

抽象代数笔记

詹奇

Last updated: November 22, 2024

Contents

1. 域与线性空间	1
1.1. 定义与例子	1
1.2. 域的同态	2
1.3. 域的特征	4
1.4. 域的扩张	4
1.5. 代数闭包	6
1.6. Galois 群初探	7
2. 环与模	9
2.1. 定义与例子	9
2.2. 环与模同态	10
2.3. 子环, 理想与商环	11
2.4. 同态基本定理与中国剩余定理	12
2.5. 整环与整除性	13
2.6. 多项式环	16
2.7. 主理想整环上的有限生成模分类	16
3. 群与群作用	16
3.1. 定义与例子	16
3.2. 子群, 正规子群与商群	17
3.3. 同态基本定理	18
3.4. 群作用与 Sylow 定理	19
3.5. 对称群	21
4. Galois 理论	22

本文是刘思齐老师的[抽象代数课程](#)笔记。

1. 域与线性空间

1.1. 定义与例子

定义 1.1.1 (域): 一个域系指以下资料:

- 集合 F , 有 $1_F, 0_F \in F$ 满足 $1_F \neq 0_F$, 有时简写为 $1, 0$.
- F 上的加法记为 $+$, 满足加法结合律, 加法交换律, 有加法单位元 0 与加法逆元 $-a$. (这保障了加法逆元是唯一的).
- F 上的乘法记为 $*$, 满足乘法结合律, 乘法交换律, 有乘法单位元 1 , 对于非零元 a , 有乘法逆元 a^{-1} . (这保障了乘法逆元是唯一的).
- 乘法对加法的分配律成立.

我们记 F^* 为 F 中所有非零元素的集合.

为了说明为什么我们要求 $0_F \neq 1_F$, 有以下引理:

引理 1.1.1:

1. $0_F \cdot 0_F = 0_F$.
2. $\forall x \in F, x \cdot 0_F = 0_F$

证明:

1. $0_F = 0_F + 0_F = 0_F \cdot 0_F + 0_F \cdot 0_F$, 两边减去 $0_F \cdot 0_F$ 即得.
2. $x \cdot 0_F = x \cdot (0_F + 0_F) = x \cdot 0_F + x \cdot 0_F$, 两边减去 $x \cdot 0_F$ 即得.

□

由此可见, 若 $0_F = 1_F$, 那么 F 中所有元素满足 $x = x \cdot 1_F = x \cdot 0_F = 0_F$, 这显然不是我们所期望的.

同理, 若对于域 F 上的 0_F 有逆元, 那么我们有 $0_F = a \cdot 0_F = 1_F$, 又推出了域中所有元素都是 0_F .

例子 1.1.1 (域):

1. 有理数域 \mathbb{Q} , 实数域 \mathbb{R} , 复数域 \mathbb{C} , 对于我们熟知的加法和乘法运算构成域.
2. $F = \mathbb{Q}(\sqrt{2}) = \{x + \sqrt{2}y \mid x, y \in \mathbb{Q}\}$.
3. $F = \mathbb{Q}(\sqrt[3]{2}) = \{x + \sqrt[3]{2}y \mid x, y \in \mathbb{Q}\}$
4. $F = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{x_1 + x_2\sqrt{2} + x_3\sqrt{3} + x_4\sqrt{4} \mid x_i \in \mathbb{Q}\}$.
5. 任取素数 p , $F = \mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}$, 其中加法和乘法都是模 p 的. 其中乘法逆的存在是不显然的. 对于 F 中任意一个非零元 k , 有, 我们考虑映射 $T: F_p^* \rightarrow F_p^*: y \mapsto ky$, 易证 T 是双射, 从而存在逆元 m 使得 $km = 1$.
6. 设 F 是一个域, 则 $F(x) = \left\{ \frac{P(x)}{Q(x)} \mid P(x), Q(x) \in F[x], Q(x) \neq 0 \right\}$ 同样构成域.
7. $k = \mathbb{C}(x, \sqrt{x^3+2})$, 可以视作 $\mathbb{C}(x)(y)$ 其中 $y^2 = x^3 + 2$, 则 $k = \{R_1(x) + R_{x(y)} \mid R_1, R_2 \in \mathbb{C}(x)\}$.

定义 1.1.2 (线性空间): 设 F 是一个域, V 是一个集合, 若 V 上定义了加法运算 $+: V \times V \rightarrow V$, 以及数乘运算 $*: F \times V \rightarrow V$, 满足以下条件:

1. 对于任意 $u, v, w \in V$, 有 $u + (v + w) = (u + v) + w$.
2. 对于任意 $v \in V$, 有 $v + 0 = v$.
3. 对于任意 $v \in V$, 存在 $w \in V$, 使得 $v + w = 0$.
4. 对于任意 $v \in V$, 有 $1v = v$.
5. 对于任意 $a, b \in F, v \in V$, 有 $a(bv) = (ab)v$.
6. 对于任意 $a \in F, u, v \in V$, 有 $a(u + v) = au + av$.
7. 对于任意 $a, b \in F, v \in V$, 有 $(a + b)v = av + bv$.

线性空间的观点对于研究域的结构有很大的帮助, 例如我们可以将 $\mathbb{Q}(\sqrt{2})$ 视作 \mathbb{Q} 上的二维线性空间. \mathbb{R} 可以视作 \mathbb{Q} 上的无穷维线性空间.

例子 1.1.2: $\mathbb{F}_4 = \mathbb{F}_2(\alpha) = \{x + \alpha y \mid x, y \in \mathbb{F}_2\}$. 其中的问题是我们该取什么样的 α . 考虑 $\mathbb{F}_2[x]$ 上的所有二次多项式 $f(x) = x^2 + px + q$, 及 $x^2, x^2 + x, x^2 + 1, x^2 + x + 1$. 其中前三个都是可约的, 所以我们取 α 满足 $\alpha^2 + \alpha + 1 = 0$.

1.2. 域的同态

我们先从线性空间上的同态(线性映射)开始.

定义 1.2.1 (线性映射): 设 V_1, V_2 是域 F 的线性空间, 若映射 $f: V_1 \rightarrow V_2$ 满足:

1. 对于任意 $u, v \in V_1$, 有 $f(u + v) = f(u) + f(v)$.
2. 对于任意 $a \in F, v \in V_1$, 有 $f(av) = af(v)$.

那么我们称 f 是一个线性空间的同态, 即线性映射.

类似地, 我们可以定义域的同态.

定义 1.2.2 (域的同态): 设 F_1, F_2 是域, 若映射 $f: F_1 \rightarrow F_2$ 满足:

1. $f(0_{F_1}) = 0_{F_2}, f(1_{F_1}) = 1_{F_2}$.
2. 对于任意 $a, b \in F_1$, 有 $f(a + b) = f(a) + f(b)$.
3. 对于任意 $a, b \in F_1$, 有 $f(ab) = f(a)f(b)$.

那么我们称 f 是域的同态.

不同于群和环的同态, 事实上域的同态是一个“没什么用”的概念, 有下面的定理:

定理 1.2.1: 设 F_1, F_2 是域, $f: F_1 \rightarrow F_2$ 是域的同态, 则 f 是单射.

证明: 设 $a, b \in F_1$ 满足 $f(a) = f(b)$. 设 $x = b - a$. 若 $x \neq 0$, 那么存在 $y \in F_1$, 使得 $xy = 1$. 那么有 $0 \cdot f(y) = (f(b) - f(a)) \cdot f(y) = f(1) = 1$, 矛盾. 所以 $x = 0$, 即 $a = b$. \square

这也就说明若存在一个 $\varphi: F_1 \rightarrow F_2$, 那么我们视 F_1 为 F_2 的子域, 所以在研究域的时候, 我们不关心域的同态, 而更关心子域和域扩张的概念.

定义 1.2.3 (子域与扩域): 设 F 是域, 若 E 是 F 的子集, 且 E 也构成域, 那么我们称 E 是 F 的子域, 同时称 F 是 E 的扩域, 记为 F/E .

定义 1.2.4 (域的同构): 设 F_1, F_2 是域, 若存在双射 $\varphi: F_1 \rightarrow F_2$, 且满足域的同态, 那么我们称 F_1 与 F_2 是同构的. 若 $F_1 = F_2$, 我们称 φ 是域 F_1 的自同构. 我们称在自同构下不变的元素为域 F_1 的不动域.

例子 1.2.1:

1. $\mathbb{R}/\mathbb{Q}, \mathbb{C}/\mathbb{R}, \mathbb{Q}(\sqrt{2})/\mathbb{Q}, \mathbb{F}_4/\mathbb{F}_2$.
2. $f: \mathbb{C} \rightarrow \mathbb{C}, x + iy \mapsto x - iy$ 是域 \mathbb{C} 的自同构, 其中不动域是实数域 \mathbb{R} .
3. $\mathbb{Q}(\sqrt{2})$ 与 $\mathbb{Q}(\sqrt{3})$ 不存在同态.

事实上, \mathbb{Q}, \mathbb{F}_p 是某种程度上的“最小”域, 我们有以下定理:

定理 1.2.2: \mathbb{Q}, \mathbb{F}_p 没有真子域.

定理 1.2.3: 若 F 是 E 的扩域, 则 F 是 E 上的线性空间, 我们记 $[F : E] = \dim_E F$, 称为 F/E 的次数. 若 $[F : E] < \infty$, 则称 F/E 为有限扩张.

