近世代数

Fir1247

2023 年 03 月-2022 年 7 月

前言

本文档为 2023 年春季学期叶郁老师的《近世代数》课程笔记。

为避免歧义，本文档中的 $\subset$，相当于 $\subseteq, \subseteqq$，均表示“包含于”的意思，且只使用第一种形式；本文档中的 $\subsetneq$，相当于 $\subsetneqq$，均表示“真包含于”的意思，且只使用第一种形式。

我一直记不清楚的符号：

1. 群的中心：$Z(G) = C(G) \overset{\text{def}}{=} \{g \in G | gh = hg, \forall h \in G\}$.
2. 一般线性群：$GL_n(F)$，指域 F 上所有 n 阶可逆矩阵组成的乘法群。
3. 特殊线性群：$SL_n(F)$，指域 F 上所有行列式为 1 的 n 阶矩阵组成的乘法群，是 $GL_n(F)$ 的一个重要子群。
4. 一般射影线性群：$PGL_n(F) \overset{\text{def}}{=} GL_n(F)/Z(GL_n(F))$，也就是线性相关的矩阵定义为等价之后划分的等价类，类似于射影空间。
5. 群的自同构群：$Aut(G)$.
6. 群的内自同构群：$Inn(G)$，由群内元素 g 诱导的自同构映射 $f_g : x \mapsto gxg^{-1}$ 全体，同构于 $G/Z(G)$.

Fir1247

目录

第一章　群

1.1　集合论预备知识

1.2　群的基本概念

1.3　子群与陪集分解

1.4　循环群

1.5　正规子群、商群、同态定理

1.6　置换群

定义 1.6.1 集合到自身上的一一对应称为置换。有限集 A 的置换表示为：

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_n) \end{pmatrix}$$

有限群的全体置换构成一个群，称为对称群，对称群的任何子群都叫做置换群。一般用 $S(A)$ 表示有限集 A 的对称群，用 S_n 表示 n 元对称群。

如下置换被称为 k-轮换：

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_k \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$$

简记为 $(a_1 a_2 \cdots a_k)$.

不相交的轮换的复合可交换，不计次序地，每个置换可以被唯一标识成没有公共元素的一些轮换之积。

长度为 2 的轮换被称为对换，每个置换都可以被表示成有限个对换之积[1]。这种表示不唯一，但所含对换个数的奇偶性是不变的，由此被分类成奇置换和偶置换。考虑置换群到二元乘法群的映射

$$f : S_n \to \{\pm 1\}, n \geqslant 2$$

f 把偶置换映射到 1，奇置换映射到 -1，则 f 是一个满的群同态，$Ker(f)$ 就是全体偶置换构成的子群，称为 n 元交错群，一般记作 A_n.

把 σ 写成互不相交的轮换乘积，其中 k-轮换出现的次数为 λ_k，称 σ 的型为

$$1^{\lambda_1} 2^{\lambda_2} \cdots n^{\lambda_n}$$

[1] 见例 2.1.3

而且 $1\lambda_1 + 2\lambda_2 + \cdots + n\lambda_n = n.$

例 1.6.1

$$\begin{aligned}&(123456)(1234567)\\=&\begin{pmatrix}1&2&3&4&5&6\\2&3&4&5&6&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7\\2&3&4&5&6&7&1\end{pmatrix}\\=&\begin{pmatrix}1&2&3&4&5&6&7\\3&4&5&6&1&7&2\end{pmatrix}\\=&(135)(2467)\end{aligned}$$

例 1.6.2

$$\sigma(a_1\cdots a_k)\sigma^{-1}(y)=\begin{cases}y & ,y\notin\{\sigma(a_1),\cdots,\sigma(a_k)\}\\ \sigma(a_{i+1}) & ,y=\sigma(a_i)\end{cases}$$

此式表明了轮换逆映射的性质。

例 1.6.3 任何一个 k-轮换可以写成 $k-1$ 个对换的乘积。

证明： 例如：$(a_1\cdots a_k)=(a_1a_k)(a_1a_{k-1})\cdots(a_1a_3)(a_1a_2).$

例 1.6.4 $(12),(13),\cdots,(1n)$ 为 n 元对称群 S_n 的一组生成元。

证明： 任何一个置换能被写成不交的轮换之积，再由例 2.1.3 可知任何一个轮换能别写成对换之积，而任何一个对换 $(ij)=(1i)(1j)(1i)$，于是结论得证。

定义 1.6.2 对于 $\sigma\in S_n$，称 (i,j) 为其逆序对，指的是 $1\leqslant i<j\leqslant n$ 但 $\sigma(i)>\sigma(j)$. σ 的逆序数定义为

$$|\{(i,j)|1\leqslant i<j\leqslant n,\sigma(i)>\sigma(j)\}|$$

即逆序对的个数。若 τ 为对换，则 σ 与 $\sigma\tau$ 的逆序数奇偶性相反。

因此奇置换的逆序数为奇数，偶置换的逆序数为偶数，这是奇偶置换的另一种等价定义。

定理 1.6.1 存在唯一的群同态 $\varepsilon:S_n\to\{\pm1\}$ 使得对一对换 τ，$\varepsilon(\tau)=-1.$

证明： 把奇置换映到 -1，偶置换映到 1，所得的 ε 就满足所求。

复习： $H\triangleleft G$ 的三个等价定义：
(1). $\forall g\in G,gH=Hg.$
(2). $\forall g\in G,gHg^{-1}=H.$
(3). $\forall g\in G,h\in H,g^{-1}hg\in H.$

元素共轭的定义：$h,k\in G$，若 $\exists g\in G,k=ghg^{-1}$，称 h 与 k 共轭。

子群共轭的定义：H,K 都是 G 的子群，若 $\exists g\in G,K=\{ghg^{-1}|h\in H\}$，称 H 与 K 共轭。

由此我们得到两个推论：共轭子群都是自身的子群是正规的；正规子群中任意元素所在共轭类必定包含于正规子群中，即正规子群必定为若干个共轭类之并，关于共轭运算是封闭的。这两个结论后面会用到。

定理 1.6.2 对称群中，两个置换共轭的充要条件为有相同的型。

定理 1.6.3 $n \geqslant 5$ 时，交错群 A_n 是单群[2]，且是 S_n 的唯一非平凡正规子群。

注： $A_1 = \{1\}$，$A_2 = \{1\}$，$A_3 \cong \mathbb{Z}/3\mathbb{Z}$，而 A_4 不是单群，因为 $K_4 \triangleleft A_4$.

引理 1.6.1 A_n 由三轮换生成。

证明： 只考虑 $n \geqslant 4$，注意到

$$\begin{aligned}(ij)(ji) &= 1\\ (ij)(jk) &= (ikj), i \neq j \neq k\\ (ij)(kl) &= (ij)(jk)(jk)(kl) = (ijk)(jkl), i \neq j \neq k \neq l\end{aligned}$$

而偶置换必然能分解成偶数个对换之积，所以引理得证。

引理 1.6.2 对于 $m \geqslant 5$，A_n 中所有的 3-轮换在 A_n 中共轭。

证明： 我们来证明 A_n 种所有的 3-轮换都在 A_n 中共轭到 (123).

设 σ 为 A_n 中的 3-轮换，它显然在 S_n 共轭到 (123):

$$(123) = \pi\sigma\pi^{-1}, \exists \pi \in S_n$$

如果 $\pi \in A_n$ 则引理成立，否则取 $\pi' = (45)\pi$，则 $\pi' \in A_n$，且 $\pi'\sigma\pi'^{-1} = (45)(123)(45) = (123)$.

证明： **(Pf of Thm)** 设 $\{1\} \neq N \triangleleft A_n$，若证明 N 中含有一个 3-轮换，由于 3-轮换在 A_n 中彼此共轭，因为共轭类包含在正规子群当中，N 就包含所有的 3-轮换，从而生成 A_n，也就是 $N = A_n$. 如此一来，定理就得证了，下面我们证明 N 中含有一个 3-轮换。

设 $\sigma \in N, \sigma \neq (1)$，可以分解成不交的轮换

$$\sigma = \pi_1\pi_2\cdots\pi_k$$

不妨剔除所有的 1-轮换，分情况讨论：

Case 1: 若某些 π_i 至少长度为 4，重排后不妨设为 $\pi_1 = (12\cdots r), r \geqslant 4$. 设 $\varphi = (123)$，则 $\varphi\sigma\varphi^{-1} \in N$，且

$$\begin{aligned}\varphi\sigma\varphi^{-1} &= \varphi\pi_1\varphi^{-1}\pi_2\cdots\pi_k\\ &= \varphi\pi_1\varphi^{-1}\pi_1^{-1}\sigma\\ &= (123)(12\cdots r)(132)(r\cdots 21)\sigma\\ &= (124)\sigma\end{aligned}$$

从而 $(124) = \varphi\sigma\varphi^{-1}\sigma^{-1} \in N$.

Case 2: 如果所有的 π_i 长度均不大于 3，且至少有两个长度为 3. 不失一般性，设 $\pi_1 = (123)$，$\pi_2 = (456)$，取 $\varphi = (124)$，则

$$\begin{aligned}\varphi\sigma\varphi^{-1} &= \varphi\pi_1\pi_2\varphi^{-1}\pi_3\cdots\pi_k\\ &= \varphi\pi_1\pi_2\varphi^{-1}\pi_2^{-1}\pi_1^{-1}\sigma\\ &= (124)(123)(456)(142)(465)(132)\sigma\\ &= (12534)\sigma\end{aligned}$$

也就是说 $(12534) = \varphi\sigma\varphi^{-1}\sigma^{-1} \in N$，再由 Case 1，从 5-轮换出发又可以得到 3-轮换。

[2]指不含非平凡正规子群的群，换言之，其正规子群只能是 $\{1\}$ 或其本身。

Case 3: 如果只有一个长度为 3 的轮换，其余轮换长度均小于 3，不失一般性，设 $\varphi=(123)$，则其余轮换均为 2-轮换，则 $\sigma^2=\pi_1^2=(132)\in N$.

Case 4: 如果所有的轮换长度都为 2，则必然 $k>1$，记 $\pi_1=(12)$，$\pi_2=(34)$，设 $\varphi=(123)$，则

$$\begin{aligned}\varphi\sigma\varphi^{-1}&=\varphi\pi_1\pi_2\varphi^{-1}\pi_3\cdots\pi_k\\&=\varphi\pi_1\pi_2\varphi^{-1}\pi_2^{-1}\pi_1^{-1}\sigma\\&=(123)(12)(34)(132)(34)(12)\sigma\\&=(13)(24)\sigma\end{aligned}$$

于是 $(13)(24)\in N$，设 $\psi=(135)$，则

$$(13)(24)\psi(13)(24)\psi^{-1}=(13)(24)(135)(13)(24)(153)=(135)\in N$$

1.7 群在集合上的作用

定义 1.7.1 设 G 是群，集合 X 不是空集，映射

$$\varphi:G\times X\to X,(g,x)\mapsto g\cdot x$$

满足：

(1) $g(hx)=(gh)x,\forall g,h\in G,x\in X$

(2) $1_G\cdot x=x$.

则这个映射称为群 G 在 X 上的一个左作用，类似地可定义右作用。

例 1.7.1 群乘法 $m:G\times G\to G$ 就是一个 G 在自身上的作用。

注： 如果 φ 为群 G 在 X 上的一个左作用，那么对于每个 g 可以定义

$$\rho_g\overset{\text{def}}{=}\varphi(g,*):X\to X$$

那么有：

1° $\rho_1=\varphi(1,*)=\mathrm{Id}_X\in S(X)$.

2° $\rho_g\circ\rho_h=\rho_{gh}\in S(X)$.

3° $\rho_{g^{-1}}=\rho_g^{-1}$.

4° $\rho_f(\rho_g\rho_h)=\rho_{fgh}=(\rho_f\rho_g)\rho_h$.

G 中的每个元素，对应了集合 X 上的一个置换，可见 G 在 ρ 下的像集为 $S(X)$ 的子群，

$$\rho:G\to S(X),g\mapsto\rho_g$$

给出了一个群同态。这被叫做群 G 的一个表示。

定义 1.7.2 事实上，G 在 X 上的作用，与 G 到 $S(X)$ 的群同态是一一对应的。那么从表示出发我们当然也可以得到群的作用，设有表示（群同态）：

$$\rho:G\to S(X)$$

我们定义 $g\cdot x\overset{\text{def}}{=}\rho(g)(x)$. 则此定义给出了 G 在 X 上的一个作用，我们用 $G\circlearrowright X$ 表示 G 作用在 X 上。

$G \circlearrowright X$，在 X 上可以定义等价关系：

$$x \sim y \overset{\text{def}}{\Leftrightarrow} \exists g \in G, y = g \cdot x$$

对于 $\forall x \in X$，定义

$$\mathcal{O}_x = \{g \circ x | g \in G\} \subset X$$

称为 x 在 G 作用下的轨道。如果 $\exists x \in X, X = \mathcal{O}_x$，称 G 在 X 上的作用可迁或传递，

$$G_x = \{g \in G | g \circ x = x\} \leqslant G$$

称为 x 的稳定子群。

例 1.7.2 考虑 X 与其对称群 $S(X)$，则

$$S(X) \times X \to X, (\sigma, x) \mapsto \sigma(x)$$

给出了 X 上的群作用，其相应的表示为 $S(X) \to^{\text{id}} S(X)$.

