}(\alpha_1)) \cdots (x - \tilde{\iota}(\alpha_n)) \in E'[x]
 \end{aligned}$$

另一方面, 我们知道在 $E'[x]$ 中我们有

$$f(x) = (x - \beta_1) \cdots (x - \beta_n).$$

由 $E'[x]$ 为 UFD, 以上我们得到了两个 $f(x)$ 的不可约分解, 在相差一个根的重排下, 对任意 $1 \leq i \leq n$, 我们有

$$x - \tilde{\iota}(\alpha_i) = x - \beta_i,$$

进而可得

$$\tilde{\iota}(\alpha_i) = \beta_i.$$

由于 $\beta_1, \dots, \beta_n$ 在 F 上生成 E' , 我们有

$$E' \subset \text{Im}(\tilde{\iota}).$$

因此 $\tilde{\iota}$ 是域同构. □

例 27.3.20.

我们考虑 $F = \mathbb{Q}$, 记 $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. 我们知道 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 为 $f(x)$ 的分裂域扩张. 注意到存在一个域同构:

$$\iota_1 : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2}),$$

满足 $\iota_1|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$, 且 $\iota_1(\sqrt{2}) = \sqrt{2}$.

另一方面, 我们也可以有另一个域同构:

$$\iota_2 : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2}),$$

满足 $\iota_2|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$, 且 $\iota_2(\sqrt{2}) = -\sqrt{2}$.

考虑以上的例子, 我们自然就是有了一个问题. 如果 E/F 和 E'/F 都是多项式 $f(x) \in F[x] \setminus F$ 的分裂域, 存在多少个域同构

$$\iota : E \rightarrow E',$$

满足 $\iota|_F = \text{id}_F$? 我们选定一个域同构

$$\iota_0 : E \rightarrow E',$$

则任取 E 到 E' 的域同构 ι , 考虑符合, 我们总有

$$\iota_0 \circ \iota = \sigma \in \text{Aut}(E),$$

满足 $\sigma|_F = \text{id}_F$.

另一方面, 任给 E 的自同构 σ , 我们可以通过 $\iota_0^{-1} \circ \sigma$ 得到 E 到 E' 的域同构. 但是这里有一个问题就是 σ 不一定满足 $\sigma|_F = \text{id}_F$. 我们记

$$\text{Aut}_F(E) = \{\sigma \in \text{Aut}(E) \mid \sigma|_F = \text{id}_F\}.$$

因此, 我们有

$$\#\{\iota : E \rightarrow E', \iota|_F = \text{id}_F\} = \#\text{Aut}_F(E).$$

设 $\deg f(x) = n$. 我们记 $f(x)$ 在 E 中的根为 $\alpha_1, \dots, \alpha_n$, 任取 $\iota \in \text{Aut}_F(E)$, 注意到 ι 若将由 $\iota(\alpha_1), \dots, \iota(\alpha_n)$ 决定. 另一方面, 由之前分裂域同构意义下唯一的证明, 存在 $\sigma \in S_n$, 满足对任意 $1 \leq i \leq n$, 有

$$\iota(\alpha_i) = \alpha_{\sigma(i)}.$$

因此, 我们有一个上限

$$\#\text{Aut}_F(E) \leq n!.$$

实际上, 我们还可以如下进行更精细的估计. 设 $f(x) \in F[x]$ 的不可约分解如下:

$$f(x) = p_1(x)^{m_1} \cdots p_k(x)^{m_k},$$

其中 $p_1(x), \dots, p_k(x)$ 都是 F 上首一不可约多项式且两两不同.

考虑 $\alpha_1 \in E$, 由之前的讨论, 我们知道存在 $p_i(x)$, 满足

$$p_i(\alpha_1) = 0.$$

不妨设 $i = 1$. 由此, 我们有

$$p_1(\iota(\alpha_1)) = \iota(p_1(\alpha_1)) = 0.$$

因此对任意 $1 \leq i \leq n$, 存在域同构 ι , 元素 α_i , 满足

$$\iota(\alpha_1) = \alpha_i,$$

的一个必要条件为

$$p_1(\alpha_i) = 0.$$

反过来, 若 α_i 满足 $p_1(\alpha_i) = 0$, 我们域同构 ϕ :

$$F(\alpha_1) \cong F(\alpha_i).$$

注意到在 $F(\alpha_1)[x]$ 中, 我们有分解

$$f(x) = (x - \alpha_1)f_1(x).$$

对 E, E' , 以及多项式 $f_1(x) \in F(\alpha_1)[x]$ 使用定理, 我们可以将 ϕ 开拓到 E 上, 并且可以进一步验证所得的域同态是一个同构, 记为 ι . 注意到 $\iota|_{F(\alpha_1)} = \phi$, 因此

$$\iota(\alpha_1) = \alpha_i.$$

利用这个观察我们可以证明以下定理.

定理 27.3.21

记 E/F 是 $f(x) \in F[x] \setminus F$ 的分裂域扩张. 我们有如下结论:

$$\#\text{Aut}_F(E) \leq [E : F],$$

且等号成立当且仅当 $f(x)$ 所有的不可约因子都没有重根.

证明. 我们使用归纳法, 对 $f(x)$ 的次数进行归纳. 记 $\deg f(x) = n \in \mathbb{N}^*$.

若 $n = 1$, 则 $E = F$, 因此

$$\#\text{Aut}_F(F) = 1 = [F : F].$$

注意到 $f(x)$ 不可约且没有重根. 因此结论成立.

下边假设 $n > 1$, 并假设结论对 $\deg f(x) \leq n - 1$ 时都成立. 下边假设 $\deg f(x) = n$. 我们考虑以下集合分解

$$\begin{aligned} & \text{Aut}_F(E) \\ &= \bigcup_{\{\alpha_i | p_1(\alpha_i)=0\}} \{\iota \in \text{Aut}_F(E) \mid \iota(\alpha_1) = \alpha_i\}, \end{aligned}$$

考虑 α_1 的像, 我们知道以上集合是一个不交并. 因此我们有

$$\begin{aligned} & \# \text{Aut}_F(E) \\ &= \sum_{\{\alpha_i | p_1(\alpha_i)=0\}} \#\{\iota \in \text{Aut}_F(E) \mid \iota(\alpha_1) = \alpha_i\}. \end{aligned}$$

由之前的讨论, 我们知道对任意 $p_1(x)$ 的在 E 中的根 α 和 α' , 存在一个域同构

$$\iota : E \rightarrow E,$$

满足 $\iota(\alpha) = \alpha'$, 且 $\iota|_F = \text{id}_F$.

因此对任意 $f(x)$ 在 E 中的 α_i 满足 $p_1(\alpha_i) = 0$, 记 $\iota_0 \in \text{Aut}_F(E)$, 满足

$$\iota_0(\alpha_1) = \alpha_i,$$

我们有

$$\{\iota \in \text{Aut}_F(E) \mid \iota(\alpha_1) = \alpha_i\} = \iota_0 \circ \{\iota \in \text{Aut}_F(E) \mid \iota(\alpha_1) = \alpha_1\},$$

注意到由于 ι_0 为域同构, 因此 ι_0 给出集合

$$\{\iota \in \text{Aut}_F(E) \mid \iota_0(\alpha_1) = \alpha_i\},$$

以及

$$\{\iota \in \text{Aut}_F(E) \mid \iota_0(\alpha_1) = \alpha_1\},$$

之间的双射. 由此可得

$$\#\{\iota \in \text{Aut}_F(E) \mid \iota_0(\alpha_1) = \alpha_1\} = \#\{\iota \in \text{Aut}_F(E) \mid \iota_0(\alpha_1) = \alpha_i\}.$$

在 $F(\alpha_1)[x]$ 中考虑分解

$$f(x) = (x - \alpha_1)f_1(x),$$

则 $E/F(\alpha_1)$ 为 $f_1(x)$ 的分裂域扩张. 由于 $\deg f_1(x) = n - 1$, 由归纳假设, 我们有

$$\#\text{Aut}_{F(\alpha_1)}(E) \leq [E : F(\alpha_1)].$$

且等号成立当且仅当 $f_1(x) \in F(\alpha_1)[x]$ 的不可约因子没有重根.

另外注意到

$$\#\{\alpha_i | p_1(\alpha_i) = 0\} \leq \deg p_1(x) = [F(\alpha_1) : F],$$

且等号成立当且仅当 $p_1(x)$ 没有重根.

综上所述, 我们有以下估计

$$\#\text{Aut}_F(E) \leq [F(\alpha_1) : F][E : F(\alpha_1)] = [E : F],$$

且等号成立当且仅当 $f(x)$ 所有不可约因子没有重根.

最后一点详细地说, 若存在 $p_j(x)$ 有重根, 我们可以将 $f(x)$ 的不可约因子重新排列, 使得 $p_j(x)$ 为第一个, 重复以上操作知道不等号严格.

若任意 $p_j(x)$ 都没有重根, 注意到 $f_1(x)$ 在 $F(\alpha_1)[x]$ 中的不可约因子是 $p_1(x), \dots, p_k(x)$ 在 $F(\alpha_1)[x]$ 中的因子, 因此也没有重根. 因此两处不等号中的等号都成立.

综上所述, 定理结论对 $\deg f(x) = n$ 时成立. $\square$

27.3.3 例子

我们考虑 $F = \mathbb{Q}$. 考虑多项式 $f = (x^2 - 2)(x^2 - 3)$. 因此 f 的分裂域为 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

另一方面, 我们可以考虑 $\alpha = \sqrt{3} + \sqrt{2}$. 由代数元对加法封闭, 我们知道 α 也是 $\mathbb{Q}$ 上的代数元, 并且 $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. 我们可以计算 $\alpha^{-1} = \sqrt{3} - \sqrt{2}$. 因此我们同时也有

$$\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}), \quad \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

因此 $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. 我们可以验证 $\sqrt{2} + \sqrt{3}$ 的最小多项式为:

$$f_\alpha = x^4 - 10x^2 - 49.$$

令 $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, 任取 $\varphi \in \text{Aut}_{\mathbb{Q}}(E)$, φ 由 $\varphi(\sqrt{2})$ 和 $\varphi(\sqrt{3})$ 决定. 注意到 φ 固定 $\sqrt{2}$ 和 $\sqrt{3}$ 在 $\mathbb{Q}$ 上的最小多项式, 因此我们有

$$\varphi(\{\sqrt{2}, -\sqrt{2}\}) = \{\sqrt{2}, -\sqrt{2}\}, \quad \varphi(\{\sqrt{3}, -\sqrt{3}\}) = \{\sqrt{3}, -\sqrt{3}\}$$

我们考虑 $E/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, 注意到 $\text{id}_{\mathbb{Q}}$ 到 $\mathbb{Q}(\sqrt{2})$ 的开拓 φ_1 有两种, 分别对应 $\varphi_1(\sqrt{2}) = \sqrt{2}$ 和 $\varphi_1(\sqrt{2}) = -\sqrt{2}$. 由于 $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, 固定 φ_1 到 E 上的开拓 φ 有两种, 分别对应 $\varphi(\sqrt{3}) = \sqrt{3}$ 和 $\varphi(\sqrt{3}) = -\sqrt{3}$.

综上所述, 我们有

$$|\text{Aut}_{\mathbb{Q}}(E)| = 4 = [E : \mathbb{Q}].$$

27.4 尺规作图

本节中, 我们主要关心的是平面欧氏几何中尺规作图的问题. 具体规则为, 任意给定两点, 我们可以画出过这两点的直线, 以及以一个点为圆心, 两点之间距离为半径的圆. 我们希望知道在这个规则下, 经过有限次作画, 我们可以在平面上画出哪些几何图形. 比较出名的三个问题为:

- (i) 三等分角;
- (ii) 化圆为方: 求一个正方形, 其面积等于已知的圆盘的面积;
- (iii) 倍立方: 求做一个立方体使其体积为给定立方体的 2 倍.

在尺规作图中, 通常我们是从一些已知点出发, 构造新的点, 利用得到的点来做出图形.

我们考虑平面 $\mathbb{R}^2 \cong \mathbb{C}$. 任给 $\mathbb{C}$ 中不同的两点 w 和 z , 我们记 $\text{Line}(w, z) \subset \mathbb{C}$ 中过 w 和 z 的直线, $\text{Circle}(w, z) \subset \mathbb{C}$ 为以 w 为圆心, 过 z 的圆.

定义 27.4.1

任给一个 $\mathbb{C}$ 的至少包含两个点的子集 T , 我们称 z 可以由 T 中的点**尺规作出**, 若以下情况至少有一种成立

- (i) 存在 $w_1, w_2, z_1, z_2 \in T$, 满足 $w_i \neq z_i$, 且 $\{z'\} = \text{Line}(w_1, z_1) \cap \text{Line}(w_2, z_2)$;
- (ii) 存在 $w_1, w_2, z_1, z_2 \in T$, 满足 $w_i \neq z_i$, 且 $z' \in \text{Line}(w_1, z_1) \cap \text{Circle}(w_2, z_2)$;
- (iii) 存在 $w_1, w_2, z_1, z_2 \in T$, 满足 $w_i \neq z_i$, 且 $z' \in \text{Circle}(w_1, z_1) \cap \text{Circle}(w_2, z_2)$.

定义 27.4.2

我们称一个点 $z = a + b\sqrt{-1} \in \mathbb{C}$ 为**可构造数**, 若存在 $n \in \mathbb{N}^*$, 以及 $\mathbb{C}$ 中的一个子集 $\{\alpha_1, \dots, \alpha_n\}$, 满足

- (i) α_1 由 $\{0, 1\}$ 中的点尺规作出;
- (ii) 对任意 $2 \leq i \leq n$, α_i 由 $\{0, 1, \alpha_1, \dots, \alpha_{i-1}\}$ 中的点尺规作出.

且 $z = \alpha_n$. 我们约定 $0, 1$ 也为可构造数, 并用 K 记所有可构造数构成的 $\mathbb{C}$ 的子集.

尺规作图中的问题是否有解通常与所需的点是否是可构造有关. 我们下边先看一些可构造点的例子:

整数

我们首先观察 $\{0, 1\}$. 因此 $\{0, 1, 2, -1, \exp \pi i/3, \exp -\pi i/3\}$ 中的点都是可构造数.

有理数

取 $n \in \mathbb{N}^*$, 我们考虑 $\text{Circle}(n, n) \cap \text{Circle}(0, 1) = \{z_1, z_2\}$. 利用平面几何的知识, 我们有 $\text{Line}(z_1, z_2) \cap \text{Line}(0, 1) = \{1/2n\}$. 因此, 任意 $m/n \in \mathbb{Q}$ 都是可构造数.

一般情形**定理 27.4.3 (定理 4.3.1)**

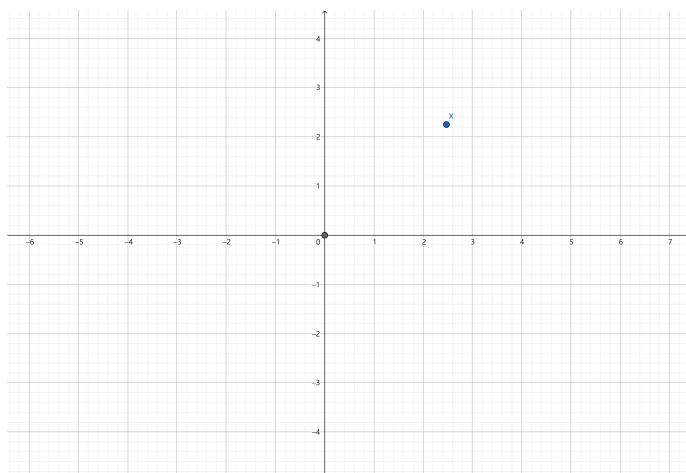
若 $w, z \in K$, 则 $w + z, -w, wz, \bar{w} \in K$.

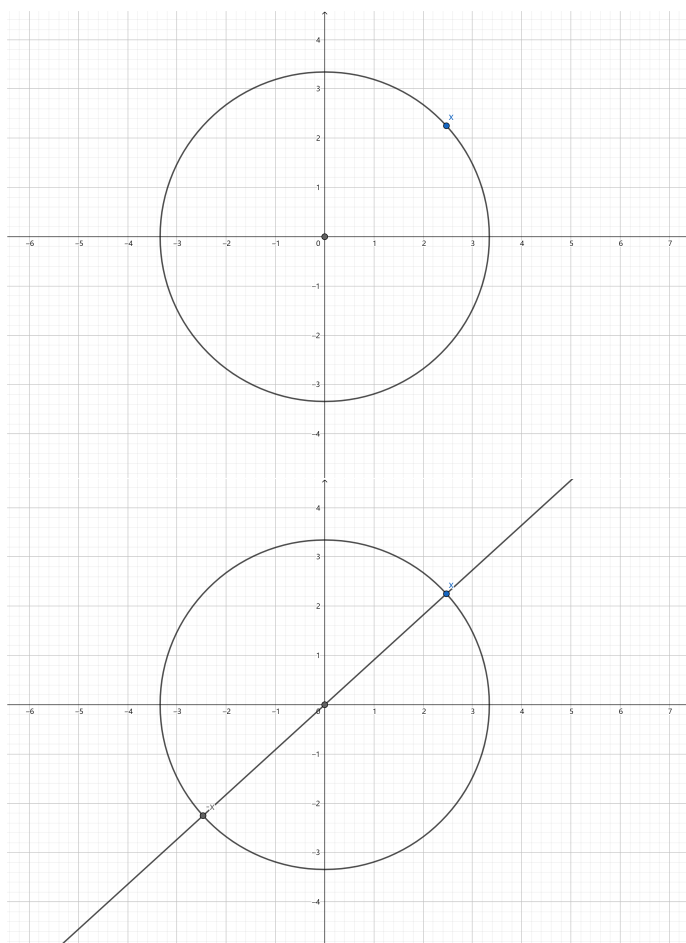
若 $w \neq 0$, 则 $w^{-1} \in K$.

若 $w^2 = z$ 且 $z \in K$, 则 $w \in K$.

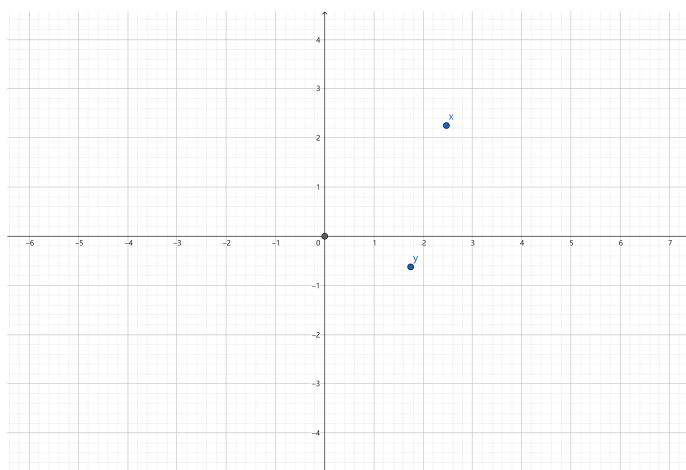
简要证明. 以下我们用图给出一般的构造办法:

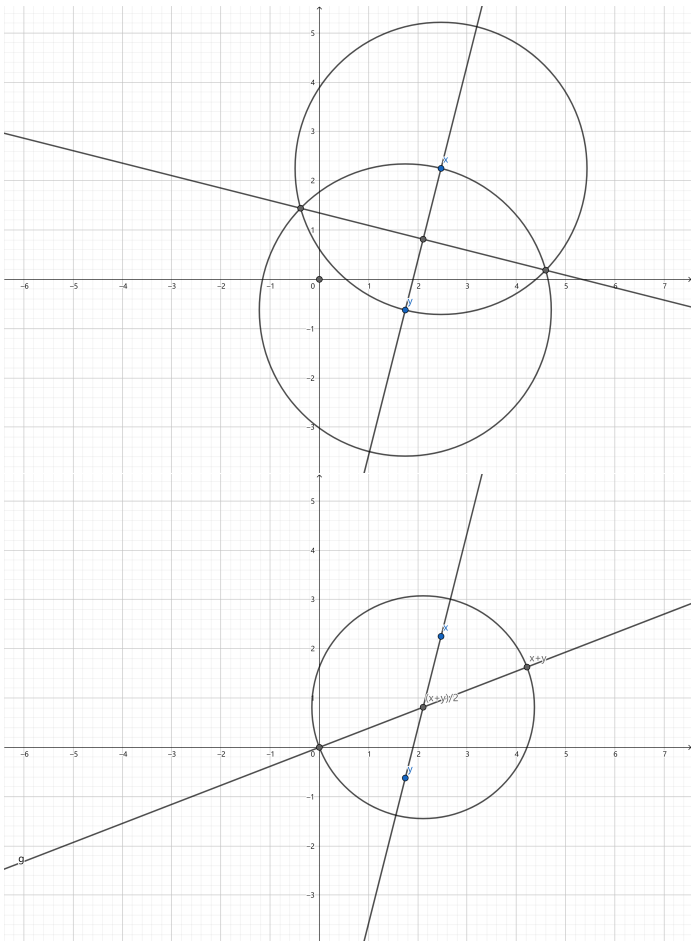
- (i) $-w$



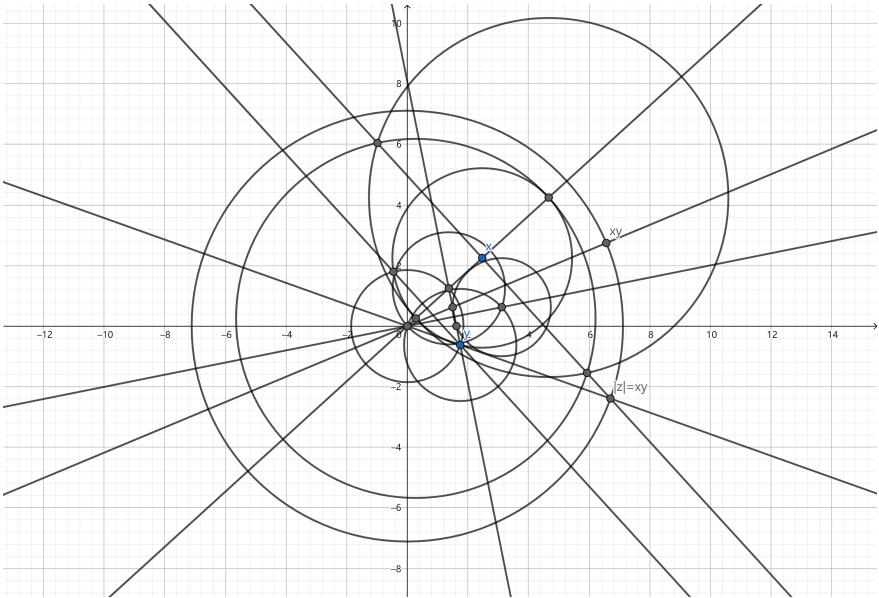


(ii) $w + z$

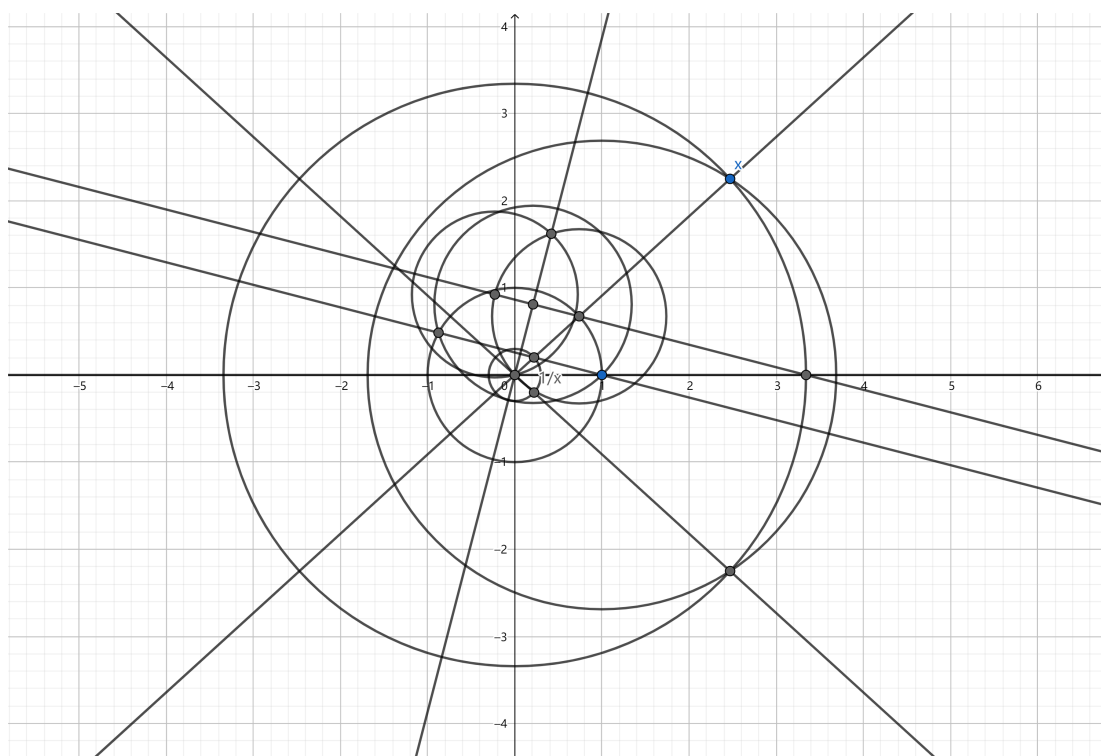




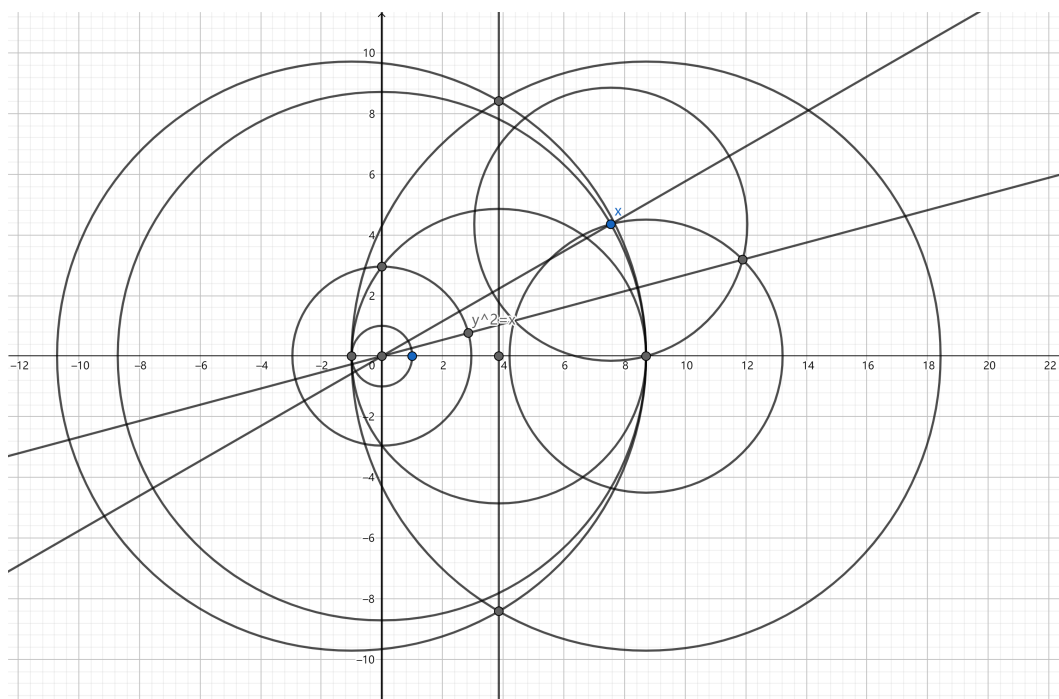
(iii) wz



(iv) w^{-1}



(v) w 满足 $w^2 = z$



□

推论 27.4.4

- (1) $\operatorname{Im} w, \operatorname{Re} w, |w| \in K$;
 (2) K 为一个域 $\mathbb{Q}$ 的扩张.

对任意 $i \in \mathbb{N}$, E_i 都是 $\mathbb{Q}$ 的扩张. 此外, 由 M_0 的对称性 E_i 在 $\mathbb{C}$ 的共轭作用下不变. 也即若 $z \in E_i$, 我们有 $\bar{z} \in K$, 继而有 $\operatorname{Im} z, \operatorname{Re} z, |z| \in K$.

注 27.4.5.

$\mathbb{C}$ 的子域并不都是在共轭作用下不变的. 例如, 我们考虑 $\omega \in \mathbb{C}$ 为 3 次单位根. 因此 $\omega \sqrt[3]{2}$ 为 $x^3 = 2$ 的一个根. 我们考虑 $\mathbb{Q}(\omega \sqrt[3]{2})$ 为 $\mathbb{Q}$ 的扩张, 不满足在共轭作用下不变的性质. (否则, $\mathbb{Q}(\omega \sqrt[3]{2}) = \mathbb{Q}(\omega, \sqrt[3]{2})$, 单前一个是 $\mathbb{Q}$ 的 3 次扩张, 后一个是 $\mathbb{Q}$ 的 6 次扩张, 矛盾.)

更强一点的概念还有全实域 totally real field, 也就是所有到 $\mathbb{C}$ 的同态的像都在 $\mathbb{R}$ 中的域. $\mathbb{Q}$ 为一个全实域. 一个不是全实域的例子就是 $\mathbb{Q}(\sqrt[3]{2})$, 它和 $\mathbb{Q}(\omega \sqrt[3]{2})$ 同构.

下边我们进一步用坐标来研究这些扩张的性质.

回顾: 平面上一条直线的方程为

$$xa + yb = c.$$

一个圆的方程为

$$(x - a)^2 + (y - b)^2 = r^2.$$

- (i) $z \in \operatorname{Line}(w_1, z_1) \cap \operatorname{Line}(w_2, z_2)$:

$$\begin{cases} xa_1 + yb_1 = c_1 \\ xa_2 + yb_2 = c_2 \end{cases}$$

因此若 $w_1, w_2, z_1, z_2 \in E$, 则 $z \in E$.

- (ii) $z \in \operatorname{Line}(w_1, z_1) \cap \operatorname{Circle}(w_2, z_2)$:

$$\begin{cases} xa_1 + yb_1 = c_1 \\ (x - a_2)^2 + (y - b_2)^2 = r^2 \end{cases}$$

因此若 $w_1, w_2, z_1, z_2 \in E$, 则 $[E(z) : E] \leq 2$.

- (iii) $z \in \operatorname{Circle}(w_1, z_1) \cap \operatorname{Circle}(w_2, z_2)$:

$$\begin{aligned} & \begin{cases} (x - a_1)^2 + (y - b_1)^2 = r_1^2 \\ (x - a_2)^2 + (y - b_2)^2 = r_2^2 \end{cases} \\ \rightarrow & \begin{cases} (a_2 - a_1)(2x - a_1 - a_2) + (b_2 - b_1)(2y - b_1 - b_2) = (r_1 - r_2)(r_1 + r_2) \\ (x - a_2)^2 + (y - b_2)^2 = r_2^2 \end{cases} \end{aligned}$$

因此若 $w_1, w_2, z_1, z_2 \in E$, 则 $[E(z) : E] \leq 2$.

由以上讨论, 我们可以得到如下定理

定理 27.4.6 (定理 4.3.2)

设 $\alpha \in \mathbb{C}$. α 为可构造数当且仅当存在 $r \in \mathbb{N}$ 以及一系列 $\mathbb{Q}$ 的扩张

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_r,$$

满足:

- (i) 若 $r > 0$, 对任意 $0 \leq i \leq r-1$, $[K_{i+1} : K_i] = 2$;
- (ii) $\alpha \in K_r$.

证明. 设 $\alpha \neq 0, 1$, 由可构造数的定义, 我们有 $\alpha_1, \dots, \alpha_n = \alpha$, 满足

$$\alpha \in \mathbb{Q}(\alpha_1, \dots, \alpha_n) = \mathbb{Q}(\alpha_1) \cdots (\alpha_n).$$

记 $F_i = \mathbb{Q}(\alpha_1, \dots, \alpha_i)$. 由此前关于方程组的解的讨论, 我们得出 $[F_{i+1} : F_i] \leq 2$ 对任意 $0 \leq i \leq n-1$ 成立. 因此将 F_i 中不同的域取出, 我们有

$$K_0 \subset \cdots \subset K_r,$$

满足 $[K_{i+1} : K_i] = 2$ 对任意 $0 \leq i \leq r-1$ 成立. 定理的必要性得证.

下证充分性. 任取 K_i 上的二次扩张 $K_i(\alpha)$, 则存在 K_i 上的一个二次多项式, 满足 α 为这个二次多项式的根. 由定理 3.4.1 可知, 二次根可以用尺规构造出, 因此 α 可从 K_i 利用尺规构造出. 因此若存在一系列域扩张, 满足定理条件, 则 α 可构造. $\square$

注 27.4.7.

进行 l 次 2 次扩张和进行一次 2^l 次扩张是不同的 (虽然扩张的总的次数相同).

以上构造过程也可以被推广到更一般的情况. 设 $s \in \mathbb{N}^*$, $z_1, \dots, z_s \in \mathbb{C}$. 我们记它们的复共轭为 $\bar{z}_1, \dots, \bar{z}_s$. 我们记所有可以通过尺规作图从

$$\{0, 1, z_1, \dots, z_s\}$$

得到的数构成的 $\mathbb{C}$ 的子集为 E .

定理 27.4.8 (定理 4.3.5)

记 $z \in \mathbb{C}$, 则 $z \in E$ 当且仅当存在 $t \in \mathbb{N}$ 以及一系列

$$F := \mathbb{Q}(z_1, \dots, z_s, \bar{z}_1, \dots, \bar{z}_s)$$

的扩张

$$F = F_0 \subset F_1 \subset \cdots \subset F_t,$$

满足:

- (i) 若 $t > 0$, 对任意 $0 \leq i \leq t-1$, $[F_{i+1} : F_i] = 2$;
- (ii) $\alpha \in F_t$.

例 27.4.9.

我们现在考虑尺规作图中的一些问题:

(i) 三等分角.

我们利用三倍角的公式:

$$\begin{aligned}\cos(3\theta) &= \cos(2\theta)\cos(\theta) - \sin(2\theta)\sin\theta \\ &= 2\cos^3\theta - \cos\theta - 2\sin^2\theta\cos\theta \\ &= 2\cos^3\theta - \cos\theta - 2(1 - \cos^2\theta)\cos\theta \\ &= 4\cos^3\theta - 3\cos\theta.\end{aligned}$$

三等分角, 可以被转化为已知 $\cos(3\theta)$ 求 $\cos\theta$. 以上我们可以将等式看作是 $\cos\theta$ 的方程, 因此是 3 次方程. 我们假设 $\cos(3\theta) \in \mathbb{Q}$, 因此多项式

$$4x^3 - 3x - \cos(3\theta) \in \mathbb{Q}[x].$$

若其不可约, 那么 $\cos\theta$ 就是 $[\mathbb{Q}(\cos(\theta)) : \mathbb{Q}] = 3$, $3 \nmid 2^l$ 与定理矛盾, 因此无法做出 (例如 $\pi/3$). 但在特殊情况下, 例如 $3\theta = \pi/2$, 多项式 $4x^3 - 3x$ 可约, 我们得到 $\cos\theta$ 为一个 2 次方程的解, 我们可以三等分 $\pi/2$.

(ii) 化圆为方.

圆的面积为 πr^2 , 其中 r 为半径. 正方形的面积为 a^2 , 其中 a 为其边长. 我们可以假设 $r = 1$. 因此, 此问题可以转化为是否可以用尺规做出 $\sqrt{\pi}$. 由于 $\sqrt{\pi}$ 为 $\mathbb{Q}$ 上的超越元, 因此不能做出.

(iii) 倍立方.

我们可以假设给出的立方体边长为 1. 则该问题可以转化为是否可以用尺规做出 $\sqrt[3]{2}$. 由于 $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \nmid 2^l$, 因此不能做出.

(iv) 画正 n 边形.

我们总是可以假设该 n 边形的中心在原点, 一个顶点是 1. 因此, 该问题就是问 $\exp(2\pi i/n)$ 是否是可构造的. 我们知道 $\exp(2\pi i/n)$ 是 $x^n - 1$ 的根, 因此其最小多项式整除 $x^n - 1$. 我们只需要找出 n 使得 $\exp(2\pi i/n)$, 满足定理 4.3.1 的要求. 例如, $n = 3, 4, 5, 6, 8, 12, 15, 17, \dots$ (我们在 Galois 理论课程中还会更仔细的研究这个问题)

27.5 域的代数闭包

由之前的讨论, 我们知道, 对任意域 F 以及其上的多项式 f , 我们都可以找到一个域的扩张 K 使得 f 在 K 上有根. 如果 f 的根在 F 中, 则 $F = K$, 我们不需要将 F 扩张出去; 否则, K 将真包含 F . 如果 F 中有多项式 g 在 K 上没有根, 那么我们就需要进一步取 K 的扩张来得到一个域 E 使得 f 和 g 都在 E 中有根.

一个自然的问题就是: 是否存在一个域 F 的代数扩张 $\bar{F}$, 使得任给 $f \in F[x]$, f 都在 $\bar{F}$ 中分裂?

以上讨论似乎给了我们一种方法去寻找这个 "最大的 F 的代数扩张". 另一方面, 在对分裂域的研究中我们已经看到了, 一个多项式的分裂域是依赖于其构造的, 并不是唯一的. 因此如果我们希望通过 $f \in F[x]$ 的分裂域 E_f 和 $g \in F[x]$ 的分裂域 E_g 来研究 $fg \in F[x]$ 的分裂域 E_{fg} , 我们需要找到一个更大的域同时包含 E_f 和 E_g , 这样 E_f 和 E_g 中的元素才可以进行代数运算, 从而使我们建立其与 E_{fg} 之间的联系.

例 27.5.1.

令 $F = \mathbb{Q}$. 我们记

$$f(x) = x^2 - 2, \quad g(x) = x^3 - 3, \quad h(x) = f(x)g(x).$$

我们记 f 和 g 的分裂域分别为

$$E_f = \mathbb{Q}[x]/\langle x^2 - 2 \rangle, \quad E_g = \mathbb{Q}(\sqrt[3]{3}, \omega) \subset \mathbb{C},$$

其中 ω 是 $\mathbb{C}$ 中的三次单位根. 此时 $E_f \setminus F$ 和 $E_g \setminus F$ 中元素之间的运算没有定义.

因此从这个角度来说, 如果可能的话, 我们也需要这样的一个 "所有 F 上的多项式在里边都是分裂" 的代数扩张的存在.

在本节, 我们将讨论这个 F 的 "最大的代数扩张" 的存在性和唯一性.

27.5.1 定义

我们先给出一些定义.

定义 27.5.2

设 K 为一个 F 的代数扩张. 若任给 F 中多项式 $f(x)$ 都在 K 中分裂, 我们称 K 为 F 的**代数闭包**.

域的代数闭包的另一种定义方法.

定义 27.5.3

任给一个域 K , 我们称之为**代数封闭**的, 若其满足任给 $f \in K[x]$, f 在 K 中有根.

注 27.5.4.

由代数封闭这个定义, 我们可以得出 K 上的任意多项式 f 都在 K 上分裂.

定义 27.5.5

任给一个域 F , 我们称 F 的一个代数扩张 K 是 F 的**代数闭包**, 若 K 是代数封闭的.

命题 27.5.6

两种代数封闭的定义是等价的.

注 27.5.7.

第二个定义看似比第一个定义要求更多, 第一个要求是 F 上所有多项式在其扩域 K 中分裂, 第二个要求的是 F 的扩域 K 上所有的多项式在 K 中分裂.

证明. 若 K 是 F 的代数扩张, 且代数封闭, 由于 $F[x] \subset K[x]$, 由代数封闭的定义, 我们有 F 上所有多项式都在 K 中分裂.

反过来, 若 F 中所有的多项式在 K 中分裂, 假设 K 不是代数封闭的, 那么存在 $K[x]$ 的一个多项式 f , 满足 f 在 K 中没有根. 我们不妨设 f 不可约.

我们可以构造 K 的代数扩张 E 使得 f 在 E 中有根 $\alpha \in E \setminus K$. 因此 α 在 K 上的最小多项式为 f . 由于 E/K 和 K/F 都为代数扩张, 因此 E/F 为代数扩张, α 为 F 上的代数元, 我们记 $g \in F[x]$ 为 α 的最小多项式. 由包含关系 $F \subset K \subset E$, 我们在 $K[x]$ 中有

$$f(x) \mid g(x).$$

由于 F 上所有多项式都在 K 上分裂, 且 $f \in K[x]$ 不可约, 因此 $\deg f = 1$. 因此在 $E[x]$ 中我们有 $f(x) = x - \alpha$. 所以 $\alpha \in K$, 矛盾. $\square$

定理 27.5.8

任给一个域 F , 记 K 为 F 的代数扩张. 我们有如下等价描述:

- (i) 每个 K 上的不可约多项式都在 K 中分裂.
- (ii) 每个 F 上的不可约多项式都在 K 中分裂.
- (iii) 如果存在代数扩张 K'/K , 则 $K' = K$.

注 27.5.9.

在证明了代数闭包的存在性和唯一性, 由最后一条我们可以看出, 一个域 F 的代数闭包可以被认为是 F (在同构意义下) "最大" 的代数扩张.

27.5.2 域的代数闭包的存在性

本节我们证明

定理 27.5.10

任给一个域 F , 其代数闭包存在.

注 27.5.11.

由于我们希望得到一个包含所有 F 的代数扩张的代数扩张. 若考虑直接使用 F 所有代数扩张来构造最大的代数扩张, 则需要注意类似于集合论里罗素悖论的问题, 也就是说需要说明得到的仍然是一个集合. 证明中会涉及一个偏序集中最大元素存在性的问题, 因此会用到 Zorn 引理.

我们这里给出的证明的具体办法可以认为是在一个更一般的情形下使用 Kronecker 构造. 该证明过程中也需要用到 Zorn 引理.

证明. 我们考虑 $F[x]$. 任给 F 上的一个不可约多项式 f ,

$$f(x) = a_0 + a_1x + \cdots + a_nx^n.$$

我们设一个形式变量 x_f , 然后考虑以下 F 上的多元多项式环

$$F[\dots, x_f, \dots].$$

并考虑其中的一元多项式

$$f(x_f) = a_0 + a_1x_f + \cdots + a_nx_f^n.$$

我们记 $I = \langle f(x_f) | f \in F[x] \text{ 且不可约} \rangle$ 为 $F[\dots, x_f, \dots]$ 的一个理想.

首先 I 是一个真理想. 若不然 $1 \in I$, 因此存在有限多个 $f_1, \dots, f_k \in F[x]$ 不可约, 以及有限多个 $g_1, \dots, g_k \in F[\dots, x_f, \dots]$ 满足:

$$g_1 f_1(x_{f_1}) + \dots + g_k f_k(x_{f_k}) = 1.$$

此处注意, 尽管我们有无穷多个形式变量, 但由多项式环的定义 $F[\dots, x_f, \dots]$ 中的每个多项式只涉及有限多个变量.

两个多项式相等, 则其在任何域上诱导的函数(如果有定义的话)也相同. 特别地, 我们考虑 F 的扩张 E , 满足任意 $f_i(x_{f_i})$ 在 E 中有一个根 α_i . 我们令 $x_{f_i} = \alpha_i$, 其他 g_j 牵扯到的形式变量取值为 0, 则左边为 0, 右边为 1, 矛盾. 因此 I 是一个真理想.

我们记 $\mathbf{m}$ 为包含 I 的极大理想. 我们记

$$K_1 := F[\dots, x_f, \dots] / \mathbf{m}.$$

任给 F 上多项式 f , 我们有 $x_f + \mathbf{m}$ 为 f 在 K_1 中的解 (因为 $f(x_f) \in \mathbf{m}$). 由于 $F[\dots, x_f, \dots]$ 由 $F \cup \{x_f | f \in F[x] \text{ 且不可约}\}$ 生成的环, 因此

$$K_1 = F(\{x_f + \mathbf{m} | f \in F[x] \text{ 不可约}\}).$$

因此 K_1 为 F 的代数扩张, 且任意 F 的不可约多项式都在 K_1 中有一个根.

使用归纳构造, 我们得到一系列域扩张列

$$\dots / K_n / K_{n-1} / \dots / K_1 / K_0 = F$$

满足任取 $n \in \mathbb{N}^*$, K_{n+1} 都是从 K_n 出发由以上构造得到的. 由代数扩张的传递性, 我们知道对任意 $n \in \mathbb{N}$, K_n / F 为代数扩张. 我们记

$$K = \bigcup_{n \in \mathbb{N}} K_n.$$

任取 $\alpha \in K$, 存在 K_n , 满足 $\alpha \in K_n$, 因此为 F 上的代数元. 因此 K/F 为一个代数扩张. 任取 $f \in F[x]$ 为一个不可约多项式. 由于每一个从 K_i 到 K_{i+1} , $f \in K_{i+1}[x]$ 的不可约因子的次数的最大值严格小于 $f \in K_i[x]$ 的不可约因子的次数的最大值. 记 $k = \deg f$, 则 f 在 K_k 中分裂. 因此 K/F 为 F 的代数闭包. $\square$

注 27.5.12.

在以上证明中, 我们使用了 Zorn 引理. 特别地, 以下三项等价:

- (i) 任何交换幺环中都存在极大理想.
- (ii) 选择公理.
- (iii) Zorn 引理.

27.5.3 域的代数闭包的唯一性

这里我们证明代数闭包的在同构意义下是唯一的. 这个证明需也要用到 Zorn 引理. 我们首先证明以下结论.

命题 27.5.13

设 E/F 为一个域的代数扩张, 我们记 K 为 F 的代数闭包. 则存在一个域单同态

$$\varphi : E \rightarrow K,$$

满足 $\varphi|_F = id_F$.

证明. 我们考虑如下集合:

$$\mathcal{M} = \{(L, \varphi_L) \mid L \text{ 为 } E/F \text{ 的中间域, 有 } \varphi_L : L \rightarrow K, \text{ 且 } \varphi_L|_F = \text{id}_F\}.$$

该集合非空, 因为包含元素 (F, j) , 满足 $j : F \rightarrow K$ 为域的嵌入. 我们可以在这个集合里定义一个偏序关系:

- $(L, \varphi_L) \preceq (L', \varphi_{L'})$ 当且仅当 L 为 L'/F 的中间域, 且 $\varphi_{L'}|_L = \varphi_L$.

设 $\mathcal{C}$ 为一个 $\mathcal{M}$ 中的一个链:

$$\mathcal{C} = \{(L_1, \varphi_1) \prec (L_2, \varphi_2) \prec \cdots\}.$$

我们记

$$E' = \bigcup \{L \mid (L, \varphi) \in \mathcal{C}\},$$

也是 E/F 的一个中间域. 任给 $\alpha \in E'$, 则存在一个二元组 $(L, \varphi) \in \mathcal{C}$, 使得 $\alpha \in L$. 我们可以定义如下域的单同态

$$\theta : E' \rightarrow K,$$

对任意 $(L, \varphi) \in \mathcal{C}$, $\alpha \in L$, 满足 $\theta(\alpha) = \varphi(\alpha)$. 由偏序关系的定义, 我们知道 θ 是良定义的. 因此 (E', θ) 是 $\mathcal{C}$ 的上界. 因此, 我们可以使用 Zorn 引理, 集合 $\mathcal{M}$ 中有极大元. 我们将其记作 (E_1, θ_1) .

我们要证明 $E_1 = E$. 我们使用反证法. 由 E/F 为代数扩张, 我们知道 E/E_1 也是代数扩张. 若存在 $\alpha \in E \setminus E_1$, 我们记 $f_\alpha \in E_1[x]$ 为其最小多项式. 考虑 $\theta_1(f_\alpha) \in K[x]$. 由于 K 代数封闭, 因此 $\theta_1(f_\alpha)$ 在 K 中分裂:

$$\theta_1(f_\alpha)(x) = (x - \beta_1) \cdots (x - \beta_k).$$

由于 $\theta_1(f_\alpha)(\beta_1) = 0$, 由定理 27.3.13, 我们有域同态:

$$\theta_2 : E_1(\alpha) \rightarrow K,$$

满足 $\theta_2|_{E_1} = \theta_1$, 且 $\theta_2(\alpha) = \beta_1$. 因此

$$(E_1, \theta_1) \prec (E_1(\alpha), \theta_2).$$

这与 (E_1, θ_1) 的极大性矛盾. 因此 $E_1 = E$. 令 $\varphi = \theta_1$ 即为命题所要求的映射. $\square$

定理 27.5.14

任给一个域 F , 设域 K 和 K' 都是 F 的代数闭包, 则存在一个域同构 $\varphi : K \rightarrow K'$, 满足

$$\varphi|_F = \text{id}_F.$$

证明. 由以上命题, 我们有域同态

$$\varphi : K \rightarrow K',$$

$$\psi : K' \rightarrow K,$$

满足 $\varphi|_F = \text{id}_F$ 以及 $\psi|_F = \text{id}_F$. 考虑同态的符合 $\iota = \psi \circ \varphi$, 我们有同态

$$\iota : K \rightarrow K,$$

且 $\iota|_F = \text{id}_F$. 下边使用反证法来证明 ι 是一个域同构.

若 ι 不是域同构, 则 ι 不是满同态, 因此存在 $\alpha \in K \setminus \iota(K)$.

由于 K/F 为代数扩张, 且 $\iota(K)$ 为 K/F 的中间域, 因此 α 为 $\iota(K)$ 上的代数元. 我们记 $g_\alpha(x) \in \iota(K)[x]$ 为 α 在 $\iota(K)$ 上的最小多项式. 注意到 $\alpha \notin \iota(K)$, 因此

$$\deg g_\alpha(x) > 1.$$

注意到

$$\iota' : K \rightarrow \iota(K),$$

为一个域同构, 我们考虑它的逆

$$\iota^{-1} : \iota(K) \rightarrow K.$$

则 $\iota(g_\alpha)(x) \in K[x]$ 不可约. 由于 K 代数封闭, 因此

$$\deg g_\alpha(x) = \deg \iota^{-1}(g_\alpha)(x) = 1,$$

矛盾. 因此我们有 $\iota(K) = K$ 以及 ι 为双射. 因此 ψ 为满射, 所以是同构.

对 $\varphi \circ \psi$ 做类似的讨论, 我们可以得到 φ 为同构. □

注 27.5.15.

以及上以上证明说明如果一个域 K 是 F 的代数闭包, 那么任何 K 到自己的 F -自同态都是 F -自同构.

27.5.4 例子

虽然我们在证明代数闭包的存在性的时候使用了比较复杂的构造, 看似需要经过无限次扩张才能得到代数闭包, 但实际上一个域 F 的代数闭包 K 关于 F 的扩张次数并不总是无限的.

例 27.5.16.

实数域 $\mathbb{R}$ 的代数闭包为 $\mathbb{C}$. 注意到

$$[\mathbb{C} : \mathbb{R}] = 2.$$

例 27.5.17.

$\mathbb{Q}$ 的代数闭包 $\overline{\mathbb{Q}}$ 不是 $\mathbb{C}$, 而是严格被 $\mathbb{C}$ 包含, 因为 π 是 $\mathbb{Q}$ 上的超越元, 因此 $\mathbb{C}$ 不是 $\mathbb{Q}$ 的代数扩张. 另一方面, 所有 $\mathbb{Q}$ 上的多项式也是 $\mathbb{R}$ 上的多项式, 因此在 $\mathbb{C}$ 中分裂. 因此 $\mathbb{C}$ 中有 $\mathbb{Q}$ 的代数闭包.

以上两个例子中, 我们同时注意到 $\mathbb{R}$ 中的不可约多项式次数最多为 2, 而 $\mathbb{Q}$ 上的不可约多项式次数是没有上界的, 例如任意素数 p 对应的 p -次单位根的最小多项式为

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1 \in \mathbb{Q}[x].$$

因为素数没有上界, 因此 $\mathbb{Q}$ 上的不可约多项式没有上界. 另一个例子考虑对任意 $n \in \mathbb{N}^*$, 取多项式

$$x^n - 2 \in \mathbb{Q}[x],$$

由 Eisenstein 判别法, 我们知道这个多项式不可约. 因此实际上对任意 $n \in \mathbb{N}^*$, 我们都可以找到 $\mathbb{Q}[x]$ 上找到 n -次不可约多项式. 这实际上就告诉我们任取 $n \in \mathbb{N}^*$, 我们都有

$$[\overline{\mathbb{Q}} : \mathbb{Q}] > n.$$

注 27.5.18.

教材中给出了如下定义: 任给一个扩张 E/F , 我们记

$$E_0 := \{\alpha \in E \mid \alpha \text{ 为 } F \text{ 上的代数元}\}.$$

我们称 E_0 为 F 在 E 中的代数闭包. 注意这个定义里, 我们并不要求 F 中所有多项式在 E 上分裂, 或者 E/F 为一个代数闭包. 我们这里只是将 E 中所有 F 的代数元收集起来得到一个 E 中包含 F 的最大的代数扩张. 而我们以上给出的代数闭包只和 F 有关.

上边例子中提到的 $\overline{\mathbb{Q}}$ 按照这里的定义实际上就是 $\mathbb{Q}$ 在 $\mathbb{C}$ 中的代数闭包.

27.6 域的正规扩张

我们已经知道了, 任取一个域 F , 满足 $F[x]$ 所有 1 次多项式分裂的 F 的最小的代数扩张是 F , 而使得所有多项式分裂的 F 的代数扩张是 F 的代数闭包. 任给一个多项式 $f(x) \in F[x] \setminus F$, 我们可以构造出 E/F 为 $f(x)$ 的分裂域, 即为在同构意义下最小的令 $f(x)$ 分裂的域. 这个定义可以推广到对 $F[x]$ 中的一族多项式的讨论中.

定义 27.6.1

任取 $S \subset F[x]$, 我们称 E/F 为 S 的分裂域扩张, 如果其满足

- (i) 任给 $f \in S$, f 在 E 上分裂;
- (ii) 任给 E' 为 E/F 的中间域, 使得任意 $f \in S$ 都在 E' 中分裂, 则 $E = E'$.

注 27.6.2.

由第二点可以看出, 多项式集合 S 的分裂域为满足 S 中所有多项式分裂的最小的 F 的扩张. 若 E/F 为 S 的分裂域, 我们记

$$A = \{\alpha \in E \mid \exists f(x) \in S, f(\alpha) = 0\},$$

那么第二个条件实际上等价于 $E = F(A)$.

注 27.6.3.

如果

$$S = \{f_1(x), \dots, f_k(x)\} \subset F[x] \setminus F,$$

那么 S 的分裂域就是

$$g(x) = f_1(x) \cdots f_k(x) \in F[x] \setminus F,$$

的分裂域. 因此这个新的定义只有在 $|S| = \infty$ 才是对多项式的分裂域非平凡的推广. 特别地, 如果

$$S = F[x],$$

那么 S 的分裂域为 F 的代数闭包.

我们首先观察分裂域的一个简单的情形. 考虑 $\mathbb{Q}$ 上的多项式 $x^2 - 2$, 及其在 $\mathbb{C}$ 中的分裂域 $\mathbb{Q}(\sqrt{2})$. 由之前的讨论我们知道 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 是一个次数为 2 的代数扩张. 任取 $a, b \in \mathbb{Q}$, 我们有 $\alpha = a + b\sqrt{2}$ 为 $\mathbb{Q}$ 上代数元. 记 $f_\alpha \in \mathbb{Q}[x]$ 为 α 的最小多项式. 注意到

$$\deg f_\alpha(x) \leq 2,$$

且 $f_\alpha(\alpha) = 0$, 因此 $f_\alpha(x)$ 在 $\mathbb{Q}(\alpha)$ 上分裂. 换言之, 任意在 $\mathbb{Q}(\sqrt{2})$ 上有根的 $\mathbb{Q}[x]$ 中不可约多项式在 $\mathbb{Q}(\sqrt{2})$ 分裂. 这个性质就是我们在定义正规扩张时所使用的.

定义 27.6.4 (教材定义 4.6.2)

记 F 为一个域. 我们称代数扩张 E/F 为 F 的一个**正规扩张**, 如果任取不可约多项式 $f(x) \in F[x]$, 都有以下两种情况中的一种发生:

- (i) f 在 E 中没有根;
- (ii) f 在 E 中分裂.

注 27.6.5.

第一个条件并不能说明 $f(x) \in E[x]$ 仍是不可约的. 考虑一下的例子. 记 $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2})$. 我们考虑 $f(x) = x^4 - 2 \in \mathbb{Q}[x]$.

注意 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约. 若我们将其考虑为 $\mathbb{Q}(\sqrt{2})$ 上的多项式, 则有

$$f(x) = (x^2 - \sqrt{2})(x^2 + \sqrt{2}).$$

注意到 $f(x)$ 此时仍旧没有根, 但是在 $\mathbb{Q}(\sqrt{2})[x]$ 中可约. 我们可以考虑其根 $\sqrt[4]{2}$. 它在 $\mathbb{Q}$ 和 $\mathbb{Q}(\sqrt{2})$ 中的最下多项式分别为 $x^4 - 2$ 和 $x^2 - \sqrt{2}$. 这里我们有

$$x^2 - \sqrt{2} \mid x^4 - 2.$$

更一般的, 考虑域扩张 E/F . 设 K 为 E/F 的中间域. 若 $\alpha \in E$ 为 F 的代数元, 则 α 也是 K 上的代数元. 我们考虑 α 在 F 上的最小多项式 $f(x)$ 和 K 上的最小多项式 $g(x)$, 则在 $K[x]$ 中有

$$g(x) \mid f(x).$$

此外, 由正规扩张与多项式的分裂域的关系, 我们注意到 $\mathbb{Q}(\sqrt{2})$ 为 $\mathbb{Q}$ 的正规扩张.

之前的例子中, 我们看到了 $x^2 - 2 \in \mathbb{Q}[x]$ 的分裂域扩张 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 满足正规扩张的定义. 由此我们就有了两个问题:

- (i) 是不是所有的分裂域扩张都是正规扩张?
- (ii) 反过来, 是不是所有的正规扩张都是分裂域扩张?

以及以上两个问题的答案都是肯定的. 我们将其整理为以下定理:

定理 27.6.6 (教材定理 4.6.6, 命题 4.6.7)

E/F 为一个正规扩张, 当且仅当存在 $F[x] \setminus F$ 的非空子集 S , 满足 E/F 是 S 的分裂域扩张.

证明. 假设 E 为 F 的正规扩张, 我们记

$$S = \{f \in F[x] \mid f \text{ 在 } E \text{ 中分裂}\}.$$

我们要证 E/F 为 S 的分裂域扩张.

我们注意到任给多项式 $f \in S$, f 在 E 中分裂, 因此我们只需要验证 E 是最小的满足这样性质的 F 的扩张. 我们考虑任意扩张 E/F 的中间域 K , 假设任意 $f \in S$ 都在 K 中分裂. 我们需要证明 $K = E$.

我们是用反证法. 如果 $K \subsetneq E$, 我们可以考虑 $\alpha \in E \setminus K$. 由于 E/F 为代数扩张, 因此 α 为 F 的代数元. 我们考虑 α 的最小多项式 f_α . 因为 $\alpha \in E$, 由正规扩张的定义, f_α 在 E 中分裂. 因此 $f_\alpha \in S$.

由于 K/F 为 S 的分裂域扩张, 因此 f_α 在 K 中分裂, 我们有 $\alpha \in K$, 矛盾. 因此 E/F 为 S 的分裂域扩张.

反过来我们设 S 为 $F[x] \setminus F$ 的一个非空子集, 设 E/F 为 S 的分裂域扩张. 我们需要证明 E 是一个正规扩张.

我们设 $f(x) \in F[x]$ 为一个不可约多项式. 我们需要证明若 $f(x)$ 在 E 有根, 则 $f(x)$ 在 E 上分裂. 实际上, 我们可以将问题简化为对 S 有限情况的讨论. 这是因为每个 E 中的元素都在 F 的一个有限扩张中.

我们记

$$A = \{\alpha \in E \mid \exists h(x) \in S, h(\alpha) = 0\},$$

则 $E = F(A)$.

我们设 β 为 $f(x)$ 的一个根. 并设 $\alpha_1, \dots, \alpha_k \in A$ 满足 $\beta \in F(\alpha_1, \dots, \alpha_k)$. 设 $\alpha_1, \dots, \alpha_k$ 在 F 上的最小多项式分别为 $f_1(x), \dots, f_k(x)$, 记

$$g(x) = f_1(x) \cdots f_k(x).$$

由于 E/F 为 S 的分裂域, 因此 $g(x)$ 在 F 上分裂. 我们记

$$R = \{\alpha \in E \mid g(\alpha) = 0\},$$

则 $F(R)/F$ 为 $g(x) \in F[x]$ 的分裂域扩张. 为方便讨论, 我们记 $K = F(R)$. 由 R 的定义, 我们有 $\beta \in K$. 下边我们需要证明 $f(x)$ 在 K 上分裂. (问题转化为考虑有限扩张的情形.)

我们考虑 H/K 为 $f(x) \in K[x]$ 的分裂域扩张. 若 β 是 $f(x)$ 在 H 中仅有的根, 则 $K = H$, $f(x)$ 在 K 中分裂, 因此也在 E 中分裂. 因此命题得证.

现在假设在 H 中, $f(x)$ 有另一个根 $\gamma \neq \beta$. 我们考虑 H 的子域 $F(\beta)$, $F(\gamma)$ 以及 $K(\gamma)$. 为了方便理解, 我们首先把已经出现的域之间的关系展示在以下交换图中:

$$\begin{array}{ccccc}
 & & H & & \\
 & \nearrow & & \nwarrow & \\
 K(\gamma) & \xrightarrow{\quad \tilde{\iota} \quad} & K(\beta) = K & & \\
 \uparrow & & \uparrow & & \\
 F(\gamma) & \xrightarrow{\quad \iota \quad} & F(\beta) & & \\
 \uparrow & & \uparrow & & \\
 F & \xrightarrow{\quad \text{id}_F \quad} & F & &
 \end{array}$$

其中

- $\hookrightarrow$ 表示子域的嵌入同态;
- id_F 为 F 上的恒等同态;
- ι 为 id_F 在 $F(\beta)$ 上的开拓, 并满足 $\iota(\beta) = \gamma$;
- $\tilde{\iota}$ 为 ι 在 K 上的开拓.

以上开拓的存在性是由之前证明的定理 27.3.13 和 ?? 保证的. 注意由于 $g(x) \in F[x]$, 因此我们可以将其看作 $F(\beta)$ 上的多项式以及 $F(\gamma)$ 上的多项式, 由于

$$K = F(\beta)(R), \quad K(\gamma) = F(\gamma)(R),$$

因此 K 为 $g(x) \in F(\beta)[x]$ 的分裂域, $K(\gamma)$ 为 $g(x) \in F(\gamma)[x]$ 的分裂域.

我们注意到以下嵌入同态

$$j: K \hookrightarrow K(\gamma).$$

因此有以下同态

$$\varphi = j \circ \tilde{\iota}: K(\gamma) \rightarrow K(\gamma).$$

注意到 $\varphi|_F = \text{id}_F$. 考虑扩张塔

$$K(\gamma)/\varphi(K(\gamma))/F,$$

我们有

$$[K(\gamma):F] = [K(\gamma):\varphi(K(\gamma))][\varphi(K(\gamma)):F] = [K(\gamma):\varphi(K(\gamma))][K(\gamma):F],$$

由于 $[K(\gamma):F] < \infty$, 因此我们有

$$[K(\gamma):\varphi(K(\gamma))] = 1,$$

因此 $K(\gamma) = \varphi(K(\gamma))$, 我们有 φ 为一个域同构. 因此 j 为满射, 特别地有 $\gamma \in K$. 因此 $f(x)$ 在 K 上分裂. $\square$

注 27.6.7.

证明中 H 的选取是为保证我们讨论里所有的记号, 特别是 γ 有定义. 以上交换图也可以理解为发生在 H 中. 实际上证明的后半部分 (从引入记号 K 开始) 就是该定理有限扩张的版本证明.

推论 27.6.8 (教材习题 4.6 练习 12.)

若 E/F 为一个正规扩张, 则对任意 E/F 的中间域 K , 有 E/K 是一个正规扩张.

证明. 由于 E/F 为正规扩张, 所以 E 是 $F[x]$ 的某个子集 S 的分裂域. 我们记 S 中的多项式在 E 中的根的集合为

$$A = \{\alpha \in E \mid \exists f(x) \in S, f(\alpha) = 0\},$$

则有 $E = F(A)$.

注意到

$$S \subset F[x] \subset K[x],$$

因此 $K(A)$ 为 S 在 K 上的分裂域. 我们有

$$E = F(A) \subset K(A) \subset E$$

因此 $E = K(A)$. 因此 E/K 为正规扩张. $\square$

推论 27.6.9

设域扩张 E/F 满足

$$[E : F] < \infty,$$

则以下两个叙述等价

- (i) E/F 为正规扩张;
- (ii) 存在 $g(x) \in F[x] \setminus F$, 使得 E/F 为 $g(x)$ 的分裂域.

证明. 由于

$$[E : F] < \infty,$$

存在 $n \in \mathbb{N}^*$, 以及有限多个元素

$$\alpha_1, \dots, \alpha_n \in E,$$

满足 $E = F(\alpha_1, \dots, \alpha_n)$. 我们记

$$f_1(x), \dots, f_n(x) \in F[x],$$

分别为 $\alpha_1, \dots, \alpha_n$ 在 F 上的最小多项式, 并记

$$g(x) = f_1(x) \cdots f_n(x) \in F[x].$$

由于 E/F 为正规扩张, 且不可约多项式

$$f_1(x), \dots, f_n(x) \in F[x],$$

在 E 中有根, 因此这些多项式在 E 中分裂, 我们进而有 $g(x)$ 在 E 中分裂. 我们记

$$R = \{\alpha \in E \mid g(\alpha) = 0\},$$

注意到

$$\{\alpha_1, \dots, \alpha_n\} \subset R,$$

因此

$$E = F(\alpha_1, \dots, \alpha_n) \subset F(R) \subset E.$$

由此可得 E 为 $g(x) \in F[x]$ 的分裂域. □

正规闭包

一个代数扩张 K/F 并不一定是一个正规扩张. 通过考虑 K 的扩域以及 K 的子域, 我们可以考虑与 K/F 相关的两个 F 的正规扩张. 我们首先考虑 K 的扩域, 引入 K/F 的正规闭包的概念.

定义 27.6.10

任取 K/F 为 F 的扩张, 我们称 K 的一个扩张 E 为 F 关于扩张 K/F 的**正规闭包**, 如果其满足

- (i) E/F 是一个正规扩张;
- (ii) 任给 E' 为 E/K 的中间域, 使得 E'/F 是一个正规扩张, 则 $E' = E$.

注 27.6.11.

笼统讲, 我们将 K 扩张出去找到一个最小的 F 的(包含 K 的)正规扩张. 这里的包含关系是 $E/K/F$.

推论 27.6.12

设域扩张 K/F 满足

$$[K : F] < \infty,$$

则 K/F 有一个有限次的正规闭包扩张 E/K .

证明. 由于 K/F 为一个有限扩张, 存在有限多个元素 $\alpha_1, \dots, \alpha_n \in K$, 满足

$$K = F(\alpha_1, \dots, \alpha_n).$$

我们记

$$f_1(x), \dots, f_n(x) \in F[x],$$

分别为

$$\alpha_1, \dots, \alpha_n \in K,$$

的最小多项式. 记

$$g(x) = f_1(x) \cdots f_n(x) \in F[x].$$

我们记 E 为 $g(x) \in F[x]$ 的分裂域, 因此 E/F 为一个正规扩张.

下证 E 最小. 假设 M 为一个中间域, 满足

$$E/M/K/F,$$

且 M/F 为一个正规扩张, 由于不可约多项式

$$f_1(x), \dots, f_n(x) \in F[x],$$

在 K 中有根, 因此在 M 中有根, 因此

$$f_1(x), \dots, f_n(x) \in F[x],$$

在 M 中分裂. 记

$$R = \{\alpha \in E \mid g(\alpha) = 0\},$$

注意到

$$\{\alpha \in E \mid \exists i \in \{1, \dots, n\}, f_i(\alpha) = 0\} = \{\alpha \in E \mid g(\alpha) = 0\},$$

因此

$$R \subset M.$$

综上所述, 我们有

$$E = F(R) \subset M \subset E.$$

因此 $E = M$. □

代数扩张 E/F 与 $\text{Aut}_F(E)$ 的正规子群

下边我们讨论代数扩张 E/F 中的 F 的正规扩张中间域 K , 我们将主要关注 K 在 $\text{Aut}_F(E)$ 中的元素作用下的像. 这里我们将考虑 E/F 为正规扩张的情形.

以下引理是后续讨论的一个基础:

引理 27.6.13

设 F 为一个域, 任取 $f(x) \in F[x]$ 为一个不可约多项式, 记 E/F 为 $f(x) \in F[x]$ 的分裂域扩张, 并记

$$\alpha_1, \dots, \alpha_n \in E,$$

为 $f(x)$ 在 E 中的根, 则对任意 α_i 和 α_j , 存在一个 E 的 F -自同构 φ , 满足

$$\varphi(\alpha_i) = \alpha_j.$$

证明. 由于 α_i 和 α_j 在 F 上的最小多项式都是 f , 因此存在域同构

$$\iota : F(\alpha_i) \rightarrow F(\alpha_j).$$

满足 $\iota|_F = \text{id}_F$, 且 $\iota(\alpha_i) = \alpha_j$.

注意到

- $E/F(\alpha_i)$ 为 $f \in F(\alpha_i)[x]$ 的分裂域扩张,
- $E/F(\alpha_j)$ 为 $f \in F(\alpha_j)[x]$ 的分裂域扩张,
- $\iota(f) = f$,

由推论 ??, 同态 ι 可以开拓为一个 E 到 E 的域同构 φ . 因此我们有 E 的自同构将 α_i 送到 α_j . $\square$

注 27.6.14.

沿用引理中的记号, 我们记

$$R = \{\alpha \in E \mid f(\alpha) = 0\},$$

即为 f 在 E 中的根集. 由于 E 上的 F -自同构不改变代数元的最小多项式, 因此任取 $\sigma \in \text{Aut}_F(E)$, 我们有

$$\sigma(R) = R,$$

由此我们得到 $\text{Aut}_F(E)$ 在 R 上的一个群作用. 以上引理在说这个群作用是可递的.

一个正规扩张 E/F 的中间域 K 也可能给出一个正规扩张 K/F . 以下定理给出了一个判定方法.

定理 27.6.15 (教材习题 4.6 练习 10. 14.)

设域正规扩张 E/F , 满足

$$[E : F] < \infty.$$

记 K 为扩张 E/F 的一个中间域. 以下叙述等价:

- (i) K/F 为一个正规扩张;
- (ii) 任给 E 的自同构 σ 满足 $\sigma|_F = \text{id}_F$, 则 $\sigma(K) \subset K$;
- (iii) 任给 E 的自同构 σ 满足 $\sigma|_F = \text{id}_F$, 则 $\sigma(K) = K$.

证明. (i) $\implies$ (ii) 我们假设 K/F 为一个正规扩张. 考虑任意 $\alpha \in K$. 我们记 $f_\alpha \in F[x]$ 为 α 的最小多项式. 由于

$$\sigma|_F = \text{id}_F,$$

我们有

$$\sigma(f_\alpha(\alpha)) = f_\alpha(\sigma(\alpha)),$$

因此 $\sigma(\alpha)$ 为 f_α 的一个根. 记

$$R = \{\beta \in E \mid f_\alpha(\beta) = 0\}.$$

由于 f_α 在 K 中分裂, 因此

$$\sigma(\alpha) \in R \subset K,$$

因此 $\sigma(K) \subset K$.

(ii) $\implies$ (iii) 我们考虑域扩张

$$K/\sigma(K)/F,$$

由于 $\sigma|_F = \text{id}_F$, 我们有

$$[\sigma(K) : F] = [\sigma(K) : \sigma(F)] = [K : F],$$

利用

$$[K : F] = [K : \sigma(K)][\sigma(K) : F],$$

我们有 $[K : \sigma(K)] = 1$. 因此 $K = \sigma(K)$.

(iii) $\implies$ (i) 任给 $\alpha \in K$, 记 $f_\alpha(x) \in F[x]$ 为 α 的最小多项式. 我们需要证明 $f_\alpha(x)$ 在 K 中分裂. 由于 E/F 为一个正规扩张, 因此 $f_\alpha(x)$ 在 E 中分裂.

我们记

$$R = \{\beta \in E \mid f_\alpha(\beta) = 0\}.$$

任取

$$\sigma \in \text{Aut}_F(E),$$

我们有

$$\sigma(R) = R.$$

利用之前的引理, 我们知道 $\text{Aut}_F(E)$ 在 R 上的作用是可递的, 因此

$$\text{Aut}_F(E)(\alpha) = R.$$

因此

$$R = \text{Aut}_F(E)(\alpha) \subset K,$$

我们有 $f_\alpha(x)$ 在 K 上分裂. 因此 K/F 为一个正规扩张. □

注 27.6.16.

以上结论对无限正规扩张也是满足的. 对任意代数元总是存在某一个有限扩张中, 此时我们可以利用对有限扩张的讨论.

注 27.6.17.

