# 抽象代数笔记

副标题

Zhang Liang

2025 年 4 月 14 日

# 前言标题

前言内容

2025 年 4 月 14 日

# 目录

# 第一章　域

## 1.1　域的定义

### 1.1.1　域

**定义 1.1.1: 域**

设 $F$ 是一个集合，如果存在两个运算 $+: F\times F\to F$ 和 $\cdot: F\times F\to F$，分别称为加法和乘法，并且满足：

①（加法单位元存在）存在一个元素 $0_F\in F$，称为零元，$\forall x\in F, x+0_F=0_F+x=x$

②（加法逆存在）$\forall x\in F, \exists(-x)\in F, \text{s.t.} x+(-x)=(-x)+x=0_F$，$(-x)$ 称为 $x$ 的加法逆元

③（加法交换律）$\forall x,y\in F, x+y=y+x$

④（加法结合律）$\forall x,y,z\in F, (x+y)+z=x+(y+z)$

⑤（乘法单位元存在）存在一个元素 $1_F\in F, 1_F\neq 0_F$，称为一元，$\forall x\in F, x\cdot 1_F=1_F\cdot x=x$

⑥（乘法逆存在）$\forall x\in F-0_F, \exists x^{-1}\in F, \text{s.t. } x\cdot x^{-1}=x^{-1}\cdot x=1$，$x^{-1}$ 称为 $x$ 的乘法逆元

⑦（乘法交换律）$\forall x,y\in F, x\cdot y=y\cdot x$

⑧（乘法结合律）$\forall x,y,z\in F, (x\cdot y)\cdot z=x\cdot(y\cdot z)$

⑨（乘法分配律）$\forall x,y,z\in F, x\cdot(y+z)=x\cdot y+x\cdot z$

### 1.1.2　域的性质

1.

**命题 1.1.1.** 加法和乘法的单位元是唯一的。

**证明：** 先考虑加法的单位元。假设命题不成立，那么我们不妨假设 $0_1, 0_2$ 都是 $F$ 的零元,$0_1 \neq 0_2$

那么 $0_1 = 0_1 + 0_2 = 0_2$，于是有 $0_1 = 0_2$，与假设矛盾。于是加法的单位元唯一。

同理可证，乘法的单位元也是唯一的。 □

2. **命题 1.1.2.** $\forall a$，加法的逆 $-a$ 是唯一的。

   如果还有 $a \neq 0$，那么乘法的逆 $a^{-1}$ 也是唯一的。

   **证明：** 先考虑加法逆，不妨假设命题不成立，那么 $\exists b, c, a + b = 0, a + c = 0, b \neq c$

   于是，$b = b + 0 = b + (a + c) = (a + b) + c = 0 + c = c$，这与假设矛盾。于是加法逆唯一。

   同理可证，乘法逆也是唯一的。 □

3. **证明：** $a \cdot 0 = 0$ □

   **证明：** $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$

   $\Rightarrow a \cdot 0 + (-a \cdot a) = a \cdot 0 + a \cdot 0 + (-a \cdot 0)$

   $\Rightarrow 0 = a \cdot 0$ □

   立即有以下推论：

   **推论 1.1.1**

   $ab = 0 \Rightarrow a = 0 \vee b = 0$

   **证明：** 假设 $a \neq 0$，那么 $b = a^-1 \cdot 0 = 0$，命题得证 □

4. **命题 1.1.3.** $-a = (-1) \cdot a$

   **证明：** $a + (-a) = 0 = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a$

   $\Rightarrow (-a) + a + (-a) = (-a) + a + (-1) \cdot a$

   $\Rightarrow -a = (-1) \cdot a$ □

   随后我们即可得出以下推论

   **推论 1.1.2**

   $(-1) \cdot (-x) = x$

**证明:** 我们只需证明：$(-1)(-1)=1$

因为 $(-1)(-1)+(-1)\cdot 1=0$

$\Rightarrow (-1)(-1)+(-1)=0 \Rightarrow (-1)(-1)=1$

那么，$(-1)(-x)=(-1)(-1)\cdot x=1\cdot x=x$ □

**推论 1.1.3**

$(-x)(-x)=x\cdot x$

**证明:** 运用前面的推论中的结果，$(-x)(-x)=x\cdot(-1)(-1)\cdot x=x\cdot 1\cdot x=x\cdot x$ □

## 1.2 域的同态

**定义 1.2.1: 域的同态**

$F_1,F_2$ 是两个域，如果存在一个映射 $\varphi: F_1\to F_2$，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 $\varphi(x\cdot y)=\varphi(x)\cdot\varphi(y)$

值得注意的是，与我们之前了解到的线性空间同构不同，域的同态完全没有对映射的满射性、单射性作任何限制。但是，

以下定理证明，两个域如果同态，那么同态映射是一个单射

**定理 1.2.1: 域同态的单射性**

若 $\varphi: F_1\to F_2$ 是 $F_1$ 到 $F_2$ 的同态，那么 $\varphi$ 是单射

**证明:** 不妨假设命题不成立。于是，$\exists x_1\neq x_2 \text{s.t. } \varphi(x_1)=\varphi(x_2)$

那么有：$\varphi(x_1-x_2)=\varphi(x_1)-\varphi(x_2)=0_{F_2}$

因为我们已经假设了 $x_1\neq x_2$，于是 $(x_1-x_2)^{-1}$ 存在。将上式乘以 $\varphi\left((x_1-x_2)^{-1}\right)$ 得：

$1_{F_2}=\varphi(1_{F_1})\varphi\left((x_1-x_2)^{-1}(x_1-x_2)\right)=\varphi\left((x_1-x_2)^{-1}\right)\varphi\left((x_1-x_2)\right)=0_{F_1}$