特别地，$S_n \circlearrowright \{1, 2, \cdots, n\}$，$n$ 的稳定子群 $G_n = S_{n-1} = S(\{1, 2, \cdots, n-1\})$.

例 1.7.3 群 G 上的乘法运算，是 G 在其本身上的作用，且对于 $\forall h \in G, \mathcal{O}_h = G$，从而群作用可迁，$h$ 的稳定子群为 $G_h = \{1\}$.

定理 1.7.1 $G \circlearrowright X$，$\forall x \in X$，有双射：

$$G/G_x \to \mathcal{O}_x, aG_x \mapsto a \cdot x$$

推论 1.7.1 设 $|G| < \infty$，则：

$|\mathcal{O}_x| = [G : G_x]$，称为轨道长度。

$|X| = \sum_{x \in I} |\mathcal{O}_x| = \sum_{x \in I} [G : G_x]$，这里的 I 为轨道的完全代表元系。

定理 1.7.2 设 $G \circlearrowright X$，$x \in X$，$a \in G$，$x' = a \cdot x$，则

1° $\{g \in G | gx = x'\} = aG_x$

2° $G_{ax} = aG_x a^{-1}$

定义 1.7.3 $G \circlearrowright X$ 对应的表示为 ρ，于是

$$\text{Ker}\rho = \{g | gx = x, \forall x \in X\} = \bigcap_{x \in X} G_x \lhd G$$

称为群作用的核。

例 1.7.4 证明：$GL_2(\mathbb{F}_2) = GL_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$.

我们考虑 $GL_2(\mathbb{F}_2) \circlearrowright X = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$，于是 $S(X) = S_3$，从而 $\rho : GL_2(\mathbb{F}_2) \to S_3$ 是群同态。而 $\text{Ker}\rho = \{I_2\}$，所以是单射，进而是群同构。

定理 1.7.3 (Caylay) 任一（有限）群是（有限阶）对称群的子群。

证明： 左乘作用诱导群同态 ρ，而 $\text{Ker}\rho = \bigcap_{g \in G} G_g = \{1_G\}$，是单射。

定义 1.7.4 考虑

$$G \times G \to G$$
$$(g, x) \mapsto gxg^{-1}$$

称为 G 在 G 上的共轭作用。

与之对应的表示满足 $\rho : G \to \mathrm{Inn}G \leqslant \mathrm{Aut}G \leqslant S(G)$.

注意到此时 $|G| = |\mathcal{O}_x||G_x|$, 因为 $G\backslash G_x$ 与 $\mathcal{O}_x$ 一一对应。以及对于 $G \circlearrowleft X, \varnothing \neq Y \subset X$, 若 $g \cdot Y \subset Y, \forall g \in G$, 则诱导了 G 在子集 Y 上的作用。

对 $x \in G$,

$$c_x = \mathcal{O}_x = \{gxg^{-1} | g \in G\}$$

称为 x 所在的共轭类, 而

$$Z_G(x) = G_x = \{g \in G | gxg^{-1} = x\}$$

称为 x 的中心化子。而对于 $T \subset G$, T 的中心化子定义为

$$\begin{aligned} Z_G(T) &= \bigcap_{t \in T} Z_G(t) \\ &= \{g \in G | gt = tg, \forall t \in T\} \end{aligned}$$

定理 1.7.4 设 $|G| < \infty$, 则
(1). $|G| = |c_x| \cdot |Z_G(x)|$.
(2). $|G| = \sum_{x \in I} |c_x| = |Z(G)| + \sum_{x \in I, |c_x| \geqslant 2} |c_x|$, 其中 I 为共轭类的完全代表元系。

推论 1.7.2 设 G 为 p 群[3], X 为集合, $|X| = n$, $(n, p) = 1$, $G \circlearrowleft X$, 则 X 有不动点, 即 $\exists x \in X$ 使得 $g \cdot x = x, \forall x \in G$. 特别地, G 有非平凡中心。

证明:

注: 对于 $n \geqslant 3$, $Z(S_n) = \{1_G\}$.

定义 1.7.5 设 $H \leqslant G$, 记

$$c_H = \{gHg^{-1} | g \in G\}$$

为 H 的共轭子群, 这里 $gHg^{-1} \leqslant G$. 则有可迁作用

$$G \times c_H \to c_H$$
$$(g, H_1) \mapsto g \cdot H_1 := gH_1g^{-1}$$

H 在 G 的共轭作用下的稳定子群

$$N_G(H) = G_H = \{g \in G | gHg^{-1} = H\}$$

称为 H 在 G 中的正规化子。

显然, $H \leqslant N_G(H)$, $|c_H| = |G|\backslash|N_G(H)|$.

于是 $G \circlearrowleft c_H$ 诱导了 $\rho : G \to S(c_H)$, 进而

$$\mathrm{Ker}\rho = \bigcap_{g \in G} N_G(gHg^{-1}) = \bigcap_{g \in G} gN_G(H)g^{-1}$$

称为共轭作用的核。

[3] p 为素数, $|G| = p^r, r \geqslant 1$.

例 1.7.5 设 $|G|=n$，p 为 n 的最小的素因子，那么 $[G:H]=p \Rightarrow H \triangleleft G.$

特别地，若 $[G:H]=2$，则 $H \triangleleft G.$

值得一提的是，$H \triangleleft N_G(H)$ 是 G 中包含 H，且 H 在其中正规的最大子群。

证明：

1.8 Sylow 定理

定理 1.8.1 (Cauchy) p 为 $|G|$ 的素因子，则 G 中存在 p 阶元。

证明：

定义 1.8.1 $n=|G|=p^r \cdot m$，$(p,m)=1$，$H \leqslant G$，若 $|H|=p^k$，$1 \leqslant k \leqslant r$，则称 H 为一个 p-子群。

若 $|H|=p^r$，则称 H 为一个 Sylow$p$-子群。记 G 的全体 Sylow$p$-子群为 $\mathrm{Syl}_p(G)$.

我们目标在于证明 Sylow$p$-子群存在，从而任一 p^k 阶子群存在。

定理 1.8.2 (Sylow) p 素，$|G|=p^r m$，$(p,m)=1$，则

(1). G 存在 Sylow$p$-子群。

(2). 任一 Sylow$p$-子群 P，以及一个 p-子群 Q，则存在 $g \in G$，使得 $Q \leqslant gPg^{-1}$.

(3). 记 Sylow$p$-子群的个数为 $N(p)$，则 $N(p) \equiv 1 \bmod p, N(p)||G| \Rightarrow N(p)|m$.$p$-子群也有相同的性质。

(4). 如果 G 的一个 Sylow$p$-子群为 A，则 $N(p)=[G:N_G(A)]$.

引理 1.8.1 $P \in \mathrm{Syl}_p(G), Q \leqslant G$ 为 p-子群，则 $H=Q \cap N_G(P)=Q \cap P.$

例 1.8.1 p，q 为素数，$p \neq q$，则 pq 阶群非单群，p^2q 阶群非单群。

例 1.8.2 不是“素数阶循环群”的有限单群，阶最小为 60，且 60 阶单群同构于 A_5.

他妈的，摆了，不学了。

1.9 自由群与群的表现

定义 1.9.1 对于非空集合 S，元素 $x_i \in S$ 称为字母，$x_1x_2\cdots x_n$ 称为单词或者文字。

定义空文字为空集 $\varnothing$，记作 1. 如果文字 w 由 n 个字母组成，那么就说文字 w 的长度为 $l(w)=n.$

记 $W(S)$ 为 S 上文字全体，定义两段文字的运算为：

$$x_1\cdots x_m \cdot y_1\cdots y_n = x_1\cdots x_m y_1\cdots y_n$$

显然满足结合律。$W(S)$ 在上述运算下形成一个含幺半群，称为集合 S 生成的自由含幺半群。

进一步地，找一个和 S 等势的集合，记为 S^{-1}，对应地位每个 $s \in S$ 配对一个 $s^{-1} \in S^{-1}$，并规定 $s \cdot s^{-1}=s^{-1} \cdot s=1$，那么可以验证，$W(S \cup S^{-1})$ 是一个群。

称 $w \in W(S \cup S^{-1})$ 是一个既约文字，如果 w 不可化简（约化）。如果既约文字 w' 能被文字 w 经过若干次约化得到，称之为 w 的一个既约形式。实际上可以证明，$w \in W(S \cup S^{-1})$ 有着唯一的既约形式。于是可以在 $W(S \cup S^{-1})$ 上定义等价关系：

$$w \sim w' \Leftrightarrow w, w' \text{有相同的既约形式}$$

并记 $F(S)=W(S\cup S^{-1})/_{\sim}$ 为等价类的集合，全体既约形式是其完全代表元系。

在 $F(S)$ 上定义乘法：

$$[w_1]\cdot[w_2]=[w_1\cdot w_2]$$

不难验证良定和结合律。于是 $F(S)$ 在上述乘法下形成一个群，称为由集合 S 生成的自由群。若 S 有限，则成为有限生成自由群。

例 1.9.1 设 $S=\{a\}$，则

$$F(S)=\{\cdots,a^{-1},1,a,a^2,\cdots\}\cong\mathbb{Z}$$

当 $|S|\geqslant 2$ 时，$F(S)$ 不是 Abel 群。

定理 1.9.1 每个群都是自由群的商群；每个有限生成群都是有限生成自由群的商群。

证明： 设 G 为群，取 G 的一个生成元系 Σ（例如可取 $\Sigma=G$）. 定义集合

$$S=\{X_a|a\in\Sigma\}$$

并考虑映射 $f:F(S)\to G$，其中 $f(X_a)=a$，$f(X_a^{-1})=a^{-1}$，然后对于

$$A_i\in\Sigma\cup\Sigma^{-1}(1\leqslant i\leqslant n)$$

定义

$$f(A_1\cdots A_n)=f(A_1)\cdots f(A_n)$$

易证 f 是群同态，并且是满的，因为对于每个生成元 $a\in\Sigma$，$a=f(X_a)\in\mathrm{Im}f$，从而 $G=\langle\Sigma\rangle=\mathrm{Im}f$. 根据同态基本定理，

$$G\cong F(S)/\mathrm{Ker}f$$

结论得证。

定义 1.9.2 设 G 同构于自由群 $F(S)$ 的商群：$F(S)/K$，则 G 是由 $F(S)=\Sigma$ 生成的。

进一步，对于 K 中的每个元素 α，G 中就有一个等式 $f(\alpha)=1_G$.K 中有多少元素，G 中就相应有多少个关系。

如果 P 是 K 的一个子集，且 K 是自由群中包含 P 的最小正规子群（即 P 生成的正规子群），则 K 中的每个元素均可由 P 在 $F(S)$ 中的全部共轭集合的元素运算出来。

反映在群 G 中，G 的所有关系均可由 P 中元素给出的关系推导出来。我们把由 P 中元素给出的那些关系全体叫做群 G 的定义关系集，并且群 G 写成

$$G=\langle\Sigma|f(\alpha)=1,\forall\alpha\in P\rangle$$

这种刻画群的方式叫做群 G 的一个表现。

例 1.9.2 令 $S=\{a,b\}$，K 是 $F(S)$ 中元素 a^3 和 $(ab)^2$ 生成的正规子群，如果 $G\cong F(S)/K$，则 G 的结构可以写成

$$G=\left\langle A,B|A^3=(AB)^2=1\right\rangle$$

例 1.9.3 用 φ 表示关系集合为空集，$G=\langle S|\varphi\rangle$ 即是以 S 为基的自由群，因为此时 $K=\{1\}$，$G\cong F(S)$.

例 1.9.4 $\mathbb{Z}_n \cong \langle a\rangle / \langle a^n\rangle = F(S)/\langle a^n\rangle$，其中 $S = \langle a\rangle$. 其中 $S = \{a\}$，因为 n 阶循环群的表现为

$$\mathbb{Z}_n = \langle a | a^n = 1\rangle$$

例 1.9.5 二面体群 D_n 是指正 n 边形对称群，是 $2n$ 阶群，它有生成元系 $\{\sigma, \tau\}$，满足

$$\sigma^n = \tau^2 = 1, (\tau\sigma)^2 = 1$$

令 F 是以 $\{a, b\}$ 为基的自由群，则有群的满同态：

$$f : F \to D_n$$

$$f(a) = \sigma, f(b) = \tau$$

由同态基本定理可知

$$D_n \cong F/\mathrm{Ker}f$$

注意到

$$f(a^n) = f(b^2) = f((ba)^2) = 1$$

令 K 是 F 中 $\{a^n, b^2, (ba)^2\}$ 生成的正规子群，则 $K \leqslant \mathrm{Ker}f$.