我们下边考虑正规扩张 E/F 的正规中间域 K , 即 $E/K/F$, 满足 K/F 正规. 利用以上定理, 我们可以证明

$$\text{Aut}_K(E) \triangleleft \text{Aut}_F(E).$$

这部分我们将在 Galois 基本定理的部分做进一步的讨论.

27.7 域的可分扩张

27.7.1 可分扩张的定义及一些基本结论

定义

我们首先回顾一下与可分相关的定义. 设 F 为一个域.

定义 27.7.1 (教材定义 4.4.16)

记 $f \in F[x]$ 为一个次数为 $n > 0$ 的不可约多项式. 记 K/F 为 f 的分裂域扩张. 我们称 f 在 F 上是 **可分的**, 在 K 中我们有两两不同的 n 个元素 $\alpha_1, \dots, \alpha_n \in K$, 使得

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

一个 F 上的次数大于 0 的多项式是 **可分的**, 若其每个不可约因子都是可分的.

定义 27.7.2 (教材定义 4.6.1)

设 E/F 为一个域扩张. 我们称 $\alpha \in E$ 为 F 上的 **可分元**, 若 α 是 F 上的代数元且其在 F 上的最小多项式可分. 我们称 E/F 为 F 的一个 **可分扩张**, 若 E 中的元素都是 F 上的可分元.

我们首先给出以下可分扩张的基本性质.

命题 27.7.3

设 E/F 为一个可分扩张, K 为一个中间域. 则 E/K 和 K/F 都是可分的.

证明. 由于 E 中元素都是 F 上的可分元, 因此 K 中元素也都是 F 上的可分元. 由此 K/F 为可分扩张.

由于 E/F 为代数扩张, 因此任取 $\alpha \in E$ 都同时是 F 和 K 上的代数元. 记

$$f_\alpha(x) \in F[x] \text{ 和 } g_\alpha(x) \in K[x]$$

分别为 α 在 F 上和 K 上的最小多项式. 记 M/K 为 $f_\alpha(x) \in K[x]$ 的分裂域扩张. 因此存在 $\alpha_1, \dots, \alpha_n \in M$, 满足

$$f_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

考虑 $L = F(\alpha_1, \dots, \alpha_n)$ 为 M/F 的中间域. 我们有 L/F 为 f_α 的分裂域扩张. 由于 α 在 F 上可分, 因此 $\alpha_1, \dots, \alpha_n \in M$ 两两不同.

在 $K[x]$ 中, 我们有 $g_\alpha(x) \mid f_\alpha(x)$. 因此 $g_\alpha(x)$ 在 M 中分裂, 且根两两不同. 因此 α 为 K 上的可分元. E/K 为一个可分扩张. $\square$

可分扩张的判定

考虑域扩张 E/F , 在之前关于分裂域的学习中, 我们曾经建立了 $\text{Aut}_F(E)$ 和 $[E : F]$ 之间的联系. 以下我们将看到使用这些结论可以来证明一个扩张的可分性.

我们仍从单扩张开始讨论, 考虑推论 ?? 可以得到以下定理.

定理 27.7.4 (教材命题 4.4.12)

设 $F(\alpha)/F$ 为一个单代数扩张, 且 $[F(\alpha) : F] = n$. 记 α 在 F 上的最小多项式为

$$f_\alpha(x) = \text{Irr}(\alpha, F).$$

设

$$\varphi : F \rightarrow K,$$

为一个域同态. 则

(i) φ 在 $F(\alpha)$ 上的开拓的个数满足

$$\#\{\tilde{\varphi} : F(\alpha) \rightarrow K \mid \tilde{\varphi}|_F = \varphi\} \leq [F(\alpha) : F].$$

(ii) 上式中等号 "=" 成立当且仅当以下两个条件成立

- (a) $\varphi(f_\alpha)(x)$ 在 K 上分裂;
- (b) α 在 F 上可分.

利用以上定理归纳, 我们可以得到以下关于 F 的有限扩张的类似结论.

定理 27.7.5 (教材定理 4.4.13)

设 E/F 为一个域有限扩张. 对任意 $\alpha \in E$, 记

$$f_\alpha(x) = \text{Irr}(\alpha, F) \in F[x].$$

设

$$\varphi : F \rightarrow K$$

为一个域同态. 则

(i) φ 在 E 上的开拓的个数满足

$$\#\{\tilde{\varphi} : E \rightarrow K \mid \tilde{\varphi}|_F = \varphi\} \leq [E : F].$$

(ii) 上式中等号 "=" 成立当且仅当以下两个条件成立

- (a) 对任意 $\alpha \in E$, 都有 $\varphi(f_\alpha)(x)$ 在 K 上分裂;
- (b) E/F 为可分扩张.

证明. 由于 E/F 为一个有限扩张, 因此存在 $\alpha_1, \dots, \alpha_s \in E$, 满足

$$E = F(\alpha_1, \dots, \alpha_s).$$

如果存在 φ 在 E 上的开拓 $\tilde{\varphi}$, 则 $\tilde{\varphi}$ 由 $\alpha_1, \dots, \alpha_s$ 的像

$$\tilde{\varphi}(\alpha_1), \dots, \tilde{\varphi}(\alpha_s) \in K,$$

决定.

我们考虑扩张塔

$$E = F(\alpha_1, \dots, \alpha_s) / \cdots / F(\alpha_1, \alpha_2) / F(\alpha_1) / F.$$

我们记

$$F_0 = F, \quad F_i = F(\alpha_1, \dots, \alpha_i) \quad (1 \leq i \leq s).$$

通过依次确定 $\tilde{\varphi}(\alpha_1), \dots, \tilde{\varphi}(\alpha_s)$, 我们可以将 φ 依次开拓到 $F_1, F_2, \dots, F_s = E$, 并且相邻的两个开拓后一个是前一个的开拓. 利用交换图来表示就是

$$\begin{array}{ccc}
 F = F_0 & \xrightarrow{\varphi} & K \\
 j_0 \downarrow & \nearrow \varphi_1 & \uparrow \\
 F_1 & & \\
 j_1 \downarrow & \nearrow \varphi_2 & \\
 F_2 & & \\
 j_2 \downarrow & \nearrow \varphi_n = \tilde{\varphi} & \\
 \vdots & & \\
 j_{n-1} \downarrow & & \\
 E = F_s & &
 \end{array}$$

通过在每一步使用前一个定理, 我们有 φ 在 E 上的开拓 $\tilde{\varphi}$ 的个数满足小于等于

$$\#\{\tilde{\varphi} : E \rightarrow K \mid \tilde{\varphi}|_F = \varphi\} \leq [F(\alpha_1, \dots, \alpha_s) : F(\alpha_1, \dots, \alpha_{s-1})] \cdots [F(\alpha_1) : F] = [E : F].$$

这里需要说明的是, 从 φ_i 开拓到 φ_{i+1} 时, 我们使用了前一个定理. 得到的是以下不等式

$$\#\{\varphi_{i+1} : F_{i+1} \rightarrow K \mid \varphi_{i+1}|_{F_i} = \varphi_i\} \leq [F_{i+1} : F_i].$$

注意虽然左边是对任意固定的 φ_i 讨论有多少种可能的到 F_{i+1} 的开拓 φ_{i+1} , 依赖于 φ_i 的选取, 但是右边不依赖于 φ_i 的选取. 这是我们可以得到之前的不等式的原因.

我们下边证明等号 = 成立的充要条件. 我们首先考虑 $\alpha_1, \dots, \alpha_s$. 记它们在 F 上的最小多项式分别为

$$f_1(x) = \text{Irr}(\alpha_1, F), \dots, f_s(x) = \text{Irr}(\alpha_s, F).$$

我们将证明等号成立当且仅当

- (i) $\varphi(f_1)(x), \dots, \varphi(f_s)(x)$ 在 K 上分裂;
- (ii) $\alpha_1, \dots, \alpha_s$ 在 F 上可分.

我们仍考虑之前的交换图, 将 φ 向越来越大的扩域上开拓的过程中, 依次得到

$$\varphi_1, \dots, \varphi_s = \tilde{\varphi}.$$

注意到对任意 $0 \leq i \leq s-1$, 我们有

$$\#\{\varphi_{i+1} : F_{i+1} \rightarrow K \mid \varphi_{i+1}|_{F_i} = \varphi_i\} \leq [F_{i+1} : F_i].$$

如果有

$$\#\{\tilde{\varphi} : E \rightarrow K \mid \tilde{\varphi}|_F = \varphi\} = [E : F],$$

我们有对任意 $0 \leq i \leq s-1$,

$$\#\{\varphi_{i+1} : F_{i+1} \rightarrow K \mid \varphi_{i+1}|_{F_i} = \varphi_i\} = [F_{i+1} : F_i].$$

特别地, 考虑 $i=0$, 则有

$$\#\{\varphi_1 : F(\alpha_1) \rightarrow K \mid \varphi_1|_F = \varphi\} = [F(\alpha_1) : F].$$

由前一个定理知道

(i) $\varphi(f_1)(x)$ 在 K 中分裂.

(ii) α_1 在 F 上可分.

我们观察之前整个证明过程中发现我们并没有对生成元组有任何要求, 即之前的讨论 E 关于 F 的任意一组有限的生成元以任意的顺序排列都是成立的. 因此, 要证明 α_i ($1 < i \leq s$) 满足之前的两个条件, 我们只需要将 $\alpha_1, \dots, \alpha_s$ 重排, 使得 α_i 排在第一个即可得到

(i) $\varphi(f_i)(x)$ 在 K 中分裂.

(ii) α_i 在 F 上可分.

反过来假设对任意 $1 \leq i \leq s$, 都有

(i) $\varphi(f_i)(x)$ 在 K 中分裂.

(ii) α_i 在 F 上可分.

我们记

$$g_i(x) = \text{Irr}(\alpha_i, F_{i-1}),$$

则有

$$g_i(x) \mid f_i(x) \in F_{i-1}[x].$$

由于 $f_i(x)$ 可分, 因此 $g_i(x)$ 可分. 由于

$$\varphi_{i-1}(g_i)(x) \mid \varphi_{i-1}(f_i)(x) = \varphi(f_i)(x) \in K[x],$$

且 $\varphi(f_i)(x)$ 分裂, 因此 $\varphi_{i-1}(g_i)(x)$ 在 K 上分裂. 因此对任意 $1 \leq i \leq s$, 我们都有

$$\#\{\varphi_i : F_i \rightarrow K \mid \varphi_i|_{F_{i-1}} = \varphi_{i-1}\} = [F_i : F_{i-1}].$$

因此

$$\#\{\tilde{\varphi} : E \rightarrow K \mid \tilde{\varphi}|_F = \varphi\} = [E : F].$$

现在我们考虑 E 中其它的元素. 注意到任取 $\beta \in E$, 由于 $\alpha_1, \dots, \alpha_s$ 在 F 上生成 E , 因此

$$\beta_1 = \beta, \beta_2 = \alpha_1, \dots, \beta_{s+1} = \alpha_s,$$

也在 F 上生成 E , 即

$$E = F(\beta_1, \dots, \beta_{s+1}).$$

重复之前的讨论, 我们有若

$$\#\{\tilde{\varphi}: E \rightarrow K \mid \tilde{\varphi}|_F = \varphi\} = [E:F],$$

则 β 在 F 上可分, 且 $\varphi(f_\beta)(x)$ 在 K 中分裂.

反过来, 若对任意 $\alpha \in E$, 都有

(i) $\varphi(f_\alpha)(x)$ 在 K 中分裂.

(ii) α 在 F 上可分.

由于

$$\{\alpha_1, \dots, \alpha_s\} \subset E,$$

因此我们有

$$\#\{\tilde{\varphi}: E \rightarrow K \mid \tilde{\varphi}|_F = \varphi\} = [E:F].$$

□

注 27.7.6.

E 中所有元素在 F 上可分意味着 E/F 是一个可分扩张.

推论 27.7.7

设 $F(\alpha)/F$ 为一个单代数扩张. 则 $F(\alpha)/F$ 为一个可分扩张当且仅当 α 在 F 上可分.

证明. 记 f_α 为 α 的最小多项式, 并记其次数为 n . 记 E 为 f_α 的分裂域. 因此 E/F 是一个正规扩张. 也即所有 E 中元素在 F 上的最小多项式在 E 中分裂.

记

$$\iota: F \rightarrow E,$$

为域的嵌入同态. 若 α 可分, 则由之前的定理我们知道

$$\#\{\tilde{\iota}: F(\alpha) \rightarrow E \mid \tilde{\iota}|_F = \iota\} = [F(\alpha): F].$$

因此 $F(\alpha)/F$ 为一个可分扩张.

反过来, 若 $F(\alpha)/F$ 为可分扩张, 则 α 在 F 上可分. □

之前的定理的证明过程可以给出以下推论.

推论 27.7.8 (教材命题 4.9.1)

设 $L = F(\alpha_1, \dots, \alpha_r)$ 为一个有限扩张. 则 L/F 为一个可分扩张, 当且仅当 $\alpha_1, \dots, \alpha_r$ 为 F 上可分元.

由此, 我们得到可分这个性质关于四则运算封闭, 即

推论 27.7.9 (教材推论 4.9.2)

记 E/F 为一个域扩张. 设 $\alpha, \beta \in E$ 为 F 上的可分元, 则 $\alpha \pm \beta, \alpha\beta, \alpha\eta^{-1}$ ($\beta \in E^*$) 都是 F 上的可分元.

注 27.7.10.

这些结论说明, 如果我们知道一个代数扩张的生成元, 只需研究生成元的可分性, 我们就可以知道这个代数扩张是不是可分的. 我们不需要按照定义去验证扩域中每一个元素都是子域上的可分元.

可分扩张的传递性

我们考虑可分扩张的是否传递的问题. 记 E, K, F 为域, 我们将证明以下定理:

定理 27.7.11 (教材定理 4.9.6)

设 E/K 和 K/F 都是可分扩张, 则 E/F 为可分扩张.

证明. 我们需要证明任取 $\alpha \in E$, α 为 F 上的可分元. 记 $a_1, \dots, a_n \in K$, 满足 α 在 K 中的最小多项式为

$$f_\alpha(x) = a_0 + a_1x + \cdots + a_nx^n.$$

我们考虑 K/F 的中间域 $M = F(a_1, \dots, a_n)$. 注意到

$$f_\alpha(x) \in M[x] \subset K[x].$$

由于 $f_\alpha(x)$ 在 $K[x]$ 中不可约, 因此在 $M[x]$ 中不可约. 又由于

$$f_\alpha(\alpha) = 0,$$

因此我们有

$$\text{Irr}(\alpha, M) = \text{Irr}(\alpha, K) = f_\alpha(x).$$

由于 E/K 可分, 因此 $f_\alpha(x) \in M[x] \subset K[x]$ 可分, 因此 α 在 M 上可分.

我们考虑

$$M(\alpha)/M/F.$$

由于 K/F 可分, 因此 M/F 可分. 由于 α 在 M 上可分, 因此 $M(\alpha)/M$ 可分. 因此, 若我们证明了以上定理在有限扩张的情形, 由以上讨论, 我们就证明了一般的情形的结论.

下设 $[K : F] = m$, $[E : K] = n$.

设 $\alpha_1, \dots, \alpha_m \in K$, 满足

$$K = F(\alpha_1, \dots, \alpha_m).$$

记 $\alpha_1, \dots, \alpha_m$ 在 F 上的最小多项式分别为

$$f_1(x) = \text{Irr}(\alpha_1, F), \dots, f_m(x) = \text{Irr}(\alpha_m, F).$$

我们记

$$f(x) = f_1(x) \cdots f_m(x) \in F[x] \subset K[x],$$

并记 L_f/K 为 $f(x)$ 的分裂域扩张.

设 $\beta_1, \dots, \beta_n \in E$, 满足

$$E = K(\beta_1, \dots, \beta_n).$$

记 $\beta_1, \dots, \beta_n$ 在 F 上的最小多项式分别为

$$g_1(x) = \text{Irr}(\beta_1, F), \dots, g_n(x) = \text{Irr}(\beta_n, F),$$

我们记

$$g(x) = g_1(x) \cdots g_n(x) \in F[x] \subset L_f[x]$$

并记 L_g/L_f 为 $g(x)$ 的分裂域扩张.

另外记 $\beta_1, \dots, \beta_n$ 在 K 上的最小多项式分别为

$$h_1(x) = \text{Irr}(\beta_1, K), \dots, h_n(x) = \text{Irr}(\beta_n, K).$$

注意到 $[E : F] = [E : K][K : F] = mn$. 我们只需要证明 E 到 L_g 的 F -同态的个数为 mn .

我们考虑以下交换图:

$$\begin{array}{ccccc} F & \longrightarrow & K & \longrightarrow & E \\ \downarrow \text{id}_F & & \downarrow \varphi & & \downarrow \tilde{\varphi} \\ F & \longrightarrow & L_f & \longrightarrow & L_g \end{array}$$

这里水平方向上的映射都是包含嵌入. 注意到由于 K/F 为可分扩张, 且 $f(x)$ 在 L_f 中分裂, 因此我们有 $[K : F]$ 个不同的 id_F 在 K 上的开拓.

任取 id_F 在 K 上的开拓 φ , 由于 E/K 可分, 且对任意 $1 \leq i \leq n$, 由于

$$\varphi(h_i)(x) \mid \varphi(g_i)(x) = g_i(x),$$

我们有 $\varphi(h_i)(x)$ 在 L_g 上分裂, 因此 φ 在 E 上的两两不同的开拓有 $[E : K]$ 个.

综合以上所得结论, 我们有 id_F 在 E 上的两两不同的开拓共有

$$[K : F][E : K] = [E : F]$$

个, 因此 E/F 可分. □

27.7.2 不可分不可约多项式

由定义, 我们知道若 $f(x) \in F[x]$ 不可分, 则 $f(x)$ 在其分裂域中有重根. 在之前的课后练习中, 我们给出过一种利用形式微商定义重根的方法, 这里利用分裂域, 我们给出另一种, 后边我们会看到两种定义的等价的.

定义 27.7.12

记 F 为一个域, $f \in F[x]$. 记 E/F 为 f 的分裂域扩张. 设 $\alpha \in E$, 若存在自然数 $k \in \mathbb{N}^*$, 满足

$$(x - \alpha)^k \mid f(x) \in E[x],$$

我们称 α 为 $f(x)$ 的**根**, 并称最大的满足以上整除关系的自然数 k 为根 α 的**重数**. 若 $f(x)$ 的一个根 α 的重数大于 1, 我们称之为 $f(x)$ 在 E 上的**重根**.

我们下边利用形式微商给出 f 有重根的判定方法.

定义 27.7.13 (教材定义 4.8.1)

任取 $f(x) \in F[x]$, 假设我们记 $f(x) = a_0 + a_1x + \cdots + a_nx^n$, 称多项式

$$Df(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$$

为 f 的**形式微商**.

注 27.7.14.

这里注意 $f(x)$ 是 n 次多项式并不意味着 $Df(x)$ 为 $n-1$ 次多项式. 后边我们会看到如果 n 是域的特征, 那么 $na_n = 0$.

命题 27.7.15 (教材命题 4.8.2)

我们有

$$D : F[x] \rightarrow F[x],$$

为一个 F -线性映射: 对任意 $f(x), g(x) \in F[x]$, 对任意 $a \in F$, 我们有

$$D(f+g)(x) = Df(x) + Dg(x), \quad D(af)(x) = a(Df(x)).$$

我们进一步还有 Leibniz 法则

$$D(fg)(x) = Df(x)g(x) + f(x)Dg(x).$$

以下定理是常用的判断任意多项式是否有重根的工具.

定理 27.7.16 (教材定理 4.8.4)

记 F 为一个域, $f(x) \in F[x] \setminus F$ 为一个多项式. 记 E/F 为 $f(x)$ 的分裂域扩张. 则以下叙述等价

- (i) $f(x)$ 在 E 中有重根;
- (ii) 存在 $\alpha \in E$, 满足 $f(\alpha) = Df(\alpha) = 0$;
- (iii) 存在 $g(x) \in F[x]$ 有 $\deg g > 0$, 满足

$$g(x) \mid \gcd(f(x), Df(x)).$$

证明. (i) $\implies$ (ii): 设 α 为 f 在 E 中的重根. 因此在 $E[x]$ 中, 有 $f(x) = (x - \alpha)^k f_1(x)$. 我们考虑如下计算:

$$Df(x) = k(x - \alpha)^{k-1} f_1(x) + (x - \alpha)^k Df_1(x).$$

由于 $k > 1$, 我们有 $Df(\alpha) = 0$.

(ii) $\implies$ (iii): 注意到 α 为 F 上的代数元, 我们记 $g(x) \in F[x]$ 为 α 在 F 上的最小多项式, 满足 $\deg g > 0$. 由于 $f(\alpha) = Df(\alpha) = 0$, 因此

$$g(x) \mid f(x), \quad g(x) \mid Df(x).$$

(iii) $\implies$ (i): 若 $g(x) \in F[x]$ 有 $\deg g > 0$, 满足 $g(x) \mid f(x)$, 则存在 $h(x) \in F[x]$, 满足

$$f(x) = g(x)h(x).$$

由于 E/F 为 $f(x)$ 的分裂域扩张, 因此 $g(x)$ 在 E 上分裂. 我们记 $\alpha \in E$ 为 $g(x)$ 的一个根. 在 $E[x]$ 中, 我们有

$$g(x) = (x - \alpha)g_1(x).$$

因此, 在 $E[x]$ 中, 存在 $f_1(x)$ 满足

$$f(x) = (x - \alpha)f_1(x).$$

考虑其形式微商:

$$Df(x) = f_1(x) + (x - \alpha)Df_1(x).$$

由于 $g(x) \mid Df(x)$, 因此 $Df(\alpha) = 0$, 因此 $f_1(\alpha) = 0$. 由此, 我们有

$$(x - \alpha) \mid f_1(x).$$

因此存在 $f_2(x) \in E[x]$, 满足

$$f_1(x) = (x - \alpha)f_2(x).$$

综合以上所得, 我们有

$$f(x) = (x - \alpha)^2 f_2(x) \in E[x],$$

也即 α 为 $f(x)$ 在 E 中的重根. □

注 27.7.17.

这里给出的判定方法不要求多项式不可约.

由于 F 上代数元 α 不可分等价于其最小多项式在其分裂域中有重根. 我们有如下定理

定理 27.7.18 (教材定理 4.8.8)

记 F 为一个域, $f(x) \in F[x]$ 为一个不可约多项式, 则 $f(x)$ 不可分当且仅当 $\text{Ch}F = p > 0$, 且

$$f(x) = b_0 + b_1x^p + b_2x^{2p} + \cdots + b_nx^{np}.$$

证明. 记

$$f(x) = a_0 + a_1x + \cdots + a_mx^m.$$

记 E/F 为 $f(x)$ 的分裂域扩张, 设 $\alpha \in E$ 为 $f(x)$ 的重根, 我们有

$$Df(\alpha) = f(\alpha) = 0.$$

注意 $f(x)$ 为 α 的最小多项式, 因此

$$Df(x) \in \langle f(x) \rangle,$$

因此我们有

$$f(x) \mid Df(x).$$

另一方面, 由形式微商的定义, 我们有

$$\deg Df \leq \deg f - 1 < \deg f.$$

因此

$$Df(x) = a_1 + 2a_2x + \cdots + ma_mx^{m-1} = 0.$$

这等价于

$$a_1 = 2a_2 = \cdots = ma_m = 0.$$

由于 $a_m \neq 0$, 因此 $ma_m = 0$ 当且仅当 $\text{Ch}F = p > 0$, 且 $p \mid m$.

任取 $k \in \mathbb{N}^*$, 若 $\gcd(k, p) = 1$, 由 $ka_k = 0$ 以及域的特征的定义, 我们有 $a_k = 0$. 因此存在 $n \in \mathbb{N}^*$, $b_0, \dots, b_n \in F$, 满足

$$f(x) = b_0 + b_1x^p + \cdots + b_nx^{np}.$$

反过来, 若存在素数 p , 满足 $\text{Ch}F = p$, 且 f 有以上形式, 我们有

$$Df(x) = 0,$$

因此

$$\gcd(f(x), Df(x)) = f(x) \in F[x] \setminus F.$$

由之前的定理, 我们有 $f(x)$ 在其分裂域中有重根, 因此 $f(x)$ 不可分.

实际上, 我们可以考虑多项式

$$g(x) = b_0 + b_1x + \cdots + b_nx^n,$$

则 $f(x) = g(x^p)$.

我们考虑 E_g/F 为 g 的分裂域扩张. 多项式 $g \in E_g[x]$ 有如下分解:

$$g(x) = (x - \beta_1) \cdots (x - \beta_n).$$

因此在 $E_g[x]$ 中有

$$f(x) = (x^p - \beta_1) \cdots (x^p - \beta_n).$$

我们考虑 E/E_g 为 f 的分裂域扩张. 对任意 $1 \leq i \leq n$, 记 $\alpha_i \in E$, 满足 $\alpha_i^p = \beta_i$. 由于 $\text{Ch}F = p$, 我们有 $\text{Ch}E = p$,

$$f(x) = (x - \alpha_1)^p \cdots (x - \alpha_n)^p.$$

有重根. 注意到

$$E = F(\beta_1, \dots, \beta_n)(\alpha_1, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_n).$$

因此 E/F 也是 $f \in F[x]$ 的分裂域扩张. 所有 f 有重根, 不是可分的. $\square$

注 27.7.19.

以上证明并不能说明多有根的次数为 p , 所得的 $\beta_1, \dots, \beta_n$ 有可能有相同的元素. 后边我们会专门讨论一个不可约不可分多项式的根可能的次数.

例 27.7.20 (教材习题 4.4 练习 2.).

记 p 为一个素数. 记 $\mathbb{F}_p(t)$ 为 $\mathbb{F}_p$ 的多项式环的分式域. 我们考虑其多项式环 $\mathbb{F}_p(t)[x]$. 以下我们证明

$$f(x) = x^p - t \in \mathbb{F}_p(t)[x],$$

不可约.

利用 Gauss 引理, 我们只需要证明

$$f(x) \in \mathbb{F}_p[t][x],$$

不可约. 注意到 $\mathbb{F}_p[t]$ 是一个 PID, 因此不可约元素都是素元素. 另一方面 $t \in \mathbb{F}_p[t]$ 是不可约元素, 因此由 Eisenstein 判别法, 考虑素元素 t , 我们有 $x^p - t$ 不可约.

记 $E/\mathbb{F}_p(t)$ 为 $x^p - t$ 的分裂域. 记 $\beta \in E$ 为 $x^p - t$ 的一个根, 则我们有

$$\beta^p - t = 0,$$

考虑到

$$\text{Ch}E[x] = \text{Ch}E = \text{Ch}\mathbb{F}_p(t) = p,$$

利用 Frobenius 同态, 在 $E[x]$ 中, 我们有

$$x^p - t = x^p - \beta^p = (x - \beta)^p.$$

因此 β 为 $x^p - t$ 的 p -重根, 多项式 $x^p - t \in \mathbb{F}_p(t)[x]$ 不可分.

以上定理实际上刻画了所有的不可约不可分多项式. 以下是这个定理的一个直接推论.

推论 27.7.21 (教材推论 4.8.6)

设 F 为一个域. 若 $\text{Ch}F = 0$, 则

- (i) 所有的 $F[x] \setminus F$ 中的多项式都可分.
- (ii) 所有 F 的代数扩张都是可分扩张.

定义 27.7.22

设 F 为一个域, 若 F 上所有的次数大于 0 的多项式都可分, 我们称 F 为一个**完备域**.

注 27.7.23.

域完备的一个直接推论就是其代数扩张都是可分扩张.

27.7.3 Frobenius 同态

注意到特征为 0 的域都是完备的. 下边我们将讨论特征为 $p > 0$ 的域的完备性. 这部分的讨论使用的主要工具是 Frobenius 同态. 设 F 为一个特征为素数 p 的域. 回顾 F 上可以定义 Frobenius 同态:

$$\begin{aligned} \text{Fr} : F &\rightarrow F, \\ a &\mapsto a^p. \end{aligned}$$

我们之前已经使用过多次该同态来证明一些与特征为 p 的域相关的问题.

我们之前讨论过一个域的特征为 $p > 0$ 当且仅当其包含的素域与 $\mathbb{F}_p$ 同构. 以下为了方便讨论, 我们将直接考虑 $\mathbb{F}_p$ 的扩张. 我们首先证明以下命题.

命题 27.7.24

若 $F/\mathbb{F}_p$ 为一个域扩张, 则有

$$\mathbb{F}_p = \{a \in F \mid \text{Fr}(a) = a\}.$$

利用 Fermat 小定理, 我们知道 $\mathbb{F}_p$ 中的元素都满足 $a^p = a$. 因此这个命题不平凡的地方在于另一个方向的包含, 也即 F 中满足 $a^p = a$ 的元素都在 F 的素域中.

证明. 记 $a \in F$, 满足 $a^p = a$, 则 a 为多项式

$$x^p - x \in F[x],$$

的一个根. 注意到这是一个 p 次多项式, 因此在 F 中至多有 p 个根.

由 Fermat 小定理知 $\mathbb{F}_p$ 中的元素都是该多项式的根, 且

$$|\mathbb{F}_p| = p,$$

因此

$$\mathbb{F}_p = \{a \in F \mid \text{Fr}(a) = a\}.$$

□

命题 27.7.25

设 $F/\mathbb{F}_p$ 为一个域扩张. 若 $F/\mathbb{F}_p$ 是一个代数扩张, 则 F 上的 Frobenius 自同态 Fr 为一个自同构.

下边我们将证明一个更一般的结论. 以上命题是该结论的一个特殊情况.

引理 27.7.26

任取一个扩张 E/F , 若 $[E : F] < \infty$, 则 $\text{End}_F(E) = \text{Aut}_F(E)$.

证明. 只需证明任意一个 F -自同态

$$\varphi : E \rightarrow E,$$

都是满射. 由于 φ 为 F -自同态, 我们有以下扩张塔

$$E/\varphi(E)/F.$$

因此我们有以下扩张次数的关系

$$[E : F] = [E : \varphi(E)][\varphi(E) : F].$$

由于

$$[\varphi(E) : F] = [E : F] < \infty,$$

我们有

$$[E : \varphi(E)] = 1,$$

因此 φ 为满射, 进而为同构.

□

引理 27.7.27

设域 E 为域 F 的代数扩张, 则 $\text{End}_F(E) = \text{Aut}_F(E)$.

证明. 我们只需证明任意 E 到 E 的 F -同态 φ 都是满射.

设 $\alpha \in E$, 记其最小多项式为 $f_\alpha(x) \in F[x]$.

设

$$\alpha = \alpha_1, \dots, \alpha_k \in E,$$

为 $f_\alpha(x)$ 在 E 中所有的根, 考虑 E/F 的中间域

$$K = F(\alpha_1, \dots, \alpha_k).$$

由于

$$\varphi(f_\alpha)(x) = f_\alpha(x),$$

我们有

$$\varphi(\{\alpha_1, \dots, \alpha_k\}) \subset \{\alpha_1, \dots, \alpha_k\}$$

由于 φ 为单射, 因此 φ 限制在

$$\{\alpha_1, \dots, \alpha_k\}$$

上为双射. 存在一个元素 α_i , 满足 $\varphi(\alpha_i) = \alpha$. 由此可得

$$\alpha \in \varphi(E).$$

因此 φ 为满射. □

注 27.7.28.

若 $F/\mathbb{F}_p$ 为一个代数扩张, 由于 Fr 为 F 的 $\mathbb{F}_p$ -自同态, 因此 Fr 为 F 的 $\mathbb{F}_p$ -自同构.

一个特征为 p 的域 F 上的 Frobenius 同态 Fr 为同构的一个推论就是任取 $a \in F$, 存在 $b \in F$, 满足

$$b^p = a.$$

结合之前关于不可约不可分多项式的判定工具, 我们有以下推论.

推论 27.7.29 (教材推论 4.8.10 改)

设 $F/\mathbb{F}_p$ 为一个域扩张. 若 $F/\mathbb{F}_p$ 是一个代数扩张, 则 F 完备.

证明. 考虑 F 上的 Frobenius 同态 Fr . 由于 $F/\mathbb{F}_p$ 为代数扩张, 同态 Fr 为 F 的一个自同构. 任取 $f(x) \in F[x]$ 满足

$$f(x) = a_0 + a_1 x^p + \dots + a_n x^{np},$$

存在 $b_0, \dots, b_n \in F$, 满足对任意 $0 \leq i \leq n$,

$$b_i^p = a_i.$$

因此

$$f(x) = (b_0 + b_1 x + \dots + b_n x^n)^p.$$

注意到 a_n 不为 0, 因此 b_n 不为 0. 由于 $n > 0$ 且 $p > 1$, 我们有 $f(x)$ 可约.

因此若 $f(x) \in F[x]$ 不可约, 由定理 27.7.18, 我们有 f 可分, 因此 F 完备. □

注 27.7.30.

设 F 为 $\mathbb{F}_p$ 的扩张, 但非代数扩张. 我们并不能说 F 不完备. 我们可以考虑 F 为一个代数封闭的域, 则所有的不可约多项式都是 1 次的. 因此此时 F 完备. 例如考虑 $\mathbb{F}_p(t)$ 的代数闭包.

我们注意到以上结论实际上是 Fr 为同构, 则 F 完备的一个推论. 我们考虑另一个方向.

命题 27.7.31

设 $F/\mathbb{F}_p$ 为一个域扩张, 若 F 上的 Frobenius 同态 Fr 不是同构, 则 F 不完备.

证明. 若 Fr 不是同态, 则 Fr 不是满射. 因此存在一个元素 $a \in F$, 满足多项式

$$x^p - a \in F[x]$$

在 F 中没有根, 因此不可约. 由定理 27.7.18, 我们知道 $x^p - a$ 不可分, 因此 F 不完备. $\square$

我们将之前的结论整理在一起得到一个特征为 p 的域是完备的一个充要条件.

推论 27.7.32 (教材定理 4.8.9)

设 F 为一个特征为素数 p 的域. 则 F 完备当且仅当其上的 Frobenius 同态映射为同构.

引理 27.7.33

设 F 为一个域, E/F 为一个有限扩张. 设我们有 E 的自同态:

$$\varphi: E \rightarrow E,$$

满足 $\varphi|_F$ 为 F 的自同构. 则 φ 为一个 E 的自同构.

证明. 我们只需证明 φ 是一个满射. 考虑

$$[E:F] = [E:\varphi(E)][\varphi(E):\varphi(F)] = [E:\varphi(E)][\varphi(E):F] = [E:\varphi(E)][E:F],$$

因此

$$[E:\varphi(E)] = 1.$$

我们得到 φ 为满射. $\square$

思考 27.7.34

该引理去掉 E/F 有限的条件还成立么?

命题 27.7.35 (教材推论 4.8.11)

完备域的代数扩张仍是完备域.

证明. 记 F 为一个完备域, E/F 为一个代数扩张.

由于域和其扩张有相同的特征, 若 $\text{Ch}F = 0$, 则 $\text{Ch}E = 0$. 因此 E 完备.

若 $\text{Ch}F = p$ 为一个素数, 那么我们只需证明 E 上的 Frobenius 同态 Fr 为一个同构即可, 这也等价于证明 Fr 为一个满射.

任取 $\alpha \in E$, 我们考虑 $F(\alpha)$. 则有

$$\text{Fr}(F(\alpha)) = F^p(\alpha^p).$$

这里

$$F^p := \{a^p \mid a \in F\}.$$

由于 F 完备, 因此 $F^p = F$. 因此 $F^p(\alpha^p) = F(\alpha^p)$ 为 $F(\alpha)/F$ 的中间域. 我们考虑

$$[F(\alpha) : F] = [F(\alpha) : F(\alpha^p)][F(\alpha^p) : F] = [F(\alpha) : F(\alpha^p)][F(\alpha) : F].$$

因此

$$[F(\alpha) : F(\alpha^p)] = 1,$$

我们有

$$\alpha \in F(\alpha) = F(\alpha^p) = \text{Fr}(F(\alpha)).$$

由此可得

$$\alpha \in \text{Fr}(E).$$

因此 Fr 为满射, 我们有 E 完备. □

27.7.4 不可分多项式

我们在这部分中讨论不可分多项式以及纯不可分扩张.

不可分不可约多项式的根的重数

记 F 为一个特征为素数 p 的域. 记 $f(x) \in F[x]$ 为一个多项式. 记

$$f(x) = \sum_{k \geq 0} a_k x^k.$$

由多项式的定义我们知道其中只有有限多项 a_k 不为 0. 我们考虑 f 的所有系数非零项的次数的最大公约数

$$d = \gcd(k \mid a_k \neq 0).$$

引理 27.7.36

任取非零自然数 s 满足 $s \mid d$, 存在多项式 $g \in F[x]$, 满足 $f(x) = g(x^s)$.

例 27.7.37.

我们考虑 F 上多项式

$$f(x) = x^{16} + x^4 + 1 \in F[x].$$

注意到

$$d = \gcd(0, 4, 16) = 4.$$

令 $s = 2$, 我们有

$$g_1(x) = x^8 + x^2 + 1, \quad f(x) = g_1(x^2).$$

令 $s = 4$, 我们有

$$g_2(x) = x^4 + x + 1, \quad f(x) = g_2(x^4).$$

考虑 d 的素数分解, 将其记为

$$d = p^m d_1,$$

满足 $p \nmid d_1$. 下边我们记 $g(x) \in F[x]$ 满足

$$f(x) = g(x^{p^m}).$$

命题 27.7.38 (教材定理 4.8.8)

沿用以上记号, 若 $f(x)$ 不可约, 则多项式 $g(x) \in F[x]$ 不可约且可分.

证明. 若在 $F[x]$ 中有

$$g(x) = g_1(x)g_2(x),$$

由于 $g(x^{p^m}) = f(x)$, 我们有

$$f(x) = g_1(x^{p^m})g_2(x^{p^m}).$$

由于 $f(x)$ 不可约, 我们有

$$\deg g_1(x^{p^m}) = 0 \text{ 或 } \deg g_2(x^{p^m}) = 0.$$

因此我们有

$$\deg g_1(x) = 0 \text{ 或 } \deg g_2(x) = 0.$$

由此可得 $g(x)$ 不可约.

若 g 不可分, 则 g 有如下形式:

$$g(x) = a_0 + a_1 x^p + \cdots + a_n x^{np}.$$

因此 f 有

$$f(x) = a_0 + a_1 x^{p^{m+1}} + \cdots + a_n x^{np^{m+1}}.$$

因此 $p^{m+1} \mid d$, 我们有 $p \mid d_1$, 矛盾. 因此 g 可分. □

命题 27.7.39 (教材定理 4.8.8)

沿用以上之前的记号, 记 E/F 为 $f(x)$ 的分裂域扩张. 则 $f(x)$ 在 E 中的所有根有相同的重数 p^m .

证明. 我们考虑 E_g/F 为 g 的分裂域扩张. 在 $E_g[x]$ 中有

$$g(x) = (x - \beta_1) \cdots (x - \beta_n),$$

进而有

$$f(x) = (x^{p^m} - \beta_1) \cdots (x^{p^m} - \beta_n).$$

由于 g 可分, 我们有 $\beta_1, \dots, \beta_n$ 两两不同.

记 E'/E_g 为 $f(x) \in E_g[x]$ 的分裂域扩张. 对任意 $1 \leq i \leq n$, 记 $\alpha_i \in E'$, 满足

$$\alpha_i^{p^m} = \beta_i.$$

由于 $\text{Ch} E' = \text{Ch} F = p$, 考虑 Frobenius 同态映射, 我们有

$$f(x) = (x - \alpha_1)^{p^m} \cdots (x - \alpha_n)^{p^m}.$$

因此

$$E' = F(\beta_1, \dots, \beta_n)(\alpha_1, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_n).$$

因此 E'/F 为 $f(x) \in F[x]$ 的分裂域扩张. 由于分裂域在同构意义下唯一, 我们不妨设 $E = E'$.

由于 $\beta_1, \dots, \beta_n$ 两两不同, 因此 $\alpha_1, \dots, \alpha_n$ 两两不同. 因此 $f(x)$ 在 E 中所有根都是 p^m 重. $\square$

(**)纯不可分扩张

定义 27.7.40 (教材习题 4.9 练习 5)

记 E/F 为一个代数扩张. 我们称 E/F 为一个**纯不可分扩张**, 若任取 $\alpha \in E \setminus F$, 则 α 不是 F 上的可分元.

注 27.7.41.

注意到不可分元素只可能出现在特征为素数 p 的域的扩张中, 因此我们本节将只考虑特征为 p 的域.

注 27.7.42.

若 $E = F$, 则定义条件自然满足. 有的资料里会要求 $F \subsetneq E$.

注 27.7.43.

教材中定义了**纯不可分元** (习题 4.9 练习 5). 我们应该注意按照这个定义, 一个元素为 F 上的纯不可分元并不意味着该元素不可分. 按照教材的定义, 可分元也是纯不可分元.

命题 27.7.44

记 F 为一个特征为素数 p 的域. 记 E/F 为一个域扩张. 则以下两个叙述等:

- (i) E/F 为纯不可分扩张;
- (ii) 任取 $\alpha \in E$, α 在 F 上的最小多项式 $f_\alpha \in F[x]$ 有如下形式:

$$f_\alpha(x) = x^{p^s} - a,$$

这里 $s \in \mathbb{N}$, $a \in F$.

证明. 考虑命题 27.7.38. $\square$

推论 27.7.45

设 E/K 和 K/F 为代数扩张. 若 E/K 和 K/F 都是纯不可分扩张, 当且仅当 E/F 为纯不可分扩张.

推论 27.7.46

设 E/F 为有限的纯不可分扩张. 则存在 $m \in \mathbb{N}$, 满足 $[E : F] = p^m$.

记 E/F 为一个代数扩张. 记

$$E_0 = \{\alpha \in E \mid \alpha \text{ 在 } F \text{ 上可分}\}.$$

由推论 27.7.7, 我们知道

$$E_0 \subset F(E_0) \subset E_0.$$

命题 27.7.47

E_0 为 E/F 的中间域, 且满足

- (i) E_0/F 为可分扩张;
- (ii) 若 E/E_0 的中间域 E' , 满足 E'/F 为可分的, 则 $E_0 = E'$.

定义 27.7.48

我们称 E_0 为 F 在 E 中的**可分闭包**.

命题 27.7.49

记 E/F 为一个代数扩张, $E_0 \subset E$ 为 F 的可分闭包. 则 E/E_0 为一个纯不可分扩张.

第六部分

Galois 理论

第二十八章 Galois 扩张

28.1 域的自同构的不变子域

定义 28.1.1 (教材定义 4.5.1)

域 F 上扩张 E 的 F -自同构的全体构成一个群, 被称为扩张 E/F 的 **Galois 群**, 被记为 $\text{Gal}(E/F)$.

注 28.1.2.

这个群实际上就是我们之前讨论的 $\text{Aut}_F(E)$, 我们以下将使用记号 $\text{Gal}(E/F)$.

由引理 27.7.27, 我们有

推论 28.1.3 (教材引理 4.5.4)

设 E/F 为 F 的一个代数扩张, K 为 E/F 的中间域. 我们有

- (i) $\text{End}_F(E) = \text{Gal}(E/F)$;
- (ii) $\text{End}_K(E) = \text{Gal}(E/K)$;
- (iii) $\text{End}_F(K) = \text{Gal}(K/F)$.

证明. 若 E/F 为代数扩张, 则 E/K 和 K/F 都是代数扩张. 由引理 27.7.27 直接得到以上命题. $\square$

设 E/F 为一个扩张. 设 $\varphi \in \text{Gal}(E/F)$.

定义 28.1.4

我们定义同构 φ 的**不变子域**为:

$$\text{Inv}(\varphi) := \{a \in E \mid \varphi(a) = a\}.$$

命题 28.1.5

集合 $\text{Inv}(\varphi)$ 构成 E/F 的一个中间域.

证明. 由 F -同构的定义, 我们有 $F \subset \text{Inv}(\varphi)$. 特别地, 我们有

$$0, 1 \in \text{Inv}(\varphi).$$

由 φ 为一个域同构映射, 任取 $a, b \in \text{Inv}(\varphi)$, 我们有

$$\begin{aligned}\varphi(a+b) &= \varphi(a) + \varphi(b) = a+b \\ \varphi(ab) &= \varphi(a)\varphi(b) = ab\end{aligned}$$

因此 $\text{Inv}(\varphi)$ 对加法和乘法封闭.

对任意 $a \in \text{Inv}(\varphi)$, 我们有

$$\varphi(-a) = -\varphi(a) = -a,$$

若 $a \in \text{Inv}(\varphi)^*$, 则

$$\varphi(a^{-1}) = (\varphi(a))^{-1} = a^{-1},$$

所以 $\text{Inv}(\varphi)$ 对加法构成子群, $\text{Inv}(\varphi)^*$ 对乘法构成子群. 因此 $\text{Inv}(\varphi)$ 为 E/F 的中间域. $\square$

类似地, 我们有如下定义.

定义 28.1.6

任取 $\text{Gal}(E/F)$ 的非空子集 S , 我们定义 S 的**不变子域**为

$$\text{Inv}(S) := \{a \in E \mid \forall \varphi \in S, \varphi(a) = a\}.$$

命题 28.1.7

我们有

$$\text{Inv}(S) = \bigcap_{\varphi \in S} \text{Inv}(\varphi).$$

注 28.1.8.

因此 $\text{Inv}(S)$ 也是 E/F 的中间域.

以上命题的一个直接推论如下

推论 28.1.9 (教材引理 4.6.12)

任取 $\text{Gal}(E/F)$ 的两个非空子集 S_1 和 S_2 , 若 $S_1 \subset S_2$, 则 $\text{Inv}(S_1) \supset \text{Inv}(S_2)$.

我们也可以从中间域出发来寻找不变子域包含中间域的 $\text{Gal}(E/F)$ 中的元素.

定义 28.1.10

设 K 为 E/F 的中间域. 我们定义如下 $\text{Gal}(E/F)$ 的子集:

$$\Gamma(K) := \{\varphi \in \text{Gal}(E/F) \mid \varphi|_K = id_K\}.$$

命题 28.1.11

集合 $\Gamma(K)$ 构成 $\text{Gal}(E/F)$ 的一个子群.

证明. 注意到恒等同构映射在其中. 因此 $\Gamma(K)$ 非空. 由 $\Gamma(K)$ 的定义, 我们可以验证任取 $\varphi_1, \varphi_2 \in \Gamma(K)$, 任取 $a \in K$, 我们有

$$(\varphi_1 \circ \varphi_2)(a) = \varphi_1(\varphi_2(a)) = \varphi_1(a) = a.$$

以及

$$(\varphi_1)^{-1}(a) = a.$$

因此 $\Gamma(K) \subset \text{Gal}(E/F)$ 为一个子群. □

注 28.1.12.

我们有 $\Gamma(K) = \text{Gal}(E/K)$.

命题 28.1.13 (教材引理 4.6.12)

若 $E/K_1/K_2/F$ 为一列域扩张, 我们有 $\Gamma(K_1) < \Gamma(K_2)$.

注 28.1.14.

这个命题的逆命题是不对的. 我们可以考虑下边这个例子. 取 $F = \mathbb{F}_p(t)$ 为 $\mathbb{F}_p$ 上的多项式环的分式域. 考虑 $x^p - t \in \mathbb{F}_p(t)[x]$ 的分裂域 $E = \mathbb{F}_p(t)(\alpha)$, 满足 $\alpha^p = t$. 我们有

$$\text{Gal}(E/F) = \{id\}.$$

这是由于任取 $\varphi \in \text{Gal}(E/F)$, 考虑 α 的像, 则 $\varphi(\alpha)$ 必须是 $x^p - t$ 的根. 由于这个多项式有只有一个 p 重根 α , 因此 $\varphi(\alpha) = \alpha$. 由于 $\varphi|_F = id_F$, 因此 $\varphi = id$.

这样我们就有

$$\Gamma(\mathbb{F}_p(t)) = \{id\} = \Gamma(\mathbb{F}_p(t)(\alpha)).$$

令 $K_1 = \mathbb{F}_p(t)$, $K_2 = \mathbb{F}_p(t)(\alpha)$, 就得出了以上命题逆命题的反例.

命题 28.1.15

任取 $S \subset \text{Gal}(E/F)$, 任取 K 为 E/F 的中间域, 我们有如下关系:

- (i) $\Gamma(\text{Inv}(S)) \supset S$.
- (ii) $\text{Inv}(\Gamma(K)) \supset K$.
- (iii) $\text{Inv}(\Gamma(\text{Inv}(S))) = \text{Inv}(S)$.
- (iv) $\Gamma(\text{Inv}(\Gamma(K))) = \Gamma(K)$

证明. (i) 若 $\varphi \in S$, 则 φ 固定 $\text{Inv}(S)$, 因此属于 $\Gamma(\text{Inv}(S))$.

- (ii) 若 $a \in K$, 则 a 被 $\Gamma(K)$ 中所有元素固定, 因此 $a \in \text{Inv}(\Gamma(K))$.
- (iii) 由于 $\Gamma(\text{Inv}(S)) \supset S$, 推论 28.1.9 告诉我们 $\text{Inv}(\Gamma(\text{Inv}(S))) \subset \text{Inv}(S)$. 另一方面, 我们考虑 (i), 将 S 替换为 $\text{Inv}(S)$, 有 $\text{Inv}(\Gamma(\text{Inv}(S))) \supset \text{Inv}(S)$. 因此二者相等.
- (iv) 使用 (ii) 和命题 28.1.13, 证明与 (iii) 类似.

□

注 28.1.16.

我们注意到任给一个子集 $S \subset \text{Gal}(E/F)$, 我们都有一个 $\text{Gal}(E/F)$ 的子群 $\Gamma(\text{Inv}(S))$ 与 S 有相同的不变域. 同时, 我们考虑 S 在 $\text{Gal}(E/F)$ 中生成的子群 $\langle S \rangle$, 由

$$S \subset \langle S \rangle \subset \Gamma(\text{Inv}(S)),$$

我们有 $\text{Inv}(\langle S \rangle) = \text{Inv}(S)$. 因此以下我们将只考虑 S 为 $\text{Gal}(E/F)$ 的子群情形.

注 28.1.17.

我们后续会考虑命题 28.1.9 中令 S_1 和 S_2 都为子群的情形, 并证明其逆命题在 $[E:F]$ 有限也是对的. (见推论 28.2.14)

我们记 $\mathcal{P}(\text{Gal}(E/F))$ 为 $\text{Gal}(E/F)$ 所有子群的集合, $\mathcal{P}(E/F)$ 为所有 E/F 扩张中间域的集合. 则我们之前定义 Γ 和 Inv 为两个映射:

$$\begin{aligned}\text{Inv} : \mathcal{P}(\text{Gal}(E/F)) &\rightarrow \mathcal{P}(E/F) \\ \Gamma : \mathcal{P}(E/F) &\rightarrow \mathcal{P}(\text{Gal}(E/F))\end{aligned}$$

28.2 Galois 扩张的定义及其等价性质

定义 28.2.1 (教材定义 4.6.11)

设 E/F 为一个域的代数扩张. 我们称 E 为 F 的一个 **Galois 扩张**, 若 E/F 是一个正规, 可分扩张.

我们首先回顾一些之前证明的结论. 首先是之前介绍的一些关于特殊扩张与中间域的关系.

推论 28.2.2 (推论 3.3.6)

若 E/F 为一个正规扩张, 则对任意中间域 K , E/K 也是一个正规扩张.

命题 28.2.3

若 E/F 为一个可分扩张, 则对任意中间域 K , E/K 和 K/F 都是可分扩张.

推论 28.2.4

若 E/F 为一个 Galois 扩张, 则对任意中间域 K , E/K 是一个 Galois 扩张.

其次是关于代数扩张的自同态与自同构的关系.

推论 28.2.5 (推论 28.1.3, 教材引理 4.5.4)

设 E/F 为 F 的一个代数扩张, K 为 E/F 的中间域. 我们有

- (i) $\text{End}_F(E) = \text{Gal}(E/F)$;
- (ii) $\text{End}_K(E) = \text{Gal}(E/K)$;
- (iii) $\text{End}_F(K) = \text{Gal}(K/F)$.

最后是当 E/F 为有限扩张的时候, 我们可以利用以下定理对 $|\text{Gal}(E/F)|$ 进行估计.

定理 28.2.6 (定理 27.7.5)

设 E/F 为一个域扩张满足 $[E : F] = n$. 对任意 $\alpha \in E$, 及其最小多项式为 f_α . 设 $\varphi : F \rightarrow L$ 为一个域同态. 则

- (i) 若 E/F 为一个可分扩张, 且对任意 $\alpha \in E$, 满足 $\varphi(f_\alpha)$ 在 L 中分裂, 则有且仅有 n 个 E 到 L 的域同态是 φ 的延拓.
- (ii) 否则, 存在少于 n 个 E 到 L 的域同态是 φ 的扩张.

注 28.2.7.

这里 (i) 中条件可以翻译为 E/F 为一个可分, 正规扩张. 以上结论实际上告诉了我们一个域有限扩张 E/F 的次数 $[E : F]$ 和该扩张的 Galois 群的元素个数之间满足

$$[E : F] \geq |\text{Gal}(E/F)|.$$

在本节最后, 我们会使用 Dedekind 无关性定理来给出以上不等式的另一个证明.

命题 28.2.8

记 E 为一个域, $\text{Aut}(E)$ 为 E 的自同构. 设

$$G = \{\varphi_1, \dots, \varphi_m\} < \text{Aut}(E)$$

为一个有限子群, 并记 $F = \text{Inv}(G)$. 考虑 E 的一个有限子集

$$B = \{a_1, \dots, a_n\} \subset E.$$

以下叙述等价:

(i) $(a_1, \dots, a_n)$ 为 F -线性无关.

(ii) E^m 中的向量

$$\left(\begin{bmatrix} \varphi_1(a_1) \\ \vdots \\ \varphi_m(a_1) \end{bmatrix}, \dots, \begin{bmatrix} \varphi_1(a_n) \\ \vdots \\ \varphi_m(a_n) \end{bmatrix} \right)$$

为 E -线性无关.

(iii) E^m 中的向量

$$\left(\begin{bmatrix} \varphi_1(a_1) \\ \vdots \\ \varphi_m(a_1) \end{bmatrix}, \dots, \begin{bmatrix} \varphi_1(a_n) \\ \vdots \\ \varphi_m(a_n) \end{bmatrix} \right)$$

为 F -线性无关.

证明. 我们考虑 (i) $\implies$ (ii) $\implies$ (iii) $\implies$ (i) 的顺序.

若 $(a_1, \dots, a_n)$ 为 F -线性相关, 则存在 $(u_1, \dots, u_m) \in (F^n)^*$, 满足

$$u_1 a_1 + \dots + u_n a_n = 0.$$

由于 $F = \text{Inv}(G)$, 因此, 对任意 $\varphi \in G$, 对任意 $u \in F$, 满足 $\varphi(u) = u$. 由此, 我们可得

$$u_1 \begin{bmatrix} \varphi_1(a_1) \\ \vdots \\ \varphi_m(a_1) \end{bmatrix} + \dots + u_m \begin{bmatrix} \varphi_1(a_n) \\ \vdots \\ \varphi_m(a_n) \end{bmatrix} = \begin{bmatrix} \varphi_1(u_1 a_1 + \dots + u_n a_n) \\ \vdots \\ \varphi_m(u_1 a_1 + \dots + u_n a_n) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

由于 $(u_1, \dots, u_m) \in (F^n)^*$, 因此

$$\left(\begin{bmatrix} \varphi_1(a_1) \\ \vdots \\ \varphi_m(a_1) \end{bmatrix}, \dots, \begin{bmatrix} \varphi_1(a_n) \\ \vdots \\ \varphi_m(a_n) \end{bmatrix} \right)$$

为 F -线性相关. 因此我们有 (iii) $\implies$ (i).

由于 $F \subset E$, 因此 E -线性无关可以推出 F -线性无关. 因此我们有 (ii) $\implies$ (iii).

下边我们将主要证明 (i) $\implies$ (ii).

考虑以下 E 上的线性方程组:

$$\begin{cases} \varphi_1(a_1)x_1 + \varphi_1(a_2)x_2 + \dots + \varphi_1(a_n)x_n = 0 \\ \varphi_2(a_1)x_1 + \varphi_2(a_2)x_2 + \dots + \varphi_2(a_n)x_n = 0 \\ \dots \\ \varphi_m(a_1)x_1 + \varphi_m(a_2)x_2 + \dots + \varphi_m(a_n)x_n = 0 \end{cases}$$

假设

$$\left(\begin{bmatrix} \varphi_1(a_1) \\ \vdots \\ \varphi_m(a_1) \end{bmatrix}, \dots, \begin{bmatrix} \varphi_1(a_n) \\ \vdots \\ \varphi_m(a_n) \end{bmatrix} \right)$$

为 E -线性相关, 则以上方程组在 E 中有非平凡解. 我们考虑以上方程组的解集 S , 并记 S^* 为非零解集. 定义映射

$$W: S^* \rightarrow \mathbb{N} \\ \underline{b} = (b_1, \dots, b_n) \rightarrow \#\{i \in \{1, \dots, n\} \mid b_i \neq 0\}.$$

由于 W 的值域为有限集, 因此存在 S^* 中的元素实现 $\min W$. 由于 S^* 中所有元素都至少有一个位置不为 0, 因此

$$\min W > 0.$$

令 $\underline{c} = (c_1, \dots, c_n) \in S^*$, 满足

$$W(\underline{c}) = \min W.$$

不妨设 $c_1 \neq 0$. 任取 $a \in E^*$, 我们有

$$a\underline{c} = (ac_1, \dots, ac_n) \in S^*,$$

也是以上方程组的非平凡解, 且

$$W(\underline{c}) = W(a\underline{c}).$$

因此我们可以进一步假设 $c_1 = 1$. (取 $a = c_1^{-1}$)

下证 $c_2, \dots, c_n \in F$. 任取 $\varphi \in G$, 有

$$\{\varphi \circ \varphi_1, \dots, \varphi \circ \varphi_m\} = G = \{\varphi_1, \dots, \varphi_m\}.$$

因此 φ 将方程组中的方程顺序做了置换. 因此

$$\varphi(\underline{c}) = (\varphi(1), \varphi(c_2), \dots, \varphi(c_n)),$$

也是原方程组的解. 由于 $\varphi(a) = 0$ 当且仅当 $a = 0$, 则

$$\varphi(\underline{c}) = (\varphi(1), \varphi(c_2), \dots, \varphi(c_n)) \in S^*,$$

且

$$W(\varphi(\underline{c})) = W(\underline{c}).$$

若存在 $c_i \notin F$, 不妨设 $i = 2$. 由于 $F = \text{Inv}(G)$, 因此存在 $\varphi \in G$, 满足 $\varphi(c_2) \neq c_2$. 因此我们有了一个新的解:

$$\underline{c} - \varphi(\underline{c}) = (0, c_2 - \varphi(c_2), \dots, c_n - \varphi(c_n)).$$

由于 $c_2 - \varphi(c_2) \neq 0$, 因此

$$\underline{c} - \varphi(\underline{c}) \in S^*,$$

此外由于 $\varphi(0) = 0$, 因此

$$W(\underline{c} - \varphi(\underline{c})) \leq W(\underline{c}) - 1 < W(\underline{c}).$$

这与 $\underline{c}$ 的取法矛盾. 因此 $c_2, \dots, c_n \in F$.

注意到 $id \in G$, 因此我们有

$$a_1 + c_2 a_2 + \cdots + c_n a_n = 0.$$

由于 $(1, c_2, \dots, c_n) \in (F^n)^*$, 因此

$$(a_1, \dots, a_n),$$

在 E 中 F -线性相关. 由此, 我们有 (i) $\implies$ (ii). □

利用以上命题, 我们可以证明下边的 Artin 引理及相关结论. 之后我们就可以将以上提到的结论一起整合为一个关于有限 Galois 扩张的定理.

命题 28.2.9 (Artin 引理)

设 E 为一个域, 记 $\text{Aut}(E)$ 为 E 的自同构. 设 $G < \text{Aut}(E)$ 为一个有限子群, 并记 $F = \text{Inv}(G)$. 则我们有

$$[E : F] \leq |G|.$$

注 28.2.10.

我们之前的定理讲到, 如果 $[E : F]$ 有限, 则 $|\text{Gal}(E/F)| \leq [E : F]$. 而 Artin 引理讨论的是另一个方向. 注意与之前的定理不同的是这里 F 并不是任取的, 而是 G 的不变子域.

证明. 我们记

$$G = \{\varphi_1, \dots, \varphi_m\}$$

我们考虑 E 中的非零元素:

$$a_1, \dots, a_n,$$

并考虑以下 E 上的线性方程组:

$$\begin{cases} \varphi_1(a_1)x_1 + \varphi_1(a_2)x_2 + \cdots + \varphi_1(a_n)x_n = 0 \\ \varphi_2(a_1)x_1 + \varphi_2(a_2)x_2 + \cdots + \varphi_2(a_n)x_n = 0 \\ \cdots \\ \varphi_m(a_1)x_1 + \varphi_m(a_2)x_2 + \cdots + \varphi_m(a_n)x_n = 0 \end{cases}$$

注意到若 $m < n$, 则该方程组在 E 中有非平凡解. 因此

$$\left(\begin{bmatrix} \varphi_1(a_1) \\ \vdots \\ \varphi_m(a_1) \end{bmatrix}, \dots, \begin{bmatrix} \varphi_1(a_n) \\ \vdots \\ \varphi_m(a_n) \end{bmatrix} \right)$$

为 E -线性相关. 由命题 28.2.8, 我们有 $(a_1, \dots, a_n)$ 为 F -线性相关. 因此 E 中的极大 F -线性无关组的元素个数不能超过 m , 也即 G 的元素个数. 因此我们有

$$[E : F] \leq |G|.$$

□

Artin 引理的一个推论是

推论 28.2.11

考虑 E/F 为一个域扩张. 任取 $H < \text{Gal}(E/F)$, 记 $K = \text{Inv}(H)$, 则

$$|H| = [E : K],$$

且 $H = \text{Gal}(E/K)$.

证明. 由定理 27.7.5, 我们知道

$$|H| \leq |\text{Gal}(E/K)| \leq [E : K].$$

另一方面, 由 Artin 引理, 我们知道

$$[E : K] \leq |H|.$$

因此我们有以上结论. 由于 $H < \text{Gal}(E/K)$, 且有相同的元素数目, 因此

$$H = \text{Gal}(E/K).$$

□

推论 28.2.12 (教材引理 4.6.13)

设 E/F 为有限扩张, 则映射

$$\Gamma \circ \text{Inv} : \mathcal{P}(\text{Gal}(E/F)) \rightarrow \mathcal{P}(\text{Gal}(E/F)),$$

为恒等映射 $\text{id}_{\mathcal{P}(\text{Gal}(E/F))}$.

证明. 由前一个推论, 任取 $\text{Gal}(E/F)$ 的子群 H , 记 $K = \text{Inv}(H)$ 为其不变子域. 我们有

$$H = \text{Gal}(E/K)$$

另一方面由映射 Γ 的定义, 我们总有

$$\text{Gal}(E/K) = \Gamma(K).$$

因此我们有

$$H = \Gamma(K) = (\Gamma \circ \text{Inv})(H).$$

□

注 28.2.13.

这里注意以上推论对任意有限扩张都成立, 并不仅仅是对 Galois 扩张. 从这里我们可以看出 Galois 扩张相比于一般有限扩张特殊的地方是关于另一个符合 $\text{Inv} \circ \Gamma$.

推论 28.2.14 (教材引理 4.6.12)

设 E/F 为有限扩张, 任取 $\text{Gal}(E/F)$ 的子群 H_1 和 H_2 , 若

$$\text{Inv}(H_1) \supset \text{Inv}(H_2),$$

则我们有 $H_1 < H_2$.

证明. 由

$$\text{Inv}(H_1) \supset \text{Inv}(H_2),$$

我们有

$$H_1 = \Gamma(\text{Inv}(H_1)) < \Gamma(\text{Inv}(H_2)) = H_2.$$

□

定理 28.2.15

设 E/F 为一个域的有限扩张. 以下叙述等价:

- (i) E/F 为一个 Galois 扩张;
- (ii) $|\text{Gal}(E/F)| = [E : F]$;
- (iii) 存在 $G < \text{Gal}(F/E)$, 满足 $F = \text{Inv}(G)$;
- (iv) $F = \text{Inv}(\text{Gal}(E/F))$.

证明. 注意到前两个之间的等价是定理 27.7.5 在 $L = E$ 情形下的等价叙述. 另一方面 (iii) $\implies$ (iv) 可以由以下关系得出:

$$F \subset \text{Inv}(\text{Gal}(E/F)) \subset \text{Inv}(G) = F.$$

而 (iv) $\implies$ (iii) 只需取 $G = \text{Gal}(E/F)$ 即可.

我们下边将证明 (ii) $\implies$ (iv) $\implies$ (ii).

- (1) **(ii) $\implies$ (iv)** 记中间域 $K = \text{Inv}(\text{Gal}(E/F))$. 由 (i) 和 (ii) 等价, 我们知道 E/F 为一个 Galois 扩张. 由推论 28.2.4, 我们知道 E/K 是一个 Galois 扩张, 因此

$$|\text{Gal}(E/K)| = [E : K].$$

另一方面, 由 K 和 $\text{Gal}(E/K)$ 的定义, 任取 $\varphi \in \text{Gal}(E/F)$, $\varphi|_K = \text{id}_K$, 因此

$$\varphi \in \text{Gal}(E/K).$$

因此作为 E 到自己的映射的集合, 我们有

$$\text{Gal}(E/F) \subset \text{Gal}(E/K).$$

另一方面, 由于 K 为中间域, E 的一个 K -自同构也是一个 F -自同构, 因此

$$\text{Gal}(E/K) \subset \text{Gal}(E/F)$$

因此

$$\text{Gal}(E/F) = \text{Gal}(E/K).$$

将以上信息组合在一起, 我们有

$$[E : F] = |\text{Gal}(E/F)| = |\text{Gal}(E/K)| = [E : K]$$

第一个等号, 是条件 (ii), 第二个等号是由于两个集合相等, 第三个等号是对 Galois 扩张 E/K 使用 (i) 和 (ii) 等价. 我们考虑域扩张的次数关系,

$$[E : F] = [E : K][K : F],$$

可得 $[K : F] = 1$, 因此 $K = F$.

(2) (iv) $\implies$ (ii) 我们使用 Artin 引理的推论 28.2.11, 并令 $H = \text{Gal}(E/F)$ 即可.

□

我们也可以考虑证明 (iv) $\implies$ (i).

(iv) $\implies$ (i) 的证明. 任取 $\alpha \in E$, 我们记 α 在 F 上的最小多项式为 f_α . 另一方面, 我们考虑 α 在 $\text{Gal}(E/F)$ 下作用的轨道:

$$A = \{\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r\},$$

并构造

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_r).$$

注意到任取 $\varphi \in \text{Gal}(E/F)$, 我们有

$$\{\varphi(\alpha_1), \dots, \varphi(\alpha_r)\} = \{\alpha_1, \dots, \alpha_r\},$$

又由于 f 展开后的系数都是 $\alpha_1, \dots, \alpha_r$ 的对称多项式, 因此

$$\varphi(f) = f \in E[x].$$

由于 $\text{Inv}(\text{Gal}(E/F)) = F$, 因此 $f \in F[x]$. 注意到 $f(\alpha) = 0$, 因此我们有

$$f_\alpha \mid f.$$

另一方面, 任给 F 上的不可约多项式 g , 设 g 在 E 中有根, 并记 R 为 g 在 E 中的根集. 则任取 $\varphi \in \text{Gal}(E/F)$, $\varphi(R) = R$.

由构造可知, f 在 E 中的根集为

$$A = \{\alpha_1, \dots, \alpha_r\}.$$

若 $f(x)$ 可约, 我们记 $f(x)$ 的不可约分解为

$$p_1(x) \cdots p_k(x),$$

由于 $f(x)$ 没有重根, 因此 $p_1(x), \dots, p_k(x)$ 两两不同.

分别记

$$A_1, \dots, A_k,$$

为 $p_1(x), \dots, p_k(x)$ 在 E 中的根. 若存在 $i \neq j$, 使得 A_i 和 A_j 非空, 则 A 中存在两个 $\text{Gal}(E/F)$ 作用下不变的子集, 这与 $\text{Gal}(E/F)$ 在 A 上作用是可递的 (因为 A 是一个轨道) 矛盾. 因此 $k = 1$, 多项式 $f(x)$ 不可约.

由于 $\alpha_1, \dots, \alpha_r$ 两两不同, 因此 $f(x) = f_\alpha(x)$ 可分, 由 $f(x)$ 的构造, $f(x) = f_\alpha(x)$ 在 E 中分裂.

由上可知, E/F 为一个正规可分扩张, 所以是 Galois 扩张. □

推论 28.2.16

设 E/F 为有限扩张, 任取 $\text{Gal}(E/F)$ 的子群 H , 则我们有 $E/\text{Inv}(H)$ 为一个 Galois 扩张.

证明. 我们记 $K = \text{Inv}(H)$. 考虑 $\text{Gal}(E/K) = (\Gamma \circ \text{Inv})(H)$, 注意到 $H < \text{Gal}(E/K)$, 且满足 $\text{Inv}(H) = K$, 因此 E/K 为一个 Galois 扩张. □

定理 28.2.17 (教材定理 4.5.5 Dedekind 无关性定理)

设 E/F 为一个域扩张. 记 $n \in \mathbb{N}^*$. 设 $\varphi_1, \dots, \varphi_n \in \text{Gal}(E/F)$ 为 n 个不同的同构, 则任取 $a_1, \dots, a_n \in E$, 若有映射相等

$$a_1\varphi_1 + \cdots + a_n\varphi_n = 0,$$

则 $a_1 = \cdots = a_n = 0$.

证明. 我们使用归纳法证明. 对 $n = 1$ 的情形, $\varphi \in \text{Gal}(E/F)$ 为 F -同构, 因此不是零映射, 由于 E 中没有零因子, 因此若 $a\varphi = 0$, 则有 $a = 0$.

我们假设结论对 $1 \leq k \leq n-1$ 的情形成立, 我们考虑 n 个 F -同构的情形. 记 $a_1, \dots, a_n \in E$, 满足

$$a_1\varphi_1 + \cdots + a_n\varphi_n = 0,$$

由于 $\varphi_1 \neq \varphi_n$, 因此存在 $a \in E$, 满足 $\varphi_1(a) \neq \varphi_n(a)$. 我们有如下两个等式:

$$a_1\varphi_1(a)\varphi_1(x) + \cdots + a_{n-1}\varphi_{n-1}(a)\varphi_{n-1}(x) + a_n\varphi_n(a)\varphi_n(x) = 0,$$

$$a_1\varphi_n(a)\varphi_1(x) + \cdots + a_{n-1}\varphi_n(a)\varphi_{n-1}(x) + a_n\varphi_n(a)\varphi_n(x) = 0.$$

第一个等式来自于 $\varphi_1, \dots, \varphi_n$ 均为 F -同构. 由此, 我们有

$$a_1(\varphi_1(a) - \varphi_n(a))\varphi_1(x) + \cdots + a_{n-1}(\varphi_{n-1}(a) - \varphi_n(a))\varphi_{n-1}(x) = 0,$$

考虑 $\varphi_1, \dots, \varphi_{n-1}$, 由归纳假设我们有 $a_1(\varphi_1(a) - \varphi_n(a)) = 0$, 由于 $\varphi_1(a) - \varphi_n(a) \neq 0$, 因此 $a_1 = 0$. 此时考虑

$$a_2\varphi_2 + \cdots + a_n\varphi_n = 0,$$

由归纳假设, 我们知道 $a_2 = \cdots = a_n = 0$. □

推论 28.2.18 (教材定理 4.5.6)

设 E/F 为一个域扩张. 若 $|\text{Gal}(E/F)|$ 中有 n 个不同的元素 $\varphi_1, \dots, \varphi_n$, 则 $[E : F] \geq n$.

证明. 我们假设 $[E : F] = r < n$. 设

$$a_1, \dots, a_r,$$

为 E 作为 F 线性空间的基. 考虑以下线性方程组

$$\begin{cases} \varphi_1(a_1)x_1 + \cdots + \varphi_n(a_1)x_n = 0 \\ \cdots \\ \varphi_1(a_r)x_1 + \cdots + \varphi_n(a_r)x_n = 0 \end{cases}$$

线性方程的个数小于未知数的个数, 因此有非平凡解. 记为

$$u_1, \dots, u_n \in E,$$

由 $\varphi_1, \dots, \varphi_n$ 为域同构, 任给

$$y = y_1a_1 + \cdots + y_ra_r \in E,$$

其中 $y_1, \dots, y_r \in F$, 我们有

$$\begin{aligned} & u_1\varphi_1(y) + \cdots + u_n\varphi_n(y) \\ &= u_1 \left(\sum_{i=1}^r y_i \varphi_1(a_i) \right) + \cdots + u_n \left(\sum_{i=1}^r y_i \varphi_n(a_i) \right) \\ &= y_1 \left(\sum_{i=1}^n u_i \varphi_i(a_1) \right) + \cdots + y_r \left(\sum_{i=1}^n u_i \varphi_i(a_r) \right) \\ &= 0. \end{aligned}$$

因此

$$u_1\varphi_1 + \cdots + u_n\varphi_n = 0.$$

由 Dedekind 无关性定理, 我们有

$$u_1 = \cdots = u_n = 0,$$

与 $(u_1, \dots, u_n)$ 为非零解矛盾, 因此 $[E : F] \geq n$. □

推论 28.2.19

设 E/F 为一个有限扩张, 我们有 $|\text{Gal}(E/F)| \leq [E : F]$.