与 $0_{F_2}\neq 1_{F_2}$ 矛盾，于是命题得证。 □

在证明这一点后，我们可以类似地引入域的同构：

**定义 1.2.2: 域的同构**

设 $\varphi : F_1 \to F_2$ 是 $F_1$ 到 $F_2$ 的同态

如果 $\varphi$ 还是个满射，那么我们称 $\varphi$ 是一个同构；

特别地，如果有 $F_1 = F_2$，我们称 $\varphi$ 是一个自同构。

并且引入自同构的不动域的概念：

**定义 1.2.3: 自同构域的不动域**

设 $\sigma : F \to F$ 是 $F$ 的自同构，那么我们称集合

$\{x \in F | \sigma(x) = x\}$ 为 $F$ 的不动域

“不动域”这一名称是合理的，因为利用域同构的定义容易证明不动域是一个域，而且是 $F$ 的一个子域。

## 1.3 域的特征

### 1.3.1 域的特征的定义

**定义 1.3.1: 域的特征**

设 $F$ 是一个域，定义以下映射 $N : \mathbb{N} \ni n \mapsto n_F \in F$，满足：

$N(0) = 0_F, N(n+1) = n_F + 1_F$

那么，如果 $N$ 是一个单射，我们称 $F$ 的特征为 0，记作 $\mathrm{Char}F = 0$；

否则，我们将满足 $N(p) = 0_F, p > 0$ 的最小正整数称为 $F$ 的特征，记作 $\mathrm{Char}F = p$。

我们首先需要证明的是，任何一个域都是具有特征的，因为对于定义中的第二种情形，我们并不知道这样的 $p$ 是否一定存在。

**定理 1.3.1: 域特征的存在性**

任何域 $F$ 的特征 $\mathrm{Char}F$ 均存在

**证明：** 我们只需要证明第二种情形。

容易证明，$N(m+n) = N(m) + N(n)$。（仿照 Peano 公理下证明加法性质的方式即可）

于是，因为 $N$ 不是单射，于是一定有 $a, b \in \mathbb{N}, a > b, N(a) = N(b)$

于是有 $N(a-b)=N(a)-N(b)=0_F$。

那么 $\{m|N(m)=0_F\}\neq\emptyset$，因此这样的最小整数 Char$F$ 存在 □

接下来考虑几个性质

### 1.3.2 域的特征的性质

**命题 1.3.1.** *设 $F$ 是一个域，那么或者 $Char\ F=0$，或者 $Char\ F=p$ 是素数*

**证明：** 我们只需要证明当 Char $F=p>0$ 时，$p$ 是素数

不妨假设命题不成立，那么一定有 $1<q<p, 1<r<p, p=qr$

容易证明，$N(qr)=N(q)N(r)$。（仿照 Peano 公理下证明乘法性质的方式即可）

但是，因为 $N(qr)=0$，于是 $N(q)=0\vee N(r)=0$，这与定义中 $p$ 是使 $N(x)=0$ 成立的最小正整数矛盾。

于是命题得证。 □

**定理 1.3.2: 同态域的特征相等**

设 $\varphi:E\to F$ 是域 $E$ 到域 $F$ 的同态

那么有：Char $E=$ Char $F$

**证明：** 我们不妨假设结论不成立。

首先我们证明，不可能 Char $E=0$, Char $F=p, p$ 为素数。

此时，$\varphi\left(N_E(p)\right)=N_F(p)=0_F$，此处 $N_E, N_F$ 分别是 $N$ 在对应 $E, F$ 的情况下的映射

那么按照同态的定义，一定有 $N_E(p)=0_E$，但是这与 Char E $=0$ 矛盾。

那么只需要考虑当 Char $E=p$, Char $F=q, p, q$ 为素数,$p\neq q$

那么，有 $\varphi\left(N_E(q)\right)=N_F(q)=0_F$

那么按照同态的定义，一定有 $N_E(q)=0_E$，这说明 $p\mid q$，这与 $q$ 是素数矛盾。

所以假设不成立，命题得证。 □

## 1.4 域的扩张

### 1.4.1 域的扩张的定义

**定义 1.4.1: 子域**

设 $E, F$ 是两个域，$E \subseteq F$

如果 $0_F, 1_F \in E$，并且 $F$ 中的加法和乘法对 $E$ 形成一个域，

那么我们称 $E$ 是 $F$ 的一个子域，并称 $F$ 是 $E$ 的一个域扩张，

记作 $F \backslash E$

如果 $E \backslash F$，$F \cong G$，那么我们也称：在同构意义下 $E \backslash G$。

此后我们所说的子域，默认指的是同构意义下的子域。

借助域的扩张的概念，我们可以证明一些比较简单的结论

**命题 1.4.1.** 域 $F$ 如果有 $Char\ F = 0$，那么 $\mathbb{Q}$ 是它的子域；如果有 $Char\ F = p$，那么 $F_p$ 是它的子域

**证明:** 如果 $\mathrm{Char}\ F = 0$，那么 $F$ 是无限集。因为 $0_F, 1_F \in F$，那么一定也有 $n_F \in F, n \in \mathbb{N}$。

那么，$-n_F \in F$；进一步地，一定有 $a \cdot b^{-1} \in F, a, b \in \{\pm n_F\}$。

那么，一定有 $F \backslash \mathbb{Q}$。

如果 $\mathrm{Char}\ F = p$，$p$ 是素数。那么，$\{0_F, \cdots, (p-1)_F\}$ 由映射 $N$ 的性质一定是一个域。

那么，一定有 $F \backslash F_p$ □

### 1.4.2 有限扩张

从域的定义容易看出，$F$ 也可以视为 $E$ 上的一个线性空间。

**定义 1.4.2: 域的扩张次数**

如果 $F \backslash E$，那么我们记 $[F : E] := dim_E F$，并称 $F$ 是 $E$ 由 $[F : E]$ 次扩张得到的。

如果 $[F : E]$ 有限，我们称 $F$ 是 $E$ 的有限扩张，反之称它是无限扩张。

有限扩张的概念可以让我们立即得出以下结论

**定理 1.4.1: 域的元素个数仅可能无限或者是 $p^k$**

一个域的元素个数，或者是无限，或者是 $p^k$，其中 $p$ 是一个素数，$k$ 是正整数

**证明:** 事实上，我们只需要证明有限域 $F$ 的个数只可能是 $p^k$

设 $\text{Char } F = p$，那么一定有 $F \backslash F_p$

因为 $F$ 是有限域，所以一定有 $[F : F_p] = d$ 有限，那么此时 $|F| = p^d$。因为 $p$ 一定为素数，因此命题得证。 □

### 1.4.3 有限生成扩张

**定义 1.4.3: 域的生成扩张**

设 $E, F$ 是两个域，$E \backslash F$，集合 $S \subseteq E$

那么我们定义包含 $F, S$ 中全部元素的最小域，即

$$F(S) := \bigcap_{(F \cup S) \subseteq K, E \backslash K} K$$

称为在 $F$ 上由 $S$ 生成的 $E$ 的子域

**定义 1.4.4: 有限生成与无限生成**

设 $E, F$ 是两个域，$E \backslash F$

如果存在一个集合 $S \subseteq E, F(S) = E$，那么我们称 $E$ 是 $F$ 的有限生成扩张；

如果对于任意的有限集 $S \subseteq E, F(S) \neq E$，那么我们称 $E$ 是 $F$ 的无限生成扩张

显然有以下性质

**命题 1.4.2.** 有限扩张都是有限生成扩张

**证明:** 设 $E \backslash F, [E : F] = n < +\infty$。

那么 $E$ 是 $F$ 上的一个线性空间，我们取它的一组基 $\{\alpha_1, \cdots, \alpha_n\}$

于是 $E = \text{span}_F(\alpha_1, \cdots, \alpha_n)$。由线性生成的性质，那么有

$E = F(\alpha_1, \cdots, \alpha_n)$。于是命题得证。 □

值得注意的是，这个命题如果反过来则不成立，比如说：

**例 1.4.1.** $\mathbb{Q}(e)$ 是 $\mathbb{Q}$ 的有限生成扩张，但是不是 $\mathbb{Q}$ 的有限扩张

**证明:** 不妨假设命题不成立，那么有 $[\mathbb{Q}(e) : \mathbb{Q}] = n < +\infty$

那么，因为线性空间中，数量多于维数的一组向量一定线性相关，那么 $1, e, \cdots, e^n$ 线性相关

$\Rightarrow \exists a_0, \cdots, a_n \in \mathbb{Q}, a_0 + a_1 e + \cdots + a_n e^n = 0$