现在考虑商群 F/K，以 A 和 B 分别表示 a, b 在 F/K 中的像，则 $A^n = B^2 = (BA)^2 = 1$. F/K 可由 $\{A, B\}$ 生成，由于

$$BA = A^{-1}B^{-1} = A^{n-1}B$$

F/K 中元素均可以表示成 $A^iB^j (0 \leqslant i \leqslant n-1, 0 \leqslant j \leqslant 1)$ 从而 $|F/K| \leqslant 2n$.

$$2n = |D_n| = |F/\mathrm{Ker}f| = \frac{|F/K|}{|\mathrm{Ker}f|/|K|} \leqslant \frac{2n}{|\mathrm{Ker}f|/|K|}$$

所以 $K = \mathrm{Ker}f$，$D_n \cong F/K$. 于是 D_n 有如下表现

$$D_n = \left\langle a, b | a^n = b^2 = (ba)^2 = 1\right\rangle$$

例 1.9.6 矩阵群 $G = \langle A, B\rangle$，其中

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$$

满足 $A^4 = 1, B^2 = A^2, BA = A^3B$，等价于

$$A^4 = B^2A^2 = BABA^3 = 1$$

这里 1 代表单位矩阵。可以直接验证 $|G| = 8$.

令 $Q_8 = \langle a, b | a^4 = 1, b^2 = a^2, ba = a^3b\rangle$，其中的每个元素都能表示成 $a^ib^j (0 \leqslant i \leqslant 3, 0 \leqslant j \leqslant 1)$ 的形式，所以 $|Q_8| \leqslant 8$.

令 F 是以 $S = \{a, b\}$ 为基的自由群，则有群的满同态：

$$f : F \to G$$

$$f(a) = A, f(b) = B$$

则 $G \cong F/\mathrm{Ker}f$，现在求 $\mathrm{Ker}f$.

由于 $f(a^4) = f(b^2a^2) = f(baba^3) = 1$，令 K 是 F 中 $a^4, b^2a^2, baba^3$ 生成的正规子群，$K \leqslant \mathrm{Ker}f$. 而 $F/K \cong Q_8$，其阶数小于等于 8，故

$$8 = |G| = |F/\mathrm{Ker}f| = \frac{|F/K|}{|\mathrm{Ker}f|/|K|} \leqslant \frac{8}{|\mathrm{Ker}f|/|K|}$$

所以 $K = \mathrm{Ker}f$，进而可以证明 $G \cong Q_8$，也就是说 G 的一个表示就是

$$G = \left\langle a, b | a^4 = 1, b^2 = a^2, ba = a^3b \right\rangle$$

注： 上面两个例子的方法完全一致，都是找到若干限制条件直至商群 F/K 的阶数不大于目标群的阶数，例如最后一个例子中，目标群的性质诱导的三个限制条件 $a^4 = 1, b^2 = a^2, ba = a^3b$，使得商群 $F/K \cong Q_8$ 阶数不大于 8，于是正好能证明 $K = \mathrm{Ker}f$.

定义 1.9.3 设 S 为任意集合，表现为

$$F = \langle S | ba = ab, \forall a, b \in S \rangle$$

的群叫做以 S 为基的自由阿贝尔群（即除了交换性条件以外没有其他任何关系）。

类似于定理 1.9.1，可以证明：每个（有限生成）阿贝尔群都是（有限生成）自由阿贝尔群的商群。

定义 1.9.4 设 $G_1, \cdots, G_n$ 是群，在集合的直积

$$G = G_1 \times \cdots \times G_n = \{(g_1, \cdots, g_n) | g_i \in G_i, 1 \leqslant i \leqslant n\}$$

中定义运算

$$(g_1, \cdots, g_n)(g_1', \cdots, g_n') = (g_1g_1', \cdots, g_ng_n')$$

易验证 G 对此运算成群，叫做 $G_1, \cdots, G_n$ 的直积。

引理 1.9.1 设 $H, K \leqslant G$，$H \cap K = \{1\}$，$G = HK$，且对于每个 $h \in H, k \in K, hk = kh$. 则 $G \cong H \times K$.

定理 1.9.2 设 $G_1, \cdots, G_n \triangleleft G$，$n \geqslant 2$，则下列条件等价：
(1). $G = G_1 \times \cdots \times G_n$.
(2). G 中每个元素都能被唯一地表示成 $g_1 \cdots g_n, g_i \in G_i, \forall 1 \leqslant i \leqslant n$.
(3). $G = G_1 \cdots G_n$，且 $\forall 1 \leqslant m < n$，$(G_1 \cdots G_m) \cap G_{m+1} = \{1\}$.

定理 1.9.3 有限生成自由阿贝尔群 G 同构于有限个无限循环群的直积：$G \cong \mathbb{Z}^r$，并定义 $\mathrm{rank}(G) = r$. 两个这样的群同构当且仅当它们的秩相等。

1.10 有限生成阿贝尔群的结构

在本节中，我们把阿贝尔群中的运算写成加法形式，从而幺元素为 0，元素 a 的逆为 $-a$，n 个 a 运算得到 na，有限阶元素 a 的阶 n 满足 $na = 0$，直积则改称为直和 $\oplus$，但 n 个 A 的直和仍写作 A^n，而 $nA = \{na | a \in A\}$.

定义 1.10.1 $a,b\in G$，$aba^{-1}b^{-1}$ 被称为 a 与 b 的换位子，记作 $[a,b]$.
G 中换位子全体生成的群称为 G 的换位子群或导子群，记为 $[G,G]$ 或 G'.

例 1.10.1 G 交换，则 $G'=\{1\}$；$G=S_n$，则 $G'=A_n$.

推论 1.10.1 $G'\triangleleft G$，且 G/G' 是阿贝尔群。

推论 1.10.2 如果 $\varphi:G\to A$ 是 G 到阿贝尔群 A 的群同态，则 $\mathrm{Ker}\varphi\geqslant G'$.

证明： 均由定义直接验证。

定义 1.10.2 对于集合 S，定义

$$\mathbb{Z}(S)=F(S)\backslash F'(S)=\left\langle S|xyx^{-1}y^{-1},x,y\in S\right\rangle$$

称为由 S 生成的自由阿贝尔群。回忆定义 1.9.3.

定理 1.10.1 有限生成自由阿贝尔群 F 的每个非平凡子群 G 仍是有限生成自由阿贝尔群，而且 $\mathrm{rank}(G)\leqslant\mathrm{rank}(F)$. 更确切地说，令 $n=\mathrm{rank}(F)$，则存在 F 的一组基 $\{x_1,\cdots,x_n\}$，一个整数 $r\leqslant n$ 和一组正整数 $d_1,\cdots,d_r$，且 $d_1|d_2|\cdots|d_r$，并且 G 是以 $\{d_1x_1,\cdots,d_rx_r\}$ 为基的自由阿贝尔群。

定理 1.10.2 每个有限生成自由阿贝尔群 A 均同构于

$$\mathbb{Z}^r\oplus\mathbb{Z}_{m_1}\oplus\cdots\oplus\mathbb{Z}_{m_l}$$

其中 $r,t\geqslant 0$，$1\leqslant m_1\leqslant\cdots\leqslant m_t$ 且 $m_1|m_2|\cdots|m_t$.

定义 1.10.3 A 是有限生成阿贝尔群，以 A_t 表示 A 中有限阶元素全体，如果 a 和 b 分别是 A 中阶数为 r 和 s 的元素，则 a^{-1} 和 ab 的阶分别是 r 和 $\mathrm{lcm}(r,s)$，从而 A_t 是 A 的子群，称之为 A 的扭子群。易知 A_t 还是有限阿贝尔群。

定理 1.10.3 设 A 和 B 都是有限生成阿贝尔群，那么
(1) 存在 A 的有限生成自由阿贝尔子群 A_f，使得 $A=A_f\oplus A_t$.
(2) 如果 $A=A_f\oplus A_t$，$B=B_f\oplus B_t$，则

$$A\cong B\Leftrightarrow\mathrm{rank}(A_f)=\mathrm{rank}(B_f)\text{ and }A_t\cong B_t$$

定理 1.10.4 设 A 为有限阿贝尔群，$A\neq\{0\}$.
(1) 存在 $1<m_1|m_2|\cdots|m_t(t\geqslant 1)$，使得

$$A\cong\mathbb{Z}_{m_1}\oplus\cdots\oplus\mathbb{Z}_{m_t}$$

且 $\{m_1,\cdots,m_t\}$ 由 A 唯一确定，叫做不变因子。
(2) 存在一组正整数 $\{p_1^{s_1},\cdots,p_k^{s_k}\}$，其中 p_i 都是（不必不相同）素数，$s_1,\cdots,s_k$ 为正整数，使得

$$A\cong\mathbb{Z}_{p_1^{s_1}}\oplus\cdots\oplus\mathbb{Z}_{p_k^{s_k}}$$

且 $\{p_1^{s_1},\cdots,p_k^{s_k}\}$ 由 A 唯一确定，叫做初等因子。

定理 1.10.5 关于两个有限生成阿贝尔群，以下命题等价：
(1) 同构；
(2) 有相同的秩和初等因子；
(3) 有相同的秩和不变因子。
特别地，关于两个有限阿贝尔群，它们同构当且仅当有相同的初等因子当且仅当有相同的不变因子。

第二章　环和域

2.1　环和域的基本概念

定义 2.1.1 一个环是指一个三元组 $(R,+,\cdot)$，满足：
(1) $(R,+)$ 为加法群[1]；
(2) $(R,\cdot)$ 为半群；
(3) 满足分配律，即左乘或者右乘是群同态。
更进一步，如果满足：
(4) 存在乘法幺元[2]，则称为含幺环。
(5) 乘法交换，称为交换群。
(6) $(R\backslash\{0_R\},\cdot)$ 为阿贝尔群，则称为域。
(7) 除了零元以外可逆，称之为除环。
都是在对乘法做一些限制。

例 2.1.1 $R=\{0\}\Leftrightarrow 0=1$，只有一个元素的环，称为零环。
$\mathbb{Z}$，$\mathbb{Z}/n\mathbb{Z}$，环，含幺，交换。$\mathbb{Z}$ 不是域，而当且仅当 n 是质数时 $\mathbb{Z}/n\mathbb{Z}$ 是域。

例 2.1.2 对于一个环，可以考察它的全体 n 阶矩阵：

$$M_n(R)=\{(r_{ij})_{n\times n}:r_{ij}\in R\}$$

关于矩阵加法和乘法也是一个环。并且 $M_n(R)$ 是幺环当且仅当 R 是幺环。充分性显然，必要性：假设矩阵群的幺元是 $I=(r_{ij})_{n\times n}$，考虑除第一行第一列 a_{11} 之外都是零的矩阵与 I 相乘，可以得到 $a_{11}r_{11}=r_{11}a_{11}=a_{11}$，再取一些其他的特殊矩阵就可得证。

例 2.1.3

$$\mathbb{H}=\{a+bi+cj+dk:a,b,c,d\in\mathbb{R}\}$$

加法自然定义，乘法定义为：

$$1\cdot i=i\cdot 1,1\cdot j=j\cdot 1,1\cdot k=k\cdot 1$$

$$i^2=j^2=k^2=-1$$

$$ij=k=-ji,jk=i=-kj,ki=j=-ik$$

于是

$$(a+bi+cj+dk)(a'+b'i+c'j+d'k)=aa'-bb'-cc'-dd'+$$
$$(ab'+ba'+cd'-dc')i+(ac'+ca'+db'-bd')j+(ad'+da'+bc'-cb')k$$

[1]一般说加法群就是指交换群，加法幺元记作 0_R，或者在不引起歧义的前提下记作 0.
[2]记作 1_R，或者在不引起歧义的前提下记作 1.

