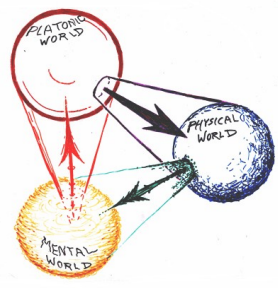
抽象代数讲义

作者：Hongxin Yang 南风

时间：January 28, 2026



目录

第 1 章 基础知识

Definition 1.1 (常见的群与子群)

设V为一n维线性空间

1.则$End(V)$为V上线性变换构成的群,其中$GL(V)$为可逆变换构成的群记为一般线性群

2.$SL(V)$为行列式为1的变换群

3.$O(V)$是正交变换群

4.$SO(V)$是第一类正交变换群

若有群G,我们记G上的自同态全体为$Hom(G)$此为幺半群其中幺元为id_G,并记G上自同构全体为$Aut(G)$为群

若有群$G, a \in G$,定义G上的共轭映射为 $\mathrm{Ad}_a : G \to G \quad g \mapsto aga^{-1}$称为由$a$诱导的共轭映射或者是由$a$诱导的内自同构

此时 $\mathrm{Ad}_a \in Aut(G)$ 同时我们记 $\mathrm{Inn}(G) = \{\mathrm{Ad}_a |\ a \in G\}$ 此时不难验证$Inn(G)$为$Aut(G)$的正规子群称之为内自同构群

把商群$Aut(G)/Inn(G)$为外自同构群记为$Out(G)$

Proposition 1.1 (同余的基础性质)

1. 同余是一个等价关系
2. 若$a \equiv b, c \equiv d$，则$a \pm c \equiv b \pm d (\mathrm{mod} n)$
3. 若$a \equiv b, c \equiv d$，则$ac \equiv bd (\mathrm{mod} n)$
4. 若$ac \equiv bc (\mathrm{mod} n), (c, n) = 1$，则$a \equiv b (\mathrm{mod} n)$
5. 若$a \equiv b (\mathrm{mod} n), m \mid n$，则$a \equiv b (\mathrm{mod} m)$
6. 若$a \equiv b (\mathrm{mod} n)$，则$(a, n) = (b, n)$
7. 若$a \equiv b (\mathrm{mod} n), d$为$a, b, n$的一个公因子，$a = da_1, b = db_1, n = dn_1$，则$a_1 \equiv b_1 (\mathrm{mod} n_1)$

Definition 1.2 (完全剩余代表系 1)

对于一个给定的模数n,全体整数按模n同余分成一些等价类,此时的等价类叫做整数模n的剩余类

含整数a的剩余类记作$\bar{a}$,剩余类$\bar{a}$的任一个元素叫做$\bar{a}$的一个代表

在每个剩余类中任取一个代表r_i，由这些代表组成的集合叫做整数模n的一个

整数模n的一个完全剩余代表系S也可以这样来刻画

1）每个整数和S中一个元素模n同余

2）S中元素两两互不同余

Proposition 1.2

设$(a, n) = 1$，则一次同余方程$ax \equiv b (\mathrm{mod} n)$有解而且只有一个解其中两个解相同 $\Longleftrightarrow x_1 \equiv x_2 (\mathrm{mod} n)$

Proof 由于$(a, n) = 1$，存在整数u, v使得$ua + vn = 1$

两边乘b得$uba + vbn = b$．令$ub = c$，则$ca \equiv b - vbn \equiv b (\mathrm{mod} n)$，即$x \equiv c$为其一解

其次，令c_1, c_2为任意两个解，于是$ac_1 \equiv b (\mathrm{mod} n) \quad ac_2 \equiv b (\mathrm{mod} n)$

相减得$a(c_1 - c_2) \equiv 0 (\mathrm{mod} n)$，由于$(a, n) = 1$，根据同余的性质4，有$c_1 \equiv c_2 (\mathrm{mod} n)$，即$c_1, c_2$为同一解

Note 考虑下列一次同余方程组 $\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \cdots\cdots\cdots\cdots \\ x \equiv b_r \pmod{n_r} \end{cases}$ 其中$n_1, n_2, \cdots, n_r$为大于1的整数，两两互素，$b_1, b_2, \cdots, b_r$是任意给定的整数

如果$x = c \in \mathbb{Z}$代入上方程组使得同余式同时都成立，则c叫做方程组的一个解

上方程组的两个解c_1和c_2看作是相同的当且仅当$c_1 \equiv c_2 \left(\mathrm{mod} \prod_{i=1}^{r} n_i\right)$

Proposition 1.3

下列一次同余方程组 $\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \cdots\cdots\cdots\cdots \\ x \equiv b_r \pmod{n_r} \end{cases}$

设一次同余方程组中大于1的整数$n_1, n_2, \cdots$，n_r两两互素，$b_1, b_2, \cdots, b_r$是任意给定的整数，则有解而且只有一解

Proof 记$N = n_1 \times \cdots \times n_r$　记$N_i = \dfrac{N}{n_i}$

此时$(N_i, n_i) = 1 \Longrightarrow$ 存在N_i^*与n_i^*使得$N_i N_i^* + n_i n_i^* = 1 \Longrightarrow N_i N_i^* \equiv 1 \pmod{n} \Longrightarrow N_i N_i^* b_i \equiv b_i \pmod{n}$

且注意到N_i中含有$n_j\ (j \neq i)$故$N_i N_i^* \equiv 0 \pmod{n}$

那么$x = \sum_{i=1}^{r} b_i N_i N_i^*$即为一个解

且若x_1与x_2满足方程组那么$n_i | x_1 - x_2 \Longrightarrow \prod_{i=1}^{r} n_i | x_1 - x_2$故$x_1$与$x_2$为同一解

Definition 1.3

设n为一正整数，在$0, 1, 2, \cdots, n-1$中与n互素的整数的个数记作$\varphi(n)$，叫做欧拉函数

由知道，$\varphi(n)$也就是那些模n的剩余类的个数，这些剩余类是由与n互素的整数组成的

从剩余类取出的代表组成的集合叫模$\boldsymbol{n}$的既约剩余代表系

一个既约剩余代表系T也可以这样来刻画

1）任一个与n互素的整数必与T中一个数模n同余

2）T中整数与n互素而且模n两两不同余

设$r_1, r_2, \cdots, r_N, N = \varphi(n)$，为模$n$的一个既约剩余代表系，$(a, n) = 1$，则$ar_1, ar_2, \cdots, ar_N$仍是模$n$的一个既约剩余代表系

据互素性质和同余性质4，$ar_1, ar_2, \cdots, ar_N$与n互素而且两两互不同余$\pmod{n}$，它们可以作为模n的既约剩余代表系的不同元素

而此代表系恰有N个元素，所以$ar_1, ar_2, \cdots, ar_N$是模n的既约剩余代表系.

Theorem 1.1 (欧拉函数性质)

1.设p为素数，则$\varphi(p^m) = p^m\left(1 - \dfrac{1}{p}\right)$，其中$m \geqslant 1$

2.设$n = n_1 n_2, (n_1, n_2) = 1, n_i \geqslant 1$，则$\varphi(n) = \varphi(n_1)\varphi(n_2)$

3.设$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, p_1, p_2, \cdots, p_r$为不同素数，$e_i \geqslant 1$，则$\varphi(n) = n\left(1 - \dfrac{1}{p_1}\right)\left(1 - \dfrac{1}{p_2}\right)\cdots\left(1 - \dfrac{1}{p_r}\right)$

Proof 1.因为在$S = \{0, 1, 2, \cdots, p^m - 1\}$中除去$p$的倍数，剩下的都与$p$互素，而$S$中$p$的倍数恰好有$\dfrac{p^m}{p}$个

因此S中与p互素的整数的个数为$p^m - p^{m-1}$

2.$\varphi(n_i)$简记作$N_i, i = 1, 2$. 设$r_1, \cdots, \mathrm{r}_{N_1}$和$s_1, \cdots, s_{N_2}$分别为模$n_1$和模$n_2$的既约剩余代表系

根据孙子定理,存在整数$t_{ij}\ (i=1,\cdots,N_1, j=1,\cdots,N_2)$使得$t_{ij}\equiv r_i\ (\mathrm{mod}n_1)\quad t_{ij}\equiv s_j\ (\mathrm{mod}n_2)$

我们来证明$t_{ij}\ (i=1,\cdots,N_1, j=1,\cdots,N_2)$为模$n_1n_2$的一个既约剩余代表系

首先,由于$(r_i,n_1)=1$,有$\left(t_{ij},n_1\right)=1$,由于$\left(s_j,n_2\right)=1$,有$\left(t_{ij},n_2\right)=1$因而$\left(t_{ij},n_1n_2\right)=1$

其次t_{ij}互不同余.假若$t_{ij}\equiv t_{kl}\ (\mathrm{mod}n_1n_2)$，一方面有$t_{ij}\equiv t_{kl}\ (\mathrm{mod}n_1)$，它化为$r_i\equiv r_k\ (\mathrm{mod}n_1)$，从而$i=k$

另一方面有$t_{ij}\equiv t_{kl}\ (\mathrm{mod}n_2)$，它化为$s_j\equiv s_l\ (\mathrm{mod}n_2)$，从而$j=l$

所以t_{ij}互不同余$(\mathrm{mod}n_1n_2)$

最后设a为任一与n互素的整数，根据r_i和s_j的定义，存在r_i和s_j，使得$a\equiv r_i\ (\mathrm{mod}n_1), a\equiv s_j\ (\mathrm{mod}n_2)$

于是根据孙子定理有$a\equiv t_{ij}(\mathrm{mod}n)$，所以$t_{ij}\ (i=1,\cdots,N_1, j=1,\cdots,N_2)$是模$n$的一个既约剩余代表系

这证明了$\varphi(n)=\varphi\left(n_1\right)\varphi\left(n_2\right)$

第 2 章 群论 I-Group Theory

2.1 群的基本概念与性质

2.1.1 半群

Definition 2.1 (代数运算)

设A,B,D是三个集合，一个由$A\times B$到D的映射$\circ$称为$A\times B$到D的一个代数运算.

当$A=B=D$时，则称$A\times A$到A的代数运算为A的代数运算.

Definition 2.2 (集合的分划)

$S=\{A_a \mid A_a\in 2^A, A_a\neq\varnothing, \alpha\in I, I \text{ 为某个指标集}\}$

(1) $\bigcup\limits_{a\in 1} A_a=A$;

(2)当$A_a\neq A_\beta$时，$A_a\cap A_\beta=\varnothing$.

其中每一个A_a称为S的一个分块(类)

Proposition 2.1 (等价类与性质)

设$\sim$是集合A上的等价关系

令$\bar{a}=\{x \mid x\sim a, x\in A\}$为$\bar{a}$的等价类.

1.$a\in\bar{a}$

2.$b,c\in a. \Rightarrow b\sim c$

3.$b\in\bar{a}, x\sim b\Rightarrow x\sim\bar{a}$

4.$a\sim b\Leftrightarrow\bar{a}=\bar{b}$

Theorem 2.1

集合A的一个等价关系E可以决定A的一个分类S_E;反之，集合A的一个分类S也可以决定A的一个等价关系E_s.

Proof 1.设E为集合A上的一等价关系，构造子集族为$S_E=\{\bar{a} \mid a\in A\}$

显然$\bigcup\limits_{a\in A}\bar{a}=A$此外，我们要证明若$\bar{a}\neq\bar{b}$会有$\bar{a}\cap\bar{b}=\varnothing$

我们考虑逆否形式若$\bar{a}\cap\bar{b}\neq\varnothing$那么存在$c$; $st. a\sim c, b\sim c\Rightarrow a\sim b$那么根据性质$\bar{a}=\bar{b}$

2.另外，设$S=\{A_a\}$是A的一个分类，由S规定A的一个关系$E_S: aE_Sb\Leftrightarrow a,b$属于同一个子集$A_a$.

(1)$\forall a\in A$，因为$\bigcup\limits_{a\in !} A_u=A$，即$a$必落在某一个子集$A_a$中，所以，$aE_sa$;

(2)若aE_sb，即a,b同属于某一个子集A_a，则b,a也同属于这个子集，即有bE_sa;

(3)若aE_sb, bE_sc，即a,b同属于某一个子集A_a，b,c也同属于某一个子集A_β，因为两个子集A_α与A_β有公共元素c，即$A_\alpha\cap A_\beta\neq\varnothing$

根据分类的条件有$A_\alpha=A_\beta$，所以，a与c属于同一个子集A_a，即aE_sc.从而证得E_s是A的一个等价关系.

Proposition 2.2 (广义结合律)

令$x_1,\cdots,x_n,y_1,\cdots,y_m\in S$，则$x_1\cdot x_2\cdots x_n\cdot y_1\cdot y_2\cdots y_m=(x_1\cdot x_2\cdots x_n)\cdot(y_1\cdot y_2\cdots y_m)$

Proof 对m做数学归纳。当$m=1$时，由定义直接得到。

接下来，假设$x_1\cdot x_2\cdots x_n\cdot y_1\cdot y_2\cdots y_k=(x_1\cdot x_2\cdots x_n)\cdot(y_1\cdot y_2\cdots y_k)$则我们有

$$
\begin{aligned}
&x_1\cdot x_2\cdots x_n\cdot y_1\cdot y_2\cdots y_{k+1}\\
=&((x_1\cdot x_2\cdots x_n)\cdot(y_1\cdot y_2\cdots y_k))\cdot y_{k+1}\\
=&(x_1\cdot x_2\cdots x_n)\cdot((y_1\cdot y_2\cdots y_k)\cdot y_{k+1})\\
=&(x_1\cdot x_2\cdots x_n)\cdot(y_1\cdot y_2\cdots y_{k+1})
\end{aligned}
$$

Definition 2.3 (半群)

设S为一非空集合，其上有

1.代数运算$\circ$

2.$\circ$满足三元结合律即$(a\circ b)\circ c=a\circ(b\circ c)$

Definition 2.4 (单位元)

若在$(S,\circ)$半群上存在e_l元使得$\forall a\in S$，有$e_la=a$则称e_l为左单位元

同理可定义右单位元

若存在e元使得$\forall a\in S$，有$ea=ae=a$则称e为单位元

Theorem 2.2 (单位元的唯一性)

若一个半群上同时存在左单位元与右单位元那么二者相同，且单位元唯一

Proof 由题有$\forall a,\quad e_1a=a.\quad ae_2=a$

那么$e_1=e_1e_2=e_2$重复利用左右性质即可

设e为单位元，下证唯一性，若还有一个e^*为单位元那么$e=e^*e=e^*$同理可得

Example 2.1 半群中左右单位元单独存在的例子

设$S=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix}\mid a,b\in R\right\}$，证明$S$关于矩阵的乘法作成半群，且$S$有左单位元，但没有右单位元。

若考虑$S_1=\left\{\begin{pmatrix}a&0\\b&0\end{pmatrix}\mid a,b\in R\right\}$，其有右单位元但无左单位元

Definition 2.5 (左右逆元)

设$(S,\circ)$为半群且有单位元e

若对于$a\in S,\exists x\in S$都有$xa=e$那么称x为a的左逆元，a为左可逆

同理可定义右逆元和右可逆

若对于$a\in S,\exists x\in S$都有$xa=ax=e$那么称x为a的逆元

Theorem 2.3 (逆元唯一性)

若半群$(S,\circ)$上存在单位元e，若对于$a\in S$，同时存在其左逆元和右逆元那么二者相同，且逆元唯一

Proof 由题设$x_1a=e\quad ax_2=e$那么$x_1=x_1e=x_1(ax_2)=(x_1a)x_2=ex_2=x_2$

设$xa=ax=e$若还有$x^*a=ax^*=e$那么$x=xe=x(ax^*)=(xa)x^*=ex^*=x^*$

Definition 2.6 (幺半群)

若 $(S,\circ)$ 为半群且还有单位元 (幺元) 则称为幺半群

1.代数运算 $\circ$

2. $\circ$ 满足三元结合律

3.存在单位元

Definition 2.7 (交换幺半群)

我们说 $(S,*)$是一个交换幺半群, 当其是一个幺半群, 且该运算满足交换律, 即$\forall x,y\in S, x*y=y*x$

Definition 2.8 (子幺半群)

令 $(S,\cdot)$是一个幺半群, 若$T\subset S$, 我们说 $(T,\cdot)$是 $(S,\cdot)$的一个子幺半群, 若$e\in T$, 且T在乘法下封闭, 即

1.$e\in T$　　2.$\forall x,y\in T, x*y\in T$

Definition 2.9 (子幺半群同态)

假设 $(S,\cdot),(T,*)$是两个幺半群, 且$f:S\to T$是一个映射

我们称f是一个幺半群同态, 当f保持了乘法运算, 且把单位元映到了单位元。

1.$\forall x,y\in S, f(x\cdot y)=f(x)*f(y)$

2.$f(e)=e'$

其中, e和e'分别是 $(S,\cdot)$和 $(T,*)$的单位元。

Definition 2.10 (生成子幺半群)

假设 $(S,\cdot)$是一个幺半群, 而$A\subset S$是一个子集。我们定义由A生成的子幺半群, 记作$\langle A\rangle$, 是指S中所有包含了A的子幺半群的交集。

$\langle A\rangle=\bigcap\{T\subset S: T\supset A, T \text{ 是子幺半群}\}$

假设 $(S,\cdot)$是一个幺半群, 而$A\subset S$是一个子集。则$\langle A\rangle$也是一个子幺半群。因此, 这是包含了A的最小的子幺半群。

Definition 2.11 (子幺半群同构)

假设 $(S,\cdot),(T,*)$是两个幺半群, 且$f:S\to T$是一个映射, 我们称f是一个幺半群同构, 当f是一个双射, 且是一个同态。

1.f是双射

2.$\forall x,y\in S, f(x\cdot y)=f(x)*f(y)$

3.$f(e)=e'$

其中, e和e'分别是 $(S,\cdot)$和 $(T,*)$的单位元。

Proposition 2.3

若$f:(S,\cdot)\to(T,*)$是一个幺半群同构, 则$f^{-1}:T\to S$是一个幺半群同态。因此, f^{-1}也是个幺半群同构。

Proof 令$x',y'\in T$, 我们只需证明$f^{-1}(x'*y')=f^{-1}(x')\cdot f^{-1}(y')$。

为了方便起见, 根据f是一个双射, 我们可以令$x=f^{-1}(x'), y=f^{-1}(y')$。

我们只需证明$f^{-1}(x'*y')=x\cdot y$。而由于f是幺半群同态, 所以$f(x\cdot y)=f(x)*f(y)=x'*y'$。

反过来说, $f^{-1}(x'*y')=x\cdot y=f^{-1}(x')\cdot f^{-1}(y')$。这就证明了这个命题。

Example 2.2 幺半群元素仅存在左逆元不存在右逆元 存在幺半群S及$a \in S$, a存在左逆元, 但不存在右逆元.
所有3×3的列满秩矩阵即可，幺元为单位阵关键利用满秩分解

2.1.2 群

Definition 2.12 (群的定义)

令 $(G,\cdot)$是一个么半群, 我们说它是一个群, 当G中所有元素都是可逆的。
换言之, 若.是G上的一个二元运算, 则我们称 $(G,\cdot)$是个群, 或G对构成群
当这个运算满足结合律, 存在单位元, 且每个元素具有逆元。再进一步展开来说, 同样等价地
则我们称 $(G,\cdot)$是个群, 当
(1) 是G上的一个二元运算,
(2) $\forall x,y,z\in G, x\cdot(y\cdot z)=(x\cdot y)\cdot z$
(3) $\exists e\in G,\forall x\in G, x\cdot e=e\cdot x=x$
(4) $\forall x\in G,\exists y\in G, x\cdot y=y\cdot x=e$

Theorem 2.4 (么半群到群的构造)

令 $(S,\cdot)$是一个么半群, 令G是其所有可逆元素构成的子集, 则 $(G,\cdot)$是个群。

Proof 首先结合律完全继承自S, 不需要证明。而单位元是可逆的, 因此$e\in G$。
剩下要证明G中每个元素都有 (G中的) 逆元, 而这几乎是显然的。
假设$x\in G$, 则x是可逆元素, 我们取$y\in S$, 使得$x\cdot y=y\cdot x=e$(这里要注意我们只能首先保证y在全集S中)。
接下来我们要证明$y\in G$, 即y可逆, 而这是显然的, 因为x正是它的逆。所以$y\in G$。这样, 就证明了 $(G,\cdot)$是个群。

Definition 2.13 (一般线性群)

我们对于那些$n*n$可逆实矩阵构成的乘法群, 称为 (实数上的)n阶一般线性群, 记作 $(GL(n,\mathbb{R}),\cdot)$
由于一个矩阵可逆当且仅当其行列式不为零, 因此$GL(n,\mathbb{R})=\{A\in M(n,\mathbb{R}):\det(A)\neq 0\}$

Theorem 2.5 (定义 check 群的弱化版本)

(1) 如果半群G有一个左单位元e, 并且对于$\forall a\in G$, 存在左逆元$a^{-1}\in G$, 使得$a^{-1}a=e$, 则G是一个群.
按群的定义, 只要证明a的左逆元a^{-1}也是右逆元, 左单位元e也是右单位元即可.
(2) 如果半群G有一个右单位元e, 并且对于$\forall a\in G$, 存在右逆元$a^{-1}\in G$, 使得$aa^{-1}=e$, 则G是一个群.

Proof $\forall a\in G$, 由条件知, 有左逆元$a^{-1}\in G$, 使得$a^{-1}a=e$, 而对于a^{-1}当然也在G中存在左逆元a', 使得$a'a^{-1}=e$, 那么

$$aa^{-1}=e\left(aa^{-1}\right)=\left(a'a^{-1}\right)\left(aa^{-1}\right)$$

$$=a'\left(a^{-1}a\right)a^{-1}=a'ea^{-1}=a'a^{-1}=e,$$

所以, a的左逆元a^{-1}也是a的右逆元, 即a在G中有逆元a^{-1}.又由于$ae=a\left(a^{-1}a\right)=\left(aa^{-1}\right)a=ea=a$, 知$e$是$G$的单位元.

Corollary 2.1

如果G是半群, 那么G是群的 $\Leftrightarrow \forall a,b\in G$, 方程$ax=b$和$ya=b$在$G$中有解.

Proof 必要性.因为G是群, 则$a\in G$在G中有逆元a^{-1}, 则$a^{-1}b, ba^{-1}\in G$, 将它们分别代入方程$ax:=b$和$ya=b$, 有

$$a\left(a^{-1}b\right)=\left(aa^{-1}\right)b=eb=b,$$

$$\left(ba^{-1}\right)a=b\left(a^{-1}a\right)=be=b,$$

即$a^{-1}b, ba^{-1}$分别为方程$ax=b$和$ya=b$的解.

充分性.先证G有左单位元e.因为G是非空集合,取定$b \in G$,则方涅$yb = b$在G中有解e,即存在G中的元事e,使得$eb = b$.
要证e就是G的左单位元,则需证:对于$\forall a \in G$,有$ea = a$."
$\forall a \in G, b \in G$,方程$bx = a$在G中有解c,即$bc = a$,于是$ea = e(bx) = (eb)c = bx = a$,得$e$是$G$的一个左单位元.
再者,任取$a \in G$,方程$ya = e$在G中有解a',即$a'a = e$,得a'是a的一个左逆元.
从而得G中的每一个元a都有左逆元.再根据上个命题,可知G是一个群.

Theorem 2.6

设$(G, \cdot)$是有限半群,如果在G中满足消去律,则$(G, \cdot)$作成群。

Proof 由命题知,只须证明$\forall a, b \in G$,方程$ax = b, ya = b$在G中有解即可.
设$G = \{a_1, a_2, \cdots, a_n\}$,对于$\forall a, b \in G$,我们作集合$G$的子集$G' = \{aa_1, aa_2, \cdots, aa_n\} \subseteq G$,当$i \neq j$时,有$aa_i \neq aa_j$,
不然的话,由消去律知$a_i = a_j$,与假设矛盾.
因此,G'中有n个不同的元素,从而得$G = G'$.这样以上方程中的元素$b \in G = G'$,也就是说,存在k,使得$b = aa_k$.
则a_k是方程$ax = b$的解.同样可证$ya = b$在G中有解.

Example 2.3 非有限半群满足消去律未必构成群例子

此定理若去掉有限这个条件,则结论不成立.例如S = {所有非零整数}。
对于普通乘法运算来说是一个满足消去律的半群,但S关于数的乘法不构成群.

Example 2.4 半群中存在左幺元且每个元有右逆元不一定是群

首先左单位元的定义不要求其唯一随便取一个集合
在上面定义二元运算满足$x^*y = y$，那么满足结合律，所有元素x都是左单位元，对所有元素x，所有元素y都是右逆。
那么我们就构造$\{a, b\}$验证即可发现$\{a, b\}$并没有一个严格意义上的单位元

2.2 群同态与同构与子群

Definition 2.14 (群同态)

令 $(G,\cdot),(G',*)$ 是两个群, 且 $f:G\to G'$ 是一个映射

我们称 f 是一个群同态, 当其保持了乘法运算, 即 $\forall x,y\in G, f(x\cdot y)=f(x)*f(y)$

Proposition 2.4 (群同态对逆元与单位元保持)

若 $f:(G,\cdot)\to(G',*)$ 是一个群同态, 则

1. $f(e)=e'$
2. $f\left(x^{-1}\right)=f(x)^{-1}$。

Proof (1)由 $e'f(e)=f(e)=f(ee)=f(e)f(e)$, 因为 G' 是群, 两边右消去 $f(e)$ 得 $f(e)=e'$;

(2)因为 $f\left(a^{-1}\right)f(a)=f\left(a^{-1}a\right)=f(e)=e'$, 所以 $[f(a)]^{-1}=f\left(a^{-1}\right)$.

Remark 我们特别要指出这跟我们之前定义的幺半群同态不太一样, 其实观察证明过程就知道, 我们有一个重要的操作是消去. 这在一般幺半群中并不具备

Example 2.5 幺半群同态的局限例子 设 $A=\{e,a\}$ $B=\{1,x,y\}$

$\cdot$	e	a
e	e	a
a	a	a

$\cdot$	1	x	y
1	1	x	y
x	x	x	y
y	y	y	y

容易证明 A,B 关于各自的乘法运算均作成有单位元的半群, 其单位元分别为 e 和 1.

令 $f:A\to B, e\mapsto x, a\mapsto y$, 则 f 是一个半群的同态映射, 但 $f(e)=x\neq 1$.

Definition 2.15 (子群与平凡子群定义)

设 H 是群 G 的一个非空子集, 如果 H 关于群 G 的代数运算也作成一个群, 则我们称 H 是 G 的一个子群, 记为 $H<G$.

设 G 是任意一个群, 则 G 必有 G 本身, G 的单位元 e 构成的单元素子集 $\{e\}$ 作为其子群.

这两个子群称为群 G 的平凡子群, 除平凡子群外的其他子群称为真子群.

Proposition 2.5 (子群保持单位元与逆元, 子群的必要条件)

设 H 是群 G 的一个子群, 则

1. H 的单位元 e_H 就是 G 的单位元 e_G
2. $a\in H,;a$ 在 H 中的逆元 a' 就是 a 在 G 中的逆元 a^{-1}.

Proof 由于 H 中的代数运算与 G 中的代数运算是一致的, 故有 $e_He_G=e_H=e_He_H$, 两边同时左消去 e_H, 即有 $e_G=e_H$;

同样, 由 $a'a=e_H=e_G=a^{-1}a$, 两边同时右消去 a 得 $a'=a^{-1}$.

Theorem 2.7 (子群的判定定理)

设G是一个群, 那么G的非空子集H作成G的子群的充分必要条件是：

(1)$\forall a,b\in H$, 有$ab\in H$ 且 $\forall a\in H$, 有$a^{-1}\in H$. (保持运算, 保持逆元)

(2)$\forall a,b\in H$, 有$ab^{-1}\in H$

Proof (1) 先证充分性.由 (1)知H关于G的代数运算是封闭的, 由于结合律在G中成立, 在H中也自然成立;

由于$H\neq\varnothing$, 取$a\in H$, 由后半句话知$a^{-1}\in H$, 故$a^{-1}a=e_G\in H$, 即H中包含G的单位元e_G, 而这个单位元e_G自然也是H的单位元e_H;

由于H中的任意一个元素a在G中的逆元a^{-1}也在H中, 即$a^{-1}a=e_G=e_H\in H$, 得a在H中存在逆元a^{-1}.

所以, H关于G的代数运算作成群.

再证必要性.假如H是一个群, (1)显然成立; 至于后半句, 可由前文性质知.

(2) 证明只要证明条件 (2) 与 (1)与等价即可.

由 (1)容易得到 (2).反之, $\forall a\in H$, 由于$aa^{-1}=e\in H$, 得$ea^{-1}=a^{-1}\in H$, 即 (1) 后半段成立;

$\forall a,b\in H$, 由 (2)知$b^{-1}\in H$, 故$ab=a\left(b^{-1}\right)^{-1}\in H$,

Definition 2.16 (群同态的核与像, 单满同态, 自同态)

1.令$f:(G,\cdot)\to(G',*)$是一个群同态, 则我们定义f的核与像, 记作 $\ker(f)$与 $\mathrm{im}(f)$, 分别为

$\mathrm{Ker}(f)=\{x\in G:f(x)=e'\}\subset G$

$\mathrm{Im}(f)=\{y\in G':\exists x\in G,y=f(x)\}=\{f(x):x\in G\}]\subset G'$

2.令$f:(G,\cdot)\to(G',*)$是一个群同态, 我们称f是一个满同态当f是满的, 称f是一个单同态当f是单的

3.群G的所有自同态构成一么半群记为$Hom\,(G)$

Theorem 2.8 (核与像为子群定理)

令$f:(G,\cdot)\to(G',*)$是一个群同态, 则核是定义域的子群, 像是陪域的子群, 即

1.$\mathrm{Ker}(f)<G$

2.$\mathrm{Im}\,(f)<G'$

Proof 先证明第一个子群关系。我们利用$f(e)=e'$来说明$e\in\ker(f)$

接着, 假设$x,y\in\ker(f)$, 只需证明$xy^{-1}\in\ker(f)$

利用同态的性质, $f\left(xy^{-1}\right)=f(x)f(y)^{-1}=e'e'^{-1}=e'$, 这就证明了$xy^{-1}\in\ker(f)$

第一个子群关系得证。

再证明第二个子群关系。同样由于$f(e)=e'$, 我们有$e'\in\mathrm{im}(f)$。

接着, 假设$y=f(x),y'=f\left(x'\right)\in\mathrm{im}(f)$, 只需证明$yy'^{-1}\in\mathrm{im}(f)$。

同样利用同态的性质, $yy'^{-1}=f(x)f\left(x'\right)^{-1}=f\left(xx'^{-1}\right)\in\mathrm{im}(f)f$。

第二个子群关系也得证。这样我们就证完了整个命题。

Corollary 2.2

设$f:G\to G'$为群同态,

1.若$H<G$; 那么$f\,(H)<G'$

2.若$H'<G'$; 那么$f^{-1}\,(H')<G$

Theorem 2.9 (单同态与满同态的判别法)

设f是群G到G'的同态映射,e是G的单位元,则

(1)f是单同态当且仅当 $\mathrm{Ker}f = \{e\}$

(2)f是满同态当且仅当 $\mathrm{Im}f = G'$.

Proof 满同态判定十分简单我们略去不说明

假设f是单的,那么因为$f(e) = e'$,因此若$f(x) = e'$,则利用单射的性质我们一定有$x = e$,这就证明了核是平凡的 (这个方向是显然的)

另一个方向不那么显然。我们假设 $\ker(f) = \{e'\}$。假设$x, x' \in G$,使得$f(x) = f(x')$,我们只须证明$x = x'$

在这里,我们同时右乘$f(x')^{-1}$,得到$f(x)f\left(x'^{-1}\right) = f\left(xx'^{-1}\right) = e'$。

而因为核是平凡的,所以必须有$xx'^{-1} = e$。接下来同时右乘x',我们就得到$x = x'$。这就证明了这个命题。

Definition 2.17 (群同构)

令$f : (G, \cdot) \to (G', *)$是一个映射,我们称$f$是一个群同构,当$f$既是一个双射,又是一个群同态

群 G 的所有自同构构成一个群记为 Aut(G)

Proposition 2.6

若$f : (G, \cdot) \to (G, *)$是一个群同构,则$f^{-1}$也是群同构

Proof 因为f^{-1}也是双射,所以我们只须证明f^{-1}是群同态

令$x', y' \in G'$,假设$x' = f(x), y' = f(y)$。则$x' * y' = f(x \cdot y)$,故$f^{-1}(x' * y') = x \cdot y = f^{-1}(x) \cdot f^{-1}(y)$。这就完成了证明。

Definition 2.18 (群的直积)

令$(G, \cdot_1), (G', \cdot_2)$是两个群,我们构造它们的直积,不妨记$(G \times G', *)$

对于$(x, y), (x', y') \in G \times G'$,我们定义逐坐标的乘积,为$(x, y) * (x', y') = (x \cdot r_1 x', y \cdot 2y')$

Proposition 2.7

若$(G, \cdot_1), (G', \cdot\cdot_2)$是两个群,则它们的直积$(G \times G', *)$还是一个群

Proof 封闭性:因为G在$\cdot_1$下封闭,G'在$\cdot_2$下封闭,而$G \times G'$的元素乘积是逐坐标定义的,则$G \times G'$在$* = (\cdot\cdot_1, \cdot_2)$下也是封闭的

结合律:同样,逐坐标有结合律,故整体也有结合律。单位元:不难想象,(e, e')是直积的

单位元:对于任意$(x, y) \in G \times G'$,我们有$(x, y) * (e, e') = (x \cdot_1 e, y \cdot_2 e') = (x, y)$,另一边也是同理,这就证明了$(e, e')$是直积的单位元

逆元:同样不难想象,对于任意$(x, y) \in G \times G'$,$\left(x^{-1}, y^{-1}\right)$是$(x, y)$的逆元。证明是类似的,这里省略。

Definition 2.19

令$(G_{i,i})_{i \in I}$是一族群,其中I是一个指标集。我们定义它们的直积为$\left(\prod_{i \in I} G_i, *\right)$,同样通过逐点的乘积

对于$(x_i)_{i \in I}, (y_i)_{i \in I} \in \prod_{i \in I} G_i$,我们定义$(x_i)_{i \in I} * (y_i)_{i \in I} = (x_i \ _i \ y_i)_{i \in I}$

Remark 不难将上述直积的性质推广

Proposition 2.8

若$(G_i, ^*)_{i \in I}$是一族群,$j \in I$是任意指标,则投影映射$p_j : \prod_{i \in I} G_i \to G_j$是个群同态。

Proposition 2.9 (子群在 (可以推广到任意多个) 交运算下还是子群)

若有群G和子群：$H<G, K<G$那么$H\cap K<G$

Exercise 2.1 设S是群G的任意非空子集, 证明：$H_S=\{x\in G\mid xs=\mathrm{sx}, \forall s\in S\}$是$G$的子群

Proof 由于单位元e与G中的任意元素都可交换, 所以, $e\in H_S$, H_S非空

$\forall a,b\in H_S$, 即对于$\forall s\in S$有$as=sa, bs=sb$, 从而 $(ab)s=a(bs)=a(sb)=(as)b=(sa)b=s(ab)$,

再由$as=sa$得$a^{-1}s=sa^{-1}$, 所以, $ab, a^{-1}\in H_S$。证得H_S是G的一个子群。

Example 2.6 子群的积未必是子群的例子

按照上述的HK的集合的构造

若有群G且有子群$H<G; K<G$但是未必有$HK<G$

Proof 例如取$G=S_3$ $A=\{(1),(12)\}$ $B=\{(1),(13)\}$ $AB=\{(1),(13)(12),(132)\}$不是子群

Theorem 2.10 (乘积为子群的充要条件)

G为群，$H<G, K<G$

那么$HK<G\iff HK=KH$进一步有$HK<G\iff HK=KH\iff HK$与KH都是G子群

Proof 一方面若$HK=KH$那么$HK<G$是显然的

另一方面若$HK<G$那么$\forall h_1,k_1,h_2,k_2$都有$h_1k_1h_2k_2=h_3k_3\Longrightarrow k_1h_2=h_1^{-1}h_2k_3k_2^{-1}\in HK$

于是$KH\subseteq HK$

再者对于$\forall h,k$ $(hk)^{-1}\in HK\Longrightarrow (hk)^{-1}=h^*k^*\Longrightarrow hk=(k^*)^{-1}(h^*)^{-1}\in KH$

于是$HK\subseteq KH$

所以$HK=KH$

同理可证$HK<G\iff HK=KH$综合就有$HK<G\iff HK=KH\iff HK$与KH都是G子

Example 2.7 子群的并未必是子群例子

群G的两个子群H_1, H_2的并$H_1\cup H_2$未必是G的子群

Proof

我们给出两个反例。

取$G=(\mathbf{Z},+), H_1=2\mathbf{Z}, H_2=3\mathbf{Z}$, 则$H_1\cup H_2$中的元素或为偶数, 或为3的倍数

因为$2\in H_1\subseteq H_1\cup H_2$, $3\in H_2\subseteq H_1\cup H_2$, 但$2+3=5\notin H_1\cup H_2$, 因为5既不是偶数, 也不是3的倍数

由此可以看出$H_1\cup H_2$关于加法运算不封闭, 所以它不是G的子群。

$G=A_4$其二阶子群其中有$H=\{(1),(12)(34)\}$与$K=\{(1),(13)(24)\}$但是$H\cup K=\{(1),(12)(34),(13)(24)\}$

但是$H\cup K$不是子群 (可见陪集与拉格朗日定理一节的命题) 简单来说就是$|H\cup K|$为三阶群为循环群但是其中元素都不是循环生成元

故$H\cup K$不是子群

Theorem 2.11 (子群的并为子群的充要条件)

G是一个群，$A<G, B<G$

那么$A\cup B$是G的子群$\iff A<B$或$B<A$

Proof 一方面：若$A < B$或$B < A$。不妨设$A < B$那么$A \cup B = B < G$

另一方面：若$A \cup B$是子群不妨记为C。由子群承接性那么A就是C的子群，B是C的子群

两个子群的并是一子群说明A或B一定不是真子群也就是说当中必有一个就为$C = A \cup B$

那么就有$A < B$或$B < A$

2.3 有限群

Definition 2.20 (阶的定义)

对于群G中的一个元来a, 如果存在正整数m, 使得$a^m = e$成立,
而且m是使上述等式成立的最小正整数, 则称m为元a的阶, 记为$|a| = m$;
如果这样的整数m不存在, 则称元a的阶为无限。

只含有有限个元素的群叫做有限群, 否则叫做无限群.有限群G所含的元来个数叫做群的阶, 记为$|G|$.
对于无限群的阶有时找们也记为$|G|$.

Theorem 2.12

设群G中的元a的阶为m, 那么$a^n = e$.当且仅当$m \mid n$.

Proof 若$a^n = e$, 令$n = mq + r$, $(q, r \in \mathrm{Z}, 0 \leqslant r < m)$于是有$e = a^n = a^{n+r} = (a^m)^q\, a^r = a^r$, 由于$a$的阶$m$的最小性, 得$r = 0$.即$m \mid n$.
反之.若$m \mid n$, 可设$n = mk$, 于是$a^n = a^{mk} = (a^m)^k == e$.

Corollary 2.3

由此可得判断m是否是元素a的阶的一个等价条件, 即推论正整数m是元素a的阶的方分必要条件是
(1)$a^m = e$;
(2)如果$a^n = e$, 则$m \mid n$.e的最小正整数.

Theorem 2.13

有限群中的每一个元的阶都有限

Proof 设G是一个有限群, 且$|G| = n, \forall a \in G$, 则有G中元素的序列$a, a^2, a^3, \cdots, a^{\pi+1} \in G$,
由于G中的元素只有n个.故必有两个元素相同, 设$a^i = a'$, 且$i > j$, 于是存在正整数$k = i - j$, 使$a^k = e$, 故a的阶有限.
进一步可知, 元素a的阶不超过群G的阶.

Example 2.8 元素阶都有限但群阶无限列子

这个定理的逆命题不成立, 即存在这样的无限群G, 其中的每一个元素的阶都有限.
例如, 在复数域C中所有n次单位根组成的集合$U = \{a \in \mathrm{C} \mid a^n = 1, n \text{ 为任意正整数}\}$,
可知U关于数的乘法作成一个群, 且是无限群, 但对每一个$a \in U$, 都存在一个$n \in \mathrm{N}$, 使得$a^n = 1$, 即a的阶有限.

Proposition 2.10

设S是一个有单位元的半群, G_S是S中所有可逆元组成的集合
G_S关于S的代数运算作成一个群。特别当S为群时, $G_S = S$

Proof 因为S中的单位元e_S是个可逆元, 所以G_S不是空集。
$\forall a, b \in G_S$, 因为 $(ab)\left(b^{-1}a^{-1}\right) = \left(b^{-1}a^{-1}\right)(ab) = e_S$, 得$ab \in G_S$, 得$G_S$关于$S$的代数运算是封闭的。
关于代数运算的结合律是具有遗传性的。G_S中的每一个元素可逆即为条件。

所以,G_S关于S的代数运算作成一个群。当S为群时,S中的任何元素都是可逆元时,$\forall s \in S$,有$s \in G$,即$G_S = S$。

Theorem 2.14

设G为一个群,

(1) a与a^{-1}同阶

(2) ab与ba同阶

(3) f是群G到G'的映射,$a \in G$.若f是群同构，,证明a的阶等于$f(a)$的阶．若f是群同态，上述结论是否成立？为什么？

Proof (1) 先证a与a^{-1}中有一个阶数为无限阶.

若$|a| = \infty$.断言$\left|a^{-1}\right| = \infty$.反之若$\left|a^{-1}\right| = n$

那么$\left(a^{-1}\right)^n = e$此时$(a^n)^{-1} = e$那么$a^n = e$与$\infty$矛盾故$\left|a^{-1}\right| = \infty$

同理可证另一边换言之a与a^{-1}阶数要么同为∞要么同为有限

再证若$|a| = m; \left|a^{-1}\right| = n$ $m, n < \infty$下证$m = n$

已知$a^m = e$且$\left(a^{-1}\right)^m = (a^m)^{-1} = e^{-1} = e$那么$n|m$同理$m|n$

故相等

(2) 同理可证只要发现$(ab)^m = abab\cdots ab = a\,(ba)^{m-1}\,b = e \Longrightarrow (ba)^{m-1}\,b = a^{-1} \Longrightarrow (ba)^{m-1}\,ba = e \Longrightarrow (ba)^m = e$即可

(3) 证明设$a, f(a)$的阶分别为k, l,从而结合$a^k = e$,则$e = f\left(a^k\right) = (f(a))^k$,从而$l \mid k$

同理$k \mid l$，故$k = l$，也即a与$f(a)$有同样的阶

若f为群同态则不一定成立,如考虑$\mathbb{Z}_4 = \left\{e, a, a^2, a^3\right\} \to \mathbb{Z}_2 = \{e, a\}$,其中$f(a) = a^2$,从而可知$a$的阶为4,但$f(a)$的阶为1,从而命题不再

Proposition 2.11 (群同态下像与原像的阶)

设$f: G \to G'$为群同态映射,$a \in G$,$f(a)$的阶有限

证明：a的阶为无限,或是能被$f(a)$的阶整除的有限阶

Proof 如果a的阶为无限,则结论正确

如果a的阶为有限阶,设$|a| = n$,即$d^n = e$,那么,$e' = f(e) = f\left(d'\right) = [f(a)]^n$,所以,$f(a)$的阶整除$a$的阶$n$。

Proposition 2.12 (元素幂次的阶与可交换元的阶)

$\$$***I***:设群G中的元a的阶为d， $k \in \mathbb{N}$

证明：a^k的阶为$\dfrac{d}{(d,k)}$,这里(d,k)是d,k的最大公因数$\Longrightarrow$进而a^k的阶为d当且仅当$(d,k) = 1$

II:设a, b分别是群G中元，$ab = ba$， $|a| = m$且$|b| = n$

(1) 证明：$\operatorname{ord}(ab) \mid \operatorname{lcm}(m,n)$

(2) 若$(m,n) = 1$，证明ab的阶为mn

(3) 若$\langle a\rangle \cap \langle b\rangle = \{e\}$，证明：$ab$的阶为$[m,n]$($[m,n]$表示$m,n$的最小公倍数)

(4) 并举例$ab \neq ba$且$\operatorname{ord}(ab) = \infty$

III:设群G中两个元g, h可换,$o(g) = m, o(h) = n$.记$(m,n), [m,n]$分别是m,n的最大公因子和最小公倍数.则

(1)$o\left(g^n h^m\right) = \dfrac{[m,n]}{(m,n)}$;

(2)G中存在阶为(m,n)的元;

(3)G中存在阶为$[m,n]$的元.

Proof *I* :

我们设a^k的阶为l此时我们知道$\left(a^k\right)^{\frac{d}{(d,k)}}=e\Longrightarrow l\left|\frac{d}{(d,k)}\right.$

且因为$a^{kl}=e=a^d$那么我们有$d|kl\Longrightarrow\frac{d}{(d,k)}|kl\Longrightarrow\frac{d}{(d,k)}|l$

$\Longrightarrow l=\frac{d}{(d,k)}$

Proof *II* :

(1) 注意到$(ab)^{\operatorname{lcm}(m,n)}=a^{\operatorname{lcm}(m,n)}b^{\operatorname{lcm}(m,n)}=e\Longrightarrow\operatorname{ord}(ab)\mid\operatorname{lcm}(m,n)$

(2) 法一：此时我们设$o(ab)=k$

此时我们发现$(ab)^{mn}=a^{mn}b^{mn}=e$故我们有$k|mn$

其次a^n的阶为$\frac{m}{(m,n)}=m$且b^m的阶为$\frac{n}{(n,m)}=n$

$(ab)^m=b^m$且$(ab)^n=a^n\Longrightarrow o\left((ab)^m\right)=n$且$o\left((ab)^n\right)=m$

故结合ab的阶为k我们有$n=\frac{k}{(k,m)}$与$m=\frac{k}{(k,n)}\Longrightarrow n|k$与$m|k$又$(m,n)=1\Longrightarrow mn\mid k$

故$k=mn$故ab的阶为mn

法二:设$|ab|=k$。因为$(ab)^{mn}=a^{mn}b^{mn}=(a^m)^n(b^n)^m=e^ne^m=e$,得$k\mid mn$;

另一方面,由于$ab=ba,e=(ab)^{mk}=a^{mk}b^{mk}=(a^m)^kb^{mk}=b^{mk}$,得$n\mid mk$,又因为$(m,n)=1$,所以,$n\mid k$

同理,由于$e=(ab)^{nk}=a^{nk}b^{nk}=a^{nk}(b^n)^k=a^{nk}$,得$m\mid nk$,又因为$(m,n)=1$,所以,$m\mid k$

最后,由$(m,n)=1,n|k,m|k$,得到$mn\mid k$

综上所述,我们证得：$|ab|=k=mn$

(3) 设ab的阶为d那么显然$(ab)^{[m,n]}=e\Longrightarrow d|[m,n]$　此时$\langle a\rangle=\left\{e,a,a^2\cdots a^{m-1}\right\}$与$\langle b\rangle=\left\{e,b,b^2\cdots b^{n-1}\right\}$

此时$a^db^d=e=b^n\Longrightarrow a^d=b^{n-d}\in\langle a\rangle\cap\langle b\rangle\Longrightarrow$故$a^d=e=b^{n-d}\Longrightarrow m|d$且$n|d\Longrightarrow[m,n]\,|d\Longrightarrow d=[m,n]$

(4) 在$GL_2(\mathbb{R})$中取$A=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$　$B=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$

$\operatorname{ord}(A)=3$　$\operatorname{ord}(B)=4$　且$AB=\begin{pmatrix}1&0\\-1&1\end{pmatrix}$但是$\operatorname{ord}(AB)=\infty$

Proof *III* :

(1)因$o(g^n)=\frac{m}{(m,n)}$,　$o(h^m)=\frac{n}{(m,n)}$,　$g^nh^m=h^mg^n$　$\left(\frac{m}{(m,n)},\frac{n}{(m,n)}\right)=1$

故由已知结论知$o(g^nh^m)=\frac{m}{(m,n)}\frac{n}{(m,n)}=\frac{[m,n]}{(m,n)}$.

(2)设$m=p_1^{m_1}\cdots p_t^{m_t},n=p_1^{n_1}\cdots p_t^{n_t}$,其中$p_1,\cdots,p_t$是互不相同的素数,$m_i,n_i$均为非负整数.

不妨设$m_i\geqslant n_i,1\leqslant i\leqslant l;m_i<n_i,l+1\leqslant i\leqslant t.$

令$a=p_1^{m_1}\cdots p_l^{m_l}$,　$b=p_{l+1}^{n_{l+1}}\cdots p_t^{n_t}$.

则g^a的阶为$p_{l+1}^{m_{l+1}}\cdots p_t^{m_t}$,　h^b的阶为$p_1^{n_1}\cdots p_l^{n_l}$.

