



華東師範大學
EAST CHINA NORMAL UNIVERSITY

抽象代数

笔记

© syqwq
East China Normal University

Contents

1. 域论、线性空间	3
1.1. 定义和例子	3
1.2. 域的同态	8
1.3. 域的特征 (characteristic)	11
1.4. 域的扩张	13
2. 环论、模论	18
3. 群论、群作用	19
4. Galois 理论	20

Chapter 1

域论、线性空间

1.1 定义和例子

Definition 1.1.1 域.

假设集合 F 有如下元素和定义在 F 上的运算：

- 零元: $0 := 0_F$
- 单位元: $1 := 1_F \neq 0_F$
- 加法: $+: F \times F \rightarrow F, (x, y) \mapsto x + y$
- 乘法: $\cdot: F \times F \rightarrow F, (x, y) \mapsto x \cdot y$

并且, F 上的加法和乘法满足:

1. 加法结合律: $(x + y) + z = x + (y + z)$
2. 加法交换律: $x + y = y + x$
3. 加法单位元: $x + 0 = 0 + x = x$
4. 加法逆元: $\forall x \in F, \exists y \in F, x + y = y + x = 0$, 记作 $-x$
5. 乘法结合律: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. 乘法交换律: $x \cdot y = y \cdot x$
7. 乘法单位元: $x \cdot 1 = 1 \cdot x = x$
8. 乘法逆元: $\forall x \in F^*, \exists y \in F, x \cdot y = y \cdot x = 1$, 记作 x^{-1}
9. 分配律:
 1. $x \cdot (y + z) = x \cdot y + x \cdot z$
 2. $(x + y) \cdot z = x \cdot z + y \cdot z$

则称 F 是一个域.

Lemma 1.1.1 关于零元.

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

Proof.

- 考虑如下事实:

$$\begin{aligned} a &= 0 \cdot (0 + 1) = 0 \cdot 1 = 0 \\ &= 0 \cdot 0 + 0 \cdot 1 = 0 \cdot 0 + 0 = 0 \cdot 0 \end{aligned}$$

- 考虑 $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$, 令 $y = -(x \cdot 0)$, 得到

$$y + x \cdot 0 = y + x \cdot 0 + x \cdot 0 \Leftrightarrow 0 = x \cdot 0$$

■

注意到在定义中, 我们要求 $0_F \neq 1_F$, 若 $0 = 1$, 则 $\forall x \in F, x = x \cdot 1 = x \cdot 0 = 0$, 于是 $F = \{0\}$, 太平凡了, 于是我们排除这种情况.

又注意到, 在乘法逆元定义中我们要求 $x \neq 0$, 这是因为假设 $x = 0$ 有乘法逆 y , 则 $x \cdot y = y \cdot x = 1 \Rightarrow 0 \cdot y = y \cdot 0 = 1 \Rightarrow 1 = 0$, 则与上一条矛盾.

Remark 1.1.1 非零元记号.

为了方便讨论, 我们将域中的非零元记作 $F^* = F \setminus \{0\}$

Remark 1.1.2 逆元是唯一的.

- 加法逆元是唯一的. 假设 对于 x 存在两个加法意义下的逆元 y_1, y_2 , 则

$$y_1 = y_1 + 0 = y_1 + x + y_2 = 0 + y_2 = y_2$$

因此, $y_1 = y_2$.

- 乘法逆元是唯一的. 证明类似, 此处略.

Example 1.1.1 一些域的例子.

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- $F = \mathbb{Q}(\sqrt{2}) = \{x + \sqrt{2}y \mid x, y \in \mathbb{Q}\}$
可以验证, 每个元素确实存在加法逆元和乘法逆元 (分母有理化)
- $F = \mathbb{Q}(\sqrt[3]{2})$

Proof $F = \mathbb{Q}(\sqrt[3]{2})$. 记 $\alpha = \sqrt[3]{2}$, $F = \{x + y\alpha + z\alpha^2 \mid x, y, z \in \mathbb{Q}\}$, 我们主要考虑乘法逆

$$\begin{aligned} \frac{1}{x + y\alpha + z\alpha^2} &= \frac{y - z\alpha}{(x + y\alpha + z\alpha^2)(y - z\alpha)} = \frac{*}{x(y - z\alpha) + \alpha(y^2 - z^2\alpha^2)} \\ &= A \cdot \frac{1}{s + t\alpha} = \frac{s^2 - st\alpha + t^2\alpha^2}{(s + t\alpha)(s^2 - st\alpha + t^2\alpha^2)} \\ &= \frac{*}{s^3 - t^3\alpha^3} = \frac{*}{s^3 - 2t^3} \in F \end{aligned}$$

Remark 1.1.3 $F[x]$ 与 $F(x)$.

注意区分 $F[x]$ 和 $F(x)$, 前者是 $\left\{ \sum_{i \geq 0} a_i x^i \mid a_i \in F \right\}$, 后者是在域 F 中添加 x 生成的新的域.

Proposition 1.1.1 $\mathbb{Q}(\alpha)$ 是域.

设 $\alpha \in \mathbb{C}$ 是 $f(x)$ 的根, 其中 f 是 \mathbb{Q} 上的首一不可约多项式, $\deg f = n$, 则有:

$$F = \mathbb{Q}(\alpha) = \{x_1 + x_2\alpha + \cdots + x_n\alpha^{n-1} \mid x_i \in \mathbb{Q}\}$$

F 是一个域.