但是，这与 $e$ 是超越数矛盾。于是命题得证 □

### 1.4.4 代数扩张

我们首先提出代数元的概念

**定义 1.4.5: 代数元**

设 $E \backslash F$ 是一个域扩张，$u \in E$ 如果满足：

$\exists p(x) \in F[x], p(u) = 0$，那么我们称 $u$ 是 $F$ 上的代数元

我们如下定义代数扩张

**定义 1.4.6: 代数扩张和超越扩张**

设 $E \backslash F$ 是一个域扩张

如果 $\forall u \in E$，$u$ 是 $F$ 的代数元，那么我们称 $E$ 是 $F$ 的代数扩张；

反之，如果 $\exists u \in E$，$u$ 不是 $F$ 的代数元，那么我们称 $E$ 是 $F$ 的超越扩张。

接下来我们考虑代数、有限、有限生成三种扩张之间的联系

1. 有限扩张都是代数扩张

**定理 1.4.2: 有限扩张都是代数扩张**

任何有限扩张都是代数扩张

**证明:** 设 $E, F$ 是两个域，$[E : F] = n < +\infty$

取 $\forall \alpha \in E$，考虑集合 $\{1, \alpha, \cdots, \alpha^n\}$

因为这个集合有 $n+1 > [E : F]$ 个元素，因此它一定线性相关；这代表着

$\exists a_0, \cdots, a_n$ 不全为 $0, a_0 + a_1\alpha + \cdots a_n\alpha^n = 0$

因此 $\alpha$ 是多项式 $\sum\limits_{k=0}^{n} a_k x^k \in F[x]$ 的一个根

所以 $\alpha$ 是 $F$ 的代数元，于是命题得证。 □

2. 有限扩张的组合和拆分也是有限的

**命题 1.4.3.** 设 $E,K,F$ 是三个域，$E\backslash K, K\backslash F$，并且 $E\backslash F$ 是有限扩张。

那么，$E\backslash K, K\backslash F$ 是有限扩张，并且有 $[E:F]=[E:K]\cdot[K:F]$

**证明：** 我们首先证明 $E\backslash K, K\backslash F$ 是有限扩张。

显然，$K\backslash F$ 一定是有限扩张，因为 $K$ 是 $E$ 在 $F$ 上的线性子空间，而 $[E:F]$ 有限。

我们不妨假设 $E\backslash K$ 不是有限的，那么一定可以取一组无限基 $\{e_\alpha|\alpha\in A\}$

考虑 $F$ 上的线性组合 $\sum\limits_{i=1}^{\infty} a_i e_{\alpha_i}, \alpha_i\in A$

我们可以断言：这个线性组合在 $\exists a_i\neq 0$ 时不为零，因为 $F\subseteq K$，所以这个线性组合也可以视为 $K$ 上的，

而线性无关向量组的子向量组也是线性无关的；

但是，这是不可能的：因为我们知道 $[K:F]$ 有限，一个无限集不可能线性无关。所以 $[E:K]$ 一定有限。

接下来证明 $[E:F]=[E:K]\cdot[K:F]$

假设 $[E:K]=m, [K:F]=n$，取 $E$ 在 $K$ 上的一组基 $\{\alpha_1,\cdots,\alpha_m\}$，$K$ 在 $F$ 上的一组基 $\{\beta_1,\cdots,\beta_n\}$

$\forall \eta\in E, \exists a_1,\cdots,a_m, \eta=a_1\alpha_1+\cdots+a_m\alpha_m$

对系数作展开，有：

$$\exists b_{ij}, \eta=(b_{11}\beta_1+\cdots+b_{1n}\beta_n)\alpha_1+\cdots+(b_{m1}\beta_1+\cdots+b_{mn}\beta_n)\alpha_m$$
$$=\sum_{i=1,j=1}^{i=m,j=n} b_{ij}\alpha_i\beta_j$$
$$=\sum_{i=1}^{m}\left(\sum_{j=1}^{n} b_{ij}\beta_j\right)\alpha_i$$

令 $\eta=0$，因为 $\{\alpha_1,\cdots,\alpha_m\}$ 线性无关，一定有 $\sum\limits_{j=1}^{n} b_{ij}\beta_j=0$

但是，$\{\beta_1,\cdots,\beta_n\}$ 线性无关，所以一定有 $b_{ij}=0$。所以 $\{\alpha_i\beta_j\}$ 是 $E$ 在 $F$ 上的一组基

所以 $[E:F]=mn=[E:K]\cdot[K:F]$，命题得证 □

利用这个命题可以得出以下推论

**推论 1.4.3: 素数次扩张不存在平凡子域**

若 $E\backslash F$ 是一个有限扩张，$[E:F]=p$ 为素数

那么 $E,F$ 没有非平凡的中间域，即 $E\backslash K\backslash F \Leftrightarrow E=K\vee F=K$

**证明：** 这是显然的，因为素数的因子仅有 1 和自身；而 $[K:F]=1$ 当且仅当 $K,F$ 在同构意义下相等。 □

**推论 1.4.4: 单代数扩张一定是有限扩张**

设 $E, F$ 是两个域，$E = F(u), u$ 是 $F$ 的代数元

那么 $E = F(u)$ 是一个有限扩张，并且 $[E : F] = \deg f(x)$，其中 $f(x)$ 是 $u$ 的极小多项

**证明:** 取 $u$ 的极小多项式 $f(x) \in F[x]$，设 $f(x) = \sum_{k=0}^{n} a_k x^k, a_n = 1$

因为 $f(u) = 0$，所以有 $x^n = -\sum_{i=0}^{n-1} a_k x^k$

于是，任意的 $\alpha^k$ 均可以由 $1, \alpha, \cdot, \alpha^{n-1}$ 线性表出，这表示

$E = F(u) = \{a_0 + \cdots + a_{n-1}u^{n-1}\}$

于是 $E$ 中任意一个元素可由 $\{1, \cdots, u^{n-1}\}$ 线性表出。但是 $u$ 的极小多项式的次数为 $n$，所以这个集合一定线性无关，也就是它是 $E$ 的基

所以 $[E : F] = n < +\infty$ □

3. 有限生成的代数扩张是有限扩张

**定理 1.4.5: 有限生成的代数扩张是有限扩张**

$E \backslash F$ 是有限扩张 $\Leftrightarrow E = F(u_1, \cdots, u_n)$ 其中 $u_1, \cdots, u_n$ 是 $F$ 的代数元

**证明:** 首先证明充分性。

取 $E$ 在 $F$ 上的一组基 $\{u_1, \cdots, u_n\}$

我们说，一定有 $E = F(u_1, \cdots, u_n)$，因为:

$E = \mathrm{span}_F(u_1, \cdots, u_n) \subseteq F(u_1, \cdots, u_n)$

但是，同时也有 $F(u_1, \cdots, u_n) \subseteq E$，因为 $E$ 是一个域，而 $u_1, \cdots, u_n \in E$

所以只需要证明 $u_1, \cdots, u_n$ 是 $F$ 的代数元。但是，有限扩张都是代数扩张，按照代数扩张的定义可知这是成立的。

接下来证明必要性。这是更加显然的，因为我们已经证明了单代数扩张有限，那么有

$[F(u_1, \cdots, u_n) : F] = [F(u_1, \cdots, u_n) : F(u_1, \cdots, u_{n-1})] \cdots [F(u_1) : F] < +\infty$ □

