近世代数讨论班

曾梦辰

最后编译: 2023 年 7 月 26 日

目录

前言

本讲义是 2023 年 7 月作者举办的面向新二年级同学的近世代数讲义. 使用讲义的时候, 作者默认了读者学习了北师大的高等代数 I, II 课程.

部分参考书籍与我们推荐阅读的书籍如下: 对于中文书籍, [1] 是北师大近世代数课程的教材; 而 [2] 则是一本比较 “升级” 的教材, 介绍了更加现代的内容. 对于英文书籍, [3] 是标准的教材; [4] 是一本偏向入门的书籍, 但在一开始便以较高观点引入范畴等内容, 适合作为研究生级别教材学习; [5] 是著名的字典, 以大而全闻名, 适合用来查阅.

预备知识

我们具体列举希望读者掌握的预备知识如下.

首先, 讲义中会使用与北师大高等代数课程不同的记号 $\mathbb{Z}/n\mathbb{Z}$ 表示模 n 剩余类环, 并且会直接使用同余记号 mod 记属于同一等价类的元素.

接下来我们定义群环域.

定义 0.1. 设 X 是一个集合, 具有二元运算 $*: X \times X \to X$, 并有公理

G1 对 $a, b, c \in X$ 有 $(a * b) * c = a * (b * c)$;

G2 存在 $e \in X$, 使得对任意 $a \in X$ 有 $a * e = e * a = a$;

G3 对 $a \in X$, 存在 $b \in X$ 使得 $a * b = b * a = e$;

Ab 对任意 $a, b \in X$, 有 $a * b = b * a$;

如果 X 上还有另一二元运算 $\cdot : X \times X \to X$, 此时还有公理

R1 对 $a, b, c \in X$ 有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

R2 存在 $1 \in X$, 使得对任意 $a \in X$ 有 $a \cdot 1 = 1 \cdot a = a$;

R3 对任意 $a, b \in X$, 有 $a \cdot b = b \cdot a$;

Ds 对 $a, b, c \in X$ 有 $(a * b) \cdot c = a \cdot c * b \cdot c, a \cdot (b * c) = a \cdot b * a \cdot c$;

F 对任意 $a \in X \backslash \{e\}$, 存在 $b \in X$ 使得 $a \cdot b = 1$;

如果 X 满足 G1∼G3, 那么称 X 是一个**群**; 如果群 X 还满足 Ab, 则称 X 是一个 **Abel 群**. 如果 X 是 Abel 群, 且满足 R1 与 Ds, 那么称 X 是一个**环**; 如果环 X 满足 R2, 那么称 X **含幺**; 如果环 X 满足 R3, 那么称 X 是**交换环**. 如果 X 是交换环且满足 F, 那么称 X 是一个**域**.

记号 0.2. 习惯上, 一般对群的运算会采用两种记号: 一种是乘法记号 $\cdot$, 在实际书写中会直接省略这个点; 另一种是加法记号 $+$. 乘法记号会用在一般的群或者环满足 R1 与 Ds 的运算上, 加法记号会用在 Abel 群的运算上. 运用乘法记号时,

G3 中定义的逆元会记作 a^{-1}. 运用加法记号时, G2 中定义的加法零元记为 0, G3 中定义的逆元记为 $-a$. 对域而言, F 中定义的逆元记为 a^{-1}.

本讲义中如果不另外说明, 环都是含幺的.

习惯上会用一些特定的字母表示特定的代数结构, 例如群用 G 表示, 环用 R 表示, 交换环用 A 表示, 域用 F 或 k 表示.

然后是置换群的基本概念.

命题 0.3. *集合 $\{1,2,\cdots,n\}$ 到自身的双射构成群, 记为 S_n, 称为n* **阶置换群**.

记号 0.4. 对 $\sigma \in S_n$, 我们会用

$$\begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$$

来表示一个置换.

命题 0.5. *一个***轮换***定义为*

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$$

记为 $(a_1a_2\cdots a_n)$. 每一个置换都可以写成不相交轮换的乘积, 这种写法在不计次序的意义下唯一.

最后是关于矩阵的两种群.

定义 0.6. 域 k 上的 n 阶**一般线性群** $\mathrm{GL}_n(k)$ 定义为 k 上所有可逆的 n 阶矩阵构成的群. 域 k 上的 n 阶**特殊线性群** $\mathrm{SL}_n(k)$ 定义为 k 上所有行列式为 1 的 n 阶矩阵构成的群.

第一章　群与环的结构

1.1　同态

代数学研究代数对象及它们之间的态射. 这里的 “态射” 指的是保持代数运算结构的映射, 一般称为同态. 严格的定义如下:

定义 1.1.
- 设 G, G' 是两个群, 映射 $f: G \to G'$ 称为 (G 到 G' 的) 一个**群同态**, 如果 f 满足对任意 $a, b \in G$ 有 $f(ab) = f(a)f(b)$.
- 设 R, R' 是两个环, 映射 $f: R \to R'$ 称为 (R 到 R' 的) 一个**环同态**, 如果 f 满足
  (1) $f(a+b) = f(a) + f(b)$;
  (2) $f(ab) = f(a)f(b)$;
  (3) $f(1_R) = 1_{R'}$.
  其中 $1_R, 1_{R'}$ 分别是 R 与 R' 的乘法幺元.

在本讲义中, 我们会直接使用同态的相关运算性质而不加证明, 读者有疑问时不妨自行证明, 大部分的证明都与线性映射类似[1].

使用同态, 我们可以定义子群及子环:

定义 1.2. 设 X, X' 是群 (环), $X' \subset X$, 如果包含映射 $i: X' \to X$ 是群 (环) 同态, 那么称 X' 是 X 的子群 (环). 如果 $X' \neq \{e\}(\{0\}), X$, 那么称 X' 是真子群 (环).

定义 1.2 无外乎就是说 X' 在 X 的运算下成群或者环, 请读者自行证明这一点. 等价的一些检验方法有

[1] 实际上, 线性映射就是向量空间之间的同态.

- (对群) 关于除法封闭;
- (对环) 关于减法和乘法封闭, 包含幺元.

等价性在高等代数 I 课程中有过证明.

对于两个群或者环, 我们可以定义他们之间的同构, 这时它们在代数运算的意义下可以看作是一样的.

定义 1.3. 设 X, X' 是两个群或者环, 如果存在同态 $f : X \to X'$, $g : X' \to X$ 使得 $f \circ g = \mathrm{id}_{X'}$, $g \circ f = \mathrm{id}_X$, 那么称 X 与 X' 同构.

定义 1.4. 一个群 G 的所有自同构构成一个群, 称为 G 的自同构群, 记为 $\mathrm{Aut}(G)$.

习题 1.1. 如果 $f : X \to X'$ 是同态且是双射, 证明 f 是同构.

对同态, 我们会考虑同态的核.

定义 1.5. 对群而言, 设 $f : G \to G'$ 是一个群同态, 定义 f 的**核** $\ker f := f^{-1}(e)$. 对环而言, 设 $g : R \to R'$ 是一个环同态, 定义 g 的核为 $\ker g := g^{-1}(0)$.

核的定义与线性映射的核的定义是相同的. 同态的核是很重要的研究对象, 我们将要用核定义两种很重要的子集.

引理 1.6. *如果 $f : G \to G'$ 是同态, 那么 $\ker f$ 是 G 的子群.*

证明. 我们证明 $\ker f$ 在 G 的运算下成群. 这只需要证明 $\ker f$ 关于除法封闭. 对 $a, b \in \ker f$, 考虑 $f(ab^{-1})$. 由于 $f(b)f(b^{-1}) = f(bb^{-1}) = f(e)$, 而 $f(e) = f(ee) = f(e)f(e)$ 得出 $f(e) = e$, 所以 $f(b^{-1}) = (f(b))^{-1}$. 因此 $f(ab^{-1}) = f(a)(f(b))^{-1} = ee^{-1} = e$, 即 $ab^{-1} \in \ker f$. □

定义 1.7. 设 G 是一个群, 如果 $N \subset G$ 是一个同态的核, 那么称 N 是 G 的一个**正规子群**, 并记作 $N \lhd G$. 设 R 是一个环, 如果 $\mathfrak{a} \subset R$ 是一个同态的核, 那么称 $\mathfrak{a}$ 是 R 的一个**理想**.

同样的, 当 $N \neq \{e\}, G$, $\mathfrak{a} \neq \{0\}, R$ 时, 称 N 或 $\mathfrak{a}$ 为真正规子群或真理想.

命题 1.8 (正规子群的性质)**.** *设 $N \lhd G$, 那么对任意 $g \in G$ 及 $n \in N$, 有 $gng^{-1} \in N$.*

证明. 设 $N = \ker f$, 那么有 $f(gng^{-1}) = f(g)f(n)(f(g))^{-1} = f(n) = e$, 所以 $gng^{-1} \in \ker f = N$. □

命题 1.9 (理想的性质)**.** 设 $\mathfrak{a}$ 是 R 的理想.

(1) $\mathfrak{a}$ 是 R 的子加群;

(2) 对任意的 $a \in \mathfrak{a}$ 与 $r \in R$, 有 $ar, ra \in \mathfrak{a}$.

证明. (1) 环同态是两个环之间关于加法的群同态.
(2) 设 $\mathfrak{a} = \ker f$, 那么有 $f(ar) = f(a)f(r) = 0 \cdot f(r) = 0$, 因此 $ar \in \mathfrak{a}$. 同理 $ra \in \mathfrak{a}$. □

评注 1.10. 从以上命题可以看出, 我们定义的理想在一些教材中会被合理地称作 "双侧理想", 除此之外还有所谓的 "左理想" 和 "右理想", 不过我们目前不讨论这些精细的定义.

1.2 等价关系与商

我们熟悉如下的一个命题:

命题 1.11. 集合 X 上的一个等价关系 $\sim$ 唯一决定 X 的一个分划, 这个分划得到的等价类集称为 X 的**商集**, 记为 $X/\sim$.

我们在本节考虑两种等价关系: 首先是子群诱导的等价关系, 这种等价关系可以得到关于有限群子群阶数 (即元素个数) 的整除关系; 其次是正规子群和理想诱导的等价关系, 这种等价关系可以使得商集上具有良定义的代数运算.

1.2.1 Lagrange 定理

设群 G 具有子群 G'. 考虑关系 $a \sim b \iff a^{-1}b \in G'$. 我们验证这是一个等价关系:

自反性 $a^{-1}a = e \in G'$;

对称性 如果 $a^{-1}b \in G'$, 那么 $b^{-1}a = (ab^{-1})^{-1} \in G'$;

传递性 如果 $a^{-1}b, b^{-1}c \in G$, 那么 $a^{-1}c = a^{-1}bb^{-1}c \in G$.

因此 $\sim$ 给出 G 的一个分划. 这个分划具有如下的一个性质:

命题 1.12. $G/\sim$ 的每个等价类的基数均相等, 且都等于 $|G'|$.

证明. 设 C 是一个等价类, 我们建立 G' 到 C 的一个双射. 任取 $a \in C$, 定义

$$\begin{aligned}\varphi : G' &\to C\\ g &\mapsto ag\end{aligned}$$

首先这个映射是良定义的, 因为有 $a^{-1}ag = g \in G'$. 其次这个映射一定是单射, 因为 $ag = ag' \implies g = g'$. 最后这个映射一定是满射, 因为对任意 $b \in C$, 设 $a^{-1}b = g'$, 那么就有 $b = aa^{-1}b = ag'$. 因此 φ 是一个双射, 有 $|C| = |G'|$. $\square$

通过命题 1.12 的证明, 我们可以看出 $G/\sim$ 的每一个等价类都由 G 中的一个元素左乘 G' 中所有元素得到. 于是我们定义

定义 1.13. 定义 G' 的一个**左陪集**为 $aG' := \{ag' \in G |\ g' \in G'\}$.