Proof. 我们主要考虑乘法逆. 设 $f(\alpha) = \alpha^n + b_1\alpha^{n-1} + \cdots + b_{n-1}\alpha + b_n = 0$, 对于形式更高阶的, 可以通过带余除法, 最终化成次数最高不超过 $n-1$ 的形式, 因此我们考虑如下的乘法逆:

$$\frac{1}{g(\alpha)} = \frac{1}{x_1 + x_2\alpha + \cdots + x_n\alpha^{n-1}}$$

首先我们有 $(f, g) = 1$, 于是 $\exists u, v \in \mathbb{Q}[\alpha], ug + vf = 1$, 回到上面的式子

$$\frac{1}{g(\alpha)} = \frac{u}{ug + vf}(\alpha) = u(\alpha) \in \mathcal{P}_{n-1}(\alpha) = F$$

■

Example 1.1.2 在有理数域中加入两个无理数.

4. 考虑 $F = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{x_1 + x_2\sqrt{2} + x_3\sqrt{3} + x_4\sqrt{6} \mid x_i \in \mathbb{Q}\}$, 也是域.

Proof. 首先, 加法和乘法的封闭性容易验证. 我们考虑乘法逆.

$$\frac{1}{x_1 + x_2\sqrt{2} + x_3\sqrt{3} + x_4\sqrt{6}} = \frac{y_1 + y_2\sqrt{2} + y_3\sqrt{3} + y_4\sqrt{6}}{(x_1 + x_2\sqrt{2} + x_3\sqrt{3} + x_4\sqrt{6})(y_1 + y_2\sqrt{2} + y_3\sqrt{3} + y_4\sqrt{6})}$$

因此, 现在的核心任务就是考虑如何取 y_i 的值, 能够使得分母是一个有理数. 我们将分母展开之后, 进行待定系数, 求解线性方程组即可. 我们只需要无理数项的系数为 0, 因此只有三个方程, 而有四个未知数, 因此一定有非零解. ■

加了两个无理数, 也确实构成一个域. 但是其实, 加了这两个无理数和加一个无理数的效果是一样的.

我们来看看 $F' = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. 按照 Proposition 1.1.1 的思路, 考虑能否找到一个多项式使得 $\alpha = \sqrt{2} + \sqrt{3}$ 是他的根. 通过平方, 移项, 平方, 不难得到 $f(\alpha) = \alpha^4 - 10\alpha^2 + 1 = 0$, 利用 Eisenstein 判别法可以得到 f 是一个不可约多项式, 因此我们断言:

$$F' = \{x_1 + x_2\alpha + x_3\alpha^2 + x_4\alpha^3 \mid x_i \in \mathbb{Q}\}$$

接下来, 要说明: $F = F'$. 手玩得到:

$$\begin{cases} \alpha^3 = 11\sqrt{2} + 9\sqrt{3} \\ \alpha = \sqrt{2} + \sqrt{3} \end{cases}$$

因此, $\sqrt{2}, \sqrt{3}$ 都可以用 α 的多项式表示出来, 而他们又可以生成整个 F , 因此整个 F 都可以用 F' 表示出来. 或者可以这样考虑 $F = \text{span}(1, \sqrt{2}, \sqrt{3}, \sqrt{6}), F' = \text{span}(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$, 而线性方程组又给出了这两组基之间的基变换, 并且可以验证是双射, 因此这两组基可以互相线性表出, 从而他们张成的空间实际上是同一个空间.

我们把这种只加一个元的域扩张叫做**单扩张**, 加若干元的扩张叫**有限扩张**. 在一定条件下, 有限域扩张就是单扩张.

Example 1.1.3 有限域的例子.

5. $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$
6. $\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

Proof. 通过列加法表、乘法表, 不难验证他们都构成域. ■

Example 1.1.4 模素数剩余系构成的有限域.

7. 设 $p \in \mathbb{N} \cap \mathbb{P}$, 则整数集的模 p 剩余系: $\mathbb{F}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$ 是一个域.

Proof. 考虑乘法逆. 对于 $\bar{k} \in \mathbb{F}_p^*$, 由于 $p \in \mathbb{P}$, 那么 $k \perp p$, 根据 Bezout 定理, 有: $\exists u, v \in \mathbb{Z}, uk + vp = 1$ 两侧取模可得 \bar{u} 就是 \bar{k} 的乘法逆.

另解. 构造一个映射 $T: \mathbb{F}_p \rightarrow \mathbb{F}_p, y \mapsto ky$, 接下来, 我们证明: $\ker T = \{0\}$. 如果 $T(y) = 0 \Leftrightarrow ky \equiv 0 \Leftrightarrow ky = pm \Leftrightarrow p \mid y \Leftrightarrow y = \bar{0}$, 因此, 我们可以把映射限制到 \mathbb{F}_p^* 上, 为了证明每个元素都存在逆元, 我们只需要证明 T 是双射. 由于 T 是有限集合上的映射, 因此只需要证明 T 是单射即可. 考虑 $T(y_1) = T(y_2)$, 即 $ky_1 = ky_2 \Leftrightarrow k(y_1 - y_2) \equiv 0 \Leftrightarrow y_1 \equiv y_2$, 因此 T 是单射. 从而, 1 在 T 的原像是唯一且存在的. ■

Remark 1.1.4.

若 $p \notin \mathbb{P}, m \in \mathbb{N}, m \geq 2, \mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$, 则乘法逆不一定存在. 比如 $m = 4, 2 \cdot 2 = 0$, 而 $\bar{2} \neq \bar{0}$, 此时称 2 为零因子.