4. 代数扩张的复合也是代数扩张

**定理 1.4.6: 代数扩张的复合也是代数扩张**

设 $E\backslash K\backslash F$，

如果 $E\backslash K, K\backslash F$ 都是代数扩张，那么 $E\backslash F$ 也是代数扩张

**证明：** 取 $\forall\alpha\in E$

因为 $E\backslash K$ 是代数扩张，所以 $\exists f(x)\in K[x], f(\alpha)=0$

设 $f(x)=a_0+\cdots+a_nx^n$，取 $R=F(a_0,\cdots,a_n)$

因为 $a_0,\cdots,a_n\in K$，而 $K\backslash F$ 是代数扩张，所以 $a_0,\cdots,a_n$ 是 $F$ 的代数元

那么，按照前面的定理，一定有 $[R:F]<+\infty$

接下来考虑 $R(\alpha)$，因为 $a_0,\cdots,a_n\in R$，所以 $\alpha$ 是 $R$ 的代数元，那么就有 $[R(\alpha):R]<\infty$

所以 $[R(\alpha):F]=[R(\alpha):R]\cdot[R:F]<+\infty$

但是，$R\backslash F$，所以一定也有 $[F(\alpha):F]<+\infty$，又因为有限扩张都是代数扩张，所以 $\alpha$ 是 $F$ 的代数元，于是命题得证。 □

三种扩张的关系可以用以下图示概括

$$\begin{tikzcd}
\text{Infinite extension} \arrow[r, shift left, "is"] \arrow[d, shift left, "is"] & \text{Algebraic extension} \arrow[l, shift left, "if infinite-generate"] \\
\text{Infinite-generate extension} \arrow[u, shift left, "if Algebraic"] &
\end{tikzcd}$$

## 1.5 代数闭包

**定义 1.5.1: 相对代数闭包**

设 $E\backslash F$ 是一个域扩张，那么我们称

$K=\{\alpha\in E|\alpha\text{是}F\text{上的代数元}\}$ 是 $F$ 在 $E$ 上的相对代数闭包

**定义 1.5.2: 代数闭域**

如果域 $K$ 没有真代数扩张，即 $K$ 的任意一个代数扩张 $K'\backslash K$ 都有 $K'=K$

那么我们称 $K$ 是一个代数闭域

**定义 1.5.3: 绝对代数闭包**

如果 $\overline{F}\backslash F$ 是一个代数扩张，且 $\overline{F}$ 是一个代数闭域

那么我们称 $\overline{F}$ 是 $F$ 的绝对代数闭包，记作 $\overline{F}$

我们早就发现，似乎代数扩张并不能无限的扩张，而是会有一个终点，这个终点其实就是代数闭包，以下命题指出了这个事实。

**命题 1.5.1.** 如果 $K$ 是 $F$ 在 $E$ 上的代数闭包，
那么如果 $E\backslash K'\backslash K$ 且 $K'\backslash K$ 是代数扩张，那么 $K'=K$

**证明：** 因为 $K\backslash F, K'\backslash K$ 都是代数扩张，所以 $K'\backslash F$ 也是代数扩张
因为代数闭包即是全部可以通过代数扩张得到的元素的集合，所以必定有 $K'=K$ □

显然绝对代数闭包的定义和以下等价

**命题 1.5.2.** 如果 $K$ 是 $F$ 在 $E$ 上的相对代数闭包，且 $E$ 是一个代数闭域，那么 $K$ 是 $F$ 的绝对代数闭包

**证明：** 只需证明 $K$ 是一个代数闭域
没法证，得用商环………… □

**定理 1.5.1: 绝对代数闭包的存在性**

任意一个域 $F$ 的绝对代数闭包 $\overline{F}$ 都存在，并且在同构意义下唯一

**证明：** 要用 Zorn 引理…… □

# 第二章　环、模

## 2.1　环的定义

### 2.1.1　环的定义

**定义 2.1.1**

$R$ 是一个集合，如果存在两个运算 $+: R\times R\to R$ 和 $\cdot: R\times R\to R$

分别称为加法和乘法，满足下列条件：

①（加法单位元存在）存在一个元素 $0_R\in R$，称为加法单位元，使得对于任意 $x\in R$，有 $x+0_R=0_R+x=x$。

②（加法交换律）$\forall x,y\in R, x+y=y+x$

③（加法结合律）$\forall x,y,z\in R,(x+y)+z=x+(y+z)$

④（加法逆存在）$\forall x\in R,\exists -x\in R$，称为加法逆，使得 $x+(-x)=0_R$

⑤（乘法结合律）$\forall x,y,z\in R,(x\cdot y)\cdot z=x\cdot(y\cdot z)$

⑥（左分配律）$\forall x,y,z\in R, x\cdot(y+z)=x\cdot y+x\cdot z$

（右分配律）$\forall x,y,z\in R,(y+z)\cdot x=y\cdot x+z\cdot x$

那么我们称 $(R,+,\cdot)$ 是一个环，简称为环 $R$。

相比域的定义，环的定义仅涉及 6 条性质，去除了单位元存在、可交换、可逆三条性质。在研究环时，我们有时也会考虑存在单位元和可交换的环，因此有以下定义：

**定义 2.1.2: 交换环、幺环**

如果环 $R$ 满足：$\forall x,y\in R, x\cdot y=y\cdot x$，那么我们称 $R$ 是一个交换环；

如果环 $R$ 满足：$\exists 1_R\in R,\forall x\in R, 1_R\cdot x=x\cdot 1_R=x$，称为乘法单位元，

### 2.1.2 环的性质

### 2.1.3 整环

**定义 2.1.3: 零因子**

设 $R$ 是一个环，如果 $\exists x, y \in R, x, y \neq 0_R$，使得 $x \cdot y = 0_R$，那么我们称 $x, y$ 是 $R$ 的零因子。

**定义 2.1.4: 整环**

如果环 $R$ 是一个交换幺环，并且不包含零因子，那么我们称 $R$ 是一个整环。

**定理 2.1.1: 循环的整环必有素零因子**

设 $R$ 是一个整环，

我们定义：$N : \mathbb{Z} \ni n \mapsto n_R \in R$，满足 $(n+1)_F = n_F + 1_F$

如果 $\exists a \in R, a \neq 0, \exists n \in \mathbb{N}_+, n_F a = 0_R$

那么存在素数 $p$，$\forall b \in R, p_R b = 0_R$

**证明:** 取 $\forall b \in R,$

$0_R = 0_R \cdot b = (n_R a)b = a(n_R b)$

因为 $a \neq 0$，而 $R$ 是整环，所以一定有 $n_R b = 0$，因此，$\{k \in \mathbb{N}_+ | k_R b = 0\}$ 不是空集。

取 $p$ 为使 $p_R b = 0$ 的最小正整数。如果 $p$ 是素数，命题成立；

如果 $p$ 不是素数，那么只需要对 $p$ 作唯一分解，那么有 $\left(\prod_{i=1}^{q} p_{i_R}\right) b = 0$

那么，一定存在一个 $p_{i_R} b = 0$，此时命题也是成立的。 □

### 2.1.4 子环

我们也类似地提出后续我们会提及的子环的概念。

**定义 2.1.5: 子环**

设 $R$ 是一个环，集合 $S \subseteq R$，

如果 $S$ 对 $R$ 上的加法和乘法也构成一个环，那么我们称 $S$ 是 $R$ 的子环。

# 2.2 环的同态

我们类似于域的同态，定义出环的同态。

## 2.2.1 定义

**定义 2.2.1: 环同态**

设 $R, S$ 是两个环，如果映射 $\varphi : R \to S$ 满足：

$\forall a, b \in R, \varphi(a+b) = \varphi(a) + \varphi(b), \varphi(ab) = \varphi(a)\varphi(b)$