将等价关系与商集翻译称陪集的语言就是

命题 1.14. *左陪集 aG' 与 bG' 相等当且仅当 $a^{-1}b \in G'$.*

命题 1.15. *设 G' 是 G 的子群, 那么适当选取代表元, G 有陪集分解 $G = \coprod aG'$.*

当 G 是有限群时, 通过陪集分解, 我们能立刻得到

定理 1.16 (Lagrange)**.** *设 G 是有限群, G' 是 G 的子群, 那么 G' 的阶整除 G 的阶.*

与左陪集相同, 我们也可以定义右陪集:

定义 1.17. 定义 G' 的一个**右陪集**为 $G'a := \{g'a \in G |\ g' \in G'\}$.

命题 1.18. *右陪集 $G'a$ 与 $G'b$ 相等当且仅当 $ab^{-1} \in G'$.*

命题 1.19. *设 G' 是 G 的子群, 那么适当选取代表元, G 有陪集分解 $G = \coprod G'a$.*

1.2.2 商群与商环

首先, 我们证明正规子群的陪集类上将会存在群的乘法.

定理 1.20. *设群 G 与子群 $N \subset G$ 满足对任意 $g \in G$ 及 $n \in N$ 有 $gng^{-1} \in N$, 那么 N 的陪集类构成一个群, 记为 G/N, 并且 $\pi : G \to G/N, a \mapsto aN$ 构成典范同态.*

证明. 我们在 G/N 上定义乘法

$$(aN, bN) \mapsto abN$$

一旦证明这个乘法是良定义的, 将立刻得到 φ 是同态. 如果 $c \in aN, d \in bN$, 有

$$(ab)^{-1}cd = b^{-1}a^{-1}cd = b^{-1}(a^{-1}c)b(b^{-1}d) \in N$$

所以乘法是良定义的. G/N 显然在这个乘法下成群. □

推论 1.21. *$N \lhd G$ 当且仅当对任意 $g \in G$ 及 $n \in N$, 有 $gng^{-1} \in N$.*

习题 1.2. 证明正规子群的左陪集与右陪集相等, 即 $N \lhd G$ 时有 $aN = Na$.

对环而言, 也有类似结论, 证明也是类似的.

定理 1.22. *设 $\mathfrak{a}$ 是环 R 的子加群, 满足命题 1.9 中的性质, 那么 $\mathfrak{a}$ 的陪集类构成一个环, 记为 $R/\mathfrak{a}$, 并且 $\pi : R \to R/\mathfrak{a}, r \to r + \mathfrak{a}$ 构成典范同态.*

推论 1.23. *命题 1.9 给出了子加群为理想的充分必要条件.*

关于商结构, 我们有如下的一些定理.

定理 1.24 (第一同构定理)**.** *设 $\varphi : G \to H$ 是群的满同态, 那么一定有 $G/\ker\varphi$ 与 H 同构, 且同构映射 $\overline{\varphi}$ 使得以下图表交换*

$$\begin{tikzcd}
G \arrow[d, "\pi"] \arrow[dr, "\varphi"] & \\
G/\ker\varphi \arrow[r, dashed, "\overline{\varphi}"] & H
\end{tikzcd}$$

证明. 定义映射

$$\begin{aligned} \overline{\varphi} : G/\ker\varphi &\to H \\ a\ker\varphi &\mapsto \varphi(a) \end{aligned}$$

对 $b \in G$ 满足 $a\ker\varphi = b\ker\varphi$, 有 $b^{-1}a \in \ker\varphi$,

$$b\ker\varphi \mapsto \varphi(b) = \varphi(b)\varphi(b^{-1}a) = \varphi(a)$$

从而 $\overline{\varphi}$ 是良定义的, 并且易于发现是同态. 并且由定义, $\overline{\varphi}$ 使得上述图表交换, 从而由 φ 满知 $\overline{\varphi}$ 是满射. 最后我们说明 $\overline{\varphi}$ 是单射, 如果 $\varphi(a) = \varphi(b)$, 那么 $\varphi(a^{-1}b) = e$, 从而 $a^{-1}b \in \ker\varphi$, 即 $a\ker\varphi = b\ker\varphi$. □

定理 1.25 (对应定理)**.** *设 $f: G \to G'$ 是满的群同态, 那么对 G 包含 $\ker f$ 的子群 H, 及 G' 的子群 H', 有*

(1) $f(H)$ 是 G' 的子群, $f^{-1}(H')$ 是 G 包含 $\ker f$ 的子群;

(2) G 包含 $\ker f$ 的子群与 G' 的子群通过 f 一一对应;

(3) 如果 $H \lhd G$, 那么也有 $f(H) \lhd G'$;

(4) 如果进一步地 G 是有限群, 那么 $|H| = |\ker f||f(H)|$.

证明. (1) 注意到 $f(h_1)(f(h_2))^{-1} = f(h_1 h_2^{-1})$ 即可.
(2) 只需验证不同的子群对应的子群不同. 设 $H_1 \neq H$ 是 G 包含 $\ker f$ 的子群, 那么至少存在两个陪集 $a\ker f$ 与 $b\ker f$ 分属于两个子群, 此时 $f(a) \neq f(b)$. 反过来也同理.
(3) 设 $h \in H$, 那么对 $f(a) \in G'$ (f 满) 有 $f(a)f(h)(f(a))^{-1} = f(aha^{-1}) \in f(H)$, 从而 $f(H) \lhd G'$.
(4) 由第一同构定理即得. □

习题 1.3. 陈述并证明环的第一同构定理和对应定理. (注意对应定理是理想间的对应)

1.3 乘积

我们分别讨论群和环上的乘积结构.

1.3.1 乘积群

设 G, G' 是两个群, 一种简单的构造新群的方式是考虑它们的 Descartes 积, 即在 $G \times G'$ 上定义乘法

$$(g_1, g_1') \cdot (g_2, g_2') = (g_1 g_2, g_1' g_2')$$

容易验证这个乘法使得 $G \times G'$ 成为一个群.

定义 1.26. 上述构造称为 G 与 G' 的**直积**.

而另一种更有趣且更重要的构造是子群间的乘积.

定理 1.27. *设 H,K 是 G 的子群, 定义映射 $f: H\times K\to G,(h,k)\mapsto hk$. 记 f 的像集为 HK.*

(1) *f 是单射当且仅当 $H\cap K=\{e\}$;*

(2) *f 是同态当且仅当 H 中所有的元素与 K 中所有元素交换;*

(3) *如果 H 是 G 的正规子群, 那么 HK 是 G 的子群;*

(4) *f 是 $H\times K$ 到 G 的同构, 当且仅当 $HK=G$, $H\cap K=\{e\}$ 且 H,K 为 G 的正规子群.*

证明. (1) $h_1k_1=h_2k_2 \iff h_1h_2^{-1}=k_2k_1^{-1}\in H\cap K$, 那么就有 f 是单射当且仅当 $H\cap K=\{e\}$.
(2) 注意到 $f(h_1h_2,k_1k_2)=h_1h_2k_1k_2$, $f(h_1,k_1)f(h_2,k_2)=h_1k_1h_2k_2$, 两者相等当且仅当 $h_2k_1=k_1h_2$, 由任意性, 此即 H,K 中所有元素交换.
(3) 只需验证 HK 中的元素关于除法封闭. 取 h_1k_1,h_2k_2, 有

$$h_1k_1(h_2k_2)^{-1}=h_1((k_1k_2^{-1})h_2^{-1}(k_2k_1^{-1}))(k_1k_2^{-1})\in HK$$

(4) 又假设可知 f 满且单, 从而是双射. 而 $H,K\lhd G$, 考虑 $hkh^{-1}k^{-1}$, 有

$$(hkh^{-1})k^{-1}=h(kh^{-1}k^{-1})\in H\cap K$$

所以 $hkh^{-1}k^{-1}=e$, 即 h,k 交换.[2] 因此 f 是一个同态, 而且是双射, 从而是同构. □

1.3.2 环上的乘积

我们首先类似群定义环的直积.

定义 1.28. 两个环的**直积**是它们的 Descartes 积及其上自然的运算.

设 $\mathfrak{a},\mathfrak{b}$ 是环 R 的理想. 定义一个新的理想 $\mathfrak{a}+\mathfrak{b}=\{a+b\in R|\ a\in\mathfrak{a},b\in\mathfrak{b}\}$, 容易证明这确实是一个理想. 类似于定理 1.27, 我们可以定义理想的直和.

定义 1.29. 设 $\mathfrak{a},\mathfrak{b}$ 是环 R 的理想. 如果 $\mathfrak{a}\cap\mathfrak{b}=\{0\}$, $\mathfrak{a}+\mathfrak{b}=R$, 那么称 R 是 $\mathfrak{a}$ 与 $\mathfrak{b}$ 的**直和**, 并记 $R=\mathfrak{a}\oplus\mathfrak{b}$.

习题 1.4. 证明当 $R=\mathfrak{a}\oplus\mathfrak{b}$ 时, $\mathfrak{a}$ 与 $\mathfrak{b}$ 均包含单位元.

[2]这个技巧叫做取**交换子**.

按照习题 1.4 中的结论, $\mathfrak{a},\mathfrak{b}$ 可以看成是环. 那么按照定理 1.27, 我们有 $\mathfrak{a}\times\mathfrak{b}$ 与 $\mathfrak{a}\oplus\mathfrak{b}$ 作为加群同构, 并且这个同构可以延拓为环同构. 因此, 我们认为两个环的直积和直和是一样的.

环的直积有一个重要的结论, 即中国剩余定理.

定义 1.30. 设 $\mathfrak{a},\mathfrak{b}$ 是交换环 A 的理想, 如果 $\mathfrak{a}+\mathfrak{b}=A$, 那么称 $\mathfrak{a},\mathfrak{b}$ **互素**.

定理 1.31 (中国剩余定理)**.** *设交换环 A 的理想 $\mathfrak{a},\mathfrak{b}$ 互素, 那么有同构 $A/(\mathfrak{a}\cap\mathfrak{b})\simeq A/\mathfrak{a}\times A/\mathfrak{b}$.*

证明. 定义同态

$$\begin{aligned}\varphi: A &\to A/\mathfrak{a}\times A/\mathfrak{b}\\ a &\mapsto (a+\mathfrak{a},a+\mathfrak{b})\end{aligned}$$

对 $(x+\mathfrak{a},y+\mathfrak{b})$, 取 $a+b=1$ 及 $z=ay+bx$, 就有

$$\begin{aligned}z\equiv bx\equiv x &\pmod{\mathfrak{a}}\\ z\equiv ay\equiv y &\pmod{\mathfrak{b}}\end{aligned}$$

从而 $\varphi(z)=(x+\mathfrak{a},y+\mathfrak{b})$, 即 φ 是满射. 另一方面, $a\in\ker\varphi$ 当且仅当 $a\in\mathfrak{a}\cap\mathfrak{b}$, 所以第一同构定理给出了 $A/(\mathfrak{a}\cap\mathfrak{b})\simeq A/\mathfrak{a}\times A/\mathfrak{b}$. □

需要指出的是, 上面有关环的定义与结论都不局限在两项. 特别地, 中国剩余定理也有一般的有限多个理想的形式, 我们陈述整数的版本, 并直接给出一个常用的计算公式:

定理 1.32. *设 $n_1,\cdots,n_m$ 是两两互素的整数, 那么同余方程组*

$$\begin{aligned}x\equiv a_1 &\pmod{n_1}\\ x\equiv a_2 &\pmod{n_2}\\ &\cdots\\ x\equiv a_m &\pmod{n_m}\end{aligned}$$

有模 $N=n_1\cdots n_m$ 意义下的唯一解

$$x\equiv\sum_{i=1}^{m}a_i\frac{N}{n_i}l_i \pmod{N}$$

其中 l_i 满足 $l_iN/n_i\equiv 1 \pmod{n_i}$.