Example 1.1.5 函数域.

8. 设 F 是一个域. $F(x) = \left\{ \frac{p(x)}{q(x)} \mid p(x), q(x) \in F[x], q(x) \neq 0 \right\}$
9. $K = \mathbb{C}(x, \sqrt{x^3 + 2}) = \mathbb{C}(x)(y) \sim \mathbb{Q}(\sqrt{2}) = \{R_1(x) + R_2(x)y \mid R_1, R_2 \in \mathbb{C}[x], y = \sqrt{x^3 + 2}\}$, 此处类比向 \mathbb{Q} 中加入 $\sqrt{2}$. 这个 K 是一条代数曲线上的亚纯函数.

Definition 1.1.2 线性空间.

设 F 是一个域, 集合 V 和上面定义两个运算:

- 加法: $+: V \times V \rightarrow V$
- 数乘: $\cdot: F \times V \rightarrow V$

如果 $0_V \in V$, 且满足:

1. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$
2. $\alpha + \beta = \beta + \alpha$
3. $\alpha + 0_V = 0_V + \alpha = \alpha$
4. $\forall \alpha \in V, \exists 1\beta \in V$ s.t. $\alpha + \beta = \beta + \alpha = 0_V$, 且 $-\alpha \triangleq \beta$
5. $(xy)\alpha = x(y\alpha)$
6. $1_F \cdot \alpha = \alpha$
7. $(x + y)\alpha = x\alpha + y\alpha$
8. $x(\alpha + \beta) = x\alpha + x\beta$

则称集合 V 连同它上面的两个运算为域 F 上的线性空间 V .

Example 1.1.6 线性空间的例子.

1. $\mathbb{Q}(\sqrt{2})$ 是 \mathbb{Q} 上的 2 维线性空间.
2. $\mathbb{Q}(\sqrt[3]{2})$ 是 \mathbb{Q} 上的 3 维空间.
3. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 是 \mathbb{Q} 上的 4 维空间.
4. $F(x)$ 是无穷维的线性空间.
5. K 是 $\mathbb{C}(x)$ 上的 2 维线性空间.
6. \mathbb{R} 是 \mathbb{Q} 上的无穷维空间.
7. \mathbb{C} 是 \mathbb{R} 上的 2 维空间.

通过类比 Proposition 1.1.1, 我们来看一些更复杂的例子.

Theorem 1.1.1.

$p \in \mathbb{P}, d \in \mathbb{Z}_+$, 记 $q = p^d$, 则存在一个 q 元有限域 \mathbb{F}_q .

Proof. 取 \mathbb{F}_p 上的一个 d 次不可约多项式 $f(x)$, 构造商环 $K = \mathbb{F}_p[x]/\langle f(x) \rangle$ 可以看成是 $f(\alpha) = 0$, 从而得到一个域 \mathbb{F}_p 上的 d 维线性空间, 一组基为 $1, x, x^2, \dots, x^{d-1}$. 因此 K 一共有 p^d 个元素. 接下来考虑乘法逆是否存在. $\forall g(x) \in K, \deg g < d$ 且 f 是不可约多项式, 因此 $(f, g) = 1$, 从而由 Bezout 定理, $\exists u, v \in K$ s.t. $uf + vg = 1$, 模掉 f , 得到 g 的逆元为 v . 因此 K 就是所要求的 \mathbb{F}_q . ■

Example 1.1.7 四元数.

10. 考虑四元数 $\mathbb{F}_4 = \{x + y\alpha \mid x, y \in \mathbb{F}_2\} = \mathbb{F}_2(\alpha)$ 的结构.

Solution. $\mathbb{F}_2 = \{0, 1\}$, 为了方便研究, 我们画出 \mathbb{F}_2 的加法表和乘法表:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

考虑 $\mathbb{F}_2[x] : f(x) = x^2 + px + q$ 中的不可约多项式, 其中 $p, q \in \mathbb{F}_2$.

首先, $f(x) \in \{x^2, x^2 + x, x^2 + 1, x^2 + x + 1\}$, 其中的不可约多项式实际上只有 $x^2 + x + 1$. 因此若 $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, 则 α 满足 $\alpha^2 + \alpha + 1 = 0 \Leftrightarrow \alpha^2 = 1 + \alpha$. 此时, $\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha = \alpha^2\}$. 接下来我们可以验证这样的 \mathbb{F}_4 是否是域. 利用加法表和乘法表:

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

·	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

发现乘法逆其实是 $\alpha^{-1} = \alpha^2$. 因此这确实是一个域. □

类似的, 我们还可以找到一些比较简单的可以手玩的例子.

Example 1.1.8.

11. $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$, 其中 $\alpha^2 = 2$ 或 $\alpha^2 + 1 = 0$.

12. $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$, 其中 $\alpha^3 = 1 + \alpha$.

1.2 域的同态

Definition 1.2.1 线性空间的同态.

设 V_1, V_2 是域 F 上的线性空间, 若映射 $\varphi: V_1 \rightarrow V_2$ 满足:

1. $\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$
2. $\varphi(k\alpha) = k\varphi(\alpha)$

则称 φ 是同态.

其实, 同态就是保运算的映射.

Definition 1.2.2 域的同态.

