代数学笔记

群、环、模、域、Galois 理论

作者：Galois 爱求五次根

组织：深北莫代数分析小组

时间：2022/9/19

不要以为抹消过去，重新来过，即可发生什么改变。——比企谷八幡

目录

第 1 章 群

1.1 基本概念

1.1.1 群公理化

定义 1.1 (群第一公理化)

利用下面四条性质可以公理化定义群:

G1: (二元运算存在性) $(\exists \perp : G \times G \to G)(\forall a, b \in G)(\exists! c \in G) : (c = a \perp b)$

G2: (结合性) $(\forall a, b, c \in G) : a \perp (b \perp c) = (a \perp b) \perp c$

G3: (左中性元存在性) $(\exists e \in G)(\forall a \in G) : e \perp a = a$

G4: (左对称元存在性) $(\forall a \in G)(\exists b \in G) : b \perp a = e$

称满足 **G1G2** 的集合 G 与其上给定运算 $\perp$, 即序偶 $(G, \perp)$ 为半群, 称满足 **G1G2G3** 的序偶 $(G, \perp)$ 为幺半群, 称满足 **G1G2G3G4** 的序偶 $(G, \perp)$ 为群。若 $\perp$ 采用加法记号, 称序偶 $(G, \perp)$ 为加群, 若采用乘法记号, 称序偶 $(G, \perp)$ 为倍群

♣

性质 C1: 左中性元也为右中性元, 左对称元也为右对称元

证明 给定 a, 记 b 为 a 左对称元, c 为 b 左对称元, e 为左中性元, 则有 $bab = eb = b$, 左乘 c 有 $cbab = cb \Rightarrow eab = e \Rightarrow ab = e$, 于是 b 为 a 右对称元, 则有 $ae = aba = ea = a$, 于是 e 为右中性元

性质 C2: (中性元唯一性) $(\exists! e \in G)(\forall a \in G) : (ae = ea = a)$

证明 $(\exists e' \in G)(e' \neq e) : [(\forall a \in G)(ae' = e'a = a) \Rightarrow (e'e = e) \wedge (e'e = e') \Rightarrow (e' = e)]$

性质 C3: (可除性) $(\forall a, b \in G) : [(\exists x \in G)(ax = b) \wedge (\exists y \in G)(ya = b)]$

证明 存在性由 $x = a^{-1}b, y = ba^{-1}$ 即有

性质 C4: (除法唯一性) $(\forall a, b \in G) : [(\exists! x \in G)(ax = b) \wedge (\exists! y \in G)(ya = b)$

证明 $(\forall x_1, x_2 \in G) : [(ax_1 = ax_2) \Rightarrow (a^{-1}ax_1 = a^{-1}ax_2) \Rightarrow (x_1 = x_2)], (\forall y_1, y_2 \in G) : [(y_1a = y_2a) \Rightarrow (y_1aa^{-1} = y_2aa^{-1}) \Rightarrow (y_1 = y_2)]$

定义 1.2 (群第二公理化)

利用下面三条性质可以公理化定义群:

G1: (二元运算存在性) $(\exists \perp : G \times G \to G)(\forall a, b \in G)(\exists! c \in G) : (c = a \perp b)$

G2: (结合性) $(\forall a, b, c \in G) : a \perp (b \perp c) = (a \perp b) \perp c$

C3: (可除性) $(\forall a, b \in G) : [(\exists x \in G)(a \perp x = b) \wedge (\exists y \in G)(y \perp a = b)]$

♣

性质 G3: (左中性元存在性) $(\exists e \in G)(\forall a \in G) : e \perp a = a$

证明 由可除性 $(\forall a \in G)(\exists y \in G) : ya = a$, 记 y 为 e 即证

性质 G4: (左对称元存在性) $(\forall a \in G)(\exists b \in G) : b \perp a = e$

证明 由可除性 $(\forall a, e \in G)(\exists b \in G) : ba = e$

性质 C1: 左中性元也为右中性元, 左对称元也为右对称元

证明 给定 a, 记 b 为 a 左对称元, c 为 b 左对称元, e 为左中性元, 则有 $bab = eb = b$, 左乘 c 有 $cbab = cb \Rightarrow eab = e \Rightarrow ab = e$, 于是 b 为 a 右对称元, 则有 $ae = aba = ea = a$, 于是 e 为右中性元

性质 C2: (中性元唯一性) $(\exists! e \in G)(\forall a \in G) : (ae = ea = a)$

证明 $(\exists e' \in G)(e' \neq e) : [(\forall a \in G)(ae' = e'a = a) \Rightarrow (e'e = e) \wedge (e'e = e') \Rightarrow (e' = e)]$

性质 C4: (除法唯一性) $(\forall a, b \in G) : [(\exists! x \in G)(ax = b) \wedge (\exists! y \in G)(ya = b)$

证明 $(\forall x_1,x_2\in G):[(ax_1=ax_2)\Rightarrow(a^{-1}ax_1=a^{-1}ax_2)\Rightarrow(x_1=x_2)],(\forall y_1,y_2\in G):[(y_1a=y_2a)\Rightarrow(y_1aa^{-1}=y_2aa^{-1})\Rightarrow(y_1=y_2)]$

定义 1.3 (群子集)

称由群 $(G,\perp)$ 的元素所组成的任意集合为群子集；设 A,B 是群 $(G,\perp)$ 两个群子集，则约定 $AB=\{a\perp b|(\forall a\in A)(\forall B\in B)\},A^{-1}=\left\{a^{-1}|(\forall a\in A)\right\}$。特别地，当 $A=\{a\}$ 为单点集时，记 $AB=aB,BA=Ba$，这些符号对半群与么半群可同样使用。

定义 1.4 (子群)

若群 $(G,\perp)$ 集合 G 的非空子集 H 对 G 的运算也为一个群，则称 $(H,\perp)$ 为 $(G,\perp)$ 的子群，记为 $H\leqslant G$。显然 $H=\{e\}$（e 为 G 的中性元）与 $H=G$ 均为 G 的子群，称为 G 的平凡子群，称其他子群为非平凡子群。若子群 $H\neq G$，则称 H 为 G 的真子群，记为 $H<G$

定理 1.1 (子群判别法)

设 H 是群 G 的非空子集，则下列条件等价：

1) H 为 G 子群

2) 单位元：$1\in H$；可逆性：$(a\in H)\Rightarrow(a^{-1}\in H)$；封闭性：$(a,b\in H)\Rightarrow(ab\in H)$

3) 可逆性：$(a\in H)\Rightarrow(a^{-1}\in H)$；封闭性：$(a,b\in H)\Rightarrow(ab\in H)$

4)（判别法）$a,b\in H$，则 $ab^{-1}\in H$

证明 1) $\Rightarrow$ 2). 由 H 对 G 的运算构成群知 $a,b\in H$，则 $ab\in H$。又 H 有单位元 $1'$，即有 $1'\cdot1'=1'$。设 $1'$ 在 G 中的对称元为 $1'^{-1}$，则有 $1=1'\cdot1'^{-1}=(1'\cdot1')\cdot1'^{-1}=1'$，故 $1\in H$。设 a 在 H 中的对称元为 a'，于是 $aa'=1'=1$，即 $a'=a^{-1}$，故 $a^{-1}\in H$。由此知 2) 成立

2) $\Rightarrow$ 3). 显然

3) $\Rightarrow$ 4). 若 $a,b\in H$，则 $a,b^{-1}\in H$，则有 $ab^{-1}\in H$

4) $\Rightarrow$ 1). 由 $H\neq\varnothing$ 有 $\exists a\in H$，则有 $1=aa^{-1}\in H$，又由 $1,a\in H$ 有 $a^{-1}=1\cdot a^{-1}\in H$。又若 $a,b\in H$，由 $b^{-1}\in H$ 得 $ab=a\left(b^{-1}\right)^{-1}\in H$。由此得 G 的运算也是 H 的运算。H 有单位元 1，对 $a\in H$ 有逆元 a^{-1}，结合律显然成立，故 H 为 G 子群

注 可更形式化地改述为：设 G 为群，若 $H\subseteq G,H\neq\varnothing$，则下列命题等价：

1) $H\leqslant G$

2) $H^2\subseteq H$ 且 $H^{-1}\subseteq H$

3) $HH^{-1}\subseteq H$（或 $H^{-1}H\subseteq H$）

性质（条件可并性）

设 $(H_i)_{i\in I}$ 为群 G 子群族，若

$$(\forall i,j\in I)(\exists k\in I):(H_i\subset H_k)\wedge(H_j\subset H_k)$$

则 $\bigcup_{i\in I}H_i$ 为 G 子群

证明 设 $U=\bigcup_{i\in I}H_i$，则 $e_G\in U\Rightarrow U\neq\varnothing$；$(x,y\in U)\Rightarrow(\exists i,j\in I):(x\in H_i)\wedge(y\in H_j)$，由假设 $(\exists k\in I):(x,y\in H_k)$，同理得 $xy^{-1}\in H_k\subset U$，即有 $(x,y\in U)\Rightarrow(xy^{-1}\in U)$，由判别法 (1.1) 即证

性质（可交性）

设 $(H_i)_{i\in I}$ 为群 G 子群族，则 $\bigcap_{i\in I}H_i$ 为 G 子群

证明 设 $M=\bigcap_{i\in I}H_i$，则 $e_G\in M\Rightarrow M\neq\varnothing$；$(x,y\in M)\Rightarrow(\forall i\in I):(x,y\in H_i)\Rightarrow(\forall i\in I)(xy^{-1}\in H_i\subset M)\Rightarrow(xy^{-1}\in M)$，由判别法 (1.1) 即证

1.1.2 置换与循环群

定义 1.5 (置换)

给定集 Ω 与双射 $\sigma:\Omega\to\Omega$，若 Ω 为无限集，称 σ 为集 Ω 的变换，若 Ω 为有限集，则称 σ 为集 Ω 的置换。

若给定集 $\Omega_n=\{1,2,\cdots,n\}$ 与双射 $\sigma:\Omega_n\to\Omega_n$，则称 σ 为自然置换 ♣

注 下文将证明 Cayley 定理，即任意群同构于某个变换群，任意有限群同构于某个置换群，于是下文的置换可先仅考虑自然置换的情形

定义 1.6 (自然置换形式化记号)

若 $\sigma(j)=\sigma_j(j=1,2,\cdots,n)$，则记为

$$\sigma=\begin{pmatrix}1&2&\cdots&n\\ \sigma_1&\sigma_2&\cdots&\sigma_n\end{pmatrix}$$

♣

注 （自然置换合成）

设置换 $\sigma,\tau\in S_n$，它们的乘法对应于映射合成的一般法则：$(\sigma\tau)(i)=\sigma(\tau(i))$ 例如对于置换

$$\sigma=\begin{pmatrix}1&2&3&4\\ 2&3&4&1\end{pmatrix},\quad \tau=\begin{pmatrix}1&2&3&4\\ 4&3&2&1\end{pmatrix}$$

有

$$\sigma\tau=\begin{pmatrix}1&2&3&4\\ 2&3&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\ 4&3&2&1\end{pmatrix}=\begin{matrix}1&2&3&4\\ \downarrow&\downarrow&\downarrow&\downarrow\\ 4&3&2&1\\ \downarrow&\downarrow&\downarrow&\downarrow\\ 1&4&3&2\end{matrix}=\begin{pmatrix}1&2&3&4\\ 1&4&3&2\end{pmatrix}$$

同时

$$\tau\sigma=\begin{pmatrix}1&2&3&4\\ 4&3&2&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\ 2&3&4&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\ 3&2&1&4\end{pmatrix}$$

则 $\sigma\tau\neq\tau\sigma$

命题 1.1 (变换群)

集 Ω 的全体变换为群，记为 S_n ♠

证明 i) 乘法结合性：$\forall\alpha,\beta,\gamma\in S_n:(\alpha\beta)\gamma=\alpha(\beta\gamma)$

ii) 左单位元存在性：$\forall\pi\in S_n,e\pi=\pi$

iii) 左逆元：$\forall\pi\in S_n:\pi^{-1}\pi=e$

注 特别地，称集 Ω 的全体置换为对称群，若 M 为 n 元集，称 M 的全变换群为 n 阶对称群，记为 $S(M)$

性质 （n 阶对称群基数）

$\mathrm{Card}(\mathrm{S_n})=|S_n|=n!$

证明 由 σ 为双射有 $\sigma_1,\sigma_2,\cdots,\sigma_n$ 为 $1,2,\cdots,n$ 的一个排列。显然 $1,2,\cdots,n$ 的任一排列 $\tau_1,\tau_2,\cdots,\tau_n$ 都给出一个置换且不同排列给出不同的置换，则有 $|S_n|=n!$

定义 1.7 (n 阶对称群方幂归纳定义)

现设 π 为 S_n 中任意置换，其方幂 π^s 归纳定义如下：

$$\pi^s=\begin{cases}\pi\left(\pi^{s-1}\right), & 若 s>0,\\ e, & 若 s=0,\\ \pi^{-1}\left(\left(\pi^{-1}\right)^{(-s-1)}\right), & 若 s<0.\end{cases}$$

这时显然有

$$\pi^s\pi^t=\pi^{s+t}=\pi^t\pi^s, s,t\in\mathbb{Z}$$

(当 s 与 t 同号时，顺序添上 π 或 π^{-1}，当 s 与 t 异号时，用 e 代替 $\pi\pi^{-1},\pi^{-1}\pi$)

定义 1.8 (置换的阶)

任意置换 $\pi\in S_n$ 均可以找到唯一确定的自然数 $q=q(\pi)$ 使得全部不同的方幂包含在集合 $\langle\pi\rangle=\left\{e,\pi,\cdots,\pi^{q-1}\right\}$ 中，且 $\pi^q=e$，则称 q 为置换 π 的阶

定义 1.9 (置换 π 等价)

设置换 $\pi\in S_n$，若

$$(\exists s\in\mathbb{Z}): j=\pi^s(i)$$

则称两个点 $i,j\in\Omega$ 为 π 等价的

注 (置换 π 等价)

考虑

$$i=\pi^0(i), j=\pi^s(i)\Rightarrow i=\pi^{-s}(j), j=\pi^s(i), k=\pi^t(j)\Rightarrow k=\pi^{s+t}(i)$$

显然得到了 Ω 上的一个等价关系

定义 1.10 (循环)

根据 π 等价关系可以写出

$$\Omega=\Omega_1\cup\cdots\cup\Omega_p$$

其中集合 Ω 划分成了两两不相交的类 $\Omega_1,\cdots,\Omega_p$，称这些类为 π 轨道 (如此命名是因为每一个点 $i\in\Omega$ 恰属于一个轨道，并且若 $i\in\Omega_k$，则 Ω_k 由元素 π 的方幂作用在点 i 上的像组成：$i,\pi(i),\pi^2(i),\cdots,\pi^{l_k-1}(i)$，称 $l_k=|\Omega_k|$ 为 π 轨道 Ω_k 的长度)

显然有 $l_k\leqslant q=\mathrm{Card}\langle\pi\rangle$，$\pi^{l_k}(i)=i$，并且 l_k 为具有上述性质的最小数，令

$$\pi_k=\left(i,\pi(i),\cdots,\pi^{l_k-1}(i)\right)=\begin{pmatrix}i & \pi(i) & \cdots & \pi^{l_k-2}(i)\\ \pi(i) & \pi^2(i) & \cdots & \pi^{l_k-1}(i)\end{pmatrix}$$

则得一个置换，称为长度为 l_k 的循环，经常记为 $(i_1i_2\cdots i_t)$。特别地，称长度为 2 的循环为对换。长度为 1 的循环常记为 (1)。

若 $(\forall 1\leqslant k\leqslant t, 1\leqslant l\leqslant s): i_k\neq j_l$，则称两个循环 $(i_1i_2\cdots i_t)$ 和 $(j_1j_2\cdots j_s)$ 不交

注 (循环)

循环 π_k 使集合 $\Omega\backslash\Omega_k$ 中所有的点保持不变，而任取点 $j\in\Omega_k,\pi(j)=\pi_k(j)$ 这一性质提供了称两个循环 $\pi_s,\pi_t,s\neq t$ 为无关的或不交的依据，因为任取 $i\in\Omega_k,\pi_k^{l_k}(i)=i$，则有 $\pi_k^{l_k}=e$

定理 1.2 (置换循环分解)

S_n 中每一个置换 $\pi\neq e$ 都为长度大于等于 2 的不交循环的乘积。该分解精确到循环的顺序是唯一的

证明 [证明一：] 由上述定义有划分 $\Omega=\Omega_1\cup\cdots\cup\Omega_p$，其对应于置换 π 到乘积的分解

$$\pi=\pi_1\pi_2\cdots\pi_p \tag{1.1}$$

其中任意两个循环可换序：$\pi=\pi_1\pi_2\cdots\pi_p=\pi_{l_1}\pi_{l_2}\cdots\pi_{l_p}$。可以假定 $l_1\geqslant l_2\geqslant\cdots\geqslant l_m>l_{m+1}=\cdots=l_p=1$。若循环 $\pi_k=(i)$ 的长度为 1，则为恒等置换，这样的循环在乘积 (1.1) 中可以省略：

$$\pi=\pi_1\pi_2\cdots\pi_m,\quad l_k>1,\quad 1\leqslant k\leqslant m \tag{1.2}$$

假设还有形如公式 (1.2) 的另一种分解 $\pi=\alpha_1\alpha_2\cdots\alpha_r$，也为不交循环的乘积，并设符号 i 在 π 下改变。这时存在 $\pi_1,\cdots,\pi_m$ 中的一个（且仅有一个）循环 π_s，使得 $\pi_s(i)\neq i$，同时存在 $\alpha_1,\cdots,\alpha_r$ 中的一个循环 α_t，使得 $\alpha_t(i)\neq i$。显然有 $\pi_s(i)=\pi(i)=\alpha_t(i)$，若

$$\pi_s^k(i)=\pi^k(i)=\alpha_t^k(i) \tag{1.3}$$

则将置换 π 作用于这一等式并运用 π 与 π_s^k 和 α_t^k 的交换性得

$$\pi\pi_s^k(i)=\pi^{k+1}(i)=\pi\alpha_t^k(i)$$

因而 $\pi_s^k\pi(i)=\pi^{k+1}(i)=\alpha_t^k\pi(i)$，最后

$$\pi_s^{k+1}(i)=\pi^{k+1}(i)=\alpha_t^{k+1}(i)$$

综上，等式 (1.3) 对任意 $k=0,1,2,\cdots$ 成立，但循环是被它的方幂在任意一个发生改变的符号上的作用唯一确定的，则 $\pi_s=\alpha_t$，然后再对 m 或 r 用归纳法即证

证明 [证明二：(存在性初等证明)] 设 $\sigma\in S_n,\sigma\neq(1)$。由条件可以取 $i_1\in\{1,2,\cdots,n\}$ 使得 $\sigma(i_1)\neq i_1$。考虑 $i_1,\sigma(i_1),\sigma^2(i_1),\cdots\in\{1,2,\cdots,n\}$，由 n 有限则必存在 $t_1<t_2$ 使得 $\sigma^{t_1}(i_1)=\sigma^{t_2}(i_1)$，即有 $\sigma^{t_2-t_1}(i_1)=i_1$。令 t 为满足 $\sigma^t(i_1)=i_1$ 的最小的正整数，由 i_1 的选取知 $t>1$。则 σ 在 $\{i_1,\sigma(i_1),\cdots,\sigma^{t-1}(i_1)\}$ 上的限制构成一个循环。

若 $\{1,2,\cdots,n\}\backslash\{i_1,\sigma(i_1),\cdots,\sigma^{t-1}(i_1)\}$ 元素在 σ 下均不变，则 $\sigma=(i_1\sigma(i_1)\cdots\sigma^{t-1}(i_1))$；否则在 $\{i_1,\sigma(i_1),\cdots,\sigma^{t-1}(i_1)\}$ 之外取一个在 σ 下变动的元素 j_1（注意 $(\forall k,l\in\mathbb{Z}):\sigma^k(j_1)\neq\sigma^l(i_1)$，否则导致 $j_1=\sigma^{l-k}(i_1)$，与 j_1 的选取矛盾），有限次重复上面讨论即得分解存在性。唯一性同上。

推论 1.1 (置换对换分解)

任一置换可以写为对换的乘积

♡

证明 由定理 (1.2)，仅需证任一循环可分解为对换乘积。不难验证 $(i_1i_2\cdots i_t)=(i_1i_t)(i_1i_{t-1})\cdots(i_1i_3)(i_1)$

定义 1.11 (置换符号)

设 $\pi\in S_n$，将 π 分解成对换的乘积：$\pi=\tau_1\tau_2\cdots\tau_k$，则称

$$\varepsilon_\pi=(-1)^k$$

为 π 的符号（亦称符号差或奇偶性）

♣

定理 1.3 (置换符号唯一性)

设 π 为 S_n 中一个置换，将 π 分解成对换的乘积：

$$\pi=\tau_1\tau_2\cdots\tau_k \tag{1.4}$$

其符号由置换 π 唯一确定并不依赖于式 (1.4) 的分解方法，即对于给定的 π 整数 k 给出的奇偶性唯一。此外任取 $\alpha,\beta\in S_n$，有

$$\varepsilon_{\alpha\beta}=\varepsilon_\alpha\varepsilon_\beta$$

♡

证明 1) 设除式 (1.4) 外还有一个分解

$$\pi=\tau_1'\tau_2'\cdots\tau_{k'}' \tag{1.5}$$

且数 k 与 k' 不同。定理的结论等价于整数 $k+k'$ 为一个偶数。因为 $(\tau_s')^2 = e$ 且式 (1.4) 与式 (1.5) 给出 $\tau_1\tau_2\cdots\tau_k = \tau_1'\tau_2'\cdots\tau_{k'}'$，用 $\tau_{k'}', \cdots, \tau_2', \tau_1'$ 从右侧顺序去乘这一等式的两边得 $\tau_1\tau_2\cdots\tau_k\tau_{k'}'\cdots\tau_2'\tau_1' = e$。问题归结为：设

$$e = \sigma_1\sigma_2\cdots\sigma_{m-1}\sigma_m, m > 0 \tag{1.6}$$

为单位置换到对换乘积的一个分解，则 m 是一个偶数。该命题可用下述方法实现：将 e 的表达式 (1.6) 转化成 $m-2$ 个对换的乘积。继续这一过程，若 m 为奇数就得到了一个对换 τ，但显然 $e \neq \tau$，只需给出将 m 个因子削减为 $m-2$ 个的依据。

2) 设 $s, 1 \leqslant s \leqslant n$ 为任意一个包含在对换 $\sigma_2, \cdots, \sigma_m$ 中的整数，设

$$e = \sigma_1\cdots\sigma_{p-1}\sigma_p\sigma_{p+1}\cdots\sigma_m$$

使得 $\sigma_p = (st)$，而 $\sigma_{p+1}, \cdots, \sigma_m$ 不包含 s。对于 σ_{p-1}，有下述四种可能性：

a) $\sigma_{p-1} = (st)$; 这时 $\sigma_{p-1}\sigma_p = (st)(st)$ 从 e 的写法中排除则得 $m-2$ 个对换的分解式

b) $\sigma_{p-1} = (sr), r \neq s, t$; 则

$$\sigma_{p-1}\sigma_p = (sr)(st) = (st)(rt)$$

于是将 s 向左移动了一个位置，对换的个数 m 没有改变

c) $\sigma_{p-1} = (t.r), r \neq s, t$; 则

$$\sigma_{p-1}\sigma_p = (tr)(st) = (sr)(tr)$$

再次出现 b) 的情况，s 向左位移而对换的个数 m 没有改变

d) $\sigma_{p-1} = (qr), \{q, r\} \cap \{s, t\} = \varnothing$; 这时

$$\sigma_{p-1}\sigma_p = (qr)(st) = (st)(qr)$$

若出现情况 a) 目的达到，否则不断重复 b)-d) 的处理方式可以将 s 移动到左边第一个位置。综上或者有情况 a)，或者到达下述极限情况：$e = \sigma_1'\sigma_2'\cdots\sigma_m', \sigma_1' = (st')$，且 s 不进入 $\sigma_2', \cdots, \sigma_m'$. 于是，当 $k > 1$ 时 $\sigma_k'(s) = s$，但 $s = e(s) = \sigma_1'(s) = t' \neq s$。该矛盾证明了情况 a) 必须出现，从而 m 为偶数，则关于 ε_π 不变性的论断正确

3) 若 $\alpha = \tau_1\cdots\tau_k, \beta = \tau_{k+1}\cdots\tau_{k+l}$，则 $\alpha\beta = \tau_1\cdots\tau_k\tau_{k+1}\cdots\tau_{k+l}$，且 $\varepsilon_\alpha = (-1)^k, \varepsilon_\beta = (-1)^l, \varepsilon_{\alpha\beta} = (-1)^{k+l} = (-1)^k(-1)^l = \varepsilon_\alpha\varepsilon_\beta$

定义 1.12 (置换奇偶性)

若 $\varepsilon_\pi = 1$，则称置换 $\pi \in S_n$ 为偶置换，若 $\varepsilon_\pi = -1$，则称 π 为奇置换。 ♣

推论 1.2 (置换循环分解符号性质)

设置换 $\pi \in S_n$ 分解为长为 $l_1, l_2, \cdots, l_m$ 的互不相交的循环的乘积. 则

$$\varepsilon_\pi = (-1)^{\sum_{k=1}^{m}(l_k-1)}.$$

♡

证明 根据定理 (1.3) 有

$$\varepsilon_\pi = \varepsilon_{\pi_1\cdots\pi_m} = \varepsilon_{\pi_1}\cdots\varepsilon_{\pi_m}$$

其中 $\varepsilon_{\pi_k} = (-1)^{l_k-1}$，因为 π_k 可以写成 $l_k - 1$ 个对换的乘积，最后

$$\varepsilon_\pi = (-1)^{l_1-1}\cdots(-1)^{l_m-1} = (-1)^{\sum_{i=1}^{m}(l_k-1)}$$

命题 1.2 (奇偶置换基数)

S_n 中偶置换的个数等于奇置换的个数，且有

$$|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}.$$

♠

证明 将 S_n 写成并集 $S_n = A_n \cup \bar{A}_n$，其中 $A_n = \{\pi \in S_n \mid \varepsilon_\pi = 1\}$ 为偶置换的集合，$\bar{A} = S_n \backslash A_n$ 为奇置换的集合。设 $\tau = (ij)$ 为任意对换。S_n 到自身的映射 $L_\tau : \pi \mapsto \tau\pi$ 为双射（L_τ 为单射：$\tau\alpha = \tau\beta \Rightarrow \alpha = \beta$，不难看出 L_τ^2 为恒等映射，则 $L_\tau^{-1} = L_\tau$）。L_τ 可表示成在集合 $S_n = \{\pi_1 = e, \pi_2, \pi_3, \cdots, \pi_N\}$ 上的一个 $N = n!$ 阶置换：

$$L_\tau = \begin{pmatrix} \pi_1 & \pi_2 & \pi_3 & \cdots & \pi_N \\ \tau\pi_1 & \tau\pi_2 & \tau\pi_3 & \cdots & \tau\pi_N \end{pmatrix}$$

类似地有

$$R_\tau = \begin{pmatrix} \pi_1 & \pi_2 & \pi_3 & \cdots & \pi_N \\ \pi_1\tau & \pi_2\tau & \pi_3\tau & \cdots & \pi_N\tau \end{pmatrix}$$

也为 S_n 上一个置换。注意到 $\varepsilon_{\tau\pi} = \varepsilon_\tau \varepsilon_\pi = -\varepsilon_\pi$，则有

$$L_\tau(A_n) = \bar{A}_n, \quad L_\tau(\bar{A}_n) = A_n.$$

亦即 S_n 中偶置换的个数等于奇置换的个数，又由性质 (1.1.2) 则有

$$|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$$

命题即证

定义 1.13 (生成子群)

设 S 为群 G 非空子集，用 $\langle S\rangle$ 表示 G 的包含 S 的最小子群，即 S 生成的子群。显然 $\langle S\rangle$ 为 G 中所有包含 S 的子群之交

♣

定理 1.4 (生成子群构造)

设 S 为群 G 的非空子集，则有

$$\langle S\rangle = \left\{x_1 x_2 \cdots x_m \mid x_i \in S \cup S^{-1}, 1 \leqslant i \leqslant m, m \in \mathbf{N}\right\}.$$