并且如果 $R, S$ 均是幺环，$\varphi(1_R) = 1_S$

那么我们称 $\varphi$ 是一个 $R$ 到 $S$ 的环同态。

**定义 2.2.2: 单同态、满同态、同构**

假设有环同态 $\psi : R \to S$

如果 $\psi$ 是单射，那么称它是一个单同态；

如果 $\psi$ 是满射，那么称它是一个满同态；

如果 $\psi$ 是双射，称它是一个同构，记作 $R \cong S$；

同构是最严格的同态，表示两个环在结构上是完全相同的，有以下显而易见的事实：

**命题 2.2.1.** 如果 $\psi : R \to S$ 是一个环同构，那么 $\psi^{-1} : S \to R$ 也是一个环同构

**证明：** $\psi\left(\psi^{-1}(a) + \psi^{-1}(b)\right) = \psi\left(\psi(a)\right) + \psi\left(\psi(b)\right) = a + b$

因为 $\psi$ 是双射，所以有 $\psi^{-1}(a) + \psi^{-1}(b) = \psi(a+b)$

同理，$\psi\left(\psi^{-1}(a)\psi^{-1}(b)\right) = \psi\left(\psi(a)\right)\psi\left(\psi(b)\right) = ab$

$\Rightarrow \psi^{-1}(a)\psi^{-1}(b) = \psi(ab)$，于是命题得证 □

## 2.2.2 同态的性质

1. 同态一定将零元映射到零元

   **命题 2.2.2.** 设 $\varphi : R \to S$ 是一个环同态，那么 $\varphi(0_R) = 0_S$

   **证明：** $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$

   $\Rightarrow -\varphi(0_R) + \varphi(0_R) = -\varphi(0_R) + \varphi(0_R) + \varphi(0_R)$

   $\Rightarrow \varphi(0_R) = 0_S$ □

2. 同态把逆元映射到逆元

**命题 2.2.3.** 设 $\varphi: R \to S$ 是一个环同态，那么 $\varphi(-a) = -\varphi(a)$

**证明：** 注意到，$0_S = \varphi(0_R) = \varphi(a + (-a)) = \varphi(a) + \varphi(-a) \Rightarrow \varphi(-a) = -\varphi(a)$ □

### 2.2.3 同态的核、像

**定义 2.2.3: 环同态的核、像**

设 $\psi: R \to S$ 是一个环同态，我们定义：

$\ker\psi = \{a \in R | \psi(a) = 0_S\}$，称为 $\psi$ 的核

$\mathrm{Im}\ \psi = \{\psi(a) | a \in R\}$，称为 $\psi$ 的像

与域的同态不同，环的同态的核并不是平凡的，因为域同态未必是单射。因此，我们需要研究环同态的核与像。

但是，受限于目前的知识，我们暂时无法证明核与像的一些进阶性质，我们仅仅证明一些简单的性质。

**命题 2.2.4.** 设 $\psi: R \to S$ 是一个环同态，那么 $\ker\psi$ 是一个 $R$ 的子环

**证明：** 取 $\forall a, b \in \ker\psi$，那么有 $\psi(a) = \psi(b) = 0$

我们注意到：$\psi(0_R) = 0_S \Rightarrow 0_R \in \ker\psi, a + 0_R = a$

$\psi(a + (-a)) = 0_S \Rightarrow \psi(a) + \psi(-a) = 0_S \Rightarrow \psi(-a) = 0_S \Rightarrow -a \in \ker\psi, a + (-a) = 0_R$

加法的交换律、结合律，乘法的结合律，左、右分配律是显然成立的。 □

**命题 2.2.5.** 设 $\psi: R \to S$ 是一个环同态，那么 $Im\ \psi$ 是一个 $S$ 的子环

**证明：** 取 $\forall a, b \in \mathrm{Im}\ \psi$，那么有 $\exists x, y \in R, \psi(x) = a, \psi(y) = b$

我们注意到：$\psi(0_R) = 0_S \Rightarrow 0_S \in \mathrm{Im}\ \psi, \psi(x) + \psi(0_R) = \psi(x)$

$\psi(x) + \psi(-x) = \psi(x + (-x)) = \psi(0_R) = 0_S \Rightarrow \psi(-x) = -\psi(x) = -a \in \mathrm{Im}\ \psi, a + (-a) = 0_S$

加法的交换律、结合律，乘法的结合律，左、右分配律是显然成立的。 □

**定理 2.2.1: 满同态把子环映射到子环**

设 $R, S$ 是两个环，$\varphi : R \to S$ 是一个满同态，$I = \ker\varphi$ 是一个子环，那么：

任意一个 $R$ 的子环 $R' \subseteq R$，其在 $\varphi$ 下的像 $S' = \varphi(R')$ 是 $S$ 的一个子环；

同时，任意一个 $S$ 的子环 $S'$，$R' = \{r \in R | \varphi(r) \in S'\}$ 也是一个包含了 $I$ 的 $R$ 的子环

**证明:** 首先先证明第一条结论。

$\forall a, b \in R' = \varphi(a) + \varphi(b) = \varphi(a+b) \in S'$

$\varphi(a) \cdot \varphi(b) = \varphi(ab) \in S'$

$\varphi(a) + \varphi(0_R) = \varphi(a) \in S', \varphi(a) + \varphi(-a) = \varphi(0_R) = 0_S$

然后证明第二条结论

首先，因为 $\forall r \in \ker\varphi, \varphi(r) = 0$，所以一定有 $\ker\varphi \in R'$

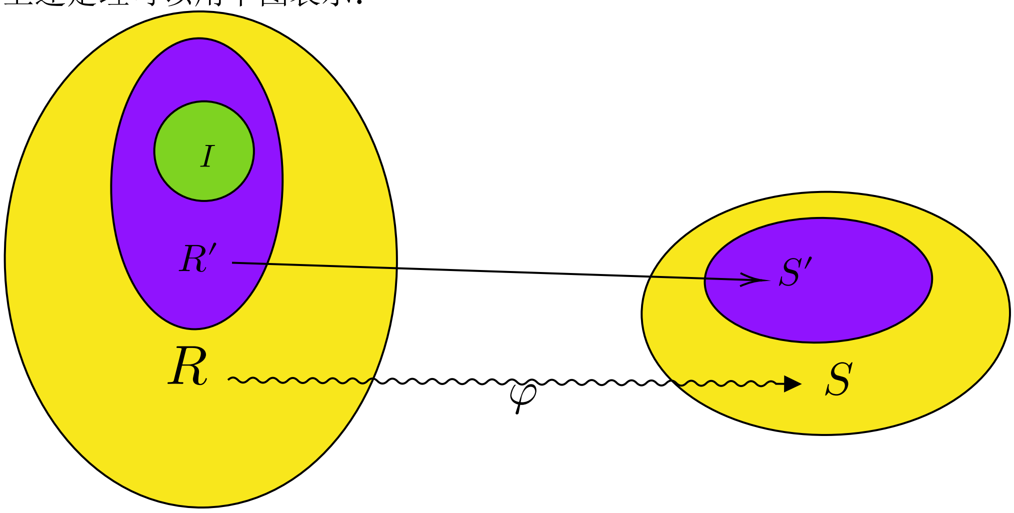
$\forall a, b \in R'$，一定有 $\varphi(a), \varphi(b) \in S'$，所以 $\varphi(a+b) = \varphi(a) + \varphi(b) \in S' \Rightarrow a + b \in R'$