注 28.2.20.

这个结论也可以由定理 27.7.5 得到.

第二十九章 Galois 基本定理

由定理 28.2.15 我们有下命题

命题 29.0.1

设 E/F 为一个有限的 Galois 扩张, 则对任意中间域 K , 我们有

- (i) $|\text{Gal}(E/K)| = [E : K]$;
- (ii) $K = \text{Inv}(\text{Gal}(E/K))$.

我们现在准备好叙述 *Galois* 基本定理.

定理 29.0.2

设 E/F 为一个有限 Galois 扩张. 我们有以下结论

- (i) 映射 Inv 和 Γ

$$\text{Inv} : \mathcal{P}(\text{Gal}(E/F)) \rightarrow \mathcal{P}(E/F), \quad \Gamma : \mathcal{P}(E/F) \rightarrow \mathcal{P}(\text{Gal}(E/F))$$

均为双射, 且满足

$$\text{Inv} \circ \Gamma = \text{id}_{\mathcal{P}(E/F)}, \quad \Gamma \circ \text{Inv} = \text{id}_{\mathcal{P}(\text{Gal}(E/F))},$$

- (ii) 任取 $\text{Gal}(E/F)$ 的子群 H , 我们有 $[\text{Gal}(E/F) : H] = [\text{Inv}(H) : F]$.
- (iii) $\text{Gal}(E/F)$ 的子群 H 为其正规子群, 当且仅当 $\text{Inv}(H)/F$ 为一个正规扩张. (因此 $\text{Inv}(H)/F$ 为一个 Galois 扩张.)

注 29.0.3.

回顾一下记号:

$$\mathcal{P}(\text{Gal}(E/F)) = \{\text{Gal}(E/F) \text{ 的子群}\}, \quad \mathcal{P}(E/F) = \{E/F \text{ 的中间域}\}.$$

定理中给出的 E/F 的中间域与 $\text{Gal}(E/F)$ 的子群的对应被称为 *Galois* 对应.

证明. (i) 中第二个关系已经在 28.2.12 中证明了. 我们考虑第一个关系. 任取 K 为 E/F 的中间域, 我们有

$$\text{Inv} \circ \Gamma(K) = \text{Inv}(\text{Gal}(E/K)) = K,$$

第二个等式是由于 E/K 为 Galois 扩张.

(ii) 任取 $\text{Gal}(E/F)$ 的子群 H , 我们记 $K = \text{Inv}(H)$. 则有

$$|\text{Gal}(E/F)| = [E : F] = [E : K][K : F] = |H|[K : F].$$

由 $|\text{Gal}(E/F)| = [\text{Gal}(E/F) : H]|H|$, 我们得到结论.

我们先证明 (iii) 中的必要性. 设 $H \triangleleft \text{Gal}(E/F)$. 因此任取 $\varphi \in \text{Gal}(E/F)$, 我们有 $\varphi H \varphi^{-1} = H$.

记 K 为 H 的不变域. 因此 $\text{Gal}(\varphi(K)/F)$ 的不变域为 $\varphi(K)$. 由于 $\varphi H \varphi^{-1} = H$, 我们有 $\varphi(K) = K$, 对任意 $\varphi \in \text{Gal}(E/F)$ 成立.

任取 $\alpha \in K$, 我们记 $f_\alpha \in F[x]$ 为 α 的最小多项式. 由于 E/F 为正规扩张, f_α 在 E 中分裂, 且 $\text{Gal}(E/F)$ 作用在 f_α 的根集上是可递的 (引理 27.6.13). 因此 f_α 在 K 中分裂. 因此 K/F 为一个正规扩张.

再证 (iii) 的充分性. 若 H 的不变域 K , 满足 K/F 为一个正规扩张, 我们有

$$H = \text{Gal}(E/K).$$

需要证明任取 $\varphi \in \text{Gal}(E/F)$, 都有 $\varphi H \varphi^{-1} = H$.

我们将证明任取 $\psi \in H$, 我们有 $\varphi \psi \varphi^{-1}|_K = \text{id}_K$. 我们只需证明任取 K 中的元素, 存在 K/F 的一个中间域 L , 满足 $\varphi \psi \varphi^{-1}|_L = \text{id}_L$.

任取 $\alpha \in K$, 我们考虑其最小多项式 $f_\alpha \in F[x]$. 记 $\alpha = \alpha_1, \alpha_2, \dots, \alpha_s$ 为 f_α 在 E 中所有的根. 由于 K/F 为正规扩张, 因此 $\alpha_1, \alpha_2, \dots, \alpha_s$ 都在 K 中. 我们考虑

$$L = F(\alpha_1, \alpha_2, \dots, \alpha_s).$$

任取 $\varphi \in \text{Gal}(E/F)$, 我们有 $\varphi(L) = L$, 且在集合

$$\{\alpha_1, \alpha_2, \dots, \alpha_s\},$$

上的作用是一个置换. 我们记这个置换为 $\sigma \in S_s$, 则有以下计算: 对任意 $1 \leq i \leq s$, 我们有

$$(\varphi \psi \varphi^{-1})(\alpha_i) = (\varphi \psi)(\alpha_{\sigma^{-1}(i)}) = \varphi(\alpha_{\sigma^{-1}(i)}) = \alpha_i.$$

因此 $\varphi \psi \varphi^{-1}|_L = \text{id}_L$. 因此 $\varphi H \varphi^{-1} \subset H$. 因此 $\varphi H \varphi^{-1} = H$. 所以 H 为 G 的一个正规子群. $\square$

推论 29.0.4

若 E/F 为一个有限 Galois 扩张, 则 E/F 有有限多个中间域.

证明. 由于 E/F 为一个有限的 Galois 扩张, 因此

$$|\text{Gal}(E/F)| = [E : F] < \infty.$$

$\text{Gal}(E/F)$ 为一个有限集, 其子群个数小于其子集个数

$$2^{|\text{Gal}(E/F)|},$$

因此有限. 由 Galois 对应, 我们知道 E/F 的中间域个数有限. $\square$

一个有无穷多个中间域的有限扩张的例子

如果我们不要求 E/F 为 Galois 扩张, 则以上结论不成立. 以下为一个反例.

我们考虑域 F 为有限域上的二元多项式环的分式域 $\mathbb{F}_p(t_1, t_2)$. 注意到 t_1 和 t_2 都是 $\mathbb{F}_p$ 上的超越元, 并且是代数无关的. 换句话说, 如果我们考虑

$$F = \mathbb{F}_p(t_1, t_2) = \mathbb{F}_p(t_1)(t_2),$$

那么 t_2 为域 $\mathbb{F}_p(t_1)$ 上的超越元 (考虑通分, 也等价于是环 $\mathbb{F}_p[t_1]$ 上的超越元).

我们考虑 F 上的二元多项式环: $F[x, y]$. 并考虑多项式

$$x^p - t_1 \text{ 和 } y^p - t_2.$$

记这两个多项式在 $F[x, y]$ 中生成的理想为

$$I = \langle x^p - t_1, y^p - t_2 \rangle.$$

我们回顾环论里的两个结论. 我们考虑交换幺环 R 上的理想 I 和 J 满足 $J \subset I$. 我们有如下商环同构:

$$R/I \cong (R/J)/(I/J).$$

以及关于多项式环的同构

$$(R/I)[x] \cong R[x]/I[x].$$

我们考虑 $F[x, y]$ 中的理想

$$J = \langle x^p - t_1 \rangle,$$

则有

$$F[x, y]/I \cong (F[x, y]/J)/(I/J).$$

另一方面, 我们有

$$F[x, y](x^p - t_1) = (F[x](x^p - t_1))[y].$$

因此, 我们有

$$F[x, y]/J \cong (F[x]/(F[x](x^p - t_1)))[y].$$

由于 $x^p - t_1 \in F[x]$ 为一个不可约元素, 且 $\text{Ch} F = p$, 因此商环

$$F[x]/(F[x](x^p - t_1))$$

是 $x^p - t_1 \in F[x]$ 的分裂域. 我们记 $\sqrt[p]{t_1} \in F[x]/(F[x](x^p - t_1))$ 为 $x^p - t_1$ 的根, 则有

$$F[x]/(F[x](x^p - t_1)) = F(\sqrt[p]{t_1}).$$

我们考虑环同态:

$$\phi: F[x][y]/J \rightarrow F(\sqrt[p]{t_1})[y].$$

由于 t_1 和 t_2 在 F 上代数无关, $y^p - t_2$ 在 $F(\sqrt[p]{t_1})$ 中没有根. 因此 $y^p - t_2 \in F(\sqrt[p]{t_1})[y]$ 不可约.

我们考虑

$$F(\sqrt[p]{t_1})[y]/\langle y^p - t_2 \rangle,$$

为 $y^p - t_2 \in F(\sqrt[p]{t_1})[y]$ 的分裂域. 我们记 $y^p - t_2$ 在 $F(\sqrt[p]{t_1})[y]/\langle y^p - t_2 \rangle$ 中的根为 $\sqrt[p]{t_2}$, 则有

$$F[x, y]/I \cong F(\sqrt[p]{t_1})(\sqrt[p]{t_2}).$$

推论 29.0.5

I 为 $F[x, y]$ 的极大理想.

命题 29.0.6

$F(\sqrt[p]{t_1}, \sqrt[p]{t_2})/F$ 有无穷多个中间域.

证明. 对任意 $a \in F$, 我们考虑 $F(a\sqrt[p]{t_1} + \sqrt[p]{t_2})$.

我们将证明任给 F 中两个元素 $a \neq b$, 我们有

$$F(a\sqrt[p]{t_1} + \sqrt[p]{t_2}) \neq F(b\sqrt[p]{t_1} + \sqrt[p]{t_2}).$$

我们使用反证法. 否则, 我们记

$$F(a\sqrt[p]{t_1} + \sqrt[p]{t_2}) = F(b\sqrt[p]{t_1} + \sqrt[p]{t_2}).$$

则有

$$(a - b)\sqrt[p]{t_1} \in F(a\sqrt[p]{t_1} + \sqrt[p]{t_2}).$$

因此 $\sqrt[p]{t_1} \in F(a\sqrt[p]{t_1} + \sqrt[p]{t_2})$, 我们进一步有 $\sqrt[p]{t_2} \in F(a\sqrt[p]{t_1} + \sqrt[p]{t_2})$. 因此

$$F(a\sqrt[p]{t_1} + \sqrt[p]{t_2}) = F(\sqrt[p]{t_1}, \sqrt[p]{t_2}).$$

有之前的讨论, 我们知道

$$[F(a\sqrt[p]{t_1} + \sqrt[p]{t_2}) : F] = [F(\sqrt[p]{t_1}, \sqrt[p]{t_2}) : F] = p^2.$$

另一方面, 考虑 Frobenius 同态, 我们有

$$(a\sqrt[p]{t_1} + \sqrt[p]{t_2})^p = a^p t_1 + t_2 \in F,$$

因此 $a\sqrt[p]{t_1} + \sqrt[p]{t_2}$ 在 F 上最小多项式的次数不超过 p . 因此

$$[F(a\sqrt[p]{t_1} + \sqrt[p]{t_2}) : F] = \deg(a\sqrt[p]{t_1} + \sqrt[p]{t_2}, F) \leq p.$$

矛盾.

因此任给 F 中元素 $a \neq b$, 我们有

$$F(a\sqrt[p]{t_1} + \sqrt[p]{t_2}) \neq F(b\sqrt[p]{t_1} + \sqrt[p]{t_2}).$$

由于 F 中有无穷多个元素, 因此 $F(\sqrt[p]{t_1}, \sqrt[p]{t_2})/F$ 有无穷多个中间域. □

第三十章 多项式的 Galois 群

设 F 为一个域, $f(x) \in F[x]$ 为一个多项式, 我们记 E 为 $f(x)$ 的分裂域. 在本节中我们总是假设 f 在 E 中**没有重根**, 则 E/F 为一个 Galois 扩张. 我们称 $G_f = \text{Gal}(E/F)$ 为多项式 f 的 Galois 群. 我们将主要讨论 $f(x)$ 与其 Galois 群 G_f 之间的关系.

30.1 多项式的 Galois 群在根集上的作用

我们记 $R = \{\alpha_1, \dots, \alpha_n\}$ 为 f 在 E 中的根的集合.

注 30.1.1.

注意到我们主要考虑 Galois 扩张, 因此我们需要假设多项式 f 可分, 若 f 在 E 中有重根, 则存在 $f \in F[x]$ 中的不可约因子 $g \in F[x]$, 满足 $g^2 \mid f$. 设在 $F[x]$ 中, 我们有 $f = g^2 h$, 则 $gh \in F[x]$ 的分裂域也为 E , 且与 f 有相同的根集 R . 因此我们主要考虑没有重根的多项式. 同时由于 f 没有重根, 我们有 $|R| = \deg f$.

引理 30.1.2

Galois 群 G_f 的任意元素都诱导 R 上为一个置换. 该对应诱导一个 G_f 到 S_n 置换群的一个群单同态.

证明. 对任意 $\alpha \in E$, 记 $f_\alpha \in F[x]$ 为 α 的最小多项式, 任取 $\varphi \in G_f$,

$$0 = \varphi(f_\alpha(\alpha)) = f_\alpha(\varphi(\alpha)).$$

因此 $\varphi(R) \subset R$. 由于 R 为一个有限集, 且 φ 为一个单射, 因此 φ 为 R 上的一个置换.

我们考虑 G_f 由 F -同构映射的复合给出的群结构, 则有以上对应为一个群同态. 另一方面, 由于 $E = F(\alpha_1, \dots, \alpha_n)$, 因此若 $\alpha_1, \dots, \alpha_n$ 的像确定, 则 F -同构确定. 因此是一个单同态. $\square$

我们之前已经证明了 $\text{Inv}(G_f) = F$. 因此对任意的 $\alpha \in E \setminus F$, 都存在一个 $\varphi \in G_f$, 满足 $\varphi(\alpha) \neq \alpha$. 考虑 φ 诱导的 $E[x]$ 的环自同构, 我们有以下引理.

引理 30.1.3

任取 $g(x) \in E[x]$, 若对任意 $\varphi \in G_f$, 都有 $\varphi(g) = g$, 那么 $g(x) \in F[x]$.

由此, 我们可以证明以下关于多项式是否可约的判别法:

命题 30.1.4

多项式 $f(x) \in F[x]$ 不可约, 当且仅当 G_f 在 R 上的作用是可递的.

设 G 为一个群, X 为一个非空集合. 设 G 在 X 上有一个群作用. 我们称 G 在 X 上的作用是**可递的** (transitive), 若对任意 $a, b \in X$, 存在 $g \in G$, 满足 $g(a) = b$ (也即 g 在 X 上的作用将 a 送到 b).

证明. 我们先假设 $f(x) \in F[x]$ 不可约, 由于 E/F 为 f 的分裂域, 我们有

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

我们在本章开头假设多项式 $f(x)$ 没有重根, 因此 $\alpha_i = \alpha_j$ 当且仅当 $i = j$.

任取 $\alpha \in R$, 我们记其在 G_f 作用下的轨道为

$$O_\alpha = G_f(\alpha) = \{\alpha = \alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_k}\}, \quad \{i_1, \dots, i_k\} \subset \{1, \dots, n\}.$$

由之前的引理, 我们知道 $O_\alpha \subset R$. 我们考虑多项式

$$g(x) = (x - \alpha_{i_1}) \cdots (x - \alpha_{i_k}) \in E[x],$$

则有任取 $\varphi \in G_f$, $\varphi(g) = g$. 因此 $g(x) \in F[x]$.

由于 $g(\alpha) = 0$, 因此在 $F[x]$ 中有 $f(x) | g(x)$. 另一方面 $1 \leq \deg g \leq \deg f$, 因此 $g = f$. 我们继而有 $O_\alpha = R$, 因此 G_f 在 R 上的作用是可递的.

现在我们假设 $f = gh$, 满足 $\deg g > 0$, 且 $\deg h > 0$, 我们取 α 为 g 的根, β 为 h 的根, 设

$$f_\alpha | g | f,$$

为 α 在 $F[x]$ 中的最小多项式,

$$f_\beta | h | f,$$

为 β 在 $F[x]$ 中的最小多项式.

如果存在一个元素 $\varphi \in G_f$, 满足 $\varphi(\alpha) = \beta$, 我们有

$$f_\alpha(x) = f_\beta(x).$$

由以上讨论知

$$f_\alpha(x)^2 | f(x) \in F[x].$$

这和我们假设 f 没有重根矛盾. 因此 G_f 在 R 上的作用不是可递的. $\square$

注 30.1.5.

我们记 S_n 由 G_f 在 R 上的作用诱导的子群为 G . 这里要注意的是, G_f 的作用可递并不意味着 $G = S_n$. 这仅仅是说, 对任意 $j \in \{1, \dots, n\}$, 存在 $\sigma \in G$, 满足 $\sigma(1) = j$.

我们下边要讨论的问题就是是否存在 $G_f \cong S_n$ 的情形. 答案是肯定的. 我们考虑 $F = \mathbb{Q}$, $f(x)$ 为一个 p 次不可约多项式, 这里 p 为一个素数. 记 E 为 f 的分裂域.

命题 30.1.6

若 $f(x)$ 有且仅有两个复根 (其他 $p - 2$ 个根为实根), 则 $G_f \cong S_p$.

证明. 这里主要用到以下一些结论:

- (i) S_p 可以有任意一个对换 (ij) 和一个 p -阶轮换生成.
- (ii) 复数域的共轭域同构诱导了 E 的一个 $\mathbb{Q}$ -同构, 且为 R 上作用为一个对换.
- (iii) 记一个复根为 α , 则 $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p \mid [E : F]$, 因此 G_f 有一个 p 阶子群是一个循环群.

□

例 30.1.7.

多项式 $x^3 - 2 \in \mathbb{Q}[x]$ 满足以上条件.

对任意 $n \in S_n$, 我们也可以将其实现为某个 Galois 扩张的 Galois 群. 记 F 为一个域. 我们考虑 F 上的 n 元有理分式域 $F(x_1, \dots, x_n)$. 考虑其中的初等对称多项式

$$\begin{aligned} p_1(x_1, \dots, x_n) &= \sum_{1 \leq i \leq n} x_i, \\ p_2(x_1, \dots, x_n) &= \sum_{1 \leq i < j \leq n} x_i x_j, \\ &\dots \\ p_n(x_1, \dots, x_n) &= x_1 \cdots x_n, \end{aligned}$$

在 F 上生成的域 $F(p_1, \dots, p_n)$. 我们有域扩张塔

$$F(x_1, \dots, x_n) / F(p_1, \dots, p_n) / F.$$

考虑 $F(p_1, \dots, p_n)$ 上的多项式

$$f(x) = x^n - p_1 x^{n-1} + \cdots + (-1)^n p_n \in F(p_1, \dots, p_n)[x].$$

注意到

$$f(x) = (x - x_1) \cdots (x - x_n) \in F(x_1, \dots, x_n)[x].$$

因此

$$F(x_1, \dots, x_n) / F(p_1, \dots, p_n),$$

为 $f(x)$ 的分裂域扩张. 由于 $x_1, \dots, x_n$ 两两不同, 因此这是一个 Galois 扩张. 利用 n 元多项式环的泛性质, 任取 σ , 我们有

$$\varphi_\sigma : F(x_1, \dots, x_n) \rightarrow F(x_1, \dots, x_n),$$

满足任取 x_i , 有 $\varphi_\sigma(x_i) = x_{\sigma(i)}$ 为一个 $F(p_1, \dots, p_n)$ -自同构. 因此任意

$$\{x_1, \dots, x_n\},$$

的置换都可以实现为一个 $\text{Gal}(F(x_1, \dots, x_n) / F(p_1, \dots, p_n))$ 的一个元素在这个集合上的限制.

另一方面, 由之前的引理

$$\text{Gal}(F(x_1, \dots, x_n) / F(p_1, \dots, p_n)),$$

通过在 $f(x)$ 的根集上的置换嵌入到 S_n 中.

综上所述, 我们有

$$\text{Gal}(F(x_1, \dots, x_n) / F(p_1, \dots, p_n)) \cong S_n.$$

注 30.1.8.

为方便讨论, 以下我们称 $F(x_1, \dots, x_n) / F(p_1, \dots, p_n)$ 为一个泛扩张.

30.2 多项式的判别式

我们考虑

$$\Delta(f) = \prod_{i < j} (\alpha_i - \alpha_j).$$

记 $\sigma \in S_n$ 为一个 n -元置换群元素, 则

$$\sigma.\Delta(f) := \prod_{i < j} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) = (-1)^{\rho(\sigma)} \Delta(f).$$

其中 $\rho(\sigma)$ 为 σ 的逆序数.

若 $\text{Ch}F = 2$, 则 $\sigma.\Delta(f) = \Delta(f)$ 对任意 $\sigma \in S_n$ 都成立.

若 $\text{Ch}F \neq 2$, 则 $\sigma.\Delta(f) = \Delta(f)$ 当且仅当 $\sigma \in A_n$.

定义 30.2.1

我们称

$$D(f) = \Delta(f)^2,$$

为多项式 f 的**判别式**.

由以上对于 $\Delta(f)$ 的讨论, 我们知道

$$\sigma.D(f) = D(f).$$

因此 $D(f) \in \text{Inv}(G_f) = F$.

命题 30.2.2

设 $\text{Ch}(F) \neq 2$, 则 $G < A_n$ 为 n -元交错群的子群当且仅当 $\Delta(f) \in F$.

证明. 我们任取 $\varphi \in G_f$, 记 $\sigma \in G$ 为 φ 诱导的 f 的根的置换,

$$\varphi(\Delta) = (-1)^{\rho(\sigma)} \Delta = \Delta.$$

由于 E/F 为 Galois 扩张, $\text{Inv}(G_f) = F$, 因此 $\Delta \in F$ 当且仅当 $\rho(\sigma)$ 为偶数, 也即 $\sigma \in A_n$. $\square$

30.3 泛扩张

本节我们讨论泛扩张. 任何有限群 G 都可以通过在 G 上的左平移作用嵌入到 n 元置换群中, 其中 $n = |G|$, 以上讨论有如下的推论.

推论 30.3.1

任取有限群 G , 存在一个 Galois 扩张 E/F , 满足 $\text{Gal}(E/F) \cong G$.

证明. 记 G 为一个有限群 n 为 G 的阶. 我们考虑对称群 S_n .

考虑以上讨论的 Galois 扩张

$$F(x_1, \dots, x_n)/F(p_1, \dots, p_n).$$

注意到

$$\text{Gal}(F(x_1, \dots, x_n)/F(p_1, \dots, p_n)) \cong S_n.$$

利用 G 在 G 上的左平移作用, 我们有群 G 同构于 S_n 的一个子群. 因此存在

$$H < \text{Gal}(F(x_1, \dots, x_n)/F(p_1, \dots, p_n)),$$

满足

$$H \cong G.$$

考虑 Galois 对应, 我们有

$$\text{Gal}(F(x_1, \dots, x_n)/\text{Inv}(H)) = H \cong G.$$

□

下设自然数 $n > 1$, 考虑 $G = A_n$ 即 n 元交错群, 我们有

$$[S_n : A_n] = 2.$$

因此利用 Galois 对应以及 Galois 扩张的性质, 我们有

$$[\text{Inv}(A_n) : F(p_1, \dots, p_n)] = [S_n : A_n] = 2.$$

考虑

$$\Delta(f) = \prod_{i < j} (x_i - x_j),$$

利用之前的讨论我们知道

$$\sigma.\Delta(f) = (-1)^{\rho(\sigma)}\Delta(f).$$

因此

$$\Delta(f) \in \text{Inv}(A_n).$$

若 $\text{Ch}F \neq 2$, 则

$$\Delta(f) \notin F(p_1, \dots, p_n).$$

这是因为

$$(12).\Delta(f) = -\Delta(f) \neq \Delta(f).$$

我们考虑扩张塔

$$\text{Inv}(A_n)/F(p_1, \dots, p_n)(\Delta(f))/F(p_1, \dots, p_n),$$

则有

$$2 = [\text{Inv}(A_n) : F(p_1, \dots, p_n)] = [\text{Inv}(A_n) : F(p_1, \dots, p_n)(\Delta(f))][F(p_1, \dots, p_n)(\Delta(f)) : F(p_1, \dots, p_n)]$$

由 $\Delta(f) \notin F(p_1, \dots, p_n)$, 我们有

$$[F(p_1, \dots, p_n)(\Delta(f)) : F(p_1, \dots, p_n)] \neq 1,$$

因此

$$[\text{Inv}(A_n) : F(p_1, \dots, p_n)(\Delta(f))] = 1,$$

这等价于

$$\text{Inv}(A_n) = F(p_1, \dots, p_n)(\Delta(f)).$$

30.4 $\mathbb{Q}$ 上的五次以下多项式的 Galois 群的分类

本节我们讨论 $\mathbb{Q}$ 上次数小于 5 的多项式的 Galois 群的分类问题.

30.4.1 一次多项式

任取 $\mathbb{Q}$ 上的一次多项式, $\mathbb{Q}$ 本身就是该多项式的分裂域. 因此其 Galois 群只有 id , 是平凡的. 当然 1 个元素的置换群是单位群.

30.4.2 二次多项式

任取 $\mathbb{Q}$ 上的二次多项式 $f(x)$, 通过配方和换元, 我们总是可以假设 $f(x)$ 有以下形式

$$f(x) = x^2 - a \in \mathbb{Q}[x].$$

取决于 a 是否可以写为一个有理数的平方, 这里有两种可能的情形需要讨论, 也分别对应 $f(x)$ 是否可约, 同时也分别对应 S_2 的仅有的两个子群 $\{e\}$ 和 S_2 .

如果 a 是一个有理数的平方, 即存在 $b \in \mathbb{Q}$, 满足 $b^2 = a$, 则 $f(x)$ 在 $\mathbb{Q}[x]$ 中有分解

$$f(x) = (x - b)(x + b) \in \mathbb{Q}[x].$$

因此其分裂域为 $\mathbb{Q}$, 其 Galois 群 G_f 为单位群.

如果 a 不是任何有理数的平方, 即不存在 $b \in \mathbb{Q}$, 满足 $b^2 = a$, 那么 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约. 我们记 $E/\mathbb{Q}$ 为 $f(x)$ 的分裂域扩张. 任取 $\alpha \in E$ 为 $f(x)$ 的根, 我们有

$$f(x) = (x - \alpha)(x + \alpha) \in \mathbb{Q}(\alpha)[x].$$

因此 $f(x)$ 在 $\mathbb{Q}(\alpha)$ 中分裂, 即有 $E = \mathbb{Q}(\alpha)$. 因此

$$|G_f| = [E : \mathbb{Q}] = \deg f(x) = 2.$$

我们有 $G_f \cong S_2$.

30.4.3 三次多项式

我们考虑 f 为一个三次多项式:

$$f(x) = x^3 + ax^2 + bx + c.$$

利用对称多项式的基本定理和韦达定理, 我们有

$$D(f) = a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2.$$

命题 30.4.1

若 f 不可约且次数为 3, 则 $G_f \cong A_3$ 或者 S_3 .

证明. 注意 $|S_3| = 6$. 因此 $|G_f| \mid 6$. 由于 f 不可约, 因此 G_f 在 f 在 E 中的根集 R 上的作用是可递的. 因此 $|G_f| \geq 3$. 因此我们有

$$G_f \cong S_3 \text{ 或者 } G_f \cong A_3.$$

□

推论 30.4.2

若 f 不可约且次数为 3, 则

(i) 若 $\sqrt{D(f)} \in F$, 则 $G_f \cong A_3$.

(ii) 若 $\sqrt{D(f)} \notin F$, 则 $G_f \cong S_3$.

推论 30.4.3

若 f 不可约且次数为 3, 则

(i) 若 $\sqrt{D(f)} \in F$, 则 $[E : F] = 3$.

(ii) 若 $\sqrt{D(f)} \notin F$, 则 $[E : F] = 6$.

注 30.4.4.

记号 $\sqrt{D(f)}$ 表示的是 $D(f)$ 在 E 中的一个二次根, 也就是一个元素 $w \in E$, 满足

$$w^2 = D(f).$$

例 30.4.5 ($f(x) = x^3 - 2 \in \mathbb{Q}[x]$).

考虑 f 的分裂域扩张 $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}$, 其中 ω 为三次本原单位根.

这里 $a = 0, b = 0, c = -2$. 我们有

$$D(f) = -27 \times 4.$$

因此 $G_f \cong S_3$. 我们记 $\varphi, \psi \in G_f$ 分别为

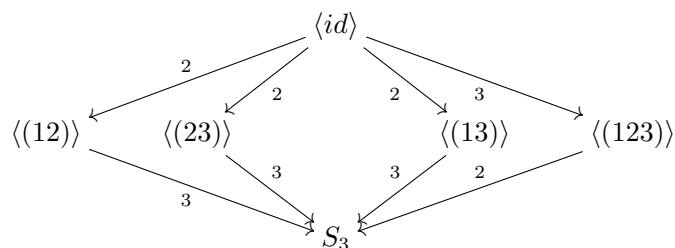
$$\varphi : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \omega \mapsto \omega^2 \end{cases} \quad \psi : \begin{cases} \sqrt[3]{2} \mapsto \omega \sqrt[3]{2} \\ \omega \mapsto \omega \end{cases}$$

Galois 群 G_f 和 S_3 之间的同构可以通过将 φ 和 ψ 分别送到 (12) 和 (123) 得到.

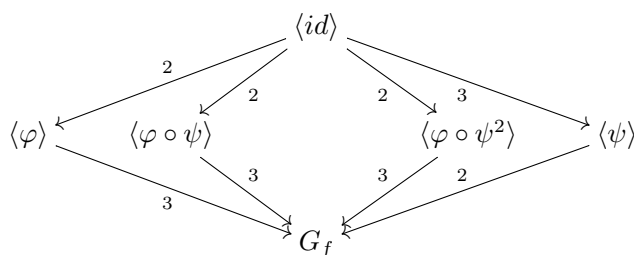
我们考虑 S_3 所有的子群如下 (用生成元表示):

$$\{\langle id \rangle, \langle (12) \rangle, \langle (23) \rangle, \langle (13) \rangle, \langle (123) \rangle, S_3\}.$$

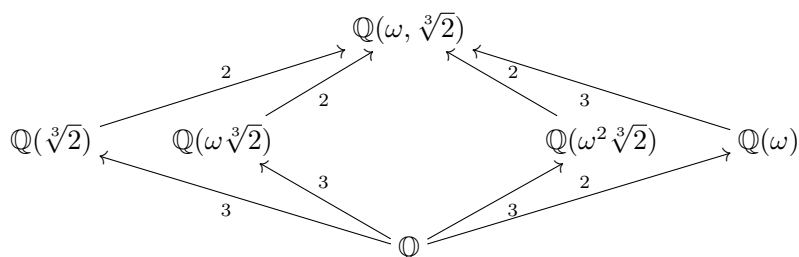
为了描述这些子群之间的关系, 我们使用以下图表:



上图可以转化为 G_f 的子群关系图



通过 Galois 对应, 我们有以下关于扩张 $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}$ 中间域的图



例 30.4.6 ($f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$).

记 $\alpha, \beta, \gamma \in \mathbb{C}$ 为 $f(x)$ 的根. 我们考虑 f 的分裂域扩张 $\mathbb{Q}(\alpha, \beta, \gamma)/\mathbb{Q}$.

这里 $a = 0, b = -3, c = 1$. 我们计算

$$D(f) = -4b^3 - 27c^2 = 81$$

由于 $\sqrt{D(f)} \in \mathbb{Q}$, 我们有 $G_f \cong A_3$. 我们知道 A_3 为一个由 (123) 生成的 3 阶循环群. 因此我们有

$$\begin{array}{c} \{id\} \\ \downarrow 3 \\ \text{Gal}(\mathbb{Q}(\alpha, \beta, \gamma)/\mathbb{Q}) \end{array}$$

对应的中间域有

$$\begin{array}{c} \mathbb{Q}(\alpha, \beta, \gamma) \\ \uparrow 3 \\ \mathbb{Q} \end{array}$$

因此扩张 $\mathbb{Q}(\alpha, \beta, \gamma)/\mathbb{Q}$ 只有平凡的中间域 $\mathbb{Q}(\alpha, \beta, \gamma)$ 和 $\mathbb{Q}$. 注意 $\mathbb{Q}(\alpha)$ 为扩张 $\mathbb{Q}(\alpha, \beta, \gamma)/\mathbb{Q}$ 的中间域, 且不同于 $\mathbb{Q}$, 因此我们有

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, \beta, \gamma).$$

因此我们知道 $\beta, \gamma \in \mathbb{Q}(\alpha)$.

我们可以进一步计算 β 和 γ 在 $\mathbb{Q}(\alpha)$ 中的表达式. 由韦达定理, 我们知道

$$\begin{cases} \alpha + \beta + \gamma = 0 \\ \alpha\beta + \alpha\gamma + \beta\gamma = -3 \\ \alpha\beta\gamma = -1 \end{cases}$$

由以上计算, 我们知道

$$\Delta(f) = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) = 9 \text{ 或者 } -9.$$

我们不妨设 $\Delta(f) = 9$, 则有

$$\beta - \gamma = \frac{9}{(\alpha - \beta)(\alpha - \gamma)} = \frac{9}{\alpha^2 - (\beta + \gamma)\alpha + \beta\gamma} = \frac{9\alpha}{2\alpha^3 - 1} = \frac{3\alpha}{2\alpha - 1}.$$

因此, 我们有

$$\beta = \frac{1}{2} \left(-\alpha + \frac{3\alpha}{2\alpha - 1} \right), \quad \gamma = \frac{1}{2} \left(-\alpha - \frac{3\alpha}{2\alpha - 1} \right)$$

使用待定系数法来计算 $(2\alpha - 1)$ 的逆. 设 $p, q, r \in \mathbb{Q}$, 满足

$$(2\alpha - 1)(p\alpha^2 + q\alpha + r) = 1.$$

则有

$$2p\alpha^3 + 2q\alpha^2 + 2r\alpha - p\alpha^2 - q\alpha - r - 1 = 2p\alpha^3 + (2q - p)\alpha^2 + (2r - q)\alpha - (r + 1) = 0$$

我们有

$$\begin{cases} 2q - p = 0 \\ \frac{2r - q}{2p} = -3 \\ \frac{-r - 1}{2p} = 1 \end{cases}$$

解得

$$p = \frac{4}{3}, \quad q = \frac{2}{3}, \quad r = -\frac{11}{3}$$

因此

$$\beta = \alpha^2 - 2, \quad \gamma = -\alpha^2 - \alpha + 2.$$

30.4.4 四次多项式

我们也可以使用类似的方法讨论四次不可约多项式, 除了判别式之外, 我们还需要一些其它的技巧.

考虑 $\mathbb{Q}$ 上多项式

$$f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Q}[x].$$

记 $E/\mathbb{Q}$ 为 f 的分裂域扩张. 由 $\text{Ch } \mathbb{Q} = 0$ 可知 $E/\mathbb{Q}$ 为一个 Galois 扩张. 我们知道 G_f 与 4-元置换群 S_4 的某个子群同构. 我们下边讨论一下 f 的 Galois 群 G_f 的分类问题.

若 f 在 E 中有重根, 则存在一个 $\mathbb{Q}$ 上的不可约多项式整除 f . 因此 f 或者可以写为 1 个 2 次多项式的平方, 或者可以写为一个 1 次多项式的平方和 1 个 2 次多项式的平方. 无论哪种情况, 我们都可以把 E 看作是一个次数更低的 $\mathbb{Q}$ 上的多项式的分裂域, 而这个已经在前边的部分讨论过了. 我们开头假设 f 在 E 中没有重根, 即 f 在 E 中有四个不同的根, 分别记为 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$.

另一方面, 若 f 可约, 则 f 可以写为两个次数大于等于 1 的多项式的乘积. 若其中一个多项式的次数为 1, 则 f 在 $\mathbb{Q}$ 中有一个根, 则 $E/\mathbb{Q}$ 是一个 3 次多项式的分裂域. 由之前的讨论, 我们已经知道了 G_f 的分类. 另一方面, f 可以分解为两个 2 次不可约多项式的情形我们将在后边讨论. 因此以下将假设 f 为 $\mathbb{Q}$ 上不可约 4 次多项式.

同时我们注意到可以通过变量替换 $x \mapsto x + \frac{q}{4}$ 将多项式 f 变为

$$x^4 + px^2 + qx + r \in \mathbb{Q}[x].$$

因此, 不失一般性地, 我们假设 f 的 3 次项系数为 0. 记 $\alpha_1, \dots, \alpha_4$ 为 f 在 E 中的根. 为避免记号过于复杂, 以下我们将 G_f 与 S_4 中对应的子群等同起来, 将 G_f 考虑为 S_4 的一个子群.

我们记

$$\beta = \alpha_1 + \alpha_2,$$

$$\gamma = \alpha_1 + \alpha_3,$$

$$\delta = \alpha_1 + \alpha_4.$$

通过直接计算, 我们可以验证:

$$\beta^2 = -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4),$$

$$\gamma^2 = -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4),$$

$$\delta^2 = -(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3).$$

记 $K = \mathbb{Q}(\beta^2, \gamma^2, \delta^2)$. 利用韦达定理, 我们可以证明 $K/\mathbb{Q}$ 为以下多项式的分裂域扩张:

$$g(x) = x^3 + 2px^2 + (p^2 - 4r)x - q^2 \in \mathbb{Q}[x].$$

并且其判别式满足 $D(g) = D(f)$. 我们称多项式 g 被称为 f 的**预解式**. 利用 $\{\beta, \gamma, \delta\}$ 与 $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ 之间的关系, 我们可以进一步证明 $E = \mathbb{Q}(\beta, \gamma, \delta)$.

由于我们只考虑 f 是不可约的情形, 因此, 我们只需要考虑 S_4 中的可递子群 (在 $\{1, 2, 3, 4\}$ 上作用是可递的), 并研究其中哪些是可以被实现为某个不可约 4 次多项式的 Galois 群.

考虑 S_4 中的子群

$$V = \langle (12)(34), (13)(24) \rangle,$$

我们称之为 **Klein 四元群** (Viergruppe or Vierergruppe). 我们可以证明 V 为 S_4 的交换的正规子群(练习). 任取 $G < S_4$, 记 $m = [G : G \cap V]$. 我们有以下结论 (证明作为练习):

- (i) 若 G 可递, 则 $|G| = 4, 8, 12$ 或 24 .
- (ii) 若 $|G| = 12$, 则 $G = A_4$.
- (iii) 若 $|G| = 8$, 则 $G \cong D_4$, 这里 D_4 为二面体群.
- (iv) 若 $|G| = 4$, 则 $G \cong \mathbb{Z}_4$ 或 $G = V$.
- (v) 我们有 $m \mid 6$.

由这些讨论, 我们可以得到所有 S_4 的可递子群. 利用之前的讨论, 我们得到以下 $\mathbb{Q}$ 上 4 次不可约多项式的 Galois 群(作为 S_4 的子群)所有可能的情形.

判别式	f	g	G_f	$m = [\mathbb{Q}(\beta^2, \gamma^2, \delta^2) : \mathbb{Q}]$
在 $\mathbb{Q}$ 中没有二次根		在 $\mathbb{Q}[x]$ 上不可约	S_4	6
在 $\mathbb{Q}$ 中有二次根		在 $\mathbb{Q}[x]$ 上不可约	A_4	3
在 $\mathbb{Q}$ 中没有二次根	在 $K[x]$ 中可约	在 $\mathbb{Q}[x]$ 上可约	$\cong \mathbb{Z}_4$	2
在 $\mathbb{Q}$ 中没有二次根	在 $K[x]$ 中不可约	在 $\mathbb{Q}[x]$ 上可约	二面体群 D_4	2
在 $\mathbb{Q}$ 中有二次根		在 $\mathbb{Q}$ 中分裂	V	1

下边考虑 f 是 $\mathbb{Q}$ 上的两个不可约多项式的乘积的情形. 在讨论一般情形之前, 我们先来看一个例子.

例 30.4.7 ($f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$).

我们考虑 f 的分裂域扩张 $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. 由之前的讨论, 我们知道

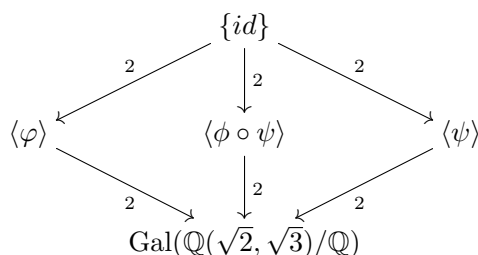
$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4.$$

(可以通过证明 $x^2 - 3$ 在 $\mathbb{Q}(\sqrt{2})[x]$ 中不可约得到.) 因此 $|\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})| = 4 = 2^2$. 因此 $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ 为一个交换群.

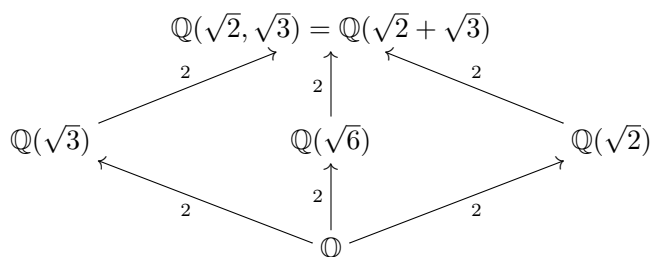
我们考虑以下两个 $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ 的元素

$$\varphi : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases}, \quad \psi : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

有以下 $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ 子群关系图:



对应的中间域的关系图如下



以上结论对一般的情形也成立. 我们考虑 $a, b \in \mathbb{Q}$, 满足 a, b, ab 都不是某个有理数的平方. 可以证明此时有

$$x^2 - b \in \mathbb{Q}(\sqrt{a})[x]$$

不可约. 因此有

$$[\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}] = 4.$$

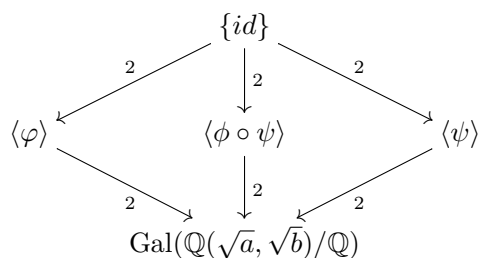
即多项式

$$(x^2 - a)(x^2 - b) \in \mathbb{Q}[x],$$

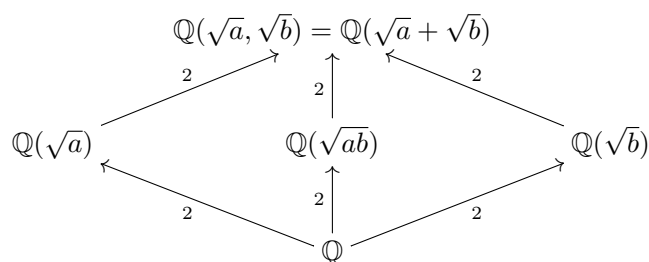
的分裂域是 $\mathbb{Q}$ 的 4 次扩张, 所以对应的 Galois 群也是 4 阶交换群. 我们进一步可以考虑以下两个 $\text{Gal}(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q})$ 的元素

$$\varphi : \begin{cases} \sqrt{a} \mapsto -\sqrt{a} \\ \sqrt{b} \mapsto \sqrt{b} \end{cases}, \quad \psi : \begin{cases} \sqrt{a} \mapsto \sqrt{a} \\ \sqrt{b} \mapsto -\sqrt{b} \end{cases}$$

有以下 $\text{Gal}(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q})$ 子群关系图:



对应的中间域的关系图如下



30.5 Galois 反问题

以上我们讨论了给定一个多项式有哪些方法可以帮助我们寻找该多项式的 Galois 群. 我们也讨论了是不是所有的有限群都可以实现为一个 Galois 扩张的 Galois 群. 我们虽然给出了正面的答案, 但是还有一些遗憾. 注意到在构造一个 Galois 群同构于一个有限群 G 的 Galois 扩张 E/F 的时候, 我们使用的域 F 是变化的. 如果我们固定一个域 F , 是否可以将任意一个有限群 G 都实现为 F 的某个 Galois 扩张呢? 这就是所谓的一个域 F 上的 Galois 反问题. 例如我们可以考虑 $\mathbb{Q}$ 上的 Galois 反问题. 这个问题目前还没有完全解决.

第三十一章 *Galois 理论与几何

在继续之前,我们先来看一个 Galois 理论应用的例子. 通过这个例子我们希望说明 Galois 理论不仅仅可以用来研究代数扩张,也可以用在超越扩张的研究中. 本节所涉及的内容也体现了 Galois 理论和几何之间的一些联系.

我们首先考虑一个简单的例子. 考虑 $\mathbb{C}(t)$ 复数域上的有理分式域,并将其看作是 $\mathbb{C}$ 的扩张. 我们考虑 $\mathbb{C}(t)$ 的 $\mathbb{C}$ -自同构

$$\varphi : \mathbb{C}(t) \rightarrow \mathbb{C}(t),$$

满足 $\varphi(t) = t^{-1}$. 注意到 $\varphi^2 = \text{id}$, 因此

$$G = \langle \varphi \rangle < \text{Gal}(\mathbb{C}(t)/\mathbb{C}),$$

是一个 2 阶子群.

考虑以下扩张塔

$$\mathbb{C}(t)/\mathbb{C}(t+t^{-1})/\mathbb{C}.$$

我们注意到 t 是多项式

$$f(x) = x^2 - (t+t^{-1})x + 1 \in \mathbb{C}(t+t^{-1})[x],$$

的一个根, 并且

$$\mathbb{C}(t) = \mathbb{C}(t+t^{-1})(t),$$

因此

$$[\mathbb{C}(t) : \mathbb{C}(t+t^{-1})] \leq 2.$$

注意到

$$\varphi(t+t^{-1}) = t+t^{-1},$$

因此我们有扩张塔

$$\mathbb{C}(t)/\text{Inv}(G)/\mathbb{C}(t+t^{-1})$$

注意到

$$\begin{aligned} & [\mathbb{C}(t) : \mathbb{C}(t+t^{-1})] \\ &= [\mathbb{C}(t) : \text{Inv}(G)][\text{Inv}(G) : \mathbb{C}(t+t^{-1})] \\ &\geq [\mathbb{C}(t) : \text{Inv}(G)] \\ &\geq |\text{Gal}(\mathbb{C}(t)/\text{Inv}(G))| \\ &\geq |G| = 2. \end{aligned}$$

因此

$$[\mathbb{C}(t) : \mathbb{C}(t+t^{-1})] = 2.$$

这也告诉我们

$$[\mathbb{C}(t) : \text{Inv}(G)] = 2 = |G|, \quad [\text{Inv}(G) : \mathbb{C}(t+t^{-1})] = 1.$$

第一个式子说明 $\mathbb{C}(t)/\text{Inv}(G)$ 是一个 Galois 扩张, 第二个式子说明

$$\text{Inv}(G) = \mathbb{C}(t + t^{-1}).$$

以上讨论可以被推广到更一般的情形. 记 F 为一个域, 我们考虑 $F(t)$ 为 F 上的有利分式域. 任取 $\alpha \in F(t) \setminus F$, 存在 $p(t), q(t) \in F[t]$, 满足

$$\alpha = \frac{p(t)}{q(t)},$$

且满足在 $F[t]$ 中有

$$\gcd(p(t), q(t)) = 1.$$

我们首先证明一个在本节讨论中常用的命题.

命题 31.0.1

任取 $\alpha \in F(t) \setminus F$, 记号 $p(t)$ 和 $q(t)$ 如上, 我们有

- (i) α 在 F 上超越;
- (ii) $p(x) - \alpha q(x) \in F(\alpha)[x]$ 在 $F(\alpha)[x]$ 上不可约;
- (iii) $[F(t) : F(\alpha)] = \max\{\deg p(t), \deg q(t)\}$.

证明. 首先证明 α 在 F 上超越. 我们将是用反证法. 假设存在 $f(x) \in F[x]^*$, 满足 $f(\alpha) = 0$. 我们记

$$f(x) = a_0 + a_1x + \cdots + a_kx^k,$$

则有

$$0 = f(\alpha) = a_0 + a_1 \frac{p(t)}{q(t)} + \cdots + a_k \left(\frac{p(t)}{q(t)} \right)^k.$$

由此可得

$$a_0q(t)^k + a_1q(t)^{k-1}p(t) + \cdots + a_kp(t)^k = 0.$$

将最后一项移到等式右边可得

$$a_0q(t)^k + a_1q(t)^{k-1}p(t) + \cdots = -a_kp(t)^k.$$

注意到以上等式左边可以被 $q(t)$ 整除, 而由于

$$\gcd(p(t), q(t)) = 1,$$

右边不能被 $q(t)$ 整除. 因此矛盾. 由此可得 α 在 F 上超越.

下边证明多项式

$$p(x) - \alpha q(x)$$

在 $F(\alpha)[x]$ 上不可约.

注意到 $F(\alpha)$ 是 $F[\alpha]$ 的分式域, 利用 Gauss 引理, 我们只需证明多项式

$$p(x) - \alpha q(x),$$

在 $(F[\alpha])[x]$ 中不能分解为两个次数大于 0 的多项式就可以了.

注意到 $F[\alpha][x]$ 可以看作是 F 上以 α 和 x 为变元的二元多项式环. 我们也可以将其看作是 $F[x]$ 上以 α 为变元的一元多项式环. 任取

$$f(x, \alpha) \in F[x, \alpha],$$

我们记

$$\deg_{\alpha} f(x, \alpha),$$

为其作为 $(F[x])[\alpha]$ 中的元素关于 α 的次数. 注意到

$$\deg_{\alpha}(p(x) - \alpha q(x)) = 1.$$

设存在 $(F[\alpha])[x]$ 中两个多项式 $g(x, \alpha)$ 和 $h(x, \alpha)$, 满足

$$p(x) - \alpha q(x) = g(x, \alpha)h(x, \alpha).$$

注意到以上多项式都非零.

我们将这些多项式看作是 α 的多项式则有

$$\deg_{\alpha}(p(x) - \alpha q(x)) = \deg_{\alpha} g(x, \alpha) + \deg_{\alpha} h(x, \alpha).$$

因此我们有

$$\deg_{\alpha} g(x, \alpha) = 0 \text{ 或者 } \deg_{\alpha} h(x, \alpha) = 0,$$

即

$$g(x, \alpha) = g(x) \in F[x] \text{ 或者 } h(x, \alpha) = h(x) \in F[x].$$

我们不妨设 $g(x, \alpha) = g(x) \in F[x]$, 则在 $F[x]$ 中有

$$g(x) \mid \gcd(p(x), q(x)) = 1.$$

因此 $g(x) \in F^*$ 即为 $F[\alpha][x]$ 中的单位. 由此可得 $p(x) - \alpha q(x)$ 在 $F(\alpha)[x]$ 中不可约.

注意到

$$p(t) - \alpha q(t) = p(t) - \frac{p(t)}{q(t)} q(t) = 0.$$

由前一个结论, 我们有

$$\text{Irr}(t, F(\alpha)) = p(t) - \alpha q(t).$$

另一方面

$$F(t) = F(\alpha)(t).$$

因此

$$[F(t) : F(\alpha)] = \deg(p(x) - \alpha q(x)).$$

由于 $\alpha \notin F$, 因此

$$\deg(p(x) - \alpha q(x)) = \max\{\deg p(x), \deg q(x)\},$$

即得结论. □

我们先看由以上命题得到的一个对本节开始所举例子的推广.

例 31.0.2.

我们考虑 $F = \mathbb{C}$ 上的有利分式域. 记 $\varphi, \psi \in \text{Gal}(\mathbb{C}(t)/\mathbb{C})$, 分别满足

$$\varphi(t) = \xi_n t \text{ 和 } \psi(t) = t^{-1},$$

其中 ξ_n 为一个 $n > 1$ 次单位根.

注意到

$$o(\varphi) = n, \quad o(\psi) = 2,$$

且

$$\psi \circ \varphi \circ \psi^{-1} = \varphi^{n-1},$$

因此

$$G = \langle \varphi, \psi \rangle < \text{Gal}(\mathbb{C}(t)/\mathbb{C}),$$

同构于 D_n 为正 n 边形对应的二面体群.

我们考虑元素

$$t^n + t^{-n} \in \mathbb{C}(t),$$

在 $\mathbb{C}$ 上生成的域, 我们有扩张塔

$$\mathbb{C}(t)/\mathbb{C}(t^n + t^{-n})/\mathbb{C}.$$

注意到

$$t^n + t^{-n} \in \text{Inv}(G),$$

因此我们有

$$\mathbb{C}(t)/\text{Inv}(G)/\mathbb{C}(t^n + t^{-n})/\mathbb{C}.$$

注意到

$$t^n + t^{-n} = \frac{t^{2n} + 1}{t^n},$$

由之前的明天, 我们有

$$[\mathbb{C}(t) : \mathbb{C}(t^n + t^{-n})] = 2n.$$

由于

$$G < \text{Gal}(\mathbb{C}(t)/\text{Inv}(G)),$$

因此

$$[\mathbb{C}(t) : \text{Inv}(G)] \geq |\text{Gal}(\mathbb{C}(t)/\text{Inv}(G))| \geq 2n.$$

利用扩张次数的关系

$$[\mathbb{C}(t) : \mathbb{C}(t^n + t^{-n})] = [\mathbb{C}(t) : \text{Inv}(G)][\text{Inv}(G) : \mathbb{C}(t^n + t^{-n})],$$

我们有

$$[\mathbb{C}(t) : \text{Inv}(G)] = 2n = |G|, \quad [\text{Inv}(G) : \mathbb{C}(t^n + t^{-n})] = 1.$$

第一个等式告诉我们 $\mathbb{C}(t)/\text{Inv}(G)$ 是 Galois 扩张, 第二个等式告诉我们

$$\text{Inv}(G) = \mathbb{C}(t^n + t^{-n}).$$

以上可以被用来研究 $\text{Gal}(F(t)/F)$ 的有限子群. 以下讨论将告诉我们, 这也等价于研究 $\text{PGL}(2, F)$ 的有限子群. 我们记

$$\text{GL}(2, F) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in F, \quad ad - bc \in F^* \right\}.$$

以下命题将该群和 $\text{Gal}(F(t)/F)$ 联系起来.

命题 31.0.3

考虑 F 的有利分式域扩张 $F(t)/F$, 我们有以下结论

(i) 任取 $A \in \text{GL}(2, F)$, 我们记

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

则

$$\begin{aligned} \varphi_A : F(t) &\rightarrow F(t), \\ \frac{p(t)}{q(t)} &\mapsto \frac{p\left(\frac{at+b}{ct+d}\right)}{q\left(\frac{at+b}{ct+d}\right)}. \end{aligned}$$

定义 $F(t)$ 上的一个 F -自同构.

(ii) 以下定义一个群满同态

$$\begin{aligned} \Phi : \text{GL}(2, F) &\rightarrow \text{Gal}(F(t)/F), \\ A &\mapsto \varphi_{A^{-1}}. \end{aligned}$$

(iii) 同态 Φ 的核为

$$\ker \Phi = \{aI_2 \mid a \in F^*\},$$

其中 I_2 为 F 系数的 2 阶单位方阵.

证明. 第一个结论直接验证可得, 我们在此略过. (注意域上方阵可逆当且仅当方阵行列式可逆)

以上定义 Φ 为一个群同态可以直接验证, 我们在此略过. 下边将主要证明 Φ 是一个满同态. 任取

$$\varphi \in \text{Gal}(F(t)/F),$$

我们考虑扩张塔

$$F(t)/F(\varphi(t))/F.$$

注意到 $\varphi(t) \notin F$, 我们记

$$\varphi(t) = \frac{p(t)}{q(t)},$$

满足 $p(t)$ 和 $q(t)$ 都是 $F[t]$ 中元素且互素.

由之前的命题知道

$$[F(t) : F(\varphi(t))] = \max\{\deg p(t), \deg q(t)\}.$$

由于 φ 为域同构, 因此

$$[F(t) : F(\varphi(t))] = 1.$$

我们有

$$p(t) = at + b, \quad q(t) = ct + d.$$

其中 $a, b, c, d \in F$.

注意到 $ad - bc = 0$, 则有 $p(t)/q(t) \in F$, 与 $F(t) = F(\varphi(t))$ 矛盾, 因此取

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

则有 $\varphi = \varphi_A$.

最后一个结论直接验证可得, 证明在此略过. $\square$

推论 31.0.4

我们有群同构

$$\text{Gal}(F(t)/F) \cong \text{PGL}(2, F).$$

注 31.0.5.

注意到群 $\text{PGL}(2, F)$ 可以通过分式线性变换作用在 $F \cup \{\infty\}$. 以上讨论反映了 Galois 理论与几何之间一些联系. 关于这部分延申内容可以搜索 Invariant Theory. 我们这里可以先给出一些观察使我们对这个联系有一个初步的印象.

我们考虑 $\text{PGL}(2, \mathbb{C})$ 中的三个元素

$$A_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}.$$

记

$$G = \langle A_1, A_2, A_3 \rangle.$$

我们可以验证 $G \cong S_4$. 考虑分式线性变换, 我们可以看到 G 在 $\hat{\mathbb{C}}$ 上的作用可以诱导一个在

$$S = \{0, 1, -1, i, -i, \infty\},$$

上的作用. 这个集合在几何上有一定的特殊性. 一方面, 我们将 $\mathbb{C}$ 看作 $\mathbb{R}^2$ 作为

$$\mathbb{R}^3 = \{(a, b, c) \mid a, b, c \in \mathbb{R}\},$$

中的 (a, b) -平面, 则 S 是以 $(\pm 1, 0, 0)$, $(0, \pm 1, 0)$ 和 $(0, 0, \pm 1)$ 为顶点的八面体在对 (a, b) -平面做球极投影时的像. 另一方面, 从三维双曲几何的角度, 这是一个正双曲八面体的 6 个顶点.

之前得到的群 G 实际上对应的是以上提到的双曲八面体的对称群. 通过考虑双曲八面体和欧式八面体顶点之间的对应, G 也同构于以上提到的 $\mathbb{R}^3$ 中八面体的对称群.

考虑群同构

$$\text{Gal}(\mathbb{C}(t)/\mathbb{C}) \cong \text{PGL}(2, \mathbb{C}),$$

我们分别记 A_1, A_2 和 A_3 对应 Galois 群中元素为 f_1, f_2 和 f_3 , 并记

$$H = \langle f_1, f_2, f_3 \rangle < \text{Gal}(\mathbb{C}(t)/\mathbb{C}).$$

我们可以证明

$$\text{Inv}(H) = \mathbb{C} \left(\frac{(t^8 + 14t^4 + 1)^3}{t^4(t^4 - 1)^4} \right).$$

之前的讨论告诉我们

$$[\mathbb{C}(t) : \text{Inv}(H)] = \max\{\deg(t^8 + 14t^4 + 1)^3, \deg t^4(t^4 - 1)^4\} = 24 = |S_4| = |H|.$$

因此 $\mathbb{C}(t)/\text{Inv}(H)$ 是一个 Galois 扩张, Galois 群为 H .

当我们看到这个结论的时候第一个反应可能是, 这个生成元

$$\frac{(t^8 + 14t^4 + 1)^3}{t^4(t^4 - 1)^4},$$

是怎么找到的. 具体过程会比较复杂, 但是我们可以注意到一点, 那就是以上提到的 $\mathbb{R}^3$ 中的八面体的八个面都是正三角形, 而当我们首先从 $\mathbb{R}^3$ 的单位球中心出发将八个面的中心投射到单位球面上, 然后通过球极投影将单位球面上这八个点投射到 $\hat{\mathbb{C}}$ 的时候, 所得的 8 个点是

$$t^8 + 14t^4 + 1,$$

在 $\mathbb{C}$ 上的 8 个根.

第三十二章 有限域

本节我们主要讨论有限域的情形. 因此本节讨论的域的素域都与某个 $\mathbb{F}_p$ 同构, 因此都可看作是某个 $\mathbb{F}_p$ 的有限扩张.

32.1 有限域的描述

我们首先对有限域作为一个有限集的势做一个描述.

命题 32.1.1

设 E 为一个有限域, 且 $\text{Ch}E = p \neq 0$. 则存在一个 $n \in \mathbb{N}$, 满足 $|E| = p^n$.

证明. 由于 E 为 $\mathbb{F}_p$ 的一个有限扩张, 因此存在 $n = [E : \mathbb{F}_p]$. 设 $\alpha_1, \dots, \alpha_n \in E$ 为 E 的一组 F -基. 作为 $\mathbb{F}_p$ -线性空间, 我们可以将 E 写为

$$E = \mathbb{F}_p\alpha_1 \oplus \cdots \oplus \mathbb{F}_p\alpha_n.$$

因此 $|E| = p^n$. □

命题 32.1.2

任取 $n \in \mathbb{N}^*$, 我们考虑 $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. 则 $f(x)$ 的分裂域 E 满足

$$|E| = p^n.$$

证明. 我们首先证明 $f(x)$ 无重根. 只需考虑其形式微商, 我们有

$$Df(x) = -1.$$

因此 $f(x)$ 和 $Df(x)$ 没有公共根. 因此 $f(x)$ 无重根, $f(x)$ 可分. 设 E/F 为 $f(x)$ 的分裂域, 因此 E/F 为 Galois 扩张.

记 R 为 $f(x)$ 的根的集合.

$$R := \{\alpha \in E \mid \alpha^{p^n} = \alpha\}.$$

因此 $E = F(R)$.

我们考虑 Frobenius 同态映射, 则对任意 $\alpha \in E$, 我们有 $\alpha \in R$ 当且仅当 $\text{Fr}^n(\alpha) = \alpha$. 因此 R 是 Fr^n 生成 G_f 的子群的不变子域, 因此为 $E/\mathbb{F}_p$ 的一个中间域, 且包含 $f(x)$ 在 E 中所有的根. 因此 $R = E$. 我们有 $|E| = p^n$. □

注 32.1.3.

在这个证明中, 我们已经看到作为 G_f 的元素,

$$\text{Fr}^n = \text{id}.$$

因此 Fr 的阶整除 n . 在下一节的讨论中, 我们会看到实际上 Fr 的阶就是 n .

我们下边要说明在同构意义下 $f(x)$ 的分裂域 E 是唯一的 p^n 阶有限域.

命题 32.1.4

设 K 为一个有限域, 满足 $|K| = p^n$, 则 K 同构于 $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ 的分裂域 E .

证明. 由于 $|K| = p^n$, 因此 $\text{Ch}K \mid p^n$, 因此 $\text{Ch}K = p$. 其次, 我们考虑乘法群 K^* , 有 $p^n - 1$ 个元素, 因此所有 K^* 中元素的阶都整除 $p^n - 1$, 也即任取 $\alpha \in K^*$, 我们有

$$\alpha^{p^n - 1} = 1.$$

等价的, 我们有

$$\alpha^{p^n} = \alpha.$$

另一方面, 我们总有 $0^{p^n} = 0$. 因此 K 为 $\mathbb{F}_p$ 的扩张, 且 $f(x)$ 在 K 中有 p^n 个根, 因此在 K 中分裂. 又由于 $|K| = p^n$, 因此 K 为 $f(x)$ 的分裂域. $\square$

推论 32.1.5

记 p 为一个素数, $n \in \mathbb{N}^*$. 设 E 为一个有限域, 满足 $|E| = p^n$. 则 $E/\mathbb{F}_p$ 为一个 Galois 扩张.

或者更一般的, 我们有

推论 32.1.6

若 L/K 为一个域扩张, 且 $|L| < \infty$, 则 L/K 为一个 Galois 扩张.

32.2 有限域的同构群

我们下边考虑一个特征为 $p \neq 0$ 的有限域 E 的同构群 $\text{Aut}(E) = \text{Gal}(E/\mathbb{F}_p)$ 的性质. 我们考虑 E^* . 这是一个乘法群, 满足交换且有限. 由有限生成交换群的结构定理, 我们知道

$$E^* \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_s},$$

满足 $d_1, \dots, d_s \in \mathbb{N} \setminus \{0, 1\}$, 且 $d_1 \mid d_2 \mid \cdots \mid d_s$.

因此对任意 $\alpha \in E^*$, 我们有 $\alpha^{d_s} = 1$. 进一步, 我们有 d_s 为最小的满足这个性质的自然数.

命题 32.2.1

设 E 为一个域, G 为 E^* 的一个有限子群, 则 G 是一个循环群.

证明. 由有限生成交换群的分类可知, 存在一个 $d_s \in \mathbb{N}^*$, 为最小的满足任意一个元素 $\alpha \in G$, 都有 $\alpha^{d_s} = 1$. 因此 G 中元素是 $x^{d_s} - 1 \in E[x]$ 的根. 由于多项式 $x^{d_s} - 1$ 最多有 d_s 个根, 因此 $|G| \leq d_s$. 另一方面, 存在 $\alpha \in G$, 满足 α 的阶为 d_s , 因此 $|G| \geq d_s$.

综上所述, 我们知道 $|G| = d_s$, 且存在元素 $\alpha \in G$, 满足 $G = \langle \alpha \rangle$ 为一个循环群. $\square$

推论 32.2.2

设 E 为一个有限域, 则 E^* 为一个循环群.

注 32.2.3.

注意到之前的讨论实际上说明 E^* 中的元素实际上是多项式

$$x^{p^n-1} - 1 \in \mathbb{F}_p[x],$$

的根的集合. 后边当我们开始讨论分圆扩张的时候, 这样的元素称为 $\mathbb{F}_p$ 上的单位根. 以上推论说明存在一个阶为 (p^n-1) 的单位根, 在后边分圆扩张的讨论中, 我们将称之为 (p^n-1) -阶本原单位根.

推论 32.2.4

记 p 为一个素数, $n \in \mathbb{N}^*$. 设 E 为一个有限域, 满足 $|E| = p^n$. 则 $\text{Aut}(E) = \text{Gal}(E/\mathbb{F}_p)$ 为一个阶为 n 的循环群, 且生成元为 Fr .

证明. 由 Galois 扩张的性质, 我们有

$$|\text{Aut}(E)| = [E : \mathbb{F}_p] = n.$$

我们记 d 为 Fr 在 $\text{Aut}(E)$ 中的阶. 注意到任取 $\alpha \in E$, $\text{Fr}^n(\alpha) = \alpha^{p^n} = \alpha$. 因此 $d \leq n$. 另一方面, 由于 E^* 为循环群, 存在阶为 $p^n - 1$ 的元素. 因此 $n \leq d$. 所以 $d = n$. 由于 $|\text{Aut}(E)| = n$, 因此 Fr 生成 $\text{Aut}(E)$ 且阶为 n . $\square$

有限域 E 的单位群为一个循环群的另一个推论如下.

推论 32.2.5

记 p 为一个素数. 设 E 为 $\mathbb{F}_p$ 的一个有限扩张, 则存在 $\alpha \in E$, 满足 $E = \mathbb{F}_p(\alpha)$, 也即 E 为一个单扩张.

证明. 由于 E^* 为一个循环群, 我们考虑 E^* 的生成元记为 α . 注意到对任意 $\beta \in E^*$, 存在 $k \in \mathbb{N}^*$, 满足

$$\beta = \alpha^k,$$

因此 $E = \mathbb{F}_p(\alpha)$. $\square$

我们可以将其进一步推广为

推论 32.2.6

设 E/F 为一个域扩张, 且 E 有限, 则存在 $\alpha \in E$, 满足 $E = F(\alpha)$.

考虑有限域的子域, 我们有如下结论.

推论 32.2.7

记 p 为一个素数, $n \in \mathbb{N}^*$. 设 E 为一个有限域, 满足 $|E| = p^n$.

- (i) 任取 F 为 E 的一个子域, 则存在 $m \in \mathbb{N}^*$, 满足 $m \mid n$, 且 $|F| = p^m$.
- (ii) 任取 $m \in \mathbb{N}^*$, 满足 $m \mid n$, 存在 E 的一个子域 F , 满足 $|F| = p^m$.

证明. (i) 不妨设 E 为 $\mathbb{F}_p$ 的扩张. 由于 $|E| = p^n$, 我们有

$$[E : \mathbb{F}_p] = n.$$

任取 E 的一个子域 F , 则 F 为 $E/\mathbb{F}_p$ 的中间域. 由域有限扩张的次数关系, 我们有

$$[E : \mathbb{F}_p] = [E : F][F : \mathbb{F}_p].$$

因此存在一个非零自然数 $m = [F : \mathbb{F}_p]$, 满足 $|F| = p^m$. 同时, 由次数关系我们有 $m \mid n$.

(ii) 我们考虑域扩张 $E/\mathbb{F}_p$. 由之前的讨论我们知道这是一个 Galois 扩张. 因此我们有 $E/\mathbb{F}_p$ 的中间域与 Galois 群 $\text{Gal}(E/\mathbb{F}_p)$ 之间的一一对应.

由之前的讨论, 我们知道

$$\text{Gal}(E/\mathbb{F}_p) \cong \mathbb{Z}_n.$$

因此 $\text{Gal}(E/\mathbb{F}_p)$ 与 $\mathbb{Z}_n$ 的子群有一一对应. 因此任取非零自然数 $m \mid n$, 我们有 $\text{Gal}(E/\mathbb{F}_p)$ 的一个 n/m 阶子群 H . 记 H 的不变子域, 也就是其对应的中间域为 F .

由于 $[\text{Gal}(E/\mathbb{F}_p) : H] = [F : \mathbb{F}_p]$, 因此 $|F| = p^m$. □

注 32.2.8.

我们有以下一些列的一一对应:

$$\{E/\mathbb{F}_p \text{ 的中间域}\} \xleftrightarrow{1:1} \{\text{Gal}(E/\mathbb{F}_p) \text{ 的子群}\} \xleftrightarrow{1:1} \{\mathbb{Z}_n \text{ 的子群}\}$$

另一方面, 我们也可以得到 E^* 生成元的一些信息.

推论 32.2.9

记 p 为一个素数. 任取 $n \in \mathbb{N}^*$, 存在 $f(x) \in \mathbb{F}_p[x]$, 满足 $f(x)$ 不可约, 且次数为 n .

证明. 任取 $n \in \mathbb{N}^*$, 由之前的结论可知, 存在一个 $\mathbb{F}_p$ 的扩张 E , 满足 $|E| = p^n$.

又由于有限域的单位群为循环群, 因此存在 $\alpha \in E$ 为 E^* 的生成元, 且满足 $E = \mathbb{F}_p(\alpha)$.

由于 $[E : \mathbb{F}_p] = n$, 因此 $\deg(\alpha, \mathbb{F}_p) = n$. 考虑 α 在 $\mathbb{F}_p$ 上的最小多项式 f , 即为所求. □

推论 32.2.10

记 p 为一个素数. 任取 $n \in \mathbb{N}^*$, 任取 $f(x) \in \mathbb{F}_p[x]$ 次数为 n 且不可约, 则在 $\mathbb{F}_p[x]$ 中有

$$f(x) \mid x^{p^n} - x.$$

证明. 由 f 不可约, 我们考虑

$$E := \mathbb{F}_p[x]/\langle f \rangle,$$

则有

$$[E : \mathbb{F}_p] = \deg f = n.$$

因此 E 中元素都是 $x^{p^n} - x$ 的根.

另一方面, 我们取 $\alpha = x + \langle f \rangle \in E$ 为 f 的根. 由 f 不可约知

$$f(x) \mid x^{p^n} - x.$$

□

我们进一步有

推论 32.2.11

记 p 为一个素数. 任取 $m, n \in \mathbb{N}^*$, 满足 $m \mid n$, 任取 $f(x) \in \mathbb{F}_p[x]$ 次数为 m 且不可约, 则在 $\mathbb{F}_p[x]$ 中有

$$f(x) \mid x^{p^n} - x.$$

证明. 我们考虑

$$K := \mathbb{F}_p[x]/\langle f \rangle,$$

满足 $[K : \mathbb{F}_p] = m$. 因此 $|K| = p^m$. 记 α 为 f 在 K 中的根.

我们记 $E/\mathbb{F}_p$ 为 $x^{p^n} - x \in \mathbb{F}_p[x]$ 分裂域扩张. 由之前推论 32.2.7, 我们知道 E 中有一个子域 L 满足 $|L| = p^m$.

由命题 32.1.4, 存在一个域同构

$$\iota : K \rightarrow L.$$

注意到 $\mathbb{F}_p$ 为 K 和 L 的素域, ι 限制在 $\mathbb{F}_p$ 上是恒等映射. 因此考虑 ι 诱导的 $K[x]$ 到 $L[x]$ 的环同构, ι 固定 $\mathbb{F}_p[x]$ 中的多项式.

因此 L 中存在元素 $\beta = \iota(\alpha)$ 也是 $\iota(f) = f$ 的根. 另一方面, β 是 $x^{p^n} - x$ 的根. 因此我们有

$$f \mid x^{p^n} - x.$$

□

以上讨论可以给我们以下推论:

推论 32.2.12

有限域上的多项式都可分. 因此有限域都是完备域.

证明. 由之前两个关于 $\mathbb{F}_p$ 上不可约多项式的讨论, 我们注意到, 由于

$$x^{p^n} - x \in \mathbb{F}_p[x],$$

可分, 因此任意因子也可分. 因此 $\mathbb{F}_p$ 上多项式都可分.