♡

证明 令 $\bar{S} = \left\{x_1 x_2 \cdots x_m \mid x_i \in S \cup S^{-1}, 1 \leqslant i \leqslant m, m \in \mathbf{N}\right\}$，由 $\langle S\rangle$ 为子群且 $S \subseteq \langle S\rangle$ 知 $S^{-1} \subseteq \langle S\rangle$，则 $S \subseteq \bar{S} \subseteq \langle S\rangle$。又 $\langle S\rangle$ 为含 S 的最小子群，故只需证 $\bar{S}$ 为子群，则有 $\bar{S} = \langle S\rangle$

设 $x_1 x_2 \cdots x_m \in \bar{S}, y_1 y_2 \cdots y_n \in \bar{S}$，则 $y_i^{-1} \in S \cup S^{-1} (1 \leqslant i \leqslant m)$，则有

$$(x_1 x_2 \cdots x_m)(y_1 y_2 \cdots y_n)^{-1} = x_1 x_2 \cdots x_m y_n^{-1} y_{n-1}^{-1} \cdots y_2^{-1} y_1^{-1} \in \bar{S},$$

因而 $\bar{S}$ 为 G 子群，故 $\bar{S} = \langle S\rangle$

定义 1.14 (生成系与循环群)

若 S 为群 G 的子集且 $G = \langle S\rangle$（允许 $S = \varnothing$），则称 S 为 G 的生成系或称 G 由 S 生成，记为 $\langle S\rangle$。若 G 有一个含有限个元素的生成组，则称 G 是有限生成的。称仅由一个元素 a 生成的群 $G = \langle a\rangle$ 为循环群，若 $G = \langle a\rangle$ 为循环群，则称 a 为 G 的生成元

♣

定义 1.15 (群元素阶)

对于群 G 中任意元素 a，称 $\langle a\rangle$ 的阶为元素 a 的阶，记为 $\mathrm{o}(a)$，即 $\mathrm{o}(a) = |\langle a\rangle|$。由此定义知，$\mathrm{o}(a)$ 为满足 $a^n = e$ 的最小的正整数 n，若这样的正整数 n 不存在，则称 a 的阶为无穷阶，记为 $o(a) = \infty$。称群中所有元素的阶的最小公倍数为群的方次数，记为 $\exp(G)$，若最小公倍数不存在，则称其方次数为 ∞

♣

1.1.3 陪集与正规子群

定义 1.16 (同余关系)

设二元关系“≡”为集 A 上等价关系，若“≡”满足

$$(\forall a,b,c,d\in A)[(a\equiv b)\wedge(c\equiv d)\Rightarrow(ac\equiv bd)]$$

则称关系为 A 上同余关系，称 a 的等价类为 a 的同余类

定义 1.17 (陪集)

设 H 为群 G 子群，则称群子集 gH 为 H 在 G 中一个左陪集；对称地称 Hg 为 H 在 G 中的一个右陪集（旁系，同余类）

命题 1.3 (陪集单位元存在性)

设 H 为群 G 子群，则 $(g\in H)\Rightarrow(gH=H)\wedge(Hg=H)$

证明 由群的元素的性质显然即证

命题 1.4 (非空子群群子集性质)

设 H 为群 G 非空子集，则有下列命题等价：

1)H 为群 G 子群

2)$(H^{-1}=H)\wedge(HH=H)$

3)$H^{-1}H=H$

证明 由命题 (1.3) 显然有 1) ⇒ 2), 1) ⇒ 3)；2) ⇒ 3) 显然成立；由 $(\forall a\in H)(\forall b\in H^{-1})(\exists h\in H):a^{-1}b\in H$，则由判别法 (1.1) 有 H 为 G 子群，即有 3) ⇒ 1)

命题 1.5 (子群群子集交换性充要条件)

设 H_1,H_2 为 G 子群，则有

$$H_1H_2=H_2H_1\Leftrightarrow H_1H_2\text{为群}$$

证明 充分性：由 H_1H_2 为群，$h_1h_2\in H_1H_2$ 且 $h_2^{-1}h_1^{-1}=h_1h_2\in H_2H_1$，则 $h_1h_2\in H_1H_2\Leftrightarrow h_2^{-1}h_1^{-1}=h_1h_2\in H_2H_1$；必要性：$(H_1H_1)(H_2H_2)=H_1(H_1H_2)H_2=(H_1H_2)(H_1H_2)=H_1H_2$，则有 $(h_1h_2\in H_1H_2)\Rightarrow(h_1h_2)(h_1h_2)^{-1}=e\in H_1H_2$，由判别法 (1.1) 知 H_1H_2 为群

定理 1.5 (陪集等价类存在性)

设 H 为群 G 子群，则

$$R(a,b)=\{(a,b)|(\forall a,b\in G)(a^{-1}b\in H)\}$$

为集合 G 上等价关系，且 a 所在等价类为 aH

证明 传递性：$(a^{-1}b\in H)\wedge(b^{-1}c\in H)\Rightarrow(a^{-1}bb^{-1}c=a^{-1}c\in H)$；对称性：$a^{-1}b\in H\Rightarrow(a^{-1}b)^{-1}=b^{-1}a\in H$；自反性：$R(a,a)$ 为真等价于 $a^{-1}a=e\in H$，又由 $b=a(a^{-1}b)$ 知 $R(a,b)$为真 $\Leftrightarrow(a^{-1}b\in H)\Leftrightarrow b\in aH$，则 a 所在等价类为 aH

定理 1.6 (分解定理)

设 H 为群 G 子群，$a,b\in G$，则有下列命题等价：

1)$aH\cap bH\neq\varnothing$

2)$aH = bH$
3)$a^{-1}b \in H$

♡

证明 1) ⇒ 2)：设 $(\exists h_1, h_2 \in H) : (ah_1 = bh_2)$，则 $(ah_1 = bh_2) \Rightarrow (h_1 h_2^{-1} = a^{-1}b)$，又 $(h_1, h_2 \in H) \Rightarrow (a^{-1}b \in H)$，则有 $bH = a(a^{-1}bH) = aH$；2) ⇒ 3)：$a \in aH = bH$，则 $(\exists h_3 \in H) : a = bh_3$，则 $a^{-1}b = h_3^{-1} \in H$，同理有 3) ⇒ 2)；2) ⇒ 1) 显然

定义 1.18 (分解)

称群 G 由子群 H 的不交左陪集集合构成的划分为群 G 在子群 H 的左分解（G 对 H 左陪集空间），对称有群 G 在子群 H 的右分解（G 对 H 右陪集空间）；若群 G 对 H 左陪集空间基数有限，称基数为 H 在 G 中指标，记为 $[G : H]$

♣

定理 1.7 (陪集等价类为同余类的充要条件)

设 H 为群 G 子群，关系 $R(a,b) = \{(a,b) | (\forall a, b \in G)(a^{-1}b \in H)\}$ 为集合 G 上同余关系的充要条件为

$$(\forall g \in G)(\forall h \in H) : ghg^{-1} \in H$$

♡

证明 由定理 (1.5)，关系 $R(a,b)$ 集合 G 上等价关系。

充分性：设 $a, b, c, d \in G, R(a,b), R(c,d)$，则 $(\exists h_1, h_2 \in H) : (b = ah_2) \wedge (d = ch_2)$，则

$$c^{-1}h_2^{-1}h_1^{-1}c \in H \Rightarrow d^{-1}ab^{-1}c \in H \Rightarrow (\exists h \in H) : ac = bdh \Rightarrow (ac)^{-1}(bd) \in H \Rightarrow R(ab, cd)$$

必要性：设关系 R 为集合 G 上同余关系，则

$$R(g, gh) \wedge R(g^{-1}, g^{-1}) \Rightarrow R(e, ghg^{-1}) \Rightarrow ghg^{-1} \in H$$

定理即证

定理 1.8 (关于同余关系商集的性质)

设 H 为群 G 子群，关系 $R(a,b) = \{(a,b) | (\forall a, b \in G)(a^{-1}b \in H)\}$ 为集合 G 上同余关系，G/H 为群 G 关于同余关系商集，则 G/H 为群

♡

证明 由关系为同余关系有 $(\forall a, b \in G) : (aH)(bH) = (ab)H$，则 $(aHbH)cH = (abc)H = aH(bHcH), (1H)(aH) = aH, (a^{-1}H)(aH) = 1H$，则 G/H 为群

定义 1.19 (商群)

称群 G 关于同余关系 $R(a,b) = \{(a,b) | (\forall a, b \in G)(a^{-1}b \in H)\}$ 的商集为群 G 对 H 的商群

♣

定义 1.20 (正规子群)

设 H 为群 G 子群，若 $(\forall g \in G) : gH = Hg$，则称 H 为 G 正规子群（不变子群）

♣

定理 1.9 (子群正规性充要条件)

设 H 为群 G 子群，则有下列命题等价：

1)H 为群 G 正规子群，亦即 $(\forall g \in G) : gH = Hg$
2)$(\forall g \in G) : gHg^{-1} = H$
3)$(\forall g_1, g_2 \in G) : g_1 H g_2 H = g_1 g_2 H$

♡

证明 2) ⇒ 1)：$(\forall g \in G)(\forall h \in H) : gh = ghg^{-1}g = (ghg^{-1})g \in Hg$，则 $gH = Hg$；

1) ⇒ 3)：设 $g_1, g_2 \in G, h_1, h_2, h \in H$，由 1) 有 $(\exists h_1' \in H) : h_1 g_2 = g_2 h_1', (\exists h' \in H) : g_2 h = h' g_2$，则

$g_1h_1g_2h_2 = g_1g_2h_1'h_2 \in g_1g_2H, g_1g_2h = g_1h'g_2e \in g_1Hg_2H$，则有 $g_1Hg_2H = g_1g_2H$；

3) $\Rightarrow$ 2)：设 $g \in G, h \in H$，则 $ghg^{-1} = ghg^{-1}e \in gHg^{-1}H = gg^{-1}H = H$，则 $ghg^{-1} \in H$；又由 $h = g\left(g^{-1}hg\right)g^{-1} \in gHg^{-1}$，则有 $gHg^{-1} = H$

定理 1.10 (Lagrange 定理)

设 H 为有限群 G 子群，则有 $[G:1] = [G:H][H:1]$，即有限群子群的阶为该有限群的因子 ♡

证明 由定理 (1.3) 有映射 $f: H \to aH, h \mapsto ah$ 为双射，由 Cantor-Bernstein 定理 (??) 有 $\mathrm{Card}(aH) = [H:1]$，又由定理 (1.6) 有 $G = \bigcup\limits_{a\in G} aH$ 为不交并，则 $[G:1] = [G:H][H:1]$

注 实际上该定理对无限群也成立

1.1.4 群自同构与群在集上作用

命题 1.6 (自同构群)

任意集 G 关于任意关系 R 的自同构全体为群 ♠

证明 设 f 为 M 关于关系 R 的自同构，则二元运算结合性显然；左中性元：$id_M \circ f = f$；左对称元：由 f 为双射，则必有逆映射，则有 $f^{-1} \circ f = id_M$

注 称该群为集 M 的自同构群

定义 1.21 (群自同构群)

记群 G 的群自同构的全体为 $Aut(G)$ ♣

定义 1.22 (群在集上作用)

设 G 为群，X 为非空集，若映射 $f: G \times X \to X$ 满足下列条件：

1)$(\forall x \in X): f(e,x) = x$

2)$(\forall g_1, g_2 \in G)(\forall x \in X): f(g_1g_2, x) = f(g_1, f(g_2, x))$

则称 f 定义了群 G 在 X 上的一个作用（出于对称性，仅考虑群 G 在 X 上的左作用）。经常简记为 $f(g,x) = g(x), g \in G, x \in X$

特别地，若 $(\forall g \in G)()\forall x \in X): g(x) = x$，则称作用为群 G 在 X 上的平凡作用 ♣

定义 1.23 (群上平移作用)

设 G 为群，取 $X = G$，定义 $f_1: x \mapsto f_1(g,x) = L_g(x) = gx$，称 f_1 决定的 G 在 G 上作用为由 g 决定的左平移作用；定义 $f_2: x \mapsto f_2(g,x) = R_g(x) = xg$，称 f_2 决定的 G 在 G 上作用为由 g 决定的右平移作用；定义 $f_3: x \mapsto f_3(g,x) = \mathrm{ad}\, g(x) = gxg^{-1}$，称 f_3 决定的 G 在 G 上作用为由 g 决定的伴随作用。另外，记 $L_G = \{L_g | g \in G\}, R_G = \{R_g | g \in G\}$ ♣

命题 1.7 (群上平移作用对称群性质)

设 G 为 n 元群，则 L_G, R_G 均为 n 阶对称群 S_n 子群 ♠

证明 显然有 $L_aL_b = L_{ab}, L_e = id_G, L_a^{-1} = L_{a^{-1}}$；设 $G = \{g_1, \cdots, g_n\}$，则 $L_a: G \to G, g_i \mapsto ag_i$ 有 $ag_i = ag_j \Rightarrow g_i = g_j$，则 L_a 为置换；$(L_a, L_b \in L_G) \Rightarrow (L_{ab^{-1}} \in L_G)$，则 L_G 为 n 阶对称群 S_n 子群，对称地有 R_G 为 n 阶对称群 S_n 子群

定理 1.11 (Cayley 定理)

设 G 为群，则有 $G \cong L_G \cong R_G$ ♡

证明 记 $L : G \to L_G, a \mapsto L_a$，显然 L 为满射：又 $L(a) = L(b) \Rightarrow L_a = L_b \Rightarrow L_a(1) = L_b(1) = b$，则 L 为双射；又 $(a, b \in G) \Rightarrow L(ab) = L_{ab} = L_a L_b = L(a)L(b)$，则 L 为 G 到 L_G 同构，即 $G \cong L_G$，同理有 $G \cong R_G$

注 综合 Cayley 定理 (1.11) 与命题 (1.7)，注意到前文的自然置换与置换的区别是非本质的，二者是同构的，下文不再予与区分

命题 1.8 (群上伴随作用自同构性)

设 G 为群，$g \in G$，则 G 上伴随作用 $\operatorname{ad} g, x \mapsto gxg^{-1}$ 为 G 自同构 ♠

证明 设 $\overline{x} = gxg^{-1}$，则 $x = g^{-1}\overline{x}g$，于是 $\operatorname{ad} g$ 为双射；$\overline{x} \cdot \overline{y} = (gxg^{-1})(gyg^{-1}) = \overline{x \cdot y}$

注 下称该自同构为 G 由 g 决定的内自同构，其全体记为 $\operatorname{Inn}(G)$

推论 1.3 (群在子群上伴随作用自同构性)

设 G 为群，$g \in G$，X 为 G 子群，则 $f : X \to X, x \mapsto gxg^{-1}$ 为 G 自同构 ♡

证明 由命题 (1.8) 即得

注 称 gxg^{-1} 为 x 的共轭群元素，称 gXg^{-1} 为子群 X 的共轭子群

命题 1.9 (内自同构与自同构群正规性)

设 G 为群，则内自同构 $\operatorname{Inn}(G)$ 为自同构群 $\operatorname{Aut}(G)$ 的正规子群 ♠

证明 设 $g_1, g_2 \in G, f_{g_1}, f_{g_2} \in \operatorname{Inn}(G)$，则有

$$f_{g_1} f_{g_2}^{-1} = L_{g_1} R_{g_1^{-1}} (L_{g_2} R_{g_2^{-1}})^{-1} = L_{g_1} L_{g_2}^{-1} R_{g_1^{-1}} R_{g_2^{-1}}^{-1} = L_{g_1 g_2^{-1}} R_{(g_1 g_2^{-1})^{-1}} = ad g_1 g_2^{-1}$$

则 $\operatorname{Inn}(G)$ 为 $\operatorname{Aut}(G)$ 子群，又由

$$(\forall g, a \in G)(\forall \theta \in \operatorname{Aut}(G)) : \theta(\operatorname{ad} g)(a) = \theta(gag^{-1}) = \theta(g)a\theta(g)^{-1} = \operatorname{ad}(\theta(g))(a)$$

则 $\operatorname{Inn}(G)$ 为 $\operatorname{Aut}(G)$ 正规子群

注 由该命题，下直接称群的内自同构全体为内自同构群

定义 1.24 (外自同构)

设 G 为群，$\operatorname{Inn}(G)$ 为 G 自同构群，$\operatorname{Aut}(G)$ 为 G 内自同构群，则称除 $\operatorname{Aut}(G)$ 外的 G 的自同构为 G 的外自同构 ♣

命题 1.10 (子群正规性充要条件)

设 G 为群，$g \in G$，X 为 G 子群，则 X 为 G 正规子群的充要条件为 X 为所有 G 内自同构下不变的子群 ♠

证明 显然有 $(\forall g \in G)(gXg^{-1} = X) \Leftrightarrow (\forall g \in G)(gX = Xg)$

注 条件减弱为 $gXg^{-1} \subseteq X$ 亦可，因为 $(\forall g^{-1} \in G)(g^{-1}Xg \subseteq X)$ 得 $gXg^{-1} \supseteq X$，合并即 $gXg^{-1} = X$

注 因此也称正规子群为不变子群

1.1.5 群同态与群同态基本定理

定义 1.25 (群同态与群同构)

设 $(G_1,\times_1),(G_2,\times_2)$ 为两个群（或半群、幺半群），f 为 G_1 到 G_2 的映射，若 f 满足

$$(\forall x,y\in G_1):f(x\times_1 y)=f(x)\times_2 f(y)$$

则称 f 为 G_1 到 G_2 的一个群同态。若 f 为满射，则称 f 为满同态；若 f 为双射，则称 f 为群同构，称群 G_1 与群 G_2 同构，记为 $G_1\cong G_2$

♣

定义 1.26 (自然同态)

设 H 为群 G 的正规子群，记 G 到商群 G/H 的自然映射为

$$\pi:\pi(g)=gH,\quad \forall g\in G$$

则 π 为 G 到 G/H 上的同态，称 π 为自然同态

若 G 为一个半群（或幺半群），“R” 为 G 中一个同余关系，则 G 到商半群（或商幺半群）G/R 的自然映射 π 为同态，也称 π 为自然同态

♣

性质 （群同态合成性质）

若 f 为群 G_1 到群 G_2 的群同态，g 为群 G_2 到群 G_3 的群同态则

1) gf 为 G_1 到 G_3 的群同态

2) 若 f,g 为满同态，则 gf 为满同态

3) 若 f,g 为同构，则 gf 为同构

证明 1) 纯形式地有 $(\forall a,b\in G_1)$ 满足 $gf(a),gf(b)\in G_3$ 且

$$gf(ab)=g(f(ab))=g(f(a)f(b))=(gf(a))(gf(b))$$

则 gf 为 G_1 到 G_3 的同态

2) 由 $f(G_1)=G_2,g(G_2)=G_3$ 即得 $gf(G_1)=G_3$

3) 由 g,f 为双射，则 gf 也为双射

性质 （群同态保幺性与保逆性）

设 f 为群 G_1 到群 G_2 的群同态，e_1,e_2 分别为 G_1,G_2 的单位元，则有

$$(\forall a\in G_1):f(e_1)=e_2,f\left(a^{-1}\right)=f(a)^{-1}$$

证明 显然有 $f(e_1)=f\left(e_1^2\right)=f(e_1)f(e_1)$，则有 $f(e_1)=f(e_1)f(e_1)^{-1}=e_2$。又 $a\in G_1$ 有 $f(e_1)=f\left(aa^{-1}\right)=f(a)f\left(a^{-1}\right)$，则有 $f\left(a^{-1}\right)=f(a)^{-1}f(e_1)=f(a)^{-1}$

性质 （群同态保群性）

设 f 为群 G_1 到群 G_2 的群同态，则 $f(G_1)$ 为 G_2 子群

证明 由性质 (1.1.5) 得，$e_2=f(e_1)\in f(G_1)$，且 $f(a),f(b)\in f(G_1)$ 有 $f(a)f(b)^{-1}=f\left(ab^{-1}\right)\in f(G_1)$，则由子群判别法 (1.1) 有 $f(G_1)$ 为 G_2 子群

注： 该性质表明 f 可看成 G_1 到 $f(G_1)$ 的同态

性质 群同构关系为等价关系

证明 若 $f:G_1\to G_2$ 为群同构，则 $f^{-1}:G_2\to G_1$ 也为群同构，即若 $G_1\cong G_2$，则 $G_2\cong G_1$；由性质 (1.1.5) 有，若 $G_1\cong G_2,G_2\cong G_3$，则 $G_1\cong G_3$；自反性取单位映射即证

定义 1.27 (群同态核)

设 f 为群 G_1 到群 G_2 的群同态，则称 G_2 的单位元 e_2 的原像集合

$$\ker f=f^{-1}(e_2)=\{x\in G_1\mid f(x)=e_2\}$$

为 f 的群同态核 ♣

定理 1.12 (群同态基本定理)

设 f 为群 G 到群 H 上群同态，则下列命题成立：

1) (群同态核正规性) $\ker f$ 为 G 正规子群

2) 若 π 为 G 到商群 $G/\ker f$ 上的自然同态，则存在 $G/\ker f$ 到 H 上同构 $\bar{f}$ 满足

$$f=\bar{f}\cdot\pi$$

♡

证明 1) 设 e,e' 分别为 G,H 单位元，则由性质 (1.1.5) 有 $f(e)=e'$。由群同态核定义有

$$(\forall x,y\in\ker):f\left(xy^{-1}\right)=f(x)f\left(y^{-1}\right)=f(x)f(y)^{-1}=e'$$

则 $\ker f$ 为 G 的子群，且有

$$(\forall z\in G):f\left(zxz^{-1}\right)=f(z)f(x)f(z)^{-1}=e'$$

则得

$$(\forall z\in G)(\forall x\in\ker f):zxz^{-1}\in\ker f$$

子群正规性充要条件 (1.9) 即得 $\ker f$ 为 G 正规子群

2) 由 f 为 G 到 H 上映射，则 f 在 G 中诱导一个等价关系

$$R:xRy,\quad x,y\in G$$

当且仅当 $f(x)=f(y)$，即 $f(x)f(y)^{-1}=f\left(xy^{-1}\right)=e'$，亦即 $xy^{-1}\in\ker f$

则 f 诱导的等价关系恰为 G 的正规子群 $\ker f$ 诱导的同余关系，即有 $G/R=G/\ker f$ 且

$$\pi(x)=\pi(y)\text{ 当且仅当}f(x)=f(y)$$

又有 $G/\ker f$ 到 H 的双射 $\bar{f}$，满足 $\bar{f}\cdot\pi=f$。另由

$$(\forall x,y\in G):\bar{f}(\pi(x)\pi(y))=\bar{f}(\pi(xy))=f(xy)=f(x)f(y)=\bar{f}(\pi(x))\cdot\bar{f}(\pi(y))$$

则知 $\bar{f}$ 为 $G/\ker f$ 到 H 上同构

定理 1.13 (群同态下含核子群与像的关系)

设 f 为群 G 到群 H 上群同态，f 的核为 $\ker f$，则下列命题成立：

1) (含核子群到像子群间双射) f 为 G 中包含 $\ker f$ 的子群与 H 子群间双射

2) (保正规性) 含核子群到像子群间双射 f 把正规子群一一对应到正规子群

3) (保商群性) 若 G_1 为 G 的正规子群，$\ker f\subset G_1$，则 $G/G_1\cong H/f(G_1)$

♡

证明 1) 设 G 中包含 $\ker f$ 的子群的集合为 Σ，而 H 的子群的集合为 Γ。设 $G_1\in\Sigma$，则 G_1 在 $f|_{G_1}$ 下的像，由性质 (1.1.5) 可得 $f(G_1)$ 为 H 的子群，即 $f(G_1)\in\Gamma$，则 f 为 Σ 到 Γ 的映射。反之，设 $H_1\in\Gamma$，e' 为 H 单位元，则 H_1 在 f 下原像的集合

$$G_1=f^{-1}(H_1)=\{x\in G\mid f(x)\in H_1\}\supseteq\{x\in G\mid f(x)=e'\}=\ker f$$

满足

$$(\forall x,y\in G_1):f\left(xy^{-1}\right)=f(x)f(y)^{-1}\in H_1$$

则 $xy^{-1}\in G_1$，由子群判别法 (1.1) 即得 G_1 为 G 的子群，故 $G_1\in\Sigma$，则 f^{-1} 可视为 Γ 到 Σ 的映射。由 $f\left(f^{-1}(H_1)\right)=H_1$ 得 $ff^{-1}=\mathrm{id}_\Gamma$

设 $G_1\in\Sigma$，显然 $G_1\subseteq f^{-1}(f(G_1))$，则有

$$[\forall u\in f^{-1}(f(G_1))](\exists v\in G_1):f(u)=f(v)$$

由 $ff^{-1}=\mathrm{id}_\Gamma$ 有 $uv^{-1}\in\ker f\subseteq G_1$，则有 $u\in G_1$，即有 $f^{-1}(f(G_1))=G_1$，亦即 $f^{-1}f=\mathrm{id}_\Sigma$，则 f 为 G 中包含 $\ker f$ 的子群与 H 的子群间双射

2) 设 $G_1\in\Sigma$ 且 G_1 为 G 正规子群。由性质 (1.1.5) 有

$$(\forall a\in G_1)(\forall x\in G):f(x)f(a)f^{-1}(x)=f\left(xax^{-1}\right)$$

亦即

$$(\forall f(x)\in H):f(x)f(G_1)f^{-1}(x)=f(G_1)$$

则由子群正规性充要条件 (1.9) 有 $f(G_1)$ 为 H 正规子群；

反之，若 $H_1\in\Gamma$，H_1 为 H 正规子群，由性质 (1.1.5) 有

$$(\forall b\in f^{-1}(H_1))(\forall y\in G):f\left(yby^{-1}\right)=f(y)f(b)f(y)^{-1}\in H_1$$

则 $yby^{-1}\in f^{-1}(H_1)$，则由子群正规性充要条件 (1.9) 有 $f^{-1}(H_1)$ 为 G 正规子群

3) 设 $G_1\in\Sigma$ 且 G_1 为 G 正规子群，由结论 2) 的证明有 $f(G_1)$ 为 H 正规子群。令 π' 为 H 到商群 $H/f(G_1)$ 的自然同态，则有 G 到 $H/f(G_1)$ 上群同态 $\pi'\cdot f$，注意到 $H/f(G_1)$ 单位元为 $f(G_1)$，则

$$\ker(\pi' f)=\{x\in G\mid \pi' f(x)=f(G_1)\}=\{x\in G\mid f(x)\in f(G_1)\}=f^{-1}(f(G_1))=G_1$$

设 π 为 G 到 G/G_1 的自然同态，则由群同态基本定理 (1.12) 知有 G/G_1 到 $H/f(G_1)$ 的群同构 $\bar{f}$ 满足 $G/G_1\cong H/f(G_1)$

推论 1.4

设 N 为群 G 正规子群，π 为 G 到商群 G/N 上自然同态，则 π 为 G 中所有包含 N 的子群与 G/N 的所有子群间的双射，且正规子群与正规子群相对应。又若 H 为 G 正规子群，$N\subseteq H$，则有 $G/H\cong(G/N)/(H/N)$

♡

证明 将定理 (1.13) 中 H 换成 G/N，f 换成 π，推论即证

定理 1.14 (群同态下子群与像的关系)

设 N 为群 G 正规子群，π 为 G 到商群 G/N 上自然同态，H 为 G 子群，则有下列命题成立：

1) HN 为 G 中包含 N 的子群且 $HN=\pi^{-1}(\pi(H))$

2) $H\cap N$ 为 H 正规子群且 $H\cap N=\ker(\pi|_H)$，其中 $\pi|_H$ 表示 π 在 H 上限制

3) $(HN)/N\cong H/(H\cap N)$

♡

证明 1) 根据性质 (1.1.5)，由 H 为 G 子群有 $\pi(H)$ 为 G/N 子群，且 $\pi^{-1}(\pi(H))$ 为 G 唯一包含 N 且像为 $\pi(H)$ 的子群。显然，$HN\supseteq N$，又设 $h_i\in H,n_i\in N(i=1,2)$，则有

$$h_1n_1(h_2n_2)^{-1}=h_1h_2^{-1}\left(h_2\left(n_1n_2^{-1}\right)h_2^{-1}\right)\in HN$$

则 HN 为 G 中含 N 的子群且 $\pi(h_1n_1)=\pi(h_1)\pi(n_1)=\pi(h_1)$，则 $\pi(HN)\subseteq\pi(H)$。又由 $H\subseteq HN$，则 $\pi(H)=\pi(HN)$，则有 $HN=\pi^{-1}(\pi(H))$