称之为四元数环。实际上它就是一个除环，定义共轭

$$\overline{a+bi+cj+dk}=a-bi-cj-dk$$

则

$$(a+bi+cj+dk)(\overline{a+bi+cj+dk})=a^2+b^2+c^2+d^2=|a+bi+cj+dk|^2$$

于是

$$(a+bi+cj+dk)^{-1}=\frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$$

例 2.1.4 定义

$$\mathbb{H}'=\left\{\begin{pmatrix}\alpha & \beta\\ \overline{\beta} & \overline{\alpha}\end{pmatrix}:\alpha,\beta\in\mathbb{C}\right\}\subset M_2(\mathbb{C})$$

$\mathbb{H}'$ 在矩阵乘法下形成一个子环。

实际上存在一个 $\mathbb{H}$ 到 $\mathbb{H}'$ 的双射：

$$i\mapsto\begin{pmatrix}i & \\ & -i\end{pmatrix},j\mapsto\begin{pmatrix} & i\\ -i & \end{pmatrix},i\mapsto\begin{pmatrix} & i\\ i & \end{pmatrix},$$

$$a+bi+cj+dk\mapsto\begin{pmatrix}a+bi & c+di\\ -c+di & a-bi\end{pmatrix}$$

可以验证，这是一个“环同构”。

例 2.1.5 对于一个 R 环，可以定义一个多项式环：

$$R[x]=\{a_0+a_1x+a_2x^2+\cdots+a_nx^n:a_n\neq 0,\forall a_i\in R\}$$

需要强调的是，这里多项式的系数必须是有限项非零，作为区分，我们定义形式幂级数

$$R[[x]]=\{a_0+a_1x+a_2x^2+\cdots:\forall a_i\in R\}\cong R^{\mathbb{N}}$$

性质：R 含幺当且仅当 $R[x]$ 含幺当且仅当 $R[[x]]$ 含幺。

$\mathbb{F}$ 是一个域，对于 $\mathbb{F}[x]$ 中的元素：

$$a_0+\cdots+a_nx^n$$

可逆当且仅当 $a_1=\cdots=a_n=0,a_0\neq 0$. 而 $\mathbb{F}[[x]]$ 中的元素只需要保证常数项 $a_0\neq 0$ 即可，我们可以待定系数法逐项求出逆。一个例子是

$$(1-x)(1+x+x^2+\cdots)=1$$

对于一般的 $a_0+a_1x+a_2x^2+\cdots$，假设其逆为 $b_0+b_1x+b_2x^2+\cdots$，于是

$$(1+a_1x+a_2x^2+\cdots)(1+b_1x+b_2x^2+\cdots)=$$
$$1+(a_1+b_1)x+(a_2+b_2+a_1b_1)x^2+\cdots$$

$$\begin{aligned}b_1&=1-a_1\\ b_2&=1-a_2-a_1(1-a_1)\\ &\vdots\end{aligned}$$

定理 2.1.1 $\mathbb{F}$ 为域，$(M,\cdot)$ 是一个半群，则记

$$\mathbb{F}M=\{a_1m_1+a_2m_2+\cdots+:m_i\in M,a_i\in\mathbb{F},\forall i\}$$

即以 M 为基构成的向量空间。则 $\mathbb{F}M$ 是一个环。

特别地，$\mathbb{F}M$ 是含幺环 $\Leftrightarrow M$ 是含幺半群。

例 2.1.6 域 $\mathbb{F}$ 上的多项式环 $\mathbb{F}[x]$ 就是这种构造：

$$M=\{1,x,x^2,x^3,\cdots\}\cong\mathbb{N}$$

例 2.1.7 设 Q 是一个有向图，$\mathbb{F}$ 是域，$\mathbb{F}Q$ 是指以 Q 中所有道路为基的向量空间。这里 Q 上的道路乘法定义为：首尾相接，否则为零。

可以验证这样的道路乘法是满足结合律的，Q 构成一个半群。

那么什么时候 $\mathbb{F}Q$ 含幺呢？需要让每一条道路与之相乘都等于原来的道路，取 $1_{\mathbb{F}Q}$ 为所有顶点道路之和，每一条道路只有唯一的一个起点，所以右乘到 $1_{\mathbb{F}Q}$ 上等于自身，左乘同理（唯一终点）。因此 $\mathbb{F}Q$ 含幺 $\Leftrightarrow Q$ 有有限个顶点。

2.2 环的基本性质

定理 2.2.1 设 R 为环，则

(1) 0 是加法幺元，$0\cdot a=a\cdot 0=0$.

(2) $(na)b=n(ab)=a(nb)$，$n>0$ 时这里 na 定义为 n 个 a 相加，$n<0$ 则取负。

(3) 如果含幺环，$(-1)\cdot a=-a$.

(4)

$$\sum_{i=1}^{m}a_i\sum_{j=1}^{n}b_j=\sum_{i=1}^{m}\sum_{j=1}^{n}a_ia_j.$$

证明：

(1) $0\cdot a=(0+0)\cdot a=0\cdot a+0\cdot a\Rightarrow 0\cdot a=0$.

(2) $(a+a+\cdots a)b=(ab+ab+\cdots+ab)=a(b+b+\cdots+b)$.

(3) $(-1)\cdot a+a=(-1)\cdot a+1\cdot a=0\cdot a=0$.

(4) 分配律展开即可。

例 2.2.1 $x,y\in R,xy=yx\Rightarrow(x+y)^n=\sum_{k=0}^{n}C_n^kx^ky^{n-k}$.

$yx=q\cdot xy\Rightarrow(x+y)^n=\sum_{k=0}^{n}a_kx^ky^{n-k}$，系数 a_k 是多少呢？

定义 2.2.1 $0\neq a,b\in R$，若 $ab=0$，则称 a 是 R 的一个左零因子，b 是 R 的一个右零因子。既是左零因子，又是右零因子，则称之为零因子。

a 是左零因子 $\Leftrightarrow$

$$l_a:R\to R,x\mapsto ax,\mathrm{Ker}l_a\neq 0$$

定义 2.2.2 R 非平凡含幺环，存在 $ab=1$，称 b 左可逆，a 右可逆，a 是 b 的左逆元，b 是 a 的右逆元。

a 可逆即是指 a 左右可逆。

a 右可逆 $\Leftrightarrow 1\in\mathrm{Im}l_a\Leftrightarrow\mathrm{Im}l_a=R$，即 l_a 是满射

左零因子没有左逆，左可逆则不是左零因子。

$|R|<\infty$，含幺环，$a\in R$ 左可逆 $\Leftrightarrow$ 右可逆 $\Leftrightarrow l_a$ 双射 $\Leftrightarrow r_a$ 双射。

记 $u(R)=R^\times=\{a\in R:a\text{可逆}\}$，$R$ 中可逆元称为单位。

定义 2.2.3 若 R 是环，
(1) R 是含幺交换环且不含零因子（注意零元不是零因子），称之为整环。
(2) R 是含幺交换环且 $u(R) = R\backslash\{0\}$，即非零元可逆，称之为域。
(3) R 是含幺环且 $u(R) = R\backslash\{0\}$，称之为体，或者除环。

注： 有限整环 $\Rightarrow$ 域，有限体 $\Rightarrow$ 域。

例 2.2.2 $\mathbb{H}$ 和 $\mathbb{H}'$ 都是除环，不是域。

注： $\mathbb{R}, \mathbb{C}, \mathbb{H}$ 是 $\mathbb{R}$ 上所有的有限维可除代数。这里可除代数就是除环的意思。有时候不区分代数和环的概念，涉及到子环的概念之后，二者才需要区分。

定义 2.2.4 R 是环，$\varnothing \neq S \subset R$，若 S 在 R 上的加法和乘法下也构成环，则称之为 R 的一个子环。

S 是 R 的子环当且仅当 $(S, +)$ 是子群，$(S, \cdot)$ 是子半群。

子环的交仍是子环。

注： 如果 R 是含幺环，一般会要求其子环包含 1_R.

定义 2.2.5 代数一般要指明是什么上的代数，如 $\mathbb{F}$ 是域，环 R 是 $\mathbb{F}$ 上的线性空间，加法定义为线性空间上的自然加法，而要求乘法运算是双线性映射，此时称 R 是 $\mathbb{F}$ 上的代数。

定理 2.2.2 R 是环，在 $R \oplus \mathbb{Z}$ 上，我们希望定义一个新的乘法，使得 $(R \oplus \mathbb{Z}, \cdot)$ 为含幺环。我们定义为

$$(a, m)(b, n) = (ab + mb + na, mn)$$

幺元 $1 = (0, 1)$，$R \oplus \mathbb{Z}$ 包含 R 作为一个子环。

这个例子表明，环范畴和含幺环范畴是等价的。

定义 2.2.6 $(R_1 \times R_2, +, \cdot)$ 形成环，称为环 R_1 和 R_2 的乘积，记作 $R_1 \times R_2$.

$R_1 \times R_2$ 含幺当且仅当 R_1 和 R_2 都含幺。

类似定义多个环的乘积 $R_1 \times \cdots \times R_n$.

如果 $e_i \in Z(R)$，$e_i^2 = e_i$，$e_i e_j = 0 (\forall i \neq j)$，称之为中心幂等元。

定理 2.2.3 R 为含幺环，1_R 可以分解为若干中心幂等元的和：

$$1_R = e_1 + \cdots + e_n$$

则 $R = R_1 \times \cdots \times R_n$，$R_i = Re_i$.

2.3 环同态

定义 2.3.1 映射 $f : R \to T$ 称为环同态，如果

$$f(a + b) = f(a) + f(b), f(ab) = f(a)f(b)$$

即保持运算。进一步，如果 $f : 1_R \mapsto 1_T$，称之为含幺环同态。

单同态、满同态、同构，都是取决于加法群的。

例 2.3.1 有关 $\mathbb{H}$ 和 $\mathbb{H}'$ 的环同构，见例 2.1.4

例 2.3.2

$$f : M_n(R) \to M_{n+1}(R), A \mapsto \begin{pmatrix} A & \\ & 0 \end{pmatrix}$$

是一个环同态，但不是含幺环同态。

$$f : M_n(R) \times M_m(R) \to M_{n+m}(R), (A, B) \mapsto \begin{pmatrix} A & \\ & B \end{pmatrix}$$

是含幺环同态。

如果 S 是 R 的子环，恒等映射 $S \to R$ 是一个环同态。

例 2.3.3 R 是含幺环，则存在唯一的含幺环同态 $\varphi : \mathbb{Z} \to R$. 整数环可以由 1 生成，所以 $\varphi(1) = 1_R$.

而去掉含幺的条件就不唯一了。

注： $\forall e \in R, e^2 = e \Rightarrow$ 存在唯一环同态 $\varphi : \mathbb{Z} \to R$ 使得 $\varphi(1) = e$.

定义 2.3.2 R 的自同构群记作 $\mathrm{Aut}(R)$.

例 2.3.4 $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{Id}\}$，因为 $\mathbb{Z}$ 作为加法群，只有两个群同构：$1 \mapsto 1$ 和 $1 \mapsto -1$，而后者不是乘法半群同态。

$\mathrm{Aut}(\mathbb{Q})$ 如何？假设 $\varphi \in \mathrm{Aut}(\mathbb{Q})$，$\mathbb{Z}$ 作为 $\mathbb{Q}$ 的子环，φ 必须满足 $n \mapsto n, \forall n \in \mathbb{Z}$，进而也有

$$\varphi : \frac{n}{m} = \frac{1}{m} \cdot n \mapsto \frac{n}{m}$$

所以 $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{Id}\}$

$\mathrm{Aut}(\mathbb{R})$ 如何？$\varphi(1) = 1$，因为把幂等元映到幂等元，而 $\varphi(1)$ 显然不能等于 0，从而 $\varphi(p) = p, \forall p \in Q$，而

$$a > 0 \Rightarrow \varphi(a) = \varphi(\sqrt{a})^2 \geqslant 0$$

从而可知

$$\varphi(a - b) \geqslant 0, \forall a > b$$

从而

$$\varphi(a) \geqslant \varphi(b), \forall a > b$$

然而 $\varphi(a) \neq \varphi(b), a \neq b$，所以 φ 严格单调，又因为 $\varphi|_{\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$，根据有理数的稠密性可知，$\varphi$ 只能是恒等映射，即 $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{Id}\}$.

那么 $\mathrm{Aut}(\mathbb{C})$ 如何？详见域扩张的内容。

定义 2.3.3 R 是含幺环，我们知道只存在唯一的一个环同态：

$$\varphi : \mathbb{Z} \to \mathbb{R}, 1 \mapsto 1_R$$

如果存在一个 $n \geqslant 0$，使得 $\mathrm{Ker}\varphi = n\mathbb{Z}$，称为环 R 的特征，如果不存在，则称特征为 0.

$\mathrm{char}(R) = 0 \Rightarrow \varphi : \mathbb{Z} \hookrightarrow R$，$\mathrm{char}(R) = n \Rightarrow \varphi : \mathbb{Z}/_{n\mathbb{Z}} \hookrightarrow R$

注： 对于一个一般的环 R，其特征定义为使得 $nr = 0, \forall r \in R$ 成立的最小正整数 n，如果不存在，则称它的特征为 0. 一般这个概念不怎么用得上。

定理 2.3.1 R，R' 交换环，$\varphi : R \to R'$ 环同态，则
(1) $\forall \alpha' \in R'$，存在唯一的环同态：

$$\tilde{\varphi} : R[x] \to R'$$

$$\tilde{\varphi}|_R = \varphi, \varphi(x) = \alpha'.$$

(2) $\forall \alpha'_1, \cdots, \alpha'_n \in R'$，存在唯一环同态：

$$\tilde{\varphi} : R[x_1, \cdots, x_n] \to R'$$

$$\tilde{\varphi}|_R = \varphi, \varphi(x_i) = \alpha'_i, \forall i.$$

注： $\varphi : R \to R'$ 诱导出：

$$\tilde{\varphi} : R[x] \to R'[x], \sum a_i x^i \mapsto \sum \varphi(a_i) x^i$$

$\forall \alpha \in Z(R)$，定义映射：

$$ev_\alpha : R[x] \to R, f(x) \mapsto f(\alpha)$$

是一个环同态。

例 2.3.5 $\alpha \in \mathbb{C}$,

$$ev_\alpha : \mathbb{Z}[x] \to \mathbb{C}, f(x) \mapsto f(\alpha)$$

如果 $\mathrm{Ker}(ev_\alpha) = \{0\}$，即 α 不满足任何一个整系数方程的解，则称其是超越元，否则称之为代数元。

定义 2.3.4 R 是环，I 是其子环，满足：

$$xR, Rx \subset I, \forall x \in I$$

等价于：

$$\forall r \in R, i \in I, ri \in I, ir \in I$$

称 I 为 R 的一个理想，记作 $I \trianglelefteq R$.