任取 F 为 $\mathbb{F}_p$ 的一个有限扩张, 任取 $f \in F[x]$ 不可约. 记 E/F 为 f 的分裂域扩张. 记 $\alpha \in E$ 为 f 的一个根. 记 $g \in \mathbb{F}_p[x]$ 为 α 在 $\mathbb{F}_p$ 上的最小多项式. 因此在 $E[x]$ 中, 我们有

$$f(x) \mid g(x).$$

由于 g 可分, 因此 f 可分. □

推论 32.2.13

记 p 为一个素数. 任取 $n \in \mathbb{N}^*$, 记

$$\Omega_n := \{f \in \mathbb{F}_p[x] \mid f \text{ 不可约, 且次数为 } d \in \mathbb{N}^*, \text{ 满足 } d \mid n\},$$

我们有

$$x^{p^n} - x = \prod_{f \in \Omega_n} f(x).$$

证明. 任取 $f(x) \in \mathbb{F}_p[x]$ 不可约, 满足 $\deg f = d$, 且 $d \mid n$, 由之前的推论, 我们知道

$$f(x) \mid x^{p^n} - x.$$

因此 Ω_n 包含在 $x^{p^n} - x$ 的不可约因子的集合中.

另一方面, 任取 $f(x) \in \mathbb{F}_p[x]$ 不可约, 且满足

$$f(x) \mid x^{p^n} - x.$$

我们有一列域扩张 $E/K/\mathbb{F}_p$, 满足 $K/\mathbb{F}_p$ 为 f 的分裂域, $E/\mathbb{F}_p$ 为 $x^{p^n} - x$ 的分裂域. 因此我们有

$$|K| = p^d,$$

满足 $d \mid n$. 因此 $\deg f \mid n$. 由此, 我们得到 $x^{p^n} - x$ 的不可约因子的集合包含在 Ω_n 中.

因此 $x^{p^n} - x$ 的不可约因子的集合等于 Ω_n . 注意到 $x^{p^n} - x \in \mathbb{F}_p[x]$ 没有重根, 因此所有的不可约因子的次数都为 1. 因此我们有

$$x^{p^n} - x = \prod_{f \in \Omega_n} f(x).$$

□

任取素数 p 和非零自然数 n , 通常我们使用记号 $\mathbb{F}_{p^n}$ 来记有 p^n 个元素的域.

注 32.2.14.

由于有 p^n 个元素的域在同构意义下唯一, 因此我们这样做是有意义的. 另一方面, 我们需要注意的是, 当 $n > 1$ 时, 这个记号和 $\mathbb{Z}_{p^n}$ 代表的意义是不同的.

我们将给出一些例子来说明以上结论.

例 32.2.15 ($\mathbb{F}_4$).

我们考虑 $\mathbb{F}_2$ 上的一个不可约多项式

$$f(x) = x^2 + x + 1 \in \mathbb{F}_2[x].$$

因此我们有

$$\mathbb{F}_4 \cong \mathbb{F}_2[x]/\langle f(x) \rangle.$$

我们记 $\alpha \in \mathbb{F}_4$ 为 $f(x)$ 的一个根, 则

$$\alpha^2 + \alpha + 1 = 0.$$

因此

$$\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}.$$

注意到

$$\mathbb{F}_4^* \cong \mathbb{Z}_3.$$

这里我们考虑 α 的各个次方:

$$\alpha^1 = \alpha, \quad \alpha^2 = \alpha + 1, \quad \alpha^3 = \alpha^2 + \alpha = 1.$$

因此 α 为 $\mathbb{F}_4^*$ 的生成元.

我们考虑 $x^4 - x$, 则在 $\mathbb{F}_2[x]$ 中, 我们有分解

$$x^4 - x = x(x-1)(x^2 + x + 1).$$

注意到在 $\mathbb{F}_2[x]$ 中, 我们有

$$x^2 + 1 = (x+1)^2.$$

因此 $x^4 - x$ 的不可约因子就是所有 $\mathbb{F}_2[x]$ 中次数被 2 整除的不可约因子.

这其中, 我们注意到

$$x^2 - x \mid x^4 - x.$$

这是由于 $\mathbb{F}_2 \subset \mathbb{F}_4$ 是一个子域.

注 32.2.16.

当我们考虑特征为 2 的域 F 的时候, 任给 $\alpha \in F$, 我们有

$$\alpha = -\alpha.$$

例 32.2.17 ($\mathbb{F}_8$).

我们考虑 $\mathbb{F}_8$. 这是 $x^3 - x \in \mathbb{F}_2[x]$ 的分裂域. 在 $\mathbb{F}_2[x]$ 中, 我们有

$$x^8 - x = x(x-1)(x^3 + x^2 + 1)(x^3 + x + 1) \in \mathbb{F}_2[x].$$

记 $x^3 + x + 1$ 在 $\mathbb{F}_8$ 中的根为 β , 则有

$$\beta^3 + \beta + 1 = 0.$$

我们将 $\mathbb{F}_8$ 中的元素用 β 表达如下:

$$\mathbb{F}_8 = \{0, 1, \beta, \beta + 1, \beta^2, \beta^2 + 1, \beta^2 + \beta, \beta^2 + \beta + 1\}.$$

考虑单位群, 我们有 $\mathbb{F}_8^* \cong \mathbb{Z}_7$. 考虑 β 的各个次方:

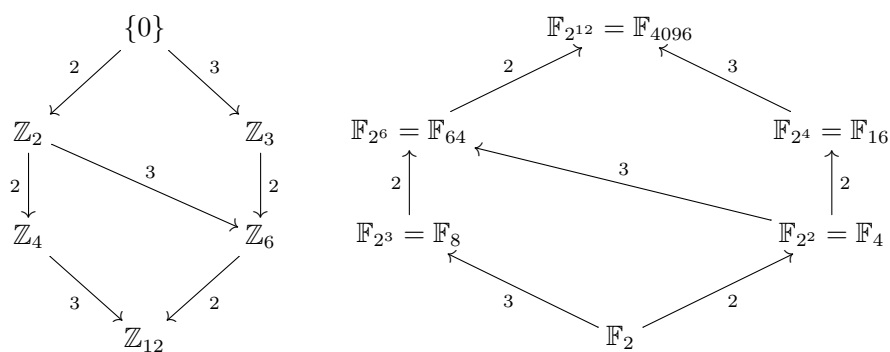
$$\begin{aligned}\beta^1 &= \beta \\ \beta^2 &= \beta^2 \\ \beta^3 &= \beta + 1 \\ \beta^4 &= \beta^2 + \beta \\ \beta^5 &= \beta^2 + \beta + 1 \\ \beta^6 &= \beta^2 + 1 \\ \beta^7 &= \beta^3 + \beta = 1\end{aligned}$$

观察 $x^8 - x \in \mathbb{F}_2[x]$ 素因子分解, 我们并没有找到 $x^4 - x$ 的分解, 这是由于 $8 = 2^3$. 因此 $\mathbb{F}_8$ 的子域元素个数, 或者为 2^1 或者为 2^3 . 而 $2 \nmid 3$, 因此 $\mathbb{F}_4$ 不是 $\mathbb{F}_8$ 的子域. 另一方面, 我们仍可找到 $x^2 - x$, 因为 $\mathbb{F}_2$ 为 $\mathbb{F}_8$ 的子域.

由前边的讨论, 我们知道任意有限域关于其任意素域都是 Galois 扩张, 并且 Galois 群是一个循环群.

例 32.2.18 ($\mathbb{F}_{2^{12}} = \mathbb{F}_{4096}$).

我们知道 $\text{Gal}(\mathbb{F}_{2^{12}}/\mathbb{F}_2) \cong \mathbb{Z}_{12}$. 由此, 我们可以得到 Galois 群的子群的图以及对应的 $\mathbb{F}_{2^{12}}/\mathbb{F}_2$ 中间域的图.



第三十三章 本原元

33.1 本原元的定义

考虑一个代数扩张 E/F .

定义 33.1.1

若存在 $\alpha \in E$, 满足 E 为 α 在 F 的单扩张, 我们称 α 为 E/F 的**本原元**.

尽管看起来使用一个元素来扩张似乎是有限扩张中一个比较特殊的情形, 下边的定理告诉我们, 实际上在讨论可分扩张的时候, 所有有限扩张都是单扩张. 本节中我们将证明如下定理:

定理 33.1.2

设 F 为一个域, E/F 为一个有限可分扩张. 则 E/F 为一个单扩张, 也即存在 $\alpha \in E$, 满足 $E = F(\alpha)$.

我们首先证明以下命题.

命题 33.1.3

设 E/F 为一个域代数扩张. 则 E/F 为一个单扩张当且仅当 E/F 的中间域个数有限.

证明. 首先证明 E/F 的中间域有限, 则 E/F 为单扩张. 若 F 为有限域, 则上节中我们已经证明 E/F 为单扩张. 因此只需考虑 F 无限的情形.

注意到由中间域有限可得 $[E : F] < \infty$, 否则我们可以找到 F -维数越来越大的无穷多个中间域, 矛盾.

由于 E/F 为有限扩张, 因此可以找到 $\alpha_1, \dots, \alpha_n \in E$, 满足 $E = F(\alpha_1, \dots, \alpha_n)$. 任取 $\beta \in F$, 我们考虑中间域

$$F(\alpha_1 + \beta\alpha_2, \alpha_3, \dots, \alpha_n).$$

注意到 $|F| = \infty$, 而 E/F 只有有限多个中间域, 因此存在 $\beta, \gamma \in F$ 不同的元素, 满足

$$K = F(\alpha_1 + \beta\alpha_2, \alpha_3, \dots, \alpha_n) = F(\alpha_1 + \gamma\alpha_2, \alpha_3, \dots, \alpha_n).$$

因此

$$\alpha_2 = (\beta - \gamma)^{-1}((\alpha_1 + \beta\alpha_2) - (\alpha_1 + \gamma\alpha_2)) \in K$$

因此 $K = E$. 注意, 生成元组从 $\{\alpha_1, \dots, \alpha_n\}$ 变成了

$$\{\alpha_1 + \beta\alpha_2, \alpha_3, \dots, \alpha_n\},$$

数目减少 1. 重复以上讨论 $n-1$ 次, 我们就得到一个元素 α , 使得 $E = F(\alpha)$. 因此 E/F 为一个单扩张.

下证若 E/F 为一个单扩张, 则中间域数目有限. 设 $E = F(\alpha)$. 假设存在无穷多个 E/F 扩张的中间域. 我们可以假设这些中间域都与 E 和 F 不同, 因此 α 不在其中. 记 α 在 F 中的最小多项式为 $f_\alpha(x)$. 任取中间域 K , 我们考虑 α 在 K 中的最小多项式 g_α , 则有 $g_\alpha \mid f_\alpha$. 因此有有限个不同的 g_α . 只需证明 g_α 可以决定 K .

设 $g_\alpha(x) = a_0 + a_1x + \cdots + a_rx^r \in K[x]$. 考虑 $L = F(a_0, \dots, a_r)$, 由于 $L \subset K$, 多项式 g_α 在 $L[x]$ 不可约. 注意 $[E:L] = r = [E:K]$. 因此 $K = L$. 也即 K 由 g_α 的系数决定. 因此 E/F 只有有限多个中间域. $\square$

下边证明定理 33.1.2.

定理 33.1.2 的证明. 任给一个 E/F 为一个有限可分扩张, 设 $E = F(\alpha_1, \dots, \alpha_n)$, 记 $f_1, \dots, f_n \in F[x]$ 为 $\alpha_1, \dots, \alpha_n$ 的最小多项式. 记 E' 为 $f = f_1 \cdots f_n$ 的分裂域. 记 $\beta_1, \dots, \beta_k \in E'$ 为 f 所有的根, 则 $\beta_1, \dots, \beta_k$ 均可分, 因此 $E' = F(\beta_1, \dots, \beta_k)$ 是可分扩张.

此外, 由之前关于正规扩张与分裂域之间的关系, 我们知道 E'/F 也是一个正规扩张. 因此 E'/F 为一个 Galois 扩张. 由于 E'/F 中间域个数与 $\text{Gal}(E'/F)$ 的子群个数相同, 因此为有限多个. 因此 E/F 的中间域个数为有限多个. 由之前命题, 我们知道 E/F 为一个单扩张. $\square$

33.2 一个有限 Galois 扩张中如何找本原元

记 E/F 为一个有限 Galois 扩张. 因此 E/F 有有限多个中间域记做

$$\{K_1, \dots, K_s\},$$

其中 $s \in \mathbb{N}^*$.

任取 $\alpha \in E$, 我们考虑 $F(\alpha) \subset E$ 为 E/F 的中间域. 因此存在 $1 \leq i \leq s$, 满足

$$F(\alpha) = K_i.$$

若 $s > 1$, 且 $K_s = E$, 我们只需要找到一个元素不在

$$K_1 \cup \cdots \cup K_{s-1},$$

中, 则 $F(\alpha) = E$.

例 33.2.1.

考虑 Galois 扩张 $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. 该扩张的所有中间域为

$$\{\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{2}, \sqrt{3})\}.$$

我们知道 $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$ 且 $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. 此外, 若 $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{6})$, 则有

$$\sqrt{2} = \sqrt{6}(\sqrt{2} + \sqrt{3}) - 2(\sqrt{2} + \sqrt{3})$$

$$\sqrt{3} = 3(\sqrt{2} + \sqrt{3}) - \sqrt{6}(\sqrt{2} + \sqrt{3})$$

因此 $\mathbb{Q}(\sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, 矛盾. 此外 $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$, 因此我们有

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

注 33.2.2.

这个例子中我们也可以通过观察 $\text{Gal}(E/\mathbb{Q}(\sqrt{2} + \sqrt{3}))$ 证明其等于 $\{\text{id}\}$ 来说明 $\sqrt{2} + \sqrt{3}$ 为本原元.

第三十四章 根式扩张

34.1 定义

定义 34.1.1

考虑一个域扩张 E/F , 我们称 $\alpha \in E$ 为 F 上的一个 n -次根, 若有 $\alpha^n \in F$.

定义 34.1.2

我们称一个域扩张 E/F 为一个**根式扩张**, 若存在一个扩张塔

$$E = E_s / \cdots / E_1 / E_0 = F,$$

满足对任意 $0 \leq i \leq s-1$, 存在 $n_i \in \mathbb{N}^*$, $\alpha_{i+1} \in E_{i+1}$, 满足 $\alpha_{i+1}^{n_i} \in E_i$, 且 $E_{i+1} = E_i(\alpha_{i+1})$.

定义 34.1.3

记 F 为一个域, $f(x) \in F[x]$. 我们称 f 是**根式可解**的, 若存在 F 的一个根式扩张 E , 使得 f 在 E 上分裂.

记 F 为一个域. 我们关心的主要问题就是任给 $f(x) \in F[x]$, 它是否有根式解. 在讨论一般的情形前, 我们将依次讨论如下几种特殊多项式:

- $x^n - 1$ (分圆扩张);
- $x^n - \alpha$ (循环扩张);
- $(x^n - \alpha_1) \cdots (x^n - \alpha_k)$ (Kummer 扩张).

34.2 分圆扩张

34.2.1 条件设定

记 F 为一个域. 记 $n \in \mathbb{N}^*$ (不一定是素数), 我们考虑多项式 $x^n - 1 \in F[x]$, 并记 E 为 $x^n - 1$ 的分裂域. 若 $\text{Ch}F = p \mid n$, 即存在 $k \in \mathbb{N}^*$, 满足 $n = pk$, 则我们有

$$x^n - 1 = (x^k - 1)^p.$$

因此以下我们将假设 $\text{Ch}F \nmid n$.

由于

$$D(x^n - 1) = nx^{n-1},$$

而 0 不是 $x^n - 1$ 的根. 因此 $x^n - 1$ 无重根. 所以 E/F 是一个 Galois 扩张. 我们将讨论 $\text{Gal}(E/F)$.

34.2.2 分圆多项式

我们记 R 为 $x^n - 1$ 在 E 中所有的根. 注意到 R 构成 E 的一个子群, 由命题 32.2.1 可知, R 为一个 n -阶循环群. 因此任意 R 中的元素的阶 k 都整除 n .

定义 34.2.1

我们称 R 中的一个元素 ε 为 **n -阶本原单位根**, 若其阶为 n , 也即 $\varepsilon^n = 1$, 且对任意 $1 \leq j < n$, $\varepsilon^j \neq 1$.

以下是两个本原单位根直接由定义可得性质.

引理 34.2.2 (教材引理 4.11.2)

若 F 的特征为 p , 则 F 有 n -阶本原单位根当且仅当 $p \nmid n$.

证明. 由于 $p \mid n$ 当且仅当 $x^n - 1$ 有重根. 而重根的阶小于 n . 由此可得引理. $\square$

引理 34.2.3 (教材引理 4.11.3)

设 ε 为一个 n -阶本原单位根, 则 ε^k 为一个 n -阶本原单位根当且仅当 $\gcd(k, n) = 1$.

n -阶本原单位根的数目可以由欧拉函数给出.

定义 34.2.4

我们称以下函数为**欧拉函数**:

$$\begin{aligned} \phi : \mathbb{N}^* &\rightarrow \mathbb{N}^* \\ n &\mapsto \#\{d \in \{1, \dots, n\} \mid \gcd(d, n) = 1\} \end{aligned}$$

任给一个大于 1 的自然数 n , 考虑其素数分解:

$$n = p_1^{k_1} \cdots p_r^{k_r}.$$

其中 $p_1, \dots, p_r$ 为两两不同的素数, $k_1, \dots, k_r$ 为非零自然数. 我们有

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

注 34.2.5.

一个非零自然数与 n 最大公约数是 1 当且仅当它不能被 $p_1, \dots, p_r$ 中的任何一个整除.

推论 34.2.6

记 F 为一个域, $n \in \mathbb{N} \setminus \{0, 1\}$, 且 $\text{Ch}F \nmid n$, 则 F 中有 $\phi(n)$ 个 n -阶本原单位根.

由前一个引理, 我们知道对任意 $n \in \mathbb{N}^*$, 且 $\text{Ch}F \nmid n$, 共有 $\phi(n)$ 个 n -阶本原单位根.

定义 34.2.7

记 F 为一个域, n 为一个非零自然数, 且不被 F 的特征整除. 我们称 $x^n - 1 \in F[x]$ 的分裂域扩张 E/F 为 F 的**分圆扩张**.

命题 34.2.8

任取 R 中的 n -阶本原单位根 ε , 则 $E = F(\varepsilon)$, 且 $f(x) \in E[x]$ 有如下分解:

$$x^n - 1 = (x - 1)(x - \varepsilon) \cdots (x - \varepsilon^{n-1}).$$

我们记 $R_n \subset R$ 为 n -阶本原单位根的集合.

定义 34.2.9

任取 $n \in \mathbb{N}^*$, 我们定义 $F[x]$ 中的 **n -阶分圆多项式** 如下:

$$\Psi_n(x) := \prod_{\varepsilon \in R_n} (x - \varepsilon) \in F[x].$$

注 34.2.10.

我们知道 $\Psi_n(x) \in E[x]$. 由于 $\text{Gal}(E/F)$ 中的元素保持 $x^n - 1$ 的根的阶, 因此 $\Psi_n(x)$ 关于 $\text{Gal}(E/F)$ 的作用对称, 也即所有 $\text{Gal}(E/F)$ 中元素都固定该多项式. 因此 $\Psi_n(x) \in F[x]$. 此外由之前对 n -阶本原单位根的讨论, 我们知道 $\Psi_n(x)$ 的次数为 $\phi(n)$.

因此我们有如下关系:

命题 34.2.11

$$x^n - 1 = \prod_{d|n} \Psi_d(x).$$

我们首先证明以下引理.

引理 34.2.12

- (i) 记 E/F 为一个域扩张. 记 $f, g \in F[x]$, 以及 $h \in E[x]$. 若在 $E[x]$ 中有, $f = gh$, 则 $h \in F[x]$;
- (ii) 记 A 为一个整环, F 为 A 的分式域. 记 $f, g \in A[x]$ 为首一多项式, 并记 $h \in F[x]$. 若在 $F[x]$ 中有 $f = gh$, 则 $h \in A[x]$.

证明. 首先证明 (i).

我们记

$$g(x) = a_0 + \cdots + a_m x^m \in F[x], \quad h(x) = b_0 + \cdots + b_n x^n \in E[x].$$

由于 $gh = f \in F[x]$, 因此我们有 $a_m b_n \in F$. 由 $a_m \in F^*$, 我们有 $b_n \in F$. 因此我们有

$$g(x)h(x) = g(x)(h_1(x) + b_n x^n) = g(x)h_1(x) + b_n x^n g(x).$$

因此 $f_1(x) = g(x)h_1(x) \in F[x]$. 由归纳法, 我们可以证明 h 所有的系数都在 F 中. 因此 $h \in F[x]$.

(ii) 的证明与 (i) 类似. 注意我们要利用 g 的首项系数为 1 这个条件. (在 (i) 的证明中, 我们利用的是 g 的首项系数可逆这个条件.) $\square$

推论 34.2.13

(i) 记 $F_0 \subset F$ 为 F 的素域, 则对任意 $n \in \mathbb{N}^*$, $\Psi_n(x) \in F_0[x]$.

(ii) 若进一步有 $F_0 = \mathbb{Q}$, 则对任意 $n \in \mathbb{N}^*$, $\Psi_n(x) \in \mathbb{Z}[x]$.

34.2.3 关于分圆多项式是否可约的讨论

设 $n \in \mathbb{N}^*$, 取 $\Psi_n(x) \in F[x]$. 我们记 K_n/F 为 $\Psi_n(x)$ 的分裂域扩张. 由 $\Psi_n(x)$ 的定义我们知道任取一个 n -次本原单位根 ε , 我们有 $K_n = F(\varepsilon)$.

我们固定一个 n -次本原单位根 ε , 则所有 n -次本原单位根可以记为

$$\varepsilon^{k_1}, \dots, \varepsilon^{k_s},$$

这里 $k_1, \dots, k_s$ 为自然数, 满足 $1 < k_1 < \cdots < k_s < n$.

命题 34.2.14

在 $\mathbb{Z}_n$ 中, 集合

$$\{\overline{k_1}, \dots, \overline{k_s}\},$$

为 $\mathbb{Z}_n$ 中的单位群 $U_n < \mathbb{Z}_n$.

证明. 由本原单位根的定义, 我们知道对任意 $1 \leq j \leq s$,

$$\gcd(k_j, n) = 1.$$

因此我们有 $a, b \in \mathbb{Z}$, 满足

$$ak_j + bn = 1,$$

因此在

$$\overline{ak_j} = \overline{1}.$$

因此 $\overline{k_j}$ 为 $\mathbb{Z}_n$ 中的单位.

反过来任取 k , 满足 $\overline{k}$ 为 $\mathbb{Z}_n$ 的单位, 我们有整数 a, b , 满足

$$ak - 1 = bn.$$

因此

$$\gcd(k, n) = 1.$$

从而 ε^k 为一个 n -次本原单位根. $\square$

我们用以下记号来记上边提到的映射:

$$\Pi: R_n \rightarrow U_n.$$

考虑 $\text{Gal}(K_n/F)$. 由于 $K_n = F(\varepsilon)$, 因此任意 $\varphi \in \text{Gal}(K_n/F)$ 都由 $\varphi(\varepsilon)$ 决定. 由于 φ 保持 n 次单位根的阶, 因此, $\varphi(\varepsilon)$ 也是一个本原单位根, 即存在 $k_i \in \{1, k_1, \dots, k_s\}$, 满足

$$\varphi(\varepsilon) = \varepsilon^{k_i}.$$

由此我们得到一个 $\text{Gal}(K_n/F)$ 到 U_n 的映射 $\Theta: \varphi \mapsto \overline{k_i}$.

注 34.2.15.

这里我们考虑的是 $\overline{k_i}$ 在 U_n 上的作用. 这个作用将 U_n 中的元素做了一个置换.

命题 34.2.16

映射 $\Theta: \text{Gal}(K_n/F) \rightarrow U_n$ 是一个群单同态.

证明. 任取 $\text{Gal}(K_n/F)$ 中的元素 φ 和 ψ , 设其在 Θ 下的像分别为 $\overline{k_i}$ 和 $\overline{k_j}$. 考虑 $\varphi \circ \psi$ 在 Θ 下的像为 $\overline{k_l}$. 我们做如下计算:

$$\varepsilon^{k_l} = (\varphi \circ \psi)(\varepsilon) = \varphi(\psi(\varepsilon)) = \varphi(\varepsilon^{k_j}) = (\varphi(\varepsilon))^{k_j} = \varepsilon^{k_i k_j}.$$

因此 $\overline{k_l} = \overline{k_i} \cdot \overline{k_j}$. 单射由 $k_1, \dots, k_s$ 的取值范围可知. □

由以上讨论, 任取 $\sigma \in \text{Gal}(K_n/F)$, 我们有如下交换图:

$$\begin{array}{ccc} R_n & \xrightarrow{\Pi} & U_n \\ \sigma \downarrow & & \downarrow \Theta(\sigma) \\ R_n & \xrightarrow{\Pi} & U_n \end{array}$$

推论 34.2.17

$\text{Gal}(K_n/F)$ 是一个交换群.

我们回顾之前的关于多项式的 Galois 群的结论:

命题 34.2.18 (命题 30.1.4)

记 F 为一个域, $f \in F[x]$. 记 E/F 为 f 的分裂域扩张. 则多项式 f 不可约当且仅当 $\text{Gal}(E/F)$ 在 f 的根集上的作用是可递的.

推论 34.2.19

$\text{Gal}(K_n/F)$ 在 Ψ_n 的根集上作用是传递的当且仅当 Θ 是满射, 也即 $\text{Gal}(K_n/F) \cong U_n$.

证明. 若 $\text{Gal}(K_n/F)$ 在 Ψ_n 的根集上作用是传递的, 则对任意 ε^{k_i} , 存在 $\sigma \in \text{Gal}(K_n/F)$, 满足 $\sigma(\varepsilon) = \varepsilon^{k_i}$. 由命题 34.2.14, 我们知道 Θ 是满射.

反过来, 若 Θ 是满射, 则对任意 ε^{k_i} , 我们考虑 $\overline{k_i} \in U_n$, 记 $\sigma \in \text{Gal}(K_n/F)$ 为 $\overline{k_i}$ 对应的元素, 则有

$$\sigma(\varepsilon) = \varepsilon^{k_i}.$$

因此 $\text{Gal}(K_n/F)$ 在 R_n 上的作用是传递的. $\square$

推论 34.2.20

任取素数 $q \neq \text{Ch}F$, 则 Ψ_q 或者在 F 上分裂, 或者 $\text{Gal}(K_q/F)$ 为非平凡循环群.

证明. 由于 q 为素数, 因此 $\mathbb{Z}_q$ 为域. 由之前对有限域的讨论中的结论, U_q 为一个循环群. 因此 $\text{Gal}(K_q/F)$ 同构于 U_q 的一个子群, 也是一个循环群. $\square$

注 34.2.21.

设素数 $q \neq \text{Ch}F$, 注意若 Ψ_q 在 F 上不分裂, 我们并不能说 Ψ_q 不可约. 考虑一下例子.

我们考虑 $F = \mathbb{F}_2$, 并考虑 Ψ_7 . 在 $\mathbb{F}_2[x]$ 中, 我们有

$$\Psi_7 = (x^3 + x^2 + 1)(x^3 + x + 1),$$

即不分裂又可约.

若 F 的特征为 0, 它的素域与 $\mathbb{Q}$ 同构, 我们可以将其看作是 $\mathbb{Q}$ 的扩张. 由之前的讨论知道在此情形下, 分圆多项式 Ψ_n 是 $\mathbb{Q}$ 上的多项式, 也是 $\mathbb{Z}$ 上的多项式.

命题 34.2.22

对任意 $n \in \mathbb{N}^*$, 分圆多项式 Ψ_n 在 $\mathbb{Q}$ 上不可约.

证明. 由 Gauss 引理, 我们只需要证明 Ψ_n 在 $\mathbb{Z}[x]$ 中不可约. 由于 Ψ_n 为首一多项式, 若 Ψ_n 在 $\mathbb{Z}[x]$ 中可约, 则存在两个次数大于 1 的首一多项式 $g, h \in \mathbb{Z}[x]$, 满足

$$\Psi_n(x) = g(x)h(x).$$

我们进一步假设 $g(x) \in \mathbb{Z}[x]$ 不可约. 注意到任给一个本原单位根 ε , 我们有 $g(\varepsilon) = 0$ 或 $h(\varepsilon) = 0$ 有且仅有一个成立. ($\mathbb{Q}$ 上多项式都可分, 因此没有重根.)

引理 34.2.23

任给一个 n -阶本原单位根 ε , 满足 $g(\varepsilon) = 0$, 任给一个素数 p , 满足 $p \nmid n$, 则

$$g(\varepsilon^p) = 0.$$

证明. 注意到 ε^p 为一个本原单位根, 因此若 $g(\varepsilon^p) \neq 0$, 我们有 $h(\varepsilon^p) = 0$. 考虑 $f(x) = h(x^p)$, 则 ε 为 f 的根. 因为 g 不可约, 我们在 $\mathbb{Z}[x]$ 中有

$$f(x) = g(x)f_1(x).$$

我们现在考虑由自然同态

$$\mathbb{Z} \rightarrow \mathbb{Z}_p,$$

诱导的多项式环的自然同态

$$\mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x].$$

我们有

$$\bar{g}(x)\bar{f}_1(x) = \bar{f}(x) = \bar{h}(x^p) = \bar{h}^p(x).$$

任给 $\bar{g}(x) \in \mathbb{Z}_p[x]$ 的不可约因子 $\bar{q}(x)$, 我们有

$$\bar{q}(x) \mid \bar{h}(x).$$

因此

$$\bar{q}^2 \mid \bar{g}\bar{h} = \bar{\Psi}_n.$$

也即 $\bar{\Psi}_n$ 在其分裂域中有重根. 这与 $p \nmid n$, 矛盾. □

考虑 $x^n - 1$ 在 $\mathbb{Z}[x]$ 到 $\mathbb{Z}_p[x]$ 的由 $\mathbb{Z}$ 到 $\mathbb{Z}_p$ 的自然映射诱导的环同态下的像. 因为 $p \nmid n$, 多项式 $x^n - \bar{1} \in \mathbb{Z}_p[x]$ 在其分裂域里没有重根, 因此多项式 $\bar{\Psi}_n$ 没有重根.

任取 θ 为 h 的一个根. 由于 θ 也是 n -阶本原单位根, 因此存在 $d \in \mathbb{N}^*$, 满足

$$\theta = \varepsilon^d,$$

且 $\gcd(d, n) = 1$. 考虑 d 的素数分解, 我们有

$$\theta = \varepsilon^{p_1^{k_1} \cdots p_s^{k_s}}.$$

所有 p_i 都满足 $p_i \nmid n$. 我们重复之前讨论可得

$$\{\varepsilon^{p_1}, \varepsilon^{p_1^2}, \dots, \varepsilon^{p_1^{k_1} \cdots p_s^{k_s}}\},$$

包含在 g 的根集中. 因此 θ 为 g 的根, 矛盾.

因此 $\Psi_n = g$ 在 $\mathbb{Q}[x]$ 中不可约. □

推论 34.2.24

任取 $n \in \mathbb{N}^*$, 考虑 $\Psi_n \in \mathbb{Q}[x]$ 的分裂域扩张 $K_n/\mathbb{Q}$, 我们有

$$\text{Gal}(K_n/\mathbb{Q}) \cong U_n.$$

34.2.4 U_n 的结构

任给一个大于 1 的自然数 n , 我们首先了解一下 $\mathbb{Z}_n$ 的结构. 考虑 n 的素数分解:

$$n = p_1^{k_1} \cdots p_s^{k_s}.$$

我们将把环 $\mathbb{Z}_n$ 与以下环的直积联系起来:

$$\mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{k_s}}.$$

我们将使用的工具是中国剩余定理.

(中国剩余定理) 设 R 为一个交换幺环, 我们称两个 R 的理想 I 和 J 互素, 若 $I+J=R$. 记 $I_1, \dots, I_s$ 为 R 的两两互素的理想, 并对任意 $1 \leq i \leq s$, 记

$$\pi_i : R \rightarrow R/I_i.$$

则如下映射:

$$\begin{aligned} \phi : R &\rightarrow R/I_1 \oplus \cdots \oplus R/I_s, \\ a &\mapsto (\pi_1(a), \dots, \pi_s(a)) \end{aligned}$$

为一个满同态, 且有

$$\ker \phi = \bigcap_{i=1}^s I_i.$$

因此我们有如下结论.

命题 34.2.25

我们有如下环同构:

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{k_s}}.$$

因此作为推论, 我们有如下关于 U_n 的分解:

推论 34.2.26

我们有如下群同构:

$$U_n \cong U_{p_1^{k_1}} \oplus \cdots \oplus U_{p_s^{k_s}}.$$

利用这个结果我们可以更方便的计算一个分圆扩张的 Galois 群.

命题 34.2.27

- (i) 若自然数 $k \geq 2$, 则 $U_{2^k} \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$; 若 $k=1$, 则 $U_2 \cong \{1\}$.
- (ii) 单位群 U_n 为循环群当且仅当 $n = p^k, 2p^k$ 或者 4 , 其中 p 为一个奇素数, $k \in \mathbb{N}$.

证明. (i) 由直接验证知, 若 $k=1$, 则 $U_2 \cong \{1\}$; 若 $k=2$, 则 $U_4 \cong \mathbb{Z}_2$. 因此以下假设 $k \geq 3$. 由之前对欧拉函数的讨论知

$$|U_{2^k}| = 2^k \left(1 - \frac{1}{2}\right) = 2^{k-1}.$$

我们考虑 $5 \in U_{2^k}$, 及以下对 5^k 的计算:

- $5^{2^0} = 1 + 2^2 = 1 + l_2 2^2, 2 \nmid l_2;$
- $5^{2^1} = (1 + l_2 2^2)^2 = 1 + 2l_2 2^2 + l_2^2 2^4 = 1 + l_3 2^3, 2 \nmid l_3;$
- $5^{2^2} = (1 + l_3 2^3)^2 = 1 + 2l_3 2^3 + l_3^2 2^6 = 1 + l_4 2^4, 2 \nmid l_4;$
- $\dots$
- $5^{2^{k-3}} = (1 + l_{k-2} 2^{k-2})^2 = 1 + 2l_{k-2} 2^{k-2} + l_{k-2}^2 2^{k-2} = 1 + l_{k-1} 2^{k-1}, 2 \nmid l_{k-1};$

$$\bullet \quad 5^{2^{k-2}} = (1 + l_{k-1}2^{k-1})^2 = 1 + 2l_{k-1}2^{k-1} + l_{k-1}^2 2^{k-1} = 1 + l_k 2^k, \quad 2 \nmid l_k.$$

注意到 $\bar{5}$ 的阶整除 2^{k-1} . 以上计算最后两个等式告诉我们, $\bar{5}$ 的阶为 2^{k-2} . 因此, $\bar{5}$ 生成的 U_{2^k} 的子群为

$$\{\bar{1}, \bar{5}, \bar{5}^2, \dots, \bar{5}^{2^{k-2}-1}\}.$$

我们考虑集合

$$\{-\bar{1}, -\bar{5}, -\bar{5}^2, \dots, -\bar{5}^{2^{k-2}-1}\}.$$

下证该集合也有 2^{k-2} 个元素且与 $\bar{5}$ 生成的群交集为空集. 我们取 $a, c \in \{0, 1\}$, $b, d \in \{0, \dots, 2^{k-2}-1\}$, 并假设

$$(-1)^a 5^b \equiv (-1)^c 5^d \pmod{2^k}.$$

由于 $k \geq 3$, 因此

$$(-1)^a 5^b \equiv (-1)^c 5^d \pmod{4}.$$

由以上两个关系, 我们有 $a = c$ 且 $b = d$.

因此

$$U_{2^k} = \{\pm 1\} \times \{\bar{1}, \bar{5}, \bar{5}^2, \dots, \bar{5}^{2^{k-2}-1}\}.$$

我们可以构造 $\mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$ 到 U_{2^k} 的群同构:

$$\begin{aligned} \eta: \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}} &\rightarrow U_{2^k} \\ (\bar{a}, \bar{b}) &\mapsto \overline{(-1)^a 5^b} \end{aligned}$$

(ii) 练习

□

34.2.5 可构造正多边形

设 $n \geq 3$, 记 P_n 为 $\mathbb{C}$ 上的一个正多边形, 满足其中心在 $z = 0$, 且 $z = 1$ 是其一个顶点. 我们这里关心的问题是对于哪些 n , 我们可以从 0 和 1 两个点出发, 利用尺规将 P_n 作出. 注意到 P_n 可构造等价于

$$\varepsilon = e^{\frac{2\pi i}{n}},$$

是一个 $\mathbb{Q}$ 上的可构造数. 另一方面 ε 是 $\mathbb{Q}$ 上的一个 n -阶本原单位根.

由定理 ??, 我们知道 ε 可构造当且仅当存在一系列域扩张

$$\mathbb{Q} = K_0 \subset K_1 \subset \dots \subset K_m,$$

满足对任意 $1 \leq j \leq m$, $[K_j : K_{j-1}] = 2$, 且 $\varepsilon \in K_m$. 我们将用这个结论来给出与 n 相关的与 ε 可构造等价的叙述.

我们首先假设 ε 可构造, 因此存在 $k \in \mathbb{N}$, 满足

$$\deg(\varepsilon, \mathbb{Q}) = \phi(n) = 2^k.$$

另一方面, 我们考虑 n 的素数分解. 若存在 $l \in \mathbb{N}^*$, 满足 $n = 2^l$, 则

$$\phi(n) = 2^l \left(1 - \frac{1}{2}\right) = 2^{l-1}.$$

若 n 有素数因子 2, 且有奇素数因子, 则有

$$n = 2^l p_1^{k_1} \dots p_s^{k_s},$$

其中 $p_1, \dots, p_s$ 为两两不同的奇素数, $l, k_1, \dots, k_s \in \mathbb{N}^*$. 因此

$$\phi(n) = 2^l p_1^{k_1} \cdots p_s^{k_s} \frac{1}{2} \frac{p_1 - 1}{p_1} \cdots \frac{p_s - 1}{p_s} = 2^{l-1} p_1^{k_1-1} \cdots p_s^{k_s-1} (p_1 - 1) \cdots (p_s - 1).$$

因此 $\phi(n) = 2^k$ 当且仅当对任意 $1 \leq i \leq s$, 存在 m_i , 满足

$$p_i = 2^{m_i} + 1,$$

同时 $k_i = 1$.

若 n 为奇数, 重复以上讨论, 我们得到关于 p_i 和 k_i 相同的结论.

命题 34.2.28

若存在一个自然数 $m \in \mathbb{N}$, 满足 $2^m + 1$ 是一个素数, 那么存在一个自然数 l , 满足 $m = 2^l$.

证明. 我们考虑多项式

$$f(x) = x^m + 1 \in \mathbb{Z}[x].$$

我们首先假设 m 为一个奇数, 则在 $\mathbb{Z}[x]$ 中有

$$x + 1 \mid x^m + 1.$$

由于整系数多项式在整数取值得到的仍是整数, 我们有

$$2 + 1 \mid 2^m + 1.$$

这与 $2^m + 1$ 为一个素数矛盾. 因此 m 为一个偶数.

假设 $m = 2^l m_1$, 其中 $l \in \mathbb{N}^*$, 且 $2 \nmid m_1$. 我们考虑多项式

$$g(x) = x^{m_1} + 1 \in \mathbb{Z}[x].$$

则有 $f(x) = g(x^{2^l})$. 与之前的讨论相同, 我们在 $\mathbb{Z}[x]$ 中有

$$x + 1 \mid x^{m_1} + 1,$$

因此

$$x^{2^l} + 1 \mid x^m + 1.$$

由此可得

$$2^{2^l} + 1 \mid 2^m + 1.$$

这与 $2^m + 1$ 为一个素数矛盾. 因此 $m = 2^l$. □

定义 34.2.29

若一个素数可以写为 $2^{2^l} + 1$ 的形式, 其中 $l \in \mathbb{N}$, 我们称之为一个 **Fermat 素数**.

综上所述, 我们有如下命题.

命题 34.2.30

记自然数 $n \geq 3$.

- (i) 若正 n -边形 P_n 可构造, 则存在一个自然数 k , 使得 $\phi(n) = 2^k$.
- (ii) $\phi(n) = 2^k$, 当且仅当 n 的奇素数因子(若存在)均为 Fermat 素数, 且在 n 的素数分解中次数为 1.

我们下边将讨论条件 $\phi(n) = 2^k$ 的充分性.

我们记 $E/\mathbb{Q}$ 为 $x^n - 1$ 的分裂域扩张, 因此是一个 Galois 扩张, 且

$$E = \mathbb{Q}(\varepsilon).$$

假设存在 $k \in \mathbb{N}^*$, $\phi(n) = 2^k$. 因此 $|\text{Gal}(E/\mathbb{Q})| = 2^k$.

利用 Sylow 定理我们有以下 $\text{Gal}(E/\mathbb{Q})$ 的子群列:

$$\{id\} = H_0 < H_1 < \cdots < H_k = \text{Gal}(E/\mathbb{Q}),$$

满足对任意 $0 \leq j \leq k$, 满足 $|H_j| = 2^j$. 因此对任意 $0 \leq j \leq k-1$,

$$[H_{j+1} : H_j] = 2.$$

利用 Galois 对应, 我们有一列域的扩张:

$$E = L_0 \supset L_{k-1} \supset \cdots \supset L_k = \mathbb{Q}.$$

满足对任意 $0 \leq j \leq k$,

$$H_j = \text{Gal}(E/L_j).$$

对任意 $1 \leq j \leq k$, E/L_j 是一个 Galois 扩张, 因此

$$[L_j : L_{j-1}] = [\text{Gal}(E/L_{j-1}) : \text{Gal}(E/L_j)] = 2.$$

命题 34.2.31

记 n 为一个大于等于 3 的自然数, 记 $\varepsilon = e^{\frac{2\pi i}{n}}$. 若存在 $k \in \mathbb{N}$, 满足 $\phi(n) = 2^k$, 则 ε 为可构造数.

综上所述, 我们得到以下正 n 边形可构造的等价条件.

定理 34.2.32

记 n 为一个大于等于 3 的自然数. 正 n 边形可构造当且仅当存在 $k \in \mathbb{N}$, 满足 $\phi(n) = 2^k$, 当且仅当 n 的奇素数因子(若存在)都是 Fermat 素数, 且在 n 的素数分解中的次数都为 1.

注 34.2.33.

这里需要注意的是若 $\mathbb{C}$ 中一个 $\mathbb{Q}$ 上的代数数在 $\mathbb{Q}$ 上的次数为 2 的某个次方, 我们并不能说明该数可构造. 比如, 我们考虑多项式

$$x^4 - 4x + 2 \in \mathbb{Q}[x].$$

利用 Eisenstein 判别法, 我们知道该多项式不可约, 因此在 $\mathbb{C}$ 中的根在 $\mathbb{Q}$ 上的次数为 $4 = 2^2$. 另一方面, 我们可以验证该多项式的 Galois 群为 S_4 , 因此元素个数为 $24 = 2^3 \times 3$. 记 $E \subset \mathbb{C}$ 为该多项式的分裂域. 记 H 为 S_4 的 Sylow-2 子群, 记 K 为 H 的不变子域. 我们有

$$[K : \mathbb{Q}] = [\text{Gal}(E/\mathbb{Q}) : H] = 3.$$

若以上多项式的根均可构造, 则 E 中元素均可构造. 然而 $K \setminus \mathbb{Q}$ 中的元素在 $\mathbb{Q}$ 上的次数为 3, 因此不可构造, 矛盾.

34.3 循环扩张

记 F 为一个域. 任取大于 0 的自然数 n , 任取 F 中非零元素 a , 我们考虑 F 上如下类型的多项式:

$$f(x) = x^n - a \in F[x].$$

为了避免重根的影响, 我们仍旧假设当 F 的特征为 p 时, $p \nmid n$.

我们记 K/F 为 f 的分裂域扩张, 并记 f 在 K 中的根集为

$$R = \{\alpha_1, \dots, \alpha_n\}.$$

因此

$$K = F(\alpha_1, \dots, \alpha_n).$$

注意到在 K 中, 我们有

$$(\alpha_1 \alpha_j^{-1})^n = a a^{-1} = 1.$$

我们记 $\varepsilon_j = \alpha_1 \alpha_j^{-1}$. 由于 f 在 K 中没有重根, 因此

$$\{\varepsilon_1, \dots, \varepsilon_n\} \subset K$$

两两不同. 由此, 我们有 $x^n - 1$ 在 K 中分裂.

由 $p \nmid n$, 我们有 n -阶本原单位根, 记为 ε . 我们记 $\alpha = \alpha_1 \in R$, 则 $f(x)$ 的根集 R 可以记为

$$R = \{\alpha, \varepsilon\alpha, \dots, \varepsilon^{n-1}\alpha\}.$$

我们有以下扩张列:

$$F \subset F(\varepsilon) \subset F(\varepsilon, \alpha) = K.$$

定理 34.3.1

记 n 为大于 1 的自然数, 考虑 $x^n - a \in F[x]$, 满足 $\text{Ch}F \nmid n$. 记 K/F 为 $x^n - a$ 的分裂域扩张. 则

- (i) K 中有 n -阶本原单位根, 记为 ε .
- (ii) $\text{Gal}(K/F(\varepsilon))$ 为一个循环群, 满足 $|\text{Gal}(K/F(\varepsilon))| \mid n$.
- (iii) $x^n - a \in F(\varepsilon)[x]$ 不可约当且仅当 $|\text{Gal}(K/F(\varepsilon))| = n$.

证明. 第一个结论已经在之前的讨论中证明过了.

任取 $\varphi \in \text{Gal}(K/F(\varepsilon))$, 该自同构由 α 的像决定. 我们设

$$\varphi(\alpha) = \varepsilon^k \alpha.$$

则对任意 $0 \leq j \leq n-1$, 有

$$\varphi(\varepsilon^j \alpha) = \varepsilon^{j+k} \alpha.$$

我们由此可以构造一个群同态:

$$\eta: \text{Gal}(K/F(\varepsilon)) \rightarrow S_n,$$

满足任取 $\varphi \in \text{Gal}(K/F(\varepsilon))$, 我们有

$$\eta(\varphi) = (1 \cdots n)^k.$$

因此 $\text{Gal}(K/F(\varepsilon))$ 同构于由 $(1 \cdots n)$ 生成的 S_n 中的循环子群的一个子群. 由此有结论 (ii).

由之前关于多项式不可约的讨论, 我们知道 $x^n - a$ 不可约当且仅当 $\text{Gal}(K/F(\varepsilon))$ 在 R 上的作用时可递的. 又由以上讨论可知, $\text{Gal}(K/F(\varepsilon))$ 在 R 上作用可递当且仅当

$$\text{Gal}(K/F(\varepsilon)) \cong \langle (1 \cdots n) \rangle.$$

因此有结论 (iii). □

我们考虑一个特殊情形: n 为一个不同于 F 的特征的素数.

命题 34.3.2

记 q 为素数, 考虑 $x^q - a \in F[x]$, 满足 $\text{Ch}F \nmid q$. 则

- (i) $x^q - a$ 或者在 F 中有一个根, 或者在 $F[x]$ 不可约.
- (ii) 若 $x^q - a$ 在 F 上有根, 则 $x^q - a$ 在 F 上分裂, 当且仅当 F 包含 q -阶本原单位根.

证明. 我们考虑 K/F 为 $x^q - a$ 的分裂域. 记 α 为 $x^q - a$ 在 K 中的一个根, ε 为 q -阶本原单位根. 因此

$$K = F(\alpha, \varepsilon).$$

若 $x^q - a$ 在 $F[x]$ 中可约. 记 g 为 $x^q - a$ 的一个不可约因子, 则存在

$$\emptyset \neq \{k_1, \dots, k_s\} \subsetneq \{0, \dots, q-1\},$$

满足

$$g(x) = (x - \varepsilon^{k_1} \alpha) \cdots (x - \varepsilon^{k_s} \alpha) \in F[x].$$

因此, 我们有

$$g(x) = b_0 + b_1 x + \cdots + b_s x^s.$$

特别地, 我们有

$$(-1)^s b_0 = \varepsilon^{k_1 + \cdots + k_s} \alpha^s \in F.$$

注意到

$$((-1)^s b_0)^q = \alpha^{sq} = a^s \in F.$$

由于 $\gcd(s, q) = 1$, 我们有整数 $u, v \in \mathbb{Z}$, 满足,

$$((-1)^s b_0)^{uq} a^{vq} = a.$$

因此 $((-1)^s b_0)^{uq} a^{vq}$ 为 $x^q - a$ 的一个根.

我们有

$$[K : F] = [K : F(\varepsilon)][F(\varepsilon) : F].$$

由于 $x^q - a$ 在 F 中有根, 因此在 $F(\varepsilon)$ 中有根. 由定理 34.3.1, 我们有 $[K : F(\varepsilon)] < q$, 且整除 q , 因此

$$[K : F(\varepsilon)] = 1,$$

也即 $x^q - a$ 在 $F(\varepsilon)$ 中分裂.

因此 $x^q - a$ 在 F 中分裂当且仅当 $F(\varepsilon) = F$, 也即 $\varepsilon \in F$. □

定义 34.3.3

一个有限 Galois 扩张 E/F 为一个**循环扩张**, 若其 Galois 群为循环群.

定理 34.3.4

设 K/F 为一个次数 n 的循环扩张. 设 F 的特征不整除 n . 若 F 包含 n -阶本原单位根, 则存在元素 $a \in F$, 满足

- (i) $x^n - a \in F[x]$ 不可约;
- (ii) K/F 为 $x^n - a$ 的分裂域扩张;
- (iii) 若 $\alpha \in K$ 为 $x^n - a$ 的一个根, 则 $K = F(\alpha)$.

证明. 我们记 φ 为 $\text{Gal}(K/F)$ 的生成元, 因此

$$\text{Gal}(E/F) = \{id, \varphi, \varphi^2, \dots, \varphi^{n-1}\}.$$

记 $\varepsilon \in F$ 为 n -阶本原单位根. 由 Dedekind 无关性定理, 我们知道存在 $\beta \in K$, 满足

$$\alpha = \beta + \varepsilon\varphi(\beta) + \dots + \varepsilon^{n-1}\varphi^{n-1}(\beta) \neq 0.$$

注意到 $\varphi(\alpha) = \varepsilon^{-1}\alpha$, 因此 $\alpha \notin F$ ($\text{Inv}(\text{Gal}(K/F)) = F$), 且

$$\varphi(\alpha^n) = (\varphi(\alpha))^n = \alpha^n.$$

由于 φ 生成 $\text{Gal}(K/F)$, 我们有 $\alpha^n \in F$. 令 $a = \alpha^n$, 我们考虑多项式

$$x^n - a \in F[x].$$

注意到该多项式在 $K[x]$ 中分裂:

$$x^n - a = (x - \alpha) \cdots (x - \varepsilon^{n-1}\alpha).$$

由于 $\alpha \notin F$, $\varepsilon \in F$, 因此 $x^n - a$ 在 F 中无根. 我们记 $F(\alpha)$ 为 K/F 的中间域. 由以上讨论知, $F(\alpha)/F$ 为 $x^n - a$ 的分裂域. 因此为正规扩张. 由 Galois 基本定理证明中的讨论, 我们有

$$\text{Gal}(F(\alpha)/F) = \{\varphi|_{F(\alpha)} \mid \varphi \in \text{Gal}(K/F)\}.$$

注意到

$$\varphi(\alpha) = \varepsilon^{-1}\alpha,$$

因此 $\text{Gal}(F(\alpha)/F)$ 在 $x^n - a$ 的根集

$$\{\alpha, \varepsilon\alpha, \dots, \varepsilon^{n-1}\alpha\}$$

上的作用是可递的. 因此 $x^n - a \in F[x]$ 是不可约的. 我们有

$$[F(\alpha) : F] = \deg(x^n - a) = n.$$

又由于

$$n = [K : F] = [K : F(\alpha)][F(\alpha) : F] = n[K : F(\alpha)],$$

我们有

$$K = F(\alpha),$$

K 为 $x^n - a \in F[x]$ 的分裂域.

□

例 34.3.5.

我们这里给出一个 n 次循环扩张但不包含 n -阶本原单位根的例子. 我们考虑 $\mathbb{Q}$ 上的三次多项式

$$x^3 - 3x + 1.$$

由之前对三次多项式的 Galois 群的讨论, 我们知道这个多项式的 Galois 群是一个三阶循环群. 但是它的分裂域里并没有三次本原单位根. (它的三个根都是实根)

34.4 Kummer 扩张

我们将以上讨论继续推广到更一般的情形. 考虑 E/F 为一个有限 Galois 扩张, 且 $\text{Gal}(E/F)$ 为一个交换群的情形.

设 G 为一个有限交换群, 我们将其看作 $\mathbb{Z}$ -模. 我们称 $d \in \mathbb{N}^*$ 为 G 的**零化指数**(exponent), 若

$$\text{ann}(G) = d\mathbb{Z}.$$

其中 $d = 1$ 当且仅当 $G = \{id\}$.

定理 34.4.1

设 E/F 为一个有限 Galois 扩张, 且 $\text{Gal}(E/F)$ 为一个零化指数为 $d \in \mathbb{N}^*$ 的交换群. 设 F 中有 d 阶本原单位根. 则存在 $a_1, \dots, a_s \in F$, 满足 E/F 为

$$(x^d - a_1) \cdots (x^d - a_s) \in F[x],$$

的分裂域扩张.

证明. 我们对 $[E : F]$ 做归纳.

注意到 $\text{Gal}(E/F)$ 中有 d -阶元素. 因此 $[E : F] \geq d$. 若 $[E : F] = 1$, 则

$$\text{Gal}(E/F) = \{id\}.$$

因此 $E = F$. 同时有 $d = 1$, 因此结论成立.

下设结论对 $[E : F] < n$ 都成立. 考虑 $[E : F] = n$ 的情形. 由于 $\text{Gal}(E/F)$ 为有限交换群, 由有限交换群的结构定理, 我们有

$$\text{Gal}(E/F) = G \oplus H,$$

这里 $G \cong \mathbb{Z}_d$, 且 H 的零化指数整除 d .

记 $K = \text{Inv}(G)$, 则有 K/F 为一个正规扩张, 因此也是 Galois 扩张, 且

$$\text{Gal}(K/F) \cong \text{Gal}(E/F)/\text{Gal}(E/K) \cong H.$$

由于 $r \mid d$, F 中有 r -阶本原单位根, 且 $[K : F] < n$. 因此由归纳假设, 我们有 $b_1, \dots, b_{s-1} \in F$, 满足 K/F 为

$$(x^r - b_1) \cdots (x^r - b_{s-1}) \in F[x],$$

的分裂域.

我们记 β_i 为 $x^r - b_i \in F[x]$ 在 K 中的一个根. 对任意 $1 \leq i \leq s-1$, 我们记

$$a_i = b_i^{\frac{d}{r}}.$$

记 ε 为一个 d -阶本原单位根, 我们考虑

$$x^d - a_i = \prod_{j=0}^{d-1} (x - \varepsilon^j \beta_i).$$

因此 K/F 为

$$(x^d - a_1) \cdots (x^d - a_{s-1}) \in F[x],$$

的分裂域.

然后我们重复定理 34.3.4 的证明. 记 $\varphi \in G$ 为 G 的生成元, 我们注意到

$$\text{Gal}(E/F) = \{\varphi^j \circ \psi \mid 0 \leq j \leq d-1, \psi \in H\}.$$

由 Dedekind 无关性定理, 我们有 $\beta \in E$, 满足

$$\alpha = \sum_{\psi \in H} \psi(\beta) + \varepsilon \sum_{\psi \in H} (\varphi \circ \psi)(\beta) + \cdots + \varepsilon^{d-1} \sum_{\psi \in H} (\varphi^{d-1} \circ \psi)(\beta) \neq 0.$$

由于 $\varphi(\alpha) = \varepsilon^{-1}\alpha$, 因此

$$\varphi(\alpha^d) = (\varphi(\alpha))^d = \alpha^d.$$

此外对任意 $\psi \in H$,

$$\psi(\alpha^d) = (\psi(\alpha))^d = \alpha^d.$$

因此 $\alpha^d \in F \subset K$. 由定理 34.3.4, 我们知道存在 $a_s = \alpha^d \in F \subset K$, 满足 E/K 为多项式

$$x^d - a_s \in F[x] \subset K[x],$$

的分裂域. 因此 E/F 为

$$(x^d - a_1) \cdots (x^d - a_s) \in F[x],$$

的分裂域. □

定义 34.4.2

设 E/F 为一个有限扩张. 我们称 E/F 为一个**指数 (exponent) 为 $d \in \mathbb{N}^*$ 的 Kummer 扩张**, 若 E/F 为多项式

$$(x^d - a_1) \cdots (x^d - a_s) \in F[x],$$

的分裂域扩张, 且 F 中有 d -阶本原单位根.

注 34.4.3.

注意到由之前关于本原单位根的存在性的讨论, 我们已经知道了 $\text{Ch}F \nmid d$, 因此, E/F 为一个 Galois 扩张.

我们下边考虑以上证明的关于 Kummer 扩张的反命题.

定理 34.4.4

设 E/F 为一个指数为 $d \in \mathbb{N}^*$ 的 Kummer 扩张, 则其 Galois 群 $\text{Gal}(E/F)$ 为有限交换群, 且 $\text{Gal}(E/F)$ 的零化指数整除 d .

证明. 记 $\varepsilon \in F$ 为一个 d -阶本原单位根. 设 E/F 为多项式

$$(x^d - a_1) \cdots (x^d - a_s) \in F[x],$$

的分裂域扩张. 对任意 $1 \leq i \leq s$, 记 $\alpha_i \in E$ 为 $x^d - a_i$ 的一个根. 则

$$E = F(\alpha_1, \dots, \alpha_s).$$

任取 $\varphi, \psi \in \text{Gal}(E/F)$, 任取 $1 \leq i \leq s$, 我们有

$$\varphi(\alpha_i) = \varepsilon^{m_i} \alpha_i, \quad \psi(\alpha_i) = \varepsilon^{n_i} \alpha_i.$$

因此我们有

$$(\varphi \circ \psi)(\alpha_i) = \varphi(\psi(\alpha_i)) = \varphi(\varepsilon^{n_i} \alpha_i) = \varepsilon^{m_i + n_i} \alpha_i = \psi(\varepsilon^{m_i} \alpha_i) = \psi(\varphi(\alpha_i)) = (\psi \circ \varphi)(\alpha_i).$$

因此我们有 $\varphi \circ \psi = \psi \circ \varphi$, $\text{Gal}(E/F)$ 为一个有限交换群. 考虑

$$\varphi^d(\alpha_i) = \varepsilon^{dm_i} \alpha_i = \alpha_i,$$

因此 $\varphi \in \text{Gal}(E/F)$ 的阶整除 d . 因此 $\text{Gal}(E/F)$ 的零化指数整除 d . $\square$

34.5 多项式的根式解

关于可解群的讨论可以参考前边章节 10.7.

记 F 为一个域, 记 $f(x) \in F[x]$ 为一个可分多项式. 记 $G_f(F)$ 为 $f(x) \in F[x]$ 的 Galois 群. 我们称 $f \in F[x]$ 根式可解 (solvable by radicals), 若 f 在 F 的某个根式扩张里分裂. 我们将研究 f 有无根式解和 G_f 是否可解之间的关系. 我们将对两个方向分别进行讨论.

34.5.1 若 G_f 可解

定理 34.5.1

若 G_f 可解, 且 $\text{Ch}F \nmid |G_f(F)|$, 则 f 有根式解.

证明. 记 $n = |G_f(F)|$. 注意到 $\text{Ch}F \nmid n$, 因此我们可以讨论 F 上的 n -阶本原单位根. 若 F 中没有 n -阶本原单位根, 我们考虑 F 的关于某个 n -阶本原单位根的单扩张 $K = F(\varepsilon)$. 考虑 E/K 为 f 的分裂域扩张. 因此我们有如下扩张列 $E/K/F$. 注意到 f 和 $x^n - 1$ 都是 F 上的可分多项式, 因此 E/K 和 E/F 都是 Galois 扩张.

我们将 f 看作是 K 上的多项式, 则可考虑 $f(x) \in K[x]$ 的 Galois 群 $G_f(K)$. 注意到 $G_f(F)$ 和 $G_f(K)$ 都是 f 的在对应分裂域中根集的置换. 我们在做根的置换的时候需要保持根之间满足的在对应域上的代数关系. 由于前者需固定 F 中的元素, 后者需固定 K 中的元素, 因此后者可以看作是前者的子群:

$$G_f(K) < G_f(F).$$

由于 $G_f(F)$ 可解, 因此 $G_f(K)$ 可解. 因此存在以下有限的次正规子群列

$$\{id\} = H_s \triangleleft H_{s-1} \triangleleft \cdots \triangleleft H_0 = G_f(K),$$

满足对任意 $1 \leq i \leq s$, H_{i-1}/H_i 是一个循环子群. 由 Galois 基本定理, 我们可以找到一列域扩张

$$E = E_s \supset E_{s-1} \supset \cdots \supset E_0 = K,$$

满足对任意 $0 \leq i \leq s$,

$$H_i = \text{Gal}(E/E_i).$$

进一步由 Galois 基本定理我们还有

$$\text{Gal}(E_i/E_{i-1}) \cong H_{i-1}/H_i.$$

因此

$$[E_i : E_{i-1}] = |H_{i-1}/H_i|.$$

由于

$$|H_{i-1}/H_i| \mid |H_{i-1}| \mid |G_f(K)| \mid |G_f(F)| = n,$$

因此 $[E_i : E_{i-1}]$ 整除 n , 因此 $\text{Ch}E_{i-1} = \text{Ch}F$ 不整除 $[E_i : E_{i-1}]$. 此外 E_{i-1} 中包含 n -阶本原单位根, 因此也包含 $[E_i : E_{i-1}]$ -阶本原单位根, 由定理 34.3.4, 我们知道 E_i/E_{i-1} 是一个根式扩张. 由于 K/F 也是根式扩张, 因此 f 有根式解. $\square$

34.5.2 若 f 是根式可解的

现在我们考虑另一个方向

定理 34.5.2

设存在一列域扩张

$$E = E_s \supset E_{s-1} \supset \cdots \supset E_0 = F,$$

且对任意 $1 \leq i \leq s$, 存在 $\alpha_i \in E_i$, $n_i \in \mathbb{N}^*$, 满足

$$\alpha_i^{n_i} \in E_{i-1}, \quad E_i = E_{i-1}(\alpha_i),$$

且 $\text{Ch}F \nmid n_i$. 若 $f \in F[x]$ 在 E 中分裂, 则 G_f 可解.

定理证明第一次尝试. 我们记 $n = n_1 \cdots n_s$. 由于 $\text{Ch}E = \text{Ch}F$ 不整除任意 n_i , 因此 E 上有 n -阶本原单位根. 若 E 不包含 n -阶本原单位根, 我们考虑 E 的单扩张 $E(\varepsilon)$, 满足 ε 为一个 n -阶本原单位根. 考虑以下域扩张列

$$E(\varepsilon) = E_s(\varepsilon) \supset E_{s-1}(\varepsilon) \supset \cdots \supset E_1(\varepsilon) \supset E_0(\varepsilon) \supset E_0 = F.$$

注意到 $E(\varepsilon)/F$ 仍是根式扩张, 且对任意 $1 \leq i \leq s$, $E_i(\varepsilon)/E_{i-1}(\varepsilon)$ 均为 Galois 扩张. 此外 $F(\varepsilon)/F$ 也是 Galois 扩张. (这是由于若包含 n -阶本原单位根, 则对任意 $d \mid n$, 包含 d -阶本原单位根.) 同时 f 在 $E(\varepsilon)$ 上分裂. $\square$

我们下一步希望使用 Galois 对应来找到一列子群. 然而此处有一个问题就是由于正规扩张没有传递性, 因此我们并不知道 $E(\varepsilon)/F$ 是否是一个 Galois 扩张. 为了解决这个问题, 我们需要先介绍以下两个定理.

定理 34.5.3

设 K/F 为一个 Galois 扩张. 记 $L = K(\alpha)$, 满足存在 $n \in \mathbb{N}^*$, $\alpha^n \in K$, 且 $\text{Ch}F \nmid n$, 则存在一个域扩张 E/L , 满足 E/K 为根式扩张, 且 E/F 为 Galois 扩张.

证明. 记 ε 为 L 上的 n -阶本原单位根, 并考虑扩张列

$$L(\varepsilon)/L/K/F.$$

记 $a = \alpha^n \in K$, 我们在 $L(\varepsilon)[x]$ 中有

$$x^n - a = (x - \alpha) \cdots (x - \varepsilon^{n-1}\alpha).$$

因此 $L(\varepsilon)/K$ 为一个 Galois 扩张. 由条件我们有 K/F 为 Galois 扩张. 但我们不一定有 $L(\varepsilon)/F$ 为 Galois 扩张. 我们将构造 $L(\varepsilon)$ 的根式扩张 E 满足 E/F 为 Galois 扩张.

我们考虑 $\text{Gal}(K/F)$. 构造一个 $L(\varepsilon)$ 上一个关于这个群对称的多项式:

$$f(x) = \prod_{g \in \text{Gal}(K/F)} (x^n - g(a)).$$

考虑 $E/L(\varepsilon)$ 为 f 的分裂域扩张. 注意到

$$\text{Gal}(K/F)(a) \subset K,$$

因此 $f \in K[x]$. 因此 E/K 为 $f(x)$ 的分裂域扩张, 且是根式扩张.

另一方面, f 关于 $\text{Gal}(K/F)$ 作用对称, 且 K/F 为 Galois 扩张, 因此

$$f(x) \in F[x].$$

因此 E/F 为一个 Galois 扩张. □

定理 34.5.4

若有扩张列

$$K_s/K_{s-1}/\cdots/K_1/K_0 = F,$$

满足对任意 $1 \leq i \leq s$, 存在 $\alpha_i \in K_i$, 以及 $n_i \in \mathbb{N}^*$, 满足

$$\alpha_i^{n_i} \in K_{i-1}, \quad K_i = K_{i-1}(\alpha_i),$$

且 $\text{Ch}F \mid n_1 \cdots n_s$, 则存在 E/K_s , 满足 E/F 为 Galois 根式扩张.

证明. 我们对 s 使用归纳法.

当 $s = 0$ 时, $K_0 = F$. 因此取 $x^n - 1 \in F$, 考虑 E/F 为 $x^n - 1$ 的分裂域即满足要求.

下设结论对 $0 \leq i \leq s-1$ 都整理, 因此我们有 L/K_{s-1} , 满足 L/F 为 Galois 根式扩张. 考虑多项式

$$f(x) = x^{n_s} - \alpha_i^{n_s} \in K_{s-1}[x].$$

记 $f_1(x)$ 为 α_i 在 $K_{s-1}[x]$ 中的最小多项式. 记 $h(x) \in L[x]$ 为 $f_1(x)$ 的一个不可约因子, 我们考虑

$$L_1 \cong L[x]/\langle h(x) \rangle.$$

因此存在 $\beta \in L_1$, 满足

$$h(\beta) = f(\beta) = 0.$$

因此我们有域同态:

$$\iota: K_s \rightarrow L_1,$$

满足 $\iota|_{K_{s-1}} = id_{K_{s-1}}$. 我们可以将 K_s 看作是 L_1 的子域.

至此, 我们有 $L_1/L/F$ 满足前一个定理的条件, 因此存在一个 L_1 的扩张 E , 满足 E/F 为 Galois 扩张, 且 E/L 为根式扩张.

由于根式扩张具有传递性, 因此 E/F 也是根式扩张. 定理得证. □

定理 34.5.2 的证明. 由之前的定理, 我们不妨假设 E/F 是一个 Galois 扩张. 因此对任意 $1 \leq i \leq s$, E/E_i 都是 Galois 扩张. 由于 $x^{n_i} - \alpha_i^{n_i}$ 在 E 中分裂, E 中有 n_i -阶本原单位根. 我们记 n 为 n_i 的最小公倍数, 因此我们有 E 中有 n -阶本原单位根, 记为 ε . 考虑以下域扩张列

$$E = E_s \supset E_{s-1}(\varepsilon) \supset \cdots \supset E_1(\varepsilon) \supset E_0(\varepsilon) \supset E_0 = F.$$

由 Galois 基本定理, 我们有以下次正规子群列:

$$\{id\} = H_s \triangleleft H_{s-1} \triangleleft \cdots \triangleleft H_0 \triangleleft H'_0,$$

满足对任意 $0 \leq i \leq s$, 我们有

$$H_i = \text{Gal}(E(\varepsilon)/E_i(\varepsilon)),$$

并有

$$H_0 = \text{Gal}(E(\varepsilon)/F).$$

对任意 $1 \leq i \leq s$, 我们有

$$H_{i-1}/H_i = \text{Gal}(E(\varepsilon)/E_{i-1}(\varepsilon))/\text{Gal}(E(\varepsilon)/E_i(\varepsilon)) \cong \text{Gal}(E_i(\varepsilon)/E_{i-1}(\varepsilon))$$

由之前对循环扩张的讨论, 我们知道 $\text{Gal}(E_i(\varepsilon)/E_{i-1}(\varepsilon))$ 为一个循环群. 同时由于 $F(\varepsilon)/F$ 为 $x^n - 1 \in F[x]$ 的分裂域扩张, 因此 $\text{Gal}(F(\varepsilon)/F)$ 为一个交换群. 因此 H'_0/H_0 是一个交换群. 因此 $\text{Gal}(E(\varepsilon)/F)$ 为一个可解群.

由于 f 在 $E(\varepsilon)$ 中分裂, 因此存在 K 为 $E(\varepsilon)/F$ 的中间域, 且 K/F 为 f 的分裂域扩张. 因此 K/F 为一个正规扩张. 由 Galois 基本定理, 我们有

$$G_f(F) \cong \text{Gal}(K/F) \cong \text{Gal}(E(\varepsilon)/F)/\text{Gal}(E(\varepsilon)/K).$$

因此 $G_f(F)$ 可解. □

34.5.3 五次及以上多项式的可解性

在之前对交错群的部分, 我们在命题 8.3.7 中证明了当 $n \geq 5$ 的时候 A_n 是单群. 因此 A_n 不可解, 我们进而有 S_n 不可解. 因此, 若域 F 上的一个多项式 $f(x) \in F[x]$ 的 Galois 群满足 $G_f \cong S_n$, 则该多项式没有根式解.

这个结论在 $\mathbb{Q}$ 上的版本就是 Abel-Ruffini 定理.

定理 34.5.5 (Abel-Ruffini)

一个 $\mathbb{Q}$ 上一般的次数大于等于 5 的多项式不可解.

这里的"一般"可以在测度意义下理解为满足 Galois 群同构于 S_n 的多项式构成一个满测度子集.

当然当 $n \geq 5$ 的时候, S_n 不可解并不意味着 S_n 所有子群都不可解. 特别地, 若我们考虑 S_n 可递的子群, 是可以找到可解的子群的. 比如 $(12 \cdots n)$ 生成的循环群就是可解群. 因此, 并不是所有次数大于等于 5 的多项式都不可解. Galois 的工作给出了一个 $\mathbb{Q}$ 上多项式可解的充要条件.

定理 34.5.6 (Galois)

一个 $\mathbb{Q}$ 上的多项式可解当且仅当其 Galois 群可解.

这也给出了 Abel-Ruffini 定理的一个证明.

第七部分

范畴论

第三十五章 范畴论基础

我们在之前的章节中已经了解了多种代数结构. 在学习这些代数结构的过程中, 我们可能注意到有一些概念和结论虽然是关于不同的代数结构, 但是这些概念的引入, 构造以及一些结论的叙述以及证明都有一定的相似性. 比如, 我们在每种代数结构中都是通过集合加运算的方式引入的; 都可以讨论子结构和商结构; 同类型的代数结构之间都是通过与此类代数结构相容的映射联系起来的; 各种代数结构都有同态基本定理, 其叙述和证明有一定的相似性; 当我们考虑群的扩张和模的扩张的时候都引入了正合列的概念, 并且都有关于短正合列的短五引理; 关于群和模都有合成列的概念, 并且都有 Krull-Schmidt 定理等等. 这类相似性也会出现在不同的数学分支之间.

Eilenberg 和 MacLane 于二十世纪四十年代在对代数拓扑的研究中引入的范畴的概念为我们提供了一个框架, 使我们可以将这类相似性以一种严格的抽象的方式清晰的表现出来. 经过不断的发展, 在今天范畴论已经被广泛的应用在几乎所有的数学分支的研究中. 它可以帮助我们不同的理论以及不同的数学分支之间构造联系, 并用统一的范畴的语言表述出来 (参考 [22, 24]).

范畴论的一个基本概念是范畴. 每个范畴的基本构造包括两个部分: 范畴的对象以及将对象联系起来的态射. 每个态射都是从一个对象(被称为源)到另一个对象(被称为目标). 如果一个态射的目标和另一个态射的源相同, 那么这两个态射也可以复合起来. 例如, 在交换群的范畴里, 每个对象都是一个交换群, 不同对象之间的态射就是一个群同态.