2) 由 N 为 G 正规子群，则 $(\forall h\in H)(\forall a\in N\cap H):hah^{-1}\in N\cap H$，则 $N\cap H$ 为 H 正规子群。又 $\pi|_H(h)=\pi(h)$，则 $\ker(\pi|_H)=H\cap N$

3) 由 $\pi(HN)=\pi(H),\ker(\pi|_{HN})=HN\cap N=N$，则 $HN/N\cong\pi(H)$，另有 $\pi(H)=\pi|_H(H),\ker(\pi|_H)=N\cap H$，则 $\pi(H)\cong H/H\cap N$，则 $(HN)/N\cong H/(H\cap N)$

1.2 特殊群

1.2.1 Sylow 子群与 Sylow 定理

定义 1.28 (群在集上作用有效与可递)

称 g 定义了群 G 在 X 上的一个作用，若当且仅当 $g=e$ 时有 $(\forall x\in X):g(x)=x$，称群 G 在 X 上作用有效；若 $(\forall x,y\in X)(\exists g\in G):y=g(x)$，则称群 G 在 X 上作用可递，称 X 为群 G 的齐性空间 ♣

定义 1.29 (轨道与迷向子群)

设群 G 作用在 X 上，$x\in X$，则称 X 中子集 $O_x=\{g(x)|g\in G\}$ 为 x 的轨道，称 G 中子集 $F_x=\{g|(g\in G)(g(x)=x)\}$ 为 x 的迷向子群 ♣

定理 1.15 (轨道与迷向子群性质)

设群 G 作用在集合 X 上，则下列命题成立：

1) 在 X 中定义关系 R:

$$xRy\Leftrightarrow(\exists g\in G)y=g(x)$$

则 R 为等价关系且 x 所在的等价类为 x 的轨道 O_x

2) G 在 O_x 上作用可递

3) G 在 O_x 上作用有效的充要条件为 F_x 中所包含的 G 的正规子群仅为 $\{e\}$

4) 设 $x,y\in X,g\in G$，若 $y=g(x)$，则有

$$F_{g(x)}=F_y=gF_xg^{-1}=\mathrm{ad}\,g\,(F_x)$$

♡

证明 1) 自反性：设 $x,y,z\in X$，由 $e(x)=x$ 即得 $(\forall x\in X)xRx$；对称性：由 $g(x)=y$ 得 $g^{-1}(y)=g^{-1}(g(x))=x$，即 $xRy\Rightarrow yRx$；传递性：由 xRy,yRz 得 $(\exists g_1,g_2\in G):[(y=g_1(x))\wedge(z=g_2(y))]$，则 $z=g_2g_1(x)$，即 xRz。则 R 为等价关系，由 R 的定义得 x 的等价类为 O_x

2) 由 1) 结论已知 $(\forall z,y\in O_x)(\exists g\in G):g(y)=z$，则 G 在 O_x 上的作用可递

3) 设 σ 为 G 到 S_{O_x} 的同态，满足 $(\forall y\in O_x):\sigma(g)y=g(y)$。则 G 在 O_x 上作用有效当且仅当 $\ker\sigma=\{e\}$。由群同态基本定理 (1.12) 有 $\ker\sigma$ 为 G 正规子群，而 $\ker\sigma\subseteq F_x$

充分性：若 F_x 中所含 G 的正规子群仅为 $\{e\}$，则必有 $\ker\sigma=\{e\}$；必要性：设 N 为 G 正规子群，$N\subseteq F_x$，则 $(\forall h\in N)(\forall g\in G):g^{-1}hg\in N\subseteq F_x$，则 $h(g(x))=g\left(g^{-1}hg(x)\right)=g(x)$，即 $h\in\ker\sigma$，即 $N\subseteq\ker\sigma$。则若 G 在 O_x 上作用有效，则有 $\ker\sigma=\{e\}$，由此得 $N=\{e\}$，即 $\{e\}$ 为 F_x 所包含的唯一的 G 的正规子群

4) 设 $g(x)=y$ 且 $g_1\in F_y$，则有 $y=g_1(y)$，则 $g_1g(x)=g(x)$，则 $g_2=g^{-1}g_1g\in F_x$，则 $g_1=gg_2g^{-1}\in\mathrm{ad}\,g\,(F_x)$；反之，若 $g_2\in F_x$，则有

$$gg_2g^{-1}(y)=gg_2g^{-1}(g(x))=g(x)=y$$

则 $gg_2g^{-1}\in F_y$，则有 $F_y=\mathrm{ad}\,g\,(F_x)$

注 该定理表明若群 G 作用在集 X 上，则可将 X 分解为轨道之并，而不同的轨道互不相交。G 在每个轨道上的作用可递，但是否有效则由迷向子群所含 G 的正规子群来决定。实际上，G 在每个轨道上的作用相当于 G 在某个左陪集空间上的作用，于是引进作用等价的概念

定义 1.30 (群在集上作用等价)

设群 G 作用在集 X 与 X' 上，若存在 X 到 X' 上的双射 ϕ 满足

$$(\forall g\in G)(\forall x\in X):g(\phi(x))=\phi(g(x))$$

则称 G 在 X, X' 上的作用等价 ♣

定理 1.16 (作用可递必要条件)

设群 G 在 X 上作用可递，$x \in X$，则 G 在 X 上作用与 G 在 G/F_x 上左平移作用等价 ♡

证明 因 G 在 X 上的作用可递，则有 $X = O_x = \{g(x) \mid g \in G\}$，构造 G/F_x 到 X 的映射 ϕ 满足 $(\forall g \in G): \phi(gF_x) = g(x)$。由 $g_1F_x = g_2F_x$ 等价于 $g_1^{-1}g_2 \in F_x$，等价于 $g_1^{-1}g_2(x) = x$，等价于 $g_1(x) = g_2(x)$，则 ϕ 为 G/F_x 到 X 上双射，又有

$$(\forall h \in G): \phi(h(gF_x)) = \phi(hgF_x) = hg(x) = h(\phi(gF_x))$$

则 G 在 G/F_x 与 X 上的作用等价

推论 1.5 (轨道基数)

设有限群 G 作用在集合 X 上，O_x 为 $x \in X$ 的轨道，则 O_x 中元素个数 $|O_x| = [G : F_x]$，进而 $|O_x| \mid |G|$ ♡

证明 G 在 O_x 上作用可递，则由定理 (1.16)，则与 G 在 G/F_x 上作用等价，则 $|O_x| = [G : F_x]$

定义 1.31 (共轭类与中心化子)

设 G 为群，$g \in G$，则称 g 在伴随作用下轨道为以 g 为代表的共轭类，记为 C_g，若 $h \in C_g$，则称 h 与 g 共轭；称 g 在伴随作用下迷向子群为 g 在 G 中的中心化子，记作 $C_G(g)$，称 G 上伴随作用的核为 G 的中心，记为 $\mathrm{Ker}(\mathrm{ad}) = C(G)$ ♣

注 (共轭类与中心化子)

若 $g, h \in G$ 共轭，即有 $k \in G$ 满足 $h = kgk^{-1}, C_g = \{kgk^{-1} \mid k \in G\}$, $C_G(g) = C(g) = \{k \in G \mid kg = gk\}, C(G) = \ker ad = \{k \in G \mid kg = gk, \forall g \in G\}$

定理 1.17 (共轭类，中心化子，中心性质)

设 G 为群，则下列命题成立：

1) $C(G)$ 为 G 的正规子群且 $\mathrm{ad}\, G$ 与 $G/C(G)$ 同构
2) G 中共轭关系为等价关系，进而 G 的共轭类集为 G 的划分
3) 若 G 为有限群，$g \in G$，则 g 共轭类 C_g 基数满足 $|C_g| = [G : C(g)]$，进而为 $|G|$ 的因数
4) $h \in C(G)$ 等价于 $|C_h| = 1$ 等价于 $h \in \bigcap\limits_{g \in G} C(g)$

♡

证明 由定理 (1.15) 与定理 (1.17)，及共轭、$C(g), C(G)$ 的定义即证

定义 1.32 (p 群)

设 p 为素数，若群 G 的阶为 p 的方幂，即 $|G| = [G : e] = p^k (k \in \mathbb{N})$，$e$ 为 G 的么元，则称 G 为一个 p 群 ♣

定理 1.18 (p 群在集上作用性质)

设 p 群 G 作用在集 X 上，$|X| = n$，则下列命题成立：

1) $t \equiv n (\mathrm{mod} p)$，其中 $t = |\{x \in X \mid (\forall g \in G): g(x) = x\}|$
2) 当 $(n, p) = 1$ 时，$t \geqslant 1$，即 $(\exists x \in X)(\forall g \in G): g(x) = x$
3) G 的中心 $C(G) \neq \{e\}$

♡

证明 1) 设 X 的轨道可分解为 $X=O_{x_1}\cup O_{x_2}\cup\cdots\cup O_{x_m}$，则当且仅当 $|O_x|=1$ 时 $(\forall g\in G):g(x)=x$，则

$$n=t+\sum_{|O_{x_i}|\neq 1}|O_{x_i}|$$

由推论 (1.5) 得 $|O_{x_i}|\,||G|$。由 G 为 p 群，$|O_{x_i}|>1$，则 $p\,||O_{x_i}|$

2) 若 $(n,p)=1$，则由 1) 得 $t\neq 0$，则 2) 成立

3) 考虑 G 在 G 上的伴随作用，当且仅当 $x\in C(G)$ 时 $(\forall g\in G):\mathrm{ad}\,g(x)=x$。显然 $e\in C(G)$，则 $|C(G)|\geqslant 1$，又 $p\,||G|$，则由 1) 得 $|G|\equiv|C(G)|(\mathrm{mod}p)$，则 $|C(G)|>1$，即 $C(G)\neq\{e\}$

引理 1.1

设 p 为素数，$n=p^lm,(m,p)=1$，若 $k\in\mathbb{N},k\leqslant l$，则 $p^{l-k}\|C_n^{p^k}$，其中 $\|$ 表示恰能整除，$C_n^{p^k}$ 为组合数 ♡

证明 由组合数定义有

$$C_n^{p^k}=\frac{n}{p^k}\frac{n-1}{p^k-1}\cdots\frac{n-(p^k-1)}{p^k-(p^k-1)}=\prod_{i=0}^{p^k-1}\frac{n-i}{p^k-i}$$

则设 i 满足 $1\leqslant i\leqslant p^k-1$ 且 i 有分解 $i=jp^t$，其中 $(j,p)=1$，则有 $t<k\leqslant l$，这时

$$n-i=p^lm-p^tj=p^t\left(p^{l-t}m-j\right)$$

$$p^k-i=p^t\left(p^{k-t}-j\right)$$

则 $p^t\|(n-i),p^t\|\left(p^k-i\right)$，则 $p^{l-k}\|C_n^{p^k}$

定义 1.33 (Sylow p 子群)

设 G 为 p^lm 阶群，p 为素数且 $(p,m)=1$，则称 G 的 p^l 阶子群为 G 的 Sylow p 子群 ♣

定理 1.19 (Sylow 第一定理)

设 G 为 p^lm 阶群，其中 p 为素数，$l\geqslant 1,(p,m)=1$，则对任意 $1\leqslant k\leqslant l$，G 中必有 p^k 阶子群 ♡

证明 设 X 为 G 中所有含 p^k 个元素的子集的集合，即 $X=\left\{A\subseteq G\,|\,|A|=p^k\right\}$，显然 $|X|=C_n^{p^k}$，其中 $n=p^lm$。另外，映射 $G\times X\to X,(g,A)\mapsto f(g,A)=gA=\{ga\mid a\in A\}$ 定义了 G 在 X 上作用，则 X 有轨道分解

$$X=\bigcup O_A,\quad |X|=\sum|O_A|$$

由引理 (1.1) 得 $p^{l-k}||C_n^{p^k}$，则 $(\exists A\in X):p^{l-k+1}\nmid|O_A|$。设 F_A 为 A 的迷向子群，则由推论 (1.5) 与 Lagrange 定理 (1.10) 有

$$|O_A|=[G:F_A]=\frac{p^lm}{[F_A:e]}$$

则 $p^k\,|\,[F_A:e]$

另一方面有 $(\forall a\in A)(\forall g\in F_A):g(a)=ga\in A$，则 $F_A\cdot a\subseteq A$，则 $|F_A\cdot a|=|F_A|\leqslant|A|=p^k$。由此得 $[F_A:e]=p^k$，即 F_A 为 p^k 阶子群

注 该定理给出了 Sylow p 子群的存在性

定理 1.20 (Sylow 第二定理)

设 G 为 p^lm 阶群，p 为素数，$(p,m)=1$，若 P 为 G 的 Sylow p 子群，H 为 G 的 p^k 阶子群，则 $(\exists g\in G):H\subseteq gPg^{-1}$。特别地，$G$ 的 Sylow p 子群相互共轭 ♡

证明 将 G 在 G/P 上左平移作用限制在 H 上，则有 H 在 G/P 上左平移作用

$$(\forall h\in H)(\forall g\in G):h(gP)=hgP$$

由 $|H|=p^k,|G/P|=m,(p,m)=1$，则由定理 (1.18) 的结论 2) 有 G/P 中含有元素 gP，其轨道仅含 gP，即 $(\forall h\in H):hgP=gP$，则 $hg\in gP,H\subseteq gPg^{-1}$

特别地，若 $|H|=p^l$，则 $H=gPg^{-1}$

定理 1.21 (Sylow 第三定理)

设 G 为 p^lm 阶群，p 为素数，$(p,m)=1$，又设 G 中 Sylow p 子群的个数为 k，则有下列命题成立：

1) 当且仅当 $k=1$ 时，G 的 Sylow p 子群 P 为 G 的正规子群

2) $k\mid m,k\equiv 1(\mathrm{mod}p)$

♡

证明 1) 设 P 为 G 的 Sylow p 子群，显然对于 $\forall g\in G,gPg^{-1}$ 也为 G 的 Sylow p 子群。又若 P_1 为 G 的另一 Sylow p 子群，由 Sylow 第二定理 (1.20) 有 $(\exists g_1\in G):g_1Pg_1^{-1}=P_1$，则 $X=\left\{gPg^{-1}\mid g\in G\right\}$ 为 G 中 Sylow p 子群的集合

若 $|X|=1$，即 $gPg^{-1}=P(\forall g\in G)$，则 P 为 G 正规子群；反之，若 P 为 G 正规子群，则 $gPg^{-1}=P$，故 $|X|=1$

2) 设 $|X|=k$，则 $G\times X$ 到 X 的映射

$$f(g,P_1)=gP_1g^{-1},\quad \forall g\in G,P_1\in X$$

定义了 G 在 X 上作用，由 Sylow 第二定理 (1.20) 有该作用可递。设 F_P 为 P 的迷向子群，即

$$F_P=\left\{g\in G,\mid gPg^{-1}=P\right\}=N_G(P)$$

显然，P 为正规子群 F_P，则 $p^l\mid |F_P|$，则

$$k=|X|=[G:F_P],\quad [G:F_P]\mid m$$

将上面 G 在 X 上的作用限制为 P 在 X 上的作用，显然 $P\in X,P$ 在 P 作用下的轨道 $O'_P=\{P\}$。若另有 $P_1\in X$，在 P 作用下的轨道 $O'_{P_1}=\{P_1\}$，即有 $gP_1g^{-1}=P_1(\forall g\in P)$。由 Sylow 第二定理 (1.20) 有 $(\exists h\in G):P_1=hPh^{-1}$，则 $g\left(hPh^{-1}\right)g^{-1}=hPh^{-1}$，则 $h^{-1}gh\in F_P$。则 $h^{-1}Ph,P$ 均为 F_P 的 Sylow p 子群，又 P 为 F_P 正规子群，则由 1) 得 $h^{-1}Ph=P$，则 $P=P_1$，则包含一个元素的 X 的轨道仅有一个，由定理 (1.18) 结论 1) 有 $k\equiv 1(\mathrm{mod}p)$

1.2.2 可解群与幂零群

1902 年，英国群论学家 William Burnside 通过长期探索发现：4 万阶以下的奇数阶群都可解，于是他猜想任意奇数阶群都可解，这即为群论发展史上起到重大作用的 Burnside 猜想。该猜想后来被 Feit 和 Thompson 合作证明。他们的证明长达 255 页，开启了群论学家写长文章的先河

定义 1.34 (换位子群)

设 G 为群，$g,h\in G$，称 $g^{-1}h^{-1}gh$ 为 g,h 的换位子，记为 $[g,h]$，若 H,K 都为 G 的子群，称

$$[H,K]=\langle\{[h,k]\mid h\in H,k\in K\}\rangle$$

为 H,K 的换位子群。特别地，称 $[G,G]$ 为 G 的换位子群（或称导群）

♣

性质 （换位子性质）

设 G 为群，$g,h\in G$，则下列命题成立：

1) （换位性）$[g,h]^{-1}=[h,g]$

2) （群元素可换充要条件）$gh=hg$ 的充要条件为 $[g,h]=1$

3) （群同态保换位性）设 $\varphi:G\to H$ 为群同态，$g,h\in G$，则 $\varphi([g,h])=[\varphi(g),\varphi(h)]$

性质 （换位子群性质）

设 H,K 为群 G 的正规子群，则下列命题成立：

1)（正规子群换位子群保正规性）$[H,K]$ 为 G 的正规子群

2)（正规子群换位子群为交集子集）$[H,K]\subseteq H\cap K$

证明 1) 取 $\varphi=\mathrm{ad}g,g\in G$，则 $(\forall h\in H)(\forall k\in K):\mathrm{ad}\,g([h,k])=[\mathrm{ad}\,g(h),\mathrm{ad}\,g(k)]$。由 H,K 为 G 的正规子群，$\mathrm{ad}\,g(h)\in H,\mathrm{ad}\,g(k)\in K$，则 $\mathrm{ad}_g([h,k])\in[H,K]$，则 $[H,K]$ 为 G 的正规子群

2) 由 $h^{-1}k^{-1}h\in K,k^{-1}hk\in H$，则 $[h,k]=h^{-1}k^{-1}hk\in H\cap K$，则 $[H,K]\subseteq H\cap K$

注 特别地，就推出群 G 的换位子群为 G 的正规子群

性质（相对正规子群商群交换性充要条件）

设 N 为群 G 的正规子群，则 G/N 为 Abel 群的充要条件为 $[G,G]\subseteq N$

证明 设 $\pi:G\to G/N$ 为自然同态，则 G/N 为 Abel 群当且仅当 $(\forall x,y\in G):\pi(x)\pi(y)=\pi(y)\pi(x)$，当且仅当 $\pi\left(x^{-1}y^{-1}xy\right)=\bar{e}$（$\bar{e}$ 为 G/N 的单位元），当且仅当 $[x,y]\in\mathrm{Ker}\,\pi=N$，当且仅当 $[G,G]\subseteq N$

注 特别地，有 $G/[G,G]$ 为 Abel 群

定义 1.35（导出列、降中心列和升中心列归纳定义）

在群 G 中归纳定义 $\left\{G^{(k)}\right\},\{\Gamma_k(G)(\text{ 或 }G^k)\},\{C_k(G)\}$ 为

$$G^{(0)}=G,\quad G^{(k)}=\left[G^{(k-1)},G^{(k-1)}\right],\quad k\geqslant 1$$

$$G^1=\Gamma_1(G)=G,\quad G^k=\Gamma_k(G)=[G,\Gamma_{k-1}(G)]=[G,G^{k-1}],\quad k\geqslant 2$$

$$C_0(G)=\{1\},\quad C_k(G)/C_{k-1}(G)=C\left(G/C_{k-1}(G)\right),\quad k\geqslant 1$$

则称群 G 中序列

$$G=G^{(0)}\supseteq G^{(1)}\supseteq G^{(2)}\supseteq\cdots$$

$$G=\Gamma_1(G)\supseteq\Gamma_2(G)\supseteq\cdots$$

$$C_0(G)\subseteq C_1(G)\subseteq C_2(G)\subseteq\cdots$$

为 G 的导出列、降中心列和升中心列 ♣

注（升中心列存在性）

需指出 $C_k(G)$ 存在，显然 $C_1(G)=C(G)$。设 π_1 为 G 到 $G/C_1(G)$ 上自然同态，令

$$C_2(G)=\pi_1^{-1}\left(C\left(G/C_1(G)\right)\right)$$

则 $C_2(G)$ 为 G 正规子群且

$$C_1(G)\subseteq C_2(G),\quad C_2(G)/C_1(G)=C\left(G/C_1(G)\right)$$

再令 π_2 为 G 到 $G/C_2(G)$ 上自然同态，则

$$C_3(G)=\pi_2^{-1}\left(C\left(G/C_2(G)\right)\right)$$

继续进行即得所有 $C_k(G)$

定义 1.36（可解群与幂零群）

设 G 为群，若 $(\exists k\in\mathbb{N}^*):G^{(k)}=\{e\}$，则称 G 为可解群，若 $(\exists k\in\mathbb{N}^*):G^k=\{e\}$，则称 G 为幂零群 ♣

性质（可解群性质）

设 G 为群，H 为群 G 子群，N 为群 G 正规子群，则下列命题成立：

1)（可解群子群可解性）若 G 为可解群，则子群 H 为可解群

2)（关于正规子群商群群可解性必要条件）若 G 为可解群，则商群 G/N 为可解群

3)（关于正规子群商群群可解性充分条件）若正规子群 N 与商群 G/N 为可解群，则 G 为可解群

证明 1) 由 H 为 G 子群，则 $H^{(k)}\subseteq G^{(k)}$，由 G 为可解群，则由可解群定义与群同态保幺性 (1.1.5) 有 H 可解

2) 由 N 为群 G 正规子群，考虑自然同态 $\pi:G\to G/N$，则 $(\forall g,h\in G):\pi([g,h])=\pi\left(g^{-1}h^{-1}gh\right)=[\pi(g),\pi(h)]$，则 $\pi\left(G^{(k)}\right)=(\pi(G))^{(k)}=(G/N)^{(k)}$。由 G 可解，则由可解群定义与群同态保幺性 (1.1.5) 有 G/N

可解

3) 若 G/N 可解，则 $(k\in\mathbb{N}):(G/N)^{(k)}=\{\bar{e}\}$，则 $\pi\left(G^{(k)}\right)=(\pi(G))^{(k)}=(G/N)^{(k)}=\{\bar{e}\}$，则 $G^{(k)}\subseteq \operatorname{Ker}\pi=N$。由 N 可解与 1) 结论，其子群 $G^{(k)}$ 也可解，则存在 $l\in\mathbb{N}$ 使得 $\left(G^{(k)}\right)^{(l)}=\{e\}$，则 $G^{(k+l)}=\left(G^{(k)}\right)^{(l)}=\{e\}$，则 G 可解

定理 1.22 (Abel 群单性充要条件)

设 G 为 Abel 群，则 G 为单群（无非平凡正规子群）的充要条件为 G 为素数阶群 ♡

证明 充分性：由 G 为 Abel 群，则对 $(\forall a\in G)(a\neq e)$ 有 $\langle a\rangle$ 为 G 的正规子群。若 G 为单群，则 $G=\langle a\rangle$ 为循环群；若 G 为无限群，则有 $\langle a^2\rangle$ 为 G 非平凡正规子群；若 $|G|=n$ 不为素数，设 k 为其非平凡因子，则 $\langle a^k\rangle$ 为 G 的非平凡正规子群，则 Abel 单群仅能为素数阶群

必要性：若 G 的阶为素数 p，则 a 的阶为 p 的因子，则也为 p，则 $\langle a\rangle=G$，则 G 的子群仅有 G 和 $\{e\}$，则 G 为单群

定义 1.37 (次正规序列与正规序列)

设群 G 中有子群序列

$$G=G_1\supset G_2\supset\cdots\supset G_t\supset G_{t+1}=\{e\} \tag{1.7}$$

若满足 G_{i+1} 为 $G_i(i=1,\cdots,t)$ 的正规子群，记为 $G_{i+1}\triangleleft G_i(i=1,\cdots,t)$，则称序列为次正规序列，称 t 为次正规序列的长度，称 G_i/G_{i+1} 为次正规序列的因子；此外，若在次正规序列中 G_i 为 G 正规子群，则称此序列为正规序列

若 G 的次正规序列的因子 G_i/G_{i+1} 都为单群，则称该次正规序列为 G 的合成序列，称 G_i/G_{i+1} 为 G 的合成因子；若合成序列为正规序列，则称该序列为主序列

若序列 (1.7) 中的每个子群 G_i 都在序列 (1.8) 中出现，则称群 G 中的次正规序列 (1.8)

$$G=G_1'\supset G_2'\supset\cdots\supset G_s'\supset G_{s+1}'=\{e\} \tag{1.8}$$

为序列 (1.7) 的加细 ♣

定理 1.23 (有限群可解性充要条件)

设 G 为有限群，则下列条件等价：

1) G 为可解群

2) 存在 G 的正规序列 $G=G_1\supset G_2\supset\cdots\supset G_t=\{e\}$ 使得 G_i/G_{i+1} 为 Abel 群，其中 $i=1,2,\cdots,t-1$

3) 存在 G 的次正规序列 $G=G_1'\supset G_2'\supset\cdots\supset G_s'=\{e\}$ 使得 G_i'/G_{i+1}' 为 Abel 群，其中 $i=1,2,\cdots,s-1$

4) 存在 G 的次正规序列 $G=G_1''\supset G_2''\supset\cdots\supset G_r''=\{e\}$ 使得 G_i''/G_{i+1}'' 为素数阶群，其中 $i=1,2,\cdots,r-1$ ♡

证明 1)⇒ 2) 由 G 可解，则 G 的导出列即为一个正规序列，其因子都为 Abel 群

2)⇒ 3) 显然

3)⇒ 4) 将 3) 的次正规序列加细为合成序列，其合成因子为 Abel 单群，由 Abel 群单性充要条件 (1.22) 有 Abel 单群为素数阶群

4)⇒ 1) 由 G_r'' 和 G_{r-1}''/G_r'' 都为素数阶群，则为可解群。由性质 (1.2.2) 得 G_{r-1}'' 为可解群。归纳：若 G_i'' 可解，因 G_{i-1}''/G_i'' 为素数阶群，则 G_{i-1}'' 也为可解群，则 $G=G_1$ 也为可解群

1.2.3 自由幺半群与自由群

由一个非空集合构造么半群与群的思想或方法, 就是所谓自由么半群与自由群的思想和方法. 这种思想和方法不仅在群论中, 而且在其他数学分支中都是重要的

定义 1.38 (自由么半群)

设 $X=\{a_1,a_2,\cdots,a_n\}$ 为一个集合，称 X 中有限长序列

$$x_1x_2\cdots x_i,\quad x_1,x_2,\cdots,x_i\in X$$

为字，当 $i=0$ 时，称该序列为空字，记为 $\wedge$

记所有字的集合为 $\tilde{X}$，在 $\tilde{X}$ 上定义乘法

$$(x_1x_2\cdots x_i)(y_1y_2\cdots y_j)=x_1x_2\cdots x_iy_1y_2\cdots y_j$$

显然 $\tilde{X}$ 对该乘法为以 $\wedge$ 为单位元的么半群，称该么半群为由 X 生成的自由么半群

♣

定理 1.24

设集合 X 非空，S 为么半群，f 为 X 到 S 的映射，则存在唯一的从 $\tilde{X}$ 到 S 的同态 ϕ，满足

$$(\forall x\in X):\phi(x)=f(x)$$

♡

证明 存在性：定义 $\tilde{X}$ 到 S 的映射 $\phi:\phi(\wedge)=e$，e 为 S 的单位元，$\phi(x_1x_2\cdots x_i)=f(x_1)f(x_2)\cdots f(x_i)$，则 ϕ 显然为同态

唯一性：若 ψ 为 $\tilde{X}$ 到 S 的同态且 $\psi(x)=f(x)$，则

$$\psi(x_1x_2\cdots x_i)=\psi(x_1)\psi(x_2)\cdots\psi(x_i)=f(x_1)f(x_2)\cdots f(x_i)=\phi(x_1x_2\cdots x_i)$$

即 ϕ 唯一

注 由此得任意么半群均可视为自由么半群的同态像

定义 1.39 (相邻)