这两个阶显然是互素的,且g^a与h^b可换,因此g^ah^b的阶为$(m,n)=p_1^{n_1}\cdots p_l^{n_l}p_{l+1}^{m_{l+1}}\cdots p_t^{m_t}$

(3)类似可证.只需令$a=p_{l+1}^{m_{l+1}}\cdots p_t^{m_t}$　$b=p_1^{n_1}\cdots p_l^{n_l}$

2.4 循环群与生成群的例子与性质

Proposition 2.13

令 $(G,\cdot)$是一个群, 任取$x\in G$。则$f:(\mathbb{Z},+)\to(G,\cdot)$, 定义为$f(n)=x^n$, 是一个群同态。

注意这里不能推广到群同构, 因为单射很难满足, 就如例子x的阶数有限即可

Definition 2.21 (由元素生成群)

令 $(G,\cdot)$是一个群, 且$x\in G$, 则$\langle x\rangle$, 被称为由x生成的群, 定义为$\langle x\rangle=\{x^n:n\in\mathbb{Z}\}$

Definition 2.22 (由子集生成群)

设S是群G中一个非空子集, 令$S^{-1}=\left\{a^{-1}\mid a\in S\right\}$, 记$\langle S\rangle=\left\{x_1\cdots x_m\mid m\in\mathbb{N},x_1,\cdots,x_m\in S\cup S^{-1}\right\}$.

容易验证$\langle S\rangle$是G的一个子群, 称为S生成的子群.

如果$\langle S\rangle=G$, 则称S为群G的一个生成组.如果群G有一个有限的生成组，则称G为有限生成群

且我们有等价刻画$\langle S\rangle=\bigcap\{H\subset G:H\supset S,H<G\}$因此中由$S$生成的子群$\langle S\rangle$, 是包含了$S$的最小子群

Proof 注意到若$S\subseteq H<G$, 则$S\cup S^{-1}\subseteq H$, 从而由封闭性可知$\langle S\rangle\subseteq H$, 即有$\langle S\rangle\subseteq\bigcap_{S\subseteq H<G}H$

而另一方面，显然$\langle S\rangle<G$，从而$\bigcap_{S\subseteq H<G}H\subseteq\langle S\rangle$，从而两者相等，即证.

Definition 2.23 (循环群)

令 $(G,\cdot)$是一个群。若存在$x\in G$, 使得$G=\langle x\rangle$, 则G被称为一个循环群, 而x被称为G的一个生成元

Proposition 2.14 (循环群的构造方法一)

证明：n阶群是循环群当且仅当G中存在n阶的元素

Proof 设G是由元素a生成的n阶循环群, 则生成元a的阶与群G的阶相等, 即G中元素a, 它的阶为n

反之, 如果n阶群G中存在一个n阶的元素a, 则由a生成的G的子群 (a)中含有n个元素, 众而有$G=(a)$, 得G是一个循环群。

Proposition 2.15

令 $(G,\cdot)$是一个群, 则$\langle x\rangle=\langle\{x\}\rangle$

Proof 根据定义和性质, $\langle\{x\}\rangle$是包含了$\{x\}$的最小的子群

因此要证明这个最小的子群就是$\langle x\rangle$, 我们只须证明两点

一, $\langle x\rangle$是个子群;

二, 如果一个子群H包含了$\{x\}$, 那么它一定要包含整个$\langle x\rangle$

首先, 刚才我们已经利用同态的性质, 证明了$\langle x\rangle$是个子群

这就证明了第一点。第二点几乎也是显然的.我们假设H是个子群, 且$x\in H$

那么根据子群包含单位元, 且有乘法和逆元的封闭性, 我们有$e\in H$, 并且递归地, 对于$n\in\mathbb{N}_1,x^n=x\cdots x\in H,x^{-n}=x^{-1}\cdots x^{-1}\in H$

这就证明了$H\supset\langle x\rangle$

上面这个命题美妙地证明了这个由x生成的群, 确实就是由子集$\{x\}$生成的子群。

未来我们也会看到很多类似的命题。我们一定要注意, 不要被一些定义所误导了

例如这里$\langle x\rangle$的定义本身, 实际上不能说明这就是由子集$\{x\}$生成的子群, 所以我们是需要用命题来证明的, 这并不是完全平凡的结论

Theorem 2.15 (循环群的交换性质)

循环群都是交换群

Proof 设$G=\langle a\rangle$;故任何两个元素x,y都可以写为$x=a^m;y=a^n$显然可交换

Definition 2.24 (有限与无限循环群)

设一个$G=\langle a\rangle$且$|G|<\infty$称G为有限循环群,显然此时$|a|=|G|<\infty$.反之称为无限循环群

Theorem 2.16 (无限阶循环群)

1.所无限阶循环群同构

2.无限阶循环群仅有恰有两个生成元a，a^{-1}

Proof 1.构造$\varphi:\mathbb{Z}\to\langle a\rangle\quad n\mapsto a^n$　其中$G=\langle a\rangle$为无限阶循环群

容易验证φ为一个双射故所有无限阶循环群同构

2.若a^n为一个生成元此时$\Longrightarrow G=\langle a^n\rangle$，则$a$可写成$a^n$的幂：$a=(a^n)^k=a^{nk}$

$\Longrightarrow nk=1$，所以$n=\pm1$

反过来$n=\pm1$的时候显然为循环生成元总之$G=\langle a^n\rangle$

Proof 首先证明$x^n(n\in\mathbb{Z})$是两两不同的

假设有两个相同，不失一般性假设$m>n\in Z,x^m=x^n$,则$x^{m-n}=e$,故x是有有限阶的

这就矛盾了。接着,如果$x^n(n\in\mathbb{Z})$可以生成这个群,那么$x\in\langle x^n\rangle$,于是存在$m\in\mathbb{Z}$使得$x=(x^n)^m$,于是$x^{nm-1}=0$

由于x是无限阶的,所以$nm=1$,那么这样的n只能是±1。另外,显然x^{-1}也可以生成这个群。这就证明了恰好是这两个生成元

Theorem 2.17 (有限阶循环群)

0.所有有限阶r阶循环群同构于$\mathbb{Z}_r$

1.令$G=\langle x\rangle$是一个n阶循环群.假设$1\leqslant m\leqslant n$,则x^m的阶为$|x^m|=\dfrac{n}{\gcd(n,m)}$（这里的$m$可以变为$\mathbb{N}^+$）

2.令$G=\langle x\rangle$是一个n阶循环群.那么若另有一个元素y其$|y|=n\Leftrightarrow y$也为G的一个生成元

3.令$G=\langle x\rangle$是一个n阶循环群,则$x^m(1\leqslant m\leqslant n)$是个生成元,当且仅当$\gcd(m,n)=1$

特殊的r阶循环群有$\varphi(r)$个循环生成元形如a^n其中$n\in\mathbb{Z}_r$

Proposition 2.16

1.循环群$G=\langle a\rangle$的任一子群都形如$\langle a^l\rangle,l\in\mathbb{N}$，从而也是循环群

2.循环群的同态像也为循环群,且将生成元映至生成元

3.设$G=\langle a\rangle$是m阶循环群，设$m=dq$则$\langle a^q\rangle$为d阶子群，

指出若$H<G$且$|H|\,|d$则$H\subseteq\langle a^q\rangle$，则$\langle a^q\rangle$是唯一的$d$阶子群

Proof 若G是有限阶循环群$\Longrightarrow$设H是G的非平凡子群

令$l=\min\{m\in\mathbb{N}^*\mid a^m\in H\}$,则$a^l\in H$,从而$\langle a^l\rangle\subseteq H$.

反之,若$a^m\in H$,则作带余除法$m=ql+r$，其中$0\leqslant r<l$.于是$a^r=a^{m-ql}=a^m\cdot(a^l)^{-q}\in H$

由l的取法知$r=0$,即$m=lq$.因此$H\subseteq\langle a^l\rangle$.故$H=\langle a^l\rangle$为循环群.注意到$l=0$和$1$恰好对应于平凡子群,因此任何子群都形如$\langle a^l\rangle,l\in\mathbb{N}$

若G是无限阶循环群则不防考察$\mathbb{Z}$而我们知道其子群只有$m\mathbb{Z}$形式故即可

2.如果群 G′是群 G 的同态象,即存在同态满射$f:G\to G',\forall b\in G'$,则存在$x\in G$,使得$f(x)=b$.
由于G为循环群,设$G=(a)$,那么有$x=a^n,n\in\mathbb{Z}$,由f为同态,得$b=f(x)=f\left(a^n\right)=[f(a)]^n$
所以得$G'=(f(a))$为循环群,其生成元为$f(a)$.

Proposition 2.17

在n阶循环群G中,对每个n的正因子m,阶为m的元恰好有$\varphi(m)$个,其中φ为欧拉函数,并证明$\sum_{m|n}\varphi(m)=n$

Proof 设$G=\langle a\rangle$为n阶循环群，设G中是m阶的元素个数为$\psi_G(m)$，设$G_1=\left\langle a^{n/m}\right\rangle$为唯一的$m$阶子群
我们有$\sum_{m|n}\psi_G(m)=n$
任取x为G中任一m阶元则我们知$\langle x\rangle=G_1\Longrightarrow$所有的$m$阶元必定在$G_1$中
则个数$\psi_G(m)=\varphi(m)$证毕

Proposition 2.18

证明：设G为n阶循环群,$k\mid n$,则存在G的唯一k阶子群
同样证明其逆命题：设G为n阶群,且对n的每个因子m都存在G的唯一m阶子群,证明G为循环群
同样的手法可以证明：有限群G的不同子群有不同的阶那么G为循环群

Proof 先证明第一个：$G=\langle a\rangle=\left\{e,a\cdots a^{n-1}\right\}$此时我们构造$H=\left\langle a^l\right\rangle$使得$o\left(a^l\right)=\dfrac{n}{(n,l)}=k$从而$H$为$k$阶子群
这只需$(n,l)=\dfrac{n}{k}$只需$l=\dfrac{n}{k}$即可
进一步因为循环群的子群都形如$\langle a^m\rangle$故唯一性证毕
再证明第二个：设群G中的元素阶全体为$d_1\cdots d_t$
从而对于任一阶d.若有a,b阶都为d从而由d阶子群的唯一性知道$\langle a\rangle=\langle b\rangle$
$\Longrightarrow$存在$1\leqslant k<d$使得$b=a^k$此时我们还有k与d的关系：$o(b)=o\left(a^k\right)=\dfrac{d}{(d,k)}=d\Longrightarrow(k,d)=1$
因此这样的b我们有$\varphi(d)$个其中φ为欧拉函数
这表明按照元素的阶划分,阶为d_i的元素个数有$\varphi(d_i)$个,因此$\sum_{i=1}^{t}\varphi(t_i)=n=\sum_{m|n}\varphi(m)$
由d_i均为n的因子,从而$d_1\cdots d_t$恰为n的因子全体,进而可知存在$d_i=n\Longrightarrow G$为n阶元

✍ **Exercise 2.2** 找出$(\mathbf{Z}_{15},+)$的一切生成元和$\mathbf{Z}_{15}$的所有子群

Proof 由于$\mathbf{Z}_{15}$的生成元即为与15互素的那些整数所在的类,因此$\mathbf{Z}_{15}$的所有生成元为：$\overline{1},\overline{2},\overline{4},\overline{7},\overline{8},\overline{11},\overline{13},\overline{14}$,共8个
由于循环群的子群仍是循环群,所以$\mathbf{Z}_{15}$的子群也是循环群
要求$\mathbf{Z}_{15}$的所有子群,只需求出$\mathbf{Z}_{15}$中所有元素生成的子群即可
因此$\mathbf{Z}_{15}$的所有子群为：
$H_1=(\overline{1})=(\overline{2})=(\overline{4})=(\overline{7})=(\overline{8})=(\overline{11})=(\overline{13})=(\overline{14})=\mathbf{Z}_{15}$,
$H_2=(\overline{3})=(\overline{6})=(\overline{9})=(\overline{12})=\{\overline{0},\overline{3},\overline{6},\overline{9},\overline{12}\}$,
$H_3=(\overline{5})=(\overline{10})=\{\overline{0},(\overline{5}),(\overline{10})\}$
$H_4=(\overline{0})$。

✍ **Exercise 2.3** 设H是$(\mathrm{Z},+)$的子群,则$H=\{0\}$或$H=(m)$(此时m为H中的最小正整数).

Proof 如果$H=\{0\}$,则结论成立.
如果$H\neq\{0\}$,则H中含有非零数k,由于H是Z的子群,则有$-k\in H$.由此可以看出不论k是正是负,H中总存在正整数
我们取m为H中的最小正整数.下面证明：$H=\langle m\rangle=\{mk\mid k\in\mathrm{Z}\}$.

因为$\langle m\rangle$是包含m的最小子群,而子群H中含有m,所以$\langle m\rangle \subseteq H$.
反之,$\forall h \in H$,那么由整数的带余除法知,$h = qm + r$,其中$q, r \in \mathbb{Z}, 0 \leqslant r < m$
因为$r = h - qm \in H$,由m的最小性得$r = 0$,因此$h = qm \in \langle m\rangle$,从而得$H \subseteq \langle m\rangle$.所以$H = \langle m\rangle$.

作为到现在群论的学习我们要给出几个特殊的例子作为学习，以及上文提到的任何有限群和无限群同构，我们常常注意以下几种

Example 2.9 $\mathbb{Z}_4$ 群

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$
1.$\mathbb{Z}_4$是循环群
2.$\mathbb{Z}_4$是交换群

Example 2.10 *Klein*四元群

*Klein*四元群 $\{e, a, b, c\}$ 满足 $|a| = |b| = |c| = 2; ab = c; bc = a; ac = b$
1.*Klein*四元群为交换群
2.*Klein*四元群不是循环群,但是可以由 $\{a, b\}$ 两个元素生成

Example 2.11 D_3 群

$D_3 : \{e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$
1.D_3不是循环群
2.D_3不是交换群
3.$\sigma\tau = \tau\sigma^2$
4.$Order\,(\sigma) = Order\,(\sigma^2) = 3 \quad Order\,(\tau) = Order\,(\tau\sigma) = Order\,(\tau\sigma^2) = 2$

Note 之后我们将证明一个四元素群要么同构于 Klein 四元群要么同构于 $\mathbb{Z}_4$。一个六元素群要么同构于 D_3 要么同构于 $\mathbb{Z}_6$

Lemma 2.1

*Lemma*1：若 $(m,n)=1$; 那么 $(\mathbb{Z}_{mn}^*,\times)\cong(\mathbb{Z}_m^*,\times)\oplus(\mathbb{Z}_n^*,\times)$

Proof

Proof：构造映射 $\mathscr{B}:(\mathbb{Z}_{mn}^*,\times)\longrightarrow(\mathbb{Z}_m^*,\times)\oplus(\mathbb{Z}_n^*,\times)\quad x\bmod mn\longmapsto(x\bmod m,x\bmod n)$

那么 $Ker\mathscr{B}=\{x:\ x\bmod m=1且x\bmod n=1\}=\{x:\ x\bmod mn=1\}$ 故为单射

其次 $\left|\mathscr{B}\left(\mathbb{Z}_{mn}^*\right)\right|=\left|\mathbb{Z}_{mn}^*\right|=\varphi(mn)=\varphi(m)\varphi(n)=\left|\mathbb{Z}_m^*\right|\times\left|\mathbb{Z}_n^*\right|=\left|(\mathbb{Z}_m^*,\times)\oplus(\mathbb{Z}_n^*,\times)\right|$ 故为满射

(上述一行 $\left|\mathscr{B}\left(\mathbb{Z}_{mn}^*\right)\right|=\left|\mathbb{Z}_{mn}^*\right|$ 其实不那么显然有个问题是是否存在 $x\neq y$ 使得 $x=mt_1+l_1\ \ y=mt_3+l_1$)

(但这实际上是不会出现的因为 $x\neq y$ 所以在 $\mathbb{Z}_{mn}^*$ 中余数不会相同所以实际上上述这么设就有不合理性)

再者同态显然

Lemma 2.2

*Lemma*2：若 p 为质数, 对于模 p 意义下的 n 次整系数多项式 $f(x)$, 同余方程 $f(x)\equiv 0(\mathrm{mod}p)$ 至多有 n 个整数解

Lemma 2.3

*Lemma*3：对于奇质数 p; $\mathbb{Z}_{p^k}^*$ 为循环群其中 k 为自然数.且 $\mathbb{Z}_{p^k}^*\cong\mathbb{Z}_{(p-1)p^{k-1}}$

Proof

1°：当 $k=1$ 时, 此时

$\forall d|p-1$ (即 $p-1$ 的正因子), 令 $S(d)=\{\bar{a}:\ ord_p(a)=d\}$ 这里 a 是指在 $\mathbb{Z}_p^*$ 中阶为 d 的元素

因为 $\mathbb{Z}_p^*=\{\bar{1};\cdots\overline{p-1}\}$ 那么对于任意的元素 $a\in\mathbb{Z}_p^*$, 由拉格朗日定理知道 a 的阶一定整除 $p-1$ 所以 a 一定属于某个 $S(d)$

因而 $S(d)$ 划分了 $\mathbb{Z}_p^*$

若 $S(d)=\oslash$ 那么 $|S(d)|=0$

若 $S(d)\neq\oslash$ 此时 $\exists\bar{a}\in S(d)\ \ s.t.\ a^d\equiv 1\ (mod\ p)$ 即 $\bar{a}$ 在 $\mathbb{Z}_p^*$ 中阶为 d

此时由 *Lemma*2 知道 $x^d\equiv 1\ (modp)$ 在模 p 意义下的解最多 d 个且 $1;a;\cdots a^{d-1}$ 即为方程的 d 个解且两两模 p 不同余

那么我们有 $S(d)\subseteq\{1,a\cdots a^{d-1}\}$

(实际上若存在 $a^2\equiv 3\ (mod\ p)$ 和 $a^8\equiv 3\ (mod\ p)$ 意味着 $a^6\equiv 1\ (mod\ p)$ 这与 a 的阶为 d 即最小性矛盾)

此时 $ord\left(a^k\right)=\frac{d}{(d,k)}$ 所以若 a^k 阶为 $d\Longleftrightarrow(d,k)=1$

所以 k 的取法就取 $\varphi(d)$ 个 (欧拉函数表示)

故 $|S(d)|=0$ 或者 $\varphi(d)$

这时由 $S(d)$ 划分知 $\sum_{d|p-1}|S(d)|=\left|\mathbb{Z}_p^*\right|=p-1$ 而 $\sum_{d|p-1}|S(d)|\leqslant\sum_{d|p-1}\varphi(d)=p-1$ (这是由欧拉函数的性质知道的)

那么故对于每一 $d|p-1$ 都应该有 $|S(d)|=\varphi(d)\neq 0$ 才能取到等号

特别地对于 $d=p-1$ 那么 $|S(p-1)|=\varphi(p-1)\neq 0$ 这也是由 p 为奇素数所决定的

即 $\mathbb{Z}_p^*$ 中存在阶为 $p-1$ 的元素故 $\mathbb{Z}_p^*$ 为循环群

2°：下面我们证明 $\mathbb{Z}_p^*$ 中一定存在生成元 g，使得 $g^{p-1}\not\equiv 1\left(\mathrm{mod}p^2\right)$

设 g 是 Z_p^* 中的任意一个生成元, 如果 g 不满足上式, 即 $g^{p-1}\equiv 1\left(\mathrm{mod}p^2\right)$

那么断言 $g+p$ 一定满足, 因为 $(g+p)^{p-1}\equiv g^{p-1}+p(p-1)g^{p-2}\equiv 1-pg^{p-1}\left(\mathrm{mod}p^2\right)$

又 g 不含因子 p $\left($可以从 $g^{p-1}\equiv 1\left(\mathrm{mod}p^2\right)$ 看出也可以从 g 是 Z_p^* 中的任意一个生成元看出$\right)$ 故 $g+p$ 满足条件.

3°：现设 g 是满足上述条件的 Z_p^* 的生成元, 对于任意的 $\beta\in N$, 我们断言存在 $k_\beta,(k_\beta,p)=1$ 使得 $g^{\varphi\left(p^\beta\right)}\equiv 1+k_\beta p^\beta\ (mod\ p^{\beta+2})$

事实上, 当 $\beta=1$ 时, 所证明式子 $g^{\varphi\left(p^\beta\right)}\equiv 1+k_\beta p^\beta\ (mod\ p^{\beta+2})\Longleftrightarrow g^{p-1}\equiv 1+k_1p\ (mod\ p^3)$

由 g 为 $\mathbb{Z}_p^*$ 生成元知道 $g^{p-1}\equiv 1\ (mod\ p)$ 且 $g^{p-1}\not\equiv 1\left(\mathrm{mod}p^2\right)$

此时就有 $g^{p-1}=pt+1$ 且 t 中无 p 因子不然与 $g^{p-1}\not\equiv 1\left(\mathrm{mod}p^2\right)$ 矛盾

可知 $\beta=1$ 时上式成立

利用归纳法,先假设结论对于β成立，则$g^{\varphi(p^\beta)} \equiv 1 + k_\beta p^\beta \ (mod\ p^{\beta+1})$ 其中k_β与p互素
$g^{\varphi(p^{\beta+1})} = \left(g^{\varphi(p^\beta)}\right)^p = \left(1 + k_\beta p^\beta\right)^p \equiv 1 + k_\beta p^{\beta+1} \left(\mathrm{mod} p^{\beta+2}\right)$.由于$\left(k_\beta, p\right) = 1$故命题对$\beta + 1$成立
综上，命题对$\forall \beta \in N$成立。

4°：最后,我们将证明上述的g就是$Z_{p^k}^*$的生成元.
记$r = \mathrm{ord}_{Z_{p^k}^*}(g)$,则有$r \mid (p-1)p^{k-1}$(这里用到$\varphi\left(p^k\right) = (p-1)\,p^{k-1}$欧拉函数的性质)
又$\mathrm{ord}_{Z_p^*}(g) = p - 1$且$Z_p^*$是$Z_{p^k}^*$的子群,故不妨设$r = (p-1)p^{\beta-1}(\beta \le k)$
(因为在$Z_{p^k}^*$中是模p^k,这个模的数比p大,因而g生成元在前$p-1$次的循环模p^k与模p没什么本质区别故r可以表示为上述形式)
由于$g^r = g^{(p-1)p^{\beta-1}} = g^{\varphi(p^\beta)} = 1 + k_\beta p^\beta \not\equiv 1 \left(\mathrm{mod} p^{\beta+1}\right)$,结合$g^r \equiv 1 \left(\mathrm{mod} p^k\right)$可得$\beta \ge k$，所以$\beta = k$
(由上一行知道$g^r = p^k t + 1$;此时若$\beta < k$即$\beta + 1 \leqslant k$此时$g^r = p^k t + 1 = p^{\beta+1}\left(t p^{k-\beta-1}\right) + 1$矛盾)
故$r = (p-1)p^{\beta-1}$那么$\mathrm{ord}_{Z_{p^k}^*}(g) = \varphi\left(p^k\right)$,即$g$是$Z_{p^k}^*$的生成元,$Z_{p^k}^*$是循环群
根据上述定理,对于奇质数p,$Z_{p^k}^*$是循环群,由于$\left|Z_{p^k}^*\right| = \varphi\left(p^k\right) = (p-1)p^{k-1}$,故$Z_{p^k}^*$同构于$Z_{(p-1)p^{k-1}}$

Lemma 2.4

*Lemma*4 : $\forall \alpha \geqslant 3$我们有,对于任意奇数$a = 2k+1$,均有$a^{2^{\alpha-2}} \equiv 1 \left(\mathrm{mod} 2^\alpha\right)$.

Proof $(2k+1)^{2^{\alpha-2}}$每一项为$C_{2^{\alpha-2}}^i (2k)^i$那么在模$2^\alpha$意义下$i$取值从$0, 1 \cdots 2^\alpha$可以缩小到考虑$0, 1 \cdots \alpha - 1$
其次每一项为$\frac{2^{\alpha-2}\cdot\left(2^{\alpha-2}-1\right)\cdots\left(2^{\alpha-2}-(i-1)\right)}{i!} \cdot 2^i \cdot k^i = \frac{2^{\alpha-2+i}\cdot\left(2^{\alpha-2}-1\right)\cdots\left(2^{\alpha-2}-(i-1)\right)}{i!} \cdot k^i$
所以当$\alpha - 2 + i \geqslant \alpha$也不用考虑了.但是实际操作时我们再细致一点
那么$(2k+1)^{2^{\alpha-2}} \equiv 1 + 2^{\alpha-2} \cdot (2k) + \frac{2^{\alpha-2}\left(2^{\alpha-2}-1\right)}{2!} \cdot (2k)^2 \equiv 1 + 2^{\alpha-1}k - 2^{\alpha-1}k^2 + 2^{2\alpha-3}k^2$
$\equiv \underbrace{1 - 2^{\alpha-1}k\,(k-1) + 2^{2\alpha-3}k^2}_{\text{这里}k(k-1)\text{一定有个因子2}} \equiv \underbrace{1 + 2^{2\alpha-3}k^2}_{\text{因为}2\alpha-3\geqslant\alpha} \equiv 1\ (mod\ 2^\alpha)$

Lemma 2.5

*Lemma*5 : $\mathrm{ord}_{2^\alpha}(5) = 2^{\alpha-2}\ (\forall \alpha \geqslant 3)$

Proof *Proof*：由*Lemma*4知道上述引理说明对于任意奇数a，有$\mathrm{ord}_{2^\alpha}(a) \mid 2^{\alpha-2}$并且$\mathrm{ord}_{2^\alpha}(a)$一定为$2^\lambda$的形式
下面证明$\mathrm{ord}_{2^\alpha}(5) = 2^{\alpha-2}$,显然,这只需要证明当$\alpha \ge 3$时,$5^{2^{\alpha-3}} \not\equiv 1 \left(\mathrm{mod} 2^\alpha\right)$.我们将用归纳法证明。
当$\alpha = 3$时 $\Longleftrightarrow$ 证：$ord_8(5) = 2$显然正确
当$\alpha = k \geqslant 3$是时假设已经成立我们就有$5^{2^{k-3}} \not\equiv 1 \left(\mathrm{mod} 2^k\right)$　$WTS : 5^{2^{k-2}} \not\equiv 1 \left(\mathrm{mod} 2^{k+1}\right)$
此时由归纳假设知道$5^{2^{k-3}} \equiv 1 \left(\mathrm{mod} 2^{k-1}\right) \Longrightarrow 5^{2^{k-3}} = 2^{k-1}(2L+1) + 1$
(这里用$2L+1$代表奇数不然就与$5^{2^{k-3}} \not\equiv 1 \left(\mathrm{mod} 2^k\right)$矛盾)
那么$5^{2^{k-2}} = 1 + (2L+1)^2 2^{2k-2} + (2L+1)2^k$又由于$k \ge 3$,故$2k - 2 \ge k + 1$,
故有$5^{2^{k-2}} \equiv 1 + 2^k \left(\mathrm{mod} 2^{k+1}\right)$.综上,当$\alpha \ge 3$时，$5^{2^{\alpha-3}} \not\equiv 1 \left(\mathrm{mod} 2^\alpha\right)$。

Lemma 2.6

*Lemma*6 : $\mathbb{Z}_{2^\alpha}^*$同构于$\mathbb{Z}_2 \oplus \mathbb{Z}_{2^{\alpha-2}}\ (\alpha \geqslant 3)$

Proof 因为$\mathrm{ord}_{2^\alpha}(5) = 2^{\alpha-2}$,所以在$\mathbb{Z}_{2^\alpha}^*$中，$5^1, 5^2, \cdots, 5^{2^{\alpha-2}}$两两不同,$-5^1, -5^2, \cdots, -5^{2^{\alpha-2}}$也两两不同
显然$5^{k_1} \equiv 1 \left(\mathrm{mod} 2^\alpha\right), -5^{k_2} \equiv -1 \left(\mathrm{mod} 2^\alpha\right)$.故$5^{k_1} \not\equiv -5^{k_2} \left(\mathrm{mod} 2^\alpha\right)$.而$\left|\mathbb{Z}_{2^\alpha}^*\right| = 2^{\alpha-1}$
所以,$\pm 5^1, \pm 5^2, \cdots, \pm 5^{2^{\alpha-2}}$刚好构成$\mathbb{Z}_{2^\alpha}^*$的全部元素,即$\mathbb{Z}_{2^\alpha}^*$同构于$\mathbb{Z}_2 \oplus \mathbb{Z}_{2^{\alpha-2}}$。

Theorem 2.18 (循环群的自同构群结构)

我们来探讨循环群的$Aut\,(G)$的结构

当$n=2^{e_0}\prod_{i=1}^{k}p_i^{e_i}\ (e_0\geq 2)$时，$\mathrm{Aut}\,(\mathbb{Z}_n)$同构于$\left(\bigoplus_{i=1}^{k}\mathbb{Z}_{(p_i-1)p_i^{e_i-1}}\right)\bigoplus\mathbb{Z}_{2^{e_0-2}}\bigoplus\mathbb{Z}_2$

当$n=2^{e_0}\prod_{i=1}^{k}p_i^{e_i}\ (e_0=1)$时，$\mathrm{Aut}\,(\mathbb{Z}_n)$同构于$\bigoplus_{i=1}^{k}\mathbb{Z}_{(p_i-1)p_i^{e_i-1}}$

Proof 我们来探讨循环群的$Aut\,(G)$的结构

由于循环群同构与$\mathbb{Z}$与$\mathbb{Z}_n$所以我们来探讨$Aut\,(\mathbb{Z})$与$Aut\,(\mathbb{Z}_n)$

其次对于循环群的自同构,其一定把生成元映至生成元，故一个自同构σ只需由其在生成元的作用唯一决定

(I) :对于$Aut\,(\mathbb{Z})$,其生成元只有$1,-1\Longrightarrow Aut\,(\mathbb{Z})\cong\mathbb{Z}_2$

(II) :

对于$Aut\,(\mathbb{Z}_n)$;我们知道$\mathbb{Z}_n$的生成元构成集合$\mathbb{Z}_n^*=\{a:\ (a,n)=1\}$且知一个自同构$\sigma$只需由其在生成元1的作用唯一决定

我们记$\sigma\,(1)=a$这样为形式记作σ_a.那么$\forall\sigma_a,\sigma_b\in Aut\,(\mathbb{Z}_n)$我们有$\sigma_{ab}\,(1)=ab=\sigma_a\,(1)\,\sigma_b\,(1)$

则σ诱导了一个：$\mathscr{A}:\left(\mathbb{Z}_n^*,\times\right)\longrightarrow Aut\,(\mathbb{Z}_n)\quad a\longmapsto\sigma_a$的同态且为同构因一个自同构$\sigma$只需由其在生成元1的作用唯一决定

所以$Aut\,(\mathbb{Z}_n)\cong\left(\mathbb{Z}_n^*,\times\right)$

对于$m\in\mathbb{N}$，$(a,m)=1$，称使得$a^n\equiv 1(\mathrm{mod}m)$成立的最小正整数为$a$模$m$的阶,记作$\mathrm{ord}_m(a)$,或$\delta_m(a)$.

若$\mathrm{ord}_m(a)=\varphi(m)$,则称$a$为模$m$的原根.可见,$a$模$m$的阶就是$\bar{a}$在模$m$乘法群中的阶,即$\mathrm{ord}_m(a)=|\bar{a}|$

模m的原根对映于模m乘法群中的生成元。

我们针对$\left(\mathbb{Z}_n^*,\times\right)$中的$n$进行素因数分解$n=p_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}$

由$Lemma2.1$知道$\mathbb{Z}_n^*\cong\mathbb{Z}_{p_1^{e_1}}^*\oplus\mathbb{Z}_{p_2^{e_2}}^*\oplus\cdots\cdots\oplus\mathbb{Z}_{p_n^{e_n}}^*$

由$Lemma2.3$知道对于奇质数p;$\mathbb{Z}_{p^k}^*$为循环群其中k为自然数.且$\mathbb{Z}_{p^k}^*\cong\mathbb{Z}_{(p-1)p^{k-1}}$

$\Longrightarrow\mathbb{Z}_n^*\cong\mathbb{Z}_{2^{e_1}}^*\oplus\mathbb{Z}_{(p_2-1)p_2^{e_2-1}}\oplus\cdots\cdots\oplus\mathbb{Z}_{(p_n-1)p_n^{e_n-1}}\cong Aut\,(\mathbb{Z}_n)\oplus\mathbb{Z}_{(p_2-1)p_2^{e_2-1}}\oplus\cdots\cdots\oplus\mathbb{Z}_{(p_n-1)p_n^{e_n-1}}$

当$e_1=1$时.$Aut\,(\mathbb{Z}_2)\cong\mathbb{Z}_{2^1}^*\cong\{e\}$　　当$e_1=2$时.$Aut\,(\mathbb{Z}_4)\cong\mathbb{Z}_{2^2}^*\cong\mathbb{Z}_2$(根据生成元对应到生成元易知)

由$Lemma2.6$知道综合起来得到

综上，我们有如下结论：

当$n=2^{e_0}\prod_{i=1}^{k}p_i^{e_i}\ (e_0\geq 2)$时，$\mathrm{Aut}\,(\mathbb{Z}_n)$同构于$\left(\bigoplus_{i=1}^{k}\mathbb{Z}_{(p_i-1)p_i^{e_i-1}}\right)\bigoplus\mathbb{Z}_{2^{e_0-2}}\bigoplus\mathbb{Z}_2$

当$n=2^{e_0}\prod_{i=1}^{k}p_i^{e_i}\ (e_0=1)$时，$\mathrm{Aut}\,(\mathbb{Z}_n)$同构于$\bigoplus_{i=1}^{k}\mathbb{Z}_{(p_i-1)p_i^{e_i-1}}$

Theorem 2.19

在有理数加群$\mathbb{Q}$上定义同余关系，$a\sim b\Longleftrightarrow a-b\in\mathbb{Z}$

1.$\mathbb{Q}/\mathbb{Z}$该由同余关系诱导的正规子群，是一个无限的$Abelian$群

2.令p为一素数，令$\mathbb{Z}(p^\infty):=\left\{\overline{\frac{a}{b}}\in\mathbb{Q}/\mathbb{Z}\ \middle|\ a,b\in\mathbb{Z}且b=p^i\ (i\geqslant 0)\right\}$为一$\mathbb{Q}/\mathbb{Z}$的无限子群

3.对任一素数p，$\mathbb{Z}(p^\infty)$是由$\left\{\overline{\frac{1}{p^n}}\ \middle|\ n\in\mathbb{Z}\right\}$生成的

4.令H为$\mathbb{Z}(p^\infty)$的子群则有如下论断

I：每一个$\mathbb{Z}(p^\infty)$的元素均有有限的阶为p^n类型

II：若H中至少有一个元素有阶p^k，且H中无任何元素的阶比p^k大，则H是一循环群$H=\left\langle\overline{\frac{1}{p^k}}\right\rangle,H\cong\mathbb{Z}_{p^k}$

III：若H中元素阶无上界，则$H=\mathbb{Z}(p^\infty)$

IV：$\mathbb{Z}(p^\infty)$唯一的真子群，仅仅是有限的循环群$C_n=\left\langle\overline{\frac{1}{p^n}}\right\rangle(n=1,2\cdots)\ \ \langle 0\rangle=C_0<C_1<\cdots<$

V：令$x_1,x_2\cdots$为一$Abel$群中的元素，使得$|x_1|=p$且$px_2=x_1,px_3=x_2\cdots\cdots$则$\langle x_1,x_2,\cdots x_n\cdots\rangle\cong\mathbb{Z}(p^\infty)$

VI：H是$\mathbb{Z}(p^\infty)$子群但是$H\neq\mathbb{Z}(p^\infty)$则此时$\mathbb{Z}(p^\infty)/H\cong\mathbb{Z}(p^\infty)$

Proof 1.$\mathbb{Q}/\mathbb{Z}$是一无限的$abel$群，若为有限的设为$\{\overline{r_1},\overline{r_2}\cdots\overline{r_n}\}$那么根据等价类知识，我们总可以选取这些$r_i\in[0,1]$此时任取$[0,1]$上的除$r_i$以外的有理数，总不属于任何一个$\overline{r_i}$，矛盾

2.显然对于$\overline{\frac{a_1}{p^{i_1}}}$与$\overline{\frac{a_2}{p^{i_2}}}\ (i_1<i_2)\in\mathbb{Z}(p^\infty)$则$\overline{\frac{a_1}{p^{i_1}}}+\overline{\frac{a_2}{p^{i_2}}}=\overline{\frac{a_1p^{i_2-i_1}+a_2}{p^{i_2}}}\in\mathbb{Z}(p^\infty)$且任一$\overline{\frac{a_1}{p^{i_1}}}$具有逆元$\overline{\frac{-a_1}{p^{i_1}}}\in\mathbb{Z}(p^\infty)$

故$\mathbb{Z}(p^\infty)$为一子群，且应当说明如下注意点，$\overline{\frac{a}{p^k}}=\overline{\frac{ap}{p^{k+1}}}$

3.这是显然的

4.I：$\mathbb{Z}(p^\infty)$任一元素形如$\overline{\frac{a}{p^k}}$类型其阶显然$\underbrace{\overline{\frac{a}{p^k}}+\cdots+\overline{\frac{a}{p^k}}}_{p^k个}=\overline{0}\Longrightarrow\mathrm{ord}\left(\overline{\frac{a}{p^k}}\right)|p^k$　又p为素数故$\mathrm{ord}\left(\overline{\frac{a}{p^k}}\right)$是形如$p^n$类型的

4.II：由题干知不妨设该元素为H中的$\overline{\frac{a}{p^t}}$类型其中$(a,p)=1$，其阶为p^k

$\Longrightarrow\overline{\frac{ap^k}{p^t}}=\overline{0}\Longrightarrow p^t|ap^k\Longrightarrow k\geqslant t$　若严格的有$t<k$那么$\overline{\frac{a}{p^t}}$其阶显然$\leqslant t<k$与已知矛盾

故$t=k$

故该元素类型一定为$\overline{\frac{a}{p^k}}$且a与p互素则此时我们实际上有$\left\langle\overline{\frac{a}{p^k}}\right\rangle=\left\langle\overline{\frac{1}{p^k}}\right\rangle$

显然$\overline{\frac{a}{p^k}}\in\left\langle\overline{\frac{1}{p^k}}\right\rangle$由于互素可设$as+p^kn=1\Longrightarrow\left\langle\overline{\frac{1}{p^k}}\right\rangle=\left\langle\overline{\frac{as+p^kn}{p^k}}\right\rangle=\left\langle\overline{\frac{as}{p^k}}\right\rangle$而$\frac{as}{p^k}\in\left\langle\overline{\frac{a}{p^k}}\right\rangle$

故我们知道了H中包含$\overline{\frac{a}{p^k}}$类型故$\left\langle\overline{\frac{a}{p^k}}\right\rangle=\left\langle\overline{\frac{1}{p^k}}\right\rangle\subseteq H$，且因为$H$中元素再无比$p^k$阶更大的了

故在保证分子分母互素下，分母的p^i类型最多只能为p^k类型

故$H\subseteq\left\langle\overline{\frac{1}{p^k}}\right\rangle\Longrightarrow$故$H=\left\langle\overline{\frac{1}{p^k}}\right\rangle\Longrightarrow H\cong\mathbb{Z}_{p^k}$

4.III：显然我们有$H\subseteq\mathbb{Z}(p^\infty)$断言有$\mathbb{Z}(p^\infty)\subseteq H$

若不然意味着存在着$\overline{\frac{a}{p^k}}\notin H$（不妨设$a$与$p$互素）故$H$中就缺少了$\overline{\frac{1}{p^k}}\Longrightarrow H$缺少$\left\langle\overline{\frac{1}{p^k}}\right\rangle$

断言H中必定缺少如下形式$\overline{\frac{b}{p^s}}\ (s\geqslant k+1,b\in\mathbb{Z})$，若存在一个这样的形式$\overline{\frac{b}{p^s}}$

那么经过约分操作后总可以设存在$\overline{\frac{b}{p^s}}$（b与s互素）故存在$\overline{\frac{1}{p^s}}\Longrightarrow$存在$\overline{\frac{1}{p^k}}$矛盾

故H中元素的阶都可以被p^k控制矛盾

4.IV：令H为$\mathbb{Z}(p^\infty)$的真子群，则H中的元素一定有上界，不妨设H中分母最大的一个元素拿出设其形式$\overline{\frac{a}{p^k}}$(a与p互素)

则$\overline{\frac{1}{p^k}} \in H \Longrightarrow \overline{\left\langle \frac{1}{p^k} \right\rangle} \subseteq H$此时根据II就无任何元素的阶再大于$p^k$

4.V：我们只需构造如下的映射$\varphi : x_i \mapsto \overline{\frac{1}{p^i}}$ 扩充出去即可

4.VI：若$H \neq \mathbb{Z}(p^\infty)$则不妨设$H = \left\langle \overline{\frac{1}{p^n}} \right\rangle$

构造$abel$群$G = \langle x_1 \cdots x_m \cdots \rangle$其中$x_i = \overline{\frac{1}{p^{n+i}}} + H$则$G \cong \mathbb{Z}(p^\infty)$

构造$\mathbb{Z}(p^\infty)/H \to G$的映射$\varphi : \overline{\frac{1}{p^i}} + H \mapsto \overline{\frac{1}{p^{i+n}}} + H$即可为同构映射

2.5 对称群与置换群

Definition 2.25 (对称群, 置换群定义)

设G为一群

则G上所有的双射构成一个群S_G称为G的对称群(全变换群),S_G的一个元素称为G的一个变换,

S_G的一个子群称为G上的一个变换群

特别地当G为n元有限群,此时我们称S_G为S_n为n元对称群,S_n的一个元素称为一个n元置换

S_n的一个子群称为置换群

Theorem 2.20 (变换群 Cayley 定理)

任何一个群与一个变换群同构

Proof 设G为一个群.

任意选定$a \in G$ 构造$\sigma_a : G \to G \quad , x \mapsto ax, \forall x \in G$

构造$G^* = \{\sigma_a : \ a \in G\}$

我们先证明G^*确为一个变换群

任取一个G^*的元素为σ_a我们断言其一定为G上的一个一一变换

首先$\forall b \in G$, 存在$ab^{-1} \in G$使得$\sigma_a\left(a^{-1}b\right) = b$故为满射

其次若$ax_1 = ax_2 \Rightarrow x_1 = x_2$故为单射

再者G^*关于映射显然封闭因为一一变换即双射复合仍然是双射且容易知道$\sigma_a\sigma_b = \sigma_{ab}$

最后G^*关于逆封闭容易知道$\sigma_a\sigma_{a^{-1}} = \sigma_{a^{-1}}\sigma_a = \mathrm{Id}$

我们在证明G与G^*同构

构造$f : G \to G^* \quad a \mapsto \sigma_a, \forall a \in G$

1.$\sigma_a\sigma_b = \sigma_{ab}$满足同态

2.若$a \neq b$任取$x \in G$那么$ax \neq bx$那么$\sigma_a(x) \neq \sigma_b(x)$自然$\sigma_a \neq \sigma_b$那么$f(a) \neq f(b) \Rightarrow f$为单射

3.由G^*的构造方法显然f为满射

综上证毕

Definition 2.26

有限集合A上的一个一一变换叫做A的一个置换时

A的全体置换作成的一一变换群$E(A)$叫做n次对称群,记为S_n.S_n中的元素叫做n次置换.显然S_n的阶数为 n!

我们用如下形式来表示一个置换$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$

Corollary 2.4

每一个有限群都与一个置换群同构.或者说,任一个n所群G与S_n的某个子群同构.

Definition 2.27 (循环置换)

设$i_1, i_2, \cdots, i_r (r \leqslant n)$是集合$A = \{1, 2, \cdots, n\}$中不同的元素

如果σ置换恰好使得$i_1 \xrightarrow{\sigma} i_2 \xrightarrow{\sigma} \cdots \xrightarrow{\sigma} i_r \xrightarrow{\sigma} i_1$

我们称为r阶循环置换,记为$\sigma=(i_1 i_2\cdots i_r)$，$2-$循环环具换叫做对换.特别将恒等变换记为$\varepsilon=(1)=(2)=\cdots=(n)$.

Theorem 2.21 (n 次置换分解为循环置换定理)

任意一个n次置换σ都可以分解为有限个互不相交 (即无公共元素) 的循环置换的乘积且分解形式除排列次序之外是唯一的

Proof 我们用数学归纳法来证明.当σ为恒等变换时,即σ不变动任何元素时,定理是对的.

假设对于最多变动$r-1$个元素的置换定理成立,现在我们来看变动r个元素的置换σ.

我们任取一个被σ变动的元素i_1,从i_1出发可以找到一列元素：

$$i_1 \xrightarrow{\sigma} i_2 \xrightarrow{\sigma} i_3 \xrightarrow{\sigma} \cdots \xrightarrow{\sigma} i_k \xrightarrow{\sigma} i_1 = i_{k+1}$$

由于n为有限数,因此总有某个i_{k+1}已重复前面出现过的元素,不妨设i_{k+1}是第一个重复前面元素的.

那么i_{k+1}不可能是$i_s(2\leqslant t\leqslant k)$,因为$i_1,i_2,\cdots,i_k$互不相同

若不然不妨假设若$i_{k+1}=i_2$那么就有i_1与i_k在σ下的像都为$i_{k+2}=i_2$而$i_1\neq i_k$与一一变换矛盾故只有$i_{k+1}=i_1$.

因此,我们有因为σ只变动r个元素,即$r\geqslant k$.若$r=k$,则本身已是一个循环置换了.结论成立.

若$r>k$,那么

$$\begin{aligned}\sigma &= \begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n \\ i_2 & i_3 & \cdots & i_1 & i'_{k+1} & \cdots & i'_r & i_{r+1} & \cdots & i_n \end{pmatrix} \\ &= \begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n \\ i_2 & i_3 & \cdots & i_1 & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n \end{pmatrix} \cdot \begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n \\ i_1 & i_2 & \cdots & i_k & i'_{k+1} & \cdots & i'_r & i_{r+1} & \cdots & i_n \end{pmatrix} \\ &= \begin{pmatrix} i_1 i_2 & \cdots & i_k \end{pmatrix} \quad \sigma_1.\end{aligned}$$

其中σ_1只变动$r-k<r$个元素,且σ_1中所变动的元素与$k-$循环置换$(i_1 i_2\cdots i_k)$所变动的元素互不相同.

由归纳假设，σ_1可以写成若干个互不相交的循环置换的乘积$\sigma_1=\eta_1\eta_2\cdots\eta_s$,在这些循环置换中$i_1,i_2,\cdots,i_k$全不出现.

所以可以表示成互不相交的循环置换之积$\sigma=(i_1 i_2\cdots i_k)\,\eta_1\eta_k\cdots\eta_s$

唯一性

假设σ还有一个表示成两两不相交轮换乘积的式子：$\sigma=\tau_1\tau_2\cdots\tau_s$.

任取在σ下变动的元素a,则在$\sigma_1,\sigma_2,\cdots,\sigma_t$中存在唯一的$\sigma_l$,使得$\sigma_l(a)\neq a$.

这是因为σ_k不会相交所以只存在唯一一个

同理,在$\tau_1,\tau_2,\cdots,\tau_s$中存在唯一的$\tau_k$,使得$\tau_k(a)\neq a$.我们有$\sigma_l^m(a)=\sigma^m(a)=\tau_k^m(a),\quad m=0,1,2,\cdots.\sigma_l=\tau_k$.

继续这样的讨论,可得$t=s$,并且在适当排列$\tau_1,\tau_2,\cdots,\tau_s$的次序后,有$\sigma_i=\tau_i,i=1,2,\cdots,t$.从而唯一性成立.

Proof 取$a\in\{1,2,\cdots,n\}$,作序列$a=\sigma^0(a),\sigma(a),\sigma^2(a),\cdots$其中,$\sigma^0$是恒等置换$id$

这个序列一定包含重复的文字,记$\sigma^m(a)$是第一个与前面相重复的文字,并设它与$\sigma^k(a)(0\leqslant k<m)$重复

若$k>0$，则$\sigma^{k-1}(a)=\sigma^{m-1}(a)$,这与$m$的选择矛盾.因此$k=0$,即$\sigma^m(a)=a$

作轮换$\sigma_1=\left(a,\sigma(a),\cdots,\sigma^{m-1}(a)\right)$则$\sigma$与$\sigma_1$在文字$a,\sigma(a),\cdots,\sigma^{m-1}(a)$上的作用相同

但注意到σ_1在除了$\left(a,\sigma(a),\cdots,\sigma^{m-1}(a)\right)$上的作用是恒等映射,但我们并不清楚$\sigma$在除$\left(a,\sigma(a),\cdots,\sigma^{m-1}(a)\right)$上的作用如何

若$m=n$,此时我们就知道σ在序列下即为$\left(a,\sigma(a),\cdots,\sigma^{n-1}(a)\right)$此时这些元素互不相同即为$1\sim n$所有

σ_1同样如此则$\sigma=\sigma_1$此时σ已经确定好了它就是$\left(a,\sigma(a),\cdots,\sigma^{n-1}(a)\right)$这样一个轮换

若$m<n$此时取$b\notin\left(a,\sigma(a),\cdots,\sigma^{m-1}(a)\right)$仿照上面再做一个轮换$\sigma_2=\left\{b,\sigma(b),\cdots,\sigma^{l-1}(b)\right\}$

则σ与σ_2在$\left\{b,\sigma(b),\cdots,\sigma^{l-1}(b)\right\}$上的作用相同.而且因$\sigma$是单射,知道$\sigma_1$与$\sigma_2$不相交

这样继续下去，直到$1,2,\cdots,n$用完为止，得到有限个不相交的轮换$\sigma_1,\sigma_2,\cdots,\sigma_s$使$\sigma=\sigma_1\sigma_2\cdots\sigma_s$

注意到，由于对a,b等的选择可以不同，选择的先后也可以不同，所以上述各轮换$\sigma_1,\sigma_2,\cdots,\sigma_s$的次序可以不同

但任一文字c所在的轮换是唯一的，即$(c,\sigma(c),\ \sigma^2(c),\cdots)$，虽然形式上未必是以$c$开始

因此，任一n元置换表为不相交轮换的乘积时，如果不计次序，表法是唯一的.