1.3. 域的特征

定义 1.3.1 (域的特征): 设 F 是域, 若存在最小的正整数 n , 使得 $n1_F = 0_F$, 那么我们称 n 为域 F 的特征, 记为 $\text{char}(F) = n$. 若不存在这样的 n , 我们称 F 的特征为 0.

容易看出如果域的特征是正的, 那么它一定是素数. 若 $\text{char}(F) = 0$, 那么 \mathbb{Q} 是 F 的子域; 若 $\text{char}(F) = p$, 那么 \mathbb{F}_p 是 F 的子域. (注意这里的子域可以看作是存在一个域同态而不是严格的包含). 这就是说明了每个域都是 \mathbb{Q} 或 \mathbb{F}_p 的扩域.

在正特征的域上有一个有趣的运算. 若 $\text{char} F = p > 0$, 我们考虑 $(x+y)^p$, 由二项式定理, 我们有: $(x+y)^p = x^p + y^p + C_p^1 x^{p-1}y + \dots + C_p^{p-1}xy^{p-1} + y^p = x^p + y^p$. 我们记 $\sigma : F \rightarrow F$ 满足 $x \mapsto x^p$, 由上面的性质容易发现 σ 是一个域同构, 我们称 σ 为域 F 的 Frobenius 自同构.

1.4. 域的扩张

定义 1.4.1: 设 E/F 是一个域扩张, 对于 E 中的子集 S , 有 $F(S)$ 为 E 中包含 $F \cup S$ 的最小子域, 称为 F 在 S 上生成的域. 若 S 是有限的且 $F(S) = E$, 我们称 E 是由 F 上的有限生成扩张. 若对 E 的任意有限子集, $F(S) \neq E$, 则称 E 为无限生成的.

例子 1.4.1:

1. $\mathbb{Q}(\sqrt{2})$ 是 \mathbb{Q} 上的有限生成扩张, 也是有限扩张.
2. $\mathbb{R}(x)$ 有有理函数域是 \mathbb{R} 上的有限生成扩张, 但不是有限扩张.
3. $F = \mathbb{Q}$, $E = \mathbb{Q}\left(2^{\frac{1}{2^k}}\right)$, $k = 1, 2, \dots$. 我们考虑逐步添加元素. $E_1 = \mathbb{Q}\left(2^{\frac{1}{2}}\right)$, $E_2 = E_1\left(2^{\frac{1}{2^2}}\right) = \mathbb{Q}\left(2^{\frac{1}{2^2}}\right)$, 容易得到 $E_k = \mathbb{Q}\left(2^{\frac{1}{2^k}}\right)$. $F = E_0 \subseteq E_1 \subseteq \dots$, $E = \bigcup_{k=1}^{\infty} E_k$.

我们研究的域扩张要解决的问题: 一个尽可能简单的域扩张是什么样的?

定理 1.4.1: 有限扩张一定是有限生成扩张, 反之不然.

证明: 若 $[E : F] = n$, 可推得 $E = \text{Span}_{F(e_1, \dots, e_n)} E$, $E = F(e_1, \dots, e_n)$. □

定义 1.4.2 (代数扩张与超越扩张): 设扩域 E/F , 若 $u \in E$ 存在 $f(u) = 0$, $f \neq 0$, $f \in F[x]$, 则称 u 为 F 上的代数元. 若 $\frac{E}{F}$ 中的每个元素都是代数元, 则称 E/F 为代数扩张. 若存在 $u \in E$ 使得 u 不是任何 $f \in F[x]$ 的根, 则称 u 为超越元, E/F 为超越扩张.

例子 1.4.2:

1. $\mathbb{Q}(\sqrt{2})$ 为代数扩张.
2. $\mathbb{Q}(x), \mathbb{Q}(\pi)$ 为超越扩张.

现在有了三个“不太大”的扩张, 有限扩张, 有限生成扩张和代数扩张, 我们的目标是理解这三个概念之间的关系, 从而理解域上较小的扩张是什么样的.

我们先证明一些有关代数数的性质.

引理 1.4.1: 设 E/F , α, β 是 F 上的代数元, 则 $\alpha + \beta$ 和 $\alpha\beta$ 也是代数元.

这一引理有不同的证法. 一种证法基于对称多项式的理论直接构造出对应的多项式, 我们这里给出另一种证法.

证明: 设 $f(\alpha) = 0, f \in F[x], g(\beta) = 0, g \in F[x], \deg f = n, \deg g = m$. 定义 $h(y) = R_x(f(x), g(y - x)) \in F[y]$. 其中 $R_{x(A[x], B[x])}$ 为多项式 A, B 关于变量 x 的结式. 我们断言 $h(\alpha + \beta) = 0$, 这是因为 $f(x)$ 与 $g(\alpha + \beta - x)$ 有公共根 $x = \alpha$. 对于 $\alpha\beta$ 同理. \square

现在我们来具体的关系.

定理 1.4.2: 有限扩张一定是代数扩张, 反之不然.

证明: 设 $[E/F] = n$ 是有限扩张. 对于任意 $u \in E$, 我们要找 $f \in F[x]$ 使得 $f(u) = 0$. 考虑 $1, u, u^2, \dots \in E$. 由 $\dim_F(E) = n$, 所以 $1, u, u^2, \dots, u^n$ F -线性相关, 所以存在 $b_0, \dots, b_n \in F$ 不全为 0, 使得 $b_0 + b_1 u + \dots + b_n u^n = 0$, 故 u 是代数元.

反例: $F = \mathbb{Q}, E = \mathbb{Q}\left(2^{\frac{1}{2^k}}\right), k = 1, 2, \dots$ 是代数扩张, 但不是有限生成扩张, 更不是有限扩张. \square

由上文的例子我们知道代数扩张不能推出有限生成扩张, 有限生成扩张也不能推出代数扩张. 看起来代数扩张和有限生成扩张都是不太好的扩张, 但下面的定理告诉我们, 有限生成扩张和代数扩张的交集是一个很好的扩张.

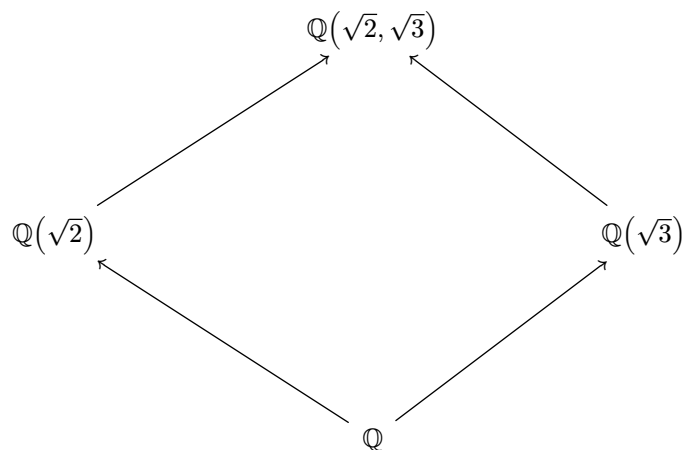
定理 1.4.3: 有限生成的代数扩张是有限扩张. 具体来说, 对于域扩张 E/F , 以下两个事实等价:

1. E/F 是有限扩张.
2. $E = F(u_1, \dots, u_n)$, 其中 u_1, \dots, u_n 是 F 上的代数元. 此时 E/F 是代数扩张.

1. (1) \Rightarrow (2). 设 $[E : F] = n, u_1, \dots, u_n$ 是 E/F 的基, 则 $E = F(u_1, \dots, u_n)$. 因为 E/F 是代数扩张, 所以 u_1, \dots, u_n 是代数元.
2. (2) \Rightarrow (1). 为了证明这一点, 我们需要一些定义和引理.

定义 1.4.3 (中间域): 设 E/F , 则域 K 是 E 和 F 的中间域, 若 $F \subseteq K \subseteq E$.

例子 1.4.3: 下图即为中间域的一个例子.



引理 1.4.2 (维数公式): 设 E/F 是有限扩张, K 是一个中间域, 则 $[E : F] = [E : K][K : F]$.

证明: 有限维线性空间的线性子空间自然也是有限的. 设 u_1, \dots, u_n 是 K/F 的基, v_1, \dots, v_m 是 E/K 的基, 下面构造 E/F 的基. 对于 $\beta \in E$, 存在 $\alpha_1, \dots, \alpha_m \in K$ 使得 $\beta = \alpha_1 v_1 + \dots + \alpha_m v_m$, 对于每个 α_i 存在 $a_{i1}, \dots, a_{in} \in F$, 使得 $\alpha_i = a_{i1} u_1 + \dots + a_{in} u_n$, 整理可得 $\beta = \sum_{i=1}^m \sum_{j=1}^n a_{ij} u_j v_i$. 所以 $\dim_F E \leq n \cdot m$. 下证 $u_j v_i$ 线性无关. 设 $\sum_{i,j} c_{ij} u_j v_i = 0$, 推得 $\sum_i (\sum_j c_{ij} u_j) v_i = 0$. 由 v_1, \dots, v_m 线性无关, 所以 $\sum_j c_{ij} u_j = 0$, 由 u_1, \dots, u_n 线性无关, 得 $c_{ij} = 0$. \square

引理 1.4.3: 单代数扩张是有限扩张.

