



抽象代数

数学学院励志书院数学试验班师生联合党支部

主编：郭晨旭（24）、但振鹏（24）、吕语馨（24）、严博森（24）

校对：李松泽（24）

2026.9



数学与统计学院
SCHOOL OF MATHEMATICS AND STATISTICS



励志书院
LIZHI COLLEGE

西安交通大学数学学院励志书院
数学试验班师生联合党支部



写在前面的话

本笔记专为备考司飞老师的《抽象代数》课程而整理，参考复旦大学陈猛老师的《抽象代数讲义》和司飞老师自编讲义。由于司飞老师刚刚任教该课程一年，本笔记旨在为同学们提供一定量的训练，补充一定的例子，由于时间关系，难免出错，敬请大家批评指正。

司飞老师课程任务重，时间紧，讲述的内容都是抽象代数最核心最重要的问题，但由于该课程具有一定的抽象性，刚开始学习该课程容易将抽象的性质和具体的例子相分离，我们在这份讲义中特地加入了大大小小许多的例子和注记，希望大家能够根据例子更好地学习这门课程。这份讲义随后也会将 24 级的考试题附在后面，但由于样本较少，在考试前不能将全部重心放在往年题上，要熟悉代数结构的性质，也希望在未来的日子里，这份讲义能够不断地得到补充和丰富。

目录

1	群论	3
1.1	群的基本定义与简单例子	3
1.2	置换群 S_n 与交错群 A_n	5
1.3	陪集、Lagrange 定理，正规子群与商群	6
1.4	群同态与同构基本定理	10
1.5	群的直积	13
1.6	群作用	14
1.7	Sylow 定理	15
1.8	综合大题	16
2	环论	17
2.1	环、整环与域	17
2.2	理想与商环	22
2.3	环同态与同构	26
2.4	多项式环	29
2.5	分式域、欧氏整区与主理想整区	33
2.5.1	整区的分式域	34
2.5.2	欧氏整区	35
2.5.3	主理想整区	36
2.6	整区上的因式分解	37
2.6.1	本原多项式与高斯引理	40
3	模论	41
3.1	模、模同态等	42
3.2	主理想整环 (PID) 上的有限生成模	43



4 域扩张和伽罗瓦理论	43
4.1 域扩张的定义与扩张次数	43
4.2 代数扩张与极小多项式	45
4.3 分裂域与代数闭域	47
4.4 域扩张的嵌入与自同构	49
4.5 正规扩张与可分扩张	51
4.6 Galois 扩张与 Galois 基本定理	53
4.7 有限域	57
4.8 多项式 Galois 群的计算（拓展阅读）	59
4.9 可解扩张与根式可解性（拓展阅读）	60
4.10 知识串联与自测	61



1 群论

1.1 群的基本定义与简单例子

定义 1.1 (群). 设 G 为非空集合, $*$: $G \times G \rightarrow G$ 是集合上的二元运算, 满足下面三条公理:

1. 结合律: 对任意 $a, b, c \in G$, $(a * b) * c = a * (b * c)$;
2. 存在单位元: 存在 $e \in G$, 对任意 $g \in G$, 有 $g * e = e * g = g$;
3. 每个元素存在逆元: 对任意 $g \in G$, 存在 $g^{-1} \in G$, 使得

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

则称 $(G, *)$ 是一个群。

- 只满足结合律: 称为**半群**;
- 满足结合律 + 存在单位元: 称为**么半群**;
- 如果进一步满足交换性 $\forall a, b \in G, ab = ba$, 称 G 为 **Abel (交换) 群**。

注意: 群定义要求运算封闭, 即运算结果仍然落在集合 G 内, 二元运算定义已经自带封闭性。我们考虑矩阵集合 $V = \{A \in \mathbb{R}^{n \times n} \mid \det(A) = 0\}$ 以及矩阵加法 “+”, $(V, +)$ 符合定义 1.1 中的三条性质, 但是 V 对于矩阵加法不封闭, 所以并不能说 $(V, +)$ 是一个群。

命题 1.2. 在任意群中:

1. 单位元是唯一的;
2. 每个元素的逆元是唯一的。

证明. (1) 设 e, e' 都是单位元。由单位元定义:

$$e = e * e' = e'.$$

故单位元唯一。

(2) 设 $g \in G$, g_1^{-1}, g_2^{-1} 都是 g 的逆元:

$$g_1^{-1} = g_1^{-1}e = g_1^{-1}(gg_2^{-1}) = (g_1^{-1}g)g_2^{-1} = e g_2^{-1} = g_2^{-1}.$$

逆元唯一。 □

注意: 如果按照群的元素个数分类的话, 还可以将群分为**无限群**和**有限群**。如果集合 G 有 n 个元素, 我们称之为 **n 阶有限群**。

例 1.3. 1. $(\mathbb{Z}, +)$: 整数加法 Abel 群。单位元 0, a 的逆元 $-a$; 无限群。

2. $(\mathbb{Z}/7\mathbb{Z}, +)$: 模 7 剩余类加法 Abel 群, 7 阶有限群。



3. $(\mathbb{R}^*, \cdot)$: 非零实数乘法 Abel 群; 单位元 1, a 逆元 $1/a$ 。
 4. $GL_2(\mathbb{R})$: 2 阶实可逆矩阵, 矩阵乘法。非 Abel 群。
 5. $SU(2) = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{C}, |a|^2 + |b|^2 = 1 \right\}$, 矩阵乘法成群, 非交换, 集合与 4 维欧氏空间中单位球面 S^3 一一对应。
- 注意: $GL_2(\mathbb{R})$ 取 $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, 直接验算 $AB \neq BA$, 验证非交换。

定义 1.4 (元素的阶). 设 G 是群, $g \in G$ 。如果存在正整数 m , 使得 $g^m = e$, 满足该等式的最小正整数叫做元素 g 的阶, 记作 $o(g)$ 。若不存在这样的正整数, 则称 g 为无限阶元素。

事实: 有限群中任意元素的阶一定是有限的。

注意: 加法群中记号 g^m 等价于 $m \cdot g = \underbrace{g + g + \cdots + g}_m$ 。

例 1.5. 1. $G = \mathbb{Z}/8\mathbb{Z}$ (加法): $o(\bar{1}) = 8, o(\bar{2}) = 4, o(\bar{4}) = 2, o(\bar{0}) = 1$ 。

2. $G = (\mathbb{R}^*, \cdot)$, 元素 2: 对任意正整数 $m, 2^m \neq 1$, 2 是无限阶。

3. $G = \mathbb{Z}$ (加法), 元素 5: 无限阶, 不存在正整数 m 使得 $m \cdot 5 = 0$ 。

4. $G = \mathbb{Z}/12\mathbb{Z}, o(\bar{9}) = 4: 4 \cdot \bar{9} = \bar{36} = \bar{0}$, 更小正整数不满足。

定义 1.6 (子群). 设 G 是群, H 是 G 的非空子集。若 H 关于 G 的运算本身也构成群, 则称 H 是 G 的子群, 记作 $H \leq G$ 。

子群三个等价判定条件:

1. $\forall a, b \in H$, 有 $ab \in H$ 且 $a^{-1} \in H$;
2. $\forall a, b \in H$, 有 $ab^{-1} \in H$; (考试高频)
3. H 非空, 对乘法、取逆运算封闭。

例 1.7. 1. $G = \mathbb{Z}, H = 4\mathbb{Z} = \{4k \mid k \in \mathbb{Z}\}$, 加法子群。

2. $G = GL_3(\mathbb{R}), H = SL_3(\mathbb{R}) = \{A \in GL_3(\mathbb{R}) \mid \det A = 1\}$, 子群。

3. $G = \mathbb{Z}/12\mathbb{Z}, H = \langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$, 循环子群。 $\langle g \rangle$ 的定义见定义 1.4

4. $G = \mathbb{C}^*$ (非零复数乘法), $H = \{z \in \mathbb{C}^* \mid |z| = 1\}$ 单位圆, 乘法子群。

定义 1.8 (生成子群, 循环群). 设 $S \subset G$ 是非空子集。定义

$$\langle S \rangle = \bigcap_{S \subseteq H \leq G} H,$$

称为由集合 S 生成的子群, 它是包含 S 的最小子群。其元素可以写成

$$\langle S \rangle = \{g_1^{e_1} g_2^{e_2} \cdots g_k^{e_k} \mid k \geq 0, g_i \in S, e_i = \pm 1\}.$$

若存在一个元素 $g \in G$ 使得 $G = \langle g \rangle$, 则称 G 是循环群。



例 1.9. 1. $\mathbb{Z} = \langle 1 \rangle$, 无限循环加法群。

2. $\mathbb{Z}/15\mathbb{Z} = \langle \bar{1} \rangle$, 15 阶有限循环群; 也可以是 $\langle \bar{2} \rangle$ 。

3. $G = \mathbb{C}^*$, $S = \{e^{\frac{2\pi i}{5}}\}$, $\langle S \rangle$ 是 5 次单位根乘法循环群。

4. $G = \mathbb{Z}/24\mathbb{Z}$, $\langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}, \bar{12}, \bar{16}, \bar{20}\}$, 6 阶循环子群。

练习 1.10. 设 $G = \langle g \rangle$ 是 n 阶循环群。证明: G 的任意子群仍是循环群; 对 n 的每一个正因子 d , G 中存在且仅存在一个 d 阶子群。

证明. 任取子群 $H \leq G$ 。若 $H = \{e\}$, 显然是循环群。若 H 不是平凡子群, 取

$$m = \min\{t > 0 \mid g^t \in H\}.$$

断言 $H = \langle g^m \rangle$ 。

任取 $g^k \in H$, 做整数带余除法: $k = qm + r$, $0 \leq r < m$ 。

$$g^r = g^{k-qm} = g^k \cdot (g^m)^{-q} \in H.$$

由 m 的极小性, 必须 $r = 0$ 。于是 $g^k = (g^m)^q$, 得到 $H = \langle g^m \rangle$, 故子群必循环。

设 d 是 n 的正因子, 记 $n = d \cdot t$ 。取元素 g^t 。计算阶: $(g^t)^d = g^{td} = g^n = e$ 。若 $0 < k < d$, $(g^t)^k = g^{tk} \neq e$, 故 $o(g^t) = d$, 则 $\langle g^t \rangle$ 就是一个 d 阶子群。

唯一性: 任取一个 d 阶子群 H' , 已经证明循环, 设 $H' = \langle g^{m_0} \rangle$ 。阶 $o(g^{m_0}) = \frac{n}{\gcd(m_0, n)} = d$ 。

$$\frac{n}{\gcd(m_0, n)} = d \Rightarrow \gcd(m_0, n) = t = \frac{n}{d}.$$

于是 $g^{m_0} \in \langle g^t \rangle$, $H' \subseteq \langle g^t \rangle$; 两者阶相等, 故 $H' = \langle g^t \rangle$ 。唯一性得证。□

1.2 置换群 S_n 与交错群 A_n

定义 1.11. 记 $[n] = \{1, 2, \dots, n\}$ 。 S_n 是集合 $[n]$ 上全部双射 (置换) 构成的群, 运算为映射复合。 $|S_n| = n!$ 。

d -轮换 $(i_1 i_2 \cdots i_d)$: 把 $i_1 \mapsto i_2, i_2 \mapsto i_3, \dots, i_d \mapsto i_1$, 其余元素不动。两个轮换称为不交, 如果它们作用的元素集合交集为空。

引理 1.12. 任意非恒等置换 $\sigma \in S_n$, 都可以唯一地写成若干两两不交轮换的乘积。

证明. 对 n 做数学归纳。 $n = 1$, 平凡成立。假设对集合大小小于 n 的置换成立。取 $\sigma \neq \text{id}$, 存在 $x \in [n]$, $\sigma(x) \neq x$ 。考虑序列 $x, \sigma(x), \sigma^2(x), \dots$ 。集合有限, 序列必有重复。记

$$m = \min\{k > 0 \mid \sigma^k(x) = x\}.$$

得到轮换 $\sigma_1 = (x \sigma(x) \sigma^2(x) \dots \sigma^{m-1}(x))$ 。令 $\sum = [n] \setminus \{x, \sigma(x), \dots, \sigma^{m-1}(x)\}$, σ 将 $\sum$ 映射到自身。 σ 在 $\sum$ 上诱导置换 σ' 。 $\sigma = \sigma_1 \circ \sigma'$ 。 $|\sum| < n$, 归纳假设 σ' 分解为不交轮换乘积。合并得到 σ 的不交轮换分解。唯一性略。□



例 1.13. 1. $\sigma = (134)(25) \in S_5$, 不交轮换分解; 阶 $\text{lcm}(3, 2) = 6$ 。

2. $\sigma = (1234) \in S_4$, 4- 轮换, 阶 4。

3. $\sigma = (12)(13)$, 不是不交; 化简 (132) , 一个 3- 轮换。

4. S_4 中 $\sigma = (12)(34)$, 两个不交对换, 阶 2。

5. $\sigma = (123)(456)(78) \in S_8$, 阶 $\text{lcm}(3, 3, 2) = 6$ 。

注意: 置换的阶等于它不交轮换分解各个轮换长度的最小公倍数。

定义 1.14 (奇偶置换, 交错群). 2- 轮换 (ij) 称为对换。任何置换可以写成若干对换的乘积; 虽然分解方式不唯一, 但是对换个数的奇偶性是确定不变的。

- 偶置换: 可以写成偶数个对换的乘积;
- 奇置换: 可以写成奇数个对换的乘积。

$$A_n = \{\sigma \in S_n \mid \sigma \text{ 是偶置换}\},$$

称为交错群。

命题 1.15. $|A_n| = \frac{n!}{2}$ 。

例 1.16. 1. $A_3 = \{e, (123), (132)\}$, 3 阶循环群。

2. A_4 , 12 阶; 包含 8 个 3- 轮换, 3 个双对换, 单位元。

3. $(123) \in A_5$, 偶置换, 写成 $(13)(12)$, 两个对换。

4. $(1234) \in S_4$, 4- 轮换, $(14)(13)(12)$, 三个对换, 奇置换, 不属于 A_4 。

5. $V_4 = \{e, (12)(34), (13)(24), (14)(23)\} \subset A_4$ 。

1.3 陪集、Lagrange 定理, 正规子群与商群

定义 1.17 (左、右陪集). 设 $H \leq G$ 。

- 左陪集: $aH = \{ah \mid h \in H\}$;
- 右陪集: $Ha = \{ha \mid h \in H\}$ 。

注释: 一般情况下 $aH \neq Ha$, 只有正规子群才相等。

引理 1.18. 设 $H \leq G$, 对任意 $a, b \in G$:

1. $aH = bH \iff a^{-1}b \in H$;
2. 要么 $aH = bH$, 要么 $aH \cap bH = \emptyset$ 。

全体左陪集构成集合 G 的一个划分。



证明. (1) $\Rightarrow$: 若 $aH = bH$, $b \cdot e \in bH = aH$, $\exists h \in H$, $b = ah$, 于是 $a^{-1}b = h \in H$.

$\Leftarrow$: $a^{-1}b \in H$, 记 $h_0 = a^{-1}b$, $b = ah_0$. $bH = ah_0H = a(h_0H) = aH$, 得到 $aH = bH$.

(2) 反证. 若 $aH \cap bH \neq \emptyset$, 取 $x \in aH \cap bH$, 于是 $x = ah_1 = bh_2$, 得到 $a^{-1}b = h_1h_2^{-1} \in H$. 利用 (1), $aH = bH$. 故交集非空则陪集相等; 交集为空或者相等, 二者必居其一.

全体左陪集两两不交, 并且每个 $g \in G$, $g \in gH$, 全部元素被覆盖, 构成集合分划. $\square$

定理 1.19. 子群 H 的所有左陪集与所有右陪集之间存在一一映射.

定义 1.20 (子群的指数). 设 G 为任意群, $H \leq G$. 记左陪集集合

$$G/H := \{gH \mid g \in G\}.$$

定义 H 在 G 中的指数 $[G : H]$ 为集合 G/H 的基数:

$$[G : H] \stackrel{\text{def}}{=} |G/H|.$$

例 1.21. 1. $G = \mathbb{Z}$, $H = 3\mathbb{Z}$, 左陪集 $0 + 3\mathbb{Z}$, $1 + 3\mathbb{Z}$, $2 + 3\mathbb{Z}$, $[G : H] = 3$.

2. $G = S_3$, $H = \langle (12) \rangle = \{e, (12)\}$. 左陪集: $eH = \{e, (12)\}$; $(13)H = \{(13), (123)\}$; $(23)H = \{(23), (132)\}$, $[G : H] = 3$.

3. $G = \mathbb{Z}/12\mathbb{Z}$, $H = \langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}\}$. 陪集: $\bar{0} + H$, $\bar{1} + H$, $\bar{2} + H$, $\bar{3} + H$, $[G : H] = 4$.

4. $G = \text{GL}_2(\mathbb{R})$, $H = \text{SL}_2(\mathbb{R})$; 任取 $A \in \text{GL}_2(\mathbb{R})$, 左陪集 $A \cdot \text{SL}_2(\mathbb{R})$.

定理 1.22 (Lagrange 定理). G 是有限群, $H \leq G$, 则

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

推论:

1. 对任意 $g \in G$, $o(g) \mid |G|$;

2. 若 $|G| = p$ 为素数, 则 G 一定是循环群。

证明. 由引理, G 可以写成有限个两两不交左陪集的并:

$$G = a_1H \sqcup a_2H \sqcup \cdots \sqcup a_{[G:H]}H.$$

映射 $h \mapsto a_ih$ 是 $H \rightarrow a_iH$ 的双射, 每个陪集元素个数都是 $|H|$.

$$|G| = \sum_{i=1}^{[G:H]} |a_iH| = [G : H] \cdot |H|.$$

推论 1: 任取 $g \in G$, $\langle g \rangle \leq G$. Lagrange 定理 $|\langle g \rangle| = o(g)$, $o(g) \mid |G|$.

推论 2: $|G| = p$ 素数. 任取 $g \neq e \in G$, $o(g) \mid p$. $o(g) \neq 1$, 故 $o(g) = p$. 于是 $G = \langle g \rangle$, 循环群. $\square$

例 1.23. 1. $|S_3| = 6$. 子群阶只能是 1, 2, 3, 6. 不存在 4 阶、5 阶子群。



2. $|G| = 15$, 元素阶只能 1, 3, 5, 15, 不存在阶为 2, 4, 6, 7, ... 的元素。
3. A_4 , $|A_4| = 12$ 。注意: 我们无法保证对于 $|G|$ 的每一个因子 d , 找到一个 d 阶子群。12 的因子包括 6, A_4 没有 6 阶子群。这一点我们会留做练习。
4. $|G| = 7$ (素数), G 必循环, 任何非单位元生成整个群。

注释: Lagrange 定理只是必要条件, 不是充分条件; 因子不一定对应子群, A_4 无 6 阶子群是经典反例。

练习 1.24. 证明 A_4 没有 6 阶子群。

解. $|A_4| = 12$ 。反证: 假设存在子群 $H \leq A_4$, $|H| = 6$, 则指数 $[A_4 : H] = 2$, 于是 $H \triangleleft A_4$ 。 A_4 元素: 恒等; 8 个 3- 轮换; 3 个双对换 $(12)(34), (13)(24), (14)(23)$ 。一个 6 阶群一定含有 2 阶元与 3 阶元。若包含一个 3- 轮换, 由正规子群共轭封闭, 则全部 8 个 3- 轮换都落在 H , 与 $|H| = 6$ 矛盾。故不存在 6 阶子群。□

定义 1.25 (正规子群). 设 $H \leq G$, 记号 $H \triangleleft G$ 。下面三条条件彼此等价:

1. $\forall g \in G, gHg^{-1} \subset H$;
2. $\forall g \in G, gHg^{-1} = H$;
3. $\forall g \in G, gH = Hg$ 。

练习 1.26. 若子群 $H \leq G$ 的指数 $[G : H] = 2$, 证明 $H \triangleleft G$ 。

证明. 指数为 2, 则左陪集分解 $G = H \sqcup aH$; 右陪集分解 $G = H \sqcup Ha$ 。集合中不属于 H 的部分只能相等, 故 $aH = Ha$ 。

任取 $g \in G$: 如果 $g \in H$, 显然 $gH = H = Hg$; 如果 $g \notin H$, 则 $gH = aH = Ha = Hg$ 。于是对所有 $g \in G$, $gH = Hg$, 满足正规子群条件, $H \triangleleft G$ 。□

例 1.27. 1. 交换群 G 的任意子群都是正规子群。

2. $A_n \triangleleft S_n$, 指数 $[S_n : A_n] = 2$, 利用上面习题直接得到正规。
3. $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$ 。
4. $G = \mathbb{Z}$, 任意子群 $m\mathbb{Z} \triangleleft \mathbb{Z}$, $\mathbb{Z}$ 交换。

定义 1.28 (商群). 若 $H \triangleleft G$, 集合 $G/H = \{aH \mid a \in G\}$, 定义运算

$$(aH) \cdot (bH) := abH.$$

良定义证明: 若 $aH = a'H$, $bH = b'H$, 即 $a'^{-1}a \in H$, $b'^{-1}b \in H$ 。

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

因为 H 正规, $b'^{-1}(a'^{-1}a)b' \in H$, 同时 $b'^{-1}b \in H$; 乘积属于 H , 得到 $a'b'H = abH$ 。运算与代表元无关, 良定义。

此时 $(G/H, \cdot)$ 成为群, 称为 G 模 H 的商群。



例 1.29. 1. $\mathbb{Z}/m\mathbb{Z}$, 整数模 m 商群。

2. S_3/A_3 , 2 阶商群, 同构 $\mathbb{Z}/2\mathbb{Z}$ 。

3. $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*$ 。

4. $G = \mathbb{Z}/12\mathbb{Z}$, $H = \langle 4 \rangle$, 商群 G/H 是 4 阶循环群。

定义 1.30 (换位子群). 对 $x, y \in G$, 定义换位子 $[x, y] = xyx^{-1}y^{-1}$ 。换位子子群

$$[G, G] = \langle \{[x, y] \mid x, y \in G\} \rangle.$$

命题 1.31. $[G, G] \triangleleft G$, 并且:

1. $G/[G, G]$ 是 Abel 群;

2. 如果 $N \triangleleft G$ 且 G/N 是交换群, 则必有 $[G, G] \subseteq N$ 。

简言之: $[G, G]$ 是使得商群交换的最小正规子群。

证明. 先证 $[G, G] \triangleleft G$ 。任取 $g \in G$, 生成元 $[x, y]$:

$$g[x, y]g^{-1} = gxyx^{-1}y^{-1}g^{-1} = [gxg^{-1}, gyg^{-1}]$$

仍然是换位子, 属于生成元集合。于是共轭把生成元映到生成元, 故 $\forall g \in G, g[G, G]g^{-1} \subseteq [G, G]$, 正规。

(1) 商群 $G/[G, G]$ 。任取陪集 $x[G, G], y[G, G]$ 。

$$xyx^{-1}y^{-1} = [x, y] \in [G, G] \Rightarrow xy[G, G] = yx[G, G].$$

乘法交换, 商群 Abel。

(2) G/N 交换, $\forall x, y \in G, xyN = yxN$, 于是 $xyx^{-1}y^{-1} \in N$ 。所有换位子属于 N , 生成子群包含全部换位子, $[G, G] \subseteq N$ 。□

例 1.32. 1. G Abel, 则全部换位子 $[x, y] = e$, $[G, G] = \{e\}$ 。

2. $G = S_3$, $[S_3, S_3] = A_3$; 商群 S_3/A_3 是 2 阶 Abel 群。

3. $G = S_4$, $[S_4, S_4] = A_4$ 。

4. $G = \mathbb{Z}/6\mathbb{Z}$ Abel, 换位子子群是平凡子群 $\{0\}$ 。

定义 1.33 (单群). 一个群 G , 若除了 $\{e\}$ 和自身 G 之外没有其他正规子群, 则称 G 是单群。

定理 1.34. 1. A_4 不是单群。存在正规子群 Klein 四元群

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}.$$

2. 当 $n \geq 5$, A_n 是单群。

练习 1.35. 验证 $V_4 \triangleleft A_4$ 。



证明.