Proposition 2.19

S_n中的每一个置换都可以表示成若干个对换之积.

Proof 证明利用定理3,只需证明每一个k一循环置换都可以表示成若干个对换之积即可.

事实上,当$k>1$时,$(i_1 i_2 \cdots i_k)=(i_1 i_k)\left(i_1 i_{L_1}\right)\cdots(i_1 i_3)(i_1 i_2)$

若$k=1$,有$(i_1)=(i_1 i_2)(i_1 i_2)$.

我们注意到：同一个置换表示成若干个对换之积的方法可以是多种的,同时也没有要求这些对换互不相交.s

Proposition 2.20 (循环置换重要性质)

(1)两个不相交的循环置换的乘积可以交换

(2) $(i_1 i_2 \cdots i_k)^{-1}=(i_k \cdots i_2 i_i)$;

(3)k循环置换$(i_1 i_2 \cdots i_k)$的阶是k

(4) S_n可以由集合$\{(12),(13),\cdots,(1n)\}$生成,即任意一个$n$次置换$\sigma$都可用若干个上述集合中的对换来表示

(5) $(a_1 b_1)(a_1 \cdots a_m, b_1 \cdots b_n)=(a_1 \cdots a_m)(b_1 \cdots b_n)$

(6) $(a_1 b_1)(a_1 \cdots a_m)(b_1 \cdots b_n)=(a_1 \cdots a_m, b_1 \cdots b_n)$

(7) 若$\alpha=(i_1 \cdots i_k)$，$\beta=(j_1 \cdots j_s)$若α，β不相交则 $\operatorname{ord}(\alpha\beta)=\operatorname{lcm}(k,s)$

Proof (1)设两个不相交的循环置换为$\sigma=(i_1 i_2 \cdots i_k)$，　$\tau=(j_1 i_2 \cdots j_r)$

其中自然数集$A=\{i_1,i_2,\cdots,i_k\}$与$B=\{j_1,j_2,\cdots,j_r\}$没有公共的元素

任意$x\in\{1,2,\cdots,n\}$,只可能：(1)$x\in A, x\notin B$; (2)$x\in B, x\notin A$; (3)$x\notin A$且$x\notin B$

讨论即可并不复杂

(2) (3) 检验即可注意 (3) 要说明阶要是最小的正整数

(4) 知S_n中的每一个置换都可以表示成若干个对换之积。

因此,我们只需证明任意一个对换可用集合$\{(12),(13),\cdots,(1n)\}$中的某些对换来表示即可

任意给出个对换(ij),如果i,j中有一个是1,则(ij)就是所给集合中元素,结论正确

如果i,j都不是1,则有$(ij)=(1i)(1j)(1i)$。所以，任意一个n次置换σ都可用集合$\{(12),(13),\cdots,(1n)\}$中的若干个对换来表示

(5) (6) 直接检验即可

(7) 若$\alpha=(i_1 \cdots i_l)$与$\beta=(j_1 \cdots j_s)$不相交，设$r=\operatorname{ord}(\alpha\beta)$,设$\operatorname{ord}(\alpha)=l$且$\operatorname{ord}(\beta)=s$

故$(\alpha\beta)^{\operatorname{lcm}(l,s)}=\alpha^{\operatorname{lcm}(l,s)}\beta^{\operatorname{lcm}(l,s)}=e$故$\operatorname{ord}(\alpha\beta)=r\mid\operatorname{lcm}(l,s)$

断言$l\mid r=\operatorname{ord}(\alpha\beta)$且$s\mid r=\operatorname{ord}(\alpha\beta)$　从而r是l与s的公倍数从而是最小公倍数的倍数进而得到：$\operatorname{lcm}(l,s)\mid r=\operatorname{ord}(\alpha\beta)$

下面证明这个断言：若$l\nmid r$则$\alpha^r\neq id$此时故存在$x\in(i_1 \cdots i_l)$使得$\boldsymbol{\alpha}^r(x)\neq x$

但我们知道此时x与$\boldsymbol{\alpha}^r(x)\in(i_1 \cdots i_l)$故仍然不属于$(j_1 \cdots j_s)$此时

$(\boldsymbol{\alpha\beta})^r(x)=\boldsymbol{\alpha}^r(\boldsymbol{\beta}^r(x))=\boldsymbol{\alpha}^r(x)\neq x$这与$\boldsymbol{\alpha\beta}$的阶数为$r$矛盾因为$(\boldsymbol{\alpha\beta})^r=id$

Definition 2.28 (偶置换与奇置换)

可以证明每一个置换,虽然可以用不同的方法表示成若干个对换之积,但每一种表示的对换个数的奇偶性是不变的.

一个置换σ如果可以表示成偶数个对换之积,则称σ偶置换.反之奇置换

因S_n中两个偶置换的积仍是偶置换,所以S_n中所有偶置换构成的集合作成S_n的一个子群

我们称这个子群为n次交错群,记为A_n.例如：$A_3=\{(1),(123),(132)\}$.

Note 设V是数域$\mathbb{P}$上的n维线性空间，$\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n$为其一组基

对任意$\sigma\in S_n$,定义V上线性变换π_σ满足$\pi_\sigma(\varepsilon_i)=\varepsilon_{\sigma(i)}$线性变换理论告诉我们这样的$\pi_\sigma$是存在唯一的

这样我们得到一个映射$\pi:S_n\to \mathrm{GL}(V),\quad \sigma\mapsto\pi_\sigma$容易验证这是一个单同态

我们再次构造映射$\det:\ GL(V)\to P^*,\ \mathscr{A}\to\det(\mathscr{A})$显然这是一个满同态,同态核为$\mathrm{Ker}\det=SL(V)$

映射合成得到群同态$\det\circ\pi:S_n\to\mathbb{P}^*$这一同态的像集为$\{1,-1\}$(当$n>1$时)

该同态的核记为A_n那么我们有$A_n\lhd S_n$(即将映射到1的为核),我们将A_n记为n元交错群

此时我们通过群同态$\det\circ\pi:S_n\to\mathbb{P}^*$就知道偶置换之积仍然为偶置换,而由对称性我们易知$|A_n|=\dfrac{n!}{2}$

Definition 2.29 (置换的型)

设$\sigma\in S_n$，将σ表示成没有公共元素的轮换之积，设长为r的轮换共有λ_r个$(1\le r\le n)$，则称置换σ的型为$1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$

Lemma 2.7 (S_n 中共轭类作用的效果)

在S_n中,$\sigma\in S_n$,那么$\sigma\begin{pmatrix}i&j&\cdots&k\\m&n&\cdots&p\end{pmatrix}\sigma^{-1}=\begin{pmatrix}\sigma(i)&\sigma(j)&\cdots&\sigma(k)\\\sigma(m)&\sigma(n)&\cdots&\sigma(p)\end{pmatrix}$

特殊地$\sigma(r_1,r_2\cdots r_k)\sigma^{-1}=(\sigma(r_1),\cdots,\sigma(r_k))$

Proof 直接验证即可

Theorem 2.22

1.S_n中任何两个轮换共轭$\iff$两个轮换长度一样

2.S_n中两个置换共轭$\iff$有相同的型

Proof 1.对于任意r轮换$(i_1\cdots i_r)$那么对于$\forall\varphi\in S_n$那么$\varphi(i_1\cdots i_r)\varphi^{-1}=(\varphi(i_1)\cdots\varphi(i_r))$

对于两个轮换$(i_1\cdots i_r)$与$(j_1\cdots j_r)$只需构造$\varphi:i_1\to j_1\cdots i_r\to j_r\ else$恒等

2.对于置换$\varphi\in S_n$将其写成若干不交的轮换乘积比如$\varphi=(ab)(xyz)\cdots(\alpha\beta\gamma\eta)$

那么$\sigma\varphi\sigma^{-1}=\sigma(ab)(xyz)\cdots(\alpha\beta\gamma\eta)\sigma^{-1}=\sigma(ab)\sigma^{-1}\sigma(xyz)\sigma^{-1}\cdots\sigma(\alpha\beta\gamma\eta)\sigma^{-1}=(\sigma(a),\sigma(b))(\sigma(x),\sigma(y),\sigma(z))\cdots(\sigma(\alpha))$

因而长度一样

若σ与σ^*有相同长度的型,$\sigma=(ab\cdots c)\cdots(\alpha\beta\cdots\gamma)$与$\sigma^*=(a^*b^*\cdots c^*)\cdots(\alpha^*\beta^*\cdots\gamma^*)$

那么构造$\varphi=\begin{pmatrix}a&b&\cdots&c&\cdots&\alpha&\beta&\cdots&\gamma\\a^*&b^*&\cdots&c^*&\cdots&\alpha^*&\beta^*&\cdots&\gamma^*\end{pmatrix}$即可有$\varphi\sigma\varphi^{-1}=\sigma^*$

Proposition 2.21

S_n中型为$1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$的置换共有$\dfrac{n!}{\prod\limits_{i=1}^{n}i^{\lambda_i}\lambda_i!}$由此证明$\sum\limits_{\lambda}\dfrac{1}{\prod\limits_{i=1}^{n}i^{\lambda_i}\lambda_i!}=1$

其中λ取遍所有的型，即λ取遍所有的数组$(\lambda_1,\lambda_2,\cdots,\lambda_n)$,$\lambda_i$均为非负整数且满足$\lambda_1+2\lambda_2+\cdots+n\lambda_n=n$

Proof 令$\mathbb{P}(\lambda_1,\lambda_2,\cdots,\lambda_n)$是$S_n$中型为$1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$的置换的集合，$\mathbb{P}_n$是$n$个字母$1,2,\cdots,n$的所有排列的集合

定义映射$\pi:\mathbb{P}_n\mapsto\mathbb{P}(\lambda_1,\lambda_2,\cdots,\lambda_n)$如下：$\forall p=(p_1,p_2,\cdots,p_n)\in\mathbb{P}_n$，令$\pi(p)$是这样的置换：

在排列p中,从左至右前λ_1个字母均作为长为1的轮换因子,接下来依次作为λ_2个对换因子,等等

即$\pi(p)=\underbrace{(p_1)\cdots(p_{\lambda_1})}_{\lambda_1}\underbrace{(p_{\lambda_1+1}p_{\lambda_1+2})\cdots(p_{\lambda_1+2\lambda_2-1}p_{\lambda_1+2\lambda_2})}_{\lambda_2}\cdots$显然$\pi$是满射

对任一$\alpha\in\mathbb{P}(\lambda_1,\cdots,\lambda_n),\pi^{-1}(\alpha)$中恰好含有$\prod\limits_{i=1}^{n}i^{\lambda_2}\lambda_i!$个排列

要看出这一点只要注意到两个事实：其一，一个长为i的轮换$(t_1\cdots t_i)$有i种写法：$(t_1t_2\cdots t_i),(t_2\cdots t_it_1)\cdots,(t_it_1\cdots t_{i-1})$
其二，λ_i个两两不相交的长为i的轮换是两两乘积可换的
由此可见$\left|\pi^{-1}(\alpha)\right|$只与$\alpha$的型相关，故有$|\mathbb{P}_n|=\left|\pi^{-1}(\alpha)\right||\mathbb{P}(\lambda_1,\cdots,\lambda_n)|,\quad\forall\alpha\in\mathbb{P}(\lambda_1,\cdots,\lambda_n)$
即$|\mathbb{P}(\lambda_1,\cdots,\lambda_n)|=\dfrac{n!}{\prod\limits_{i=1}^{n}i^{\lambda_2}\lambda_i!}$当$\lambda$取遍所有的型时，有$\sum\limits_{\lambda}|\mathbb{P}(\lambda_1,\cdots,\lambda_n)|=|S_n|$，由此即得到所要证的等式.

Proposition 2.22

证明$S_n=\langle(12),(13),\cdots(1n)\rangle=\langle(12),(12\cdots n)\rangle$与$A_n=\langle(123),(124),\cdots,(12n)\rangle$

Proof 1.$\langle(12),(13),\cdots(1n)\rangle\subseteq S_n$且$\forall\varphi\in S_n$将$\varphi$写为不相交的轮换乘积,其中任意一个轮换$(i_1i_2\cdots i_r)$
而我们知道$(i_1i_2\cdots i_r)=(i_1i_r)(i_1i_{r-1})\cdots(i_1i_2)$此时我们仅需证明$(i_1i_k)$可以有$\langle(12),(13),\cdots(1n)\rangle$表示
这只需注意到$(i_1i_k)=(1i_1)(1i_k)(1i_1)$

2.再考虑$H_n=\langle\{(12),(12\cdots n)\}\rangle\subseteq S_n$下说明$S_n=\langle(12),(13),\cdots(1n)\rangle\subseteq\langle(12),(12\cdots n)\rangle=H_n$
注意到$(12)(12\cdots n)=(23\cdots n)$
从而$(1n)=(n\cdots21)(23\cdots n)=(12\cdots n)^{n-1}(23\cdots n)=(12\cdots n)^{n-1}(12)(12\cdots n)\in H_n$
进而$(12\cdots n-1)=(1n)(12\cdots n)\in H_n$因此不难归纳得到（12），$\cdots,(1,n-1)$均在$H_n$中
进而$H_n=S_n$

3.对于A_n,熟知当$n\geq3$时,A_n可由所有3轮换生成这是因为如下：$\forall i,j,k,l$互异有$(ij)(ik)(jik)$且$(ij)(kl)=(ij)(jk)(jk)(kl)$
因而两个不同的对换乘积一定是三轮换乘积从而A_n中任何元素都可以写成三轮换乘积
而对于任意$j\neq k,(1jk)=(12k)(12j)(12j)$,从而同理对互不相同的$i,j,k$，有$(ijk)=(jki)=(j1i)(j1k)(j1k)=(1ij)(1kj)(1kj)$
从而任一3轮换可由（123），$\cdots,(12n)$生成，从而可知$A_n=\langle\{(123),\cdots,(12n)\}\rangle$，即证.

Theorem 2.23 (有限单群分类第二大块)

当$n \geqslant 5$时, A_n是单群.

Proof 一个群G是单群的常规办法通常是：
寻找G的生成元组A使得A中任何两个元素在G中共轭, 如果G任何非平凡正规子群N都包含A中一个元素
则必包含A的所有元素, 因此就是G本身.下面我们就按照这个思路来证明如下定理.

(I)首先, 我们证明当$n \geqslant 3$时, A_n由所有$3-$轮换生成.对于互不相同的i,j,k,l, 有 $(ij)(ik) = (jik), (ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl)$,
因此两个不同的对换的乘积一定是$3-$轮换乘积.
而A_n中任何元素都可以写成偶数个对换的乘积, 因此A_n由$3-$轮换生成.
(即我们找到了A_n的生成元组为$3-$轮换)

(II)其次, 我们证明当$n \geqslant 5$时, A_n中所有$3-$轮换是一个共轭类.
对于任意$3-$轮换(ijk), 若存在$\sigma \in A_n$使得$\sigma(i) = 1, \sigma(j) = 2, \sigma(k) = 3$, 因此$\sigma(ijk)\sigma^{-1} = (123)$.
如果$\sigma \notin A_n$即A_n不是偶置换, 则 $(45)\sigma \in A_n$, 且 $(45)\sigma(ijk)\sigma^{-1}(45) = (123)$.
因此, 所有$3-$轮换都与 (123)共轭.
(即我们找到了A_n的所有生成元组中都是共轭的)

(III)最后, 我们来证明A_n没有非平凡正规子群.只需证明若$N \triangleleft A_n, N \neq \{e\}$, 则$N$含有一个$3-$轮换.
任取$\sigma \in N, \sigma \neq (1)$, 将$\sigma$分解成不相交的轮换的乘积.我们分情况讨论.

(1)若σ的分解中含有$r-$轮换, $r \geqslant 4$, 不妨设$\sigma = (12\cdots r)\tau$, $\tau \in S_{r+1,\cdots,n}$(若$\tau \in S_r$那么跟之前的 $(1,2\cdots r)$ 合并起来即可).
由于N是正规子群, 故 $(123)\sigma(123)^{-1} \in N$, 因此 $(123)\sigma(123)^{-1}\sigma^{-1} \in N$.
另一方面, $(123)\sigma(123)^{-1}\sigma^{-1} = (123)(\sigma(1)\sigma(3)\sigma(2)) = (123)(324) = (124)$.
于是 $(124) \in N$, 即N中包含一个$3-$轮换.

(2)若σ的分解不含长度大于3的轮换, 若分解中的$3-$轮换至少有两个
不妨设$\sigma = (123)(456)\tau$, 则 $(124)\sigma(124)^{-1}(\sigma)^{-1} = (124)(253) = (12534)$.
再利用 (1)可知N中含$3-$轮换.

(3)若σ的分解中只有一个$3-$轮换, 不妨设$\underbrace{\sigma = (123)\tau}_{\text{因为根据}\sigma\text{分解}\tau\text{与}(123)\text{不相交,所以交换}}$, 其中$\tau$与 (123)可交换且$\tau^2 = (1)$, 则$\sigma^2 = (132) \in N$.

(4)若σ的分解中不含长度大于2的轮换, 即σ是不相交对换的乘积
不妨设为$\sigma = (12)(34)\tau$, 则 $(123)\sigma(123)^{-1}\sigma^{-1} = (123)(241) = (13)(24) \in N$.
进一步, 有 $(135)(13)(24)(153)(13)(24) = (135)(351) = (153) \in N$.因此, N中必含有$3-$轮换.故$N = A_n$.

Note [S_4 与 S_3 中元素]

S_4

(1)⟶ 1阶

(12), (13), (14), (23), (24), (34)⟶ 2阶

(123), (132), (124), (142), (134), (143), (234), (243)⟶ 3阶

(1234), (1243), (1324), (1342), (1423), (1432)⟶ 4阶

(12)(34), (13)(24), (14)(23).⟶ 2阶 (利用不相交可交换)

S_3:

(1) ⟶ 1阶

(12) , (13) , (23) ⟶ 2阶

(123) , (132) ⟶ 3阶

Note [A_4 与 A_3 中元素]

A_4 :

因为任意一个k循环置换 $(i_1 i_2 \cdots i_k)$ 都可以表示成$k-1$个对换的积, 即 $(i_1 i_2 \cdots i_k) = (i_1 i_k)(i_1 i_{k-1}) \cdots (i_1 i_3)(i_1 i_2)$,

所以, S_4中的对换与4 – 循环置换都是奇置换得

$$A_4 = \begin{cases} (1) \\ (123), (132), (124), (142), (134), (143), (234), (243) \\ (12)(34), (13)(24), (14)(23) \end{cases}$$

$$A_3 = \{(1), (123), (132)\}$$

Exercise 2.4 $Klein_4 = \{e, a, b, ab\}$, 由乘法表

	e	***a***	***b***	***ab***
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

(1)找出B_4的所有子群;

(2)找出S_4中与B_4同构的子群。

Proof (1)B_4的所有子群为 : $H_1 = \{e\}, H_2 = B_4, H_3 = \{e, a\}, H_4 = \{e, b\}, H_5 = \{e, ab\}$。$B_4$共有五个子群

(2) 由于两个同构的群所含元素的个数一样, 在同构映射下相对应的元素的阶相等

所以, 与B_4同构的群含有4个元素, 且除单位元外的其余3个元素都是2阶元

因为S_4中2阶元有 (12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23), 再根据运算的封闭性我们可得S_4中与B_4同构的子群有

$H_1 = \{(1), (12), (34), (12)(34)\}$,

$H_2 = \{(1), (13), (24), (13)(24)\}$,

$H_3 = \{(1), (14), (23), (14)(23)\}$,

$H_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$

2.6 陪集与拉格朗日定理

设G是一个群,H是G的一个子群,利用子群H在G中的元素之间规定一个二元关系E_L : $aE_Lb \Leftrightarrow a^{-1}b \in H$.
因为 : (1)$\forall a \in G, a^{-1}a = e \in H$,所以$aE_La$;
(2)若aE_Lb,即$a^{-1}b \in H$,由于H是G的子群,因此$\left(a^{-1}b\right)^{-1} = b^{-1}a \in H$,得$bE_La$
(3)若aE_Lb, bE_Lc,于是$a^{-1}b \in H.b^{-1}c \in H$,从而$\left(a^{-1}b\right)\left(b^{-1}c\right) = a^{-1}c \in H$,所以$aE_Lc$.
这样我们得到的二元关系E_L是一个等价关系.
根据等价关系E_L,我们可以得到一个G的分类$S = \{\bar{a} \mid a \in G\}$,其中$\bar{a} = \{x \mid x \in G, aE_Lx\}$.
对于等价类$\bar{a}$,我们有如下的说明$\bar{a} = \{x \mid x \in G, aE_Lx\} = \left\{x \mid x \in G, a^{-1}x \in H\right\} = \{x \mid x \in G, \exists h \in H, x = ah\}$.

Definition 2.30 (左陪集)

令G是一个群,$H < G$是一个子群,$a \in G$。则aH是H的一个左陪集 (由a引出)
定义为$\bar{a} = aH = \{ax \ : x \in H\}$也就是说,由$a$引出的$H$的左陪集,就是用$a$左乘了$H$中的每一个元素所得到的
特别地,$eH = H$也是一个左陪集
未来我们会知道,在H是正规子群的时候,我们可以定义陪集的乘法,而此时这个特殊的陪集eH $=$ H就会起到单位元的作用。

Note 同理可以定义右陪集的概念

Proposition 2.23 (左陪集的与原集的关系)

令G是一个有限群,$H < G$是一个子群,$a \in G.b \in G, a \neq b$
那么H与aH之间存在双射.那么进一步有$|H| = |aH|$与aH与bH之间也有双射

Proof 我们通过左乘a来定义$f : H \to aH \quad f(x) = ax$则$f$显然是一个双射.特别地,$|H| = |aH|$
再通过双射的传递性显然知道aH与bH之间有双射

Proposition 2.24 (全集的左陪集分拆与左陪集相互之间关系)

设H是G的子群,那么
(1)$G = \bigcup_{a \in G} aH$ (全体左陪集构成了全集的分拆)
(2) 对于$\forall aH, bH$,有$aH \cap bH = \varnothing$或$aH = bH$;
(3)$aH = bH \Leftrightarrow a^{-1}b \in H$;
(4)$aH = (e)\ H \Leftrightarrow a \in H$.

Proof (1) (2) 根据等价关系很容易知道或者如下说明
根据对称性,我们只须证明$aH \subset bH$即可。任取aH中的元素$ah(h \in H)$,则$ah = \left(bh_2h_1^{-1}\right)h = b\left(h_2h_1^{-1}h\right) \in bH$。这就完成了证明。
(3) $aH = bH \Leftrightarrow aH \cap bH \neq \varnothing \Leftrightarrow ah_1 = bh_2 \Leftrightarrow a^{-1}b = h_1h_2^{-1} \in H$
(4) 根据 (3) $a^{-1}e \in H \Rightarrow a \in H$

Proposition 2.25 (左陪集与右陪集存在一一对应)

设H是群G的子群,记$S_L = \{aH \mid a \in G\}, \quad S_R = \{Ha \mid a \in G\}$
则存在集合S_L到S_R的一个一一映射.

Proof 作映射$f : S_L \to S_R, \quad aH \mapsto Ha^{-1}$
先验证良定义对于$a_1H = a_2H$要验证$f(a_1H) = f(a_2H)$即验证$Ha_1^{-1} = Ha_2^{-1}$
即$\forall h_1a_1^{-1}$要存在$h^* \in H$满足$h^*a_2^{-1} = h_1a_1^{-1}$那么理应取$h^* = h_1a_1^{-1}a_2$而$a_1^{-1}a_2 \in H$这是因为$a_1H = a_2H$所以成立

说明f是单射将上述推导过程反过来,即可知f是单射.满射显然

Example 2.12元素的右陪集和左陪集未必时刻相等

设$G=S_3=\{(1),(12),(13),(23),(123),(132)\},H=\{(1),(12)\}$,则$H$是$G$的一个子群,那么,$G$关于$H$的所有左陪集为

$(1)H=(12)H=H$

$(13)H=\{(13),(123)\}=(123)H$

$(23)H=\{(23),(132)\}=(132)H$

因而,G关于H的左陪集分解为$G=H\cup(13)H\cup(23)H$

右陪集如下

$H(1)=H(12)=\{(1),(12)\}$

$H(13)=H(132)=\{(13),(132)\}$

$H(23)=H(123)=\{(23),(123)\}$

因而,G关于子群H的右陪集分解为$G=S_3=H\cup H(13)\cup H(23)$.

1.显然当群G为交换群时$aH=Ha$

2.当群G不是交换群时,对于G中的元素a来说,子群H的左陪集aH未必等于右陪集Ha

如该例子中的S_3与H就有$H(13)=\{(13),(132)\}\neq(13)H=\{(13),(123)\}$.

另外一个例子是如下的

设$G=\mathrm{GL}(2,\mathbb{C}),T$为$G$中对角矩阵构成的子群，则对$A=\begin{pmatrix}1&1\\0&1\end{pmatrix}$,$AT\neq TA$.

既然这样,那么我们就可以把G分拆成H的一系列左陪集

我们称这个由左陪集构成的集族为商集G/H，$G/H=\{a_1H,a_2H\cdots a_kH\}$

我们记这些左陪集的个数为$[G:H]$,称为H在G中的指数。

Definition 2.31 (商集与陪集的指数)

令G是一个有限群,$H<G$是一个子群

则商集G/H定义为$G/H=\{aH:a\in G\}$

我们把这个商集的大小称为H在G中的指数,记为$[G:H]$,即$[G:H]=|G/H|$

Theorem 2.24 (拉格朗日定理)

令G是一个有限群,$H<G$是一个子群,则$|G|=[G:H]|H|$则有特别地,$|H|\Big||G|$

Proof 因G是有限群,H在G中的左陪集个数必有限

假设G关于H的左陪集分解为$G=a_1H\cup a_2H\cup\cdots\cup a_kH$,其中$k=[G:H]$.

由前文得$|a_iH|=|H|$，$i=1,2,\cdots,k$,又因为左陪集分解中的各个左陪集两两不相交,因此$|G|=k\cdot|H|=[G:H]\cdot|H|$.

Corollary 2.5

设G是有限群，$K<G,H<K$，则有$[G:H]=[G:K]\cdot[K:H]$

Proof 一方面：$|G|=|G/K|\cdot|K|=|G/K|\cdot|K/H|\cdot|H|$.另一方面：$|G|=|G/H|\cdot|H|$

$\Longrightarrow|G/K|\cdot|K/H|\cdot|H|=|G/H|\cdot|H|\Longrightarrow[G:H]=[G:K]\cdot[K:H]$

Corollary 2.6

1.有限群G中每一个元素的阶都是G阶数的因数

2.素数阶的群一定为循环群且同构于$(\mathbb{Z}_p,+)$

♡

Proof 1.$\forall a\in G$,作子群$H=\langle a\rangle$,首先很显然$\langle a\rangle$的阶有限,则有$|H|=|a|$

根据$Lagrange$定理,有$|G|=[G:H]\cdot|H|=[G:H]\cdot|a|$.

2.假设$|G|=p$为素数,那么G中元素的阶要么为1要么为p

如果为1即平凡子群$\{e\}$;如果为p那么该元素就为循环生成元

Proposition 2.26 (4 阶群同构定理)

设群G的阶为4,则G在同构意义下或为循环群$\mathbb{Z}_4$,或为$Klein$四元群.

Proof 由于G为4阶群,那么由推论知G中元素的阶只可能是4的因数,即为$1,2,4$.

若G中包含4阶元a,则$\langle a\rangle$是G的4阶子群,而G中仅有4个元素,故$G=(a)$为4阶循环群由有限循环群知识知,$G\cong \mathrm{Z}_4$.

若G中不包含4阶的元素,则G中除单位元e外,还有三个元素a,b,c,它们的阶都为2.

由有限群一节中的练习得G为交换群.记$G=\{e,a,b,c\}$

由于G中消去律成立,故ab不能是a(若$ab=a$,则有$b=e$),ab也不能是b(若$ab=b$,则有$a=e$),ab也不能是e(若$ab=e=aa$,则有$a=b$)

那么只能是$ab=c$同理$ba=c$同理有$ac=ca=b$; $bc=cb=a$

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Proposition 2.27 (6 阶群同构定理)

设群G的阶数为6,那么群G要么同构于$(\mathbb{Z}_6,+)$要么同构于D_3

Proof 群G中的元素阶数只能为$1,2,3,6$

若群G中有六阶元显然G就同构于$(\mathbb{Z}_6,+)$

若群G中没有六阶元,此时群G中除了e之外的元素阶数只能为$2,3$,根据前文叙述群G的阶数为偶数那么肯定存在二阶元τ

下面断言群G中一定会有三阶元,反之若不存在三阶元σ,那么群G中只有$1,2$阶元

那么就预先构成了$\{e,a,b\}\to\{e,a,b,ab\}$, 这时不会出现ba元, 因为阶为2就有$abab=e\Rightarrow a^2bab=a\Rightarrow bab=a\Rightarrow ab=ba$

同理aba也不会出现也就是说$\{e,a,b,ab\}$是最大的群了无法再扩充下去了.矛盾

故群G中必定有$1,2,3$阶元都存在

那么预先构成了群$G=\{e,\tau,\sigma\}\to\{e,\tau,\sigma,\sigma^2\}$

这时$\sigma^2\neq\sigma$因为σ阶数原因,且$\sigma^2\neq\tau$若$\sigma^2=\tau\Rightarrow\sigma^4=\tau^2\Rightarrow\sigma^3\sigma=e\Rightarrow\sigma=e$矛盾故$\sigma^2$扩充合理

其次$\to\{e,\tau,\sigma,\sigma^2,\tau\sigma\}$这时因为$\underbrace{\tau\sigma\neq\tau,\tau\sigma\neq\sigma}_{\text{不然会有单位元}},\underbrace{\tau\sigma\neq\sigma^2}_{\text{不然相等}}$所以$\tau\sigma$扩充合理

这时$\to\{e,\tau,\sigma,\sigma^2,\tau\sigma,\sigma\tau\}$因为$\sigma\tau\neq\tau\neq\sigma\neq\sigma^2$跟上行同理,且$\sigma\tau\neq\tau\sigma$若不然根据有限群一节练习,知道$\tau\sigma$的元素阶为6与若群$G$中没有六阶元一开始假设矛盾

同理$\tau\sigma^2$对$\{e,\tau,\sigma,\sigma^2,\tau\sigma\}$扩充也合理而群$G$的阶数为6那么只能暗示$\tau\sigma^2=\sigma\tau$所以该群为$\{e,\tau,\sigma,\sigma^2,\tau\sigma,\tau\sigma^2\}$为$D_3$

Corollary 2.7 (不可交换群的元素个数限制)

若G为非交换群, 则G中至少含有6个元素, 从而说明S_3是含有元素个数最少的不可交换群 ♡

Proof

当G是1阶群时, 显然G是交换群; 当G是2阶, 3阶, 5阶群时, 由于它们是素数阶群, 知素数阶群必是循环群, 而循环群一定是交换群
所以, 当G是2阶, 3阶, 5阶群时, 也是交换群;
当G是4阶群时, 得G同构于以4为模的剩余类加群$\boldsymbol{Z}_4$或$Klein$四元群B_4, 而这两个群都是交换群, 所以G也是交换群
由上面的讨论可知非交换群至少含有6个元素。而S_3是一个含有6个元素的非交换群。

Proposition 2.28 (A_4 的所有子群与拉格朗日定理逆命题不成立例子)

找出A_4的所有子群, 且 4 阶子群为唯一的正规子群, 由此证明$Lagrange$定理的逆命题不成立
$Lagrange$定理指时是 : 有限群G时任意一个子群H时阶必是群G的阶的一个因数
但可以看出 : 对有限群G的阶数的某个因数就不一定存在子群, 使得子群的阶好是这个因数. 如$|A_4| = 12$的因数6。

Proof 设H是A_4的子群, 因为A_4为12阶群, 所以, H的阶必是12的一个因数, 即$|H| = 1, 2, 3, 4, 6, 12$
(1) 当$|H| = 1$时, 得$H_1 = \{(1)\}$
(2) 当$|H| = 12$时, 得$H_2 = A_4$
(3) 当$|H| = 2$时, 由于2是一个素数, 则H必是由某个2阶元生成的循环群
而A_4中的2阶元有3个 : $(12)(34)$, $(13)(24)$, $(14)(23)$
得A_4的2阶子群有$H_3 = \{(1), (12)(34)\}$, $H_4 = \{(1), (13)(24)\}$, $H_5 = \{(1), (14)(23)\}$

(4) 当$|H| = 3$时, 由于3也是一个素数, 则H必是由某个3阶元生成的循环群
而A_4中的3阶元有8个 : (123), (132), (124), (142), (134), (143), (234), (243)
得A_4的3阶子群有$H_6 = \{(1), (123), (132)\}$, $H_7 = \{(1), (124), (142)\}$, $H_8 = \{(1), (134), (143)\}$, $H_9 = \{(1), (234), (243)\}$,

(5)$|H| = 4$时, 由于A_4中没有4阶元, 所以, H只有与B_4同构, 由对称群与置换群一节的练习
可得S_4中与B_4同构的子群共有四个

$$N_1 = \{(1), \quad (12), \quad (34), \quad (12)(34)\},$$
$$N_2 = \{(1), \quad (13), \quad (24), \quad (13)(24)\},$$
$$N_2 = \{(1), \quad (14), \quad (23), \quad (14)(23)\},$$
$$N_4 = \{(1), \quad (12)(34), \quad (13)(24), \quad (14)(23)\}$$

而且这四个S_4的子群中只有N_4是A_4的子群, 因为 $(12), (13), (14), (23), (24), (34)$不是偶置换
得A_4的4阶子群只有$H_{10} = \{(1), (12)(34), (13)(24), (14)(23)\}$。

(6) 当$|H| = 6$时, 由于A_4中没有6阶元, H不可能是循环群, 故H只能同构于$D_3 = \{e, \tau, \sigma, \sigma^2, \tau\sigma, \tau\sigma^2\}$
其中$\tau, \tau\sigma, \tau\sigma^2$阶数为2阶.$\sigma$与$\sigma^2$阶数为3阶
而A_4中只有 $(12)\,(34)$ $(13)\,(24)$ $(14)\,(23)$ 三个为二阶元, 那么对应为$\tau, \tau\sigma, \tau\sigma^2$
且有 $(12)\,(34) \times (13)\,(24) = (14)\,(23)$ 但是$\tau, \tau\sigma, \tau\sigma^2$无论如何二个相乘都不会等于第三个, 所以没有六阶子群

(7) 当$|H| = 12$时, $H = A_4$

Proposition 2.29 (S_3 的所有子群)

S_3的所有子群：$\{(1)\}$ $\{(1),(12)\}$ $\{(1),(13)\}$ $\{(1),(23)\}$ $\{(1),(123),(132)\}$ S_3

Exercise 2.5 写出A_4关于$H=\{(1),(12)(34),(13)(24),(14)(23)\}$的左陪集分解以及右陪集分解

Proof A_4关于H的左陪集分解为$A_4=H\cup(123)H\cup(132)H$,

其中

$H=\{(1),(12)(34),(13)(24),(14)(23)\}$

$(123)H=\{(123),(134),(243),(142)\}$,

$(132)H=\{(132),(234),(124),(143)\}$;

A_4关于H的右陪集分解为$A_4=H\cup H(123)\cup H(132)$,

其中

$H=\{(1),(12)(34),(13)(24),(14)(23)\}$

$H(123)=\{(123),(243),(142),(134)\}$

$H(132)=\{(132),(143),(234),(124)\}$。

Note 下面来讲述如何求解一个群 G 关于某个子群的陪集分解算法

Proof 有限群G,其子群H

1.显然由前文知$|aH|=|H|$不管分解的形式如何多样但是个数一定为$[G:H]=\dfrac{|G|}{|H|}$

2.其次由前文知$aH=H\Leftrightarrow a\in H$

3.我们预先选择H作为第一个并集中的元素

4.在$G-H$中选择一个元素x去得到xH(这样得到的$xH\neq H$)

5.在$G-H-xH$中选择一个元素y去得到yH(这样得到的$yH\neq H\neq xH$)

6.如此往复我们每一次得到的新的zH其个数$|zH|=|H|$那么经过有限步操作最终可以结束并得到全部G

Theorem 2.25 (指数与陪集分解拓展公式)

1.设G为一群,$K<G,H<G$且$K\subseteq H\Longrightarrow[G:K]=[G:H][H:K]$

2.设G为一群,$K<G,H<G\Longrightarrow[HK:K]=[H:H\cap K]$

3.设G为一群，$K<G,H<G\Longrightarrow|HK|\cdot|H\cap K|=|H|\cdot|K|$

4.已知$H<G,K<G$则$[H:H\cap K]\leqslant[G:K]$且若$[G:K]$的指数有限，那么$[H:H\cap K]=[G:K]\Longleftrightarrow G=KH$

5.设G为一群,$H<G,K<G\Longrightarrow[G:H\cap K]\leqslant[G:H][G:K]$且取等当且仅当$G=HK$

(若$[G:H]$与$[G:K]$互素$\Longrightarrow G=HK$)

(若$[G:H]=k_1$与$[G:K]=k_2<\infty$则$\operatorname{lcm}(k_1,k_2)\,|\,[G:H\cap K]$)

6.设G为一群,$A<G,B<G\Longrightarrow g(A\cap B)=g(A)\cap g(B)$且若$[G:A][G:B]$有限那么$[G:A\cap B]$指数也有限

7.设G为一群,$K<G,H<G,\Longrightarrow|HgK|=|H|\left[K:K\cap g^{-1}Hg\right]=|K|\left[H:H\cap gKg^{-1}\right]$

且HgK可以定义等价关系从而双陪集分解了G

Proof 1.我们想要把这个性质形象地用陪集嵌套子陪集的方式来刻画,进而把这个命题作为推论

假设$G/H=\{a_iH\}_{i\in I}$,$H/K=\{b_jK\}_{j\in J}$。有没有一种可能,我们有$G/K=\{a_ib_jK\}_{i\in I,j\in J}$呢?

这里的含义是,枚举法中的这些陪集都是两两不同的。答案是肯定的。我们只要证明了这个条件,原命题就成为直接推论了。

我们要证明两件事。
第一,这些a_ib_jK枚举尽了所有K在G中的左陪集;
第二,这些a_ib_jK是两两无交的。

第一:令$aK \in G/K(a \in G)$。假设$a \in a_iH$,其中$a = a_ih(h \in H)$。
进一步假设$h \in b_jK$,故$aK = a_ihK \subset a_ib_jK$。因为左陪集要么相等,要么无交,故$aK = a_ib_jK$,这就证明了第一点
第二:假设$a_ib_jK = a_{i'}b_{j'}K$。同时右乘上H(指在集合意义上,同时右乘上H的所有元素),由于$b_j, b_{j'} \in H$到$b_jK = b_{j'}K$
这就告诉我们$b_j = b_{j'}$,这就证明了第二点
综上所述,嵌套子群的陪集也是如我们预期的那样嵌套,这样,作为推论,我们证明了原命题。

Proof 2.显然HK是hK这样陪集的并.H是$h(H \cap K)$这样陪集的并
那么$h_1K = h_2K \Longleftrightarrow h_1h_2^{-1} \in K \Longleftrightarrow h_1h_2^{-1} \in K \cap H \Longleftrightarrow h_1(H \cap K) = h_2(H \cap K)$
那么二者陪集分解的个数相同

法二:我们注意到对任意$hk = h_1k_1$,从而$h^{-1}h_1 = kk_1^{-1}$,从而有$h^{-1}h_1 = kk_1^{-1} = q \in H \cap K$,从而$h_1 = hq, k_1 = q^{-1}k$
从而对$|H||K|$中的所有元素中,可根据是否相等划为若干等价类,且每个等价类中均有$|H \cap K|$个元素,即有$|HK| = |H||K|/|H \cap K|$.

Proof 3.法一:由2.知$[H : H \cap K] = [HK : K] \leqslant [G : K]$这是显然的
此时当若$[G : K]$的指数有限,那么$[H : H \cap K] = [G : K] \Longleftrightarrow G = KH$

法二:构造映射从$[H : H \cap K]$陪集到$[G : K]$陪集的映射:$\varphi : (H \cap K)h \mapsto Kh$
则$Kh_1 = Kh_2 \Longleftrightarrow h_2h_1^{-1} \in K \Longleftrightarrow h_2h_1^{-1} \in K \cap H \Longleftrightarrow (H \cap K)h_1 = (H \cap K)h_2$
故该映射为单射,故$[H : H \cap K] \leqslant [G : K]$
若$[G : K]$的指数有限此时$[H : H \cap K] = [G : K] \Longleftrightarrow \varphi$为双射$\Longleftrightarrow G = KH$

Proof 4.
由本定理的1.我们已经有了$[G : H \cap K] = [G : H][H : H \cap K]$
所以下证$[H : H \cap K] \leqslant [G : K]$即可
这就是3.所说明的,取等号当且仅当$G = KH$

若$[G : H]$与$[G : K]$互素那么$[G : H]$与$[G : K]$都有限那么紧接着用我们刚刚证明过的$[G : H \cap K]$也有限了
进一步$[G : H \cap K] = [G : H][H : H \cap K]$
$\Longrightarrow [G : H] \mid [G : H \cap K]$同理$[G : K] \mid [G : H \cap K]$
又$[G : H]$与$[G : K]$互素$\Longrightarrow [G : H][G : K] \mid [G : H \cap K]$
又$[G : H \cap K] \leqslant [G : H][G : K]$
$\Longrightarrow [G : H \cap K] = [G : H][G : K]$
取等了故$G = HK$

若在互素的情况下还知道G的阶数有限则可以不从3.知道$G = HK$
而从$[G : H \cap K] = [G : H][G : K]$可知
$$\Longrightarrow \frac{|G|}{|H \cap K|} = \frac{|G|}{|H|} \cdot \frac{|G|}{|K|}$$
此外进一步若$|G|$有限那么根据2.我们有$|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|} = |G|$
$\Longrightarrow$由G有限故$G = AB$

只要知道若 $[G:H]=k_1$ 与 $[G:K]=k_2<\infty$
则 $[G:H]\mid[G:H\cap K]$ 且 $[G:K]\mid[G:H\cap K]\Longrightarrow \operatorname{lcm}(k_1,k_2)\mid[G:H\cap K]$

Proof 5.第一问不难得到但是结论很深刻表明交的陪集可以等价于陪集的交
第二问法一：可由上行理解轻松得到
第二问法二：可由3.的公式立马得到

Proof 6.做陪集分解 $HgK=\bigcup_{i=1}^{r}Hgk_i$ (其中 $k_i\in K$) $\Longrightarrow$ 那么我们有 $|HgK|=r\cdot|Hg|=r\cdot|H|$
其中 $Hgk_i=Hgk_j\Longleftrightarrow gk_ik_j^{-1}g^{-1}\in H\Longleftrightarrow k_ik_j^{-1}\in g^{-1}Hg\Longleftrightarrow k_ik_j^{-1}\in\left(g^{-1}Hg\cap K\right)\Longleftrightarrow\left(g^{-1}Hg\cap K\right)k_i=\left(g^{-1}Hg\cap K\right)k_j$
我们接下来想要去说明 $\left[K:K\cap g^{-1}Hg\right]=r$ 就要去说明 $K\cap g^{-1}Hg$ 在 K 中与 H 在 HgK 中是共用同一组指标的
而我们已经说明了 $Hgk_i=Hgk_j\Longleftrightarrow\left(g^{-1}Hg\cap K\right)k_i=\left(g^{-1}Hg\cap K\right)k_j$
故我们说明了 $\left(g^{-1}Hg\cap K\right)k_i\ (1\leqslant i\leqslant r)$ 是 K 中一组两两不交的陪集
故我们剩下的是 K 是否就等于这些陪集的并呢
此时 $\left(g^{-1}Hg\right)K=\left(g^{-1}Hg\right)k_1\sqcup\cdots\cdots$
$\Longrightarrow K\cap\left(g^{-1}Hg\right)K=\left[K\cap\left(g^{-1}Hg\right)k_1\right]\sqcup\cdots\cdots$
$\Longrightarrow K=\left[K\cap\left(g^{-1}Hg\right)\right]k_1\sqcup\cdots\cdots$ (这里很重要运用吸收关系)
即把 K 切实的分解为了 $\left[K\cap\left(g^{-1}Hg\right)\right]$ 的并
$\Longrightarrow\left[K:K\cap g^{-1}Hg\right]=r$
故 $|HgK|=|H|\cdot\left[K:K\cap g^{-1}Hg\right]$
同理可以证明另一边

我们来证明双陪集分解的确是存在的分解了 G 其中 $|G|=n$
首先我们认识到 $G=\bigcup_{i=1}^{n}Hg_iK$ 接下来我们需要从中弄出一些两两不交的陪集
我们下面说明 $Hg_1K\cap Hg_2K\neq\varnothing\Longleftrightarrow Hg_1K=Hg_2K$
一方面
若 $Hg_1K\cap Hg_2K\neq\varnothing$ 那么 $h_1g_1k_1=h_2g_2k_2\Longrightarrow g_1=h_1^{-1}h_2g_2k_2k_1^{-1}$
此时 $\forall hg_1k\in Hg_1K$ 我们有 $hg_1k=hh_1^{-1}h_2g_2k_2k_1^{-1}k\in Hg_2K\Longrightarrow$ 故 $Hg_1K\subseteq Hg_2K$ 同理可证另一边
$\Longrightarrow Hg_1K=Hg_2K$
另一方面是显然的
故的确可以分解为双陪集的无交并其中等价关系即 $x\sim y\Longleftrightarrow x\in HyK$

Theorem 2.26 (群陪集分割相同代表元定理)

设H是群G的指数为n的子群，证明：存在$g_1,\cdots,g_n\in G$使得$G=\bigcup_{i=1}^{n}g_iH=\bigcup_{i=1}^{n}Hg_i$.

Proof 由$H<G$，从而可知，存在G的双陪集分解，使得$G=\bigcup AgA$
而事实上我们进一步可以将每个AgA看作若干不交陪集的并，即存在$a_i,b_i\in A$使得$AgA=\bigcup Aga_i=\bigcup b_igA$
进而可得到划分的陪集均有$\left[A:A\cap gAg^{-1}\right]$个，从而我们可以考虑$AgA=\bigcup Ab_iga_i=\bigcup b_iga_iA$
其中利用了$Ab_i=a_iA=A$
从而我们对双陪集分解中的每个g，都可以选取出与g有关的b_i,a_i使得$G=\bigcup AgA=\bigcup\bigcup Ab_iga_i=\bigcup\bigcup b_iga_iA$
则考虑$g_1\cdots,g_n$选取为所有b_iga_i即可.

2.7 正规子群与商群

Definition 2.32 (正规子群与平凡正规子群)

设H是G的一个子群, 如果$\forall a \in G, aH = Ha$, 那么, 称H是G的一个正规子群 (或称正规子群), 记作$H \triangleleft G$.

对于正规子群H来说, 因为其左陪珏aH和右陪集Ha都相等, 我们就不必区分左、右陪集, 通常称为H的陪集.

任意一个群G, 单位元子群$\{e\}$与G双身都是G的正规子群.因为$\forall a \in G$, 有

$aG = G = Ga, a\{e\} = \{ae\} = \{a\} = \{ea\} = \{e\}a.$

我们称这两个正规子群为群G的平凡正规子群.

Proposition 2.30 (交换群的任何子群都是正规子群)

交换群G的任意子群H都是G的正规子群.因为$\forall a \in G$, 有$aH = \{ah \mid h \in H\} = \{ha \mid h \in H\} = Ha$.

Theorem 2.27 (正规子群的判定定理)

设H是G的子群, 则下面四个条件等价

(1)H是G的正规子群

(2)$\forall a \in G$, 有$aHa^{-1} = H$

(3)$\forall a \in G$, 有$aHa^{-1} \subseteq H$

(4)$\forall a \in G, \forall h \in H$, 有$aha^{-1} \in H$.

Proof 证明我们按照如下途径证明 : (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1).

(1) $\Rightarrow$ (2)因H是G的正规子群，故对于$\forall a \in G$有$aH = Ha$, 于是$aHa^{-1} = (aH)a^{-1} = (Ha)a^{-1} = H\left(aa^{-1}\right) = He = H$.

(2) $\Rightarrow$ (3)显然.

(3) $\Rightarrow$ (4)由于$aHa^{-1} \subseteq H$, 故$\forall a \in G, \forall h \in H$, 有$aha^{-1} \in H$.

(4) $\Rightarrow$ (1)任意取定$a \in G$, 要证$aH = Ha$.对于$\forall ah \in aH$, 由于$aha^{-1} \in H$, 则存在$h_1 \in H$, 使$aha^{-1} = h_1 \Rightarrow ah = h_1 a \in Ha \Rightarrow aH \subseteq Ha$;

另一方面, $\forall ha \in Ha$, 由于$a^{-1}ha = a^{-1}h\left(a^{-1}\right)^{-1} \in H$, 故存在$h_2 \in H$, 使$a^{-1}ha = h_2 \Rightarrow ha = ah_2 \in aH \Rightarrow Ha \subseteq aH$.

所以, 对于$\forall a \in G$, 有$aH = Ha$.从而证得H是G的正规子群。

Example 2.13 正规子群不具有传递性例子

设$G = \left\{\begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \mid r, s \in \mathbb{Q}, r \neq 0\right\}$.