范畴论的第二个基本概念是函子. 我们可以将其看作是范畴之间的"同态", 并利用它来构建范畴之间的联系. 简单的说, 从范畴 C_1 到 C_2 的函子以一种相容的方式将 C_1 的对象送到 C_2 的对象, 并将 C_1 的态射送到 C_2 的态射. 例如, 我们之前在讨论模的张量积的时候, 通过将任意左 R -模 M 与一个 R 模 D 做左张量积 $D \otimes_R M$, 我们可以构造从 R -模范畴到交换群范畴的函子.

范畴论的第三个基本概念是自然变换. 它帮助我们构建给定两个范畴之间的两个函子之间的联系. 实际上在最初引入范畴的概念的过程中, Eilenberg 和 MacLane 关心的就是某种自然变换. 他们在 [15] 中, 使用有限维向量空间作为例子来说明自然变换这个概念. 我们考虑一个 $\mathbb{R}$ 上的有限维线性空间 V . 通过考虑 V 的一组基及其对偶基, 我们可以得到 V 到 V^* 作为线性空间同构的. 然而这个同构依赖于 V 的基选取. 另一方面, 任给一个向量 $v \in V$, 考虑在 v 处取值, 我们得到一个 V^* 上的线性函数. 由此我们得到一个 V 到 V^{**} 的线性同构:

$$\alpha_V : V \rightarrow V^{**}.$$

我们注意到这个同构是不依赖于 V 的基的选取, 是"自然"的.

注意到以上线性同构 α_V 的构造方式并不依赖于 V 的选取, 并且我们还有以下进一步的观察. 设 V_1 和 V_2 为两个 $\mathbb{R}$ 上的有限维线性空间, 并记

$$L : V_1 \rightarrow V_2,$$

为一个线性映射, 则有唯一的一个 $(V_1)^{**}$ 到 $(V_2)^{**}$ 的满足以下交换图的线性映射 L^{**} :

$$\begin{array}{ccc} V_1 & \xrightarrow{\alpha_{V_1}} & (V_1)^{**} \\ L \downarrow & & \downarrow L^{**} \\ V_2 & \xrightarrow{\alpha_{V_2}} & (V_2)^{**} \end{array}$$

我们后边会看到取两次对偶是一个线性空间范畴到自己的函子. 此外, 如果将任意 V 送到 V , 任意 L 送到 L , 我们就有了一个恒等的函子. 以上构造的一系列 α_V 实际上给出了两个函子之间一个"自然"的联系.

在本章中, 我们将对范畴的这些基本概念做一个介绍. 需要注意的是, 范畴论是一种高度抽象的理论, 因此我们在介绍的过程中需要通过观察大量的实例来熟悉并理解范畴论所要说明的内容.

35.1 范畴

我们首先给出范畴的定义.

定义 35.1.1

一个**范畴** C 包含:

- $\text{Ob } C$: 一族**对象** $A, B, C, \dots$,
- $\text{Mor } C$: 一族**态射**(或者**箭头**) $f, g, h, \dots$,

满足

- 1) 每一个态射 f 都有一个对象作为**源**(记作 $\text{dom}(f)$) 和一个对象作为**目标**(记作 $\text{cod}(f)$);
- 2) 每一个对象 A 都有一个源和目标都是 A 的**恒等态射**(记作 1_A);
- 3) 任取态射 f 和 g , 若 $\text{cod}(f) = \text{dom}(g)$, 则我们有唯一的一个从 $\text{dom}(f)$ 到 $\text{cod}(g)$ 的态射作为态射 f 和 g 的**复合**, 并记作 gf .

态射的复合满足以下公理:

- a) 任取态射 f , 有 $1_{\text{cod}(f)}f = f1_{\text{dom}(f)} = f$;
- b) 任取态射 f, g 和 h , 若三个态射满足条件 $\text{cod}(f) = \text{dom}(g)$ 和 $\text{cod}(g) = \text{dom}(h)$, 则我们有 $f(gh) = (fg)h$.

注 35.1.2.

从恒等态射的性质可以看出, 对任意范畴的任意对象 A , 其对应的恒等态射是唯一的. 由此我们可以得到一个范畴中所有对象的全体和所有恒等态射的全体之间的一个天然的一一对应.

为了方便讨论, 我们通常使用记号 $f: A \rightarrow B$ 或者 $A \xrightarrow{f} B$ 来记一个以 A 为源并以 B 为目标的态射 f . 需要注意的是, 虽然我们借用了之前映射的记号, 但是这里我们想表达的仅仅是 f 将 A 和 B 联系了起来, 范畴结构的定义关心的是这样的联系是否可以复合, 是否满足结合律, 是否有一个特殊的记为恒等态射的联系. 而具体每个对象代表什么, 以及每个态射是如何得到的, 则需要考虑具体的例子.

类似的情况也出现在之前对各种代数结构的讨论中. 例如, 群结构的抽象定义只关心的是集合上是否有一个二元运算, 并且这个运算是否满足结合律, 有么元, 任意元素都有逆元的性质. 至于这个群的元素代表什么, 二元运算是如何得到的, 这个取决于我们考虑的例子是什么. 从这个角度我们也可以理解一点为什么我们称范畴论是一个高度抽象的语言.

在后续的讨论中, 我们将会在一些例子中看到, 态射或者箭头的定义并不总是来自于映射. 有时我们也会将一个态射的箭头反向来构造态射. 如果 A 和 B 都是集合, 态射 f 来自于一个 A 到 B 的映射, 当我们将 f 的箭头反向的时候, 仅仅是得到一个从 B 到 A 的态射. 读者不需要纠结于所得的态射是否来自于一个映射之类的疑惑.

我们也可以使用另一种理解范畴结构的方法. 一个图是由点和连接点的线构成的. 我们称一个图是有向的如果任意一个连接两个点之间的线都有一个方向. 通过将一个范畴中的对象看作点, 态射看作有向的连接点的线, 我们可以将这个范畴结构等同于一个有向图.

例 35.1.3.

我们首先来看一些来自之前的章节内容的范畴的例子.

范畴	记号	对象	态射
么半群	Monoid	么半群	么半群同态
群	Group	群	群同态
交换群	Ab	交换群	群同态
环	Ring	环	环同态
交换环	CRing	交换环	环同态
域	Field	域	域同态
左 R -模	$_R\mathbf{Mod}$	左 R -模	左 R -模同态
右 R -模	$\mathbf{Mod}_R$	右 R -模	右 R -模同态
F -向量空间	$\mathbf{Vect}_F$	F -向量空间	F -线性变换

由于以上各个例子中的态射都来自于例子中的对象之间的映射, 考虑映射的复合, 我们就得到了态射的复合.

例 35.1.4.

正如在本章开头提到的, 范畴论也在其它数学分支的研究中发挥作用. 我们这里给出一些与其它数学分支相关的范畴的例子.

- 1) 在拓扑领域中, 我们主要研究的是空间的拓扑结构的性质. 拓扑空间之间与拓扑结构相容的映射是连续映射. 我们可以考虑所有的拓扑空间, 以及相互之间的连续映射, 得到拓扑空间的范畴, 记作 **Top**.
- 2) 在黎曼几何领域中, 我们主要研究的是带有黎曼度量的微分流形的性质. 微分流形是一个带有微分结构的局部上和 $\mathbb{R}^n$ 相同的拓扑空间. 微分流形之间是通过具有光滑性的连续映射联系起来的. 我们可以构造光滑流形范畴 **Mfld**, 即对象为光滑微分流, 态射为光滑映射的范畴.
- 3) 我们也可以将所有具有偏序关系的集合作为对象, 并将这些集合之间保持偏序关系的映射作为态射来构造一个范畴 **Pset**.
- 4) 当然我们也可以考虑将所有的集合都看作对象, 然后将所有的集合之间的映射作为态射来得到一个集合的范畴 **Set**. 注意到空集 $\emptyset$ 也是一个集合. 任给一个集合 A , 都有唯一的一个映射 $f: \emptyset \rightarrow A$. 另一方面, 若 A 非空, 则不存在 A 到 $\emptyset$ 的映射. 从集合论的角度来看, 一个从集合 B 到集合 C 的映射 φ 是 $B \times C$ 的一个满足如下条件的子集: 任取 $b \in B$, 存在 $c \in C$, 满足 $(b, c) \in \varphi$. 若 B 为空集, 则 $\emptyset \times C = \emptyset$ 有唯一的子集 $\emptyset$, 且以上条件自然满足. 因此有唯一的映射 $\varphi: \emptyset \rightarrow C$. 另一方面, 若 C 为空集, 且 B 非

空, 则任取 $b \in B$, 不存在 $c \in C$, 满足 $(b, c) \in B \times \emptyset = \emptyset$ (其中没有元素). 因此不存在 B 到 $\emptyset$ 的映射.

类似于之前的例子, 这里所有例子中的态射都来自于对象间的映射, 因此考虑映射的复合, 我们就有态射的复合.

注 35.1.5.

罗素悖论告诉我们不存在包含所有集合的集合. 考虑群范畴 **Group**, 由于我们可以在任意的集合上构造群结构, 范畴 **Group** 中所有的对象并不构成集合. 由此可见, 我们考虑的范畴的所有对象或者所有态射所构成的并不一定总是集合. 因此我们在定义范畴的时候并没有使用 "集合" 这个术语.

针对这个问题的一种处理办法是使用 Zermelo–Fraenkel 公理系统给出的小集合/大集合, 或者集合/类的概念. 另一种处理办法是通过引入新公理的方式引入 "宇宙" 这个概念. 笼统地说, 由于所有的集合不构成集合, 我们就在集合的基础上引入一个新的概念, 比如 "大集合". 由于所有大集合的放在一起也会面临相同的问题, 我们就在此基础上引入一个新的概念, 比如 "超大集合". Grothendieck 宇宙就是沿着这个思路的一种严格化的结果. 关于这部分内容的详细讨论见 [6].

以上讨论的这个与集合论有关的问题在构建范畴论的时候是应该被严肃对待的. 不过本部分的主要目的是介绍范畴论的基础, 并借助之前部分的内容使读者对范畴论的基本概念和结论有初步的了解. 对该问题过多的关注可能会增加读者对本章内容在理解上的复杂度, 从而偏离撰写本部分的初衷. 因此我们将不对这个问题做过多的讨论, 暂用 "一族" 或 "全体" 这样的笼统的说法. 此外集合之间的映射也可以被推广到对比集合更一般的概念的讨论中, 我们也不在此做详细讨论, 而是仍直接使用 "映射" 这个称呼.

定义 35.1.6

如果一个范畴所有的态射构成一个集合, 我们称该范畴为一个**小范畴**. 如果一个范畴不是小范畴, 我们称之为一个**大范畴**.

由之前的讨论, 一个范畴中任意一个对象对应唯一的一个恒等态射. 因此一个小范畴中的对象的全体也是一个集合. 另一方面, 我们注意到之前给出的范畴的例子中的对象都不构成集合, 因此所涉及的范畴都不是小范畴. 不过它们有另一个共同的特征: 任意两个对象之间的所有态射的全体构成一个集合.

定义 35.1.7

如果一个范畴中, 任意两个对象之间的态射构成集合, 那么我们称该范畴为一个**局部小**的范畴.

注 35.1.8.

我们在之前对代数结构的讨论中经常使用 $\text{Hom}(A, B)$ 来记两个具有同类型的代数结构的对象 A 和 B 之间的同态的集合. 在所涉及的代数结构的范畴中, 我们沿用这个记号 $\text{Hom}(A, B)$ 来记以对象 A 为源并以对象 B 为目标的所有态射构成的集合, 并将该记号推广到对一般的局部小的范畴的讨论中.

若范畴 C 是局部小的, 任给其中的两个对象 A 和 B , 我们用 $\text{Hom}(A, B)$ 来记所有以 A 为源, 以 B 为目标的态射构成的集合, 有时为了包含范畴的信息, 我们也会使用记号

$\text{Hom}_C(A, B)$ 或 $\mathcal{C}(A, B)$ 来表示这个集合. 当我们考虑一般的范畴的时候, 给定的两个对象之间的所有态射的全体并不一定是一个集合. 不过为了方便讨论, 我们将仍使用这个记号.

之前表格中的例子以及例子 1)–4) 有一个共同的特点: 每一个范畴都对应于某种 (代数, 拓扑, 集合等等) 结构, 其中的对象都是带有该类型结构的集合, 而态射是由两个对象之间与该类型结构相容的映射给出的. 下边几个例子将告诉我们这样的性质并不是一个范畴必须具有的.

- 例 35.1.9.** 1) 记 R 为一个交换幺环. 我们将所有非零自然数看作对象, 任给两个非零自然数 m 和 n , 我们考虑所有大小为 $n \times m$ 的 R -矩阵, 将每个矩阵定为一个从 m 到 n 的态射. 任给态射 $m \xrightarrow{M} n$ 和 $n \xrightarrow{N} k$, 考虑矩阵乘法, 我们有复合态射 $m \xrightarrow{NM} k$. 对每个 $m \in \mathbb{N}^*$, 其对应的恒等态射为 m -阶单位阵给出的态射. 我们将这样构造出的范畴记作 Mat_R , 并称之为环 R 上的矩阵范畴.
- 2) 任给一个群 G , 我们可以构造一个仅包含 G 作为唯一的对象的范畴 (记作 $\mathbf{BG}$). 该范畴的态射为 G 的元素, 而态射的复合来自于 G 的运算. 这里要说明的是, 任意元素 $g \in G$ 都只是形式上给出一个态射, 记号 $g: G \rightarrow G$ 也仅是形式记号. 我们并没有将其看作为一个明确的映射 G 到 G 的映射. 我们也可以从一般的带幺元的半群出发来做类似的构造.
- 3) 任给一个具有偏序关系 $\leq$ 的非空集合 P , 任取 $x, y \in P$, 我们定义存在 $x \rightarrow y$ 当且仅当 $x \leq y$. 偏序关系满足传递性. 任取 $x, y, z \in P$, 若有 $x \leq y$ 以及 $y \leq z$, 则有 $x \leq z$. 因此任给态射 $x \rightarrow y$ 和 $y \rightarrow z$, 我们将 $x \leq z$ 对应的态射 $x \rightarrow z$ 定为二者的复合. 偏序关系满足自反性, 因此对任意 $x \in P$, 都有 $x \leq x$. 我们将 $x \leq x$ 对应的态射定为 x 到自己的恒等态射 1_x . 在这个设定下, 我们可以验证态射复合满足的公理. 因此以上构造给出一个范畴 (记作 $(P, \leq)$).
- 4) 如果一个范畴中除了恒等态射以外没有其它的态射, 我们称之为一个**离散范畴**.
- 5) 如果一个范畴 $\mathcal{C}$ 满足 $\text{Ob } \mathcal{C} = \emptyset$ 以及 $\text{Mor } \mathcal{C} = \emptyset$, 我们称之为**空范畴**, 记作 $\mathbf{0}$.

在我们讨论代数结构的时候, 每种代数结构对应的同态帮助我们在具有该类型代数结构的不同对象之间建立了联系. 我们可以进一步使用同态去比较具有同类型代数结构的对象. 如果两个具有同类型代数结构的对象之间可以通过同态建立元素间一一对应, 也即存在一个既是单射又是满射的同态, 那么我们就称二者在代数意义下是相同的, 也即二者是同构的. 我们可以将同构的概念推广到对一般的范畴的讨论中.

我们记 $\mathcal{C}$ 为一个范畴.

定义 35.1.10

任取 $\mathcal{C}$ 中的一个态射 $A \xrightarrow{f} B$, 若存在一个态射 $B \xrightarrow{g} A$, 满足

$$fg = 1_B \quad \text{且} \quad gf = 1_A,$$

我们称态射 f 为一个**同构**.

任取 $\mathcal{C}$ 中的两个对象 A 和 B , 若存在同构从 A 到 B 的同构, 我们称 A 和 B **同构**, 并记作 $A \cong B$.

任取 $\mathcal{C}$ 中的两个对象 A 和 B , 我们仍借用之前对代数结构讨论中的记号, 用 $\text{Isom}(A, B)$ 来记所有以 A 为源并以 B 为目标的同构的全体 (可能为空集). 如果 $\mathcal{C}$ 中的一个态射 f 的

源和目标都为对象 A , 我们称 f 为 A 的一个**自同态**. 如果进一步有 f 为一个同构, 我们称 f 为 A 的一个**自同构**. 我们记 A 的自同态的全体和自同构的全体分别为 $\text{End}(A)$ 和 $\text{Aut}(A)$.

我们来观察一下之前提到的一些范畴中构成同构的态射.

例 35.1.11. 1) 任意一个范畴中的恒等态射都是同构态射.

2) 各种代数结构范畴中的同构态射就是由相应代数结构同构给出的态射给出, 比如群范畴 **Group** 中的群同构给出的态射, 环范畴 **Ring** 中的环同构给出的态射等等.

3) 拓扑空间范畴 **Top** 中的同构态射由拓扑空间之间的同胚映射给出.

4) 集合范畴 **Set** 中的同构态射由双射给出.

5) 交换幺环 R 上的矩阵范畴 Mat_R 中的同构态射由可逆方阵给出.

6) 任意一个群 G 对应的范畴 **BG** 中所有的态射都是同构态射.

7) 任取一个偏序集 P , 考虑到偏序关系的反对称性, 范畴 $(P, \leq)$ 中的同构态射只有恒等态射.

定义 35.1.12

如果一个范畴中的任意一个态射都是同构, 我们称这个范畴是一个**群胚**.

例 35.1.13 (群作为一个范畴).

我们之前提到一个群 G 给出的范畴 **BG** 中所有的态射都是同构. 反过来, 如果一个范畴 $\mathcal{C}$ 是只有一个对象的小群胚, 那么其所有的态射构成一个群. 因此我们也可以将群等同于一个只有一个对象的小群胚.

例 35.1.14 (三角剖分范畴).

任给一个欧式平面中的边数大于等于 4 的多边形 P 区域, 我们可以考虑添加两两不相交的对角线的方式对其做三角剖分, 即当我们沿着这些对角线切割之后得到的是有限多个三角形. 注意到 P 的三角剖分并不唯一. 通过简单的分析, 我们会发现所有的 P 的三角剖分需要的对角线数目是相同的. 下边我们将构造一个 P 的 Ptolemy 群胚 $\mathbf{Pt}(P)$.

为了方便讨论, 我们定义 P 的一个三角剖分为 P 的一族对角线 T , 满足 $P \setminus (\cup T)$ 为一族三角形区域. 任给 P 的一个三角剖分 T , 注意到每个对角线 $\alpha \in T$ 都在 P 的一个四边形区域 Q 中, 并且 Q 的边界是 P 的边界或者是 T 中的对角线. 注意到 Q 除了 α 之外, 还有另一个对角线 β . 我们用 β 替换 α 的到一个新的对角线的集合 $T' = (T \setminus \{\alpha\}) \cup \{\beta\}$, 也构成 P 的一个三角剖分. 我们称这样对三角剖分的改变为一个基本操作.

由于 P 只有有限多个对角线, 通过直接验证, 我们可以得到以下两个关于基本操作的事实. 第一个是任何一个基本操作都是可逆的. 如果使用以上的记号, 当我们从 T 得到 T' 之后, 可以对 T' 通过用 α 替换 β 继续做一个基本操作. 这样我们就又回到了 T . 第二个是任取 P 的两个三角剖分 T_1 和 T_2 , 我们都可以通过对 T_1 进行一系列的基本操作得到 T_2 .

我们定义 $\mathbf{Pt}(P)$ 的对象为 P 的三角剖分, 其中的态射为所有的任意有限多个基本操作的复合. 在这个定义下, 态射的复合是定义良好的, 并且满足结合律; 同时, 任给一个 P 的三角剖分 T , 其对应的恒等态射就是将 T 送到 T 的基本操作的复合; 最后, 由之前对基本操作的讨论可知, 任何态射都是同构. 因此, 我们有了一个小群胚. 注意到 P 只有有限多个对角线和有限多个三角剖分, 因此 $\mathbf{Pt}(P)$ 是一个小范畴.

子范畴

类似于对代数结构的讨论, 我们这里也可以观察一个范畴的一部分是否构成范畴, 从而得到子范畴的概念.

定义 35.1.15

记 $\mathcal{C}$ 为一个范畴. 如果一个范畴 $\mathcal{D}$ 中的对象和态射是 $\mathcal{C}$ 中的对象和态射, 并且 $\mathcal{D}$ 中的恒等态射和复合规则也与 $\mathcal{C}$ 中的相同. 我们称 $\mathcal{D}$ 为 $\mathcal{C}$ 的一个**子范畴**.

我们下边考虑一下之前的一些例子中的范畴的子范畴.

例 35.1.16. 1) 交换群范畴 **Ab** 是 **Group** 的子范畴.

2) 域范畴 **Field** 是环范畴 **Ring** 的子范畴

3) 光滑流形范畴 **Mfld** 是拓扑空间范畴 **Top** 的子范畴.

4) 偏序集的范畴 **Pset** 是集合范畴 **Set** 的子范畴.

综合之前关于群胚和子范畴的讨论, 我们有以下三个事实:

命题 35.1.17

- 1) 任给一个范畴 $\mathcal{C}$, 考虑其中所有的对象, 以及所有的恒等态射, 我们得到了 $\mathcal{C}$ 的一个构成离散范畴的子范畴.
- 2) 任给一个范畴 $\mathcal{C}$, 考虑其中一部对象, 以及所有的这些对象之间的态射, 我们得到 $\mathcal{C}$ 的一个子范畴. 特别地, 任取 $\mathcal{C}$ 的对象 A , 考虑所有 A 到 A 的态射, 我们得到 $\mathcal{C}$ 的一个子范畴.
- 3) 任给一个范畴 $\mathcal{C}$, 考虑其中一部对象, 以及所有的这些对象之间构成同构的态射, 我们得到 $\mathcal{C}$ 的一个构成群胚的子范畴. 特别地, 任取 $\mathcal{C}$ 的对象 A , 考虑所有 A 到 A 的构成同构的态射, 我们得到 $\mathcal{C}$ 的一个构成群胚的子范畴. 如果进一步 $\text{Isom}(A, A)$ 为一个集合, 则 $\text{Isom}(A, A)$ 关于态射的复合构成一个群.

证明. 证明可以通过直接验证定义得到, 此处省略. □

两个范畴的笛卡尔积和不交并

在之前对代数结构的讨论中, 任给两个同类型的代数结构, 我们可以通过做直和等方式来构造新的同类型的代数结构. 这里我们介绍两种常见的从两个范畴出发来构造新范畴的方法: 取笛卡尔积和取不交并.

任取范畴 $\mathcal{C}$ 和 $\mathcal{D}$, 我们定义二者的**笛卡尔积** $\mathcal{C} \times \mathcal{D}$ 为满足以下条件的范畴:

- 其中任意一个对象为一个有序对 (A, X) , 满足 $A \in \text{Ob } \mathcal{C}$ 和 $X \in \text{Ob } \mathcal{D}$, 即

$$\text{Ob } (\mathcal{C} \times \mathcal{D}) = \text{Ob } \mathcal{C} \times \text{Ob } \mathcal{D};$$

- 其中任意一个的态射一个有序对 (f, u) , 满足 $f \in \text{Mor } \mathcal{C}$ 和 $u \in \text{Mor } \mathcal{D}$, 即

$$\text{Mor } \mathcal{C} \times \mathcal{D} = \text{Mor } \mathcal{C} \times \text{Mor } \mathcal{D};$$

- 两个态射 (f, u) 和 (g, v) 之间的复合定义为

$$(f, u)(g, v) = (fg, uv).$$

范畴 $\mathcal{C}$ 和 $\mathcal{D}$ 的不交并 $\mathcal{C} \amalg \mathcal{D}$ 则被定义为满足如下条件的范畴:

- $\text{Ob}(\mathcal{C} \amalg \mathcal{D}) = \text{Ob}\mathcal{C} \amalg \text{Ob}\mathcal{D}$, 即为 $\text{Ob}\mathcal{C}$ 和 $\text{Ob}\mathcal{D}$ 的不交并;
- $\text{Mor}(\mathcal{C} \amalg \mathcal{D}) = \text{Mor}\mathcal{C} \amalg \text{Mor}\mathcal{D}$, 即为 $\text{Mor}\mathcal{C}$ 和 $\text{Mor}\mathcal{D}$ 的不交并;
- 由以上构造可以看出两个 $\mathcal{C} \amalg \mathcal{D}$ 中的态射可以复合仅当他们同为 $\mathcal{C}$ 中的态射或者同为 $\mathcal{D}$, 我们直接沿用 $\mathcal{C}$ 和 $\mathcal{D}$ 中态射复合即得 $\mathcal{C} \amalg \mathcal{D}$ 中态射得复合.

我们可以通过直接验证范畴的定义中的条件来说明以上两个范畴定义良好.

例 35.1.18.

任取两个群 Γ 和 Γ' , 我们可以定义 $\Gamma \oplus \Gamma'$ 为二者的直和. 考虑范畴的笛卡尔积 $\mathbf{B}\Gamma \times \mathbf{B}\Gamma'$. 我们有一个自然的 $\mathbf{B}\Gamma \times \mathbf{B}\Gamma'$ 到 $\mathbf{B}(\Gamma \oplus \Gamma')$ 的函子 F 定义如下:

$$F_0(\Gamma, \Gamma') = \Gamma \oplus \Gamma',$$

考虑 Γ 和 Γ' 到 $\Gamma \oplus \Gamma'$ 的群同态

$$\begin{array}{ccc} i : \Gamma \rightarrow \Gamma \oplus \Gamma' & \text{和} & i' : \Gamma' \rightarrow \Gamma \oplus \Gamma' \\ a \mapsto (a, e') & & a' \mapsto (e, a') \end{array}$$

由此, 我们得到 $\mathbf{B}\Gamma \times \mathbf{B}\Gamma'$ 到 $\mathbf{B}(\Gamma \oplus \Gamma')$ 的态射之间的对应:

$$\begin{array}{ccc} F_1 : \text{Mor}(\mathbf{B}\Gamma \times \mathbf{B}\Gamma') & \rightarrow & \text{Mor}\mathbf{B}(\Gamma \oplus \Gamma') \\ (a, a') & \mapsto & (a, a'). \end{array}$$

下边我们考虑群胚范畴 $\mathbf{B}\Gamma$ 和 $\mathbf{B}\Gamma'$ 的不交并, 并说明这与群之间的自由积相关. 记 $\Gamma * \Gamma'$ 为这两个群的自由积. 我们有一个自然的 $\mathbf{B}\Gamma \amalg \mathbf{B}\Gamma'$ 到 $\mathbf{B}(\Gamma * \Gamma')$ 的函子 G 定义如下. 关于对象, 我们有

$$G_0(\Gamma) = G_0(\Gamma') = \Gamma * \Gamma',$$

将 Γ 和 Γ' 中的元素看作 $\Gamma * \Gamma'$ 中的元素, 我们得到 Γ 和 Γ' 到 $\Gamma * \Gamma'$ 自然的嵌入同态

$$\begin{array}{ccc} j : \Gamma \rightarrow \Gamma * \Gamma' & \text{和} & j' : \Gamma' \rightarrow \Gamma * \Gamma' \\ a \mapsto a & & a' \mapsto a' \end{array}$$

由此我们得到态射之间的对应关系:

$$G_1 : \text{Mor}(\mathbf{B}\Gamma \amalg \mathbf{B}\Gamma') \rightarrow \text{Mor}\mathbf{B}(\Gamma * \Gamma').$$

注 35.1.19.

我们在后续对积和余积的部分对这类构造做进一步地讨论.

35.2 对偶

在之前的讨论中, 我们提到可以通过将态射的箭头反向来构造新的态射. 由此我们引入反范畴的概念.

定义 35.2.1

记 $\mathcal{C}$ 为一个范畴. 我们称以下构造的范畴为 $\mathcal{C}$ 的**反范畴**, 并记作 $\mathcal{C}^{\text{op}}$:

- $\text{Ob } \mathcal{C}^{\text{op}}$ 由 $\mathcal{C}$ 中所有的对象构成;
- $\text{Mor } \mathcal{C}^{\text{op}}$ 和 $\text{Mor } \mathcal{C}$ 之间通过箭头反射构建出一个一一对应, 即
 - 任给 $\mathcal{C}$ 中的一个态射 $A \xrightarrow{f} B$, 都有 $\mathcal{C}^{\text{op}}$ 中的唯一的一个态射 $B \xrightarrow{f^{\text{op}}} A$ 与之对应;
 - 任给 $\mathcal{C}^{\text{op}}$ 中的一个态射 $B \xrightarrow{g} A$, 都有 $\mathcal{C}$ 中的一个态射 $A \xrightarrow{f} B$, 满足 $g = f^{\text{op}}$;
- 该一一对应与态射的复合相容, 即任取 $\mathcal{C}$ 中的态射 f 和 g , 考虑其对应的 $\mathcal{C}^{\text{op}}$ 中的态射 f^{op} 和 g^{op} , 我们有

$$(fg)^{\text{op}} = g^{\text{op}} f^{\text{op}}.$$

- 任取 $\mathcal{C}^{\text{op}}$ 中的对象 A , 其对应的恒等态射为 1_A^{op} .

注 35.2.2.

形式上看, 箭头反转两次就回到了初始状态. 因此我们可以将 $(\mathcal{C}^{\text{op}})^{\text{op}}$ 和 $\mathcal{C}$ 自然的等同起来. 以下, 任取范畴 $\mathcal{C}$, 我们将记 $(\mathcal{C}^{\text{op}})^{\text{op}} = \mathcal{C}$.

反范畴的定义虽然只是形式上将箭头反向, 但是其所代表的构造在实际数学研究中并不少见. 我们这里给出几个例子.

例 35.2.3. 1) 记 R 为一个交换幺环. 我们考虑一个新的范畴 Mat_R^t . 这个范畴的对象为非零自然数. 任取对象 m 和 n , 从 m 到 n 的态射为大小为 $m \times n$ 的 R -矩阵. 任取态射 $m \xrightarrow{M} n$ 和 $n \xrightarrow{N} k$, 二者的复合定义为 $m \xrightarrow{MN} k$. 环 R 上的矩阵范畴 Mat_R 的反范畴 Mat_R^{op} 可以被等同为范畴 Mat_R^t .

- 2) 记 G 为一个群. 我们可以定义其对应的反群 G^{op} . 该群中的元素仍为 G 中的元素. 记群 G 中的运算为 $*$, 则其反群 G^{op} 中的运算定义如下:

$$\begin{aligned} \circ : G^{\text{op}} \times G^{\text{op}} &\rightarrow G^{\text{op}}, \\ (g, g') &\mapsto g' * g. \end{aligned}$$

群 G 对应的范畴 $\mathbf{BG}$ 的反范畴 $(\mathbf{BG})^{\text{op}}$ 可以被等同为范畴 $\mathbf{BG}^{\text{op}}$.

- 3) 任给一个具有偏序关系 $\leq$ 的非空集合 P , 任取 $x, y \in P$, 我们定义存在 $y \rightarrow x$ 当且仅当 $x \leq y$. 由此我们可以得到一个新的范畴 (记作 $(P, \geq)$). 范畴 $(P, \leq)$ 的反范畴 $(P, \leq)^{\text{op}}$ 可以被等同为范畴 $(P, \geq)$.

注 35.2.4.

以上例子中 "范畴之间的等同" 类似于之前讨论代数结构时的同构. 我们将在函子的部分对其意义做进一步说明.

从范畴和其反范畴的关系的出发, 我们可以进一步得到范畴论中的一个重要结论: **对偶原理**.

定理 35.2.5 (对偶原理)

如果一个结论 φ 对一个范畴 $\mathcal{C}$ 成立, 通过将 φ 中所有态射的箭头反向, 我们可以得到一个对 $\mathcal{C}^{\text{op}}$ 成立的对偶的结论 φ^{op} .

在对范畴的讨论中, 对偶原理可以给我们 "买一送一" 的效果. 注意到反范畴也是范畴. 如果一个结论对任意范畴成立, 那么这个结论对任意一个范畴 $\mathcal{C}$ 及其反范畴 $\mathcal{C}^{\text{op}}$ 同时成立. 那么关于 $\mathcal{C}^{\text{op}}$ 的结论可以看作是关于范畴 $\mathcal{C}$ 的结论的对偶的结论. 我们只需要把关于之前结论证明中的所有态射箭头反向, 就可以得到关于这个新结论的证明. 我们下边给出一个例子来进行说明.

命题 35.2.6

任取一个范畴 $\mathcal{C}$, 任取 $\mathcal{C}$ 的一个态射 $f : A \rightarrow B$, 则态射 f 为一个同构当且仅当对任意对象 $C \in \mathcal{C}$, 以下给出一个双射:

$$\begin{aligned} f_* : \text{Hom}(C, A) &\rightarrow \text{Hom}(C, B), \\ g &\mapsto fg. \end{aligned}$$

考虑以上结论关于 $\mathcal{C}^{\text{op}}$ 的叙述的对偶叙述, 我们有以下结论.

命题 35.2.7

任取一个范畴 $\mathcal{C}$, 任取 $\mathcal{C}$ 的一个态射 $f : A \rightarrow B$, 则态射 f 为一个同构当且仅当对任意对象 $C \in \mathcal{C}$, 以下给出一个双射:

$$\begin{aligned} f^* : \text{Hom}(A, C) &\rightarrow \text{Hom}(B, C), \\ g &\mapsto gf. \end{aligned}$$

我们给出命题 35.2.6 的证明, 将命题 35.2.7 的证明留作练习.

命题 35.2.6 的证明. 若 $f : A \rightarrow B$ 是一个同构, 则存在 $h : B \rightarrow A$, 满足 $hf = 1_A$ 且 $fh = 1_B$.

任取态射 $g, g' \in \text{Hom}(C, A)$, 如果有 $fg = fg'$, 考虑与 h 的复合, 我们有

$$g = 1_A g = (hf)g = h(fg) = h(fg') = (hf)g' = 1_A g' = g'.$$

因此 f_* 是单射. 另一方面, 任取 $\tilde{g} \in \text{Hom}(C, B)$, 我们有复合 $h\tilde{g} \in \text{Hom}(C, A)$, 满足

$$f(h\tilde{g}) = (fh)\tilde{g} = \tilde{g}.$$

因此 f_* 为满射, 进而有 f_* 为双射.

反之, 我们考虑 $C = B$, 由于

$$f^* : \text{Hom}(A, B) \rightarrow \text{Hom}(B, B),$$

为双射, 考虑 $1_B \in \text{Hom}(B, B)$, 存在一个 $h \in \text{Hom}(B, A)$, 满足 $fh = 1_B$.

另一方面, 复合 $hf \in \text{Hom}(A, A)$, 因此

$$f(hf) = (fh)f = f.$$

我们考虑 $C = A$, 由于

$$f^* : \text{Hom}(A, A) \rightarrow \text{Hom}(A, B),$$

为双射, 并且 $f1_A = f$, 因此我们有

$$hf = 1_A.$$

综上所述, 态射 f 为一个同构. □

注 35.2.8.

以上给出的只是形式上的定义和讨论. 对偶的现象在实际的数学研究中是经常出现的, 只不过形式上并不是如以上给出的那样. 我们之后会讲到函子的概念. 函子可以帮助我们联系不同的范畴. 从这个角度, 范畴和反范畴是通过一种所谓的 "反变函子" 联系起来的. 在实际研究中, 我们会见到很多自然的反变函子的例子. 反变函子有时可以联系来自不同领域的范畴, 并给出它们之间的对偶关系. 我们可以利用这种对偶关系将一个范畴内的问题转化为另一个范畴内的问题, 从而帮助我们简化问题并为我们提供新的解决问题的思路. 我们将在对反变函子的讨论中给出更多的例子.

以上两个命题给出了态射构成同构等价性质. 如果将这些性质中关于 f_* 和 f^* 的条件弱化, 我们就有了单态射和满态射的概念.

定义 35.2.9

任给一个范畴 $\mathcal{C}$, 考虑其中的一个态射 $f : A \rightarrow B$.

- 我们称态射 f 是一个**单态射**, 若任给 $\mathcal{C}$ 中的对象 C 以及态射 $g, h : C \rightarrow A$, 都有 $fg = fh$ 当且仅当 $g = h$;
- 我们称态射 f 是一个**满态射**, 若任给 $\mathcal{C}$ 中的对象 C 以及态射 $g, h : B \rightarrow C$, 都有 $gf = hf$ 当且仅当 $g = h$;

在以上两个命题的讨论中, 我们分别用到了同构的两个性质.

定义 35.2.10

任给一个范畴 $\mathcal{C}$, 考虑其中的一个态射 $f : A \rightarrow B$.

- 我们称态射 f **左可逆**, 若存在一个态射 $g : B \rightarrow A$, 满足 $gf = 1_A$;
- 我们称态射 f **右可逆**, 若存在一个态射 $g : B \rightarrow A$, 满足 $fg = 1_B$.

注 35.2.11.

使用类似证明命题 35.2.6 的方法, 我们可以看出任给一个范畴 $\mathcal{C}$, 考虑其中的一个态射 $f : A \rightarrow B$, 如果态射 f 左可逆, 则 f 是单态射; 如果 f 右可逆, 则 f 是满态射. 同时, 我们也有以下三个叙述等价:

- 1) 态射 f 为一个同构;
- 2) 态射 f 既是单态射又是满态射;
- 3) 态射 f 既是左可逆又是右可逆.

35.3 函子

类似于之前我们通过同态将同类型的代数结构联系起来, 两个范畴之间是通过函子联系起来的. 笼统地说, 一个从范畴 $\mathcal{C}$ 到范畴 $\mathcal{D}$ 的函子将 $\mathcal{C}$ 的对象和 $\mathcal{D}$ 的对象以及 $\mathcal{C}$ 的态射和 $\mathcal{D}$ 的态射分别联系起来, 同时这种联系还与 $\mathcal{C}$ 和 $\mathcal{D}$ 中的态射与对象之间的关系, 恒等态射以及态射的复合相容.

定义 35.3.1

一个从范畴 $\mathcal{C}$ 到 $\mathcal{D}$ 函子 $F = (F_0, F_1) : \mathcal{C} \rightarrow \mathcal{D}$ 由

$$F_0 : \text{Ob } \mathcal{C} \rightarrow \text{Ob } \mathcal{D} \quad \text{和} \quad F_1 : \text{Mor } \mathcal{C} \rightarrow \text{Mor } \mathcal{D},$$

两个映射构成, 并且二者满足以下条件:

- 1) 对任意 $f \in \text{Mor } \mathcal{C}$, 有 $\text{dom}(F_1(f)) = F_0(\text{dom}(f))$ 和 $\text{cod}(F_1(f)) = F_0(\text{cod}(f))$;
- 2) 对任意 $A \in \text{Ob } \mathcal{C}$, 有 $F_1(1_A) = 1_{F_0(A)}$;
- 3) 对任意 $f, g \in \text{Mor } \mathcal{C}$, 有 $F_1(fg) = F_1(f)F_1(g)$.

注 35.3.2.

利用一个范畴和其反范畴之间的联系, 范畴 $\mathcal{C}$ 到 $\mathcal{D}$ 的函子和范畴 $\mathcal{C}^{\text{op}}$ 到 $\mathcal{D}^{\text{op}}$ 之间存在着自然的一一对应.

我们可以通过函子的观点来重现观察之前的在讨论各种代数结构中出现的同态. 以下我们以群同态来进行说明.

例 35.3.3.

记 G 和 G' 为两个群. 我们首先考虑之前定义的群胚 $\mathbf{BG}$ 和 $\mathbf{BG}'$. 任何 G 到 G' 的群同态都可以看作是这两个群胚之间的函子. 更具体地, 我们设存在同态 $F : G \rightarrow G'$. 通过将对象 G 送到 G' , 并将态射 g 送到 $F(g)$, 由群同态的定义, 我们可以验证这个对应给出了两个群胚之间的函子.

群同态还可以在两个群的子群之间构建联系. 我们也可以从函子的角度来说明. 对群 G , 我们考虑 G 的子群作为对象, 任取 G 的两个子群 H_1 和 H_2 , 存在态射 $\iota : H_1 \rightarrow H_2$ 当且仅当 $H_1 < H_2$. 由此我们给出了 G 的子群范畴 $\mathbf{PG}$. 类似地, 我们也可以构造范畴 $\mathbf{PG}'$.

仍考虑群同态 $F : G \rightarrow G'$, 则我们可以定义映射

$$\begin{aligned} F_0 : \mathbf{PG} &\rightarrow \mathbf{PG}', \\ H &\mapsto F(H). \end{aligned}$$

另一方面, 任取 $\mathbf{PG}$ 的态射 $\iota : H_1 \rightarrow H_2$, 由定义我们有 $H_1 < H_2$. 由于 F 为同态, 我们有 $F_0(H_1) < F_0(H_2)$. 定义 $F_1(\iota)$ 为态射 $\iota' : F_0(H_1) \rightarrow F_0(H_2)$, 通过直接计算我们可以验证同态 F 通过 (F_0, F_1) 给出了 $\mathbf{PG}$ 到 $\mathbf{PG}'$ 的一个函子.

下边我们再来看一些函子的例子.

例 35.3.4. 1) 任给两个范畴 $\mathcal{C}$ 和 $\mathcal{D}$, 我们可以通过将所有 $\mathcal{C}$ 的对象送到 $\mathcal{D}$ 的某个对象 A , 并将所有 $\mathcal{C}$ 的态射送到 A 对应的恒等态射 1_A 来构造常值函子.

- 2) 如果一个范畴 $\mathcal{C}$ 是范畴 $\mathcal{D}$ 的子范畴, 那么从 $\mathcal{C}$ 到 $\mathcal{D}$ 自然的嵌入给出了一个包含函子 $\iota = (\iota_0, \iota_1)$, 其定义如下:

$$\begin{array}{ccc} \iota_0 : \text{Ob } \mathcal{C} \rightarrow \text{Ob } \mathcal{D} & \text{和} & \iota_1 : \text{Mor } \mathcal{C} \rightarrow \text{Mor } \mathcal{D} \\ A \mapsto A & & f \mapsto f \end{array}.$$

作为一个特殊情形, 当 $\mathcal{C} = \mathcal{D}$ 时, 我们称 ι 为恒等函子.

- 3) 任取一个集合 A , 我们可以考虑由其所有子集构成的幂集 $\mathcal{P}(A)$. 注意到任意集合 A 到集合 B 的映射 f 都可以诱导出幂集之间的映射

$$\begin{array}{l} \mathcal{P}(f) : \mathcal{P}(A) \rightarrow \mathcal{P}(B), \\ P \mapsto f(P). \end{array}$$

由此我们得到了一个集合范畴 **Set** 到自己的函子 F , 满足

$$F_0(A) = \mathcal{P}(A) \quad \text{且} \quad F_1(f) = \mathcal{P}(f).$$

- 4) 之前定义的很多范畴的对象都是具有相同类型的结构的集合, 而对象间的态射都是与该种结构相容的映射给出的. 因此我们可以通过将关于所涉及的结构的信息忘掉来构造这些范畴到集合范畴 **Set** 的函子. 例如, 考虑群范畴 **Group**, 我们可以如下定义函子 $F = (F_0, F_1)$:

$$\begin{array}{ccc} F_0 : \text{Ob } \mathbf{Group} \rightarrow \text{Ob } \mathbf{Set} & \text{和} & F_1 : \text{Mor } \mathbf{Group} \rightarrow \text{Mor } \mathbf{Set} \\ A \mapsto A & & f \mapsto f \end{array}.$$

并称这样的函子为遗忘函子.

此外一个集合上的某种类型的结构是在另一种类型的结构上附加一些条件得到的. 我们也可以在相关的范畴之间定义遗忘函子. 以下是一些例子

- 通过忘掉流形结构中的转移映射的光滑性, 我们有遗忘函子 $\mathbf{Mlfd} \rightarrow \mathbf{Top}$;
 - 记 F 为一个域, 通过忘掉纯量乘法, 我们有遗忘函子 $\mathbf{Vect}_F \rightarrow \mathbf{Ab}$;
 - 记 R 为一个幺环, 通过忘掉纯量乘法, 我们有遗忘函子 $\mathbf{Mod}_R \rightarrow \mathbf{Ab}$;
 - 通过忘掉环上的乘法结构, 我们有遗忘函子 $\mathbf{Ring} \rightarrow \mathbf{Ab}$.
- 5) 我们也可以通过向一个集合添加某种结构的方式来构造与遗忘函子方向相反的函子. 以群范畴 **Group** 为例. 任给一个集合, 我们都可以构造以这个集合的元素为自由基的自由群. 将集合 A 和 B 分别看作自由群 $\ast_{\alpha \in A} \mathbb{Z}$ 和 $\ast_{\alpha \in B} \mathbb{Z}$ 的自由基, 由自由群的泛性质, 任何映射 $f : A \rightarrow B$ 都可以延拓为一个群同态 $\tilde{f} : \ast_{\alpha \in A} \mathbb{Z} \rightarrow \ast_{\alpha \in B} \mathbb{Z}$. 由此, 我们构造了一个从 **Set** 到 **Group** 的函子:

$$\begin{array}{ccc} F_0 : \text{Ob } \mathbf{Set} \rightarrow \text{Ob } \mathbf{Group} & \text{和} & F_1 : \text{Mor } \mathbf{Set} \rightarrow \text{Mor } \mathbf{Group} \\ A \mapsto \ast_{\alpha \in A} \mathbb{Z} & & f \mapsto \tilde{f} \end{array}.$$

称之为自由函子. 类似地, 我们也可以构造 $\mathbf{Set} \rightarrow \mathbf{Ab}$, $\mathbf{Set} \rightarrow \mathbf{Mod}_R$ 等自由函子. 注意到这些构造都和相应的代数结构中的自由构造相关, 此类构造满足所谓的 "泛性质". 在后边的章节, 我们将对自由函子及其相关做进一步的讨论.

- 6) 范畴论构建的一个动机就是对代数拓扑中一些结论的研究. 笼统地说, 在代数拓扑领域, 我们使用代数的方法来研究拓扑空间. 在这个过程中, 我们不可避免地需要构建代

数结构与拓扑结构之间的联系. 如果使用范畴论的语言, 这就是说我们需要去构建拓扑空间范畴到一些代数结构范畴的函子.

笼统地说, 拓扑学主要研究 "连续". 一个空间的拓扑结构就是对空间里每个点的附近的描述(给出每个点附近的邻域基). 利用拓扑结构, 我们可以讨论拓扑空间之间的连续映射. 拓扑空间的一个基本性质就是连通性. 我们可以使用不同方法来描述拓扑空间的连通性. 尽管这些方法并不等价, 但都是欧式空间连通性的自然的推广. 这其中的一种方法就是使用道路来研究一个空间的连通性. 任给一个拓扑空间 X , 我们称一个连续映射

$$\gamma : [0, 1] \rightarrow X,$$

为一个 X 中的(带参数的)道路. 任给两个道路 γ 和 η 满足 $\gamma(1) = \eta(0)$, 我们可以通过先沿着 γ 前进, 再沿着 η 前进的方式得到一个新的道路, 并称之为 γ 和 η 的复合 $\gamma * \eta : [0, 1] \rightarrow X$. 复合道路 $\gamma * \eta$ 的详细定义如下: 任取 t , 我们定义

$$(\gamma * \eta)(t) = \begin{cases} \gamma(2t) & 0 \leq t \leq \frac{1}{2} \\ \eta(2t - 1) & \frac{1}{2} \leq t \leq 1 \end{cases}$$

另一方面, 任给两个端点相同的道路, 如果我们可以把其中一个道路通过连续变动的方式变为另一个道路, 我们称二者同伦等价. 任取 X 中的一个点 x , 我们考虑 X 从 x 出发并回到 x 的道路的同伦类, 记作 $\pi_1(X, x)$. 以上定义的道路的复合给出了 $\pi_1(X, x)$ 上的一个群结构. 我们由此得到了 X 关于基点 x 的基本群. 注意到基本群的构造过程依赖于 x 的选取. 如果 X 的道路连通的, 则不同基点给出的基本群是同构的. 而如果 X 不连通, 则对不同基点, 以上定义的空间 X 的基本群可能是不同的.

我们记 $\mathbf{Top}_*$ 为带基点的拓扑空间的范畴. 这个范畴中的对象是所有带一个基点的拓扑空间, 态射为将基点送到基点的连续映射. 利用以上讨论, 我们有函子 $\mathbf{Top}_* \rightarrow \mathbf{Group}$. 这个函子将对象 (X, x) 送到对象 $\pi_1(X, x)$, 将态射

$$f : (X, x) \rightarrow (Y, y),$$

送到态射

$$f_* : \pi_1(X, x) \rightarrow \pi_1(Y, y).$$

7) 记 G 为一个群, X 为一个非空集合. 我们考虑一个映射

$$\Phi : G \times X \rightarrow X.$$

如果这个映射满足以下两个条件:

- 对任意 $g, g' \in G$ 和任意 $x \in X$, 我们有 $(gg')x = g(g'x)$;
- 对任意 $x \in X$, 我们有 $ex = x$.

我们称映射 Φ 诱导出一个群 G 在 X 上的左作用. 如果我们固定第一个位置为 $g \in G$, 则映射 Φ 诱导出一个 X 到子集的映射

$$\begin{aligned} \varphi_g = \Phi(g, \cdot) : X &\rightarrow X, \\ x &\mapsto \phi(g, x). \end{aligned}$$

因此, 我们有一个从 G 到 X 的对称群 S_X 的同态 $\varphi : g \mapsto \varphi_g$.

利用范畴论的语言, 我们可以将以上观察用函子的形式表达出来. 我们考虑 G 对应的群胚 $\mathbf{BG}$, 以及集合范畴 $\mathbf{Set}$. 以上构造可以被看作是一个函子 $F : \mathbf{BG} \rightarrow \mathbf{Set}$. 这里 F_0 将 $\mathbf{BG}$ 唯一的对象 G 送到 $\mathbf{Set}$ 的对象 X , 并将 $\mathbf{BG}$ 中任意态射 g 送到 $\mathbf{Set}$ 的态

射 φ_g . 因此任意 G 的像 X 非空的函子 $\mathbf{BG} \rightarrow \mathbf{Set}$, 则对应的是一个 G 在 X 上的左作用.

类似地, 我们也可以构造 G 在具有某种结构的集合 X 上的作用. 考虑 G 在 X 上的作用. 如果 X 为一个群, 我们可以要求对任意 $g \in G$, 以上构造的 φ_g 还要保持 X 的群结构, 即为一个群同构, 则我们称 G 通过群同构作用在群 X 上.

如果 X 为一个线性空间, 我们可以要求对任意 $g \in G$, 以上构造的 φ_g 还需要保持 X 的线性结构, 即为一个线性同构, 则我们称 G 通过线性同构作用的在线性空间 X 上. 此时我们称 φ 为一个 G 的线性表示.

8) 考虑以下多项式方程

$$x^3 + y + z = 0.$$

任给一个交换环 R , 我们都可以将其考虑为 R 上的方程, 并尝试求解, 并记解集为 $S(R) \subset R \times R \times R$. 注意到任取两个交换环 R 和 R' , 并设 $f: R \rightarrow R'$ 为一个环同态, 则 f 诱导了一个 $S(R)$ 到 $S(R')$ 的映射. 由此我们得到了一个从交换环范畴 $\mathbf{CRing}$ 到集合范畴 $\mathbf{Set}$ 的函子. 这种对应关系被广泛的使用在代数几何中.

注 35.3.5.

不同于之前部分中讨论的代数结构的同态, 函子的像不一定时子范畴. 我们这里通过一个简单的例子进行说明. 记范畴 $\mathcal{C}$ 满足

$$\text{Ob } \mathcal{C} = \{A, B, C, D\} \quad \text{和} \quad \text{Mor } \mathcal{C} = \{1_A, 1_B, 1_C, 1_D, A \xrightarrow{f} B, C \xrightarrow{g} D\},$$

范畴 $\mathcal{C}'$ 满足

$$\text{Ob } \mathcal{C}' = \{A', B', D'\} \quad \text{和} \quad \text{Mor } \mathcal{C}' = \{1_{A'}, 1_{B'}, 1_{C'}, A' \xrightarrow{f'} B', B' \xrightarrow{g'} C', A' \xrightarrow{g'f'} C'\}.$$

考虑定义函子 $F: \mathcal{C} \rightarrow \mathcal{D}$ 满足

$$F_0(A) = A', F_0(B) = F_0(C) = B', F_0(D) = C',$$

以及

$$F_1(f) = f', F_1(g) = g'.$$

注意到 $A' \xrightarrow{g'f'} C'$ 不在 F_1 的像中, 因此 $F(\mathcal{C})$ 不是一个范畴.

任取三个范畴 $\mathcal{C}, \mathcal{C}'$ 以及 $\mathcal{C}''$, 设存在函子 $F: \mathcal{C} \rightarrow \mathcal{C}'$ 和 $F': \mathcal{C}' \rightarrow \mathcal{C}''$, 我们可以构造二者的复合函子 $G: \mathcal{C} \rightarrow \mathcal{C}''$, 满足任取 $\mathcal{C}$ 的对象 A 以及态射 f , 我们有

$$G_0(A) = F'(F_0(A)) \quad \text{以及} \quad G_1(f) = F'_1(F_1(f)).$$

如果我们将每个范畴看作对象, 范畴之间的函子看作态射, 考虑恒等函子和以上函子的复合, 似乎也可以得到一个范畴. 但是这里将会遇到类似于 "所有的集合不构成集合" 的悖论. 通常我们将对象限制为小范畴, 然后利用函子作为态射, 可以到的一个小范畴的范畴, 通常记作 $\mathbf{Cat}$.

在之前介绍反范畴的时候, 我们注意到一个范畴和其反范畴之间也存在一个自然的联系. 这种联系类似于函子, 只是其中的复合规则反向了. 实际上这种类似的构造我们之前也介绍过. 在讨论群同态, 环同态等概念的时候, 我们就介绍了一个反同态的概念.

为了区分这两种不同类型的范畴之间的联系. 我们称之前介绍的函子为协变函子. 而类似于范畴与其反范畴之间的关系的函子被称为反变函子, 其具体定义如下:

定义 35.3.6

一个从范畴 $\mathcal{C}$ 到 $\mathcal{D}$ 反变函子 $F = (F_0, F_1) : \mathcal{C} \rightarrow \mathcal{D}$ 由

$$F_0 : \text{Ob } \mathcal{C} \rightarrow \text{Ob } \mathcal{D} \quad \text{和} \quad F_1 : \text{Mor } \mathcal{C} \rightarrow \text{Mor } \mathcal{D},$$

两个映射构成, 并且二者满足以下条件:

- 1) 对任意 $f \in \text{Mor } \mathcal{C}$, 有 $\text{cod}(F_1(f)) = F_0(\text{dom}(f))$ 和 $\text{dom}(F_1(f)) = F_0(\text{cod}(f))$;
- 2) 对任意 $A \in \text{Ob } \mathcal{C}$, 有 $F_1(1_A) = 1_{F_0(A)}$;
- 3) 对任意 $f, g \in \text{Mor } \mathcal{C}$, 有 $F_1(fg) = F_1(g)F_1(f)$.

注 35.3.7.

从定义我们也可以将一个 $\mathcal{C}$ 到 $\mathcal{D}$ 的反变函子等同于一个 $\mathcal{C}^{\text{op}}$ 到 $\mathcal{D}$ 的协变函子. 利用 $(\mathcal{C}^{\text{op}})^{\text{op}} = \mathcal{C}$ 的关系, 利用注 35.3.2, 我们也可以将 $\mathcal{C}$ 到 $\mathcal{D}$ 的反变函子等同于一个 $\mathcal{C}$ 到 $\mathcal{D}^{\text{op}}$ 的协变函子.

我们首先给出一些反变函子的例子.

例 35.3.8. 1) 任给一个范畴 $\mathcal{C}$ 以及其反范畴 $\mathcal{C}^{\text{op}}$, 考虑将 $\mathcal{C}$ 的对象 A 送到 $\mathcal{C}^{\text{op}}$ 的对象 A , 将 $\mathcal{C}$ 的态射 f 送到 $\mathcal{C}^{\text{op}}$ 的态射 f^{op} , 我们得到了一个反变函子.

2) 任给一个群 G , 类似于之前关于 G 在集合上的左作用的讨论, 任意从范畴 $\mathbf{BG}$ 到 $\mathbf{Set}$ 的反变函子对应的是一个 G 在某个集合上的右作用.

3) 记 U 为一个域 F 上的线性空间. 任取 F 上的线性空间 V 和 W , 设 $f : V \rightarrow W$ 为一个线性映射, 则任取线性映射 $g : W \rightarrow U$, 我们都有线性映射 $g \circ f : V \rightarrow U$. 由此, 我们得到了一个线性映射

$$\begin{aligned} \Phi_f : \text{Hom}(W, U) &\rightarrow \text{Hom}(V, U), \\ g &\mapsto g \circ f. \end{aligned}$$

利用以上讨论, 我们得到了一个反变函子 $F : \mathbf{Vect}_F \rightarrow \mathbf{Vect}_F$, 满足任取对象 V 以及态射 $V \xrightarrow{f} X$, 有

$$F_0(V) = \text{Hom}(V, U) \quad \text{以及} \quad F_1(f) = \Phi_f : \text{Hom}(W, U) \rightarrow \text{Hom}(V, U).$$

若 $U = F$, 则任取 F 上线性空间 V , 线性空间 $\text{Hom}(V, F)$ 为 V 的对偶空间, 记作 V^* . 以上反变函子告诉我们, 任意 V 到 W 的线性映射 f , 都给出了 W^* 到 V^* 的线性映射 f^* , 并且任取线性映射

$$f_1 : V_1 \rightarrow V_2 \quad \text{以及} \quad f_2 : V_2 \rightarrow V_3,$$

我们有

$$(f_2 \circ f_1)^* = f_1^* \circ f_2^*.$$

函子的复合

任取三个范畴 $\mathcal{C}$, $\mathcal{C}'$ 以及 $\mathcal{C}''$, 设存在函子 $F: \mathcal{C} \rightarrow \mathcal{C}'$ 和 $F': \mathcal{C}' \rightarrow \mathcal{C}''$, 我们定义函子 F 和 F' 的复合为 $F' \circ F: \mathcal{C} \rightarrow \mathcal{C}''$, 满足任取 $\mathcal{C}$ 的对象 A 以及态射 f , 我们有

$$(F' \circ F)_0(A) = F'_0(F_0(A)) \quad \text{以及} \quad (F' \circ F)_1(f) = F'_1(F_1(f)).$$

根据考虑协变函子和反变函子的定义, 我们有以下两种情形:

- 若 F 和 F' 均为协变函子或者均为反变函子, 则 $F' \circ F$ 为协变函子;
- 若 F 和 F' 一个为协变函子, 一个为反变函子, 则 $F' \circ F$ 为反变函子.

注 35.3.9.

为了方便讨论, 后文的 "函子" 指代协变函子, 如果需要区分协变函子和反变函子, 我们将进行说明.

定义 35.3.10

考虑一个函子 $F: \mathcal{C} \rightarrow \mathcal{D}$. 若对任意 $A, B \in \text{Ob } \mathcal{C}$, 都有

$$\begin{aligned} \text{Hom}(A, B) &\rightarrow \text{Hom}(F_0(A), F_0(B)) \\ f &\mapsto F_1(f) \end{aligned}$$

为单射, 我们称函子 F 是**忠实**的. 若对任意 $A, B \in \text{Ob } \mathcal{C}$, 以上映射是满射, 我们称函子 F 是**完全**的.

注 35.3.11.

函子 $\mathcal{C} \xrightarrow{F} \mathcal{D}$ 的忠实或者完全的性质都是局部性质. 我们考虑的是 F_1 限制在任意一对 $\mathcal{C}$ 的对象 A 和 B 之间的所有的态射的全体 $\text{Hom}(A, B)$ 是单射还是满射. 当一个函子 F 是忠实的, 仍可能出现两个态射 f 和 g 被 F_1 送到同一个态射上; 当一个函子是完全的时候, 仍可能出现一些 $\mathcal{D}$ 的对象不在 F_0 的像中或者一些 $\mathcal{D}$ 的态射不在 F_1 的像中.

例 35.3.12. 1) 任取范畴 $\mathcal{C}$, 以及它的一个子范畴 $\mathcal{D}$, 则 $\mathcal{D}$ 到 $\mathcal{C}$ 的嵌入函子是一个即忠实的函子. 如果任取 $\mathcal{D}$ 的对象 A 和 B , 假设任意 $\mathcal{C}$ 中 A 到 B 的态射都在 $\mathcal{D}$ 中, 这个嵌入函子同时也是完全的.

2) 之前介绍遗忘函子时所举的例子皆为忠实的.

本章至此已经介绍了许多函子的例子. 读者可以根据忠实函子和完全函子的定义自行验证每个例子中的函子是否满足忠实或者完全的条件.

35.4 自然变换

在介绍完范畴和函子的概念之后, 我们来重新回顾 Eilenberg 和 MacLane 所给出的关于线性空间的例子. 这个例子考虑的是一个给定域 F 上的有限维线性空间构成的范畴 $\mathbf{Vect}_{F,0}$, 以及这个范畴上的两个函子: 一个是恒等函子 ι , 另一个是取两次对偶的函子 $(-)^{**}$.

将这种关系推广到对一般的范畴的讨论中, 我们就有了自然变换的概念.

定义 35.4.1

设 $\mathcal{C}$ 和 $\mathcal{D}$ 为两个范畴, F 和 G 都是 $\mathcal{C}$ 到 $\mathcal{D}$ 的函子. 函子 F 到 G 的**自然变换** α 为 $\mathcal{D}$ 的一族态射

$$(F_0(A) \xrightarrow{\alpha_A} G_0(A))_{A \in \text{Ob } \mathcal{C}},$$

满足任取 $A \in \text{Ob } \mathcal{C}$, 以及任意 $f \in \text{Hom}_{\mathcal{C}}(A, B)$ 都有

$$\begin{array}{ccc} F_0(A) & \xrightarrow{\alpha_A} & G_0(A) \\ F_1(f) \downarrow & & \downarrow G_1(f) \\ F_0(B) & \xrightarrow{\alpha_B} & G_0(B) \end{array}$$

注 35.4.2.

我们通常将以上提到的 $\mathcal{C}$, $\mathcal{D}$, F , G 以及 α 之间的关系用下图表示:

$$\begin{array}{ccc} & F & \\ \mathcal{C} & \begin{array}{c} \searrow \alpha \\ \downarrow \\ \nearrow \end{array} & \mathcal{D} \\ & G & \end{array}$$

通过直接验证, 之前介绍的下边我们来看一些自然变换的例子.

例 35.4.3. 1) 我们首先来考虑之前提到的向量空间及其对偶空间的例子. 记 $\mathbb{F}$ 为一个域, 仍记 ι 为有限维向量空间范畴 $\mathbf{Vect}_{\mathbb{F},0}$ 到自己的恒等函子, 记 $(-)^{**}$ 为线性空间取两次对偶的函子. 任取一个有限维 $\mathbb{F}$ -向量空间 V , 对任意向量 $v \in V$, 其对应的 V^{**} 中的元素为

$$\begin{aligned} v^{**} : V^* &\rightarrow V^*, \\ f &\mapsto f(v). \end{aligned}$$

我们可以定义线性映射

$$\begin{aligned} \alpha_V : V &\rightarrow V^{**}, \\ v &\mapsto v^{**}. \end{aligned}$$

任取 V 和 W 两个有限维的 $\mathbb{F}$ -向量空间, 记 $\varphi : V \rightarrow W$ 为一个线性映射, 我们有线性映射

$$\begin{aligned} \varphi^{**} : V^{**} &\rightarrow W^{**}, \\ v^{**} &\mapsto \varphi(v)^{**}, \end{aligned}$$

并可以进而验证线性映射 φ , φ^{**} , α_V 以及 α_W 满足以下交换图:

$$\begin{array}{ccc} V & \xrightarrow{\alpha_V} & V^{**} \\ \varphi \downarrow & & \downarrow \varphi^{**} \\ V & \xrightarrow{\alpha_W} & W^{**} \end{array}$$

考虑 $\mathbf{Vect}_{\mathbb{F},0}$ 中态射的定义, 我们有态射 φ , φ^{**} , α_V 以及 α_W 满足 $\alpha_W \varphi = \varphi^{**} \alpha_V$. 因此

$$(V \xrightarrow{\alpha_V} V^{**})_{V \in \text{Ob } \mathbf{Vect}_{\mathbb{F},0}},$$

构成 ι 到 $(-)^{**}$ 的自然变换.

- 2) 这里我们介绍一个群范畴 **Group** 中的例子. 任给一个群 G , 我们记 $[G, G]$ 为其正规子群, 并记

$$G^{ab} := G/[G, G],$$

为 G 的交换化. 我们记 G 到 G^{ab} 的自然同态为 π_G . 在之前对群结构的讨论中, 我们知道任给 G 的正规子群 N , 其对应的商群 G/N 是交换群当且仅当 $[G, G] \triangleleft N$. 因此我们可以认为 G^{ab} 是 G 的商群中最大的交换群.

任取群 H , 我们记其交换化为 H^{ab} , 并记 π_H 为 H 到 H^{ab} 的自然同态. 任给 G 到 H 的同态 φ , 通过与 H 到 H^{ab} 的自然同态的复合, 我们得到同态

$$\psi = \pi_H \circ \varphi : G \rightarrow H^{ab}.$$

由于 H^{ab} 交换, 因此 $\psi(G)$ 作为 H^{ab} 也是一个交换群. 由群同态基本定理, 我们知道 $[G, G]$ 包含在 $\ker \psi$ 中, 因此存在为一个 G^{ab} 到 H^{ab} 的群同态 $\bar{\varphi}$, 满足以下交换图

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \pi_G \downarrow & \searrow \psi & \downarrow \pi_H \\ G^{ab} & \xrightarrow{\bar{\varphi}} & H^{ab} \end{array}$$

从范畴的角度考虑, 以上讨论告诉我们取交换化给出了 **Group** 范畴到自己的一个函子 F^{ab} , 并且以下一族态射

$$(G \xrightarrow{\pi_G} G^{ab})_{G \in \text{Ob } \mathbf{Group}},$$

构成了恒等函子 ι 到 F^{ab} 的自然变换.

- 3) 任取交换环 R , 以及非零自然数 n , 我们考虑 R 上的 n 阶方阵构成的半群 $\text{Mat}_{n \times n}(R)$. 记 S 为一个交换环, 任意一个 R 到 S 的环同态 φ , 都诱导出唯一的一个 $\text{Mat}_{n \times n}(R)$ 到 $\text{Mat}_{n \times n}(S)$ 的半群同态 φ' . 这给出了交换环范畴 **CRing** 到半群范畴 **Monoid** 的一个函子 F . 另一方面, 任意一个交换环 R 都关于其乘法结构构成一个半群. 这给出了另一个 **CRing** 到 **Monoid** 的函子 G .

考虑 R 上 n -阶方阵的取行列式映射:

$$\begin{aligned} \det_R : \text{Mat}_{n \times n}(R) &\rightarrow R, \\ M &\mapsto \det_R M. \end{aligned}$$

行列式的性质告诉我们这个映射是一个半群同态, 即任取 $M, N \in \text{Mat}_{n \times n}(R)$, 我们有

$$\det_R(MN) = \det_R M \det_R N.$$

沿用之前的记号, 我们可以验证以下交换图成立:

$$\begin{array}{ccc} \text{Mat}_{n \times n}(R) & \xrightarrow{\varphi} & \text{Mat}_{n \times n}(S) \\ \det_R \downarrow & & \downarrow \det_S \\ R & \xrightarrow{\varphi'} & S \end{array}$$

从范畴的角度, 这里的一族态射

$$(\det_R)_{R \in \text{Ob } \mathbf{CRing}},$$

构成函子 F 和函子 G 的一个自然同态.

- 4) 最后我们给出一个平凡的例子. 任意一个函子 $F: \mathcal{C} \rightarrow \mathcal{D}$, 都有一个到自己的恒等自然变换 $\mathbf{1}_F$:

$$\mathcal{C} \begin{array}{c} \xrightarrow{F} \\ \Downarrow \mathbf{1}_F \\ \xrightarrow{F} \end{array} \mathcal{D}.$$

这里任取 $A \in \text{Ob } \mathcal{C}$, 我们有

$$(\mathbf{1}_F)_A = \mathbf{1}_{F_0(A)}.$$

函子间并不一定总存在自然变换. 我们用下边的例子进行说明.

例 35.4.4.

记 G 为一个群. 考虑其对应的群胚 $\mathbf{BG}$. 任给 $\mathbf{BG}$ 到集合范畴 $\mathbf{Set}$ 的函子 F , 设 $F_0(G) = X$. 由之前的讨论我们知道, 若 X 非空, 则该函子对应于 G 在 X 上的一个左作用.

设 F' 为另一个 $\mathbf{BG}$ 到 $\mathbf{Set}$ 的函子, 记 $F'_0(G) = Y$. 由于 $\mathbf{BG}$ 只有一个对象, 因此若 α 为 F 到 F' 的自然变换, 则 α 只有一个态射 $\varphi: X \rightarrow Y$, 且对任意 $\mathbf{BG}$ 的态射 g , 满足以下交换图

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & Y \\ F_1(g) \downarrow & & \downarrow F'_1(g) \\ X & \xrightarrow{\varphi} & Y \end{array}$$

考虑集合范畴 $\mathbf{Set}$ 中态射的定义, 则 φ 为一个满足以下条件的映射: 任取 $x \in X$, 都有

$$\varphi(F_1(g)(x)) = F'_1(g)(\varphi(x)).$$

这样的映射被称为一个 G -等变映射. 因此 $\mathbf{BG}$ 到 $\mathbf{Set}$ 的函子之间的自然变换是由 G -等变映射得到的.

我们下边给出一个例子来说明存在两个有 G -作用的集合之间并不总存在 G -等变映射. 考虑群 G 包含至少两个元素. 我们考虑 $X = \{x\}$ 为一个单元素集. 作为集合 $Y = G$. 群 G 在 X 上有唯一的一个平凡的作用. 另一方面, 我们考虑 G 在 G 上的左平移作用. 在这种情况下, 不存在 X 到 Y 的 G -等变映射. 因此这两个群作用对应的 $\mathbf{BG}$ 到 $\mathbf{Set}$ 两个函子之间就不存在自然变换.

以下我们再给出一个自然变换不存在的例子.

例 35.4.5.

考虑集合范畴 $\mathbf{Set}$. 我们可以如下定义一个函子 F , 满足任取对象 $A \in \text{Ob } \mathbf{Set}$ 以及态射 $f \in \text{Mor } \mathbf{Set}$, 有 $F_0(A) = \emptyset$ 以及 $F_1(A) = \mathbf{1}_\emptyset$. 我们下边将说明不存在从恒等函子 ι 到该函子的自然变换.

若存在从 ι 到 F 的自然变换, 则对任意 $\mathbf{Set}$ 的对象 A , 都有一个态射

$$\iota_0(A) = A \xrightarrow{\alpha_A} \emptyset = F_0(A),$$

满足自然变换定义中需要的条件. 这里注意到 $\mathbf{Set}$ 中的态射来自于集合之间的映射. 若一个集合 A 非空, 则不存在 A 到 $\emptyset$ 的映射, 因此 $\mathbf{Set}$ 中不存在 A 到 $\emptyset$ 的态射. 由此可知以上需要的 α_A 是不存在的, 这告诉我们不存在 ι 到 F 的自然变换.

给定的两个函子之间也可能存在多个不同的自然变换. 我们下边给出一个例子进行说明. 记 $\mathcal{C}$ 为一个离散范畴, $\mathcal{D}$ 为任意一个不同于空范畴的范畴. 注意到 $\mathcal{C}$ 为一个离散范畴,

其中只有恒等态射, 因此任意从 $\mathcal{C}$ 出发的函子 F 都被对象之间的对应关系 F_0 确定. 考虑将所有的 $\mathcal{C}$ 的对象对应到 $\mathcal{D}$ 的一个对象所给出的函子 F . 任取 $\mathcal{C}$ 的态射 $A \xrightarrow{1_A} A$, 则对任意 $F_0(A)$ 到自己的态射 α_A , 我们都有

$$\begin{array}{ccc} F_0(A) & \xrightarrow{\alpha_A} & F_0(A) \\ \downarrow \mathbf{1}_{F_0(A)} & & \downarrow \mathbf{1}_{F_0(A)} \\ F_0(A) & \xrightarrow{\alpha_A} & F_0(A) \end{array}.$$

因此对任意 $A \in \text{Ob } \mathcal{C}$, 任选一个 $\alpha_A \in \text{Hom}_{\mathcal{D}}(F_0(A), F_0(A))$ 所得的一族 $\mathcal{D}$ 的态射都构成 F 到自己的自然变换.