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}.$$

对任意 $\tau \in A_4$, $\sigma \in V_4$, 置换共轭公式:

$$\tau(ij)(kl)\tau^{-1} = (\tau(i)\tau(j))(\tau(k)\tau(l)).$$

共轭之后仍然是两个不交对换的乘积, 仍然属于 V_4 。于是 $\tau V_4 \tau^{-1} \subseteq V_4$, 得到 $V_4 \triangleleft A_4$ 。□

1.4 群同态与同构基本定理

定义 1.36 (群同态、同构). 设 G_1, G_2 为群。映射 $f: G_1 \rightarrow G_2$, 若满足

$$\forall x, y \in G_1, \quad f(xy) = f(x)f(y),$$

称 f 是群同态。

- 单同态: f 为单射;
- 满同态: f 为满射;
- 同构: 既单又满, 记作 $G_1 \cong G_2$ 。

定义核与像:

$$\ker f = \{x \in G_1 \mid f(x) = e_{G_2}\}, \quad \text{Im } f = \{f(x) \mid x \in G_1\}.$$

命题 1.37. $\ker f \triangleleft G_1$, $\text{Im } f \leq G_2$ 。

证明. 第一步证明 $\ker f \leq G_1$ 。 $f(e_1) = f(e_1 e_1) = f(e_1)f(e_1)$, 两边乘 $f(e_1)^{-1}$, $f(e_1) = e_2$, $e_1 \in \ker f$, 非空。 $\forall a, b \in \ker f$:

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e_2 e_2^{-1} = e_2 \Rightarrow ab^{-1} \in \ker f.$$

子群判定条件成立, $\ker f \leq G_1$ 。

正规: 任取 $g \in G_1$, $k \in \ker f$ 。

$$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)e_2f(g)^{-1} = e_2.$$

$gkg^{-1} \in \ker f$, $\ker f \triangleleft G_1$ 。

证明 $\text{Im } f \leq G_2$ 。 $e_2 = f(e_1) \in \text{Im } f$ 。 $\forall f(x), f(y) \in \text{Im } f$,

$$f(x)f(y)^{-1} = f(xy^{-1}) \in \text{Im } f.$$

子群条件成立, $\text{Im } f \leq G_2$ 。□

例 1.38. 1. $\det: \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^*$, 行列式同态, 满同态; 核 $\text{SL}_n(\mathbb{R})$ 。

2. $\text{sgn}: S_n \rightarrow \{\pm 1\}$, 符号同态; 核 A_n 。



3. $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$, 自然投影, 加法群满同态; 核 $m\mathbb{Z}$ 。

4. $f: \mathbb{Z} \rightarrow \mathbb{C}^*$, $f(k) = e^{2\pi i k/5}$, 同态; 核 $5\mathbb{Z}$ 。

5. 包含映射 $i: A_3 \rightarrow S_3$, 单同态, 不是满同态。

定理 1.39 (第一同构定理 (同态基本定理)). 若 $f: G_1 \rightarrow G_2$ 是群同态, 则

$$G_1/\ker f \cong \operatorname{Im} f.$$

同构映射: $\varphi: G_1/\ker f \rightarrow \operatorname{Im} f$, $\varphi(x\ker f) = f(x)$ 。

证明. 1. 良定义: 若 $x\ker f = x'\ker f$, 则 $x'^{-1}x \in \ker f$, $f(x'^{-1}x) = e_2$, 于是 $f(x')^{-1}f(x) = e_2$, $f(x) = f(x')$ 。映射定义与代表元无关。

2. 同态:

$$\varphi((x\ker f)(y\ker f)) = \varphi(xy\ker f) = f(xy) = f(x)f(y) = \varphi(x\ker f)\varphi(y\ker f).$$

3. 单射: $\varphi(x\ker f) = \varphi(y\ker f) \Rightarrow f(x) = f(y) \Rightarrow f(y^{-1}x) = e_2 \Rightarrow y^{-1}x \in \ker f \Rightarrow x\ker f = y\ker f$ 。

4. 满射: 任取 $y \in \operatorname{Im} f$, $\exists x \in G_1$, $f(x) = y$, 于是 $\varphi(x\ker f) = y$ 。

既单又满的同态, 故是同构。 □

定理 1.40 (第二同构定理). 设 $H \triangleleft G$, $K \leq G$, 则 $HK \leq G$, $H \cap K \triangleleft K$, 并且

$$HK/H \cong K/(H \cap K).$$

证明. $H \triangleleft G$, $HK = KH$ 。 HK 非空。任取 $h_1k_1, h_2k_2 \in HK$ 。

$$(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1(k_1k_2^{-1}h_2^{-1}(k_1k_2^{-1})^{-1})k_1k_2^{-1} \in HK.$$

得到 $HK \leq G$ 。

构造映射 $f: K \rightarrow HK/H$, $f(k) = kH$ 。验证同态: $f(k_1k_2) = k_1k_2H = (k_1H)(k_2H) = f(k_1)f(k_2)$ 。

满射: 任意 $hkH = kH$, 每个 HK/H 的元素都形如 kH , $k \in K$, 满射。

求核:

$$\ker f = \{k \in K \mid kH = H\} = \{k \in K \mid k \in H\} = H \cap K.$$

$H \cap K$ 是 K 的正规子群。同态基本定理:

$$K/\ker f \cong \operatorname{Im} f \Rightarrow K/(H \cap K) \cong HK/H.$$

□

定理 1.41 (第三同构定理). 设 $H \triangleleft G$, $N \triangleleft G$, $H \subseteq N$, 则 $N/H \triangleleft G/H$, 并且

$$(G/H)/(N/H) \cong G/N.$$



证明. 构造映射 $\varphi: G/H \rightarrow G/N$, $\varphi(gH) = gN$.

良定义: $gH = g'H$, $g'^{-1}g \in H \subseteq N$, $g'^{-1}g \in N$, 于是 $gN = g'N$.

同态: $\varphi(g_1H \cdot g_2H) = \varphi(g_1g_2H) = g_1g_2N = (g_1N)(g_2N) = \varphi(g_1H)\varphi(g_2H)$.

满射: 对任意 $gN \in G/N$, $\varphi(gH) = gN$, 满。

核:

$$\ker \varphi = \{gH \mid gN = N\} = \{gH \mid g \in N\} = N/H.$$

$\ker \varphi = N/H$, 故 $N/H \triangleleft G/H$.

第一同构定理:

$$(G/H)/\ker \varphi \cong \text{Im } \varphi \Rightarrow (G/H)/(N/H) \cong G/N.$$

□

定理 1.42 (子群对应定理). $\pi: G \rightarrow G/H$ 为自然投影 $g \mapsto gH$. 给出双射

$$\{K \mid H \subseteq K \leq G\} \longleftrightarrow \{\bar{K} \mid \bar{K} \leq G/H\},$$

该对应保持正规性: $K \triangleleft G \iff \pi(K) \triangleleft G/H$.

例 1.43. 1. $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/12\mathbb{Z}$; 包含 $12\mathbb{Z}$ 的 $\mathbb{Z}$ 的子群是 $d\mathbb{Z}$, $12\mathbb{Z} \subseteq d\mathbb{Z} \iff d \mid 12$; 对应 $\mathbb{Z}/12\mathbb{Z}$ 的全部子群。

2. $S_3 \rightarrow S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$; 包含 A_3 的子群: A_3, S_3 ; 对应 $\mathbb{Z}/2\mathbb{Z}$ 的子群 $\{\bar{0}\}, \mathbb{Z}/2\mathbb{Z}$ 。

3. $\text{GL}_2(\mathbb{R}) \rightarrow \mathbb{R}^*$, $\ker = \text{SL}_2(\mathbb{R})$; $\text{GL}_2(\mathbb{R})/\text{SL}_2(\mathbb{R}) \cong \mathbb{R}^*$ 。

4. $G = \mathbb{Z}/30\mathbb{Z}$, $H = \langle \bar{5} \rangle$; 商群 $G/H \cong \mathbb{Z}/5\mathbb{Z}$ 。

5. $H = V_4 \triangleleft A_4$; A_4/V_4 同构 $\mathbb{Z}/3\mathbb{Z}$ 。

练习 1.44. 证明 $\text{SL}_n(\mathbb{R}) \triangleleft \text{GL}_n(\mathbb{R})$, 并且

$$\text{GL}_n(\mathbb{R})/\text{SL}_n(\mathbb{R}) \cong \mathbb{R}^*.$$

证明. 任取 $B \in \text{GL}_n(\mathbb{R})$, $A \in \text{SL}_n(\mathbb{R})$ 。

$$\det(BAB^{-1}) = \det(B)\det(A)\det(B^{-1}) = \det(B) \cdot 1 \cdot \det(B)^{-1} = 1.$$

于是 $BAB^{-1} \in \text{SL}_n(\mathbb{R})$, 由正规子群等价条件得 $\text{SL}_n(\mathbb{R}) \triangleleft \text{GL}_n(\mathbb{R})$. 构造行列式映射

$$\det: \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^*, \quad A \mapsto \det(A).$$

由行列式性质 $\det(XY) = \det(X)\det(Y)$, $\det$ 是群同态, 并且是满射。

$$\ker(\det) = \{A \in \text{GL}_n(\mathbb{R}) \mid \det(A) = 1\} = \text{SL}_n(\mathbb{R}).$$

由同态基本定理

$$\text{GL}_n(\mathbb{R})/\ker(\det) \cong \text{Im}(\det) = \mathbb{R}^*.$$

□



1.5 群的直积

定义 1.45 (外直积). G_1, G_2 是两个群. 集合 $G_1 \times G_2$, 定义运算

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2).$$

则 $G_1 \times G_2$ 构成群, 称为外直积. 单位元 (e_1, e_2) 。

定义 1.46 (内直积). 设 G 是群, $H_1, H_2 \triangleleft G$, 满足

1. $G = H_1 H_2$;
2. $H_1 \cap H_2 = \{e\}$ 。

则称 G 是 H_1, H_2 的内直积, 此时有 $G \cong H_1 \times H_2$ 。

推广到 n 个正规子群 $H_1, \dots, H_n \triangleleft G$:

$$G = H_1 H_2 \cdots H_n, \quad H_i \cap \prod_{j \neq i} H_j = \{e\}.$$

例 1.47. 1. $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, Klein 四元群。

2. $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\gcd(2, 3) = 1$ 。

3. $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, 10 阶循环群。

4. $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, 12 阶循环群。

5. $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, 12 阶 Abel 非循环群。

定理 1.48 (中国剩余定理). $\gcd(m, n) = 1 \implies \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ 。并且可以由此推广到一般形式: 设 $m_1, m_2, \dots, m_k$ 为正整数, 且两两互素: $\gcd(m_i, m_j) = 1, i \neq j$ 。令 $M = m_1 m_2 \cdots m_k$, 则有加法群同构

$$\mathbb{Z}/M\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}.$$

同构映射为

$$\varphi(x + M\mathbb{Z}) = (x + m_1\mathbb{Z}, x + m_2\mathbb{Z}, \dots, x + m_k\mathbb{Z}).$$

练习 1.49. 设 G 是 4 阶群, 证明 G 要么同构于 $\mathbb{Z}/4\mathbb{Z}$, 要么同构于 $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 。

证明. $|G| = 4$. 情形 1: G 中存在 4 阶元素 g , 则 $G = \langle g \rangle \cong \mathbb{Z}/4\mathbb{Z}$ 。

情形 2: 没有 4 阶元素. 由 Lagrange 定理, 所有非单位元的阶只能是 2, 即 $\forall x \in G, x^2 = e$ 。对任意 $a, b \in G$,

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

所以 G 是 Abel 群. 取 a, b 为两个不同的 2 阶非单位元. 令 $H_1 = \langle a \rangle, H_2 = \langle b \rangle$. H_1, H_2 都是正规子群, $H_1 \cap H_2 = \{e\}$, $G = H_1 H_2$. 于是 $G \cong H_1 \times H_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. $\square$



1.6 群作用

定义 1.50 (群作用). 设 G 是群, X 是集合。映射 $G \times X \rightarrow X$, 记作 $(g, x) \mapsto g \cdot x$, 满足

1. $e \cdot x = x, \forall x \in X$;
2. $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x, \forall g_1, g_2 \in G, x \in X$ 。

记 $G \curvearrowright X$, 称 G 作用在集合 X 上。

- 轨道: $G \cdot x = \{g \cdot x \mid g \in G\}$;
- 稳定子 (迷向子群): $\text{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}$, 它是 G 的子群。

定理 1.51 (轨道 - 稳定子定理). G 为有限群, 作用在有限集合 X 上。对任意 $x \in X$, 存在集合双射

$$G/\text{Stab}_G(x) \xrightarrow{\sim} G \cdot x, \quad g \text{Stab}_G(x) \mapsto g \cdot x.$$

于是

$$|G \cdot x| = [G : \text{Stab}_G(x)].$$

把 X 拆分为互不相交轨道的并, 取轨道代表元集合 T :

$$|X| = \sum_{x \in T} |G \cdot x| = \sum_{x \in T} \frac{|G|}{|\text{Stab}_G(x)|}.$$

证明. 定义映射 $\psi : G/\text{Stab}_G(x) \rightarrow G \cdot x$, $\psi(g\text{Stab}_G(x)) = g \cdot x$ 。

良定义: 若 $g_1\text{Stab}_G(x) = g_2\text{Stab}_G(x)$, 则 $g_2^{-1}g_1 \in \text{Stab}_G(x)$ 。

$$(g_2^{-1}g_1) \cdot x = x \Rightarrow g_1 \cdot x = g_2 \cdot x.$$

满射: 轨道定义, 每个轨道元素形如 $g \cdot x$, $\psi(g\text{Stab}_G(x)) = g \cdot x$ 。

单射: $\psi(g_1\text{Stab}_G(x)) = \psi(g_2\text{Stab}_G(x))$, 即 $g_1x = g_2x$, $(g_2^{-1}g_1)x = x$, $g_2^{-1}g_1 \in \text{Stab}_G(x)$, 陪集相等。双射成立。

集合 X 划分成轨道不交并, 每个轨道基数等于指数, 求和公式得到。□

例 1.52. 1. $G = S_3$, 作用集合 $X = \{1, 2, 3\}$ (自然置换作用)。轨道 $G \cdot 1 = \{1, 2, 3\}$; $\text{Stab}_{S_3}(1) = \{e, (23)\}$ 。 $|G \cdot 1| = 3 = [S_3 : \text{Stab}]$ 。

2. $G = S_4$, 共轭作用在自己上面; 元素 (12) 的轨道就是全部对换, 共 6 个。

3. $G = \mathbb{Z}/6\mathbb{Z}$, 加法群作用集合 $X = \mathbb{Z}/6\mathbb{Z}$, 左平移 $g \cdot x = g + x$; 整个集合是一条轨道。

4. G 共轭作用于自身; 单位元 e 的轨道只有 $\{e\}$, $\text{Stab}_G(e) = G$ 。

5. $G = \langle (1234) \rangle \leq S_4$, 作用 $X = \{1, 2, 3, 4\}$; 轨道 $\{1, 2, 3, 4\}$; $\text{Stab} = \{e\}$ 。



定义 1.53 (中心, 中心化子, 类方程).

$$Z(G) = \{g \in G \mid \forall x \in G, gx = xg\} \quad \text{群的中心.}$$

$$C_G(a) = \{g \in G \mid ga = ag\}, \quad a \text{ 的中心化子.}$$

G 通过共轭作用于自身: $g \cdot a = gag^{-1}$. a 的轨道就是它的共轭类; $\text{Stab}_G(a) = C_G(a)$. 得到类方程:

$$|G| = |Z(G)| + \sum_{\text{非中心共轭类}} [G : C_G(a)].$$

例 1.54. 1. $G = S_3$, $Z(S_3) = \{e\}$; 类方程 $6 = 1 + 2 + 3$.

2. $G = A_4$, $Z(A_4) = \{e\}$.

3. G Abel 群, $Z(G) = G$, 全部共轭类大小为 1。

4. $G = Q_8$ 四元数群, $|G| = 8$, $Z(G) = \{\pm 1\}$. 类方程 $8 = 2 + 2 + 2 + 2$.

5. $G = S_4$, $Z(S_4) = \{e\}$.

1.7 Sylow 定理

定义 1.55 (Sylow p -子群). G 有限群, $|G| = p^r s$, p 为素数, $p \nmid s$. 若子群 $P \leq G$ 满足 $|P| = p^r$, 则称 P 是 G 的一个 Sylow p -子群. 记 n_p 为 G 中 Sylow p -子群的个数.

定理 1.56 (Sylow 定理). 1. 存在性: Sylow p -子群一定存在;

2. $n_p \equiv 1 \pmod{p}$;

3. G 的所有 Sylow p -子群互相共轭;

4. $n_p = [G : N_G(P)]$, 并且 $n_p \mid s$.

其中 $N_G(P) = \{g \in G \mid gPg^{-1} = P\}$ 是 P 在 G 中的正规化子。

例 1.57. 1. $|G| = 12 = 2^2 \cdot 3$. Sylow 2-子群阶 4; Sylow 3-子群阶 3. A_4 , $n_3 = 4$, $4 \equiv 1 \pmod{3}$, $n_3 \mid 4$.

2. $|G| = 15 = 3 \cdot 5$, $n_3 = 1$, $n_5 = 1$, Sylow 子群正规。

3. S_3 , $|S_3| = 6 = 2 \cdot 3$; Sylow 2-子群阶 2, $n_2 = 3 \equiv 1 \pmod{2}$.

4. $|G| = 20 = 2^2 \cdot 5$, $n_5 \mid 4$, $n_5 \equiv 1 \pmod{5}$, 只能 $n_5 = 1$, Sylow 5 子群正规。

5. S_4 , $|S_4| = 24 = 2^3 \cdot 3$, Sylow 2-子群阶 8; $n_3 = 4$.

练习 1.58. 证明: 15 阶群必为循环群。



证明. $|G| = 15 = 3 \cdot 5$.

先看 $p = 3$: $n_3 \mid 5$, $n_3 \equiv 1 \pmod{3}$. n_3 的可能取值为 1, 5. $5 \not\equiv 1 \pmod{3}$, 故 $n_3 = 1$. 唯一 Sylow 3-子群 $P_3 \triangleleft G$, $|P_3| = 3$.

再看 $p = 5$: $n_5 \mid 3$, $n_5 \equiv 1 \pmod{5}$. 候选 1, 3. $3 \not\equiv 1 \pmod{5}$, 得到 $n_5 = 1$. Sylow 5-子群 $P_5 \triangleleft G$, $|P_5| = 5$.

$P_3 \cap P_5 = \{e\}$, 计算

$$|P_3 P_5| = \frac{|P_3| |P_5|}{|P_3 \cap P_5|} = 15,$$

故 $G = P_3 P_5$. P_3, P_5 均正规, G 是内直积, $G \cong P_3 \times P_5 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. 由于 $\gcd(3, 5) = 1$, $\mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$, 故 G 是循环群. $\square$

1.8 综合大题

练习 1.59. 设 G 是有限群, $H \leq G$, 并且 $[G : H] = p$, p 是素数. 证明: H 包含 G 的正规子群 N , 使得 G/N 同构于 S_p 的一个子群.

证明. G 左作用于 H 的全部左陪集集合 $X = G/H$. 集合大小 $|X| = [G : H] = p$. 群作用诱导群同态 $\rho : G \rightarrow S_X \cong S_p$.

$$\ker \rho = \{g \in G \mid \forall aH \in X, gaH = aH\}.$$

任取 $g \in \ker \rho$, 取 $a = e$, $gH = H$, 得到 $g \in H$, 于是 $\ker \rho \subseteq H$. 记 $N = \ker \rho$, $N \triangleleft G$, $N \subseteq H$. 同态基本定理:

$$G/N = G/\ker \rho \cong \text{Im}(\rho) \leq S_p.$$

命题证毕. $\square$

练习 1.60. 证明不存在阶为 56 的单群.