证明: 设 $E = F(u)$, u 是 F 上的代数元, 我们要证明 $[E : F] < \infty$. 设 $f \in F[x]$, $f \neq 0$ 使得 $f(u) = 0$, 并且 f 是满足该条件的次数最小的首一多项式. 设 $\deg f = n$, 则 $E = f(u) = \text{Span}_F(1, u, \dots, u^{n-1})$, 由此 $\dim_F E = n$, 是有限的. \square

回到我们想要证明的结论, 我们同样可以逐个添加元素. $F \subseteq F(u_1) \subseteq F(u_1, u_2) \subseteq \dots \subseteq F(u_1, \dots, u_n)$. 每次的扩张都是单代数扩张, 也就是有限扩张, 维数就是有限的. 而由维数公式我们知道最终的维数也就是 $[F(u_1, u_2) : F(u_1)] \cdot [F(u_1) : F] \cdot \dots$

至此, 我们证明了有限生成的代数扩张一定是有限扩张. \square

定理 1.4.4: 若 $F \subseteq K \subseteq E$, 其中 K/F 代数, E/K 代数, 那么 E/F 代数.

证明: 设 $\alpha \in E$, 存在 $f \in K[x]$, $f \neq 0$, $f(\alpha) = 0$. 设 $f(x) = x^n + a_1 x^{n-1} + \dots + a_n$, $a_i \in K$. 设 $K' = F(a_1, \dots, a_n)$, 注意到 a_1, \dots, a_n 在 F 上代数, 则 K'/F 是有限扩张. 再注意到 $K'(\alpha)/K'$ 是一个单扩张, 所以 $K'(\alpha)/K'$ 是有限扩张, 可得 $[K'(\alpha) : F] = [K'(\alpha) : K'] [K' : F] < \infty$, 也是有限扩张. 因为 $F \subseteq K'$, 所以 $F(\alpha) \subseteq K'(\alpha)$ 也是有限扩张. 所以 $F(\alpha)$ 是代数扩张, α 是代数元. \square

1.5. 代数闭包

上一节我们考虑的是小的扩张长什么样, 这一节我们讨论大的扩张, 尤其是大的代数扩张.

定义 1.5.1 (代数闭包): 设 F 是域, 若 E/F 是代数扩张, $K = \{\alpha \in E \mid \alpha \text{ 在 } E \text{ 代数}\}$, 显然 K 是中间域, 我们称 K 是 F 在 E 中的代数闭包.

若 K 没有真代数扩张, 我们称 K 是代数闭域.

若 K/F 是代数扩张且 K 是代数闭域, 我们称 K 是 F 的一个(绝对)代数闭包.

例如 \mathbb{C} 就是代数闭的.

定理 1.5.1: \mathbb{Q} 在 \mathbb{C} 中的相对代数闭包就是 \mathbb{Q} 的一个绝对代数闭包.

证明: 我们证明一个更一般的版本: E 是代数闭的, F 是 E 的子域, K 是 F 在 E 中的代数闭包, 则 K 是 F 的绝对代数闭包.

只需证明 K 是代数闭的. 假设 K' 是 K 的一个代数扩张, $\alpha \in K'$, 则由 α 的极小多项式 $f(x) \in K[x]$, 因为 $K \subseteq E$, 所以 $f(x) \in E[x]$, 所以 $f(x) = (x - \alpha_1) \dots (x - \alpha_n) \in K[x]$, $\alpha_i \in E$. 另一方面 α_i 是 K 上的代数元, 因为 K 是相对代数闭包, 所以 $\alpha_i \in K$, 所以 $f(x) = x - \alpha$. 最终我们得到 $K' = K$. \square

1.6. Galois 群初探

一个自然的问题是我们还没有定义抽象的群, 那么该如何讨论 Galois 群. 事实上在 Galois 研究时他并没有采用抽象的群概念, 而是考虑一种特殊的群, 即置换群.

定义 1.6.1 (对称群): 设集合 X , $S(X) = \{\sigma : X \rightarrow X \mid \sigma \text{ 是双射}\}$, 我们可以定义映射的复合和逆运算, 也有单位映射 e . 事实上它满足如下性质:

1. $(\sigma\tau)\mu = \sigma(\tau\mu)$.
2. $\sigma e = e\sigma = \sigma$.
3. $\sigma\sigma^{-1} = \sigma^{-1}\sigma = e$.

我们称 (S, e) 是 X 上的对称群.

事实上上述的性质其实就是抽象群的定义.

我们一般不需要研究整个置换, 而是研究一部分的封闭子集, 也就引出了置换群的概念.

定义 1.6.2 (置换群): 若 $G \subseteq S$ 满足于任意 $\sigma, \tau \in G$, 有 $\sigma\tau \in G$, $\sigma^{-1} \in G$, 则称 G 是 X 上的置换群.

更进一步的, 我们可以定义域 E 上的自同构群, 记为 $\text{Aut}(E) = \{\sigma \in S(E) \mid \sigma(0) = 0, \sigma(1) = 1, \sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta), \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta), \dots\}$.

定义 1.6.3 (Galois 群): 设 E/F 是域扩张, 我们定义 $\text{Gal}(E/F) = \{\sigma \in \text{Aut}(E) \mid \sigma|_F = \text{id}_F\}$, 称为 E/F 的 Galois 群.

定理 1.6.1: 若 E/F 是有限扩张, 则 $\text{Gal}(E/F)$ 是有限群.

证明: 设 $E = \text{Span}_{F(u_1, \dots, u_n)}$, 其中 u_n 在 F 上代数. 对于 u_1 , 有极小多项式 $f_1 \in F[x]$, 满足 $f_1(u_1) = \mu_1^n + a_1 u_1^{n-1} + \dots + a_n = 0, a_i \in F$.

设 $\sigma \in \text{Aut}(E), \sigma|_F = \text{id}_F$, 考虑 σ 作用 $f_1 \cdot \sigma(f_1(u_1)) = \sigma(0) = 0 = \sigma(u_1^n + \dots + a_n) = f_1(\sigma(u_1))$.

这就说明了对于 $X_1 = \{\sigma \in E \mid f_1(\sigma) = 0\}$, $\sigma|_{X_1}$ 是 X_1 的一个置换. 同样的对于任意 u_i 取 f_i , 定义 $X = \bigcup_{i=1}^n X_i$, σ 是 X 上的一个置换. 由于 X 是有限集, 所以 σ 是有限的. \square

定义 1.6.4 (不动域): 设 E 是一个域, 且 $G \leq \text{Aut}(E)$, 定义 $\text{Inv}(G) = \{\alpha \in E \mid \sigma(\alpha) = \alpha, \sigma \in G\}$, 称为 G 的不动域.

定理 1.6.2 (Artin 引理): 设 E 是域, $G \leq \text{Aut}(E)$, 则 $\text{Inv}(G)$ 是 E 的子域, 且 $[E : F] \leq |G|$, 于是 E/F 是有限扩张.

证明: 设 $G = \{\eta_1 = e, \dots, \eta_n\}, |G| = n$. 下证对于 $m > n$, E 中的任意 u_1, \dots, u_m 是线性相关的. 考虑 $\eta_j(x_1 \mu_1 + \dots + x_m \mu_m) = x_1 \eta_j(\mu_1) + \dots + x_m \eta_j(\mu_m) = 0$, 一定有非零解, 所以存在 $(x_1, \dots, x_m) \in E^m$. 下证 $x_j \in F$.

我们从这些解挑一个含 0 元素最多的解, 记为 $x = x_1, \dots, x_m$, 不妨假设 $x_1 \neq 0, x_1 = 1$, 下证 $x_2, \dots, x_m \in F$. 假设 $x_2 \notin F$, 则存在 $\eta \in G$ 使得 $\eta(x_2) \neq x_2$, 考虑 $\eta(x) = (1, \eta(x_2), \dots, \eta(x_m))$, 显然 $\eta(x)$ 仍是方程的解, 且 $\eta(x)$ 0 的个数和 x 中个数一样多.

考虑 $\eta(x) - x$ 仍然是方程组的解, 但包含更多的 0, 另一方面 $\eta(x_2) - x_2 \neq 0$, 矛盾! \square

事实上我们可以证明 $[E : F] = |G|$, 但这需要一些额外的知识.

有了这两个方向的引理, 我们可以考虑它们的复合, 就有了下面两个问题:

Q1. E/F 是有限扩张, $G = \text{Gal}(E/F)$ 是有限群, 我们可以定义 $F' = \text{Inv}(G)$ 由定义可知 $F \subseteq F'$. 问题是 F' 与 F 能否相等?

Q2. 有 E 域, $G \leq \text{Aut}(E)$, 我们有 $F = \text{Inv}(G)$, 其中 E/F 是有限扩张, 于是 $G' = \text{Gal}(E/F)$ 是有限群, 由定义可知 $G \subseteq G'$. 问题是 G 与 G' 能否相等?

对于 Q2, 我们的结论是肯定的, 这也被称为 Artin 定理.

而对于 Q1, 则不能保证, Galois 理论研究的就是在什么样的有限扩张 E/F 可以使得 $\text{Inv}(\text{Gal}(E/F)) = F$.