自然变换的纵复合以及函子范畴

记 $\mathcal{C}$ 和 $\mathcal{D}$ 为两个范畴. 设 F, G 和 H 都是 $\mathcal{C}$ 到 $\mathcal{D}$ 的函子, 并设 α 为 F 到 G 的自然变换, β 为 G 到 H 的自然变换. 我们可以将以上提到的 $\mathcal{C}, \mathcal{D}, F, G, H, \alpha$ 和 β 之间的关系用下图表示

$$\begin{array}{ccc} & F & \\ & \downarrow \alpha & \\ \mathcal{C} & \xrightarrow{G} & \mathcal{D} \\ & \downarrow \beta & \\ & H & \end{array}$$

考虑自然变换的定义, 任取 $\mathcal{C}$ 的态射 $A \xrightarrow{f} B$, 我们有以下交换图

$$\begin{array}{ccc} F_0(A) & \xrightarrow{F_1(f)} & F_0(B) \\ \alpha_A \downarrow & & \downarrow \alpha_B \\ G_0(A) & \xrightarrow{G_1(f)} & G_0(B) \\ \beta_A \downarrow & & \downarrow \beta_B \\ H_0(A) & \xrightarrow{H_1(f)} & H_0(B) \end{array}$$

则以下 $\mathcal{D}$ 的一族态射

$$(\beta_A \circ \alpha_A)_{A \in \text{Ob } \mathcal{C}},$$

构成一个 F 到 H 的自然变换. 我们称之为 α 和 β 的**纵复合**, 记为 $\beta \circ \alpha$, 表示如下图

$$\begin{array}{ccc} & F & \\ & \downarrow \beta \circ \alpha & \\ \mathcal{C} & \xrightarrow{H} & \mathcal{D} \\ & \downarrow H & \end{array}.$$

自然变换可以看作是函子之间的态射. 沿着这个想法, 我们可以如下定义函子范畴. 任给范畴 $\mathcal{C}$ 和 $\mathcal{D}$, 则 $\mathcal{C}$ 到 $\mathcal{D}$ 的**函子范畴**的对象为 $\mathcal{C}$ 到 $\mathcal{D}$ 的函子; 任取两个 $\mathcal{C}$ 到 $\mathcal{D}$ 的函子 F 和 G , 该函子范畴中 F 到 G 的态射是 F 到 G 的自然变换, 态射的复合由自然变换的纵复合给出. 我们将该范畴记作 $[\mathcal{C}, \mathcal{D}]$.

我们来验证一下态射的复合满足范畴定义中所需要的条件. 由自然变换的纵复合的定义可知, 自然变换的纵复合的结合律由 $\mathcal{D}$ 中态射的结合律保证. 由之前的讨论, 任意一个函

子 F 都有一个到自己的恒等自然变换 $\mathbf{1}_F$. 利用 $\mathcal{D}$ 中恒等态射的性质, 直接验证可得, 任取自然变换 $F \xrightarrow{\alpha} G$ 和 $G \xrightarrow{\beta} F$, 我们都有

$$\alpha \circ \mathbf{1}_F = \alpha, \quad \mathbf{1}_F \circ \beta = \beta.$$

由此可知范畴 $[\mathcal{C}, \mathcal{D}]$ 定义良好.

例 35.4.6.

之前我们讨论过一个群 Γ 的群胚范畴 $\mathbf{B}\Gamma$ 到集合范畴 $\mathbf{Set}$ 的每个函子对应的是一个带有 Γ -左作用的集合. 因此函子范畴 $[\mathbf{B}\Gamma, \mathbf{Set}]$ 即为所有带有 Γ -左作用的集合的范畴. 如前文所讨论的, 两个对象之间的态射是一个 Γ -共变映射.

自然变换的横复合

我们也可以考虑函子的复合对自然变换的影响. 记 $\mathcal{C}, \mathcal{C}'$ 和 $\mathcal{C}''$ 为三个范畴. 记 F 和 G 均为 $\mathcal{C}$ 到 $\mathcal{C}'$ 的函子, F' 和 G' 均为 $\mathcal{C}'$ 到 $\mathcal{C}''$ 的函子. 由之前对函子的复合的讨论, 我们有 $F' \circ F$ 和 $G' \circ G$ 均为 $\mathcal{C}$ 到 $\mathcal{C}''$ 的函子. 设存在 F 到 G 存在自然变换 α , 以及 F' 到 G' 的自然变换 β , 则我们有下图

$$\begin{array}{ccccc} \mathcal{C} & \xrightarrow{F} & \mathcal{C}' & \xrightarrow{F'} & \mathcal{C}'' \\ & \Downarrow \alpha & & \Downarrow \beta & \\ \mathcal{C} & \xrightarrow{G} & \mathcal{C}' & \xrightarrow{G'} & \mathcal{C}'' \end{array}$$

任取 $\mathcal{C}$ 的一个态射 $A \xrightarrow{f} B$, 我们有以下交换图:

$$\begin{array}{ccc} F_0(A) & \xrightarrow{F_1(f)} & F_0(B) \\ \alpha_A \downarrow & & \downarrow \alpha_B \\ G_0(A) & \xrightarrow{G_1(f)} & G_0(B) \end{array}$$

这里有 4 个 $\mathcal{D}$ 中的态射, 考虑自然变换 β , 我们有以下交换图

$$\begin{array}{ccccc} F'_0(F_0(A)) & \xrightarrow{\beta_{F_0(A)}} & G'_0(F_0(A)) & & \\ \downarrow F'_1(\alpha_A) & \searrow F'_1(F_1(f)) & \downarrow & \searrow G'_1(F_1(f)) & \\ F'_0(F_0(B)) & \xrightarrow{\beta_{F_0(B)}} & G'_0(F_0(B)) & & \\ \downarrow F'_1(\alpha_B) & & \downarrow G'_1(\alpha_A) & & \\ F'_0(G_0(A)) & \xrightarrow{\beta_{G_0(A)}} & G'_0(G_0(A)) & & \\ \downarrow F'_1(G_1(f)) & \searrow F'_1(G_1(f)) & \downarrow & \searrow G'_1(G_1(f)) & \\ F'_0(G_0(B)) & \xrightarrow{\beta_{G_0(B)}} & G'_0(G_0(B)) & & \end{array}$$

从该图我们可以看出 $\mathcal{C}''$ 中的以下这族态射

$$(G'_1(\alpha_A)\beta_{F_0(A)})_{A \in \text{Ob } \mathcal{C}}$$

构成函子 $F' \circ F$ 和 $G' \circ G$ 之间的自然变换. 我们称之为 α 和 β 的**横复合**, 并记作

$$\beta * \alpha,$$

表示如下图

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{F' \circ F} & \mathcal{C}'' \\ & \Downarrow \beta * \alpha & \\ & G' \circ G & \end{array}$$

注意到由于上图交换, 对任意 $A \in \text{Ob } \mathcal{C}$, 我们有

$$(\beta * \alpha)_A = G'_1(\alpha_A)\beta_{F_0(A)} = \beta_{G_0(A)}F'_1(\alpha_A).$$

沿用之前的记号, 从上一个交换图中, 我们还可以得到其它的观察.

1) 考虑 $\mathcal{C}$ 到 $\mathcal{C}''$ 的两个函子 $F' \circ F$ 和 $G' \circ F$, 我们有下图

$$\mathcal{C} \xrightarrow{F} \mathcal{C}' \begin{array}{c} \xrightarrow{F'} \\ \Downarrow \beta \\ \xrightarrow{G'} \end{array} \mathcal{C}''$$

对任意 $A \in \text{Ob } \mathcal{C}$, 我们有

$$\begin{array}{ccccc} F'_0(F_0(A)) & \xrightarrow{\beta_{F_0(A)}} & G'_0(F_0(A)) & & \\ & \searrow F'_1(F_1(f)) & & \searrow G'_1(F_1(f)) & \\ & F'_0(F_0(B)) & \xrightarrow{\beta_{F_0(B)}} & G'_0(F_0(B)) & \end{array}$$

由此可得范畴 $\mathcal{C}''$ 中的以下这族态射

$$(\beta_{F_0(A)})_{A \in \text{Ob } \mathcal{C}},$$

构成从 $F' \circ F$ 到 $G' \circ F$ 的自然变换, 记作 βF . 我们可以将其用下图表示:

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{F' \circ F} & \mathcal{C}'' \\ & \Downarrow \beta F & \\ & G' \circ F & \end{array}$$

类似地, 范畴 $\mathcal{C}''$ 中的以下这族态射

$$(\beta_{G_0(A)})_{A \in \text{Ob } \mathcal{C}},$$

构成从 $F' \circ G$ 到 $G' \circ G$ 的自然变换 βG .

2) 考虑 $\mathcal{C}$ 到 $\mathcal{C}''$ 的两个函子 $F' \circ F$ 和 $F' \circ G$, 我们有下图

$$\mathcal{C} \begin{array}{c} \xrightarrow{F} \\ \Downarrow \alpha \\ \xrightarrow{G} \end{array} \mathcal{C}' \xrightarrow{F'} \mathcal{C}''.$$

对任意 $A \in \text{Ob } \mathcal{C}$, 我们有

$$\begin{array}{ccc} F'_0(F_0(A)) & & \\ \downarrow F'_1(\alpha_A) & \searrow F'_1(F_1(f)) & \\ & F'_0(F_0(B)) & \\ & \downarrow F'_1(\alpha_B) & \\ F'_0(G_0(A)) & & \\ & \searrow F'_1(G_1(f)) & \\ & F'_0(G_0(B)) & \end{array}$$

由此可得范畴 $\mathcal{C}''$ 中的以下这族态射

$$(F'_1(\alpha_A))_{A \in \text{Ob } \mathcal{C}},$$

构成从 $F' \circ F$ 到 $F' \circ G$ 的自然变换, 记作 $F'\alpha$. 我们可以将其用下图表示:

$$\begin{array}{ccc} & F' \circ F & \\ \mathcal{C} & \begin{array}{c} \searrow \downarrow F'\alpha \nearrow \\ \end{array} & \mathcal{C}'' \\ & F' \circ G & \end{array}.$$

类似地, 范畴 $\mathcal{C}''$ 中的以下这族态射

$$(G'_1(\alpha_A))_{A \in \text{Ob } \mathcal{C}},$$

构成从 $G' \circ F$ 到 $G' \circ G$ 的自然变换 $G'\alpha$.

以上我们得到了 4 个从 $\mathcal{C}$ 到 $\mathcal{C}''$ 的函子间的自然变换. 考虑

$$\begin{array}{ccc} & F' \circ F & \\ \mathcal{C} & \begin{array}{c} \searrow \downarrow F'\alpha \nearrow \\ \downarrow \beta G \nearrow \\ \end{array} & \mathcal{C}'' \\ & G' \circ G & \end{array},$$

利用之前的交换图, 我们得到以下关系

$$(\beta G) \circ (F'\alpha) = \beta * \alpha.$$

利用这个观察我们可以进一步得到以下自然变换的纵复合与横复合之间的关系.

命题 35.4.7

设范畴 $\mathcal{C}$, $\mathcal{C}'$ 以及 $\mathcal{C}''$, 函子 F, F', G, G', H, H' , 以及自然变换 α, α', β 和 β' 满足下图关系:

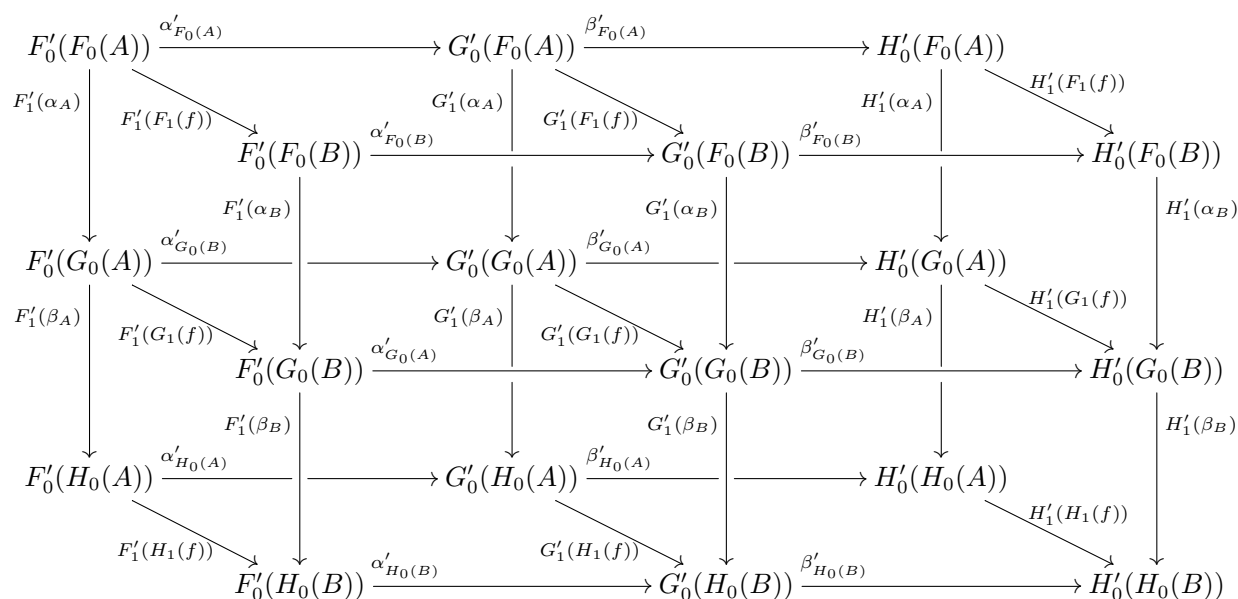
$$\begin{array}{ccccc} & F & & F' & \\ \mathcal{C} & \begin{array}{c} \searrow \downarrow \alpha \nearrow \\ \downarrow G \end{array} & \mathcal{C}' & \begin{array}{c} \searrow \downarrow \alpha' \nearrow \\ \downarrow G' \end{array} & \mathcal{C}'' \\ & H & & H' & \end{array},$$

则我们有

$$(\beta \circ \alpha) * (\beta' \circ \alpha') = (\beta' * \beta) \circ (\alpha' * \alpha).$$

我们这里将给出任给一个 $\mathcal{C}$ 的态射 $A \xrightarrow{f} B$, 我们能得到的涉及以上给函子以及各自自然变换的一个交换图. 通过观察图中的 $F'(F(A))$ 到 $H'(H(A))$ 不同的有向道路以及 $F'(F(B))$

到 $H'(H(B))$ 的有向道路, 我们就可以得到以上命题的结论. 具体的证明过程留作练习.



注 35.4.8.

我们可以将命题中的关系表达为下图

$$\begin{array}{ccc}
 \mathcal{C} & \xrightarrow{F} & \mathcal{C}' \\
 \downarrow \beta \circ \alpha & & \downarrow \beta' \circ \alpha' \\
 \mathcal{C} & \xrightarrow{H} & \mathcal{C}''
 \end{array}
 =
 \begin{array}{ccc}
 \mathcal{C} & \xrightarrow{F' \circ F} & \mathcal{C}'' \\
 \downarrow \alpha' * \alpha & & \downarrow \beta' * \beta \\
 \mathcal{C} & \xrightarrow{G' \circ G} & \mathcal{C}'' \\
 \downarrow \beta' \circ \alpha' & & \downarrow \beta' \circ \alpha' \\
 \mathcal{C} & \xrightarrow{H' \circ H} & \mathcal{C}''
 \end{array}$$

注 35.4.9.

在以上的讨论中, 我们使用交换图来描述所涉及的范畴的对象, 态射, 范畴之间的函子等各个部分之间的关系. 在一般的讨论中, 合理的利用交换图将帮助我们理清思路.

2-范畴

在之前的讨论中, 我们展示了范畴, 范畴间的函子以及函子间的自然变换的关系. 利用这些关系, 我们可以将以上提到的各部分组合起来的到一个新的结构. 这是我们将讨论的 2-范畴的一个例子. 我们可以将范畴看作点, 范畴间的函子看作是线, 进而可以将函子间的自然变换看作线扫过的面. 如果考虑所有范畴的全体, 借用维数的概念, 任意一个范畴是一个 0-维对象, 任意一个函子是 1-维对象, 任意一个自然变换是一个 2-维对象. 笼统地说, 一个 2-范畴就是一个由 0-维对象, 1-维对象和 2-维对象满足某种关系构成的结构.

当然如果我们考虑范畴, 函子和自然变换, 则不可比避免地需要考虑所有的范畴的全体. 类似于所有集合的全体, 这里也有一些涉及到集合论的一些问题需要处理. 如之前注记中提到的, 为了不偏离本部分的初衷, 我们此处仍使用 "一族" 或者 "全体" 这样笼统的说法.

借用之前讨论中的记号, 2-范畴的具体定义如下.

定义 35.4.10

一个 2-范畴 $\mathcal{C}$ 由三部分构成

- $\text{Ob } \mathcal{C}$: 一族对象, 通常记作 $A, B, C, \dots$;
- $\text{Mor}_1 \mathcal{C}$: 一族 1-态射 (对象之间的态射), 通常记作 $f, g, h, \dots$, 用单箭头 $\rightarrow$ 表示;
- $\text{Mor}_2 \mathcal{C}$: 一族 2-态射 (具有相同的源和目标的态射之间的态射), 通常记作 $\alpha, \beta, \gamma, \dots$, 用 $\Rightarrow$ 表示;

并且对象, 1-态射和 2-态射满足:

- 1) 任取对象 A , 存在一个恒等 1-态射 $A \xrightarrow{1_A} A$;
- 2) 任取 1-态射 f 和 g , 满足 $\text{dom}(f) = \text{cod}(g)$, 存在唯一的一个 1-态射 $\text{cod}(f) \xrightarrow{gf} \text{dom}(g)$, 称为 f 和 g 的复合;
- 3) 任取 1-态射 $A \xrightarrow{f} B$, 存在一个恒等 2-态射 $f \xRightarrow{1_f} f$;

- 4) 任取 2-态射 α 和 β , 满足 $A \begin{array}{c} \xrightarrow{f} \\ \Downarrow \alpha \\ \xrightarrow{g} \end{array} B$, 存在有唯一的 2-态射 $A \begin{array}{c} \xrightarrow{f} \\ \Downarrow \beta \circ \alpha \\ \xrightarrow{h} \end{array} B$, 称

为 α 和 β 的**纵复合**;

- 5) 任取 2-态射 α 和 α' , 满足 $A \begin{array}{c} \xrightarrow{f} \\ \Downarrow \alpha \\ \xrightarrow{g} \end{array} A' \begin{array}{c} \xrightarrow{f'} \\ \Downarrow \alpha' \\ \xrightarrow{g'} \end{array} A''$, 存在唯一的 2-态射 $A \begin{array}{c} \xrightarrow{f'f} \\ \Downarrow \alpha' * \alpha \\ \xrightarrow{g'g} \end{array} A''$,

称为 α 和 α' 的**横复合**.

1-态射之间的复合, 以及 2-态射之间的纵复合和横复合都满足之前范畴定义中态射复合的性质, 同时若 2-态射 α, α', β 和 β' 满足

$$A \begin{array}{c} \xrightarrow{f} \\ \Downarrow \alpha \\ \xrightarrow{g} \end{array} B \begin{array}{c} \xrightarrow{f'} \\ \Downarrow \alpha' \\ \xrightarrow{g'} \end{array} C, \quad A \begin{array}{c} \xrightarrow{f} \\ \Downarrow \beta \\ \xrightarrow{h} \end{array} B \begin{array}{c} \xrightarrow{f'} \\ \Downarrow \beta' \\ \xrightarrow{h'} \end{array} C,$$

则我们有

$$(\beta \circ \alpha) * (\beta' \circ \alpha') = (\beta' * \beta) \circ (\alpha' * \alpha).$$

注 35.4.11.

类似地, 我们可以构造 3-范畴, 4-范畴等等.

35.5 范畴的等价

范畴之间是通过函子联系起来的. 通过函子, 我们可以比较两个范畴的结构. 由此, 我们如下给出范畴同构的定义.

定义 35.5.1

记 $\mathcal{C}$ 和 $\mathcal{D}$ 为两个范畴. 如果存在两个函子 $F: \mathcal{C} \rightarrow \mathcal{D}$ 和 $G: \mathcal{D} \rightarrow \mathcal{C}$, 满足

$$G \circ F = \iota_{\mathcal{C}} \quad \text{和} \quad F \circ G = \iota_{\mathcal{D}},$$

这里 $\iota_{\mathcal{C}}$ 和 $\iota_{\mathcal{D}}$ 分别为 $\mathcal{C}$ 和 $\mathcal{D}$ 上的恒等函子, 那么我们称范畴 $\mathcal{C}$ 和范畴 $\mathcal{D}$ 同构.

由定义可以看出当两个范畴同构的时候, 二者对象的全体之间存在一个双射, 同时二者的态射的全体之间也存在一个双射. 在实际讨论中, 当我们描述范畴 "相同" 中, 同构可能是一个过强的条件. 我们使用下边的例子来进行说明.

记 $\mathbb{F}$ 为一个域. 在讨论 $\mathbb{F}$ 上的有限维线性空间的时候, 有两个观察:

- 任给一个 $\mathbb{F}$ 上的有限维线性空间 V , 都存在一个自然数 $n \in \mathbb{N}$, 满足 V 和 $\mathbb{F}^n$ 线性同构.
- 任给两个 $\mathbb{F}$ 上有限维线性空间 V 和 W , 以及一个线性变换 $f: V \rightarrow W$, 任取 V 的一组基 $\mathcal{B}$ 和 W 的一组基 $\mathcal{C}$, 考虑 V 中向量 v 的 $\mathcal{B}$ -坐标和 $f(v)$ 作为 W 的向量的 $\mathcal{C}$ -坐标之间的关系, 我们就可以给出 f 关于 $\mathcal{B}$ 和 $\mathcal{C}$ 的一个矩阵表示, 记作 $[f]_{\mathcal{B}, \mathcal{C}}$. 我们通常将坐标向量记作列向量, 因此该矩阵的大小为 $\dim_{\mathbb{F}} W \times \dim_{\mathbb{F}} V$. 当我们选取不同的基的时候, 通过乘以坐标变换矩阵, 我们能得到 f 在新的基底下的矩阵表示.

所以如果我们关心的是 $\mathbb{F}$ -线性空间的抽象的线性结构的性质的话, 我们只需要对所有的线性空间 $\mathbb{F}^n$ 以及这些线性空间之间由矩阵给出的线性变换进行研究即可. 用范畴的语言来说, 如果我们考虑 $\mathbb{F}$ 上的矩阵范畴 $\mathbf{Mat}_{\mathbb{F}}$ 和有限维向量空间范畴 $\mathbf{Vect}_{\mathbb{F}, 0}$, 二者 "在某种意义上是相同的". 我们下边在范畴论里对这点进行详细的说明.

之前的讨论告诉我们, 通过对范畴 $\mathbf{Vect}_{\mathbb{F}, 0}$ 中每一个对象选取一组基的方式, 我们可以构造一个范畴 $\mathbf{Vect}_{\mathbb{F}, 0}$ 到 $\mathbf{Mat}_{\mathbb{F}}$ 的函子 F . 任取 $\mathbf{Vect}_{\mathbb{F}, 0}$ 的对象 V , 我们有 $F_0(V) = \dim_{\mathbb{F}} V$. 另一方面, 由于对任意对象 V 我们都选取了一组基 $\mathcal{B}_V$, 那么任取 $\mathbf{Vect}_{\mathbb{F}, 0}$ 的一个态射 $V \xrightarrow{f} W$, 我们有 $F_1(f) = [f]_{\mathcal{B}_V, \mathcal{B}_W}$ 为一个大小为 $\dim V$. 注意到这是 $\mathbf{Mat}_{\mathbb{F}}$ 中从 $\dim V$ 到 $\dim W$ 的态射.

反过来, 由 $\mathbf{Mat}_{\mathbb{F}}$ 到 $\mathbf{Vect}_{\mathbb{F}, 0}$ 也存在一个自然的函子 G . 任取 $\mathbf{Mat}_{\mathbb{F}}$ 的对象 $n \in \mathbb{N}$, 我们有 $G_0(n) = \mathbb{F}^n$. 任取 $\mathbf{Mat}_{\mathbb{F}}$ 态射 $m \xrightarrow{M} n$, 我们有 $G_1(M)$ 为 $\mathbb{F}^m$ 到 $\mathbb{F}^n$ 的由左乘 M 给出的线性映射所给出的 $\mathbb{F}^m$ 到 $\mathbb{F}^n$ 的态射.

任取 $\mathbf{Mat}_{\mathbb{F}}$ 对象 n , 记 $\mathcal{B}_n$ 为我们在构造函数子 F 时为 $\mathbf{Vect}_{\mathbb{F}, 0}$ 的对象 $\mathbb{F}^n$ 选取的基底. 另记 $\mathcal{C}_n$ 为线性空间 $\mathbb{F}^n$ 的典范基. 记 $\alpha_n = [\text{id}_{\mathbb{F}^n}]_{\mathcal{B}_n, \mathcal{C}_n}$ 为恒等线性变换关于这两组基的矩阵表示. 注意到这是一个可逆矩阵. 我们可以将其看作 $\mathbf{Mat}_{\mathbb{F}}$ 中 n 到自己的态射.

任取 $\mathbf{Mat}_{\mathbb{F}}$ 的态射 $m \xrightarrow{M} n$, 我们有以下 $\mathbf{Mat}_{\mathbb{F}}$ 中态射构成的交换图

$$\begin{array}{ccc} m & \xrightarrow{(F \circ G)(M)} & n \\ \alpha_m \downarrow & & \downarrow \alpha_n \\ m & \xrightarrow{M} & n \end{array}$$

由此, 以下这族 $\mathbf{Mat}_{\mathbb{F}}$ 的态射

$$(\alpha_n)_{n \in \text{Ob } \mathbf{Mat}_{\mathbb{F}}},$$

就构成了 $\mathbf{Mat}_{\mathbb{F}}$ 的函子 $F \circ G$ 到恒等函子 ι 的自然变换 α .

对任意 $\mathbf{Mat}_{\mathbb{F}}$ 的对象 m , 我们可以考虑 α_m 的逆矩阵 $\beta_m = \alpha_m^{-1}$, 则任取 $\mathbf{Mat}_{\mathbb{F}}$ 的态射 $m \xrightarrow{M} n$, 可得到以下交换图

$$\begin{array}{ccc} m & \xrightarrow{(F \circ G)(M)} & n \\ \uparrow \beta_m & & \downarrow \beta_n \\ m & \xrightarrow{M} & n \end{array}.$$

由此, 以下这族 $\mathbf{Mat}_{\mathbb{F}}$ 的态射

$$(\beta_n)_{n \in \text{Ob } \mathbf{Mat}_{\mathbb{F}}},$$

就构成了 $\mathbf{Mat}_{\mathbb{F}}$ 的函子 $F \circ G$ 到恒等函子 ι 的自然变换 β . 考虑自然变换的纵复合, 我们有

$$\alpha \circ \beta = \mathbf{1}_{F \circ G}, \quad \beta \circ \alpha = \mathbf{1}_{\iota \mathbf{Mat}_{\mathbb{F}}}.$$

作为 $[\mathbf{Mat}_{\mathbb{F}}, \mathbf{Mat}_{\mathbb{F}}]$ 的态射, 以上告诉我们 α 和 β 都是同构.

另一方面, 我们考虑从 $\mathbf{Vect}_{\mathbb{F},0}$ 到自己的函子 $G \circ F$ 和恒等函子 $\iota_{\mathbf{Vect}_{\mathbb{F},0}}$, 通过将坐标变换矩阵对应到线性变换, 我们也可以得到 $G \circ F$ 到 $\iota_{\mathbf{Vect}_{\mathbb{F},0}}$ 的自然变换 α' . 同样地, 由于坐标变换矩阵可逆, 因此对应的线性变换也可逆. 由此可得作为在 $[\mathbf{Vect}_{\mathbb{F},0}, \mathbf{Vect}_{\mathbb{F},0}]$ 的态射, α' 是一个同构.

以上例子告诉我们, 利用自然变换以及函子空间的同构态射, 我们可以给出一个更宽泛的描述 "范畴相同" 的概念: 范畴等价.

定义 35.5.2

任给两个范畴 $\mathcal{C}$ 和 $\mathcal{D}$, 以及两个从 $\mathcal{C}$ 到 $\mathcal{D}$ 的函子 F 和 G , 设 α 为一个从 F 到 G 的自然变换. 若 α 作为 $[\mathcal{C}, \mathcal{D}]$ 的态射是一个同构, 我们称 α 为 F 到 G 的一个**自然同构**. 此时我们记作 $F \cong G$.

考虑同构态射的定义, 我们有以下结论.

命题 35.5.3

任给两个范畴 $\mathcal{C}$ 和 $\mathcal{D}$, 以及两个从 $\mathcal{C}$ 到 $\mathcal{D}$ 的函子 F 和 G , 设 α 为一个从 F 到 G 的自然变换, 则 α 为一个自然同构当且仅当任取 $A \in \mathcal{C}$, 范畴 $\mathcal{D}$ 中的态射 α_A 为同构.

考虑自然变换的纵复合以及同构态射的定义, 我们可以直接证明这个命题. 证明的具体过程留作练习.

利用自然同构, 我们给出以下范畴等价的定义.

定义 35.5.4

我们称两个范畴 $\mathcal{C}$ 和 $\mathcal{D}$ **等价**, 若存在函子 $F: \mathcal{C} \rightarrow \mathcal{D}$ 以及函子 $G: \mathcal{D} \rightarrow \mathcal{C}$, 同时满足

$$F \circ G \cong \iota_{\mathcal{D}} \quad \text{和} \quad G \circ F \cong \iota_{\mathcal{C}}.$$

此时, 我们称 F 和 G 为 $\mathcal{C}$ 和 $\mathcal{D}$ 之间的**范畴等价**.

利用同构, 我们引入本质满函子的概念.

定义 35.5.5

我们称一个从范畴 $\mathcal{C}$ 到范畴 $\mathcal{D}$ 的函子 F 是**本质满的**, 若对任意 $\mathcal{D}$ 的对象 B , 都存在 $\mathcal{C}$ 的对象 A , 满足

$$F_0(A) \cong B,$$

即 $\mathcal{D}$ 存在一个中 $F(A)$ 到 B 的同构态射.

我们进而有以下函子为范畴等价的一个等价条件.

定理 35.5.6

考虑函子 $F : \mathcal{C} \rightarrow \mathcal{D}$. 以下两个叙述等价:

- 1) F 为一个范畴等价;
- 2) F 为一个完全忠实的, 且本质满的函子.

证明. 1) $\implies$ 2): 设函子 F 为一个范畴等价, 则存在函子 $G : \mathcal{D} \rightarrow \mathcal{C}$, 满足 $\alpha : G \circ F \cong \iota_{\mathcal{C}}$ 和 $\beta : F \circ G \cong \iota_{\mathcal{D}}$.

任取 $\mathcal{C}$ 的对象 A 和 B , 任取 $\mathcal{C}$ 的一个态射 $A \xrightarrow{f} B$, 利用 $G \circ F$ 和 $\iota_{\mathcal{C}}$ 之间的自然同构 α , 我们有

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow \alpha_A & & \downarrow \alpha_B \\ G_0(F_0(A)) & \xrightarrow{G_1(F_1(f))} & G_0(F_0(B)) \end{array}$$

即 $G_1(F_1(f))\alpha_A = \alpha_B f$. 由于 α 为自然同构, 因此 α_A 和 α_B 均为同构态射. 记 $\alpha_A^{-1} \in \text{Hom}_{\mathcal{C}}(G_0(F_0(A)), A)$, 满足 $\alpha_A \alpha_A^{-1} = \mathbf{1}_{G_0(F_0(A))}$. 因此 α_A^{-1} 也是同构态射. 注意到以上交换图对任意 $f \in \text{Hom}_{\mathcal{C}}(A, B)$ 均成立. 利用命题 35.2.7 和 35.2.7 的结论, 我们有

$$\begin{aligned} (\alpha_B)_* \circ (\alpha_A^{-1})^* : \text{Hom}_{\mathcal{C}}(A, B) &\rightarrow \text{Hom}_{\mathcal{C}}(G_0(F_0(A)), G_0(F_0(B))), \\ f &\mapsto \alpha_B f \alpha_A^{-1}, \end{aligned}$$

是双射. 注意到 $(\alpha_B)_* \circ (\alpha_A^{-1})^* = G_1 \circ F_1|_{\text{Hom}_{\mathcal{C}}(A, B)}$. 因此 $F_1|_{\text{Hom}_{\mathcal{C}}(A, B)}$ 是单射. 由此可知 F 为一个忠实函子.

另一方面, 我们考虑任取 $\mathcal{D}$ 的一个态射 $F_0(A) \xrightarrow{g} F_0(B)$, 利用 $F \circ G$ 和 $\iota_{\mathcal{D}}$ 之间的自然同构 β , 我们有

$$\begin{array}{ccc} F_0(A) & \xrightarrow{g} & F_0(B) \\ \downarrow \beta_{F_0(A)} & & \downarrow \beta_{F_0(B)} \\ (F_0 \circ G_0)(F_0(A)) & \xrightarrow{(F_1 \circ G_1)(g)} & (F_0 \circ G_0)(F_0(B)) \end{array}$$

即 $(F_1 \circ G_1)(g)\beta_{F_0(A)} = \beta_{F_0(B)}g$. 由于 β 为自然同构, 因此 $\beta_{F_0(A)}$ 和 $\beta_{F_0(B)}$ 均为同构态射. 记 $\beta_{F_0(A)}^{-1} \in \text{Hom}_{\mathcal{D}}((F_0 \circ G_0)(F_0(A)), F_0(A))$, 满足 $\beta_{F_0(A)} \beta_{F_0(A)}^{-1} = \mathbf{1}_{(F_0 \circ G_0)(F_0(A))}$. 因此 $\beta_{F_0(A)}^{-1}$ 也是同构态射. 注意到以上交换图对任意 $g \in \text{Hom}_{\mathcal{D}}((F_0 \circ G_0)(F_0(A)), F_0(B))$ 均成立. 利用命题 35.2.7 和 35.2.7 的结论, 我们有

$$\begin{aligned} (\beta_{F_0(B)})_* \circ (\beta_{F_0(A)}^{-1})^* : \text{Hom}_{\mathcal{D}}(F_0(A), F_0(B)) &\rightarrow \text{Hom}_{\mathcal{D}}((F_0 \circ G_0)(F_0(A)), (F_0 \circ G_0)(F_0(B))), \\ g &\mapsto \beta_{F_0(B)} g \beta_{F_0(A)}^{-1}, \end{aligned}$$

是双射. 注意到 $(\beta_{F_0(B)})_* \circ (\beta_{F_0(A)}^{-1})^* = F_1 \circ G_1|_{\text{Hom}_{\mathcal{D}}(F_0(A), F_0(B))}$. 因此 $F_1|_{\text{Hom}_{\mathcal{C}}(G_0(F_0(A)), G_0(F_0(B)))}$ 是满射. 因此

$$F_1|_{\text{Hom}_{\mathcal{C}}(A, B)} = F_1|_{\text{Hom}_{\mathcal{C}}(G_0(F_0(A)), G_0(F_0(B)))} \circ ((\alpha_B)_* \circ (\alpha_A^{-1})^*),$$

也是满射由此可知 F 为一个完全函子.

任取 $\mathcal{D}$ 中的对象 C , 我们考虑 $\mathcal{C}$ 中的对象是 $G_0(C)$, 由于 $F \circ G$ 和 $\iota_{\mathcal{D}}$ 自然同构, 因此态射 $\beta_C : F_0(G_0(C)) \rightarrow C$ 为一个同构, 即有 $F_0(G_0(C)) \cong C$. 因此 F 是本质满的.

要证明另一个方向, 我们需要构造函数 $G : \mathcal{D} \rightarrow \mathcal{C}$, 满足 $G \circ F \cong \iota_{\mathcal{C}}$ 和 $F \circ G \cong \iota_{\mathcal{D}}$. 这个构造的过程需要用到选择公理.

任取 X 为 $\mathcal{D}$ 的对象, 由于 F 是本质满的, 因此可以找到 $\mathcal{C}$ 的对象 A , 满足 $F_0(A) \cong X$. 我们定义 $G_0(X) = A$. 任取 $X \in \text{Ob } \mathcal{D}$, 我们选取一个同构态射 $F_0(A) \xrightarrow{g_X} X$

任取 $\mathcal{D}$ 的态射 $X \xrightarrow{g} Y$, 记 $A = G_0(X)$, $B = G_0(Y)$ 为 $\mathcal{C}$ 的对象. 下证存在一个 A 到 B 的态射 f . 注意到在 F 是完全忠实的, 因此我们有以下双射

$$\begin{aligned} \text{Hom}_{\mathcal{C}}(A, B) &\rightarrow \text{Hom}_{\mathcal{D}}(F_0(A), F_0(B)), \\ f &\mapsto F_1(f). \end{aligned}$$

记 g_Y 的逆为 $Y \xrightarrow{g_Y^{-1}} F_0(B)$. 我们考虑 $\mathcal{D}$ 中态射的复合 $g_Y^{-1} \circ g \circ g_X$, 则得到态射 $F_0(A) \xrightarrow{g'} F_0(B)$. 因此存在唯一的 $f \in \text{Hom}_{\mathcal{C}}(A, B)$, 满足 $F_1(f) = g'$. 我们定义 $G_1(g) = f$.

由之前的构造 $\mathcal{D}$ 的态射 g_X 选取不依赖于 f . 直接验证定义可知, 以上构造的 $G = (G_0, G_1)$ 是一个从 $\mathcal{C}$ 到 $\mathcal{D}$ 的函子, 并且满足 $G \circ F = \iota_{\mathcal{C}}$. 要说明 $F \circ G \cong \iota_{\mathcal{D}}$, 我们考虑之前构造的 g_X^{-1} , 将其收集起来就得到了 $F \circ G$ 和 $\iota_{\mathcal{D}}$ 之间的一个自然变换, 由于每一个组成部分都是同构态射, 因此该自然变换是自然同构.

至此我们证明 F 是一个范畴等价. $\square$

注 35.5.7.

以上定理告诉我们, 一个函子 $F : \mathcal{C} \rightarrow \mathcal{D}$ 是一个范畴等价的话, 那么 $F(\mathcal{C})$ 就是 $\mathcal{D}$ 的一个子范畴, 并且在 $\mathcal{D}$ 中的任意一个对象都可以通过同构态射和 $F(\mathcal{C})$ 中的对象联系起来.

让我们回到这部分开始给出的 $\mathbf{Mat}_{\mathbb{F}}$ 和 $\mathbf{Vect}_{\mathbb{F}, 0}$ 的例子. 实际上之前的讨论说明了这两个范畴是等价的. 实际上, 我们是将 $\mathbf{Mat}_{\mathbb{F}}$ 看作是 $\mathbf{Vect}_{\mathbb{F}, 0}$ 形如 $\mathbb{F}^n$ 为对象及其相互之间所有的线性变换构成的子范畴. 以上定理给出的范畴等价的等价条件在这个例子中的所反映的是我们在线性代数中所熟知的一个结论: 任意 $\mathbb{F}$ 上的 n -维线性空间都和 $\mathbb{F}^n$ 线性同构.

实际上, 对一般的范畴等价, 我们也可以做类似的讨论. 以下是范畴等价的等价条件的一个直接的推论.

推论 35.5.8

若 $F : \mathcal{C} \rightarrow \mathcal{D}$ 为一个范畴等价, 则 $F(\mathcal{C})$ 构成 $\mathcal{D}$ 的一个完全子范畴, 并且该子范畴满足如下性质: 任取 $\mathcal{D}$ 的一个对象 Y , 都有 $F(\mathcal{C})$ 的一个对象 X , 满足 $X \cong Y$.

该推论告诉我们若 $F : \mathcal{C} \rightarrow \mathcal{D}$ 是一个范畴等价, 则 F 的像 $F(\mathcal{C})$ 是 $\mathcal{D}$ 的一个与 $\mathcal{C}$ 等价, 且嵌入函子是本质满的特殊的子范畴. 更一般地, 我们有如下骨架的概念.

定义 35.5.9

任取范畴 $\mathcal{C}$, 记 $\mathcal{C}'$ 为范畴 $\mathcal{C}$ 的一个完全子范畴. 若任取 $A \in \text{Ob } \mathcal{C}$, 都有唯一的 $B \in \text{Ob } \mathcal{C}'$, 满足 $A \cong B$, 我们称 $\mathcal{C}'$ 为 $\mathcal{C}$ 的一副**骨架**. 特别地, 如果一个范畴是自己的骨架, 那么就称该范畴为一个**骨架形范畴**.

注 35.5.10.

由范畴等价的等价条件以及骨架的定义, 我们可以看出一个范畴和其任意的一个骨架都是等价的.

我们首先来说明范畴的骨架的存在性.

命题 35.5.11

任意范畴都有一个骨架.

证明. 任取一个范畴 $\mathcal{C}$. 注意到对象的同构满足自反性, 对称性和传递性, 因此在 $\text{Ob } \mathcal{C}$ 上定义了一个等价关系. 任取 $A \in \text{Ob } \mathcal{C}$, 我们记 $[A]$ 为所有 $\text{Ob } \mathcal{C}$ 中与 A 同构的对象构成的全体, 也即关于同构等价关系的等价类. 利用选择公理, 任给等价类 $[A]$, 我们选取一个代表元 $A' \in [A]$. 考虑这样的代表元的全体构成的完全子范畴, 即为 $\mathcal{C}$ 的一个骨架. $\square$

例 35.5.12. (i) 在 $\mathbf{Vect}_{\mathbb{F},0}$ 中, 所有 $\mathbb{F}^n$ 给出的完全子范畴就是 $\mathbf{Vect}_{\mathbb{F},0}$ 的一个骨架.

(ii) 如果 $\mathcal{C}$ 是一个离散范畴, 那么 $\mathcal{C}$ 就是自己就是一个骨架, 此时 $\mathcal{C}$ 是一个骨架形范畴.

注意到在 $\mathbf{Vect}_{\mathbb{F},0}$ 中, 我们可以对每一个维数 n 取一个 $\mathbb{F}$ -线性空间, 考虑这些对象给出的 $\mathbf{Vect}_{\mathbb{F},0}$ 的完全子范畴, 我们也得到一个骨架. 但是另一方面, 离散范畴的骨架就是其自身, 因此此类范畴有唯一的骨架. 由此我们看出, 范畴的骨架在严格意义下是不一定唯一的. 但另一方面, 在 $\mathbf{Vect}_{\mathbb{F},0}$ 的例子中, 任取两个骨架, 我们都可以找到二者之间一个自然的同构.

命题 35.5.13

一个范畴任意两个骨架之间都是同构的, 因此任意范畴的骨架在同构意义下是唯一的.

该命题的证明可以同构直接构造同构函子得到, 具体细节留作练习.

作为该命题的一个推论, 我们可以得到如下范畴同构和范畴等价之间的关系.

推论 35.5.14

两个范畴 $\mathcal{C}$ 和 $\mathcal{D}$ 等价当且仅当它们的骨架同构.

第三十六章 函子的伴随

36.1 伴随

记 $\mathcal{C}$ 和 $\mathcal{D}$ 为两个等价的范畴. 在之前的章节中, 我们看到二者之间的等价是通过一对满足特殊关系的函子

$$F: \mathcal{C} \rightarrow \mathcal{D} \quad \text{和} \quad G: \mathcal{D} \rightarrow \mathcal{C},$$

联系起来的. 这样的两个函子被称为范畴等价. 之后, 我们进一步证明了一个函子是范畴等价当且仅当它是完全忠实, 且本质满的. 因此, 任给 $A \in \text{Ob } \mathcal{C}$ 以及 $X \in \text{Ob } \mathcal{D}$, 我们有双射

$$\text{Hom}_{\mathcal{D}}(F_0(A), X) \cong \text{Hom}_{\mathcal{C}}(G_0(F_0(A)), G_0(X)).$$

由于 $G \circ F$ 与 $\text{id}_{\mathcal{C}}$ 自然同构, 我们可以进一步得到双射

$$\varphi_{A,X}: \text{Hom}_{\mathcal{D}}(F_0(A), X) \cong \text{Hom}_{\mathcal{C}}(A, G_0(X)).$$

这个双射与 $\mathcal{C}$ 和 $\mathcal{D}$ 中的态射也有很好的互动. 任取 $\mathcal{D}$ 中态射 $X \xrightarrow{u} Y$, 我们有

$$\begin{aligned} u_*: \text{Hom}_{\mathcal{D}}(F_0(A), X) &\rightarrow \text{Hom}_{\mathcal{D}}(F_0(A), Y), \\ v &\mapsto uv, \end{aligned}$$

以及

$$\begin{aligned} (G_1(u))_*: \text{Hom}_{\mathcal{C}}(A, G_0(X)) &\rightarrow \text{Hom}_{\mathcal{C}}(A, G_0(Y)), \\ f &\mapsto G_1(u)f. \end{aligned}$$

并且二者满足一下交换图

$$\begin{array}{ccc} \text{Hom}_{\mathcal{D}}(F_0(A), X) & \xrightarrow{u_*} & \text{Hom}_{\mathcal{D}}(F_0(A), Y) \\ \varphi_{A,X} \downarrow & & \downarrow \varphi_{A,Y} \\ \text{Hom}_{\mathcal{C}}(A, G_0(X)) & \xrightarrow{(G_1(u))_*} & \text{Hom}_{\mathcal{C}}(A, G_0(Y)) \end{array}$$

类似地, 任取 $\mathcal{C}$ 中的态射 $A \xrightarrow{f} B$, 我们有一下交换图

$$\begin{array}{ccc} \text{Hom}_{\mathcal{D}}(F_0(B), X) & \xrightarrow{(F_1(f))^*} & \text{Hom}_{\mathcal{D}}(F_0(A), X) \\ \varphi_{B,X} \downarrow & & \downarrow \varphi_{A,X} \\ \text{Hom}_{\mathcal{C}}(B, G_0(X)) & \xrightarrow{f^*} & \text{Hom}_{\mathcal{C}}(A, G_0(X)) \end{array}$$

这种现象被称为函子 F 和 G 的伴随. 更一般地, 我们有如下定义.

定义 36.1.1 (伴随的定义)

任取范畴 $\mathcal{C}$ 和 $\mathcal{D}$, 记

$$F : \mathcal{C} \rightarrow \mathcal{D} \quad \text{和} \quad G : \mathcal{D} \rightarrow \mathcal{C}.$$

为两个函子. 我们称函子 F 为 G 的**左伴随** (同时称 G 为 F 的**右伴随**), 记作 $F \dashv G$, 若对任意 $A \in \text{Ob } \mathcal{C}$ 和 $X \in \text{Ob } \mathcal{D}$, 都有双射

$$\varphi_{A,X} : \text{Hom}_{\mathcal{D}}(F_0(A), X) \xrightarrow{\cong} \text{Hom}_{\mathcal{C}}(A, G_0(X)),$$

满足任取 $A \xrightarrow{f} B \in \text{Mor } \mathcal{C}$ 以及 $X \xrightarrow{u} Y \in \text{Mor } \mathcal{D}$, 都有以下交换图

$$\begin{array}{ccccc} \text{Hom}_{\mathcal{D}}(F_0(B), X) & \xrightarrow{(F_1(f))^*} & \text{Hom}_{\mathcal{D}}(F_0(A), X) & \xrightarrow{u_*} & \text{Hom}_{\mathcal{D}}(F_0(A), Y) \\ \downarrow \varphi_{B,X} & & \downarrow \varphi_{A,X} & & \downarrow \varphi_{A,Y} \\ \text{Hom}_{\mathcal{C}}(B, G_0(X)) & \xrightarrow{f^*} & \text{Hom}_{\mathcal{C}}(A, G_0(X)) & \xrightarrow{(G_1(u))^*} & \text{Hom}_{\mathcal{C}}(A, G_0(Y)) \end{array}$$

我们称双射 $\varphi_{A,X}$ 的全体

$$\varphi := (\varphi_{A,X})_{A \in \text{Ob } \mathcal{C}, X \in \text{Ob } \mathcal{D}}$$

为**伴随变换**, 并称 (F, G, φ) 为一个**伴随对**.

注 36.1.2.

我们通常使用记号 $\mathcal{C} \xrightleftharpoons[\varphi]{F} \mathcal{D}$ 来表示函子 F 是函子 G 的左伴随.

函子伴随是一个比等价更一般的概念, 并且是一个我们在研究范畴时常见的现象. 我们这里来给出一些例子来进行说明.

例 36.1.3 (自由函子和遗忘函子).

我们可以在不同范畴对之间构造自由函子和遗忘函子, 并且不同情形下同类型函子构造是类似的. 此处我们以集合范畴 **Set** 和群范畴 **Group** 之间的自由函子和遗忘函子来进行说明. 我们记 **Group** 到 **Set** 的遗忘函子为 F , 并记 **Set** 到 **Group** 的自由函子为 G .

任取一个集合 A , 记 F^A 为集合 A 生成的自由群, 并将 A 看作是 F^A 的一组自由基. 任取群同态 $u : F^A \rightarrow X$, 通过忘掉群结构, 我们有一个映射 $u : F^A \rightarrow X$, 通过将映射 u 限制在 A 上, 我们得到了一个映射

$$v = u|_A : A \rightarrow X.$$

考虑集合范畴和群范畴的定义, 以上讨论帮助我们构造了以下映射

$$\begin{aligned} \varphi_{A,X} : \text{Hom}_{\mathcal{D}}(F_0(A), X) &\rightarrow \text{Hom}_{\mathcal{C}}(A, G_0(X)) \\ u &\mapsto v = u|_A \end{aligned}$$

利用之前的构造直接验证可得这是一个双射. 此处应注意 $G_0(F_0(A)) \neq A$.

我们下边验证这样的双射满足伴随定义中的交换图. 任取集合 B 以及映射 $f : A \rightarrow B$, 由自由群的泛性质, 可得

$$F_1(f) : F_0(A) \rightarrow F_0(B).$$

考虑群同态 $u : F_0(B) \rightarrow X$, 通过复合我们有群同态

$$u' = (F_1(f))^*(u) : F_0(A) \rightarrow X.$$

将其看作集合之间的映射, 并将其限制在子集 A 上, 我们得到映射

$$v' = (F_1(f))^*(u)|_A : A \rightarrow X.$$

另一方面, 将 u 看作集合间的映射, 并限制在 B 上可得 $v : B \rightarrow X$. 以上提到的映射之间满足以下交换图: 我们有以下交换图:

$$\begin{array}{ccccc} & & v' & & \\ & \curvearrowright & & \curvearrowleft & \\ A & \xrightarrow{f} & B & \xrightarrow{v} & X \\ \downarrow i_A & & \downarrow i_B & & \downarrow \text{id}_X \\ F_0(A) & \xrightarrow{F_1(f)} & F_0(B) & \xrightarrow{u} & X \\ & \curvearrowleft & & \curvearrowright & \\ & & u' & & \end{array}$$

这里 i_A 和 i_B 分别将 A 和 B 送到其在 $F_0(A)$ 和 $F_0(B)$ 对应的元素. 因此我们有以下交换图:

$$\begin{array}{ccc} \text{Hom}_{\mathcal{D}}(F_0(B), X) & \xrightarrow{(F_1(f))^*} & \text{Hom}_{\mathcal{D}}(F_0(A), X) \\ \downarrow \varphi_{B,X} & & \downarrow \varphi_{A,X} \\ \text{Hom}_{\mathcal{C}}(B, G_0(X)) & \xrightarrow{f^*} & \text{Hom}_{\mathcal{C}}(A, G_0(X)) \end{array}$$

另一半交换图的验证过程类似, 此处不再赘述. 由此可得, 自由函子 F , 遗忘函子 G 以及映射族 $\varphi = (\varphi_{A,X})_{A \in \text{Ob } \mathcal{C}, X \in \text{Ob } \mathcal{D}}$ 构成一个伴随对 (F, G, φ) , 表示如下图

$$\mathbf{Set} \begin{array}{c} \xrightarrow{F} \\ \xleftarrow[\varphi]{\perp} \\ \xleftarrow{G} \end{array} \mathbf{Group}.$$

注意到这里遗忘函子 G 并不是自由函子 F 的左伴随. 例如, 假设 X 是一个有限群, 则其到自由群只有平凡同态, 即将所有元素都送到自由群的幺元. 但是任给一个至少包含两个元素的集合 A , 作为集合 X 到 A 的映射多余 1 个. 因此不存在 $\text{Hom}_{\mathcal{C}}(G_0(X), A)$ 到 $\text{Hom}_{\mathcal{D}}(X, F_0(A))$ 的双射. 这个例子也说明函子作为其他函子的左伴随是一个比作为范畴等价更一般的概念.

如果函子 F 和 G 来自于范畴等价, 则函子 F 和 G 互为左伴随, 且互为右伴随. 另一方面, 之前的例子告诉我们一个函子 G 是另一个函子 F 的右伴随不能保证 G 是 F 的左伴随. 下边的例子告诉我们, 一个函子 G 也可能同时为一个函子 F 的左伴随和一个函子 H 的右伴随, 且 F 和 H 不同.

例 36.1.4.

36.2 伴随变换与 Hom-函子

注意到在函子伴随的定义中, 我们所用的性质与在定义自然变换中使用的性质形式上相似. 实际上, 考虑局部小范畴的情形, 范畴变换是下边将介绍的 Hom-函子之间的自然变换.

Hom-函子

记 $\mathcal{C}$ 为一个局部小范畴. 任给其中的两个对象 A, B , 我们通常称 $\text{Hom}_{\mathcal{C}}(A, B)$ 为一个 Hom-集. 利用 Hom-集我们可以如下构造一个从乘积范畴 $\mathcal{C}^{\text{op}} \times \mathcal{C}$ 到集合范畴 **Set** 的函子 Hom, 满足:

$$\begin{aligned}\text{Hom}_0 : \text{Ob}(\mathcal{C}^{\text{op}} \times \mathcal{C}) &\rightarrow \text{Ob } \mathbf{Set}, \\ (A, B) &\mapsto \text{Hom}_{\mathcal{C}}(A, B).\end{aligned}$$

任取态射 $(A \xrightarrow{f^{\text{op}}} C, B \xrightarrow{g} D) \in \text{Mor}(\mathcal{C}^{\text{op}} \times \mathcal{C})$, 通过态射的复合我们有映射

$$\begin{aligned}\psi_{f^{\text{op}}, g} : \text{Hom}_{\mathcal{C}}(A, B) &\rightarrow \text{Hom}_{\mathcal{C}}(C, D), \\ h &\mapsto ghf.\end{aligned}$$

由此我们定义 $\text{Hom}_1(f^{\text{op}}, g) = \psi_{f^{\text{op}}, g}$.

如果 $G : \mathcal{D} \rightarrow \mathcal{C}$ 是两个局部小范畴之间的函子, 则我们考虑 $\mathcal{C}$ 中的 Hom-集定义从 $\mathcal{C}^{\text{op}} \times \mathcal{D}$ 出发的 Hom-函子记作 Hom_G . 具体地, 我们有

$$\begin{aligned}(\text{Hom}_G)_0 : \text{Ob}(\mathcal{C}^{\text{op}} \times \mathcal{D}) &\rightarrow \text{Ob } \mathbf{Set}, \\ (A, X) &\mapsto \text{Hom}_{\mathcal{C}}(A, G_0(X)).\end{aligned}$$

任取态射 $(A \xrightarrow{f^{\text{op}}} B, X \xrightarrow{u} Y) \in \text{Mor}(\mathcal{C}^{\text{op}} \times \mathcal{D})$, 通过态射的复合我们有映射

$$\begin{aligned}(\text{Hom}_G)_1(f^{\text{op}}, u) : \text{Hom}_{\mathcal{C}}(A, G_0(X)) &\rightarrow \text{Hom}_{\mathcal{C}}(B, G_0(Y)), \\ h &\mapsto (G_1(u))hf.\end{aligned}$$

类似地, 如果 $F : \mathcal{C} \rightarrow \mathcal{D}$, 我们可以考虑 $\mathcal{D}$ 中的 Hom-集来定义 $\mathcal{C}^{\text{op}} \times \mathcal{D}$ 出发的 Hom-函子, 记作 ${}_F\text{Hom}$. 具体地, 我们有

$$\begin{aligned}({}_F\text{Hom})_0 : \text{Ob}(\mathcal{C}^{\text{op}} \times \mathcal{D}) &\rightarrow \text{Ob } \mathbf{Set}, \\ (A, X) &\mapsto \text{Hom}_{\mathcal{D}}(F_0(A), X).\end{aligned}$$

任取态射 $(A \xrightarrow{f^{\text{op}}} B, X \xrightarrow{u} Y) \in \text{Mor}(\mathcal{C}^{\text{op}} \times \mathcal{D})$, 通过态射的复合我们有映射

$$\begin{aligned}({}_F\text{Hom})_1(f^{\text{op}}, u) : \text{Hom}_{\mathcal{D}}(F_0(A), X) &\rightarrow \text{Hom}_{\mathcal{D}}(F_0(B), Y), \\ h &\mapsto uhF_1(f).\end{aligned}$$

注 36.2.1.

任取局部小范畴 $\mathcal{C}$ 和 $\mathcal{D}$, 以及函子 $F : \mathcal{C} \rightarrow \mathcal{D}$ 以及 $G : \mathcal{D} \rightarrow \mathcal{C}$, 我们记从 $\mathcal{C}^{\text{op}} \times \mathcal{D}$ 出发的关于 F 和 G 的 Hom-函子为 ${}_F\text{Hom}_G$. 若 F 或 G 为恒等函子, 我们略去对应的记号, 记做 Hom_G 或者 ${}_F\text{Hom}$. 若二者均为恒等函子, 我们将其记作 Hom.

伴随变换是 Hom-函子之间的自然变换

重新观察伴随变换的定义, 我们会发现这实际上是两个 Hom-函子之间的自然变换. 仍记 $\mathcal{C}$ 和 $\mathcal{D}$ 为两个局部小范畴, 并考虑函子 $F : \mathcal{C} \rightarrow \mathcal{D}$ 和 $G : \mathcal{D} \rightarrow \mathcal{C}$. 设 (F, G, φ) 构成一个伴随对. 我们考虑 F 和 G 给出的 $\mathcal{C}^{\text{op}} \times \mathcal{D}$ 到集合范畴 **Set** 的 Hom-函子, 分别记作 ${}_F\text{Hom}$ 和 Hom_G .

任取 $\mathcal{C}^{\text{op}} \times \mathcal{D}$ 的态射 $(A, X) \xrightarrow{(f^{\text{op}}, u)} (B, Y)$, 考虑伴随变换, 我们有双射 $\varphi_{A, X}$ 和 $\varphi_{B, Y}$, 满足

$$\begin{array}{ccc}\text{Hom}_{\mathcal{D}}(F_0(A), X) & \xrightarrow{({}_F\text{Hom})_1(f^{\text{op}}, u)} & \text{Hom}_{\mathcal{D}}(F_0(B), Y) \\ \downarrow \varphi_{A, X} & & \downarrow \varphi_{B, Y} \\ \text{Hom}_{\mathcal{D}}(A, G_0(X)) & \xrightarrow{(\text{Hom}_G)_1(f^{\text{op}}, u)} & \text{Hom}_{\mathcal{D}}(B, G_0(Y))\end{array}$$

由此可知伴随变换是函子 ${}_F\text{Hom}$ 到 Hom_C 的自然变换.

36.3 单位和余单位

记 $\mathcal{C}$ 和 $\mathcal{D}$ 为两个范畴, 并记 $F: \mathcal{C} \rightarrow \mathcal{D}$ 和 $G: \mathcal{D} \rightarrow \mathcal{C}$ 为两个函子. 设 (F, G, φ) 为一个伴随对. 任取 $A \in \text{Ob } \mathcal{C}$ 和 $X \in \text{Ob } \mathcal{D}$, 我们有

$$\varphi_{A,X}: \text{Hom}_{\mathcal{D}}(F_0(A), X) \rightarrow \text{Hom}_{\mathcal{C}}(A, G_0(X)).$$

任取 $B \in \text{Ob } \mathcal{C}$, 并取 $X = F_0(B)$, 我们有以下映射的复合:

$$\text{Hom}_{\mathcal{C}}(A, B) \rightarrow \text{Hom}_{\mathcal{D}}(F_0(A), F_0(B)) \rightarrow \text{Hom}_{\mathcal{C}}(A, G_0(F_0(B))).$$

利用伴随变换定义中的交换图, 任取 $\mathcal{C}$ 中的态射 $A \xrightarrow{f} B$, 我们有以下交换图:

$$\begin{array}{ccccc} \text{Hom}_{\mathcal{C}}(B, B) & \xrightarrow{f^*} & \text{Hom}_{\mathcal{C}}(A, B) & \xleftarrow{f_*} & \text{Hom}_{\mathcal{C}}(A, A) \\ \downarrow F_1 & & \downarrow F_1 & & \downarrow F_1 \\ \text{Hom}_{\mathcal{D}}(F_0(B), F_0(B)) & \xrightarrow{(F_1(f))^*} & \text{Hom}_{\mathcal{D}}(F_0(A), F_0(B)) & \xleftarrow{(F_1(f))_*} & \text{Hom}_{\mathcal{D}}(F_0(A), F_0(A)) \\ \downarrow \varphi_{B, F_0(B)} & & \downarrow \varphi_{A, F_0(B)} & & \downarrow \varphi_{A, F_0(A)} \\ \text{Hom}_{\mathcal{C}}(B, G_0(F_0(B))) & \xrightarrow{f^*} & \text{Hom}_{\mathcal{C}}(A, G_0(F_0(B))) & \xleftarrow{(G_1(F_1(f)))_*} & \text{Hom}_{\mathcal{C}}(A, G_0(F_0(A))) \end{array}.$$

我们考虑恒等态射 $\mathbf{1}_A$ 和 $\mathbf{1}_B$, 则有

$$\begin{array}{ccccc} \mathbf{1}_B & \xrightarrow{f^*} & f & \xleftarrow{f_*} & \mathbf{1}_A \\ \downarrow F_1 & & \downarrow F_1 & & \downarrow F_1 \\ \mathbf{1}_{F_0(B)} & \xrightarrow{(F_1(f))^*} & F_1(f) & \xleftarrow{(F_1(f))_*} & \mathbf{1}_{F_0(A)} \\ \downarrow \varphi_{B, F_0(B)} & & \downarrow \varphi_{A, F_0(B)} & & \downarrow \varphi_{A, F_0(A)} \\ \varphi_{B, F_0(B)}(\mathbf{1}_{F_0(B)}) & \xrightarrow{f^*} & \varphi_{A, F_0(B)}(F_1(f)) & \xleftarrow{(G_1(F_1(f)))_*} & \varphi_{A, F_0(A)}(\mathbf{1}_{F_0(A)}) \end{array}.$$

因此我们有 $f^* \varphi_{B, F_0(B)}(\mathbf{1}_{F_0(B)}) = (G_1(F_1(f)))_*(\varphi_{A, F_0(A)}(\mathbf{1}_{F_0(A)}))$. 分别记 $\eta_A = \varphi_{A, F_0(A)}(\mathbf{1}_{F_0(A)})$ 和 $\eta_B = \varphi_{B, F_0(B)}(\mathbf{1}_{F_0(B)})$, 以上关系给出下边的交换图

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \eta_A \downarrow & & \downarrow \eta_B \\ G_0(F_0(A)) & \xrightarrow{G_1(F_1(f))} & G_0(F_0(B)) \end{array}$$

因此态射族

$$\eta := (\eta_A)_{A \in \text{Ob } \mathcal{C}},$$

构成 $\iota_{\mathcal{C}}$ 到 $G \circ F$ 的自然变换:

$$\begin{array}{ccc} & \iota_{\mathcal{C}} & \\ \mathcal{C} & \xrightarrow{\quad} & \mathcal{C} \\ & \eta \downarrow & \\ & G \circ F & \end{array}$$

类似地, 任取 $Y \in \text{Ob } \mathcal{D}$, 并取 $A = G_0(Y)$, 我们有以下映射的复合:

$$\text{Hom}_{\mathcal{D}}(F_0(G_0(Y)), X) \rightarrow \text{Hom}_{\mathcal{C}}(G_0(Y), G_0(X)).$$

利用伴随变换定义中的交换图, 任取 $\mathcal{D}$ 中的态射 $X \xrightarrow{u} Y$, 我们有以下交换图:

$$\begin{array}{ccccc} \mathrm{Hom}_{\mathcal{D}}(F_0(G_0(Y)), Y) & \xrightarrow{(F_1(G_1(u)))^*} & \mathrm{Hom}_{\mathcal{D}}(F_0(G_0(X)), Y) & \xleftarrow{u_*} & \mathrm{Hom}_{\mathcal{D}}(F_0(G_0(X)), X) \\ \downarrow \varphi_{G_0(Y), Y} & & \downarrow \varphi_{G_0(X), Y} & & \downarrow \varphi_{G_0(X), X} \\ \mathrm{Hom}_{\mathcal{C}}(G_0(Y), G_0(Y)) & \xrightarrow{(G_1(u))^*} & \mathrm{Hom}_{\mathcal{C}}(G_0(X), G_0(Y)) & \xleftarrow{(G_1(u))^*} & \mathrm{Hom}_{\mathcal{C}}(G_0(X), G_0(X)) \end{array}$$

我们考虑恒等态射 $\mathbf{1}_{G_0(X)}$ 和 $\mathbf{1}_{G_0(Y)}$, 由于伴随变换中的映射都是双射, 我们有 $\mathcal{D}$ 中的态射

$$\epsilon_X = \varphi_{G_0(X), X}^{-1}(\mathbf{1}_{G_0(X)}), \epsilon_Y = \varphi_{G_0(Y), Y}^{-1}(\mathbf{1}_{G_0(Y)}), v = \varphi_{G_0(X), Y}^{-1}(G_1(u)),$$

满足

$$\begin{array}{ccccc} \epsilon_Y & \xrightarrow{(F_1(G_1(u)))^*} & v & \xleftarrow{u_*} & \epsilon_X \\ \downarrow \varphi_{G_0(Y), Y} & & \downarrow \varphi_{G_0(X), Y} & & \downarrow \varphi_{G_0(X), X} \\ \mathbf{1}_{G_0(Y)} & \xrightarrow{(G_1(u))^*} & u & \xleftarrow{(G_1(u))^*} & \mathbf{1}_{G_0(X)} \end{array}.$$

注意到 $v = \epsilon_Y(F_1(G_1(u))) = u\epsilon_X$, 因此我们有交换图

$$\begin{array}{ccc} F_0(G_0(X)) & \xrightarrow{F_1(G_1(u))} & F_0(G_0(Y)) \\ \epsilon_X \downarrow & & \downarrow \epsilon_Y \\ X & \xrightarrow{u} & Y \end{array}$$

因此态射族

$$\epsilon := (\epsilon_X)_{X \in \mathrm{Ob} \mathcal{D}},$$

构成 $F \circ G$ 到 $\mathcal{D}$ 的自然变换:

$$\mathcal{D} \begin{array}{c} \xrightarrow{F \circ G} \\ \Downarrow \epsilon \\ \xrightarrow{\quad} \end{array} \mathcal{D}.$$

定义 36.3.1

沿用以上记号, 自然变换 η 和 ϵ 分别被称作伴随对 (F, G, φ) 的**单位**和**余单位**.

一个伴随对的单位和余单位进一步满足以下三角等式.

命题 36.3.2

记 $F: \mathcal{C} \rightarrow \mathcal{D}$ 和 $G: \mathcal{D} \rightarrow \mathcal{C}$ 为两个函子. 设 (F, G, φ) 为一个伴随对, 并将其单位和余单位分别记作 η 和 ϵ . 我们有以下两个关于自然变换的三角等式

$$\begin{array}{ccc} F & \xrightarrow{F\eta} & F \circ G \circ F \\ & \searrow \mathbf{1}_F & \downarrow \epsilon_F \\ & & F \end{array} \quad \text{和} \quad \begin{array}{ccc} G & \xrightarrow{\eta G} & G \circ F \circ G \\ & \searrow \mathbf{1}_G & \downarrow G\epsilon \\ & & G \end{array}$$

即我们有自然变换的纵复合

$$(\epsilon F) \circ (F\eta) = \mathbf{1}_F \quad \text{和} \quad (\epsilon G) \circ (G\eta) = \mathbf{1}_G.$$

证明. 任取 $A \in \text{Ob } \mathcal{C}$ 以及任意 $X \in \text{Ob } \mathcal{D}$, 我们需要证明以下两个交换图:

$$\begin{array}{ccc} F_0(A) & \xrightarrow{F_1(\eta_A)} & F_0(G_0(F_0(A))) \\ & \searrow \mathbf{1}_{F_0(A)} & \downarrow \epsilon_{F_0(A)} \\ & & F_0(A) \end{array} \quad \text{以及} \quad \begin{array}{ccc} G_0(X) & \xrightarrow{\eta_{G_0(X)}} & G_0(F_0(G_0(X))) \\ & \searrow \mathbf{1}_{G_0(X)} & \downarrow G_1(\epsilon_X) \\ & & G_0(X) \end{array}$$

成立.

由 F 和 G 伴随, 我们首先考虑以下交换图

$$\begin{array}{ccc} \text{Hom}_{\mathcal{D}}(F_0(G_0(F_0(A))), F_0(A)) & \xrightarrow{(F_1(\eta_A))^*} & \text{Hom}_{\mathcal{D}}(F_0(A), F_0(A)) \\ \downarrow \varphi_{G_0(F_0(A)), F_0(A)} & & \downarrow \varphi_{A, F_0(A)} \\ \text{Hom}_{\mathcal{C}}(G_0(F_0(A)), G_0(F_0(A))) & \xrightarrow{(\eta_A)^*} & \text{Hom}_{\mathcal{C}}(A, G_0(F_0(A))) \end{array}$$

考虑 $\mathbf{1}_{G_0(F_0(A))} \in \text{Hom}_{\mathcal{C}}(G_0(F_0(A)), G_0(F_0(A)))$, 利用 $\epsilon_{F_0(A)}$ 和 η_A 得到以下关系

$$\begin{array}{ccc} \epsilon_{F_0(A)} & \xrightarrow{\quad} & \epsilon_{F_0(A)} \circ F_1(\eta_A) \\ \downarrow & & \downarrow \\ \mathbf{1}_{G_0(F_0(A))} & \xrightarrow{\quad} & \eta_A \end{array}$$

并进一步得到

$$\epsilon_{F_0(A)} \circ F_1(\eta_A) = \mathbf{1}_{F_0(A)}.$$

我们接着考虑下边的交换图

$$\begin{array}{ccc} \text{Hom}_{\mathcal{D}}(F_0(G_0(X)), F_0(G_0(X))) & \xrightarrow{(\epsilon_X)^*} & \text{Hom}_{\mathcal{D}}(F_0(G_0(X)), X) \\ \downarrow \varphi_{G_0(X), F_0(G_0(X))} & & \downarrow \varphi_{G_0(X), X} \\ \text{Hom}_{\mathcal{C}}(G_0(X), G_0(F_0(G_0(X)))) & \xrightarrow{(G_1(\epsilon_X))^*} & \text{Hom}_{\mathcal{C}}(G_0(X), G_0(X)) \end{array}$$

考虑 $\mathbf{1}_{F_0(G_0(X))} \in \text{Hom}_{\mathcal{D}}(F_0(G_0(X)), F_0(G_0(X)))$, 利用 $\epsilon_{F_0(A)}$ 和 η_A 得到以下关系

$$\begin{array}{ccc} \mathbf{1}_{F_0(G_0(X))} & \xrightarrow{\quad} & \epsilon_X \\ \downarrow & & \downarrow \\ \eta_{G_0(X)} & \xrightarrow{\quad} & G_1(\epsilon_X) \circ \eta_{G_0(X)} \end{array}$$

并进一步得到

$$G_1(\epsilon_X) \circ \eta_{G_0(X)} = \mathbf{1}_{G_0(X)}.$$

下边任取 $\mathcal{C}$ 的态射 $A \xrightarrow{f} B$, 利用自然变换 η , 我们有

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \eta_A \downarrow & & \downarrow \eta_B \\ G_0(F_0(A)) & \xrightarrow{G_1(F_1(f))} & G_0(F_0(B)) \end{array}$$

利用函子 F 的作用, 我们有以下交换图

$$\begin{array}{ccc} F_0(A) & \xrightarrow{F_1(f)} & F_0(B) \\ F_1(\eta_A) \downarrow & & \downarrow F_1(\eta_B) \\ F_0(G_0(F_0(A))) & \xrightarrow{F_1(G_1(F_1(f)))} & F_0(G_0(F_0(B))) \end{array}.$$

利用自然变换 ϵ , 我们可以将以上交换图扩展为下图

$$\begin{array}{ccc}
 F_0(A) & \xrightarrow{F_1(f)} & F_0(B) \\
 \downarrow F_1(\eta_A) & & \downarrow F_1(\eta_B) \\
 F_0(G_0(F_0(A))) & \xrightarrow{F_1(G_1(F_1(f)))} & F_0(G_0(F_0(B))) \\
 \downarrow \epsilon_{F_0(A)} & & \downarrow \epsilon_{F_0(B)} \\
 F_0(A) & \xrightarrow{F_1(f)} & F_0(B)
 \end{array}$$

由此可得 $(\epsilon F) \circ (F\eta) = \mathbf{1}_F$, 即第一个三角等式.

类似地, 任取 $\mathcal{D}$ 中的态射 $X \xrightarrow{u} Y$, 我们有以下交换图

$$\begin{array}{ccc}
 G_0(X) & \xrightarrow{G_1(u)} & G_0(Y) \\
 \downarrow \eta_{G_0(X)} & & \downarrow \eta_{G_0(Y)} \\
 G_0(F_0(G_0(X))) & \xrightarrow{G_1(F_1(G_1(u)))} & G_0(F_0(G_0(Y))) \\
 \downarrow G_1(\epsilon_X) & & \downarrow G_1(\epsilon_Y) \\
 F_0(X) & \xrightarrow{F_1(f)} & F_0(Y)
 \end{array}$$

由此可得 $(\epsilon G) \circ (G\eta) = \mathbf{1}_G$, 即第二个三角等式. $\square$

下边这个结论告诉我们, 单位和余单位的存在性以及满足三角等式的性质也可以反过来用来刻画函子之间的伴随.