设 F_1, F_2 是两个域. 若 $\varphi: F_1 \rightarrow F_2$ 满足:

1. $\varphi(0_{F_1}) = 0_{F_2}$
2. $\varphi(1_{F_1}) = 1_{F_2}$
3. $\varphi(x + y) = \varphi(x) + \varphi(y)$
4. $\varphi(xy) = \varphi(x)\varphi(y)$

则称 φ 是同态.

若 φ 是同态, 有以下事实:

1. $\varphi(-x) = -\varphi(x)$
2. $\varphi(x^{-1}) = \varphi(x)^{-1}$

Theorem 1.2.1 域同态是单射.

若 $\varphi: F_1 \rightarrow F_2$ 是域同态, 则 φ 是单射.

Proof. 假设 $\varphi(x_1) = \varphi(x_2), x = x_2 - x_1$, 则

$$\varphi(x) = \varphi(x_1) - \varphi(x_2) = 0$$

若 $x \neq 0$, 则存在 x^{-1} , 于是

$$\text{LHS} \Rightarrow \varphi(x) \cdot \varphi(x^{-1}) = 1$$

$$\text{RHS} \Rightarrow 0 \cdot \varphi(x^{-1}) = 0$$

而 $0 \neq 1$, 因此 $\forall x_1 \neq x_2, \varphi(x_1) \neq \varphi(x_2)$. ■

Definition 1.2.3 子域、域扩张.

若 F 是域, E 是 F 的子集, 若满足:

1. $0_F \in E$
2. $1_F \in E$
3. $\forall x, y \in E, x + y \in E, xy \in E$
4. $\forall x \in E, -x \in E$
5. $\forall x \in E \setminus \{0\}, x^{-1} \in E$

则称 E 为 F 的子域, F 为 E 的一个扩域. 记作 F/E .

Remark 1.2.1.

若存在同态 $\varphi: F_1 \rightarrow F_2$, 则 F_1 可以称为 F_2 的子域.

同态一定是单射.

Definition 1.2.4 域的同构.

若 $\varphi: F_1 \rightarrow F_2$ 是域的同态, 若 φ 是满射, 则称 φ 是同构.

特别的, 如果 $F_1 = F_2$, 则称 φ 是 F 的自同构.

Example 1.2.1 子域的例子.

1. \mathbb{R}/\mathbb{Q}
2. \mathbb{C}/\mathbb{R}
3. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$
4. $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$
5. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \cong \mathbb{Q}(\sqrt{2} + \sqrt{3})$
6. $\mathbb{F}_4/\mathbb{F}_2$

Definition 1.2.5 不动域.

设 $\sigma: F \rightarrow F$ 是 F 的自同构, 则 $E = \{x \in F \mid \sigma(x) = x\}$ 是一个子域, 叫做 σ 的不动域.

Example 1.2.2 自同构的例子.

设 $\bar{}: \mathbb{C} \rightarrow \mathbb{C}, x + yi \mapsto x - yi$, 可以验证满足:

1. $\overline{0} = 0$
2. $\overline{1} = 1$
3. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
4. $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$

则 $\bar{}$ 的不动域为 $z = \bar{z} \Rightarrow \mathbb{R}$.

Example 1.2.3 另一个例子.

定义 $\sigma: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2}), x + \sqrt{2}y \mapsto x - \sqrt{2}y$ 也是自同构.

Proof. 设 $z_1 = x_1 + \sqrt{2}y_1, z_2 = x_2 + \sqrt{2}y_2$, 容易验证他满足域同构的所有要求. 考虑他的不动域: $z = \sigma(z) \Rightarrow x + \sqrt{2}y = x - \sqrt{2}y \Rightarrow z \in \mathbb{Q}$. ■

Problem 1.2.1 二次域之间的关系.

$\mathbb{Q}(\sqrt{2})$ 和 $\mathbb{Q}(\sqrt{3})$ 有什么关系?

Solution. 没什么关系. 不存在同态 $\varphi: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{3})$. 若有同态 φ , 令 $a = \varphi(\sqrt{2}) = x + \sqrt{3}y$, 则 $a^2 = \varphi(\sqrt{2})^2 = \varphi(2) = \varphi(1) + \varphi(1) = 2$, 所以有 $(x + \sqrt{3}y)^2 = 2 \Rightarrow x, y \in \emptyset$. □

可见不同的二次域之间没啥关系.

Theorem 1.2.2 域与线性空间.

若 F/E , 则 F 是 E 的线性空间. 我们记 $[F : E] = \dim_E(F)$ 为 F 作为 E 的线性空间的维数, 称为 F/E 的次数.

Proof. 这很显然. ■

Proposition 1.2.1.

\mathbb{Q} 没有真子域.

Proof. 设 $E \subseteq \mathbb{Q}$, 且 $1 \in E, 0 \in E$. 若 E 为子域, 那么:

- 加法封闭: $\mathbb{N} \subseteq E$
- 加法有逆: $\mathbb{Z} \subseteq E$
- 乘法有逆: $\mathbb{Q} \subseteq E$

因此, $E = \mathbb{Q}$. ■

Proposition 1.2.2.

\mathbb{F}_q 没有真子域, 其中 $p \in \mathbb{P}$.

Proof. 设 \mathbb{F}_p/E , 于是有 $\#E, \#\mathbb{F}_p < \infty$, 因为 \mathbb{F}_p 可以看成是 E 上的线性空间, 考虑一组基和任意 $x \in \mathbb{F}_p$ 在这个基下的坐标, 可以得到 $\#\mathbb{F}_p = (\#E)^d$, 其中 $d = [F : E]$. 又 $p \in \mathbb{P}$, 我们得到 $d = 1, \#E = \#\mathbb{F}_p$, 因此 $E = \mathbb{F}_p$. ■

Definition 1.2.6 有限扩张.

