华东师范大学
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
2. 环、模 7
3. 群、群作用 8
4. Galois 理论 9

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: $+ : F \times F \to F, (x, y) \mapsto x + y$
- 乘法: $\cdot : F \times F \to F, (x, y) \mapsto x \cdot y$

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. $(x + y) \cdot z = x \cdot z + y \cdot z$

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.

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- $F = \mathbb{Q}\left(\sqrt{2}\right) = \{x + \sqrt{2}y \mid x, y \in \mathbb{Q}\}$
  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）
- $F = \mathbb{Q}\left(\sqrt[3]{2}\right)$

Proof $F = \mathbb{Q}\left(\sqrt[3]{2}\right)$. 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

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

■

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

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

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 $F' = \mathbb{Q}\big(\sqrt{2} + \sqrt{3}\big)$. 按照 Proposition 1.1.1 的思路， 我们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，我们只要说明： $F = F'$. 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 $F = \operatorname{span}\big(1, \sqrt{2}, \sqrt{3}, \sqrt{6}\big), F' = \operatorname{span}\big(1, \alpha, \alpha^2, \alpha^3, \alpha^4\big)$ ，而我们的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，因此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**. 我们后面会看到，其实在一定条件下，有限域扩张就是单扩张.

Example 1.1.3 有限域的例子.
- $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$
- $\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

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

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

另解. 构造一个映射 $T : \mathbb{F}_p \to \mathbb{F}_p, y \mapsto ky$，接下来，我们证明： $\ker T = \{0\}$. 如果 $T(y) = 0 \Leftrightarrow ky \equiv 0 \Leftrightarrow ky = pm \Leftrightarrow p \mid y \Leftrightarrow y = \overline{0}$，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. ■

Chapter 2
环、模

Chapter 3
群、群作用

Chapter 4
Galois 理论