命题 36.3.3

记 $F: \mathcal{C} \rightarrow \mathcal{D}$ 和 $G: \mathcal{D} \rightarrow \mathcal{C}$ 为两个函子, 则 F 为 G 的左伴随, 当且仅当存在自然变换

$$\mathcal{C} \begin{array}{c} \xrightarrow{\iota_{\mathcal{C}}} \\ \Downarrow \eta \\ \xrightarrow{G \circ F} \end{array} \mathcal{C} \quad \text{和} \quad \mathcal{D} \begin{array}{c} \xrightarrow{F \circ G} \\ \Downarrow \epsilon \\ \xrightarrow{\iota_{\mathcal{D}}} \end{array} \mathcal{D},$$

满足三角等式

$$\begin{array}{ccc}
 F & \xrightarrow{F\eta} & F \circ G \circ F \\
 & \searrow \mathbf{1}_F & \downarrow \epsilon_F \\
 & & F
 \end{array}
 \quad \text{和} \quad
 \begin{array}{ccc}
 G & \xrightarrow{G\eta} & G \circ F \circ G \\
 & \searrow \mathbf{1}_G & \downarrow G\epsilon \\
 & & G
 \end{array}$$

证明. 我们已经在之前的讨论中证明了必要性. 下边证明充分性. 假设存在自然变换

$$\mathcal{C} \begin{array}{c} \xrightarrow{\iota_{\mathcal{C}}} \\ \Downarrow \eta \\ \xrightarrow{G \circ F} \end{array} \mathcal{C} \quad \text{和} \quad \mathcal{D} \begin{array}{c} \xrightarrow{F \circ G} \\ \Downarrow \epsilon \\ \xrightarrow{\iota_{\mathcal{D}}} \end{array} \mathcal{D},$$

并满足三角等式

任取 $A \in \text{Ob } \mathcal{C}$ 和 $X \in \text{Ob } \mathcal{D}$, 我们都有态射

$$\eta_A: A \rightarrow G_0(F_0(A)) \quad \epsilon_X: F_0(G_0(X)) \rightarrow X.$$

我们考虑以下映射的复合

$$\varphi_{A,X} : \text{Hom}_{\mathcal{D}}(F_0(A), X) \xrightarrow{G_1} \text{Hom}_{\mathcal{C}}(G_0(F_0(A)), G_0(X)) \xrightarrow{(\eta_A)^*} \text{Hom}_{\mathcal{C}}(A, G_0(X))$$

以及

$$\psi_{A,X} : \text{Hom}_{\mathcal{C}}(A, G_0(X)) \xrightarrow{F_1} \text{Hom}_{\mathcal{C}}(F_0(A), F_0(G_0(X))) \xrightarrow{(\epsilon_X)_*} \text{Hom}_{\mathcal{C}}(F_0(A), X)$$

任取 $u \in \text{Hom}_{\mathcal{D}}(F_0(A), X)$, 我们有下图来描述其在 $\psi_{A,X} \circ \varphi_{A,X}$ 下的像

$$\begin{array}{ccc}
 F_0(A) & \xrightarrow{u} & X \\
 & \downarrow G_1 & \\
 A & \xrightarrow{\eta_A} G_0(F_0(A)) & \xrightarrow{G_1(u)} G_0(X) \\
 \downarrow F_1 & & \downarrow F_1 \\
 F_0(A) & \xrightarrow{F_1(\eta_A)} F_0(G_0(F_0(A))) & \xrightarrow{F_1(G_1(u))} F_0(G_0(X)) \\
 \searrow \mathbf{1}_{F_0(A)} & \downarrow \epsilon_{F_0(A)} & \downarrow \epsilon_X \\
 & F_0(A) & \xrightarrow{u} X
 \end{array}
 \quad
 \begin{array}{c}
 \in \text{Hom}_{\mathcal{D}}(F_0(A), X) \\
 \downarrow (\eta_A)^* \circ G_1 \\
 \in \text{Hom}_{\mathcal{C}}(A, G_0(X)) \\
 \downarrow F_1 \\
 \in \text{Hom}(F_0(A), F_0(G_0(X))) \\
 \downarrow (\epsilon_X)_* \\
 \in \text{Hom}(F_0(A), X)
 \end{array}$$

其中左下角的 $\mathbf{1}_{F_0(A)}$ 来自于第一个三角等式. 由此, 对任意 $u \in \text{Hom}_{\mathcal{D}}(F_0(A), X)$, 都有

$$(\psi_{A,X} \circ \varphi_{A,X})(u) = u,$$

即

$$\psi_{A,X} \circ \varphi_{A,X} = \text{id}_{\text{Hom}_{\mathcal{D}}(F_0(A), X)}.$$

类似地, 任取 $f \in \text{Hom}_{\mathcal{C}}(A, G_0(X))$, 我们有下图来描述其在 $\varphi_{A,X} \circ \psi_{A,X}$ 下的像

$$\begin{array}{ccc}
 A & \xrightarrow{f} & G_0(X) \\
 \downarrow F_1 & & \\
 F_0(A) & \xrightarrow{F_1(f)} F_0(G_0(X)) & \xrightarrow{\epsilon_X} X \\
 \downarrow G_1 & \downarrow F_0 & \downarrow G_1 \\
 G_0(F_0(A)) & \xrightarrow{G_1(F_1(f))} G_0(F_0(G_0(X))) & \xrightarrow{G_1(\epsilon_X)} G_0(X) \\
 \uparrow \eta_A & \uparrow \eta_A & \nearrow \mathbf{1}_{G_0(X)} \\
 A & \xrightarrow{f} & G_0(X)
 \end{array}
 \quad
 \begin{array}{c}
 \in \text{Hom}_{\mathcal{C}}(G_0(F_0(A)), G_0(X)) \\
 \downarrow (\epsilon_X)_* \circ F_1 \\
 \in \text{Hom}_{\mathcal{C}}(F_0(A), X) \\
 \downarrow G_1 \\
 \in \text{Hom}(G_0(F_0(A)), G_0(X)) \\
 \downarrow (\eta_A)_* \\
 \in \text{Hom}(A, G_0(X))
 \end{array}$$

其中右下角的 $\mathbf{1}_{G_0(X)}$ 来自于第二个三角等式. 由此, 对任意 $f \in \text{Hom}_{\mathcal{D}}(A, G_0(X))$, 都有

$$(\varphi_{A,X} \circ \psi_{A,X})(f) = f,$$

即

$$\varphi_{A,X} \circ \psi_{A,X} = \text{id}_{\text{Hom}_{\mathcal{C}}(A, G_0(X))}.$$

综上所述, 映射 $\varphi_{A,X}$ 为一个双射. 我们还需要验证 $(\varphi_{A,X})_{A \in \text{Ob } \mathcal{C}, X \in \text{Ob } \mathcal{D}}$ 是自然的, 即满足所需要的交换图.

任取 $u \in \text{Hom}_{\mathcal{D}}(F_0(B), X)$, 以及 $\mathcal{C}$ 中态射 $A \xrightarrow{f} B$, 由下图

$$\begin{array}{ccccc} F_0(A) & \xrightarrow{\quad} & F_0(B) & \xrightarrow{\quad} & X \\ & \downarrow & & \downarrow & \\ G_0(F_0(A)) & \xrightarrow{\quad} & G_0(F_0(B)) & \xrightarrow{\quad} & G_0(X) \\ & \uparrow & & \uparrow & \\ A & \xrightarrow{\quad} & B & & \end{array}$$

可知 $\varphi_{A,X}(uF_1(f)) = f\varphi_{B,X}(u)$.

另一方面, 任取 $u \in \text{Hom}_{\mathcal{D}}(F_0(A), X)$ 以及 $\mathcal{D}$ 中的态射 $X \xrightarrow{v} Y$, 由下图可知

$$\begin{array}{ccccccc} F_0(A) & \xrightarrow{\quad u \quad} & X & \xrightarrow{\quad v \quad} & Y \\ & \downarrow G_1 & & \downarrow G_1 & \\ A & \xrightarrow{\eta_A} & G_0(F_0(A)) & \xrightarrow{G_1(u)} & G_0(X) & \xrightarrow{G_1(v)} & G_0(Y) \end{array}$$

可得 $G_1(v)\varphi_{A,X}(u) = \varphi_{B,X}(vu)$.

至此, 我们证明了 (F, G, φ) 构成一个伴随对. 因此 F 为 G 的左伴随. $\square$

注 36.3.4.

以上说明我们也可以使用满足明天中条件的函子 F 与 G 和自然变换 η 与 ϵ 构成的四元组 (F, G, η, ϵ) 来给出一个伴随对. 伴随对 (F, G, η, ϵ) 各部分之间的关系以及三角等式也有可以用以下图表表示:

$$\begin{array}{c} \begin{array}{ccccc} & & \iota_{\mathcal{C}} & & \\ & \nearrow & \Downarrow \eta & \searrow & \\ \mathcal{C} & \xrightarrow{F} & \mathcal{D} & \xrightarrow{G} & \mathcal{C} & \xrightarrow{F} & \mathcal{D} \\ & & \Downarrow \epsilon & & \downarrow \iota_{\mathcal{D}} & & \end{array} \\ = \begin{array}{ccc} \mathcal{C} & \xrightarrow{F} & \mathcal{C} \\ \Downarrow 1_{\mathcal{C}} & & \uparrow F \\ \mathcal{C} & \xrightarrow{F} & \mathcal{C} \end{array} \end{array}$$

和

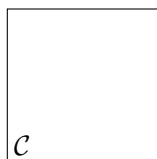
$$\begin{array}{c} \begin{array}{ccccc} & & \iota_{\mathcal{D}} & & \\ & \nearrow & \Downarrow \epsilon & \searrow & \\ \mathcal{D} & \xrightarrow{F} & \mathcal{D} & \xrightarrow{G} & \mathcal{C} & \xrightarrow{F} & \mathcal{D} \\ & & \Downarrow \epsilon & & \downarrow \iota_{\mathcal{D}} & & \end{array} \\ = \begin{array}{ccc} \mathcal{C} & \xrightarrow{F} & \mathcal{C} \\ \Downarrow 1_{\mathcal{C}} & & \uparrow F \\ \mathcal{C} & \xrightarrow{F} & \mathcal{C} \end{array} \end{array}$$

36.4 自然变换的可视化

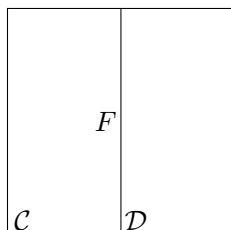
我们也可以使图画对范畴, 函子和自然变换之间的关系进行可视化. 利用这个可视化, 我们可以对伴随对 (F, G, η, ϵ) 中各部分之间关系以及三角等式有更直观的了解.

这个可视化大体的思路是利用平面里的不同区域来代表不同的范畴, 相邻区域之间用可能带节点的不自交的曲线分开, 节点将这条线分成小段, 每一段代表一个这两个区域所代表的两个范畴之间的一个函子, 节点代表一个自然变换. 作为约定, 我们将每个区域也同时看作是该区域对应的范畴到自己的恒等函子, 并将每个函子对应的节点之间的连线也同时看作是函子到自己的恒等自然变换. 通常在阅读图形的时候, 函子的方向是从左到右, 自然变换的方向是从上到下. 所具体的构造如下.

任给一个范畴 $\mathcal{C}$, 我们将其表示为以下区域

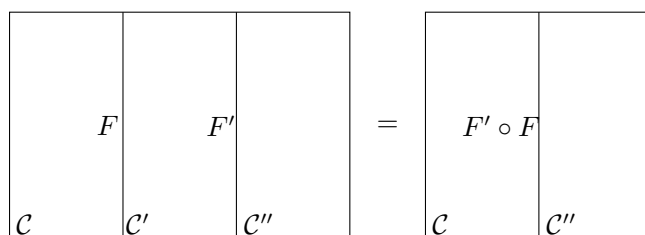


按照我们的约定, 我们也可以将其认作 $\mathcal{C}$ 到 $\mathcal{C}$ 的恒等函子. 任取一个函子 $F : \mathcal{C} \rightarrow \mathcal{D}$, 我们将其表达为

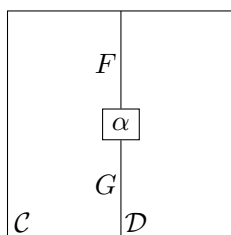


按照约定, 该图也可以表达一个 F 到 F 的恒等自然变换 1_F .

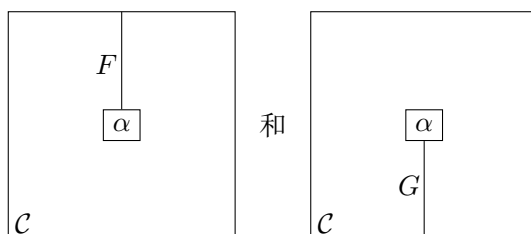
任取两个函子 $F : \mathcal{C} \rightarrow \mathcal{C}'$ 和 $F' : \mathcal{C}' \rightarrow \mathcal{C}''$, 我们可以用下图来表示二者的复合 $F' \circ F$:



任取两个函子 $F : \mathcal{C} \rightarrow \mathcal{D}$ 和 $G : \mathcal{C} \rightarrow \mathcal{D}$, 设二者之间存在自然变换 $\alpha : F \Rightarrow G$, 我们可以用下图表示



设 $\mathcal{D} = \mathcal{C}$, 则 $G = \iota_{\mathcal{C}}$ 的情形和 $F = \iota_{\mathcal{C}}$ 的情形分别对应



任取三个函子 $F : \mathcal{C} \rightarrow \mathcal{D}$, $G : \mathcal{C} \rightarrow \mathcal{D}$ 以及 $H : \mathcal{C} \rightarrow \mathcal{D}$, 设存在自然变换 $\alpha : F \Rightarrow G$ 以及 $\beta : G \Rightarrow H$, 则纵复合 $\beta \circ \alpha$ 的图示如下:

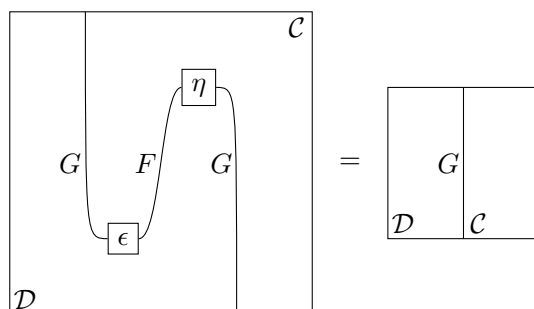
任取三个函子 $F, G : \mathcal{C} \rightarrow \mathcal{C}'$, 和 $F', G' : \mathcal{C}' \rightarrow \mathcal{C}''$, 设存在自然变换 $\alpha : F \Rightarrow G$ 以及 $\alpha' : F' \Rightarrow G'$, 则横复合 $\alpha' * \alpha$ 的图示如下:

任取函子 $F, G, H : \mathcal{C} \rightarrow \mathcal{C}'$, 和 $F', G', H' : \mathcal{C}' \rightarrow \mathcal{C}''$, 设存在自然变换 $\alpha : F \Rightarrow G$ 和 $\beta : G \Rightarrow H$ 以及 $\alpha' : F' \Rightarrow G'$ 和 $\beta' : G' \Rightarrow H'$, 自然变换的横复合和纵复合之间的关系也可以用类似的图来描述:

回到对伴随对的讨论, 我们考虑一个伴随对 (F, G, η, ϵ) , 则得到以下四个图

我们可以将关于 $F \circ G \circ F$ 的三角等式可以表示为以下图的等式:

类似地, 我们可以将关于 $G \circ F \circ G$ 的三角等式可以表示为以下图的等式:



注 36.4.1.

这种将范畴, 函子以及自然变换用图像展示出来的办法可以帮助我们在范畴论的计算中理清头绪. 利用图形进行讨论的合理性来自于函子以及自然变换之间各种复合之间的关系.

我们首先来考虑伴随的复合.

命题 36.4.2

任给伴随对

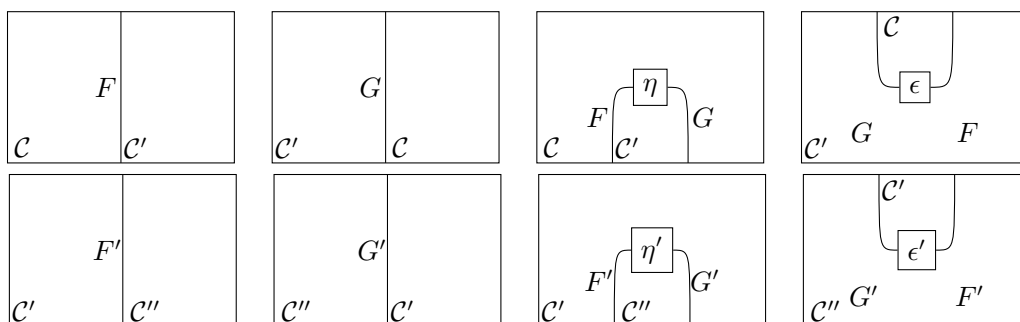
$$\mathcal{C} \xrightleftharpoons[G]{F} \mathcal{C}' \quad \text{和} \quad \mathcal{C}' \xrightleftharpoons[G']{F'} \mathcal{C}'',$$

我们都有伴随对

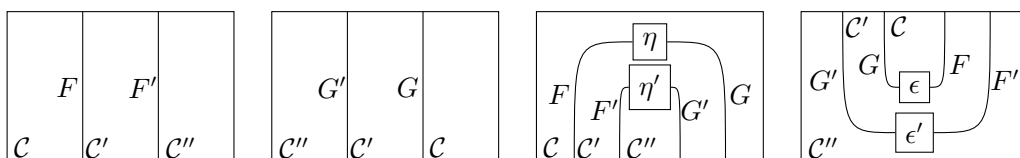
$$\mathcal{C} \xrightleftharpoons[G' \circ G]{F' \circ F} \mathcal{C}''.$$

证明. 我们将以上伴随对记作 (F, G, η, ϵ) 和 $(F', G', \eta', \epsilon')$, 其中 η 和 η' 分别为相应的伴随对的单位, ϵ 和 ϵ' 分别为相应的伴随对的余单位. 下边我们将利用线形图来进行讨论. 严格的证明留作练习.

以上两个伴随对给出以下线形图



将以上图示中标注范畴相同的区域拼接起来, 我们有下图.



注意到左边两个分别代表的是 $F' \circ F$ 和 $G' \circ G$. 我们接着来看第三个图. 考虑水平方向的线依次经过哪些函子, 则有

- 最上方的水平线给出的是函子 $\iota_{\mathcal{C}}$;
- 穿过两个自然变换之间的水平线给出的函子是 $G \circ F$;
- 最下方的函子是 $G \circ G' \circ F' \circ F$.

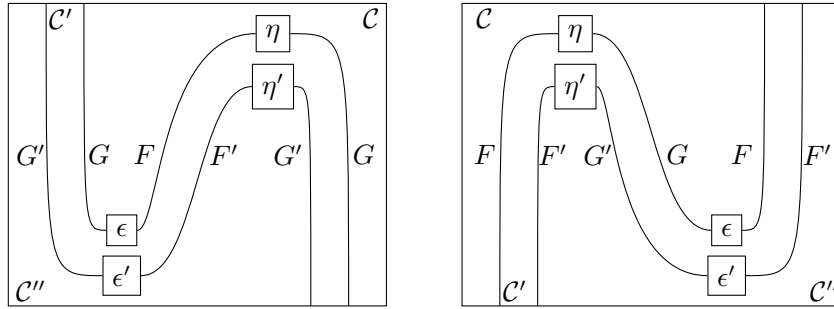
考虑穿过 η 的水平线, 我们有 η 给出 $\iota_{\mathcal{C}}$ 到 $G \circ F$ 的自然变换 (由条件给出). 考虑穿过 η' 的水平线, 我们有 $G\eta'F$ 给出 $G \circ F$ 到 $G \circ G' \circ F' \circ F$ 的自然变换 (通过自然变换与函子的复合得到). 考虑自然变换的纵合成, 我们有

$$\tilde{\eta} := (G\eta'F) \circ \eta,$$

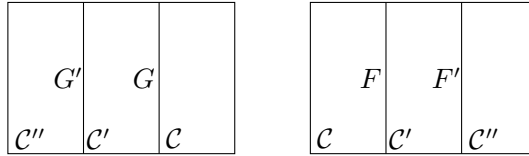
是一个从 $\iota_{\mathcal{C}}$ 到 $(G \circ G') \circ (F' \circ F)$ 的自然变换. 我们对最后一个图做类似地讨论可知

$$\tilde{\epsilon} := \epsilon' \circ (F'\epsilon G')$$

是一个 $\iota_{\mathcal{C}'}$ 到 $(F' \circ F) \circ (G \circ G')$ 的自然变换. 最后我们来验证三角等式. 将之前的各图拼接起来, 我们可以得到



由于 (F, G, η, ϵ) 和 $(F', G', \eta', \epsilon')$ 都是伴随对, 我们可以将这些曲线拉直得到下图



由此可得三角等式

$$\begin{aligned} ((F \circ F') \cdot \tilde{\epsilon}) \circ (\tilde{\eta} \cdot (G \circ G')) &= \mathbf{1}_{G \circ G'}. \\ (\tilde{\epsilon} \cdot (G \circ G')) \circ ((F' \circ F) \cdot \tilde{\eta}) &= \mathbf{1}_{F' \circ F}. \end{aligned}$$

因此 $F \circ F'$ 是 $G' \circ G$ 的左伴随, 单位和余单位分别为 $\tilde{\eta} = (G\eta'F) \circ \eta$ 和 $\tilde{\epsilon} = \epsilon' \circ (F'\epsilon G')$ $\square$

回顾范畴等价的定义, 我们发现其与伴随使用单位和余单位的描述相似. 记 $\mathcal{C}$ 和 $\mathcal{D}$ 为两个等价范畴. 因此存在函子 $F: \mathcal{C} \rightarrow \mathcal{D}$ 和 $G: \mathcal{D} \rightarrow \mathcal{C}$ 满足 $G \circ F \cong \iota_{\mathcal{C}}$ 和 $F \circ G \cong \iota_{\mathcal{D}}$, 即存在自然同构

$$\eta: \iota_{\mathcal{C}} \Rightarrow G \circ F \quad \text{和} \quad \epsilon: F \circ G \Rightarrow \iota_{\mathcal{D}}.$$

因此此时函子对 (F, G) 有自然的单位和余单位. 但是我们不能直接用 (F, G, η, ϵ) 来说明 F 是 G 的左伴随, 这是由于 η 和 ϵ 并不一定满足三角等式. 当然我们知道此时的函子 F 确实为 G 的左伴随, 并且 G 也是 F 的左伴随, 因此一个自然的问题就是此时的 η 和 ϵ 距离与 F 和 G 一起构成一个伴随对还差多远. 为方便讨论, 我们称以上得到的 (F, G, η, ϵ) 为一个同构对.

命题 36.4.3

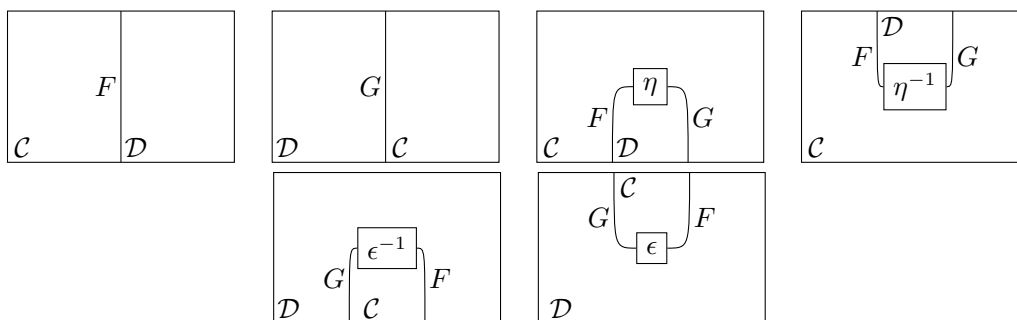
若函子 F 和 G 与自然变换 η 和 ϵ 构成同构对 (F, G, η, ϵ) , 则存在一个自然变换

$$\epsilon' : F \circ G \Rightarrow \text{id}_{\mathcal{D}},$$

使得 (F, G, η, ϵ') 构成伴随对, 且 ϵ' 是唯一的.

证明. 我们仍使用线形图来进行讨论.

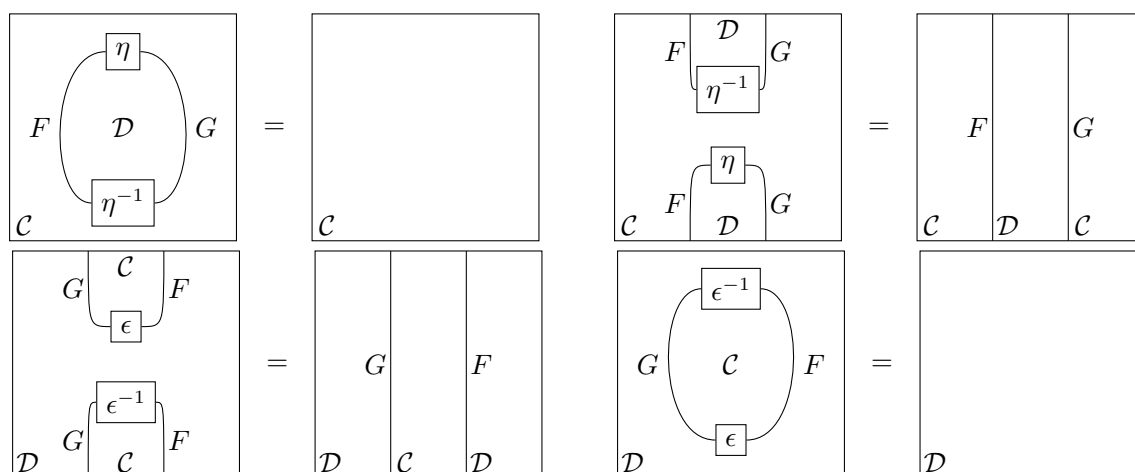
注意到 η 和 ϵ 均为自然同构, 将它们的逆分别记作 η^{-1} 和 ϵ^{-1} . 我们有以下线形图



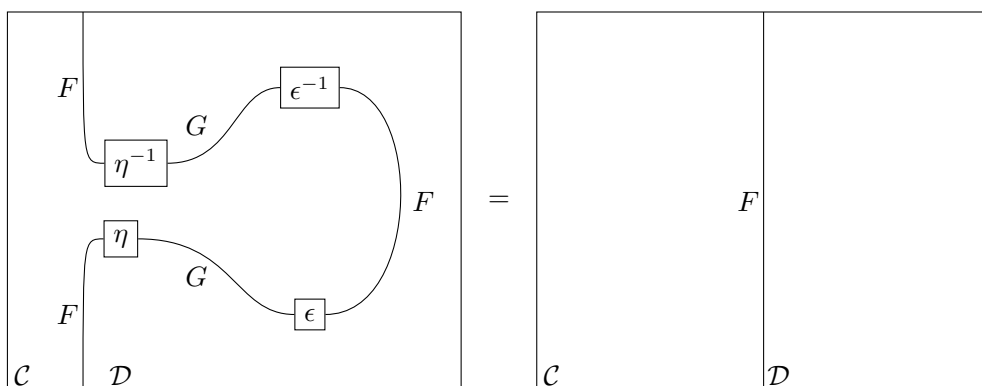
考虑自然变换 η 和 ϵ 与它们的逆的关系, 我们有

$$\begin{aligned}\eta^{-1} \circ \eta &= \mathbf{1}_{\text{id}_{\mathcal{C}}}, \\ \eta \circ \eta^{-1} &= \mathbf{1}_{G \circ F}, \\ \epsilon^{-1} \circ \epsilon &= \mathbf{1}_{F \circ G}, \\ \epsilon \circ \epsilon^{-1} &= \mathbf{1}_{\text{id}_{\mathcal{D}}}.\end{aligned}$$

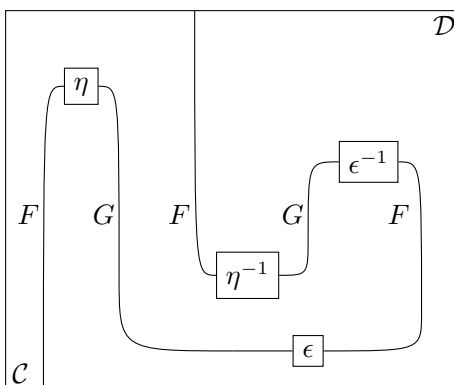
这些等式可以用以下图的等式表示:



因此考虑自然变换的纵复合与横复合之间的关系, 我们有以下图的等式



利用自然变换的纵复合和横复合之间的关系, 我们可以将上图调整为下图



我们考虑不同高度的水平线, 图中 η 右边的线从上到下代表的是以下一系列的函子以及之间的自然变换

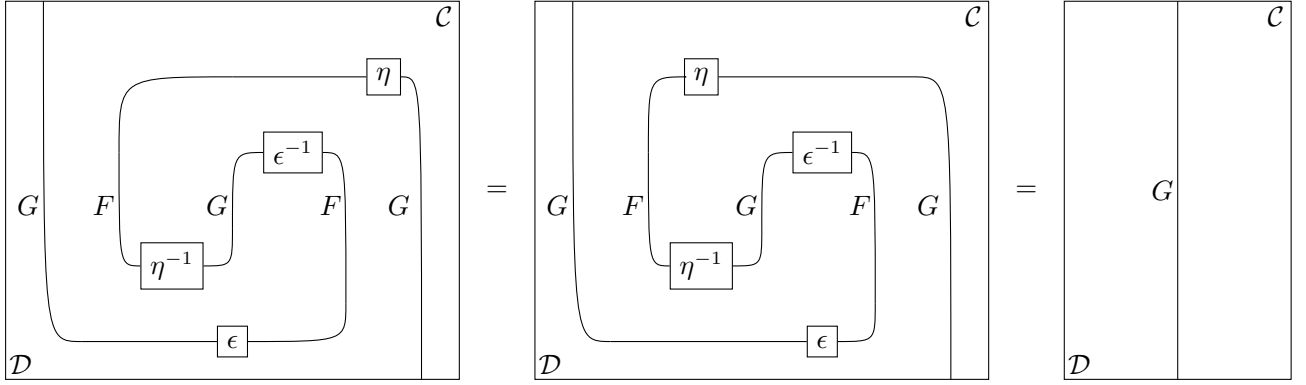
$$\begin{aligned}
 F \circ G &= \iota_{\mathcal{D}} \circ F \circ G \\
 &\downarrow \epsilon^{-1} \cdot (F \circ G) \\
 F \circ G \circ F \circ G & \\
 &\downarrow F \cdot \eta^{-1} \cdot G \\
 F \circ \iota_{\mathcal{C}} \circ G &= F \circ G \\
 &\downarrow \epsilon \\
 &\iota_{\mathcal{D}}
 \end{aligned}$$

因此, 我们记

$$\epsilon' = \epsilon \circ (F \cdot \eta^{-1} \cdot G) \circ (\epsilon^{-1} \cdot (F \circ G)),$$

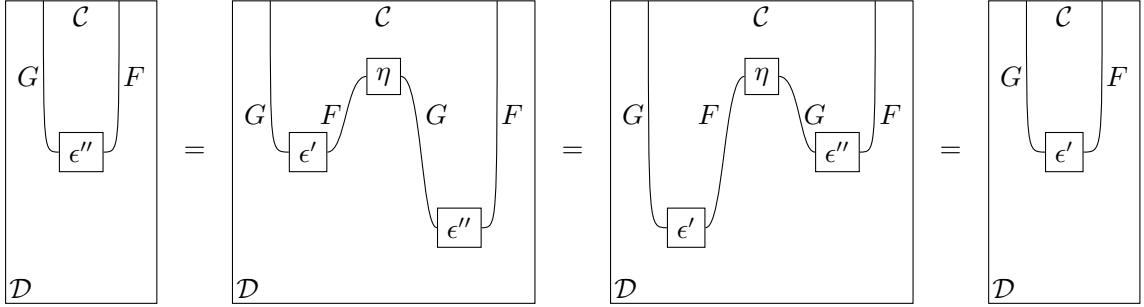
即满足三角等式 $(\epsilon' \cdot F) \circ (F \cdot \eta) = \mathbf{1}_F$.

类似地, 关于 $G \circ F \circ G$ 的三角等式 $(G \cdot \epsilon') \circ (\eta \cdot G) = \mathbf{1}_G$ 可以由下边的图之间的等式得到, 具体的证明过程留作练习.



综上所述, 我们得到 (F, G, η, ϵ') 构成一个伴随对.

下证 ϵ' 是唯一的. 记自然变换 $\epsilon'' : F \circ G \Rightarrow \text{id}_{\mathcal{D}}$ 也与 F, G 和 η 一起构成一个伴随对 (F, G, η, ϵ'') , 下边的图的等式告诉我们 $\epsilon'' = \epsilon'$:



这仍考虑不同高度的水平线给出的函子和自然变换, 以上所表达的等如下

$$\begin{aligned}
 \epsilon'' &= \epsilon'' \circ \mathbf{1}_{F \circ G} = \epsilon'' \circ (F \cdot \mathbf{1}_G) \\
 &= \epsilon'' \circ (F \cdot ((G \cdot \epsilon') \circ (\eta \cdot G))) = \epsilon'' \circ ((F \circ G) \cdot \epsilon') \circ (F \cdot \eta \cdot G) \\
 &= \epsilon' \circ (\epsilon'' \cdot (F \circ G)) \circ (F \cdot \eta \cdot G) = \epsilon' \circ (((\epsilon'' \cdot F) \circ (F \cdot \eta)) \cdot G) \\
 &= \epsilon' \circ (\mathbf{1}_F \cdot G) = \epsilon' \circ \mathbf{1}_{F \circ G} = \epsilon'
 \end{aligned}$$

这其中从第一行和第二行之间的等号是关于利用三角等式

$$(G \cdot \epsilon') \circ (\eta \cdot G) = \mathbf{1}_G$$

给出的前两幅图的相等, 第二行和第三行之间的等号是关于利用 $F \circ G \circ F \circ G$ 到 $\text{id}_{\mathcal{D}}$ 的自然变换

$$\epsilon'' \circ ((F \circ G) \cdot \epsilon') = \epsilon'' * \epsilon' = \epsilon' \circ (\epsilon'' \cdot (F \circ G))$$

给出的中间两幅图之间的相等, 第三行和第四行之间等号是关于利用三角等式

$$(\epsilon'' \cdot F) \circ (F \cdot \eta) = \mathbf{1}_F$$

给出的最后两副图之间的相等. □

注 36.4.4.

类似地, 我们也有自然变换唯一的自然变换 $\eta' : \text{id}_{\mathcal{C}} \Rightarrow G \circ F$, 满足 (F, G, η', ϵ) 构成一个伴随对. 此外, 证明过程也说明由此得到得自然变换 ϵ' 和 η' 均为自然同构. 我们进而有 $(G, F, \epsilon'^{-1}, \eta'^{-1})$ 和 $(G, F, \epsilon'^{-1}, \eta'^{-1})$ 也均为伴随对.

第三十七章 泛性质

回顾之前对遗忘函子和自由函子之间的伴随的讨论中,自由函子的构造来自于线性空间(或者更一般的自由模的泛性质).类似的性质我们在对其它代数结构的讨论中也有涉及.一般地讲,当我们考虑用生成元来描述一个代数结构的时候,不可避免的需要讨论生成元之间的关于所涉及的运算的关系.如果生成元之间除了一些必要的关系外,不存在其它的关系,我们称该代数结构是由这些生成元自由生成的.自由生成的代数结构具有泛性质,即如果代数结构 A 是由集合 S 自由生成的,则任取一个同类型的代数结构 B ,任意一个从集合 S 到集合 B 的映射都可以延拓为代数结构 A 到代数结构 B 的同态.

本章我们从范畴的角度来对泛性质做一些讨论.

37.1 泛性质

我们首先通过一些例子来获得一些对泛性质初步的介绍.

例 37.1.1.

记 $A = \{a\}$ 为一个单点集.任取一个集合 B ,我们都有唯一的一个从 B 到 A 的映射.

这里的结论包含了映射的存在性和唯一性两个部分.另一方面,如果我们希望一个集合 X 满足这个性质,这个集合 X 虽然不一定是 A ,但一定是一个单点集.这是由于,如果 X 为空集,非空集合不存在到空集的映射;如果 X 包含至少两个元素,任给集合 B 我们都可以定义 B 到 X 的映射,但是这样的映射不是唯一的.

类似地,我们也可以考虑空集 $\emptyset$.在之前的讨论中,我们知道任给集合 B ,都存在一个从空集 $\emptyset$ 到 B 的映射,并且这样的映射是唯一的.同时,这个性质实际上也刻画了空集.注意到只有空集可以有到空集的映射.

在以上例子中,我们使用了类似于"存在唯一的...满足..."的叙述.这样的性质通常被称为**泛性质**.以上例子告诉我们单点集和空集具有某种泛性质.另一方面,在以上讨论中,我们也观察到在所有集合中,满足以上泛性质的集合似乎(在相差一个双射的意义下)是唯一的,即以上两个泛性质也可以反过来在同构意义下分别刻画单点集和空集.这些现象在以下例子中也有反应.

例 37.1.2.

记 $n \in \mathbb{N}^*$.我们考虑实数域 $\mathbb{R}$ 上的线性空间 $\mathbb{R}^n$,并记 $(u_1, \dots, u_n)$ 为 $\mathbb{R}^n$ 的一组基.线性空间 $\mathbb{R}^n$ 具有以下泛性质:任取一个 $\mathbb{R}$ -线性空间 V ,以及向量 $v_1, \dots, v_n \in V$,则存在唯一的一个线性映射

$$\varphi: \mathbb{R}^n \rightarrow V,$$

满足 $\varphi(u_1) = v_1, \dots, \varphi(u_n) = v_n$.反过来,任何具有以上性质的 $\mathbb{R}$ -线性空间必然是一个 n 维 $\mathbb{R}$ -线性空间,即与 $\mathbb{R}^n$ 线性同构.

我们也可以考虑 0 维 $\mathbb{R}$ -线性空间 $\mathbf{0}$.该线性空间满足以下两个泛性质:

- 任取 $\mathbb{R}$ -线性空间 V , 存在唯一的一个 $\mathbf{O}$ 到 V 的线性映射;
- 任取 $\mathbb{R}$ -线性空间 V , 存在唯一的一个 V 到 $\mathbf{O}$ 的线性映射.

注意到以上任意一个性质都可以反过来刻画 0 维 $\mathbb{R}$ -线性空间.

37.2 起点对象与终点对象

为了从范畴的角度来对泛性质进行讨论, 我们引入起点对象和终点对象的概念.

定义 37.2.1

记 $\mathcal{C}$ 为一个范畴, 我们称对象 $I \in \text{Ob } \mathcal{C}$ 为一个**起点对象**, 若其满足任取对象 $A \in \text{Ob } \mathcal{C}$, 都存在唯一的一个从 I 到 A 的态射 $I \rightarrow A$.

定义 37.2.2

记 $\mathcal{C}$ 为一个范畴, 我们称对象 $T \in \text{Ob } \mathcal{C}$ 为一个**终点对象**, 若其满足任取对象 $A \in \text{Ob } \mathcal{C}$, 都存在唯一的一个从 A 到 T 的态射 $A \rightarrow T$.

之前讨论的例子告诉我们

- 1) 空集 $\emptyset$ 是集合范畴 **Set** 的起点对象; 而任意单点集是 **Set** 的终点对象;
- 2) 域 $\mathbb{R}$ 上的零维线性空间 $\mathbf{O}$ 是 $\mathbb{R}$ -线性空间范畴 $\mathbf{Vect}_{\mathbb{R}}$ 的起点对象和终点对象.

我们首先来看一些其它的例子, 具体的验证过程留作练习.

例 37.2.3. 1) 空拓扑空间 $\emptyset$ 是拓扑空间范畴 **Top** 的起点对象; 而任意单点拓扑空间是 **Top** 的终点对象;

2) 任意单点拓扑空间是非空拓扑空间范畴 **Top*** 的终点对象, 而 **Top*** 没有起点对象;

3) 平凡群 $\{e\}$ 同时是群范畴 **Group** 的起点对象和终点对象;

4) 零环同时是环范畴 **Ring** 的起点对象和终点对象.

注 37.2.4.

在以上例子中, 我们注意到在有的范畴里, 一个对象可以同时是起点对象和终点对象. 此时我们称其为**零对象**.

实际上并不是所有的范畴都是既有起点对象也有终点对象. 我们来看以下几个例子.

例 37.2.5. 1) 群 G 对应的群胚范畴 **BG** 中只有一个对象 G . 当 G 中有至少两个元素时, 对象 G 既不是起点对象也不是终点对象;

2) 考虑域范畴 **Field**. 任意域同态都是单射. 任给一个域 F , 我们总是可以通过超越扩张的方式得到一个势严格更大的域 F' . 因此 **Field** 中没有终点对象. 另一方面, 由于到素域的域同态只能从一个特征相同的素域出发, 因此 **Field** 中没有起点对象;

3) 考虑特征为 0 的域构成的范畴 $\mathbf{Field}_0$. 素域 $\mathbb{Q}$ 为一个起点对象. 类似地, 特征为素数 p 的域构成的范畴 $\mathbf{Field}_p$ 中, 素域 $\mathbb{F}_p$ 为一个起点对象.

注 37.2.6.

我们注意到起点对象和终点对象是一组对偶的概念. 记 $\mathcal{C}$ 为一个范畴, 对象 A 为 $\mathcal{C}$ 的起点对象当且仅当 A 为 $\mathcal{C}^{\text{op}}$ 的终点对象. 利用对偶原理, 任意对起点对象成立的结论都有一个对偶结论对终点对象成立, 反之亦然.

在之前的例子中, 我们注意到一个范畴中可能存在不同的起点对象.

命题 37.2.7

记 $\mathcal{C}$ 为一个范畴. 若 I 和 I' 均为 $\mathcal{C}$ 中的起点对象, 则 I 和 I' 同构.

证明. 由于 I 和 I' 都是 $\mathcal{C}$ 的起点对象, 我们有态射 $I \xrightarrow{f} I'$ 和态射 $I' \xrightarrow{f'} I$. 考虑态射的复合, 我们有 $I \xrightarrow{f'f} I$, 由于 I 只有一个到 I 的态射 $\mathbf{1}_I$, 因此 $f'f = \mathbf{1}_I$. 类似地, 我们也有 $ff' = \mathbf{1}_{I'}$. 因此 f 和 f' 都是同构, 我们有 I 和 I' 同构. $\square$

利用对偶原理, 我们有与该结论对偶的关于终点对象的结论.

推论 37.2.8

记 $\mathcal{C}$ 为一个范畴. 若 T 和 T' 均为 $\mathcal{C}$ 中的终点对象, 则 T 和 T' 同构.

记 I 为 $\mathcal{C}$ 的一个起点对象, T 为 $\mathcal{C}$ 的一个终点对象. 任取 $\mathcal{C}$ 的对象 A 和 B , 我们有态射 $I \xrightarrow{f} A$, $I \xrightarrow{g} B$, $A \xrightarrow{f'} T$ 和 $B \xrightarrow{g'} T$. 任取 A 到 B 的态射 h , 注意到复合 hf 是一个从 I 到 B 的态射, 由于这样的态射是唯一的, 我们有 $g = hf$, 即以下交换图

$$\begin{array}{ccc} I & \xrightarrow{f} & A \\ & \searrow g & \downarrow h \\ & & B \end{array}$$

类似地, 注意到复合 $g'h$ 是一个从 A 到 T 的态射, 由于这样的态射是唯一的, 我们有 $f' = g'h$, 即以下交换图

$$\begin{array}{ccc} A & \xrightarrow{f'} & T \\ \downarrow h & \nearrow g' & \\ B & & \end{array}$$

我们也可以使用伴随来描述起点对象和终点对象. 我们考虑 $\mathbf{1}$ 范畴, 即只有一个元素记作 e 以及一个态射 $\mathbf{1}_e$. 记 $\mathcal{C}$ 为一个范畴. 我们有唯一的一个函子 $G_{\mathcal{C}} : \mathcal{C} \rightarrow \mathbf{1}$. 若函子 $F : \mathbf{1} \rightarrow \mathcal{C}$ 是 $G_{\mathcal{C}}$ 的左伴随, 则 $F_0(e)$ 为 $\mathcal{C}$ 的起点对象. 要说明这点, 我们记伴随对为 $(F, G_{\mathcal{C}}, \varphi)$. 任取 $A \in \text{Ob } \mathcal{C}$, 我们有双射

$$\varphi_{e,A} : \text{Hom}_{\mathcal{D}}(F_0(e), A) \rightarrow \text{Hom}_{\mathcal{C}}(e, G_0(A)) = \{\mathbf{1}_e\}.$$

因此, 任取 $A \in \text{Ob } \mathcal{C}$, 存在唯一的从 $F_0(e)$ 到 A 的态射, 记 $F_0(e)$ 为起点对象.

注意到 $\mathbf{1}$ 到 $\mathcal{C}$ 的函子与 $\mathcal{C}$ 中的对象之间存在着——对应. 以上结论告诉我们, 若存在某个 $\mathbf{1}$ 到 $\mathcal{C}$ 的函子是 $G_{\mathcal{C}}$ 的左伴随, 则对应的 $\mathcal{C}$ 的对象就是一个起点对象. 反过来, 任取 $\mathcal{C}$

的一个起点对象, 我们也可以得到 G_C 的一个左伴随. 由此可知 G_C 的左伴随函子和 C 中的起点对象之间存在一一对应. 利用对偶原理, 我们也有 G_C 的右伴随函子和 C 中的终点对象之间存在一一对应.

37.3 逗号范畴

在之前讨论泛性质的时候, 我们注意到 $\mathbb{R}^n$ ($n \in \mathbb{N}^*$) 也具有某种泛性质. 不过为了描述这类泛性质, 我们需要首先确定 $\mathbb{R}^n$ 的一组基 S , 泛性质继而可以用以下交换图来表示:

$$\begin{array}{ccc} S & \xrightarrow{j} & \mathbb{R}^n \\ & \searrow f & \downarrow \exists! L_f \\ & & V \end{array}$$

其中 j 为 S 到 $\mathbb{R}^n$ 的嵌入映射, V 为一个 $\mathbb{R}$ -线性空间, f 为一个 S 到 V 的映射. 线性空间 $\mathbb{R}^n$ 的泛性质保证了线性映射 L_f 的存在性和唯一性.

更一般的, 我们可以将 $\mathbb{R}^n$ 等同于 S 在自由函子下的像, 利用集合范畴 **Set** 和 $\mathbb{R}$ -线性空间范畴 $\mathbf{Vect}_{\mathbb{R}}$ 之间的自由函子 F 和遗忘函子 U 来在 **Set** 中重新表述上图:

$$\begin{array}{ccc} S & \xrightarrow{j} & U(F(S)) \\ & \searrow f & \downarrow \exists! U_0(L_f) \\ & & U(V) \end{array}$$

我们考虑的泛性质实际上是在固定 S (因此也固定了 $U(F(S))$ 和 j) 之后, 任给 f , 都存在一个唯一的 $U_0(L_f)$. 为了方便讨论, 我们引入逗号范畴.

定义 37.3.1

任取范畴 $\mathcal{C}$, $\mathcal{C}'$ 和 $\mathcal{C}''$ 以及函子 F 和 F' 满足

$$\begin{array}{ccc} & \mathcal{C}' & \\ & \downarrow F' & \\ \mathcal{C} & \xrightarrow{F} & \mathcal{C}'' \end{array}$$

逗号范畴 (记作 $(F \Rightarrow F')$ 或 $F \downarrow F'$) 定义如下:

- 其中的对象为如下形式的三元组 (A, f'', A') , 满足 $A \in \text{Ob } \mathcal{C}$, $A' \in \text{Ob } \mathcal{C}'$, 以及 $f'' \in \text{Hom}_{\mathcal{C}''}(F_0(A), F'_0(A'))$;
- 任取两个对象 (A, f'', A') 和 (B, g'', B') , 一个从 (A, f'', A') 到 (B, g'', B') 的态射为一个二元组 (h, h') 其中 $h \in \text{Hom}_{\mathcal{C}}(A, B)$, $h' \in \text{Hom}_{\mathcal{C}'}(A', B')$, 满足

$$\begin{array}{ccc} F(A) & \xrightarrow{f''} & F'(A') \\ \downarrow F_1(h) & & \downarrow F'_1(h') \\ F(B) & \xrightarrow{g''} & F'(B') \end{array} \quad ;$$

- 对象 (A, f'', A') 的恒等态射为 $(1_A, 1_{A'})$;
- 态射 (h_1, h'_1) 和 (h_2, h'_2) 的复合为

$$(h_1, h'_1)(h_2, h'_2) = (h_1 h_2, h'_1 h'_2).$$

注 37.3.2.

最初人们使用记号 (F, F') 来记此类范畴, 因此称之为逗号范畴, 并将该称呼保留至今.

我们回到之前的例子. 令 $\mathcal{C} = \mathbf{1}$, $\mathcal{C}' = \mathbf{Vect}_{\mathbb{R}}$ 且 $\mathcal{C}'' = \mathbf{Set}$. 任意 $\mathbf{1}$ 到 $\mathbf{Set}$ 的函子 F 都由 $F_0(e) \in \text{Ob } \mathbf{Set}$ 决定. 因此我们用 $\text{Ob } \mathbf{Set}$ 来记 $\mathbf{1}$ 到 $\mathbf{Set}$ 的函子. 仍用 U 记 $\mathbf{Vect}_{\mathbb{R}}$ 到 $\mathbf{Set}$ 的遗忘函子, 我们考虑逗号范畴 $(S \Rightarrow U)$.

$$\begin{array}{ccc} & \mathbf{Vect}_{\mathbb{R}} & \\ & \downarrow U & \\ \mathbf{1} & \xrightarrow{S} & \mathbf{Set} \end{array}$$

考虑其中的对象 $(S, j, U(F(S)))$. 向量空间 $F(S)$ 的泛性质等价于 $(S, j, U(F(S)))$ 为 $(S \Rightarrow U)$ 的起点对象.

考虑之前的讨论, 我们发现起点元素可以和函子的左伴随以及逗号范畴联系起来. 我们首先给出以下结论.

命题 37.3.3

设存在函子的伴随 $\mathcal{C} \xrightleftharpoons[F]{G} \mathcal{D}$, 并记伴随对为 (F, G, η, ϵ) . 任取 $A \in \text{Ob } \mathcal{C}$, 态射 η_A 所对应的逗号范畴 $(A \Rightarrow G)$ 的对象 $(e, \eta_A, F_0(A))$ 为一个起点对象.

证明. 我们考虑

$$\begin{array}{ccc} & & \mathcal{D} \\ & & \downarrow G \\ 1 & \xrightarrow{A} & \mathcal{C} \end{array}$$

给出的逗号范畴 $(A \Rightarrow G)$, 并考虑其中的对象 $(e, \eta_A, F_0(A))$. 任取 $X \in \text{Ob } \mathcal{D}$, 考虑对象 (e, f, X) , 其中

$$f: A \rightarrow G(X).$$

若存在从 $(e, \eta_A, F_0(A))$ 到 (e, f, X) 的态射, 则存在态射 $F_0(A) \xrightarrow{u} X$, 满足

$$\begin{array}{ccc} A & \xrightarrow{\eta_A} & G_0(F_0(A)) \\ \downarrow 1_A & & \downarrow G_1(u) \\ A & \xrightarrow{f} & G_0(X) \end{array}$$

考虑命题的证明. 我们使用相同的记号可知态射 $u = \psi_{A,X}(f) = \epsilon_X \circ u$ 满足以上交换图. 另一方面, 任取 $F_0(A) \xrightarrow{v} X$, 使得 $G_1(v)$ 满足以上交换图, 则有 $\varphi_{A,X}(v) = f$. 因此我们有

$$v = \psi_{A,X}(\varphi_{A,X}(v)) = \psi_{A,X}(f) = u.$$

因此满足条件的态射 $F_0(A) \xrightarrow{u} X$ 是唯一的. 由此可知 $(e, \eta_A, F_0(A))$ 为逗号范畴 $(A \Rightarrow G)$ 的一个起点对象. $\square$

实际上, 我们可以使用逗号范畴的起点元素来给函子的左伴随另一个等价的描述.

定理 37.3.4

设存在函子 $\mathcal{C} \xrightleftharpoons[F]{G} \mathcal{D}$, 则以下两个叙述等价:

1. 函子 F 为函子 G 的左伴随;
2. 存在一个自然变换 $\eta: \iota_{\mathcal{C}} \Rightarrow G \circ F$, 满足任取 $A \in \text{Ob } \mathcal{C}$, 态射 η_A 所对应的逗号范畴 $(A \Rightarrow G)$ 的对象 $(e, \eta_A, F_0(A))$ 为一个起点对象.

证明. 之前的命题已经给出了一个方向 $(1. \Rightarrow 2.)$ 的证明. 下边我们来证明另一个方向. $\square$

推论 37.3.5

一个函子 $G: \mathcal{D} \rightarrow \mathcal{C}$ 有一个左伴随函子当且仅当任取 $A \in \mathcal{C}$, 逗号范畴 $(A \Rightarrow G)$ 中有一个起点对象.

注 37.3.6.

以上推论可以帮助我们构造更多伴随函子的例子. 此外以上推论也告诉我们函子的伴随和相关范畴中存在满足某种泛性质的对象紧密相关.

注 37.3.7.

利用对偶原理, 我们可以证明 F 为 G 的左伴随, 当且仅当存在一个自然变换 $\epsilon: F \circ G \Rightarrow \text{id}_{\mathcal{D}}$, 满足任取 $X \in \text{Ob } \mathcal{D}$, 都有 $(G_0(X), \epsilon_X, e)$ 为逗号范畴 $(F \Rightarrow X)$ 的一个终点对象. 因此我们进一步可得, 一个函子 F 具有右伴随函子当且仅当任取 $X \in \text{Ob } \mathcal{D}$, 逗号范畴 $(F \Rightarrow X)$ 都有一个终点对象.

第三十八章 函子的可表性

我们考虑非空集合范畴 **Set**. 我们记 A 为一个单点集. 当我们任取一个对象 $B \in \text{Ob } \mathbf{Set}$, 其所对应的集合 $\text{Hom}(A, B)$ 由所有 A 到 B 的映射构成. 注意到每一个这样的映射实际上对应的是 B 的一个元素, 我们可以将 $\text{Hom}(A, B)$ 理解为集合 B 自己. 笼统地说, 从 A 看 B , 我们实际上看到的是 B 的元素.

我们考虑群范畴 **Group**, 并考虑其中的无限循环群 $\mathbb{Z}$. 根据之前的讨论, 其作为一个元素生成的自由群的泛性质可以用逗号范畴来描述. 任给一个群 G , 我们总有 $\mathbb{Z}$ 到 G 的群同态. 每一个群同态

$$\varphi: \mathbb{Z} \rightarrow G,$$

都是由 1 的像 $\varphi(1) = g$ 决定的. 因此当我们从 $\mathbb{Z}$ 看 G 的时候, 即考虑 $\text{Hom}(\mathbb{Z}, G)$ 中的态射, 我们理解为是在描述 G 的元素. 类似地, 我们也可以考虑任意一个素数 p , 并考虑所有从 p 阶循环群 $\mathbb{Z}_p$ 到 G 的态射. 而这等同于在描述 G 中的 1 阶和 p 阶元素.

这些例子告诉我们, 如果我们清楚了一个对象的性质, 当我们考虑从该对象看其它对象的时候, 我们实际上也是在描述目标对象的某些信息. 对这部分的研究涉及我们下边将要介绍的可表函子的概念. 为避免一些集合论中的问题, 我们约定本节仅讨论局部小范畴. 类似地构造可以推广到更一般的情况, 但这需要推广集合的概念.

38.1 可表函子

记 $\mathcal{C}$ 为一个局部小范畴, 我们考虑之前定义的 Hom-函子

$$\text{Hom}: \mathcal{C}^{\text{op}} \times \mathcal{C} \rightarrow \mathbf{Set}.$$

任取对象 $A \in \text{Ob } \mathcal{C}$, 通过在考虑从 A 出发的态射, 我们有函子 $\text{Hom}(A, -): \mathcal{C} \rightarrow \mathbf{Set}$.

定义 38.1.1

我们称一个函子 $F: \mathcal{C} \rightarrow \mathbf{Set}$ 是**可表的**, 如果存在 $A \in \text{Ob } \mathcal{C}$, 满足

$$F \cong \text{Hom}(A, -).$$

此时, 我们称 $\text{Hom}(A, -)$ 为 F 的一个**表示**.

注 38.1.2.

当然作为平凡的例子, 每一个函子 $\text{Hom}(A, -)$ 都是可表的.

我们考虑本节开始介绍的几个例子

例 38.1.3.

考虑非空集合范畴 $\mathbf{Set}^*$. 取 A 为一个单点集, 并考虑函子 $\mathrm{Hom}(A, -)$. 任取 $B \in \mathrm{Ob} \mathbf{Set}$, 我们有

$$\mathrm{Hom}(A, B) \cong B,$$

并且这种同构关于 B 是自然的. 因此 $\mathrm{Hom}(A, -) \cong \iota_{\mathbf{Set}}$. 由此可知函子 $\iota_{\mathbf{Set}}$ 是可表的.

例 38.1.4.

考虑群范畴 $\mathbf{Group}$, 以及遗忘函子 $U : \mathbf{Group} \rightarrow \mathbf{Set}$. 考虑无限循环群 $\mathbb{Z}$, 之前的讨论告诉我们

$$\mathrm{Hom}(\mathbb{Z}, G) \cong U_0(G).$$

同时这种同构关于 G 是自然的. 因此 $\mathrm{Hom}(\mathbb{Z}, -) \cong U$. 由此可知遗忘函子 U 是可表的.

我们考虑之前提到的

命题 38.1.5

考虑伴随函子 $\mathcal{C} \xrightleftharpoons[G]{F} \mathcal{D}$. 设 $\mathcal{C}$ 和 $\mathcal{D}$ 都是局部小范畴. 任取 $A \in \mathrm{Ob} \mathcal{A}$, 函子

$$\mathrm{Hom}_{\mathcal{C}}(A, G(-)) : \mathcal{D} \rightarrow \mathbf{Set},$$

可表.

证明. 由于 F 为 G 的左伴随, 任取 $X \in \mathrm{Ob} \mathcal{D}$, 我们有自然的双射

$$\mathrm{Hom}_{\mathcal{C}}(A, G(X)) \cong \mathrm{Hom}_{\mathcal{D}}(F(A), X).$$

关于 A 和 X 都是自然的, 因此 $\mathrm{Hom}_{\mathcal{C}}(A, G(-)) \cong \mathrm{Hom}_{\mathcal{D}}(F(A), -)$, 因此是一个可表函子. $\square$

我们也可以考虑以上构造对偶的情形. 记 $\mathcal{C}$ 为一个局部小范畴, 任取对象 $A \in \mathrm{Ob} \mathcal{C}$, 通过考虑到 A 的态射, 我们可以构造函数 $\mathrm{Hom}(-, A) : \mathcal{C}^{\mathrm{op}} \rightarrow \mathbf{Set}$.

定义 38.1.6

我们称一个函子 $F : \mathcal{C}^{\mathrm{op}} \rightarrow \mathbf{Set}$ 是**可表的**, 如果存在 $A \in \mathrm{Ob} \mathcal{C}$, 满足

$$F \cong \mathrm{Hom}(-, A).$$

此时, 我们称 $\mathrm{Hom}(-, A)$ 为 F 的一个**表示**.

注 38.1.7.

当然作为一个平凡的例子, 每一个函子 $\mathrm{Hom}(-, A)$ 都是可表的.

例 38.1.8.

我们考虑集合范畴的反范畴 $\mathbf{Set}^{\mathrm{op}}$. 任给一个集合 B , 我们可以考虑其幂集 $P_0(B)$, 即所有子

集的集合. 任取态射 $B \xrightarrow{f} B' \in \text{Mor } \mathbf{Set}$, 我们考虑

$$\begin{aligned} P_1(f) : P_0(B') &\rightarrow P_0(B), \\ C' &\mapsto f^{-1}(C'). \end{aligned}$$

由此, 我们得到了一个函子 $P : \mathbf{Set}^{\text{op}} \rightarrow \mathbf{Set}$.

注意到任意子集 $C \subset B$ 对应于一个 B 到 $A = \{0, 1\}$ 的映射 χ_C , 满足对任意 $x \in B$, $\chi_C(x) = 1$ 当且仅当 $x \in C$. 由此我们有

$$P_0(B) \cong \text{Hom}(B, A).$$

我们可以进一步验证这个同构关于 B 是自然的, 因此我们有 $P \cong \text{Hom}(-, A)$, 函子 P 是可表的.

考虑 $A \in \text{Ob } \mathcal{C}^{\text{op}}$ 和 $\text{Hom}(A, -) \in \text{Ob } [\mathcal{C}, \mathbf{Set}]$ 的对应关系, 我们可以得到函子

$$\text{Hom}(\bullet, -) : \mathcal{C}^{\text{op}} \rightarrow [\mathcal{C}, \mathbf{Set}];$$

考虑 $A \in \text{Ob } \mathcal{C}$ 和 $\text{Hom}(-, A) \in \text{Ob } [\mathcal{C}^{\text{op}}, \mathbf{Set}]$ 的对应关系, 我们可以得到函子

$$\text{Hom}(-, \bullet) : \mathcal{C} \rightarrow [\mathcal{C}^{\text{op}}, \mathbf{Set}].$$

定义 38.1.9

我们称以上定义的函子 $\text{Hom}(-, \bullet)$ 为 $\mathcal{C}$ 的 *Yoneda 嵌入*.

38.2 Yoneda 引理

记 $\mathcal{C}$ 为一个局部小范畴. 考虑其对应的函子范畴 $[\mathcal{C}^{\text{op}}, \mathbf{Set}]$. 由之前的讨论, 我们知道该范畴中包含一部分由可表函子给出的对象. 我们考虑本节最初的问题, 如果从一个可表函子来看其他的函子, 我们会看到什么? 这就是 Yoneda 引理将要告诉我们的. 注意到由定义任给一个可表函子 $F : \mathcal{C}^{\text{op}} \rightarrow \mathbf{Set}$, 都存在一个对象 $A \in \text{Ob } \mathcal{C}$, 满足 $F \cong \text{Hom}(-, A)$. 因此我们下边将只考虑由形如 $\text{Hom}(-, A)$ 的对象出发的 $[\mathcal{C}^{\text{op}}, \mathbf{Set}]$ 中的态射.

注意到函子范畴中的态射是函子间的自然变换. 记 $A \in \text{Ob } \mathcal{C}$, $X \in \text{Ob } [\mathcal{C}^{\text{op}}, \mathbf{Set}]$. 设 $\alpha : \text{Hom}(-, A) \Rightarrow X$ 为一个自然变换, 记做

$$\begin{array}{ccc} & \text{Hom}(-, A) & \\ \mathcal{C}^{\text{op}} & \begin{array}{c} \xrightarrow{\quad} \\ \Downarrow \alpha \\ \xrightarrow{\quad} \end{array} & \mathbf{Set} \\ & X & \end{array}$$

定理 38.2.1 (Yoneda 引理)

记 $\mathcal{C}$ 为一个局部小范畴. 任取 $A \in \text{Ob } \mathcal{C}$, 以及 $X \in \text{Ob } [\mathcal{C}^{\text{op}}, \mathbf{Set}]$, 都有双射:

$$\text{Hom}_{[\mathcal{C}^{\text{op}}, \mathbf{Set}]}(\text{Hom}(-, A), X) \cong X_0(A),$$

并且该双射关于 A 和 X 是自然的.

考虑对偶的情形, 任取 $A \in \text{Ob } \mathcal{C}^{\text{op}}$, 以及 $Y \in \text{Ob } [\mathcal{C}, \mathbf{Set}]$, 都有双射:

$$\text{Hom}_{[\mathcal{C}, \mathbf{Set}]}(\text{Hom}(A, -), Y) \cong Y_0(A),$$

并且该双射关于 A 和 Y 是自然的.

我们可以先考虑一个平凡的情形.

例 38.2.2.

考虑函子 X 取将所有 $\mathbf{N}$ 的对象都送到 $\emptyset$, 并将所有态射都送到 $\mathbf{1}_{\emptyset}$ 的函子, 则我们有 $X_0(A) = \emptyset$. 因此 $\text{Hom}_{[\mathcal{C}^{\text{op}}, \mathbf{Set}]}(\text{Hom}(-, A), X) = \emptyset$, 即不存在从 $\text{Hom}(-, A)$ 到 X 的自然变换. 这个实际上也可以由直接观察得到. 注意到任取 A , 我们都有 $\text{Hom}(A, A)$ 非空, 但是 $X_0(A) = \emptyset$, 因此不存在 $\text{Hom}(A, A)$ 到 $X_0(A)$ 的映射, 进而说明不存在从 $\text{Hom}(-, A)$ 到 X 的自然变换.

以上所提到的自然的双射也可以表述为两个 $\mathcal{C}^{\text{op}} \times [\mathcal{C}^{\text{op}}, \mathbf{Set}]$ 到 $\mathbf{Set}$ 的函子之间的自然变换. 注意到左边实际上是由

$$(A, X) \longmapsto (\text{Hom}(-, A), X) \longmapsto \text{Hom}_{[\mathcal{C}^{\text{op}}, \mathbf{Set}]}(\text{Hom}(-, A), X)$$

作为对象的映射给出的函子, 而右边则由

$$(A, X) \longmapsto X_0(A)$$

作为对象的映射给出的函子. Yoneda 引理告诉我们以上得到的两个函子之间存在一个自然同构.

Yoneda 引理的证明. 我们只给出第一部分结论的证明. 第二部分结论与第一部分互为对偶结论. 我们将其留作练习.

我们首先来考虑任给 $A \in \text{Ob } \mathcal{C}$, 以及 $X \in \text{Ob } [\mathcal{C}^{\text{op}}, \mathbf{Set}]$, 如何构造一个从 $\text{Hom}_{[\mathcal{C}^{\text{op}}, \mathbf{Set}]}(\text{Hom}(-, A), X)$ 到 $X_0(A)$ 的双射.

注意到任取 $\alpha \in \text{Hom}_{[\mathcal{C}^{\text{op}}, \mathbf{Set}]}(\text{Hom}(-, A), X)$, 我们可以考虑

$$\begin{aligned} \alpha_A : \text{Hom}(A, A) &\rightarrow X_0(A), \\ \mathbf{1}_A &\mapsto \alpha_A(\mathbf{1}_A). \end{aligned}$$

由此, 我们可以定义映射

$$\begin{aligned} \varphi_{A, X} : \text{Hom}_{[\mathcal{C}^{\text{op}}, \mathbf{Set}]}(\text{Hom}(-, A), X) &\rightarrow X_0(A), \\ \alpha &\mapsto \alpha_A(\mathbf{1}_A). \end{aligned}$$

另一方面, 任取 $x \in X_0(A)$, 我们需要构造一个 $\text{Hom}(-, A)$ 到 X 的自然变换, 即任取 $B \in \text{Ob } \mathcal{C}^{\text{op}}$, 构造一个映射

$$\beta_{x, B} : \text{Hom}(B, A) \rightarrow X_0(B),$$

作为态射, 并且 $\beta_x = (\beta_{x,B})_{B \in \text{Ob } \mathcal{C}^{\text{op}}}$ 构成一个自然变换.

任取 B 以及态射 $B \xrightarrow{f} A \in \text{Mor } \mathcal{C}$, 由于 $X : \mathcal{C}^{\text{op}} \rightarrow \mathbf{Set}$ 为一个函子, 我们有映射

$$X_1(f^{\text{op}}) : X_0(A) \rightarrow X_0(B),$$

我们定义

$$\begin{aligned} \beta_{x,B} : \text{Hom}(B, A) &\rightarrow X_0(B), \\ f &\mapsto X_1(f^{\text{op}})(x). \end{aligned}$$

任取态射 $B \xrightarrow{g} C \in \text{Mor } \mathcal{C}$, 我们需要证明以下交换图成立

$$\begin{array}{ccc} \text{Hom}(C, A) & \xrightarrow{g^*} & \text{Hom}(B, A) \\ \beta_{x,C} \downarrow & & \downarrow \beta_{x,B} \\ X_0(C) & \xrightarrow{X_1(g^{\text{op}})} & X_0(B) \end{array}$$

任取态射 $C \xrightarrow{h} A$, 考虑函子 X , 我们有

$$X_1((hg)^{\text{op}})(x) = X_1(g^{\text{op}}h^{\text{op}})(x) = (X_1(g^{\text{op}}) \circ X_1(h^{\text{op}}))(x).$$

由此得到以上交换图, 因此 β_x 为一个自然变换. 由此我们定义

$$\begin{aligned} \psi_{A,X} : X_0(A) &\rightarrow \text{Hom}_{[\mathcal{C}^{\text{op}}, \mathbf{Set}]}(\text{Hom}(-, A), X), \\ x &\mapsto \beta_x. \end{aligned}$$

下证 $\varphi_{A,X} \circ \psi_{A,X}$ 为 $X_0(A)$ 上的恒等映射, 而 $\psi_{A,X} \circ \varphi_{A,X}$ 为 $\text{Hom}_{[\mathcal{C}^{\text{op}}, \mathbf{Set}]}(\text{Hom}(-, A), X)$ 上的恒等映射. 具体过程留作练习.

下边我们来证明以上构造的双射 $\varphi_{A,X}$ 是自然的, 即任取态射 $B \xrightarrow{f} A \in \text{Mor } \mathcal{C}$ 以及 $\alpha : X \Rightarrow Y$, 我们要证明以下交换图成立:

$$\begin{array}{ccccc} \text{Hom}_{[\mathcal{C}^{\text{op}}, \mathbf{Set}]}(\text{Hom}(-, A), X) & \xrightarrow{\circ f_*} & \text{Hom}_{[\mathcal{C}^{\text{op}}, \mathbf{Set}]}(\text{Hom}(-, B), X) & \xrightarrow{\alpha \circ} & \text{Hom}_{[\mathcal{C}^{\text{op}}, \mathbf{Set}]}(\text{Hom}(-, B), Y) \\ \varphi_{A,X} \downarrow & & \varphi_{B,X} \downarrow & & \varphi_{B,Y} \downarrow \\ X_0(A) & \xrightarrow{X_1(f^{\text{op}})} & X_0(B) & \xrightarrow{\alpha_A} & Y_0(B) \end{array}$$

其中 $f_* : \text{Hom}(-, B) \Rightarrow \text{Hom}(-, A)$ 为与 f 复合给出的自然变换, 满足任给 $C \in \text{Ob } \mathcal{C}$, 都有

$$\begin{aligned} f_* : \text{Hom}(C, B) &\rightarrow \text{Hom}(C, A), \\ g &\mapsto fg. \end{aligned}$$

任取 $\beta \in \text{Hom}_{[\mathcal{C}^{\text{op}}, \mathbf{Set}]}(\text{Hom}(-, A), X)$, 我们有

$$\begin{array}{ccccc} \beta & \xrightarrow{\quad} & \beta \circ f_* & \xrightarrow{\quad} & \alpha \circ (\beta \circ f_*) \\ \downarrow & & \downarrow & & \downarrow \\ \beta_A(\mathbf{1}_A) & \xrightarrow{\quad} & (\beta \circ f_*)_B(\mathbf{1}_B) & \xrightarrow{\quad} & (\alpha \circ (\beta \circ f_*))_B(\mathbf{1}_B) \end{array}$$

注意到 $(\beta \circ f_*)_B(\mathbf{1}_B) = \beta_A(f) = X_1(f^{\text{op}})(\beta_A(\mathbf{1}_A))$. 因此左边交换图成立. 右半边可以通过自然变换的纵复合直接验证得到. $\square$

推论 38.2.3

任意局部小范畴 $\mathcal{C}$ 的 Yoneda 嵌入

$$\mathrm{Hom}(-, \bullet) : \mathcal{C} \rightarrow [\mathcal{C}^{\mathrm{op}}, \mathbf{Set}],$$

和

$$\mathrm{Hom}(\bullet, -) : \mathcal{C}^{\mathrm{op}} \rightarrow [\mathcal{C}, \mathbf{Set}],$$

都是完全忠实的.

证明. 利用对偶原理, 我们只需证明第一个函子是完全忠实的即可.

任取 $A, B \in \mathcal{C}$, 由 Yoneda 引理, 借用之前的记号, 我们知道存在双射

$$\psi_{A, \mathrm{Hom}(-, B)} : \mathrm{Hom}(A, B) \rightarrow \mathrm{Hom}_{[\mathcal{C}^{\mathrm{op}}, \mathbf{Set}]}(\mathrm{Hom}(-, A), \mathrm{Hom}(-, B)).$$

由之前的构造知 $\psi_{A, \mathrm{Hom}(-, B)}$ 即为 $\mathrm{Hom}(-, \bullet)_1$. 因此函子 $\mathrm{Hom}(-, \bullet)$ 是完全忠实的. $\square$

以上推论进一步有如下直接的推论.