若 $[F : E] < \infty$, 则称 F/E 是有限扩张.

Remark 1.2.2 E -代数.

若 F/E 是有限扩张, 且 $n = [F : E]$, 则可以取 F 的一组基 e_1, e_2, \dots, e_n , 不妨设 $e_1 = 1$, 则有

$$e_i \cdot e_j = \sum_{k=1}^n c_{ij}^k e_k \quad c_{ij}^k \in E$$

因此, $\forall x = \sum_{i=1}^n x_i e_i, y = \sum_{j=1}^n y_j e_j$, 我们有

$$xy = \sum_{k=1}^n \left(\sum_{i=1}^n \sum_{j=1}^n c_{ij}^k x_i y_j \right) e_k$$

此时, 称 F 为一个 E -代数.

Example 1.2.4.

1. $\mathbb{C} = \text{span}_{\mathbb{R}}(1, i)$

1.3 域的特征 (characteristic)

Definition 1.3.1 域的特征.

F 是域. 定义映射 $N : \mathbb{N} \rightarrow F, n \mapsto n_F$, 即

$$\begin{cases} N(0_{\mathbb{N}}) = 0_F \\ N(n+1) = N(n) + 1_F \end{cases}$$

若 N 为单射, 则称 F 的特征为 0, 记作 $\text{char } F = 0$.

若 N 不是单射, 则存在一个最小的 $p \in \mathbb{N}^*$ s.t. $N(p) = 0$, 此时 $\text{char } F = p$.

Remark 1.3.1.

对于上述的 $N : \mathbb{N} \rightarrow F$, 可以证明他满足:

1. $N(n+m) = N(n) + N(m)$
2. $N(n \cdot m) = N(n) \cdot N(m)$
3. $N(n-m) = N(n) - N(m)$

Proof. 先考虑第 1 条性质, \mathbb{N} 上定义的加法是 $+: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}, (x, y) \rightarrow x + y$, 即

$$\begin{cases} n + 0 \triangleq n \\ n + (m + 1) \triangleq (n + m) + 1 \end{cases}$$

我们把 $N(n+m) = N(n) + N(m)$ 看成是关于 m 的命题 $P(m)$, 利用数学归纳法:

1. $P(0) : N(n) = N(n) + N(0) = N(n)$

$$\begin{aligned} 2. \quad & P(n + (m + 1)) : N(n + (m + 1)) = N(n + m) + N(1), \\ & \text{LHS} = N((n + m) + 1) = N(n + m) + 1_F = N(n) + N(m) + 1_F \\ & \text{RHS} = N(n) + N(m) + 1_F \end{aligned}$$

因此对于加法是对的.

考虑 \mathbb{N} 上的乘法 $\cdot : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}, (x, y) \rightarrow x \cdot y$, 即

$$\begin{cases} n \cdot 0 \triangleq 0 \\ n \cdot (m + 1) \triangleq n \cdot m + n \end{cases}$$

同理利用数学归纳, 证明略. ■

Proposition 1.3.1 有限域的特征为素数.

若 $\text{char } F = p \neq 0$, 则 $p \in \mathbb{P}$.

Proof. 反证法. 若 $p = q \cdot r, 1 < q, r < p$, 则 $N(p) = N(q \cdot r) = N(q) \cdot N(r)$, 由于 $N(p) = 0$, 则 $N(q) = 0 \vee N(r) = 0$, 与 p 是特征的定义矛盾. 因此 $p \in \mathbb{P}$. ■

Proposition 1.3.2.

1. 若 $\text{char } F = 0$, 则 F/\mathbb{Q} .
2. 若 $\text{char } F = p > 0$, 则 F/\mathbb{F}_p .

Proof. 注意: $F/E \Rightarrow$ 存在同态 $\varphi : E \rightarrow F$.

1. 考虑构造映射 $N : \mathbb{N} \rightarrow F, n \mapsto n_F$, 不难发现是单射, 于是 $\mathbb{N} \subseteq F \Rightarrow \mathbb{Z} \subseteq F \Rightarrow \mathbb{Q} \subseteq F \Leftrightarrow F/\mathbb{Q}$.
2. 考虑构造映射 $N : \mathbb{F}_p \rightarrow F, n \mapsto n_F$, 发现他是同态, 因此 F/\mathbb{F}_p . ■

Proposition 1.3.3.

若 $\varphi : E \rightarrow F$ 是域同态, 则 $\text{char } E = \text{char } F$.

Proof. 若 $\text{char } E = 0$, 则 $E/\mathbb{Q} \Rightarrow F/\mathbb{Q} \Rightarrow \text{char } F = 0$. 若 $\text{char } E = p \in \mathbb{P}$, 注意到 $\varphi(n \cdot 1_E) = n \cdot 1_F, n \in \mathbb{N}$, 不难得到 $\varphi(p_E) = \varphi(0_E) = 0_F$, 因此 $\text{char } F \mid p$, 又因为 $p \in \mathbb{P}$ 得到 $\text{char } F = p = \text{char } E$. ■

Definition 1.3.2 Frobenius 自同构.