证明. $56 = 2^3 \cdot 7$. 设 G , $|G| = 56$. 记 n_7 为 Sylow 7-子群的个数. Sylow 定理: $n_7 \mid 8$, $n_7 \equiv 1 \pmod{7}$. n_7 的可能: 1, 8.

Case1: $n_7 = 1$, Sylow 7-子群 $P_7 \triangleleft G$, 非平凡正规子群, G 不单.

Case2: $n_7 = 8$. 每个 Sylow 7-子群阶 7, 7 阶素数群, 非单位元阶 7. 不同 Sylow 7-子群交集只能是 $\{e\}$. 8 个 Sylow 7 子群, 每个子群有 6 个非单位元. 总共 $8 \times 6 = 48$ 个阶 7 的元素. G 总元素 56 个, 剩下 $56 - 48 = 8$ 个元素. Sylow 2-子群阶恰好 8, 这 8 个元素恰好构成唯一 Sylow 2-子群, $n_2 = 1$. 于是 Sylow 2-子群正规.

两种情况都存在非平凡正规子群. 56 阶群不可能是单群. $\square$

练习 1.61. 设 G 有限群, $N \triangleleft G$. 如果 G/N 和 N 都是可交换群, 问 G 是否一定可交换? 若是证明, 若否举反例.

证明. 不一定 Abel. 反例: $G = S_3$, 取 $N = A_3 \triangleleft S_3$. $N = A_3$, 3 阶循环, Abel. 商群 S_3/A_3 , 2 阶群, 也是 Abel. 但是 S_3 本身不是交换群. $\square$



练习 1.62. 设 G 是有限群, P 是 G 的 Sylow p -子群。证明 $N_G(N_G(P)) = N_G(P)$ 。

证明. 记 $M = N_G(P)$ 。显然 $M \subseteq N_G(M)$ 。只需证明 $N_G(M) \subseteq M$ 。任取 $g \in N_G(M)$, 则 $gMg^{-1} = M$ 。而 $P \leq M$, 于是 $gPg^{-1} \leq gMg^{-1} = M$ 。 P 是 M 的 Sylow p -子群; gPg^{-1} 也是 M 的 Sylow p -子群。在 M 内部 Sylow p -子群互相共轭。 $\exists m \in M$, 使得 $m(gPg^{-1})m^{-1} = P$ 。于是 $(mg)P(mg)^{-1} = P$, 得到 $mg \in N_G(P) = M$ 。 $m \in M$, $mg \in M$, 则 $g \in M$ 。于是 $N_G(M) \subseteq M$ 。 $N_G(N_G(P)) = M = N_G(P)$ 。□

2 环论

2.1 环、整环与域

本节讨论和环有关的基本概念、基本性质, 比较多且杂, 需要仔细理解并记忆, 在概念后会紧跟一些常见的例子方便理解。在本节中, 除特别说明外, 均考虑含么环。

定义 2.1 (环, ring). 设 R 是一个非空集合, R 上有两个二元运算

$$+, \cdot : R \times R \longrightarrow R,$$

分别称为加法和乘法。若满足:

1. $(R, +)$ 是一个 Abel 群, 其零元记为 0;
2. $(R, \cdot)$ 满足结合律, 即对任意 $a, b, c \in R$,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c);$$

3. 加法与乘法满足分配律, 即

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c,$$

则称 $(R, +, \cdot)$ 为一个环。

通常省略运算符号, 将环直接记为 R 。

定义 2.2 (交换环与含么环). 若对任意 $a, b \in R$ 都有

$$ab = ba, ($$

则称 R 为交换环; 否则称为非交换环。

若存在 $1 \in R$, 使得对任意 $a \in R$ 都有

$$1a = a1 = a,$$

则称 1 为 R 的单位元, 并称 R 为含么环。



例 2.3 (零环). 设

$$R = \{0\},$$

定义

$$0 + 0 = 0, \quad 0 \cdot 0 = 0.$$

则 R 构成一个含幺环, 并且

$$0 = 1.$$

这样的环称为**零环**。

例 2.4 (常见的交换环). 在通常的加法和乘法下,

$$\mathbb{Z}, \quad \mathbb{Q}, \quad \mathbb{R}, \quad \mathbb{C}$$

都是含幺交换环。

其中 $\mathbb{Z}$ 不是域, 而 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 都是域。

例 2.5 (矩阵环). 设 R 是一个含幺环, 则

$$M_n(R) = \{(a_{ij}) \mid a_{ij} \in R, 1 \leq i, j \leq n\}$$

在通常的矩阵加法和矩阵乘法下构成一个含幺环。

其零元为零矩阵, 其单位元为

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

当 $n > 1$ 且 R 非零时, $M_n(R)$ 通常不是交换环。

例 2.6 (映射环). 设 $(A, +)$ 是一个 Abel 群, 记

$$\text{End}(A) := \{f : A \rightarrow A \mid f \text{ 是群同态}\}.$$

对 $f, g \in \text{End}(A)$ 定义

$$(f + g)(a) = f(a) + g(a),$$

并定义乘法为映射的复合

$$f \cdot g := f \circ g.$$

则

$$\text{End}(A)$$

构成一个含幺环, 其零元为零映射, 单位元为恒等映射 id_A 。



例 2.7 (环的直积). 设 $R_1, \dots, R_n$ 都是环, 定义

$$R_1 \times \cdots \times R_n$$

上的运算为逐坐标运算:

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n),$$

$$(a_1, \dots, a_n)(b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n).$$

则其构成一个环。

若每个 R_i 都是含幺环, 则

$$1 = (1_{R_1}, \dots, 1_{R_n}).$$

命题 2.8 (环的基本性质). 设 R 是一个环, 则对任意 $a, b \in R$, 有

$$0a = a0 = 0.$$

此外,

$$(-a)b = a(-b) = -(ab),$$

以及

$$(-a)(-b) = ab.$$

若 R 含幺, 则

$$-a = (-1)a.$$

证明. 由分配律,

$$0a = (0 + 0)a = 0a + 0a.$$

在加法群中消去 $0a$, 得到

$$0a = 0.$$

同理可得 $a0 = 0$ 。

再由

$$0 = (a + (-a))b = ab + (-a)b$$

得到

$$(-a)b = -(ab).$$

其余结论类似。 □

定义 2.9 (子环, subring). 设 $S \subseteq R$ 是一个非空子集。若

1. $(S, +)$ 是 $(R, +)$ 的子群;
2. S 对乘法封闭, 即任意 $a, b \in S$ 都有

$$ab \in S,$$



则称 S 为 R 的一个子环。

若 R 是含幺环且 $1_R \in S$, 则称 S 为含幺子环。

例 2.10.

$$M_n(\mathbb{Q}) \subseteq M_n(\mathbb{R})$$

是一个子环。

此外,

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

是 $\mathbb{C}$ 的一个子环, 称为高斯整数环。

定义 2.11 (中心). 设 R 是一个环, 定义

$$Z(R) := \{a \in R \mid ax = xa, \forall x \in R\}.$$

称 $Z(R)$ 为 R 的中心。

命题 2.12. $Z(R)$ 是 R 的一个交换子环。

特别地,

$$R \text{ 是交换环} \iff Z(R) = R.$$

定义 2.13 (幂零元). 设 R 是一个环。如果存在正整数 n 使得

$$a^n = 0,$$

则称 $a \in R$ 为一个幂零元。

定义 2.14 (零因子与单位元). 设 R 是一个环, $a \in R - \{0\}$ 。

如果存在

$$b \in R - \{0\}$$

使得

$$ab = 0 \quad \text{或} \quad ba = 0,$$

则称 a 是一个零因子。

若 R 是含幺环, 并存在 $b \in R$ 使

$$ab = ba = 1,$$

则称 a 是一个单位元, b 称为 a 的逆元。

命题 2.15 (消去律). 设 $c \in R - \{0\}$ 不是零因子。若

$$ac = bc$$

或

$$ca = cb,$$

则

$$a = b.$$



定义 2.16 (单位群). 设 R 是含么环, 定义

$$R^\times := \{a \in R \mid a \text{ 是单位元}\}.$$

则

$$(R^\times, \cdot)$$

构成一个群, 称为 R 的**单位群**。

定义 2.17 (整环、整区、可除环与域). 设 R 是一个非零含么环。

1. 若 R 没有零因子, 则称 R 为**整环** (domain)。
2. 若 R 是交换的整环, 则称 R 为**整区** (integral domain)。
3. 若 R 的所有非零元都是可逆的, 即

$$R^\times = R - \{0\},$$

则称 R 为**除环或体** (divisible ring)。

4. 若 R 是交换的除环, 则称 R 为**域** (field)。

例 2.18.

$$\mathbb{Q}, \mathbb{R}, \mathbb{C}$$

都是域, 而

$$\mathbb{Z}$$

是整区但不是域。

事实上,

$$\mathbb{Z}^\times = \{1, -1\},$$

因此 2 在 $\mathbb{Z}$ 中不可逆。

例 2.19 (直积环不是整环). 设 R, S 是两个非零环, 则在

$$R \times S$$

中

$$(1_R, 0)(0, 1_S) = (0, 0).$$

因此 $R \times S$ 含有非零零因子, 从而不是整环。

例 2.20 (四元数体). 记

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\},$$

其乘法满足

$$i^2 = j^2 = k^2 = -1,$$

$$ij = k, \quad jk = i, \quad ki = j,$$

以及

$$ji = -k, \quad kj = -i, \quad ik = -j.$$

因此 $\mathbb{H}$ 是一个非交换可除环, 但不是交换域。



命题 2.21. 有限的整区是除环。

证明. 设 R 是有限整区, 取任意 $a \in R - \{0\}$ 。

由于

$$a, a^2, a^3, \dots$$

只有有限多个可能的值, 因此存在

$$m > n > 0$$

使得

$$a^m = a^n.$$

于是

$$a^n(a^{m-n} - 1) = 0.$$

由于 R 是整区且 $a^n \neq 0$, 由消去律得到

$$a^{m-n} = 1.$$

因此 a 可逆。

所以 R 中每个非零元都可逆, 即 R 是域。 □

注记 2.22. 这种思想在很多场合都会用到, 如同余中证明阶的存在性可以用。

例 2.23. 对于素数 p ,

$$\mathbb{Z}/p\mathbb{Z}$$

是一个域。

例如在 $\mathbb{Z}/5\mathbb{Z}$ 中,

$$2^{-1} = 3,$$

因为

$$2 \cdot 3 = 6 \equiv 1 \pmod{5}.$$

2.2 理想与商环

本节比较重要的是理想, 商环的基本定义, 以及极大理想、素理想的定义和判定条件, 以及极大理想和素理想的包含关系。

定义 2.24 (理想, ideal). 设 R 是一个环, $I \subseteq R$ 是非空子集。若满足:

1. $(I, +)$ 是 $(R, +)$ 的加法子群;
2. 对任意 $r \in R$ 与 $a \in I$, 都有

$$ra \in I, \quad ar \in I,$$

(分别叫做左吸收性和右吸收性)

则称 I 为 R 的一个**双边理想**。

除特别说明外, 本节所说理想均指双边理想。若只满足左吸收性, 则称为左理想。



注记 2.25. 理想对于环可以类比于正规子群对于群，它们都保证了后面定义商运算的合理性。

例 2.26 (平凡理想). 对任意环 R ,

$$\{0\} \quad \text{和} \quad R$$

都是 R 的理想，称为平凡理想。

定理 2.27. 设 R 是一个非零含么交换环，则 R 是域当且仅当 R 只有平凡理想。

例 2.28 ($\mathbb{Z}$ 的理想). 整数环 $\mathbb{Z}$ 的所有理想恰好是

$$n\mathbb{Z} = (n), \quad n = 0, 1, 2, \dots$$

例如

$$(2) = 2\mathbb{Z}, \quad (6) = 6\mathbb{Z}.$$

定义 2.29 (商环, quotient ring). 设 I 是 R 的一个理想。加法商群

$$R/I = \{r + I \mid r \in R\}$$

上的加法定义为

$$(r + I) + (s + I) = (r + s) + I$$

乘法定义为

$$(r + I)(s + I) := rs + I.$$

则 R/I 构成一个环，称为 R 关于 I 的商环 (quotient ring)。

注记 2.30. 上述乘法与陪集代表元的选取无关。

证明. 假设

$$r + I = r' + I, \quad s + I = s' + I.$$

则存在 $a, b \in I$ 使得

$$r = r' + a, \quad s = s' + b.$$

于是

$$\begin{aligned} rs - r's' &= (r' + a)(s' + b) - r's' \\ &= r'b + as' + ab. \end{aligned}$$

由于 I 是理想，

$$r'b, as', ab \in I.$$

因此

$$rs - r's' \in I,$$

从而

$$rs + I = r's' + I.$$

□



例 2.31 (剩余类环). 对正整数 n ,

$$\mathbb{Z}/n\mathbb{Z}$$

是模 n 的剩余类环。

例如

$$\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}.$$

其中

$$\bar{2} + \bar{3} = \bar{1},$$

而

$$\bar{2} \cdot \bar{3} = \bar{2}.$$

命题 2.32. 设 R 是一个含幺环, I 是 R 的一个理想, 则 $I = R$ 当且仅当存在一个 $v \in R^\times$ 且 $v \in I$ 。

命题 2.33. 设 $\{I_\lambda\}_{\lambda \in \Lambda}$ 是 R 的一族理想, 则

$$\bigcap_{\lambda \in \Lambda} I_\lambda$$

也是理想。

定义 2.34 (生成的理想). 设 $S \subseteq R$ 。定义

$$(S) = \bigcap_{\substack{I \text{ 理想} \\ S \subseteq I}} I.$$

称 (S) 为包含 S 的最理想, 即由 S 生成的理想。

若

$$S = \{a_1, \dots, a_n\},$$

则写作

$$(a_1, \dots, a_n).$$

若

$$I = (a),$$

则称 I 为主理想。

命题 2.35. 若 R 为含幺环, 则

$$(S) = \left\{ \sum_{i=1}^n r_i s_i k_i \mid r_i, k_i \in R, s_i \in S, n \geq 1 \right\}.$$

定义 2.36 (理想的和与积). 设 R 是环, n 是一个正整数, $I_1, I_2, \dots, I_n$ 是 R 的 n 个理想。记

$$S = \left\{ \prod_{i=1}^n b_i = b_1 b_2 \dots b_n \mid b_i \in I_i, 1 \leq i \leq n \right\}.$$

定义:



(1) 理想的和

$$\sum_{i=1}^n I_i = I_1 + I_2 + \cdots + I_n = \left\{ \sum_{i=1}^n a_i \mid a_i \in I_i, 1 \leq i \leq n \right\},$$

称为理想 $I_1, I_2, \dots, I_n$ 的和。

(2) 理想的乘积

$$\prod_{i=1}^n I_i = I_1 I_2 \cdots I_n = \left\{ \sum_{i=1}^m c_i \mid c_i \in S, 1 \leq i \leq m, m \in \mathbb{N} \right\},$$

称为理想 $I_1, I_2, \dots, I_n$ 的乘积。

命题 2.37. 在 $\mathbb{Z}$ 中,

$$(a) + (b) = (\gcd(a, b)),$$

并且

$$(a) \cap (b) = (\text{lcm}(a, b)).$$

此外,

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

定理 2.38 (理想对应定理). 考虑商映射 $j: R \rightarrow R/I$, $j(r) = \bar{r} = r + I$, $\forall r \in R$.

(1) 设 T 是 R/I 的一个理想, 记 $j^{-1}(T) = \{r \in R \mid j(r) \in T\}$, 则 $j^{-1}(T)$ 是包含 I 的理想; 设 J 是 R 的理想, 记 $J/I = \{a + I \mid a \in J\} \subseteq R/I$, 则 J/I 是 R/I 的理想。

(2) 我们有如下——对应关系:

$$\{T \mid T \text{ 是 } R/I \text{ 的理想}\} \longleftrightarrow \{J \mid J \text{ 是 } R \text{ 的理想且 } J \supseteq I\},$$

$$T \longmapsto j^{-1}(T), \quad J \longmapsto J/I.$$

定义 2.39 (极大理想, maximal ideal). 设 I 是交换含么环 R 的理想。若 $I \neq R$ 且若理想 J 满足 $I \subseteq J$, 则 $J = I$ 或 $J = R$, 则称 I 为一个极大理想 (maximal ideal)。

定理 2.40. 设 R 是交换含么环, 且 $I \neq R$ 。则

$$I \text{ 是极大理想} \iff R/I \text{ 是域}.$$

证明. 若 I 是极大理想, 则 R/I 没有非平凡理想。由域的理想判别准则, R/I 是域。

反之, 若 R/I 是域, 则其只有

$$\{0\}, \quad R/I$$

两个理想。根据理想对应定理, I 必为极大理想。 □

例 2.41. 在 $\mathbb{Z}$ 中,

$$(p)$$

是极大理想, 当且仅当 p 为素数。



定义 2.42 (素理想, prime ideal). 设 R 是交换环, P 是 R 的一个理想。若

$$P \neq R$$

且对任意 $a, b \in R$,

$$ab \in P \implies a \in P \text{ 或 } b \in P,$$

则称 P 为一个**素理想** (prime ideal)。

定理 2.43. 设 R 是交换含么环, P 是 R 的一个理想。则

$$P \text{ 是素理想} \iff R/P \text{ 是整区}.$$

例 2.44. 在 $\mathbb{Z}$ 中,

$$(p)$$

是素理想, 当且仅当 p 为素数或 $p = 0$ 。

注记 2.45. 在交换含么环中,

$$\text{极大理想} \implies \text{素理想}.$$

但在一般非交换环中, 该结论未必成立。

2.3 环同态与同构

本节比较重要的是环同态基本定理, 类似的结论在高等代数第二学期有讲过。

定义 2.46 (环同态, ring homomorphism). 设 R_1, R_2 是两个环。映射

$$f: R_1 \longrightarrow R_2$$

称为一个**环同态** (ring homomorphism), 如果对任意 $a, b \in R_1$ 都有

$$f(a + b) = f(a) + f(b),$$

$$f(ab) = f(a)f(b).$$

命题 2.47. 设 $f: R_1 \rightarrow R_2$ 是环同态, 则

$$f(0) = 0,$$

并且对任意 $a \in R_1$,

$$f(-a) = -f(a).$$

更一般地,

$$f(a_1 + \cdots + a_n) = f(a_1) + \cdots + f(a_n).$$



定义 2.48 (核与像). 设 $f: R_1 \rightarrow R_2$ 为环同态。定义

$$\ker f := \{a \in R_1 \mid f(a) = 0\},$$

称为 f 的核。

定义

$$\operatorname{Im} f := \{f(a) \mid a \in R_1\},$$

称为 f 的像。

命题 2.49. 若 $f: R_1 \rightarrow R_2$ 是非零环同态, 则 $\ker f$ 是 R_1 的理想。若 R_1, R_2 都是含么环, 则 $\operatorname{Im} f$ 是 R_2 的含么子环。

例 2.50 (自然商映射). 设 I 是 R 的一个理想。自然映射

$$\pi: R \longrightarrow R/I, \quad r \longmapsto r + I$$

是满的环同态, 并且

$$\ker \pi = I.$$

例 2.51. 设 $\alpha \in \mathbb{C}$ 。定义

$$\operatorname{ev}_\alpha: \mathbb{C}[x] \longrightarrow \mathbb{C}, \quad f(x) \longmapsto f(\alpha).$$

则 ev_α 是环同态。

定义 2.52 (环同构). 若环同态 $f: R_1 \longrightarrow R_2$ 同时是双射, 则称 f 是一个环同构。

如果存在环同构 $R_1 \longrightarrow R_2$, 则称 R_1, R_2 同构, 记为 $R_1 \cong R_2$ 。

定理 2.53 (环同态基本定理). (很重要) 设 $f: R_1 \longrightarrow R_2$ 是非零环同态, 则存在自然环同构

$$\bar{f}: R_1 / \ker f \xrightarrow{\sim} \operatorname{Im} f,$$

定义为

$$\bar{f}(a + \ker f) = f(a).$$

证明. 先验证 $\bar{f}$ 良定义。

若

$$a + \ker f = b + \ker f,$$

则

$$a - b \in \ker f,$$

所以

$$f(a - b) = 0,$$

即

$$f(a) = f(b).$$

因此 $\bar{f}$ 与代表元的选择无关。



其次, $\bar{f}$ 保持加法和乘法。

由 f 的定义,

$$\bar{f}(a + \ker f) = f(a).$$

容易验证其为满射, 而若

$$\bar{f}(a + \ker f) = 0,$$

则

$$f(a) = 0,$$

因此

$$a \in \ker f.$$

所以

$$a + \ker f = \ker f.$$

故 $\bar{f}$ 为单射。

□

例 2.54 (复数与实矩阵). 定义

$$\varphi : \mathbb{C} \longrightarrow M_2(\mathbb{R})$$

为

$$\varphi(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

则 φ 是单射且是环同态。

因此

$$\mathbb{C} \cong \text{Im } \varphi \subseteq M_2(\mathbb{R}).$$

而且

$$\det \varphi(a + bi) = a^2 + b^2 = |a + bi|^2.$$

定理 2.55 (第三同构定理). 设 $I \subseteq J$ 是 R 的两个理想, 则

$$R/J \cong (R/I)/(J/I).$$

证明. 定义

$$f : R/I \longrightarrow R/J, \quad a + I \longmapsto a + J.$$

则 f 是满射, 并且

$$\ker f = J/I.$$

由环同态基本定理得到结论。

□

注记 2.56. 这个定理当时司老师的考试中基本没有涉及, 但可以作为了解。

定义 2.57 (互素理想). 设 I, J 是含么交换环 R 的理想. 若

$$I + J = R,$$

则称 I, J 是互素的。



定理 2.58 (中国剩余定理). 设

$$n_1, \dots, n_k$$

两两互素, 则

$$\mathbb{Z}/(n_1 \cdots n_k)\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