推论 38.2.4

记 $\mathcal{C}$ 为一个局部小范畴. 任取 $A, B \in \mathrm{Ob} \mathcal{C}$, 以下两个叙述等价:

- 1) $A \cong B$;
- 2) $\mathrm{Hom}(-, A) \cong \mathrm{Hom}(-, B)$;
- 3) $\mathrm{Hom}(A, -) \cong \mathrm{Hom}(B, -)$.

结合之前关于伴随函子的讨论, 我们可以证明一个函子的左伴随函子, 如果存在的话, 在自然同构意义下是唯一的.

推论 38.2.5

记 $\mathcal{C}$ 和 $\mathcal{D}$ 均为局部小范畴. 设函子 $G : \mathcal{D} \rightarrow \mathcal{C}$ 有两个左伴随函子 $F, F' : \mathcal{C} \rightarrow \mathcal{D}$, 则 $F \cong F'$.

证明. 由之前的命题, 任取 $A \in \mathrm{Ob} \mathcal{C}$, 我们有 $\mathrm{Hom}(A, G(-))$ 可表, 且

$$\mathrm{Hom}(F(A), -) \cong \mathrm{Hom}(A, G(-)) \cong \mathrm{Hom}(F'(A), -).$$

利用之前的推论, 我们有 $F(A) \cong F'(A)$ 对任意 A 都成立, 并且这个同构是自然的. 因此 $F \cong F'$. $\square$

38.3 可表性与泛性质

我们也可以将泛性质与函子的可表联系起来. 我们首先给出以下两个互为对偶的结论.

命题 38.3.1

记 $\mathcal{C}$ 为一个局部小范畴. 设函子 $X : \mathcal{C}^{\text{op}} \rightarrow \mathbf{Set}$ 可表, 并记 $\text{Hom}(-, A)$ 为其一个表示. 则存在一个元素 $u \in X_0(A)$, 对任意 $B \in \text{Ob } \mathcal{C}$ 以及 $x \in X_0(B)$, 存在唯一的态射 $f : B \rightarrow A \in \text{Mor } \mathcal{C}$, 满足

$$X_1(f^{\text{op}})(u) = x.$$

设函子 $Y : \mathcal{C} \rightarrow \mathbf{Set}$ 可表, 并记 $\text{Hom}(A, -)$ 为其一个表示. 则存在一个元素 $u \in Y_0(A)$, 对任意 $B \in \text{Ob } \mathcal{C}$ 以及 $y \in Y_0(B)$, 存在唯一的态射 $g : A \rightarrow B$, 满足

$$Y_1(g)(u) = x.$$

证明. 我们仍证明命题的前半部分. 后半部分可以由对偶原理直接得到.

由于 X 可以由 $\text{Hom}(-, A)$ 表示, 因此我们有自然同构 $\alpha : \text{Hom}(-, A) \xrightarrow{\cong} X$. 因此对任意 $B \in \text{Ob } \mathcal{C}$, 我们有自然的双射

$$\alpha_B : \text{Hom}(B, A) \rightarrow X_0(B).$$

任取 $x \in X_0(B)$, 令 $f \in \text{Hom}(B, A)$, 满足 $x = \alpha_B(f)$.

由 Yoneda 引理, 我们有自然的双射

$$\varphi_{A, X} : \text{Hom}_{[\mathcal{C}^{\text{op}}, \mathbf{Set}]}(\text{Hom}(-, A), X) \rightarrow X_0(A).$$

记 $u = \varphi_{A, X}(\alpha) = \alpha_A(\mathbf{1}_A)$. 任取态射 $B \xrightarrow{f} A$, 我们有

$$X_1(f^{\text{op}})(u) = \alpha_B(f) = x \in X_0(B).$$

□

注 38.3.2.

注意到以上构造对任意自然同构 $\alpha : \text{Hom}(-, A) \xrightarrow{\cong} X$ 都成立. 我们通常称 u 为一个泛元素.

下边我们仍以实数域上向量空间范畴 $\mathbf{Vect}_{\mathbb{R}}$ 和集合范畴 $\mathbf{Set}$ 之间的自由函子 F 和遗忘函子 U 以及逗号范畴为例, 来说明可表函子与泛性质之间的关系.

任取一个集合 S , 我们考虑 Hom-函子

$$Y = \text{Hom}(S, U(-)) : \mathbf{Vect}_{\mathbb{R}} \rightarrow \mathbf{Set}$$

函子 F 为 U 的左伴随, 所以我们有函子的自然同构 $\text{Hom}(S, U(-)) \cong \text{Hom}(F(S), -)$. 取 $A = F(S)$. 以上命题给出以下结论: 我们有一个元素 $u \in Y_0(A) = \text{Hom}(S, U(F(S)))$, 任取对象 $V \in \text{Ob } \mathbf{Vect}_{\mathbb{R}}$ 以及 $f \in Y_0(A) = \text{Hom}(S, U(V))$, 存在唯一的态射 $g : F(S) \rightarrow V$, 满足以下交换图

$$\begin{array}{ccc} S & \xrightarrow{u} & U(F(S)) \\ & \searrow f & \downarrow \exists! U(g) \\ & & U(V) \end{array}$$

这正是我们之前讨论的与向量空间有关的泛性质.

以下我们利用可表函子来给出泛性质的定义.

定义 38.3.3

记 $\mathcal{C}$ 为一个局部小范畴. 我们称一个对象 $A \in \mathcal{C}$ 具有**泛性质**, 若存在一个可表函子 $F : \mathcal{C}^{\text{op}} \rightarrow \mathbf{Set}$ (或者 $F : \mathcal{C} \rightarrow \mathbf{Set}$), 以及一个泛元素 $u \in F_0(A)$, 满足 $F \cong \text{Hom}(-, A)$ (或者 $F \cong \text{Hom}(A, -)$).

在本节最后, 作为例子, 我们来讨论一下向量空间的张量积. 仍考虑实数域 $\mathbb{R}$ 上的向量空间范畴 $\mathbf{Vect}_{\mathbb{R}}$. 任取两个向量空间 U 和 V , 我们可以定义双线性函子

$$X = \mathbf{Bilin}(U, V; -) : \mathbf{Vect}_{\mathbb{R}} \rightarrow \mathbf{Set}.$$

具体地说, 任取 $W \in \text{Ob } \mathbf{Vect}_{\mathbb{R}}$, 我们有

$$X_0(W) = \mathbf{Bilin}(U, V; W),$$

即所有从 $U \times V$ 到 W 的双线性映射构成的集合. 任取态射 $W \xrightarrow{f} W' \in \text{Mor } \mathbf{Vect}_{\mathbb{R}}$, 我们有

$$\begin{aligned} X_1(f) : \mathbf{Bilin}(U, V; W) &\rightarrow \mathbf{Bilin}(U, V; W'), \\ g &\mapsto fg. \end{aligned}$$

任给一个双线性映射

$$f : U \times V \rightarrow W,$$

任取 $u \in U$, 我们有 $f(u, -) \in \text{Hom}(V, W)$; 类似地, 任取 $v \in V$, 我们有 $f(-, v) \in \text{Hom}(U, W)$. 由此, 我们有函子的同构

$$\mathbf{Bilin}(U, V; -) \cong \text{Hom}(U, \text{Hom}(V, -)) \cong \text{Hom}(V, \text{Hom}(U, -)).$$

通过构造张量积 $U \otimes V$, 我们可以验证 $\mathbf{Bilin}(U, V; -) \cong \text{Hom}(U \otimes V, -)$, 因此可表. 由之前的讨论知, 在线性同构意义下, U 和 V 的张量积是唯一的. 利用 Yoneda 引理, 我们知道

$$\text{Hom}(U, \text{Hom}(V, W)) \cong \mathbf{Bilin}(U, V; W) \cong \text{Hom}(U \otimes V, W).$$

由此我们可以得到之前提到的 $\otimes$ -函子为 Hom -函子的左伴随.

第三十九章 极限和余极限

在分析中, 当我们考虑实数序列的时候会考虑这个序列是否收敛的问题. 如果一个实数序列 $(x_n)_{n \in \mathbb{N}}$ 在 n 趋于无穷的时候收敛到某一个实数 a , 我们通常记作

$$\lim_{n \rightarrow \infty} x_n = a.$$

如果我们仔细考虑一下序列以及极限, 会有一些有趣的结论. 一方面, 如果我们考虑一个实数集的子集, 如果该子集不是一个闭集, 通过取聚点, 我们可以向该子集中添加新的元素. 另一方面, 一个序列的极限也满足某种泛性质. 例如, 我们考虑一个点 y , 如果存在一个指标 $N \in \mathbb{N}$, 对任意 $n > N$, 都有 $x_n \leq y$, 那么我们就有 $a \leq y$.

实际上, 极限及其对偶概念余极限在数学各个领域中以许多不同的形式出现. 取极限或者取余极限的操作通常伴随着一些具有某些泛性质的对象的出现. 在本节中, 我们将对这两个概念进行一些讨论.

39.1 定义

当我们考虑一个实数序列的时候, 我们使用自然数来作为下标, 对这个序列的元素进行标记. 这个标记帮助我们在讨论中对序列中的元素进行定位. 我们可以这样的标记看作是一个自然数集到实数的映射. 这帮助我们将序列推广到更一般的情况, 使得我们可以使用任何集合来作为指标集. 比如, 当我们考虑三维欧氏空间 $\mathbb{R}^3$ 里的一条曲线的时候, 我们可以将其看作是区间 $[0, 1]$ 或者 $\mathbb{R}$ 到 $\mathbb{R}^3$ 的一个映射的像. 而所考虑的映射本身给了所考虑的曲线的一个参数化.

记 $\mathcal{C}$ 为一个范畴. 沿着这个思路, 我们给出如下的定义.

定义 39.1.1

任取小范畴 $\mathcal{D}$, 我们称一个函子 $F: \mathcal{D} \rightarrow \mathcal{C}$ 为一个 $\mathcal{C}$ 中的 $\mathcal{D}$ -形图.

注 39.1.2.

这里的范畴 $\mathcal{D}$ 可以被理解为用来给出指标, 我们下边将称其为指标范畴.

任取 $\mathcal{C}$ 的对象 $A \in \text{Ob } \mathcal{C}$, 一个常值 $\mathcal{D}$ -形图是一个常值函子 $\mathcal{D} \rightarrow \mathcal{C}$ 将所有的对象都送到 A , 并将所有的态射送到 1_A . 我们使用 A 来记该函子.

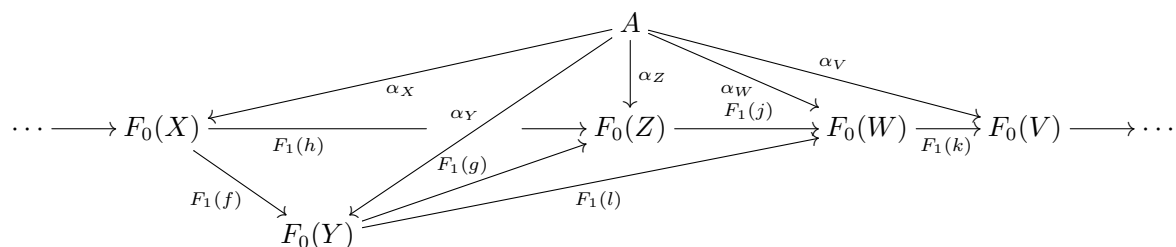
定义 39.1.3

任给 $\mathcal{C}$ 上的一个 $\mathcal{D}$ -形图 F , 任取对象 $A \in \text{Ob } \mathcal{C}$, 范畴 $\mathcal{C}$ 中一个以 F 为底以 A 顶点的锥是一个从常值 $\mathcal{D}$ -形图 A 到 F 的自然变换 $\alpha: A \rightarrow F$. 类似地, 范畴 $\mathcal{C}$ 中一个以 D 为顶以 B 底点的倒锥是一个从 F 到常值 $\mathcal{D}$ -形图 B 的自然变换 $\beta: B \rightarrow F$.

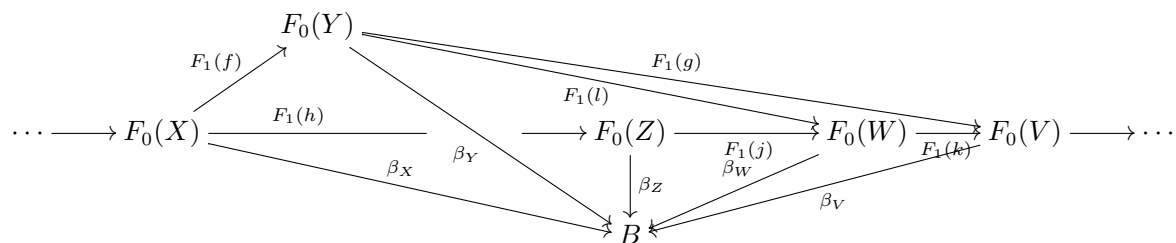
注 39.1.4.

从定义可以看出, 锥和倒锥是对偶的概念. 如果希望统一语言, 我们也可以将倒锥称为余锥.

利用交换图, 一个锥看起来如下图:



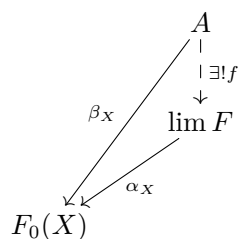
而一个倒锥看起来如下图



我们使用泛性质来定义极限和余极限.

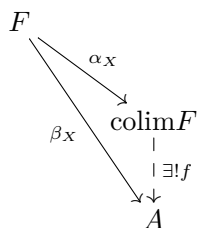
定义 39.1.5

任取范畴 $\mathcal{C}$ 上的一个 $\mathcal{D}$ -形图 F , 若存在 $\mathcal{C}$ 中的对象 $\lim F \in \text{Ob } \mathcal{C}$, 以及一个以 F 为底以 $\lim F$ 为顶点的锥 α , 并满足任给其它以 F 为底的锥 $\beta : A \Rightarrow F$, 都有唯一的一个态射 $f : A \rightarrow \lim F$, 满足对任意 $X \in D$, 都有 $\beta_X = \alpha_X \circ f$:



我们称 $\lim F$ 为 F 的**极限**, 并称 α 为 F 的**极限锥**.

类似地, 若存在 $\mathcal{C}$ 中的对象 $\text{colim } F \in \text{Ob } \mathcal{C}$, 以及一个以 F 为顶以 $\text{colim } F$ 为底点的锥 α , 并满足任给其它以 F 为顶的锥 $\beta : F \Rightarrow A$, 都有唯一的一个态射 $f : \text{colim } F \rightarrow A$, 满足对任意 $X \in D$, 都有 $\beta_X = f \circ \alpha_X$:



我们称 $\lim F$ 为 F 的**余极限**, 并称 α 为 F 的**余极限锥**.

注 39.1.6.

由定义我们可以看出极限和余极限是对偶的概念.

注 39.1.7.

作为一个特殊情况如果 $\mathcal{D}$ 为空范畴, 即其中没有对象和态射, 此时 $\mathcal{C}$ 上的 $\mathcal{D}$ -形图只有一个空图. 因此若说明一个对象 $A \in \text{Ob } \mathcal{C}$ 是空图的极限, 我们只需要验证任取对象 $B \in \text{Ob } \mathcal{C}$, 都存在唯一的一个态射 $B \rightarrow A$. 因此空图的极限是终点对象.

作为对偶的情形, 范畴 $\mathcal{C}$ 的空图的余极限是 $\mathcal{C}$ 中的起点对象.

39.2 例子

我们这里通过极限和余极限的概念来解读一些我们常见的构造.

积和余积

如果下标范畴 $\mathcal{D}$ 为一个离散范畴, 那么范畴 $\mathcal{C}$ 中的 $\mathcal{D}$ -形图实际上就是在 $\mathcal{C}$ 中选一组用 $\text{Ob } \mathcal{D}$ 标记的对象. 此时一个 $\mathcal{D}$ -形图 F 的极限就是所有 $(F_0(X))_{X \in \text{Ob } \mathcal{D}}$ 的积, 而余极限就是这些 $\mathcal{C}$ 的对象的余积.

例 39.2.1 (集合范畴).

如果 $\mathcal{C}$ 为集合范畴 **Set**, 则 **Set** 上一个 D -形图 F 的极限为

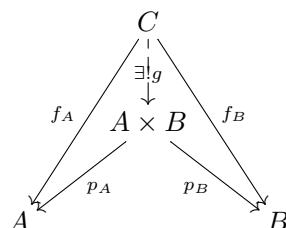
$$\lim F = \prod_{X \in \text{Ob } \mathcal{D}} F_0(X),$$

即所有 $F_0(X)$ 的笛卡尔积.

我们考虑 $\mathcal{D}$ 只有两个对象 X 和 Y 的情形. 记 $F_0(X) = A$ 以及 $F_0(Y) = B$. 考虑笛卡尔积 $A \times B$, 并记其到 A 的投影为 p_A , 到 B 的投影为 p_B , 则任给一个以 F 为底的锥, 即存在一个集合 C 以及映射 $f_A : C \rightarrow A$ 和 $f_B : C \rightarrow B$, 可以验证我们总可以找到映射

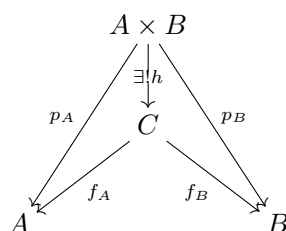
$$\begin{aligned} g : C &\rightarrow A \times B, \\ c &\mapsto (f_A(c), f_B(c)), \end{aligned}$$

满足以下交换图:

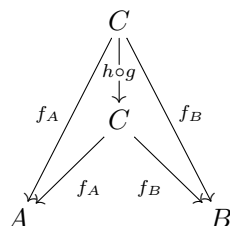


并且该映射 g 是唯一的. 由此可知 $A \times B$ 的确为 F 的一个极限.

如果进一步有 C 也是一个 F 的极限, 则有映射 $h : A \times B \rightarrow C$, 满足以下交换图



注意到 $h \circ g$ 为一个 C 到 C 的映射满足



由于满足以上交换图的 C 到 C 的映射是唯一的, 而 1_C 即满足要求, 因此 $h \circ g = 1_C$, 同样地, 我们也可以证明 $g \circ h = 1_{A \times B}$. 因此 g 和 h 都是双射, F 的极限在同构意义下是唯一的.

集合范畴上 **Set** 一个 $\mathcal{D}$ -形图 F 的余极限为

$$\text{colim } F = \coprod_{X \in \text{Ob } \mathcal{D}} F_0(X),$$

即所有 $F_0(X)$ 的不交并. 具体的验证过程留作练习. 作为对偶情形, 我们也可以证明 F 的余极限在同构意义下是唯一的.

以下我们再给出几个范畴的例子. 具体的验证留作练习.

例 39.2.2 (实数域上的向量空间范畴).

考虑 $\mathcal{C} = \mathbf{Vect}_{\mathbb{R}}$. 一个 $\mathcal{D}$ -形图 F 的极限是所有向量空间 $F_0(X)$ 的直积, 而 F 的余极限是所有向量空间 $F_0(X)$ 的直和.

当然若 $\mathcal{D}$ 只有有限多个对象的时候, 由于有限多个向量空间的直积和直和没有区别, 此时 F 的极限和余极限相同.

例 39.2.3 (实数集全序范畴 $(\mathbb{R}, \leq)$).

考虑 $\mathcal{C} = (\mathbb{R}, \leq)$. 该范畴对象为所有的实数. 任取两个实数 x 和 y , 存在一个态射 $x \rightarrow y$ 当且仅当 $x \leq y$. 任取 $\mathcal{D}$ -形图 F , 其极限为任意 $a \in \mathbb{R}$, 满足

$$a = \min\{F_0(X) \mid X \in \text{Ob } \mathcal{D}\}.$$

相应地, 其余极限为任意 $b \in \mathbb{R}$, 满足

$$b = \max\{F_0(X) \mid X \in \text{Ob } \mathcal{D}\}.$$

在这个例子中, 我们看到若 $\mathcal{D}$ 的对象数目无限, 则 F 的极限或者余极限有可能不存在.

推出和拉回

考虑以下范畴 $\mathcal{D}$, 满足 $\text{Ob } \mathcal{D} = \{X, Y, Z\}$ 和

$$\text{Hom } \mathcal{D} = \{\mathbf{1}_X, \mathbf{1}_Y, \mathbf{1}_Z, X \xrightarrow{u} Y, Z \xrightarrow{v} Y\}.$$

我们用下图记范畴 $\mathcal{D}$:

$$X \xrightarrow{u} Y \xleftarrow{v} Z.$$

任意范畴 $\mathcal{C}$ 中 $\mathcal{D}$ -形图 F 的极限, 若存在的话, 被称为**拉回**. 考虑 $\mathcal{D}$ 的反范畴 $\mathcal{D}^{\text{op}}$, 任意 $\mathcal{C}$ 中的 $\mathcal{D}^{\text{op}}$ -形图 G 的余极限, 存在的话, 被称为**推出**.

我们以集合范畴为例来讨论. 任取 $\mathbf{Set}$ 中的 $\mathcal{D}$ -形图 F , 我们记 $A = F_0(X)$, $B = F_0(Y)$, $C = F_0(Z)$, 并记 $f = F_1(u)$ 和 $g = F_1(v)$, 则有

$$\begin{array}{ccc} & A & \\ & \downarrow f & \\ C & \xrightarrow{g} & B \end{array}$$

记 $\lim F$ 为其极限, 则有映射 $h_A : \lim F \rightarrow A$ 和 $h_C : \lim F \rightarrow C$ 满足

$$\begin{array}{ccc} \lim F & \xrightarrow[h_A]{} & A \\ h_C \downarrow & & \downarrow f \\ C & \xrightarrow{g} & B \end{array}$$

另一方面, 任取一个以 F 为底以集合 D 为顶点的锥 p , 我们都有映射 $i : D \rightarrow \lim F$, 满足

$$\begin{array}{ccccc} D & & & & \\ & \searrow p_A & & & \\ & & \lim F & \xrightarrow{h_A} & A \\ & \swarrow p_B & \downarrow h_C & & \downarrow f \\ & & C & \xrightarrow{g} & B \end{array}$$

我们下边说明 $\lim F$ 的存在性. 考虑以下集合

$$A \times_B C := \{(a, c) \in A \times C \mid f(a) = g(c)\}.$$

映射 h_A 和 h_C 分别为到 A 和到 C 的投影映射. 我们可以验证 $A \times_B C$ 为 F 的一个极限.

下边考虑推出. 任取 **Set** 上一个 $\mathcal{D}^{\text{op}}$ -形图 G , 我们记 $P = G_0(X)$, $Q = G_0(Y)$, $R = G_0(Z)$, 并记 $s = G_1(u^{\text{op}})$ 和 $t = G_1(v^{\text{op}})$, 则有

$$\begin{array}{ccc} Q & \xrightarrow{t} & R \\ s \downarrow & & \\ P & & \end{array}$$

记 $\text{colim}G$ 为其余极限, 则有映射 $k_P : P \rightarrow \text{colim}G$ 和 $k_R : R \rightarrow \text{colim}G$ 满足

$$\begin{array}{ccc} Q & \xrightarrow{t} & R \\ s \downarrow & & \downarrow r_R \\ P & \xrightarrow{r_P} & \text{colim}G \end{array}.$$

另一方面, 任取一个以 G 为顶以集合 E 为底点的倒锥 l , 我们都有映射 $j : \text{colim}G \rightarrow E$, 满足

$$\begin{array}{ccc} Q & \xrightarrow{t} & R \\ s \downarrow & & \downarrow k_R \\ P & \xrightarrow{k_P} & \text{colim}G \\ & \searrow l_P & \nearrow l_R \\ & & E \end{array} \quad \begin{array}{c} \exists! j \\ \text{---} \end{array}.$$

我们下边说明 $\text{colim}G$ 的存在性. 考虑以下集合

$$P \bigsqcup_Q R := P \amalg R / \sim.$$

这里等价关系 $\sim$ 定义如下

$$\sim := \{(p, r) \in P \times R \mid s(p) = t(r)\}.$$

映射 k_P 和 k_R 分别为从 P 和到 R 出发的嵌入映射. 我们可以验证 $P \bigsqcup_Q R$ 为 G 的一个余极限.

我们这里考虑一个简单的以上余极限的例子. 考虑 $Q = P \cap R$, 映射 s 和 t 都是嵌入映射, 则并集 $P \cup R$ 即为所对应的 G 的余极限.

$$\begin{array}{ccc} P \cap R & \xrightarrow{t} & R \\ s \downarrow & & \downarrow k_R \\ P & \xrightarrow{k_P} & P \cup R \\ & \searrow l_P & \nearrow l_R \\ & & E \end{array} \quad \begin{array}{c} \exists! j \\ \text{---} \end{array}.$$

注 39.2.4.

集合 $P \bigsqcup_Q R$ 看起来像是把 P 和 R 沿着 Q 粘起来得到的. 在几何与拓扑中, 使用地图册的方式来描述流形并用之来研究从流形出发的映射使用的正是这种构造以及其作为余极限的性质.

正向极限和逆向极限

考虑以下指标范畴 $\mathcal{D}$:

$$\begin{aligned}\text{Ob } \mathcal{D} &= \{\dots, X_n, \dots, X_1, X_0\}; \\ \text{Mor } \mathcal{D} &= \{\mathbf{1}_{X_n} \mid n \in \mathbb{N}\} \cup \{u_n : X_{n+1} \rightarrow X_n \mid n \in \mathbb{N}\}.\end{aligned}$$

我们可以用下图来表示该范畴:

$$\dots \xrightarrow{u_n} X_n \xrightarrow{u_{n-1}} \dots \xrightarrow{u_1} X_1 \xrightarrow{u_0} X_0.$$

其反范畴 $\mathcal{D}^{\text{op}}$ 则可以用下图来表示

$$X_0 \xrightarrow{u_0^{\text{op}}} X_1 \xrightarrow{u_1^{\text{op}}} \dots \xrightarrow{u_{n-1}^{\text{op}}} X_n \xrightarrow{u_n^{\text{op}}} \dots.$$

记 $\mathcal{C}$ 为一个范畴. 任取 $\mathcal{C}$ 中的一个 $\mathcal{D}$ -形图 F , 对任意 $n \in -\mathbb{N}$, 我们记 $A_n = F_0(X_n)$, 则 F 的余极限被称为 $(A_n)_{n \in \mathbb{N}}$ 的**正向极限**. 任取 $\mathcal{C}$ 中的一个 $\mathcal{D}^{\text{op}}$ -形图 G , 对任意 $n \in -\mathbb{N}$, 我们记 $B_n = G_0(X_n)$, 则 G 的余极限被称为 $(B_n)_{n \in \mathbb{N}}$ 的**逆向极限**.

我们下边来看一些正向极限和逆向极限的例子. 这些例子都是在相关课程的学习中常见的例子, 故所有的验证过程略去.

例 39.2.5 (集合偏序范畴).

我们考虑所有集合关于偏序关系构成的范畴 $\mathbf{Pset}$, 其中任给两个集合 A 和 B , 存在 $A \rightarrow B$ 当且仅当 $A \subset B$. 使用以上记号, 一个 $\mathbf{Pset}$ 上的 $\mathcal{D}$ -形图 F 对应的是一个集合降链

$$\dots \subset A_n \subset \dots \subset A_1 \subset A_0.$$

其对应的正向极限即为所有集合 A_n 的交集

$$\lim F = \bigcap_{n \in \mathbb{N}} A_n.$$

另一方面, 任意 $\mathbf{Pset}$ 上的 $\mathcal{D}^{\text{op}}$ -形图 G 对应的是一个集合升链

$$B_0 \subset B_1 \subset \dots \subset B_n \subset \dots.$$

其对应的正向极限即为所有集合 B_n 的并集

$$\text{colim } G = \bigcup_{n \in \mathbb{N}} B_n.$$

例 39.2.6 (实数域上向量空间范畴).

我们考虑实数域 $\mathbb{R}$ 上的向量空间构成的范畴 $\mathbf{Vect}_{\mathbb{R}}$. 考虑以下的 $\mathcal{D}$ -形图

$$\dots \xrightarrow{f_n} \mathbb{R}^n \xrightarrow{f_{n-1}} \dots \xrightarrow{f_1} \mathbb{R} \xrightarrow{f_0} \{0\}.$$

其中任取 $n \in \mathbb{N}^*$, 线性映射 f_n 定义如下

$$\begin{aligned}f_n &: \mathbb{R}^{n+1} \rightarrow \mathbb{R}^n, \\ (x_1, \dots, x_{n+1}) &\mapsto (x_1, \dots, x_n).\end{aligned}$$

则 F 的极限为直积

$$\prod_{n \in \mathbb{N}} \mathbb{R}$$

另一方面, 考虑以下的 $\mathcal{D}^{\text{op}}$ -形图

$$\{0\} \xrightarrow{g_0} \mathbb{R} \xrightarrow{g_1} \cdots \xrightarrow{g_{n-1}} \mathbb{R}^n \xrightarrow{f_n} \cdots.$$

其中任取 $n \in \mathbb{N}^*$, 线性映射 g_n 定义如下

$$\begin{aligned} g_n : \mathbb{R}^n &\rightarrow \mathbb{R}^{n+1}, \\ (x_1, \dots, x_n) &\mapsto (x_1, \dots, x_n, 0). \end{aligned}$$

则 G 的余极限为直和

$$\bigoplus_{n \in \mathbb{N}} \mathbb{R}$$

例 39.2.7 (实数序范畴).

我们考虑实数集关于序关系构成的范畴 $(\mathbb{R}, \leq)$. 一个 $(\mathbb{R}, \leq)$ 上的 $\mathcal{D}$ -形图 F 对应的是一个上升序列

$$\cdots \leq x_n \leq \cdots \leq x_1 \leq x_0.$$

其对应的正向极限即为上确界

$$\lim F = \sup\{x_n \in \mathbb{R} \mid n \in \mathbb{N}\}.$$

另一方面, 任意 $(\mathbb{R}, \leq)$ 上的 $\mathcal{D}^{\text{op}}$ -形图 G 对应的是一个下降序列

$$y_0 \leq y_1 \leq \cdots \leq y_n \leq \cdots.$$

其对应的正向极限即为下确界

$$\text{colim} G = \inf\{y_n \in \mathbb{R} \mid n \in \mathbb{N}\}.$$

我们知道一个实数序列的上确界或下确界不一定存在, 我们在数学分析中是通过添加 $+\infty$ 和 $-\infty$ 来处理在 $\mathbb{R}$ 中没有上下确界的情况.

附录 A 同态基本定理

A.1 环同态的像与原像

设 R 和 R_1 为两个环. 设存在环同态 $\phi: R \rightarrow R_1$. 我们记 ϕ 的核和像分别为 $\ker \phi$ 和 $\text{Im } \phi$.

对任意 $u \in R_1$, 我们记其在 ϕ 下的原像集为

$$\phi^{-1}(u) := \{a \in R \mid \phi(a) = u\} \subset R.$$

若 $u = 0$, 则 $\phi^{-1}(0) = \ker \phi$.

若 $u \notin \text{Im } \phi$, 则 $\phi^{-1}(u) = \emptyset$.

命题 1.1.1

设 $u \in \text{Im } \phi$, 则 $\phi^{-1}(u)$ 在 R 中对加法封闭, 当且仅当 $u = 0$.

证明. 若 $u = 0$, $\phi^{-1}(0) = \ker \phi$ 为 R 的一个理想, 对加法封闭.

设 $u \neq 0$, 由 $u \in \text{Im } \phi$, 存在 $a \in R$, 满足 $\phi(a) = u$. 由 ϕ 为环同态, 我们有

$$\phi(a + a) = \phi(a) + \phi(a) = u + u = 2u.$$

我们使用反证法. 若 $\phi^{-1}(u)$ 对加法封闭, 则有 $a + a \in \phi^{-1}(u)$, 因此 $2u = u$. 我们有 $u = 0$, 矛盾. $\square$

命题 1.1.2

设 $u \in \text{Im } \phi$, 任给 $a \in \phi^{-1}(u)$, 我们有

$$\phi^{-1}(u) = a + \ker \phi.$$

注 1.1.3.

回顾: $a + \ker \phi := \{a + c \mid c \in \ker \phi\} \subset R$.

证明. 设 $a \in \phi^{-1}(u)$.

任给 $\phi^{-1}(u)$ 中元素 b , 由于 ϕ 是一个同态, 我们有

$$\phi(-a + b) = -\phi(a) + \phi(b) = u - u = 0.$$

因此 $-a + b \in \ker \phi$. 我们可以将 b 写为 $b = a + (-a + b)$, 其中 $-a + b \in \ker \phi$. 由此, 我们得到

$$\phi^{-1}(u) \subset a + \ker \phi.$$

另一方面, 设 $c \in \ker \phi$. 由 ϕ 为一个环同态, 我们有

$$\phi(a + c) = \phi(a) + \phi(c) = u + 0 = u.$$

因此 $\phi^{-1}(u) \supset a + \ker \phi$. 综上所述, 我们有 $\phi^{-1}(u) = a + \ker \phi$. $\square$

推论 1.1.4

对任意 $a, b \in R$, 我们有 $\phi(a) = \phi(b)$ 当且仅当 $a - b \in \ker \phi$.

我们可以利用 ϕ 的原像构造 R 中的一个等价关系: R 中两个元素等价当且仅当它们在 ϕ 下的像相同, 也即

$$\bullet \forall a, b \in R, a \sim b \Leftrightarrow \phi(a) = \phi(b).$$

由以上推论, 以下两个商环相等 $R/\sim = R/\ker \phi$.

注 1.1.5.

以上说明, 由考虑原像得到的 R 上的等价关系和考虑 R 上由理想 $\ker \phi$ 诱导的等价关系相同.

注 1.1.6.

注意到以上讨论中我们只用到了环上的加法. 对于乘法, 我们不能做太多事情. 因为对于一般的环, 类似于加法的分解 $b = a + (b - a)$ 不一定存在, 并且对任意 $a \in R$, 都有 $a \ker \phi \subset \ker \phi$.

注 1.1.7.

注意到以上讨论并没有用到加法的交换性, 因此, 后边我们会看到以上讨论实际上对任意群同态都成立.

A.2 集合之间的映射

在这一部分, 我们先忘掉代数结构, 讨论一下集合之间的映射. 设 R, R_1 和 R_2 为三个非空集合, 并有映射:

$$\phi: R \rightarrow R_1, \quad \psi: R \rightarrow R_2,$$

满足 ϕ 为满射. 为了方便区分, 我们使用 a, b, c 表示 R 中的元素, u, v, w 表示 R_1 中的元素, x, y, z 表示 R_2 中的元素.

问: 什么情况下存在一个映射 $\bar{\psi}: R_1 \rightarrow R_2$, 使得以下交换图成立:

$$\begin{array}{ccc} R & \xrightarrow{\psi} & R_2 \\ \phi \downarrow & \nearrow \bar{\psi} & \\ R_1 & & \end{array}$$

注 1.2.1.

我们希望能得到一个映射 $\bar{\psi}$. 根据定义, 一个关系若想成为映射, 需要满足以下两个条件:

(i) (定义域为整个 R_1) 对任意 $u \in R_1$, 存在 $x \in R_2$, 满足 $\bar{\psi}(u) = x$,

(ii) (R_1 中任意元素有唯一的像) 对任意 $u \in R_1$, 若 $\bar{\psi}(u) = x_1$ 且 $\bar{\psi}(u) = x_2$, 则 $x_1 = x_2$.

我们先假设 $\bar{\psi}$ 存在, 来看看需要什么条件 (必要条件).

若该映射 $\bar{\psi}: R_1 \rightarrow R_2$ 存在, 我们有 $\psi = \bar{\psi} \circ \phi$. 因此

- 对任意 $a \in R$, 我们有 $\psi(a) = \bar{\psi}(\phi(a))$.

命题 1.2.2

任给 $a, b \in R$, 我们有 $\phi(a) = \phi(b) \implies \psi(a) = \psi(b)$.

证明. 考虑任意 $a, b \in R$, 满足 $\phi(a) = \phi(b)$, 记 R_1 中的元素

$$u = \phi(a) = \phi(b),$$

我们有 $\bar{\psi}(u) = \psi(a)$ 且 $\bar{\psi}(u) = \psi(b)$. 因此 $\psi(a) = \psi(b)$. □

推论 1.2.3

对任意 $u \in R_1$, 存在 $x \in R_2$, 满足

$$\phi^{-1}(u) \subset \psi^{-1}(x).$$

证明. 任取 $u \in R_1$, 由于 ϕ 为满射, 存在 $a \in R$, 满足 $u = \phi(a)$. 我们记 $x = \psi(a)$. 因此 $a \in \phi^{-1}(u)$ 且 $a \in \psi^{-1}(x)$.

任给 $b \in R$, 若 $b \in \phi^{-1}(u)$, 则有 $\phi(a) = \phi(b)$. 由之前命题, 我们有 $\psi(a) = \psi(b)$. 因此 $b \in \psi^{-1}(x)$. 因此我们有 $\phi^{-1}(u) \subset \psi^{-1}(x)$. □

注 1.2.4.

$\phi^{-1}(u)$ 和 $\psi^{-1}(x)$ 均为 R 的子集.

注 1.2.5.

以上说明了存在 $\bar{\psi}$ 的一个必要条件是,

- 对任意 $a \in R$, 我们有 $\phi^{-1}(\phi(a)) \subset \psi^{-1}(\psi(a))$.

注意这里 ϕ^{-1} 和 ψ^{-1} 为取原像集, 不是逆映射.

我们下边将说明这也是充分条件. 充分性的证明是一个构造性证明: 我们将由已知条件构造出这个映射.

命题 1.2.6

设 R, R_1 和 R_2 为三个非空集合, 并有映射:

$$\phi: R \rightarrow R_1, \quad \psi: R \rightarrow R_2,$$

满足 ϕ 为满射. 若对任意 $a \in R$, 我们有 $\phi^{-1}(\phi(a)) \subset \psi^{-1}(\psi(a))$, 则存在一个映射 $\bar{\psi}: R_1 \rightarrow R_2$, 使得以下交换图成立:

$$\begin{array}{ccc} R & \xrightarrow{\psi} & R_2 \\ \phi \downarrow & \nearrow \bar{\psi} & \\ R_1 & & \end{array}$$

进一步地, 这样的映射 $\bar{\psi}$ 是唯一的.

证明. 我们将如下构造映射 $\bar{\psi}: R_1 \rightarrow R_2$, 并验证 $\bar{\psi}$ 是良定义的.

任取 $u \in R_1$, 由于 ϕ 为满射, 因此存在 $a \in R$, 满足 $\phi(a) = u$. 我们记 $x = \psi(a)$. 定义

$$\bar{\psi}(u) := x.$$

我们只需验证这个定义不依赖于 a 的选取. 也即, 取任意 $b \in \phi^{-1}(u)$, 我们得到的 $\bar{\psi}(u)$ 是相同的.

由条件: $\phi^{-1}(\phi(a)) \subset \psi^{-1}(\psi(a))$, 我们有 $\phi^{-1}(u) \subset \psi^{-1}(x)$, 因此 $\bar{\psi}$ 不依赖于 $a \in \phi^{-1}(u)$ 的选取. 由此 $\bar{\psi}$ 是良定义 (不依赖 a 推出有唯一的一个 x 与 u 对应).

其次, 我们需要验证 $\bar{\psi}$ 满足交换图. 任取 $a \in R$, 我们记 $\phi(a) = u$, 以及 $\psi(a) = x$. 由 $\bar{\psi}$ 定义, 对任意 $a \in R$, 我们有

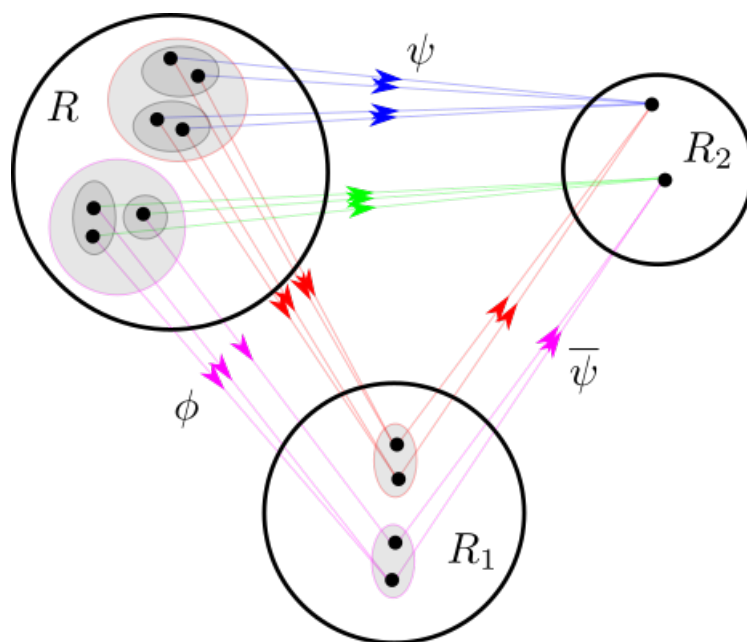
$$\psi(a) = x = \bar{\psi}(u) = \bar{\psi}(\phi(a)) = (\bar{\psi} \circ \phi)(a).$$

因此 $\psi = \bar{\psi} \circ \phi$.

设 $\tilde{\psi}: R_1 \rightarrow R_2$ 为另一个满足要求的映射, 对任意 u , 任取 $a \in \phi^{-1}(u)$, 我们有

$$\tilde{\psi}(u) = \tilde{\psi}(\phi(a)) = (\tilde{\psi} \circ \phi)(a) = \psi(a) = \bar{\psi}(u).$$

因此 $\tilde{\psi} = \bar{\psi}$, 满足要求的映射 $\bar{\psi}$ 唯一. □



从集合 R 的划分的角度来看, 我们希望由 ϕ 的原像构成的划分比由 ψ 的原像构成的划分细, 也就是说, 对任意 $u \in R_1, x \in R_2$, 我们有 $\phi^{-1}(u) \cap \psi^{-1}(x) = \emptyset$ 或者 $\phi^{-1}(u) \subset \psi^{-1}(x)$.

A.3 群同态基本定理

如果我们将环看作加法群, 那么环同态也是加法群同态. 我们在这节里, 在之前集合的基础上加上一个群结构条件, 来讨论群同态基本定理.

我们现在考虑 $(G, *)$, $(G_1, *_1)$ 和 $(G_2, *_2)$ 都为群(不一定是交换群)的情形. 假设有群同态映射:

$$\phi: G \rightarrow G_1, \quad \psi: G \rightarrow G_2,$$

满足 ϕ 为满同态. 为了方便区分, 我们仍使用 a, b, c 表示 G 中的元素, u, v, w 表示 G_1 中的元素, x, y, z 表示 G_2 中的元素. 我们记 G, G_1 和 G_2 的幺元分别为 e, e_1 和 e_2 . 回顾 ϕ 和 ψ 的核分别为:

$$\ker \phi := \{a \in G \mid \phi(a) = e_1\}, \quad \ker \psi := \{a \in G \mid \psi(a) = e_2\}.$$

命题 1.3.1

沿用以上设定. 若存在映射 $\bar{\psi}: G_1 \rightarrow G_2$, 使得以下交换图成立:

$$\begin{array}{ccc} G & \xrightarrow{\psi} & G_2 \\ \phi \downarrow & \nearrow \bar{\psi} & \\ G_1 & & \end{array}$$

则映射 $\bar{\psi}$ 是一个群同态.

证明. 任取 G_1 中元素 u 和 v , 由于 ϕ 是满射, 存在 $a, b \in G$, 满足 $\phi(a) = u, \phi(b) = v$. 由于 ϕ 为同态, 因此 $\phi(a * b) = u *_1 v$.

回顾 $\bar{\psi}$ 的定义: 对任意 $u \in G_1$, 任取 $a \in \phi^{-1}(u) \subset G$, 定义 $\bar{\psi}(u) = \psi(a)$.
由于 ψ 是一个同态, 我们有

$$\begin{aligned}\bar{\psi}(u *_1 v) &= \psi(a * b) \\ &= \psi(a) *_2 \psi(b) \\ &= (\bar{\psi} \circ \phi)(a) *_2 (\bar{\psi} \circ \phi)(b) \\ &= \bar{\psi}(u) *_2 \bar{\psi}(v)\end{aligned}$$

□

当所有映射都是群同态之后, 之前命题里关于 $\bar{\psi}$ 存在的充要条件就可以被如下简化.

命题 1.3.2

沿用本节开头设定. 以下两个叙述等价:

- (i) 对任意 $a \in G$, 有 $\phi^{-1}(\phi(a)) \subset \psi^{-1}(\psi(a))$,
- (ii) $\ker \phi \subset \ker \psi$.

证明. 第一节关于逆像的讨论也适用于一般群. 我们考虑 $\phi: G \rightarrow G_1$. 任给 $u \in G_1$, 任取 $a \in G$, 满足 $\phi(a) = u$, 我们有

$$\phi^{-1}(u) = a * \ker \phi.$$

这是因为, 任给 $b \in G$, 满足 $\phi(b) = u$, 由于 ϕ 为群同态, 我们有 $\phi(a^{-1} * b) = e_1$. 因此 $a^{-1} * b \in \ker \phi$, $b = a * (a^{-1} * b) \in a * \ker \phi$. 另一方面, 任给 $c \in \ker \phi$, 我们有

$$\phi(a * c) = \phi(a) *_1 \phi(c) = \phi(a) = u.$$

因此, $a * c \in \phi^{-1}(u)$. 所以我们有集合相等

$$\phi^{-1}(\phi(a)) = a * \ker \phi$$

(群不一定交换, 作为集合, 我们也有 $\phi^{-1}(u) = \ker \phi * a$).

类似的, 我们也可以证明

$$\psi^{-1}(\psi(a)) = a * \ker \psi.$$

因此, 我们有 $\phi^{-1}(\phi(a)) \subset \psi^{-1}(\psi(a))$ 当且仅当 $\ker \phi \subset \ker \psi$. □

由以上讨论, 我们有如下命题:

命题 1.3.3

设 G, G_1 和 G_2 为三个群, 并有群同态映射:

$$\phi: G \rightarrow G_1, \quad \psi: G \rightarrow G_2,$$

满足 ϕ 为满射. 那么存在一个群同态映射 $\bar{\psi}: G_1 \rightarrow G_2$, 使得以下交换图成立:

$$\begin{array}{ccc} G & \xrightarrow{\psi} & G_2 \\ \phi \downarrow & \nearrow \bar{\psi} & \\ G_1 & & \end{array}$$

当且仅当我们有 $\ker \phi \subset \ker \psi$.

进一步地, 若存在这样的映射 $\bar{\psi}$, 则 $\bar{\psi}$ 是唯一的.

定理 1.3.4 (定理1.4.21)

设 G 和 G' 为两个群, 并设有满同态映射:

$$f: G \rightarrow G'.$$

记 $N = \ker f \triangleleft G$, 并记 $\pi: G \rightarrow G/N$ 为其对应的自然同态. 那么

(i) 存在一个群同构映射

$$\bar{f}: G/N \rightarrow G',$$

使得以下交换图成立:

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \pi \downarrow & \nearrow \bar{f} & \\ G/N & & \end{array}$$

进一步地, 这样的映射 $\bar{f}$ 是唯一的.

(ii) f 建立了 G 中包含 N 的子群与 G' 中的子群之间的一一对应,

(iii) f 将 G 中包含 N 的正规子群对应到 G' 的正规子群.

(iv) 若 $N \subset H \triangleleft G$, 则有

$$G/H \cong G'/f(H).$$

命题 1.3.3 保证了同态 $\bar{f}$ 的存在性. 之后我们需要证明它是双射得到 (i). 然后利用子群, 正规子群在群满同态映射下的像仍是子群和正规子群的性质得到 (ii) 和 (iii). (iv) 是对以下同态的复合使用 (i)

$$G \rightarrow G' \rightarrow G'/f(H).$$

A.4 环同态基本定理

我们现在考虑 R, R_1 和 R_2 都为环的情形. 假设有同态映射:

$$\phi: R \rightarrow R_1, \quad \psi: R \rightarrow R_2,$$

满足 ϕ 为满同态. 为了方便区分, 我们使用 a, b, c 表示 R 中的元素, u, v, w 表示 R_1 中的元素, x, y, z 表示 R_2 中的元素.

命题 1.4.1

沿用以上设定. 若存在映射 $\bar{\psi}: R_1 \rightarrow R_2$, 使得以下交换图成立:

$$\begin{array}{ccc} R & \xrightarrow{\psi} & R_2 \\ \phi \downarrow & \nearrow \bar{\psi} & \\ R_1 & & \end{array}$$

则映射 $\bar{\psi}$ 是一个环同态.

证明. 由于 ϕ 和 ψ 也是加法群同态, 由命题 1.3.1, 我们知道 $\bar{\psi}$ 是一个加法群同态.

另一方面, 任取 R_1 中元素 u 和 v , 由于 ϕ 是满射, 存在 $a, b \in R$, 满足 $\phi(a) = u, \phi(b) = v$. 由于 ϕ 是一个环同态, 我们也有 $\phi(ab) = uv$. 由于 ψ 是一个环同态, 我们有

$$\begin{aligned}\bar{\psi}(uv) &= \psi(ab) \\ &= \psi(a)\psi(b) \\ &= (\bar{\psi} \circ \phi)(a)(\bar{\psi} \circ \phi)(b) \\ &= \bar{\psi}(u)\bar{\psi}(v)\end{aligned}$$

综上所述, $\bar{\psi}$ 是一个环同态.

□

在命题 1.3.3 的基础上, 我们考虑以上命题, 则有以下命题:

命题 1.4.2

设 R, R_1 和 R_2 为三个环, 并有同态映射:

$$\phi: R \rightarrow R_1, \quad \psi: R \rightarrow R_2,$$

满足 ϕ 为满射. 存在一个环同态映射 $\bar{\psi}: R_1 \rightarrow R_2$, 使得以下交换图成立:

$$\begin{array}{ccc} R & \xrightarrow{\psi} & R_2 \\ \phi \downarrow & \nearrow \bar{\psi} & \\ R_1 & & \end{array}$$

当且仅当我们有 $\ker \phi \subset \ker \psi$.

进一步地, 若存在这样的映射 $\bar{\psi}$, 则 $\bar{\psi}$ 是唯一的.

我们可以考虑不同的 R, R_1, R_2, ϕ 和 ψ 的选取, 从而得到一些特殊情形下的结论.

推论 1.4.3

设 R 和 R_1 为两个环, I 为 R 的一个理想, 并设有同态映射:

$$\phi: R \rightarrow R_1.$$

记 $\pi: R \rightarrow R/I$ 为自然同态. 那么存在一个环同态映射 $\bar{\phi}: R/I \rightarrow R_1$, 使得以下交换图成立:

$$\begin{array}{ccc} R & \xrightarrow{\phi} & R_1 \\ \pi \downarrow & \nearrow \bar{\phi} & \\ R/I & & \end{array}$$

当且仅当我们有 $I \subset \ker \phi$.

进一步地, 若存在这样的映射 $\bar{\phi}$, 则 $\bar{\phi}$ 是唯一的.

推论 1.4.4

设 R 为一个环, I 和 J 为 R 的两个理想. 考虑自然同态:

$$\pi_I : R \rightarrow R/I, \quad \pi_J : R \rightarrow R/J.$$

那么存在一个环同态映射 $\phi : R/I \rightarrow R/J$, 使得以下交换图成立:

$$\begin{array}{ccc} R & \xrightarrow{\pi_J} & R/J \\ \pi_I \downarrow & \nearrow \phi & \\ R/I & & \end{array}$$

当且仅当我们有 $I \subset J$.

进一步地, 若存在这样的映射 ϕ , 则 ϕ 是唯一的.

定理 1.4.5 (定理 2.4.5)

设 R 和 R_1 为两个环, 并设有满同态映射:

$$\phi : R \rightarrow R_1.$$

记 $I = \ker \phi$ 为 R 的一个理想, $\pi : R \rightarrow R/I$ 为其对应的自然同态. 那么

(i) 存在一个环同构映射

$$\bar{\phi} : R/I \rightarrow R_1,$$

使得以下交换图成立:

$$\begin{array}{ccc} R & \xrightarrow{\phi} & R_1 \\ \pi \downarrow & \nearrow \bar{\phi} & \\ R/I & & \end{array}$$

进一步地, 这样的映射 $\bar{\phi}$ 是唯一的.

(ii) 存在 R 中包含 I 的子环与 R_1 中的子环之间的一一对应, 且将理想送到理想.

(iii) 若 J 为 R 的一个包含 I 的理想, 则有

$$R/J \cong R_1/\phi(J).$$

注 1.4.6.

这里由环同态基本定理, 我们可以得到这个同态映射 $\bar{\phi}$, 之后我们需要验证 $\bar{\phi}$ 是单射和满射, 因此是一个环同构.

A.5 例子

我们可以考虑 $R = \mathbb{Z}$, $R_1 = \mathbb{Z}_6$ 以及 $R_2 = \mathbb{Z}_2$, 并考虑 $\mathbb{Z}$ 到 $\mathbb{Z}_6$ 和 $\mathbb{Z}_2$ 的自然同态, 分别记作 π_6 和 π_2 . 回顾:

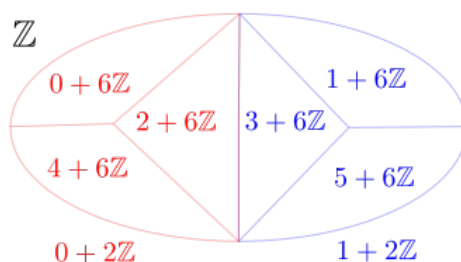
$$\mathbb{Z}_2 := \{0 + 2\mathbb{Z}, 1 + 2\mathbb{Z}\};$$

$$\mathbb{Z}_6 := \{0 + 6\mathbb{Z}, 1 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 3 + 6\mathbb{Z}, 4 + 6\mathbb{Z}, 5 + 6\mathbb{Z}, 6 + 6\mathbb{Z}\}$$

我们已知有如下交换图:

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\pi_2} & \{0 + 2\mathbb{Z}, 1 + 2\mathbb{Z}\} \\ & \searrow \pi_6 & \nearrow \overline{\pi_2} \\ & & \{0 + 6\mathbb{Z}, 1 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 3 + 6\mathbb{Z}, 4 + 6\mathbb{Z}, 5 + 6\mathbb{Z}, \} \end{array}$$

我们也可以从 $\mathbb{Z}$ 的分划来理解, 有如下示意图:



A.6 模同态基本定理

设 R 为一个幺环, M , M_1 和 M_2 为三个 R -模. 假设有模同态映射:

$$\phi : M \rightarrow M_1, \quad \psi : M \rightarrow M_2,$$

满足 ϕ 为满同态. 为了方便区分, 我们使用 a, b, c 表示 R 中的元素, u, v, w 表示 M 中的元素, x, y, z 表示 M_1 中的元素.

命题 1.6.1

沿用以上设定. 若存在映射 $\overline{\psi} : M_1 \rightarrow M_2$, 使得以下交换图成立:

$$\begin{array}{ccc} M & \xrightarrow{\psi} & M_2 \\ \phi \downarrow & \nearrow \overline{\psi} & \\ M_1 & & \end{array}$$

则映射 $\overline{\psi}$ 是一个模同态.

证明. 由于 ϕ 和 ψ 也是群同态, 由命题 1.3.1, 我们知道 $\overline{\psi}$ 是一个群同态.

另一方面, 任取 R 中元素 a , 任取 M_1 中元素 x , 由于 ϕ 是满射, 存在 $u \in M$, 满足 $\phi(u) = x$. 由于 ϕ 是一个模同态, 我们也有 $\phi(au) = ax$. 由于 ψ 是一个模同态, 我们有

$$\begin{aligned}\bar{\psi}(ax) &= \psi(au) \\ &= a\psi(u) \\ &= a(\bar{\psi} \circ \phi)(u) \\ &= a\bar{\psi}(x)\end{aligned}$$

综上所述, $\bar{\psi}$ 是一个模同态.

□

命题 1.6.2

设 R 为一个幺环, M , M_1 和 M_2 为三个 R -模, 并有模同态映射:

$$\phi: M \rightarrow M_1, \quad \psi: M \rightarrow M_2,$$

满足 ϕ 为满射. 存在一个环同态映射 $\bar{\psi}: M_1 \rightarrow M_2$, 使得以下交换图成立:

$$\begin{array}{ccc} M & \xrightarrow{\psi} & M_2 \\ \phi \downarrow & \nearrow \bar{\psi} & \\ M_1 & & \end{array}$$

当且仅当我们有 $\ker \phi \subset \ker \psi$.

进一步地, 若存在这样的映射 $\bar{\psi}$, 则 $\bar{\psi}$ 是唯一的.

定理 1.6.3 (定理3.1.17)

设 R 为一个幺环. M 和 M_1 为两个 R -模, 并设有模的同态映射:

$$\phi : M \rightarrow M_1.$$

记 $N = \ker \phi$ 为 M 的子模, $\pi : M \rightarrow M/N$ 为其对应的自然同态. 那么

(i) 存在一个模同构映射

$$\bar{\phi} : M/N \rightarrow M_1,$$

使得以下交换图成立:

$$\begin{array}{ccc} M & \xrightarrow{\phi} & M_1 \\ \pi \downarrow & \nearrow \bar{\phi} & \\ M/N & & \end{array}$$

进一步地, 这样的映射 $\bar{\phi}$ 是唯一的.

(ii) 存在 M 中包含 N 的子模与 M_1 中的子模之间的一一对应.

(iii) 若 N_1 为 M 的一个包含 N 的子模, 则有

$$M/N_1 \cong M_1/\phi(N_1).$$

A.7 总结

由集合间的映射的定义, 在给定满射 ϕ 和映射 ψ 的前提下, 我们对什么时候存在一个映射 $\bar{\psi}$, 使得 $\psi = \bar{\psi} \circ \phi$ 进行了讨论, 找到了 $\bar{\psi}$ 存在的充要条件 (命题 1.2.6).

若所考虑的集合上有某种代数结构 (群, 环, 模), 并且 ϕ 和 ψ 都是关于该种结构的 (群, 环, 模) 同态映射, 那么所找到的 $\bar{\psi}$ 也是关于该种结构的 (群, 环, 模) 同态映射 (命题 1.3.1, 命题 1.4.1, 命题 1.6.1).

另一方面, 在有 (群, 环, 模) 等代数结构之后, $\bar{\psi}$ 首先是一个群同态, 之前找到的 $\bar{\psi}$ 存在的充要条件可以进行一定的简化 (命题 1.3.2). 最终我们得到了该代数结构 (群, 环, 模) 对应的结论.

附录 B 直积与直和

在讨论群, 环, 模的时候, 直和和直积是通常会遇到的从已有的代数结构出发来构造新的相应的代数结构的方法. 大概的想法来自于以下简单的观察: 任给两个带有某种代数运算的集合 A 和 B , 我们首先可以构造二者的笛卡尔积 $A \times B$. 任取两个 $A \times B$ 中的元素, 我们可以考虑第一个位置使用 A 中的运算, 第二个位置上使用 B 的运算来构造 $A \times B$ 上的运算.

因此这两个概念中重要的一步就是构造涉及的集合的笛卡尔积. 我们首先讨论如何将上边两个集合的笛卡尔积的概念推广到任意多个非空集合的笛卡尔积.

B.1 非空集合的笛卡尔积

记 A 和 B 为两个非空集合. 我们定义二者的笛卡尔积为:

$$A \times B := \{(a, b) \mid a \in A, b \in B\}.$$

类似地, 我们可以考虑有限多个非空集合 (一个集合可能出现多次) 将每个集合中地元素取出按照顺序排列得到一个有限序列. 将这些序列收集起来就是这些非空集合地笛卡尔积.

记 $n \in \mathbb{N} \setminus \{0, 1\}$, $A_1, \dots, A_n$ 为 n 个非空集合, 我们定义这些集合地笛卡尔积为:

$$A_1 \times \cdots \times A_n := \{(a_1, \dots, a_n) \mid a_1 \in A_1, \dots, a_n \in A_n\}.$$

我们可以继续将这个概念推广到可数无穷多个非空集合的情形. 记 $(A_n)_{n \in \mathbb{N}}$ 为一列非空集合, 我们定义这些集合的笛卡尔积为

$$\prod_{n \in \mathbb{N}} A_n := \{(a_n)_{n \in \mathbb{N}} \mid \forall n \in \mathbb{N}, a_n \in A_n\}.$$

如果我们希望继续将以上概念推广到更一般的情形, 就会遇到一个问题. 当我们考虑有限, 甚至可数无限的时候, 我们可以借用 $\mathbb{N}$ 上的序关系, 将这些非空集合做一个排列, 然后通过类似数列的方式将笛卡尔积中的元素表达出来. 但是当我们开始考虑不可数无限的时候, 这样并不是总是可以做到的.

我们可以换一种思路来重写以上的集合. 注意到在表达非空集合的笛卡尔积中的元素, 我们实际上需要的就是在每个集合中取出一个元素, 将这些元素放在一起. 每个元素还需要做一个标记, 使得我们在看到这堆元素的时候知道每个元素来自哪个集合. 因此, 笛卡尔积的元素实际上到这些非空集合的集合有一个一一对应.

从映射的角度, 我们可以将之前有限多个非空集合的笛卡尔积以及可数无穷多个非空集合的笛卡尔积重新表达如下:

(i) 记 $n \in \mathbb{N} \setminus \{0, 1\}$, 以及非空集合 $A_1, \dots, A_n$, 我们定义这些集合的笛卡尔积为

$$A_1 \times \cdots \times A_n := \left\{ f : \{1, \dots, n\} \rightarrow \bigcup_{i=1}^n A_i \mid \forall i \in \{1, \dots, n\}, f(i) \in A_i \right\}.$$

(ii) 记 $(A_n)_{n \in \mathbb{N}}$ 为一列非空集合, 我们定义这些集合的笛卡尔积为

$$\prod_{n \in \mathbb{N}} A_n := \left\{ f : \mathbb{N} \rightarrow \bigcup_{n \in \mathbb{N}} A_n \mid \forall n \in \mathbb{N}, f(n) \in A_n \right\}.$$

这样我们就可以将这个概念推广到更一般的情形. 任取 Ω 为一个非空集合(作为指标集), 我们考虑一族非空集合 $(A_\alpha)_{\alpha \in \Omega}$, 定义这些集合的笛卡尔积为

$$\prod_{\alpha \in \Omega} A_\alpha := \left\{ f : \Omega \rightarrow \bigcup_{\alpha \in \Omega} A_\alpha \mid \forall \alpha \in \Omega, f(\alpha) \in A_\alpha \right\}.$$

接下来, 我们将讨论如何构造任意一族某种代数结构的直积和直和.

B.2 群的直积与直和

记 Ω 为一个非空集合, $(G_\alpha)_{\alpha \in \Omega}$ 为一族群. 对任意 $\alpha \in \Omega$, 我们记 $*_\alpha$ 为 G_α 中的运算. 我们考虑这族群作为集合的笛卡尔积

$$\prod_{\alpha \in \Omega} G_\alpha,$$

并如下定义这个集合上的运算: 任取

$$f, g \in \prod_{\alpha \in \Omega} G_\alpha,$$

我们定义

$$(f * g)(\alpha) := f(\alpha) *_\alpha g(\alpha).$$

我们称

$$\left(\prod_{\alpha \in \Omega} G_\alpha, * \right),$$

为 $(G_\alpha)_{\alpha \in \Omega}$ 的**直积**, 通常记作

$$\bigotimes_{\alpha \in \Omega} G_\alpha.$$

这个群的幺元 e 满足对任意 $\alpha \in \Omega$, 有

$$e(\alpha) = e_\alpha \in G_\alpha,$$

其中 e_α 为 G_α 的幺元. 任取

$$f \in \bigotimes_{\alpha \in \Omega} G_\alpha,$$

其逆元 f^{-1} 满足对任意 $\alpha \in \Omega$, 有

$$f^{-1}(\alpha) = f(\alpha)^{-1}.$$

当 Ω 无限的时候, 我们可以考虑这个群中一类特殊的元素. 这些元素满足只有有限多个 $\alpha \in \Omega$ 的像不是幺元. 我们记

$$\left\{ f : \Omega \rightarrow \bigcup_{\alpha \in \Omega} G_\alpha \mid \forall \alpha \in \Omega, f(\alpha) \in G_\alpha \text{ 且只有有限多个 } \alpha \in \Omega \text{ 满足 } f(\alpha) \neq e_\alpha \right\}.$$

注意到这个集合关于群运算封闭, 且构成子群. 我们称之为 $(G_\alpha)_{\alpha \in \Omega}$ 的**直和**, 通常记作

$$\bigoplus_{\alpha \in \Omega} G_\alpha.$$

从以上定义就可以看出, 当 Ω 有限的时候, 群的直积与直和没有区别. 只有当 Ω 无限的时候, 二者才会有不同.

B.3 环/模的直积与直和

我们在介绍环和模的时候就可以看出,二者实际上都是在交换群附加一些其它的结构得到的. 因此,我们在定义环的直积或者模的直积的时候,我们先考虑作为群的直积,然后只需要用类似的方法将这个附加的结构延申到这个群的直积上得到一个环或者模即可. 考虑环和模中零元的性质,关于加法群的直和就给出了环的直和或者模的直和.

附录 C 尝试在给定域之间的所有同态的集合上构造运算

我们之前讨论过给定群之间的同态集合上的代数结构, 曾有如下结论

- (i) 任给群 G 和交换群 H , 我们知道 $\text{Hom}(G, H)$ 关于如下乘法运算构成群: 任取 $\phi, \psi \in \text{Hom}(G, H)$, 任取 $g \in G$, 定义

$$(\phi + \psi)(g) = \phi(g) + \psi(g),$$

注意到这个运算给出了 $\text{Hom}(G, H)$ 上一个加法群结构;

- (ii) 我们令 $G = H = M$ 为某个加法交换群, 考虑 M 的自同态的集合 $\text{End}(M)$, 在之前的加法运算基础上, 我们还可以有一个复合运算, 由此我们在 $\text{End}(M)$ 上得到了一个幺环结构;
- (iii) 任取 M 和 N 两个交换群, 设 M 和 N 上有某个幺环 R 上的模结构, 则加法群 $\text{Hom}(M, N)$ 中有一个由 R -模同态构成的子群 $\text{Hom}_R(M, N)$ 上边有一个 $Z(R)$ -模结构, 其中 $Z(R)$ 为 R 的中心. 这个结论的一个例子就是一个域 F 的两个线性空间 V 和 W 之间所有线性映射的集合 $\text{Hom}_F(V, W)$ 也是 F -线性空间.

如果我们试图对域之间的同态的集合考虑类似的问题, 则会遇到一些问题. 任取 F 和 E 两个域, 记 $\text{Hom}(F, E)$ 为所有从 F 到 E 的域同态的集合, 任取 $\phi, \psi \in \text{Hom}(F, E)$, 我们尝试对任意 $a \in F$ 定义:

$$(\phi + \psi)(a) = \phi(a) + \psi(a).$$

注意到这个运算和域上的加法相容, 但是当我们考虑乘法之后就出问题了. 任取 $a, b \in F$, 我们有

$$(\phi + \psi)(ab) = \phi(ab) + \psi(ab) = \phi(a)\phi(b) + \psi(a)\psi(b).$$

另一方面

$$(\phi + \psi)(a)(\phi + \psi)(b) = \phi(a)\phi(b) + \phi(a)\psi(b) + \psi(a)\phi(b) + \psi(a)\psi(b).$$

注意到如果令 $\phi = \psi$, $a = b = 1_F$, 则如果 $\phi + \psi$ 是域同态, 则有 $\text{Ch}F = \text{Ch}E = 2$. 然而

$$(\phi + \phi)(a) = 2\phi(a) = 0,$$

因此 $\phi + \phi$ 不是域同态.

我们下边把条件放宽, 考虑 F 到 E 的环同态, 继续以上的讨论, 但后续我们还需要

$$\phi(a)\psi(b) + \psi(a)\phi(b) = 0$$

令 $b = 1_F$, 则有

$$\phi(a) = -\psi(a),$$

另一方面, 考虑 $\text{Ch}E = 2$, 我们有

$$\phi(a) = -\phi(a),$$

因此对任意 $a \in F$, 我们有:

$$\phi(a) = \psi(a).$$

所以

$$\text{Hom}(F, E) = \{\mathbf{0}, \phi\}.$$

其中 $\mathbf{0}$ 为将所有元素送到 0_E 的环同态映射. 由此我们得到一个加法群结构. 注意到为了得到这个结构, 我们需要 F 和 E 满足一些必要条件.

实际上我们可以把以上讨论推广到对稍微一般一些的环的讨论中. 例如, 我们考虑 $\mathbb{Z}$, 实际上

$$\text{End}(\mathbb{Z}) = \{\mathbf{0}, \mathbf{1}\}.$$

其中 $\mathbf{0}$ 将所有整数送到 0, $\mathbf{1}$ 将任意 $n \in \mathbb{Z}$ 送到 n .

注意到之前对于域同态中关于 1 的像的条件的讨论对于 $\mathbb{Z}$ 也适用. 注意到之前定义的群同态之间的运算除了复合之外, 在这里都不在适用. 因此可以在 $\text{End}(\mathbb{Z})$ 上利用复合给出一个半群结构. 如果考虑自同构, 则 $\text{Aut}(\mathbb{Z}) = \{\mathbf{1}\}$.

另一方面, 我们考虑 $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, 则考虑 $\mathbb{F}_2$ 的环自同态集合, 考虑以上定义的计算, 则有群同构

$$\text{End}(\mathbb{F}_2) \cong \mathbb{F}_2.$$

另一方面 $\mathbb{F}_2$ 的域同构关于复合构成的群满足

$$\text{Aut}(\mathbb{F}_2) \cong \{e\}.$$

实际上 $\mathbb{F}_2$ 是一个素域, 因此 $\mathbb{F}_2$ 上的域同构必须是一个 $\mathbb{F}_2$ 上的恒等映射. 因此 $\text{Aut}(\mathbb{F}_2)$ 是一个平凡群.

参考文献

- [1] 邓少强, 朱富海, 抽象代数, 科学出版社.
- [2] 孟道骥, 陈良云, 史毅茜, 白瑞蒲, 抽象代数1—代数学基础, 科学出版社.
- [3] 聂灵沼, 丁石孙, 代数学引论, 高等教育出版社.
- [4] 柯斯特利金, 代数学引论, (张英伯, 牛凤文, 郭文彬译), 高等教育出版社
- [5] Michael Artin, *Algebra*, Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.
- [6] M. Artin, A. Grothendieck, J-L. Verdier, *Théorie des Topos et Cohomologie Étale des Schémas. s. Tome 1: Théorie des topos. Séminaire de Geometrie Algebrique du Bois-Marie 1963-1964 (SGA 4)*, Lecture Notes in Mathematics 269, Springer-Verlag Berlin Heidelberg, 1972.
- [7] M.F. Atiyah and L.G. MacDonald, *Introduction to Commutative Algebra*, Westview Press Reading, MA, 1969.
- [8] Nicolas Bourbaki, *Éléments de mathématique. Algèbre, Chapitres 1 à 3*, Springer, Berlin, Heidelberg, 1998
- [9] Nicolas Bourbaki, *Éléments de mathématique. Algèbre, Chapitres 4 à 7*, Springer, Berlin, Heidelberg, 2003
- [10] Nicolas Bourbaki, *Éléments de mathématique. Algèbre, Chapitres 8*, Springer, Berlin, Heidelberg, 2022
- [11] C. Chevalley, *On the Theory of Local Rings*, Ann. of Math. 44 (1943), 690708. URL <https://www.jstor.org/stable/1969105>.
- [12] David A. Clark, *A quadratic field which is Euclidean but not norm-Euclidean*, Manuscripta Math.83(1994), no.3-4, 327-330.
- [13] David A. Cox, *Galois Theory*, John Wiley and Sons, Inc., 2004.
- [14] David S. Dummit and Richard M. Foote, *Abstract Algebra*, John Wiley and Sons, Inc., 2003
- [15] S. Eilenberg and S. MacLane, *General theory of natural equivalences*, Trans. Amer. Math. Soc.58(1945), 231-294.
- [16] D. J. H. Garling, *A course in Galois theory*, Cambridge University Press, Cambridge, 1986
- [17] Malcolm Harper, $\mathbb{Z}[\sqrt{14}]$ is Euclidean, Canad. J. Math.56(2004), no.1, 55-70.
- [18] Nathan Jacobson, *Basic Algebra I*, Dover Publication, Garden City, New York, 2009
- [19] Nathan Jacobson, *Basic Algebra II*, Dover Publication, Garden City, New York, 2009
- [20] Israel Kleiner, *A History of Abstract Algebra*, Birkhäuser, Boston, 2007
- [21] William Judson LeVeque, *Topics in number theory. Vol. I, II.*, Dover Publications, Inc., Mineola, NY, 2002
- [22] S. MacLane, *Categories for the Working Mathematician*, Springer New York, NY 2013
- [23] E. Noether, *Idealtheorie in Ringbereichen*, Math. Annalen 83 (1921), 24 66. URL <https://eudml.org/doc/158855>. English translation by D. Berlyne <https://arxiv.org/abs/1401.2577>.
- [24] E. Riehl, *Category theory in context*, Dover Publications, 2016
- [25] Alexander Paulin, *Introduction to Abstract Algebra* (讲义) University of California, Berkeley
- [26] Charles C. Pinter, *A Book of Abstract Algebra*, Dover Publication, New York, 1990
- [27] Samir Siksek, *Introduction to Abstract Algebra* (讲义), University of Warwick