证明是直接的, 代入计算即可.

1.4 生成关系

首先我们定义由一个集合生成的子群.

定义 1.33. 设 G 是一个群, 集合 $X \subset G$, 称X **生成的子群**为

$$\langle X\rangle := \{a_1^{\varepsilon_1}a_2^{\varepsilon_2}\cdots a_n^{\varepsilon_m} \mid a_i \in X, \varepsilon_i = \pm 1, i = 1, 2\cdots, m, m \in \mathbb{N}\}$$

其中的 a_i 一般有重复. 如果 $G = \langle X\rangle$, 则称 G **由** X **生成**. 当 X 是有限集时, 称 G 是**有限生成群**.

我们考虑由一个元素生成的群.

定义 1.34. 设 $C = \langle a\rangle$, 那么称 C 是**循环群**.

循环群的结构是简单的.

命题 1.35. *设 C 是循环群, 那么 C 的阶数为无穷大时, C 同构于 $\mathbb{Z}$; C 的阶数为 n 时, C 同构于 $\mathbb{Z}/n\mathbb{Z}$.*

定义 1.36. 设 G 是群, $a \in G$, 那么定义 a 的**阶**为 $\langle a\rangle$ 的阶.

由 Lagrange 定理可以得到:

推论 1.37. *有限群中元素的阶整除群的阶.*

定理 1.38 (Fermat 小定理)**.** *设 p 是素数, 那么对整数 a 有 $a^p \equiv a \pmod p$.*

习题 1.5. 证明费马小定理.

然后我们来定义一个集合生成的理想. 为了方便, 我们只讨论交换环.

定义 1.39. 设 X 是交换环 A 的子集, 那么 X 生成的理想定义为

$$\langle X\rangle = \left\{\sum_{i=1}^{m} r_i a_i \,\middle|\, r_i \in A, a_i \in X, i = 1, 2, \cdots, m, m \in \mathbb{N}\right\}$$

当 X 有限时, 称 $\langle X\rangle$ 是有限生成的.

关于理想的有限生成有两个等价的条件. 第一个是

定义 1.40. 称交换环 A 满足**升链条件**, 如果对于任意上升的理想链 $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$, 都存在正整数 n 使得 $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots$.

关于第二个条件, 我们需要回忆偏序关系.[3]

定义 1.41. 非空集合 P 上的一个**偏序关系** $\prec$ 满足传递性, 自反性与反对称性, 即

(1) $a \prec b, b \prec c \implies a \prec c$;

(2) $a \prec a$;

(3) $a \prec b, b \prec a \implies a = b$.

一个具有偏序关系的集合称为**偏序集**. 偏序集 P 上的一个**极大元** m 满足对任意 $a \in P$, 如果 $m \prec a$, 那么 $a = m$.

命题 1.42. *设 A 是交换环, 则如下三个命题等价:*

(1) A 满足升链条件;

(2) A 中任意理想的集合存在极大元 (以包含关系为偏序);

(3) A 中任意的理想都是有限生成的.

证明. (1) $\implies$ (2): 用反证法, 假设 $\mathscr{I}$ 是 A 中一些理想构成的非空集合, 且其中没有极大元. 我们归纳地构造一列理想列: 取 $\mathfrak{a}_1 \in \mathscr{I}$; 假定 $\mathfrak{a}_n$ 已经构造, 那么由于 $\mathfrak{a}_n$ 不是极大元, 存在 $\mathfrak{a}_{n+1}$ 使得 $\mathfrak{a}_n \subsetneqq \mathfrak{a}_{n+1}$. 因此 A 中存在严格上升的理想列

$$\mathfrak{a}_1 \subsetneqq \mathfrak{a}_2 \subsetneqq \cdots \subsetneqq \mathfrak{a}_n \subsetneqq \cdots$$

这与升链条件矛盾.

(2) $\implies$ (3): 取理想集

$$\mathscr{F} = \{\langle X \rangle \mid X \subset A \text{ 有限}\}$$

那么由假设, $\mathscr{F}$ 有极大元, 设为 $\langle x_1, \cdots, x_n \rangle$. 断言 $A = \langle x_1, \cdots, x_n \rangle$. 如若不然, 存在 $x \in A$ 使得 $x \notin \langle x_1 \cdots, x_n \rangle$, 那么 $\langle x_1, \cdots, x_n \rangle \subsetneqq \langle x_1, \cdots, x_n, x \rangle$, 这与 $\langle x_1, \cdots, x_n \rangle$ 的极大性矛盾. 所以 $A = \langle x_1, \cdots, x_n \rangle$ 是有限生成的.

(3) $\implies$ (1): 设 $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ 是上升的理想链, 取

$$\mathfrak{a} = \bigcup_{n \geq 1} \mathfrak{a}_n$$

[3] 如果读者跳过了 Nother 性这一节, 那么偏序关系可以在环的极大理想处学习.

容易验证 $\mathfrak{a}$ 是一个理想. 设 $\mathfrak{a} = \langle x_1, \cdots, x_m \rangle$. 那么每个 x_i 一定属于某个理想 $\mathfrak{a}_{n_i}$, 取 $N = \max\{n_i |\ i = 1, 2, \cdots, m\}$, 就有 $\langle x_1, \cdots, x_m \rangle \subset \mathfrak{a}_N$. 那么对任意 $n \geq N$, 都有

$$\langle x_1, \cdots, x_m \rangle = \mathfrak{a}_N \subset \mathfrak{a}_n \subset \mathfrak{a} = \langle x_1, \cdots, x_m \rangle$$

从而 $\mathfrak{a}_n = \mathfrak{a}_N$, 即 A 满足升链条件. □

定义 1.43. 如果交换环 A 满足升链条件, 那么称 A 是 **Noerther** 的.

1.5 例题与习题

例 1.1. 设 $p < q$ 是两个素数, 我们证明 pq 阶群 G 至多只有一个 q 阶子群. 假设 Q, S 是两个 G 的 q 阶子群, 由于素数阶群都是循环群, 所以他们的交为 $\{e\}$ (请读者证明这两个断言). 对任意 $q_1, q_2 \in Q$, 有 $q_1^{-1} q_2 \in S \implies q_1^{-1} q_2 = e$, 则 $q_1 = q_2$, 从而 Q 中的元素分属于不同的 S 的陪集中. 因此对 G 做陪集分解, G 至少有 q 个 S 的陪集, 从而 $|G| \geq |Q||S| = q^2 > pq$, 矛盾. 所以 G 至多有一个 q 阶子群.

例 1.2. 我们将在本例中计算 $\mathbb{Q}$ 的自同构群. 设 $f \in \operatorname{Aut} \mathbb{Q}$, 我们先验地给出 $f(1) = r (r \neq 0)$. 对于正整数 n, 通过归纳法可以得到 $f(n) = rn$. 而对负整数 m, 有

$$0 = f(0) = f(m) + f(-m) \implies f(m) = -f(-m) = -(-rm) = rm$$

对有理数 p/q, 我们有

$$qf(p/q) = \underbrace{f(p/q) + \cdots + f(p/q)}_{q\text{个}} = f(p) = pr$$

从而 $f(p/q) = r(p/q)$. 因此对所有 $x \in \mathbb{Q}$ 有 $f(x) = rx$. 注意到如果 $g(x) = sx$ 是另一个自同构, 那么有 $f \circ g(x) = rsx$. 从而有 $\operatorname{Aut} \mathbb{Q} \simeq \mathbb{Q}^*$, 即有理数乘法群.

例 1.3. 我们将在本例中证明第三同构定理, 以演示如何使用第一同构定理. 第三同构定理断言, 如果 H, N 是 G 的正规子群且 $N \subset H$, 那么有

$$\frac{G}{H} \simeq \frac{G/N}{H/N} \tag{1.1}$$

首先需要证明 $H/N \lhd G/N$, 这只需要注意到

$$(gN)(hN)(g^{-1}N) = N(ghg^{-1})NN = ghg^{-1}N \in H/N$$

即可. 而定义同态

$$\begin{aligned} \varphi : G/N &\to G/H \\ gN &\mapsto gH \end{aligned}$$

由于 $N \subset H$, 上述定义是良好的. 我们考虑 $\ker \varphi$, 有 $\varphi(gN) = H \iff g \in H$, 那么等价于 $gN \in H/N$. 所以 $\ker\varphi = H/N$, 第一同构定理给出 (1.1) 式.

例 1.4. 我们将在本例中讨论根式理想. 设 A 是交换环, $\mathfrak{a}$ 是 A 的理想. 定义 $\sqrt{\mathfrak{a}} = \{a \in A|\ a^n \in \mathfrak{a}, \exists n \in \mathbb{N}\}$. 我们证明 $\sqrt{\mathfrak{a}}$ 是 A 的理想. 首先对于 $a, b \in \sqrt{\mathfrak{a}}$, 设 $a^n \in \mathfrak{a}, b^m \in \mathfrak{a}$. 由于 A 是交换环, A 上二项式定理成立, 从而有

$$(a-b)^{m+n} = \sum_{i=0}^{m+n} (-1)^{m+n-i} \binom{m+n}{i} a^i b^{m+n-i} \tag{1.2}$$

在以上 $m+n$ 个求和项中, $0 \le i \le n$ 时 $b^{m+n-i} \in \mathfrak{a}$, $n+1 \le i \le m+n$ 时 $a^i \in \mathfrak{a}$, 所以求和式 $(a-b)^{m+n}$ 在 $\mathfrak{a}$ 中, 即 $\sqrt{\mathfrak{a}}$ 是 A 的子加群. 其次对于 $a \in \sqrt{\mathfrak{a}}, r \in A$, 有 $(ra)^n = r^n a^n \in \sqrt{\mathfrak{a}}$. 综上可知 $\sqrt{\mathfrak{a}}$ 是 A 的理想.

例 1.5. 我们将在本例讨论环的直和作为余积的性质. 设 $\mathfrak{a}, \mathfrak{b}$ 是环 R 的理想, $R = \mathfrak{a} \oplus \mathfrak{b}$. 假设对环 A 有同态 $f : \mathfrak{a} \to A, g : \mathfrak{b} \to A$, 那么存在唯一的同态 $\varphi : R \to A$ 使得下图交换

$$\begin{tikzcd}
\mathfrak{a} \arrow[dr, "i_1"] \arrow[ddr, "f"'] & & \mathfrak{b} \arrow[dl, "i_2"'] \arrow[ddl, "g"] \\
& R \arrow[d, dashed, "\varphi"] & \\
& A &
\end{tikzcd}$$

图中 i_1, i_2 分别是 $\mathfrak{a}, \mathfrak{b}$ 的典范嵌入映射. 事实上, 对 $r = a + b$, 定义 $\varphi : r \mapsto f(a) + g(b)$. 那么显然 φ 使得图表交换, 只需说明唯一性. 假设 ψ 也使图表交换,

那么考虑 $\varphi-\psi$, 对 $r=a+b$ 有

$$\begin{aligned}\varphi(r)-\psi(r)&=f(a)+g(b)-\psi(a)-\psi(b)\\&=f(a)-\psi(i_1(a))+g(b)-\psi(i_2(b))\\&=f(a)-f(a)+g(b)-g(b)\\&=0\end{aligned}$$

因此 $\varphi=\psi$, 即同态是唯一的.

习题 1.6. 证明在偶数阶群中, 方程 $x^2=e$ 有偶数个解.

习题 1.7. 证明群 G 是 Abel 群当且仅当 $g\to g^{-1}$ 是 G 的自同构, 即 $G\to G$ 的同构.

习题 1.8. 设 G 是群, $Z(G)$ 是 G 的**中心**, 即 $Z(G):=\{z\in G|\ \forall g\in G: gz=zg\}$.

