華東師範大學
EAST CHINA NORMAL UNIVERSITY

抽象代数

笔记

© syqwq
East China Normal University

Contents

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

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.

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

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

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

■

Remark 1.1.3 $F[x]$ 与 $F(x)$.
注意区分 $F[x]$ 和 $F(x)$，前者是 $\left\{\sum_{i\geq 0} a_i x^i \,\middle|\, a_i \in F\right\}$，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 $F=\mathbb{Q}\big(\sqrt{2},\sqrt{3}\big)=\{x_1+x_2\sqrt{2}+x_3\sqrt{3}+x_4\sqrt{6}\mid x_i\in\mathbb{Q}\}$，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， 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 $F=\mathrm{span}\big(1,\sqrt{2},\sqrt{3},\sqrt{6}\big), F'=\mathrm{span}\big(1,\alpha,\alpha^2,\alpha^3,\alpha^4\big)$ ，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： $\mathbb{F}_p=\{\overline{0},\overline{1},\cdots,\overline{p-1}\}$ 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，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. ■

Remark 1.1.4.
若 $p\notin\mathbb{P}, m\in\mathbb{N}, m\geq 2, \mathbb{Z}_m=\left\{\overline{0},\overline{1},\cdots,\overline{m-1}\right\}$，则乘法逆不一定存在. 比如 $m=4, 2\cdot 2=0$，而 $\overline{2}\neq\overline{0}$，此时称 2 为零因子.

Example 1.1.5 函数域.
8. 设 F 是一个域. $F(x)=\left\{\frac{p(x)}{q(x)}\,\middle|\, p(x),q(x)\in F[x], q(x)\neq 0\right\}$
9. $K=\mathbb{C}\left(x,\sqrt{x^3+2}\right)=\mathbb{C}(x)(y)\sim\mathbb{Q}\left(\sqrt{2}\right)=\left\{R_1(x)+R_2(x)y\,\middle|\, R_1,R_2\in\mathbb{C}[x], y=\sqrt{x^3+2}\right\}$，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： $+:V\times V\to V$
- 数乘： $\cdot:F\times V\to V$

如果 $0_V\in N$，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. $\mathbb{Q}\left(\sqrt{2}\right)$ 是 $\mathbb{Q}$ 上的 2 维线性空间.
2. $\mathbb{Q}\left(\sqrt[3]{2}\right)$ 是 $\mathbb{Q}$ 上的 3 维空间.
3. $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ 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. 还不会证明 👀 💦 💦 💦 ■

Example 1.1.7 四元数.
10. 考虑四元数 $\mathbb{F}_4=\{x+y\alpha\,|\,x,y\in\mathbb{F}_2\}=\mathbb{F}_2(\alpha)$ 的结构.

Solution. $\mathbb{F}_2=\{\bar{0},\bar{1}\}$，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

$\cdot$	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

$\cdot$	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

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 $\varphi : V_1 \to V_2$ 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 $\varphi : F_1 \to F_2$ 满足:
1. $\varphi\left(0_{F_1}\right) = 0_{F_2}$
2. $\varphi\left(1_{F_1}\right) = 1_{F_2}$
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 $\varphi : F_1 \to F_2$ 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. $x \in E \setminus \{0\}, x^{-1} \in E$

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 $\varphi : F_1 \to F_2$，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 $\varphi : F_1 \to F_2$ 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. $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$
4. $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)/\mathbb{Q}\left(\sqrt{2}\right)$
5. $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) \cong \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$
6. $\mathbb{F}_4/\mathbb{F}_2$

Definition 1.2.5 不动域.
设 $\sigma : F \to F$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 $\overline{} : \mathbb{C} \to \mathbb{C}, x + yi \mapsto x - yi$，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 $\overline{}$ 的不动域为 $z = \overline{z} \Rightarrow \mathbb{R}$.

Example 1.2.3 另一个例子.
定义 $\sigma : \mathbb{Q}\left(\sqrt{2}\right) \to \mathbb{Q}\left(\sqrt{2}\right), x + \sqrt{2}y \mapsto x - \sqrt{2}$ 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.
$\mathbb{Q}\left(\sqrt{2}\right)$ 和 $\mathbb{Q}\left(\sqrt{3}\right)$ 有什么关系?