则G对于矩阵的乘法运算作成一个群且$\begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} r^{-1} & -r^{-1}s \\ 0 & 1 \end{pmatrix}$

令$H = \left\{\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \mid t \in \mathbb{Q}\right\}$

容易验证H是G的一个子群.

因为$\forall \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \in G, \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \in H$, 有$\begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} r & rt+s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} r^{-1} & -r^{-1}s \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & rt \\ 0 & 1 \end{pmatrix} \in H$.

得H是G的正规子群 (这样验证正规子群要比利用其他条件方便些, 请读者自行比较).

我们有H是G的正规子群.

令$K = \left\{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z}\right\}$容易验证$K$是$H$的一个子群.

由于$\forall\begin{pmatrix}1&s\\0&1\end{pmatrix},\begin{pmatrix}1&t\\0&1\end{pmatrix}\in H$,有$\begin{pmatrix}1&s\\0&1\end{pmatrix}\begin{pmatrix}1&t\\0&1\end{pmatrix}=\begin{pmatrix}1&s+t\\0&1\end{pmatrix}=\begin{pmatrix}1&t\\0&1\end{pmatrix}\begin{pmatrix}1&s\\0&1\end{pmatrix}$
所以H是一个交换群,从而得H的任意子群必是正规子群,所以K也是H的正规子群.
但是,K不是G的正规子群.
例如,我们取$\begin{pmatrix}1&1\\0&1\end{pmatrix}\in K,\begin{pmatrix}0.5&1\\0&1\end{pmatrix}\in G$,则$\begin{pmatrix}0.5&1\\0&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}0.5&1\\0&1\end{pmatrix}^{-1}=\begin{pmatrix}1&0.5\\0&1\end{pmatrix}\notin K.$

Example 2.14 子群不是正规子群的例子

1.群$G=S_3\quad H<G\quad H=\{(1),(12)\}\quad (13)H\neq(H)(13)$

Proposition 2.31 (子群的积–子群与正规子群命题)

定义$\langle H\cup K\rangle=H\vee K$
1.$H\lhd G$且$K<G\Longrightarrow HK<G$且$KH<G$
2.$H\lhd G$且$K\lhd G\Longrightarrow HK\lhd G$且$KH\lhd G$
3.$H\lhd G$且$K\lhd G\Longrightarrow(H\cap K)\triangleleft G$
4.$H<G$且$N\lhd G\Longrightarrow H\cap N\lhd H$
5.$H<G$且$N\lhd G\Longrightarrow N\lhd HN$
6.$H<G$且$K\lhd G\Longrightarrow\langle H\cup K\rangle=H\vee K=HK=KH$且有$K$为$H\vee K$的正规子群
7.$H<G$且$K\lhd G$且$H\cap K=\{e\}\Longrightarrow H$与$K$的元素乘积可交换
该命题指出两个子群的积未必是子群但是若有一个子群变为正规子群即可,更进一步积也会变为正规子群

Proof 该命题指出两个子群的积未必是子群但是若有一个子群变为正规子群即可,更进一步积也会变为正规子群
我们在这特别指出在子群那一节我们就已经知道了两个子群的积未必是G的子群
两个子群的交一定为G子群
4.
显然$H\cap N\subset H$其次$H\cap N<H$这是因为H，N分别是子群就可以做到了
其次正规性:$\forall h\in H$和$a\in H\cap N\quad WTS:hah^{-1}\in H\cap N$
(一方面$a\in H$因为H是子群所以$hah^{-1}\in H$另一方面由N为正规子群所以$\in N$)

5.
显然$N\subset HN$首先$N<HN$因为N是子群就可以了再证正规性:$\forall hn\in HN\quad\forall n_1\in N\quad WTS:hnn_1(hn)^{-1}\in N$
$hnn_1(hn)^{-1}=\underbrace{hnn_1n^{-1}}_{\in N}h^{-1}$由$N$正规性即可

6.显然的$HK(KH)\subseteq H\vee K$
且对于$\forall x\in H\vee K$则$x=h_1k_1\cdots h_sk_s$
(事实上本来应该写为$x=t_1\cdots t_l$其中$t_i\in H$或K的形式但是我们这种手法也可以无非是可以取其中一些为单位元)
而$h_1^{-1}k_1h_1\in K$记$h_1k_1h_1^{-1}=k_1'\Longrightarrow h_1k_1=k_1'h_1$
则$x=h_1k_1\cdots h_sk_s=k_1'\cdots k_s'h_1\cdots h_s\in KH$
则$KH=(HK)=H\vee K$

Proposition 2.32

设H是G的一个正规子群,G/H表示H的所有左陪集作成的集合,即$G/H=\{aH\mid a\in G\}$
则G/H关于运算:$\forall aH,bH\in G/H,\quad (aH)(bH)=(ab)H$作成一个群.

Proof 首先我们来证明运算的定义是合理的.如果$a_1H=a_2H,\ b_1H=b_2H$那么有$a_1a_2^{-1}\in H$且$b_1b_2^{-1}\in H$
下证$a_1b_1H=a_2b_2H$即要证$a_1b_1\left(a_2b_2\right)^{-1}\in H$此时$a_1\underbrace{b_1b_2^{-1}}_{\in H}a_2^{-1}=\underbrace{a_1Ha_2^{-1}=Ha_1a_2^{-1}}_{\text{正规子群}}\in H$

1.封闭性显然
2.验证结合律$\left[\left(a_1H\right)\left(a_2H\right)\right]\left(a_3H\right)=\left[a_1a_2H\right]\left(a_3H\right)=\left(\left[a_1a_2\right]a_3\right)H=\left(a_1\right)a_2a_3H=\left(a_1H\right)\left[\left(a_2H\right)\left(a_3H\right)\right]$关键是$a$元素在$G$只能够有
3.单位元显然为$eH=H$
4.aH的逆元显然为$a^{-1}H$

Definition 2.33 (商群定义)

由群G的正规子群H的所有陪集作成的商集合G/H作成的群,叫做G关于正规子群H的商群
其代数运算为$(aH)(bH)=(ab)H,\forall aH,bH\in G/H$我们特别指出该商群是由正规子群诱导出来的

Property

因为子群H在G中的指数$[G:H]$就是H的陪集个数,即G/H中所含元素个数就是H在G中的指数,也就是说$|G/H|=[G:H]$.
当G为有限群时,根据$Lagrange$定理有$|G|=|G/H|\cdot|H|$.

Example 2.15 一般子群一般不可诱导出商群例子

S_3中
$(1)H=(12)H=\{(1),(12)\}$
$(13)H=(123)H=\{(13),(123)\}$
$(23)H=(132)H=\{(23),(132)\}$
但是$[(1)H][(13)H]=(13)H$而$[(12)H][(123)H]=(23)H$

Example 2.16 设$G=(\mathrm{Z},+),H=(m)=\{km\mid k\in\mathrm{Z}\}$,则$H$是Z的一个正规子群,$H$在Z中的陪集恰有$m$个
即商群G/H有m个元素:$H,1+H,2+H,\cdots,(m-1)+H$,其中$h+H=\{h+km\mid k\in\mathrm{Z}\}$,恰好是$h$所在的以$m$为模的剩余类$\bar{h}$,即$h+H=\bar{h}$.
所以作为集合,我们有$\mathrm{Z}_m=\mathrm{Z}/H=\mathrm{Z}/(m)$.而且以$m$为模的剩余类的运算与陪集的运算是一致的,所以,作为加群仍有$\mathrm{Z}_m=\mathrm{Z}/H=\mathrm{Z}/(m)$.

Proposition 2.33 (交换群与循环群商群的性质)

1.设G是交换群,那么G的商群仍是交换群
2.证明循环群的商群仍是循环群。

Proof 设G的商群为G/N,其中N是G的一个正规子群。$\forall aN,bN\in G/N$,则$aNbN=abN=baN=bNaN$所以,G/N是交换群

设G的商群为G/N,其中N是G的一个正规子群。$\forall xN\in G/N,x\in G$,因为G是循环群,则可设$G=(a)$
那么x可表示成a^n,从而有$xN=a^nN=(aN)^n$。由此证得G的商群G/N是由元素aN生成的循环群,即$G/N=(aN)$

Example 2.17 每一个子群都是正规子群

设G含有8个元素：$\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\pm\begin{pmatrix}i&0\\0&-i\end{pmatrix},\pm\begin{pmatrix}0&1\\-1&0\end{pmatrix},\pm\begin{pmatrix}0&i\\i&0\end{pmatrix},$(其中$i^2=-1$)

G关于矩阵乘法作成一个群，并且G的每一个子群都是正规子群。

Proof

因为结合律成立、单位元$\begin{pmatrix}1&0\\0&1\end{pmatrix}$存在，且每个矩阵都是可逆矩阵是显然的

所以，要证明G关于矩阵乘法作成一个群，关键是验证运算的封闭性这点验证即可

下面证明G的任意子群都是正规子群

因为G的单位元是E而且$-E$是2阶元，其余的6个元素$\pm A,\pm B,\pm C$都是四阶元

设H是8阶群G的子群，则H只可能是1阶子群，2阶子群，4阶子群以及8阶子群

当H分别是1阶子群和8阶时，$H=\{E\},H=G$为平凡子群，是正规子群；

当H是2阶子群时，因为素数阶群是循环群，则H是由一个2阶元生成的，而G中的2阶元只有$-E$，所以，G的2阶阶子群H只能是$\{E,-E\}$

因为E与$-E$与任何矩阵都可交换，所以，H是G的正规子群；

当H是4阶子群时，则H在G中的指数$[G:H]=2$，则可知H是G的正规子群

综上所述，G的每一个子群H都是正规子群。

我们也可以换一个观点来看待正规子群.给定G的子群H，我们定义G上元素的等价关系$aRb\Leftrightarrow a^{-1}b\in H$从而得到$G/H$.

要把G的乘法自然地诱导成G/H上的乘法就需要满足：aRb,cRd，是否一定有$acRbd$?

如果是这样，陪集空间就可以把G上的运算继承下来.为此我们引入比等价关系更进一步的二元关系一一同余关系.

Definition 2.34 (同余关系)

设集合A中有二元运算$*$，如果A的一个等价关系R在该运算下仍然保持，即对任意$a,b,c,d\in A,aRb,cRd\Longrightarrow(a*c)R(b*d)$

则称R为A关于运算$*$的一个同余关系.此时，a所在的等价类$\bar{a}$，也叫作a的同余类.

显然同余关系是一个等价关系可以来划分

Theorem 2.28

设G是群，$H<G$，则下列条件等价：

(1)$H\triangleleft G$;

(2)对任意$g\in G,gH=Hg$;

(3)对任意$a,b\in G,aH\cdot bH=abH$.这里$aH\cdot bH=\{ah_1bh_2\mid h_1,h_2\in H\}$.

Proof (1) $\Rightarrow$ (2).因$H\triangleleft G$，故对任意$g\in G,h\in H$，有$gh=ghg^{-1}g\in Hg$;　$hg=gg^{-1}hg\in gH$.故$gH=Hg$.

(2) $\Rightarrow$ (3).由 (2)有$Hb=bH$，故$aH\cdot bH=a(Hb)H=a(bH)H=(ab)HH=abH$.

(3) $\Rightarrow$ (1).已知$H<G$，对任意$g\in G,h\in H$，由 (3)可得$ghg^{-1}=ghg^{-1}e\in gH\cdot g^{-1}H=gg^{-1}H=eH=H$.因此$H\triangleleft G$.

由上述定理知，当且仅当H是G的正规子群

任两个左陪集的乘积一定是一个左陪集，并且乘积的代表元就是原来两个左陪集代表元的乘积.

于是我们可以在左陪集空间G/H上定义乘法$aH\cdot bH=abH$.

Theorem 2.29

设G是群，$H\triangleleft G$，则G/H对上述运算构成一个群，称为G对H的商群.

Proof 因为H是G的正规子群，根据前面的讨论，上面的运算是合理的.

又对任意$aH, bH, cH \in G/H$有$(aH \cdot bH) \cdot cH = abH \cdot cH = (abc)H = aH \cdot (bc)H = aH \cdot (bH \cdot cH)$.
于是,结合律成立.其次,$eH = H$是这一运算的左么元,因为对任意$aH \in G/H$,有$eH \cdot aH = (ea)H = aH$.
再次,G/H中任一元aH有左逆元$a^{-1}H$,因为$a^{-1}H \cdot aH = \left(a^{-1}a\right)H = eH$,所以,左陪集空间$G/H$构成一个群.

Theorem 2.30 (群同态下正规子群的性质)

设$f: G \to G'$是一个群同态映射,且$H \triangleleft G, H' \triangleleft G'$,那么
(1)$f^{-1}(H') \triangleleft G$
(2)f为满同态时,$f(H) \triangleleft G'$

Proof 由前文知:$f^{-1}(H') < G, f(H) < G'$,因此只需证明正规性
(1)$\forall x \in G, a \in f^{-1}(H')$,即$f(a) \in H'$,所以$f\left(xax^{-1}\right) = f(x)f(a)f\left(x^{-1}\right) = f(x)f(a)[f(x)]^{-1}$,其中$f(x) \in G'$
因为H'是G'的正规子群,从而有$f(x)f(a)[f(x)]^{-1} \in H'$,得$xax^{-1} \in f^{-1}(H')$。证得$f^{-1}(H') \triangleleft G$
(2)$\forall x' \in G', a' \in f(H)$,则存在$a \in H, x \in G, f(x) = x', f(a) = a'$,由于$(x')\, a'\, (x')^{-1} = f(x)f(a)[f(x)]^{-1} = f\left(xax^{-1}\right)$
因为H是G的正规子群,从而有$xax^{-1} \in H$,即$(x')\, a'\, (x')^{-1} = f\left(xax^{-1}\right) \in f(H)$.证得则$f(H)$是$G'$的正规子群。

Corollary 2.8

群G, $H < G$ $H' < G'$ $f: G \to G'$
那么$Kerf \triangleleft H$

♡

Example 2.18 同态不是满同态正规性无法传递例子

设$f: G \to G'$是群满同态,N是G的不变子群
举例说明,如果f不是满射的时候,$f(N)$不一定是G'的不变子群。
例如,取 G = $S_3, H = A_3, G' = S_4, f(x) = x \in S_4$ $(x \in S_3)$,则A_3是S_3的不变子群,但是 f $(A_3) = A_3$却不是S_4的不变子群。

2.8 共轭类，中心化子等

Definition 2.35 (共轭类与共轭子群)

设H是群G的一个子群

(1)对于每一个$a\in G$,集合aHa^{-1}是一个G的子群 (称它为H的共轭子群),并且$H\cong aHa^{-1}$

(2)设A,B是群G中的两个子集,若存在$g\in G$使得$gAg^{-1}=B$则称A和B共轭

不难看看出共轭关系是等价关系,每个等价类被称为共轭类

Proof (1)先证aHa^{-1}是一个G的子群。$\forall ah_1a^{-1},ah_2a^{-1}\in aHa^{-1}$

有$\left(ah_1a^{-1}\right)\left(ah_2a^{-1}\right)=a\left(h_1h_2\right)a^{-1}\in aHa^{-1}\qquad \left(ah_1a^{-1}\right)^{-1}=ah_1^{-1}a^{-1}\in aHa^{-1},$

所以,aHa^{-1}是一个G的子群

再证$H\cong aHa^{-1}$

作映射 $f:\mathrm{H}\to\mathrm{Ha}^{-1},\quad h\mapsto aha^{-1}$,易知$f$是一个一一映射

f保持运算,因为$\forall h_1,h_2\in H$,有$f\left(h_1h_2\right)=a\left(h_1h_2\right)a^{-1}=\left(ah_1a^{-1}\right)\left(ah_2a^{-1}\right)=f\left(h_1\right)f\left(h_2\right)$

Definition 2.36 (正规化子，中心化子，中心)

设M是群G的子集.则

1.令$N_G(M)=\left\{g\in G\mid gMg^{-1}=M\right\}$是$G$的子群,叫做$M$的正规化子.

2.令$C_G(M)=\left\{g\in G\mid g^{-1}ag=a,\forall a\in M\right\}=\{g\in G\mid ag=ga,\forall a\in M\}$;这也是$G$的子群,叫做$M$的中心化子.

由于$g^{-1}ag=a$相当于$ag=ga$,从而$C_G(M)$即是G中与M中每个元素均可换的元素全体.

3.因此$C_G(G)$中元素就是与G中每个元素均可交换的那些元素,这叫做G的中心元素而子群$C(G)=C_G(G)$叫做G的中心.

Corollary 2.9

1.G为阿贝尔群$\Longleftrightarrow G=C(G)$.所以,$C(G)$的大小反映了群$G$的交换性程度.

2.显然$C_G\lhd G$

3.又由定义知$C_G(M)<N_G(M)$.并且对单个元素集$a\in G,C_G(a)=N_G(a)$.

♡

Theorem 2.31 (共轭与中心化与正规化联系)

1.设M是群G的子集,则与M共轭的子集个数等于$[G:N_G(M)]$.(若$M<G$那么M的共轭子群个数即为$[G:N_G(M)]$)

2.特殊地设$a\in G$,则与a共轭的元素个数等于$[G:N_G(a)]=[G:C_G(a)]$

3.若$H<G$那么不仅有$N_G(H)<G$且$H\triangleleft N_G(H)$;

4.$H\triangleleft G\Longleftrightarrow N_G(H)=G$.

Proof 证明与M共轭的子集有形式$g^{-1}Mg(g\in G)$.但是

$$\begin{aligned}g^{-1}Mg=g'^{-1}Mg'&\Leftrightarrow g'g^{-1}Mgg'^{-1}=M\\&\Leftrightarrow gg'^{-1}\in N_G(M)\\&\Leftrightarrow N_G(M)g=N_G(M)g'.\end{aligned}$$

从而M的共轭子集数等于G对$N_G(M)$的陪集个数.证毕.

Definition 2.37 (自然同态)

给定G的正规子群H,即$(H \triangleleft G)$则自然同态$\pi: G \to G/H \quad g \mapsto gH$

1.π是满同态

2.$\mathrm{Ker}\pi = H$

Proof 1.满同态显然因为G/H元素是陪集自然分拆了整个G

2.$Ker\pi = \{g: \ g \in G且gH = eH = H\} = \{g: \ g \in G, g \in H\} = H$

Proposition 2.34

设G是有限群,H是G的n阶子群,如果H是G仅有的一个n阶子群,则H是G的正规子群

Proof 由正规子群的判定定理得到一个子群是正规子群当且仅当其共轭群是其自己

但根据我们上文已经知道了一个子群的共轭子群与其自身同构

因而只有一个n阶子群所以其共轭子群是自己所以为正规子群

✍ **Exercise 2.6** 在S_4中,求出所有分$H = \{(1), (123), (132)\}$共轭的子群

Definition 2.38 (内自同构群, 外自同构群)

设G为群,$a \in G$,定义映射 $\mathrm{Ad}_a: G \to G$为 $\mathrm{Ad}_a(g) = aga^{-1}, \quad \forall g \in G$,则

1.$\mathrm{Ad}_a \in \mathrm{Aut}(G)$,称为由$a$决定的内自同构或者说由 a 诱导的共轭映射.

2.记 $\mathrm{Inn}(G) = \{\mathrm{Ad}_a \mid a \in G\}$,则 $\mathrm{Inn}(G)$为 $\mathrm{Aut}(G)$的正规子群,称为G的内自同构群.

3.商群 $\mathrm{Aut}(G)/\mathrm{Inn}(G)$称为$G$的外自同构群,记为$OutG$.

4.内自同构群 $\mathrm{Inn}(G)$的一个性质：$\mathrm{Inn}(G) \cong G$(若$Ker\psi = C(G)$则$\mathrm{Inn}(G) \cong G/C(G)$)

其中具有如下性质：$\mathrm{Ad}_{ab} = \mathrm{Ad}_a\mathrm{Ad}_b \quad (\mathrm{Ad}_a)^{-1} = \mathrm{Ad}_{a^{-1}} \quad Inn(G)$ 中幺元为 $\mathrm{Ad}_e = id$

且若G为交换群那么$InnG = \{\mathrm{Ad}_a \mid a \in G\} = \{id\}$

Proof 1°首先,对任意$a, b, c \in G$,有 $\mathrm{Ad}_a\mathrm{Ad}_b(c) = a\left(bcb^{-1}\right)a^{-1} = (ab)c(ab)^{-1} = \mathrm{Ad}_{ab}(c)$.因此 $\mathrm{Ad}_a\mathrm{Ad}_b = \mathrm{Ad}_{ab}$.(封闭性)

2°于是 $\mathrm{Ad}_{a^{-1}}\mathrm{Ad}_a = \mathrm{Ad}_a\mathrm{Ad}_{a^{-1}} = \mathrm{Ad}_e = \mathrm{id}$.因此 Ad_a是双射,其逆是 $\mathrm{Ad}_{a^{-1}}$.

3°其次,对任意$g, h \in G$,有 $\mathrm{Ad}_a(gh) = agha^{-1} = aga^{-1}aha^{-1} = \mathrm{Ad}_a(g)\mathrm{Ad}_a(h)$

因此 $\mathrm{Ad}_a \in \mathrm{Aut}(G)$.(2°3°)

4°进一步,$\mathrm{Ad}_a\left(\mathrm{Ad}_b\right)^{-1} = \mathrm{Ad}_a\mathrm{Ad}_{b^{-1}} = \mathrm{Ad}_{ab^{-1}} \in \mathrm{Inn}(G)$.

因此 $\mathrm{Inn}(G) < \mathrm{Aut}(G)$.

又对任意$\varphi \in \mathrm{Aut}(G), a, g \in G$,有$\varphi\mathrm{Ad}_a\varphi^{-1}(g) = \varphi\left(a\varphi^{-1}(g)a^{-1}\right) = \varphi(a)g\varphi(a)^{-1} = \mathrm{Ad}_{\varphi(a)}(g)$.

所以$\varphi\mathrm{Ad}_a\varphi^{-1} = \mathrm{Ad}_{\varphi(a)} \in \mathrm{Inn}(G)$.故 $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$.

设$\psi: G \to \mathrm{Inn}(G), a \mapsto T_a$.直接验证知$\psi$是双射，有$\psi(a) = T_a$，则$\psi(ab) = T_{ab} = T_aT_b = \psi(a)\psi(b)$，所以$G \cong \mathrm{Inn}(G), \mathrm{Inn}(G) \cong G$

且容易知道$Ker\psi = C(G) = \{a \in G \mid \ a与G中任一元均可交换\}$

Corollary 2.10 (正规子群的等价定义)

1.群G的子群H是正规子群当且仅当H是G到某个群的一个同态的核.

2.经过上文我们知道：一个子群是正规子群当且仅当其共轭子群是其自身

3.$H < G$那么H是G的正规子群 $\Longleftrightarrow$ H是G中一些共轭类的并

4.$H \lhd G \Longleftrightarrow H$的正规化子$N_G(H) = G$
5.H在$Inn(G)$的作用下不变

Example 2.19 商群同构无法在上层同构下传递例子

举例说明下面的命题不正确：设G, G'是群，$N \triangleleft G, N' \triangleleft G'$，且有$G \simeq G', N \simeq N'$，则必有$G/N \simeq G'/N'$.

Proof 例如$\mathbb{Z}_2 \otimes \mathbb{Z}_4/\mathbb{Z}_2$可能等于$\mathbb{Z}_4$可能等于$\mathbb{Z}_4$

Example 2.20 $\mathrm{Inn}(G) \neq \mathrm{Aut}(G)$ 例子

G为$(\mathbb{Z}, +)$整数加群中因为$\mathbb{Z}$为交换群所以$\mathrm{Inn}(G) = \{id\}$但是$\mathrm{Aut}(G)$中至少有$\pm id$

2.9 同态基本定理

Theorem 2.32 (群同态基本定理)

设f是群G到G'的一个同态映射

令$N=\mathrm{Ker}f$, 则存在G/N到G'的唯一的单同态f^*, 使得$f=f^*\circ\psi$, 其中ψ是G到G/N的自然同态.

Proof 令$f^*:\ G/Kerf\to G'\quad aKerf\mapsto f(a)$

(I) : well – definied : 任意取$a_1\mathrm{Ker}f=a_2\mathrm{Ker}f\quad$ WTS : $f(a_1)=f(a_2)$

有$a_1^{-1}a_2\in Kerf\Rightarrow f\left(a_1^{-1}a_2\right)=e'\Longrightarrow f(a_1)^{-1}f(a_2)=e'\Longrightarrow f(a_2)=f(a_1)$

(II) : f^*为单射即$well-definied$的逆过程

(III) : f^*为同态 WTS : $f^*(a_1Kerf\cdot a_2Kerf)=f^*(a_1Kerf)f^*(a_2Kerf)$

$LHS=f(a_1a_2)=f(a_1)f(a_2)=f^*(a_1Kerf)f^*(a_2Kerf)=RHS$

(IV) : 验证$f=f^*\circ\psi$此时$f^*\circ\psi(a)=f^*(aKerf)=f(a)$

(V) : 唯一性 : 假设存在$g\quad g:\ G/Kerf\to G'\quad aKerf\mapsto f(a)$也满足$f=g\circ\psi$

那么$f(a)=g\circ\psi(a)=g(aKerf)$与$f^*$映射法则一致

Theorem 2.33 (群同构第一基本定理)

令$f:G\to G'$是一个群同态

1.$\ker(f)\triangleleft G$, 且G在 $\ker(f)$上的商群同构于 $\mathrm{im}(f)$, 即$G/\ker(f)\simeq\mathrm{im}(f)$

2.特别地, 若f是满同态, 则$G/\ker(f)\simeq G'$

3.若f是单同态, 则$G/\{e\}\simeq G\simeq\mathrm{im}(f)$

4.若G是有限群, 则$\dfrac{|G|}{|\ker(f)|}=|\mathrm{im}(f)|$

Proof

法一 : 根据同态基本定理 : 由于f为满射, 而由$f^*\circ\psi=f$, 而f为满射 $\Rightarrow$ f^*满射又且为单射得f是同构映射, 所以$G/\mathrm{Ker}f\xrightarrow{f^*}G'$.

法二 :

首先$Kerf\lhd G$前文已经证明了

接下来, 我们要找到一个从商群$G/\ker(f)$到像集 $\mathrm{im}(f)$的同构映射

我们称这个映射叫$\tilde{f}:G/\ker(f)\to\mathrm{im}(f)$, 对于$a\in G$, 定义为$\tilde{f}(a\ker(f))=f(a)$

为了方便起见，在不会引起歧义的情况下，我们令$N=\ker(f)$, 也即$\tilde{f}(aN)=f(a)$

考虑到陪集代表元的不唯一性, 我们要证明良定义性。假设$aN=a'N$, 或$a^{-1}a'\in N$, 只须证明$f(a)=f(a')$

而这是因为$f(a')=f\left(aa^{-1}a'\right)=f(a)f\left(a^{-1}a'\right)=f(a)e'=f(a)$这就证明了良定义性。

接下来, 我们要证明$\tilde{f}$既是同态, 也是双射 (单射 + 满射)

同态 : 令$a,b\in G$, 则$\tilde{f}(aN)=f(a)$, $\tilde{f}(bN)=f(b)$, 而$\tilde{f}((aN)(bN))=\tilde{f}(abN)=f(ab)=f(a)f(b)=\tilde{f}(aN)\tilde{f}(bN)$

这就证明了$\tilde{f}$是一个同态

单射：只须证明 $\ker(\tilde{f})=\{N\}$。假设$\tilde{f}(aN)=e'$, 则根据定义, $f(a)=e'$, 故$a\in\ker(f)=N$, 所以$aN=N$, 这就证明了$\tilde{f}$是一个单射

满射 : 令$a'\in\mathrm{im}(f)$, 取$a\in G$使得$a'=f(a)$。因此, $\tilde{f}(aN)=f(a)=a'$, 这就证明了$\tilde{f}$是一个满射

综上所述, $\tilde{f}$是一个从商群$G/\ker(f)$到像集 $\mathrm{im}(f)$的同构。作为结论, $G/\ker(f)\simeq\mathrm{im}(f)$

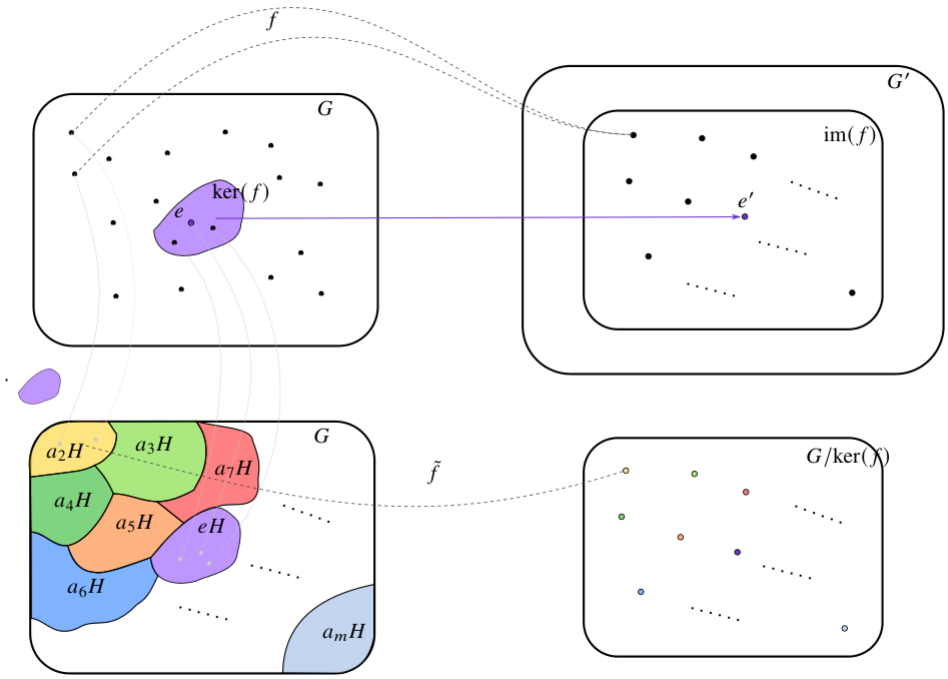


图 2.1: 群同构第一定理示意图

Corollary 2.11

这个定理告诉我们：一个群G的同态象 Imf与G的商群$G/\mathrm{Ker}f$在同构意义下是同一个群.
而商群与正规子群是可以相互确定的，因此对于一个群G来说，找出群G的所有正规子群，就可以作出G所有商群
从而可得在同构意义下G的所有同态象.
由此我们也看到，两个群之间的任一个满同态都可以看作一个群到某一个商群上的自然同态；
要找出一个群G的所有同态像，就相当于找出G的所有的商群，也就相当于找出G的所有的正规子群.

Theorem 2.34 (同构第二基本定理)

设f是群G到群G'的满同态，$N = \mathrm{Ker}f$，则
(1)f建立了G中包含$N = Kerf$的子群与G'中子群间的双射；
(2)f把正规子群对应到正规子群；
(3) 对任意的 Ker$f \subset H_1, H_2 \subset G$，则$H_1 < H_2 \Longleftrightarrow \varphi(H_1) < \varphi(H_2)$
(4) 设 Ker$f \subset H < G$则 $[G : H] = [G' : \varphi(H)]$
(5) 若$H \triangleleft G, N \subseteq H$，则$G/H \simeq G'/f(H)$.

Proof

(1)首先，对任何G中包含N的子群K，$f(K)$是G'的子群，则f建立了G中包含N的子群的集合到G'中子群的集合的一个映射$K \mapsto f(K)$.仍
下面我们证明这是双射.
对任何G'的子群H'，考虑H'的完全原像$f^{-1}(H') = \{g \in G \mid f(g) \in H'\}$
则容易验证$f^{-1}(H')$是G的包含N的子群，而且$f\left(f^{-1}(H')\right) = H'$.
因此上面的映射是满射.
此外，如果H_1, H_2是G中两个包含N的子群，且$f(H_1) = f(H_2)$
则对任何$h_1 \in H_1$，$f(h_1) \in f(H_2)$，因此存在$h_2 \in H_2$使得$f(h_1) = f(h_2)$
于是$f(h_2)^{-1} f(h_1) = e' \Rightarrow f\left(h_2^{-1}h_1\right) = e' \Rightarrow h_2^{-1}h_1 \in N \subseteq H_2$又因为$h_2^{-1} \in H_2$因此$h_1 \in H_2$，故$H_1 \subseteq H_2$.同理$H_2 \subseteq H_1$.因此$H_1 = H_2$.
这说明上述映射是单射，因此是双射.

(2)由上一节即可知道

(3)由 (2)知$f(H)$是G'的正规子群.
设π'为G'到$G'/f(H)$的自然同态,考虑G到$G'/f(H)$的映射$\pi'\circ f$
显然$\pi'\circ f$是满同态.(满同态复合一个满同态)
又 $\mathrm{Ker}\,(\pi'\circ f)=f^{-1}\left(\pi^{-1}\left(e'f(H)\right)\right)=f^{-1}(f(H))$,那么我们有$f^{-1}\left(f\left(H\right)\right)\supset H$当单射时取等
因$N\subseteq H$,(这是因为$f\left(H\right)$是G'正规子群自然包含了e'那么$f^{-1}\left(f\left(H\right)\right)$自然包含了$Kerf$)
那么由 (1) 问知道, 由 (1)建立的双射知 $\mathrm{Ker}\,(\pi'\circ f)=H$.
故由同态基本定理得$G/H\simeq G'/f(H)$.

Corollary 2.12 (群同构第二基本定理应用在自然满同态上)

设G是群,$N\triangleleft G$,π是G到G/N的自然满同态,则
1.π建立了G中包含N的子群与G/N的子群间的双射
2.而且把正规子群对应到正规子群.
3.又若$H\triangleleft G,N\subseteq H$,则$G/H\simeq(G/N)/(H/N)$.

Theorem 2.35 (群同构第三定理)

$\varphi:\ G\to G'$的群满同态, $N=Ker\varphi\lhd G,\quad H<G$
1.HN是H在φ下的像$\varphi\left(H\right)$的完全原像且有$\varphi\left(H\right)=\varphi\left(HN\right)$
2.$H/H\cap N\cong\varphi\left(H\right)=\varphi\left(HN\right)$

Proof 1.我们已经有$N\lhd HN<G$此时$\varphi\left(HN\right)=\{\varphi\left(hn\right):\ \ h\in H,n\in N\}\overset{N=Ker\varphi}{=\!=\!=}\{\varphi\left(h\right):\ \ h\in H\}=\varphi\left(H\right)$
由同构第二基本定理我们知道:φ建立了G中包含N的子群与G'中的子群的一一对应
那么HN就与$\varphi\left(H\right)$建立了对应1.就证毕
2.考虑$\varphi|_H:\ H\to G'$ 此时$Ker\left(\varphi|_H\right)=\{h\in H:\ \ \varphi|_H\left(h\right)=e'\}=H\cap N$
我们知道了$\varphi|_H:H\to\varphi\left(HN\right)$的满同态映射由同构第一基本定理有$H/H\cap N\cong\varphi\left(HN\right)=\varphi\left(H\right)$

Corollary 2.13 (群同构第三定理应用在自然满同态上)

设G是群,$N\triangleleft G$,π是G到G/N的自然满同态,$H<G$
(1)$N\lhd HN<G$且$HN=\pi^{-1}(\pi(H))$即HN是H在映射π下的像集合$\pi(H)$的完全原像$\pi^{-1}(\pi(H))$.
(2)$\mathrm{Ker}\,(\pi|_H)=H\cap N$,从而 $(H\cap N)\triangleleft H$.
(3)$HN/N\simeq H/(H\cap N)$.

Proof (1)$N\lhd HN<G$由上一节前文显然
此外,显然有$N\subseteq HN$,又$\pi(HN)=\{hnN\mid h\in H,n\in N\}=\{hN\mid h\in H\}=\pi(H)$
即G中包含同态核N的子群HN在π映射下的像集是G/N中的子群$\pi(H)$.于是由同构第二定理 (1) 结论知道
π建立的双射就把HN对应到$\pi(H)$,从而$HN=\pi^{-1}(\pi(H))$.

(2)考虑群同态 $\pi|_H:H\to G/N$,有 $\mathrm{Ker}\,(\pi|_H)=\{h\in H|\ \ \pi|_H(h)=\pi(N)\}=H\cap N$.

(3)由 (1)知$\pi(H)=\pi(HN)=HN/N$,所以π是H到HN/N的满同态映射.
由同构第一基本定理有$H/(\mathrm{Ker}\,(\pi|_H))\simeq HN/N$而由 (2),$\mathrm{Ker}\,(\pi|_H)=H\cap N$,故$HN/N\simeq H/(H\cap N)$.

Proposition 2.35

设H,K是G的两个不变子群则$HK,H\cap K$都是G的不变子群,且

$HK/K\cong H/(H\cap K)$.

$HK/H\cong K/(H\cap K)$.

Proof 正规子群与商群的合理性由上一节很显然知道

作$f:H\to HK/K,\quad h\mapsto hK,\forall h\in H$.

则f是H到HK/K的映射.

$\forall(hk)K\in HK/K$.由于$k\in K$,则有$(hk)K=hK$,在f下有原象h,使得$f(h)=hK=(hk)K$,那么f为满射.易见f保持运算.

即为满同态

再根据同构第一基本定理,我们只需证明 Ker$f=H\cap K$即可.

$$\begin{aligned}\text{Ker}f&=\{h\mid h\in H,f(h)=K\}\\ \text{因}\qquad&=\{h\mid h\in H,hK=K\}\\ &=:h\mid h\in H,h\in K\}=H\cap K.\end{aligned}$$

所以.同理可得 $HK/K\cong H/(H\cap K)$.

$HK/H\cong K/(H\cap K)$.

在上面的定理中,如果只要求一个同构式成立,则定理的条件可放宽些.

例如,设K是群G的不变子群,H是G的子群,也有$HK/K\cong H/(H\cap K)$.

✍ **Exercise 2.7** 设$N\triangleleft G,K\triangleleft$ G,如果$N\cap K=\{e\},(N\cup K)=G$,则$G/N\cong K$

Proof 我们有知:$G=NK$,则$G/N=NK/N,\quad K/N\cap K=K/\{e\}=K$

根据上个命题有$NK/N\cong K/N\cap K$得$G/N\cong K$。

Proposition 2.36

If $N_1\lhd G_1$ and

2.10 Category——A little Comment

Definition 2.39 (Category)

A category consists of

- a collection of objects $X, Y, Z, \ldots$
- a collection of morphisms $f, g, h, \ldots$

so that:

- Each morphism has specified domain and codomain objects; the notation $f : X \to Y$ signifies that f is a morphism with domain X and codomain Y.
- Each object has a designated identity morphism $1_X : X \to X$.
- For any pair of morphisms f, g with the codomain of f equal to the domain of g, there exists a specified composite morphism[4] gf whose domain is equal to the domain of f and whose codomain is equal to the codomain of g, i.e.,:

$$f : X \to Y, \quad g : Y \to Z \quad \rightsquigarrow \quad gf : X \to Z.$$

This data is subject to the following two axioms:

- For any $f : X \to Y$, the composites $1_Y f$ and $f 1_X$ are both equal to f.
- For any composable triple of morphisms f, g, h, the composites $h(gf)$ and $(hg)f$ are equal and henceforth denoted by hgf.

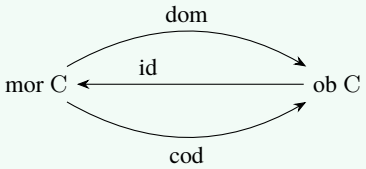
$$f : X \to Y, \quad g : Y \to Z, \quad h : Z \to W \quad \rightsquigarrow \quad hgf : X \to W.$$

That is, the composition law is associative and unital with the identity morphisms serving as two-sided identities.

Definition 2.40 (Small Category with Locally Small)

A category is **small** if it has only a set's worth of arrows.

Actually, a small category has only a set's worth of objects. If C is a small category, then there are functions



that send a morphism to its domain and its codomain and an object to its identity.

A category is *locally small* if between any pair of objects there is only a set's worth of morphisms.

It is traditional to write

$$C(X, Y) \quad \text{or} \quad \mathrm{Hom}(X, Y) \tag{2.1}$$

for the set of morphisms from X to Y in a locally small category C.[14] The set of arrows between a pair of fixed objects in a locally small category is typically called a *hom-set*, whether or not it is a set of "homomorphisms" of any particular kind. Because the notation (1.1.8) is so convenient, it is also adopted for the collection of morphisms between a fixed pair of objects in a category that is not necessarily locally small.

Definition 2.41 (Monomorphism,Epimorphism,Isomorphism)

An **isomorphism** in a category is a morphism $f\colon X \to Y$ for which there exists a morphism $g\colon Y \to X$ so that $gf = 1_X$ and $fg = 1_Y$. The objects X and Y are **isomorphic** whenever there exists an isomorphism between X and Y, in which case one writes $X \cong Y$.

An **endomorphism**, i.e., a morphism whose domain equals its codomain, that is an isomorphism is called an **automorphism**.

A morphism $f : x \to y$ in a category is

(i) a **monomorphism** if for any parallel morphisms $h, k : w \rightrightarrows x$, $fh = fk$ implies that $h = k$; or

(ii) an **epimorphism** if for any parallel morphisms $h, k : y \rightrightarrows z$, $hf = kf$ implies that $h = k$.

Definition 2.42

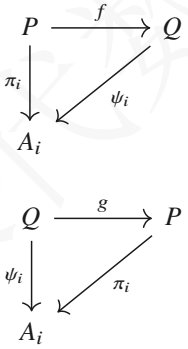
Let C be a category and $\{A_i\}_{i\in I}$ a family of objects of C. A **product** for the family $\{A_i \mid i \in I\}$ is an object P of C together with a family of morphisms $\{\pi_i : P \to A_i \mid i \in I\}$ such that for any object B and family of morphisms $\{g_i : B \to A_i \mid i \in I\}$, there is a unique morphism $\varphi : B \to P$ such that $\pi_i \circ \varphi = g_i$ for all $i \in I$.

Theorem 2.36

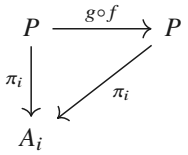
If $(P, \{\pi_i\})$ and $(Q, \{\psi_i\})$ are both products of the family $\{A_i \mid i \in I\}$ of objects of a category C, then P and Q are equivalent.

Proof

Since P and Q are both products, there exist morphisms $f : P \to Q$ and $g : Q \to P$ such that the following diagrams are commutative for each $i \in I$:



Composing these gives for each $i \in I$ a commutative diagram:



Thus $g \circ f : P \to P$ is a morphism such that $\pi_i \circ (g \circ f) = \pi_i$ for all $i \in I$. But by the definition of product there is a unique morphism with this property. Since the map $1_P : P \to P$ is also such that $\pi_i \circ 1_P = \pi_i$ for all $i \in I$, we must have $g \circ f = 1_P$ by uniqueness. Similarly, using the fact that Q is a product, one shows that $f \circ g = 1_Q$. Hence $f : P \to Q$ is an equivalence.

Definition 2.43 (Coproduct)

A **coproduct** (or **sum**) for the family $\{A_i \mid i \in I\}$ of objects in a category C is an object S of C, together with a family of morphisms $\{t_i : A_i \to S \mid i \in I\}$ such that for any object B and family of morphisms $\{\psi_i : A_i \to B \mid i \in I\}$, there is a unique morphism $\psi : S \to B$ such that $\psi \circ t_i = \psi_i$ for all $i \in I$.

Theorem 2.37

If $(S, \{t_i\})$ and $(S', \{\lambda_i\})$ are both coproducts for the family $\{A_i \mid i \in I\}$ of objects of a category C, then S and S' are equivalent.

Definition 2.44

A **concrete category** is a category C together with a function σ that assigns to each object A of C a set $\sigma(A)$ (called the **underlying set** of A) in such a way that:

1. every morphism $A \to B$ of C is a function on the underlying sets $\sigma(A) \to \sigma(B)$;
2. the identity morphism of each object A of C is the identity function on the underlying set $\sigma(A)$;
3. composition of morphisms in C agrees with composition of functions on the underlying sets.

Note

Concrete categories are frequently useful since one has available not only the properties of a category, but also certain properties of sets, subsets, etc. Since in virtually every concrete category we are interested in, the function σ assigns to an object its underlying set in the usual sense (as in the examples above), we shall denote both the object and its underlying set by the same symbol and omit any explicit reference to σ. There is little chance of confusion since we shall be careful in a concrete category C to distinguish morphisms of C (which are by definition also functions on the underlying sets) and maps (functions on the underlying sets, which may not be morphisms of C).

Definition 2.45

Let F be an object in a concrete category C, X a nonempty set, and $i : X \to F$ a map (of sets). F is **free on the set** X provided that for any object A of C and map (of sets) $f : X \to A$, there exists a unique morphism of C, $\overline{f} : F \to A$, such that $\overline{f} \circ i = f$ (as a map of sets $X \to A$).

Theorem 2.38

If C is a concrete category, F and F' are objects of C such that F is free on the set X and F' is free on the set X' and $|X| = |X'|$, then F is equivalent to F'.

Proof Since F, F' are free and $|X| = |X'|$, there is a bijection $f : X \to X'$ and maps $i : X \to F$ and $j : X' \to F'$. Consider the map $jf : X \to F'$. Since F is free, there is a morphism $\varphi : F \to F'$ such that the diagram:

$$\begin{array}{ccc} X & \xrightarrow{f} & X' \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle j} \\ F & \xrightarrow{\varphi} & F' \end{array}$$

is commutative. Similarly, since the bijection f has an inverse $f^{-1} : X' \to X$ and F' is free, there is a morphism $\psi : F' \to F$ such that:

$$\begin{array}{ccc} X' & \xrightarrow{f^{-1}} & X \\ {\scriptstyle j}\downarrow & & \downarrow{\scriptstyle i} \\ F' & \xrightarrow{\psi} & F \end{array}$$

is commutative. Combining these gives a commutative diagram:

$$\begin{array}{ccc} X & \xrightarrow{1_X} & X \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle i} \\ F & \xrightarrow{\psi\circ\varphi} & F \end{array}$$

Hence $(\psi \circ \varphi) \circ i = i \circ 1_X = i$. But $1_F \circ i = i$. Thus by the uniqueness property of free objects we must have $\psi \circ \varphi = 1_F$. A similar argument shows that $\varphi \circ \psi = 1_{F'}$. Therefore F is equivalent to F'.

Definition 2.46 (范对象与余范对象)

An object I in a category C is said to be **universal** (or **initial**) if for each object C of C there exists one and only one morphism $I \to C$. An object T of C is said to be **couniversal** (or **terminal**) if for each object C of C there exists one and only one morphism $C \to T$.

Proposition 2.37

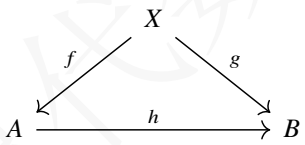
Any two universal [resp. couniversal] objects in a category C are equivalent.

Proof

Let I and J be universal objects in C. Since I is universal, there is a unique morphism $f : I \to J$. Similarly, since J is universal, there is a unique morphism $g : J \to I$. The composition $g \circ f : I \to I$ is a morphism of C. But $1_I : I \to I$ is also a morphism of C. The universality of I implies that there is a unique morphism $I \to I$, whence $g \circ f = 1_I$. Similarly the universality of J implies that $f \circ g = 1_J$. Therefore $f : I \to J$ is an equivalence. The proof for couniversal objects is analogous.

Example 2.21

Let F be a free object on the set X (with $i : X \to F$) in a concrete category C. Define a new category $\mathfrak{D}$ as follows. The objects of $\mathfrak{D}$ are all maps of sets $f : X \to A$, where A is (the underlying set of) an object of C. A morphism in $\mathfrak{D}$ from $f : X \to A$ to $g : X \to B$ is defined to be a morphism $h : A \to B$ of C such that the diagram:



is commutative (that is, $hf = g$). Verify that $1_A : A \to A$ is the identity morphism from f to f in $\mathfrak{D}$ and that h is an equivalence in $\mathfrak{D}$ if and only if h is an equivalence in C. Since F is free on the set X, there is for each map $f : X \to A$ a unique morphism $\tilde{f} : F \to A$ such that $\tilde{f}i = f$. This is precisely the statement that $i : X \to F$ is a universal object in the category $\mathfrak{D}$.

Example 2.22 Let $\{A_i \mid i \in I\}$ be a family of objects in a category C. Define a category $\mathcal{S}$ whose objects are all pairs $(B, \{f_i \mid i \in I\})$, where B is an object of C and for each i, $f_i : B \to A_i$ is a morphism of C. A morphism in $\mathcal{S}$ from $(B, \{f_i \mid i \in I\})$ to $(D, \{g_i \mid i \in I\})$ is defined to be a morphism $h : B \to D$ of C such that $g_i \circ h = f_i$ for every $i \in I$. Verify that 1_B is the identity morphism from $(B, \{f_i\})$ to $(B, \{f_i\})$ in $\mathcal{S}$ and that h is an equivalence in $\mathcal{S}$ if and only if h is an equivalence in C.

If a product exists in C for the family $\{A_i \mid i \in I\}$ (with maps $\pi_k : \prod A_i \to A_k$ for each $k \in I$), then for every $(B, \{f_i\})$ in $\mathcal{S}$ there exists a unique morphism $f : B \to \prod A_i$ such that $\pi_i \circ f = f_i$ for every $i \in I$. But this says that $(\prod A_i, \{\pi_i \mid i \in I\})$ is a couniversal object in the category $\mathcal{S}$.

Similarly the coproduct of a family of objects in C may be considered as a universal object in an appropriately constructed category.