设集合 $X=\{a_1,a_2,\cdots,a_n\}$，集合 $X'=\{a_1',a_2',\cdots,a_n'\},X\cap X'=\varnothing$，又 $a_i\mapsto a_i'$ 为 X 到 X' 上的双射，设 $X^*=X\cup X'$，设 $x\in X^*$，定义 x' 为

$$x'=\begin{cases}a_i, & x=a_i'\\ a_i', & x=a_i\end{cases}\tag{1.9}$$

并且记 X^* 生成的自由么半群为 $\widetilde{X^*}$

设 $w_1,w_2\in\widetilde{X^*}$ 且 $(\exists g,h\in\widetilde{X^*})(\exists x\in X^*)$ 满足

$$\begin{cases}w_1=gh\\ w_2=gxx'h\end{cases}\quad\text{或}\quad\begin{cases}w_1=gxx'h\\ w_2=gh\end{cases}$$

则称 w_1 与 w_2 相邻

♣

定理 1.25 (自由群存在性)

$\widetilde{X^*}$ 为集合 X^* 生成的自由么半群，在 $\widetilde{X^*}$ 中定义关系 $\sim$: $w_1,w_2\in\widetilde{X^*}$，则 $w_1\sim w_2$。若存在 $\widetilde{X^*}$ 中序列 $w_1=v_1,v_2,\cdots,v_l=w_2$ 满足 v_i 与 v_{i+1} 相邻，则 “$\sim$” 为 $\widetilde{X^*}$ 中同余关系，并且 $\widetilde{X^*}$ 对于 $\sim$ 的商么半群 $\widetilde{X^*}/\sim=F(X)$ 为群

♡

证明 1) 首先证 $\sim$ 为等价关系。$(\forall w\in\widetilde{X^*})$，取 $v_1=w=w\wedge,v_2=wa_1a_1'\wedge,v_3=w\wedge=w$，则 v_1 与 v_2 相邻，v_2 与 v_3 相邻，则有 $w\sim w$。又设 $w_1\sim w_2$，即有 $w_1=v_1,v_2,\cdots,v_l=w_2$ 且 v_i 与 v_{i+1} 相邻。令 $u_i=v_{l-i+1}$，

则 $u_1=w_2,u_2,\cdots,u_l=w_1$ 且 u_i 与 u_{i+1} 相邻，则 $w_2\sim w_1$。再设 $w_1\sim w_2,w_2\sim w_3$，则存在序列：

$$w_1=v_1,v_2,\cdots,v_l=w_2,\quad v_i\text{ 与}v_{i+1}\text{ 相邻}$$

$$w_2=u_1,u_2,\cdots,u_m=w_3,\quad u_j\text{ 与}u_{j+1}\text{ 相邻}$$

则序列 $w_1=v_1,v_2,\cdots,v_l=u_1,u_2,\cdots,u_m=w_3$ 的任意挨着两项相邻，则 $w_1\sim w_3$

2) 证 $\sim$ 为同余关系。注意到，若 u_1 与 u_2 相邻，即有 $u_1=gh,u_2=gxx'h$，则对任意 v 有 $u_1v=ghv,u_2v=gxx'hv$，则 u_1v 与 u_2v 相邻。同理有 vu_1 与 vu_2 相邻。设 $w_1\sim w_2,u_1\sim u_2$，则由序列

$$w_1u_1=v_1u_1,v_2u_1,\cdots,v_lu_1=w_2u_1$$

得 $w_1u_1\sim w_2u_1$，同理 $w_2u_1\sim w_2u_2$，则 $w_1u_1\sim w_2u_2$，即 $\sim$ 为同余关系

3) 证明商么半群 $F(X)=\widetilde{X^*}/\sim$ 为群，仅需证 $F(X)$ 中任一元素可逆。对 $\forall x\in\widetilde{X}^*,\wedge$ 为空字，x' 如式 (1.9)，则有 $\wedge xx'\wedge=xx',\wedge=\wedge\wedge$，即 xx' 与 $\wedge$ 相邻，因而 $\wedge\sim xx'$。又若 $x_1x_2\cdots x_m\in\widetilde{X^*}$，则有 $x'_mx'_{m-1}\cdots x'_2\in\tilde{X}^*$ 且

$$(x_1x_2\cdots x_m)\left(x'_mx'_{m-1}\cdots x'_1\right)=x_1x_2\cdots x_mx'_m\cdots x'_1\sim\wedge$$

则 $F(X)$ 中元素均可逆，则为群

注 称 $\widetilde{X^*}/\sim=F(X)$ 为由 X 生成的自由群

定理 1.26

设 X 为一非空集，G 为群，又 f 为 X 到 G 的映射，则存在唯一的 $F(X)$ 到 G 的同态 ψ 满足 $(\forall x\in X):\psi(\bar{x})=f(x)$，其中 $\bar{x}$ 表示 x 在 $F(X)=\widetilde{X^*}/\sim$ 中的同余类 ♡

证明 首先将 f 延拓为 X^* 到 G 的映射，仍以 f 表示，满足 $((\forall x'\in X')):f(x')=f(x)^{-1}$，由定理 (1.24) 得有唯一的么半群 $\widetilde{X^*}$ 到 G 的同态 ϕ 满足 $(\forall x\in X^*):\phi(x)=f(x)$，若 $\widetilde{X^*}$ 中元素 w_1 与 w_2 相邻，不妨设

$$w_1=gh,w_2=gxx'h,\quad g,h\in\widetilde{X^*},\quad x,x'\in X^*$$

其中 x' 如式 (1.9)，则有

$$\phi(w_2)=\phi(g)\phi(x)\phi(x')\phi(h)=\phi(g)\phi(h)=\phi(w_1)$$

即得 $w_1\sim w_2\Rightarrow\phi(w_1)=\phi(w_2)$

对于 $F(X)=\widetilde{X^*}/\sim$ 中的元素 $\bar{w}$，定义 $\psi(\bar{w})=\phi(w)$，则有 ψ 为同态且 $(\forall x\in X):\psi(\bar{x})=f(x)$，显然 ψ 唯一

推论 1.6

设 G 为有限生成群，则 G 同构于一个自由群的商群 ♡

证明 设 $G=\langle g_1,g_2,\cdots,g_n\rangle,X=\{a_1,a_2,\cdots,a_n\}$，定义 X 到 G 的映射 f：

$$(\leqslant i\leqslant n):f(a_i)=g_i$$

于是由定理 (1.26) 有 $F(X)$ 到 G 的同态 ψ 满足

$$\psi(a_i)=f(a_i)=g_i,\quad 1\leqslant i\leqslant n,$$

则 $\psi(F(X))=G$，则 $G\cong F(X)/\ker\psi$

注 称 $\ker\psi$ 为 G 的生成元 $g_1,g_2,\cdots,g_n$ 间的**关系集**。若 $\ker\psi$ 也由有限个元素 $w_1,w_2,\cdots,w_r$ 生成，则称 G **可有限表现**，称

$$\psi(w_i)=e,\quad 1\leqslant i\leqslant r$$

为 G 的生成元 $g_1,g_2,\cdots,g_n$ 的一组**生成关系**

第 2 章 环

2.1 基本概念

2.1.1 环公理化

定义 2.1 (ring/环)

设 $\mathcal{R}$ 是一个非空集合，如果 $\mathcal{R}$ 中有两种二元运算，且满足以下条件：

(1) $\mathcal{R}$ 对于其中一种运算（称为“加法”）构成一个 Abelian 群，即 $\{R;+\}$ 满足下列条件：

1. R 对运算“$+$”封闭
2. 对任何 $a,b,c\in R,(a+b)+c=a+(b+c),a+b=b+a$
3. R 中存在对“$+$”的单位元，写成零元 0，使得 $a+0=a,\forall a\in R$
4. 对任何 $a\in R$，存在 a' 使得 $a+a'=0$。将 a' 记为 $-a$，称为 a 的负元

(2) $\mathcal{R}$ 对于另外一种运算（称为“乘法”）构成半群，即对任何 $a,b,c\in R$，有 $(ab)c=a(bc)$

(3) $\mathcal{R}$ 对于上述的两种运算满足左右分配律：

$$(\forall a,b,c\in R):a(b+c)=ab+ac,\ (a+b)c=ac+bc$$

则称 R 为一个环。有时为了更加清楚，也说 $\{R;+,\cdot\}$ 为一个环

♣

定义 2.2 (环第一公理化)

利用下面九条性质可以公理化定义环：

R_1：（加法运算存在性）$(\exists+:R\times R\to R)(\forall a,b\in R)(\exists!c\in G):(c=a+b)$

R_2：（加法结合性）$(\forall a,b,c\in R):a+(b+c)=(a+b)+c$

R_3：（加法左中性元存在性）$(\exists e\in R)(\forall a\in R):e+a=a$

R_4：（加法左对称元存在性）$(\forall a\in R)(\exists b\in R):b+a=e$

R_5：（加法交换性）$(\forall a,b\in R)(a+b=b+a)$

R_6：（乘法运算存在性）$(\exists\cdot:G\times G\to G)(\forall a,b\in G)(\exists!c\in R):(c=a\cdot b)$

R_7：（乘法对加法左分配律）$(\forall a,b,c\in R):c\cdot(a+b)=c\cdot a+c\cdot b$

R_8：（乘法对加法右分配律）$(\forall a,b,c\in R):(a+b)\cdot c=a\cdot c+b\cdot c$

R_9：（乘法结合性）$(\forall a,b,c\in R):a\cdot(b\cdot c)=(a\cdot b)\cdot c$

称符合公理 R_1-R_9 的代数系统 $(R,+,\cdot)$ 为结合环 (associative ring)（不引起歧义时经常简称为环 (ring)），其中的 Abel 群 $(R,+)$ 满足公理 R_1-R_5，称为环 $(R,+,\cdot)$ 的加法群，称 $(R,\cdot)$ 为环 $(R,+,\cdot)$ 的乘法半群；特别地，若仅符合公理 R_1-R_8，则称代数系统 $(R,+,\cdot)$ 为非结合环 (non-associative ring)

若结合环 $(R,+,\cdot)$ 有乘法单位元，则称结合环 $(R,+,\cdot)$ 为有单位元的结合环（或含幺结合环，不引起歧义时简称含幺环）；若结合环 $(R,+,\cdot)$ 有乘法交换性，则称结合环 $(R,+,\cdot)$ 为交换结合环 (commutative associative ring)（不引起歧义时简称交换环 (commutative ring)）

♣

注 （环公理化）

类似前面群的公理化过程，也有环的第二种公理化方法，不再说明。具体的性质的证明与前面群的证明完全相同，只是替换了符号

性质 左零元也为右零元，左相反元也为右相反元

性质 （零元唯一性）

$(\exists!0\in R)(\forall a\in R):(a+0=0+a=a)$

性质 （可减性）

$$(\forall a,b\in R):[(\exists x\in R)(a+x=b)\wedge(\exists y\in R)(y+a=b)]$$

性质 （减法唯一性）

$$(\forall a,b\in R):[(\exists! x\in R)(a+x=b)\wedge(\exists! y\in G)(y+a=b)]$$

定义 2.3 (无零因子环)

称任意两个非零元的积不为零的环为无零因子环。设 R 为环，$a,b\in R$ 且 $a\neq 0,b\neq 0$，若 $ab'=0$，则称 a 为 R 的一个左零因子 (left zero divisor)，b 为 R 的一个右零因子 (right zero divisor)，称同时为左零因子和右零因子的非零元为零因子 (zero divisor)，不引起歧义时有时记为 0

称无零因子含幺交换环为整环 (domain)

♣

2.2 初等数论基本结构

2.2.1 模 p 整数环与同余

可以先引入带余除法后再引入同余类，本节不这么做，考虑从由模 p 整数环引入的同余理论来引入经典的初等数论

定义 2.4 (整除)

设 a,b 为任意两个有理整数，其中 $b\neq 0$，若

$$(\exists q\in\mathbb{Z}):a=bq$$

则称 b 整除 a 或 a 被 b 整除，记为 $b\mid a$，称 b 为 a 的因数 (factor)，称 a 为 b 的倍数 (multiple)。反之，若整数 q 不存在，则称 b 不能整除 a 或 a 不能被 b 整除，记为 $b\nmid a$

♣

定理 2.1 (倍数线性组合性质)

若有理整数 a,b 都为有理整数 m 的倍数，则 $a\pm b$ 也为 m 的倍数

♡

证明 由 a,b 为 m 的倍数，则存在两个有理整数 a_1,b_1 满足 $a=a_1m,b=b_1m$，则有 $a\pm b=(a_1\pm b_1)m$ 由 $a_1\pm b_1$ 为整数，则 $a\pm b$ 也为 m 的倍数

推论 2.1 (倍数线性组合性质)

若有理整数 $a_1,a_2,\cdots,a_n$ 均为 m 的倍数，$q_1,q_2,\cdots,q_n$ 为任意 n 个有理整数，则 $q_1a_1+q_2a_2+\cdots+q_na_n$ 为 m 的倍数

♡

定理 2.2 (同余类存在性)

设 $\mathbb{Z}$ 为有理整数集，取有理整数 $q\geqslant 1$ 且考虑关系：p 整除 $x-y$，$x,y\in\mathbb{Z}$。则该关系为 $\mathbb{Z}$ 上等价关系

♡

证明 关系 p 整除 $x-x$ 显然为真；关系 p 整除 $x-y$ 显然蕴含关系 p 整除 $y-x$；若 p 整除 $x-y$ 且 p 整除 $y-z$，则由定理 (2.1) 有 p 整除 $x-z=(x-y)+(y-z)$

注 称该 $\mathbb{Z}$ 上等价关系为模 p 同余，经常记为

$$x\equiv y(\mathrm{mod}p)$$

读作 “x 模 p 同余于 y”，同余理论在数论里起着奠基的作用

定义 2.5 (带余除法)

考虑 $\mathbb{Z}$ 上等价关系“模 p 同余”，假定 $p \geqslant 1$。对于所有 $x \in \mathbb{Z}$，等价类 F_x 显然由形如 $x+np$ 的有理整数组成，其中 n 为任意一个有理整数，而这些类刚好有 p 个。则对于所有 $x \in \mathbb{Z}$ 可以写出

$$x = np + r \quad (0 \leqslant r < p)$$

称该式为“x 除以 p 的带余除法”，称 n 为 x 除以 p 的不完全商，称 r 为 x 除以 p 的余数

定理 2.3 (带余除法唯一性)

若 a, b 为两个有理整数，其中 $b > 0$，则有

$$(\exists q, r \in \mathbb{Z}) : a = bq + r, 0 \leqslant r < b$$

成立且 q 及 r 惟一

证明 作序列 $\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots$，则 a 必在上述序列的某两项之间，即存在一个整数 q 使得 $qb \leqslant a < (q+1)b$ 成立。令 $a - qb = r$，则 $a = bq + r$，而 $0 \leqslant r < b$。

下证 q, r 惟一性：设 q_1, r_1 是满足条件的两个整数，则

$$a = b_{q_1} + r_1, 0 \leqslant r_1 < b$$

则 $a = b_{q_1} + r_1, 0 \leqslant r_1 < b, bq_1 + r_1 = bq + r$ 则 $b(q - q_1) = r_1 - r$，于是由 r 及 r_1 都是小于 b 的正有理整数，则上式右边小于 b。若 $q \neq q_1$，则上式左边 $\geqslant b$，矛盾，因此 $q = q_1$ 而 $r = r_1$

定理 2.4 (模 p 同余与带余除法等价性)

设有理整数 x, y 对模 p 同余的充要条件为 $p \mid a - b$，即 $a = b + np, t \in \mathbb{Z}$

证明 设 $a = pq_1 + r_1, b = pq_2 + r_2, 0 \leqslant r_1 < p, 0 \leqslant r_2 < p$，若 $a \equiv b (\bmod p)$，则 $r_1 = r_2$，因此 $a - b = p(q_1 - q_2)$。反之若 $p \mid a - b$，则 $p \mid p(q_1 - q_2) + (r_1 - r_2)$，因此 $p \mid r_1 - r_2$，但这时 $|r_1 - r_2| < p$，则 $r_1 = r_2$

注 该定理表明 x 被 p 除余数确定类 F_x，而模 p 每个类为下列两两不同的等价类之一：

$$\mathrm{F}_0, \mathrm{F}_1, \cdots, \mathrm{F}_{p-1}$$

注 称定理中等价类为**模 p 同余类**，若 $a_0, a_1, \cdots, a_{p-1}$ 为 p 个有理整数，并且其中任意两数都不属于同一个同余类，则称 $(a_0, a_1, \cdots, a_{p-1})$ 为模 p 的一个**完全同余系**，其中每个数为**模 p 整数**。特别地，称 $0, 1, \cdots, p-1$ 为模 p 的**最小非负完全同余系**；当 p 为偶数时，称 $-\frac{m}{2}, \cdots, -1, 0, 1, \cdots, \frac{m}{2} - 1$ 或 $-\frac{m}{2} + 1, \cdots, -1, 0, 1, \cdots, \frac{m}{2}$ 为模 p 的**绝对最小非负完全同余系**；当 p 为奇数时，称 $-\frac{m-1}{2}, \cdots, -1, 0, 1, \cdots, \frac{m-1}{2}$ 为模 p 的**绝对最小非负完全同余系**

注 利用上述语言的约定，从 $\mathbb{Z}$ 到关于模 p 同余的商集 $\mathbb{Z}/p\mathbb{Z}$ 上的典范映射定义为令每个整数对应它被 p 除的余数

定义 2.6 (模 p 整数集加法和乘法)

在模 p 整数的集合 $\mathbb{Z}/p\mathbb{Z}$ 上定义加法和乘法：若 θ 表示从 $\mathbb{Z}$ 到 $\mathbb{Z}/p\mathbb{Z}$ 上的典范映射，则对于任意 $x, y \in \mathbb{Z}$ 有

$$\theta(x + y) = \theta(x) + \theta(y), \quad \theta(xy) = \theta(x)\theta(y)$$

定理 2.5 (模 p 同余系交换环)

配备了定义 (2.6) 定义的加法和乘法的模 p 同余系的集合 $\mathbb{Z}/p\mathbb{Z}$ 为一个交换环

证明 首先指出在 $\mathbb{Z}/p\mathbb{Z}$ 里加法的结合性：设 ξ, η, ς 为同余系内三个元素，则存在 $x, y, z \in \mathbb{Z}$ 使得 $\xi = \theta(x), \eta =$

$\theta(y), \varsigma = \theta(z)$，于是有

$$\xi + \eta = \theta(x) + \theta(y) = \theta(x+y), \quad \eta + \varsigma = \theta(y) + \theta(z) = \theta(y+z)$$

进而有

$$(\xi + \eta) + \varsigma = \theta(x+y) + \theta(z) = \theta((x+y)+z)$$
$$\xi + (\eta + \varsigma) = \theta(x) + \theta(y+z) = \theta(x+(y+z))$$

则由 $\mathbb{Z}$ 的加法结合性推出 $\mathbb{Z}/p\mathbb{Z}$ 的加法结合性。同理证明在 $\mathbb{Z}/p\mathbb{Z}$ 里乘法结合性，加法和乘法的交换性以及乘法对于加法的分配性。从关系 $\theta(1)\theta(x) = \theta(1x) = \theta(x)$ 得 $\theta(1)$ 为 $\mathbb{Z}/p\mathbb{Z}$ 乘法中性元，同理 $\theta(0)$ 为其加法中性元。最后证明 $\mathbb{Z}/p\mathbb{Z}$ 为一个交换环。

选取一个 $x \in \mathbb{Z}$，写出 $\xi = \theta(x)$，由关系

$$\theta(-x) + \theta(x) = \theta(-x+x) = \theta(0)$$

显然得 ξ 有相反元 $\theta(-x)$。则 $\mathbb{Z}/p\mathbb{Z}$ 的所有元素 ξ 均有一个相反元

注 称该环为**模 p 整数环**，$\mathbb{Z}/p\mathbb{Z}$ 有时也记为 Z_p。若 $p \neq 0$，则该环仅有有限个元素，即 p 个元素（不失一般性，假定 p 为正）

2.2.2 唯一析因环与素元

经典的素数概念将借助素元的概念引入

定义 2.7 (单位群)

设 R 为整环，$R^* = R\backslash\{0\}$ 为交换么半群且消去律成立，U 为 R^* 中可逆元素的集合（U 为一个 Abel 群），称 U 为 R 的单位群，称 U 中的元素为 R 的单位 (unit)

定义 2.8 (整除)

设 R 为整环，$R^* = R\backslash\{0\}$，$a, b \in R^*$，若 $\exists c \in R^* : b = ac$，则称 a 能整除 b，或 a 为 b 的因子，或 b 为 a 的倍式，记为 $a \mid b$。反之，称 a 不能整除 b。记为 $a \nmid b$

性质 （整除反身性）

设 R 为整环，$R^* = R\backslash\{0\}$，则 $\forall a \in R^* : a \mid a$

证明 $a = 1 \cdot a$

性质 （整除传递性）

设 R 为整环，$R^* = R\backslash\{0\}$，$a, b, c \in R^*$，则 $(a \mid b) \wedge (b \mid c) \Rightarrow a \mid c$

证明 设 $b = ad, c = be$ 即得 $c = a(de)$

性质 （单位整除任意元）

设 R 为整环，U 为 R 的单位群，则有 $(u \in U) \Rightarrow (\forall a \in R^*)(u \mid a)$

证明 $a = u\left(u^{-1}a\right)$

注 称因子 $(u \in U)$ 为**平凡因子** (trivial divisor)，称其余因子为**非平凡因子**

性质 （单位关于整除的充要条件）

设 R 为整环，$R^* = R\backslash\{0\}$，则有 $(u \in U) \Leftrightarrow (u \mid 1)$

证明 由性质 (2.2.2) 有，$u \in U$ 时，$u \mid 1$；反之，若 $u \mid 1$，即有 v 满足 $1 = vu$，则有 $v = u^{-1}(u \in U)$

定义 2.9 (相伴关系)

设 R 为整环，$R^* = R\backslash\{0\}$，$a, b \in R^*$ 且 $a \mid b, b \mid a$，则称 a 与 b 相伴，记为 $a \sim b$

性质 （相伴关系性质）

设 R 为整环，$R^*=R\backslash\{0\}$，U 为 R 的单位群，关于 $\mathbf{R}^*$ 中的相伴关系满足，$(a\sim b)\Leftrightarrow(\exists u\in U):b=au$

证明 若 $\exists u\in U):b=au$，则 $a=bu^{-1}$，则 $a\mid b,b\mid a$，即 $a\sim b$；反之，若 $a\mid b,b\mid a$，则存在 $c,d\in R^*$，使得 $b=ac,a=bd$，则 $b=b(dc)$，则有 $dc=1$，则由定义 $d,c\in U$

性质 （相伴关系必要条件）

设 R 为整环，$R^*=R\backslash\{0\}$，则 R^* 中相伴关系为么半群 R^* 中同余关系

证明 相伴关系显然为等价关系。设 $a\sim b,c\sim d$，U 为 R 单位群，则 $\exists u_1,u_2\in U$ 使得 $b=au_1$，$d=cu_2$，则 $bd=ac(u_1u_2)$。由 $u_1u_2\in U$ 即有 $ac\sim bd$，则相伴关系为同余关系

性质 （单位关于相伴关系的充要条件）

设 R 为整环，$R^*=R\backslash\{0\}$，U 为 R 的单位群，则 $u\in U\Leftrightarrow u\sim 1$

证明 由性质 (2.2.2)(2.2.2) 即得

定义 2.10 (真因子)

设 R 为整环，$R^*=R\backslash\{0\}$，$a,b\in R^*$，若 $b\mid a$，但 $a\nmid b$，则称 b 为 a 的真因子 (proper divisor)。换言之，即 b 整除 a 但不与 a 相伴

♣

性质 （单位无真因子性）

设 R 为整环，$R^*=R\backslash\{0\}$，U 为 R 的单位群，$u\in U$，则 u 没有真因子

证明 若 v 为 u 的因子，即有 $v\mid u$，又 $u\mid 1$，则有 $v\mid 1$，即 $v\in U$，亦即 v 与 u 相伴，由此 u 没有真因子

定义 2.11 (不可约元与可约元)

设 R 为整环，$R^*=R\backslash\{0\}$，U 为 R 的单位群，$a\in R^*\backslash U$。若 a 无非平凡真因子，则称 a 为不可约元 (irreducible element)；若 a 有非平凡真因子，则称 a 为可约元 (reducible element)

♣

例题 2.1 （不可约元）

在整数环 $\mathbb{Z}$ 中，$U=\{1,-1\}$，则 $a\sim b$ 当且仅当 $a=\pm b$，因而 a 为不可约元素当且仅当 a 为素数或负素数

定义 2.12 (素元)

设 R 为整环，$R^*=R\backslash\{0\}$，U 为 R 的单位群，若 $p\in R^*\backslash U$ 且满足

$$(p\mid ab)\Rightarrow(p\mid a)\vee(p\mid b)$$

则称 p 为素元 (prime element)

♣

定理 2.6 (素性必要条件)

素元必为不可约元

♡

证明 设 R 为整环，$R^*=R\backslash\{0\}$，U 为 R 的单位群，若 a 为素元 p 的一个因子，则 $\exists b\in R^*:p=ab$，则有 $p\mid a$ 或 $p\mid b$。若 $p\mid a$ ，则 a 不为 p 真因子；若 $p\mid b$，即 $\exists c\in R^*:b=pc$，则 $p=pac$，则有 $ac=1$，即 a 为平凡因子。这说明 p 没有非平凡真因子，则 p 为不可约元

注 逆命题一般不成立

定义 2.13 (素性条件)

设 R 为整环，若 R 的不可约元为素元，则称 R 满足素性条件

♣

定义 2.14 (公因子)

设 R 为整环，$R^*=R\backslash\{0\}$，$b,c\in R^*$，若 $d\in R^*$ 满足 $d\mid b,d\mid c$，则称 d 为 b,c 的公因子 (common divisor)；若对 b,c 的任一公因子 d_1 有 $d_1\mid d$，则称 d 为 b,c 的最大公因子；若 R^* 中任意两个元素的最大公因子存在，则称 R 满足最大公因子条件 ♣

引理 2.1 (最大公因子条件性质)

设 R 为整环，$R^*=R\backslash\{0\}$，$a,b,c\in R^*$，若整环 R 满足最大公因子条件，则下列断言成立：

1) 设 d 为 b,c 的一个最大公因子，则 d_1 为 b,c 的最大公因子当且仅当 $d_1\sim d$，即 b,c 的最大公因子在相伴意义下唯一，记为 (b,c)

2) $\forall a_1,a_2,\cdots,a_r\in R^*$ 均有最大公因子

3) $((a,b),c)\sim(a,(b,c))$

4) $c(a,b)\sim(ca,cb)$

5) 若 $(a,b)\sim 1,(a,c)\sim 1$，则 $(a,bc)\sim 1$r ♡

证明 1) 若 d,d_1 为 b,c 的最大公因子，则 $d\mid d_1,d_1\mid d$，显然 $d\sim d_1$；反之，若 $d_1\sim d$，则有 $d_1\mid d$，进而 $d_1\mid d,d_1\mid c$，则 d_1 为 b,c 的公因子。又若 a 为 b,c 的公因子，则 $a\mid d$，而 $d\mid d_1$，则有 $a\mid d_1$，则 d_1 为 b,c 的最大公因子

2) 令 $d_1=(a_1,a_2),d_2=(d_1,a_3),d_3=(d_2,a_4),\cdots,d=d_{r-1}=(d_{r-2},a_r)$. 下证 d 为 $a_1,a_2,\cdots,a_r$ 的最大公因子。显然 $(\forall k\in\overline{1;r-2}):d\mid d_k,d\mid a_r$。又 $d_k\mid a_{k+1}$，则有 $(\forall i\in\overline{1;r}):d\mid a_i$，即 d 为公因子。又若 $(\forall i\in\overline{1;r}):a\mid a_i$，则 $a\mid d_1$ 且依次有 $a\mid d_2,a\mid d_3,\cdots$，最后有 $a\mid d_{r-1}$，即 $a\mid d$，则 d 为最大公因子

3) 由 2) 得 $((a,b),c)$ 与 $(a,(b,c))$ 都为 a,b,c 的最大公因子，由 1) 得二者相伴

4) 设 $d=(a,b),e=(ca,cb)$，则 $cd\mid ca,cd\mid cb$，于是 $cd\mid e$，则有 $e=cdu$，由此得 $ca=ex=xucd$。于是 $a=xud$，即 $ud\mid a$，同理有 $ud\mid b$，则 $ud\mid d$，因此 $u\in U$，即 e 与 cd 相伴

5) 设 $(a,b)\sim 1$，由 4) 得 $(ac,bc)\sim c$。又 $(a,ac)\sim a$，则有 $1\sim(a,c)\sim(a,(ac,bc))\sim((a,ac),bc)\sim(a,bc)$