同构由

$$\bar{a} \mapsto (\bar{a}, \dots, \bar{a})$$

给出。

定理 2.59 (中国剩余定理的环论版本). 设 $I_1, \dots, I_l$ 是 R 的理想, 满足 $I_i + I_j = R$ 对任意的 $i \neq j$ 成立, 则有

$$R/I_1 \cdots I_l \cong R/I_1 \times \cdots \times R/I_l.$$

2.4 多项式环

本节的内容大多在高等代数课上有所涉及, 重点关注多项式的带余除法定理, 另外需要理解前面的知识在多项式环中的具体运用。

定义 2.60 (多项式环). 设 R 是一个环。记

$$R[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in R, n \geq 0\}.$$

其加法按系数相加:

$$\sum_i a_i x^i + \sum_i b_i x^i = \sum_i (a_i + b_i) x^i,$$

乘法按通常的多项式乘法定义:

$$\left(\sum_i a_i x^i\right) \left(\sum_j b_j x^j\right) = \sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k.$$

则 $R[x]$ 构成一个环, 称为 R 上的一元多项式环。

命题 2.61. 若 R 是含幺环, 则 $R[x]$ 也是含幺环, 其单位元为常多项式 1。

若 R 是交换环, 则 $R[x]$ 也是交换环。

定义 2.62. 设

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \quad a_n \neq 0.$$

称 a_n 为 f 的首项系数。

若

$$a_n = 1,$$

则称 f 为首一多项式。

定义 f 的次数为

$$\deg f = n.$$

特别地, 对非零常数多项式 f ,

$$\deg f = 0.$$



通常约定

$$\deg 0 = -\infty.$$

命题 2.63. 设 R 是整区, 且 $f, g \in R[x]$ 为非零多项式, 则

$$\deg(fg) = \deg f + \deg g.$$

$$\deg(f + g) \leq \max\{\deg f, \deg g\}.$$

命题 2.64. 若 R 是整区, 则 $R[x]$ 也是整区。若 R 是域, 则 $R[x]$ 是主理想整环。

例 2.65. $\mathbb{Z}[x]$ 是整区, 但不是域。例如 x 在 $\mathbb{Z}[x]$ 中没有逆元。

定理 2.66 (带余除法). 设 F 为域, $f \in F[t] \setminus \{0\}$ 。则对任意 $g \in F[t]$, 存在唯一的多项式 $q, r \in F[t]$, 使得

$$g = fq + r, \quad (5)$$

其中 $r = 0$ 或 $\deg(r) < \deg(f)$ 。

证明. 证明分为两部分。

存在性证明: 若 $g = 0$, 取 $q = r = 0$ 即可。现设 $g \neq 0$, 令 $m := \deg(g)$ 。我们对 m 进行归纳。

(1) 当 $m = 0$ 时, 即 $g \in F^*$ 。若 $n := \deg(f) > 0$, 取 $q = 0, r = g$; 若 $n = 0$, 取 $q = f^{-1}g, r = 0$ 。

(2) 假设对次数小于 m 的多项式结论成立。设

$$g = b_0 + b_1t + \cdots + b_mt^m, \quad b_m \neq 0,$$

并设

$$f = a_0 + a_1t + \cdots + a_nt^n, \quad a_n \neq 0.$$

若 $m \geq n$, 则考虑

$$g - b_ma_n^{-1}t^{m-n}f.$$

该多项式的 m 次项系数为

$$b_m - b_ma_n^{-1}a_n = 0,$$

因此其次数不超过 $m - 1$ 。由归纳假设, 存在 $\hat{q}, r \in F[t]$, 使得

$$g - b_ma_n^{-1}t^{m-n}f = \hat{q}f + r,$$

且 $r = 0$ 或 $\deg(r) < \deg(f)$ 。于是

$$g = (\hat{q} + b_ma_n^{-1}t^{m-n})f + r,$$

取 $q = \hat{q} + b_ma_n^{-1}t^{m-n}$, 即得所需分解。

若 $m < n$, 取 $q = 0, r = g$, 则 $\deg(r) = m < n = \deg(f)$, 满足要求。

唯一性证明: 设存在两对 $(q_1, r_1), (q_2, r_2)$ 满足条件, 即

$$fq_1 + r_1 = fq_2 + r_2.$$



若 $r_1 - r_2 = 0$, 则 $(q_1 - q_2)f = 0$ 。由于 $F[t]$ 是整区, 且 $f \neq 0$, 故 $q_1 - q_2 = 0$, 从而 $q_1 = q_2$, $r_1 = r_2$ 。

若 $r_1 - r_2 \neq 0$, 则

$$\deg(r_1 - r_2) = \deg((q_1 - q_2)f) = \deg(f) + \deg(q_1 - q_2) \geq \deg(f),$$

这与 $\deg(r_i) < \deg(f)$ ($i = 1, 2$) 矛盾。因此唯一性得证。 $\square$

注记 2.67. 带余除法中的“首项系数为单位”这一条件非常重要。

例如在 $\mathbb{Z}[x]$ 中, 考虑

$$f(x) = 2x, \quad g(x) = x^2 + 1.$$

不存在 $q(x), r(x) \in \mathbb{Z}[x]$ 满足

$$x^2 + 1 = q(x)2x + r(x)$$

且

$$\deg r < 2.$$

因此不能在一般的 $\mathbb{Z}[x]$ 中随意使用多项式带余除法。

定义 2.68 (整除). 设

$$f(x), g(x) \in R[x], \quad f(x) \neq 0.$$

若存在

$$q(x) \in R[x]$$

使

$$g(x) = q(x)f(x),$$

则称 $f(x)$ 整除 $g(x)$, 记为

$$f(x) \mid g(x).$$

定义 2.69 (零点). 设 R 是交换环, $f(x) \in R[x]$ 。若

$$f(a) = 0$$

则称 $a \in R$ 是 f 的一个零点或根。

定理 2.70 (因式定理). 设 R 是交换含幺环, $a \in R$, $f(x) \in R[x]$ 。则

$$(x - a) \mid f(x) \iff f(a) = 0.$$

证明. 由带余除法,

$$f(x) = q(x)(x - a) + r,$$

其中 r 为常数。

令 $x = a$, 得到

$$f(a) = r.$$

因此

$$(x - a) \mid f(x) \iff r = 0 \iff f(a) = 0.$$

$\square$



定理 2.71 (域上的零点个数). 设 F 是域, $0 \neq f(x) \in F[x]$. 则 f 在 F 中至多有 $\deg f$ 个不同的零点。

证明. 对 $\deg f$ 作归纳。

当 $\deg f = 0$ 时显然成立。

设 $\deg f = n > 0$. 若 f 没有零点, 结论成立。

否则设 a 是 f 的一个零点。由因式定理,

$$f(x) = (x - a)g(x),$$

其中

$$\deg g = n - 1.$$

根据归纳假设, g 至多有 $n - 1$ 个不同零点。

因此 f 至多有 n 个不同零点。 □

例 2.72. 在 $\mathbb{F}_5$ 中,

$$f(x) = x^2 - 1.$$

其根为

$$x = \bar{1}, \quad x = \bar{4}.$$

恰有两个根, 与次数一致。

注记 2.73. “次数为 n 的多项式至多有 n 个根” 要求系数所在的环是域。

例如在

$$\mathbb{Z}/4\mathbb{Z}$$

中, 多项式

$$f(x) = x^2 - 1$$

可能具有超过次数的零点, 因此域的条件不能省略。

定义 2.74 (不可约多项式). 设 R 是整区,

$$0 \neq f(x) \in R[x]$$

且 f 不是单位。

若

$$f(x) = g(x)h(x)$$

必然推出

$$g(x) \in R^\times \quad \text{或} \quad h(x) \in R^\times,$$

则称 f 为 $R[x]$ 中的不可约多项式。

例 2.75. 设 F 是域, 则 $F[x]$ 中所有一次多项式都是不可约的。

若

$$f(x) \in F[x], \quad \deg f = 2 \text{ 或 } 3,$$

则 $f(x)$ 不可约 当且仅当 f 在 F 中没有零点。



例 2.76. 在 $\mathbb{Q}[x]$ 中,

$$x^2 - 2$$

没有有理根, 因此不可约。

但在 $\mathbb{R}[x]$ 中,

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}),$$

故它可约。

命题 2.77. 设 F 是域。则

$$f(x) \in F[x]$$

不可约, 当且仅当

$$(f(x))$$

是 $F[x]$ 的极大理想。

推论 2.78. 设 F 是域。则

$$F[x]/(f(x))$$

是域, 当且仅当 $f(x)$ 是不可约多项式。

例 2.79. 在 $\mathbb{R}[x]$ 中,

$$x^2 + 1$$

没有实根, 因此不可约。

所以

$$\mathbb{R}[x]/(x^2 + 1)$$

是一个域。

事实上,

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}.$$

例 2.80. 在 $\mathbb{Z}[x]$ 中考虑

$$f(x) = x^2 + 3x + 1.$$

模 2 后得到

$$\overline{f}(x) = x^2 + x + 1$$

在 $\mathbb{F}_2$ 中没有根, 因此不可约。

注记 2.81. 这类“先模素数, 再判断不可约”的方法在整系数多项式的计算中非常常用。

2.5 分式域、欧氏整区与主理想整区

本节需要注意的知识是欧氏整区和主理想整区的定义与性质, 以及他们之间的关系, 分式域在考试时没有涉及太深的东西, 是给了具体的东西来计算。



2.5.1 整区的分式域

定义 2.82 (分式域, fractional field). 可以直接类比从 Z 得到 Q 的过程。

设 R 是一个整区。在集合

$$R \times (R - \{0\})$$

上定义关系

$$(a, b) \sim (c, d) \iff ad = bc.$$

则 $\sim$ 是一个等价关系。

记 (a, b) 的等价类为

$$\frac{a}{b}.$$

定义

$$K(R) := (R \times (R - \{0\})) / \sim.$$

在 $K(R)$ 上定义

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd},$$

以及

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}.$$

则 $K(R)$ 构成一个域, 称为 R 的**分式域** (fractional field)。

例 2.83. 整数环的分式域为

$$K(\mathbb{Z}) = \mathbb{Q}.$$

高斯整数环的分式域为

$$K(\mathbb{Z}[i]) = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

例 2.84. 若 F 是一个域, 则

$$K(F[x])$$

是以 F 为系数的一元有理函数域, 通常记作

$$F(x).$$

例如

$$\frac{x^2 + 1}{x - 1} \in \mathbb{Q}(x).$$

命题 2.85. 存在自然嵌入

$$\iota : R \longrightarrow K(R), \quad a \longmapsto \frac{a}{1}.$$

该映射为单射环同态。



2.5.2 欧氏整区

定义 2.86 (欧氏整区, euclidean domain). 设 R 是整区。若存在函数

$$\varphi : R - \{0\} \longrightarrow \mathbb{Z}_{>0}$$

使得对任意

$$a, b \in R, \quad b \neq 0,$$

存在

$$q, r \in R$$

满足

$$a = bq + r,$$

并且

$$r = 0 \quad \text{或} \quad \varphi(r) < \varphi(b),$$

则称 R 为一个**欧氏整区** (euclidean domain)。对应函数称为欧氏函数。

例 2.87. 任意域都是欧氏整区。

取

$$\varphi(a) = 1$$

即可, 因为任意 $a, b \in F$ 且 $b \neq 0$ 都可以写成

$$a = b(b^{-1}a) + 0.$$

例 2.88. 取

$$\varphi(n) = |n|.$$

整数的带余除法保证对任意 $a, b \in \mathbb{Z}$ 、 $b \neq 0$, 存在 $q, r \in \mathbb{Z}$ 满足

$$a = bq + r, \quad 0 \leq |r| < |b|.$$

因此 $\mathbb{Z}$ 是欧氏整区。

例 2.89 (多项式环). 若 F 是域, 则 $F[x]$ 是欧氏整区。取

$$\varphi(f) = \deg f.$$

带余除法正是欧氏整区条件。

例 2.90 (高斯整数环). 高斯整数环

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

是欧氏整区。

取欧氏函数为范数

$$N(a + bi) = a^2 + b^2.$$



例 2.91 (整数中的欧几里得算法). 计算

$$\gcd(252, 105).$$

首先,

$$252 = 2 \cdot 105 + 42.$$

然后

$$105 = 2 \cdot 42 + 21.$$

最后

$$42 = 2 \cdot 21 + 0.$$

因此

$$\gcd(252, 105) = 21.$$

同时由回代得到

$$21 = 105 - 2 \cdot 42$$

以及

$$42 = 252 - 2 \cdot 105.$$

因此

$$21 = 105 - 2(252 - 2 \cdot 105) = 5 \cdot 105 - 2 \cdot 252.$$

命题 2.92. 在欧氏整区中, 可以通过欧几里得算法计算最大公因子。

证明. 每次使用带余除法都使欧氏函数值严格下降, 因此经过有限步后余数必为 0。

最后一个非零余数就是最大公因子的一个代表元。

□

2.5.3 主理想整区

定义 2.93 (主理想整区, principle ideal domain). 若整区 R 的每个理想都是主理想, 则称 R 为主理想整区, 简称 PID.

定理 2.94. 每一个欧氏整区都是主理想整区。

证明. 设 $I \neq (0)$ 是 R 的一个理想。

取 $d \in I - \{0\}$ 使 $\varphi(d)$ 达到最小值。有 $(d) \subseteq I$ 。

任意取 $a \in I$, 由欧氏整区的性质, 存在 $q, r \in R$ 使 $a = dq + r$, 其中

$$r = 0 \quad \text{或} \quad \varphi(r) < \varphi(d).$$

由于 $r = a - dq \in I$, 根据 d 的最小性只能有 $r = 0$ 。因此 $a = dq \in (d)$, 所以 $I = (d)$ 。

□

命题 2.95. 有包含关系

$$\text{域} \implies \text{欧氏整区} \implies \text{PID}.$$

例 2.96. 以下都是 PID:

$$\mathbb{Z}, \quad F[x] \text{ (} F \text{ 为域)}, \quad \mathbb{Z}[i].$$



例 2.97 (不是 PID 的整区). 整数多项式环

$$\mathbb{Z}[x]$$

不是 PID。

因为理想

$$(2, x)$$

不是主理想。

命题 2.98. 设 R 是整区, 则

$$R[x] \text{ 是 PID} \iff R \text{ 是域}.$$

例 2.99. 由上面的结论, $\mathbb{Q}[x]$ 是 PID, 而 $\mathbb{Z}[x]$ 不是 PID。

2.6 整区上的因式分解

本节的内容大体与初等数论课上学的一致, 可以用整数来类比理解, 本原多项式中的部分相对来说难理解一些, 最后要弄清楚欧氏整区, PID 和 UFD 这三者间的包含关系。

定义 2.100 (整除与相伴). 设 R 是整区, $a, b \in R$ 。

若存在 $c \in R$ 使

$$b = ac,$$

则称 a 整除 b , 记作

$$a \mid b.$$

若

$$a \mid b, \quad b \mid a,$$

则称 a, b 相伴。

注记 2.101. 可用理想的语言分别描述: $a \mid b$ 即 $b \in (a)$; a 和 b 相伴即 $(a) = (b)$ 。

命题 2.102. 设 R 是整区。若 $a, b \neq 0$, 则 a, b 相伴当且仅当存在单位元

$$u \in R^\times$$

使得

$$b = ua.$$

定义 2.103 (不可约元). 设 R 是整区, 且

$$a \neq 0, \quad a \notin R^\times.$$

若对任意分解

$$a = bc$$

都有

$$b \in R^\times \quad \text{或} \quad c \in R^\times,$$

则称 a 为不可约元。



例 2.104. 在 $\mathbb{Z}$ 中, 不可约元恰好是 $\pm p$, 其中 p 为素数。

例 2.105. 若 F 是域, 则 $F[x]$ 中的每一个一次多项式都不可约。

例 2.106. 多项式 $2x+2$ 在 $\mathbb{Z}[x]$ 中不是不可约元, 但在 $\mathbb{Q}[x]$ 中, 2 是单位, 因此 $2x+2$ 与 $x+1$ 相伴。

定义 2.107 (最大公因子). 设 $a_1, \dots, a_n \in R$ 不全为 0。若 d 同时整除所有 $a_1, \dots, a_n$, 则称 d 为它们的一个公因子。

若进一步:

1. d 是 $a_1, \dots, a_n$ 的公因子;
2. 对任意公因子 c , 都有 $c \mid d$,

则称 d 为 $a_1, \dots, a_n$ 的最大公因子, 记为 $\gcd(a_1, \dots, a_n)$ 。

注记 2.108. 最大公因子一般只在相伴意义下唯一。

如果 d 是最大公因子, 且 $u \in R^\times$, 那么 ud 也是最大公因子。

定义 2.109 (最小公倍元). 若 c 同时被 $a_1, \dots, a_n$ 整除, 则称 c 为它们的一个公倍元。

1. d 是 $a_1, \dots, a_n$ 的公倍元;
2. 若对任意公倍元 d 都有 $c \mid d$,

则称 c 为 $a_1, \dots, a_n$ 的最小公倍元, 记为 $\text{lcm}(a_1, \dots, a_n)$ 。

命题 2.110. 若 R 是 PID, 则任意有限个非零元素的最大公因子和最小公倍数都存在。

定理 2.111 (裴蜀定理). 若

$$d = \gcd(a_1, \dots, a_n),$$

则存在

$$r_1, \dots, r_n \in R$$

使得

$$d = r_1 a_1 + \dots + r_n a_n.$$

定义 2.112 (唯一分解整区). 整区 R 称为**唯一分解整区** (UFD), 如果:

1. 每个非零非单位元都可以分解成有限个不可约元之积;
2. 该分解在相伴和交换因子的意义下唯一。

命题 2.113 (UFD 中的基本性质). 设 R 是 UFD。

1. $\gcd(a, b)$ 和 $\text{lcm}(a, b)$ 存在;
2. 若 $\gcd(a, b) = 1$ 且 $a \mid bc$, 则 $a \mid c$;



3. 若 a 不可约且 $a \mid bc$, 则

$$a \mid b \quad \text{或} \quad a \mid c;$$

4. a 不可约, 当且仅当 (a) 是素理想。

定义 2.114 (素元). 设 R 是整区, $p \neq 0$.

若主理想

$$(p)$$

是素理想, 则称 p 为素元。

命题 2.115. 素元一定是不可约元。

在 UFD 中, 不可约元也是素元。

例 2.116. 在 $\mathbb{Z}$ 中, 素元恰好是

$$\pm p,$$

其中 p 为素数。

但在一般整区中, “不可约元” 和 “素元” 不一定相同。

引理 2.117. 设 R 为主理想整区 (PID)。则 $a \in R$ 是不可约元当且仅当主理想 $\langle a \rangle$ 是极大理想。进一步地, 若 a 不可约且 $a \mid bc$, 则 $a \mid b$ 或 $a \mid c$ 。

证明. 先证 “不可约元 $\Rightarrow$ 极大理想”。设 $a \in R$ 不可约, 且 $\langle a \rangle \subseteq J \subseteq R$, 其中 J 是理想。由于 R 是 PID , 存在 $b \in R$ 使得 $J = \langle b \rangle$, 于是 $a \in \langle b \rangle$, 即存在 $c \in R$ 使 $a = bc$ 。因 a 不可约, 故 $b \in R^\times$ 或 $c \in R^\times$ 。若 $b \in R^\times$, 则 $J = \langle b \rangle = R$; 若 $c \in R^\times$, 则 $J = \langle b \rangle = \langle a \rangle$ 。因此 $\langle a \rangle$ 是极大理想。

再证 “极大理想 $\Rightarrow$ 不可约元”。设 $\langle a \rangle$ 是极大理想, 且 $a = bc$ 。则 $\langle a \rangle \subseteq \langle b \rangle$ 。由极大性, $\langle b \rangle = \langle a \rangle$ 或 $\langle b \rangle = R$ 。若 $\langle b \rangle = R$, 则 $b \in R^\times$; 若 $\langle b \rangle = \langle a \rangle$, 则 b 与 a 相伴, 即 a 不可约。综上, 二者等价。

最后证明: 若 a 不可约且 $a \mid bc$, 则 $bc \in \langle a \rangle$ 。由上述证明可知, $\langle a \rangle$ 是极大理想, 从而是素理想 (因为 PID 中非零素理想与极大理想等价, 或直接由素理想定义)。因此 $bc \in \langle a \rangle$ 推出 $b \in \langle a \rangle$ 或 $c \in \langle a \rangle$, 即 $a \mid b$ 或 $a \mid c$ 。□

定理 2.118. 每一个 PID 都是 UFD 。

证明. (1) 存在性:

反设存在不能写成不可约元有限乘积的非零非单位元。令

$$\Sigma = \{a \neq 0 \mid a \text{ 不能分解成有限个不可约元之积}\}.$$

取 $a_1 \in \Sigma$, 它不是不可约元, 因此 $a_1 = bc$, 其中 b, c 都是非单位元。它们中至少有一个属于 Σ , 不妨记为 a_2 。于是 $(a_1) \subsetneq (a_2)$ 。重复这一过程得到严格递增的理想链

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$$

令

$$I = \bigcup_{n \geq 1} (a_n).$$



因为 R 是 PID, 存在 $a \in R$ 使 $I = (a)$,

但是 $a \in I$, 所以对某个 N , $a \in (a_N)$, 因此 $(a) \subseteq (a_N)$, 另一方面 $(a_N) \subseteq I = (a)$, 故 $(a_N) = (a)$, 与 $(a_N) \subsetneq (a_{N+1})$ 矛盾。

所以不存在这样的 Σ 。

(2) 唯一性:

设 $a = p_1 \cdots p_n = q_1 \cdots q_m$ 是两个不可约分解。

因为 $p_1 \mid q_1 \cdots q_m$, 而 PID 中不可约元对应极大理想, 从而是素元, 所以 $p_1 \mid q_j$ 对某个 j 成立。