例子 1.6.1:

1. $E = \mathbb{Q}(\sqrt{2}), F = \mathbb{Q}$, 易知 $\text{Gal}(E/F) = \{\text{id}\}$, 所以 $F' = E \neq F$. 我们考虑 $\alpha = \sqrt[3]{2}$, 极小多项式 $f(x) = x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$. 可以看到另外两个复数根都不在 E 中, 方程的其他根没有 E 中.
2. $F = \mathbb{F}_2(T), E = F(\sqrt{T}), \sqrt{T} = s, E$ 可以写成 $\text{Span}_T(1, s)$, 考虑 $\sigma : E \rightarrow E$ 是保 F 的一个自同构, $\sigma(1) = 1, \sigma(s) = u$. 因为 $s^2 = T$, 所以 $\sigma(s)^2 = \sigma(T) = T$, 即 $u^2 = T$. 考虑 $u = a + bs, a, b \in F$, $u^2 = a^2 + b^2 T = T$, 得到 $a^2 = T(1 + b^2) = T(1 + b)^2$. 考虑两边的次数, 只能有 $a = 0, b = 1$, 所以 $u = s$, 即 $\sigma(s) = s$, 所以 $F' = E$.

为了避免这两种坏情况, 我们后面要引入分裂域, 正规扩张等概念. 对于这些问题的深入探讨, 要留到最后一部分, 等我们讨论完环论和群论的基础知识.

2. 环与模

2.1. 定义与例子

定义 2.1.1 (环): 设 R 是一个集合, 定义了加法运算 $+: R \times R \rightarrow R$, 以及乘法运算 $*: R \times R \rightarrow R$, 满足以下条件:

1. 对于任意 $a, b, c \in R$, 有 $a + (b + c) = (a + b) + c$.
2. 对于任意 $a, b \in R$, 有 $a + b = b + a$.
3. 存在 $0 \in R$, 使得对于任意 $a \in R$, 有 $a + 0 = a$.
4. 对于任意 $a \in R$, 存在 $-a \in R$, 使得 $a + (-a) = 0$.
5. 对于任意 $a, b, c \in R$, 有 $a(bc) = (ab)c$.
6. 对于任意 $a, b, c \in R$, 有 $a(b + c) = ab + ac$.
7. 对于任意 $a, b, c \in R$, 有 $(a + b)c = ac + bc$.

我们称 $(R, +, \cdot)$ 构成一个环.

若存在 $1_R \in R$ 满足 $a1_R = 1_Ra = a$, 称 1_R 为单位元, 这样的环称为幺环.

若 $ab = ba$, 我们称 R 是交换环.

例子 2.1.1 (环):

1. $\mathbb{Z}, \mathbb{Z}_m = \{0, 1, \dots, m-1\}$.
2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 等所有的域都是环.
3. 多项式环.
4. 有线性空间 V , 则 $\text{End}(V)$ 是一个环.
5. 考虑 $R = m\mathbb{Z}, m \in \mathbb{N}, m \geq 2$. R 没有单位元.
6. $\mathbb{Z}[i]$ 为 Gauss 整数环. $\mathbb{Z}[\eta_m], \eta_m = e^{2\pi \frac{i}{n}}$.
7. 设集合 X , 环 $R, R^X = \{f: X \rightarrow R\}$, 定义 $f + g = x \mapsto f(x) + g(x), fg = x \mapsto f(x)g(x)$, 则 R^X 是一个环.
8. 假设 G 是有限群, F 是群, 我们定义 $R = \text{Span}_F(G)$, 不难按定义写出 R 的加法和乘法, 叫做 G 的群代数, 这是群表示论的基础.
9. $\mathbb{H} = \text{Span}_{\mathbb{R}}(1, i, j, k)$, 其中 $1, i, j, k$ 是四元数, 定义 $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j$, 这是一个含有单位, 非交换, 非零元可逆的环. 容易看出 $(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2 > 0$.

定义 2.1.2 (模): 设 R 是一个环, M 是一个集合, 定义了加法运算 $+: M \times M \rightarrow M$, 以及乘法运算 $*: R \times M \rightarrow M$, 满足以下条件:

1. 对于任意 $a, b, c \in M$, 有 $a + (b + c) = (a + b) + c$.
2. 对于任意 $a, b \in M$, 有 $a + b = b + a$.
3. 存在 $0 \in M$, 使得对于任意 $a \in M$, 有 $a + 0 = a$.
4. 对于任意 $a \in M$, 存在 $-a \in M$, 使得 $a + (-a) = 0$.
5. 对于任意 $a, b \in R, x \in M$, 有 $a(x + y) = ax + ay$.
6. 对于任意 $a, b \in R, x \in M$, 有 $(a + b)x = ax + bx$.
7. 对于任意 $a, b \in R, x \in M$, 有 $(ab)x = a(bx)$.
8. 对于任意 $x \in M$, 有 $1x = x$.

我们称 $(M, +, \cdot)$ 构成一个左 R -模. 同理可以定义右 R -模.

例子 2.1.2 (模):

2. 环与模

1. 域上的线性空间是模.
2. $\mathbb{Z}_m, \mathbb{Z} \times \mathbb{Z}_m \rightarrow \mathbb{Z}_m$, 定义 $(a, \bar{x}) \mapsto \bar{a} \cdot \bar{x}$. 更进一步的, 如果 G 是交换群, 可以定义 $\mathbb{Z} \times G \rightarrow G$, 其中 $(a, g) \mapsto g^a$, 我们称为 \mathbb{Z} - G 模.
3. (还有很多例子但我懒得写了)

2.2. 环与模同态

定义 2.2.1 (环同态): 设 R, S 是两个环, $\varphi: R \rightarrow S$ 是一个映射, 若满足:

1. 对于任意 $a, b \in R$, 有 $\varphi(a+b) = \varphi(a) + \varphi(b)$.
2. 对于任意 $a, b \in R$, 有 $\varphi(ab) = \varphi(a)\varphi(b)$.

则称 φ 是一个环同态. 若 R, S 都是幺环, 且 $\varphi(1_R) = 1_S$, 则称 φ 是幺环同态.

其他的一些我们所期待的性质都是可以推出的, 例如 $\varphi(0) = 0, \varphi(-a) = -\varphi(a), \varphi(a^n) = \varphi(a)^n$ 等.

定义 2.2.2 (模同态): 设 R 是环, M, N 是两个模, $\varphi: M \rightarrow N$ 是一个映射, 若满足:

1. 对于任意 $a, b \in M$, 有 $\varphi(a+b) = \varphi(a) + \varphi(b)$.
2. 对于任意 $a \in R, x \in M$, 有 $\varphi(ax) = a\varphi(x)$.

则称 φ 是一个模同态.

例子 2.2.1:

1. 考虑 $\mathbb{Z} \rightarrow \mathbb{Z}_m$ 上的一个映射 $a \mapsto (n \bmod m)$ 是环同态. 有趣的是不存在环同态 $\mathbb{Z}_m \rightarrow \mathbb{Z}$. 假设存在, 则 $\varphi(1) = 1, \varphi(2) = 2, \dots, \varphi(m) = m$, 但是 $\varphi(m) = \varphi(0) = 0$, 矛盾.
2. 1 中的例子不难推广到 $\mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m$.
3. $R = F[x]$, 对于 $\alpha \in F$, 定义 $\varphi(f) = f(\alpha)$, 则 φ 是一个环同态.

定义 2.2.3: 设 $\varphi: R \rightarrow S$ 是一个环同态, 则 $\ker(\varphi) = \{a \in R \mid \varphi(a) = 0\}$, 称为 φ 的核. 而 $\text{img}(R) = \{\varphi(a) \mid a \in R\}$, 称为 φ 的像.

对于模也是一样的, 我们不再赘述.

注意到环的核与像都是在加法与乘法下封闭的, 我们可以从中提炼出子环的概念.

定义 2.2.4: 设 R 是一个环, $S \subseteq R$, 若满足 S 是 R 的子集, 且对于任意 $a, b \in S$, 有 $a+b, ab \in S$, 则称 S 是 R 的子环.

显然, 对于环同态, 它的核与像是一个子环. 不过核有一个更强的性质: $a \in \ker(\varphi), b \in R \Rightarrow ab \in \ker(\varphi)$, 这是因为 $\varphi(ab) = \varphi(a)\varphi(b) = 0\varphi(b) = 0$. 这启示我们子环和子环之间也是不同的. 对于这种子环称为理想.

定义 2.2.5: 设 R 是一个环, $I \subseteq R$, 若满足 I 是 R 的子集, 且对于任意 $a \in I, b \in R$, 有 $ab \in I$, 则称 I 是 R 的左理想. 右理想类似定义.

不难看出, 对于交换环来说 aR 自然构成一个理想, 因为 $ax + ab = a(x+y), axay = a(axy)$. 这种理想称为由 a 生成的主理想.

2. 环与模

例子 2.2.2:

1. \mathbb{Z} 中的理想都是主理想. 假设 I 是 \mathbb{Z} 的一个理想, 且 $I \neq \{0\}$, 则存在 $m \in I, m > 0$ 是最小的, 则 $I = m\mathbb{Z}$. 若存在 $n > 0$ 不能表示为 m 的倍数, 则根据裴蜀定理, 存在 $x, y \in \mathbb{Z}$ 使得 $mx + ny = \gcd(m, n) < m$, 矛盾.
2. 考虑 $R = \mathbb{Z}(\sqrt{-5})$, $I = \{a + b\sqrt{-5} \mid a \equiv b \pmod{2}\}$, 不难证明 I 是 R 的一个理想. 它不是主理想, 可以视作 $I = \text{Span} \{2, 1 + \sqrt{-5}\}$.