(1) $Z(G)$ 是 G 的正规子群;

(2) $G/Z(G)$ 同构于 G 的自同构群 $\mathrm{Aut}(G)$ 的子群. [提示: 考虑内自同构, 即每个 g 诱导了一个 $\mathrm{int}_g: G\to G, x\mapsto gxg^{-1}$.]

习题 1.9. 设 R_1,R_2 是两个环, $p_1: R_1\times R_2\to R_1, p_2: R_1\times R_2\to R_2$ 是典范投影映射. 假设对环 A 存在同态 $f: A\to R_1, g: A\to R_2$, 那么存在唯一的同态 $\varphi: A\to R_1\times R_2$ 使得下图交换

$$\begin{tikzcd} & A \arrow[dl, "f"'] \arrow[d, dashed, "\varphi"] \arrow[dr, "g"] & \\ R_1 & R_1\times R_2 \arrow[l, "p_1"] \arrow[r, "p_2"'] & R_2 \end{tikzcd}$$

习题 1.10. 设 A 是交换环, X 是 A 的非空子集, 定义 $\mathrm{Ann}(X)=\{a\in A|\ \forall x\in X: ax=0\}$. 证明 $\mathrm{Ann}(X)$ 是 A 的理想.

习题 1.11. 设 A 是交换环, $\mathfrak{a},\mathfrak{b}$ 是 A 的理想, 定义**乘积理想**

$$\mathfrak{ab}=\left\{\sum_{i=1}^m a_ib_i\ \middle|\ a_i\in\mathfrak{a}, b_i\in\mathfrak{b}, i=1,2\cdots,m, m\in\mathbb{N}\right\}$$

证明 $\mathfrak{ab}\subset\mathfrak{a}\cap\mathfrak{b}$, 并给出严格包含的例子, 并进一步证明 $\sqrt{\mathfrak{ab}}=\sqrt{\mathfrak{a}\cap\mathfrak{b}}$.

习题 1.12. 设 R 是 Noether 环, $\mathfrak{a}$ 是 R 的理想, 证明 $R/\mathfrak{a}$ 也是 Noether 环.

第二章　群的更多性质

我们在本章讨论群的更多的性质. 我们关心群的作用, 以及有限群的分类. 在此之中我们遇到的最重要的定理将会是三条 Sylow 定理.

2.1　群作用

我们在接下来几节中关注群作用和群作用的一些应用. 首先给出群作用的定义

定义 2.1. 群 G 在一个集合 S 上的**作用**是 G 到 S 的置换群的一个同态 $G \to \mathrm{Aut}_{\mathsf{Set}}(S)$[1]. 当同态是单态射时, 称作用是**忠实**的.

群作用的等价定义是

定义 2.2. 群 G 在集合 S 上的一个作用是为每个 $g \in G$ 赋予一个映射 $\varphi_g : S \to S$, 满足

(1) $\varphi_g \circ \varphi_h = \varphi_{gh}$;

(2) $\varphi_e = \mathrm{id}_S$.

记号 2.3. 为简单起见, 在不会引起混淆时一般将 $\varphi_g(a)$ 记作 ga.

最简单的群作用是群在自身的作用, 这样的作用有两种.

定义 2.4. 群 G 中的元素 a 在 G 自身的一个**左平移**为 $g \mapsto ag$; a 在 G 自身的一个**内自同构**或**共轭作用**为 $g \mapsto aga^{-1}$.

习题 2.1. 验证左平移和内自同构都是群作用.

[1]这个记号表示 S 的排列, 与一个群的自同构群区分.

通过群作用, 我们可以得到如下一条基本的定理

定理 2.5 (Cayley)**.** *任意有限群都同构于某个置换群的子群.*

证明. 考虑 G 的左平移. 对 $a, b \in G$, $ag = bg$ 可以推出 $a = b$, 所以不同的元素给出不同的变换. 因此 G 是忠实的, 从而 G 同构于 $\mathrm{Aut}_{\mathsf{Set}}(G)$ 的某个子群. 将 G 的元素一一对应于 $\{1, \cdots, n\}$ (n 为 G 的阶), 那么 $\mathrm{Aut}_{\mathsf{Set}}(G) \simeq S_n$, 可以得到 G 同构于 S_n 的子群. □

定义 2.6. 设群 G 作用在 S 上, 定义 S 上的等价关系 $\sim$ 为 $a \sim b$ 当且仅当存在 $g \in G$ 使得 $ga = b$. 定义该群作用的**轨道**为 $\sim$ 的等价类. 如果 S 上仅有一条轨道, 那么称群作用是**可迁**的.

定义 2.7. 设群 G 作用在 S 上, $s \in S$. 定义 s 的**稳定化子**为 $G_s := \{g \in G | \ gs = s\}$.

引理 2.8. *设群 G 作用在 S 上, $s \in S$. 如果 $t = gs$, 那么 $G_t = gG_sg^{-1}$.*

证明. 平凡计算. □

命题 2.9 (计数公式)**.** *设有限群 G 作用在有限集合 S 上, $s \in S$. 用 O_s 记 s 所在的轨道, 那么有 $|O_s||G_s| = |G|$.*

证明. 轻微滥用记号, 用 G/G_s 表示 G_s 所有左陪集的集合. 定义映射

$$\begin{aligned} \varphi : O_s &\to G/G_s \\ t = gs &\mapsto gG_s \end{aligned}$$

我们验证上述映射是良定义的: 如果另有 $t = g's$, 那么 $g's = gs \implies g^{-1}g' \in G_s$, 即 $gG_s = g'G_s$. 显然 φ 是满射. 如果 $gG_s = g'G_s$, 那么可以得出 $g^{-1}g' \in G_s$, 从而 $gs = g's$, 即 φ 是单射. 因此 $|O_s||G_s| = |G/G_s||G_s| = |G|$. □

我们给出共轭作用的一些应用. 共轭作用的轨道也称为**共轭类**, 在有限群中, 将所有共轭类的元素个数相加可以得到群的阶数, 这样我们就得到了

命题 2.10. *有限群 G 的**类方程**为*

$$|G| = \sum_{O\text{是共轭类}} |O|$$

特别地, 单位元的共轭类 $|O_e| = 1$, 从而方程也能写成

$$|G| = 1 + \sum_{O\text{是}e\text{以外的共轭类}} |O|$$

定义 2.11. 有限群 G 称为**p–群**, 如果 G 的阶数是 p 的方幂.

我们通过类方程给出一些简单的 p–群的结构. 回忆我们在习题 1.8 中定义了群的中心, 它包含了与群中所有元素交换的元素.

命题 2.12. *p–群的中心至少有 p 个元素.*

证明. 设 G 是 p–群. 注意到中心 $Z(G)$ 中的元素的共轭类仅包含本身, 所以类方程写作

$$|G| = \sum_{x\in Z(G)} 1 + \sum_{O\text{是}G\setminus Z(G)\text{中元素的共轭类}} |O| \tag{2.1}$$

注意到 $Z(G)$ 之外的元素轨道长度一定大于 1, 而由计数公式, 轨道长度一定整除 $|G| = p^n$, 所以长度一定是 p 的倍数. 因此 $\sum_{O\text{是}G\setminus Z(G)\text{中元素的共轭类}} |O|$ 被 p 整除. 而 (2.1) 左端为 p^n, 所以 $\sum_{x\in Z(G)} 1$ 被 p 整除, 且至少是 p, 即 $|Z(G)| \geq p$. □

对于 p^2 阶群, 还有更强的结论

命题 2.13. *p^2 阶群是 Abel 群.*

证明. 设群 G 满足 $|G| = p^2$. 由命题 2.12, $|Z(G)| \geq p$, 从而 $|Z(G)| = p$ 或 $|Z(G)| = p^2$. 对于后一种情况, 命题得证. 对于前一种情况, 我们考虑一个 $x \notin Z(G)$, 取 $Z_x = \{y \in G|\ xy = yx\}$[2], 容易验证 Z_x 是 G 的一个子群. 又因为 $x \notin Z(G)$, 所以 Z_x 真包含 $Z(G)$, 从而 $|Z_x| = p^2$. 而这说明 x 与 G 中所有元素交换, 有 $x \in Z(G)$, 矛盾. 因此 G 是 Abel 群. □

习题 2.2. 证明 p^2 阶群是循环群或者是两个 p 阶群的直积.

2.2 单群

定义 2.14. 如果群 G 没有非平凡的正规子群, 那么称 G 为**单群**.

[2]这个群叫做中心化子.

比较简单的情况是 Abel 群的情况.

命题 2.15. *Abel 群 G 是单群当且仅当 G 是素数阶循环群.*

证明. 注意到 Abel 群的任意子群都是正规的, 所以 G 是单群等价于 G 没有非平凡子群. 由 Lagrange 定理, G 是素数阶循环群时 G 没有非平凡子群. 反过来, $\mathbb{Z}$ 不是单群; 如果 G 不是循环群, 那么存在 $g \in G \backslash \{e\}$ 使得 $\langle g \rangle \subsetneqq G$; 如果 G 是循环群而不是素数阶的, 设 $|G| = mn$, $G = \langle g \rangle$, 那么 $\langle g^m \rangle \subsetneqq G$. 综上可知命题成立. $\square$

而对一般的有限群来说, 另一个常见的结论是

定理 2.16. *设 $n \geq 5$, 那么交错群 A_n 是单群.*

我们首先需要两个引理.

引理 2.17. *A_n 由 3–循环生成.*

证明. A_n 中的元素都可以写成偶数个 2–循环的乘积. 而对两个 2–循环 $(ij), (rs)$ 有 $(ij)(rs) = (ijr)(jrs)$, 所以 3–循环生成了 A_n. $\square$

引理 2.18. *$n \geq 5$ 时 A_n 中的 3–循环两两共轭.*

证明. 设 $(ijk), (i'j'k')$ 是两个 3–循环, 那么存在一个置换 σ 使得 $\sigma(i) = i', \sigma(j) = j', \sigma(k) = k'$. 如果 σ 是偶置换, 那么就有 $\sigma(ijk)\sigma^{-1} = (i'j'k')$, 从而 $(ijk), (i'j'k')$ 共轭. 如果 σ 是奇置换, 由于 $n \geq 5$, 存在与 i, j, k 不同的 r, s, 那么用 $\sigma \cdot (rs)$ 代替 σ, 仍然得到 $(ijk), (i'j'k')$ 共轭. $\square$

定理 2.16 的证明. 由前面的两个引理, 我们只需要证明 A_n 的任意非平凡正规子群 N 均包含一个 3–循环即可.

设 σ 是 id 之外不动点最多的置换. 考虑 $\langle \sigma \rangle$ 作用下的轨道, 那么存在轨道其中含有超过一个元素. 假设除了一个元素构成的轨道外, 所有轨道都只有两个元素. 由于 σ 是偶置换, 所以至少有两个这样的轨道, 那么 $\sigma = (ij)(rs)\cdots$. 设 $k \neq i, j, r, s$, $\tau = (krs)$, 取 $\sigma' = \tau\sigma\tau^{-1}\sigma^{-1}$. 那么简单计算可以得到 $\sigma'(i) = i, \sigma'(j) = j$, 并且对 $t \neq i, j, k, r, s$, 如果 t 被 σ 固定, 那么也被 σ' 固定. 因此 σ' 有更多的不动点, 矛盾.

由上述论证, $\langle\sigma\rangle$ 的轨道中至少存在一个有至少 3 个元素, 设轨道为 $O = \{i, j, k, \cdots\}$. 如果 σ 不是 3–循环, 那么 O 中至少还有两个元素, 否则 σ 中包含 $(ijkr)$, 是一个奇置换. 因此 σ 移动 i, j, k 以外的 r, s, 同理地取 $\tau = (krs)$ 及 $\sigma' = \tau\sigma\tau^{-1}\sigma^{-1}$, 那么 σ' 固定 i, j 且固定 i, j, k, r, s 以外的其他不动点, 仍然矛盾. 综合以上两点, 可以知道 σ 是一个 3–循环. □

习题 2.3. 证明 A_4 不是单群.