由于 p_1, q_j 都不可约, 它们相伴。

约去相伴元后, 对剩余乘积使用归纳假设即可得到 $m = n$, 且两个分解只差一个排列以及相伴因子。□

例 2.119. 由于 $\mathbb{Z}$ 是 PID, 因此由上述定理知 $\mathbb{Z}$ 是 UFD。

同理, $F[x]$ 是 PID, 所以也是 UFD。

2.6.1 本原多项式与高斯引理

定义 2.120 (本原多项式). 设 R 是 UFD, $f(x) = a_n x^n + \cdots + a_0 \in R[x]$ 是非零多项式。若 $\gcd(a_0, \dots, a_n) = 1$, 则称 f 为本原多项式。

例 2.121. 首一多项式一定是本原多项式。可以通过对多项式做除以所有系数的最大公因子的操作得到本原多项式。

引理 2.122 (高斯引理). 设 R 为唯一分解整区 (UFD), 则:

1. 若 $f \in R[t]$, 且在 $K[t]$ ($K = K(R)$) 中有分解 $f = a(t)b(t)$, 则存在 $r, s \in K$ 使得 $rs = 1$, 并且 $ra(t) \in R[t]$ 、 $sb(t) \in R[t]$ 。
2. 若 $f \in R[t]$, 则 f 在 $R[t]$ 中本原当且仅当 f 在 $K[t]$ 中本原。

证明. (1): 设 $a(t)$ 的系数为 $\frac{p_i}{q_i}$, $b(t)$ 的系数为 $\frac{x_i}{y_i}$, 其中 $p_i, x_i, q_i, y_i \in R$ 。取 r 为所有 q_i 的最小公倍数, s 为所有 y_i 的最小公倍数, 则 $ra(t), sb(t) \in R[t]$ 。

若 $rs \in R^\times$, 则可令 $r' = r(rs)^{-1}$, $s' = s$, 则 $r's' = 1$, 且 $r'a(t) = r(rs)^{-1}a(t) \in R[t]$, $s'b(t) \in R[t]$, 结论成立。

若 $rs \notin R^\times$, 将 rs 分解为不可约元之积: $rs = h_1 h_2 \cdots h_l$ 。由 UFD 性质, $\langle h_1 \rangle$ 是素理想, 从而 $R/\langle h_1 \rangle$ 是整区。在 $(R/\langle h_1 \rangle)[t]$ 中,

$$\overline{ra} \cdot \overline{sb} = \overline{rs} \cdot \overline{ab} = \overline{rs} \cdot \overline{f} = 0,$$

其中上划线表示在商环中的像。由于 $(R/\langle h_1 \rangle)[t]$ 是整区, 故 $\overline{ra} = 0$ 或 $\overline{sb} = 0$, 即 h_1 整除 ra 的所有系数, 或整除 sb 的所有系数。因此 $\frac{ra}{h_1} \in R[t]$ 或 $\frac{sb}{h_1} \in R[t]$ 。对 rs 的每个不可约因子重复此过程, 最终可消去所有非单位因子, 化归为 $rs \in R^\times$ 的情形。

(2): 由 (1) 直接推出: 若 f 在 $R[t]$ 中可约, 则显然在 $K[t]$ 中可约。反之, 若 f 在 $K[t]$ 中可约, 设 $f = a(t)b(t)$, 其中 $a, b \in K[t]$ 且非常数。由 (1), 存在 $r, s \in K$ 使得 $ra(t), sb(t) \in R[t]$, 且 $rs = 1$, 于是 $f = (ra)(sb)$ 给出 f 在 $R[t]$ 中的非平凡分解, 因此 f 在 $R[t]$ 中可约。□



定理 2.123. 若 R 是 UFD, 则 $R[t]$ 也是 UFD.

证明. 分解存在性: 对任意非零非常数多项式 $f \in R[t]$, 令 d 为 f 各项系数的最大公因子, 则 $f = df_0$, 其中 $f_0 \in R[t]$ 是本原多项式. 若 $d \notin R^\times$, 则 d 可分解为 R 中不可约元之积; 因此只需考虑 f 为本原多项式的情形.

将 f 视为 $K[t]$ 中的多项式. 由于 $K[t]$ 是 PID, 从而是 UFD, 故 f 在 $K[t]$ 中可分解为不可约多项式之积:

$$f = p_1 p_2 \cdots p_n, \quad p_i \in K[t] \text{ 不可约.}$$

由高斯引理 (1), 可适当调整每个 p_i 的系数 (乘以 K 中的单位), 使得 $p_i \in R[t]$ 且为本原多项式. 于是 f 在 $R[t]$ 中分解为本原不可约多项式之积. 连同 d 的分解, 即得 f 的不可约分解.

分解唯一性: 设 $f \in R[t]$ 有两个不可约分解

$$f = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m,$$

其中 p_i, q_j 均为不可约元. 若 f 是常数, 则唯一性由 R 是 UFD 保证. 若 f 非常数, 可先提取本原部分: $f = df_0$, 其中 f_0 本原. 于是 f_0 在 $R[t]$ 中的不可约因子均非常数且本原. 由高斯引理 (2), 这些因子在 $K[t]$ 中仍然不可约. 由于 $K[t]$ 是 UFD, $m = n$, 且在 $K[t]$ 中 p_i 与 $q_{\sigma(i)}$ 相伴. 因 p_i, q_j 均为本原多项式, 相伴意味着相差一个 R 中的单位 (因为在 K 中相伴, 若 $p_i = cq_j$, $c \in K$, 由本原性可推出 $c \in R^\times$). 因此在 $R[t]$ 中亦相伴. 唯一性得证. $\square$

推论 2.124. 若 R 是 UFD, 则多元多项式环 $R[t_1, t_2, \dots, t_n]$ 也是 UFD.

证明. 只需反复应用定理 10.11: $R[t_1, \dots, t_n] = R[t_1, \dots, t_{n-1}][t_n]$. 由归纳, 每个步骤都保持 UFD 性质. $\square$

例 2.125. 利用高斯引理, $x^4 + 2x^3 + 3x + 1$ 在 $\mathbb{Z}[x]$ 中的不可约性可以转化到 $\mathbb{Q}[x]$ 中判断. 因此很多整数系数多项式的不可约问题最终可以化为域上的多项式问题.

注记 2.126. (很重要) 因为 $\mathbb{Z}$ 是 UFD, 所以 $\mathbb{Z}[x]$ 虽然不是 PID, 却是 UFD.

因此

$$\text{PID} \Rightarrow \text{UFD}, \quad \text{UFD} \not\Rightarrow \text{PID}$$

又结合之前的结论, 我们得到

$$\text{欧氏整区} \Rightarrow \text{PID} \Rightarrow \text{UFD}$$

例 2.127. $\mathbb{Z}[\sqrt{-5}]$ 不是 UFD. 因为 $6 = 2 \cdot 3$, 以及 $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ 给出了本质不同的分解.

这说明一般整区中的“因式分解唯一性”并不是自动成立的.

3 模论

这一节内容 24 级不做考察, 但司飞老师上课有讲到



3.1 模、模同态等

在本讲中, 设 R 始终为含单位元的环。

定义 3.1. 设 $(M, +)$ 为阿贝尔群, 若映射

$$R \times M \rightarrow M, \quad (r, m) \mapsto r \cdot m$$

满足以下条件, 则称 M 为一个左 R -模:

- (1) $(r_1 + r_2)m = r_1m + r_2m$;
- (2) $r(m_1 + m_2) = rm_1 + rm_2$;
- (3) $(r_1r_2)m = r_1(r_2m)$;
- (4) $1 \cdot m = m$ 。

显而易见, 条件 (1) 蕴涵 $0 \cdot m = 0$, 条件 (2) 蕴涵 $r \cdot 0 = 0$ 。

例 3.2. R 作用于自身的自然左乘法诱导了 R 上的一个左 R -模结构。

例 3.3. 每个阿贝尔群 G 都可以看作一个 $\mathbb{Z}$ -模。

设 M_1 和 M_2 为 R -模。

定义 3.4. 映射 $f: M_1 \rightarrow M_2$ 称为 R -模同态, 如果:

- (1) 对任意 $x, y \in M_1$, 有 $f(x + y) = f(x) + f(y)$;
- (2) 对任意 $r \in R$ 以及 $x \in M_1$, 有 $f(r \cdot x) = rf(x)$ 。

定义 3.5. 子集 $N \subset M$ 称为 R -子模, 如果:

- (1) $(N, +) \subset (M, +)$ 为子群;
- (2) 对任意 $r \in R, n \in N$, 有 $rn \in N$ 。

例 3.6. 设 M 为 R -模, 记

$$\text{Tor}(M) := \{m \in M \mid \text{存在某个 } r \in R, \text{ 使得 } rm = 0\}$$

则 $\text{Tor}(M) \subset M$ 称为 M 的挠子模 (torsion submodule) (作为习题可以验证这确实是一个子模, 验证其为 abel 群和乘法封闭性)。

命题 3.7. 设

$$\ker(f) := \{x \in M_1 \mid f(x) = 0\}$$

且

$$\text{Im}(f) := \{f(x) \mid x \in M_1\}$$

则:

- (1) $\ker(f) \subset M_1$ 和 $\text{Im}(f) \subset M_2$ 均为 R -子模;
- (2) 存在 R -模同构

$$M_1 / \ker(f) \cong \text{Im}(f)$$

证明.

□

□



设 $S \subset M$ 为非空子集，定义

$$\langle S \rangle := \bigcap_{S \subset N, N \text{ 是 } R\text{-子模}} N$$

与环论类似，可以验证 R -子模的交集仍为 R -子模。

命题 3.8. 记号同上，则

$$\langle S \rangle = \left\{ \sum_{i=1}^n r_i m_i \mid m_i \in S, n > 0 \right\}$$

证明. 记 $\text{RHS} = T$ (即右端集合)。不难证明 T 是一个 R -模。 $\square$ $\square$

3.2 主理想整环 (PID) 上的有限生成模

定理 3.9 (主理想整环上有限生成模的结构定理).

大家可以自行查阅这个定理，定理的主要内容是说主理想整环上的有限生成模具有很好的性质，比如可以分类，并且具有类似于线性空间的某些维数不变性质，如下的有限生成 abel 群结构定理是直接推论，其还可以用来证明线性代数中的 Jordan 标准型和有利标准型，由于不是司飞老师的正课内容，不过多展开。

推论 3.10. 设 G 为有限生成阿贝尔群，则……

例 3.11. 设 M 为紧流形，则其上同调群 $H^i(X, \mathbb{Z})$ 是有限生成阿贝尔群。则

$$H^i(X, \mathbb{Z}) = H^i(X, \mathbb{Z})_f \oplus H^i(X, \mathbb{Z})_{\text{tor}}, \quad H^i(X, \mathbb{Z})_f = \mathbb{Z}^{b_i}$$

b_i 称为流形 M 的 **Betti 数** (贝蒂数)，它是一个非常基础且重要的不变量。

4 域扩张和伽罗瓦理论

本节主要讨论两个相互关联的问题：一是如何通过添加多项式的根来构造更大的域；二是如何用域的自同构群刻画这些根之间的对称性。前者是域扩张理论，后者通向 Galois 理论。全文默认所有域同态均保持单位元。

4.1 域扩张的定义与扩张次数

从 $\mathbb{Q}$ 到 $\mathbb{R}$ 、从 $\mathbb{R}$ 到 $\mathbb{C}$ ，都是把一个域放进更大的域中。域扩张首先关心：加入新元素后，作为原来域上的线性空间，维数增加了多少？

定义 4.1 (域扩张). 若 F 是域 K 的子域，则称 K/F 为一个域扩张，并称 K 为 F 的扩域。若给定的是单射域同态 $\iota: F \rightarrow K$ ，可将 F 与它的像 $\iota(F)$ 认同，仍记作 $F \subseteq K$ 。

对 $a \in F, z \in K$ ，用 K 中的乘法定义数乘 $a \cdot z = az$ 。由于域的分配律与结合律， K 自然成为 F -线性空间。



定义 4.2 (扩张次数). 域扩张 K/F 的次数为

$$[K : F] = \dim_F K.$$

若此维数有限, 称 K/F 为有限扩张; 否则称为无限扩张。

例 4.3 (从实数到复数). 每个复数唯一写成 $a + bi$ ($a, b \in \mathbb{R}$), 所以 $\{1, i\}$ 是 $\mathbb{C}$ 的一组 $\mathbb{R}$ -基, $[\mathbb{C} : \mathbb{R}] = 2$ 。特别地, 扩张次数是线性空间的维数, 并非两个域中元素个数的比值。

例 4.4 (加入一个平方根). 令 $K = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ 。它对加减乘法封闭; 若 $a + b\sqrt{2} \neq 0$, 则

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \in K.$$

分母若为 0, 由 $\sqrt{2} \notin \mathbb{Q}$ 可知 $a = b = 0$, 与所取元素非零矛盾。因此 K 是域。由于 $1, \sqrt{2}$ 在 $\mathbb{Q}$ 上线性无关, $[K : \mathbb{Q}] = 2$ 。稍后会把这个域记为 $\mathbb{Q}(\sqrt{2})$ 。

定理 4.5 (塔式公式). 若 $F \subseteq K \subseteq L$, 则

$$[L : F] = [L : K][K : F].$$

特别地, 若 $[L : F]$ 有限, 则 $[K : F]$ 和 $[L : K]$ 都有限, 且都整除 $[L : F]$ 。

证明. 先考虑两个次数都有限的情形。设 $\{u_1, \dots, u_m\}$ 是 L 的 K -基, $\{v_1, \dots, v_n\}$ 是 K 的 F -基。任意 $z \in L$ 可先展开为 $\sum_i k_i u_i$, 再把各 k_i 展开为 $\sum_j c_{ij} v_j$ ($c_{ij} \in F$), 故 $\{u_i v_j\}_{i,j}$ 张成 L 。

若 $\sum_{i,j} c_{ij} u_i v_j = 0$, 按 u_i 合并系数, 先由它们在 K 上线性无关得到 $\sum_j c_{ij} v_j = 0$; 再由 v_j 在 F 上线性无关得到所有 $c_{ij} = 0$ 。因此这些乘积也是 F -线性无关的, 共有 mn 个。

若 $[K : F]$ 无限, $K \subseteq L$ 已使 L 在 F 上无限维; 若 $[L : K]$ 无限, 则 L 中任意大的 K -线性无关组也是 F -线性无关组, 故 $[L : F]$ 无限。这也说明有无限次数时的结论。□

例 4.6 (塔式公式的一个直接应用). 由 $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ 和 $[\mathbb{C} : \mathbb{R}] = 2$ 可知, $\mathbb{C}/\mathbb{Q}$ 不可能是有限扩张: 否则塔式公式会使 $\mathbb{R}/\mathbb{Q}$ 有限; 而一个有限维的 $\mathbb{Q}$ -线性空间至多可数, $\mathbb{R}$ 却不可数。

定义 4.7 (生成子域). 设 K/F 为域扩张, $S \subseteq K$ 。 K 中所有包含 $F \cup S$ 的子域的交, 记作 $F(S)$; 它是包含 $F \cup S$ 的最小子域。若 $S = \{\alpha_1, \dots, \alpha_n\}$, 写作 $F(\alpha_1, \dots, \alpha_n)$; 只有一个元素时称 $F(\alpha)/F$ 为单扩张。

例 4.8 (生成子域的记号). 上例的域可写成 $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$: 任何包含 $\mathbb{Q}$ 和 $\sqrt{2}$ 的子域都包含右边的元素。类似地, $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$, 也是一个二次扩张。

命题 4.9 (生成子域的具体形式). 若 $\alpha_1, \dots, \alpha_n \in K$, 则

$$F(\alpha_1, \dots, \alpha_n) = \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} : f, g \in F[x_1, \dots, x_n], \quad g(\alpha_1, \dots, \alpha_n) \neq 0 \right\}.$$

证明. 右侧包含 F 与所有 α_i , 且在加、减、乘和非零元素取逆下封闭, 因此是一个子域。任何包含 F 与 α_i 的子域也必包含右侧每一个分式。由最小性, 两边相等。□

注记 4.10 (子环与子域). $F[\alpha] = \{f(\alpha) : f \in F[x]\}$ 是由 F 和 α 生成的子环, $F(\alpha)$ 还允许对非零元素取逆。例如把 x 看成有理函数域 $F(x)$ 中的未定元, 则 $1/x \in F(x)$, 但 $1/x \notin F[x]$ 。何时 $F[\alpha] = F(\alpha)$, 将在下一小节说明。



4.2 代数扩张与极小多项式

生成子域的元素一般要写成分式，但加入一个满足多项式方程的元素时，情形会简单得多。

定义 4.11 (代数元与超越元). 设 K/F 为域扩张, $\alpha \in K$ 。如果存在非零多项式 $f(x) \in F[x]$ 使得 $f(\alpha) = 0$, 称 α 在 F 上代数; 否则称为超越。若 K 的每个元素都在 F 上代数, 称 K/F 为代数扩张。

例 4.12. $\sqrt{2}$ 在 $\mathbb{Q}$ 上代数, 因为它满足 $x^2 - 2 = 0$; i 也在 $\mathbb{Q}$ 上代数, 因为它满足 $x^2 + 1 = 0$ 。每个 $a \in F$ 都在 F 上代数: a 是 $x - a$ 的根。把未定元 x 放入 $F(x)$ 时, 它在 F 上超越, 因为非零多项式不可能作为有理函数等于 0。

定义 4.13 (极小多项式). 设 α 在 F 上代数。在所有以 α 为根的非零多项式中, 取次数最小者并化为首一, 得到 α 在 F 上的极小多项式, 记为 $m_{\alpha, F}(x)$ 。

命题 4.14 (极小多项式的基本性质). 极小多项式存在且唯一, 并满足:

1. $m_{\alpha, F}$ 在 $F[x]$ 中不可约;
2. 对任意 $f \in F[x]$, $f(\alpha) = 0$ 当且仅当 $m_{\alpha, F} \mid f$ 。

证明. 代数性保证非零零化多项式存在, 故可选次数最小且首一的 $m = m_{\alpha, F}$ 。若 $f(\alpha) = 0$, 用多项式带余除法写 $f = qm + r$, 其中 $r = 0$ 或 $\deg r < \deg m$ 。代入 α 得 $r(\alpha) = 0$; 由 m 次数最小, $r = 0$ 。反之, $m \mid f$ 显然给出 $f(\alpha) = 0$ 。若还有另一首一最小次数的零化多项式 m' , 则 $m \mid m'$ 且次数相等, 故 $m = m'$ 。

若 $m = gh$, 其中 $g, h \in F[x]$ 均为正次数, 则 $0 = m(\alpha) = g(\alpha)h(\alpha)$ 。域中无零因子, $g(\alpha) = 0$ 或 $h(\alpha) = 0$, 与次数最小矛盾, 因此 m 不可约。□

例 4.15 (辨认极小多项式). $\sqrt{2}$ 是 $x^4 - 4$ 的根, 但 $x^4 - 4 = (x^2 - 2)(x^2 + 2)$ 并不是它的极小多项式。由于 $\sqrt{2} \notin \mathbb{Q}$, $x^2 - 2$ 在 $\mathbb{Q}[x]$ 中没有根, 因而不可约, 故 $m_{\sqrt{2}, \mathbb{Q}} = x^2 - 2$ 。基域很关键: $m_{\sqrt{2}, \mathbb{R}} = x - \sqrt{2}$ 。

定理 4.16 (单扩张的结构). 设 $\alpha \in K$ 。

1. 若 α 在 F 上代数, 且 $\deg m_{\alpha, F} = n$, 则

$$F(\alpha) = F[\alpha] \cong F[x]/(m_{\alpha, F}), \quad [F(\alpha) : F] = n,$$

$\{1, \alpha, \dots, \alpha^{n-1}\}$ 是它的一组 F -基。

2. 若 α 在 F 上超越, 则 $F[\alpha] \cong F[x]$, 而 $F(\alpha) \cong F(x)$, 其中 $F(x)$ 是 $F[x]$ 的分式域。

证明. 考察代入同态 $\varphi : F[x] \rightarrow K$, $f \mapsto f(\alpha)$ 。它的像是 $F[\alpha]$ 。若 α 代数, 前一命题说明 $\ker \varphi = (m_{\alpha, F})$; 第一同构定理于是给出 $F[\alpha] \cong F[x]/(m_{\alpha, F})$ 。极小多项式不可约, 故这个商环是域, 从而 $F[\alpha]$ 已经等于包含 F 与 α 的最小子域 $F(\alpha)$ 。将每个多项式除以 $m_{\alpha, F}$, 得到唯一的低于 n 次的余式, 由此得到上述基与次数。

若 α 超越, $\ker \varphi = 0$, 所以 $F[\alpha] \cong F[x]$; 再取分式域便得到 $F(\alpha) \cong F(x)$ 。□



例 4.17 (代入单扩张的结构). $m_{i,\mathbb{Q}} = x^2 + 1$, 所以 $\mathbb{Q}(i) \cong \mathbb{Q}[x]/(x^2 + 1)$, 以 $\{1, i\}$ 为 $\mathbb{Q}$ -基. 若 ζ 是非实的三次单位根, 则 $\zeta^2 + \zeta + 1 = 0$, 而 $x^2 + x + 1$ 在 $\mathbb{Q}$ 上没有根, 故 $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$, $\{1, \zeta\}$ 是一组基.

推论 4.18. $\alpha \in K$ 在 F 上代数, 当且仅当 $[F(\alpha) : F] < \infty$.

证明. 正向由单扩张的结构得到. 反向若 $[F(\alpha) : F] = n$, 则 $n + 1$ 个元素 $1, \alpha, \dots, \alpha^n$ 在 F 上线性相关, 其非平凡线性关系就是一个以 α 为根的非零多项式. $\square$

定理 4.19 (有限扩张的判定). 对域扩张 K/F , 以下条件等价:

1. $[K : F] < \infty$;
2. 存在有限多个在 F 上代数的元素 $\alpha_1, \dots, \alpha_n$, 使 $K = F(\alpha_1, \dots, \alpha_n)$.