我们知道域有特征的概念, 但当我们考虑环的时候, 这个概念似乎不太好. 以 \mathbb{Z}_6 为例, 它的特征是 6, 然而对于元素 2 来说, $3 \cdot 2 = 0$, 这似乎是一个特征为 3 的环. 为了解决这个问题, 我们引入了零因子的概念.

定义 2.2.6: 设 R 是一个环, 若存在 $a, b \in R, a \neq 0, b \neq 0$, 使得 $ab = 0$, 则称 a 和 b 是 R 中的零因子. 若交换幺环 R 中没有零因子, 则称 R 是一个整环.

而在整环上, 特征有了非常好的定义, 我们有下面的定理.

定理 2.2.1: 设 R 是一个整环, 若 $a \in R, a \neq 0, m \in \mathbb{N}, ma = 0$, 则存在素数 p 使得 $\forall b \in R, pb = 0$.

证明: 任取 $b \in R$, 考虑 $0 = 0 \cdot b = (ma)b = a(mb) = 0 \Rightarrow mb = 0$. 找素数与域上的证明类似. \square

2.3. 子环, 理想与商环

上文已经介绍过子环和理想的概念. 我们讨论一些例子.

例子 2.3.1:

1. 所有环同态的 \ker 都是理想. (后面会证明所有的理想也都是某一个环同态的 \ker).
2. R 和 $\{0_R\}$ 是 R 的理想, 称为平凡理想.
3. 若 R 是幺环, I 是理想, 且 $1_R \in I$, 则 $I = R$.
4. 若 R 是域, 则 R 的理想只有 $\{0_R\}$ 和 R 本身.
5. $R = \mathbb{C}[x]$. 我们证明这也是主理想环. 首先 $\mathbb{C}[x]$ 是一个整环. 假设理想 $I \neq 0, I \neq 1$, 假设存在多项式 $P(x) \in I, \deg p \geq 1$. 不妨设 P 在 I 是次数最下的, 这对于任意 $Q(x) \in I$, 考虑带余除法 $Q(x) = a(x)P(x) + b(x)$, 其中 $\deg b < \deg P$, 由理想定义可知 $a(x)P(x) \in I \Rightarrow b(x) \in I$. 从而 $b = 0$.
6. 考虑 $R = \mathbb{C}[x, y]$ 考虑 $I = xR + yR = \{p \in R \mid p(0, 0) = 0\}$, 这不是主理想.

上面的讨论引出了生成的概念.

定义 2.3.1: 设 R 是一个环, $a \in R$, 考虑 a 所生成的理想 $I_a = (a) = \{\sum_{i=1}^k f_k a g_k \mid f_k, g_k \in R, k \in \mathbb{N}\}$.

定义 2.3.2: 设环 R, I 是 R 的一个理想, 定义 R 上的二元关系 $\sim_I: a \sim_I b \Leftrightarrow b - a \in I$, 不难验证这是一个等价关系. 在等价类 R/I 上定义 $(a + I) + (b + I) := a + b + I; (a + I)(b + I) := (ab + I)$. 可以验证这是良定义的, 且构成一个环, 称为 R 关于 I 的商环.

不难发现, 考虑 $\pi: R \rightarrow R/I, a \mapsto a + I$, 则 π 是一个满射环同态, 且 $\ker(\pi) = I$.

例子 2.3.2:

1. $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[x]/(x^2 - 2)$
2. $\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$

2.4. 同态基本定理与中国剩余定理

定理 2.4.1 (第一同态定理): 设 $\varphi: R \rightarrow S$ 是一个环同态, 则 $R/\ker(\varphi) \cong \text{img}(\varphi)$.

证明: 记 $I = \ker(\varphi)$ 考虑映射 $\psi: R/I \rightarrow \text{Img}(\varphi), a + I \mapsto \varphi(a)$, 不难验证各种性质... \square

定理 2.4.2: 若 $\varphi: R \rightarrow S$ 是满同态, $J = \ker(\varphi)$ 是 R 的理想, 那么

1. 对于 R 中包含 J 的子环 R' , 记 $S' = \varphi(R')$, 则 S' 是 S 的子环; 反之对于 S 的子环 S' , 记 $R' = \varphi^{-1}(S')$, 则 R' 是 R 中包含 J 的子环.

特别的, 上述两条若将“子环”换成“理想”也成立, 且此时 $R/R' \cong S/S'$.

2. 对于每个包含于 J 的 R 的理想 I , 存在唯一的环同态 $\bar{\varphi}: R/I \rightarrow S$ 使得 $\varphi = \bar{\varphi} \circ \pi_I$, 其中 π_I 是 R 到 R/I 的商同态, 且此时 $\ker(\bar{\varphi}) = J/I$, 于是 $(R/I)/(J/I) \cong R/J$.

证明:

1. R' 是子环 $\Rightarrow S' = \varphi(R')$ 是子环, 容易得到.
2. S' 是子环 $\Rightarrow R'$ 是子环, 容易得到.
3. R' 是理想 $\Rightarrow S' = \varphi(R')$ 是理想. 设 $s_1 \in S', s_2 \in S$, 要证明 $s_1 s_2 \in S'$. 由定义知存在 $r_1 \in R'$ s.t. $s_1 = \varphi(r_1)$, 由满同态知存在 $r_2 \in R$ s.t. $s_2 = \varphi(r_2)$, 则 $s_1 s_2 = \varphi(r_1) \varphi(r_2) = \varphi(r_1 r_2) \in S'$.
4. S' 是理想 $\Rightarrow R'$ 是理想.
5. 要证 $R/R' \cong S/S'$, 定义 $\psi: a + R' \mapsto \varphi(a) + S'$, 良定义不难看出. 容易验证 ψ 是单的, 满的, 且为环同态.

定理的第一条证明完毕, 我们回答了对于包含 \ker 的子环或者理想的情况.

6. 首先 I 是 J 的理想, 定义 $\bar{\varphi}: R/I \rightarrow S, a + I \mapsto \varphi(a)$, 同样不难证明这是良定义的, 满的, 同态.

在验证完 $\ker(\bar{\varphi}) = J/I$ 后, 由第一同构定理自然有 $R/I/\ker(\bar{\varphi}) \cong \text{Img}(\bar{\varphi}) = S \cong R/J$, 这一结论我们称为第三同构定理.

7. $\bar{\varphi}(a + I) = \varphi(a) = 0 \Rightarrow a \in \ker(\varphi) = J \Rightarrow a + I \in J/I \Rightarrow \ker(\bar{\varphi}) \subseteq J/I$. 另一边也是显然的.
8. 最后证明唯一性.

这一部分回答的是被 \ker 包含的理想的情况. \square

上面回答了两个理想有包含关系的情况, 下面我们考虑两个理想的和与积, 显然它们都是理想.

定理 2.4.3 (第二同构定理): $\varphi: I/(I \cap J) \rightarrow (I + J)/J, x + I \cap J \mapsto x + J$ 是一个环同构.

例子 2.4.1: $R = \mathbb{Z}, I = 2\mathbb{Z}, J = 3\mathbb{Z}, I + J = \mathbb{Z}, I \cap J = 6\mathbb{Z}$, 则 $2\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$.

定义 2.4.1: 设 I, J 是 R 的理想, 若 $I + J = R$, 则称 I, J 互素. 对于么环, 这一条件等价于 $1_R \in I + J$.

定理 2.4.4 (中国剩余定理): 设 I, J 是 R 的互素理想, 则 $R/(I \cap J) \cong (R/I) \times (R/J)$.

证明:

1. 构造 $\varphi: R \rightarrow (R/I) \times (R/J), x \mapsto (x + I, x + J)$.

2. 环与模

2. 由于 $I + J = R \Rightarrow x = y + z, y \in I, z \in J$, 所以 $\varphi(x) = (z + I, y + J)$.
3. 我们要说明 φ 是满的.
4. 不难看出 $\ker(\varphi) = I \cap J$. 由环同构第一定理知结论成立.

□

接下来我们将推广到多个理想的情况. 这时我们需要额外的条件.

定义 2.4.2 (理想的乘积): 设 I, J 是 R 的理想, 定义 $IJ = \{\sum_{i=1}^n a_i b_i \mid a_i \in I, b_i \in J, n \in \mathbb{N}\}$. 这是一个理想.

$IJ \subseteq I \cap J$, 但一般来说不相等. 例如 $R = \mathbb{Z}, I = 2\mathbb{Z}, J = 2\mathbb{Z}$, 则 $IJ = 4\mathbb{Z}, I \cap J = 2\mathbb{Z}$.

我们关注什么时候 $IJ = I \cap J$.

引理 2.4.1: 设 R 是一个交换幺环, I_1, \dots, I_n 是 R 的理想, 且两两互素, 则

1. $I_1 \dots I_n = I_1 \cap \dots \cap I_n$.
2. $I_1 + \dots + I_{n-1}$ 与 I_n 互素.

证明: 采用数学归纳法.

1. 当 $n = 2$ 时 (2) 是显然的. 对于 (1), 显然有 $I_1 I_2 \subseteq I_1 \cap I_2$. 考虑 $x \in I_1 \cap I_2$, 由 $I_1 + I_2 = R$, 所以 $1_R = y + z, y \in I_1, z \in I_2$. 于是 $x = x1_R = xy + xz = yx + xz \in I_1 I_2$.
2. 当 $n > 2$ 时, $I_n + I_k = R$, 所以 $R = \prod_{k=1}^{n-1} (I_n + I_k) = I_n + I_1 \dots I_{n-1} \Leftrightarrow I_n + I_1 \cap \dots \cap I_{n-1} = R$. (1) 同样由归纳假设易得.