2.3 Sylow 定理

有限群理论中一个重要的工具是我们即将陈述的三个 Sylow 定理. 本节中的群均默认是有限群.

定义 2.19. 设素数 p 整除群 G 的阶, 那么群 G 的一个 **Sylow p–子群**是一个 p^n 阶子群, 其中 n 是 p 整除 $|G|$ 的最高次幂.

定理 2.20 (Sylow 第一定理)**.** *设素数 p 整除群 G 的阶, 那么群 G 中存在 Sylow p–子群.*

定理 2.21 (Sylow 第二定理)**.** *设 H 是 G 的 p–子群, P 是 G 的 Sylow p–子群, 那么存在 $a \in G$ 使得 $H \subset aPa^{-1}$.*

推论 2.22. *Sylow p–子群两两共轭.*

定理 2.23 (Sylow 第三定理)**.** *设 $|G| = p^n m, (p, m) = 1$, 那么 G 的 Sylow p–子群的个数整除 m, 且模 p 余 1.*

Sylow 定理的证明比较复杂, 我们将其留在附录中. 读者也可以阅读 [5, pp. 33–36]. Sylow 定理的应用十分重要, 我们给出几个例子.

例 2.1. 第零个例子是关于如何分类低阶有限群的. 比如我们分类 4 阶群, 这用不到 Sylow 定理: 按照 Lagrange 定理, 群中元素的阶只能是 $1, 2, 4$ 其一. 如果群中存在 4 阶元, 那么这个群是循环群. 不然群中除单位元外都是 2 阶元, 设群 $G := \{e, a, b, c\}$. 那么 $\{e, a\} \lhd G, \{e, b\} \lhd G$, 并且有 $ab = c$, 所以 $G \simeq \{e, a\} \times \{e, b\}$. 因此 4 阶群同构于 C_4 或 $C_2 \times C_2$.

例 2.2. 我们证明 15 阶群是循环群. 设 $|G| = 15$, 考虑 Sylow 3–子群与 Sylow 5–子群. 由 Sylow 第三定理, Sylow 3–子群的个数整除 5, 且模 3 余 1, 因此个数只能是 1. 由 Sylow 第二定理, 这说明 Sylow 3–子群是正规的, 设为 $H \lhd G$. 同理 Sylow 5–子群也是正规的, 设为 $K \lhd G$. 而显然 $H \cap K = \{e\}$, 所以 $G \simeq H \times K$. 由于 H, K 是阶数互素的素数阶循环群, 所以 $H \times K$ 是循环群 (请读者验证), 即 G 是循环群.

例 2.3. 我们证明 72 阶群不是单群. 首先有 $72 = 2^3 \times 3^2$. 设群 G 的阶为 72. 由 Sylow 第一定理, G 存在 Sylow 3–子群, 并且由 Sylow 第三定理, Sylow 3–子群的个数整除 8 而模 3 余 1, 从而为 1 或 4. 如果 Sylow 3–子群恰好只有一个, 那么由 Sylow 第二定理可知它是正规的, 从而 G 有非平凡正规子群; 如果 Sylow 3–子群有四个, 那么由 Sylow 第二定理可知 G 的共轭作用是这四个子群上的一个可迁作用, 从而诱导了一个同态 $\varphi : G \to S_4$. 由于 $|S_4| = 24$, 由对应定理可知 $\ker\varphi$ 的阶至少为 3, 而 $\ker\varphi \lhd G$, 所以 G 有非平凡正规子群. 综上, G 一定不是单群.

2.4 例题与习题

例 2.4. 我们证明 $2n$ 阶群有阶为 n 的正规子群. 由 Cayley 定理, 不妨设 G 是 S_{2n} 的 $2n$ 阶子群. 如果 G 中存在一个奇置换, 那么 G 中奇置换与偶置换一定一样多 (请读者验证), 那么 $A_{2n} \cap G$ 就是 G 的 n 阶正规子群. 因此我们只需要找一个奇置换. 注意到对任意 $g \in G \backslash \{\mathrm{id}\}$, g 没有不动点, 且若 g 的阶为 d, 那么任意一个元素在 $\langle g \rangle$ 作用下的轨道长为 d. 因此 $\langle g \rangle$ 的轨道是 $2n/d$ 个 d 元集, 从而 g 的符号为 $(-1)^{2n-2n/d} = (-1)^{2n/d}$. 而 G 中阶数超过 3 的元素一定有偶数个 (考虑对应 $a \mapsto a^{-1}$), G 中单位元是 1 阶的, 所以 G 中一定存在 2 阶元, 此时它的符号为 $(-1)^n = -1$, 从而找到一个奇置换.

例 2.5. 我们将在本例中证明 *Burnside* 引理. 设有限群 G 作用在有限集合 X 上, 记 $S^g := \{s \in X |\ gs = s\}$ 为 g 的不动点集, X 在 G 的作用下有 n 条轨道, 那么 Burnside 引理断言

$$n = \frac{1}{|G|} \sum_{g \in G} |S^g|$$

证明用到了交换求和号的技巧. 我们有

$$\begin{aligned}\sum_{g\in G}|S^g| &= \sum_{g\in G}\sum_{s\in X,gs=s}1=\sum_{s\in X}\sum_{g\in G,gs=s}1\\ &= \sum_{s\in X}|G_s|=\sum_{s\in X}\frac{|G|}{|O_s|}\\ &= \sum_{O\text{是轨道}}\sum_{s\in O}\frac{|G|}{|O|}=\sum_{O\text{是轨道}}|G|\\ &= n|G|\end{aligned}$$

例 2.6. 我们证明 $n\geq 5$ 时, S_n 没有 $n!/4$ 阶子群. 假设存在子群 G 使得 $|G|=n!/4$. 如果 G 中不存在奇置换, 有 $G\subset A_n$, 那么 G 的阶是 A_n 的一半, 从而 $G\lhd A_n$, 与 A_n 的单性矛盾. 如果 G 中存在奇置换, 那么 $G'=G\cap A_n$ 阶为 $n!/8$. 考虑 A_n 在 G' 在 A_n 中的陪集类上的左平移作用: 陪集类中有 4 个元素, 从而这个作用给出一个同态 $\varphi: A_n\to S_4$. 而 $n\geq 5$ 时 $|A_n|/|S_4|>1$, 由对应定理知 $\ker\varphi$ 非平凡, 从而 $\ker\varphi\lhd A_n$, 与 A_n 的单性矛盾. 因此 G 是不存在的.

习题 2.4. 给定一个正整数 n, 证明互不同构的 n 阶群只有有限个.

习题 2.5. 设有限群 G 可迁地作用在有限集 X 上, $N\lhd G$, 证明 X 在 N 的作用下每个轨道有同样多的元素.

习题 2.6. 分类 10 阶群.

第三章　交换环

在第 一 章讨论了环的理想之后, 我们开始具体地讨论交换环的结构.

3.1　理想与整环

3.1.1　素理想与极大理想

定义 3.1. 称环 A 的子集 S 为**乘闭子集**, 如果 S 满足 $0 \notin S, 1 \in S$, 且对 $x, y \in S$ 有 $xy = S$.

我们首先定义两种重要的理想.

定义 3.2. 设 $\mathfrak{p}$ 是环 A 的真理想, 如果 $\mathfrak{p}$ 满足对 $a, b \in R$, $ab \in \mathfrak{p}$ 可以推出 $a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$, 那么称 $\mathfrak{p}$ 为**素理想**. 所有素理想的集合记为 $\operatorname{Spec} A$.

素理想有一种等价的刻画:

命题 3.3. *设 $\mathfrak{p}$ 是环 A 的理想, 那么以下命题等价:*

(1) *$\mathfrak{p}$ 是素理想;*

(2) *$R \backslash \mathfrak{p}$ 是乘闭的;*

证明. 仅仅是重述了一遍素理想的定义. □

定义 3.4. 设 $\mathfrak{m}$ 是环 A 的真理想, 如果对任意真理想 $\mathfrak{a}$, $\mathfrak{m} \subset \mathfrak{a}$ 可以推出 $\mathfrak{m} = \mathfrak{a}$, 那么称 $\mathfrak{m}$ 为 A 的一个**极大理想**. 换言之, 极大理想是环 A 的真理想以包含关系为偏序的极大元. 所有极大理想的集合记为 $\operatorname{MaxSpec} A$.

我们在本小节需要证明的中心结论是极大理想的存在性.

引理 3.5 (Zorn)**.** 设 $(X, \prec)$ 是非空偏序集, 如果 X 中任意一条链均有上界, 那么 X 中存在极大元.

证明. Zorn 引理等价于选择公理, 参阅 [5, 附录 2.2]. $\square$

命题 3.6. 设 $\mathfrak{a}$ 是 A 的一个真理想, 那么存在极大理想 $\mathfrak{m}$ 使得 $\mathfrak{a} \subset \mathfrak{m}$.

证明. 定义 $\mathscr{I}$ 是 A 的所有包含 $\mathfrak{a}$ 的真理想的集合. 那么 $\mathfrak{a} \in \mathscr{I}$, $\mathscr{I}$ 非空. 对于 $\mathscr{I}$ 中任意一条链

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$$

考虑 $\bigcup_{n \geq 1} \mathfrak{a}_n$, 容易验证它构成一个理想. 我们需要验证 $\bigcup_{n \geq 1} \mathfrak{a}_n$ 是一个真理想, 否则 $1 \in \bigcup_{n \geq 1} \mathfrak{a}_n$, 那么对某个 $\mathfrak{a}_i$ 有 $1 \in \mathfrak{a}_i$, 矛盾. 所以 $\bigcup_{n \geq 1} \mathfrak{a}_n$ 是这条链的上界. 因此 $\mathscr{I}$ 满足 Zorn 引理的条件, 其中存在极大元 $\mathfrak{m}$. 断言 $\mathfrak{m}$ 是极大理想: 如果 $\mathfrak{b}$ 满足 $\mathfrak{m} \subset \mathfrak{b}$, 那么 $\mathfrak{b} \in \mathscr{I}$, 从而由 $\mathfrak{m}$ 在 $\mathscr{I}$ 中的极大性知 $\mathfrak{b} = \mathfrak{m}$. 因此 $\mathfrak{m}$ 是极大理想, 且包含 $\mathfrak{a}$. $\square$

推论 3.7. 环 A 中存在极大理想.

评注 3.8. 我们强调我们处理的都是含幺交换环, 如果环不含幺元, 那么极大理想很有可能就不存在了, 见下面的例子.

例 3.1. 考虑在 $\mathbb{Q}$ 上赋予平凡乘法, 即对任意 $a, b \in \mathbb{Q}$ 有 $ab = 0$. 那么此时 $\mathbb{Q}$ 构成一个不含幺元的交换环. 假设 $\mathbb{Q}$ 有一个极大理想 $\mathfrak{a}$, 那么由对应定理, $\mathbb{Q}/\mathfrak{a}$ 没有非平凡理想. 因此 $\mathbb{Q}/\mathfrak{a}$ 没有非平凡子群, 从而是单群, 但单的 Abel 群只有素数阶循环群, 不妨设 $\mathbb{Q}/\mathfrak{a} \simeq \mathbb{Z}/p\mathbb{Z}$. 取 $a \notin \mathfrak{a}$, $a = pb$, 由 Lagrange 定理可知 $p(b + \mathfrak{a}) = \mathfrak{a}$, 这与 $a \notin \mathfrak{a}$ 矛盾. 所以 $\mathfrak{a}$ 不是极大理想.