$\varphi(a) \cdot \varphi(b) = \varphi(ab) \in S' \Rightarrow ab \in R'$

$\varphi(a) + \varphi(0_R) = \varphi(a) \in S' \Rightarrow a + 0_R = a \in R', \varphi(a) + (-\varphi(a)) = 0_S \in S' \Rightarrow \varphi(-a) \in S' \Rightarrow -a \in R'$ □

值得注意的是，这个引理中，第一个结论中我们没有要求子环包含同态的核，但是我们随后又提出，从 $S$ 反向映射回来后必须包含同态的核。这并不是矛盾的，因为我们没有限定同态是双射。

上述定理可以用下图表示：



# 2.3 环的理想

## 2.3.1 理想的定义

**定义 2.3.1: 理想**

设 $R$ 是一个环，$R$ 是 $R$ 的一个子环。

如果 $\forall a \in S, b \in R, ab \in S$，那么我们称 $S$ 是 $R$ 的一个左理想；

如果 $\forall a \in S, b \in R, ba \in S$，那么我们称 $S$ 是 $R$ 的一个右理想；

如果 $S$ 既是 $R$ 的左理想，又是 $R$ 的右理想，那么我们称 $S$ 是 $R$ 的一个双理想。

显然，$\{0_R\}, R$ 都是 $R$ 的理想，我们称之为平凡理想。

我们观察到：一些环，比如说 $\mathbb{Z}$，他们有一种特殊的理想，比如说 $\forall m \in \mathbb{Z}, m\mathbb{Z}$ 是 $\mathbb{Z}$ 的一个理想。我们把这种直接由一个元素“生成”的理想叫主理想。

**定义 2.3.2: 主理想**

设 $R$ 是一个环，如果 $R$ 的一个理想 $S$ 满足：

$\exists a \in R, S = aR := \{ab | b \in R\}$，那么我们称 $S$ 是由 $a$ 生成的主理想，记作 $(a)$

## 2.3.2 理想的性质

1.

**命题 2.3.1.** 设 $\psi : R \to S$ 是一个环同态，那么 $\ker \psi$ 是 $S$ 的一个理想

**证明:** 取 $\forall a \in \ker \psi$，依核的定义，$\psi(a) = 0_S$

那么，$\forall b \in R, \psi(ab) = \psi(a)\psi(b) = 0_S, \psi(ba) = \psi(b)\psi(a) = 0_S$

因此，$ab, ba \in \ker \psi$，于是命题得证。 □

2.

**命题 2.3.2.** 设 $R$ 是一个幺环，$S$ 是 $R$ 的一个双理想，如果 $1_R \in S$，那么 $S = R$

**证明:** 依理想的定义，$\forall b \in R, 1_R b = b 1_R = b \in S$，所以 $R \subseteq S$，所以必须有 $R = S$ □

我们可以立即得出，最特殊的幺环——域，也可以应用上述性质

**推论 2.3.1: 域没有非平凡理想**

域只有平凡理想

**证明:** 设 $F$ 是一个域，$S$ 是 $F$ 的一个理想

因为域中任意元素都有逆元素，所以 $\forall a \in S, a^{-1} \in F$

而按照理想的概念，$a \cdot a^{-1} = 1_F \in S$

而按照前面的命题，$1_F \in S$，那么一定有 $S = F$，它是一个平凡理想；$\square$

# 2.4 商环

## 2.4.1 商环的定义

我们首先定义等价类，随后定义商环

**定义 2.4.1: 关于环的理想的等价类**

设 $R$ 是一个环，$S$ 是 $R$ 的一个理想

我们定义 $R \times R$ 上的一个等价关系：$\underset{I}{\sim}: \{(x,y)|x-y \in I\} \subseteq R \times R$

并定义 $a \in R$ 关于 $\underset{I}{\sim}$ 的等价类为：$a + I := \overline{a} := \{x \in R | x \underset{I}{\sim} a\}$

我们其实还需要验证以上关系的确是一个等价关系：

首先，$\forall a \in R, a \sim a$，因为 $a - a = 0_R \in I$，这说明自反性成立；

其次，如果 $a \sim b$，那么有 $a - b \in I$，而 $I$ 是一个理想，所以一定有 $b - a \in I$，所以 $b \sim a$，这说明对称性成立；

最后，如果 $a \sim b, b \sim c$，那么有 $a - b \in I, b - c \in I$，而 $I$ 是一个理想，所以一定有 $(a-b)+(b-c) = (a-c) \in I$，所以 $a \sim c$，这说明传递性成立；

**定义 2.4.2: 商环**

设 $R$ 是一个环，$I$ 是 $R$ 的一个理想，那么我们定义：

$R/I = \{a + I | a \in R\}$，称为 $R$ 关于 $I$ 的商环

并定义其中的环加法和环乘法为：

$(a+I)+(b+I) = (a+b)+I, (a+I)\cdot(b+I) = (a \cdot b)+I$

事实上，由于 $a + I$ 是一个等价类，我们还需要验证，如果 $a_1 + I = a_2 + I$，即同一等价类选取不同单位元下，运算结果是一致的。

**命题 2.4.1.** 商环的加法和乘法是良定义的 设 $R$ 是一个环，$I$ 是 $R$ 的一个理想，那么如

果 $a_1+I=a_2+I, b_1+I=b_2+I$

那么 $(a_1+I)+(b_1+I)=(a_2+I)+(b_2+I), (a_1+I)\cdot(b_1+I)=(a_2+I)\cdot(b_2+I)$

**证明：** 对于第一条，只需证明 $(a_1+b_1)-(a_2+b_2)\in I$。

因为 $(a_1+b_1)-(a_2+b_2)=(a_1-a_2)+(b_1-b_2)$，而 $a_1-a_2\in I, b_1-b_2\in I$，所以 $(a_1+b_1)-(a_2+b_2)\in I$

对于第二条，只需证明 $(a_1\cdot b_1)-(a_2\cdot b_2)\in I$。

因为 $(a_1\cdot b_1)-(a_2\cdot b_2)=(a_1\cdot b_1-a_1\cdot b_2)+(a_1\cdot b_2-a_2\cdot b_2)$

$=a_1(b_1-b_2)+(a_1-a_2)b_2\in I$，因为 $I$ 是一个理想。 □

## 2.5 同态基本定理

### 2.5.1 同态基本定理

**定理 2.5.1: 同态第一定理**

设 $R,S$ 是两个环，$\varphi: R\to S$ 是一个环同态，那么：

$$R/\ker\varphi\cong \mathrm{Im}\ \varphi \tag{2.1}$$

并且同构映射 $\psi$ 唯一，即 $\psi: R/\ker\varphi\ni a+\ker\varphi\mapsto\varphi(a)\in \mathrm{Im}\ \varphi$