□

由这一引理和前面二元版本的中国剩余定理, 我们可以得到多元版本的中国剩余定理.

定理 2.4.5 (中国剩余定理): 设 R 是交换幺环, I_1, \dots, I_n 是两两互素的理想, 此时有同构 $R/(I_1 \cap \dots \cap I_n) = (R/I_1) \times \dots \times (R/I_n)$

例子 2.4.2: $R = \mathbb{Z}, I_1 = 3\mathbb{Z}, I_2 = 5\mathbb{Z}, I_3 = 7\mathbb{Z}$, 可以得到 $R/(I_1 \cap I_2 \cap I_3) \cong R/I_1 \times R/I_2 \times R/I_3$, 即 $\mathbb{Z}/105\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

2.5. 整环与整除性

环 \supseteq 幺环 \supseteq 交换幺环 \supseteq 整环 \supseteq 整闭整环 \supseteq GCD 环 \supseteq 唯一分解整环 \supseteq 主理想整环 \supseteq 欧几里得整环 \supseteq 域.
我们这里只涉及部分概念.

定义 2.5.1 (整环): 设 R 是一个非平凡的交换幺环, 若 R 没有零因子, 则称 R 是一个整环.

我们知道对于整数环 \mathbb{Z} , 存在有理数域 $\mathbb{Q} \supseteq \mathbb{Z}$, 一个自然的想法是对于任意整环 R , 是否存在域 F 使得 $R \subseteq F$? 这个问题的答案是肯定的.

我们首先定义 $S = R/\{0\}$, 显然 S 在乘法下依旧封闭且 $1_R \in S$. 下面要构造一个域 F , 其中的元素形如 $\frac{r}{s}, r \in R, s \in S$. 考虑 $(r, s) \in R \times S$, 定义等价关系 $(r_1, s_1) \sim (r_2, s_2) \Leftrightarrow r_1 s_2 = r_2 s_1$.

考虑 $F = R \times S / \sim$, 我们可以在上面定义加法和乘法, 容易验证这是一个域, 我们称为 R 的分式域.

定理 2.5.1: 设 R 是一个整环, F 是其分式域, 若有另一个域 F' 以及单的同态 $\varphi: R \rightarrow F'$, 则存在唯一的域同态 $\psi: F \rightarrow F'$ 使得 $\varphi = \psi \circ i_R$. 换句话说, 分式域是整环的最小域.

定义 2.5.2 (素理想): 设 R 是一个非零交换幺环, I 是 R 的理想, 若 R/I 是一个整环, 则称 I 是 R 的素理想.

定理 2.5.2: I 是素理想 $\Leftrightarrow I \neq R$ 且对于任意 $a, b \in R$, 若 $ab \in I$, 则 $a \in I$ 或者 $b \in I$.

证明: 1. (\Rightarrow) R/I 非零可推出 $I \neq R$. $ab \in I \Rightarrow ab + I = (a + I)(b + I) = 0_{R/I}$. R/I 是整环可推出 $a + I = 0 \vee b + I = 0$, 即 $a \in I \vee b \in I$.

2. 反之, $I \neq R$ 可推出 R/I 非零. 考虑 $a + I, b + I \in R/I$, 若 $(a + I)(b + I) = 0$, 则 $ab \in I$, 由条件知 $a \in I \vee b \in I$, 即 $a + I = 0 \vee b + I = 0$.

□

定义 2.5.3 (极大理想): 设 R 是一个非零交换幺环, m 是 R 的理想, 若 R/m 是一个域, 则称 m 是 R 的极大理想.

显然极大理想是素理想. 和素理想一样, 极大理想也有另一种定义方式:

定理 2.5.3: m 是极大理想 $\Leftrightarrow m \neq R$ 且对于包含 m 的理想只能是 m 或者 R .

证明:

1. $\Rightarrow R/m$ 是域, 所以 R/m 的理想只能是 0 或者 R/m , 所以 R 中包含 m 的理想只能是 m 或者 R .
2. 若 R/m 不是域, 则一定存在非平凡的理想, 则 m 一定含于这个非平凡理想, 与条件矛盾.

□

定义 2.5.4 (整除): 设 R 是一个整环, $a, b \in R$, 若存在 $c \in R$ 使得 $a = bc$, 则称 b 整除 a , 记作 $b \mid a$.

定义 2.5.5 (单位): 设 R 是一个整环, 若 a 有乘法逆, 则称 a 是一个单位. R 中所有单位构成一个群, 记为 R^\times .

例子 2.5.1:

1. $R = \mathbb{Z}, R^\times = \{1, -1\}$.
2. $R = \mathbb{Z}[i], R^\times = \{1, -1, i, -i\}$.
3. $R = \mathbb{Z}[\sqrt{3}]$, 牵扯到 Pell 方程.

在谈论整数的唯一分解性时, 我们一般只讨论正数的情况; 同样的, 在谈论任意一个环的时候, 我们也希望不用考虑正负号的问题, 也就是模掉单位群:

定义 2.5.6 (相伴): $a \sim b \Leftrightarrow \exists u \in R^x, s.t. a = ub$. 不难证明这是一个等价关系.

我们下文所讨论的相等即是在相伴意义下的.

定义 2.5.7:

1. $a, b \in R, a \neq 0, b \neq 0$, 若 $a \mid b, b \nmid a$, 则称 a 是 b 的一个真因子.
2. $a \in R, a \neq 0$, 若 a 不能分解为一系列真因子的乘积, 则称 a 是不可约的.
3. $a \in R, a \neq 0$, 若 (a) 是素理想, 则称 a 是素的.

一个自然的问题是: 不可约元与素元有何关系? 结论是: 素元肯定是不可约的, 不可约的不一定是素元.

例子 2.5.2:

1. $R = \mathbb{C}[x, y]/(y^2 - x^3) = \mathbb{C}[t^2, t^3]$, 考虑 $x = x + (y^2 - x^3)$, 它是不可约的, 但不是素的.
2. $R = \mathbb{Z}[\sqrt{-3}], a = 2$, 这也是不可约但不是素的例子.

引理 2.5.1: R 是整环, $q \in R, q \neq 0, q \notin R^x, q$ 不可约 $\Leftrightarrow (q)$ 是极大主理想.

利用上述引理不难证明:

定理 2.5.4: 素元一定是不可约元.

证明: 设 p 是素的, $(p) \subseteq (a)$, 则 $p = ab$, 由素的定义, 则 $a \in (p)$ 或 $b \in (p)$. 若 $a \in (p)$, 则 $(a) = (p)$; 若 $b \in (p)$, 可得 $a \in R^x \Rightarrow (a) = R$. \square

另一方面, 在环上加一些限制之后, 不可约元就一定是素的. 这一限制就是可以谈论最大公因子.

定义 2.5.8: 对于整环 $R, a, b \in R$ 且非零.

- 若 $d \in R$ 满足 $d \mid a$ 且 $d \mid b$, 则称 d 是一个公因子.
- 设 d 是一个公因子, 若对 a, b 的另一个公因子 c 有 $c \mid d$, 则称 d 是 gcd.
- 若对任意的 $a, b \in R$, 存在 a, b 的 gcd, 则称其为 GCD 整环.

例子 2.5.3: $R = \mathbb{Z}[\sqrt{-3}]$, 取 $a = 4, b = 2(1 + \sqrt{-3})$, 2 和 $1 + \sqrt{-3}$ 都是公因子.

定理 2.5.5: 若 R 是 GCD 整环, 则 R 的不可约元是素元. 我们也称满足不可约元一定是素元的整环满足素性条件.

定义 2.5.9: 设整环 $R, a \in R$ 非零非单位, 若 a 可分解为有限个不可约元的乘积, 且这个分解在相伴意义下唯一, 则称 R 是唯一分解整环 UFD.

不难看出 UFD 一定是 GCD, 反之不然.

2. 环与模

定义 2.5.10: 设 R 是整环, 若 R 中不存在如下形式的序列, a_1, a_2, \dots , 其中每个 a_{i+1} 都是 a_i 的真因子, 则称 R 满足因子链条件 (ACCP).

定理 2.5.6: 设 R 是整环, 则 R 是 UFD 等价于 ACCP + 素性条件.

一个显然的推论是 $\text{ACCP} + \text{素性条件} \Leftrightarrow \text{UFD}$.

定义 2.5.11: 设 R 是整环, 若 R 中的每个理想都是主理想, 则称 R 是主理想整环, 简称 PID.

定理 2.5.7: PID 是 UFD, 反之不然.

)这段内容我个人比较无感, 就跳过了.

2.6. 多项式环

对于一个交换幺环 R , 不难定义 $R[x]$.

定义 2.6.1: 设 R 是 UFD, 对于 $f \in R[x]$, $f(x) = a_0 + a_1x + \dots + a_nx^n$, 称 $d = \gcd_{R(a_0, \dots, a_n)}$ 为 f 的最大公因子, 若 d 是单位, 则称 f 是本原的.

2.7. 主理想整环上的有限生成模分类

定义 2.7.1: 设 R 是 PID, M 是 R 上的模, 若存在 $a_1, \dots, a_n \in M$, 使得 $M = (a_1, \dots, a_n)$, 则称 M 是有限生成的.