3.1.2 整环与域

定义 3.9. (不一定交换的) 环 R 的**零因子**定义为满足存在元素与其相乘为 0 的元素.

定义 3.10. **整环**是含幺交换无零因子的环.

通过整环可以构造出一个域. 类似通过 $\mathbb{Z}$ 构造 $\mathbb{Q}$ 的方法, 我们定义整环的商域如下.

定义 3.11. 设 A 是整环, 在 $A\times A$ 上定义等价关系

$$(r_1,s_1)\sim(r_2,s_2):\iff r_1s_2=r_2s_1$$

将等价类记为 $[r/s]$, 那么 $A\times A/\sim$ 构成一个域, 称为 A 的**商域**, 并记为 $\operatorname{Quot}A$. A 可以看作 $\operatorname{Quot}A$ 的一个子环, 同构映射由 $a\mapsto[a/1]$ 给出.

习题 3.1. 证明一个域的商域是其自身.

整环与素理想之间可以通过商环建立起联系.

命题 3.12. 设 $\mathfrak{p}$ 是环 A 的理想, 那么 $\mathfrak{p}$ 是素理想当且仅当 $A/\mathfrak{p}$ 是整环.

证明. 假设 $A/\mathfrak{p}$ 是整环, 那么 $ab\in\mathfrak{p}$ 推出 $ab+\mathfrak{p}$, 而 $ab+\mathfrak{p}=(a+\mathfrak{p})(b+\mathfrak{p})$, 且对满足 $(a+\mathfrak{p})(b+\mathfrak{p})=\mathfrak{p}$ 的 a,b 一定有 $a+\mathfrak{p}=\mathfrak{p}$ 或 $b+\mathfrak{p}=\mathfrak{p}$, 即 $a\in\mathfrak{p}$ 或 $b\in\mathfrak{p}$. 反过来如果 $\mathfrak{p}$ 是素理想, 那么 $ab+\mathfrak{p}=\mathfrak{p}$ 推出 $ab\in\mathfrak{p}$, 就有 $a\in\mathfrak{p}$ 或 $b\in\mathfrak{p}$, 从而得到 $a+\mathfrak{p}=\mathfrak{p}$ 或 $b+\mathfrak{p}=\mathfrak{p}$. □

命题 3.13. 设 $\mathfrak{m}$ 是环 A 的理想, 那么 $\mathfrak{m}$ 是极大理想当且仅当 $A/\mathfrak{m}$ 是域.

引理 3.14. 一个整环是域当且仅当其只有平凡理想.

证明. 设 k 是整环. 如果 k 是域, 那么 k 的理想 $\mathfrak{a}$ 要么是零理想, 要么存在非零元 $a\in\mathfrak{a}$, 那么 $1=a^{-1}a\in\mathfrak{a}$, 从而 $\mathfrak{a}=k$. 如果 k 只有平凡理想, 那么对任意 $a\neq0$ 有 $\langle a\rangle=k$, 从而 $1\in\langle a\rangle$, 即 a 可逆. □

命题 3.13 的证明. 假设 $\mathfrak{m}$ 是极大理想, 那么由对应定理, $A/\mathfrak{m}$ 只有平凡理想, 从而由引理知 $A/\mathfrak{m}$ 是域. 反过来, 如果 $A/\mathfrak{m}$ 是域, 那么 $A/\mathfrak{m}$ 只有平凡理想, 从而由对应定理, A 中不存在更大的理想包含 $\mathfrak{m}$, 即 $\mathfrak{m}$ 是极大理想. □

推论 3.15. 极大理想都是素理想.

证明. 域都是整环. □

3.2 三种特殊的整环

3.2.1 唯一分解整环

我们在本小节将推广 $\mathbb{Z}$ 上的唯一分解性, 得到一类具有唯一分解性的整环. 为此, 我们将给出更广泛的整除与唯一分解的定义.

定义 3.16. 设 A 是整环.

(1) 设 $u \in A$ 满足存在 $v \in A$ 使得 $uv = 1$, 那么称 u 是一个**单位**.

(2) 设 $f, g \in A$ 满足存在 $h \in A$ 使得 $f = gh$, 那么称 g **整除** f, 并记 $g|f$. 此时称 g 是 f 的**因子**, f 是 g 的**倍元**.

(3) 如果 $f|g$ 且 $g|f$, 那么称 f 和 g **相伴**, 此时存在单位 u 使得 $f = ug$.

定义 3.17. 设 A 是整环.

(1) 如果 $f \in A$ 满足 $f = gh$ 且 g, h 都不是单位, 那么称 f 是**可约的**, 否则称 f 是**不可约的**.

(2) 设 $f \in A$, 称 f 可以分解为不可约元的乘积, 如果 $f = f_1 f_2 \cdots f_n$, 其中 f_i 都是不可约元.

(3) 设 $f \in A$, 称 f 唯一分解为不可约元的乘积, 如果对两个分解

$$f = f_1 f_2 \cdots f_l = g_1 g_2 \cdots g_m$$

有 $l = m$, 且适当调整顺序之后有 f_i 与 g_i 相伴.

定义 3.18. 整环 A 称为是**唯一分解整环 (UFD)**, 如果 A 中的任意非零且非单位的元素都可以唯一分解为不可约元的乘积.

在整数中, 素数具有性质 $p|ab \implies p|a$ 或 $p|b$, 依此我们可以类似地在整环上定义素元的概念.

定义 3.19. 设 A 是整环, 如果 $p \in A$ 满足对任意 $a, b \in A$ 有 $p|ab \implies p|a$ 或 $p|b$, 则称 p 是**素元**.

引理 3.20. *整环上的素元都是不可约元.*

证明. 假设 $p = ab$ 且 a, b 都不是单位, 那么 $p|ab$, 得出 $p|a$ 或 $p|b$, 不妨设前者成立, 那么 $a|p$ 且 $p|a$, 可知 p, a 相伴, 从而 b 是单位, 矛盾. 所以 p 不可约. □

命题 3.21. *设 A 是整环, 那么 A 是唯一分解整环的充分必要条件是*

(1) A 中的每个非零, 非单位的元素都可以分解为不可约元的乘积;

(2) A 中每个不可约元都是素元.

证明. 必要性: 设 $p|ab$, 进一步设 $ab = pr$, 那么作不可约元的分解有

$$a_1 \cdots a_l b_1 \cdots b_m = p r_1 \cdots r_n$$

由分解的唯一性, p 必然与某个 a_i 或者 b_i 相伴, 即 $p|a$ 或 $p|b$. 因此 p 是素元.
充分性: 设 $f \in A$ 有分解

$$f_1 f_2 \cdots f_l = g_1 g_2 \cdots g_m$$

我们对 $\max\{l, m\}$ 用归纳法. $\max\{l, m\} = 1$ 时有 $f_1 = g_1$, 无需证明. 假设 $\max\{l, m\} = n$, 不妨设 $m = n$, 那么有

$$f_1 | g_1 g_2 \cdots g_n$$

由于 f_1 是素元, 一定存在某个 g_i 使得 $f_1|g_i$, 而 g_i 是不可约元, 所以 f_1 与 g_i 相伴. 那么设 $f_1 = ug_i$, 在分解中约去 f_1 与 g_i 后得到

$$f_2 \cdots f_l = ug_1 \cdots \widehat{g_i} \cdots g_m$$

此时两侧不可约元个数最大值为 $n-1$, 由归纳假设有 $l-1 = m-1$, 即 $l = m$, 且调整顺序后不可约元对应相伴. 因此 A 是唯一分解整环. □

在唯一分解整环中, 可以定义两个元素的最大公因子和最小公倍式.

定义 3.22. 设 A 是唯一分解整环, $a_1, \cdots, a_n \in A$.

(1) $a_1, \cdots, a_n$ 的**最大公因子**定义为满足 $d|a_i (i = 1, \cdots, n)$, 且对任意 $d'|a_i (i = 1, \cdots, n)$ 的 d' 有 $d'|d$ 的 $d \in A$, 记为 $(a_1, \cdots, a_n)$.

(2) $a_1, \cdots, a_n$ 的**最小公倍式**定义为满足 $a_i|l (i = 1, \cdots, n)$, 且对任意 $a_i|l' (i = 1, \cdots, n)$ 的 l' 有 $l|l'$ 的 $d \in A$, 记为 $[a_1, \cdots, a_n]$.

最大公因子和最小公倍式一般来说不唯一, 会相差一个单位. 例如在 $\mathbb{Z}$ 中, $(4, 6)$ 既可以是 2 也可以是 -2.

习题 3.2. 证明唯一分解整环 A 中最大公因子和最小公倍式存在, 并且存在单位 $u \in A$ 使得 $a_1 \cdots a_n = u(a_1, \cdots, a_n)[a_1, \cdots, a_n]$.

3.2.2 主理想整环

定义 3.23. 由一个元素生成的理想称为**主理想**. 如果整环 A 的每个理想都是主理想, 那么称 A 为**主理想整环 (PID)**.

我们希望证明主理想整环是唯一分解整环. 为此, 我们需要建立主理想整环的一些性质:

命题 3.24. *在主理想整环 A 中, $p \in A\backslash\{0\}$, 那么下列命题等价:*

(1) *p 是不可约元;*

(2) *$\langle p\rangle$ 是极大理想;*

(3) *$\langle p\rangle$ 是素理想;*

(4) *p 是素元.*

证明. (1) $\implies$ (2): 假设 $\langle p\rangle \subset \mathfrak{a} \neq A$, 那么由于 A 是主理想整环, $\mathfrak{a} = \langle a\rangle$, 从而 $a|p$. 而 p 是不可约元, 这说明 a 是单位或 $a = p$, 即 $\mathfrak{a} = \langle p\rangle$, 从而 $\langle p\rangle$ 是极大理想.

(2) $\implies$ (3): 这是推论 3.15.

(3) $\implies$ (4): 设 $p|ab$, 那么 $ab \in \langle p\rangle$, 从而有 $a \in \langle p\rangle$ 或 $b \in \langle p\rangle$, 即 $p|a$ 或 $p|b$.

(4) $\implies$ (1): 这是引理 3.20. □

命题 3.25. *主理想整环 A 的主理想满足升链条件, 即对主理想的升链*

$$\langle a_1\rangle \subset \langle a_2\rangle \subset \cdots \tag{3.1}$$

存在 $n \in \mathbb{N}$ 使得 $\langle a_n\rangle = \langle a_{n+1}\rangle = \cdots$.

证明. 在 (3.1) 中取 $\mathfrak{a} = \bigcup_{i\geq 1}\langle a_i\rangle$, 那么我们熟悉这一定是一个理想. 由于 A 是主理想整环, 那么存在 $a \in \mathfrak{a}$ 使得 $\mathfrak{a} = \langle a\rangle$. 由于 $a \in \bigcup_{i\geq 1}\langle a_i\rangle$, 设 $a \in \langle a_n\rangle$, 那么

$$\langle a\rangle \subset \langle a_n\rangle \subset \langle a_{n+1}\rangle \subset \cdots \subset \langle a\rangle$$

从而就有 $\langle a_n\rangle = \langle a_{n+1}\rangle = \cdots$. □

命题 3.26. *主理想整环是唯一分解整环.*

证明. 设 A 是主理想整环, 我们证明 A 中非零非单位的元素都能分解为不可约元的乘积. 否则设存在一个 a 不可以分解为不可约元的乘积, 设 $a = a_1b_1$, 其中 a_1 不是不可约元, 不妨设其也不能分解为不可约元的乘积. 又设 $a_1 = a_2b_2$, a_2 不可以分解为不可约元的乘积. 如此归纳定义得到序列 $a_1, a_2, \cdots$, 每一项中后者都整除前者且不与前者相伴, 因此我们得到严格递增的主理想链

$$\langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \cdots$$

这与命题 3.25 矛盾. 所以 A 中的元素都可以分解为不可约元的乘积. 而由命题 3.24, A 中的不可约元都是素元, 那么由命题 3.21, 可知 A 是唯一分解整环. □

反过来一般是不成立的. 例如可以证明 $\mathbb{Z}[x]$ 是唯一分解整环 ([5, p. 182 定理 2.3]), 但是容易发现 $\langle 2, x\rangle$ 不是主理想.