例 2.3.6 $\mathbb{Z}$ 的子环是 $n\mathbb{Z}$，$n > 0$，就是一个理想。
$\mathbb{R}, \mathbb{Q}, \mathbb{C}$ 只有平凡理想。
环同态 $\varphi : R \to S$ 非零，即不把所有元素都映到零，则 $\mathrm{Ker}\varphi \trianglelefteq R$，且是真理想。

定义 2.3.5 $S \subset R$，记 $\langle S \rangle$ 为包含 S 的最小理想，称为 S 生成的理想。一个元素 a 生成的理想称为主理想，简记为 (a).
$\langle S \rangle = RS + SR + RSR$. 其中

$$RS = \left\{ \sum_{i=1}^{n} r_i s_i : n \geqslant q, r_i \in R, s_i \in S \right\}$$

定义 2.3.6 如果整环 R 中的理想均为主理想，则称 R 为主理想整环(principal ideal domain)，简称 PID.

例 2.3.7 $\mathbb{Z}$、域上的一元多项式环 $\mathbb{F}[x]$ 是 PID.

定义 2.3.7 I 是 R 的理想，则

$$\overline{R} = R/_I$$

唯一地诱导一个环结构，使得 $\pi : R \to \overline{R}, a \mapsto a + I = \overline{a}$ 是一个环同态。$\mathrm{Ker}\pi = I$. 此时 $\overline{R}$ 称为 R 对于理想 I 的商环。

理想正规子群吗？

例 2.3.8 $N \triangleleft G$，$\mathbb{F}$ 为域，我们考虑 $\mathbb{F}G$ 的一个子空间：

$$S = \{\sum_{g\in G} \lambda_g \cdot g : \sum_{g\in G} \lambda_g = 0\}$$

一组基是 $\{g - 1 : g \neq 1, g \in G\}$，$S$ 是 $\mathbb{F}G$ 的理想。

取 I 为 $\{n - 1 : n \in N\}$ 生成的理想，则

$$^{\mathbb{F}G}/_I \cong \mathbb{F}^G/_I$$

定理 2.3.2 环同态基本定理：$f : R \to R'$ 为环同态，则 $\mathrm{Ker}f \trianglelefteq R$，$\mathrm{Im}f \leqslant R'$, f 诱导了环同构：

$$R/\mathrm{Ker}f \cong \mathrm{Im}f$$

定理 2.3.3 J 是 R 的理想，$\overline{R} = R/J$，$\pi : R \to R'$ 环同态，则有

$$\{I \trianglelefteq R : I \supset J\} \leftrightarrow \{\overline{I} \trianglelefteq \overline{R}\}$$

一一对应。

$J \leqslant I \trianglelefteq R \Rightarrow I/J \trianglelefteq R/J$. 且 $(R/J)/(I/J) \cong R/I$.

例 2.3.9 高斯整环：$\mathbb{Z}[i]$，考虑元素 $1 + 3i$ 生成的主理想 $(1 + 3i)$，则

$$\mathbb{Z}[i]/(1 + 3i) \cong \mathbb{Z}/10\mathbb{Z}$$

证明： 构造映射

$$f : \mathbb{Z} \to \mathbb{Z}[i]/(1 + 3i)$$
$$n \mapsto \overline{n + (1 + 3i)}$$

先说明满射：$i \cdot (1 + 3i) = i - 3 \in I$，说明 $\overline{i} = \overline{3}$，所以 f 能映到生成元 $\overline{1}$ 和 $\overline{i}$，是满射；

再考虑 $\mathrm{Ker}f, n \in I \Rightarrow n = (1+3i)(a+bi) = a-3b+(3a+b)i \in \mathbb{Z} \Rightarrow b = -3a \Rightarrow n = 10a$，因此 $\mathrm{Ker}f = 10\mathbb{Z}$.

由环同态基本定理即得证。

例 2.3.10 R 是整环（含幺交换无零因子），如果存在环同态

$$\varphi : \mathbb{Z} \to R, n \mapsto n$$

则 $\mathrm{Ker}\varphi = (n), n \geqslant 0$. 这里的 n 就是特征。

如果特征不存在，则存在一个嵌入（单射）$\varphi : \mathbb{Z} \hookrightarrow R$. 特征为 n，存在嵌入 $\varphi : \mathbb{Z}/n\mathbb{Z} \hookrightarrow R$，它是群同态则必须要求 n 是素数，这意味着 $\mathbb{Z}/n\mathbb{Z}$ 是一个有限域。

例 2.3.11

$$I = \{(p(x), q(y)) : p(0) = q(0)\} \subset \mathbb{C}[x] \times \mathbb{C}[y]$$

即限制常数项一样的复数域上的多项式，不难验证 I 是一个子环。

$$\mathbb{C}[x, y]/(xy) \cong I$$

证明： 取映射：

$$\mathbb{C}[x, y] \to \mathbb{C}[x] \times \mathbb{C}[y]$$
$$f(x, y) \mapsto (f(x, 0), f(0, y))$$

于是 $\mathrm{Im}f = I$. 然后我们说明 $\mathrm{Ker}f = (xy)$，这是因为

$$f(x, y) \in \mathrm{Ker}f \Rightarrow f(x, 0) = f(0, y) = 0 \Rightarrow f(x, y) = g(xy)，\text{常数项为 } 0 \Rightarrow \mathrm{Ker}f = (xy)$$

例 2.3.12 R 交换环，$\mathrm{char}R = p$，p 素数，则

$$(x + y)^p = x^p + y^p$$

推论 2.3.1 R 整环，$\mathrm{char}(R) = p$ 为素数，则 $\sigma : R \to R, x \mapsto x^p$ 为单自同态。

证明： $x \in \mathrm{Ker}\sigma \Leftrightarrow x^p = 0$，所以 $x = 0$ 或 $x^{p-1} = 0$，递推之得 $x = 0$.

例 2.3.13 下面是一个环同构：

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

这是由阿贝尔群的结构自然得到的。

定理 2.3.4 (中国剩余定理) R 是含幺环，$I_1, \cdots, I_n$ 为 R 的两两互素的理想，即 $\forall I_i + I_j = R, i \neq j$. 则

$$R/(I_1 \cap \cdots \cap I_n) \cong R/I_1 \times \cdots \times R/I_n$$

证明： 先构造一个环同态：

$$f : R \to R/I_1 \times \cdots \times R/I_n, r \mapsto (r + I_1, \cdots, r + I_n)$$

$a \in \mathrm{Ker}f \Leftrightarrow a \in I_i, \forall i \Leftrightarrow a \in I_1 \cap \cdots \cap I_n$，于是 $\mathrm{Ker}f = I_1 \cap \cdots \cap I_n$，这时我们知道无论 I_i 是否两两互素，都有嵌入：

$$R/(I_1 \cap \cdots \cap I_n) \hookrightarrow R/I_1 \times \cdots \times R/I_n$$

然后我们来证明满射：设 $e_i = (\cdots, 1 + I_i, \cdots)$，其余为 0，那么 $\{e_i\}$ 是生成 $R/I_1 \times \cdots \times R/I_n$ 的，我们只需要证明 e_i 都有原像即可，不妨只考虑 e_1，求 $r_1 \in R$ 使得 $r_1 = 1(\mathrm{mod}\ I_1)$，$r_1 \in I_2 \cap \cdots \cap I_n$.

我们先证明：$I_1 + I_2 \cap \cdots I_n = R$，而 I_i 两两互素，

$$I_1 + I_j = R, j = 2, \cdots, n$$

$$R = (I_1 + I_2)(I_1 + I_3) \cdots (I_1 + I_n) \subset I_1 + I_2 \cap \cdots I_n$$

这里是因为，$(I_1 + I_2)(I_1 + I_3) \cdots (I_1 + I_n) = I_1(\cdots) + I_2 I_3 \cdots I_n \subset I_1 + I_2 \cap I_3 \cap \cdots \cap I_n$.

然后可知 $1_R = a + b, a \in I_1, b \in I_2 \cap \cdots I_n$，取 $e_i = 1_R - a$，

$$f(1_R - a) = (1 + I_1, 0, \cdots, 0)$$

e_i 同理，于是

$$\forall (a_1 + I_1, \cdots, a_n + I_n) = f(a_1 r_1 + \cdots + a_n r_n)$$

所以是满射。

2.4 整环和域

理想本质上是数的推广！本节内所有的 R 都是含幺交换环。

定义 2.4.1 $I \neq R$，$I \trianglelefteq R$，称 I 是 R 的素理想，如果 $\forall x, y \in R$，

$$xy \in I \Rightarrow x \in I \text{ or } y \in I$$

称 I 是 R 的极大理想，如果

$$\forall I \leqslant J \trianglelefteq R \Rightarrow J = R \text{ or } J = I$$

即真理想集合中的最大元。

素理想的等价定义：$I \neq R$，$I \trianglelefteq R$，R/I 是整环，即

$$\overline{xy} = 0 \Rightarrow \overline{x} = 0 \text{ or } \overline{y} = 0$$

极大理想的等价定义：$I \neq R$，$I \trianglelefteq R$，R/I 只有平凡理想。

例 2.4.1 $P \neq R$，$P \trianglelefteq R$，则下列说法等价：
(1) P 是素理想；
(2) 对于任意非空子集 $S_1, S_2 \subset R$，$S_1S_2 \subset R \Rightarrow S_1 \subset R$ or $S_2 \subset R$.
(3) R/P 是整环。

证明： 我们只说明 (1) $\Rightarrow$ (2)：$S_1S_2 \subset P$，假设 $S_1 \nsubseteq P$，$S_2 \nsubseteq P$，取 $x_1 \in S_1 \backslash P, x_2 \in S_2 \backslash P \Rightarrow x_1x_2 \in S_1S_2 \subset P, x_1x_2 \notin P$，矛盾。

例 2.4.2 $I \triangleleft R$，$I \subset P_1 \cup \cdots \cup P_n$，其中 P_i 是素理想，则存在 $I \subset P_i$.

证明： 假设这些 P_i 都不可去的，即

$$I \nsubseteq \bigcup_{j \neq i} P_i, \forall i$$

$$\Rightarrow \forall i, \exists x_i \in I \cap P_i \backslash \bigcup_{j \neq i} P_j$$

考虑 $x_1 + x_2 \cdots x_n \in I$，其中 $x_1 \in P_1$，且 $x_1 \notin P_2 \cap \cdots \cap P_n$; $x_2 \cdots x_n \in P_2 \cap \cdots \cap P_n$，且 $x_2 \cdots x_n \notin P_1$，因此 $x_1 + x_2 \cdots x_n \notin P_1$，这一步用到了素理想的性质。

例 2.4.3 事实上：如果含幺交换环 R 仅有平凡理想，则 R 是域。

$m \neq R$，$m \trianglelefteq R$，以下说法等价：
(1) m 是极大理想；
(2) R/m 为域。

注： 非交换不一定成立，例如 $R = M_2(\mathbb{R})$ 只有平凡理想，但它不是域。

R 为一般含幺环，则 $M_n(R)$ 的理想均具有 $M_n(I)$ 的形式，其中 I 是 R 的理想。

只有平凡理想的环叫做单环。不过本课程阶段我们不做研究。

推论 2.4.1 极大理想都是素理想。这是因为 m 极大 $\Rightarrow R/m$ 是域 $\Rightarrow R/m$ 是整环 $\Rightarrow m$ 素理想。

定义 2.4.2 $\max(R)$ 为全体极大理想集合，$\operatorname{spec}(R)$ 为全体素理想集合。

例 2.4.4 $\operatorname{spec}(\mathbb{Z}) = \{\{0\}, p\mathbb{Z} : p\text{素}\}$
$\max(\mathbb{Z}) = \{p\mathbb{Z} : p\text{素}\}$

例 2.4.5 $R = \mathbb{F}[x]$，$\operatorname{spec}(R) = \{\{0\}, (f(x)) : f(x)\text{不可约}\}$
$\max(R) = \{(f(x)) : f(x)\text{不可约}\}$

例 2.4.6 $\mathbb{Z}[x]$，它的一个素理想是 $(2, x)$，因为

$$\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/2\mathbb{Z}$$

也是极大理想。

定理 2.4.1 $I \neq R$，$I \trianglelefteq R$，则存在 R 的一个极大理想 m 使得 $I \subset m$.
等价形式：R/I 存在极大理想。