2.11 群的直积与直和

Theorem 2.39

If $\{G_i \mid i \in I\}$ is a family of groups, then

(i) the direct product $\prod_{i\in I} G_i$ is a group;

(ii) for each $k \in I$, the map $\pi_k : \prod_{i\in I} G_i \to G_k$ given by $f \mapsto f(k)$ [or $\{a_i\} \mapsto a_k$] is an epimorphism of groups.

Theorem 2.40

Let $\{G_i \mid i \in I\}$ be a family of groups and $\{\varphi_i : H \to G_i \mid i \in I\}$ a family of group homomorphisms. Then there is a unique homomorphism $\varphi : H \to \prod_{i\in I} G_i$ such that $\pi_i\varphi = \varphi_i$ for all $i \in I$ and this property determines $\prod_{i\in I} G_i$ uniquely up to isomorphism. In other words, $\prod_{i\in I} G_i$ is a product in the category of groups.

Proof

By Introduction, the map of sets $\varphi : H \to \prod_{i\in I} G_i$ given by $\varphi(a) = \{\varphi_i(a)\}_{i\in I} \in \prod_{i\in I} G_i$ is the unique function such that $\pi_i\varphi = \varphi_i$ for all $i \in I$. It is easy to verify that φ is a homomorphism. Hence $\prod_{i\in I} G_i$ is a product (in the categorical sense) and therefore determined up to isomorphism (equivalence) by definition

Definition 2.47

The **(external) weak direct product** *of a family of groups* $\{G_i \mid i \in I\}$, *denoted* $\prod^w_{i\in I} G_i$, *is the set of all* $f \in \prod_{i\in I} G_i$ *such that* $f(i) = e_i$, *the identity in* G_i, *for all but a finite number of* $i \in I$. *If all the groups* G_i *are (additive) abelian,* $\prod^w_{i\in I} G_i$ *is usually called the* ***(external) direct sum*** *and is denoted* $\sum_{i\in I} G_i$.

Note If I is finite, the weak direct product coincides with the direct product. In any case, we have

Theorem 2.41

If $\{G_i \mid i \in I\}$ *is a family of groups, then*

(i) $\prod^w_{i\in I} G_i$ is a normal subgroup of $\prod_{i\in I} G_i$;

(ii) for each $k \in I$, the map $\iota_k : G_k \to \prod^w_{i\in I} G_i$ given by $\iota_k(a) = \{a_i\}_{i\in I}$, where $a_i = e$ for $i \neq k$ and $a_k = a$, is a monomorphism of groups;

(iii) for each $i \in I$, $\iota_i(G_i)$ is a normal subgroup of $\prod^w_{i\in I} G_i$.

Theorem 2.42

Let $\{A_i \mid i \in I\}$ be a family of abelian groups (written additively). If B is an abelian group and $\{\psi_i : A_i \to B \mid i \in I\}$ a family of homomorphisms, then there is a unique homomorphism $\psi : \sum_{i\in I} A_i \to B$ such that $\psi \circ \iota_i = \psi_i$ for all $i \in I$ and this property determines $\sum_{i\in I} A_i$ uniquely up to isomorphism. In other words, $\sum_{i\in I} A_i$ is a coproduct in the category of abelian groups.

Proof Throughout this proof all groups will be written additively. If $0 \neq \{a_i\} \in \sum A_i$, then only finitely many of the a_i are nonzero, say $a_{i_1}, a_{i_2}, \ldots, a_{i_r}$. Define $\psi : \sum A_i \to B$ by $\psi\{0\} = 0$ and $\psi(\{a_i\}) = \psi_{i_1}(a_{i_1}) + \psi_{i_2}(a_{i_2}) + \cdots + \psi_{i_r}(a_{i_r}) = \sum_{i\in I_0} \psi_i(a_i)$, where I_0 is the set $\{i_1, i_2, \ldots, i_r\} = \{i \in I \mid a_i \neq 0\}$. Since B is abelian, it is readily verified that ψ is a homomorphism and that $\psi \circ \iota_i = \psi_i$ for all $i \in I$. For each $\{a_i\} \in \sum A_i$, $\{a_i\} = \sum_{i\in I_0} \iota_i(a_i)$, I_0 finite as above. If $\xi : \sum A_i \to B$ is a homomorphism such that $\xi \circ \iota_i = \psi_i$ for all i then

$$\xi(\{a_i\}) = \xi(\sum_{I_0} \iota_i(a_i)) = \sum_{I_0} \xi \circ \iota_i(a_i) = \sum_{I_0} \psi_i(a_i) = \sum_{I_0} \psi_i(a_i) = \psi(\sum_{I_0} \iota_i(a_i)) = \psi(\{a_i\})$$

hence $\xi = \psi$ and ψ is unique. Therefore $\sum A_i$ is a coproduct in the category of abelian groups and hence is determined up to isomorphism

(equivalence) .

Remark

The theorem is false if the word abelian is omitted. The external weak direct product is not a coproduct in the category of all groups

Note

Give an example to show that the weak direct product is not a coproduct in the category of all groups. (Hint: it suffices to consider the case of two factors $G \times H$).

In the category of groups, the coproduct is the free product, not the direct product. We show this by constructing a counterexample where the direct product $G \times H$ fails to satisfy the universal property of coproducts.

Let $G = \mathbb{Z}/2\mathbb{Z}$ and $H = \mathbb{Z}/2\mathbb{Z}$, generated by a and b respectively, with $a^2 = e_G$ and $b^2 = e_H$. Their direct product $G \times H$ is the Klein four-group, with elements (e_G, e_H), (a, e_H), (e_G, b), and (a, b).

Now, let $X = S_3$ (the symmetric group on 3 letters), and define homomorphisms $f_G : G \to S_3$ and $f_H : H \to S_3$ as follows:

$$f_G(a) = (1\ 2),$$
$$f_H(b) = (1\ 3).$$

If $G \times H$ were a coproduct, there would exist a unique homomorphism $f : G \times H \to S_3$ such that $f \circ i_G = f_G$ and $f \circ i_H = f_H$, where $i_G : G \to G \times H$ and $i_H : H \to G \times H$ are the inclusion homomorphisms defined by:

$$i_G(g) = (g, e_H),$$
$$i_H(h) = (e_G, h).$$

Specifically, this requires:

$$f(i_G(a)) = f(a, e_H) = f_G(a) = (1\ 2),$$
$$f(i_H(b)) = f(e_G, b) = f_H(b) = (1\ 3).$$

In the direct product $G \times H$, the elements (a, e_H) and (e_G, b) commute, i.e.,

$$(a, e_H) \cdot (e_G, b) = (a, b) = (e_G, b) \cdot (a, e_H).$$

Therefore, in S_3, $f(a, e_H)$ and $f(e_G, b)$ must commute. However, we have:

$$f(a, e_H) = (1\ 2),$$
$$f(e_G, b) = (1\ 3).$$

But $(1\ 2)$ and $(1\ 3)$ do not commute in S_3, since:

$$(1\ 2)(1\ 3) = (1\ 3\ 2),$$
$$(1\ 3)(1\ 2) = (1\ 2\ 3),$$

and $(1\ 3\ 2) \neq (1\ 2\ 3)$.

Thus, no such homomorphism f exists, and therefore $G \times H$ does not satisfy the universal property of coproducts. This shows that the weak direct product (direct product) is not a coproduct in the category of all groups.

Theorem 2.43

Let $\{N_i \mid i \in I\}$ be a family of normal subgroups of a group G such that

(i) $G = \langle \bigcup_{i\in I} N_i \rangle$;

(ii) for each $k \in I$, $N_k \cap \langle \bigcup_{i\neq k} N_i \rangle = \langle e \rangle$.

Then $G \cong \prod_{i\in I}^{w} N_i$.

Proof If $\{a_i\} \in \prod_{i\in I}^{w} N_i$, then $a_i = e$ for all but a finite number of $i \in I$. Let I_0 be the finite set $\{i \in I \mid a_i \neq e\}$. Then $\prod_{i\in I_0} a_i$ is a well-defined element of G, since for $a \in N_i$ and $b \in N_j$, $(i \neq j)$, $ab = ba$ by Theorem 5.3(iv). Consequently the map $\varphi : \prod_{i\in I}^{w} N_i \to G$, given by $\{a_i\} \mapsto \prod_{i\in I_0} a_i \in G$ (and $\{e\} \mapsto e$), is a homomorphism such that $\varphi \circ \iota_i(a_i) = a_i$ for $a_i \in N_i$.

Since G is generated by the subgroups N_i, every element a of G is a finite product of elements from various N_i. Since elements of N_i and N_j commute (for $i \neq j$), a can be written as a product $\prod_{i\in I_0} a_i$, where $a_i \in N_i$ and I_0 is some finite subset of I. Hence

$$\prod_{i\in I_0} \iota_i(a_i) \in \prod_{i\in I}^{w} N_i$$

and

$$\varphi\left(\prod_{i\in I_0} \iota_i(a_i)\right) = \prod_{i\in I_0} \varphi \circ \iota_i(a_i) = \prod_{i\in I_0} a_i = a.$$

Therefore, φ is an epimorphism.

Suppose $\varphi(\{a_i\}) = \prod_{i\in I_0} a_i = e \in G$. Clearly we may assume for convenience of notation that $I_0 = \{1, 2, \ldots, n\}$. Then

$$\prod_{i\in I_0} a_i = a_1 a_2 \cdots a_n = e,$$

with $a_i \in N_i$. Hence

$$a_1^{-1} = a_2 \cdots a_n \in N_1 \cap \langle \bigcup_{i\neq 1} N_i \rangle = \langle e \rangle$$

and therefore $a_1 = e$. Repetition of this argument shows that $a_i = e$ for all $i \in I$. Hence φ is a monomorphism.

Corollary 2.14

Before proving the theorem we note a special case that is frequently used: Observe that for normal subgroups $N_1, N_2, \ldots, N_r$ of a group G, $\langle N_1 \cup N_2 \cup \cdots \cup N_r \rangle = N_1 N_2 \cdots N_r = \{n_1 n_2 \cdots n_r \mid n_i \in N_i\}$ by an easily proved . In additive notation $N_1 N_2 \cdots N_r$ is written $N_1 + N_2 + \cdots + N_r$. It may be helpful for the reader to keep the following corollary in mind since the proof of the general case is essentially the same.

If $N_1, N_2, \ldots, N_r$ are normal subgroups of a group G such that $G = N_1 N_2 \cdots N_r$ and for each $1 \leq k \leq r$, $N_k \cap (N_1 \cdots N_{k-1} N_{k+1} \cdots N_r) = \langle e \rangle$, then $G \cong N_1 \times N_2 \times \cdots \times N_r$.

Definition 2.48

Let $\{N_i \mid i \in I\}$ be a family of normal subgroups of a group G such that $G = \langle \bigcup_{i\in I} N_i \rangle$ and for each $k \in I$, $N_k \cap \langle \bigcup_{i\neq k} N_i \rangle = \langle e \rangle$. Then G is said to be the **internal weak direct product** of the family $\{N_i \mid i \in I\}$ (or the **internal direct sum** if G is (additive) abelian).

Proposition 2.38

Let $\{N_i \mid i \in I\}$ be a family of normal subgroups of a group G. G is the internal weak direct product of the family $\{N_i \mid i \in I\}$ if and only if every nonidentity element of G is a unique product $a_{i_1} a_{i_2} \cdots a_{i_n}$ with $i_1, \ldots, i_n$ distinct elements of I and $e \neq a_{i_k} \in N_{i_k}$ for each $k = 1, 2, \ldots, n$.

Note

There is a distinction between internal and external weak direct products. If a group G is the internal weak direct product of groups N_i, then by definition each N_i is actually a subgroup of G and G is isomorphic to the external weak direct product $\prod_{i\in I}^{w} N_i$. However, the external weak direct product $\prod_{i\in I}^{w} N_i$ does not actually contain the groups N_i, but only isomorphic copies of them (namely the $\iota_i(N_i)$ — see Theorem 8.4 and Exercise 10). Practically speaking, this distinction is not very important and the adjectives "internal" and "external" will be omitted whenever no confusion is possible. In fact we shall use the following notation.

We write $G = \prod_{i\in I} N_i$ to indicate that the group G is the internal weak direct product of the family of its subgroups $\{N_i \mid i \in I\}$.

Theorem 2.44 (两族空间诱导的乘积映射性质)

Let $\{f_i : G_i \to H_i \mid i \in I\}$ be a family of homomorphisms of groups and let $f = \prod_{i\in I} f_i$ be the map $\prod_{i\in I} G_i \to \prod_{i\in I} H_i$, given by $\{a_i\} \mapsto \{f_i(a_i)\}$. Then f is a homomorphism of groups such that $f(\prod_{i\in I}^{w} G_i) \subset \prod_{i\in I}^{w} H_i$, $\mathrm{Ker} f = \prod_{i\in I}^{w} \mathrm{Ker} f_i$ and $\mathrm{Im} f = \prod_{i\in I}^{w} \mathrm{Im} f_i$. Consequently f is a monomorphism [resp. epimorphism] if and only if each f_i is.

Corollary 2.15

Let $\{G_i \mid i \in I\}$ and $\{N_i \mid i \in I\}$ be families of groups such that N_i is a normal subgroup of G_i for each $i \in I$.

(i) $\prod_{i\in I}^{w} N_i$ is a normal subgroup of $\prod_{i\in I}^{w} G_i$ and $\prod_{i\in I}^{w} G_i / \prod_{i\in I}^{w} N_i \cong \prod_{i\in I}^{w} G_i/N_i$.

(ii) $\prod_{i\in I}^{w} N_i$ is a normal subgroup of $\prod_{i\in I}^{w} G_i$ and $\prod_{i\in I}^{w} G_i / \prod_{i\in I}^{w} N_i \cong \prod_{i\in I}^{w} G_i/N_i$.

♡

Theorem 2.45

If $\{G_i \mid i \in I\}$ is a family of groups, then $\prod' G_i$ is the internal weak direct product of its subgroups $\{\iota_i(G_i) \mid i \in I\}$.

Proof

Let $\prod' G_i$ denote the weak direct product (restricted direct product) of the groups G_i, i.e., the set of functions $f : I \to \bigcup_{i\in I} G_i$ such that $f(i) \in G_i$ for all $i \in I$ and $f(i) = e_{G_i}$ for all but finitely many i. The group operation is defined componentwise.

For each $i \in I$, define the embedding $\iota_i : G_i \to \prod' G_i$ by:

$$(\iota_i(g))(j) = \begin{cases} g & \text{if } j = i, \\ e_{G_j} & \text{if } j \neq i. \end{cases}$$

Then $\iota_i(G_i)$ is a subgroup of $\prod' G_i$ isomorphic to G_i.

We now verify that $\prod' G_i$ is the internal weak direct product of the subgroups $\iota_i(G_i)$ by checking the following conditions:

1.Each $\iota_i(G_i)$ is normal in $\prod' G_i$.

Let $f \in \prod' G_i$ and $\iota_i(g) \in \iota_i(G_i)$. Then for any $j \in I$,

$$(f\iota_i(g)f^{-1})(j) = f(j) \cdot (\iota_i(g)(j)) \cdot f(j)^{-1}.$$

If $j \neq i$, then $\iota_i(g)(j) = e_{G_j}$, so $(f\iota_i(g)f^{-1})(j) = e_{G_j}$. If $j = i$, then $(f\iota_i(g)f^{-1})(i) = f(i)gf(i)^{-1} \in G_i$. Hence,

$$f\iota_i(g)f^{-1} = \iota_i(f(i)gf(i)^{-1}) \in \iota_i(G_i).$$

Thus, $\iota_i(G_i)$ is normal in $\prod' G_i$.

2.$\prod' G_i$ is generated by the subgroups $\iota_i(G_i)$.

Let $f \in \prod' G_i$. Since $f(i) = e_{G_i}$ for all but finitely many i, let $\{i_1, \ldots, i_n\}$ be the finite set of indices where $f(i) \neq e_{G_i}$. Then

$$f = \iota_{i_1}(f(i_1)) \cdot \iota_{i_2}(f(i_2)) \cdots \iota_{i_n}(f(i_n)).$$

Moreover, for $i \neq j$, elements of $\iota_i(G_i)$ and $\iota_j(G_j)$ commute because for any $g \in G_i$, $h \in G_j$, and $k \in I$,

$$(\iota_i(g)\iota_j(h))(k) = (\iota_j(h)\iota_i(g))(k).$$

Therefore, every element of $\prod' G_i$ can be written as a finite product of elements from the subgroups $\iota_i(G_i)$, and these elements commute pairwise.

3. For each $i \in I$, $\iota_i(G_i) \cap \langle \bigcup_{j \neq i} \iota_j(G_j) \rangle = \{e\}$.

Suppose $x \in \iota_i(G_i) \cap \langle \bigcup_{j \neq i} \iota_j(G_j) \rangle$. Then $x = \iota_i(g)$ for some $g \in G_i$, and also x can be written as a finite product of elements from $\iota_j(G_j)$ with $j \neq i$. Since elements from different $\iota_j(G_j)$ commute, we can write

$$x = \iota_{j_1}(h_1) \cdot \iota_{j_2}(h_2) \cdots \iota_{j_m}(h_m)$$

with $j_k \neq i$ for all k. Now, for the index i, we have

$$x(i) = g \quad \text{but also} \quad x(i) = e_{G_i}$$

because each $\iota_{j_k}(h_k)$ has the identity at index i. Hence, $g = e_{G_i}$, so $x = \iota_i(e_{G_i}) = e$, the identity element of $\prod' G_i$.

Since all conditions for an internal weak direct product are satisfied, we conclude that $\prod' G_i$ is the internal weak direct product of its subgroups $\iota_i(G_i)$.

Definition 2.49 (群的直积与半直积)

设H,K为两个群我们定义：$H \times K = \{(h,k) : \ h \in H, k \in K\}$并且定义$H \times K$上的乘法$(h_1,k_1)\cdot(h_2,k_2) = (h_1h_2, k_1k_2)$
不难知道：$H \times K$为一个群我们称为H与K的直积

设G与H为两个群，我们构造群同态φ： $G \to Aut(H)$ 其中$\varphi(g) = \varphi_g \in Aut(H)$即把$g$诱导出一个$H$上的自同构
在集合$\{(g,h) : \ g \in G, h \in H\}$上定义乘法$(g_1,h_1)(g_2,h_2) = \left(g_1g_2, \ \varphi_{g_2^{-1}}(h_1)h_2\right)$
不难知道：该集合是群我们称为G与H的半直积记作$G \ltimes H$
进一步$G_1 = \{(g,e_H) : \ g \in G\}$为$G \ltimes H$的子群.$H_1 = \{(e_G,h) : \ h \in H\}$为$G \ltimes H$的正规子群

另外在群G中，$N \lhd G$
若存在子群H使得$H \cap N = \{e\}, HN = G$则称G为H与N的半直积
若在半直积的基础上H甚至为正规子群就称G为H与N的直积

Note 设H,K都是群G的子群，我们来探索需要满足什么条件才会有$H \times K \cong G$.
容易想到$H \times K$到G的一个映射σ可以如下规定：
$\sigma : H \times K \to G$

$(h,k) \mapsto hk$.
σ是满射 $\Longleftrightarrow$ G中每个元素g能表示成$g = hk, h \in H, k \in K \Leftrightarrow G = HK$.

σ是单射
$\Longleftrightarrow$ 从$\sigma(h_1,k_1) = \sigma(h_2,k_2)$可推出$(h_1,k_1) = (h_2,k_2)$
$\Longleftrightarrow$ 从$h_1k_1 = h_2k_2$可推出$h_1 = h_2$且$k_1 = k_2$
$\Longleftrightarrow$ 从$h_2^{-1}h_1 = k_2k_1^{-1}$可推出$h_1 = h_2$且$k_1 = k_2$
$\Longleftrightarrow H \cap K = \{e\}$.
上述推导过程的最后一步的 $\Rightarrow$ 理由如下：假如$H \cap K \neq \{e\}$，则存在非单位元$a \in H \cap K$.于是从$h_2^{-1}h_1 = k_2k_1^{-1} = a$推出$h_1 = h_2a \neq h_2$
这与已知条件矛盾.因此$H \cap K = \{e\}$.

$\sigma[(h_1,k_1)(h_2,k_2)] = \sigma(h_1,k_1)\sigma(h_2,k_2), \quad \forall (h_1,k_1),(h_2,k_2) \in H \times K$
$\Longleftrightarrow (h_1h_2)(k_1k_2) = (h_1k_1)(h_2k_2), \forall h_1,h_2 \in H, k_1,k_2 \in K$
$\Longleftrightarrow H$中每个元素与K中每个元素可交换.

Theorem 2.46 (内直积定理)

设H,K是群G的两个子群, 则$H\times K\cong G$当且仅当下列条件成立：

(1)$G=HK$;

(2)$H\cap K=\{e\}$ (在已有 (1) 的前提下该 (2) 还可有等价叙述如：幺元分解唯一或者任意元分解唯一实际上这三者等价)

(3)H中每个元素与K中每个元素可交换. (在已经有2.的前提下这个条件可以替换为H与K都是G的正规子群)

Proof 由交换性推正规性

$\forall h\in H,\forall g=h_1k_1\in HK$那么$\underbrace{h_1k_1hk_1^{-1}h_1^{-1}=h}_{\text{交换即可}}\in H$所以为正规子群同理可证$K$

由正规性推交换性

$$\forall h\in H,\forall k_1\in K\text{已经有}k_1hk_1^{-1}\in H\Longrightarrow\begin{cases}k_1hk_1^{-1}h^{-1}\text{那么}k_1hk_1^{-1}h^{-1}\in H\\ k_1hk_1^{-1}h^{-1}\text{那么}k_1\underbrace{hk_1^{-1}h^{-1}}_{\in K}\in K\end{cases}\Longrightarrow k_1hk_1^{-1}h^{-1}\in H\cap K\Longrightarrow k_1hk_1^{-1}h^{-1}=e\text{推出交换}$$

Note 设H,K是群G的两个子群, 如果$H\times K\cong G$, 其同构映射为 $(h,k)\mapsto hk$, 那么称G是它的子群H与K的内直积

习惯上就记做$G=H\times K$

这是把 (h,k)与hk等同.此时, G中每个元素g能唯一地表示成$g=hk$, 其中$h\in H,k\in K$.

当群G的运算为加法时, 如果$H\oplus K\cong G$, 其同构映射为 $(h,k)\mapsto h+k$, 那么称G是它的子群H与K的内直和

习惯上就记做$G=H\oplus K$, 这是把 (h,k)与$h+k$等同.此时, G中每个元素g能唯一地表示成$g=h+k$, 其中$h\in H,k\in K$.

Corollary 2.16

设$G_i(i=1,2,\cdots,n)$是G的n个子群, 则$G=G_1\times G_2\times\cdots\times G_n\Longleftrightarrow$ 下述具有下述条件

(1) $G=G_1G_2\cdots G_n$;

(2)$G_i\cap\prod\limits_{i\neq j}G_j=\{e\}$; (在1.的前提下具有等价叙述为：任意元分解唯一， 幺元分解唯一实际上这三者等价)

(3) $a_ia_j=a_ja_i,(a_i\in G_i,a_j\in G_j;i,j=1,2,\cdots,n;i\neq j)$. (在2.的前提下具有等价叙述$G_i$都是$G$的正规子群)

Proposition 2.39

If a group G is the internal direct product of its subgroups H,K, then $H\cong G/K$ and $G/H\cong K$

Proposition 2.40 (外直积的一些结论)

1.给出以2为模的剩余类加群$\mathbb{Z}_2=\{\overline{0},\overline{1}\}$, 则$\mathbb{Z}_2$与$\mathbb{Z}_2$的直和是$\mathbb{Z}_2\oplus\mathbb{Z}_2=\{(\overline{0},\overline{0}),(\overline{0},\overline{1}),(\overline{1},\overline{0}),(\overline{1},\overline{1})\}$

容易知道$\mathbb{Z}_2\oplus\mathbb{Z}_2=\{(\overline{0},\overline{0}),(\overline{0},\overline{1}),(\overline{1},\overline{0}),(\overline{1},\overline{1})\}\cong Kelin4$

2.令C_n表示n阶循环群那么若 $(m,n)=1$那么$C_m\times C_n\cong C_{mn}$

Proposition 2.41 (外直积的一些性质)

在$G_1\times G_2$中我们定义$G_1^*=\{(x,e_2):\ x\in G_1\}\quad G_2^*=\{(e_1,x):\ x\in G_2\}$

1.G_1^*与G_2^*是$G_1\times G_2$的不变子群

2.且$G_1\cong G_1^*$与$G_2\cong G_2^*$ (可构造映射$G_1\to G_1^*\quad x\to(x,e_2)$)

3.$G_1^*\cap G_2^*=\{(e_1,e_2)\}$

4.$G_1\times G_2$的元素表示为$G_1^*\times G_2^*$时表示法唯一

Example 2.23

给出群H_i, K_i的例子，使得$H_1 \times H_2 \cong K_1 \times K_2$但没有任何$H_i$同构于任何$K_j$

Proof 令$H_1 = Z_2 \times Z_2$(克莱因四元群，阶为4)，$H_2 = Z_3 \times Z_3$(阶为9)

令$K_1 = Z_6$(循环群，阶为6)，$K_2 = Z_6$(循环群，阶为6

则$H_1 \times H_2 \cong Z_2 \times Z_2 \times Z_3 \times Z_3$，阶为36

这是因为$K_1 \times K_2 \cong Z_6 \times Z_6 \cong Z_2 \times Z_3 \times Z_2 \times Z_3 \cong Z_2 \times Z_2 \times Z_3 \times Z_3$，阶为36

因此$H_1 \times H_2 \cong K_1 \times K_2$。

但$H_1 \cong Z_2 \times Z_2$不同构于$K_1 \cong Z_6$(因为阶不同且一个循环一个不循环)

同样$H_2 \cong Z_3 \times Z_3$不同构于$K_2 \cong Z_6$(阶不同)。因此没有任何H_i同构于任何K_j

Example 2.24

For $i = 1, 2$, let H_i be a subgroup of G_i. Give examples to show that each of the following statements may be false:

(a) $G_1 \cong G_2$ and $H_1 \cong H_2 \Rightarrow G_1/H_1 \cong G_2/H_2$

(b) $G_1 \cong G_2$ and $G_1/H_1 \cong G_2/H_2 \Rightarrow H_1 \cong H_2$

(c) $H_1 \cong H_2$ and $G_1/H_1 \cong G_2/H_2 \Rightarrow G_1 \cong G_2$

Proof

(a) Counterexample:

Let $G_1 = G_2 = \mathbb{Z}_4 \times \mathbb{Z}_2$, so $G_1 \cong G_2$.

Let $H_1 = \langle (2,0) \rangle \cong \mathbb{Z}_2$ and $H_2 = \langle (0,1) \rangle \cong \mathbb{Z}_2$, so $H_1 \cong H_2$.

But $G_1/H_1 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $G_2/H_2 \cong \mathbb{Z}_4$, hence $G_1/H_1 \ncong G_2/H_2$.

(b) Counterexample:

Let $G_1 = G_2 = D_4$ (dihedral group of order 8), so $G_1 \cong G_2$.

Let $H_1 = \langle r \rangle \cong \mathbb{Z}_4$, then $G_1/H_1 \cong \mathbb{Z}_2$.

Let $H_2 = \langle s, r^2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then $G_2/H_2 \cong \mathbb{Z}_2$.

So $G_1/H_1 \cong G_2/H_2$, but $H_1 \ncong H_2$.

(c) Counterexample:

Let $G_1 = \mathbb{Z}_4$, $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$, so $G_1 \ncong G_2$.

Let $H_1 = 2\mathbb{Z}_4 \cong \mathbb{Z}_2$, then $G_1/H_1 \cong \mathbb{Z}_2$.

Let $H_2 = \langle (0,1) \rangle \cong \mathbb{Z}_2$, then $G_2/H_2 \cong \mathbb{Z}_2$.

So $H_1 \cong H_2$ and $G_1/H_1 \cong G_2/H_2$, but $G_1 \ncong G_2$.

2.12 Free Group

We shall show that free objects (free groups) exist in the (concrete) category of groups, and we shall use these to develop a method of describing groups in terms of "generators and relations." In addition, we indicate how to construct coproducts (free products) in the category of groups.

Given a set X we shall construct a group F that is free on the set X in the sense of Definition 7.7. If $X = \emptyset$, F is the trivial group $\langle e \rangle$. If $X \neq \emptyset$, let X^{-1} be a set disjoint from X such that $|X| = |X^{-1}|$. Choose a bijection $X \to X^{-1}$ and denote the image of $x \in X$ by x^{-1}. Finally choose a set that is disjoint from $X \cup X^{-1}$ and has exactly one element; denote this element by 1. A word on X is a sequence $(a_1, a_2, \ldots)$ with $a_i \in X \cup X^{-1} \cup \{1\}$ such that for some $n \in \mathbb{N}^*$, $a_k = 1$ for all $k \geq n$. The constant sequence $(1, 1, \ldots)$ is called the empty word and is denoted 1. (This ambiguous notation will cause no confusion.) A word $(a_1, a_2, \ldots)$ on X is said to be reduced provided that

(i) for all $x \in X$, x and x^{-1} are not adjacent (that is, $a_i = x \Rightarrow a_{i+1} \neq x^{-1}$ and $a_i = x^{-1} \Rightarrow a_{i+1} \neq x$ for all $i \in \mathbb{N}^*$, $x \in X$) and

(ii) $a_k = 1$ implies $a_i = 1$ for all $i \geq k$.

In particular, the empty word 1 is reduced.

Every nonempty reduced word is of the form $(x_1^{\lambda_1}, x_2^{\lambda_2}, \ldots, x_n^{\lambda_n}, 1, 1, \ldots)$, where $n \in \mathbb{N}^*$, $x_i \in X$ and $\lambda_i = \pm 1$ (and by convention x^1 denotes x for all $x \in X$). Hereafter we shall denote this word by $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$. This new notation is both more tractable and more suggestive. Observe that the definition of equality of sequences shows that two reduced words $x_1^{\lambda_1} \cdots x_m^{\lambda_m}$ and $y_1^{\delta_1} \cdots y_n^{\delta_n}$ ($x_i, y_j \in X; \lambda_i, \delta_j = \pm 1$) are equal if and only if both are 1 or $m = n$ and $x_i = y_i, \lambda_i = \delta_i$ for each $i = 1, 2, \ldots, n$. Consequently the map from X into the set $F(X)$ of all reduced words on X given by $x \mapsto x^1 = x$ is injective. We shall identify X with its image and consider X to be a subset of $F(X)$.

Next we define a binary operation on the set $F = F(X)$ of all reduced words on X. The empty word 1 is to act as an identity element ($w1 = 1w = w$ for all $w \in F$). Informally, we would like to have the product of nonempty reduced words to be given by juxtaposition, that is,

$$(x_1^{\lambda_1} \cdots x_m^{\lambda_m})(y_1^{\delta_1} \cdots y_n^{\delta_n}) = x_1^{\lambda_1} \cdots x_m^{\lambda_m} y_1^{\delta_1} \cdots y_n^{\delta_n}.$$

Unfortunately the word on the right side of the equation may not be reduced (for example, if $x_m^{\lambda m} = y_1^{-\delta_1}$). Therefore, we define the product to be given by juxtaposition and (if necessary) cancellation of adjacent terms of the form xx^{-1} or $x^{-1}x$; for example $(x_1^1 x_2^{-1} x_3^1)(x_3^{-1} x_2^1 x_4^1) = x_1^1 x_4^1$. More precisely, if $x_1^{\lambda_1} \cdots x_m^{\lambda_m}$ and $y_1^{\delta_1} \cdots y_n^{\delta_n}$ are nonempty reduced words on X with $m \leq n$, let k be the largest integer ($0 \leq k \leq m$) such that $x_{m-j}^{\lambda_{m-j}} = y_{j+1}^{-\delta_{j+1}}$ for $j = 0, 1, \ldots, k-1$. Then define

$$(x_1^{\lambda_1} \cdots x_m^{\lambda_m})(y_1^{\delta_1} \cdots y_n^{\delta_n}) = \begin{cases} x_1^{\lambda_1} \cdots x_{m-k}^{\lambda_{m-k}} y_{k+1}^{\delta_{k+1}} \cdots y_n^{\delta_n} & \text{if } k < m; \\ y_{m+1}^{\delta_{m+1}} \cdots y_n^{\delta_n} & \text{if } k = m < n; \\ 1 & \text{if } k = m = n. \end{cases}$$

If $m > n$, the product is defined analogously. The definition insures that the product of reduced words is a reduced word.

Theorem 2.47

If X is a nonempty set and $F = F(X)$ is the set of all reduced words on X, then F is a group under the binary operation defined above and $F = \langle X \rangle$.

Remark

The group $F = F(X)$ is called the *free group* on the set X. (The terminology "free" is explained by Theorem below.)

Proof

Since 1 is an identity element and $x_1^{\delta_1} \cdots x_n^{\delta_n}$ has inverse $x_n^{-\delta_n} \cdots x_1^{-\delta_1}$, we need only verify associativity. This may be done by induction and a tedious examination of cases or by the following more elegant device. For each $x \in X$ and $\delta = \pm 1$ let $|x^\delta|$ be the map

$F \to F$ given by $1 \mapsto x^\delta$ and

$$x_1^{\delta_1} \cdots x_n^{\delta_n} \mapsto \begin{cases} x_1^{\delta_1} \cdots x_n^{\delta_n} & \text{if } x^\delta \neq x_1^{-\delta_1}; \\ x_2^{\delta_1} \cdots x_n^{\delta_n} & \text{if } x^\delta = x_1^{-\delta_1} (= 1 \text{ if } n = 1). \end{cases}$$

Since $|x||x^{-1}| = 1_F = |x^{-1}||x|$, every $|x^\delta|$ is a permutation (bijection) of F (with inverse $|x^{-\delta}|$) by (13) of Introduction, Section 3. Let $A(F)$ be the group of all permutations of F (see page 26) and F_0 the subgroup generated by $\{|x| \mid x \in X\}$. The map $\varphi : F \to F_0$ given by $1 \mapsto 1_F$ and $x_1^{\delta_1} \cdots x_n^{\delta_n} \mapsto |x_1^{\delta_1}| \cdots |x_n^{\delta_n}|$ is clearly a surjection such that $\varphi(w_1 w_2) = \varphi(w_1)\varphi(w_2)$ for all $w_i \in F$. Since $1 \mapsto x_1^{\delta_1} \cdots x_n^{\delta_n}$ under the map $|x_1^{\delta_1}| \cdots |x_n^{\delta_n}|$, it follows that φ is injective. The fact that F_0 is a group implies that associativity holds in F and that φ is an isomorphism of groups. Obviously $F = \langle X \rangle$.

Certain properties of free groups are easily derived. For instance if $|X| \geq 2$, then the free group on X is nonabelian ($x, y \in X$ and $x \neq y \Rightarrow x^{-1}y^{-1}xy$ is reduced $\Rightarrow x^{-1}y^{-1}xy \neq 1 \Rightarrow xy \neq yx$). Similarly every element (except 1) in a free group has infinite order (Exercise 1). If $X = \{a\}$, then the free group on X is the infinite cyclic group $\langle a \rangle$ (Exercise 2). A decidedly nontrivial fact is that every subgroup of a free group is itself a free group on some set (see J. Rotman [19]).

Theorem 2.48

Let F be the free group on a set X and $t : X \to F$ the inclusion map. If G is a group and $f : X \to G$ a map of sets, then there exists a unique homomorphism of groups $\tilde{f} : F \to G$ such that $\tilde{f}t = f$. In other words, F is a free object on the set X in the category of groups.

Proof

Define $\bar{f}(1) = e$ and if $x_1^{\delta_1} \cdots x_n^{\delta_n}$ is a nonempty reduced word on X, define $\bar{f}(x_1^{\delta_1} \cdots x_n^{\delta_n}) = f(x_1)^{\delta_1} f(x_2)^{\delta_2} \cdots f(x_n)^{\delta_n}$. Since G is a group and $\delta_i = \pm 1$, the product $f(x_1)^{\delta_1} \cdots f(x_n)^{\delta_n}$ is a well-defined element of G. Verify that $\bar{f}$ is a homomorphism such that $\bar{f}t = f$. If $g : F \to G$ is any homomorphism such that $gt = f$, then

$$g(x_1^{\delta_1} \cdots x_n^{\delta_n}) = g(x_1^{\delta_1}) \cdots g(x_n^{\delta_n}) = g(x_1)^{\delta_1} \cdots g(x_n)^{\delta_n} = f(x_1)^{\delta_1} \cdots f(x_n)^{\delta_n} = \bar{f}(x_1^{\delta_1} \cdots x_n^{\delta_n}).$$

Therefore $\bar{f}$ is unique. ■

Remark

If F' is another free object on the set X in the category of groups (with $\lambda : X \to F'$), then Theorems 7.8 and 9.2 imply that there is an isomorphism $\varphi : F \cong F'$ such that $\varphi t = \lambda$. In particular $\lambda(X)$ is a set of generators of F'; this fact may also be proved directly from the definition of a free object.

Corollary 2.17

Every group G is the homomorphic image of a free group. ♡

Proof

Let X be a set of generators of G and let F be the free group on the set X. By Theorem 9.2 the inclusion map $X \to G$ induces a homomorphism $\bar{f} : F \to G$ such that $x \mapsto x \in G$. Since $G = \langle X \rangle$, the proof of Theorem 9.2 shows that $\bar{f}$ is an epimorphism.

An immediate consequence of Corollary and the First Isomorphism Theorem is that any group G is isomorphic to a quotient group F/N, where $G = \langle X \rangle$, F is the free group on X and N is the kernel of the epimorphism $F \to G$ of Corollary . Therefore, in order to describe G up to isomorphism we need only specify X, F, and N. But F is determined up to isomorphism by X (Theorem 7.8) and N is determined by any subset that generates it as a subgroup of F. Now if $w = x_1^{\delta_1} \cdots x_n^{\delta_n} \in F$ is a generator of N, then under the epimorphism $F \to G$, $w \mapsto x_1^{\delta_1} \cdots x_n^{\delta_n} = e \in G$. The equation $x_1^{\delta_1} \cdots x_n^{\delta_n} = e$ in G is called a **relation** on the generators x_i. Clearly a given group G may be completely described by specifying a set X of generators of G and a suitable set R of relations on these generators. This description is not unique since there are many possible choices of both X and R for a given group G (see Exercises 6 and 9).

Conversely, suppose we are given a set X and a set Y of (reduced) words on the elements of X. Question: does there exist a group

G such that G is generated by X and all the relations $w = e$ ($w \in Y$) are valid (where $w = x_1^{\delta_1} \cdots x_n^{\delta_n}$ now denotes a product in G)? We shall see that the answer is yes, providing one allows for the possibility that in the group G the elements of X may not all be distinct. For instance, if $a, b \in X$ and $a^1 b^{-1}$ is a (reduced) word in Y, then any group containing a, b and satisfying $a^1 b^{-1} = e$ must have $a = b$.

Given a set of "generators" X and a set Y of (reduced) words on the elements of X, we construct such a group as follows. Let F be the free group on X and N the normal subgroup of F generated by Y. Let G be the quotient group F/N and identify X with its image in F/N under the map $X \subseteq F \to F/N$; as noted above, this may involve identifying some elements of X with one another. Then G is a group generated by X (subject to identifications) and by construction all the relations $w = e$ ($w \in Y$) are satisfied ($w = x_1^{\delta_1} \cdots x_n^{\delta_n} \in Y \Rightarrow x_1^{\delta_1} \cdots x_n^{\delta_n} \in N \Rightarrow x_1^{\delta_1} N \cdots x_n^{\delta_n} N = N$); that is, $x_1^{\delta_1} \cdots x_n^{\delta_n} = e$ in $G = F/N$.

Definition 2.50

Let X be a set and Y a set of (reduced) words on X. A group G is said to be the **group defined by** the **generators** $x \in X$ and **relations** $w = e$ ($w \in Y$) provided $G \cong F/N$, where F is the free group on X and N the normal subgroup of F generated by Y. One says that $(X \mid Y)$ is a **presentation** of G.

The preceding discussion shows that the group defined by given generators and relations always exists. Furthermore it is the largest possible such group in the following sense.

Theorem 2.49 ((Van Dyck))

Let X be a set, Y a set of (reduced) words on X and G the group defined by the generators $x \in X$ and relations $w = e$ ($w \in Y$). If H is any group such that $H = \langle X \rangle$ and H satisfies all the relations $w = e$ ($w \in Y$), then there is an epimorphism $G \to H$.

Proof If F is the free group on X then the inclusion map $X \to H$ induces an epimorphism $\varphi : F \to H$ by Corollary 9.3. Since H satisfies the relations $w = e$ ($w \in Y$), $Y \subseteq \mathrm{Ker}\varphi$. Consequently, the normal subgroup N generated by Y in F is contained in $\mathrm{Ker}\varphi$. By Corollary 5.8 φ induces an epimorphism $F/N \to H/\{e\}$. Therefore the composition $G \cong F/N \to H/\{e\} \cong H$ is an epimorphism.

Remark

The elements of Y are being interpreted as words on X, products in G, and products in H as the context indicates.

The following examples of groups defined by generators and relations illustrate the sort of ad hoc arguments that are often the only way of investigating a given presentation. When convenient, we shall use exponential notation for words (for example, $x^2 y^{-3}$ in place of $x^1 x^1 y^{-1} y^{-1} y^{-1}$).

Example 2.25

Let G be the group defined by generators a, b and relations $a^4 = e, a^2 b^{-2} = e$ and $abab^{-1} = e$. Since Q_8, the quaternion group of order 8, is generated by elements a, b satisfying these relations (Exercise 4.14), there is an epimorphism $\varphi : G \to Q_8$ by Theorem 9.5. Hence $|G| \geq |Q_8| = 8$. Let F be the free group on $\{a, b\}$ and N the normal subgroup generated by $\{a^4, a^2 b^{-2}, abab^{-1}\}$. It is not difficult to show that every element of F/N is of the form $a^i b^j N$ with $0 \leq i \leq 3$ and $j = 0, 1$, whence $|G| = |F/N| \leq 8$. Therefore $|G| = 8$ and φ is an isomorphism. Thus the group defined by the given generators and relations is (isomorphic to) Q_8.

Example 2.26

The group defined by the generators a, b and the relations $a^n = e$ ($3 \leq n \in \mathbb{N}^*$), $b^2 = e$ and $abab = e$ (or $ba = a^{-1} b$) is the dihedral group D_n

Example 2.27

The group defined by one generator b and the single relation $b^m = e$ ($m \in \mathbb{N}^*$) is $\mathbb{Z}_m$

Example 2.28

The free group F on a set X is the group defined by the generators $x \in X$ and no relations (recall that $\langle \emptyset \rangle = \langle e \rangle$ by Definition 2.7). The terminology "free" arises from the fact that F is relation-free.

We close this section with a brief discussion of coproducts (free products) in the category of groups. Most of the details are left to the reader since the process is quite similar to the construction of free groups.

Given a family of groups $\{G_i \mid i \in I\}$ we may assume (by relabeling if necessary) that the G_i are mutually disjoint sets. Let $X = \bigcup_{i\in I} G_i$ and let $\{1\}$ be a one-element set disjoint from X. A word on X is any sequence $(a_1, a_2, \ldots)$ such that $a_i \in X \cup \{1\}$ and for some $n \in \mathbb{N}^*$, $a_i = 1$ for all $i \geq n$. A word $(a_1, a_2, \ldots)$ is reduced provided:

(i) no $a_i \in X$ is the identity element in its group G_j;

(ii) for all $i, j \geq 1$, a_i and a_{i+1} are not in the same group G_j;

(iii) $a_k = 1$ implies $a_i = 1$ for all $i \geq k$.

In particular $1 = (1, 1, \ldots)$ is reduced. Every reduced word $(\neq 1)$ may be written uniquely as $a_1a_2 \cdots a_n = (a_1, a_2, \ldots, a_n, 1, 1, \ldots)$, where $a_i \in X$.

Let $\prod_{i\in I} G_i$ (or $G_1 * G_2 * \cdots * G_n$ if I is finite) be the set of all reduced words on X.

$\prod_{i\in I} G_i$ forms a group, called the *free product* of the family $\{G_i \mid i \in I\}$, under the binary operation defined as follows. 1 is the identity element and the product of two reduced words $(\neq 1)$ essentially is to be given by juxtaposition. Since the juxtaposed product of two reduced words may not be reduced, one must make the necessary cancellations and contractions. For example, if $a_i, b_i \in G_i$ for $i = 1, 2, 3$, then $(a_1a_2a_3)(a_3^{-1}b_2b_1b_3) = a_1c_2b_1b_3 = (a_1, c_2, b_1, b_3, 1, 1, \ldots)$, where $c_2 = a_2b_2 \in G_2$. Finally, for each $k \in I$ the map $\iota_k : G_k \to \prod_{i\in I} G_i$ given by $e \mapsto 1$ and $a \mapsto a = (a, 1, 1, \ldots)$ is a monomorphism of groups. Consequently, we sometimes identify G_k with its isomorphic image in $\prod_{i\in I} G_i$

Theorem 2.50

Let $\{G_i \mid i \in I\}$ be a family of groups and $\prod_{i\in I} G_i$ their free product. If $\{\psi_i : G_i \to H \mid i \in I\}$ is a family of group homomorphisms, then there exists a unique homomorphism $\psi : \prod_{i\in I} G_i \to H$ such that $\psi\iota_i = \psi_i$ for all $i \in I$ and this property determines $\prod_{i\in I} G_i$ uniquely up to isomorphism. In other words, $\prod_{i\in I} G_i$ is a coproduct in the category of groups.

Proof

If $a_1a_2 \cdots a_n$ is a reduced word in $\prod_{i\in I} G_i$ with $a_k \in G_{i_k}$, define $\psi(a_1 \cdots a_n)$ to be $\psi_{i_1}(a_1)\psi_{i_2}(a_2) \cdots \psi_{i_n}(a_n) \in H$.

Exercise 2.8

1.$\mathbb{Z} \times \mathbb{Z} \cong F(x, y)/\langle x, y \mid xyx^{-1}y^{-1}\rangle$

2.$S_3 \cong F(x, y)/\langle x, y \mid xyx^{-1}y^{-1}, x^2, y^3\rangle$

3.$Q_8 \cong F(x, y)/\langle x, y \mid x^4, y^2, xyx^{-1}y^{-1}\rangle$

Proof

2.Assume$F$ is the free group on the set$\{x, y\}$. And$N$ is the normal group which is generated by$\{xyx^{-1}y^{-1}, x^2, y^3\}$. Then we can define the epimorphism,

$$\varphi : G \to S_3 \quad x \mapsto (12), \quad y \mapsto (123)$$

And we know that S_3 is generated by (12) and (123), so φ is surjective.And $Ker\varphi$ contains N, so we can define the epimorphism,

$$\tilde{\varphi} : F/N \to S_3 \quad xN \mapsto (12), \quad yN \mapsto (123)$$

.So it is enough to check the $\tilde{\varphi}$ is injective. We can see that every element in F/N has the form $x^{i_1}y^{j_1} \cdots x^{i_s}y^{j_s}N$,And by the relation in N,we can write the form as x^iy^jN, where $i = 0, 1$ and $j = 0, 1, 2$.So $|F/N| \leq 6$.But $|S_3| = 6$ and the $\tilde{\varphi}$ is also a epimorphism,So $|F/N| \geqslant 6$ so $\tilde{\varphi}$ is bijetjion.Hence we get the isomorphic $F/N \cong S_3$.(Of course,we can check the all elements x^iy^jN, $(i = 0, 1)$, $(j = 0, 1, 2)$ whose range under the $\tilde{\varphi}$ are not the identity in S_3.)

2.13 Free Abelian Group

Definition 2.51

A basis of an abelian group F is a subset X of F such that

(i) $F = \langle X \rangle$; and

(ii) for distinct $x_1, x_2, \ldots, x_k \in X$ and $n_i \in \mathbb{Z}$,

$$n_1x_1 + n_2x_2 + \cdots + n_kx_k = 0 \quad \Rightarrow \quad n_i = 0 \text{ for every } i.$$

Theorem 2.51

The following conditions on an abelian group F are equivalent.

(i) F has a nonempty basis.

(ii) F is the (internal) direct sum of a family of infinite cyclic subgroups.

(iii) F is (isomorphic to) a direct sum of copies of the additive group $\mathbb{Z}$ of integers.

(iv) There exists a nonempty set X and a function $\iota : X \to F$ with the following property: given an abelian group G and function $f : X \to G$, there exists a unique homomorphism of groups $\bar{f} : F \to G$ such that $\bar{f} \circ \iota = f$. In other words, F is a free object in the category of abelian groups.

Remark

An abelian group F that satisfies the conditions of Theorem is called a free abelian group (on the set X). By definition the trivial group 0 is the free abelian group on the null set $\varnothing$.

Proof

(i) $\Rightarrow$ (ii) If X is a basis of F, then for each $x \in X$, $nx = 0$ if and only if $n = 0$. Hence each subgroup $\langle x \rangle$ ($x \in X$) is infinite cyclic (and normal since F is abelian). Since $F = \langle X \rangle$, we also have $F = \langle \bigcup_{x \in X} \langle x \rangle \rangle$. If for some $z \in X$, $\langle z \rangle \cap \langle \bigcup_{x \in X, x \neq z} \langle x \rangle \rangle \neq 0$, then for some nonzero $n \in \mathbb{Z}$, $nz = n_1x_1 + \cdots + n_kx_k$ with $z, x_1, \ldots, x_k$ distinct elements of X, which contradicts the fact that X is a basis. Therefore $\langle z \rangle \cap \langle \bigcup_{x \in X} \langle x \rangle \rangle = 0$ and hence $F = \bigoplus_{x \in X} \langle x \rangle$ by Definition I.8.8.