**证明：** 我们考虑以下映射：

$\psi: R/\ker\varphi\ni a+\ker\varphi\mapsto\varphi(a)\in \mathrm{Im}\ \varphi$

因为 $a+\ker\varphi=b+\ker\varphi\Rightarrow a-b\in\ker\varphi\Rightarrow\varphi(a)-\varphi(b)=0$，所以它的确是映射。

首先，$\psi\left((a+\ker\varphi)+(b+\ker\varphi)\right)=\psi\left((a+b)+\ker\varphi\right)=\varphi(a+b)=\varphi(a)+\varphi(b)=\psi(a+\ker\varphi)+\psi(b+\ker\varphi)$

$\psi\left((a+\ker\varphi)\cdot(b+\ker\varphi)\right)=\psi(ab+\ker\varphi)=\varphi(ab)=\varphi(a)\varphi(b)=\psi(a+\ker\varphi)\cdot\psi(b+\ker\varphi)$

这说明 $\psi$ 是一个同态，我们接下来证明双射性。

首先证明单射性，如果 $\psi(a+\ker\varphi)=\psi(b+\ker\varphi)$，即 $\varphi(a)=\varphi(b)$，那么 $\varphi(a)-\varphi(b)=\varphi(a-b)=0_R$，所以 $a-b\in\ker\varphi$，于是 $a+\ker\varphi=b+\ker\varphi$，单射性成立。

满射性是显然的，因为显然 $\forall b\in \mathrm{Im}\ \varphi, \exists a\in R, \varphi(a)=b, \psi(a+\ker\varphi)=\varphi(a)=b$

我们最后证明同构映射唯一性

我们设 $\chi : R/\ker\varphi \to \operatorname{Im}\varphi$ 是一个同构映射。

那么，一定有 $\varphi = \chi \circ \pi_{\ker\varphi}$，其中 $\pi_{\ker\varphi} : R \ni a \mapsto a + \ker\varphi \in R/\ker\varphi$

我们注意到，$\psi(a + \ker\varphi) = \varphi(a) = \chi\left(\pi_{\ker\varphi}(a)\right) = \chi(a + \ker\varphi)$

所以一定有 $\psi = \chi$，于是命题得证。 □

### 2.5.2 同构基本定理

1. 第一同构定理

**定理 2.5.2: 同构第一定理**

设 $R, S$ 是两个环，$\varphi : R \to S$ 是一个满同态，那么：

$$R/\ker\varphi \cong S \tag{2.2}$$

并且同构映射唯一。

**证明：** 这个定理事实上是同态基本定理的一个特例，因为如果 $\varphi$ 满，那么一定有 $\operatorname{Im}\varphi = S$ □

2. 第二同构定理

**定理 2.5.3: 第二同构定理**

设 $R$ 是一个环，$S$ 是 $R$ 的一个子环，$I$ 是 $R$ 的一个理想，那么：

$$S/(S \cap I) \cong (S + I)/I \tag{2.3}$$

其中 $S + I = \{a + b | a \in S, b \in I\}$

**证明：** 我们首先验证 $S + I$ 是一个子环

$\forall z = x + y \in S + I, x \in S, y \in I, c = a + b \in S + I, a \in S, b \in I$

$z + c = (x + y) + (a + b) = (x + a) + (y + b) \in S + I$

$z \cdot c = (x + y) \cdot (a + b) = (x + y) \cdot a + (x + y) \cdot b \in I$

$x + y + (0_R + 0_R) = x + y, x + y + (-x + (-y)) = 0_R$，因此 $S + I$ 是一个子环，于是 $I$ 也是 $S + I$ 的理想

随后我们验证 $S \cap I$ 是一个理想

先验证 $S\cap I$ 是一个子环：$\forall x,y\in S\cap I, x+y\in S, x\cdot y\in I$，而 $0_R\in S, 0_R\in I\Rightarrow 0_R\in S\cap I, \forall a\in S\cap I, -a\in S, -a\in I\Rightarrow S\cap I$

再验证 $S\cap I$ 是一个理想：$\forall a\in S\cap I, b\in R, a\in S\Rightarrow ab\in S, a\in I\Rightarrow ab\in S\cap I$

我们考虑映射 $\varphi: S/(S\cap I)\ni a+S\cap I\mapsto a+I\in(S+I)/I$

它显然是一个映射，因为 $a+S\cap I=b+S\cap I\Rightarrow a-b\in S\Rightarrow a-b\in S+I\Rightarrow a+I=b+I$

我们接下来证明它是一个同态:

$\forall a+S\cap I, b+S\cap I\in S/(S\cap I), \varphi((a+S\cap I)+(b+S\cap I))=\varphi((a+b)+(S\cap I))=(a+b)+I=(a+I)+(b+I)=\varphi(a+(S\cap I))+\varphi(b+(S\cap I))$

$\varphi((a+S\cap I)\cdot(b+S\cap I))=\varphi(a\cdot b+(S\cap I))=a\cdot b+I=(a+I)\cdot(b+I)=\varphi(a+(S\cap I))\cdot\varphi(b+(S\cap I))$

再验证它是一个双射：

单射性：$\forall a+(S\cap I), b+(S\cap I)\in S/(S\cap I), \varphi(a+(S\cap I))=\varphi(b+(S\cap I))\Rightarrow a+I=b+I\Rightarrow a-b\in I\Rightarrow a-b\in S\cap I\Rightarrow a+(S\cap I)=b+(S\cap I)$（注意隐含的条件 $a,b\in S$）

满射性：$\forall(x+y)+I\in(S+I)/I, x\in S, y\in I, \varphi(x+(S\cap I))=x+I=x+y=I$，因为 $(x+y)-y=y\in I$

于是命题得证。 □

3. 第三同构定理

在考虑第三同构定理前，我们先讨论一个引理

**引理 2.5.4**

设 $R,S$ 是两个环，$\varphi:R\to S$ 是一个满同态，$I=\ker\varphi$ 是一个理想

那么对于包含于 $I$ 的任意一个 $R$ 的理想 $J$，存在唯一的环同态 $\chi:R/J\to S$，

使得 $\varphi=\chi\circ\pi_J$，其中 $\pi_J:R\ni a\mapsto a+J\in R/I$

并且此时 $\ker\chi=I/J$

**证明：** 我们考虑我们之前曾经构造的映射：$\chi:R/J\ni a+J\mapsto\varphi(a)\in S$

我们之前已经证明了它是一个同构映射，我们接下来证明 $\ker\chi=I/J$

因为 $\ker\chi=\{a+J|\chi(a+J)=0_S\}$

而 $\chi(a+J)=\varphi(a)$，所以 $a+J\in\ker\chi\Rightarrow\varphi(a)=0\Rightarrow a\in I$