证明： 证明真理想集合满足 Zorn 引理的条件即可证明存在极大元。
令 $S = \{J \neq R, J \trianglelefteq R : I \subset J\}$，$S$ 在集合包含关系下为一个偏序集，满足 Zorn 引理条件，设 X 是 S 的一个全序子集，令

$$J = \bigcup_{L \in X} L \in S$$

为 X 的上界，所以 S 有极大元 m，即为所求极大理想。
这里 $J \neq R$，否则 $1 \in L$，进而 $L = R$，与 S 定义矛盾。

推论 2.4.2 R 含幺交换环 $\Rightarrow R$ 有极大理想、素理想。

定义 2.4.3 R 含幺，S 是非空子集，称之为乘法子集，如果满足：
(1) $1 \in S$.
(2) S 在乘法下封闭。

注： I 是 R 的素理想 $\Leftrightarrow R\backslash I$ 是一个乘法子群。

定理 2.4.2 R 是含幺环，有乘法子集 S，在 $R \times S$ 上定义等价关系：

$$(r_1, s_1) \sim (r_2, s_2) \Leftrightarrow \exists s \in S \text{ s, t. } r_1 s_2 s = r_2 s_1 s$$

如果 R 是整环则可以简化为 $r_1 s_2 = r_2 s_1$. 这是一个等价关系。
$R \times S/\sim$ 上可以定义环结构，记作 $S^{-1}R$，如下：
我们定义 $R \times S/\sim$ 上的运算：

$$[\frac{s_1}{r_1}] + [\frac{s_2}{r_2}] = [\frac{s_1 r_2 + s_2 r_1}{r_1 r_2}]$$

$$[\frac{s_1}{r_1}][\frac{s_2}{r_2}] = [\frac{s_1 s_2}{r_1 r_2}]$$

且
(1) $f : R \to S^{-1}R, r \mapsto [\frac{r}{1}]$ 为含幺环的嵌入。

(2) 对任一含幺环同态 $\varphi : R \to R'$ 且 $\varphi(S) \subset R'^{\times}$，则存在唯一的 $\tilde{\varphi} : S^{-1}R \to R'$ 使得 $\varphi = \tilde{\varphi} \circ f$.

证明： 由定义，(1) 是显然的，我们来说明一下 (2).

假如 $\tilde{\varphi}$ 存在，为了满足 $\varphi = \tilde{\varphi} \circ f$，$\tilde{\varphi}$ 只能把 $[\frac{r}{1}] \mapsto \varphi(r)$，$[\frac{1}{s}] \mapsto \varphi(s)^{-1}$，因此“我们没得选”[3]：

$$\tilde{\varphi} : S^{-1}R \to R', [\frac{r}{s}] \mapsto \varphi(r)\varphi(s)^{-1}$$

这就是我们对 $\tilde{\varphi}$ 的定义，验证良定，再说明这是一个环同态就好了。

定义 2.4.4 上面定理中定义的 $S^{-1}R$ 称为 R 对于乘法子集 S 的局部化，如果 $S = R\backslash P$，则 P 是素理想，称 $S^{-1}R$ 为 R 在 P 处的局部化，记作 R_P.

如果 R 是整环，$S = R\backslash\{0\}$，$S^{-1}R$ 是一个域。这被称为 R 的分式域，或者商域，记作 $Q(R)$.

例 2.4.7 整环 $\mathbb{Z}$，p 是素数，乘法子集 $S = \{1, p, p^2, \cdots\}$，

$$S^{-1}\mathbb{Z} = \{\frac{q}{p^i} : i \in \mathbb{N}, q \in \mathbb{Z}, (p, q) = 1\}$$

它是 $\mathbb{Q}$ 的一个子环。

整环 $\mathbb{Z}$，p 是素数，乘法子集 $S = \{n \in \mathbb{Z}_+ : (n, p) = 1\}$，

$$S^{-1}\mathbb{Z} = \{\frac{q}{n} : q \in \mathbb{Z}, (n, q) = 1\} = \mathbb{Z}_{(p)}$$

含幺环 $\mathbb{F}[x]$，乘法子集 $S = \{1, x, x^2, \cdots\}$，

$$S^{-1}\mathbb{F}[x] = \mathbb{F}[x, x^{-1}] \cong \mathbb{F}[x, y]/(xy - 1)$$

为什么同构呢？

[3]叶老师经典台词。

第三章　环的因子分解

3.1　唯一因子分解整环

定义 3.1.1 R 是含幺交换环，$a,b\in R$，$b=ax$，$a\neq 0$，则称 a 为 b 的一个因子，b 为 a 的一个倍元，记作 $a|b$.

如果 $a|b$ 且 $b|a$，称 a 与 b 相伴，记作 $a\sim b$.

如果 $b=ax$，$x\notin R^\times$，$a\neq 0$，则称 a 为 b 的真因子。

例如 $\mathbb{Z}$ 中 $6=2\times 3=-1\times -6$，2 就是真因子，因为 3 不可逆；-6 不是真因子，因为 -1 可逆。

命题 3.1.1 $a,b\in R\backslash\{0\}$，$u\in R^\times$，

(1) $a|b\Leftrightarrow (b)\subset (a)$，$a\sim b\Leftrightarrow (a)=(b)$.

(2) $u\sim 1$，u 为 r 的因子，$\forall r\in R$（即 $r=uu^{-1}r$）. 若 $r\notin R^\times$ 则 u 为 r 的真因子.

(3) $a=bu\Rightarrow a\sim b$. 若 R 为整环，则是等价的：$a=bu\Leftrightarrow a\sim b$.

(4) 若 R 是整环，则 a 为 b 的真因子 $\Leftrightarrow (b)\subsetneqq (a)$.

定义 3.1.2 $p\notin R^\times$，$p\neq 0$，若 p 是素数，则对于 $\forall a,b\in R, p|ab\Rightarrow p|a$ or $p|b$，则称 p 为素元。

$a\notin u(R)$，$a\neq 0$，$a=bc\Rightarrow b$ 为单位或 c 为单位，则称 a 为不可约元。

例 3.1.1 环 $\mathbb{Z}$，素元 = 不可约元 $=\pm p$，p 为素数。

环 $\mathbb{F}[x]$，素元 = 不可约元 = 不可约多项式。

环 $\mathbb{Z}[\sqrt{-3}]=\{a+b\sqrt{-3}:a,b\in\mathbb{Z}\}$，这是一个 $\mathbb{C}$ 的子环。在这个环内，$1+\sqrt{-3}$ 是一个不可约元，因为

$$|1+\sqrt{-3}|=2$$

如果它能写成两个元之积，那么这两个元之一必然模长为 1，$|a+b\sqrt{-3}|=\sqrt{a^2+3b^2}=1\Rightarrow a=\pm 1,b=0$，为单位。然而，$1+\sqrt{-3}|4=2\times 2, 1+\sqrt{3}\nmid 2$，这说明不可约元不一定是素元。

命题 3.1.2 R 是整环，$p,a\in R\backslash\{0\}$，则：

(1) p 是素元 $\Leftrightarrow (p)$ 是素理想。

(2) a 不可约 $\Leftrightarrow (a)$ 为非平凡主理想集合中的极大元，即极大主理想。

(3) 素元 $\Rightarrow$ 不可约。

(4) PID：不可约元 $\Rightarrow$ 素元。

证明： (1) p 素元：$p|ab\Rightarrow p|a$ 或 $p|b$，$p|ab\Leftrightarrow ab\in (p)$、$p|a\Leftrightarrow a\in (p)$、$p|b\Leftrightarrow b\in (p)$，所以 (p) 是素理想，(1) 得证。

(2) 若 $(a)\subset (d)$，则 $a=de$，然而 a 不可约，所以要么 $d\in R^\times$ 是单位，$(d)=R$，要么 $e\in R^\times\Rightarrow (a)=(d)$，即 a 为极大理想。反过来是一样的。

(3) 假定 $p=ab$，$p|a \Rightarrow a=pc \Rightarrow a=abc$，则 $bc=1$，$b\in R^\times$，同理 $p|b\Rightarrow a\in R^\times$，所以 p 不可约。
(4) 由 (2)，a 不可约 $\Rightarrow (a)$ 极大主理想，R 为主理想整环 $\Rightarrow (a)$ 是极大理想，极大理想都是素理想（推论 2.4.1），再由 (1) 知 a 是素元。

定义 3.1.3 设整环 R 满足
(UF1) $\forall a\in R\backslash R^\times a\neq 0$，存在分解 $a=c_1\cdots c_n$，其中 c_i 是不可约元。即，任何一个不可逆元，都可以写成若干个不可约元的乘积。
(UF2) 上述分解是唯一的：$a=c_1\cdots c_n=b_1\cdots b_m$，则 $m=n$，且存在某一个置换 $\sigma\in S_n$，使得 $c_i\sim d_{\sigma(i)}$.
满足上述性质，称 R 为唯一因子分解整环 (uniquely factorial domain)，简称为 UFD.

注： 在 (UF2) 中，n 由 a 唯一确定，记作 $l(a)$. 对于可逆元 a，规定 $l(a)=0$.

例 3.1.2 以下是两个分别不满足 (UF1) 和 (UF2) 的例子。
$\mathbb{F}[x_1,x_2,\cdots]$，规定 $x_2^2=x_1,x_3^2=x_2,\cdots,x_{n+1}^2=x_n$，从而

$$x_1=x_2^2=x_3^4=\cdots$$

x_1 的分解不存在。
$\mathbb{Z}[\sqrt{-5}]$，$6=(1+\sqrt{-5})(1-\sqrt{-5})=2\times 3$，分解不唯一。

定义 3.1.4 R 含幺交换环，$a,b\in R$，$(a,b)\neq(0,0)$，若存在 $d\in R$，使得
(1) $d|a,d|b$，即公因子；
(2) $\forall d'|a,d'|b\Rightarrow d'|d$.
则称 d 为 a,b 的最大公因子，记作 $\gcd(a,b)$ 或者 (a,b).
同理可以定义最小公倍数，记作 $\mathrm{lcm}(a,b)$ 或者 $[a,b]$.

注： 最大公因子是可以不存在的，也可以不唯一。如果不唯一，则一定相伴，或者说相伴意义下是存在则唯一的。所以我们常常写

$$(a,b)\sim d$$

注意 $(a)+(b)=(d)\Rightarrow (a,b)\sim d$，这是最大公因子存在的一个充分条件。

例 3.1.3 $\mathbb{Z}$ 里 1 和 2 的最大公因子可以是 1 也可以是 -1.

引理 3.1.1 R 是整环，最大公因子存在，$a,b,c\in R\backslash\{0\}$，$u\in R^\times$，则
(1) $(u,a)\sim 1$.
(2) $(a,(b,c))\sim((a,b),c)$，因此我们可以定义三个元素的最大公因子。
(3) $c\cdot(a,b)\sim(ca,cb)$.
(4) $(a,b)\sim 1,(a,c)\sim 1\Rightarrow(a,bc)\sim 1$.

证明： 其实都是在拿定义倒来倒去。
(1) 可逆元只有平凡因子。
(2) 我们尝试证明 $(a,(b,c))|((a,b),c)$，最大公因子的定义告诉我们，它等价于

$$(a,(b,c))|(a,b),(a,(b,c))|c$$

等价于

$$(a,(b,c))|a,(a,(b,c))|b,(a,(b,c))|c$$

这仨式子都是显然的；反过来证法一样。

(3) 由于 $(a,b)|a$ 且 $(a,b)|b$，所以 $c(a,b)|ca$，$c(a,b)|cb$，所以 $c\cdot(a,b)|(ca,cb)$；$c|ca, c|cb \to c|(ca,cb)$，设 $(ca,cb)=cd$，所以我们只需证明 $d|(a,b)$，即 $d|a, d|b$，由于 $cd|ca, cd|cb$，所以 $d|a, d|b$，于是得证。
(4) $(a,bc)|((a,ac),bc)\sim(a,(ac,bc))\sim(a,c(a,b))\sim(a,c)\sim 1$. 于是 $(a,bc)\sim 1$.