注 若 $(a,b)\sim 1$, 则称 a 与 b **互素** (relatively prime)

定义 2.15 (唯一析因环)

设 R 为整环，$R^*=R\backslash\{0\}$，U 为 R 的单位群，若 R 满足下列条件：

1) 有限析因条件：$\forall a\in R^*\backslash U$ 可分解为有限个不可约元素的乘积，即有不可约元素 $p_i(1\leqslant i\leqslant r)$ 满足

$$a=p_1p_2\cdots p_r$$

2) 唯一分解条件：若 $a\in R^*\backslash U$ 有两种不可约元素乘积的分解

$$a=p_1p_2\cdots p_r=q_1q_2\cdots q_s$$

则有 $r=s$ 且 $\exists\pi\in S_n$，使 $p_i\sim q_{\pi(i)}(1\leqslant i\leqslant r)$。则称 R 为唯一析因环 (unique factorization domain,[arrb].UFD) 或 Gauss 环。另外，称 $|a|=r$ 为 a 的长度 (length)；若 $u\in U$，约定 $|u|=0$ ♣

定义 2.16 (因子链)

设 R 为整环，$R^*=R\backslash\{0\}$，U 为 R 的单位群，若 R^* 中的一个序列 $a_1,a_2,\cdots,a_n,a_{n+1},\cdots$ 满足

$$a_{n+1}\mid a_n,\quad n=1,2,\cdots,$$

则称该序列为 R 的一个因子链

若对 R^* 中任一因子链均有

$$(\exists m\in\mathbf{N})(\forall n\geqslant m):a_m\sim a_n$$

则称 R 满足因子链条件 ♣

引理 2.2 (因子链条件必要条件)

设 R 为整环，$R^*=R\backslash\{0\}$，U 为 R 的单位群，若 R 满足因子链条件，则必满足有限析因条件 ♡

证明 设 $a\in R^*\backslash U$，先证 a 有不可约因子。不妨设 a 可约，则 a 有非平凡真因子 a_1，即有 $a=a_1b_1$，这时 b_1 也为 a 非平凡真因子。若 a_1,b_1 都可约，则 $a_1=a_2b_2$，其中 a_2,b_2 为 a_1 真因子，以此类推可得因子链 $a,a_1,a_2,\cdots,a_n,a_{n+1},\cdots$ 且 $a_{n+1}\mid a_n$。由因子链条件 $(\exists m\in\mathbf{N})(\forall n\geqslant m):a_m\sim a_n$，则 a_m 不可约，即 a_m 为 a 的不可约因子

再证 a 可分解为有限多个不可约因子的乘积。设 p_1 为 a 的一个不可约因子，则有 $a=p_1a'$，若 $a'\in U$，命题已得证；若 $a'\in R^*\backslash U$，则 a' 有不可约因子 p_2，即 $a=p_1p_2a''$，以此类推，即得因子链 $a,a',a'',\cdots,a^{(n)},a^{(n+1)},\cdots$，，则有 s，使 $a^{(s-1)}\sim a^{(s)}$，这时 $a^{(s-1)}=p_s$ 不可约，则有 $a=p_1p_2\cdots p_s$，则 R 满足有限析因条件

定理 2.7 (唯一析因性充要条件)

设 R 为整环，则下列命题等价：

1) R 为唯一析因环（R 满足有限析因条件与唯一分解条件）
2) R 满足因子链条件与素性条件
3) R 满足因子链条件与最大公因子条件 ♡

证明 1) $\Rightarrow$ 3)。设 R 为唯一析因环，先证 R 满足因子链条件。显然有

$$|bc|=|b|+|c|$$

$$a\in U\Leftrightarrow|a|=0$$

$$b\sim c\Leftrightarrow|b|=|c|,b\mid c$$

现设 $a_1,a_2,\cdots,a_n,a_{n+1},\cdots$ 为 R^* 的一个因子链，则必有 $|a_i|\geqslant 0$ 且

$$|a_1|\geqslant|a_2|\geqslant\cdots\geqslant|a_n|\geqslant|a_{n+1}|\geqslant\cdots$$

进而有 $(\exists m\in\mathbf{N})(\forall n\geqslant m):a_m\sim a_n$，即 $|a_n|=|a_m|$，则 R 满足因子链条件

为证 R 满足最大公因子条件，设 $a\in R^*\backslash U$ 有不可约元素乘积分解 $a=q_1q_2\cdots q_s$、将 $q_1,q_2,\cdots,q_s$ 按相伴关系分类，每类取一个代表，则上述分解记为

$$a=up_1^{n_1}p_2^{n_2}\cdots p_r^{n_r},\quad u\in U,n_i>0$$

若 c 为 a 的一个非平凡因子，则有 $a=cc_1$。易证此时有分解

$$c=u_1p_1^{n_1'}p_2^{n_2'}\cdots p_r^{n_r'},\quad u_1\in U,n_i\geqslant n_i'\geqslant 0$$

现证 R 满足最大公因子条件。设 $a,b\in R^*$，若 a,b 中有一个是单位，则 1 为 a,b 的最大公因子，故假定 $a,b\in R^*\backslash U$，不妨设

$$a=up_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$$

$$b=vp_1^{m_1}p_2^{m_2}\cdots p_r^{m_r}$$

其中 $u,v\in U,p_1,p_2,\cdots,p_r$ 为互不相伴的不可约元素，$n_i\geqslant 0,m_j\geqslant 0,1\leqslant i,j\leqslant r$。令 $k_i=\min\{n_i,m_i\}$，由上述讨论有

$$d=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$$

为 a,b 的最大公因子

3) $\Rightarrow$ 2)。仅需证明素性条件成立。设 p 为一个不可约元素且 $p\nmid a,p\nmid b$，即有 $(p,a)\sim 1,(p,b)\sim 1$。由引理 (2.1) 得 $(p,ab)\sim 1$，则 $p\nmid ab$，换言之，若 $p\mid ab$，则有 $p\mid a$ 或 $p\mid b$，故 p 为素元素

2) $\Rightarrow$ 1)。由引理 (2.2) 得 R 满足有限析因条件，故仅需证因式分解唯一性。不妨设 $a\in R^*\backslash U$ 且 a 有两个不可约元素乘积的分解

$$a=p_1p_2\cdots p_s=q_1q_2\cdots q_t$$

现对 s 归纳：若 $s=1$，则 a 为不可约元素即为素元素。下设 $a \mid q_1$，由 q_1 不可约，则有 $a \sim q_1$，则 $t=1$。设命题在 $s-1$ 时已成立，现证 s 时成立。由 $p_1 \mid a$，则 $p_1 \mid q_1 q_2 \cdots q_t$，即有 q_{i_1} 满足 $p_1 \mid q_{i_1}$。由此有 $q_{i_1}=u_1 p_1\,(u_1 \in U)$，进而

$$p_2 \cdots p_s = u_1 \prod_{j \neq i_1} q_j = \prod_{j=2} q_j'$$

则 $s-1=t-1$ 且 $p_i \sim q_i' \sim q_{\pi(i)} (2 \leqslant i \leqslant s)$。因此 $s=t$ 且有 $\pi \in S_t$ 使得 $p_i \sim q_{\pi(i)} (1 \leqslant i \leqslant t)$，即 R 为一个唯一析因环

注 上述讨论并未用到 R 中的加法，因而可以认为 R^* 为满足消去律的么半群。因此可定义**唯一析因么半群**（或 Gauss **么半群**）。所以，引理 (2.1), 引理 (2.2) 与定理 (2.7) 对 Gauss 么半群也成立

注 若在 R 中约定 $a \mid 0, \forall a \in R$，此时可得若 $a \mid b, a \mid c$，则 $a \mid (b+c)$ 以及其他一些初等数论中早已熟知的性质

2.2.3 主理想整环与 Euclid 环

定义 2.17 (Euclid 环)

设 R 为整环，若存在 R 到非负整数集 $\mathbb{N} \cup \{0\}$ 的映射 δ 使得 $\forall a, b \in R, b \neq 0, \exists q, r \in R$ 满足

$$a = qb + r, \quad \delta(r) < \delta(b)$$

则称 R 为 Euclid 环

♣

定义 2.18 (理想)

设 $(R, +, \cdot)$ 为环，R_1 为 R 非空子集且 $(R_1, +, \cdot)$ 为环，则称 R_1 为 R 的子环。若子环 R_1 满足 $RR_1 \subseteq R_1$（对称地，$R_1 R \subseteq R_1$），则称 R_1 为 R 的左理想 (left ideal)（对称地，称右理想 (right ideal)）。若环 R 非空子集 I 既为环 R 左理想又为右理想，则称 I 为 R 的双边理想 (two-sided ideal)，简称理想 (ideal)

显然，$\{0\}$ 与 R 都为 R 的理想，称 $\{0\}$ 与 R 为 R 的平凡理想 (trivial ideal)

♣

注 （理想）

在交换环中，左理想、右理想与理想三个概念没有差别

性质 （理想可交性）

一个环中任意多个理想之交仍为理想

注 若 A 为环 R 的非空子集，则所有包含 A 的理想之交为一个包含 A 的理想，称该理想为**由 A 生成的理想**，记为 $\langle A \rangle$。若 $A=\{a\}$，则称 $\langle A \rangle = \langle a \rangle$ 为**由 a 生成的主理想**

定义 2.19 (主理想环)

若交换么环每个理想均为主理想，则称此环为主理想环。若主理想环为整环（即交换无零因子含么环，定义也可概述为无零因子主理想环为主理想整环），则称该环为主理想整环 (principal ideal domain，简称 PID)

♣

例题 2.2 （主理想整环）

整环 $\mathbb{Z}$ 为主理想整环

解 设 I 为 $\mathbb{Z}$ 的一个非平凡理想，则

$$(\exists m \in I) : m = \min\{|k| \mid k \in I, k \neq 0\}$$

而对于 $\forall k \in I$，若 $k=0$，则 $k = 0 \cdot m$；若 $k \neq 0$，则 $(\exists q, r \in \mathbb{Z}) : k = qm + r (0 \leqslant r < m)$，则 $r \in I$，由 m 的取法知 $r=0$，即 $k=qm$，则 $I = \langle m \rangle$，则 $\mathbb{Z}$ 为主理想整环

性质 （交换么环整除充要条件）

设 R 为交换么环，则 $a \mid b$ 的充要条件为 $\langle a \rangle \supseteq \langle b \rangle$

性质 （交换么环相伴充要条件）

设 R 为交换幺环，则 $a\sim b$ 的充要条件为 $\langle a\rangle=\langle b\rangle$

性质 设 R 为交换幺环，则 $a\sim 1$ 的充要条件为 $\langle a\rangle=\langle 1\rangle=R$

定义 2.20 (主理想升链条件)

设 R 为交换幺环，若任意主理想升链

$$\langle a_1\rangle\subseteq\langle a_2\rangle\subseteq\cdots\subseteq\langle a_n\rangle\subseteq\langle a_{n+1}\rangle\subseteq\cdots$$

都满足 $(\exists m\in\mathbb{N})(\forall n\geqslant m):\langle a_n\rangle=\langle a_m\rangle$，则称 R 满足主理想升链条件

性质 R 满足因子链条件等价于 R 满足主理想升链条件

定理 2.8 (主理想整环唯一析因性)

主理想整环必为唯一析因环

证明 仅需证一个主理想整环 R 满足主理想升链条件与最大公因子条件。设 $\langle a_1\rangle\subseteq\langle a_2\rangle\subseteq\cdots\subseteq\langle a_n\rangle\subseteq\cdots$ 为 R 中一个主理想升链。令 $I=\bigcup\limits_{i=1}^{\infty}\langle a_i\rangle$，则

$$(\forall a,b\in I)(\exists i,j\in\mathbb{N}):[(a\in\langle a_i\rangle)\wedge(b\in\langle a_j\rangle)]$$

不妨设 $j\geqslant i$，则 $a-b\in\langle a_j\rangle\subseteq I$，则 I 为 R 中加法子群。又 $(\forall c\in R):ca\in\langle a_i\rangle\subseteq I$，则 I 为 R 中理想，则 $(\exists d\in R):I=\langle d\rangle$。由 $d\in I$，则有 $(\exists m\in\mathbb{N}):d\in\langle a_m\rangle$，则有

$$(\forall n\geqslant m):I=\langle d\rangle\subseteq\langle a_m\rangle\subseteq\langle a_n\rangle\subseteq\bigcup_{i=1}^{\infty}\langle a_i\rangle=I$$

即 $\langle a_n\rangle=\langle a_m\rangle=I$，则 R 满足主理想升链条件

另外，设 $a,b\in R^*$，显然 $\langle a\rangle+\langle b\rangle$ 为 R 中理想，则 $(\exists d\in R):\langle a\rangle+\langle b\rangle=\langle d\rangle$，则有 $\langle a\rangle\subseteq\langle d\rangle,\langle b\rangle\subseteq\langle d\rangle$，即 $d\mid a,d\mid b$，即 d 为 a,b 的公因子. 又若 $c\mid a,c\mid b$, 则有 $\langle a\rangle\subseteq\langle c\rangle,\langle b\rangle\subseteq\langle c\rangle$，则 $\langle d\rangle=\langle a\rangle+\langle b\rangle\subseteq\langle c\rangle$，即有 $c\mid d$，则 d 为 a,b 的最大公因子，则 R 满足最大公因子条件

综上，R 为唯一析因环

推论 2.2

设 R 为主理想整环，若 d 为 a,b 的最大公因子，则有

$$(\exists u,v\in R):d=au+bv$$

证明 由 $\langle d\rangle=\langle a\rangle+\langle b\rangle$ 即证

推论 2.3 (Bézout's identity)

(Bézout's identity[a]) 设 R 为主理想整环，则 a,b 互素的充要条件为

$$(\exists u,v\in R):au+bv=1$$

[a]贝祖 (Étienne Bézout,1730.3.31-1783.9.27) 法国数学家，以多项式方程解数的定理而闻名

证明 必要性由推论 (2.2) 即证。充分性：若 $d=(a,b)$，则 $d\mid a,d\mid b$，则 $d\mid au+bv$，则 $d\mid 1$，则 $d\sim 1$

定义 2.21 (Euclid 环)

设 R 为整环，若存在 R 到非负整数集的映射 δ，使得

$$(\forall a,b\in R)(b\neq 0)(\exists q,r\in R):a=qb+r,\delta(r)<\delta(b)$$

则称 R 为 Euclid 环

例题 2.3 (Gauss 整数环/Euclid 环)

Gauss 整数环 $\mathbb{Z}[\sqrt{-1}]=\{a+b\sqrt{-1}\mid a,b\in\mathbb{Z}\}$ 为 Euclid 环

解 令 $\delta(a+b\sqrt{-1})=a^2+b^2$，则显然有

$$(\forall\alpha,\beta\in\mathbb{Z}[\sqrt{-1}]):\delta(\alpha\beta)=\delta(\alpha)\delta(\beta)$$

设 $\beta\neq0$，则有 $\beta^{-1}\in\mathbb{Q}[\sqrt{-1}]$，即有

$$\alpha\beta^{-1}=\mu+\nu\sqrt{-1},\quad \mu,\nu\in\mathbb{Q}$$

则

$$(\exists c,d\in\mathbb{Z}):\left[\left(|c-\mu|\leqslant\frac{1}{2}\right)\wedge\left(|d-\nu|\leqslant\frac{1}{2}\right)\right]$$

令 $\varepsilon=\mu-c,\eta=\nu-d$，则有 $|\varepsilon|\leqslant\dfrac{1}{2}$，$|\eta|\leqslant\dfrac{1}{2}$，而

$$\alpha=\beta((c+\varepsilon)+(d+\eta)\sqrt{-1})=\beta q+r$$

其中，$q=c+d\sqrt{-1}\in\mathbb{Z}[\sqrt{-1}],r=\beta(\varepsilon+\eta\sqrt{-1})=\alpha-\beta q\in\mathbb{Z}[\sqrt{-1}]$，又

$$\delta(r)=|r|^2=\delta(\beta)\left(\varepsilon^2+\eta^2\right)\leqslant\delta(\beta)(\frac{1}{4}+\frac{1}{4})<\delta(\beta)$$

则 $\mathbb{Z}[\sqrt{-1}]$ 为 Euclid 环

定理 2.9 (Euclid 环主理想性)

Euclid 环为主理想环 ♡

证明 设 I 为 Euclid 环 R 中的一个理想，若 $I=\{0\}$，显然为主理想，故假设 $I\neq\{0\}$。取 I 中元素 b 满足

$$\delta(b)=\min\{\delta(c)\mid c\in I,c\neq0\}$$

设 $a\in I$，则有 $q,r\in R$ 使上式成立。因 $a,b\in I$，则 $r=a-qb\in I$。由 b 的取法有 $r\notin I\backslash\{0\}$，则 $r=0$，则 $a\in\langle b\rangle$，则 $I=\langle b\rangle$，即 R 为主理想环

注 (辗转相除法)

在 Euclid 环中，可用如下方法求两个元素的最大公因子：

设 $a,b\in R^*$，不妨设 $\delta(a)\geqslant\delta(b)$，并记 $a=a_1,b=a_2$，则有 $(\exists q_1,a_3\in R)$ 满足

$$a_1=q_1a_2+a_3,\quad \delta\left(a_3\right)<\delta\left(a_2\right)$$

若 $a_3=0$, 则 $(a_1,a_2)\sim a_2$；设 $a_3\neq0$，则 $(a_1,a_2)\sim(a_2,a_3)$。再对 a_2,a_3 作除法运算

$$a_2=q_2a_3+a_4,\quad \delta\left(a_4\right)<\delta\left(a_3\right)$$

若 $a_4=0$，则 $(a_1,a_2)\sim(a_2,a_3)\sim a_3$；若 $a_4\neq0$, 则 $(a_1,a_2)\sim(a_2,a_3)\sim(a_3,a_4)$，继续有

$$\delta\left(a_1\right)\geqslant\delta\left(a_2\right)>\delta\left(a_3\right)>\delta\left(a_4\right)>\cdots,$$

则在有限步后必终止，即有 $a_n\neq0$，但 $a_{n+1}=0$，则有 $(a_1,a_2)\sim a_n$

注 (Euclid 环其他等价定义)

Euclid 环有许多等价定义，但共同点为辗转相除法可行。设 R 为整环

定义二：若有 R^* 到 $\mathbf{N}\cup\{0\}$ 的映射 δ 满足

1) $a\neq0,b\neq0,\delta(ab)\geqslant\delta(a)$

2) $(\forall a,b\in R)(b\neq0):a=qb+r$，其中 $r=0$ 或 $\delta(r)<\delta(b)$

则称 R 为 Euclid 环

定义三：若有 R 到 $\mathbf{N}\cup\{0\}$ 的映射 δ 满足

1) $\delta(a)\geqslant0,\delta(a)=0$ 当且仅当 $a=0$

2) $\delta(ab)=\delta(a)\delta(b)$

3) 若 $b\neq0$，则 $(\forall a\in R)(\exists q,r\in R):a=bq+r$，其中 $\delta(r)<\delta(b)$

则称 R 为 Euclid 环

定义四：若有 R 到 $\mathbf{N}\cup\{0\}$ 的映射 δ 满足
1) 若 $b\mid a$，则 $\delta(b)\leqslant\delta(a)$
2) $(\forall a,b\in R)(b\neq 0)(\exists q,r\in R):a=bq+r,\quad \delta(r)<\delta(b)$
则称 R 为 Euclid 环

2.3 集环与 σ 环

2.3.1 集环与集代数

定义 2.22 (集环)

设 $\Re$ 为非空集族，若由 $A\in\Re$ 与 $B\in\Re$ 推出 $A\triangle B\in\Re$ 与 $A\cap B\in\Re$，则称 $\Re$ 为集环 (кольцо множества)

♣

注 (集环定义合理性)
因为对于任何 A 与 B 均有

$$A\cup B=(A\triangle B)\triangle(A\cap B),\quad A\backslash B=A\triangle(A\cap B)$$

则由 $A\in\Re$ 与 $B\in\Re$ 可推出集 $A\cup B$ 与 $A\backslash B$ 也属于 $\Re$，则 $\Re$ 关于有限交与对称差的运算为封闭集族，即 $(\Re,\cap,\Delta)$ 为一个环
另外，显然集环关于形如

$$C=\bigcup_{k=1}^{n}A_k,\quad D=\bigcap_{k=1}^{n}A_k$$

的任何有限和与有限交也封闭

注 (最小集环与最大集环)
由 $A\backslash A=\varnothing$ 恒成立有任意集环都包含空集 $\varnothing$。仅由空集组成的族为所有可能的最小集环

定义 2.23 (单位与集代数)

设 $\mathfrak{S}$ 为集族，$E\in\mathfrak{S}$，若

$$(\forall A\in\mathfrak{S}):A\cap E=A$$

则称 E 为 $\mathfrak{S}$ 的单位。称具有单位的集环为集代数

♣

定理 2.10 (非空集族生成环存在唯一性)

对于任意非空集族 $\mathfrak{S}$，下列命题成立：
1) (非空集族生成环存在性) 存在包含集族 $\mathfrak{S}$ 的集环
2) (非空集合生成环极小性 (唯一性)) 若包含集族 $\mathfrak{S}$ 的集环 $\Re(\mathfrak{S})$ 为任意包含 $\Re$ 的集环的子集环，则集环 $\Re(\mathfrak{S})$ 唯一

♡

证明 考虑 $X=\{\bigcup_{A\in\mathfrak{S}}A|A\in\mathfrak{S}\}$，设 Σ 为属于 $\mathcal{P}(X)$ 且又包含 $\mathfrak{S}$ 的一切集环的总体，则显然所有这些环的交 $\mathfrak{B}=\bigcup_{\Re\in\Sigma}\Re$ 即为所要求的环 $\Re(\mathfrak{S})$，其显然也是唯一的

注 该定理表明，对于任意包含非空集族 $\mathfrak{S}$ 的集环 $\Re^*$，交 $\Re=\Re^*\cap\mathcal{P}(X)$ 为 Σ 中的集环，则 $\mathfrak{S}\subset\Re\subset\Re^*$，即 $\Re$ 满足极小性要求，由此称该环为 $\mathfrak{S}$ 上的**极小环**或 $\mathfrak{S}$ 的**生成环**，记为 $\Re(\mathfrak{S})$

定义 2.24 (半环)

设集族 $\mathfrak{S}$，若满足下列条件：

1) (含幺性) $\varnothing \in \mathfrak{S}$

2) (有限交封闭性) $(\forall A, B \in \mathfrak{S}) : A \cap B \in \mathfrak{S}$

3) (有限覆盖性) $(\forall A, A_1 \in \mathfrak{S})[(A_1 \subset A) \Rightarrow (\exists A_2, A_3, \cdots, A_n \in \mathfrak{S})(A = \bigcup\limits_{k=1}^{n} A_k)]$

则称 $\mathfrak{S}$ 为集半环，一般简称为半环 (semi-ring/полукольцо)

♣

命题 2.1 (集环半环性)

集环 $\Re$ 均为半环

♠

证明 若 A 与 $A_1 \subset A$ 属于 $\Re$，则成立分解式 $A = A_1 \cup A_2$，其中 $A_2 = A \backslash A_1 \in \Re$

定义 2.25 (有限分解式)

若任一组两两不相交的集 $A_1, A_2, \cdots, A_n$ 的并为集 A，称该并为集 A 的有限分解式

♣

引理 2.3 (集有限分解式存在性)

设集 $A_1, A_2, \cdots, A_n, A$ 属于半环 $\mathfrak{S}$，其中集 A_i 两两不交且皆包含于 A，则存在集 $A_{n+1}, \cdots, A_s \in \mathfrak{S}$ 使得集 A 的有限分解式为

$$A = \bigcup_{k=1}^{s} A_k \quad (s \geqslant n)$$

其中 M_k 为某个指标集

♡

证明 归纳：当 $n = 1$ 时由半环定义引理显然成立。假定当 $n = m$ 时引理成立，考虑满足引理条件的 $m+1$ 个集 $A_1, \cdots, A_m, A_{m+1}$。由条件有 $A = A_1 \cup A_2 \cup \cdots \cup A_m \cup B_1 \cup B_2 \cup \cdots \cup B_p$，其中 $(\forall q \in \overline{1;p}) : B_q \in \mathfrak{S}$，下记 $B_{q1} = A_{m+1} \cap B_q$，则有有限分解式 $B_q = B_{q1} \cup B_{q2} \cup \cdots \cup B_{qr_q}$，其中任意 B_{qj} 皆属于 $\mathfrak{S}$。不难看出

$$A = A_1 \cup \cdots \cup A_m \cup A_{m+1} \cup \left(\bigcup_{q=1}^{p} \left(\bigcup_{j=2}^{r_q} B_{qj} \right) \right)$$

则当 $n = m + 1$ 时引理断言得证，由归纳原理引理即证

引理 2.4 (有限集族有限分解式存在性)

任意有限个集 $A_1, \cdots, A_n$ 属于半环 $\mathfrak{S}$，则存在有限个两两不交集 $B_1, \cdots, B_t \in \mathfrak{S}$ 使得任意 $A_k (k = 1, 2, \cdots)$ 均可表示为某些集 B_s 的并：

$$A_k = \bigcup_{s \in M_k} B_s$$

♡

证明 归纳：当 $n = 1$ 时，仅需令 $t = 1, B_1 = A_1$ 即有引理成立。假设当 $n = m$ 时引理成立，考虑 $\mathfrak{S}$ 中某一组集 $A_1, \cdots, A_m, A_{m+1}$。设 $B_1, B_2, \cdots, B_t$ 为满足引理关于 $A_1, A_2, \cdots, A_m$ 条件的 $\mathfrak{S}$ 中的集，下记 $B_{s1} = A_{m+1} \cap B_s$，则根据集有限分解式存在性引理 (2.3) 有 $\mathfrak{S}$ 上有限分解式

$$A_{m+1} = \left(\bigcup_{s=1}^{t} B_{s1} \right) \cup \left(\bigcup_{p=1}^{q} B'_p \right)$$

而由半环定义有表达式 $B_s = B_{s1} \cup B_{s2} \cup \cdots \cup B_{sf_s}$，其中 $B_{sj} \in \mathfrak{S}$，由归纳假设有

$$(\forall k \in \overline{1;m}) : A_k = \bigcup_{s \in M_k} \bigcup_{j=1}^{f_s} B_{sj}$$

则集 B_{sj}, B'_p 两两不交，则有集 B_{sj}, B'_p 满足引理关于 $A_1, \cdots, A_m, A_{m+1}$ 的条件，由归纳法定理即证

定理 2.11 (半环生成环充分条件)

设 $\mathfrak{S}$ 为半环，若

$$(\forall A\in\Re(\mathfrak{S}))(\exists A_1,\cdots,A_n\in\mathfrak{S}):A=\bigcup_{k=1}^{n}A_k$$

则 $\Re(\mathfrak{S})$ 为半环 $\mathfrak{S}$ 的生成环 (кольцо,порождённое полукольиом)

♡

证明 设集合 $\Re=\left\{A=\bigcup\limits_{k=1}^{n}A_k,A_k\in\mathfrak{S}\right\}$，下证该集为环。设 $A=\bigcup\limits_{k=1}^{n}A_k,B=\bigcup\limits_{i=1}^{m}B_i$，其中 $A_k,B_i\in\mathfrak{S}$，则有

$$A\backslash B=\left(\bigcup_{k=1}^{n}A_k\right)\backslash\left(\bigcup_{i=1}^{m}B_i\right)=\bigcup_{k=1}^{n}\left(A_k\backslash\left(\bigcup_{i=1}^{m}B_i\right)\right)=\bigcup_{k=1}^{n}\left(A_k\backslash\left(\bigcup_{i=1}^{m}(A_k\cap B_i)\right)\right)$$

即有 $A\backslash B=\bigcup\limits_{k=1}^{n}\bigcup\limits_{i=1}^{n}\tilde{A}_{ik}$，其中 $\tilde{A}_{ik}\in\mathfrak{S}$，则有 $A\backslash B\in\Re$

若 $A\cap B=\varnothing$，则 $A\cup B\in\Re$；若 $A\cap B\neq\varnothing$，则 $A\cup B=(A\backslash B)\cup B\in\Re$，于是有

$$A\Delta B=(A\backslash B)\cup(B\backslash A)\in\Re,\quad A\cap B=(A\cup B)\Delta(A\Delta B)\in\Re$$

则 $\Re$ 为集环

2.3.2 σ 环与 σ 代数

定义 2.26 (σ 环与 β 环)