3.2.3 Euclid 整环

在本小节我们推广 $\mathbb{Z}$ 上的带余除法.

定义 3.27. 设 A 是整环, 映射 $\delta : A\backslash\{0\} \to \mathbb{N}$, 满足对任意 $a, b \in A$, 存在 $q, r \in A$ 使得

$$a = bq + r$$

且 $r = 0$ 或 $\delta(r) < \delta(b)$, 则称 A 为 **Euclid 整环**, δ 为 **Euclid 映射**.

我们熟知两种 Euclid 整环 $\mathbb{Z}$ 与 $k[x]$. 当 $A = \mathbb{Z}$ 时, Euclid 映射就是恒等映射; 当 $A = k[x]$ 时, Euclid 映射是多项式的度数.

我们证明本小节最主要的结论:

命题 3.28. *Euclid 整环是主理想整环.*

证明. 设 A 是 Euclid 整环, $\mathfrak{a}$ 是 A 的理想. 取集合 $S = \{\delta(x) | \ x \in \mathfrak{a}\}$, 那么 $S \subset \mathbb{N}$, 由最小数原理, 存在 $a \in \mathfrak{a}$ 使得 $\delta(a) = \min S$. 断言 $\mathfrak{a} = \langle a\rangle$. 设 $b \in \mathfrak{a}$, 那么存在 $q, r \in A$ 使得 $b = aq + r$. 如果 $r \neq 0$, 那么 $r = b - aq \in \mathfrak{a}$, 且 $\delta(r) < \delta(a)$, 与 $\delta(a) = \min S$ 矛盾. 所以 $r = 0$, 即 $b = aq$, $b \in \langle a\rangle$. 从而有 $\mathfrak{a} = \langle a\rangle$, 即 A 的任意理想是主理想. □

本小节与前一小节证明了如下的包含关系:

$$\text{Euclid 整环} \subsetneqq \text{主理想整环} \subsetneqq \text{唯一分解整环}$$

而证明这两个包含关系是严格的则超出了本讲义的范围.

例题与习题

例 3.2. 我们证明交换环 A 的诣零根满足

$$\sqrt{\{0\}} = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p} \tag{3.2}$$

一方面, 容易验证素理想都是根式理想, 所以 $\sqrt{\{0\}} \subset \sqrt{\mathfrak{p}} = \mathfrak{p}, \forall \mathfrak{p} \in \operatorname{Spec} A$, 即

$$\sqrt{\{0\}} \subset \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$$

另一方面, 如果 $a \in A \backslash \sqrt{\{0\}}$, 那么 $S := \{1, a, a^2, \cdots\}$ 是一个乘闭子集, 从而 $A \backslash S \in \operatorname{Spec} A$, $a \notin \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$, 因此

$$A \Big\backslash \sqrt{\{0\}} \subset A \Bigg\backslash \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$$

因此有 (3.2) 成立.

例 3.3. 我们在本例中证明素理想躲避引理. 设 A 是交换环, $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ 是素理想, 理想 $\mathfrak{a}$ 满足

$$\mathfrak{a} \subset \bigcup_{i=1}^{n} \mathfrak{p}_i$$

那么存在 $i \in \{1, \cdots, n\}$ 使得 $\mathfrak{a} \subset \mathfrak{p}_i$.

事实上, 对 n 用归纳法. $n = 1$ 时命题显然成立. 对 $n > 1$, 考虑集合 $A_i := \mathfrak{a} \Big\backslash \bigcup_{j \neq i} \mathfrak{p}_j$. 如果某个 $A_i = \varnothing$, 那么 $\mathfrak{a} \subset \bigcup_{j \neq i} \mathfrak{p}_j$, 由归纳假设知命题成立. 现假设每个 A_i 均非空, 反设命题不成立, 那么取 $x_i \in A_i$, 易知 $x_i \in \mathfrak{p}_i$. 考虑 $x_1 \cdots x_{n-1} + x_n \in \mathfrak{a}$, 当 $1 \leq i \leq n-1$ 时,

$$x_1 \cdots x_{n-1} + x_n \in \mathfrak{p}_i \implies x_n \in \mathfrak{p}_i$$

矛盾; 当 $i = n$ 时,

$$x_1 \cdots x_{n-1} + x_n \in \mathfrak{p}_n \implies \exists x_j \in \mathfrak{p}_n$$

仍然矛盾. 因此由归纳法可知命题成立.

例 3.4. 设 A 是整环, 我们证明 $A[x]$ 是主理想整环当且仅当 A 是域. 熟知 A 是域时 $A[x]$ 是主理想整环. 反过来, 假设 $A[x]$ 是主理想整环, 对 $a \in A \backslash \{0\}$, 考虑理想 $\langle a, x \rangle$. 由于 $A[x]$ 是主理想整环, 设 $\langle a, x \rangle = \langle b \rangle$. 那么 $b|a$, 考虑度数可知 $b \in A$. 而 $b|x$, 设 $b(cx + d) = x$, 比较系数可知 $bc = 1$, 即 b 可逆. 所以 $\langle a, x \rangle = A[x]$, 那么存在 $f(x), g(x) \in A[x]$ 使得

$$af(x) + xg(x) = 1$$

令 $x = 0$ 有 $af(0) = 1$, 即 a 可逆, 从而 A 是一个域.

例 3.5. 我们证明 $\mathbb{Z}[i]/\langle 1+i\rangle \simeq \mathbb{F}_2$. 而这只需要观察如下图表:

$$\begin{tikzcd} \mathbb{Z}[x] \arrow[r, "x^2+1"] \arrow[d, "x+1"] & \mathbb{Z}[i] \arrow[d, "i+1"] \\ \mathbb{Z} \arrow[r, "2"] & \mathbb{F}_2 \end{tikzcd}$$

习题 3.3. 设 A 是交换环, 如果 $e \in A$ 满足 $e^2 = e$, 则称 e 是幂等元.

(1) 如果 e 是幂等元, 证明 $1-e$ 也是幂等元.

(2) 证明 $A \simeq \langle e\rangle \oplus \langle 1-e\rangle$.

习题 3.4. 一个交换环称为**局部环**, 如果它有唯一的极大理想. 证明一个交换环是局部环当且仅当它的所有不可逆元构成一个理想.

习题 3.5. 交换环 A 上的**形式幂级数环** $A[[x]]$ 是所有形如

$$\sum_{n=0}^{\infty} a_n x^n$$

的元素构成的环, 其中加法与乘法与多项式的定义类似.

(1) 证明 $a_0 + a_1 x + a_2 x^2 + \cdots$ 可逆当且仅当 a_0 是单位.

(2) 设 k 是域, 证明 $k[[x]]$ 是局部环.

习题 3.6. (1) 证明 $\mathbb{Z}[\sqrt{-5}]$ 不是唯一分解整环.

(2) 证明 $\mathbb{Z}[\sqrt{-1}], \mathbb{Z}[\sqrt{-2}]$ 是唯一分解整环.

[提示: 考虑 $\mathbb{Z}[\sqrt{-1}]$ 的**模** $|a+b\sqrt{-1}|^2 = a^2+b^2$, $\mathbb{Z}[\sqrt{-2}]$ 的模类似定义.]

第四章　域

我们在本章及下一章讨论域这种更强的代数结构.

4.1　域扩张

定义 4.1. 设 K, L 是域, 满足 $K \subset L$, 那么称 L 是 K 的一个**扩域**, 并记为 L/K.

我们首先引进两个记号

记号 4.2. 设有域扩张 L/K, $S \subset L$, 那么记 $K(S)$ 为包含 S 的最小的域 (即所有包含 S 的域的交). 如果 $S = \{a_1, \cdots, a_n\}$, 也记 $K(S) = K(a_1, \cdots, a_n)$.

对 L/K, L 自然构成了一个 K–向量空间, 所以我们可以定义

定义 4.3. 定义域扩张 L/K 的**度数**为 $[L : K] := \dim_K L \in \mathbb{N} \cup \{\infty\}$.

我们定义几类扩张如下

定义 4.4. 给定域扩张 L/K.

(1) 如果 $[L : K] < \infty$, 那么称 L/K 是**有限扩张**.

(2) 设 $a \in L$, 如果 α 是 $K[x]$ 中某个多项式的根, 那么称 α 是 K 上的**代数元**, 否则称为**超越元**. 如果 α 是代数元, 所有满足 $f(\alpha) = 0$ 的多项式中次数最低的称为 α 的**极小多项式**.

(3) 如果 L 中任意一个元素都是代数元, 那么称 L/K 是**代数扩张**, 否则称为**超越扩张**.

考虑由单个代数元 α 生成的扩域, 我们有如下的引理

引理 4.5. 设 L/K, $\alpha \in L$ 是 K 上的代数元, 有极小多项式 $m(x) \in K[x]$, 那么 $K(\alpha) \simeq K[x]/\langle m(x)\rangle$, 其中 $\langle m(x)\rangle$ 是 $p(x)$ 生成的理想.

证明. 定义同态

$$\begin{aligned} \varphi : K[x] &\to K(\alpha) \\ p(x) &\mapsto p(\alpha) \end{aligned}$$

考虑核 $\ker\varphi$, 显然 $\ker\varphi \neq K[x]$, 且极小多项式 $m(x) \in \ker\varphi$. 由于 $K[x]$ 是主理想整环, $\ker\varphi$ 单生成, 且生成元整除 $m(x)$. 但容易证明 $m(x)$ 是不可约多项式, 结合 $\ker\varphi \neq K[x]$ 可知生成元与 $m(x)$ 相伴, 从而 $\ker\varphi = \langle m(x)\rangle$. 由第一同构定理即知

$$K(\alpha) \simeq \frac{K[x]}{\langle m(x)\rangle}$$ □

关于有限扩张与代数扩张, 有如下的结论

命题 4.6. 设有域扩张 M/K, $\alpha \in M$ 是 K 上的代数元当且仅当 α 包含在 K 的一个有限扩张中.

证明. 一方面, 假设 α 是代数元. 设 $\deg\alpha = n$, 那么 $1, \alpha, \cdots, \alpha^{n-1}$ 是 $K(\alpha)$ 的一组基, $K(\alpha)/K$ 是有限扩张. 另一方面, 假设 α 包含在 K 的有限扩张中, 不妨设 $[M : K] = n < \infty$. 那么 $1, \alpha, \cdots, \alpha^{n-1}, \alpha^n$ 一定线性相关, 从而 α 是一个多项式的根, 是一个代数元. □

推论 4.7. 任意有限扩张都是代数扩张.

定理 4.8 (望远镜公式)**.** 设 $K \subset L \subset M$ 均为有限扩张, 那么有 $[M : K] = [M : L][L : K]$

证明. 设 $x_1, \cdots, x_m$ 是 L/K 的一组基, $y_1, \cdots, y_n$ 是 M/L 的一组基. 我们考虑 $\{x_iy_j\}_{(i,j)\subset[m]\times[n]}$[1]. 首先对 $a_{ij} \in K$ 及指标 $(i, j) \in R \times S \subset [m] \times [n]$ 有

$$\begin{aligned} &\sum_{(i,j)\in R\times S} a_{ij}(x_iy_j) = 0 \\ \Longrightarrow &\sum_{j\in S} a_{ij}y_j = 0, \ \forall i \in R \\ \Longrightarrow &\, a_{ij} = 0, \ \forall (i, j) \in R \times S \end{aligned}$$

[1] $[m] = \{1, \cdots, m\}$, 组合数学中的常用记号.