若 F 是域, 且 $\text{char } F = p > 0$, 则映射 $\sigma : F \rightarrow F, x \mapsto x^p$ 是一个自同构, 称他为 Frobenius 自同构.

Proof. 首先, $p \in \mathbb{P}$, 考虑二项式定理:

$$(x + y)^p = x^p + \binom{p}{1} x^{p-1} y + \binom{p}{2} x^{p-2} y^2 + \cdots + y^p$$

事实上, $p \in \mathbb{P}$ 时, $p \mid \binom{p}{k} = p^k/k!$, 这是因为 $1, 2, \dots, k < p$, 从而不能整除 p , 而组合数是一个整数, 因此分子上的因子 p 被留了下来. 所以 $\binom{p}{k} = 0_F$, 进而得到 $(x+y)^p = x^p + y^p$, 容易验证 σ 满足其余的自同构要求. ■

Example 1.3.1 Frobenius 自同构 的例子.

考虑 \mathbb{F}_4 , $\text{char } \mathbb{F}_4 = 2$ 上的 Frobenius 自同构 $\sigma: \mathbb{F}_4 \rightarrow \mathbb{F}_4, x \mapsto x^2$

\cdot	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

x	0	1	α	α^2
$\sigma(x)$	0	1	α^2	α

σ 的不动域为 \mathbb{F}_2 .

1.4 域的扩张

Definition 1.4.1 有限扩张.

若 E/F , 且 $[E:F] < \infty$, 则称 E 为 F 的有限扩张.

Definition 1.4.2 有限生成扩张 与 无限生成扩张.

设 E/F 是一个域扩张. 对于 E 的子集 S , 定义 $F(S)$ 为 E 中包含 $F \cup S$ 的最小子域, 称为由 S 在 F 上生成的子域.

- 若 S 是有限的, 且 $F(S) = E$, 则称 E 是 F 上的有限生成扩张.
- 若对于 E 的任何有限子集 S , 都有 $F(S) \neq E$, 则称 E 是 F 上的无限生成扩张.

注意: 有限扩张是从维数的观点, 有限生成扩张是从构造的观点.

Example 1.4.1.

- $F = \mathbb{Q}(\sqrt{2}), \dim_{\mathbb{Q}} F = 2$
- $F = \mathbb{Q}(\sqrt{2}, \sqrt{3}), \dim_{\mathbb{Q}} F = 4$
- $F = \mathbb{R}(x)$ 是实系数有理函数域, 是有限生成但不是有限. $\dim_{\mathbb{R}} F = \infty$.
- $E = \mathbb{Q}(\sqrt{p} \mid p \in \mathbb{P})$ 是无限生成.

Example 1.4.2.

- $E = \mathbb{Q}\left(2^{\frac{1}{2^k}} \mid k = 1, 2, \dots\right), F = \mathbb{Q}$ 是无限生成.

Proof. 设 $E_0 = F, E_1 = \mathbb{Q}(2^{\frac{1}{2}}), E_2 = \mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{4}}) = \mathbb{Q}(2^{\frac{1}{4}}), \dots$ 以此类推, 于是有 $F = E_0 \subseteq E_1 \subseteq E_2 \subseteq \dots \subseteq E$, 且 $E = \bigcup_{k=1}^{\infty} E_k$, 对于 E 的任意一个有限子集 $S = \{\alpha_1, \alpha_2, \dots, \alpha_n\} \Rightarrow \exists N$ s.t. $\alpha_1, \alpha_2, \dots, \alpha_n \in E_N$, 则 $F \cup S \subseteq E_N \Rightarrow F(S) \subseteq E_N \neq E$. ■

Theorem 1.4.1 有限扩张 \Rightarrow 有限生成扩张.

有限扩张一定是有限生成扩张, 但反之未必.

Proof. 设 E/F 是有限扩张, $[E:F] = n \Rightarrow E = \text{span}_F(e_1, e_2, \dots, e_n) \Rightarrow E = F(e_1, e_2, \dots, e_n), e_1, e_2, \dots, e_n \in E$ 是有限生成扩张.

有限生成扩张不是有限扩张的反例: $\mathbb{Q}(\pi), \mathbb{Q}(x)$. 注意: π 是超越数, 即 $p(\pi) \neq 0, p \in \mathbb{Q}[x], p \neq 0$. ■

Definition 1.4.3 代数扩张、超越扩张.

E/F , 若 $u \in E$ 满足 $f(u) = 0$, 其中 $f \in F[x], f \neq 0$, 则称 u 在 F 上代数, 称 u 为 F 上的代数元; 否则称 u 是超越元.

- 若 $\forall u \in E$, u 总是 F 上的代数元, 则称 E 是 F 上的代数扩张.
- 若 $\exists u \in E$ s.t. u 不是任何 $f \in F[x], f \neq 0$ 的根, 则称 E 是 F 上的超越扩张.

Example 1.4.3 代数扩张与超越扩张的例子.

1. $\mathbb{Q}(\sqrt{2})$ 是 \mathbb{Q} 上的代数扩张.
2. $\mathbb{Q}(\pi)$ 是 \mathbb{Q} 上的超越扩张.
3. $\mathbb{Q}(x)$ 是 \mathbb{Q} 上的超越扩张.

Lemma 1.4.1 代数元的逆.

若 α 是 F 上的代数元, 则 $-\alpha, \alpha^{-1}$ 也是 F 上的代数元.