设集环 $\Re$，若满足对于可数并运算封闭，即

$$(\forall A_1,A_2,\cdots,A_n,\cdots\in\Re):\bigcup_{i=1}^{+\infty}A_i\in\Re$$

则称集环为 σ 环 (σ-кольцо)，称具有单位的 σ 环 (σ-кольцо с единицей) 为 σ 代数 (σ-алгебра)

若满足对于可数交运算封闭，即

$$(\forall A_1,A_2,\cdots,A_n,\cdots\in\Re):\bigcap_{i=1}^{+\infty}A_i\in\Re$$

则称集环为 β 环 (β-кольцо)，称具有单位的 β 环 (β-кольцо с единицей) 为 β 代数 (β-алгебра)

♣

注 (σ 代数与 β 代数定义等价性)

从对偶关系

$$\bigcup_{i=1}^{+\infty}A_i=E\backslash\left(\bigcap_{i=1}^{+\infty}(E\backslash A_i)\right),\quad\bigcap_{i=1}^{+\infty}A_i=E\backslash\left(\bigcup_{i}(E\backslash A_i)\right)$$

即得任意 σ 代数同时为 δ 代数，而任意 δ 代数同时也为 σ 代数。由此今后仅限于研究 σ 代数

例题 2.4 (σ 代数)

任意集的幂集为 σ 代数

命题 2.2 (集族上 σ 代数存在性)

设 $\mathfrak{S}$ 为集族，则存在一个包含该集族的 σ 代数

♠

证明 令 $X=\bigcup\limits_{A\in\mathfrak{S}}A$，则有 X 的幂集 $\mathcal{P}$ 为包含 $\mathfrak{S}$ 的 σ 代数

定义 2.27 (不可约 σ 代数)

设集族 $\mathfrak{S}$，令 $X=\bigcup\limits_{A\in\mathfrak{S}}A$，则存在包含集族 $\mathfrak{S}$ 的 σ 代数 $\Re$，其为 X 的幂集。若 $X=\bigcup\limits_{A\in\mathfrak{S}}A$ 为该 σ 代数的单位，则称该 σ 代数（关于族 $\mathfrak{S}$）不可约 (неприводимой по отношению к системе $\mathfrak{S}$)，不引起歧

义时，简称不可约 σ 代数 (неприводимая σ-алгебра) ♣

注 （不可约 σ 代数）

不可约 σ 代数为不包含不属于任意 $A \in S$ 的点的 σ 代数。暂限于研究这种 σ 代数

定理 2.12 (非空集族生成不可约 σ 代数)

对于任意非空集族 $\mathfrak{S}$，都存在（关于该族）不可约的 σ 代数 $\mathfrak{B}(\mathfrak{S})$，其包含 $\mathfrak{S}$ 且属于包含 $\mathfrak{S}$ 的任意 σ 代数 ♡

证明 证明方法同非空集族生成环存在唯一性定理 (2.10)

注 称 σ 代数 $\mathfrak{B}(\mathfrak{S})$ 为族 $\mathfrak{S}$ 上的**极小 σ 代数**。在分析中起重要作用的所谓 Borel σ **代数** (Борелевская σ-алгебра)，即数轴上属于所有闭区间 $[a;b]$ 全体上的极小 σ 代数

注 （集函数符号约定）

设 $y = f(x)$ 为在集 M 上的定义的且在集 N 中取值的函数，并设 $\mathfrak{M}$ 为集 M 的子集组成的某一集族，用 $f(\mathfrak{M})$ 表示所有属于 $\mathfrak{M}$ 的集的像 $f(A)$ 组成的族。此外，设 $\mathfrak{N}$ 为包含在 N 中的集的某一集族，$f^{-1}(\mathfrak{N})$ 为属于 $\mathfrak{N}$ 的集的一切原像 $f^{-1}(A)$ 组成的族

性质 下列命题成立：

1) 若 $\mathfrak{N}$ 为集环，则 $f(\mathfrak{N})$ 也为集环
2) 若 $\mathfrak{N}$ 为集代数，则 $f^{-1}(\mathfrak{N})$ 也为集代数
3) 若 $\mathfrak{N}$ 为 σ 代数，则 $f^{-1}(\mathfrak{N})$ 也为 σ 代数
4) $\mathfrak{N}\left(f^{-1}(\mathfrak{N})\right) = f^{-1}(\mathfrak{N}(\mathfrak{N}))$
5) $\mathfrak{N}\left(f^{-1}(\mathfrak{N})\right) = f^{-1}(\mathfrak{N}(\mathfrak{N}))$

第 3 章 模

3.1 基本概念

定义 3.1 (模公理化)

设 $\mathbf{R}$ 为么环，$(M,+)$ 为 Abel 群，若有

$\mathbf{M_1}$：(模性) $\exists f:\mathbf{R}\times M\to M,(a,x)\mapsto ax\in M$

$\mathbf{M_2}$：(纯量对向量左分配性) $(\forall a\in\mathbf{R})(\forall x,y\in M):a(x+y)=ax+ay$

$\mathbf{M_3}$：(向量对纯量左分配性) $(\forall a,b\in\mathbf{R})(\forall x\in M):(a+b)x=ax+bx$

$\mathbf{M_4}$：(代数左结合性) $(\forall a,b\in\mathbf{R})(\forall x\in M):(ab)x=a(bx)$

$\mathbf{M_5}$：(酉性) $(\forall x\in M):1x=x$

则称 M 为 $\mathbf{R}$ 上的一个左模，或称 M 为左 $\mathbf{R}$ 模，称 $f:\mathbf{R}\times M\to M,(a,x)\mapsto ax\in M$ 为 $\mathbf{R}$ 与 M 间乘法，称 $\mathbf{R}$ 为该模的基础环，称基础环的元素为标量，称模元素为向量

对称地定义，若有

$\mathbf{M}'_1$：(模性) $\exists f':M\times\mathbf{R}\to M,(x,a)\mapsto xa\in M$

$\mathbf{M}'_2$：(纯量对向量右分配性) $(\forall a\in\mathbf{R})(\forall x,y\in M):(x+y)a=xa+ya$

$\mathbf{M}'_3$：(向量对纯量右分配性) $(\forall a,b\in\mathbf{R})(\forall x\in M):x(a+b)=xa+xb$

$\mathbf{M}'_4$：(代数右结合性) $(\forall a,b\in\mathbf{R})(\forall x\in M):x(ab)=(xa)b$

$\mathbf{M}'_5$：(酉性) $(\forall x\in M):x1=x$

则称 M 为 $\mathbf{R}$ 上的一个右模，或称 M 为右 $\mathbf{R}$ 模，称 $f':M\times\mathbf{R}\to M,(x,a)\mapsto xa\in M$ 为 M 与 $\mathbf{R}$ 间乘法，称 $\mathbf{R}$ 为该模的基础环，称基础环的元素为标量，称模元素为向量

若 M 同时为左 $\mathbf{R}$ 模与右 $\mathbf{R}$ 模，且满足

$\mathbf{M_6}$:$(\forall a,b\in\mathbf{R})(\forall x\in M):(ax)b=a(xb)$

则称 M 为 $\mathbf{R}$ 模或 $\mathbf{R}$ 双模。若 $\mathbf{R}$ 为交换环，则左 $\mathbf{R}$ 模与右 $\mathbf{R}$ 模相等，即为 $\mathbf{R}$ 模 ♣

注 设 $(R,+,\cdot)$ 为么环，令 $R=\tilde{R}$，若 R 上乘法改为 $*:\tilde{R}\times\tilde{R}\to\tilde{R},(x,y)\mapsto y*x$，则称 $(\tilde{R},+,*)$ 为 R 反环；设 M 为 R 上右模，若反环 $\tilde{R}$ 与 M 间乘法为 $\tilde{R}\times M\to M,(a,x)\mapsto a*x=xa$，则 M 为 $\tilde{R}$ 上左模

这表明左模与右模在反环下性质相同，因此以下仅讨论左模并不妨碍命题的一般性

性质 设 M 为一个左 R 模，则满足

$$(\forall a\in R):a0=0,(\forall x\in M):0x=0$$

例题 3.1 设环 K 与正整数 $n\geqslant 1$，考虑集合 $\mathrm{K}^n=\mathrm{K}\times\cdots\times\mathrm{K}$，定义

$$(\xi_1,\cdots,\xi_n)+(\eta_1,\cdots,\eta_n)=(\xi_1+\eta_1,\cdots,\xi_n+\eta_n),\lambda\cdot(\xi_1,\cdots,\xi_n)=(\lambda\xi_1,\cdots,\lambda\xi_n)$$

则容易验证这为一个左 K 模。自然也可以把 K^n 看作右 K 模：加法如前定义，标量乘法如下定义：

$$(\xi_1,\cdots,\xi_n)\cdot\lambda=(\xi_1\lambda,\cdots,\xi_n\lambda)$$

这是一个右 K 模

注 当 $n=1$，则在构造中可以把 K 本身看作一个左 K 模，这表明“标量”也是“向量”

例题 3.2 所有的交换群 G 均可为左 Z 模

解 对 G 采用加法记号，仅需定义一个 $n\in\mathbf{Z}$ 和一个 $x\in\mathrm{G}$ 的乘积，于是定义

$$nx=\begin{cases}x+\cdots+x(n\text{ 项}), & n\geqslant 1,\\ 0, & n=0,\\ (-n)(-x), & n\leqslant -1\end{cases}$$

则容易验证所有 Z 模采用上述方法从一个交换群出发得到

注 该例表明模理论包括了交换群理论

定义 3.2 (子模)

设 M 为一个左 R 模，若 M 的子集 N 满足

1) N 为 M 子群

2) $(\forall a \in R)(x \in N) : ax \in N$

则称 N 为 M 的一个子模。显然 $\{0\}$ 与 M 都为 M 的子模，称 $\{0\}$ 与 M 为 M 的平凡子模。另外显然可以把 M 的所有子模看作一个左 R 模 ♣

性质 [条件可并性] 设 $(M_i)_{i\in I}$ 为模 M 子模族，若 $(\forall i,j \in I)(\exists k \in I) : (M_i \subset M_k) \wedge (M_j \subset M_k)$，则 $\bigcup_{i\in I} M_i$ 为 M 子模

证明 设 $U = \bigcup_{i\in I} M_i$，则 $e_M \in U \Rightarrow U \neq \varnothing$；$(x,y \in U) \Rightarrow (\exists i,j \in I) : (x \in M_i) \wedge (y \in M_j)$，由假设 $(\exists k \in I) : (x,y \in M_k)$，同理得 $xy^{-1} \in M_k \subset U$，即有 $(x,y \in U) \Rightarrow (xy^{-1} \in U)$，由子群判别法 (1.1) 即得满足子模的子群条件

性质 （可交性）

设 $(M_i)_{i\in I}$ 为模 M 子模族，则 $\bigcap_{i\in I} M_i$ 为 M 子模

证明 设 $M = \bigcap_{i\in I} M_i$，则 $e_G \in M \Rightarrow M \neq \varnothing$；$(x,y \in M) \Rightarrow (\forall i \in I) : (x,y \in M_i) \Rightarrow (\forall i \in I)(xy^{-1} \in M_i \subset M) \Rightarrow (xy^{-1} \in M)$，由子群判别法 (1.1) 即得满足子模的子群条件

定义 3.3

设 M 为环 R 上一个左模，$x_1,\cdots,x_n \in \mathrm{M}$，若存在 $a^1,\cdots,a^n \in \mathrm{R}$ 使得

$$x = a^1x_1 + \cdots + a^nx_n$$

则称所有这样的向量 $x \in M$ 为 $x_1,\cdots,x_n \in \mathrm{M}$ 的线性组合 ♣

定理 3.1

设 $x_1,\cdots,x_n$ 为一个左 R 模 M 的元素，而 M′ 为所有 $x_1,\cdots,x_n$ 的线性组合的集合，则 M′ 为含有 $x_1,\cdots,x_n$ 的 M 的最小子模 ♡

证明 显然有 $x_1 = 1\cdot x_1 + 0\cdot x_2 + \cdots + 0\cdot x_n$ 和对 $x_2,\cdots,x_n$ 的类似关系。这表明 $\mathbf{M}'$ 含有 $x_1,\cdots,x_n$。其次，对于任意 $a^1,\cdots,a^n \in \mathrm{R}$，M 的所有含有 $x_1,\cdots,x_n$ 的子模含有 $a^1x_1,\cdots,a^nx_n$，因此含有 $a^1x_1 + \cdots + a^nx_n$。于是含 $x_i(1 \leqslant i \leqslant n)$ 的 M 的所有子模包含 M′。下证 M′ 为 M 的子模。

设 $x = a^1x_1 + \cdots + a^nx_n, y = b^1x_1 + \cdots + b^nx_n$ 为 M′ 的两个元素，平凡的计算指出

$$\lambda x + \mu y = c^1x_1 + \cdots + c^nx_n$$

其中

$$c^1 = \lambda a^1 + \mu b^1, \quad \cdots, \quad c^n = \lambda a^n + \mu b^n$$

由此得到对于任意标量 λ 和 μ 有 $\lambda x + \mu y \in \mathrm{M}'$

注 称该定理中的 M′ 为 M 的由 $x_1,\cdots,x_n$ 生成的子模

定义 3.4 (模同态)

设 L 和 M 为环 R 上的两个左模，存在映射 $f : \mathrm{L} \to \mathrm{M}$，若

$$(\forall x,y \in L)(\forall \lambda,\mu \in R) : f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$$

则称映射为一个模同态或线性映射。若 f 为双射，则称 f 为从 L 到 M 上的模同构。若存在从 L 到 M 上的模同构，则称 L 与 M 模同构

给定一个左 R 模 M，称所有从 M 到 M 内的模同态为 M 的模自同态或 M 上线性算子，称从 M 到自身的所有同构为 M 上模自同构 ♣

3.2 有限生成模与线性相关

定义 3.5 (有限生成)

设 M 为一个左 R 模，而 M′ 为 M 的一个子模，若存在有限个向量 $x_1,\cdots,x_n\in \mathrm{M}'$ 使得 M′ 由这些向量生成，则称 M′ 有限生成，称 $x_1,\cdots,x_n$ 为 M′ 的一个生成元组

若模为含有有限个向量 $x_1,\cdots,x_n$，使得所有 $x\in \mathrm{M}$ 均为 $x_1,\cdots,x_n$ 的线性组合，则称该模为有限生成模 ♣

注 给定一个左 R 模 M 的元素 $x_1,\cdots,x_n$，设 x 为这些向量的一个线性组合，考虑把 x 写成给定向量的线性组合的两种方式

$$x=a^1x_1+\cdots+a^nx_n=b^1x_1+\cdots+b^nx_n$$

做差立得关系

$$\left(a^1-b^1\right)x_1+\cdots+\left(a^n-b^n\right)x_n=0$$

由此引入下面的定义

定义 3.6 (线性相关性)

设 K^n 为模，$a^1,\cdots,a^n\in K$，$x_1,\cdots,x_n\in K^n$，若满足

$$a^1x_1+\cdots+a^nx_n=0$$

则称 $(a^1,\cdots,a^n)$ 为向量组 $(x_1,\cdots,x_n)$ 之间的线性关系。特别地称线性关系 $(0,\cdots,0)$ 为平凡线性关系。

若除了平凡线性关系，不存在向量组 $(x_1,\cdots,x_n)$ 之间的其他线性关系，则称向量 $(x_1,\cdots,x_n)$ 线性无关（或称族 $\{x_i\}_{1\leqslant i\leqslant n}$ 自由），形式化即为

$$a^1x_1+\cdots+a^nx_n=0\Rightarrow a^1=\cdots=a^n=0$$

反之，则称向量组 $(x_1,\cdots,x_n)$ 非线性无关（或称向量组 $(x_1,\cdots,x_n)$ 线性相关）。换言之，即存在不全为零的标量 $a^1,\cdots,a^n$，使得 $a^1x_1+\cdots+a^nx_n=0$ ♣

注 线性无关的向量组 $(x_1,\cdots,x_n)$ 内向量必然两两不同，因为若 $x_1=x_2$，则 K^n 的元素 $(1,-1,0,\cdots,0)$ 显然为 $x_1,\cdots,x_n$ 之间的一个非平凡线性关系，但诸 a_i 两两不等对于它们线性无关不是充分条件

定义 3.7

设 K^n 为模，$a^1,\cdots,a^n\in K$，$y,x_1,\cdots,x_n\in K^n$，若有

$$y=a^1x_1+\cdots+a^nx_n$$

则称 y 与向量组 $(x_1,\cdots,x_n)$ 线性相关，亦即等价于

$$(yb+a^1x_1+\cdots+a^nx_n=0)\wedge(b\neq 0)$$

特别地，若 $y=0$，称 y 与空集线性相关 ♣

注 为了方便陈述“代数相关”时只需证明少部分基础定理，以下将模上的线性相关性归纳为三个基础定理

定理 3.2 (基础定理一)

$x_i(i \in \overline{1;m})$ 与向量组 $(x_1,\cdots,x_m)$ 线性相关

♡

证明 显然由 $(\forall i \in \overline{1;m}) : x_i = 0x_1 + \cdots + 0x_m$ 即证

定理 3.3 (基础定理二)

若 y 与向量组 $(x_1,\cdots,x_m)$ 线性相关，不与向量组 $(x_1,\cdots,x_{m-1})$ 线性相关，则 x_m 与向量组 $(x_1,\cdots,x_{m-1},y)$ 线性相关

♡

定理 3.4 (基础定理三)

若 z 与向量组 $(y_1,\cdots,y_n)$ 线性相关，$y_j(j \in \overline{1;n})$ 与向量组 $(x_1,\cdots,x_m)$ 线性相关，则 z 与向量组 $(x_1,\cdots,x_m)$ 线性相关

♡

推论 3.1 (导出定理一)

若 z 与向量组 $(y_1,\cdots,y_n)$ 线性相关，则 z 与任意包含向量组 $(y_1,\cdots,y_n)$ 的向量组 $(x_1,\cdots,x_m)$ 线性相关

♡

推论 3.2 (导出定理二)

若向量组 $(x_1,\cdots,x_{n-1})$ 线性无关而向量组 $(x_1,\cdots,x_n)$ 线性相关，则 x_n 与 $(x_1,\cdots,x_{n-1})$ 线性相关

♡

推论 3.3 (导出定理三)

有限向量组 $(x_1,\cdots,x_n)$ 必有一个（可能为空）的线性无关部分组，且 $x_i(i \in \overline{1;m})$ 与该线性无关部分组无关

♡

推论 3.4 (导出定理四/Steinitz 替换定理)

设向量组 $(y_1,\cdots,y_s)$ 线性无关，$y_j(j \in \overline{1;s})$ 都与向量组 $(x_1,\cdots,x_r)$ 线性相关，则在向量组 $(x_1,\cdots,x_r)$ 里存在一个 s 元部分组 $(x_{i_1},\cdots,x_{i_s})$ 可以用向量组 $(y_1,\cdots,y_s)$ 替换，使得由替换所得的向量组与原来的向量组 $(x_1,\cdots,x_r)$ 等价

♡

推论 3.5 (导出定理五)

两个等价的线性无关组 $(x_1,\cdots,x_r)$ 与 $(y_1,\cdots,y_s)$ 元素个数相同

♡

3.3 有限生成自由模与秩

定义 3.8

设 R 为么环，在集合 $R^n = R \times R \times \cdots \times R$ 中，若 $x = \left(x^1, x^2, \cdots, x^n\right) \in R^n$，记 x 的第 i 个分量 x^i 为 $\mathrm{ent}_i\, x$，即 $\mathrm{ent}_i\, x = x^i$，则由下列关系

$$(\forall x, y \in R^n)(\forall i \in \overline{1;n}) : \mathrm{ent}_i(x+y) = \mathrm{ent}_i\, x + \mathrm{ent}_i\, y$$

$$(\forall x \in R^n)(\forall a \in R)(\forall i \in \overline{1;n}) : \mathrm{ent}_i(ax) = a\,\mathrm{ent}_i\, x$$

定义了 R^n 的加法运算及 R 与 R^n 的乘法运算，不难验证 R^n 为一个左 R 模

♣

注 形式上令 $e_i \in R^n$ 满足 $\mathrm{ent}_j e_i = \delta_{ij}$，则有

$$(\forall x \in R^n) : x = \sum_{i=1}^{n} (\mathrm{ent}_i\, x)\, e_i$$

由此有：1) $e_1, e_2, \cdots, e_n$ 生成 R^n；2) $\sum\limits_{i=1}^{n} x^i e_i = 0 \Leftrightarrow (\forall i \in \overline{1;n}) : x^i = 0$

定义 3.9 (秩 n 自由模)

若幺环 R 上的模 M 与 R 模 R^n 同构，则称模为秩 n 自由模 ♣

定理 3.5 (模秩 n 自由充要条件)

R 模 M 为秩 n 自由模的充要条件为存在 M 中 n 个元素 $u_1, u_2, \cdots, u_n$ 满足下列条件

1) $u_1, u_2, \cdots, u_n$ 生成 M，即

$$M = Ru_1 + Ru_2 + \cdots + Ru_n \tag{3.1}$$

2) $x \in M, x = \sum\limits_{i=1}^{n} x^i u_i, x^i \in R$ 的表示法唯一，即

$$\sum_{i=1}^{n} x^i u_i = 0 \Leftrightarrow (\forall i \in \overline{1;n}) : x^i = 0 \tag{3.2}$$

♡

证明

必要性：若 M 为秩 n 的自由模，则有 R^n 到 M 的模同构 σ。令 $(\forall i \in \overline{1;n}) : u_i = \sigma(e_i)$，则有

$$\sigma\left(\sum_{i=1}^{n} x^i e_i\right) = \sum_{i=1}^{n} x^i \sigma(e_i) = \sum_{i=1}^{n} x^i u_i$$

则 $u_1, u_2, \cdots, u_n$ 生成 M

又若 $\sum\limits_{i=1}^{n} x^i u_i = 0$，则有 $\sum\limits_{i=1}^{n} x^i \sigma(e_i) = \sigma\left(\sum\limits_{i=1}^{n} x^i e_i\right) = 0$，即 $\sum\limits_{i=1}^{n} x^i e_i = 0$，因此 $x^i = 0\ (1 \leqslant i \leqslant n)$。这就证明了 $u_1, u_2, \cdots, u_n$ 也满足条件 (3.2)

充分性：设 M 中的元素 $u_1, u_2, \cdots, u_n$ 满足条件 (3.1) 与 (3.2)。构造 M 到 R^n 的映射 η

$$\eta\left(\sum_{i=1}^{n} x^i u_i\right) = \sum_{i=1}^{n} x^i e_i$$

容易验证 η 为 M 到 R^n 的模同构，即 M 为一个秩 n 自由模

注 称满足条件的 $u_1, u_2, \cdots, u_n$ 为 R 模 M 的一组基

推论 3.6

若 $u_1, u_2, \cdots, u_n$ 为秩 n 自由 R 模 M 的一组基，则 $u_1, u_2, \cdots, u_n$ 线性无关 ♡

定理 3.6

设 R 为幺环，M 为左 R 模，$u_1, u_2, \cdots, u_n$ 为 M 中 n 个元素，则 $u_1, u_2, \cdots, u_n$ 为 M 的基的充要条件为对任一左 R 模 M' 及其中 n 个元素 $v_1, v_2, \cdots, v_n$，存在唯一的 M 到 M' 的模同态 η，使得

$$(\forall i \in \overline{1;n}) : \eta(u_i) = v_i$$

♡

证明

必要性：设 $u_1, u_2, \cdots, u_n$ 为 M 一组基，又 $v_1, \cdots, v_n \in M'$，构造 M 到 M' 映射 η

$$\eta\left(\sum_{i=1}^{n} x^i u_i\right) = \sum_{i=1}^{n} x^i v_i$$

容易验证 η 为 M 到 M' 的模同态且 $(\forall i \in \overline{1;n}) : \eta(u_i) = v_i$。若 η' 为 M 到 M' 的模同态且 $(\forall i \in \overline{1;n}) :$

$\eta'(u_i)=v_i$，则

$$\eta'\left(\sum_{i=1}^{n}x^iu_i\right)=\sum_{i=1}^{n}x^i\eta'(u_i)=\sum_{i=1}^{n}x^iv_i=\eta\left(\sum_{i=1}^{n}x^iu_i\right)$$

故 $\eta'=\eta$，唯一性得证

充分性：先证 $u_1,u_2,\cdots,u_n$ 生成 M。令 $M'=\langle u_1,u_2,\cdots,u_n\rangle$，则有唯一的 M 到 M' 的同态 η，使得 $(\forall i\in\overline{1;n}):\eta(u_i)=u_i$

又设 θ 为 M' 到 M 中的嵌入映射，即 $(\forall x\in M'):\theta(x)=x$，则 $\theta\cdot\eta$ 为 M 到 M 的同态且 $(\forall i\in\overline{1;n}):\theta\cdot\eta(u_i)=u_i$。又恒等映射 id 也为 M 到 M 的同态且 $id(u_i)=u_i$，因而由唯一性知 $\theta\cdot\eta=\mathrm{id}$。故 $\eta(M)=M'=M$

现构造 M 到 R^n 的同态 σ 使得 $(\forall i\in\overline{1;n}):\sigma(u_i)=e_i$，则有

$$(\forall x\in M)(\exists x^1,x^2,\cdots,x^n\in R):x=\sum_{i=1}^{n}x^iu_i$$

则有

$$\sigma(x)=\sum_{i=1}^{n}x^i\sigma(u_i)=\sum_{i=1}^{n}x^ie_i$$

综上知 σ 为模满同态且有 $\sigma(x)=0\Rightarrow x=0$，则 σ 为 M 到 R^n 上的模同构，即 M 为秩 n 自由模

注 为了保证 σ 为模单同态，则 $\sigma(x)=0\Rightarrow x=0$ 指出向量组 $(v_1,v_2,\cdots,v_n)$ 线性无关。由该定理，也经常定义最大线性无关组的元素个数为秩

3.4 模同态与矩阵

定义 3.10 (矩阵定义)

设 R 为幺环，$a_1,\cdots,a_q$ 为右 R 模 L 的一组基，$b_1,\cdots,b_p$ 为右 R 模 M 的一组基。给定一个模同态 $f:\mathrm{L}\to\mathrm{M}$，考虑 L 内的一个向量

$$x=a_1\xi_1+\cdots+a_q\xi_q$$

和它在 M 内的像

$$f(x)=y=b_1\eta_1+\cdots+b_p\eta_p$$

令

$$\begin{cases}f(a_1)=c_1=b_1\alpha_{11}+b_2\alpha_{21}+\cdots+b_p\alpha_{p1}\\ \cdots\cdots\cdots\cdots\\ f(a_q)=c_{1q}=b_1\alpha_{1q}+b_2\alpha_{2q}+\cdots+b_p\alpha_{pq}\end{cases}\tag{3.3}$$

于是有

$$f(x)=c_1\xi_1+\cdots+c_q\xi_q=(b_1\alpha_{11}+b_2\alpha_{21}+\cdots+b_p\alpha_{p1})\xi_1+\cdots+(b_1\alpha_{1q}+\cdots+b_p\alpha_{pq})\xi_q$$

把第二个等号右端的加法按列实施，即得对于 $f(x)$ 的坐标要找的值，即

$$\begin{cases}\eta_1=\alpha_{11}\xi_1+\alpha_{12}\xi_2+\cdots+\alpha_{1q}\xi_q\\ \cdots\cdots\cdots\cdots\\ \eta_p=\alpha_{p1}\xi_1+\alpha_{p2}\xi_2+\cdots+\alpha_{pq}\xi_q\end{cases}\tag{3.4}$$

称该公式为 f 关于 L 的基 $(a_j)_{1\leqslant j\leqslant q}$ 和 M 的基 $(b_i)_{1\leqslant i\leqslant p}$ 的方程，可简记为：

$$\eta_i=\sum_{j=1}^{q}\alpha_{ij}\xi_j\quad(1\leqslant i\leqslant p)$$

反之，给定标量 $\alpha_{ij}\in\mathrm{R}(1\leqslant i\leqslant p,1\leqslant j\leqslant q)$，并且用式 (3.4) 定义一个从 L 到 M 内的映射 f，f 把关