定理 3.1.1 R 是 UFD，则：
(1) 诺特性：主理想升链稳定，即：如果

$$(a_1)\subset(a_2)\subset\cdots\subset(a_n)\subset\cdots$$

则存在 N，使得 $(a_N)=(a_{N+1})=\cdots$
(2) R 上不可约元是素元。
(3) $\forall a,b$ 不全为零，则最大公因子存在。

证明： (1) 因为这个过程相当于不断取 a_1 的真因子，由 UFD 的定义知这个过程是有限的，自然主理想升链不能永远升上去。下面是完整证明：
不妨 $l(a_1)=n\geqslant 1$，否则 $(a_1)=R$. 则一定存在且仅存在 $a_{i_1},\cdots,a_{i_n}$ 使得

$$(a_{i_1})\subsetneqq(a_{i_1+1}),\cdots,(a_{i_n})\subsetneqq(a_{i_n+1})$$

这意味着取 $N=i_n+1$ 即可。这意味着理想升链中的不等号不超过 $l(a_1)$.
(2) 设 a 不可约，$a=bc\Rightarrow b\in R^\times$ 或 $c\in R^\times$，如果 $a|bc$，设 $b=b_1\cdots b_n$，$c=c_1\cdots c_m$，则 $bc=b_1\cdots b_nc_1\cdots c_m$，从而

$$bvc=ad=ad_1\cdots d_l=b_1\cdots b_nc_1\cdots c_m$$

由分解的唯一性，要么 $a\sim b_i$，要么 $a\sim d_j$，进而 $a|b$ 或者 $a|c$，说明 a 是素元。
(3) 我们把 a,b 写成下面这种形式：

$$a\sim p_1^{m_1}\cdots p_l^{m_l}$$
$$b\sim p_1^{n_1}\cdots p_l^{n_l}$$

取

$$(a,b)\sim p_1^{\min(n_1,m_1)}\cdots p_l^{\min(n_l,m_l)}$$

即可！

定理 3.1.2 定理 3.1.1 里，UFD$\Leftrightarrow$ (1) + (2) $\Leftrightarrow$ (1) + (3).

证明： (1) + (3) $\Rightarrow$ (1) + (2)：a 不可约，则 $(a,d)\sim 1\Leftrightarrow a\nmid d$，因此：$a\nmid b, a\nmid c\Rightarrow(a,b)\sim 1,(a,c)\sim 1\Rightarrow(a,bc)\sim 1\Rightarrow a\nmid bc$.
(1) + (2) $\Rightarrow$ 定理 3.1.1：见下图，有空回来补。

例 3.1.4 $\mathbb{Z}$ 和 $\mathbb{F}[x]$ 都是 UFD.
R 是 UFD 则 $R[x]$ 也是 UFD

定义 3.1.5 R 为整环，若存在

$$\varphi: R\to\mathbb{N},\varphi(r)=0\Leftrightarrow r=0$$

或者干脆 $\varphi: R\backslash\{0\}\to\mathbb{Z}_+$. 若对于 $\forall a,b\in R, a\neq 0$，存在 $q,r\in R$ 使得 $b=qa+r$，不要求唯一，使得 $\varphi(r)<\varphi(a)$，称 R 是一个欧式整环，(Euclideee? domain)，简称为 ED.

例 3.1.5 $\mathbb{Z}$，取 φ 为绝对值函数。

$\mathbb{F}[x]$，取 φ 为 deg.

$\mathbb{Z}[\sqrt{-1}]=\{a+b\sqrt{-1}\}$，叫高斯整环，证明后来再说。可能让助教在习题课上讲一讲。

命题 3.1.3 ED⇒PID⇒UFD.

证明： 设 R 是欧式整环，I 是其理想，取 $r\in R\backslash\{0\}$，使得 $\varphi(r)$ 最小，则 $I=(r)$. 为什么呢？这是因为 I 里的元素都得被 r 整除，否则有余数，这个余数 r_0 使得 $\varphi(r_0)<\varphi(r)$，导致矛盾。从而可知 R 是主理想整环。

设 R 是主理想整环，我们假设它上有主理想升链：

$$(a_1)\subset(a_2)\subset\cdots$$

则 $I=\bigcup_{n=1}^{i}(a_n)$ 也是一个理想，一定被某个元素 a 生成，于是 $a\in(a_i),\exists i$. 这里应该是推出来了 (1) 了吧？而且主理想整环的不可约元一定是素元，推出了 (3).

命题 3.1.4 D 是 UFD⇒ $D[x]$ 也是 UFD

3.2 高斯整数环与 2 平方和问题

跳过了，说是习题课讲了？

3.3 多项式环

定义 3.3.1 R 是含幺环，$f(x)\in R[x]$ 可以写成：

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0,a_n\neq 0$$

称 n 为次数，a_nx^n 为首项，a_n 为首项系数。

两个多项式相等，当且仅当次数相同且各项系数相同。

引理 3.3.1

$$\deg(f(x)+g(x))\leqslant\max\{\mathrm{def}(f(x)),\mathrm{def}(g(x))\}$$

$$\deg(f(x)g(x))\leqslant\deg(f(x))+\deg(g(x))$$

若 $f(x)$（或 $g(x)$）首项系数不为左（右）零因子，则第二个不等式等号成立。特别地，若 R 是整环，则等号恒成立。

注： 约定 $\deg(0)=-\infty$.

引理 3.3.2 $R[x]$ 是整环 $\Leftrightarrow$ R 是整环，且此时 $R[x]^\times=R^\times$.

注： R 不是整环，则 $R[x]^\times=R^\times$ 一般不成立。

引理 3.3.3 $g(x)$ 首项系数是 R 中的可逆元，则存在唯一的 $q(x),r(x)$ 使得 $f(x)=q(x)g(x)+r(x)$，且 $\deg r(x)<\deg g(x)$.

引理 3.3.4 $f(x)\in R[x], c\in R$，存在唯一 $q(x)$ 使得 $f(x)=q(x)(x-c)+f(c)$，由于 R 不一定是交换环，约定代入值的方式是 $f(c)=a_nc^n+\cdots+a_1c+a_0$.

特别地，R 是含幺交换环时，$f(c)=0\Leftrightarrow x-c|f(x)$.

注： 假定 $h(x)=f(x)g(x)$，并不一定成立 $h(c)=f(c)g(c)$，不交换的情况下，

$$h(c)=\sum_{l=0}^{\infty}\sum_{i=0}^{\infty}a_ib_{l-i}c^l$$

$$f(c)g(c)=\sum_{l=0}^{\infty}\sum_{i=0}^{\infty}a_ic^ib_{l-i}c^{l-i}$$

不一定相等，因为一个是先相乘再赋值，一个是先赋值再相乘。如果 $g(x)$ 的系数与 x 可交换，二者相等。

推论 3.3.1 $0\neq f(x)\in R[x]$，$E\supset R$ 为整环（于是 R 也是整环），则 $f(x)=0$ 在 E 中，最多有 $\deg f(x)$ 个互不相同的根。

特别地，令 $K=Q(E)$ 为 E 的商域，于是 $f(x)\in R[x]\subset E[x]\subset K[x]$，于是 $f(x)$ 在 K 上至多存在 $\deg f(x)$ 个互不相同的根。

证明： 设 $\alpha_1,\cdots,\alpha_m$ 是 $f(x)$ 在 E 中的互不相同的根，设 $f_1(x)$ 满足：

$$f(x)=(x-\alpha_1)f_1(x)+f(\alpha_1)=(x-\alpha_1)f_1(x)$$

于是 α_2 是 $f_1(x)$ 的根，以此类推可得

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_m)f_m(x)$$

于是 $\deg f(x)\geqslant m$.

例 3.3.1 不是整环不一定成立，例如四元数体 $\mathbb{H}$，考察 $x^2+1\in\mathbb{H}[x]$，它有无穷多个根，这是因为

$$(ai+bj+ck)^2=-(a^2+b^2+c^2)$$

只要 $a^2+b^2+c^2=1$，$ai+bj+ck$ 就是一个根。

定义 3.3.2 R 是含幺交换环，$0\neq f(x)\in R[x]$，设 c 为 $f(x)$ 的 n 重根，如果满足存在 $g(x)\in R[x]$ 使得 $f(x)=(x-c)^ng(x)$，且 $g(c)\neq 0$.

我们可以定义多项式的形式微商：$f(x)=a_nx^n+\cdots+a_1x+a_0$，$f'(x)=na_nx^{n-1}+\cdots+a_1$.

定理 3.3.1 整环 $D\subset E$，$f(x)\in D[x]$，$c\in E$，

(1) c 为 $f(x)$ 的 n 重根 $\Rightarrow f(c)=f'(c)=\cdots=f^{(n-1)}(c)=0$.

(2) $\mathrm{char}(D)=0$，上式为当且仅当。

(3) D 为域，则 $(f,f')=1\Rightarrow f(x)$ 在 E 中无重根。

证明： (1) 由定义，$f(x)=(x-c)^ng(x)$，$f'(x)=(x-c)^{n-1}(ng(x)+g'(x)(x-c))$，于是 c 是 $f'(x)$ 的至少 $n-1$ 重根。

(2) $\mathrm{char}(D)=0$，意味着 $ng(x)+g'(x)(x-c)|_{x=c}=ng(c)\neq 0$，于是 c 恰好是 $f'(x)$ 的 $n-1$ 重根。
(3) D 为域，$(f,f')=1\Rightarrow f(x)g(x)+f'(x)h(x)=1$，若 c 为 $f(x)$ 在 E 中的 n 重根，于是 $f(x)=(x-c)^n f_1(x)$，这里 $f_1(x)\in E[x]$，于是 $f'(x)$ 和 $f(x)$ 在 $E[x]$ 由公因子 $x-c$，这与 $f(x)g(x)+f'(x)h(x)=1$ 矛盾，因为这意味着 1 在 $E[x]$ 中能被 $x-c$ 整除，这就矛盾。

定义 3.3.3 D 是 UFD，$0\neq f(x)=a_nx^n+\cdots+a_0\in D[x]$，称 $\gcd(a_0,a_1,\cdots,a_n)$ 为 $f(x)$ 的容积，记作 $c(f)$.

若 $c(f)\sim 1$，则称 $f(x)$ 是一个本原多项式。

注： $f(x)=c(f)h(x)$，$h(x)$ 就是一个本原多项式。而且 $h(x)$ 相伴意义下唯一。

引理 3.3.5 (Gauss 引理) 本原多项式的乘积还是本原多项式，等价于 $c(fg)=c(f)c(g)$.

证明：

命题 3.3.1 任意 $f(x)\in K[x]$，存在 $c,d\in D,d\neq 0$，和本原多项式 $f_1(x)\in D[x]$ 满足 $f(x)=\frac{c}{d}f_1(x)$，且 $f_1(x)$ 在相伴意义下唯一。

证明： 那么对于一个 $K[x]$ 中的多项式 $f(x)=\frac{q_n}{p_n}x^n+\cdots+\frac{q_0}{p_0}$，有：

$$f(x)=\frac{1}{p_1p_2\cdots p_n}(b_nx^n+\cdots+b_0)$$

然后再把后面那个多项式变成本原多项式：

$$f(x)=\frac{(b_0,\cdots,b_n)}{p_1p_2\cdots p_n}f_1(x)$$

即可。

唯一性：如果

$$f(x)=\frac{c_1}{d_1}f_1(x)=\frac{c_2}{d_2}f_2(x)$$

则 $c_1d_2f_1(x)=c_2d_1f_2(x)$，两边取容积，得到 $c_1d_2\sim c_2d_1$，因此 $f_1(x)\sim f_2(x)$.

注： 上述命题表示：$K[x]$ 中多项式等价类，与 $D[x]$ 中本原多项式一一对应。

引理 3.3.6 D 是 UFD，K 是其商域，$f(x),g(x)\in D[x]$ 为本原多项式，则在 $D[x]$ 上 $f\sim g$ 当且仅当在 $K[x]$ 上 $f\sim g$.

引理 3.3.7 $f(x)$ 在 $D[x]$ 中不可约 $\Leftrightarrow$ 下列情形之一：
(1) $f(x)=p\in D$，p 是 D 中的不可约元。
(2) $f(x)$ 是本原多项式，且在 $K[x]$ 中不可约。

证明： 必要性：设 $f(x)\in D[x]$ 且不可约，如果 $\deg f(x)=0$，设 $f(x)=p$，则 p 在 D 中不可约，否则存在 $p=p_1p_2$，p_1 和 p_2 同样属于 $D[x]$，这与 $f(x)$ 不可约矛盾；如果 $\deg f(x)>0$，设 $f(x)=c(f)f_1(x)$，则必须有 $c(f)\in D^\times$，因为 $f_1(x)$ 不是可逆元，因此 $f(x)$ 是本原多项式。假设有非平凡分解 $f(x)=g(x)h(x)$，其中 $g(x),h(x)\in K[x]$，且次数不小于 1，于是

$$f(x)=\frac{c}{d}g_1(x)h_1(x)$$

这里 g_1,h_1 是 $D[x]$ 上的本原多项式，这就得到 $df(x)=cg_1(x)h_1(x)$，两边取容积，得到 $c\sim d$，于是 $f(x)\sim g_1(x)h_1(x)\in D[x]$，这就意味着 $f(x)$ 在 $D[x]$ 上可约，矛盾。

充分性：反过来证法一样。

定理 3.3.2 D 是 UFD$\Rightarrow D[x]$ 为 UFD.