Proof. 设 $\deg f = n$, 对于加法逆, 考虑替换为 $f(-x)$, 对于乘法逆, 考虑替换为 $x^n f(\frac{1}{x})$ 即可. ■

Lemma 1.4.2 代数元的和与积.

E/F , 若 α, β 是 F 上的代数元, 则 $\alpha + \beta, \alpha\beta$ 也是 F 上的代数元.

Proof. 设 $f(\alpha) = 0, g(\beta) = 0, f, g \in F[x], \deg f = n, \deg g = m$. 记 $R_x(A[x], B[x])$ 为多项式 A, B 关于 x 的结式, 也就是 $R_x(A[x], B[x]) = 0 \Leftrightarrow A, B$ 有公共根.

定义 $h(y) = R_x(f(x), g(y-x)) \in F[y]$, 我们断言 $h(\alpha + \beta) = 0$, 因为 $f(x), g(\alpha + \beta - x)$ 有公共根 $x = \alpha$. 同理, 定义 $g(y) = R_x(f(x), x^m g(\frac{y}{x}))$, 可证 $\alpha\beta$ 为代数元. ■

Theorem 1.4.2 有限扩张 \Rightarrow 代数扩张.

有限扩张一定是代数扩张, 但反之未必.

Proof. 设 $[E : F] = n$, 则 $\forall u \in E$, 要找 $f \in F[x], f \neq 0$ s.t. $f(u) = 0$. 考虑 $1, u, u^2, \dots, u^n \in E$, 由于 $\dim_F E = n$, 因此他们线性相关, 即 $\exists a_0, a_1, \dots, a_n \in F$ 不全为 0 s.t. $a_0 + a_1 u + \dots + a_n u^n = 0$, 取 $f(x) = a_0 + a_1 x + \dots + a_n x^n$ 即可.

反例: $\mathbb{Q}(2^{\frac{1}{2^k}} \mid k = 1, 2, \dots)$. ■

Remark 1.4.1.

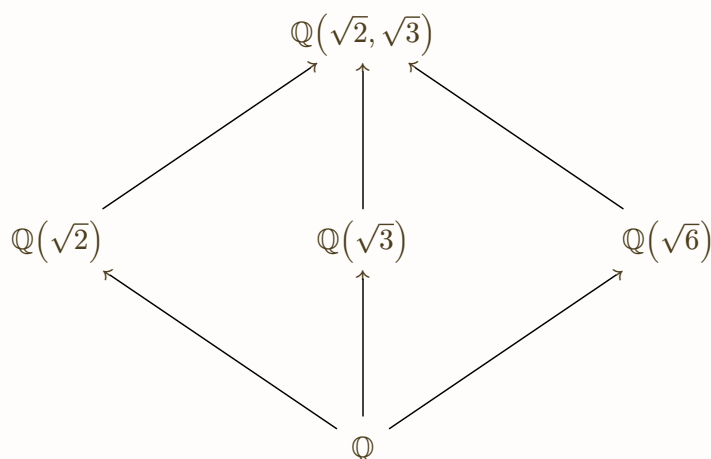
- 代数扩张 \nRightarrow 有限生成扩张. 反例: $\mathbb{Q}(2^{\frac{1}{2^k}} \mid k = 1, 2, \dots)$
- 有限生成扩张 \nRightarrow 代数扩张. 反例: $\mathbb{Q}(\pi), \mathbb{Q}(x)$.

Definition 1.4.4 中间域.

设 E/F 是一个域扩张, 若 E 的子域 K 满足 $F \subseteq K$, 则称 K 为扩张 E/F 的一个中间域.

Example 1.4.4 中间域的例子.

- $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$



- $\mathbb{F}_2 \subseteq \mathbb{F}_4 \subseteq \mathbb{F}_4(x)$

Lemma 1.4.3 维度公式.

设 E/F 是域扩张, K 是一个中间域, 则 $[E : F] = [E : K] \cdot [K : F]$.

Proof. $F \subseteq K \subseteq E$, 首先证明: $E/K, K/F$ 都是有限扩张.

先证明: $[E : F] < \infty$. 由于 $[E : F] < \infty$, E 可以看成是 F 上的有限维线性空间, 且 $\dim_F E = n$, 由于 $K \subseteq E$ 且 K 本身也是 F 上的线性空间, 则 $\dim_F K \leq \dim_F E < \infty$.

接着, 证明: $[E : K] < \infty$, 把 E 看成是 F 上的线性空间, 则取 E 的一组基 $B = \{e_1, e_2, \dots, e_n\}$, 于是 $\forall \gamma \in E$,

$$\gamma = \sum_{i=1}^n c_i e_i, c_i \in F \subseteq K$$

把 E 看成是 K 上的线性空间 $F \subseteq K, c_i \in K$, 说明 B 也张成了 K 上的线性空间 E , 因此 $\dim_K E \leq n < \infty$.

设 u_1, u_2, \dots, u_n 是 K/F 的基, v_1, v_2, \dots, v_m 是 E/K 的基, 下面构造 E/F 的基.

$\forall \beta \in E, \exists \alpha_1, \alpha_2, \dots, \alpha_m \in K$ s.t.

$$\beta = \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m$$

又 $\forall \alpha_i, \exists a_{i1}, a_{i2}, \dots, a_{in} \in F$ s.t.

$$\alpha_i = a_{i1} u_1 + a_{i2} u_2 + \dots + a_{in} u_n$$

因此, 我们有

$$\beta = \sum_{i=1}^m \left(\sum_{j=1}^n a_{ij} u_j \right) v_i = \sum_{i=1}^m \sum_{j=1}^n a_{ij} (u_j v_i)$$

于是, 我们得到 $E \subseteq \text{span}_F(u_j v_i \mid \substack{i=1,2,\dots,m \\ j=1,2,\dots,n})$, 下证 $u_j v_i$ 是线性无关的.