于 L 的给定的基坐标为 $\xi_1,\cdots,\xi_q$ 的向量 $x\in \mathrm{L}$ 变换为关于 M 的给定的基坐标为按照关系 (3.4) 算出的 $\eta_1,\cdots,\eta_p$ 的向量。事实上有

$$\begin{aligned} f(x) &= b_1\eta_1+\cdots+b_p\eta_p \\ &= b_1\left(\alpha_{11}\xi_1+\alpha_{12}\xi_2+\cdots+\alpha_{1q}\xi_q\right)+\cdots+b_p\left(\alpha_{p1}\xi_1+\alpha_{p2}\xi_2+\cdots+\alpha_{pq}\xi_p\right) \\ &= c_1\xi_1+\cdots+c_q\xi_q \end{aligned}$$

其中向量 c_j 由公式 (3.3) 给定，则 f 为一个模同态，其存在性由定理 (3.6) 保证。另外，存在唯一的一组标量 α_{ij}，使得 f 由关系 (3.4) 给定，因为计算表明 α_{ij} 必然是向量 $f(a_i)$ 关于 M 的基 $(b_j)_{1\leqslant j\leqslant q}$ 的坐标，则完全确定了 α_{ij}

由此为了定义同态 f，显然只需知道由标量 α_{ij} 组成的表格

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1q} \\ \vdots & \vdots & & \vdots \\ \alpha_{p1} & \alpha_{p2} & \cdots & \alpha_{pq} \end{pmatrix}$$

称该表格为 p 行 q 列的元素在环 R 内的矩阵，称 (α_{ij}) 为矩阵的元素，称该表格为模同态 f 关于 L 的基 $(a_j)_{1\leqslant j\leqslant q}$ 和 M 的基 $(b_i)_{1\leqslant i\leqslant p}$ 的矩阵

当 $\mathrm{L}=\mathrm{M}$，即当 f 为模 L 的一个模自同态时，经常在 L 内和 M 内使用同一个基 $a_1,\cdots,a_p$，这时则称对应矩阵为关于 L 的一个基的自同态的矩阵。所述矩阵显然有 p 行 p 列，称该矩阵为一个元素在 R 内的 p 阶方阵

♣

定理 3.7 (同态交换群)

设 L 和 M 为两个在环 K 上的左 K 模，用 $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\mathrm{M})$ 表示所有从 L 到 M 内的线性映射的集合，若映射 $f,g:\mathrm{L}\to\mathrm{M}$ 为从 L 到 M 内的模同态，则有下列命题成立：

1) 映射 $f+g:x\to f(x)+g(x)$ 也为从 L 到 M 内的模同态。

2) 配备了运算 $(f,g)\to f+g$ 的集合 $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\mathrm{M})$ 为从 L 为一个交换群

♡

证明 1) 令 $h=f+g$，则有

$$\begin{aligned} h(\lambda x+\mu y) &= f(\lambda x+\mu y)+g(\lambda x+\mu y)=\lambda f(x)+\mu f(y)+\lambda g(x)+\mu g(y) \\ &= \lambda[f(x)+g(x)]+\mu[f(y)+g(y)]=\lambda h(x)+\mu h(y) \end{aligned}$$

第一个命题得证，下证第二个命题

2) 考虑所有从 L 到 M 内的映射的集合 E，配备了运算 $(f,g)\to f+g$，显然 $(\mathrm{E},+)$ 为一个交换群。下证 $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\mathrm{M})$ 为从 L 为 E 的一个子群。$\mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\mathrm{M})$ 为从 L 显然含有 E 的中性元 (即从 L 到 M 内的处处取零值的映射)，又若 f,g 为同态，类似第一个命题证明过程，有 $f-g$ 也为同态，则由子群判别法 (1.1) 第二个命题得证

注 由该定理，称所有从环 K 上模 L 到环 K 上模 M 内的线性映射的集合 $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\mathrm{M})$ 为同态 (交换) 群

注 若 K 为交换环，$\mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\mathrm{M})$ 为从 L 到 M 内的映射的集合 E 的子模

定义 3.11 (线性型)

设 L 为环 K 上的一个右模，$f:\mathrm{L}\to\mathrm{K}$ 为从 L 到右 K 模 K 内的模同态，若满足

$$(\forall x,y\in\mathrm{L})(\forall\alpha,\beta\in\mathrm{K}):f(x\alpha+y\beta)=f(x)\alpha+f(y)\beta$$

则称 $f:\mathrm{L}\to\mathrm{K}$ 为 L 上的线性型

♣

注 (模对偶)

由定理 (3.7)，线性型为交换群 $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\mathrm{K})$ 的元素。注意到 L 上的两个线性型的和 $f+g$ 由函数 $f(x)+g(x)$ 定义。设 f 为 L 上的线性型，$\lambda\in\mathrm{K}$ 为标量，考虑 L 上的由 $g(x)=\lambda\cdot f(x)$ 定义的函数。由 $f(x\alpha+y\beta)=$

$f(x)\alpha+f(y)\beta$ 左乘 λ 后，考虑在一个环内的计算规则则有

$$(\forall x,y\in \mathrm{L})(\forall \alpha,\beta\in \mathrm{K}):g(x\alpha+y\beta)=g(x)\alpha+g(y)\beta$$

则 g 仍为 L 上的一个线性型，自然记为 $g=\lambda f$

由此对 $\mathrm{Hom_K(L,K)}$ 定义了第二个运算，即以一个标量“乘”这个集合的元素，则配备了加法和标量乘法的 $\mathrm{Hom_K(L,K)}$ 实际上为一个左 K 模

称配备了刚定义的左 K 模结构的集合 $\mathrm{Hom_K(L,K)}$ 为右 K 模 L 的对偶，通常记为 L^*

定理 3.8 (矩阵加法)

设 L 和 M 为有限生成自由 K 右模，f 和 g 为从 L 到 M 内的两个同态。设 A 和 B 为 f 和 g 关于 L 的一个基 (a_i) 和 M 的一个基 (b_j) 的矩阵，则 $f+g$（关于这两个基）的矩阵存在 ♡

证明 选择 L 的一个关于所考虑的 L 和 M 的基的矩阵 $\mathrm{A}=(\alpha_{ij})_{1\leqslant i\leqslant p,1\leqslant j\leqslant q}$，$\mathrm{B}=(\beta_{ij})_{1\leqslant i\leqslant p,1\leqslant j\leqslant q}$，则有

$$f(a_j)=b_1\alpha_{1j}+\cdots+b_p\alpha_{pj},g(a_j)=b_1\beta_{1j}+\cdots+b_p\beta_{pj}$$

令 $h=f+g$，则 h 关于所考虑的基的矩阵表示为 $\mathbf{C}=(\gamma_{ij})_{1\leqslant i\leqslant p,1\leqslant j\leqslant q}$，则有

$$h(a_j)=f(a_j)+g(a_j)=b_1(\alpha_{1j}+\beta_{1j})+\cdots+b_p(\alpha_{pj}+\beta_{pj})$$

因此 C 的元素为 $\gamma_{ij}=\alpha_{ij}+\beta_{ij}\quad(1\leqslant i\leqslant p,1\leqslant j\leqslant q)$。给定系数在 K 内的两个矩阵 $\mathrm{A}=(\alpha_{ij})$ 和 $\mathrm{B}=(\beta_{ij})$，则 $f+g$（关于这两个基）的矩阵存在

注 由该定理，称关系 $(\forall i\in\overline{1;p})(\forall j\in\overline{1;q}):\gamma_{ij}=\alpha_{ij}+\beta_{ij}\quad(1\leqslant i\leqslant p,1\leqslant j\leqslant q)$ 给定的矩阵 $\mathrm{C}=(\gamma_{ij})$ 为两个矩阵 $\mathrm{A}=(\alpha_{ij})$ 和 $\mathrm{B}=(\beta_{ij})$ 的和，记为 $A+B$

注 注意到能把元素在 K 中的 p 行 q 列的矩阵的集合看作一个加法群，且可以看作一个（左或）右 K 模，只需对于矩阵 $\mathrm{A}=(a_{ij})$ 和 $\lambda\in\mathrm{K}$，用以下公式定义 $\lambda\mathrm{A}$ 和 $\mathrm{A}\lambda$：

$$\lambda\mathrm{A}=(\lambda a_{ij}),\quad \mathrm{A}\lambda=(a_{ij}\lambda)$$

3.5 交换环上行列式与多重线性映射

第 4 章 体

4.1 基本概念

定义 4.1

利用下面三条性质可以公理化定义体：

A1：$(R,+,\cdot)$ 为结合环

A2：（非零元存在性）$(\exists a\in R)(\forall b\in R):(a+b\neq b)\wedge(b+a\neq b)$

A3：（可除性）$(\forall a,b\in R)(a\neq 0):(\exists x\in R)(ax=b)\wedge(\exists y\in R)(ya=b)$

称满足公理 A1A2A3 的代数系统 $(R,+,\cdot)$ 为体，称体 $(R,+,\cdot)$ 上的环的加法群 $(R,+)$ 为体 $(R,+,\cdot)$ 的加法群，称体 $(R,+,\cdot)$ 上非零元素的乘法群 $(R/\{0\},\cdot)$ 为体 $(R,+,\cdot)$ 的乘法群

若体 $(R,+,\cdot)$ 上的环为交换环，称体 $(R,+,\cdot)$ 为域

♣

性质 乘法左单位元存在，乘法非零元左逆元存在

证明 $(\exists a\in R):(a+b\neq b)\wedge(b+a\neq b)\Leftrightarrow(\exists a\neq 0)$，又

$$[(\forall a\neq 0,b\in R):(\exists y\in R)(ya=b)]\Rightarrow(\exists y\in R)(ya=a)$$

乘法左单位元存在性得证，下记左单位元为 1，同理有

$$[(\forall a\neq 0,b\in R):(\exists y'\in R)(y'a=b)]\Rightarrow(\exists y'\in R)(y'a=1)$$

乘法非零元左逆元存在性得证

性质 乘法单位元存在性，乘法非零元逆元存在性

性质 （乘法单位元唯一性）

$(\exists! e\in R)(\forall a\in R):(ae=ea=a)$

性质 （非零元除法唯一性）

$(\forall a\neq 0,b\in R):[(\exists! x\in R)(ax=b)\wedge(\exists! y\in R)(ya=b)$

性质 （无零因子性）

$(\forall a,b\in R)[(ab=0)\Rightarrow(a=0)\vee(b=0)]$

证明 反证：假设 $(\exists a,b\in R)(a\neq 0)\wedge(b\neq 0):[(ab=0)\Rightarrow(a=0)\vee(b=0)]$，则由除法唯一性有 $(\exists! x\in R)(ax=0)$，注意到 $x=0$ 与 $x=b\neq 0$ 均有 $ax=0$，与 x 唯一性矛盾

4.2 体上的模

注 下面要引入的向量空间，只是模的推广，但在体上的有限维向量空间上具有重要的性质：基的存在性，由此下面重新陈述关于向量空间的术语，另外给出线性代数部分最为重要的结论

定义 4.2 (向量空间公理化)

设 $\mathbf{R}$ 为体，$(M,+)$ 为 Abel 群，若有

$\mathbf{M_1}$：（模性）$\exists f:\mathbf{R}\times M\to M,(a,x)\mapsto ax\in M$

$\mathbf{M_2}$：（纯量对向量左分配性）$(\forall a\in\mathbf{R})(\forall x,y\in M):a(x+y)=ax+ay$

$\mathbf{M_3}$：（向量对纯量左分配性）$(\forall a,b\in\mathbf{R})(\forall x\in M):(a+b)x=ax+bx$

$\mathbf{M_4}$：（代数左结合性）$(\forall a,b\in\mathbf{R})(\forall x\in M):(ab)x=a(bx)$

$\mathbf{M_5}$：（酉性）$(\forall x\in M):1x=x$

则称 M 为 $\mathbf{R}$ 上的一个左向量空间，或称 M 为左 $\mathbf{R}$ 向量空间，称 $f:\mathbf{R}\times M\to M,(a,x)\mapsto ax\in M$

为 $\mathbf{R}$ 与 M 间乘法，称 $\mathbf{R}$ 为该向量空间的基础体，称基础体的元素为标量，称向量空间元素为向量
对称地定义，若有
$\mathbf{M}_1'$：（模性）$\exists f' : M \times \mathbf{R} \to M, (x,a) \mapsto xa \in M$
$\mathbf{M}_2'$：（纯量对向量右分配性）$(\forall a \in \mathbf{R})(\forall x,y \in M) : (x+y)a = xa + ya$
$\mathbf{M}_3'$：（向量对纯量右分配性）$(\forall a,b \in \mathbf{R})(\forall x \in M) : x(a+b) = xa + xb$
$\mathbf{M}_4'$：（代数右结合性）$(\forall a,b \in \mathbf{R})(\forall x \in M) : x(ab) = (xa)b$
$\mathbf{M}_5'$：（酉性）$(\forall x \in M) : x1 = x$
则称 M 为 $\mathbf{R}$ 上的一个右向量空间，或称 M 为右 $\mathbf{R}$ 模，称 $f' : M \times \mathbf{R} \to M, (x,a) \mapsto xa \in M$ 为 M
与 $\mathbf{R}$ 间乘法，称 $\mathbf{R}$ 为该向量空间的基础体，称基础体的元素为标量，称向量空间元素为向量
若 M 同时为左 $\mathbf{R}$ 向量空间与右 $\mathbf{R}$ 向量空间，且满足
$\mathbf{M}_6$:$(\forall a,b \in \mathbf{R})(\forall x \in M) : (ax)b = a(xb)$
则称 M 为 $\mathbf{R}$ 向量空间或 $\mathbf{R}$ 双向量空间。
若 $\mathbf{R}$ 为域，则左 $\mathbf{R}$ 向量与右 $\mathbf{R}$ 向量相等，即为 $\mathbf{R}$ 向量空间

♣

注 设 $(R,+,\cdot)$ 为体，令 $R = \tilde{R}$，若 R 上乘法改为 $* : \tilde{R} \times \tilde{R} \to \tilde{R}, (x,y) \mapsto y * x$，则称 $(\tilde{R},+,*)$ 为 R 上反环；设 M 为 R 上右向量空间，若反环 $\tilde{R}$ 与 M 间乘法为 $\tilde{R} \times M \to M, (a,x) \mapsto a * x = xa$，则 M 为 $\tilde{R}$ 上左向量空间

这表明左向量空间与右向量空间在体上反环下性质相同，因此以下仅讨论左或右向量空间并不妨碍命题的一般性

定理 4.1

设 M 为一个体上的有限维向量空间，X 为 M 的生成元的有限集，A 为 X 的一个子集，若 A 的元素线性无关，则存在 M 的一个基 B 满足

$$\mathrm{A} \subset \mathrm{B} \subset \mathrm{X}$$

♡

证明 考虑 X 的所有如下子集：这些子集包含 A 并且为自由的（即线性无关）。如此定义的子集显然存在，例如 A 本身。在这些子集中考虑元素数目最多的一些子集，设 B 为其中的一个子集，由定理 (3.5) 知仅需证 B 生成 M，又由 X 生成 M，则仅需证所有 $x \in \mathrm{X}$ 为 B 的元素的线性组合

若 $x \in \mathrm{B}$，定理显然。假定 $x \notin \mathrm{B}$，集合 $\mathrm{B}' = \mathrm{B} \cup \{x\}$ 包含于 X 内（比 B 含有更多的元素）。由条件则有 $\mathrm{A} \subset \mathrm{B}'$，且 B' 不可能自由（由基数最大性）。于是若用 $x_1, \cdots, x_r$ 表示 B 的不同元素，将存在非平凡线性关系

$$\lambda_1 x_1 + \cdots + \lambda_r x_r + \lambda x = 0 \tag{4.1}$$

其中 $\lambda_1, \cdots, \lambda_r, \lambda$ 不全为零。特别地，有 $\lambda \neq 0$（因为若不然，则式 (4.1) 将缩减为元素 $x_i \in \mathrm{B}$ 之间的一个非平凡的线性关系，这与 B 为自由的相矛盾）

由 $\lambda \neq 0$，又由 K 为一个体，则 λ 在 K 内可逆，用 λ 的逆元乘式 (4.1) 左端即得

$$x = -\lambda^{-1}\lambda_1 x_1 - \cdots - \lambda^{-1}\lambda_r x_r$$

则证明了所有 $x \in \mathrm{X}$ 为 B 的元素的线性组合，由此定理即证

定理 4.2 (体上向量空间基存在性)

体上的有限维向量空间具有基

♡

证明 由定理 (4.1) 知，只要存在有限生成元集的自由子集即可，而这是显然的

注 实际上，对于无穷维向量空间，基的存在性也是成立的

定理 4.3 (线性无关组元素个数)

设 M 为体 K 上的有限维向量空间，p 为一个整数，M 具有 p 个向量组成的基。若 M 的 q 个向量为线性无关的，则有 $q \leqslant p$

♡

证明 设 $(a_i)_{1\leqslant i\leqslant p}$ 为 M 的一组基，$b_1,\cdots,b_q$ 为 M 的元素。若 $q>p$，则显然存在向量 b_j 之间的一个非平凡的线性关系，以下使用数学归纳法证明

若 $p=0$，则定理平凡，这时有 $\mathrm{M}=\{0\}$，假设 $q\geqslant 1$，则有 b_j 满足关系

$$1\cdot b_1+0\cdot b_2+\cdots+0\cdot b_q=0$$

则与条件线性无关矛盾，从而 $q<1$，即有 $q\leqslant 0\leqslant p$

现假定定理对于 $p-1$ 成立。设 M' 为由 $a_1,\cdots,a_{p-1}$ 生成的 M 的子空间，则有关系

$$(\forall j\in\overline{1;q}):b_j=b'_j+\alpha_j a_p \tag{4.2}$$

其中 $b'_j\in\mathrm{M}'$，且标量 $\alpha_j\in\mathrm{K}$

若所有的 α_j 为零，则 b_j 在 M' 内。由假设有 M' 具有一个由 $p-1$ 个向量组成的基，考虑到 $q>p$ 必有 $q>p-1$，则由前面的讨论这时存在 b_j 之间的一个非平凡的线性关系

若 α_j 不全为零，不妨设 $\alpha_q\neq 0$。由 K 为体，则 α_q 可逆，而 (4.2) 的最后一个关系给出

$$a_p=\alpha_q^{-1}\left(b_q-b'_q\right)$$

代入到 (4.2) 中的其他关系得

$$(\forall j\in\overline{1;q-1}):b_j-\alpha_j\alpha_q^{-1}b_q=b'_j-\alpha_j\alpha_q^{-1}b'_q \tag{4.3}$$

关系 (4.3) 指出 $q-1$ 个向量 $b_j-\alpha_j\alpha_q^{-1}b_q$ 在子空间 M' 内。假设 $q>p$，自然有 $q-1>p-1$，由归纳假设有存在线性关系

$$\lambda_1\left(b_1-\alpha_1\alpha_q^{-1}b_q\right)+\cdots+\lambda_{q-1}\left(b_{q-1}-\alpha_{q-1}\alpha_q^{-1}b_q\right)=0$$

其中 $\lambda_1,\cdots,\lambda_{q-1}$ 不全为零，而该关系可以改写为

$$\left(\lambda_1 b_1+\cdots+\lambda_q b_q=0\right)\wedge\left(\lambda_q=-\left(\lambda_1\nu_1+\cdots+\lambda_{q-1}\nu_{q-1}\right)\right)$$

则 $b_1,\cdots,b_q$ 之间的非平凡线性关系的存在性得证，与条件矛盾，则 $q\leqslant p$

综上，定理得证

注 该定理不仅对体上的模成立，实际上对交换环上的模也成立

定理 4.4 (有限维数不变性)

设 M 为体 K 上有限维向量空间，则 M 的所有基有同样数目的元素

♡

证明 设 $(a_i)_{1\leqslant i\leqslant p}$ 和 $(b_j)_{1\leqslant j\leqslant q}$ 为 M 的两个基，而 $p=q$ 等价于 $p\leqslant q$ 和 $q\leqslant p$。由对称性只需证明 $p\leqslant q$，由定理 (3.5) 的推论，基必为线性无关组，则由定理 (4.3) 即证

注 该定理表明存在一个完全确定的整数 n，使得 M 的所有的基都具有 n 个元素，由此引入维数的概念

定义 4.3 (维数)

称体 K 上向量空间 M 的基的个数为体 K 上向量空间 M 的维数 (不引起混淆时可简称为 M 的维数)，记为

$$\dim_K(M)$$

不引起混淆时可简记为 $\dim(M)$。当 $M=\{0\}$ 时约定取 $\dim(M)=0$

♣

定理 4.5 (有限维向量空间同构充要条件)

设 L 和 M 为体 K 上有限维向量空间，则 L 和 M 同构的充要条件为 $\dim(\mathrm{L})=\dim(\mathrm{M})$

♡

证明 若存在从 L 到 M 上的模同构 f，且 f 把 L 的一个基映射到 M 的一个基上，由此则有 $\dim(\mathrm{L})=\dim(\mathrm{M})$。反之若该条件满足，设 n 为 L 和 M 的公共维数，则由定理 (3.5) 与秩 n 自由模的定义推出 L 和 M 都同构于 K^n，则二者同构

注 两个无穷维向量空间并不总是同构

定义 4.4 (零化子)

设 L 为一个体 K 上的有限维向量空间，M 为 L 的一个子向量空间，在 L 的对偶 L^* 内考虑 L 上的满足关系

$$(\forall x\in \mathrm{M}):f(x)=0$$

的线性型 f 的集合，称该集合为 M 在 L^* 内的零化子，记为 M^0

♣

注 注意到，若零化子含有两个线性型 f 和 g，并且令 $h=\alpha f+\beta g$，其中 α 和 β 为任意标量，则有

$$(\forall x\in \mathrm{M}):h(x)=\alpha\cdot f(x)+\beta\cdot g(x)=0$$

故 $h\in \mathrm{M}^0$，则零化子为 L^* 的向量子空间

定理 4.6

设 L 为一个有限维向量空间，M 为 L 的一个向量子空间，M^0 为 M 在 L^* 内的零化子，$x\in \mathrm{L}$，则有

$$x\in \mathrm{M}\Leftrightarrow(\forall f\in \mathrm{M}^0):f(x)=0$$

♡

证明 必要性显然。下证充分性：正如在定理 2 的推论 2 的证明中看到的，存在 L 的一个基 $(a_i)_{1\leqslant i\leqslant r}$ 和一个整数 $p\leqslant r$，使得 M 是由 $a_1,\cdots,a_p$ 生成的. 设 $f_1,\cdots,f_r$ 是关于基 $a_1,\cdots,a_r$ 的坐标函数，显然 M 由关系

$$f_{p+1}(x)=\cdots=f_r(x)=0$$

定义，换句话说，M^0 含有线性型 $f_{p+1}(x),\cdots,f_r(x)$，并且关系 (3) 刻画了 M 的元素的特征. 如果条件 (2) 对于所有 $f\in \mathrm{M}^0$ 成立，显然条件 (3) 因此成立. 定理证毕.

4.3 体上线性方程组

4.4 扩张

第 5 章 域

5.1 基本概念

定义 5.1 (素体)

称不包含任意非平凡子体的体为素体

定理 5.1 (素体构造)

设 Π 为一个素体，则 $\Pi\cong\mathbb{Z}_p$ （p 为素数）或 $\Pi\cong\mathbb{Q}$；反之，$\mathbb{Z}_p,\mathbb{Q}$ 都为素体

证明 设 e 为 Π 的单位元，则 $\mathbb{Z}e=\{ne\mid n\in\mathbb{Z}\}$ 为 Π 的子环且有 $\mathbb{Z}$ 到 $\mathbb{Z}e$ 的环同态 $\pi:\pi(n)=ne(n\in\mathbb{Z})$，则 $\mathbb{Z}e=\mathbb{Z}/\ker\pi$。由 $\mathbb{Z}$ 为 Euclid 环，故有 p 使得 $\ker\pi=\langle p\rangle$。则 Π 为体，则 $\mathbb{Z}e$ 为整环，即得 p 为素数或零

当 p 为素数时，$\mathbb{Z}e=\mathbb{Z}_p$ 为域，Π 无非平凡子体，则 $\Pi=\mathbb{Z}e\cong\mathbb{Z}_p$

当 $p=0$ 时，$\mathbb{Z}\cong\mathbb{Z}e$，则 $\mathbb{Z}e\subset\Pi$。此时 $\mathbb{Z}e$ 的分式域与 $\mathbb{Z}$ 的分式域，即 $\mathbb{Q}$ 同构且 $\mathbb{Z}e$ 的分式域在 Π 中，故 $\Pi\cong\mathbb{Q}$

反之，$\mathbb{Z}_p$ 对于加法为素数阶群，由 Lagrange 定理 (1.10) 知得 $\mathbb{Z}_p$ 无非平凡子群，故 $\mathbb{Z}_p$ 无非平凡子体，则 $\mathbb{Z}_p$ 为素体

若 F 为域 $\mathbb{Q}$ 的子体，则 $1\in F$，进而 $\mathbb{Z}\subset F$，则有 $\mathbb{Q}\subseteq F,F=\mathbb{Q}$，则 $\mathbb{Q}$ 为素体

注 该定理表明素体都是域，因而也称素体为**素域**

定义 5.2 (特征)

若体 K 包含的素域与 $\mathbb{Q}$ 同构，则称 K 的特征为零。若体 K 包含的素域与 $\mathbb{Z}_p$ 同构，则称 K 的特征为 p，记 K 的特征为 $\operatorname{ch}K$

定理 5.2 (特征性质)

设 K 为一个体，p 为素数，则下列命题成立

1) $\operatorname{ch}K=p$ 当且仅当 $(\forall a\in K):pa=0$

2) $\operatorname{ch}K=0$ 当且仅当 $(\forall n\in\mathbb{N}):[(na\neq0)\wedge(a\in K^*=K\backslash\{0\})]$

证明 记 K 单位元为 e，K 中素域为 Π

1) 若 $\operatorname{ch}K=p$，即 $\Pi\cong\mathbb{Z}_p$，则 $pe=0$，则 $pa=pe\cdot a=0$；反之，若 $(\forall a\in K):pa=0$，则 $pe=0$，则由定理 (5.1) 得 $\Pi\cong\mathbb{Z}_p$，则 $\operatorname{ch}K=p$

2) 若 $\operatorname{ch}K=0$，则 $\mathbb{Z}\cong\mathbb{Z}e$，则 $(\forall n\in\mathbb{N}):ne\neq0$，则 $(\forall a\in K^*):na=ne\cdot a\neq0$；反之，$(\forall n\in\mathbb{N})(\forall a\in K^*):na\neq0$，特别地，$ne\neq0$，则 $\mathbb{Z}\cong\mathbb{Z}e$，则 $\operatorname{ch}K=0$

推论 5.1

数域的特征为零

5.2 分式域

定义 5.3 (分式域)

若整环 R 为域 F 的子环且有

$$(\forall a \in F)(\exists b, c \in R) : a = bc^{-1}$$

则称 F 为 R 的分式域 ♣

例题 5.1 有理数域 Q 为整数环 Z 的分式域

定理 5.3

设 R 为整环，则 R 必有分式域 ♡

证明 令 $R^* = R\backslash\{0\}$，在集合 $R \times R^*$ 中定义加法与乘法，即

$$(\forall((a,b),(c,d)) \in R \times R^*) : (a,b) + (c,d) = (ad + bc, bd)$$

$$(\forall((a,b),(c,d)) \in R \times R^*) : (a,b)(c,d) = (ac, bd)$$

易验证 $R \times R^*$ 对上述加法与乘法均为交换么半群，零元及么元分别为 $(0,1),(1,1)$。在 $R \times R^*$ 中定义一个关系 “$\sim$”，即

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc$$

先证明关系 $\sim$ 为等价关系。由 $ab = ab$ 知 $(a,b) \sim (a,b)$，又若 $ad = cb$，则有 $(a,b) \sim= (c,d)$ 且 $cb = ad$，即 $(c,d) \sim (a,b)$。假设 $(a,b) \sim (c,d),(c,d) \sim (e,f)$，则 $adf = bcf = bde$，由 R 为整环，$d \neq 0$，则由 $af = be$，即 $(a,b) \sim (e,f)$。

其次证明关系对于 $R \times R^*$ 中的乘法为同余关系。设

$$(a,b) \sim (c,d), \quad (e,f) \sim (g,h)$$

于是有

$$(a,b)(e,f) = (ae, bf), \quad (c,d)(g,h) = (cg, dh)$$

而 $(ae)(dh) = adeh = bcfg = (bf)(cg)$，即有

$$(a,b)(e,f) \sim (c,d)(g,h)$$

再证明关系 $\sim$ 对于 $R \times R^*$ 中的加法为同余关系。设

$$(a,b) \sim (c,d), \quad (e,f) \sim (g,h)$$

则有

$$(a,b) + (e,f) = (af + be, bf), \quad (c,d) + (g,h) = (ch + dg, dh)$$

这时

$$(af + be)dh = adfh + bedh = bcfh + fgbd = (ch + dg)bf$$

则有 $((a,b) + (e,f)) \sim ((c,d) + (g,h))$

令 $F = R \times R^*/\sim$ 为商集，以 $\frac{a}{b}$ 表示 (a,b) 所在等价类，则在 F 中有加法与乘法运算：

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

显然商集对加法与乘法都为交换么半群，记零元素与么元素 $\frac{0}{1}, \frac{1}{1}$ 为 $0 = \frac{0}{1}, 1 = \frac{1}{1}$。由于 $0 \cdot d = 0 \cdot 1$, 故有 $(0,1)$

与 $(0,d)$ 等价, 即 $\dfrac{0}{1}=\dfrac{0}{d}$. 又由 $1\cdot d=1\cdot d$ 得

$$\frac{1}{1}=\frac{d}{d}=1$$

$$\frac{a}{b}+\frac{-a}{b}=\frac{ab-ab}{b^2}=\frac{0}{b^2}=0$$

则 F 对加法为交换群

又若 $\dfrac{a}{b}\neq 0$，即 $a\neq 0$，则 $(b,a)\in R\times R^*$，即 $\dfrac{b}{a}\in F$。这时

$$\frac{a}{b}\cdot\frac{b}{a}=\frac{ab}{ab}=1$$

则 $F^*=F\backslash\{0\}$ 为交换群且

$$\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}$$

又由

$$\left(\frac{a}{b}+\frac{c}{d}\right)\cdot\frac{f}{e}=\frac{ad+bc}{bd}\cdot\frac{f}{e}=\frac{adf+bcf}{bde}=\frac{adef+bcef}{bdee}=\frac{af}{be}+\frac{cf}{de}=\frac{a}{b}\cdot\frac{f}{e}+\frac{c}{d}\cdot\frac{f}{e}$$

得 F 中加法与乘法间分配律成立，故 F 为域。

由 $\dfrac{a}{1}=\dfrac{b}{1}$ 当且仅当 $a=b$ 且

$$\frac{a}{1}+\frac{b}{1}=\frac{a+b}{1},\quad \frac{a}{1}\cdot\frac{b}{1}=\frac{ab}{1},$$

则 R 为 F 的子环。对 F 中任一元素 $\dfrac{a}{b}$ 有

$$\frac{a}{b}=\frac{a}{1}\cdot\frac{1}{b}=\frac{a}{1}\cdot\left(\frac{b}{1}\right)^{-1}$$

则 F 为 R 分式域

注 该定理条件减弱为无零因子交换环也正确

定理 5.4

整环 R 的分式域 F 为以 R 为子环的最小域 ♡

证明 设 F' 为域且 R 为 F' 子环，则 F' 中子集

$$F_1=\left\{ab^{-1}\mid a,b\in R,b\neq 0\right\}$$

为 F' 子域，事实上

$$ab^{-1}+cd^{-1}=(ad+cd)(bd)^{-1},\quad -\left(ab^{-1}\right)=(-a)b^{-1}$$

故 F_1 对加法为 F' 的子群。又若 $ab^{-1},cd^{-1}\in F_1\backslash\{0\}$，则

$$\left(ab^{-1}\right)\left(cd^{-1}\right)^{-1}=(ad)(bc)^{-1}$$

故 $F_1\backslash\{0\}$ 为 $F'\backslash\{0\}$ 的子群，即 F_1 为 F 的子域。又 $\frac{a}{b}\to ab^{-1}$ 为 R 的分式域 F 到 F_1 上的同构，则有 $F\subseteq F'$.