证明： 分解存在性：若 $\deg f(x)=0$，则 $f(x)\in D$ 可知分解存在；若 $\deg f(x)>0$，由于 $K[x]$ 是一个 UFD，所以它可以分解为

$$\begin{aligned} f(x) &= g_1(x)\cdots g_s(x) \\ &= \frac{c}{d}f_1(x)\cdots f_s(x) \end{aligned}$$

这里 $g_i(x)\in K[x]$ 不可约，$f_i(x)\in D[x]$ 是本原多项式，于是 $df(x)=cf_1(x)\cdots f_s(s)$，两边取容积可得 $d\cdot c(f)=c$，于是 $d|c$，$\frac{c}{d}\in D$. 于是存在性得证。

分解唯一性：假定存在两个分解：

$$f(x)=a_1\cdots a_r f_1(x)\cdots f_s(x)=b_1\cdots b_m g_1(x)\cdots g_n(x)$$

因为 $K[x]$ 是一个 UFD，$f(x)$ 在 $K[x]$ 上的分解是唯一的，分成两部分，多项式部分是唯一的。然后因为 D 是 UFD，前面的系数分解也是唯一的。

定理 3.3.3 (Eisenstein 判别法) $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in D[x]$，$D$ 是 UFD，若存在 D 中的不可约元 p，使得 $p|a_{n-1},\cdots,p|a_1,p|a_0$，且 $p^2\nmid a_0$，则 $f(x)$ 不可约。

证明： 假设 $f(x)=g(x)h(x)$，并设 $g(x)=b_mx^m+\cdots+b_1x+b_0$，$h(x)=c_kx^k+\cdots+c_1x+c_0$，这里 $k=n-m$. 由题设可知，$p|b_0c_0$，$p^2\nmid b_0c_0$，这表明 p 只能整除 b_0 和 c_0 的其中一个，不妨设 $p|b_0$ 且 $p\nmid c_0$，取 i 使得：

$$p|b_0,p|b_1,\cdots,p|b_{i-1},p\nmid b_i$$

于是

$$a_i=b_0c_i+b_1c_{i-1}+\cdots+b_ic_0$$

除了最后一项，其余都能被 p 整除，于是 $p\nmid a_i$，这里的 $i\leqslant m<n$，这就产生矛盾。

例 3.3.2 取 $D=\mathbb{Z}$，p 是素元，即素数，取满同态 $\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z}=\mathbb{F}_p$，诱导多项式环的满同态 $\mathbb{Z}[x]\to\mathbb{F}_p[x]$.

那么，如果 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，$p|a_{n-1},\cdots,p|a_1,p|a_0$，则 $f(x)\mapsto\overline{f}(x)=x^n$，因此如果 $f(x)$ 可约，$f(x)=g(x)h(x)$，$\overline{f}(x)=\overline{g}(x)\overline{h}(x)$，不妨设 $\overline{g}(x)=x^m,\overline{h}(x)=x^{n-m}$，于是其余项系数 $b_i,c_j\in p\mathbb{Z}$，特别地 $p|b_0,p|c_0\Rightarrow p^2|b_0c_0=a_0$，矛盾。

例 3.3.3 $f(x)=1+x+\cdots+x^{p-1}\in\mathbb{Z}[x]$，$p$ 是素数，这被称为一个分圆多项式。

注意到

$$f(x)=\frac{x^p-1}{x-1}$$

令 $y=x+1$，$g(y)=\frac{(y+1)^p-1}{y}=y^{p-1}+py^{y-2}+\cdots+p$，这就是一个满足 Eisenstein 判别法的多项式，它是不可约多项式，进而 $f(x)$ 也是不可约多项式。

第四章　域扩张

4.1　域扩张的基本概念

定义 4.1.1 设 F 是一个域，首先它是一个环，考虑它的特征 $\mathrm{char}(F)$：如果为零，则 $\mathbb{Z}\to F$ 是一个嵌入，于是作局部化，自然地得到 $\mathbb{Q}\to F$ 的嵌入，也可以直接定义 $\frac{n}{m}\mapsto nm^{-1}$，实际上因为域没有非平凡理想，域之间的同态一定是嵌入；如果为 p，$\mathbb{Z}/p\mathbb{Z}\to F$ 是一个嵌入，$\mathbb{Z}/p\mathbb{Z}$ 就是一个域，常常记作 $\mathbb{F}_p$.

定义 4.1.2 子域 $F\subset K$，则称 K 为 F 的一个域扩张，记作 K/E. 记 $F(\alpha)$ 为 K 中包含 F 以及 α 的最小子域，也叫 α 生成的子域；$F(S)$ 为 K 中包含 F 以及 S 的最小子域，也叫 S 生成的子域。

实际上：

$$F(S)=\left\{\frac{p(\alpha_1,\cdots,\alpha_n)}{q(\alpha_1,\cdots,\alpha_n)}|p(x_1,\cdots,x_n),q(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n],\alpha_i\in S,n\geqslant 1\right\}$$

即所有可能的有理函数。特别地

$$F(\alpha)=\left\{\frac{f(\alpha)}{g(\alpha)}|f(x),g(x)\in E[x],g(\alpha)\neq 0\right\}$$

这就是单扩张。

定义 4.1.3 K/E，$\alpha\in K$，取赋值映射：$\mathrm{ev}_\alpha:E[x]\to K,f(x)\mapsto f(\alpha)$，这是一个环同态。那么环同态基本定理告诉我们：$\mathrm{Ker}(\mathrm{ev}_\alpha)$ 是一个理想，而且

$$E[x]/\mathrm{Ker}(\mathrm{ev}_\alpha)\cong\mathrm{Im}(\mathrm{ev}_\alpha)$$

$\mathrm{Im}(\mathrm{ev}_\alpha)$ 是 K 的子环，于是是整环，这就说明 $\mathrm{Ker}(\mathrm{ev}_\alpha)$ 是一个素理想。若 $\mathrm{Ker}(\mathrm{ev}_\alpha)=(p(x))$，$p(x)$ 是一个不可约多项式，这时称 α 为一个代数元；或者是一个零理想，$\mathrm{Ker}(\mathrm{ev}_\alpha)=0$，这意味着多项式环 $E[x]$ 可以嵌入 K 作为一个子环，进而 $E[x]$ 的商域可以嵌入进 K，这时称 α 为一个超越元。

命题 4.1.1 K/E，$\alpha\in K$，α 是 E 上的超越元，则

$$E(\alpha)\cong E(x)=Q(E[x])=\left\{\frac{f(x)}{g(x)}|f(x),g(x)\in E[x],g(\alpha)\neq 0\right\}$$

即：$\tilde{\mathrm{ev}}_\alpha:E(x)\to K,\frac{f(x)}{g(x)}\mapsto f(\alpha)g(\alpha)^{-1}$.

如果 α 是 E 上的代数元，则 $E(\alpha)=E[\alpha]\cong E[x]/(p(x))$，这里的 $p(x)=\mathrm{Ker}(\mathrm{ev}_\alpha)$ 称为 α 的极小多项式。

证明： 只证明一下代数元的情况。首先我们知道 α 在 $E[\alpha]$ 中是可逆的，实际上我们有如下刻画：$\beta \in K$，β 在 E 上代数 $\Leftrightarrow \dim_E E[\beta] < \infty$，即 $E[\beta]$ 作为一个向量空间一定是有限维的。

必要性：$\beta^m = b_{m-1}\beta^{m-1} + \cdots + b_1\beta + b_0$，于是任何一个高于 m 次的方幂都可以通过这个等式“降次”，从而 $\{1, \beta, \cdots, \beta^{m-1}\}$ 线性张成整个 $E[\beta]$；充分性：如果有限维，不妨设 m 维，则意味着 $\{1, \beta, \beta^2, \cdots, \beta^m\}$ 一定是线性相关的。

注： 设 $p(\alpha) = \alpha^n + \cdots + a_1\alpha + a_0$，必须有 $a_0 \neq 0$，否则 $p(\alpha) = \alpha q(\alpha)$，矛盾。

定义 4.1.4 K/E，K 可以自然的看成 E 上的向量空间，例如 $\mathbb{C}$ 是二维的 $\mathbb{R}$ 上的向量空间。于是称 $\dim_E K$ 为 K/E 的扩张次数，记作 $[K : E]$.

命题 4.1.2 α 在 E 上代数，$f(x)$ 是 α 的极小多项式，则 $[E(\alpha) : E] = \deg f(x) = m$，并且 $1, \alpha, \cdots, \alpha^{m-1}$ 是 $E(\alpha)$ 的一组 E-基。

反之，若 $[E(\alpha) : E] < \infty$，则 α 在 E 上代数。

定理 4.1.1 $K/M/E$，则 $[K : E] = [K : M][M : E]$.

证明： 有限的情况下，

$$M = E_{\alpha_1} \oplus \cdots \oplus E_{\alpha_n}$$
$$K = M_{\beta_1} \oplus \cdots \oplus M_{\beta_m}$$

自然就 $K = \bigoplus_{i,j} E_{\beta_i \alpha_j}$.

无限的情况也是成立的，写出指标集即可。

推论 4.1.1 K/E，$[K : E] = n$，$\forall \alpha \in K$，α 是代数元，而且其极小多项式的次数一定是 n 的因子。特别地，如果 $n = p$ 是素数，那么 $\forall \alpha \in K \backslash E$，则只能 $E(\alpha) = K$

命题 4.1.3 有限扩张 $\Leftrightarrow$ 有限生成代数扩张。

有限生成代数扩张，是指形如 $E(\alpha_1, \cdots, \alpha_n)$ 的扩张，其中生成元都是代数元，而且个数有限。

命题 4.1.4 K/M，M/F 都是代数扩张，即 $\forall \alpha \in K$，α 在 M 上是代数元。

$\Leftrightarrow K/F$ 是代数扩张。

证明： 充分性显然，因为 $F[x] \subset M[x]$.

必要性则比较麻烦，设 $\forall \alpha \in K$，则存在某个首一多项式 $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in M[x]$，使得 $p(\alpha) = 0$，这就意味着 α 在 $F(a_0, a_1, \cdots, a_{n-1})$ 上是代数的，于是

$$[F(a_0, a_1, \cdots, a_{n-1}, \alpha) : F] \leqslant n \cdot [F(a_1, \cdots, a_{n-1}) : F] < \infty$$

这里是因为 $[F(a_0, a_1, \cdots, a_{n-1}, \alpha) : F(a_0, a_1, \cdots, a_{n-1})]$ 是不大于 n 的。

证明出 $[F(a_0, a_1, \cdots, a_{n-1}, \alpha) : F]$ 是有限的，则 α 一定是代数的。

定义 4.1.5 K/E，则 K 中所有在 E 上代数的元素构成的集合，构成 K 的一个子域，称为 E 在 K 中的代数闭包。

为什么一定构成子域？设 $\alpha, \beta \in K$ 在 E 上代数，只需说明：$\alpha \pm \beta, \alpha\beta, \alpha^{-1}$ 在 E 上代数。α^{-1} 是显然的，这是因为把化零多项式同时除一个 α 的方幂即可；对于 $\alpha \pm \beta$，只需说明 $E(\alpha, \beta)$ 是代数扩张，而 $[E(\alpha, \beta) : E(\alpha)]$ 一定小于等于 $[E(\beta) : E]$，因此 $[E(\alpha, \beta) : E]$ 是有限的。

定义 4.1.6 称 E 为代数闭域, 如果 E 不存在非平凡的有限扩张, 即 $[K:E]<\infty \Rightarrow K=E$; 或等价地, E 上任意非常值多项式在 E 中必有根, 即 E 上的不可约多项式只能是一次的。记作 $E=\overline{E}$.

简单解释一下这几件事情是等价的: 假定 $f(x)$ 是一个首一的不可约多项式, 考察环 $E[x]/(f(x))$, 这是 E 的一个扩张, 如果 E 不存在非平凡的有限扩张, 这就说明 $E[x]/(f(x))=E$, 这意味着 $\deg f(x)=[E[x]/(f(x)):E]=1$, 即不可约多项式都是一次的。反之, 若 E 上不可约多项式都是一次的, 那么假定某个 $[K:E]<\infty$, 任取 $\alpha\in K$, α 的极小多项式是不可约多项式, 进而一定是一次的, 这意味着 $\alpha\in E$, 即 $K=E$.

如果 K/E 是代数扩张, K 是代数闭域, 称 K 为 E 的代数闭包, 记作 $K=\overline{E}$.

定理 4.1.2 $\overline{F}$ 存在且唯一。

例 4.1.1 例如 $\overline{\mathbb{Q}}$ 为全体代数数, $\overline{\mathbb{R}}=\mathbb{C}$.

定理 4.1.3 代数学基本定理: $\mathbb{C}=\overline{\mathbb{C}}$.

4.2 有限域

求 $G=\langle a,b|a^4=b^7=1, ab=ba^3\rangle$ 的阶数。

$ab=ba^3\Rightarrow aba=b\Rightarrow ababa=b^2a=ab^2$，即 a 与 b^2 可交换，于是

$$ab^m=b^2ab^{m-2}=\cdots=\begin{cases} b^ma & ,m\text{偶} \\ b^ma^3 & ,m \end{cases}$$