(ii) $\Rightarrow$ (iii) Theorems 直积定理与循环群的同构定理

(iii) $\Rightarrow$ (i) Suppose $F \cong \bigoplus \mathbb{Z}$ and the copies of $\mathbb{Z}$ are indexed by a set X. For each $x \in X$, let θ_x be the element $\{u_i\}$ of $\bigoplus \mathbb{Z}$, where $u_i = 0$ for $i \neq x$, and $u_x = 1$. Verify that $\{\theta_x \mid x \in X\}$ is a basis of $\bigoplus \mathbb{Z}$ and use the isomorphism $F \cong \bigoplus \mathbb{Z}$ to obtain a basis of F.

(i) $\Rightarrow$ (iv) Let X be a basis of F and $\iota : X \to F$ the inclusion map. Suppose we are given a map $f : X \to G$. If $u \in F$, then $u = n_1x_1 + \cdots + n_kx_k$ ($n_i \in \mathbb{Z}; x_i \in X$) since X generates F. If $u = m_1x_1 + \cdots + m_kx_k$ ($m_k \in \mathbb{Z}$), then $\sum_{i=1}^{k}(n_i - m_i)x_i = 0$, whence $n_i = m_i$ for every i since X is a basis. Consequently the map $\bar{f} : F \to G$, given by

$$\bar{f}(u) = \bar{f}\left(\sum_{i=1}^{k} n_i x_i\right) = n_1 f(x_1) + \cdots + n_k f(x_k),$$

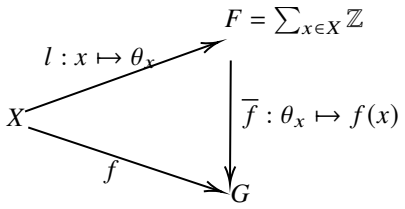
is a well-defined function such that $\bar{f}\mathfrak{I} = f$. Since G is abelian, $\bar{f}$ is easily seen to be a homomorphism. Since X generates F, any homomorphism $F \to G$ is completely determined by its action on X. Thus if $g : F \to G$ is a homomorphism such that $g\mathfrak{I} = f$, then for any $x \in X$, $g(x) = g(\iota(x)) = f(x) = \bar{f}(x)$, whence $g = \bar{f}$ and $\bar{f}$ is unique. Therefore, by Definition I.7.7 F is a free object on the set X in the category of abelian groups.

(iv) $\Rightarrow$ (iii). Given $\iota : X \to F$, construct the direct sum $\sum \mathbb{Z}$ with the copies of $\mathbb{Z}$ indexed by X. Let $Y = \{\theta_x \mid x \in X\}$ be a basis of $\sum \mathbb{Z}$ as in the proof of (iii) $\Rightarrow$ (i). The proof of (iii) $\Rightarrow$ (i) $\Rightarrow$ (iv) shows that $\sum \mathbb{Z}$ is a free object on the set Y. Since we clearly have $|X| = |Y|$, $F \cong \sum \mathbb{Z}$ by Theorem (Category section).

Note

Given any set X, the proof of Theorem indicates how to construct a free abelian group F with basis X. Simply let F be the direct sum $\sum \mathbb{Z}$, with the copies of $\mathbb{Z}$ indexed by X. As in the proof of (iii) $\Rightarrow$ (i), $\{\theta_x \mid x \in X\}$ is a basis of $F = \sum \mathbb{Z}$, and F is free on the set $\{\theta_x \mid x \in X\}$. Since the map $\iota : X \to F$ given by $x \mapsto \theta_x$ is injective, it follows easily that F is free on X in the sense of condition (iv) of

Theorem . In this situation we shall identify X with its image under ι so that $X \subset F$ and the cyclic subgroup $\langle \theta_x \rangle = \{n\theta_x \mid n \in \mathbb{Z}\} = \mathbb{Z}\theta_x$ is written $\langle x \rangle = \mathbb{Z}x$. In this notation $F = \sum_{x\in X}\langle \theta_x \rangle$ is written $F = \sum_{x\in X}\mathbb{Z}x$, and a typical element of F has the form $n_1x_1 + \cdots + n_kx_k$ $(n \in \mathbb{Z}, x_i \in X)$. In particular, $X = \iota(X)$ is a basis of F.



Lemma 2.8

1.若α，β是两个集合势，且$\beta \leqslant \alpha$且α非有限，则$\alpha + \beta = \alpha$

2.若α，β是两个集合势，且$0 \neq \beta \leqslant \alpha$且$\alpha$非有限，则$\alpha\beta = \alpha$，特别地$\alpha\aleph_0 = \alpha$

若β有限，则$\aleph_0\beta = \aleph_0$

3.令A为一集合，对于一个正整数$n \geqslant 1$，令$A^n = A \times A \times \cdots \times A$

若A为有限，则 $|A|^n = |A^n|$，若A无限，则 $|A^n| = |A|$ 且有 $\bigcup_{n=1}^{\infty} A^n = \aleph_0 |A|$

Theorem 2.52

Any two bases of a free abelian group F have the same cardinality.

Proof

First suppose F has a basis X of finite cardinality n so that $F \cong \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (n summands). For any subgroup G of F verify that $2G = \{2u \mid u \in G\}$ is a subgroup of G. Verify that the restriction of the isomorphism $F \cong \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ to $2F$ is an isomorphism $2F \cong 2\mathbb{Z} \oplus \cdots \oplus 2\mathbb{Z}$, whence $F/2F \cong \mathbb{Z}/2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$ (n summands) by Corollary I.8.11. Therefore $|F/2F| = 2^n$. If Y is another basis of F and r any integer such that $|Y| \geq r$, then a similar argument shows that $|F/2F| \geq 2^r$, whence $2^r \leq 2^n$ and $r \leq n$. It follows that $|Y| = m \leq n$ and $|F/2F| = 2^m$. Therefore $2^m = 2^n$ and $|X| = n = m = |Y|$.

If one basis of F is infinite, then all bases are infinite by the previous paragraph. Consequently, in order to complete the proof it suffices to show that $|X| = |F|$, if X is any infinite basis of F. Clearly $|X| \leq |F|$. Let $S = \bigcup_{n\in\mathbb{N}} X^n$, where $X^n = X \times \cdots \times X$ (n factors). For each $s = (x_1, \ldots, x_n) \in S$ let G_s be the subgroup $\langle x_1, \ldots, x_n \rangle$. Then $G_s \cong \mathbb{Z}y_1 \oplus \cdots \oplus \mathbb{Z}y_t$ where $y_1, \ldots, y_t$ $(t \leq n)$ are the distinct elements of $\{x_1, \ldots, x_n\}$. Therefore, $|G_s| = |\mathbb{Z}| = |\mathbb{Z}| = |S|$, by Introduction, Theorem 8.12. Since $F = \bigcup_{s\in S} G_s$, we have $|F| = |\bigcup_{s\in S} G_s| \leq |S|$, by Introduction, Exercise 8.12. But by Introduction, $|S| = |X|$, whence $|F| \leq |X|$, where $|F| = |X|$. Therefore $|F| = |X|$ by the Schroeder-Bernstein Theorem.

Definition 2.52

The cardinal number of any basis X of the free abelian group F is thus an invariant of F; $|X|$ is called the rank of F.

Proposition 2.42

Let F_1 be the free abelian group on the set X_1 and F_2 the free abelian group on the set X_2. Then $F_1 \cong F_2$ if and only if F_1 and F_2 have the same rank (that is, $|X_1| = |X_2|$).

Proof If $\alpha : F_1 \cong F_2$, then $\alpha(X_1)$ is a basis of F_2, whence $|X_1| = |\alpha(X_1)| = |X_2|$ by Theorem 1.2. The converse is Theorem in the Category section

Theorem 2.53

Every abelian group G is the homomorphic image of a free abelian group of rank $|X|$, where X is a set of generators of G.

Proof

Let F be the free abelian group on the set X. Then $F = \sum_{x\in X} Zx$ and rank $F = |X|$. By Theorem the inclusion map $X \to G$ induces a homomorphism $\bar{f} : F \to G$ such that $1x \mapsto x \in G$, whence $X \subset \text{Im } \bar{f}$. Since X generates G we must have Im $\bar{f} = G$.

We now prove a theorem that will be extremely useful in analyzing the structure of finitely generated abelian groups . We shall need

Lemma 2.9

If $\{x_1, \ldots, x_n\}$ is a basis of a free abelian group F and $a \in \mathbb{Z}$, then for all $i \neq j$ $\{x_1, \ldots, x_{j-1}, x_j + ax_i, x_{j+1}, \ldots, x_n\}$ is also a basis of F.

Proof

Since $x_j = -ax_i + (x_j + ax_i)$, it follows that $F = \langle x_1, \ldots, x_{j-1}, x_j + ax_i, x_{j+1}, \ldots, x_n\rangle$. If $k_1x_1 + \cdots + k_j(x_j + ax_i) + \cdots + k_nx_n = 0$ $(k_i \in \mathbb{Z})$, then $k_1x_1 + \cdots + (k_i + k_ja)x_i + \cdots + k_jx_j + \cdots + k_nx_n = 0$, which implies that $k_t = 0$ for all t.

Theorem 2.54

If F is a free abelian group of finite rank n and G is a nonzero subgroup of F, then there exists a basis $\{x_1, \ldots, x_n\}$ of F, an integer $r(1 \leq r \leq n)$ and positive integers $d_1, \ldots, d_r$ such that $d_1|d_2| \cdots |d_r$ and G is free abelian with basis $\{d_1x_1, \ldots, d_rx_r\}$.

Remark

Every subgroup of a free abelian group of (possibly infinite) rank α is free of rank at most α; see Theorem IV.6.1. The notation "$d_1|d_2| \cdots |d_r$" means "d_1 divides d_2, d_2 divides d_3, etc."

Proof

If $n = 1$, then $F = \langle x_1\rangle \cong \mathbb{Z}$ and $G = \langle d_1x_1\rangle \cong \mathbb{Z}$ $(d_1 \in \mathbb{N}^*)$ .Proceeding inductively, assume the theorem is true for all free abelian groups of rank less than n.

Let S be the set of all those integers s such that there exists a basis $\{y_1, \ldots, y_n\}$ of F and an element in G of the form $sy_1 + k_2y_2 + \cdots + k_ny_n$ $(k_i \in \mathbb{Z})$. Note that in this case $\{y_2, y_1, y_3, \ldots, y_n\}$ is also a basis of F, whence $k_2 \in S$; similarly $k_j \in S$ for $j = 3, 4, \ldots, n$. Since $G \neq 0$, we have $S \neq \emptyset$. Hence S contains a least positive integer d_1 and for some basis $\{y_1, \ldots, y_n\}$ of F there exists $v \in G$ such that $v = d_1y_1 + k_2y_2 + \cdots + k_ny_n$. By the division algorithm for each $i = 2, \ldots, n, k_i = d_1q_i + r_i$ with $0 \leq r_i < d_1$, whence $v = d_1(y_1 + q_2y_2 + \cdots + q_ny_n) + r_2y_2 + \cdots + r_ny_n$. Let $x_1 = y_1 + q_2y_2 + \cdots + q_ny_n$; then by Lemma $W = \{x_1, y_2, \ldots, y_n\}$ is a basis of F. Since $v \in G, r_i < d_1$ and W in any order is a basis of F, the minimality of d_1 in S implies that $0 = r_2 = r_3 = \cdots = r_n$ so that $d_1x_1 = v \in G$.

Let $H = \langle y_2, y_3, \ldots, y_n\rangle$. Then H is a free abelian group of rank $n - 1$ such that $F = \langle x_1\rangle \bigoplus H$. Furthermore we claim that $G = \langle v\rangle \bigoplus (G \cap H) = \langle d_1x_1\rangle \bigoplus (G \cap H)$. Since $\{x_1, y_2, \ldots, y_n\}$ is a basis of F, $\langle v\rangle \bigcap (G \cap H) = 0$. If $u = t_1x_1 + t_2y_2 + \cdots + t_ny_n \in G$ $(t_i \in \mathbb{Z})$, then by the division algorithm $t_1 = d_1q_1 + r_1$ with $0 \leq r_1 < d_1$. Thus G contains $u - q_1v = r_1x_1 + t_2y_2 + \cdots + t_ny_n$. The minimality of d_1 in S implies that $r_1 = 0$, whence $t_2y_2 + \cdots + t_ny_n \in G \bigcap H$ and $u = q_1v + (t_2y_2 + \cdots + t_ny_n)$. Hence $G = \langle v\rangle + (G \cap H)$, which proves our assertion .

Either $G \cap H = 0$, in which case $G = \langle d_1x_1\rangle$ and the theorem is true or $G \cap H \neq 0$. Then by the inductive assumption there is a basis $\{x_2, x_3, \ldots, x_n\}$ of H and positive integers $r, d_2, d_3, \ldots, d_r$ such that $d_2|d_3| \cdots |d_r$ and $G \cap H$ is free abelian with basis $\{d_2x_2, \ldots, d_rx_r\}$. Since $F = \langle x_1\rangle \bigoplus H$ and $G = \langle d_1x_1\rangle \bigoplus (G \cap H)$, it follows easily that $\{x_1, x_2, \ldots, x_n\}$ is a basis of F and $\{d_1x_1, \ldots, d_rx_r\}$ is a basis of G. To complete the inductive step of the proof we need only show that $d_1|d_2$. By the division algorithm $d_2 = qd_1 + r_0$ with $0 \leq r_0 < d_1$. Since $\{x_2, x_1 + qx_2, x_3, \ldots, x_n\}$ is a basis of F by Lemma 1.5 and $r_0x_2 + d_1(x_1 + qx_2) = d_1x_1 + d_2x_2 \in G$, the minimality of d_1 in S implies that $r_0 = 0$, whence $d_1|d_2$.

Corollary 2.18

If G is a finitely generated abelian group generated by n elements, then every subgroup H of G may be generated by m elements with $m \leq n$.

♡

Remark The corollary is false if the word abelian is omitted

Proof

By Theorem there is a free abelian group F of rank n and an epimorphism $\pi : F \to G$. $\pi^{-1}(H)$ is a subgroup of F, and therefore, free of rank $m \leq n$ by Theorem . The image under π of any basis of $\pi^{-1}(H)$ is a set of at most m elements that generates $\pi(\pi^{-1}(H)) = H$.

2.14 Finitely Generated Abelian Groups

Theorem 2.55

Every finitely generated abelian group G is (isomorphic to) a finite direct sum of cyclic groups in which the finite cyclic summands (if any) are of orders $m_1, \ldots, m_t$, where $m_1 > 1$ and $m_1 \mid m_2 \mid \cdots \mid m_t$.

Proof If $G \neq 0$ and G is generated by n elements, then there is a free abelian group F of rank n and an epimorphism $\pi : F \to G$ by Theorem.

If π is an isomorphism, then $G \cong F \cong Z \oplus \cdots \oplus Z$ (n summands).

If not, then by Theorem there is a basis $\{x_1, \ldots, x_n\}$ of F and positive integers $d_1, \ldots, d_r$ such that $1 \leq r \leq n$,

$$d_1 \mid d_2 \mid \cdots \mid d_r \text{ and } \{d_1 x_1, \ldots, d_r x_r\} \text{ is a basis of } K = \ker \pi.$$

Now $F = \sum_{i=1}^{n} \langle x_i \rangle$ and

$$K = \sum_{i=1}^{r} \langle d_i x_i \rangle, \text{ where } \langle x_i \rangle \cong \mathbb{Z} \text{ and under the same isomorphism } \langle d_i x_i \rangle \cong d_i \mathbb{Z} = \{d_i u \mid u \in \mathbb{Z}\}.$$

For $i = r+1, r+2, \ldots, n$ let $d_i = 0$ so that $K = \sum_{i=1}^{n} \langle d_i x_i \rangle$.

Then by Theorems

$$G \cong F/K = \sum_{i=1}^{n} \langle x_i \rangle / \left(\sum_{i=1}^{n} \langle d_i x_i \rangle \right) \cong \sum_{i=1}^{n} \langle x_i \rangle / \langle d_i x_i \rangle \cong \sum_{i=1}^{n} \mathbb{Z}/d_i\mathbb{Z}.$$

If $d_i = 1$, then $\mathbb{Z}/d_i\mathbb{Z} = \mathbb{Z}/\mathbb{Z} = 0$; if $d_i > 1$, then $\mathbb{Z}/d_i\mathbb{Z} \cong \mathbb{Z}_{d_i}$; if $d_i = 0$, then $\mathbb{Z}/d_i\mathbb{Z} = \mathbb{Z}/0 \cong \mathbb{Z}$. Let $m_1, \ldots, m_t$ be those d_i (in order) such that $d_i \neq 0, 1$ and let s be the number of d_i such that $d_i = 0$. Then

$$G \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t} \oplus (\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}),$$

where $m_1 > 1, m_1 \mid m_2 \mid \cdots \mid m_t$ and $(\mathbb{Z} \oplus \cdots \oplus \mathbb{Z})$ has rank s.

Theorem 2.56

If m is a positive integer and $m = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ ($p_1, \ldots, p_t$ distinct primes and each $n_i > 0$), then $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}$.

Proof Use induction on the number t of primes in the prime decomposition of m and the fact that

$$\mathbb{Z}_m \cong \mathbb{Z}_r \oplus \mathbb{Z}_n \quad \text{whenever} \quad (r, n) = 1,$$

which we now prove. The element $\bar{n} \in \mathbb{Z}_{rn}$ has order r whence $\mathbb{Z}_r \cong \langle \bar{n} \rangle < \mathbb{Z}_m$ and the map $\psi_1 : \mathbb{Z}_r \to \mathbb{Z}_m$ given by $k \mapsto nk$ is a monomorphism. Similarly the map $\psi_2 : \mathbb{Z}_n \to \mathbb{Z}_m$ given by $k \mapsto rk$ is a monomorphism. The map $\psi : \mathbb{Z}_r \oplus \mathbb{Z}_n \to \mathbb{Z}_m$ given by $(x, y) \mapsto \psi_1(x) + \psi_2(y) = nx + ry$ is a well-defined homomorphism. Since $(r, n) = 1$, $ra + nb = 1$ for some $a, b \in \mathbb{Z}$. Hence $k = rak + nbk = \psi(bk, ak)$ for all $k \in \mathbb{Z}_m$ and ψ is an epimorphism. Since $|\mathbb{Z}_r \oplus \mathbb{Z}_n| = rn = |\mathbb{Z}_m|, \psi$ must also be a monomorphism.

Corollary 2.19

Every finitely generated abelian group G is (isomorphic to) a finite direct sum of cyclic groups, each of which is either infinite or of order a power of a prime.

Lemma 2.10

Let G be an abelian group, m an integer and p a prime integer. Then each of the following is a subgroup of G:

(i) $mG = \{mu \mid u \in G\}$;

(ii) $G[m] = \{u \in G \mid mu = 0\}$;

(iii) $G(p) = \{u \in G \mid |u| = p^n \text{ for some } n \geq 0\}$;

(iv) $G_t = \{u \in G \mid |u| \text{ is finite}\}$.

In particular there are isomorphisms

(v) $Z_{p^n}[p] \cong Z_p (n \geq 1)$ and $p^m Z_{p^n} \cong Z_{p^{n-m}} (m < n)$.

Let H and G_i $(i \in I)$ be abelian groups.

(vi) If $g : G \to \sum_{i \in I} G_i$ is an isomorphism, then the restrictions of g to mG and $G[m]$ respectively are isomorphisms $mG \cong \sum_{i \in I} mG_i$ and $G[m] \cong \sum_{i \in I} G_i[m]$.

(vii) If $f : G \to H$ is an isomorphism, then the restrictions of f to G_t and $G(p)$ respectively are isomorphisms $G_t \cong H_t$ and $G(p) \cong H(p)$.

Proof (i)-(iv) are exercises; the hypothesis that G is abelian is essential

(v) $\overline{p^{n-1}} \in \mathbb{Z}_{p^n}$ has order p , whence $\langle \overline{p^{n-1}} \rangle \cong \mathbb{Z}_p$ and $\langle \overline{p^{n-1}} \rangle < \mathbb{Z}_{p^n}[p]$. If $u \in \mathbb{Z}_{p^n}[p]$, then $pu = 0$ in $\mathbb{Z}_{p^n}$ so that $pu \equiv 0 \pmod{p^n}$ in $\mathbb{Z}$. But $p^n | pu$ implies $p^{n-1} | u$. Therefore, in $\mathbb{Z}_{p^n}, u \in \langle \overline{p^{n-1}} \rangle$ and $\mathbb{Z}_{p^n}[p] < \langle \overline{p^{n-1}} \rangle$. For the second statement note that $\overline{p^m} \in \mathbb{Z}_{p^n}$ has order p^{n-m} . Therefore $p^m \mathbb{Z}_{p^n} = \langle \overline{p^m} \rangle \cong \mathbb{Z}_{p^{n-m}}$.

(vi) is an exercise.

(vii) is an exercise

Remark

If G is an abelian group, then the subgroup G_t defined in Lemma 2.5 is called the **torsion subgroup** of G. If $G = G_t$, then G is said to be a **torsion group**. If $G_t = 0$, then G is said to be **torsion-free**. For a complete classification of all *denumerable* torsion groups, see I. Kaplansky [17].

Corollary 2.20

If G is a finite abelian group of order n, then G has a subgroup of order m for every positive integer m that divides n.

Theorem 2.57

Let G be a finitely generated abelian group.

(i) There is a unique nonnegative integer s such that the number of infinite cyclic summands in any decomposition of G as a direct sum of cyclic groups is precisely s;

(ii) either G is free abelian or there is a unique list of (not necessarily distinct) positive integers $m_1, \ldots, m_t$ such that $m_1 > 1, m_1 | m_2 | \cdots | m_t$ and

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

with F free abelian;

(iii) either G is free abelian or there is a list of positive integers $p_1^{s_1}, \ldots, p_k^{s_k}$, which is unique except for the order of its members, such that $p_1, \ldots, p_k$ are (not necessarily distinct) primes, $s_1, \ldots, s_k$ are (not necessarily distinct) positive integers and

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

with F free abelian.

Proof

(i) Any decomposition of G as a direct sum of cyclic groups (and there is at least one by Theorem) yields an isomorphism $G \cong H \bigoplus F$, where H is a direct sum of finite cyclic groups (possibly 0) and F is a free abelian group whose rank is precisely the number s of infinite cyclic summands in the decomposition. If $\iota : H \to H \bigoplus F$ is the canonical injection $(h \mapsto (h, 0))$, then clearly $\iota(H)$ is the torsion subgroup of $H \bigoplus F$. By Lemma , $G_t \cong \iota(H)$ under the isomorphism $G \cong H \bigoplus F$. Consequently, $G/G_t \cong (F \bigoplus H)/\iota(H) \cong (F/0 \bigoplus H/H) \cong F$. Therefore, any decomposition of G leads to the conclusion that G/G_t is a free abelian group whose rank is the number s of infinite cyclic summands in the decomposition. Since G/G_t does not depend on the particular decomposition and the rank of G/G_t is an invariant , s is uniquely determined.

(iii) Suppose G has two decompositions, say

$$G \cong \sum_{i=1}^{r} \mathbb{Z}_{n_i} \bigoplus F \quad \text{and} \quad G \cong \sum_{j=1}^{d} \mathbb{Z}_{k_j} \bigoplus F',$$

with each n_i, k_i a power of a prime (different primes may occur) and F, F' free abelian; (there is at least one such decomposition by Theorem). We must show that $r = d$ and (after reordering) $n_i = k_i$ for every i. It is easy to see that the torsion subgroup of

$$\sum \mathbb{Z}_{n_i} \bigoplus F$$

is (isomorphic to)

$$\sum \mathbb{Z}_{n_i}$$

and similarly for the other decomposition. Hence

$$\sum_{i=1}^{r} \mathbb{Z}_{n_i} \cong G_t \cong \sum_{j=1}^{d} \mathbb{Z}_{k_j}$$

by Lemma . For each prime p,

$$(\sum \mathbb{Z}_{n_i})(p)$$

is obviously (isomorphic to) the direct sum of those $\mathbb{Z}_{n_i}$ such that n_i is a power of p and similarly for the other decomposition. Since

$$(\sum \mathbb{Z}_{n_i})(p) \cong (\sum \mathbb{Z}_{k_i})(p)$$

for each prime p by Lemma , it suffices to assume that $G = G_t$ and each n_i, k_i is a power of a fixed prime p (so that $G = G(p)$). Hence we have

$$\sum_{i=1}^{r} \mathbb{Z}_{p^{a_i}} \cong G \cong \sum_{j=1}^{d} \mathbb{Z}_{p^{c_j}} (1 \le a_1 \le a_2 \le \cdots \le a_r; 1 \le c_1 \le c_2 \le \cdots \le c_d).$$

We first show that in any two such decompositions of a group we must have $r = d$. Lemma and the first decomposition of G show that

$$G[p] \cong \sum_{i=1}^{r} \mathbb{Z}_{p^{a_i}}[p] \cong \mathbb{Z}_p \bigoplus \cdots \bigoplus \mathbb{Z}_p$$

(r summands), whence $|G[p]| = p^r$. A similar argument with the second decomposition shows that $|G[p]| = p^d$. Therefore, $p^r = p^d$ and $r = d$.

Let $v(1 \le v \le r)$ be the first integer such that $a_i = c_i$ for all $i < v$ and $a_v \ne c_v$. We may assume that $a_v < c_v$. Since $p^{a_v}\mathbb{Z}_{p^{a_i}} = 0$ for $a_i \le a_v$, the first decomposition and Lemma imply that

$$p^{a_v}G \cong \sum_{i=1}^{r} p^{a_v}\mathbb{Z}_{p^{a_i}} \cong \sum_{i=v+1}^{r} \mathbb{Z}_{p^{a_i - a_v}}$$

with $a_{v+1} - a_v \le a_{v+2} - a_v \le \cdots \le a_r - a_v$. Clearly, there are at most $r - (v + 1) + 1 = r - v$ nonzero summands. Similarly since $a_i = c_i$ for $i < v$ and $a_v < c_v$ the second decomposition implies that

$$p^{a_v}G \cong \sum_{i=v}^{r} \mathbb{Z}_{p^{c_i - a_v}}$$

with $1 \leq c_v - a_v \leq c_{v+1} - a_v \leq \cdots \leq c_r - a_v$. Obviously there are at least $r - v + 1$ nonzero summands. Therefore, we have two decompositions of the group $p^{a_v}G$ as a direct sum of cyclic groups of prime power order and the number of summands in the first decomposition is less than the number of summands in the second. This contradicts the part of the Theorem proved in the previous paragraph (and applied here to $p^{a_v}G$). Hence we must have $a_i = c_i$ for all i.

(ii) Suppose G has two decompositions, say

$$G \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t} \oplus F \text{ and } G \cong \mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_d} \oplus F'$$

with $m_1 > 1, m_1 | m_2 | \cdots | m_t, k_1 > 1, k_1 | k_2 | \cdots | k_d$ and F, F' free abelian; (one such decomposition exists by Theorem . Each m_i, k_j has a prime decomposition and by inserting factors of the form p^0 we may assume that the same (distinct) primes $p_1, \ldots, p_r$ occur in all the factorizations, say

$$\begin{aligned}
m_1 &= p_1^{a_{11}} p_2^{a_{12}} \cdots p_r^{a_{1r}}, \quad & k_1 &= p_1^{c_{11}} p_2^{c_{12}} \cdots p_r^{c_{1r}} \\
m_2 &= p_1^{a_{21}} p_2^{a_{22}} \cdots p_r^{a_{2r}}, \quad & k_2 &= p_1^{c_{21}} p_2^{c_{22}} \cdots p_r^{c_{2r}} \\
&\cdots & & \\
&\cdots & & \\
&\cdots & & \\
m_t &= p_1^{a_{t1}} p_2^{a_{t2}} \cdots p_r^{a_{tr}}, \quad & k_d &= p_1^{c_{d1}} p_2^{c_{d2}} \cdots p_r^{c_{dr}}
\end{aligned}$$

Since $m_1 | m_2 | \cdots | m_t$, we must have for each $j, 0 \leq a_{1j} \leq a_{2j} \leq \cdots \leq a_{tj}$. Similarly $0 \leq c_{1j} \leq c_{2j} \leq \cdots \leq c_{dj}$ for each j. By Lemmas

$$\sum_{i,j} \mathbb{Z}_{p_j^{a_{ij}}} \cong \sum_{i=1}^{t} \mathbb{Z}_{m_i} \cong G_t \cong \sum_{i=1}^{d} \mathbb{Z}_{k_i} \cong \sum_{i,j} \mathbb{Z}_{p_j^{c_{ij}}},$$

where some summands may be zero. It follows that for each $j = 1, 2, \ldots, r$

$$\sum_{i=1}^{t} \mathbb{Z}_{p_j^{a_{ij}}} \cong G(p_j) \cong \sum_{i=1}^{d} \mathbb{Z}_{p_j^{c_{ij}}}.$$

Since $m_1 > 1$, there is some p_j such that $1 \leq a_{1j} \leq \cdots \leq a_{tj}$, whence $\sum_{i=1}^{t} \mathbb{Z}_{p_j^{a_{ij}}}$ has t nonzero summands. By (iii) $\sum_{i=1}^{d} \mathbb{Z}_{p_j^{c_{ij}}}$ has exactly t nonzero summands, whence $t \leq d$. Similarly $k_1 > 1$ implies that $d \leq t$ and hence $d = t$. By (iii) we now must have $a_{ij} = c_{ij}$ for all i, j, which implies that $m_i = k_i$ for $i = 1, 2, \ldots, t$.

If G is a finitely generated abelian group, then the uniquely determined integers $m_1, \ldots, m_t$ as in Theorem (ii) are called the **invariant factors** of G. The uniquely determined prime powers as in Theorem (iii) are called the **elementary divisors** of G.

Corollary 2.21

Two finitely generated abelian groups G and H are isomorphic if and only if G/G_t and H/H_t have the same rank and G and H have the same invariant factors [resp. elementary divisors].

2.15 Jordan-Holder 定理与群的扩张

给定一个群同态$\mu: G \to B$, 不妨假定这是个满同态 (否则, 把B换成μ的像集即可), 则映射的核$N = \mathrm{Ker}\mu$为G的正规子群. 于是我们有如下的群与同态序列$N \xrightarrow{\lambda} G \xrightarrow{\mu} B$其中, λ为N到G的自然嵌入.该序列有个特别的性质 : $\mathrm{Ker}\mu = \mathrm{Im}\lambda$.

Definition 2.53 (群的扩张)

设G, A, B是群, 群同态的序列$A \xrightarrow{\lambda} G \xrightarrow{\mu} B$.如果满足 $\mathrm{Im}\lambda = \mathrm{Ker}\mu$, 则我们称序列在$G$处正合.
进一步, 若λ为单射且μ为满射, 或序列$1 \longrightarrow A \xrightarrow{\lambda} G \xrightarrow{\mu} B \longrightarrow 1$在$A, G, B$处都正合, 称为短正合序列, 也称$G$是$B$过$A$的扩张.
其中, 1表示平凡群.此时, $N = \mathrm{Im}\lambda = \mathrm{Ker}\mu$为$G$的正规子群, 满足$N \cong A, G/N \cong B$, 称$N$为扩张核.

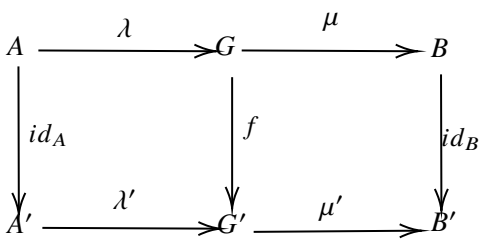
群G	正规子群N	A	商群G/N	B
数域$\mathbb{P}$ 上线性空间V	子空间W	W	商空间V/W	V/W
$G = \{e, a, a^2, a^3\}$ 为4 阶循环群	$\{e, a^2\}$	$\mathbb{Z}/2\mathbb{Z}$	$\{\bar{1}, \bar{a}\}$	$\mathbb{Z}/2\mathbb{Z}$
$\{e, a, b, c \mid a^2 = b^2 = c^2 = abc = e\}$	$\{e, a\}$	$\mathbb{Z}/2\mathbb{Z}$	$\{\bar{1}, \bar{b}\}$	$\mathbb{Z}/2\mathbb{Z}$
S_3	A_3	$\mathbb{Z}/3\mathbb{Z}$	S_3/A_3	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}$	$2\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$
$\mathrm{O}(n)$	$\mathrm{SO}(n)$	$\mathrm{SO}(n)$	$\mathrm{O}(n)/\mathrm{SO}(n)$	$\mathbb{Z}/2\mathbb{Z}$

第一个例子说明, 给定任何线性空间V的子空间W, 则作为加法群, V是商空间V/W作为加法群过子空间W的扩张.
第二例和第三例, 循环群$\mathbb{Z}_4$和$Klein$群K_4都是群$\mathbb{Z}_2$过$\mathbb{Z}_2$的扩张, 这说明同样的两个群因扩张方式的不同可能得到不同的群结构.
第四个例子中S_3是$\mathbb{Z}_2$过$\mathbb{Z}_3$的扩张, 注意到S_3是非$Abel$群, 这说明非常简单的群通过扩张可能得到结构较复杂的群.
第五个例子说明, 整数加群$\mathbb{Z}$可以看成$\mathbb{Z}_2$过自己的扩张, 因此有时扩张并不一定改变群的结构.
最后一个例子说明, $\mathrm{O}(n)$是$\mathbb{Z}_2$过 $\mathrm{SO}(n)$的扩张, 这时 $\mathrm{O}(n)$却与 $\mathrm{SO}(n)$不同构 (为什么?).

知道, 在线性空间的研究中子空间和商空间起到关键作用.事实上群的研究中由正规子群及对应的商群确定的扩张的概念也重要.
群G是B过A的扩张, 从某种意义上说, 实际上是把群G分解了, 或者说G是由A和B以某种方式拼出来的.
从上表中的例子可以看出, B过A的扩张不是唯一的.
研究群的扩张的一个自然的问题是 : B过A的扩张有多少种?其中哪些是本质上一样的?
在深入讨论这一思想之前, 我们先研究扩张的一般性质.

Theorem 2.58

设A, B, G, G'是群.
(1)若G是B过A的扩张, $G \cong G'$, 则G'也是B过A的扩张.
(2)若G, G'都是B过A的扩张, 且有群同态$f: G \to G'$使得下图可交换$\lambda' = f \circ \lambda, \mu' \circ f = \mu$, 则$f$是群同构.
此时, 称G与G'是B过A的等价扩张.



Proof (1)由扩张$1\longrightarrow A\xrightarrow{\lambda}G\xrightarrow{\mu}B\longrightarrow 1$及同构$f:G\to G'$,定义$\lambda'=f\lambda,\mu'=\mu f^{-1}$.显然$\lambda'$是单同态,$\mu'$是满同态.
进一步,$\mathrm{Ker}\mu'=\mathrm{Ker}\left(\mu f^{-1}\right)=f(\mathrm{Ker}\mu)=f(\lambda(A))=\lambda'(A)$.故$1\longrightarrow A\xrightarrow{\lambda'}G'\xrightarrow{\mu'}B\longrightarrow 1$是短正合列,即$G'$是$B$过$A$的扩张.

(2)需要证明f是双射.若$f(x)=e$,则$\mu(x)=\mu' f(x)=e$.因此$x\in\mathrm{Ker}\mu=\mathrm{Im}\lambda$.
故存在$y\in A$使得$x=\lambda(y)$.于是$\lambda'(y)=f\lambda(y)=f(x)=e$.因$\lambda'$是单射,故$y=e$,从而$x=e$,即$f$是单射.
又对任意$z\in G'$,由μ是满同态知存在x使得$\mu'(z)=\mu(x)=\mu' f(x)$.
于是$z^{-1}f(x)\in\mathrm{Ker}\mu'=\mathrm{Im}\lambda'$,则存在$y\in A$使得$z^{-1}f(x)=\lambda'(y)=f(\lambda(y))$.因此$z=f\left(x\lambda(y)^{-1}\right)\in\mathrm{Im}f$.故$f$是满射.

Theorem 2.59

设G是B过A的扩张,N是扩张核,对应的短正合序列为$A\xrightarrow{\lambda}G\xrightarrow{\mu}B$
(1)若存在$H<G$满足$G=HN,H\cap N=\{e\}$,则 $\mu|_H$ 是H到B上的同构,此时$\nu=(\mu|_H)^{-1}$ 是B到G的同态且$\mu\nu=\mathrm{id}_B$.
(2)若存在B到G的同态ν使得$\mu\nu=\mathrm{id}_B$,则$H=\nu(B)<G$且$G=HN,H\cap N=\{e\}$.

Proof (1)这就是同构基本第三定理的表示

(2)H自然是G的子群且ν是B到H的同构.
若$g\in H\cap N$,则存在$b\in B$使得$g=\nu(b)$.又因$\mu\nu=\mathrm{id}_B$,有$b=\mu\nu(b)=\mu(g)=e$,故$H\cap N=\{e\}$.
现设$g\in G$,则存在$h\in H$使得$\mu(g)=\mu(h)$.因此,$\mu\left(h^{-1}g\right)=e$,故$n=h^{-1}g\in N$,于是$g=hn$.从而$G=HN$.

Definition 2.54 (非本质扩张，平凡扩张，中心扩张)

设G是B过A的扩张,N是扩张核,对应的短正合序列为$A\xrightarrow{\lambda}G\xrightarrow{\mu}B$
1.若有$H<G$满足$G=HN,H\cap N=\{e\}$,则称此扩张为非本质扩张,此时,$G=H\ltimes N$为H与N的半直积.
2.若在非本质扩张进一步,如果$H\triangleleft G$,则称此扩张为平凡扩张,此时,$G=H\times N$为H与N的直积.
3.如果$N\subseteq C(G)$,则称此扩张为中心扩张.

Problem 2.1
(1)$\mathbb{Z}$是$\mathbb{Z}/2\mathbb{Z}$过$\mathbb{Z}$的扩张,但不是非本质扩张.
(2)$n\geqslant 3$时,S_n是$\mathbb{Z}/2\mathbb{Z}$过A_n的非本质扩张.
(3)$\mathrm{O}(n)$是$\mathbb{Z}/2\mathbb{Z}$过 $\mathrm{SO}(n)$的非本质扩张.
(4)15阶循环群是$\mathbb{Z}/3\mathbb{Z}$过$\mathbb{Z}/5\mathbb{Z}$的平凡扩张.

Lemma 2.11

类似于空间直和分解我们有
设A,B是G的子群,$G=AB$,则下列命题等价.
(1)$A\cap B=\{e\}$;
(2)任意$g\in G$,g的分解$g=ab(a\in A,b\in B)$唯一;
(3)幺元的分解唯一.

Proof (1) $\Longrightarrow$ (2) : 反证法即可
(2) $\Longrightarrow$ (3) : 自然结论
(3) $\Longrightarrow$ (1) : 反证法即可利用$e\neq k\in A\cap B$那么同样有$k^{-1}\in A\cap B$相乘即可

Lemma 2.12

设A,B是G的子群，$G=AB, A\cap B=\{e\}$，则A,B都是G的正规子群 $\Longleftrightarrow$ 对任意$a\in A, b\in B, ab=ba$.

Proof

若A,B都是G的正规子群，则对任意$a\in A, b\in B, a^{-1}b^{-1}ab=a^{-1}\left(b^{-1}ab\right)\in A$，且$a^{-1}b^{-1}ab=\left(a^{-1}b^{-1}a\right)b\in B$，因此$a^{-1}b^{-1}ab=e$，故$ab=ba$.

反之，对任意$g\in G$，存在$a\in A, b\in B$使得$g=ab$.对任意$x\in A$，由于$xb=bx$，有$gxg^{-1}=abxb^{-1}a^{-1}=axa^{-1}\in A$，因此$A\triangleleft G$.同样$B\triangleleft G$.

Theorem 2.60

设A,B为群，则B过A的平凡扩张G在同构意义下是存在唯一的.

Proof 存在性.令$G=\{(a,b)\mid a\in A, b\in B\}$，在$G$中定义乘法为$(a_1,b_1)\circ(a_2,b_2)=(a_1a_2,b_1b_2)$，$a_1,a_2\in A$，$b_1,b_2\in B$，则容易验证$G$是群.

此外，不难得到$A_1=\{(a,e_B)\mid a\in A\}, B_1=\{(e_A,b)\mid b\in B\}$都是$G$的正规子群且$G=A_1\otimes B_1$.

唯一性.设G'也是A过B的平凡扩张，则$G'=A'\otimes B'$，这里A'和B'分别是G'的同构于A和B的正规子群.

记λ为A到A'的同构，μ是B到B'的同构，则容易验证$f:G\to G', f(a,b)=\lambda(a)\mu(b)$为$G$到$G'$的群同构.

本节余下的部分我们将用扩张的思想深入研究群的结构.

设A_1是G的正规子群，$B=G/A_1$，则有短正合序列$1\longrightarrow A_1\xrightarrow{\lambda}G\xrightarrow{\mu}B\longrightarrow 1$.

如果B也有非平凡正规子群B_1，令$B_2=B/B_1$，于是又有短正合序列$1\longrightarrow B_1\xrightarrow{\lambda_1}B\xrightarrow{\mu_1}B_2\longrightarrow 1$.

这样做下去，可以得到一系列的群.表面上，这样得到的群似乎与群G关系不大.

我们换一个角度来看，考虑映射的合成$G\xrightarrow{\mu}B\xrightarrow{\mu_1}B_2$这样我们得到满同态$\mu_1\circ\mu:G\to B_2$

其核$A_0=(\mu_1\circ\mu)^{-1}(1)=\mu^{-1}(B_1)$为$G$的包含$A_1$的正规子群，且$A_0/A_1\cong B_1, G/A_0\cong B_2$.

对A_1进行类似操作，又可找到A_1的正规子群A_2.于是我们得到一个序列$G\supset A_0\supset A_1\supset A_2\supset\cdots$为了方便，我们引入如下定义.

Definition 2.55 (次正规序列、正规序列、合成序列、主序列)

1.群G中的子群序列$G=G_1\supset G_2\supset\cdots\supset G_t\supset G_{t+1}=\{e\}$.

若满足$G_{i+1}\triangleleft G_i(i=1,\cdots,t)$，则称为次正规序列，称$t$为此序列的长度，$G_i/G_{i+1}$为此序列的因子.

2.群G中的次正规序列$G=G_1'\supset G_2'\supset\cdots\supset G_s'\supset G_{s+1}'=\{e\}$称为原序列的加细：如果原序列中的每个子群$G_i$都在新序列中出现.

3.若在上述序列中$G_i\triangleleft G$，则称此序列为正规序列.

4.如果G的次正规序列的因子G_i/G_{i+1}都是单群，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.

5.进一步，如果合成序列还是正规序列，则称为主序列.

Note 如何理解G_i/G_{i-1}是单群，这意味着$G_{i-1}\lhd G_i$，在G_{i-1}与G_i中再也没有包含了G_{i-1}且是G_i的正规子群了否则根据同构定理就有G_i/G_{i-1}不是单群

Problem 2.2

(1)当$n=3$或$n\geqslant 5$时，$S_n\supset A_n\supset\{e\}$是$S_n$的主序列.

(2)$S_4\supset A_4\supset K_4\supset\langle(12)(34)\rangle\supset\{e\}$是$S_4$的合成序列不是主序列.

(3)$G=Z_{15}\supset Z_3\supset\{e\}$与$G=Z_{15}\supset Z_5\supset\{e\}$为$G$的两个不同的主序列.

Theorem 2.61 (*Schreier*(施赖埃尔) 定理)

1.有限群的任意一个次正规群列都可以加细为合成群列

2.任意有限群皆有合成群列

Proof 设$G=G_0>G_1>\ldots>G_r=\{e\}$是$G$的一个次正规群列

如果有某个$i(1\leqslant i\leqslant r)$使得$G_{i-1}/G_i$不是单群，即$G_{i-1}/G_i$有非平凡的正规子群$\bar{H}$

由群的第一同构定理可知：$\bar{H}$在典范同态$G_{i-1}\to G_{i-1}/G_i$下的反像H为G_{i-1}的正规子群，且$G_{i-1}\neq H\neq G_i$

(因$\bar{H}\neq e/G_i$且$\bar{H}\neq G_{i-1}/G_i$)

于是$G=G_0>G_1>\ldots G_{i-1}>H>G_i>\ldots>G_r=\{e\}$是$G$的长度为$r+1$的次正规群列

由于G是有限群，所以次正规群列的长度有限.故上述的加细过程必在有限步之后停止，此时相邻的两个群的商群都是单群.

这个群列就是合成群列

设G为有限群。不妨设$|G|>1$，对于次正规群列$G>\{e\}$利用1即可得证。

Theorem 2.62 ($Jordan-Hylder$定理)

设群G存在合成序列，则G的任意两个合成序列同构.特别地，G的任意两个主序列也同构.

Proof 假设G有两个次正规序列$\begin{cases}G=G_1\supset G_2\supset G_3\supset\cdots\supset G_t=\{e\},\\ G=H_1\supset H_2\supset H_3\supset\cdots\supset H_s=\{e\}.\end{cases}$

考虑$H_i=H_i\cap G_1\supseteq H_i\cap G_2\supseteq\cdots\supseteq H_i\cap G_t=\{e\}$.去掉其中相同的项就得到$H_i$的次正规序列.

(这一步不难验证$H_i\cap G_{j+1}\lhd H_i\cap G_j$)

为了使得到的序列中的其每一项都包含H_{i+1}，我们考虑$H_i=(H_i\cap G_1)H_{i+1}\supseteq(H_i\cap G_2)H_{i+1}\supseteq\cdots\supseteq(H_i\cap G_t)H_{i+1}=H_{i+1}$.

由于H_i/H_{i+1}为单群，故存在唯一的i'使得$H_i=(H_i\cap G_{i'})H_{i+1}$，且$(H_i\cap G_{i'+1})H_{i+1}=H_{i+1}$.

(这一步我们知道因为H_i/H_{i+1}为单群所以H_i与H_{i+1}之中不能再有包含了H_{i+1}且是H_i的正规子群了)

(所以针对$H_i=(H_i\cap G_1)H_{i+1}\supseteq(H_i\cap G_2)H_{i+1}$而言$(H_i\cap G_2)H_{i+1}$要么等于$H_{i+1}$要么等于$H_i$以此类推我们就有上式论断)

于是有

$$\begin{aligned}H_i/H_{i+1}&\cong(H_i\cap G_{i'})H_{i+1}/(H_i\cap G_{i'+1})H_{i+1}\\&\cong H_i\cap G_{i'}/(H_i\cap G_{i'}\cap(H_i\cap G_{i'+1})H_{i+1})\ (\text{这一步由于同构第三基本定理})\\&=H_i\cap G_{i'}/(G_{i'}\cap(H_i\cap G_{i'+1})H_{i+1})\\&=H_i\cap G_{i'}/(G_{i'}\cap H_{i+1})(H_i\cap G_{i'+1}).\end{aligned}$$

同样，对于$G_{i'}\subset G_{i'+1}$进行类似的处理，可以得到

$G_{i'}/G_{i'+1}\cong H_i\cap G_{i'}/(G_{i'}\cap H_{i+1})(H_i\cap G_{i'+1})\cong H_i/H_{i+1}$.

这样指标集$\{i\}$与$\{i'\}$存在一一对应，从而$G_{i'}/G_{i'+1}$与H_i/H_{i+1}之间的对应是一一的，因此这两个合成序列在同构意义下是唯一的.

设G的两个无重复项的合成群列为$\begin{cases}G=G_0\triangleright G_1\triangleright\cdots\triangleright G_r=\{e\},(*)\\ G=H_0\triangleright H_1\triangleright\cdots\triangleright H_s=\{e\}.(**)\end{cases}$

对第一个合成群列的长度r做数学归纳法.

若$r=1$，则G为单群.由于单群G只有两个正规子群：$\{e\}$和G，因此G的无重复项的合成群列只有一个：$G\triangleright\{e\}$.从而当$r=1$时，命题为真.

假设对于第一个合成群列的长度为$r-1$时命题成立，现在来看第一个合成群列的长度为r的情形.

先看一个特殊情形：若$G_1=H_1$，则在上述两个合成群列中去掉第一项后，就是同一个群$G_1=H_1$的合成群列，它们的长度分别为$r-1$和$s-1$.

根据归纳假设得，$r-1=s-1$，从而$r=s$；而且它们的因子群组能用某种方法配对，使得对应的因子群同构

从而$(*),(**)$的因子群组也有这样的性质.