注 该定理条件减弱为无零因子交换环也正确

注 该定理表明 R 的分式域唯一

5.3 扩张

定义 5.4 (扩域)

若域 F 为域 K 的子域，则称 K 为域 F 的扩域

设 S 为 K 的子集，则称 K 中所有包含 $F\cup S$ 的子域的交（即由 F 与 S 生成的子域）为 F 上添加 S 所得的域，也称 S 在 F 上生成的域，记为 $F(S)$

♣

注 （有限和）

以 $F[S]$ 表示下列形式的一切有限和：

$$\sum_{i_1,i_2,\cdots,i_n\geqslant 0}\alpha_{i_1i_2\cdots i_n}a_1^{i_1}a_2^{i_2}\cdots a_n^{i_n},\quad a_j\in S,\quad j=1,2,\cdots,n,\quad \alpha_{i_1i_2\cdots i_n}\in F$$

所构成的集合，显然 $F[S]$ 为 K 的子环，它的分式域恰为 $F(S)$

特别地，当 $S=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ 为有限集时，分别记

$$F[S]=F[\alpha_1,\alpha_2,\cdots,\alpha_n],\quad F(S)=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$$

定理 5.5 (扩域结构)

设 K 为域 F 的扩域，$S\subseteq K$，则下列命题成立

1) $F(S)=\bigcup\limits_{S'\subseteq S}F(S')$，其中 S' 遍历 S 所有有限子集

2) 若 $S=S_1\cup S_2$，则 $F(S)=F(S_1)(S_2)$

♡

证明 1) 显然 $F(S')\subseteq F(S)$，则 $\bigcup\limits_{S'\subseteq S}F(S')\subseteq F(S)$

反之 $(\forall a\in F(S))(\exists f,g\in F[S]):a=\dfrac{f}{g}$，由于 f,g 的表达式均为有限和的形式，则存在 S 有限子集 S_0'，使 $f,g\in F[S_0']$，则 $a=\dfrac{f}{g}\in F[S_0']\subseteq\bigcup\limits_{S'\subseteq S}F(S')$

2) 由 $F(S_1\cup S_2)$ 为 K 中包含 $F,S_1\cup S_2$ 的最小子域，而 $F,S_1,S_2\subseteq F(S_1)(S_2)$，则有

$$F\left(S_1\bigcup S_2\right)\subseteq F(S_1)(S_2)$$

反之，$F(S_1)(S_2)$ 为包含 $F(S_1),S_2$ 的最小子域，而

$$F(S_1)\subseteq F(S_1\cup S_2),\quad S_2\subseteq F(S_1\cup S_2)$$

则 $F(S_1)(S_2)\subseteq F(S_1\cup S_2)$

推论 5.2

设 K 为域 F 的扩域，$S\subseteq K$，$\alpha_1,\alpha_2,\cdots,\alpha_n\in S$，则有

$$F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$$

♡

注 定理 (5.5) 和该推论表明在一个域上添加一个有限集合 S 可转化为添加有限个元素的问题，而添加有限个元素的问题可转化成添加一个元素的问题

定义 5.5 (单扩域)

设 K 为 F 的扩域，若

$$(\exists\alpha\in K):K=F(\alpha)$$

则称 K 为 F 的单扩域

若 α 为 F 上代数元，称 $K=F(\alpha)$ 为 F 的单代数扩域

若 α 为 F 上超越元，称 $K=F(\alpha)$ 为 F 的单超越扩域

♣

定义 5.6 (扩张次数)

设 K 为域 F 的扩域，称 K 作为域 F 上线性空间的维数为 K 对 F 的扩张次数，记为 $[K:F]$，若 $[K:F]<+\infty$，则称 K 为 F 的有限扩张 ♣

注 (扩张次数)

若设 $F(\alpha)$ 为 F 的单扩张。当 α 为 F 上代数元时，$F(\alpha)$ 为 F 的有限扩张且 $[F(\alpha):F]=\deg(\alpha,F)$；当 α 为 F 上超越元时，$F(\alpha)$ 为 F 的无限扩张

定义 5.7 (代数扩张与超越扩张)

设 K 是域 F 的扩域，若 $\forall\alpha\in K$ 都为 F 上代数元，则称 K 为域 F 的代数扩张，否则称为 K 为域 F 的超越扩张 ♣

定义 5.8

设 K 为 F 的扩域，$\alpha\in K$ 为 F 上代数元。称 $F[x]$ 中以 α 为根的不可约首一多项式为 α 在 F 上不可约多项式，记为 $\mathrm{Irr}(\alpha,F)$。称它的次数为 α 在 F 上的次数，记为 $\deg(\alpha,F)$，即 $\deg(\alpha,F)=\deg(\mathrm{Irr}(\alpha,F))$ ♣

注 显然由定义有

$$\langle \mathrm{Irr}(\alpha,\mathrm{F})\rangle=\{f(x)\in F[x]\mid f(\alpha)=0\}=\{f(x)\in F[x]|\,\mathrm{Irr}(\alpha,\mathrm{F})|f(x)\}.$$

定理 5.6

设 $F(\alpha)$ 为 F 的单代数扩张，又 $\deg(\alpha,F)=n$，则 $F(\alpha)$ 为 F 上的 n 维线性空间且 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 为一组基 ♡

证明 可直接验证 $F(\alpha)$ 为 F 上线性空间，在 $F[x]$ 与 $F[\alpha]=F(\alpha)$ 之间有满同态 η 满足

$$(\forall f(x)\in F[x]):\eta(f(x))=f(\alpha)$$

而 $\ker\eta=\langle\mathrm{Irr}(\alpha,F)\rangle$。由 $\deg(\alpha,F)=n$，则 $(\exists q(x),r(x)\in F[x])$：

$$f(x)=q(x)\,\mathrm{Irr}(\alpha,F)+r(x),\quad \deg r(x)<\deg(\alpha,F)$$

$(\deg 0=-\infty)$ 则 $f(\alpha)=r(\alpha)$，则 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 生成 $F(\alpha)$。又若 $\deg s(x)<\deg(\alpha,F)$，而 $s(\alpha)=0$，则 $\eta(s(x))=0$。则 $\mathrm{Irr}(\alpha,F)\mid s(x)$，则 $s(x)=0$，即 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 线性无关，则 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 为 $F(\alpha)$ 的一组基，则 $F(\alpha)$ 的维数为 n

定理 5.7

设 K 为域 F 的扩域，$\alpha\in K$，则下列条件等价：

1) $F(\alpha)$ 为 F 的代数扩张
2) α 为 F 上代数元
3) $F(\alpha)$ 为 F 的有限扩张

♡

证明 1) $\Rightarrow$ 2). $F(\alpha)$ 为 F 的代数扩张，而 $\alpha\in F(\alpha)$，则 α 为 F 上代数元

2) $\Rightarrow$ 3). α 为 F 上代数元，故由定理 (5.6) 有 $[F(\alpha):F]=\deg(\alpha,F)<+\infty$，则 $F(\alpha)$ 为 F 的有限扩张

3) $\Rightarrow$ 1). 设 $[F(\alpha):F]=n<+\infty$。注意对于 $\forall\beta\in F(\alpha)$，若 $1,\beta,\cdots,\beta^n$ 为 $F(\alpha)$ 中 $n+1$ 个元素，则必线性相关，即存在不全为零的 $a_0,a_1,\cdots,a_n\in F$ 满足 $\sum\limits_{i=0}^{n}a_i\beta^i=0$。$f(x)=\sum\limits_{i=0}^{n}a_ix^i$，则有 $f(\beta)=0$，则 β 为 F 上代数元，则 $F(\alpha)$ 为 F 的代数扩张

推论 5.3

若 K 为域 F 有限扩张，则 K 为 F 代数扩张 ♡

5.4 分裂域

定义 5.9 (分裂域)

设 $F[x]$ 为 F 域上一元多项式环，$f(x)\in F[x],\deg f(x)=n$。若 F 的扩域 K 满足下列条件：
1) $f(x)$ 在 $K[x]$ 内可分解为一次因式之积，即 $f(x)=c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$
2) $K=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$
则称 K 为 $f(x)$ 的分裂域

♣

引理 5.1 (非零一元多项式可在有限扩张中存在根)

设 $f(x)\in F[x],\deg f(x)>0$，则存在 F 的有限扩张 E 使得 $f(x)$ 在 E 中存在根

♡

证明 不妨设 $f(x)$ 首一不可约，若存在扩张 E 包含 $f(x)$ 的根 α，即有 $f(\alpha)=0$，则由环同态 $\varphi:F[x]\to E,g(x)\mapsto g(\alpha)$ 可得 $F[x]/\langle f(x)\rangle$ 同构于 E 的子域 $F(\alpha)$。不妨取 $E=F[x]/\langle f(x)\rangle$，则 $\alpha=x+\langle f(x)\rangle\in E$ 为 E 的生成元，即 $E=F(\alpha)$ 且 $\mathrm{Irr}(\alpha,F)=f(x)$，则 α 为 $f(x)$ 在 E 中一个根

定理 5.8 (非零一元多项式分裂域存在性)

设 $f(x)\in F[x],\deg f(x)>0$，则 $f(x)$ 分裂域存在

♡

证明 对 $\deg f(x)$ 归纳：当 $\deg f(x)=1$ 时，F 即为 $f(x)$ 的分裂域；设 $\deg f(x)=n>1$，$p(x)$ 为 $f(x)$ 的一个不可约因子。从引理 (5.1) 有 F 的单代数扩张 $F_1=F(\alpha_1)$，其中 α_1 满足 $p(\alpha_1)=0$，则 $f(\alpha_1)=0$。$f(x)$ 作为 $F_1[x]$ 内多项式则有分解

$$f(x)=(x-\alpha_1)f_1(x),\quad \deg f_1(x)=\deg f(x)-1$$

则有 $f_1(x)$ 对 F_1 的分裂域

$$K=F_1(\alpha_2,\alpha_3,\cdots,\alpha_n)$$

显然 $f(x)=(x-\alpha_1)f_1(x)\in K[x]$ 且有分解 $f(x)=c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$，又

$$K=F_1(\alpha_2,\alpha_3,\cdots,\alpha_n)=F(\alpha_1)(\alpha_2,\alpha_3,\cdots,\alpha_n)=F(\alpha_1,\alpha_2,\cdots,\alpha_n),$$

则 K 为 $f(x)$ 对 F 的分裂域

注 Kronecker 对分裂域存在性给予了肯定的回答

例题 5.2 设 F 为一个域，求 $x^2+ax+b(a,b\in F)$ 的分裂域 E

解 若 x^2+ax+b 在 $F[x]$ 中可约，则 $E=F$。设 x^2+ax+b 不可约，则 x^2+ax+b 在 $F[x]/\langle x^2+ax+b\rangle$ 中有根 $\alpha_1=x+\langle x^2+ax+b\rangle$，则有分解

$$x^2+ax+b=(x-\alpha_1)(x-\alpha_2)$$

则 $E=F(\alpha_1,\alpha_2)=F(\alpha_1)$，这时 $[E:F]=2$

例题 5.3 求 $x^3-2\in\mathbb{Q}[x]$ 的分裂域 E

解 [解法一：] 已知 x^3-2 为 $\mathbb{Q}[x]$ 中不可约多项式。设 x^3-2 的一个根为 $\alpha_1=\sqrt[3]{2}$，则 $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$ 且 x^3-2 在 $\mathbb{Q}(\sqrt[3]{2})[x]$ 中有分解

$$x^3-2=(x-\alpha_1)(x^2+\alpha_1x+\alpha_1^2)$$

设 α_2 为 $x^2+\alpha_1x+{\alpha_1}^2$ 的一个根，设 $w=\dfrac{\alpha_2}{\alpha_1}$，则有

$$w^2+w+1={\alpha_2}^2{\alpha_1}^{-2}+\alpha_2{\alpha_1}^{-1}+1={\alpha_1}^{-2}({\alpha_2}^2+\alpha_1\alpha_2+{\alpha_1}^2)=0$$

即 w 为 x^2+x+1 的根，由 x^2+x+1 在 $\mathbb{Q}[x]$ 中不可约，则 $[\mathbb{Q}(w):\mathbb{Q}]=2$，则 $[E:\mathbb{Q}]=6$ 且 $E=\mathbb{Q}(\alpha_1,\alpha_2)=\mathbb{Q}(\sqrt[3]{2},w)$

解 [解法二] 令 $\omega=\dfrac{-1+\sqrt{-3}}{2}$，则 $\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2$ 为 $f(x)$ 三个复根，则 $\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2\right)$ 为 $f(x)$ 的分裂域。易得 $\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2)=\mathbb{Q}(\sqrt[3]{2},\omega)$

5.5 Galois 理论初步

定义 5.10 (Galois 群)

设 E 为 F 的扩张，称 E 到自身的 F-同态和 F-同构为 E 的 F-自同态和 F-自同构

所有 E 的 F-自同态的全体 $\mathrm{Hom}_F(E,E)$ 构成一个幺半群. 所有 E 的 F-自同构的全体构成一个群，称 F-自同构的全体为 E/F 的 Galois 群，记为 $\mathrm{Gal}(E/F)$ ♣

引理 5.2

设 E 为 F 的扩张，$\varphi\in\mathrm{Gal}(E/F)$，$R$ 为 $f(x)\in F[x]$ 在 E 中所有根的全体，则下列命题成立：

1) 同构 φ 为 R 的一个置换

2) 若 α 为 E/F 上代数元，则 $\varphi(\alpha)$ 也为代数元 ♡

证明 1) 设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0,\alpha\in R$，则 $f(\alpha)=0$。由 φ 为同构且 $\varphi(a_i)=a_i$，则有

$$\varphi(f(\alpha))=(\varphi(\alpha))^n+a_{n-1}(\varphi(\alpha))^{n-1}+\cdots+a_0=f(\varphi(\alpha))=0$$

则 $\varphi(\alpha)$ 也为 $f(x)$ 的根，则 $\varphi(R)\subseteq R$。由 φ 为双射且 R 有限，则为 R 的一个置换

2) 任意代数元 α 为其最小多项式 $\mathrm{Irr}(\alpha,F)$ 根，而 $\sigma(\alpha)$ 也为该多项式根，则为代数元

定理 5.9 (Dedekind 无关性定理)

设 E 为 F 的扩张且 $\sigma_1,\cdots,\sigma_n\in\mathrm{Gal}(E/F)$ 互不相同，则 $\sigma_1,\cdots,\sigma_n$ 作为 E 上的 F-线性变换为 E-线性无关的，即若 $x_1,\cdots,x_n\in E$ 满足 $x_1\sigma_1+\cdots+x_n\sigma_n=0$，则 $x_1=\cdots=x_n=0$ ♡

证明 归纳：当 $n=1$ 时结论显然成立；设 $n=k-1$ 时结论成立，即 $\mathrm{Gal}(E/F)$ 中任意 $k-1$ 个不同元必 E-线性无关，当 $n=k$ 时，若 $\sigma_1,\cdots,\sigma_k$ 为 E - 线性相关的，即存在 E 中不全为零的元 $a_1,\cdots,a_k$ 使得 $a_1\sigma_1+\cdots+a_k\sigma_k=0$，则对任意 $i,a_i\neq0$，否则 $\sigma_1,\cdots,\sigma_{i-1},\sigma_{i+1},\cdots,\sigma_k$ 线性相关，与归纳假设矛盾。不妨设 $a_k=1$（两端同乘 a_k^{-1} 即可），由 $\sigma_1\neq\sigma_k$，存在 $a\in E$ 使得 $\sigma_1(a)\neq\sigma_k(a)$。则对任意 $x\in E$ 有

$$a_1\sigma_1(x)+\cdots+a_{k-1}\sigma_{k-1}(x)+\sigma_k(x)=0 \tag{5.1}$$

又 $a_1\sigma_1(ax)+\cdots+\sigma_{k-1}(ax)+\sigma_k(ax)=0$，即

$$a_1\sigma_1(a)\sigma_1(x)+\cdots+a_{k-1}\sigma_{k-1}(a)\sigma_{k-1}(x)+\sigma_k(a)\sigma_k(x)=0 \tag{5.2}$$

则 (5.1) 乘以 $\sigma_k(a)$ 减去 (5.2) 可得

$$a_1\left(\sigma_k(a)-\sigma_1(a)\right)\sigma_1(x)+\cdots+a_{k-1}\left(\sigma_k(a)-\sigma_{k-1}(a)\right)\sigma_{k-1}(x)=0$$

由 x 的任意性，$a_1\neq0$ 及 $\sigma_k(a)-\sigma_1(a)\neq0$ 可得 $\sigma_1,\cdots,\sigma_{k-1}$ 为 E-线性相关的，与归纳假设矛盾，则定理成立

定理 5.10

设 $\sigma_1,\sigma_2,\cdots,\sigma_n\in\mathrm{Gal}(E/F)$ 互不相同，则 $[E:F]\geqslant n$ ♡

证明 反证：假设 $[E:F]=r<n,\alpha_1,\cdots,\alpha_r$ 为 E 的一组 F-基，考虑齐次线性方程组

$$\begin{cases}\sigma_1(\alpha_1)x_1+\cdots+\sigma_n(\alpha_1)x_n=0\\ \cdots\cdots\\ \sigma_1(\alpha_r)x_1+\cdots+\sigma_n(\alpha_r)x_n=0\end{cases}$$

由未知数个数大于方程个数，则该方程组有非零解，用 $x_1,\cdots,x_n$ 表示。对任意 $\alpha\in E$，存在 $a_1,\cdots,a_r\in F$ 使得 $\alpha=a_1\alpha_1+\cdots+a_r\alpha_r$。将上述方程组中第 i 个方程乘以 a_i 然后把所有方程相加得

$$\sum_{i=1}^{r}a_i\sigma_1(\alpha_i)x_1+\cdots+\sum_{i=1}^{r}a_i\sigma_n(\alpha_i)x_n=0$$

则 $x_1\sigma_1(\alpha)+\cdots+x_n\sigma_n(\alpha)=0$，而由 α 的任意性及 $x_1,\cdots,x_n$ 不全为零得 $\sigma_1,\cdots,\sigma_n$ 线性相关，矛盾，则 $[E:F]\geqslant n$

定理 5.11

设 G 为 $\mathrm{Aut}(E)$ 的有限子群，$F=E^G$，则 $|G|=[E:F]$ 且 $G=\mathrm{Gal}(E/F)$ ♡

证明 显然，G 为 $\mathrm{Gal}(E/F)$ 的子群，则 $|G|\leqslant|\mathrm{Gal}(E/F)|\leqslant[E:F]$。仅需证 $|G|\geqslant[E:F]$。设 $G=\{\sigma_1=\mathrm{id},\cdots,\sigma_n\}$，对任意 $\alpha_1,\cdots,\alpha_{n+1}\in E$ 考虑齐次线性方程组

$$\begin{cases}\sigma_1(\alpha_1)x_1+\cdots+\sigma_1(\alpha_{n+1})x_{n+1}=0\\ \cdots\cdots\\ \sigma_n(\alpha_1)x_1+\cdots+\sigma_n(\alpha_{n+1})x_{n+1}=0\end{cases}\tag{5.3}$$

则该方程组有非零解，设 $(b_1,b_2,\cdots,b_{n+1})$ 为所有非零解中包含零最多的解，不妨设 $b_1\neq0$。由 $\left(1,\dfrac{b_2}{b_1},\cdots,\dfrac{b_{n+1}}{b_1}\right)$ 也为解，则可假定 $b_1=1$，则对任意 $i=1,\cdots,n$ 有

$$\sigma_i(\alpha_1)+\sigma_i(\alpha_2)b_2+\cdots+\sigma_i(\alpha_{n+1})b_{n+1}=0\tag{5.4}$$

若存在 $b_i\notin F$，不妨设为 b_2，则 $(\exists\sigma\in G):\sigma(b_2)\neq b_2$。用 σ 作用在 (5.4) 上可得

$$(\sigma\sigma_i)(\alpha_1)+(\sigma\sigma_i)(\alpha_2)\sigma(b_2)+\cdots+(\sigma\sigma_i)(\alpha_{n+1})\sigma(b_{n+1})=0$$

则 $\sigma\sigma_i$ 等于某个 σ_k

注意到 $\sigma\sigma_1,\cdots,\sigma\sigma_n$ 为 G 中所有元，则上式表明 $(1,\sigma(b_2),\cdots,\sigma(b_{n+1}))$ 也为 (5.3) 的一个解，那么 $(0,b_2-\sigma(b_2),\cdots,b_{n+1}-\sigma(b_{n+1}))$ 为一个包含零更多的非零解，这与 $(b_1,b_2,\cdots,b_{n+1})$ 的取法矛盾，则 $b_2,\cdots,b_{n+1}\in F$。由 $\sigma_1=\mathrm{id}$，则有 $\alpha_1+b_2\alpha_2+\cdots+b_{n+1}\alpha_{n+1}=0$，即 $\alpha_1,\cdots,\alpha_{n+1}$ 线性相关。由此 $[E:F]\leqslant n\leqslant|G|$，又由定理 (5.10) 即得 $|G|=|\mathrm{Gal}(E/F)|=[E:F]$，则 $G=\mathrm{Gal}(E/F)$

定义 5.11 (不变子域)

设 G 为域 K 的自同构群 $\mathrm{Aut}K$ 的子群，易证 K 中子集

$$\mathrm{Inv}\,G=\{a\in K\mid g(a)=a,\forall g\in G\}$$

为 K 的子域，称该子域为 K 的 G 不变子域或 G 固定子域 ♣

定理 5.12

设 E/F 为有限扩张，则下列命题等价：

1) F 为 $\mathrm{Aut}(E)$ 的某个有限子群 G 的不变子域
2) F 为 $\mathrm{Gal}(E/F)$ 的不变子域
3) $[E:F]=|\mathrm{Gal}(E/F)|$ ♡

注 称满足上述等价条件的有限扩张 E/F 为**有限 Galois 扩张**

5.6 分圆域

5.7 有限域

有限域最早是由 Galois 提出的，因此也称 Galois 域

定义 5.12 (有限域)

称含有有限多个元素的域为有限域 ♣

性质 (域特征的素性)

一个有限域 K 的特征不为 0，其特征为一个素整数

证明 设有限域 $< K, +, \circ >$ 中的加法单位元为 0_+、乘法单位元为 $1_\circ$，用 $\times$ 表示算术乘法。对于正整数 z_1, z_2，有 $(z_1 1_\circ) \circ (z_2 1_\circ) = (z_1 \times z_2) \circ 1_\circ$

$$
\begin{aligned}
&\underbrace{(1_\circ + 1_\circ + 1_\circ + \cdots + 1_\circ)}_{z_1} \circ \underbrace{(1_\circ + 1_\circ + 1_\circ + \cdots + 1_\circ)}_{z_2} \\
&\underset{\text{域上乘法对加法的左分配律}}{=} \underbrace{\left(\underbrace{1_\circ + 1_\circ + \cdots + 1_\circ}_{z_1}\right) + \left(\underbrace{1_\circ + 1_\circ + \cdots + 1_\circ}_{z_1}\right) + \cdots + \left(\underbrace{1_\circ + 1_\circ + \cdots + 1_\circ}_{z_1}\right)}_{z_2} \\
&\underset{\text{域上加法的结合律}}{=} \underbrace{1_\circ + 1_\circ + \cdots + 1_\circ}_{z_1 \times z_2} = (z_1 \times z_2)\, 1_\circ
\end{aligned}
$$

反证：假设域 K 的特征不是素数，则 $z = z_1 \times z_2$

$$0 = z 1_\circ = (z_1 \times z_2)\, 1_\circ = (z_1 1_\circ) \cdot (z_2 1_\circ)$$

因为域是无零因子的交换幺环（域中没有零因子），所以 $z_1 1_\circ = 0$ 或 $z_2 1_\circ = 0$，这与域特征定义中的“最小值”矛盾（z_1、z_2 也是域 K 的特征但均小于 z）

5.8 论文：On the Casas-Alvero conjecture

5.9 论文：The Casas-Alvero conjecture in computational algebraic geometry

参考文献

[1] 孟道骥. 抽象代数：代数学基础 [M]. 北京: 科学出版社, 2010.

[2] 朱富海, 陈智奇. 高等代数与解析几何 [M]. 北京: 科学出版社,2018.9.

[3] 邓少强, 朱富海. 抽象代数 [M]. 北京: 科学出版社,2018.

[4] B.L. 范德瓦尔登. 代数学 [M]. 北京: 科学出版社,2009.5.

[5] А.И. 柯斯特利金. 代数学引论（第一卷）基础代数（第 2 版）[M]. 北京: 高等教育出版社, 2011.1.

[6] 戈德门特. 代数学教程 [M]. 北京: 高等教育出版社, 2013.

[7] 赵春来, 徐明耀. 抽象代数 [M]. 北京: 北京大学出版社,2008.