所以 x_iy_j 线性无关. 其次, 显然 M 中的每个元素可以表示为 x_iy_j 的 K–线性组合, 所以 $\{x_iy_j\}_{(i,j)\subset[m]\times[n]}$ 是 M/L 的一组基. 从而命题得证. □

通过望远镜公式, 我们可以证明

定理 4.9. 设 α,β 是 K 上的代数元, 那么 $\alpha\pm\beta,\alpha\beta,\alpha/\beta(\beta\neq 0)$ 均为 K 上的代数元.

证明. 考虑扩张链 $K\subset K(\alpha)\subset K(\alpha,\beta)$, 两个扩张均为代数扩张, 所以都是有限扩张. 由定理 4.8, $K(\alpha,\beta)/K$ 是代数扩张. 而 $\alpha\pm\beta,\alpha\beta,\alpha/\beta$ 均包含在 $K(\alpha,\beta)$ 中, 所以都是代数元. □

定理 4.10. 设 α 是一个由 K 上代数元系数构成的多项式的根, 那么 α 是代数的.

证明. 设

$$\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_0=0$$

且 $a_{n-1},\cdots,a_0$ 均为 K 上代数元. 考虑域扩张链

$$\begin{aligned}
K&\subset K(a_0)\\
&\subset K(a_0,a_1)\\
&\cdots\\
&\subset K(a_0,\cdots,a_{n-1})\\
&\subset K(a_0,\cdots,a_{n-1},\alpha)
\end{aligned}$$

前 n 步扩张每一步都是添加一个代数元 a_i, 所以都是有限的, 因此 K 上的扩域 $K(a_0,\cdots,a_{n-1})$ 是有限的. 而由假设, α 在 $K(a_0,\cdots,a_{n-1})$ 上代数, 所以最后一步扩张也是有限的. 因此扩张 $K(a_0,\cdots,a_{n-1},\alpha)/K$ 是有限的, 从而 α 是 K 上代数元. □

推论 4.11. 假设 $E/L,L/K$ 均为代数扩张, 那么 E/K 也是代数扩张.

4.2　分裂域

对于一个代数方程, 我们总希望能够找到一个域使得它“有根”. 而严格地描述这一点则需要定义分裂域的概念.

定义 4.12. 设 K 是域, $p(x) \in K[x]$, 如果扩域 L/K 使得 $p(x)$ 在 L 上可以分解为一次因式的乘积 (简称为**分裂**)

$$p(x) = (x-\alpha_1)\cdots(x-\alpha_n)$$

且 $L = K(\alpha_1, \cdots, \alpha_n)$, 那么称 L 是 $p(x)$ 在 K 上的**分裂域**.

本节的关键是证明分裂域的存在性与同构唯一性.

我们首先证明分裂域的存在性.

证明. 给定域 K 及 $p = p_1 p_2 \cdots p_m \in K[x]$, 其中 p_i $(i = 1, \cdots, m)$ 均不可约. 我们对 $\deg p$ 用归纳法. 当 $\deg p = 1$ 时, K 本身就是 $p(x)$ 的分裂域. 假设对 $\deg p = n-1$ 成立. 对 $\deg p = n$, 考虑域 $K_1 = K[x]/\langle p_1(x)\rangle$, 那么 p 在 K_1 上至少有一个根 α, p 在 K_1 上可以分解为

$$p(x) = (x-\alpha)p_a(x)$$

对 $p_a(x)$ 用归纳假设, 存在扩域 L/K_1 使得 $p_a(x)$ 分裂为一次因式的乘积, 从而在扩域 L/K 上 $p(x)$ 分裂为一次因式的乘积. 由归纳原理得证. □

然后我们证明分裂域的同构唯一性.

定理 4.13 (分裂域的同构唯一性)**.** 设 K 是域, $p(x) \in K[x]$, 域 K' 与 K 同构, 且 $p(x)$ 在同构映射下的像为 $p'(x)$. 设 L, L' 分别是 $p(x), p'(x)$ 的分裂域, 那么存在同构 $L \to L'$ 使得以下图表交换

$$\begin{array}{ccc} L & \xrightarrow{\sim} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\sim} & K' \end{array}$$

证明. 设 $i : K \xrightarrow{\sim} K'$ 是同构, 我们也用 i 表示延拓到 $K[x] \to K'[x]$ 的同构. 依然对 $p(x)$ 的次数用归纳法. $\deg p = 1$ 时, $K = L, K' = L'$, 命题显然成立. 假设

命题对 $\deg p = n-1$ 成立, 那么对 p 的某个不可约因子 p_1, 有

$$K(\alpha) = \frac{K[x]}{\langle p(x) \rangle} \simeq \frac{K'[x]}{\langle i(p(x)) \rangle} = K(\alpha')$$

从而可以得到交换图

$$\begin{tikzcd}
K(\alpha) \arrow[r, "\sim"] & K'(\alpha) \\
K \arrow[u] \arrow[r, "\sim"] & K' \arrow[u]
\end{tikzcd}$$

而在 $K(\alpha), K'(\alpha')$ 上 $p(x), p'(x)$ 分别分解为一次因式与一个 $n-1$ 次多项式的乘积, 从而按归纳假设, 可以得到两个 $n-1$ 次多项式的分裂域的同构

$$\begin{tikzcd}
L \arrow[r, "\sim"] & L' \\
K(\alpha) \arrow[u] \arrow[r, "\sim"] & K'(\alpha') \arrow[u]
\end{tikzcd}$$

从而有大图表

$$\begin{tikzcd}
L \arrow[r, "\sim"] & L' \\
K(\alpha) \arrow[u] \arrow[r, "\sim"] & K'(\alpha') \arrow[u] \\
K \arrow[u] \arrow[r, "\sim"] & K' \arrow[u]
\end{tikzcd}$$

交换, 即得到所欲证命题. □

评注 4.14. 需要注意到, 两个分裂域之间的同构不一定是唯一的. 例如分别使用 i, j 表示虚数单位, x^2+1 在 $\mathbb{R}$ 上的两个分裂域

$$\begin{tikzcd}
\mathbb{C} = \mathbb{R}(i) \arrow[rr, "h"] & & \mathbb{R}(j) \\
& \mathbb{R} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

其中 $h : \mathbb{R}(i) \to \mathbb{R}(j)$ 可以取为 $i \mapsto j$ 与 $i \mapsto -j$, 得到两个同构. 分裂域间不同的同构构成了多项式的 **Galois 群**, 它将在 Galois 理论中处于中心的位置.

4.3 有限域

我们在本节讨论元素个数有限的域, 也即**有限域**.

假设 F 是有限域, 那么 F 一定有正的特征 $p>0$. 那么此时素域 $\mathbb{F}_p \subset F$, F 是 $\mathbb{F}_p$ 上的向量空间. 如果 $\dim_{\mathbb{F}_p} F = n$, 那么每个坐标分量有 p 种取法, 则 $|F| = p^n$. 因此我们得到

命题 4.15. *有限域 F 的阶为 p^n, 其中 $p = \operatorname{char} F$ 是素数, $n = [F : \mathbb{F}_p]$.*

相同的论证我们可以得到

命题 4.16. *设 K, L 分别是 p^n, q^m 元域, 那么 $K \subset L$ 当且仅当 $p = q$ 且 $n | m$.*

与分裂域一样, 我们也要讨论有限域的存在性与同构唯一性.

首先我们证明有限域的存在性.

定理 4.17. *对素数 p 及 $q = p^n$, 存在 q 阶有限域.*

证明. 取 $x^q - x$ 在 $\mathbb{F}_p$ 上的一个分裂域 L, 我们证明 L 恰好由 $x^q - x$ 的所有根构成. 我们先证明 $x^q - x$ 的根构成一个域. 对根 x, y, 由 $\operatorname{char} L = p$ 可知 $\binom{q}{k} = 0,\ k = 1, \cdots, q-1$, 从而

$$\begin{aligned}(x-y)^q &= x^q - y^q \quad (p=2\text{时}1=-1,\text{ 所以均写为减号})\\ &= x - y\end{aligned}$$

所以 $x - y$ 是 $x^q - x$ 的一个根; 而当 $y \neq 0$ 时

$$\begin{aligned}\left(\frac{x}{y}\right)^q - \frac{x}{y} &= \frac{x^q y - x y^q}{y^{q+1}}\\ &= \frac{xy - yx}{y^{q+1}}\\ &= 0\end{aligned}$$

所以 x/y 也是一个根. 因此 $x^q - x$ 的根在减法与除法下封闭, 构成一个域. 由于分裂域由根生成, 所以 L 恰好由 $x^q - x$ 的根构成. 另一方面, 由于 $(x^q - x)' = qx^{q-1} - 1 = -1$, 与 $x^q - x$ 互素, 所以 $x^q - x$ 没有重根. 因此 $|L| = \deg(x^q - x) = q$. □

然后我们证明有限域的唯一性.

定理 4.18. *两个有限域同构当且仅当他们阶数相同.*

证明. 设有限域 F 的阶数为 q, 我们证明 F 一定是 $x^q - x$ 的分裂域. 这只需要证明对任意 $a \in F$ 有 $a^q = a$ 即可. $a = 0$ 时这是平凡的. 对 $a \in F^*$, 由 Lagrange 定理, $a^{|F^*|} = 1$, 即 $a^{q-1} = 1$, 从而 $a^q = a$. 因此 F 是 $x^q - x$ 的分裂域, 在同构意义下是唯一的. □

最后我们证明有限域最重要的结论之一

定理 4.19. *有限域的乘法群是循环群.*

我们首先需要一个引理

引理 4.20 (多项式的 Lagrange 定理)**.** *设 $f(x) \in k[x]$, $\deg f(x) = d$, 那么 $f(x) = 0$ 在 k 中至多有 d 个根.*

证明. 对 d 用归纳法. 当 $d = 1$ 时命题是显然的. 假设命题对 $d = n - 1$ 成立, 那么此时 n 次多项式 $f(x)$ 在 k 上要么没有根, 要么有一个根 α, 此时存在一个 $n - 1$ 次多项式 $g(x)$ 使得 $f(x) = (x - \alpha)g(x)$. 而由归纳假设, $g(x)$ 至多有 $n - 1$ 个根, 所以 $f(x) = (x - \alpha)g(x)$ 至多有 n 个根. 由归纳原理知命题得证. □

定理 4.19 的证明. 设 k 是一个 q 元域, 那么它的乘法群 k^* 阶为 $q - 1$. 设 m 是 k^* 中元素的最大值, 并设 α 的阶为 m. 那么对任意 $\beta \in k^*$, 设其阶为 d, 则 $\alpha\beta$ 的阶为 $[m, d] \leq m$, 从而 $d|m$. 因此 $\beta^m = 1$, 方程 $x^m - 1$ 有至少 $q - 1$ 个根, 由多项式的 Lagrange 定理可知 $m \geq q - 1$. 而由群的 Lagrange 定理知 $m|q - 1$, 所以 $m = q - 1$, 即 $\langle\alpha\rangle = k^*$. □

参考文献

[1] 张英伯，王恺顺。*代数学基础 (下册)*。北京师范大学出版社，**2013**。

[2] 李文威。*代数学方法 (第一卷)*。高等教育出版社，**2019**。

[3] Thomas W. Hungerford. *Algebra.* Springer-Verlag, New York-Berlin, **1980**, Reprint of the 1974 original.: xxiii+502.

[4] Paolo Aluffi. *Algebra: chapter 0.* American Mathematical Society, Providence, RI, **2009**: xx+713.

[5] Serge Lang. *Algebra.* third. Springer-Verlag, New York, **2002**: xvi+914.