特别地, 有限扩张必是代数扩张.

证明. 若满足第二条, 令 $K_0 = F$, $K_i = F(\alpha_1, \dots, \alpha_i)$. α_i 在 F 上满足的非零多项式也属于 $K_{i-1}[x]$, 所以它在 K_{i-1} 上代数. 由单扩张结构和塔式公式,

$$[K : F] = \prod_{i=1}^n [K_i : K_{i-1}] < \infty.$$

反之, 若 $[K : F] = n$, 取 K 的一组 F -基 $\alpha_1, \dots, \alpha_n$, 则 $K = F(\alpha_1, \dots, \alpha_n)$. 每个 α_i 的幂在有限维 F -线性空间 K 中线性相关, 因而 α_i 在 F 上代数. 同样的理由适用于任意 $z \in K$, 故 K/F 是代数扩张. $\square$

例 4.20 (用塔式公式计算次数). 考虑 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. 前一步是二次扩张. 若 $\sqrt{3} = a + b\sqrt{2}$ ($a, b \in \mathbb{Q}$), 平方可得 $3 = a^2 + 2b^2 + 2ab\sqrt{2}$, 故 $ab = 0$. 当 $b = 0$ 时 $a^2 = 3$; 当 $a = 0$ 时 $b^2 = 3/2$. 这两种情形都不可能为有理数解. 因此 $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, $x^2 - 3$ 在 $\mathbb{Q}(\sqrt{2})$ 上不可约. 由单扩张结构和塔式公式,

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4,$$

乘积基为 $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

定义 4.21 (复合域). 若 K_1/F 与 K_2/F 都是同一个域 Ω 的子域, 定义它们的复合域为 $K_1K_2 = F(K_1 \cup K_2)$. 它是 Ω 中同时包含 K_1 、 K_2 的最小子域.

命题 4.22 (复合域的次数). 若 $[K_1 : F] = m$ 、 $[K_2 : F] = n$ 均有限, 则

$$[K_1K_2 : F] \leq mn.$$

若 $\gcd(m, n) = 1$, 则等号成立.

证明. 取 K_1/F 的基 $u_1, \dots, u_m$ 和 K_2/F 的基 $v_1, \dots, v_n$. 令 V 为所有 $u_i v_j$ 在 F 上的张成空间. 它等于所有 $\sum_j a_j v_j$ ($a_j \in K_1$) 的集合, 因而包含 K_1 与 K_2 . 任取 $v_j v_k \in K_2$, 将它按 $v_1, \dots, v_n$ 展开, 便知 V 在乘法下封闭; 它当然也在加减法下封闭. 又 V 是 Ω 内有限维的 K_1 -代数, 且没有零因子. 若 $0 \neq z \in V$, 乘以 z 给出 K_1 -线性单射 $V \rightarrow V$, 有限维使其为满射, 于是存在 $w \in V$ 满足 $zw = 1$. 故 V 是域, 从而 $V = K_1K_2$. 由于 V 由 mn 个乘积张成, 得 $[K_1K_2 : F] \leq mn$.

塔式公式还说明 m 、 n 都整除 $[K_1K_2 : F]$. 若二者互素, mn 也整除该次数; 与上述上界合用即得等号. $\square$



例 4.23 (等号与严格不等式). $\mathbb{Q}(\sqrt{2})$ 与 $\mathbb{Q}(\sqrt{3})$ 的复合域是 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, 上例算得其次数为 $4 = 2 \cdot 2$, 尽管两个次数并不互素. 若 $K_1 = K_2 = \mathbb{Q}(\sqrt{2})$, 则复合域仍为 $\mathbb{Q}(\sqrt{2})$, 次数是 $2 < 2 \cdot 2$. 所以“次数互素”是等号成立的充分条件, 并非必要条件.

定理 4.24 (代数性的传递). 若 $F \subseteq K \subseteq L$, 且 K/F 、 L/K 都是代数扩张, 则 L/F 也是代数扩张.

证明. 任取 $\alpha \in L$, 设它在 K 上满足

$$\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0, \quad a_i \in K.$$

令 $E = F(a_0, \dots, a_{d-1})$. 各 a_i 在 F 上代数, 故由有限扩张的判定知 E/F 有限; α 在 E 上代数, 故 $E(\alpha)/E$ 有限. 塔式公式给出 $[E(\alpha) : F] < \infty$, 所以 α 在 F 上代数. $\square$

命题 4.25. 在给定扩域 K/F 中, 所有在 F 上代数的元素构成 K 的一个子域.

证明. 若 $\alpha, \beta \in K$ 都在 F 上代数, 则 $F(\alpha, \beta)/F$ 有限, 因此其中的每个元素都在 F 上代数. 特别地, $\alpha \pm \beta$ 、 $\alpha\beta$ 以及 $\beta \neq 0$ 时的 α/β 均在 F 上代数; 而 $0, 1 \in F$ 也在 F 上代数, 故结论成立. $\square$

例 4.26 (代数但无限的扩张). 令 $\overline{\mathbb{Q}} = \{z \in \mathbb{C} : z \text{ 在 } \mathbb{Q} \text{ 上代数}\}$. 由前一命题, 它是 $\mathbb{C}$ 的子域, 且 $\overline{\mathbb{Q}}/\mathbb{Q}$ 是代数扩张. 它包含每个 $\sqrt[d]{2}$ ($d \geq 1$). 多项式 $x^d - 2$ 在 $\mathbb{Q}[x]$ 中不可约: 若它可约, 由前文的 Gauss 引理, 可分解为两个正次数的首一整系数多项式; 模 2 后它们的乘积是 x^d , 因此两个常数项都为偶数, 乘积便被 4 整除, 与原多项式的常数项 -2 矛盾. 于是 $[\mathbb{Q}(\sqrt[d]{2}) : \mathbb{Q}] = d$, 这些次数没有统一上界, $\overline{\mathbb{Q}}/\mathbb{Q}$ 不是有限扩张.

4.3 分裂域与代数闭域

定义 4.27 (分裂域). 设 $f(x) \in F[x]$, $\deg f \geq 1$. 若扩域 K/F 满足:

1. f 在 $K[x]$ 中完全分解为一次因式;
2. K 由 f 的全部根在 F 上生成,

则称 K 是 f 在 F 上的分裂域. 换言之, 分裂域是使 f 完全分解的最小扩域.

例 4.28. $x^2 + 1$ 在 $\mathbb{Q}$ 上的分裂域是 $\mathbb{Q}(i)$; 在 $\mathbb{R}$ 上的分裂域是 $\mathbb{C}$. 同一个多项式相对于不同基域, 分裂域可能不同.

例 4.29 (三次多项式的分裂域). 设 $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, 取 $\alpha = \sqrt[3]{2}$, 并令 $\omega = e^{2\pi i/3}$. 三个根为 $\alpha, \omega\alpha, \omega^2\alpha$, 故分裂域为

$$K = \mathbb{Q}(\alpha, \omega).$$

由 Eisenstein 判别法, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. 又 $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ 而 $\omega \notin \mathbb{R}$, 故 $[K : \mathbb{Q}(\alpha)] = 2$. 因此 $[K : \mathbb{Q}] = 6$. 注意 $\mathbb{Q}(\alpha)$ 只含一个根, 并不是分裂域.

定理 4.30 (分裂域的存在性). 任意非常数多项式 $f(x) \in F[x]$ 都存在分裂域, 而且该分裂域是 F 的有限扩张, 其次数不超过 $(\deg f)!$.



证明. 对 $n = \deg f$ 归纳. $n = 1$ 时, f 已经在 F 中分解, 取 $K = F$ 即可. 设 $n > 1$, 取 f 的一个不可约因子 $p(x)$, 并令

$$F_1 = F[x]/(p), \quad \alpha = x + (p) \in F_1.$$

于是 F_1 是域, 且 $[F_1 : F] = \deg p \leq n$, 并且 $p(\alpha) = 0$. 把 f 看成 $F_1[x]$ 中的多项式, 则 $x - \alpha$ 整除 f , 故存在 $g(x) \in F_1[x]$ 使

$$f(x) = (x - \alpha)g(x), \quad \deg g = n - 1.$$

由归纳假设, g 在某个有限扩域 K/F_1 中有分裂域. 于是 f 在 K 中完全分解; 取 f 的全部根生成的子域, 便得到 f 在 F 上的分裂域 K_f .

此外,

$$[K_f : F] \leq [K : F] = [K : F_1][F_1 : F] \leq (n - 1)!n = n!.$$

这也证明了分裂域扩张次数的估计. □

定理 4.31 (分裂域的唯一性). 设 K, K' 都是 $f(x) \in F[x]$ 在 F 上的分裂域, 则存在保持 F 中元素不动的域同构 $K \cong K'$. 因此分裂域在 F -同构意义下唯一.

证明. 我们证明稍强的结论: 若 $\nu : F \rightarrow F'$ 是域同构, 且 $\tilde{f} = \nu(f) \in F'[x]$, 那么 f 和 $\tilde{f}$ 的分裂域之间存在延拓 ν 的域同构. 对 $n = \deg f$ 归纳.

当 $n = 1$ 时, 分裂域就是基域, 结论显然成立. 设 $n > 1$, 取 f 的不可约因子 p , 并分别取其在两个分裂域中的根 α 和 α' . 系数同构 ν 将 p 送到 $\tilde{p}$, 因此

$$F(\alpha) \cong F[x]/(p), \quad F'(\alpha') \cong F'[x]/(\tilde{p}).$$

存在唯一的域同构

$$\nu_1 : F(\alpha) \longrightarrow F'(\alpha'), \quad \nu_1|_F = \nu, \quad \nu_1(\alpha) = \alpha'.$$

在 $F(\alpha)[x]$ 中写

$$f(x) = (x - \alpha)g(x), \quad \deg g = n - 1.$$

将 g 的系数经 ν_1 映射, 得到 $\tilde{g} \in F'(\alpha')[x]$. 原分裂域是 g 在 $F(\alpha)$ 上的分裂域, 另一个分裂域是 $\tilde{g}$ 在 $F'(\alpha')$ 上的分裂域. 由归纳假设, ν_1 可延拓为这两个分裂域之间的同构. 它同时把 α 送到 α' , 因而给出所需的 F -同构 $K \cong K'$. □

定义 4.32 (代数闭域与代数闭包). 域 Ω 称为代数闭域, 如果 $\Omega[x]$ 中每个非常数多项式都在 Ω 中有根, 等价地, 每个非常数多项式都能在 $\Omega[x]$ 中完全分解.

若 $\bar{F}/F$ 是代数扩张且 $\bar{F}$ 为代数闭域, 则称 $\bar{F}$ 是 F 的一个代数闭包.

例 4.33. 代数基本定理说明 $\mathbb{C}$ 是代数闭域, 所以 $\mathbb{C}$ 是 $\mathbb{R}$ 的代数闭包. 但 $\mathbb{C}$ 不是 $\mathbb{Q}$ 的代数闭包, 因为 $\mathbb{C}/\mathbb{Q}$ 中含有 π 等超越元. $\mathbb{Q}$ 在 $\mathbb{C}$ 中所有代数元组成的 $\overline{\mathbb{Q}}$ 才是 $\mathbb{Q}$ 的一个代数闭包.

定理 4.34 (代数闭包的存在与唯一性). 每个域 F 都有代数闭包; 任意两个代数闭包在保持 F 不动的域同构意义下唯一.



证明. 先证存在性. 我们先说明: 对任意域 K , 存在一个代数扩张 K^+/K , 使 $K[x]$ 中每个非常数多项式都在 K^+ 中至少有一个根.

对每个首一非常数多项式 $f \in K[x]$ 引入一个不定元 X_f , 并在多项式环

$$R = K[X_f : f \in K[x] \text{ 首一且 } \deg f \geq 1]$$

中令 I 为所有 $f(X_f)$ 生成的理想. 理想 I 是真理想. 否则 $1 \in I$, 则表示 1 的等式只涉及有限多个多项式 $f_1, \dots, f_s$ 和有限多个不定元. 逐次添加 $f_1, \dots, f_s$ 的根, 可得某个扩域 M/K 及根 $\alpha_i \in M$. 把相关的 X_{f_i} 代入 α_i (其余有限个不定元任意取值), 等式右端全部变为 0, 左端仍为 1, 矛盾.

由 Zorn 引理, I 包含在某个极大理想 $\mathfrak{m}$ 中. 于是 $K^+ = R/\mathfrak{m}$ 是域, 且 $X_f + \mathfrak{m}$ 是 f 的一个根. K^+ 由这些在 K 上代数的元素生成, 所以 K^+/K 是代数扩张.

现在递归定义 $F_0 = F$ 、 $F_{n+1} = F_n^+$, 并令

$$\bar{F} = \bigcup_{n=0}^{\infty} F_n.$$

代数性的传递以及“任一元素只涉及有限层”说明 $\bar{F}/F$ 是代数扩张. 任取非常数多项式 $h \in \bar{F}[x]$, 它只有有限多个系数, 故这些系数全都落在某个 F_N 中; 按 F_{N+1} 的构造, h 在 $F_{N+1} \subseteq \bar{F}$ 中有根. 因此 $\bar{F}$ 是代数闭域, 存在性得证.

再证唯一性. 设 $\bar{F}$ 和 $\bar{F}'$ 是 F 的两个代数闭包. 令 $\mathcal{S}$ 为所有二元组 (L, φ) 的集合, 其中 $F \subseteq L \subseteq \bar{F}$, 且

$$\varphi : L \longrightarrow \bar{F}'$$

是固定 F 的域嵌入. 按扩张关系对 $\mathcal{S}$ 排序. 链的并给出上界, 故由 Zorn 引理存在极大元 (L, φ) .

若 $L \neq \bar{F}$, 取 $\alpha \in \bar{F} \setminus L$. 令 p 为 α 在 L 上的极小多项式. 将 p 的系数经 φ 映射后得到 $\varphi(p) \in \varphi(L)[x]$. 由于 $\bar{F}'$ 代数闭, $\varphi(p)$ 在其中有根 β . 由商环同构

$$L(\alpha) \cong L[x]/(p) \cong \varphi(L)[x]/(\varphi(p))$$

可将 φ 延拓到 $L(\alpha)$, 这与极大性矛盾. 因此 $L = \bar{F}$.

此时 $\varphi(\bar{F})$ 是 $\bar{F}'$ 的子域, 并且与代数闭域 $\bar{F}$ 同构, 因而本身代数闭. 任取 $\beta \in \bar{F}'$, 由于 $\bar{F}'/F$ 代数, β 也代数于 $\varphi(\bar{F})$; 代数闭性迫使 $\beta \in \varphi(\bar{F})$. 故 φ 满射, 从而是保持 F 不动的同构. $\square$

注记 4.35. “唯一”始终指“在 F -同构意义下唯一”, 并不是说两个代数闭包作为集合逐点相同. 实际计算时通常先固定一个代数闭包 $\bar{F}$, 随后把所有代数扩张都放在其中讨论.

4.4 域扩张的嵌入与自同构

定义 4.36 (F -嵌入与 F -自同构). 设 E/F 、 K/F 为域扩张. 若域同态 $\sigma : E \rightarrow K$ 满足 $\sigma(a) = a$ 对所有 $a \in F$ 成立, 则称 σ 为一个 F -嵌入. 若 $\sigma : E \rightarrow E$ 还是满射, 则称其为 E 的一个 F -自同构. 所有 F -自同构在复合运算下构成群, 记为 $\text{Aut}(E/F)$.



引理 4.37 (单扩张上的嵌入由生成元的像决定). 设 $E = F(\alpha)$, $\sigma : E \rightarrow K$ 是 F -嵌入, 则 σ 完全由 $\sigma(\alpha)$ 决定. 若 α 在 F 上代数, 则 $\sigma(\alpha)$ 必是 $m_{\alpha, F}(x)$ 在 K 中的根. 反过来, $m_{\alpha, F}$ 在 K 中的每个根 β 都唯一确定一个 F -嵌入

$$F(\alpha) \longrightarrow K, \alpha \longmapsto \beta.$$

证明. 因为 σ 固定 F , 所以对 $f(x) \in F[x]$ 有 $\sigma(f(\alpha)) = f(\sigma(\alpha))$, 故 σ 由 $\sigma(\alpha)$ 决定. 又

$$0 = \sigma(m_{\alpha, F}(\alpha)) = m_{\alpha, F}(\sigma(\alpha)),$$

所以 $\sigma(\alpha)$ 是极小多项式的根.

反之, 若 $m_{\alpha, F}(\beta) = 0$, 利用 $F(\alpha) \cong F[x]/(m_{\alpha, F}) \cong F(\beta)$, 即可得到把 α 送到 β 的唯一 F -嵌入. $\square$

例 4.38 (二次域的两个嵌入). 设 $E = \mathbb{Q}(\sqrt{2})$. 由于 $x^2 - 2$ 的根为 $\pm\sqrt{2}$, E 到 $\mathbb{C}$ 的 $\mathbb{Q}$ -嵌入恰有两个:

$$a + b\sqrt{2} \longmapsto a + b\sqrt{2}, \quad a + b\sqrt{2} \longmapsto a - b\sqrt{2}.$$

二者的像都落在 E 中, 因而都是 E 的 $\mathbb{Q}$ -自同构.

例 4.39 (有嵌入但没有相应自同构). 设 $E = \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. 极小多项式 $x^3 - 2$ 在 $\mathbb{C}$ 中有三个根, 故 E 到 $\mathbb{C}$ 有三个 $\mathbb{Q}$ -嵌入. 但是另外两个嵌入把 $\sqrt[3]{2}$ 送到非实根, 像不在 E 中. 因此 $\text{Aut}(E/\mathbb{Q})$ 只有恒等映射. 这正反映出 E 没有包含极小多项式的全部根.

定理 4.40 (嵌入延拓定理). 设 E/F 是代数扩张, Ω 是代数闭域. 任意域嵌入 $\sigma : F \rightarrow \Omega$ 都可延拓为从 E 到 Ω 的域嵌入. 特别地, 当 $F \subseteq \Omega$ 且 σ 是恒等映射时, 可得到一个 F -嵌入. 若 $E = F(\alpha_1, \dots, \alpha_n)$, 则可逐次选择相应极小多项式的根来延拓嵌入.

证明. 先处理有限生成情形. 令 $E_i = F(\alpha_1, \dots, \alpha_i)$, 其中 $E_0 = F$. 设已经得到 $\sigma_{i-1} : E_{i-1} \rightarrow \Omega$. 令 $m_i(x)$ 为 α_i 在 E_{i-1} 上的极小多项式, 并将其系数经 σ_{i-1} 映射, 得到

$$\sigma_{i-1}(m_i)(x) \in \sigma_{i-1}(E_{i-1})[x].$$

由于 Ω 代数闭, 该多项式在 Ω 中有根 β_i . 商环同构给出一个延拓

$$\sigma_i : E_i \longrightarrow \Omega, \quad \sigma_i|_{E_{i-1}} = \sigma_{i-1}, \quad \sigma_i(\alpha_i) = \beta_i.$$

迭代即可得到 $E \rightarrow \Omega$ 的嵌入.

对一般的代数扩张, 令 $\mathcal{T}$ 为所有二元组 (L, τ) 的集合, 其中 $F \subseteq L \subseteq E$, 且 $\tau : L \rightarrow \Omega$ 是 σ 的延拓, 按延拓关系排序. 链的并仍给出上界, 故由 Zorn 引理有极大元 (L, τ) . 若 $L \neq E$, 取 $\alpha \in E \setminus L$. 因为 E/F 代数, α 在 L 上代数; 对其极小多项式按上面的单扩张步骤即可把 τ 延拓到 $L(\alpha)$, 矛盾. 因此 $L = E$. $\square$

定义 4.41 (嵌入数). 固定包含 E 的代数闭域 Ω , 记所有 F -嵌入 $E \rightarrow \Omega$ 的集合为 $\text{Emb}(E/F)$. 其元素个数称为 E/F 的嵌入数.



定理 4.42. 若 $[E : F] < \infty$, 则

$$|\text{Emb}(E/F)| \leq [E : F].$$

特别地, $|\text{Aut}(E/F)| \leq [E : F]$.

证明. 把 E 写成 $F(\alpha_1, \dots, \alpha_n)$, 并令 $E_i = F(\alpha_1, \dots, \alpha_i)$. 固定一个 F -嵌入 $\tau : E_{i-1} \rightarrow \Omega$. 若 m_i 是 α_i 在 E_{i-1} 上的极小多项式, 则 $\tau(m_i)$ 在 Ω 中至多有 $\deg m_i = [E_i : E_{i-1}]$ 个根; 由单扩张上的嵌入对应, 每个延拓都由这些根中的一个唯一决定. 因此每个嵌入至多有 $[E_i : E_{i-1}]$ 个延拓. 逐步相乘并使用塔式公式, 得到

$$|\text{Emb}(E/F)| \leq \prod_{i=1}^n [E_i : E_{i-1}] = [E : F].$$

□

注记 4.43 (为什么要数嵌入). 扩张次数衡量 E 作为向量空间有多大, 嵌入数衡量其中有多少种“保持基域不动、又尊重四则运算”的对称方式. 有限扩张何时达到 $|\text{Aut}(E/F)| = [E : F]$, 正是 Galois 理论的核心问题.

4.5 正规扩张与可分扩张

定义 4.44 (正规扩张). 代数扩张 E/F 称为正规扩张, 如果任意在 $F[x]$ 中不可约且在 E 中有一个根的多项式, 都在 $E[x]$ 中完全分解.

