

抽象代数笔记

詹奇

Last updated: **October 10, 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	3
1.4. 域的扩张	3
1.5. 代数闭包	5
1.6. Galois 群初探	6
2. 环与模	7
2.1. 定义与例子	7
2.2. 环与模同态	8
2.3. 子环, 理想与商环	9
2.4. 同态基本定理	10
3. 群与群作用	11
4. Galois 理论	11

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.

注记. 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.

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

证明.

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

1. 域与线性空间

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 $\cdot: F \times V \rightarrow V$, 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.

1. 域与线性空间

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 $E = \text{Span}_{F(e_1, \dots, e_n)} E = F(e_1, \dots, e_n)$. □

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元的性质.

引理 1.4.1. 设 $E/F, \alpha, \beta$ 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. □

现在来看具体的关系.

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. □

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:

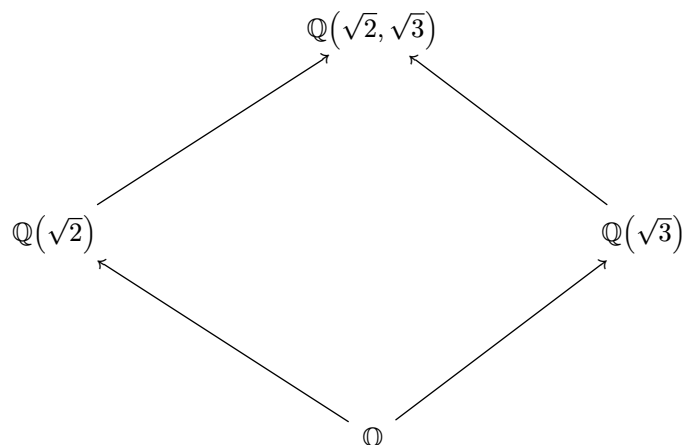
1. E/F 是有限扩张.
2. $E = F(u_1, \dots, u_n)$, 其中 u_1, \dots, u_n 是 F 上的代数元. 此时 E/F 是代数扩张.

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.

注记. 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 . $\sigma(f_1(u_1)) = \sigma(0) = 0 = \sigma(u_1^n + \dots + a_n) = f_1(\sigma(u_1))$.

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 $\eta_j(x_1\mu_1 + \dots + x_{\mu_m}) = x_1\eta_j(\mu_1) + \dots + x_m\eta_j(\mu_m) = 0$, 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! □

注记. 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 $u = a + bs, a, b \in F, u^2 = a^2 + b^2T = T$, 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.

2. 环与模

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).

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 $(a, \bar{x}) \mapsto \overline{a \cdot x}$. 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.

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 $I_a = (a) = \left\{ \sum_{i=1}^k f_i a g_i \mid f_i, g_i \in R, k \in \mathbb{N} \right\}$.

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

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... □

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

2. 环与模

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. □

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

3. 群与群作用

4. Galois 理论