下面讨论一般情形,即$G_1 \neq H_1$的情形.由于G/G_1和G/H_1都是单群,因此它们的正规子群分别只有$G/G_1, G_1/G_1$和$G/H_1, H_1/H_1$.
从而G的包含G_1的正规子群只有G, G_1;G的包含H_1的正规子群只有G, H_1.由于$G_1 \neq H_1$,因此$G_1H_1 \supsetneq G_1, G_1H_1 \supsetneq H_1$.
由于$G_1 \triangleleft G, H_1 \triangleleft G$,因此$G_1H_1 \triangleleft G$,从而$G_1H_1 = G$.(因为$G_1H_1$严格真包含了$H_1$所以不能再是$G$的正规子群了否则与$G/H_1$都是单群矛盾)
令$G_1 \cap H_1 = N_2$,则根据第一群同构定理得 $\begin{cases} N_2 \triangleleft G_1, & G_1/N_2 \cong G/H_1; \\ N_2 \triangleleft H_1, & H_1/N_2 \cong G/G_1. \end{cases}$
任意取定N_2的一个无重复项的合成群列$N_2 \triangleright N_3 \triangleright \cdots \triangleright N_t = \{e\}$
利用它做出G的两个新的无重复项的合成群列:
$$G = G_0 \triangleright G_1 \triangleright N_2 \triangleright \cdots \triangleright N_t = \{e\}, (i)$$
$$G = H_0 \triangleright H_1 \triangleright N_2 \triangleright \cdots \triangleright N_t = \{e\}. (ii)$$
比较 $(*)$和 (i),G的这两个合成群列的第二项相同,于是根据前面讨论的特殊情形的结论得,$r = t$
且 $(*)$的因子群组$G/G_1, \quad G_1/G_2, \quad G_2/G_3, \cdots, \quad G_{r-1}/G_r$ (1)
与 (i)的因子群组$G/G_1, \quad G_1/N_2, \quad N_2/N_3, \cdots, \quad N_{r-1}/N_r$ (2)
能用某种方法配对,使得对应的因子群是同构的.
再比较 $(**)$和 (ii),G的这两个合成群列的第二项相同,于是根据前面的特殊情形的结论得,$s = t$,从而$r = s$
且 $(**)$的因子群组$G/H_1, \quad H_1/H_2, \quad H_2/H_3, \cdots, \quad H_{r-1}/H_r$ (3)
与 (ii)的因子群组$G/H_1, \quad H_1/N_2, \quad N_2/N_3, \cdots, \quad N_{r-1}/N_r$ (4)
能用某种方法配对,使得对应的因子群是同构的.
由于$G/G_1 \cong H_1/N_2, \quad G_1/N_2 \cong G/H_1$
则因子群组 (1)与因子群组 (4)能够配对,使得对应的因子群是同构的.
从而 (2) 与 (3) (这是因为 (1) 与 (2) 配对, (3) 与 (4) 配对传递一下即可) 能用某种方法配对,使得对应的因子群是同构的.
这证明了对于第一个合成群列的长度为r时命题为真.

2.16 The Action of Groups on Sets

Definition 2.56 (群在集合上的作用)

设G是一个群，X是一个非空集合

若映射$f:G\times X\to X,\quad (g,x)\to f(g,x)$满足对任何$x\in X,g_1,g_2\in G$都有$f(e,x)=x$与$f(g_1g_2,x)=f(g_1,f(g_2,x))$

则称f决定了G在X上的一个作用.通常,我们将$f(g,x)$简记为$g(x)$或gx

此时两个条件我们可以简写：对任何$x\in X,g_1,g_2\in G$都有$e(x)=x$与$g_1g_2(x)=g_1(g_2(x))$

Theorem 2.63 (群同态与群作用联系)

1.G作用在集合X上其中f为作用映射$f:G\times X\to X$那么

$\forall g\in G$构造$\varphi_g:X\to X\ \ x\mapsto g(x)$那么证明$\varphi_g\in S_X$

其次构造$\psi:G\to S_X\ \ g\mapsto\varphi_g$证明该$\psi$是一个同态映射

2.若$\sigma:G\to S_X\ \ g\mapsto\sigma_g$的一个同态映射那么即可构造

G在集合X上的作用$f:G\times X\to X\ \ f(g,x)=\sigma_g(x)$

从而上述两条说明：群G在集合X上的作用全体与G到S_X的同态全体存在一一对应

Definition 2.57 (群在集合上作用分类)

设群G作用在集合X上

若对任意$x,y\in X$，存在$g\in G$使得$gx=y$，则称G在X上的作用可递，这时称X为G的齐性空间

若对$g\in G$，由$gx=x,\forall x\in X$，可以推出$g=e$，则称G在X上的作用有效

若对任意$g\in G$，$x\in X$都有$gx=x$，则称G在X上的作用平凡

Proposition 2.43

G在X上作用是有效的$\iff$该作用对应的群同态是单射

G在X上作用是平凡的$\iff$该作用对应的群同态是平凡的

G在X上作用是有效的$\Longrightarrow G$与X的一个变换群同构具体的有$G\cong\sigma(G)$

Proof 设群同态$\sigma:G\to S_X\ \ g\mapsto\sigma_g$

G在X上作用是有效的$\iff g\in G.$若$g(x)=x\ \ \forall x\in X\Rightarrow g=e\iff g\in G$若$\sigma_g(x)=x\ \ \forall x\in X\Rightarrow g=e$

$\iff g\in G$若$\sigma_g=id_{S_X}\Rightarrow g=e\iff Ker\sigma=\{e\}\iff$为单射

平凡的同理

紧接着有$G\cong\sigma(G)$单射满射显然

Proposition 2.44 (几个群作用的典型例子)

设G是一个群，令$X=G$我们可以构造如下几种群作用$f:G\times G\to G$

(1) 左平移作用：$f(g,x)=L_g(x)=gx$

(2) 右平移作用：$f(g,x)=R_{g^{-1}}(x)=xg^{-1}$

(3) 伴随(共轭)作用：$f(g,x)=\mathrm{Ad}_g(x)=gxg^{-1},andthegxg^{-1}$称为$x$的一个$conjugateofx.$

设H是G的一个子群，定义映射$f:G\times G/H\to G/H$为$f(g,xH)=(gx)H,\quad\forall g,x\in G$

则容易验证f是一个作用．这一作用也称为G在G/H上的左平移作用．

其中不难验证：左平移与右平移作用即可递也是有效，伴随作用不一定可递也不一定有效
G在G/H上的左平移作用可递但不一定有效

Lemma 2.13

群G作用在集合X上，此时在X上定义关系$R: xRy \iff \exists g \in G$使得$g(x)=y$
这是一个等价关系

Proof 1.$e(x)=x$ 2.$xRy \Longrightarrow g(x)=y$则$g^{-1}(y)=g^{-1}(g(x))=x$成立 3.$xRy, yRz$那么$g(x)=y$且$h(y)=z$那么$gh(x)=z$

Definition 2.58 (轨道)

设群G作用在集合X上，$x \in X$. 称X的子集$O_x=\{g(x) \mid g \in G\}$为$x$的轨道，若$|O_x|=1$则称$x$是$G$的不动点 The name is the orbits of G on S

Proposition 2.45

1.O_x即x所在的等价类 2.$\forall g \in G$有$gO_x=O_x$ 3.G在O_x上的作用是可递
4.G在X的作用可递 $\iff$ X仅有一个轨道

Definition 2.59 (迷向子群 (isotropy subgroup or stabilizer of x))

群G作用在集合X上，$x \in X$此时考察
$F_x=\{g \in G \mid g(x)=x\}$容易验证这是$G$当中的子群称之为迷向子群

Proposition 2.46

群G作用在集合X上，$x \in X$.其中O_x为x的轨道，F_x为x的迷向子群
1.G在O_x上的作用有效 $\iff$ F_x中包含G的正规子群只有$\{e\}$
2.令$g \in G$此时$F_{g(x)}=\mathrm{Ad}_g(F_x)=gF_xg^{-1}$

Proof 1.G作用在O_x上决定了一个群同态$\sigma: G \to S_{O_x}$ $g \mapsto \sigma_g$其中$\sigma_g: O_x \to O_x$ $y \mapsto g(y)$
此时G在O_x上的作用有效 $\iff$ 上述群同态σ为单射$Ker\sigma=\{e\}$ $\iff$ $N \triangleleft G$且$N \subseteq F_x$则$N=\{e\}$
一方面若$Ker\sigma=\{e\}$此时$N \triangleleft G$且$N \subseteq F_x$此时只需证明$N \subseteq Ker\sigma$故$\forall h \in N$
仅需证明$\sigma(h)=id_{O_x} \iff \sigma_h=id_{O_x} \iff \forall y \in O_x$成立$\sigma_h(y)=y \iff \forall y \in O_x$成立$h(y)=y$因为$y \in O_x$故$y$可写为$g(x)$ $x \in G$
$\iff \forall x \in G$成立$hg(x)=g(x) \iff \forall x \in G$成立$g^{-1}hg(x)=x$
因为$h \in N \triangleleft G$故$g^{-1}hg \in N \subseteq F_x$故上式最后成立
另一方面：若$N \triangleleft G$且$N \subseteq F_x$则$N=\{e\}$我们来证明$Ker\sigma=\{e\}$
显然$Ker\sigma \triangleleft G$此时我们仅需证明：$Ker\sigma \subseteq F_x$故$\forall h \in Ker\sigma$
仅需证：$h \in F_x \iff h(x)=x$
而$h \in Ker\sigma \Longrightarrow \sigma(h)=id_{O_x} \Longrightarrow h(x)=x$（因为$x=e(x)$自然也在$O_x$中）证毕

2.下证：$F_{g(x)}=\mathrm{Ad}_g(F_x)=gF_xg^{-1}$
一方面：$\forall h \in F_{g(x)}$仅需证$h \in gF_xg^{-1}$我们有$hg(x)=g(x) \Longrightarrow g^{-1}hg(x)=x \Longrightarrow g^{-1}hg:=t \in F_x$
故$h=gtg^{-1} \in gF_xg^{-1}$
另一方面：$\forall h \in gF_xg^{-1}$不妨设$h=gtg^{-1}$其中$t \in F_x \Longrightarrow t(x)=x$
仅需证$h \in F_{g(x)} \iff hg(x)=g(x)$而$hg(x)=gt(x)=g(x)$证毕

Definition 2.60 (群作用等价)

设群G作用在集合X与X'上, 若有X到X'的双射φ使得$g(\varphi(x))=\varphi(g(x)), \forall g\in G, x\in X$则称$G$在$X$与$X'$上的作用等价.

Theorem 2.64 (可递群作用的等价)

设群G在集合X上的作用可递, $x\in X$则G在X上的作用于G/F_x上的左平移作用等价$\left(F_x\text{为}x\text{的迷向子群}\right)$

Proof 注意到G在X上的作用可递于是$O_x=X$

首先构造双射$\varphi: G/F_x\to X\ \ gF_x\mapsto g(x)$

1.映射与单射：若$aF_x=bF_x\Longleftrightarrow b^{-1}a\in F_x\Longleftrightarrow b^{-1}a(x)=x\Longleftrightarrow a(x)=b(x)$

2.满射：$\forall h\in X=O_x$故$h=g_0(x)$故$\varphi(g_0F_x)=h$

其次我们来验证作用等价这一条

$\forall k\in G$与$gF_x\in G/F_x$此时我们要说明：$\varphi(k(gF_x))=k(\varphi(gF_x))$

此时$RHS=kg(x)=LHS$

Theorem 2.65 (轨道稳定化子定理)

$|O_x|=|G/F_x|=[G:F_x]\Longrightarrow |O_x|\Big||G|$

Proof 利用G在O_x上的作用是可递的且$x\in O_x$$\left(\text{因为}x=e(x)\right)$，那么就有双射$G/F_x\to O_x$

那么$|O_x|=|G/F_x|\Longrightarrow |O_x|\,||G|$

Example 2.29

1.If a group G acts on itself by conjugation, then the **orbit** $\{gxg^{-1}\mid g\in G\}$ of $x\in G$ is called the **conjugacy class** of x. The **isotropy group or the stabilizer of x**

$$G_x=\{g\in G\mid gxg^{-1}=x\}=\{g\in G\mid gx=xg\}$$

is called the **centralizer** of x in G and is denoted $C_G(x)$. The conjugacy classes of G form a partition of G, and the size of the conjugacy class of x is equal to the index $O_x=[G:C_G(x)]$.

2.If a subgroup H acts on G by conjugation, the **isotropy group or the stabilizer of x**

$$H_x=\{h\in H\mid hxh^{-1}=x\}=\{h\in H\mid hx=xh\}$$

is called the **centralizer of x in H** and is denoted $C_H(x)$.

3. If H acts by conjugation on the set S of all subgroups of G,the **isotropy group or the stabilizer of K** namely

$$\{h\in H\mid hKh^{-1}=K\},$$

is called the **normalizer** of K in H and denoted $N_H(K)$.

4.If G acts by conjugation on the set of all its subgroups, the **isotropy group or the stabilizer of K**

$$\{g\in G\mid gKg^{-1}=K\},$$

is called the **normalizer** of K in G and denoted $N_G(K)$.And the **orbit of K** under this action is the set of all subgroups of G that are conjugate to K equally all the conjugate groups of K

Clearly every subgroup K is normal in $N_G(K)$; K is normal in G if and only if $N_G(K)=G$.

Proposition 2.47

Let G be a finite group and K a subgroup of G.

(i) The number of elements in the conjugacy class of $x \in G$ is $[G : C_G(x)]$, which divides $|G|$;

(ii) if $x_1, \ldots, x_n (x_i \in G)$ are the distinct conjugacy classes of G, then

$$|G| = \sum_{i=1}^{n} |G : C_G(x_i)|;$$

(iii) the number of subgroups of G conjugate to K is $[G : N_G(K)]$, which divides $|G|$.

Corollary 2.22

Let G be a group.

(i) For each $g \in G$, conjugation by g induces an automorphism of G.

(ii) There is a homomorphism $G \to \mathrm{Aut}\, G$ whose kernel is $C(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$.

♡

Proof (i) If G acts on itself by conjugation, then for each $g \in G$, the map $\tau_g : G \to G$ given by $\tau_g(x) = gxg^{-1}$ is a bijection by the proof of Theorem 4.5. It is easy to see that τ_g is also a homomorphism and hence an automorphism. (ii) Let G act on itself by conjugation. By (i) the image of the homomorphism $\tau : G \to A(G)$ of Theorem is contained in $\mathrm{Aut}\, G$. Clearly

$$g \in \mathrm{Ker}\, \tau \Leftrightarrow \tau_g = 1_G \Leftrightarrow gxg^{-1} = \tau_g(x) = x \quad \text{for all } x \in G.$$

But $gxg^{-1} = x$ if and only if $gx = xg$, whence $\mathrm{Ker}\, \tau = C(G)$.

Definition 2.61

The automorphism τ_g of $\tau_g(x) = gxg^{-1}$ is called the **inner automorphism** induced by g. The normal subgroup $C(G) = \mathrm{Ker}\, \tau$ is called the **center** of G.

Corollary 2.23

1.An element $g \in G$ is in $C(G)$ if and only if the conjugacy class of g consists of g alone and hence if and only if $C_G(g) = G$.

2.Thus if G is finite and $x \in C(G)$, then $[G : C_G(x)] = 1$. Consequently, the class equation of G may be written

$$|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)],$$

where $x_1, \ldots, x_m$ $(x_i \in G - C(G))$ are distinct conjugacy classes of G and each $[G : C_G(x_i)] > 1$.

♡

Proposition 2.48

Let H be a subgroup of a group G and let G act on the set S of all left cosets of H in G by left translation. Then the kernel of the induced homomorphism $G \to A(S)$ is contained in H.

Proof

The induced homomorphism $G \to A(S)$ is given by $g \mapsto \tau_g$, where $\tau_g : S \to S$ and $\tau_g(xH) = gxH$. If g is in the kernel, then $\tau_g = 1$ and $gxH = xH$ for all $x \in G$; in particular for $x = e$, $geH = eH = H$, which implies $g \in H$.

Corollary 2.24

If H is a subgroup of index n in a group G and no nontrivial normal subgroup of G is contained in H, then G is isomorphic to a subgroup of S_n.

♡

Proof Assume the group G acts on all cosets of H in G; the kernel of $G \to A(S)$ is a normal subgroup of G contained in H and must

therefore be $\langle e \rangle$ by hypothesis. Hence, $G \to A(S)$ is a monomorphism. Therefore G is isomorphic to a subgroup of the group of all permutations of the n left cosets of H, and this latter group is clearly isomorphic to S_n.

Corollary 2.25

If H is a subgroup of a finite group G of index p, where p is the smallest prime dividing the order of G, then H is normal in G. ♡

Proof Let S be the set of all left cosets of H in G. Then $A(S) \cong S_p$ since $[G : H] = p$. Assume group acts on all cosets of H in G is left translation action.And assume K is the kernel of the homomorphism $G \to A(S)$, then K is normal in G and contained in H. Furthermore G/K is isomorphic to a subgroup of S_p. Hence $|G/K|$ divides $|S_p| = p!$. But every divisor of $|G/K| = [G : K]$ must divide $|G| = |K|[G : K]$. Since no number smaller than p (except 1) can divide $|G|$, we must have $|G/K| = p$ or 1. However $|G/K| = [G : K] = [G : H][H : K] = p[H : K] \geq p$. Therefore $|G/K| = p$ and $[H : K] = 1$, whence $H = K$. But K is normal in G.

Proposition 2.49

群G作用在集合X上,Y是X的子集,令$F_Y = \{g \in G |\ g(Y) = Y\}$

若对X的子集Z,若$\exists g \in G$是的$Z = g(Y)$那么称Z与Y在G的作用下共轭

1.F_Y是群G的子群　2.$F_{g(Y)} = \mathrm{Ad}_g(F_Y)$　3.若G为有限群则X中与Y共轭的子集恰为$[G : F_Y]$个

Proof 构造群G作用在幂集$P(X)$上$f : G \times P(X) \to P(X)$　$(g, Y) \mapsto g(Y)$

2.17 Sylow 子群

Definition 2.62 (p 子群与 Sylow p 子群)

设p是一个素数, 若群G的阶$|G|=p^k\ (k>0)$我们则称G是一个p群

若群G且$|G|=p^lm$其中p为素数, $(p,m)=1$称群G的一个p^l阶的子群为$Sylow\ p$子群

Lemma 2.14 (p 群与不动点集合引理)

设p群$G\ (|G|=p^k)$作用在集合X上, $|X|=n$

记不动点集合: $\{x\in X|\ \forall g\in G有g(x)=x\}$ 记$t=\left|\{x\in X|\ \forall g\in G有g(x)=x\}\right|$

1.$t\equiv n\ (\mathrm{mod}p)$　2.若$(n,p)=1$那么$t\geqslant 1$　3.$C(G)\neq\{e\}$

Proof 1.我们知道$X=O_{x_1}\cup O_{x_2}\cdots\cup O_{x_m}$而我们注意若一个轨道$O_x$含有不动点集合中的任何一个那么$O_x=\{x\}, |O_x|=1$

此时我们有如下的阶数估计:

$$n=|X|=\sum|O_{x_i}|=t+\sum_{|O_{x_i}|>1}|O_{x_i}|\quad(*)$$

此时对于$\sum_{|O_{x_i}|>1}|O_{x_i}|$之中的$|O_{x_i}|$有$|O_{x_i}|=[G:F_{x_i}]\ ||G|=p^k$那么有形如$|O_{x_i}|=p^s\ (s\geqslant 1)$

故对于$(*)$我们就有$p|\sum_{|O_{x_i}|>1}|O_{x_i}|\Longrightarrow t\equiv n\ (\mathrm{mod}p)$

2.此时t作为不动点集合的势, 我们断言$t\neq 0$故$t\geqslant 1$

若$t=0$此时, 我们由1.知$p|n$但与已知条件$(n,p)=1$矛盾

3.显然$e\in C(G)$我们来证明$|C(G)|>1$即可

若$x\in C(G)$则$\forall g\in G有gx=xg$即$gxg^{-1}=x$这意味着x即为G在G上共轭作用的不动点

故我们搞清楚了只需证: 即为G在G上共轭作用的不动点个数>1即可

若G在G上共轭作用的不动点个数$=1$

同样运用$n=|X|=\sum|O_{x_i}|=t+\sum_{|O_{x_i}|>1}|O_{x_i}|$　此时相当于集合X仍然为G

故p整除$n=p^k$且p又整除$\sum_{|O_{x_i}|>1}|O_{x_i}|\Longrightarrow p$整除1矛盾

Lemma 2.15

设$n=p^lm$, 其中p是素数, $(p,m)=1$且$l\geqslant 1\Longrightarrow$有$\forall 1\leqslant k\leqslant l$由$p^{l-k}\parallel C_n^{p^k}$

Proof 用$\varphi(u)$来表示正整数u中因子p的个数

下面我们就来证明$\varphi\left(C_n^{p^k}\right)=l-k$

$$此时C_n^{p^k}=\frac{n(n-1)\cdots(n-p^k+1)}{p^k(p^k-1)\cdots 1}=\frac{p^lm(n-1)\cdots(n-p^k+1)}{p^k(p^k-1)\cdots 1}=p^{l-k}m\prod_{i=1}^{p^k-1}\frac{n-i}{p^k-i}$$

故我们继续证明$\varphi\left(\prod_{i=1}^{p^k-1}\frac{n-i}{p^k-i}\right)=0$此时仅需证明$\forall 1\leqslant i\leqslant p^k-1$成立$\varphi\left(\frac{n-i}{p^k-i}\right)=0$

这只需证明$\forall 1\leqslant i\leqslant p^k-1$成立$\varphi(n-i)=\varphi\left(p^k-i\right)$

我们设$i=p^tj$此时$(p,j)=1, 0\leqslant t<k$

故$n-i=p^lm-p^tj=p^t\left(p^{l-t}m-j\right)$又$\left(p^{l-t}m-j,\ p\right)=1\Longrightarrow\varphi(n-i)=t$

故$p^k-i=p^t\left(p^{k-t}-j\right)$又$\left(p,\ p^{k-t}-j\right)=1\Longrightarrow\varphi\left(p^k-i\right)=t$

证毕

Theorem 2.66 (Sylow 第一定理)

群$G,|G|=p^lm=n,p$为一个素数,$(m,p)=1$且$l,k\in\mathbb{Z}^+$与$k\leqslant l$
$\Longrightarrow G$中一定存在p^k阶子群

Proof 我们想要找p^k阶子群于是我们在元素个数为p^k中集合上寻找
选取群G,选取集合$X=\{A\subseteq G|\ \ |A|=p^k\}$,作用:$g(A)=gA$　容易验证这是一个作用
此时$|X|=C_n^{p^k}=\sum|O_{A_i}|$(其中$O_{A_i}$为$X$中的轨道)
而根据引理我们有$p^{l-k+1}\nmid C_n^{p^k}=\sum|O_{A_i}|\Longrightarrow$至少存在一个$A_0\in X$使得$p^{l-k+1}\nmid|O_{A_0}|$
且由轨道稳定化子定理$\Longrightarrow|O_{A_0}||G|=p^lm$故不妨可以设$|O_{A_0}|=p^sm_1$(其中$s<l-k+1,m_1$为$m$的因子)
此时考察A_0的迷向子群$F_{A_0}<G$由轨道稳定化子定理知道$|F_{A_0}|=\dfrac{|G|}{|O_{A_0}|}=\dfrac{p^lm}{p^sm_1}\geqslant p^k\dfrac{m}{m_1}\geqslant p^k$
此时取$a\in A_0$则$F_{A_0}a\subseteq A_0$故$|F_{A_0}|\leqslant|A_0|=p^k$
$\Longrightarrow F_{A_0}=p^k$证毕

Proof

Assume $\mathscr{A}:=A\subseteq G|\ \ |A|=p^k$,and $|\mathscr{A}|=\binom{p^nm}{p^k}$.

And define the group action of G on $\mathscr{A}$ as $g(A)=gA$.And we know if Ω is a orbit then $|\Omega|\mid|G|$.So $|\omega|=ap^b,(a,p)=1,a\mid m,1\leqslant b\leqslant n$,

Assume $\Omega_1,\cdots\Omega_r,\Omega_1'\cdots,\Omega_s'$ are all orbits,and $|\Omega_i|=a_ip^{b_i},p\nmid a_i,b_i\leqslant n-k,|\Omega_j'|=c_jp^{d_j},d_j\geqslant n-k+1$.

Claim:$r\geqslant1$.

If not,then $|\mathscr{A}|=\sum_{j=1}^s|\Omega_j'|=p^{n-k+1}\sum_{j=1}^sc_jp^{d_j-n+k-1}$,which means $p^{n-k+1}\mid|\mathscr{A}|=\binom{p^nm}{p^k}$,.So $p^{n-k+1}\mid|\mathscr{A}|\Rightarrow p^{n-k+1}\mid p^{n-k}m\binom{p^nm-1}{p^k-1}\Rightarrow p\mid m\binom{p^nm-1}{p^k-1}$.Contradiction!

So there exists an orbit Ω_1 such that $|\Omega_1|=a_1p^{b_1},(a_1,p)=1,a_1\mid m,b_1\leqslant n-k$.And choose $A_1\in\Omega_1$ WLOG we can assume $1_G\in A_1$,because if not,we can choose any $g\in A_1$,then $g^{-1}A_1\in\Omega_1$ and $1_G\in g^{-1}A_1$. Now $|\Omega_1|=[G:G_{A_1}]$,G_{A_1} is the stabilizer of A_1. So $|G_{A_1}|=\dfrac{|G|}{|\Omega_1|}=p^{n-b_1}\dfrac{m}{a_1}$. $|G_{A_1}|\geqslant p^k$. And for any $g\in G_{A_1}$,we have $gA_1=A_1$,so $g\cdot1_G\in A_1$,which means $g\in A_1$.So $G_{A_1}\leqslant A_1$.Thus $|G_{A_1}|\leqslant|A_1|=p^k$. So $|G_{A_1}|=p^k$.And $A_1=G_{A_1}$.

Next we prove that the number of subgroup which is of order p^k is congruent to $1\mod p$ and divides m.

Firstly,we note that everyone Ω_i only has one subgroup of order p^k.Because if not,assume $H_1,H_2\leqslant G$ are two different subgroups of order p^k and both in Ω_i,then there exists $g\in G$ such that $gH_1=H_2$, so H_2 contains 1_G,thus assume $1_G\in H_2$,so there exists $h\in H_1$ such that $gh=1_G$,so $g=h^{-1}\in H_1$,thus $H_2=gH_1=h^{-1}H_1=H_1$.

Secondly,we note that Ω_j' has no subgroup of order p^k. Assume Q is a subgroup of order p^k , so we have the orbit which is generated by Q, denote it Orbit(Q), then $[G:G_Q]=p^{n-k}m$, so Orbit(Q) is not Ω_j'.

By calss equation,we have $|\mathscr{A}|=\sum_{i=1}^r|\Omega_i|+\sum_{j=1}^s|\Omega_j'|$

$$p^{n-k}m\binom{p^nm-1}{p^k-1}\equiv rp^{n-k}m(modp^{n-k+1})$$

So

$$r\equiv\binom{p^nm-1}{p^k-1}(modp)$$

By Lucas theorem we know $p^k-1=(p-1)+p(p-1)+\cdots+p^{k-1}(p-1)$ and $p^nm-1=p^n-1+p^n(m-1)=(p-1)+p(p-1)+\cdots+p^{n-1}(p-1)+p^n(m-1)$ So $\binom{p^nm-1}{p^k-1}\equiv1(modp)$.Thus $r\equiv1(modp)$.

Theorem 2.67 (Sylow 第二定理)

群$G,|G|=p^lm,p$为一个素数且$(p,m)=1$.

记P为G的一个 Sylow$p$子群。H为G的一个p^k $(k\leqslant l)$ 阶子群。记n_p为G中 Sylow $\cdot$ p子群个数

1.$\exists g\in G$使得$H\subseteq gPg^{-1}$　2.G的任意两个 Sylow $\cdot$ p子群共轭　3.$n_p=[G:N_G(P)]$

Proof 想要证明$\forall h\in H$有$h\in gPg^{-1}\Longleftrightarrow hg\in gP\Longleftrightarrow hgP=gP$(这里都是陪集的知识)

换个角度来看即h作用在gP上仍然为gP

于是考察群H作用在集合$X=G/P$上的左平移作用,我们想说明该作用存在不动点即可

此时我们知$|G/P|=m$且H为一个p群,那么由引理p群与不动点引理我们知道该作用的不动点$\geqslant 1$证毕

任取两个 Sylow $\cdot$ p子群P_1与P_2那么就知道存在g使得$P_1\subseteq gP_2g^{-1}$取阶数知道相等故$P_1=gP_2g^{-1}$

此时由本证明的前文我们就知道：记X_p为G中所有 Sylow $\cdot$ p子群的集合且$\left|X_p\right|=n_p$

此时我们就可以构造群G在X_p上的共轭作用,且该作用是可递的

任取$P\in X_p$此时其迷向子群$F_P=\left\{g\in G\mid\ gPg^{-1}=P\right\}=N_G(P)$且由轨道稳定化子定理知道

$\left|O_p\right|=\left|X_p\right|=[G:F_P]\Longrightarrow n_p=[G:N_G(P)]$

Theorem 2.68 (Sylow 第三定理)

群$G,|G|=p^lm.p$为一个素数且$(m,p)=1$

记n_p为群G中$Sylow p$子群的个数,记X_p为所有 Sylow $\cdot$ p子群的集合,记$n_p=\left|X_p\right|$

1.若P为G的一个 Sylow $\cdot$ p子群那么$P\lhd G\Longleftrightarrow n_p=1$　2.$n_p\mid m$且$n_p\equiv 1\,(\mathrm{mod}p)$

Proof 1.若P为G的一个 Sylow $\cdot$ p子群由$Sylow$第二定理知道$n_p=[G:N_G(P)]$

那么$P\lhd G\Longleftrightarrow N_G(P)=G\Longleftrightarrow n_p=1$

2.设P为G的一个 Sylow $\cdot$ p子群此时构造群P在集合X_p上的共轭作用

此时不难发现P即为该作用的不动点,此时任取不动点P_1则$\forall a\in P$有$aP_1a^{-1}=P_1\Longrightarrow a\in N_G(P_1)$

故$P<N_G(P_1)$且$P_1\triangleleft N_G(P_1)$且$N_G(P_1)<G$

此时由$|G|=p^lm$故$|N_G(P_1)|=p^*m_1$(*待定且m_1为m的因子)但是$p^l=|P_1|\,|p^*m_1$

$\Longrightarrow|N_G(P_1)|=p^lm_1$

故P与P_1均为$N_G(P_1)$当中的$Sylow\cdot p$子群故由1.知道在$N_G(P_1)$中仅仅只有一个$Sylow\cdot p$子群

$\Longrightarrow P=P1$这说明在群P在集合X_p上的共轭作用上不动点仅仅只有一个P

此时由p群与不动点引理我们就知道$n_p\equiv 1\,(\mathrm{mod}p)$

此外：由$Sylow$第二定理知道$n_p=[G:N_G(P)]\Longrightarrow\dfrac{n_p\cdot|N_G(P)|}{|P|}=\dfrac{|G|}{|P|}=m$又$P\lhd N_G(P)$

故$n_p\times[N_G(P):P]=m\Longrightarrow n_p\mid m$

Lemma 2.16

p is a prime number,and $(m,p)=1,n\geqslant 1,0\leqslant k\leqslant n$. And we assume $1\leqslant j\leqslant p^k-2$,then

$$p\nmid\binom{p^nm-j}{p^k-j}\Longleftrightarrow p\nmid\binom{p^nm-(j+1)}{p^k-(j+1)}$$

Proof

$$\binom{p^nm-j}{p^k-j}=\frac{p^nm-j}{p^k-j}\binom{p^nm-(j+1)}{p^k-(j+1)}$$

then talk about if $p\nmid j$ or $p\mid j$

Lemma 2.17

p is a prime number,and $(m,p)=1, n\geqslant 1, 0\leqslant k\leqslant n$. And we assume $1\leqslant j\leqslant p^k-2$,then

$$p\nmid \binom{p^n m-1}{p^k-1}$$

Proof

$p\nmid (p^n m-(p^k-1))=\binom{p^n m-(p^k-1)}{p^k-(p^k-1)}$ then use the previous lemma step by step to get the result.

Lemma 2.18 (Lucas Theorem)

Let p be a prime number. For any non-negative integers m and n, let their base p expansions be given by

$$m=m_k p^k+m_{k-1}p^{k-1}+\cdots+m_1 p+m_0,$$

$$n=n_k p^k+n_{k-1}p^{k-1}+\cdots+n_1 p+n_0,$$

where $0\leq m_i,n_i<p$ for all i. Then the binomial coefficient $\binom{m}{n}$ modulo p can be computed as

$$\binom{m}{n}\equiv\prod_{i=0}^{k}\binom{m_i}{n_i}\mod p.$$

Proof 不难看出，只需证：当 $m=m_1p+a_0$，$n=n_1p+b_0$ 时，

$$C_m^n\equiv C_{m_1}^{n_1}C_{a_0}^{b_0}\pmod p.$$

注意到，

$$(1+x)^m=\sum_{n=0}^{m}C_m^n x^n=\sum_{n=0}^{m}\sum_{b_0=0}^{a_0}C_m^n x^{n_1p+b_0},$$

且

$$\begin{aligned}(1+x)^{m_1p+a_0}&=((1+x)^p)^{m_1}(1+x)^{a_0}\\&=\left(\sum_{i=0}^{p}C_p^i x^i\right)^{m_1}(1+x)^{a_0}\\&\equiv(1+x^p)^{m_1}(1+x)^{a_0}\pmod p\\&=\left(\sum_{n=0}^{m}C_{m_1}^{n_1}x^{n_1p}\right)\left(\sum_{b_0=0}^{a_0}C_{a_0}^{b_0}x^{b_0}\right)\\&\equiv\sum_{n=0}^{m}\sum_{b_0=0}^{a_0}C_{m_1}^{n_1}C_{a_0}^{b_0}x^{n_1p+b_0}\pmod p.\end{aligned}$$

而 $(1+x)^m=(1+x)^{m_1p+a_0}$，故

$$C_m^n\equiv C_{m_1}^{n_1}C_{a_0}^{b_0}\pmod p.$$

第 3 章 环论

3.1 环的定义与基本性质

Definition 3.1 (环的定义)

环是一个集合R和R上两个二元运算 (通常表示成加法 $+$ 和乘法 $\cdot$) 组成的代数结构 $(R,+,)$, 且满足以下三个条件 :

(1)$(R,+)$是阿贝尔群.这个加法群的幺元素表示成0_R(或者简记为0), 叫做环R的零元素.

(2)$(R,\cdot)$是半群.这意味着R中乘法运算满足结合律.

(3)加法和乘法满足分配律.即对任意的$a,b,c\in R$, 有$a(b+c)=ab+ac,\quad (b+c)a=ba+ca.$

Remark 如果一个环对于乘法有幺元我们就称为幺环, 若一个环对于乘法可交换就称为交换环

Proposition 3.1 (环中的基本运算)

设R为环.则

(1)对每个$a\in R, 0a=a0=0$;

(2)对每个$a,b\in R, (-a)b=a(-b)=-(ab),\quad (-a)(-b)=ab$;

(3)对于$a_i,b_i\in R, \left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{m}b_j\right)=\sum_{i=1}^{n}\sum_{j=1}^{m}a_ib_j$(4)对于$n\in \mathrm{Z}, a,b\in R$, 有 $(na)b=a(nb)=n(ab)$.

(5) 若环有单位元那么其乘法单位元必定唯一

(6) $(m+n)a=ma+na\quad m(-a)=-(ma)\quad (mn)a=m(na)\quad m(a+b)=ma+mb, \forall a,b\in R, m,n\in\mathbb{Z}$

(7) $a^ma^n=a^{m+n}, (a^m)^n=a^{mn}, \forall m,n\in\mathbb{N}, a\in R$

Example 3.1 诸多环的例子

1.任何数域都是环.

2.全体整数的集合$\mathbb{Z}$在加法和乘法下也构成环.

3.现设$m\in\mathbb{Z}$, 令$\mathbb{Z}[\sqrt{m}]=\{a+b\sqrt{m}\mid a,b\in\mathbb{Z}\}$.则$\mathbb{Z}[\sqrt{m}]$也构成环

4.特别地, 当$m=-1$时有$\mathbb{Z}[\sqrt{-1}]=\{a+b\sqrt{-1}\mid a,b\in\mathbb{Z}\}$.这是历史上非常著名的环的例子, 称为$Gauss$整数环.

5.设$\mathbb{P}$为一个数域, 令$\mathbb{P}[x]$为$\mathbb{P}$上全体以x为文字的一元多项式的集合

则$\mathbb{P}[x]$在多项式的加法和乘法下构成环, 称为数域$\mathbb{P}$上的一元多项式环, 或简称为$\mathbb{P}$上的多项式环.

6.类似地, 记$\mathbb{P}^{n\times n}$为$\mathbb{P}$上全体矩阵构成的集合, 则$\mathbb{P}^{n\times n}$在矩阵的加法和乘法下构成环, 称为$\mathbb{P}$上的n阶方阵环.$\mathbb{M}_n(\mathbb{R})$

7.记实数轴上全体连续函数构成的集合为$C(\mathbb{R})$

定义加法与乘法 $(f+g)(x)=f(x)+g(x),\quad (fg)(x)=f(x)g(x),\quad x\in\mathbb{R}, f,g\in C(\mathbb{R})$,

则容易验证$C(\mathbb{R})$构成环.同样地, 记$\mathbb{R}$上全体光滑函数 (即具有任何阶的连续导数) 的集合为$C^\infty(\mathbb{R})$, 则在上述两种运算下$C^\infty(\mathbb{R})$构成环.

8.$R=\{0\}$, 即由一个零元素构成的环, 叫做零环.我们对这种环不感兴趣, 即通常总假定R不是零环.

Proposition 3.2

1.偶数环 $(2\mathbb{Z},+,\cdot)$ 是一个没有单位元的环

2.如果环有单位元和零元, 那么这二者不会相同 $(若1=0, 那么\forall a, a=a\cdot 1=a\cdot 0=0)$

Note 另一方面, 在考虑$C([0,1])$, 定义两个函数$f(x)=\begin{cases}0, & x\in\left[0,\frac{1}{2}\right],\\ 2x-1, & x\in\left(\frac{1}{2},1\right],\end{cases}\quad g(x)=\begin{cases}1-2x, & x\in\left[0,\frac{1}{2}\right],\\ 0, & x\in\left(\frac{1}{2},1\right],\end{cases}$

则f,g都是$C([0,1])$中的非零元素, 但是$fg=0$.一个环中如果出现这种现象, 则消去律不再成立.

Definition 3.2 (无零因子环)

1.设R为一个环,$a,b\in R$,且$a\neq 0,b\neq 0$,若$ab=0$,则称a为R中的一个左零因子,b为R中的一个右零因子,都简称为零因子.

2.如果在环R中,由$ax=ay,a\neq 0$,可以推出$x=y$,则称R满足左消去律;

如果由$xa=ya,a\neq 0$,可以推出$x=y$,则称R满足右消去律.

3.若一个环不是零环且没有零因子就叫做无零因子环(根据1.定义零环本身是不会成为无零因子环)

Theorem 3.1 (无零因子环的等价说明)

R为无零因子环$\Longleftrightarrow$无左零因子$\Longleftrightarrow$无右零因子$\Longleftrightarrow ab=0$一定就有$a=0$或$b=0\Longleftrightarrow a\neq 0,b\neq 0$那么$ab\neq 0$

Definition 3.3 (除环与整环与域定义)

1.R是一具有乘法单位元,乘法交换性质,无零因子环$\Longrightarrow$整环

2.设幺环R且有$R\setminus\{0\}$构成群$\Longrightarrow$除环

3.若一个除环还具有乘法交换性质$\Longrightarrow$域(亦$R\setminus\{0\}$构成$Abel$群)

4.域一定为整环

Proposition 3.3

(1)除环R是一个无零因子环.假如a为零因子.则有$a\neq 0$.且存在$b\neq 0$,使得$ab=0$.由于R为除环,a^{-1}存在.

故$b=1\cdot b=\left(a^{-1}a\right)b=a^{-1}(ab)=a^{-1}\cdot 0=0$.矛盾

(2)在除环R中,对于$\forall a,b\in R,a\neq 0$,方程$ax=b$方$ya=b$都有唯一解.因为花$b\neq 0$,上述方程在R^*中有唯一解:

若$b=0$,上述两个方程都只有零解.值得注意的是,由于除环的乘法未必满足交换律

因此,对于同样的a与b,上述两个方程的解未必相等.

因为域一定是除环,所以,上面的三条性质对于域来说也是成立的.

(3) 有限整环为域(另一版本容易知道:有限无零因子环为除环)

(4) $(\mathbb{Z}_n,+,\cdot)$构成无零因子环$\Longleftrightarrow n$为素数

(5) 进一步$(\mathbb{Z}_n,+,\cdot)$构成域$\Longleftrightarrow n$为素数

Theorem 3.2 (无零因子环导出加法阶相同定理)

设R为无零因子环,令$R^*=R-\{0\}$,则R^*中的元素对于R的加法具有相同的阶,且当这一共同的阶有限时,必为素数.

Proof 分三步来证明命题.

(1)若R^*中所有元素对于加法的阶都是无穷,则结论成立.

(2)设存在$a\in R^*$的阶为有限的.假定的a阶为n,则对任何$b\in R^*$,有$(na)b=a(nb)=0$.因为R为无零因子环,且$a\neq 0$,故$nb=0$.

这说明b的阶整除n.特别地,b的阶也是有限的.设b的阶为m,则上面的证明说明$m\mid n$,类似地也有$n\mid m$.于是$m=n$.

故R^*中所有元素对于加法的阶都等于n,亦即R中所有的非零元素具有相同的阶.

(3)设R^*中所有的元素的阶都是正整数n,我们证明n必是素数.若n不是素数,则存在正整数$n_1,n_2,n_1<n,n_2<n$,使得$n=n_1n_2$.

因为a的阶为n,故$n_1a\neq 0,n_2a\neq 0$.另一方面,我们有$(n_1a)(n_2a)=na^2=(na)a=0$.这与$R$无零因子矛盾.则$n$必为素数.至此命题得证.

Definition 3.4 (环的特征定义)

设R为无零因子环.如果R中所有的非零元都是无穷阶的,则称R的特征为0;

如果R中所有的非零元都是p阶的(由上文引理这时p必为素数),则称R的特征为p.我们将环R的特征记为$\mathrm{Ch}R$.

Proposition 3.4

1.易知数域P的特征为无限.因为数1的整数倍$n\cdot 1=0$.当且仅当$n=0$:

2.考察无零因子环$\mathbb{Z}_p$的特征为p.

3.上述讨论说明整环，除环，域的特征要么为0要么为素数

Proof 无零因子环$\mathbb{Z}_p$,事实上$\forall \bar{0}\neq \bar{k}\in \mathbb{Z}_p$那么$p\cdot \bar{k}=\overline{pk}=\bar{0}$.

而当$0<l<p$时,若$l\cdot \bar{k}=\overline{lk}=\bar{0}.\Longrightarrow p\mid lk\Longrightarrow p\mid k$矛盾

Lemma 3.1

对任何素数p及整数$k,1\leqslant k\leqslant p-1$,有$p\mid \mathrm{C}_p^k$.

Proof $C_p^k=\dfrac{p\,(p-1)\cdots(p-k+1)}{k!}$而$(p,k!)=1$且$p\mid p\,(p-1)\cdots(p-k+1)$且$k!\mid p\,(p-1)\cdots(p-k+1)$

$\Longrightarrow pk!\mid p\,(p-1)\cdots(p-k+1)$

Theorem 3.3

设R为无零因子的交换环,其特征为p,p为素数,则对任何$a,b\in R$,有$(a+b)^p=a^p+b^p,\quad (a-b)^p=a^p-b^p$.

Proof 因R为交换环,由归纳法易证:$(a+b)^p=a^p+\mathrm{C}_p^1a^{p-1}b+\cdots+\mathrm{C}_p^{p-1}ab^{p-1}+b^p$.

因$p\mid \mathrm{C}_p^k,k=1,2,\cdots,p-1$,故由$R$的特征为$p$得$\underbrace{\mathrm{C}_p^ka^{p-k}b^k}_{=0}=0,k=1,2,\cdots,p-1$.

故$(a+b)^p=a^p+b^p$.于是$(a-b)^p=(a+(-b))^p=a^p+(-b)^p=a^p+(-1)^pb^p$.

又当$p\neq 2$时,p为奇数,而当$p=2$时,由$2b^p=0$推出$b^p=-b^p$.故$(a-b)^p=a^p-b^p$

设R为无零因子的交换环,其特征为p,p为素数,则对任何$a,b\in R$及自然数n,有$(a+b)^{p^n}=a^{p^n}+b^{p^n},\quad (a-b)^{p^n}=a^{p^n}-b^{p^n}$.

Corollary 3.1

设R为无零因子的交换环,其特征为p,p为素数,则对任何$a,b\in R$及自然数n,有$(a+b)^{p^n}=a^{p^n}+b^{p^n}$,$(a-b)^{p^n}=a^{p^n}-b^{p^n}$.

Proof $(a+b)^{p^{\boldsymbol{n}}}=(a^p+b^p)^{p^{\boldsymbol{n}-1}}=\left(a^{p^2}+b^{p^2}\right)^{p^{n-2}}=\cdots\cdots$

Proposition 3.5

1.一个至少含有两个元素且无零因子的有限环是一个除环

2.有限整环为域

3.有限无零因子环为除环

4.$\mathbb{Z}_p$为无零因子环$\Longleftrightarrow p$为一个素数

5.$\mathbb{Z}_p$为域$\Longleftrightarrow p$为一个素数

Proof 1.设$(R,+,\cdot)$是一个至少含有两个元素且无零因子的有限环

要证它是一个除环,只需证$(R^*,\cdot)$是一个群.因为R中至少含有两个元素,所以,R^*是一个非空集合.

又因为R中无零因子,所以,$\forall a,b\in R^*$,即$a\neq 0,b\neq 0$,得$ab\neq 0$,也就是说,R^*关于乘法运算是封闭的.

从而得到$(R^*,\cdot)$是一个满足消去律的有限半群,得(R^*)是一个群。所以,R是一个除环

2.3.利用有限半群满足消去律为群

4.$\Longrightarrow$：显然若n不为素数那么就有$n=ab$；所以$\bar{a}\bar{b}=\bar{0}$

$\Longleftarrow$:若$\bar{a}\bar{b}=\bar{0}$且$\bar{a}\neq\bar{0}$且$\bar{b}\neq\bar{0}$那么有$p\mid ab$又因为p为素数那么$p\mid a$或者$p\mid b$此时但a与b小于p矛盾

5.同4.

Definition 3.5

无零因子交换环R可以嵌入进一个域中,该域我们称为分式域

设整环R为域F的子环,若$\forall a \in F$,存在$b, c \in R$,使得$a = bc^{-1}$,则称F为环R的分式域

Proof 设R为无零因子环,定义集合$R \times R^* = \{(a,b) \mid a \in R, b \in R^*\}$

定义集合$R \times R^*$上的运算$(a,b)+(c,d) = (ad+bc, bd)$　$(a,b)\cdot(c,d) = (ac, bd)$，　$(a,b) = (c,d) \Longleftrightarrow (ad = bc)$

1.相等是一个等价关系，加法，乘法封闭

2.$\sim$等价关系(相等)对于加法，乘法是同余关系

3.令$F = R \times R^*/\sim$　$\overline{(a,b)}$记作$\frac{a}{b}$　F上加法$\overline{(a,b)} + \overline{(c,d)} = \overline{(a,b)+(c,d)}$即$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

F上乘法$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a,b)\cdot(c,d)}$即$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

4.$(F, +, \cdot)$构成域即对于加法时$abel$群，乘法也是$abel$群

5.取定$b \neq 0$，$b \in R$则记$\bar{R} = \left\{\frac{ab}{b} \mid a \in R\right\}$容易说明$\bar{R}$为$F$的子环

6.$\bar{R} \cong R$(构造映射$\varphi : \bar{R} \to R$　$\frac{ab}{b} \to a$)

3.2 子环与环同态

Definition 3.6 (子环定义)

设R为环, R_1为R的非空子集.若R_1对于R的加法与乘法也构成环, 则称R_1为R的子环.

我们显然会有一个子环中的零元因为是在加法群中自然会继承原环中的零元宛如我们群论中一样，但是单位元却未必

Theorem 3.4 (子环判定定理)

设R为环, R_1为R的非空子集, 则R_1为R的子环的 $\Longleftrightarrow$ 对任何$a,b\in R_1$, 有$a-b\in R_1, ab\in R_1$.

Proof 必要性设R_1是R的子环, 且$a,b\in R_1$, 则因R_1对于R的加法成为加法群R的子群, 故$a-b\in R_1$.

又R_1对于R的乘法成为半群, 特别对于R的乘法封闭, 故$ab\in R_1$.

充分性若$a-b\in R_1, \forall a,b\in R_1$, 则$R_1$是$R$作为加法群的子群, 因而是加法群.又$ab\in R_1, \forall a,b\in R_1$, 故$R_1$对于$R$的乘法封闭.

由于R对于乘法满足结合律, 故R_1对于乘法也满足结合律, 从而R_1对于乘法构成半群.

注意到R满足乘法对于加法的分配律, 于是R_1也满足乘法对于加法的分配律.故R_1在R的加法和乘法下构成环.从而是R的子环.

Proposition 3.6 (子环的交还是子环)

环 (整环、除环、域)R的若干个子环 (子整环、子除环、于域) 的交仍是子环 (子整环、子除环、子域).

Proof 仅证环的情形.令$\{S_i \mid i\in I\}$ (其中I是某个指标集) 是环R的一个子环族, 因为$\forall i\in I$, 有$0\in S_i$, 得$0\in \bigcap\limits_{i\in 1} S_i\neq\varnothing$.

若$\forall a,b\in \cap S_i$, 则有$a,b\in S_i(\forall i\in I)$, 由于$S_i$都是$R$的子环, 所以$a-b\in S_i,\quad ab\in S_i,(\forall i\in I)$

从而得$a-b\in \bigcap\limits_{i\in I} S_i,\quad ab\in \bigcap\limits_{u\in 1} S_i$.所以, $\bigcap\limits_{i\in 1} S_i$是$R$的一个子环.