定理 4.45 (有限正规扩张的判定). 设 $[E : F] < \infty$. 下列条件等价:

1. E/F 正规;
2. E 是 $F[x]$ 中某个多项式的分裂域;
3. 对任意 F -嵌入 $\sigma : E \rightarrow \bar{F}$, 都有 $\sigma(E) = E$.

证明. (1) $\Rightarrow$ (2): 取有限个代数生成元 $E = F(\alpha_1, \dots, \alpha_n)$. 设 $f_i = m_{\alpha_i, F}$. 正规性保证每个 f_i 在 E 中完全分解. 令 $f = \prod_i f_i$, 则 E 包含 f 的全部根, 且由这些根生成, 故 E 是 f 的分裂域.

(2) $\Rightarrow$ (3): 设 E 是 $f \in F[x]$ 的分裂域, 令 $\sigma : E \rightarrow \bar{F}$ 为 F -嵌入. σ 把 f 的每个根送到 f 的某个根, 因此把由这些根生成的 E 映入 E , 即 $\sigma(E) \subseteq E$. 另一方面, $\sigma(E)$ 与 E 在 F 上同构, 所以 $[\sigma(E) : F] = [E : F]$; 有限维性遂给出 $\sigma(E) = E$.

(3) $\Rightarrow$ (1): 设不可约多项式 $h \in F[x]$ 在 E 中有根 α . 若 β 是 h 在 $\bar{F}$ 中的任一根, 则由单扩张上的嵌入对应, 存在 F -嵌入 $F(\alpha) \rightarrow \bar{F}$ 把 α 送到 β . 由嵌入延拓定理, 它可以延拓为 $E \rightarrow \bar{F}$ 的 F -嵌入. 条件 (3) 说明该嵌入的像仍为 E , 故 $\beta \in E$. 所以 h 在 E 中完全分解, E/F 正规. □

例 4.46. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 是正规扩张, 因为它是 $x^2 - 2$ 的分裂域. 相比之下, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是正规扩张: 由 Eisenstein 判别法, $x^3 - 2$ 在 $\mathbb{Q}[x]$ 中不可约; 它在 $\mathbb{Q}(\sqrt[3]{2})$ 中有根 $\sqrt[3]{2}$, 却没有另外两个非实根 $\omega\sqrt[3]{2}$ 、 $\omega^2\sqrt[3]{2}$.



定义 4.47 (重根与可分多项式). 设 $f(x) \in F[x]$. 若 f 在某个分裂域中的各个根互不相同, 则称 f 为可分多项式; 否则称为不可分多项式. 不可约多项式要么所有根都是单根, 要么所有根都是重根.

命题 4.48 (形式导数判别法). 设 $f(x) \in F[x]$, $f'(x)$ 为形式导数. 则

$$f \text{ 无重根} \iff \gcd(f, f') = 1.$$

特别地, 若 f 不可约, 则

$$f \text{ 不可分} \iff f'(x) = 0.$$

证明. 在分裂域中, α 是 f 的重根, 当且仅当 $f = (x - \alpha)^2 g$, 这等价于 $f(\alpha) = f'(\alpha) = 0$. 因此 f 有重根当且仅当 f 与 f' 有非常数公因子.

若 f 不可约, 则 $\gcd(f, f')$ 只能是 1 或 f . 后者等价于 $f \mid f'$; 但 $\deg f' < \deg f$ (除非 $f' = 0$), 所以只能发生在 $f' = 0$ 时. $\square$

例 4.49 (正特征中的不可分现象). 令 $F = \mathbb{F}_p(t)$, 其中 t 是超越元. 多项式

$$f(x) = x^p - t \in F[x]$$

在 $\mathbb{F}_p[t]$ 中关于素元 t 满足 Eisenstein 判别法, 因而在 $\mathbb{F}_p(t)[x]$ 中不可约; 又 $f'(x) = px^{p-1} = 0$. 若在扩域中取 $\alpha^p = t$, 则 $f(x) = (x - \alpha)^p$, 所以它只有一个不同的根, 且该根的重数为 p .

定义 4.50 (可分元素与可分扩张). 代数元 α 称为在 F 上可分, 如果 $m_{\alpha, F}(x)$ 可分. 代数扩张 E/F 称为可分扩张, 如果 E 的每个元素都在 F 上可分.

定理 4.51 (嵌入数判别). 若 $[E : F] < \infty$, 则

$$E/F \text{ 可分} \iff |\text{Emb}(E/F)| = [E : F].$$

证明. 先设 $E = F(\alpha_1, \dots, \alpha_n)$, 令 $E_i = F(\alpha_1, \dots, \alpha_i)$. 若 E/F 可分, 则每个 E_i/E_{i-1} 都可分: 因为 α_i 在 F 上的极小多项式可分, 而它在 E_{i-1} 上的极小多项式是该多项式的因子. 于是, 一个 E_{i-1} -嵌入的延拓数等于 α_i 的极小多项式的不同根数, 恰为 $[E_i : E_{i-1}]$. 逐步相乘并用塔式公式, 得到

$$|\text{Emb}(E/F)| = \prod_{i=1}^n [E_i : E_{i-1}] = [E : F].$$

反之, 设 $|\text{Emb}(E/F)| = [E : F]$, 任取 $\alpha \in E$, 令 $K = F(\alpha)$. 将 E 的嵌入限制到 K , 并结合前面的延拓数估计, 有

$$|\text{Emb}(E/F)| \leq |\text{Emb}(K/F)|[E : K] \leq [K : F][E : K] = [E : F].$$

首尾相等, 所以 $|\text{Emb}(K/F)| = [K : F]$. 而 K/F 是单扩张, $[K : F]$ 等于 α 的极小多项式次数; 嵌入数等于该极小多项式在 Ω 中的不同根数. 因此该极小多项式可分, α 在 F 上可分. 这对所有 $\alpha \in E$ 都成立, 故 E/F 可分. $\square$

定义 4.52 (完美域). 若域 F 的每个不可约多项式都可分, 则称 F 为完美域.



定理 4.53. 特征为 0 的域和有限域都是完美域。

证明. 若 $\text{char } F = 0$, 不可约多项式 f 的导数不可能为零, 故由导数判别法可分。

若 F 是有限域, $\text{char } F = p$. 假设不可约多项式 $f(x) = \sum a_i x^i$ 不可分, 则 $f' = 0$, 故所有出现的指数都被 p 整除: $f(x) = \sum_j a_{pj} x^{pj}$. 有限域上的 Frobenius 映射 $a \mapsto a^p$ 是单射, 因而是满射; 可取 $b_j \in F$ 使 $b_j^p = a_{pj}$. 于是

$$f(x) = \left(\sum_j b_j x^j \right)^p,$$

与 f 不可约矛盾。 □

注记 4.54 (两个条件各自解决什么问题). 正规性保证“一个共轭根进来, 其余共轭根也都进来”; 可分性保证“这些共轭根彼此不同”。只有同时具备这两点, 域的自同构才足够多, 扩张才成为 Galois 扩张。

4.6 Galois 扩张与 Galois 基本定理

定义 4.55 (Galois 扩张). 代数扩张 E/F 若同时正规且可分, 则称为 Galois 扩张. 此时 $\text{Aut}(E/F)$ 称为扩张的 Galois 群, 记为

$$\text{Gal}(E/F) = \text{Aut}(E/F).$$

定理 4.56 (有限 Galois 扩张的等价刻画). 设 $[E : F] < \infty$. 下列条件等价:

1. E/F 是 Galois 扩张;
2. E 是 $F[x]$ 中某个可分多项式的分裂域;
3. $|\text{Aut}(E/F)| = [E : F]$.

证明. (1) $\Rightarrow$ (2): 由有限正规扩张的判定, E 是某个 $h \in F[x]$ 的分裂域. 由于 E/F 可分, h 的每个不可约因子都是可分的; 把 h 的不同不可约因子各取一次, 得到一个可分多项式 f , 且 f 与 h 的根集相同, 所以 E 仍是 f 的分裂域。

(2) $\Rightarrow$ (1): 分裂域扩张正规. 设 f 的不同根为 $\alpha_1, \dots, \alpha_r$, 并令 $E_i = F(\alpha_1, \dots, \alpha_i)$. α_i 在 E_{i-1} 上的极小多项式整除 f , 故它可分. 因此每个 E_{i-1} -嵌入恰有 $[E_i : E_{i-1}]$ 个延拓到 E_i . 逐层相乘并使用塔式公式, 得到

$$|\text{Emb}(E/F)| = \prod_{i=1}^r [E_i : E_{i-1}] = [E : F].$$

由嵌入数判别, E/F 可分, 故 E/F 同时正规且可分。

(1) $\Rightarrow$ (3): 可分性说明 E 到 $\bar{F}$ 的 F -嵌入数等于 $[E : F]$; 正规性说明每个这样的嵌入都把 E 映到自身, 所以它们恰是 F -自同构。

(3) $\Rightarrow$ (1): 由

$$|\text{Aut}(E/F)| \leq |\text{Emb}(E/F)| \leq [E : F]$$

和假设 $|\text{Aut}(E/F)| = [E : F]$, 可知上述三个数相等. 由嵌入数判别, E/F 可分; 同时每个 F -嵌入都已经是 E 的自同构, 于是由有限正规扩张的嵌入判定, E/F 正规。 □



例 4.57 (二次扩张). 若 $d \in \mathbb{Q}$ 不是平方数, 则 $E = \mathbb{Q}(\sqrt{d})$ 是 $x^2 - d$ 的分裂域. 特征为 0 保证可分, 所以 $E/\mathbb{Q}$ 是 Galois 扩张, 且

$$\text{Gal}(E/\mathbb{Q}) = \{1, \sigma\} \cong C_2, \sigma(\sqrt{d}) = -\sqrt{d}.$$

例 4.58 (一个六次 Galois 扩张). 对 $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$, 它是可分多项式 $x^3 - 2$ 的分裂域, 故 $E/\mathbb{Q}$ 是 Galois 扩张. 前文已经算得 $[E : \mathbb{Q}] = 6$, 所以 $|\text{Gal}(E/\mathbb{Q})| = 6$. 由塔式公式 $[E : \mathbb{Q}(\omega)] = 3$, 所以 $\sqrt[3]{2}$ 在 $\mathbb{Q}(\omega)$ 上的极小多项式仍为 $x^3 - 2$; 把它送到另一个根 $\omega\sqrt[3]{2}$ 并固定 ω , 便得到 $\mathbb{Q}(\omega)$ -自同构 σ . 复共轭在 E 上的限制给出另一个 $\mathbb{Q}$ -自同构 τ . 具体地,

$$\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}, \quad \sigma(\omega) = \omega, \quad \tau(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \tau(\omega) = \omega^2.$$

它们满足 $\sigma^3 = \tau^2 = 1$ 且 $\tau\sigma\tau = \sigma^{-1}$. 六个映射 $1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau$ 在 $\sqrt[3]{2}$ 或 ω 上的取值不同, 因而彼此不同; 它们已经占满阶为 6 的 Galois 群. 因此

$$\text{Gal}(E/\mathbb{Q}) \cong S_3.$$

这里群的六个元素恰好对应三个根的六种允许置换.

定义 4.59 (固定域). 若 $H \leq \text{Aut}(E)$, 定义

$$E^H = \{a \in E : \sigma(a) = a \text{ 对所有 } \sigma \in H\}.$$

若 $a, b \in E^H$, 则对每个 $\sigma \in H$ 都有 $\sigma(a - b) = a - b$ 、 $\sigma(ab) = ab$, 并且当 $a \neq 0$ 时 $\sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1}$; 同时 $0, 1 \in E^H$. 因此 E^H 的确是 E 的子域, 称为 H 的固定域.

引理 4.60 (不同嵌入的线性无关性). 设 $\sigma_1, \dots, \sigma_n : E \rightarrow \Omega$ 是彼此不同的域同态. 若 $a_1, \dots, a_n \in \Omega$ 满足

$$a_1\sigma_1(x) + \dots + a_n\sigma_n(x) = 0 \quad \text{对所有 } x \in E,$$

则 $a_1 = \dots = a_n = 0$.

证明. 对 n 归纳. $n = 1$ 时, 令 $x = 1$ 即得 $a_1 = 0$. 设结论对 $n - 1$ 个同态成立, 并假设存在非平凡关系. 重新编号可设 $a_n \neq 0$, 且存在某个 $j < n$ 使 $a_j \neq 0$; 否则令 $x = 1$ 即会得到矛盾. 再重新编号可设 $a_1 \neq 0$. 因为 $\sigma_1 \neq \sigma_n$, 可取 $y \in E$ 使 $\sigma_1(y) \neq \sigma_n(y)$.

分别将 xy 和 x 代入原关系, 并把后一个关系乘以 $\sigma_n(y)$ 后相减, 得到

$$\sum_{i=1}^{n-1} a_i(\sigma_i(y) - \sigma_n(y))\sigma_i(x) = 0 \quad (x \in E).$$

由归纳假设, 所有系数均为零; 但当 $i = 1$ 时 $a_1(\sigma_1(y) - \sigma_n(y)) \neq 0$, 矛盾. $\square$

定理 4.61 (Artin 固定域定理). 设 H 是域 E 的一个有限自同构群, 则

$$[E : E^H] = |H|, \quad \text{Gal}(E/E^H) = H.$$

特别地, E/E^H 是有限 Galois 扩张.



证明. 设 $H = \{\sigma_1, \dots, \sigma_n\}$. 由不同嵌入的线性无关性, 存在 $x_1, \dots, x_n \in E$, 使矩阵

$$A = (\sigma_i(x_j))_{1 \leq i, j \leq n}$$

可逆. 事实上, 若对任意 $x_1, \dots, x_n$ 矩阵都不可逆, 则向量 $(\sigma_1(x), \dots, \sigma_n(x))$ 所张成的子空间是真子空间, 从而存在非零向量 $(a_1, \dots, a_n)$ 与所有这些向量正交, 这将给出一个非平凡线性关系。

任取 $x \in E$, 方程

$$A(c_1, \dots, c_n)^T = (\sigma_1(x), \dots, \sigma_n(x))^T$$

有唯一解. 对任意 $\tau \in H$ 同时作用于方程各项, 由于 $\tau \circ \sigma_i \in H$, 这只会置换矩阵的行. 因此由解的唯一性, $\tau(c_j) = c_j$, 即 $c_j \in E^H$. 矩阵 A 的某一行对应恒等映射, 故该行给出 $x = \sum_j c_j x_j$. 所以 $x_1, \dots, x_n$ 张成 E 作为 E^H -向量空间, 因而 $[E : E^H] \leq n$.

另一方面, $H \subseteq \text{Aut}(E/E^H)$, 而有限扩张的自同构数不超过扩张次数, 故

$$n = |H| \leq |\text{Aut}(E/E^H)| \leq [E : E^H] \leq n.$$

所有不等式均为等式, 结论成立. □

推论 4.62 (固定域判别). 设 $[E : F] < \infty$, 并令 $G = \text{Aut}(E/F)$. 则

$$E/F \text{ 是 Galois 扩张} \iff E^G = F.$$

证明. 由 Artin 固定域定理, $[E : E^G] = |G|$. 另一方面, 有限 Galois 扩张的等价刻画给出

$$E/F \text{ 是 Galois 扩张} \iff |G| = [E : F].$$

因为 $F \subseteq E^G \subseteq E$, 塔式公式说明 $[E : E^G] = [E : F]$ 当且仅当 $E^G = F$, 结论得证. □

定理 4.63 (Galois 基本定理). 设 E/F 为有限 Galois 扩张, $G = \text{Gal}(E/F)$. 则:

1. 中间域 $F \subseteq K \subseteq E$ 与子群 $H \leq G$ 之间存在互逆的包含反向对应

$$K \mapsto \text{Gal}(E/K), \quad H \mapsto E^H.$$

2. 若 $K \leftrightarrow H$, 则

$$[E : K] = |H|, \quad [K : F] = [G : H].$$

3. E/K 总是 Galois 扩张, 且其 Galois 群为 H .

4. K/F 是 Galois 扩张, 当且仅当 $H \trianglelefteq G$. 此时限制映射给出

$$\text{Gal}(K/F) \cong G/H.$$

证明. 对任意 $H \leq G$, Artin 定理给出 $\text{Gal}(E/E^H) = H$. 反过来, 对中间域 K , 因 E/F 可分, E/K 也可分; 因 E 是某个 F 上可分多项式的分裂域, 它也是该多项式在 K 上的分裂域, 故 E/K 正规. 因此 E/K 是 Galois 扩张, 并且

$$|\text{Gal}(E/K)| = [E : K].$$



令 $H = \text{Gal}(E/K)$ 。显然 $K \subseteq E^H$ ，而 Artin 定理与上式给出 $[E : E^H] = |H| = [E : K]$ ，所以 $E^H = K$ 。这证明对应互逆，并同时给出次数公式。

最后，若 K/F 正规，则对每个 $\sigma \in G$ ，限制 $\sigma|_K$ 是 K/F 的嵌入；由正规性的嵌入判定， $\sigma(K) = K$ 。因此限制映射 $\rho : G \rightarrow \text{Gal}(K/F)$ 有意义，其核恰为 H 。任取 K/F 的一个 F -嵌入，由嵌入延拓定理可将其延拓到 E ；由于 E/F 正规，该延拓属于 G ，所以 ρ 满射。由第一同构定理， $G/H \cong \text{Gal}(K/F)$ ，特别地 H 正规。

反之，若 $H \trianglelefteq G$ ，则对 $\sigma \in G$ 有

$$\sigma(K) = \sigma(E^H) = E^{\sigma H \sigma^{-1}} = E^H = K.$$

任意 F -嵌入 $K \rightarrow \bar{F}$ 都能延拓为 $E \rightarrow \bar{F}$ 的 F -嵌入；由于 E/F 正规，该延拓是 G 中的元素，故其在 K 上的限制保持 K 。由正规扩张的嵌入判定， K/F 正规；可分性由 E/F 可分向下传递，所以 K/F 为 Galois 扩张。□

例 4.64 (双二次扩张的完整对应). 令 $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 。定义 $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$ ，以及 $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{3}) = -\sqrt{3}$ 。则

$$G = \{1, \sigma, \tau, \sigma\tau\} \cong C_2 \times C_2.$$

三个二阶子群与三个二次中间域对应：

子群	固定域
$\langle \sigma \rangle$	$\mathbb{Q}(\sqrt{3})$
$\langle \tau \rangle$	$\mathbb{Q}(\sqrt{2})$
$\langle \sigma\tau \rangle$	$\mathbb{Q}(\sqrt{6})$

由于 G 是 Abel 群，每个子群都正规，所以三个二次中间扩张都是 Galois 扩张。

例 4.65 (S_3 例子中的正规与非正规中间域). 仍令 $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ 。子群 $\langle \sigma \rangle$ 的阶为 3，在 S_3 中正规，其固定域是 $\mathbb{Q}(\omega)$ ，所以 $\mathbb{Q}(\omega)/\mathbb{Q}$ 为 Galois 扩张。而任意阶为 2 的子群不是正规子群，其固定域是某个三次域，例如 $\mathbb{Q}(\sqrt[3]{2})$ ；相应三次扩张不是 Galois 扩张。

引理 4.66 (域的有限乘法子群是循环群). 设 M 是某个域的乘法群的有限子群，则 M 是循环群。

证明. 令 m 为 M 中所有元素阶的最小公倍数，并写成 $m = \prod_{\ell} \ell^{e_{\ell}}$ 。对每个出现的素数 ℓ ，由最小公倍数的定义，存在 $a_{\ell} \in M$ ，其阶可写成 $\ell^{e_{\ell}} s_{\ell}$ ，其中 $(s_{\ell}, \ell) = 1$ 。令 $b_{\ell} = a_{\ell}^{s_{\ell}}$ ，则 b_{ℓ} 的阶恰为 $\ell^{e_{\ell}}$ 。由于 M Abel，元素 $b = \prod_{\ell} b_{\ell}$ 的阶等于这些两两互素的阶之积，故 $|b| = m$ 。

每个 $a \in M$ 都满足 $a^m = 1$ ，所以 M 的所有元素都是多项式 $x^m - 1$ 的根。域上的非零 m 次多项式至多有 m 个根，因而 $|M| \leq m$ 。另一方面， $m = |b|$ 是 M 中某个元素的阶，由 Lagrange 定理有 $m \leq |M|$ 。所以 $m = |M|$ ，从而 $M = \langle b \rangle$ 。□

定理 4.67 (本原元定理). 每个有限可分扩张 E/F 都是单扩张，即存在 $\theta \in E$ 使 $E = F(\theta)$ 。这样的 θ 称为本原元。



证明. 若 F 为有限域, 则 E 也是有限域; 由上面的引理, 其乘法群 $E^\times$ 是循环群. 取生成元 θ , 便有 $E = F(\theta)$.

若 F 为无限域, 只需证明 $E = F(\alpha, \beta)$ 时的情形, 再作归纳. 设 $\sigma_1, \dots, \sigma_r$ 是 E/F 的全部嵌入到一个代数闭包 Ω 中. 对任意 $i \neq j$, 不可能同时有 $\sigma_i(\alpha) = \sigma_j(\alpha)$ 和 $\sigma_i(\beta) = \sigma_j(\beta)$, 否则两个嵌入在生成元 α, β 上相同, 从而彼此相同. 因此方程

$$\sigma_i(\alpha) + c\sigma_i(\beta) = \sigma_j(\alpha) + c\sigma_j(\beta)$$

至多对一个 $c \in F$ 成立. 由于 F 无限, 可以选取一个 c 避开有限多个坏值. 令 $\theta = \alpha + c\beta$, 则 $\sigma_1(\theta), \dots, \sigma_r(\theta)$ 两两不同. 它们都是 θ 的极小多项式的根, 故

$$[F(\theta) : F] \geq r = [E : F].$$

另一方面 $F(\theta) \subseteq E$, 所以 $[F(\theta) : F] \leq [E : F]$. 因此 $[F(\theta) : F] = [E : F]$, 从而 $F(\theta) = E$. $\square$

例 4.68. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. 事实上

$$(\sqrt{2} + \sqrt{3})^{-1} = \sqrt{3} - \sqrt{2},$$

所以由 $\theta = \sqrt{2} + \sqrt{3}$ 可得

$$\sqrt{2} = \frac{\theta - \theta^{-1}}{2}, \quad \sqrt{3} = \frac{\theta + \theta^{-1}}{2}.$$

所以 $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\theta)$; 反向包含显然, 故两域相等. 前文已证 $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. 另一方面,

$$\theta^2 = 5 + 2\sqrt{6} \implies (\theta^2 - 5)^2 = 24,$$

所以 θ 满足 $x^4 - 10x^2 + 1 = 0$. 该首一多项式次数等于 $[\mathbb{Q}(\theta) : \mathbb{Q}] = 4$, 因而正是 θ 在 $\mathbb{Q}$ 上的极小多项式.