所以 $\ker\chi=I/J$，我们接下来证明 $\chi$ 是唯一的，并且 $\varphi=\chi\circ\pi_J$

我们设 $\psi:R/J\to S$ 是一个同构映射。他显然也满足 $\varphi=\psi\circ\pi_J$

我们注意到，$\chi(a+J)=\varphi(a)=\psi(\pi_J(a))=\psi(a+J)$

所以一定有 $\psi=\chi$，于是命题得证。 □

**定理 2.5.5: 第三同构定理**

设 $R$ 是一个环，$I,J$ 是 $R$ 的两个理想，并且 $I\subseteq J$。

那么 $J/I$ 是 $R/I$ 的理想，并且

$$(R/I)/(J/I)\cong R/J \tag{2.4}$$

**证明:** 我们考虑满同态 $\varphi:R\ni a\mapsto a+J\in R/J$

注意到：$\ker\varphi=\{a|a+J=0_{R/J}\}=\{a|a+J=J\}=\{a|a-0_R\in J\}=J$

运用前面的引理，那么一定有一个同态 $\chi:R/I\to R/J$，并且 $\ker\chi=J/I$

接下来运用同构第一基本定理，于是有 $(R/I)/(J/I)\cong R/J$，命题得证。 □

## 2.6 模

本节我们研究一种"环上的线性空间"，也就是模

### 2.6.1 模的定义

**定义 2.6.1: 左模**

设 $R$ 是一个环，$M$ 是一个集合，如果存在两个运算 $+:M\times M\to M,\cdot_R:R\times M\to M$ 分别称为称为加法和纯量乘法，满足下列条件：

① $\exists 0_M\in M$，称为加法单位元，$\forall\alpha\in M,0_M+\alpha=\alpha+0_M=\alpha$

② $\forall\alpha,\beta\in M,\alpha+\beta=\beta+\alpha$

③ $\forall\alpha,\beta,\gamma\in M,(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$

④ $\forall\alpha\in M,\exists-\alpha\in M$，称为加法逆，使得 $\alpha+(-\alpha)=0_M$

⑤ $\forall a,b\in R,\alpha\in M,a(b\alpha)=(ab)\alpha$

⑥ $\forall a\in R,\alpha,\beta\in M,a(\alpha+\beta)=a\alpha+a\beta$

⑦ $\forall a,b\in R,\alpha\in M,(a+b)\alpha=a\alpha+b\alpha$

那么我们称 $M$ 是一个左 $R-$ 模

类似地，我们也有右模的定义：

**定义 2.6.2: 右模**

设 $R$ 是一个环，$M$ 是一个集合，如果存在两个运算 $+: M\times M\to M, \cdot_R: M\times R\to M$ 分别称为称为加法和纯量乘法，满足下列条件：

① $\exists 0_M\in M$，称为加法单位元，$\forall \alpha\in M, 0_M+\alpha=\alpha+0_M=\alpha$

② $\forall \alpha,\beta\in M, \alpha+\beta=\beta+\alpha$

③ $\forall \alpha,\beta,\gamma\in M, (\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$

④ $\forall \alpha\in M, \exists -\alpha\in M$，称为加法逆，使得 $\alpha+(-\alpha)=0_M$

⑤ $\forall a,b\in R, \alpha\in M, (\alpha a)b=\alpha(ab)$

⑥ $\forall a\in R, \alpha,\beta\in M, (\alpha+\beta)a=\alpha a+\beta b$

⑦ $\forall a,b\in R, \alpha\in M, \alpha(a+b)=\alpha a+\alpha b$

那么我们称 $M$ 是一个右 $R-$ 模

如果 $M$ 兼具左模和右模的特征，我们称 $M$ 是一个双模：

**定义 2.6.3: 双模**

如果 $M$ 既是左 $R-$ 模，又是右 $S-$ 模，并且满足：

$(a\alpha)b=a(\alpha b)$

那么我们称 $M$ 是一个 $(R,S)-$ 双模

我们也知道，环不一定有乘法单位元，因此有以下定义：

**定义 2.6.4: 幺模**

设 $R$ 是幺环，$M$ 是一个 $R-$ 模

如果 $\forall \alpha\in M, 1_R\cdot\alpha=\alpha$，那么我们称 $M$ 是一个幺模。

在后续中，除非特别做区分，我们都假定我们说的模指的是左模。

### 2.6.2 模的同态

**定义 2.6.5: 模同态**

设 $M, N$ 是两个 $R-$ 模，如果映射 $\psi : M \to N$ 满足：

$\forall \alpha, \beta \in M, \psi(\alpha + \beta) = \psi(\alpha) + \psi(\beta)$

$\forall a \in R, \alpha \in M, \psi(a\alpha) = a\psi(\alpha)$

那么称 $\psi$ 是一个从 $M$ 到 $N$ 的模同态。

### 2.6.3 商模

**定义 2.6.6: 商模**

设 $M$ 是一个模，$N$ 是 $M$ 的一个子模

# 第三章　Galois 理论

## 3.1　Galois 群

**定义 3.1.1: Galois 群**

设 $E, F$ 是两个域，$E\backslash F$ 是一个扩张，那么称

$Gal(E\backslash F) = \{\sigma \in Aut(E) | \sigma|_F = id_F\}$

是 $E\backslash F$ 的 $Galois$ 群

**定理 3.1.1: 有限扩张的 Galois 群有限**

如果 $E\backslash F$ 是有限扩张，那么 $Gal(E\backslash F)$ 是有限群

# 第四章　附录

这一部分中，对于正文中因为逻辑结构无法提及的部分，进行补充。

## 4.1　一些典型的域

### 4.1.1　$F_p$

首先约定，这一部分的讨论中，都认为 $p$ 是一个素数。

我们首先讨论的是一个典型的有限域——模 $p$ 剩余类域。

**定义 4.1.1: $F_p$**

设 $F$ 是一个域，$CharF \geqslant p$ 且 $p$ 是一个素数，

我们定义 $F_p = N(\mathbb{Z}_p)$

并定义其中的加法和乘法为：

$+_F = N^-1 \circ + \circ N, \cdot_F = N^-1 \circ \cdot \circ N$

**定理 4.1.1: $F_p$ 没有真子域**

设 $p$ 是一个素数，那么域 $F_p$ 不存在真子域，即 $F_p \backslash E \to E = F_p$

**证明：** 不妨假设命题不成立，那么一定有真子域 $E \subseteq F_p$

不妨假设 $[F_p : E] = d$，因为 $F_p$ 是有限域，那么 $|E|, |F_p|$ 都是有限的。

但是，$|F_p| = |E|^d$

$\Rightarrow p = |E|^d$，但是 $p$ 是素数，因此只可能 $d = 1$

于是 $|F_p| = |E|$，那么只可能 $F_p = E$，与假设矛盾，于是命题得证。 □

### 4.1.2 $\mathbb{Q}$

**定理 4.1.2: $Q$ 没有真子域**

$\mathbb{Q}$ 不存在真子域，即 $\mathbb{Q}\backslash E \to E = \mathbb{Q}$

**证明:** 不妨假设命题不成立，$E \subset \mathbb{Q}$ 是 $\mathbb{Q}$ 真子域。

那么，因为 $0, 1 \in E$，由域对加法封闭，那么一定有 $\mathbb{N} \subseteq E$

进一步，因为任意元素的加法逆存在，于是有 $\mathbb{Z} \subseteq E$

于是，由任意非零元素的逆存在，一定有 $\mathbb{Q} \subseteq E$。

但是，我们假设 $E \subset \mathbb{Q}$，矛盾。于是命题成立 □