设

$$\sum_{i,j} c_{ij} (u_j v_i) = \sum_i \left(\sum_j c_{ij} u_j \right) v_i = 0$$

由于 v_1, v_2, \dots, v_m 线性无关, 得到 $\forall i, \sum_{j=1}^n c_{ij} u_j = 0$. 由于 u_1, u_2, \dots, u_n 线性无关, 得到 $\forall i, j, c_{ij} = 0$.

从而得到, $[E : F] = n \cdot m = [E : K] \cdot [K : F]$. ■

Corollary 1.4.1.

若 $[E : F] = p \in \mathbb{P}$, 则 E/F 没有非平凡的中间域.

Lemma 1.4.4 单代数扩张 \Rightarrow 有限扩张.

单代数扩张都是有限扩张, 且扩张的次数就是单代数元作为生成元的极小多项式的次数.

Proof. 设 $E = F(u)$, u 是 F 上的代数元. 下证 $[E : F] < \infty$.

设 $f(x) \in F[x], f \neq 0$ s.t. $f(u) = 0$ 且 f 是满足该条件的次数最小的首一多项式. 我们称 f 为 u 的极小多项式. 有如下事实:

1. f 是唯一的.

若 f_1, f_2 , 都是极小多项式, 则 $\deg f_1 = \deg f_2$, 则 $f_1 - f_2$ 次数更低, 且 $f(u) = 0 \Rightarrow f = 0$, 矛盾.

2. f 是不可约的.

若 $f = gh, \deg f = n$, 且 $1 \leq \deg g, \deg h \leq n-1$, 于是 $f(u) = 0 \Rightarrow g(u) = 0 \vee h(u) = 0$, 矛盾.

若 f 是 $F[x]$ 中的不可约多项式, 且 $\deg f = n$, 则 $\text{span}_F(1, u, \dots, u^{n-1}) = F(u) = E$ 一定是一个域, 且 $[E : F] = n$. 证明可以参考 Proposition 1.1.1. ■

Theorem 1.4.3 有限扩张的塔性质.

设 $E/K, K/F$ 是有限扩张, 则 E/F 是有限扩张.

Proof. 设 $[E : K] = m < \infty, [K : F] = n < \infty$, 则由 Lemma 1.4.3

$$[E : F] = [E : K] \cdot [K : F] = m \cdot n < \infty$$

得证. ■

Theorem 1.4.4 有限生成扩张的塔性质.

设 $E/K, K/F$ 是有限生成扩张, 则 E/F 是有限生成扩张.

Proof. 设 S, T 都是有限的, 且 $E = K(S), K = F(T)$, 则 $E = F(T)(S) = F(T \cup S)$, 而 $T \cup S$ 也是有限的, 因此 E/F 是有限生成扩张. ■

Theorem 1.4.5 有限生成的代数扩张 \Leftrightarrow 有限扩张.

有限生成的代数扩张一定是有限扩张. 具体来说, 以下等价:

- (1) E/F 是有限扩张
- (2) $E = F(u_1, u_2, \dots, u_n)$, 其中 u_1, u_2, \dots, u_n 都是 F 上的代数元, 此时 E/F 是代数扩张.

Proof. (1) \Rightarrow (2) 比较简单. 设 $[E : F] = n$, $u_1, u_2, \dots, u_n \in E$ 是 E/F 的基, 则 $E = F(u_1, u_2, \dots, u_n)$, 因为 E/F 代数, 所以 u_i 在 F 上代数.

(2) \Rightarrow (1) 设 u_1, u_2, \dots, u_n 为代数元, 证明: $E = F(u_1, u_2, \dots, u_n)/F$ 是有限扩张. 考虑从 F 开始, 每一次加入 u_i , 由于每一次都是单代数扩张, 因此每一次都相当于一次有限扩张, 由 Theorem 1.4.3 结果仍然是有限扩张, 因此 E/F 是有限扩张. ■

Theorem 1.4.6 代数扩张的塔性质.

设 $E/K, K/F$ 是代数扩张, 则 E/F 是代数扩张.

Proof. 设 $\alpha \in E, \exists f \in K[x], f \neq 0$, 且 $f(\alpha) = 0$. 设 $f(x) = x^n + a_1x^{n-1} + \dots + a_n, a_i \in K$. 设 $K' = F(a_1, a_2, \dots, a_n)$, 注意到 a_1, a_2, \dots, a_n 在 F 上代数, 则 $[K' : F] < \infty$.

注意 $K'(\alpha)/K'$ 是一个单代数扩张, 则 $[K'(\alpha) : K'] < \infty$. 由 Theorem 1.4.3 可知 $[K'(\alpha) : F] = [K'(\alpha) : K'] \cdot [K' : F] < \infty$ (其实到这里已经足够了). 因为 $F \subseteq K'$, 所以 $F(\alpha) \subseteq K'(\alpha) \Rightarrow [F(\alpha) : F] < \infty$, 因此 $F(\alpha)/F$ 是代数扩张, 即 α 是 F 上的代数元. ■

Chapter 2

环论、模论

Chapter 3

群论、群作用

Chapter 4

Galois 理论