定理 2.7.1: 对于任意主理想整环上的有限生成模, 存在真理理想的降链 $(d_1) \supseteq (d_2) \supseteq \dots \supseteq (d_n)$, 使得 $M = (R/(d_1)) \times \dots \times (R/(d_n))$, d_i 叫不变因子.

证明有时间再讲.

3. 群与群作用

3.1. 定义与例子

定义 3.1.1: 回顾一下, 若集合 G 上定义了一个二元运算 $\cdot : G \times G \rightarrow G$, 满足结合律, 有单位元, 有逆元, 则称 (G, \cdot) 是一个群.

若群 G 上定义了一个映射 $G \times X \rightarrow X$, 满足 $1x = x$, $(ab)x = a(bx)$, 则称 (G, X) 是一个群作用.

同样不难定义群上的子群, 群同态.

例子 3.1.1:

1. 域, 线性空间, 环, 模在加法下都是群.
2. 有限群.
 1. $|G| = 1, G = \{e\}$;
 2. $|G| = 2, G = \{e, a\}, a^2 = e$, 此时 $G = \mathbb{Z}_2$;
 3. $|G| = 3, G = \{e, a, a^2\}, a^3 = e$, 此时 $G = \mathbb{Z}_3$;
 4. $|G| = 4, G_1 = \{e, a, a^2, a^3\}, a^4 = e$, 此时 $G_1 = \mathbb{Z}_4, G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$.
 5. $|G| = 5, G = \{e, a, a^2, a^3, a^4\}, a^5 = e$, 此时 $G = \mathbb{Z}_5$.
 6. $|G| = 6, G_1 = \{e, a, a^2, a^3, a^4, a^5\}, a^6 = e$, 此时 $G = \mathbb{Z}_6, G_2 = S_3 = \{e, (12), (13), (23), (123), (132)\}$. 这是第一个非交换群.
3. 无限群.
 1. $GL(V) = \{\varphi : V \rightarrow V \mid \varphi \text{ 线性, 可逆}\}$, 称为一般线性群.
 2. $SL(V) = \{\varphi \in GL(V) \mid \det(\varphi) = 1\}$, 称为特殊线性群.
 3. $O(V) = \{\varphi \in GL(V) \mid \varphi \text{ 保内积}\}$, 称为正交群.
 4. $SO(V) = \{\varphi \in O(V) \mid \det(\varphi) = 1\}$, 称为特殊正交群.
4. 多面体群

3.2. 子群, 正规子群与商群

定义 3.2.1: 设 (G, \cdot) 是一个群, $H \subseteq G$, 若 H 是 G 的子集, 且对于任意 $a, b \in H$, 有 $a \cdot b \in H$ 且 $a^{-1} \in H$, 则称 H 是 G 的子群.

定义 3.2.2 (陪集): 设 G 是一个群, $H \subseteq G$ 是一个子群, $a \in G$, 定义左陪集 $aH = \{ah \mid h \in H\} \triangleq G/H$, 右陪集 $Ha = \{ha \mid h \in H\} \triangleq H/G$.

定义 3.2.3 (正规子群): 设 G 是一个群, $H \subseteq G$ 是一个子群, 若对于任意 $a \in G$, 有 $aH = Ha$, 则称 H 是 G 的正规子群, 记为 $H \triangleleft G$.

定义 3.2.4: 设 $H \triangleleft G$, 在 G/H 上定义 $(xH)(yH) = (xy)H$, 则 G/H 是一个群, 称为 G 关于 H 的商群.

例子 3.2.1:

1. 在交换群上, 正规子群等价于子群.
2. $G_1 = \{1, c, c^2, c^3\}, H = \{1, c^2\}, G_1/H = \{H, cH\}$; 考虑另一个四个元素的群 $G_2 = \{1, a, b, ab\}, H = \{1, a\}, G_2/H = \{H, bH\}$.

我们可以发现 $H_1 \cong H_2, G_1/H_1 \cong G_2/H_2$, 然而 $G_1 \neq G_2$.

3. 定义群的中心 $Z(G) = \{a \in G \mid \forall b \in G, ab = ba\}$, 容易验证 $Z(G) \triangleleft G$.
4. 定义交换子 $[a, b] = a^{-1}b^{-1}ab$.

$[a, b]^{-1} = [b, a], g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$. 所有交换子也构成子群, 而事实上是正规子群, 记为 $[G, G]$. $G/[G, G]$ 是一个交换群.

定理 3.2.1: 子群 $|H| \mid |G|$.

3.3. 同态基本定理

定义 3.3.1: 设 (G, \cdot) 和 $(H, *)$ 是两个群, $\varphi: G \rightarrow H$ 是一个映射, 若满足 $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$, 则称 φ 是一个群同态.

定理 3.3.1: 设群同态 $\varphi: G \rightarrow H$, 则 $G/\ker(\varphi) \cong \text{Img}(\varphi)$.

定理 3.3.2: 若群同态 $\varphi: G \rightarrow H$ 是满的, 则 $H \cong G/\ker(\varphi)$.

定义 3.3.2: 设 H, K 是 G 的子群, 定义 $HK = \{hk \mid h \in H, k \in K\}$. 若 K 是正规子群, 则 HK 是子群, 且 $K \triangleleft HK$.

例子 3.3.1: $G = \{1, r, r^2, s, sr, sr^2\}$, $H = \{1, s\}$, $K = \{1, sr\}$, HK 不是子群.

三同构定理的证明和之前环的情况类似, 我们不再赘述.

定义 3.3.3:

1. 设 G 是有限群, 若有 G 的子群链 $G = G_0 > G_1 > \dots > G_k = \{e\}$ 满足每个 G_i 都是 G_{i-1} 的正规子群, 则称 k 是 G 的正规子群链的阶数.
2. 若有 G 的子群链 $G = G_0 > G_1 > \dots > G_k = \{e\}$ 满足每个 G_i 都是 G_{i-1} 的正规子群, 则称为一个次正规子群链.
3. 对于一个次正规子群链, 若 G_i/G_{i-1} 都是单群(没有非平凡的正规子群), 则称为一个合成列, 这些单群称为合成因子.

定理 3.3.3 (Jordan-Holder 定理): 有限群 G 的极小合成列有相同的长度, 且合成因子在同构意义下唯一. 即给定 $G = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_s = \{e\}$, $G = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_t = \{e\}$, 要证 $t = s$ 且 G_i/G_{i-1} 与 H_i/H_{i-1} 在调整顺序后两两同构.

证明: 对 s 归纳.

- 当 $s = 1$ 时, G 是单群, 显然成立.
- 假设 $s - 1$ 时成立, 考虑 s 的情形. 若 $G_1 = H_1$, 则结论显然成立.

若 $G_1 \neq H_1$, 因为 $G_0/G_1, H_0/H_1$ 都是单群, 所以 G_1, H_1 都是极大正规子群. 考虑 $G' = G_1 \cdot H_1$ 也是正规的. 可见 $G' = G$. 设 $G_1 \wedge H_1 = N_2$. 则 $G_0/G_1 = G_1 \cdot H_1/G_1 = H_1/G_1 \wedge H_1 = H_1/N_2$, $H_0/H_1 = G_1/N_2$. 取极小合成列 $N_2 \triangleleft N_3 \triangleleft \dots \triangleleft N_r = \{e\}$. 构造 $G = G_0 \triangleleft G_1 \triangleleft N_2 \triangleleft \dots \triangleleft N_r = H_0 \triangleleft H_1 \triangleleft N_2 \triangleleft \dots \triangleleft N_r = \{e\}$. 可得 $r = s, r = t$, 故 $s = t$. 通过这四个合成列的相互关系与归纳假设, 可得结论. \square

3. 群与群作用

在这一定理基础上, 对于研究所有有限群, 我们可以 1. 找出所有有限单群, 2. 在给定合成因子的前提下找出所有 G . 看起来第二个问题比较简单, 但事实上第二个问题到现在也没有很好的算法; 而第一个问题有限单群的分类已经基本完成了:

(1) \mathbb{Z}_p, p 为素数 (2) $A_n, n \geq 5$ (3) 李型单群 (4) 从(3)导出的 (5) 散在单群 26 个

3.4. 群作用与 Sylow 定理

这一节我们假设 G 是一个有限群, 被作用的空间也是有限的.

定义 3.4.1: 设群 G 与集合 X , 若映射 $\mu: G \times X \rightarrow X, (g, x) \mapsto gx$ 满足:

1. $ex = x$
2. $(gh)x = g(hx)$

则称 (G, X) 是一个群作用.

1. 对于 $g \in G$, 考虑 $t_g: X \rightarrow X, x \mapsto gx$ 是一个平移.
2. 对于 $x \in X$, 考虑 $Gx = \{gx \mid g \in G\}$, 称为 x 的轨道. 和陪集一样, 轨道只能相等或者不相交.
3. 我们还可以定义 $\text{stab}(x) = \{g \in G \mid gx = x\}$, 称为 x 的稳定化子群. 若 $\text{stab}(x) = G$, 则称 x 是一个不动点.

引理 3.4.1: 存在双射 $G/\text{stab}(x) \rightarrow Gx$.

根据这一引理我们可以得到一个计数的结果: $|Gx| = [G : \text{stab}(x)] = |G| / |\text{stab}(x)|$.