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

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 $e_1,e_2,\cdots,e_n$，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，$\forall x=\sum_{i=1}^{n}x_ie_i, y=\sum_{j=1}^{n}y_ie_j$，我们有

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

此时，称 F 为一个 $\boldsymbol{E}$**-代数**.

Example 1.2.4.
1. $\mathbb{C}=\mathrm{span}_{\mathbb{R}}(1,i)$

1.3 域的特征 (characteristic)

Definition 1.3.1 域的特征.
F 是域. 定义映射 $N:\mathbb{N}\to F, n\mapsto n_F$，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 $\mathrm{char}\,F=0$.
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 $\mathrm{char}\,F=p$.

Remark 1.3.1.
对于上述的 $N:\mathbb{N}\to F$，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 $+:\mathbb{N}\times\mathbb{N}\to\mathbb{N},(x,y)\to x+y$，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. $P(0):N(n)=N(n)+N(0)=N(n)$
2. $P(n+(m+1)):N(n+(m+1))=N(n+m)+N(1)$,
   $\mathrm{LHS}=N((n+m)+1)=N(n+m)+1_F=N(n)+N(m)+1_F$
   $\mathrm{RHS}=N(n)+N(m)+1_F$

因此对于加法是对的.

考虑 $\mathbb{N}$ 上的乘法 $\cdot : \mathbb{N}\times\mathbb{N}\to\mathbb{N}, (x,y)\to x\cdot y$，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 $\operatorname{char} F = p \neq 0$，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 $\operatorname{char} F = 0$，则 $F/\mathbb{Q}$.
2. 若 $\operatorname{char} F = p > 0$，则 $F/\mathbb{F}_p$.

Proof. 注意：$F/E \Rightarrow$ 存在同态 $\varphi : E\to F$.
1. 考虑构造映射 $N:\mathbb{N}\to F, n\mapsto n_F$，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 $N:\mathbb{F}_p\to F, n\mapsto n_F$，发现他是同态，因此 $F/\mathbb{F}_p$.

■

Proposition 1.3.3.
若 $\varphi : E\to F$ 是域同态，则 $\operatorname{char} E = \operatorname{char} F$.

Proof. 若 $\operatorname{char} E = 0$，则 $E/\mathbb{Q}\Rightarrow F/\mathbb{Q}\Rightarrow \operatorname{char} F = 0$. 若 $\operatorname{char} E = p\in\mathbb{P}$，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 $\operatorname{char} F \mid p$，又因为 $p\in\mathbb{P}$ 得到 $\operatorname{char} F = p = \operatorname{char} E$. ■

Definition 1.3.2 Frobenius 自同构.
若 F 是域，且 $\operatorname{char} F = p > 0$，则映射 $\sigma : F\to F, x\mapsto x^p$ 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：

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

事实上，$p\in\mathbb{P}$ 时，$p \mid \binom{p}{k} = p^{\underline{k}}/k!$，这是因为 $1,2,\cdots,k<p$，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 $\mathbb{F}_4, \operatorname{char}\mathbb{F}_4 = 2$ 上的 Frobenius 自同构 $\sigma : \mathbb{F}_4 \to \mathbb{F}_4, x \mapsto x^2$

$\cdot$	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 有限生成扩张.

设 F/E 是一个域扩张. 对于 F 的子集 S ， 定义 $E(S)$ 为 F 中包含 $E \cup S$ 的最小子域, 称为由 S 在 E 上生成的遇到. 若 S 是有限的, 且 $E(S) = F$, 则称 F 是 E 上的**有限生成扩张**.

Example 1.4.1.

1. $F = \mathbb{Q}\left(\sqrt{2}\right), \dim_{\mathbb{Q}} F = 2$
2. $F = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right), \dim_{\mathbb{Q}} F = 4$
3. $F = \mathbb{R}(x)$ 是实系数有理函数域, 是有限生成但不是有限. $\dim_{\mathbb{R}} F = \infty$.

Chapter 2
环论、模论

Chapter 3
群论、群作用

Chapter 4
Galois 理论