4.7 有限域

命题 4.69. 若 F 是有限域, 则 $\text{char } F = p$ 为某个素数, 且

$$|F| = p^n$$

对某个正整数 n 成立.

证明. 有限域不可能具有特征 0, 故其特征为素数 p , 并包含素域 $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. 把 F 看成有限维 $\mathbb{F}_p$ -线性空间, 若维数为 n , 则每个元素由 n 个 $\mathbb{F}_p$ 中的坐标唯一确定, 因此共有 p^n 个元素. $\square$

定理 4.70 (有限域的存在与唯一性). 对每个素数幂 $q = p^n$, 存在一个含 q 个元素的有限域; 任意两个含 q 个元素的有限域同构. 通常把它记为 $\mathbb{F}_q$.

证明. 在 $\mathbb{F}_p$ 的代数闭包中考察

$$f(x) = x^q - x.$$

它的导数为 $qx^{q-1} - 1 = -1$, 故没有重根. 其全部根组成集合 K . 若 $a, b \in K$, 利用特征 p 下的 Frobenius 公式, 有

$$(a + b)^q = a^q + b^q = a + b, \quad (ab)^q = a^q b^q = ab.$$



加法逆元也属于 K (当 $p = 2$ 时 $-a = a$; 当 $p \neq 2$ 时 $(-a)^q = -a^q = -a$)。若 $a \neq 0$, 则 $(a^{-1})^q = (a^q)^{-1} = a^{-1}$ 。所以 K 是域。因 f 有 q 个互不相同的根, $|K| = q$, 存在性得证。

若 L 是任意含 q 个元素的域, 则对每个 $a \in L^\times$, Lagrange 定理给出 $a^{q-1} = 1$, 故所有 $a \in L$ 都满足 $a^q = a$ 。所以 L 正是 $x^q - x$ 的分裂域。分裂域的唯一性说明任意两个这样的域同构。□

注记 4.71 (有限域的统一选取). 以下固定 $\mathbb{F}_p$ 的一个代数闭包 $\overline{\mathbb{F}}_p$, 并把 $\mathbb{F}_{p^r}$ 具体取为 $\overline{\mathbb{F}}_p$ 中 $x^{p^r} - x$ 的全部根所组成的子域。这样, 后文的子域包含关系是固定代数闭包中的实际包含关系, 而不只是同构意义下的说法。

例 4.72 (四元域). 多项式 $x^2 + x + 1$ 在 $\mathbb{F}_2$ 上不可约。若 $\alpha^2 + \alpha + 1 = 0$, 则

$$\mathbb{F}_4 = \mathbb{F}_2(\alpha) = \{0, 1, \alpha, \alpha + 1\}, \quad \alpha^2 = \alpha + 1.$$

于是 $\alpha^3 = 1$, $\mathbb{F}_4^\times = \langle \alpha \rangle$ 。非平凡的 $\mathbb{F}_2$ -自同构是 Frobenius 映射 $a \mapsto a^2$, 它交换 α 与 $\alpha + 1$ 。

例 4.73 (八元域). $x^3 + x + 1$ 在 $\mathbb{F}_2$ 上没有根, 因而不可约。若 $\beta^3 + \beta + 1 = 0$, 则

$$\mathbb{F}_8 = \mathbb{F}_2(\beta) = \{a_0 + a_1\beta + a_2\beta^2 : a_i \in \mathbb{F}_2\}.$$

计算时用关系 $\beta^3 = \beta + 1$ 把三次及以上幂降次即可。

定理 4.74 (有限域乘法群). 有限域 $\mathbb{F}_q$ 的乘法群 $\mathbb{F}_q^\times$ 是阶为 $q - 1$ 的循环群。

证明. 将“域的有限乘法子群是循环群”这一引理应用于 $M = \mathbb{F}_q^\times$ 即得; 其阶为 $q - 1$ 。□

定理 4.75 (有限域的子域). 在上述统一选取下, $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ 当且仅当 $m \mid n$ 。等价地, 抽象域 $\mathbb{F}_{p^n}$ 含有一个具有 p^m 个元素的子域, 当且仅当 $m \mid n$; 该子域唯一, 且为

$$\{a \in \mathbb{F}_{p^n} : a^{p^m} = a\}.$$

证明. 若 $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, 塔式公式给出 $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]m$, 故 $m \mid n$ 。

反之, 设 $n = mr$ 。 $x^{p^m} - x$ 的根组成 $\mathbb{F}_{p^m}$ 。若 $a^{p^m} = a$, 反复作用 r 次得 $a^{p^n} = a$, 所以这些根都属于 $\mathbb{F}_{p^n}$ 。它们构成所需子域。任一 p^m 元子域的所有元素都满足 $x^{p^m} - x = 0$, 故只能是这个根集, 唯一性成立。□

定理 4.76 (有限域的 Galois 群). 扩张 $\mathbb{F}_{p^n}/\mathbb{F}_p$ 是 Galois 扩张, 并且

$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \text{Frob}_p \rangle \cong C_n, \quad \text{Frob}_p(a) = a^p.$$

证明. $\mathbb{F}_{p^n}$ 是可分多项式 $x^{p^n} - x$ 在 $\mathbb{F}_p$ 上的分裂域, 故为 Galois 扩张。Frobenius 映射保持加法与乘法, 并固定 $\mathbb{F}_p$; 它的核为 $\{0\}$, 所以在有限集合 $\mathbb{F}_{p^n}$ 上既是单射也是满射, 因而确实是一个 $\mathbb{F}_p$ -自同构。其第 n 次幂为 $a \mapsto a^{p^n} = a$ 。若它的第 $m < n$ 次幂已为恒等, 则每个元素都是 $x^{p^m} - x$ 的根, 但该多项式至多有 $p^m < p^n$ 个根, 矛盾。所以 Frobenius 的阶为 n 。Galois 群的阶也为 $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, 故它生成整个 Galois 群。□



4.8 多项式 Galois 群的计算 (拓展阅读)

定义 4.77 (多项式的 Galois 群). 设 $f(x) \in F[x]$ 是可分多项式, K 是它在 F 上的分裂域。称

$$\text{Gal}(f/F) := \text{Gal}(K/F)$$

为 f 在 F 上的 Galois 群。它通过置换 f 的根, 自然地成为某个对称群 S_n 的子群。

命题 4.78. 若 $f(x) \in F[x]$ 是 n 次不可约可分多项式, 则 $\text{Gal}(f/F)$ 在 f 的 n 个根上传递作用。反之, 若 Galois 群在全部根上传递作用, 则这些根具有同一个极小多项式, 因而 f 在忽略常数因子后不可约。

证明. 任取两个根 α, β 。不可约性说明二者的极小多项式都是 f , 所以存在 F -嵌入 $F(\alpha) \rightarrow K$ 把 α 送到 β 。由于 K/F 正规, 该嵌入可延拓为 K 的 F -自同构, 故作用传递。具体地, 反向设 Galois 群在 f 的根集上传递, 并取其中一个根 α , 令 $m_{\alpha, F}$ 为其极小多项式。对任一根 β , 存在 $\sigma \in \text{Gal}(K/F)$ 使 $\sigma(\alpha) = \beta$, 于是

$$m_{\alpha, F}(\beta) = m_{\alpha, F}(\sigma(\alpha)) = \sigma(m_{\alpha, F}(\alpha)) = 0.$$

所以 f 的所有根都是 $m_{\alpha, F}$ 的根。反过来, $m_{\alpha, F}$ 的每个根也是 α 的一个 F -共轭元; 由嵌入延拓与 K/F 的正规性, 它也是 α 在 Galois 群作用下的像, 因而属于 f 的根集。由于 f 可分, f 与 $m_{\alpha, F}$ 具有完全相同的互异根, 故 f 是 $m_{\alpha, F}$ 的一个非零常数倍, 从而在忽略常数因子后不可约。 $\square$

定义 4.79 (判别式). 设首一多项式 $f(x)$ 的根为 $\alpha_1, \dots, \alpha_n$, 定义判别式

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \in F.$$

$\Delta(f)$ 在任意根的置换下不变, 因此是根的对称多项式; 由对称多项式基本定理, 它可以表示为 f 的系数的多项式, 所以确实属于 F 。 $\Delta(f) \neq 0$ 当且仅当 f 可分。若 $f(x) = x^3 + ax + b$, 则

$$\Delta(f) = -4a^3 - 27b^2.$$

命题 4.80 (不可约三次多项式的快速判定). 设 F 的特征不为 2, $f \in F[x]$ 是首一、不可约、可分的三次多项式。则

$$\text{Gal}(f/F) \cong \begin{cases} A_3 \cong C_3, & \Delta(f) \text{ 是 } F \text{ 中的平方;} \\ S_3, & \Delta(f) \text{ 不是 } F \text{ 中的平方.} \end{cases}$$

证明. 不可约性说明 Galois 群是 S_3 的传递子群, 因此只有 A_3 或 S_3 两种可能。令

$$\delta = \prod_{i < j} (\alpha_i - \alpha_j), \quad \delta^2 = \Delta(f).$$

偶置换固定 δ , 奇置换把 δ 变为 $-\delta$ 。由于 K/F 是 Galois 扩张, $K^{\text{Gal}(K/F)} = F$ 。因此整个 Galois 群包含在 A_3 中, 当且仅当 $\delta \in F$: 若群中全是偶置换, 则 δ 被整个群固定, 故 $\delta \in K^{\text{Gal}(K/F)} = F$; 反之, 若 $\delta \in F$, 则每个自同构都固定 δ , 而特征不为 2 且 $\delta \neq 0$, 所以不可能有自同构把 δ 送到 $-\delta$, 即不可能出现奇置换。

此外, 若 $\delta \in F$, 则 $\Delta(f) = \delta^2$ 显然是 F 中的平方; 反之, 若 $\Delta(f) = c^2$, 其中 $c \in F$, 则 $\delta^2 = c^2$, 从而 $(\delta - c)(\delta + c) = 0$ 。域无零因子, 所以 $\delta = \pm c \in F$ 。因此 $\delta \in F$ 当且仅当 $\Delta(f)$ 是 F 中的平方。于是判别式为平方时 $\text{Gal}(f/F) = A_3$, 否则 $\text{Gal}(f/F) = S_3$ 。 $\square$



例 4.81. 对 $f(x) = x^3 - 2$, 有 $a = 0, b = -2$, 故

$$\Delta(f) = -108 = -3 \cdot 6^2$$

不是 $\mathbb{Q}$ 中的平方。又 f 由 Eisenstein 判别法不可约, 所以 $\text{Gal}(f/\mathbb{Q}) \cong S_3$, 与前面直接构造自同构所得结果一致。

例 4.82 (四次多项式). 设 $f(x) = x^4 - 2, \alpha = \sqrt[4]{2}$. 它的根为 $\alpha, -\alpha, i\alpha, -i\alpha$, 分裂域为 $K = \mathbb{Q}(\alpha, i)$. 由 Eisenstein 判别法 $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, 且 $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, 所以 $i \notin \mathbb{Q}(\alpha)$, 从而 $[K : \mathbb{Q}(\alpha)] = 2$, 故 $[K : \mathbb{Q}] = 8$. 由于 K 是特征 0 下多项式 $x^4 - 2$ 的分裂域, $K/\mathbb{Q}$ 是 Galois 扩张, 所以 $|\text{Gal}(K/\mathbb{Q})| = 8$.

在 $\mathbb{Q}(i)[x]$ 中, $x^4 - 2$ 仍不可约: 若 $[K : \mathbb{Q}(i)]$ 小于 4, 塔式公式将给出 $[K : \mathbb{Q}] < 8$, 与上面的计算矛盾。因此把 α 送到另一个根 $i\alpha$ 、同时固定 i , 确实给出一个 $\mathbb{Q}(i)$ -自同构。再令 τ 为复共轭, 便得到

$$\sigma(\alpha) = i\alpha, \quad \sigma(i) = i, \quad \tau(\alpha) = \alpha, \quad \tau(i) = -i.$$

直接在生成元 α, i 上验证可得 $\sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1}$. 八个映射 $\sigma^j\tau^k$ ($0 \leq j < 4, 0 \leq k < 2$) 彼此不同, 因而已经给出全部 8 个自同构。故 $\text{Gal}(f/\mathbb{Q}) \cong D_4$, 即阶为 8 的正方形对称群。

注记 4.83 (计算 Galois 群的基本路线). 通常先做四件事: 判断多项式是否不可约; 写出或描述分裂域; 用塔式公式计算分裂域次数; 再把自同构看成根的置换, 利用次数、传递性、判别式等信息缩小可能的置换群。

4.9 可解扩张与根式可解性 (拓展阅读)

定义 4.84 (可解群). 群 G 称为可解群, 如果存在子群列

$$\{1\} = G_r \trianglelefteq G_{r-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G,$$

使每个商群 G_i/G_{i+1} 都是 Abel 群。

例 4.85. 所有 Abel 群都是可解群。 S_3 也是可解群, 因为

$$\{1\} \trianglelefteq A_3 \trianglelefteq S_3,$$

且 $A_3 \cong C_3, S_3/A_3 \cong C_2$. 但当 $n \geq 5$ 时, S_n 不可解, 因为 A_n 是非 Abel 单群。

定义 4.86 (根式扩张与根式可解). 若存在域塔

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r$$

使 $F_i = F_{i-1}(\alpha_i)$ 且 $\alpha_i^{n_i} \in F_{i-1}$, 其中 $n_i \geq 2$, 则称 F_r/F 为根式扩张。若多项式 $f \in F[x]$ 的分裂域包含在某个根式扩张中, 则称 f 在 F 上可由根式解出。

定理 4.87 (Galois 的根式可解判据 (引用)). 设 F 的特征为 0, $f(x) \in F[x]$. 则 f 可由根式解出, 当且仅当其 Galois 群 $\text{Gal}(f/F)$ 是可解群。



注记 4.88 (为何本讲义不把下面内容标成“证明”). 这个判据不属于英文讲义 Lecture 12–16 的正文; 其完整证明需要单位根扩张、循环扩张与 Kummer 理论, 而这些工具在前文均未建立。因此这里只解释两边联系的机制, 不能把它当作本定理的完整证明。

若分裂域包含在根式扩张 L/F 中, 可先把所需的单位根作为根式塔的前几步加入 (因为 $\zeta_n^n = 1 \in F$), 原基域仍是 F 。对扩充后的根式塔中的一步 $F_{i-1} \subseteq F_i = F_{i-1}(\alpha_i)$, 其中 $\alpha_i^{n_i} \in F_{i-1}$, 在含有 n_i 次单位根的情形下, 其正规闭包的 Galois 群是循环群的子群。因此, 根式塔的正规闭包的 Galois 群具有由 Abel 商群组成的正规列, 是可解群。设 N/F 是包含原多项式分裂域 K 的这一有限 Galois 正规闭包, 则限制映射给出

$$\text{Gal}(K/F) \cong \text{Gal}(N/F) / \text{Gal}(N/K),$$

所以 $\text{Gal}(K/F)$ 是可解群的商群, 因而也是可解群。

反过来, 若分裂域的 Galois 群可解, 则取其可解列, 并将子群列通过 Galois 基本定理翻译为中间域列。先在根式塔中加入适当的单位根, 再将每个 Abel 商群进一步细分为循环群; Kummer 理论表明, 在含有所需单位根的基域上, 每个这样的循环扩张都可以表示为添加某个根式。沿着这条塔逐步添加根式, 便得到包含原分裂域的根式扩张。注意: 这段论证依赖 Kummer 理论, 不能仅由本节前面已经证明的初等结论独立完成。

注记 4.89 (五次方程为什么不同). 二、三、四次一般方程的 Galois 群分别嵌入 S_2, S_3, S_4 , 这些群都可解, 因此存在统一的根式公式。五次一般方程的 Galois 群是 S_5 , 它不可解, 所以不存在适用于所有五次方程的根式公式。这并不是说每个具体五次方程都不能用根式求解; 例如 $x^5 - 2$ 的 Galois 群可解, 它仍可由根式解出。

4.10 知识串联与自测

本节最重要的逻辑链条可概括为

$$\begin{aligned} \text{极小多项式} &\implies \text{单扩张的次数与基} \implies \text{分裂域}, \\ \text{正规} + \text{可分} &\iff \text{有限 Galois 扩张} \implies \text{子群-中间域对应}, \\ x^{p^n} - x &\implies \mathbb{F}_{p^n} \implies \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle a \mapsto a^p \rangle. \end{aligned}$$

练习 4.90. 求 $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) : \mathbb{Q}]$ 。

解答. 令 $E = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt[3]{3})$ 。由 Eisenstein 判别法, $[E : \mathbb{Q}] = 2$, $[L : \mathbb{Q}] = 3$ 。若 $\sqrt[3]{3} \in E$, 则 $L \subseteq E$, 从而 $3 = [L : \mathbb{Q}]$ 应整除 $[E : \mathbb{Q}] = 2$, 矛盾。因此 $x^3 - 3$ 在 E 中没有根。由于它是三次多项式, 若在 $E[x]$ 中可约就必有一次因子, 故它在 $E[x]$ 中不可约, 从而 $[EL : E] = 3$ 。由塔式公式

$$[EL : \mathbb{Q}] = [EL : E][E : \mathbb{Q}] = 3 \cdot 2 = 6.$$

□

练习 4.91. 求 $\sqrt{2} + \sqrt{3}$ 在 $\mathbb{Q}$ 上的极小多项式。

解答. 令 $\alpha = \sqrt{2} + \sqrt{3}$ 。则 $\alpha^2 = 5 + 2\sqrt{6}$, 所以 $(\alpha^2 - 5)^2 = 24$, 即

$$\alpha^4 - 10\alpha^2 + 1 = 0.$$



由于

$$\alpha^{-1} = \sqrt{3} - \sqrt{2}, \quad \sqrt{2} = \frac{\alpha - \alpha^{-1}}{2}, \quad \sqrt{3} = \frac{\alpha + \alpha^{-1}}{2},$$

故 $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 。其中 $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ ，否则设 $\sqrt{3} = a + b\sqrt{2}$ ($a, b \in \mathbb{Q}$)。平方并比较有理部分和 $\sqrt{2}$ 部分，得到 $2ab = 0$ 且 $a^2 + 2b^2 = 3$ ；若 $b = 0$ ，则 $a^2 = 3$ ，若 $a = 0$ ，则 $b^2 = 3/2$ 。第一种情形会推出 $\sqrt{3} \in \mathbb{Q}$ ；第二种情形若写 $b = r/s$ 为既约分数，则 $2r^2 = 3s^2$ ，进而同时推出 $3 \mid r$ 与 $3 \mid s$ ，矛盾。因此 $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ 。由塔式公式 $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ ，故四次多项式 $x^4 - 10x^2 + 1$ 就是极小多项式。□

练习 4.92. 判断 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ 是否正规、是否可分、是否 Galois。

解答. $x^4 - 2$ 由素数 2 的 Eisenstein 判别法在 $\mathbb{Q}[x]$ 中不可约，因此它是 $\sqrt[4]{2}$ 在 $\mathbb{Q}$ 上的极小多项式。特征为 0，所以扩张可分。这个不可约多项式在该域中有根 $\sqrt[4]{2}$ ，但根 $i\sqrt[4]{2}$ 不在实域 $\mathbb{Q}(\sqrt[4]{2})$ 中，故扩张不正规，因而不是 Galois 扩张。□

练习 4.93. 写出 $x^4 + 1$ 在 $\mathbb{Q}$ 上的分裂域及其次数。

解答. 令 $\zeta_8 = e^{2\pi i/8}$ 。 $x^4 + 1$ 的根为 $\zeta_8, \zeta_8^3, \zeta_8^5, \zeta_8^7$ ，故分裂域为

$$\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2}).$$

这里 $i = \zeta_8^2$ 且 $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$ ，故 $\mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$ ；反过来 $\zeta_8 = (1 + i)/\sqrt{2} \in \mathbb{Q}(i, \sqrt{2})$ ，所以两域确实相等。又 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ ，而 $i \notin \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ ，故

$$[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

□

练习 4.94. 说明 $\mathbb{F}_{2^6}$ 有哪些子域。

解答. 子域与 6 的正因子对应。因为 1, 2, 3, 6 是全部正因子，所以子域恰为

$$\mathbb{F}_2, \quad \mathbb{F}_4, \quad \mathbb{F}_8, \quad \mathbb{F}_{64}.$$

每种大小的子域都是唯一的。□

练习 4.95. 设 E/F 是有限 Galois 扩张， $\text{Gal}(E/F)$ 为循环群 C_{12} 。问 E/F 有多少个中间域？其中次数为 3 的中间扩张有几个？

解答. 循环群 C_{12} 对 12 的每个正因子都有唯一子群，因此共有 6 个子群，也就有 6 个中间域。次数为 3 的中间域 K/F 对应指数为 3、即阶为 4 的子群；该子群唯一，所以这样的中间域只有一个。□

注记 4.96 (复习时建议优先掌握). 若课程不考查加星内容，应优先熟练掌握：塔式公式；极小多项式与 $F[x]/(m)$ ；分裂域的构造；正规与可分的判定；有限 Galois 扩张的等价刻画与固定域判别；Galois 基本定理；有限域的存在唯一性、子域结构和 Frobenius 自同构。多项式 Galois 群的复杂计算及根式可解性可作为拓展阅读。