设 $O = \{Gx \mid x \in X\} \subseteq 2^X$, 构造 $\pi: X \rightarrow O, x \mapsto Gx$ 满射. 由选择公理知道存在单射 $\theta: O \rightarrow X$ 满足 $\pi \circ \theta = \text{id}$. 记 $C = \text{Im}(\theta)$, 与每一个轨道恰好有一个交点, 称为一个截面.

若 x_1, x_2 属于同一个轨道 Gx , 容易看出来 $\text{stab}(x_2)$ 与 $\text{stab}(x_1)$ 只差一个共轭作用.

完成了这些准备工作, 我们考虑 $X = \bigcup_{x \in C} Gx$, 可知 $|X| = \sum_{x \in C} |Gx| = \sum_{x \in C} [G : \text{Stab}(x)]$.

下面考虑 G 在自身的共轭作用, 取 $X = G, \mu(g, x) = gxg^{-1}$. x 的轨道就是 $\{gxg^{-1} \mid g \in G\}$, 称为 x 的共轭类. x 的稳定化子就是中心化子. 若 x 是不动点, 则是一个平凡共轭类. 若不是, 则称为非平凡共轭类. 非平凡共轭类记 T .

通过这一区分, 我们知道 $|G| = |Z| + \sum_T [G : \text{stab}(x)]$. 这里的后项是非平凡共轭类的集合.

例子 3.4.1:

1. 若 $|G| = p^m, p$ 为素数, 则称为 G 为一个 p 群, 类方程为 $p^m = |Z| + \sum_{x \in T} [G : C(x)]$. 我们可知 $p \mid |Z|$.
2. 设有 n 个轨道, 则 $n = \frac{1}{|G|} \sum_{g \in G} |X^g|$, 其中 $X^g = \{x \in X \mid gx = x\}$.

证明: $\sum_{g \in G} |X^g| = \sum_{x \in X} |\text{stab}(x)| = \sum_{x \in X} \frac{|G|}{|Gx|} = |G| \sum_{x \in X} \frac{1}{|Gx|} = |G| n$.

接下来我们进入 Sylow 定理的讨论. 这一定理在探讨什么时候 $d \mid |G|$, 问是否存在 $H < G, |H| = d$. Sylow 定理告诉我们当 d 是素数的阶数时, 这一结论是对的.

引理 3.4.2: 设 G 是有限交换群, p 是素数, $p \mid |G|$, 则 G 中存在阶数为 p 的元素.

证明: 对群 G 的阶数归纳.

- $|G| = 1$, 成立.

3. 群与群作用

- 当阶数 $< |G|$ 时交换群都成立, 考虑 G . 任取 $a \in G, a \neq e$, 设 a 的阶数为 m , 若 $p \mid m$ 显然可找到这样的 p 阶元; 反之, $H = \langle a \rangle$ 是正规子群. 考虑 G/H , 由归纳假设...

□

定理 3.4.1 (Sylow-I): 假设有限群 G , 素数 p , 且 $p^k \mid |G|$, 则 G 有 p^k 阶子群.

证明: 对 $|G|$ 归纳.

- $|G| = 1$, 成立.
- 设对 $|G| < n$ 成立, 考虑 $|G| = n$. 有方程 $|G| = |Z| + \sum_{x \in T} [G : C(x)]$. 若 p 不整除 $|Z|$, 则一定存在 $p^k \mid C(x)$, 成立; 若 $p \mid |Z|$, 那么由上引理得到 Z 有 p 阶子群 $H = \langle a \rangle$. H 是 G 的正规子群, 考虑 $G/H = G', |G'| < |G|, p^{k-1} \mid |G'|$. 由归纳假设得到 G' 有 p^{k-1} 阶子群 H' , 那么我们就得到 G 有 p^k 阶子群.

□

定义 3.4.2:

1. 若 $|H| = p^k$, 则称 H 叫 p -群.
2. 若 $G, p, |G|$ 中 p 的阶为 m ,
则该群中的 p^m 阶子群叫 p -Sylow 子群.

定理 3.4.2 (Sylow-II): 群 G 中的任意两个 p -Sylow 子群都共轭.

一个显然的推论是如果只有一个 Sylow 子群, 则这个群是正规的.

证明: 我们要证明: 设 P 是 p -Sylow 子群, H 是 G 的 p -子群, $|H| = p^k$, 则存在 $g \in G$, 使得 $H \subseteq gPg^{-1}$.

考虑群作用: $\mu : H \times G/P \rightarrow G/P, (h, gP) \mapsto hgP$, 因为 $|P| = p^m$, 所以 $|G/P| = \frac{|G|}{p^m}$, 从而 p 不整除. 考虑 μ 的轨道, $|H(gP)| = 1 \vee p^l, 1 \leq l < k$. 因为不整除, 所以至少有一个不动点, 所以 $H \subseteq gPg^{-1}$. □

定理 3.4.3 (Sylow-III): 给定群 G, P 同上, 设 G 的 p -Sylow 的个数为 n_p , 再设 $[G : P] = m$, 则 $n_p \mid m$, 且 $n_p \equiv 1 \pmod{p}$.

证明: 设 G 的所有子群集合为 S , 考虑群作用 $G \times S \rightarrow S, (g, H) \mapsto gHg^{-1}$. 设 P 是 G 的一个 p -Sylow 子群, 先问它的稳定化子是什么. 由 Sylow-II 定理我们知道 $n_p = |GP| = [G : \text{stab}(P)] = [G : N_G(P)]$. 另一方面, $m = [G : P] = [G : N_G(P)][N_G(P) : P] = n_p[N_G(P) : P]$, 从而 $n_p \mid m$.

考虑另一个群作用, $P \times G/P \rightarrow G/P, (h, gP) \mapsto hgP$

□

这些定理实在看的人有点累, 不过我们利用上述三定理可以对有限群的结构做许多有趣的研究.

例子 3.4.2:

1. 设 p, q 是素数, $p < q$, 则 pq 阶群 G 一定不是单群.

考虑 G 的 q -Sylow 子群, 那么 $n_q \mid p, n_q \equiv 1 \pmod{q}$, 所以 $n_q = 1$, 从而 G 有正规子群.

2. 若 $|G| = 2024 = 2^3 \cdot 11 \cdot 23, n_{23} \mid 2^3 \cdot 11, n_{23} \equiv 1 \pmod{23}$, 所以 $n_{23} = 1$, 从而 G 有一个 23 阶正规子群.

3. 群与群作用

$G/P_{23} = G_1, |G_1| = 2^3 \cdot 11, n_{11} \mid 2^3, n_{11} = 1 \pmod{11}$, 所以 $n_{11} = 1$, 从而 G_1 有一个 11 阶正规子群.

3. $|G| = 56 \Rightarrow G$ 不是单群. $n_7 = 1 \vee n_7 = 8$. 若 $n_7 = 1$, 则 G 有正规子群;

若 $n_7 = 1$, 证毕; 若 $n_7 = 8$, 则 G 有 8 个 7 阶子群. 我们断言这些子群的交只能是单位元. 所以 G 中有一个 $e, 8 \times 6$ 个 7 阶元, 还剩 7 个元素. 再考虑 2-Sylow 子群, 阶是 8, 恰好只有一个子群, 所以是正规子群.

4. $|G| = 108 \Rightarrow G$ 不是单群.

定理 3.4.4: 最小的非交换单群是 60 阶的. (就是 A_5)

证明:

1. 平凡群显然是交换.
2. 素数阶群都交换 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59.
3. pq 型的都不单 6, 10, 14, 22, 26, 34, 38, 46, 57, 58, 5, 8, 15, 21, 33, 39, 51, 35, 55.
4. p^k 阶的都是交换的或者不单 4, 9, 25, 49, 8, 27, 16, 32.
5. 2^2p 型群, $|G| = 12, 20, 28, 44, 52$, 继续利用 Sylow 定理可以解决.
6. 3^2p 型群, $|G| = 18, 57, n_3 = 1$, 不是单群.

还有 24 和 36 阶群, 我们需要引入一个引理

引理 3.4.3: 若有限群 G 有子群 H , $[G:H] = n$, 则 H 一定包含一个 G 的正规子群 K , 且 $[G:K] \mid n!$. 特别的, 如果 $|G|$ 不整除 $n!$, 则 K 是非平凡的正规子群.

考虑 24 阶群, $24 = 2^3 \cdot 3$. 由 Sylow 第三定理则 $n_2 \mid 3, n_2 = 1 \pmod{2}$, 所以 $n_2 = 1 \vee 3$. 若是第一种情况, 则证毕; 若是第二种情况, 设 H 是一个八阶子群, 且 $24 > 3! = 6$, 由引理知存在正规子群 K .

36 阶群同理. □

3.5. 对称群

上一节我们已经知道 60 阶以下的群都是交换群或者不单的, 我们接下来要构造并证明一个 60 阶的非交换单群.

对于奇置换, 偶置换, 轮换, 循环等等定义我们不再赘述.

偶置换构成的群是 A_n , 它是 S_n 的正规子群, 且 $|S_n : A_n| = 2$.

引理 3.5.1: A_n 可由 3-循环生成.

引理 3.5.2: $n \geq 5$ 时, 所有 3-循环都是共轭的.

定理 3.5.1: $A_n, n \geq 5$ 是单群.

证明: 设 K 是 A_n 的正规子群, $K \neq \{e\}$, 要证 $K = A_n$. 由引理 1 知只需要证明包含所有 3-循环, 由引理 2 知只需要证明包含一个 3-循环. □

4. Galois 理论