Definition 3.7 (由子集生成环)

设T是环R的一个非空子集, 如果R的子环S满足 : $T\subseteq S$, 做$\bigcap\limits_{i\in I} S_i$即为$T$生成的环

1.$T\subseteq \bigcap\limits_{i\in I} S_i$　　2.$\bigcap\limits_{i\in I} S_i$是包含了$T$的最小子环

✍ **Exercise 3.1** 找出Z_6的所有子环.

Proof 设S是Z_6的一个子环, 那么 $(S,+)$必定是 $(\mathrm{Z}_6,+)$ 的一个子群, 而 $(\mathrm{Z}_6,+)$ 的子群只有$\{\bar{0}\},\{\bar{0},\bar{3}\},\{\bar{0},\bar{2},\bar{4}\},\mathrm{Z}_6$.

容易验证它们都是环Z_6的子环, 且$\{\bar{0}\}=[\bar{0}],\quad \{\bar{0},\bar{3}\}=[\bar{3}],\quad \{\bar{0},\bar{2},\bar{4}\}=[\bar{2}],\quad \mathrm{z}_6=[\bar{1}]$.

Definition 3.8 (环同态与环同构)

设R,R'是两个环, f是R到R'的一个映射

如果对于$\forall a,b\in R$, 有$f(a+b)=f(a)+f(b), f(ab)=f(a)f(b)$则称$f$为$R$到$R'$的一个同态映射.

若f为满射, 则称f是R到R'的渾同态, 这时又称R与R'同态, 记为$R\sim R'$(或$R\sim R'$);

若f为单射, 则称f是R到R'的单同态 (也叫做R在R'中的嵌入);

若f为 $-$一映射, 则称f是R到R'的同构肤射, 这时又称R与R'同构, 记为$R\cong R'$

Problem 3.1 设$R=\mathrm{Z}, R'=\mathrm{Z}_m$, $f:\mathrm{Z}\to \mathrm{Z}_m,\quad a\mapsto \bar{a}$, 显然$f$是满射.

Proof 又对于$\forall a,b\in \mathrm{Z}$,有$f(a+b)=\overline{a+b}=\bar{a}+\bar{b}=f(a)+f(b),\quad f(ab)=\overline{ab}=\bar{a}\cdot\bar{b}=f(a)\cdot f(b)$,
故f是Z到Z_m的一个满同态,即$\mathrm{Z}\sim \mathrm{Z}_m$.关于环同态也有类似于群同态的一些结果.

Proposition 3.7 (环同态的性质)

若环$R\xrightarrow{\varphi}R'$.则
(1)R的元素0的象$f(0)$是R的零元素,即$f(0)=0'$;
(2)R中的元意a的负元一a的象$f(-a)$是a的$f(a)$的负元$-f(a)$,即$f(-a)=-f(a)$;
特别的若该环同态是满同态那么
(3) 若R是交换环,则R'也是交换环;
(4) 若R有单位元1,那么R'也有单位元,且R'的单位元为$f(1)$
(5) 若R是除环则R'是除环
(6) 若R是域则R'是域

Proof 设R为除环，下面证R'是除环　φ为R到R'的满同态
此时已知$R'-\{0'\}$中的幺元为e'，$R'-\{0'\}$中的乘法结合律由满同态φ保证
下面说明$R'-\{0'\}$中的逆元：
对于$\varphi(a)\in R'-\{0'\}$可以断言$a\neq 0$否则产生矛盾，此时$\varphi\left(aa^{-1}\right)=\varphi(e)=e'=\varphi(a)\varphi\left(a^{-1}\right)$
$\Longrightarrow \varphi(a)\in R'-\{0'\}$的逆元即为$\varphi\left(a^{-1}\right)$记为$\varphi^{-1}(a)$且$\varphi^{-1}(a)\notin R'-\{0'\}$(若不然$e'=\varphi(a)\varphi\left(a^{-1}\right)$不成立)
下面说明$R'-\{0'\}$中满足封闭性：
$\forall\varphi(a),\varphi(b)\in R'-\{0'\}$　实际上我们可以断言$a,b\neq 0$若不然$\varphi(a),\varphi(b)=0'$就产生矛盾了
此时断言$\varphi(a)\cdot\varphi(b)\neq 0'$若不然$\varphi(a)\cdot\varphi(b)=0'\Longrightarrow$乘以$\varphi^{-1}(a)\Longrightarrow\varphi(b)=0'$矛盾
故R'是除环

Theorem 3.5 (子环在环同态下的性质)

若环$R'\sim R'$,S是R的子环,S'是R'的子环,那么$f(S)$是R'的于环,$f^{-1}(S')$是R的子环.
若环$R\xrightarrow{f}R'$,则$\mathrm{Ker}f=f^{-1}(0')=\{x\mid x\in R,f(x)=0'\}$是$R$的子环.

Proposition 3.8

设$R\cong R'$,则R是整环(除环、域)的充分必要条件R'是整环(除环、域).

Proof 我们仅对整环的情形给出证明.
先证必要性.设R为整环,由满射可知可知R'是有单位元的交换环,因此,只需证明R'无零因子即可.
$\forall a',b'\in R'$,若$a'b'=0'$,则存在$a,b\in R$,使得$f(a)=a',\quad f(b)=b'$,且　$0'=a'b'=f(a)f(b)=f(ab)$.
由于f为单射,故只有$ab=0$,而R无零因子,即有$a=0$或$b=0$,得$a'=f(a)=f(0)=0'$ 或$b'=f(b)=f(0)=0'$.所以,R'为整环.
再证充分性.因为$f^{-1}:R'\to R$也是同构映射,如果R'是整环,那么根据必要性可知R也是一个整环.

Example 3.2 子环中单位元的存在性特例

1.有理数域Q与其子环 Z 有相同的单位元1,但整数环 Z 的子环偶数环2Z却没有单位元.
2.$\mathbb{Z}_6=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$是有单位元$\bar{1}$的交换环.容易验证$S=\{\bar{0},\bar{2},\bar{4}\}$是$\mathbb{Z}_6$的子环,它也有单位元$\bar{4}$.
由此可见,环$\mathbb{Z}_6$与其子环S都是有单位元的环,但它们的的位元并不相同.

Example 3.3 一般环同态下单位元与交换性无法传递的例子

反例如下：设$R=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a,b\in \mathrm{Z}\right\}$作$f:R\to \mathrm{Z},\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\mapsto a$
则f是R到Z的同态满射，Z有单位元1，但R无单位元.而且Z是交换环，而R却不是交换环.

Example 3.4 无零因子性在群同态下不传递例子

1.$\mathrm{Z}\sim \mathrm{Z}_m$之间存在满同态$\varphi:a\to \bar{a}$
Z为无零因子环，但当m为合数时，Z_m是有零因子的环.

2.设$R=\{(a,b)\mid a,b\in \mathrm{Z}\}$，则$R$对于代数运算：$(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2)$，　$(a_1,b_1)\cdot(a_2,b_2)=(a_1a_2,b_1b_2)$作成一个环。
且$g:R\to \mathrm{Z},\quad (a,b)\mapsto a$是$R$到Z的满同态.$R$中零元为$(0,0)$因为$(a,0)\cdot(0,b)=(0,0)$，所以，$R$是一个有零因子的环，但Z没有零因子.

Proposition 3.9

If $\varphi:R_1\to R_2$ is a ring isomorphism, then $\varphi:R_1^{\times}\to R_2^{\times}$ is a group isomorphism

3.3 理想与商环

下面我们来研究商环.给定环R的一个子环R_1,因R对于加法成为交换群,$\{R_1;+\}$是$\{R;+\}$的正规子群
故R对于R_1有左商集R/R_1,而且R/R_1在R的加法诱导的运算下成为交换群.
如果要定义R/R_1上环的结构,就要在R/R_1上定义乘法.
一个最自然的想法是在R/R_1上定义$(a+R_1)(b+R_1)=ab+R_1,\quad a,b\in R$.不过这样的定义未必是合理的.

Example 3.5 非良定义的商环反例

举例说明存在一个环R及其子环R_1,以及$a,b,a',b'\in R$,使得在商群上R/R_1上$a+R_1=a'+R_1, b+R_1=b'+R_1$,但是$ab+R_1\neq a'b'+R_1$.

Proof 我们有环$Z\times Z$中,若$S=\{(n,n)\mid n\in Z\}$则
1.S是$Z\times Z$的子环
2.S作为$Z\times Z$的加法群的正规子群
3.对于$Z\times Z/S$该加法商群上
$(2,3)+S\sim(1,2)+S$(因为$(2,3)-(1,2)=(1,1)\in S$),其次$(4,4)+S\sim(3,3)+S$(因为$(4,4)-(3,3)=(1,1)\in S$)
但是$[(2,3)\cdot(4,4)]+S\nsim[(1,2)\cdot(3,3)]+S$(因为$(8,12)-(3,6)=(5,6)\notin S$)

我们知道,造成定义的运算不合理的原因是子环的条件无法保证左商集对应的等价关系对于R的乘法是同余关系.
现在我们分析一下使得该关系是同余关系的条件.
定义左商集R/R_1的等价关系是$a\sim b$当且仅当$a-b\in R_1$.
因此要使我们期望定义合理,就应该满足条件$a_1\sim a_2, b_1\sim b_2\Longrightarrow a_1b_1\sim a_2b_2$
这等价于$a_1-a_2\in R_1, b_1-b_2\in R_1\Longrightarrow a_1b_1-a_2b_2\in R_1$.
注意到$a_1b_1-a_2b_2=a_1b_1-a_1b_2+a_1b_2-a_2b_2=a_1(b_1-b_2)+(a_1-a_2)b_2$.
上式中,$a_1-a_2\in R_1, b_1-b_2\in R_1$,而$a_1$和$b_2$都可以任意
因此要使定义合理,R_1应该满足的条件是$ax\in R_1, ya\in R_1, \forall x,y\in R, a\in R_1$.由此我们导出下面的定义.

Definition 3.9 (理想定义)

设R为环,I为R的子环
如果I满足条件"$\forall a\in I,\forall x\in R\Longrightarrow xa\in I$",则称$I$为$R$的左理想;
如果I满足条件"$a\in I, y\in R\Longrightarrow ay\in I$",则称$I$为$R$的右理想.
若一个子环既是左理想,又是右理想,则称为双边理想.(一般我们使用理想都指双边理想)
不难看出 0 和 R 是平凡理想,理想一定是子环

Theorem 3.6 (理想的判定定理)

设R为一环,S为一非空子集
1.$\forall a,b\in S$有$a-b\in S$
2.$\forall a\in S,\forall x\in R\Longrightarrow xa\in S\ (ax\in S)\ [ax\in S, xa\in S]$
那么为一左理想(右理想)[双边理想]

Definition 3.10

一个环没有真理想的环叫做单环

Theorem 3.7

除环，域为单环

(利用$R\setminus\{0\}$构成群，反证若有一个非平凡理想，$0\neq x\in R\Longrightarrow 0\neq x^{-1}\in R\Longrightarrow 1\in R\Longrightarrow$ 理想为全集)

Proposition 3.10

1. 矩阵环中不存在真理想 2. 矩阵环中的中心化子只是子环不是理想

Proof 我们来证明$M_n(P)$中不存在真理想

设I是$M_n(P)$的一个理想，且$I\neq\{0\}$，那么，I中存在非零矩阵$A=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\vdots&\vdots&&\vdots\\a_{n1}&a_{n2}&\cdots&a_{rm}\end{pmatrix}\in I$.其中$a_{st}\neq 0$.

根据矩阵的运算有$E_{ij}=\dfrac{1}{a_{st}}E_{is}AE_{ij},\quad i,j=1,2,\cdots,n,$

因此，任意$B=\begin{pmatrix}b_{11}&b_{12}&\cdots&b_{1n}\\b_{21}&b_{22}&\cdots&b_{2n}\\\vdots&\vdots&&\vdots\\b_{n1}&b_{n2}&\cdots&b_{nn}\end{pmatrix}\in M_n(P)$有$B=\sum_{i=1}^{n}\sum_{j=1}^{n}b_{ij}E_{ij}\in I$.得$I=M_n(P)$.所以，$M_n(P)$不存在真理想.

我们由高等代数的知识可以知道，$M_n(P)$的中心$C=\{$所有n阶数量矩阵$\}$，由于$M_n(P)$没有真理想

即$M_n(P)$的中心是$M_n(P)$的子环但不是$M_n(P)$的理想.

Problem 3.2 理想的诸多例子

1.整数环$\mathbb{Z}$的任一子环必形如$m\mathbb{Z},m\geqslant 0$.容易用理想的定义验证$m\mathbb{Z}$是$\mathbb{Z}$的双边理想，因此$m\mathbb{Z},m\geqslant 0$也是$\mathbb{Z}$所有的理想

2.考虑$C(\mathbb{R})$.取定$x_0\in\mathbb{R}$，定义$Z_{x_0}(\mathbb{R})=\{f\in C(\mathbb{R})\mid f(x_0)=0\}$，则$Z_{x_0}(\mathbb{R})$是$C(\mathbb{R})$的双边理想.

3.设x为$\mathbb{R}^n$中的一点，在$C^\infty(\mathbb{R}^n)$中

我们定义$O_x=\{f\in C^\infty(\mathbb{R}^n)\mid$ 存在x的一个邻域U，使得 $f(y)=0,\forall y\in U\}$.则容易验证O_x是$C^\infty(\mathbb{R}^n)$的一个理想.

Proposition 3.11 (理想子环的交并和性质)

1.K是R的子环，J是R的子环 $\not\Longrightarrow K+J$是R的子环

2.K是R的子环，J是R的理想 $\Longrightarrow K+J$是R的子环

3.K是R的子环，J是R的理想 $\not\Longrightarrow K+J$是R的理想

4.K是R的理想，J是R的理想 $\Longrightarrow K+J$是R的理想

5.K是R的子环，J是R的理想 $\Longrightarrow J$是$K+J$的理想

6.理想的无限交也是理想 (子环的无限交也是子环)

7.K是R的子环，J是R的理想 $\not\Longrightarrow K\cap J$是$R$的理想

8.K是R的子环，J是R的理想 $\Longrightarrow K\cap J$是K的理想

9.K是R的子环，J是R的理想 $\not\Longrightarrow K\cap J$是$J$的理想

10.K是R的子环，J是R的子环 $\not\Longrightarrow K\cup J$是$R$的子环 (甚至连加强为$K,J$都为理想都可能做不到)

11.两个理想的并仍为理想充要条件是一个包含于另一个 (因为群的并仍为群充要是一个包含另一个)

12.K与J为幺环R的理想 $\Longrightarrow KJ$为R的理想

Proof $k_1j_1\cdot k_2j_2=\underbrace{k_1j_1k_2j_2}_{\in J}$

$k_1j_1-k_2j_2=\underbrace{k_1j_1}_{\in K}-\underbrace{k_2j_2}_{\in K}=k^*e\in KJ$ (这里将每一个k_ij_i看成K或者J进而再利用幺环性质)

$\Longrightarrow KJ$为R的理想

Example 3.6 K是R的子环, J是R的子环 $\nRightarrow$ $K+J$是R的子环

多项式环$F(x,y)$, 子环$F(x)$, $F(y)$

Example 3.7 K是R的子环, J是R的理想 $\nRightarrow$ $K+J$是R的理想

取环$\mathbb{Z}\times\mathbb{Z}$中：子环 (非理想) : $\{(n,n)\}$　理想 : $\{(k,l)\mid k,l$都为偶数$\}$

但$\{(n,n)\}+\{(k,l)\mid k,l$都为偶数$\}$并非理想　因为$[(1,1)+(2,4)]\times(2,3)=(6,15)\underbrace{\notin\{(n,n)\}+\{(k,l)\mid k,l都为偶数\}}$

因为该集合特点是元素两个数字一定同奇同偶

Example 3.8 K是R的子环, J是R的理想 $\nRightarrow$ $K\cap J$是R的理想

取环$\mathbb{Z}\times\mathbb{Z}$中：子环 (非理想) : $\{(n,n)\}$　理想 : $\{(k,l)\mid k,l$都为偶数$\}$

此时$\{(n,n)\}\cap\{(k,l)\mid k,l$都为偶数$\}=\{(m,m)\mid m$为偶数$\}$是$R$的子环但并非是理想

Example 3.9 K是R的子环, J是R的理想 $\nRightarrow$ $K\cap J$是J的理想

取环$\mathbb{Z}\times\mathbb{Z}$中：子环 (非理想) : $\{(n,n)\}$　理想 : $\{(k,l)\mid k,l$都为偶数$\}$

此时$\{(n,n)\}\cap\{(k,l)\mid k,l$都为偶数$\}=\{(m,m)\mid m$为偶数$\}$　但是取$\underbrace{(2,2)}_{\in\cap交}\times(4,6)\notin\cap$

Example 3.10 子环的并未必是子环反例

取$R=(\mathbf{Z},+,\cdot)$, $H_1=2\mathbf{Z}$, $H_2=3\mathbf{Z}$, 则$H_1\cup H_2$中的元素或为偶数, 或为3的倍数

因为$2\in H_1\subseteq H_1\cup H_2$,　$3\in H_2\subseteq H_1\cup H_2$, 但$2+3=5\notin H_1\cup H_2$, 因为5既不是偶数, 也不是3的倍数

由此可以看出$H_1\cup H_2$关于加法运算不封闭, 所以它不是G的子群。

现在我们介绍一下构造理想的方法.

Definition 3.11 (生成理想)

现在设S为环R的非空子集, 则R中所有包含S的理想 (这样的理想是存在的, 例如R本身就是一个) 之交仍为R的理想

称为由S生成的理想, 记为$\langle S\rangle$.

我们断言$\langle S\rangle$是R中包含集合S的最小理想.事实上, 由上面的定义, $\langle S\rangle$是理想, 且包含S.

另一方面, 因为$\langle S\rangle$是所有包含S的理想之交, 因此任何包含S的理想一定包含$\langle S\rangle$, 因此$\langle S\rangle$是最小的.

如果一个生成理想是由一个有限集合生成的我们叫做有限生成的理想

Definition 3.12 (主理想与生成元)

设I为环R的理想, 如果存在$a\in I$使得$I=\langle a\rangle$, 则称I为主理想, 而a称为I的一个生成元.

Theorem 3.8 (主理想的结构)

R是一个环, 那么由一个元素$\{a\}$生成的理想亦即R中关于a的主理想:

$\langle a\rangle=\left\{\sum x_iay_j+sa+at+na\mid x_i,y_j,s,t\in R,n\in\mathbb{Z}\right\}$.

Proof 1.令集合$I=\left\{\sum x_iay_j+sa+at+na\mid x_i,y_j,s,t\in R,n\in\mathbb{Z}\right\}$

一方面$\forall k_1,k_2\in I$此时不妨设$k_1=\sum x_i^1ay_j^1+s_1a+at_1+n_1a$与$k_2=\sum x_i^2ay_j^2+s_2a+at_2+n_2a$

$\Longrightarrow k_1-k_2\in I$

且$\forall k_1\in I$与$r\in R$此时不妨设$k_1=\sum x_i^1ay_j^1+s_1a+at_1+n_1a$

$$\Longrightarrow k_1 r = \underbrace{\sum x_i^1 a y_j^1 r}_{\text{为}\sum x_i a y_j\text{类型}} + \underbrace{s_1 a r}_{\text{为}\sum x_i a y_j\text{类型}} + \underbrace{a t_1 r}_{\text{为}at\text{类型}} + \underbrace{n_1 a r}_{=a(n_1 r)\text{为}at\text{类型}}$$

故$k_1 r \in I$

故I为一个理想

2.已知$\{a\} \subseteq I$则由$\langle a\rangle$的定义知道$\langle a\rangle \subseteq I$

3.对于任意一个包含了$\{a\}$且为R的理想I_1，此时$\sum x_i a y_j + sa + at + na \in I_1$

$\Longrightarrow I \subseteq I_1$

那么特别取$I_1 = \langle a\rangle$则有$I \subseteq \langle a\rangle$

综上得到$I = \langle a\rangle$

Corollary 3.2 (特殊环 R 下的主理想的结构)

若R是有单位元的环, 则$\langle a\rangle = \{\sum x_i a y_i \mid x_i, y_i \in R\}$;

若R是交换环, 则$\langle a\rangle = \{ra + na \mid r \in R, n \in \mathrm{Z}\}$;

若R是有单位元的交换环, 则$(a) = \{ra \mid r \in R\} = Ra = aR$.

下面我们再来看有限个元素生成的理想的结构.

Theorem 3.9 (有限个元素生成的理想结构)

设$a_1, a_2, \cdots, a_n \in R$, 那么$(a_1, a_2, \cdots, a_n) = (a_1) + (a_2) + \cdots + (a_n)$.

Proof 因为$a_i \in (a_i) \subseteq (a_1) + (a_2) + \cdots + (a_n), i = 1, 2, \cdots, n$, 根据引理知$(a_1) + (a_2) + \cdots + (a_n)$是包含元素$a_1, a_2, \cdots, a_n$的理想而$(a_1, a_2, \cdots, a_n)$是包含$a_1, a_2, \cdots, a_n$的最小理想, 从而有$(a_1, a_2, \cdots, a_n) \subseteq (a_1) + (a_2) + \cdots + (a_n)$.

另一方面$\forall a_i \in R.(i = 1, 2, \cdots, n)$, 有$(a_i) \subseteq (a_1, a_2, \cdots, a_n)$, 故$(a_1) + (a_2) + \cdots + (a_n) \subseteq (a_1, a_2, \cdots, a_n)$.

所以, $(a_1, a_2, \cdots, a_n) = (a_1) + (a_2) + \cdots + (a_n)$.

Theorem 3.10 (交换幺环上主理想乘积的结构)

若R为交换环, $K = \langle a\rangle$; $J = \langle b\rangle$为理想

$KJ = JK = \langle ab\rangle = \langle ba\rangle$

Proof $K = \langle a\rangle = \{ra + na | r \in R, n \in \mathbb{Z}\}$ $J = \langle b\rangle = \{sb + nb | s \in R, n \in \mathbb{Z}\}$ $\langle ab\rangle = \langle ba\rangle = \{hab + nab | h \in R, n \in \mathbb{Z}\}$

直接计算KJ任意一项$(ra + na)(sb + nb) \in \langle ab\rangle$即可

且$\langle ab\rangle$中任一一项$\underbrace{(h + ne)}_{\in K} ab \in KJ$

Proposition 3.12 (整数环的理想结构)

进一步, 可以证明Z的任何理想都是主理想.

Proof 设I是Z的一个理想, 若I为零理想, 则$I = (0)$;

若I为非零理想, 则I中可以取到最小正整数a, 那么我们断言有$I = (a)$.

显然有$(a) \subseteq I$

反之, $\forall b \in I$, 有$b = aq + r$, 其中$q, r \in \mathrm{z}, 0 \leqslant r < a$, 那么$r = b - aq \in I$

由于a是I中的最小正整数, 可知$r = 0$, 即$b = aq \in (a)$, 得$I \subseteq (a)$.所以, $I = (a)$.

Definition 3.13 (商环定义)

设R是一个环,I是R的理想.考虑加法群$\{R;+\}$对于子群I的商群R/I,将$a\in R$所在的等价类记为$a+I$.
在R/I上定义乘法如下:$(a+I)(b+I)=ab+I$.则集合R/I对于商群的加法以及上述乘法运算构成一个环
称为R对于理想I的商环.

Note 前面我们知道R/I对于商群的加法构成一个交换群.又由前面的分析知道,如果I是理想,则定义商集合R/I的等价关系对于R的乘法
因此运算是合理的.又由于R满足结合律,R/I的乘法也满足结合律.
最后,对任何$a,b,c\in R$有

$$\begin{aligned}((a+I)+(b+I))(c+I)&=((a+b)+I)(c+I)=(a+b)c+I\\&=(ac+bc)+I=(ac+I)+(bc+I)\\&=(a+I)(c+I)+(b+I)(c+I).\end{aligned}$$

类似可证$(a+I)((b+I)+(c+I))=(a+I)(b+I)+(a+I)(c+I)$.即分配律成立.
因此R/I是环.

Proposition 3.13 (商环的基本性质)

如果R是交换环,则R/I也是交换环;
如果R是幺环,且1是R的单位元,则R/I也是幺环,且$1+I$是R/I的单位元.
如果R是无零因子环,那么R/I未必是无零因子环$\left(\text{若}a+I\times b+I=0+I\Longrightarrow ab\in I\right)$
$\left(\text{而在}\mathbb{Z}[x]\text{中},\langle x^4\rangle\text{生成的理想为}\left\{x^4f(x):\ f(x)\in\mathbb{Z}[x]\right\}\text{那么此时}x+I\text{与}x^2+I\text{是不同的但是}x\cdot x^2=x^3\notin x^4f(x)\right)$
又例如$\mathbb{Z}$是无零因子环但是$\mathbb{Z}/\langle 4\rangle\cong\mathbb{Z}_4$是有零因子环

Exercise 3.2 在整系数多项式环$\mathbb{Z}[x]$中,我们来看理想$(2,x)$.

Proof 因为$\mathbb{Z}[x]$是一个有单位元的交换环
由定理与生成主理想的结构可知

$$\begin{aligned}(2\cdot x)&=(2)+(x)\\&=\{2f(x)\mid f(x)\in\mathbb{Z}[x]\}+\{xg(x)\mid g(x)\in\mathbb{Z}[x]\}\\&=\{2f(x)+xg(x)\mid f(x),g(x)\in\mathbb{Z}[x]\}\\&=\{2a_0+xh(x)\mid h(x)\in\mathbb{Z}[x],a_0\in\mathbb{Z}\}\\&=\{\text{常数为偶数的所有整系数多项式}\}\end{aligned}$$

下面我们来证明$(2,x)$不是$\mathbb{Z}[x]$的主理想
假如$(2,x)$是$\mathbb{Z}[x]$的一个主理想,那么存在$p(x)\in\mathbb{Z}[x]$,使得$(2,x)=(p(x))=\{p(x)f(x)\mid f(x)\in\mathbb{Z}[x]\}$.
因为$2\in(p(x)),x\in(p(x))$,即存在$q(x),h(x)\in\mathbb{Z}[x]$,使得$2=q(x)p(x),\quad x=h(x)p(x)$,由$2=q(x)p(x)$,得$p(x)=a\in\mathrm{Z}$;
又时$x=h(x)p(x)=h(x)a$,得$a=\pm1$.于是$\pm1=p(x)\in(p(x))=(2,x)$,

Exercise 3.3 设$R=\mathrm{R}[x]$是实数域R上的一元多项式环$\mathrm{C}\cong\mathrm{R}[x]/\langle x^2+1\rangle$
$I=\langle x^2+1\rangle$是R上的多项式x^2+1生成的主理想

Proof 任取$f(x)\in\mathrm{R}$
则:由带余除法得$f(x)=g(x)\left(x^2+1\right)+(ax+b)$,其中$q(x)\in\mathrm{R},a,b\in\mathrm{R}$,于是$f(x)\equiv ax+b(I)$,即在$\mathrm{R}[x]/\left(x^2+1\right)$中,
$f(x)=\overline{ax+b}$,因而$\mathrm{R}[x]/\left(x^2+1\right)$是由一切剩余类$\overline{ax+b}(a,b\in\mathrm{R})$所组成,即$\mathrm{R}[x]/\left(x^2+1\right)=\{\overline{ax+b}\mid a,b\in\mathrm{R}\}$.
如果令$\varphi:\mathrm{C}\to\mathrm{R}[x]/\left(x^2+1\right),\quad ai+b\mapsto\overline{ax+b}$,下证$\varphi$为同构映射.
φ为满射是显然的.

若$\overline{ax+b}=\overrightarrow{cx+d}$, 则 $(ax+b)-(cx+d)\in\left(x^2+1\right)$, 即 $(a-c)x+(b-d)=q(x)\left(x^2+1\right)$, 有$a=c, b=d$, 故$\varphi$为单射.

且有

$$\varphi[(a\mathrm{i}+b)+(c\mathrm{i}+d)]=\varphi[(a+c)\mathrm{i}+(b+d)]=\overline{(a+c)x+(b+d)}=\overline{(ax+b)+(cx+d)}=(\overline{ax+b})+(\overline{cx+d})=\varphi(a\mathrm{i}+b)+\varphi(c\mathrm{i}+d);$$

$$\varphi(a\mathrm{i}+b)\cdot\varphi(c\mathrm{i}+d)=(\overline{ax+b})\cdot(\overline{cx+d})=\overline{(ax+b)(cx+d)}=\overline{acx^2+(ad+bc)x+bd}$$

$$=\overline{ac\left(x^2+1\right)+(ad+bc)x+(bd-ac)}=\overline{(ad+bc)x+(bd-ac)}+\overline{ac\left(x^2+1\right)}=\overline{(ad+bc)x+(bd-ac)}$$

$$=\varphi[(ad+bc)\mathrm{i}+(bd-ac)]=\varphi[(a\mathrm{i}+b)(c\mathrm{i}+d)].$$

因此, 我们得到$\mathrm{C}\cong\mathrm{R}[x]/\left(x^2+1\right)$.

Example 3.11 子环不是理想的反例

子环一定是理想吗?不一定.

1.在环$Z\times Z$中, 若$S=\{(n,n)\mid n\in Z\}$, 则S是$Z\times Z$的子环, 但对于$a=(2,3)\in Z\times Z, u=(1,1)\in S$, 有$au=(2,3)$不属于$S$

因此, S不是$Z\times Z$的理想.

2.设$R=M_2(P)=\{$数域P上的所有2阶矩阵$\}$, $A=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix}\mid a,b\in P\right\}$

则A是R的一个子环, 但A不是R的一个理想,

因为, 取$\begin{pmatrix}1&1\\1&1\end{pmatrix}\in R$, $\begin{pmatrix}1&1\\0&0\end{pmatrix}\in A$, 有$\begin{pmatrix}1&1\\1&1\end{pmatrix}\begin{pmatrix}1&1\\0&0\end{pmatrix}=\begin{pmatrix}1&1\\1&1\end{pmatrix}\notin A$

Example 3.12 单边理想的例子

考虑实数域上的2×2矩阵环$R=M_{2\times2}(\mathbb{R})$

考虑$R_1=\left\{\begin{pmatrix}a&0\\b&0\end{pmatrix}:a\in\mathbb{R},\mathrm{b}\in\mathbb{R}\right\}$容易检验$R_1$是$R$的左理想而不是右理想

类似地，考虑$R_2=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix}:a\in\mathbb{R},b\in\mathbb{R}\right\}$容易检验$R_2$是$R$的右理想而不是左理想

Example 3.13 理想的理想不再是理想

考虑一元整系数多项式环$Z[x]$

$\left\langle x^2\right\rangle$在$\mathbb{Z}[x]$中生成的理想该理想为$\left\{x^2f(x):\ f(x)\in\mathbb{Z}[x]\right\}$

考虑$\left\langle x^3\right\rangle$在由$\left\langle x^2\right\rangle$所生成的理想$\left\{kx^3+x^5f(x)\mid k\in Z, f(x)\in Z[x]\right\}$

然而却不是$\mathbb{Z}[x]$的理想

R为域F上三阶上三角方阵环$N=\left\{\begin{bmatrix}0&0&x\\0&0&y\\0&0&0\end{bmatrix},x,y\in F\right\}$, $H=\left\{\begin{bmatrix}0&0&0\\0&0&a\\0&0&0\end{bmatrix},a\in F\right\}$

容易验证：N是R的理想, H是N的理想.但是H不是R的理想

✍ **Exercise 3.4** 在整系数多项式环Z[x]中

我们来看理想$(2,x)$.因为z[x]是一个有单位元的交换环主理想的结构可知

$$
\begin{aligned}
(2.x) &= (2) + (x) \\
&= \{2f(x) \mid f(x) \in \mathrm{Z}[x]\} + \{xg(x) \mid g(x) \in \mathrm{Z}[x]\} \\
&= \{2f(x) + xg(x) \mid f(x), g(x) \in \mathrm{Z}[x]\} \\
&= \{2a_0 + xh(x) \mid h(x) \in \mathrm{Z}[x], a_0 \in \mathrm{Z}\} \\
&= \{\text{常数为偶数的所有整系数多项式}\}
\end{aligned}
$$

下面我们来证明 $(2,x)$不是$\mathrm{Z}[x]$的主理想.

假如 $(2,x)$是$\mathrm{Z}[x]$的一个主理想, 那么存在$p(x) \in \mathrm{Z}[x]$, 使得 $(2,x) = (p(x)) = \{p(x)f(x) \mid f(x) \in \mathrm{Z}[x]\}$.

因为$2 \in (p(x)), x \in (p(x))$, 即存在$q(x), h(x) \in \mathrm{Z}[x]$, 使得$2 = q(x)p(x), \quad x = h(x)p(x)$

由$2 = q(x)p(x)$, 得$p(x) = a \in \mathrm{Z}$; 又时$x = h(x)p(x) = h(x)a$, 得$a = \pm 1$

于是 $\pm 1 = p(x) \in (p(x)) = (2,x)$, 这与 $\pm 1 \notin (2,x)$矛盾, 因此, $(2,x)$不是$\mathrm{Z}[x]$的主理想.

3.4 环的同构基本定理与反同态

Definition 3.14 (自然满同态)

设I是环R的理想, 则R到R/I的自然映射$\pi: R \to R/I, \quad \pi(a) = a + I$为一个满同态, 称为自然同态.

Lemma 3.2

$\varphi: R \to R'$为一环同态

1.Kerφ为理想

2.Imφ为子环, 若映射一开始就为满同态, 则吧理想映到理想

Theorem 3.11 (环同态基本定理)

设$f: R \to R'$是环同态映射, 令$I = \mathrm{Ker} f$

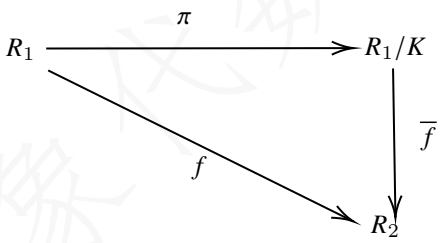
则存在R/I到R'的唯一单同态映射f^*.使得$f = f^* \circ \psi$, 其中ψ是R到R/I的自然同态.

Theorem 3.12 (环同构第一基本定理)

设f是环R_1到环R_2的满同态, 记$K = \mathrm{Ker} f$.设π为R_1到R_1/K的自然同态,

(1) 存在的商环R_1/K到R_2的同构$\bar{f}$, 使得$f = \bar{f} \circ \pi$, 即有交换图如下

(2) $R_1/Ker f \cong R_2$



Proof 首先, f作为环同态, 一定是加法群$\{R_1; +\}$到$\{R_2; +\}$的群同态; 而π作为环R_1到$R_1/\mathrm{Ker} f$的自然同态一定是加法群R_1到其商群$R_1/\mathrm{Ker} f$的环自然同态.

由群的同态基本定理我们知道, 存在由加法群$R_1/\mathrm{Ker} f$到R_2的群同构$\bar{f}$使得$f = \bar{f} \circ \pi$.

我们证明, $\bar{f}$一定为环同构.为此只需证明$\bar{f}$保持乘法.对任何$a, b \in R_1$, 有

$$\begin{aligned}\bar{f}((a+K)(b+K)) &= \bar{f}(\pi(a)\pi(b)) = \bar{f}(\pi(ab)) \\ &= \bar{f} \circ \pi(ab) = f(ab) = f(a)f(b) \\ &= \bar{f}(\pi(a))\bar{f}(\pi(b)) = \bar{f}(a+K)\bar{f}(b+K).\end{aligned}$$

这证明$\bar{f}$保持乘法.故$\bar{f}$为$R_1/\mathrm{Ker} f$到R_2的环同构, 因而$R_1/\mathrm{Ker} f \simeq R_2$, 且有上述交换图.

Remark 设R为环, 则R的任一个商环都是R的同态象, 反之一个R的同态像 (f联系) 都与$R/Ker f$同构

Theorem 3.13 (环同构第二基本定理)

设f是环R_1到环R_2的满同态, 记$K = \mathrm{Ker} f$.则

1.f诱导了R_1中包含K的子环与R_2的子环之间的一一对应, 且将理想对应到理想;

2.如果I是R_1的理想, 且包含K, 则有$R_1/I \simeq R_2/f(I)$.

Proof 由群的同态基本定理, f建立了R_1中包含K的加法子群到R_2的加法子群之间的一一对应, 记为$\tilde{f}$.
回忆一下, 这一对应是这样定义的 : 如果H为 $\{R_1;+\}$ 的包含K的加法子群, 则$\tilde{f}(H)=f(H)$(即H在f下的像集) 为 $\{R_2;+\}$ 的子群
反之, 对任何 $\{R_2;+\}$ 的子群H', $\tilde{f}^{-1}(H')=f^{-1}(H')$ (即H'的完全原像) 一定是 $\{R_1;+\}$ 的包含K的子群.

1.现在我们证明下列结论 :
(a)设H为R_1的子环, 且$H\supseteq K$, 则$f(H)$为R_2的子环.这一点在前文子环的性质就已经知道了
(b)若$H'\subseteq R_2$是子环, 则$f^{-1}(H')$是R_1的包含K的子环.显然$f^{-1}(H')$包含K, 因此只需证明其为子环.
同前面一样, 这也是前文已经明了的
(c)若$I\supset K$为R_1的理想, 则$f(I)$为R_2的理想.由 (a), $f(I)$为R_2的子环.又对任何$a'=f(a)\in f(I)$及$x'\in R_2$
由f为满射, 可取$x\in R_1$使$f(x)=x'$, 故由I为理想得$a'x'=f(a)f(x)=f(ax)\in f(I)$, $x'a'=f(x)f(a)=f(xa)\in f(I)$.
从而$f(I)$为R_2的理想.
(d)若I'为R_2的理想, 则$f^{-1}(I')$为包含K的理想.由 (b), $f^{-1}(I')$为包含K的子环.
又对任何$a\in f^{-1}(I')$及$x\in R_1$, 由I'为理想, 有$f(ax)=f(a)f(x)\in I'$, $f(xa)=f(x)f(a)\in I'$.故$ax,xa\in f^{-1}(I')$.
因此$f^{-1}(I')$为R_1的理想.
(e)除此之外由 (b) 我们知道f作为沟通R_1中包含 Ker$f$子环与R_2子环的映射是个满射
(f)若H_1, H_2是R_1中两个包含 Ker$f$的子环且$f(H_1)=f(H_2)$
故$\forall h_1\in H_1$则$\exists h_2\in H_2$使得$f(h_1)=f(h_2)\Longrightarrow h_1-h_2\in \mathrm{Ker}f$
则可令$h_1-h_2=h_3\in \mathrm{Ker}f\subseteq H_2\Longrightarrow h_1=h_2+h_3\in H_2$
故得到$H_1\subseteq H_2$同理可得$H_2\subseteq H_1$故$H_1=H_2\Longrightarrow f$为单射
综上f满足题干要求

2.设I是R_1的包含K的理想.设π'是R_2到$R_2/f(I)$的自然同态则$\pi'\circ f$是R_1到$R_2/f(I)$的满同态.
我们先证明 Ker$(\pi'\circ f)=I$.若$x\in I$, 则$f(x)\in f(I)$, 从而$\pi'(f(x))=0$, 故$x\in \mathrm{Ker}(\pi'\circ f)$;
另一方面, 若$x\in \mathrm{Ker}(\pi'\circ f)$, 则由$\pi'$的定义可知$f(x)\in f(I)$, 故$x\in f^{-1}(f(I))$.
由1.我们知道, f建立了R_1中包含K的理想到R_2的理想的一一对应$\tilde{f}$.或由第一同构定理都有$R_1/I\cong R_2/f(I)$

Corollary 3.3 (第二环同构基本定理应用在自然环满同态上)

设I_1,I_2均为环R的理想, 且$I_1\subseteq I_2$
1.则有R中包含了I_1的子环与R/I_1的子环的一一对应
2.$R/I_2\simeq (R/I_1)/(I_2/I_1)$.

Theorem 3.14 (环同构第三基本定理)

φ: $R\to R'$的环满同构, $N=Ker\varphi$是G的理想, H是G的子环
1.$H+N$是H在φ下的像$\varphi(H)$的完全原像且有$\varphi(H)=\varphi(H+N)$
2.$H/H\cap N\cong \varphi(H)=\varphi(H+N)$

Proof 一方面$H+N$是R的一个子环且知道$\varphi(H+N)=\varphi(H)$故由同构第二基本定理知道
$H+N$是H在φ下的像$\varphi(H)$的完全原像
此外构造$\varphi|_H$: $H\to\varphi(H)$该环满同态此时 Ker$\varphi|_H=H\cap N$
故由同构第一基本定理知道$H/H\cap N\cong\varphi(H)$

Corollary 3.4 (环同构第三基本定理应用在环自然满同态上)

设I,J为环R的理想, 则有同构$(I+J)/I\simeq J/(I\cap J)$.

Definition 3.15 (环的反同态与反同构)

设R_1,R_2为两个环,一个R_1到R_2的映射φ称为一个反同态,如果

(1)φ是$\{R_1;+\}$到$\{R_2;+\}$的群同态;

(2)对任何$a,b\in R_1$,有$\varphi(ab)=\varphi(b)\varphi(a)$.

如果一个反同态是一个同构,则称其为反同构.如果两个环R_1,R_2之间存在一个反同构,则称R_1与R_2是反同构的.

Problem 3.3 设$\mathbb{P}$为数域,在环$\mathbb{P}^{n\times n}$中定义映射$\varphi,\varphi(A)=A'$,则φ是一个反同构.

Definition 3.16 (环的半同态)

设R_1,R_2为两个环,一个R_1到R_2的映射φ称为一个半同态,如果

(1)φ是$\{R_1;+\}$到$\{R_2;+\}$的群同态;

(2)对任何$a,b\in R_1,\varphi(ab)=\varphi(a)\varphi(b)$或$\varphi(ab)=\varphi(b)\varphi(a)$至少有一个成立.

Proposition 3.14

一个非常有趣的问题是,是否存在真正的半同态?即是否存在一个半同态φ,φ既不是同态,也不是反同态.

设φ为环R_1到R_2的半同态,则φ或为同态,或为反同态.

Proof 我们将利用群论中任一群都不能写成两个真子群的并这一结论来证明本定理.

设φ为环R_1到R_2的半同态.对任意固定的$a\in R_1$,定义

$l_a=\{b\in R_1\mid\varphi(ab)=\varphi(a)\varphi(b)\}$,

$r_a=\{b\in R_1\mid\varphi(ab)=\varphi(b)\varphi(a)\}$.

我们断定l_a,r_a都是加法群$\{R_1;+\}$的子群.只对l_a证明,对r_a的证明类似.

因$0\in l_a$,故l_a非空.此外,若$b_1,b_2\in l_a$,则有

$$\begin{aligned}\varphi(a(b_1-b_2))&=\varphi(ab_1-ab_2)=\varphi(ab_1)-\varphi(ab_2)\\&=\varphi(a)\varphi(b_1)-\varphi(a)\varphi(b_2)\\&=\varphi(a)(\varphi(b_1)-\varphi(b_2))\\&=\varphi(a)\varphi(b_1-b_2),\end{aligned}$$

因此$b_1-b_2\in l_a$.这证明了我们的断言.

由条件,我们有$l_a\cup r_a=R_1$,因此$l_a=R_1$或$r_a=R_1$必有一个成立.

现在我们定义$R_l=\{a\in R_1\mid l_a=R_1\}$, $R_r=\{a\in R_1\mid r_a=R_1\}$.与前面类似可证,$R_l,R_r$都是加法群$\{R_1;+\}$的子群.

上面的结论说明$R_l\cup R_r=R_1$,因此我们有$R_l=R_1$或$R_r=R_1$,即φ为同态或反同态.

Proposition 3.15

设R为特征为p的无零因子交换环

证明由R到R的映射$F:a\mapsto a^p$是R的同态，称为$Frobenius$同态．试问F是否是单同态，是否是同构?

Proof 由R是特征为p的无零因子交换环，从而$F(a)+F(b)=a^p+b^p=(a+b)^p=F(a+b)$

且$F(a)F(b)=a^pb^p=(ab)^p=F(ab)$

从而F为环同态．又由$F(a)-F(b)=(a-b)^p=(a-b)(a-b)^{p-1}=0$，又无零因子

则若$a-b\neq0$，则$(a-b)^{p-1}=0$，从而归纳下去可得$a-b=0$，矛盾，故$a-b=0$，即$F(a)=F(b)$蕴含$a=b$，即为单同态

我们考虑$\mathbb{Z}_p[x]$，易见其为特征为p的交换么环，且设$f(x)g(x)=0$

则考虑首项系数可知必有一个多项式为0，进而无零因子，但显然$f(x)\mapsto(f(x))^p$不为同构，即为一个反例.

Proposition 3.16

设R为除环，证明R到任何环的非零同态一定是单同态

Proof 证明由R为除环，即R^*构成群，从而任意非零同态f

若$f(a)=f(0)=0$，断言$a=0$　否则若$a\neq 0$，那么有$f(e)=f\left(a\cdot a^{-1}\right)=f(a)f\left(a^{-1}\right)=0$，进而表明$f$为零同态，矛盾

故$a=0$

故$\forall f\left(a_1\right)=f\left(a_2\right)\Longrightarrow f\left(a_1-a_2\right)=0\Longrightarrow a_1-a_2=0\Longrightarrow a_1=a_2$

进而说明f为单同态，即证.

3.5 CRT 中国剩余定理

Lemma 3.3

设R为么环，I_1, I_2为R的理想，且$R = I_1 + I_2$

试证明对任何$a_1, a_2 \in R$，必存在$a \in R$使得$a - a_1 \in I_1, a - a_2 \in I_2$

Proof 证明由$R = I_1 + I_2$，从而存在$r_1, s_1 \in I_1, r_2, s_2 \in I_2$使得$a_1 = r_1 + r_2, a_2 = s_1 + s_2$

从而考虑$a = r_2 + s_1$，从而$a - a_1 = r_1 - s_1 \in I_1, a - a_2 = r_2 - s_2 \in I_2$，即证.

Definition 3.17

设R为么环，I, J为理想，我们称I, J互素，如果$I + J = R$，我们称R中元素x, y模理想I同余，如果$x - y \in I$，并记为$x \equiv y (\mathrm{mod} I)$

Lemma 3.4 (理想互素的等价定义)

理想互素的等价定义：设R为么环，I, J为理想，则I, J互素的充要条件为存在$a \in I, b \in J$使得$a + b = 1$

Proposition 3.17

1.Suppose $I_1, I_2, \cdots, I_n$ are ideals in a ring R . And we denote I as $I_1 \cap \cdots I_n$. Then I is also an ideal of R .We have the monomorphism

$$\varphi : R/I \to R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n$$

defined by

$$\varphi(r + I) = (r + I_1, r + I_2, \cdots, r + I_n) .$$

2. If $I_1, \cdots, I_n$ are pairwise coprime ideals, then for any $1 \leqslant j \leqslant n$,$I_j$ is prime with respect to the product of the other ideals, i.e. I_j and $\prod_{i \neq j} I_i$ are coprime.

Proof 1. 显然I为R的理想.而映射φ为环同态，且 Ker$\varphi = I$，从而由环同态基本定理得证.

2.Without loss of generality,we assume $j = 1$,then we need to prove that I_1 and $I_2 I_3 \cdots I_n$ are coprime.Since I_1 is coprime with each of $I_2, I_3, \cdots, I_n$,So

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

Then,$R = I_1 + I_2 I_3 \cdots I_n$

Theorem 3.15 (中国剩余定理)

设R为么环，且$I_1, I_2, \cdots, I_n$为两两互素的理想

则任意$r_1, r_2, \cdots, r_n \in R$，同余方程组
$$\begin{cases} x \equiv r_1 \pmod{I_1} \\ x \equiv r_2 \pmod{I_2} \\ \vdots \\ x \equiv r_n \pmod{I_n} \end{cases}$$
有解，且在模$I_1 \cap I_2 \cap \cdots \cap I_n$的意义下解唯一.

Proof 这个定理证明的核心在于：设理想I, J, K，且I与J, K均互素，则I与JK互素

首先JK由前文知道是R的理想这是没问题的其次

注意到存在$a, b \in I \ \ c \in J \ \ d \in K$使得$a + c = b + d = 1$，从而$1 = (a + c)(b + d) = (ab + ad + cb) + cd$

则存在$ab + ad + cb \in I, cd \in JK$使得和为1，故$I$与$JK$互素，由此不难归纳得到一般情形

下设$J_i=\prod_{j\neq i} I_j$为R中理想，且有上文可知I_i与J_i互素故存在$a_i\in I_i\quad b_i\in J_i$使得$a_i+b_i=1$，从而$r_ib_i-r_i=a_ir_i\in I_i$
故$r_ib_i\equiv r_i\,(\mathrm{mod} I_i)$，且任意$j\neq i$，由$b_i\in J_i$，故$r_ib_i\in I_j$，进而模$I_j$余0
综上有$x=\sum_{i=1}^{n} r_ib_i$为同余方程的一个解再设另有解x_0，则$x\equiv x_0\,(\mathrm{mod} I_i)\,,1\leq i\leq n$，从而$x\equiv x_0\,(\mathrm{mod} I_1\cap I_2\cap\cdots\cap I_n)$
综上我们完成了中国剩余定理（CRT）之证明.

Corollary 3.5

设R为幺环，且$I_1,I_2,\cdots,I_n$为两两互素的理想，则$R/\bigcap_{i=1}^{n} I_i\cong\bigoplus_{i=1}^{n} R/I_i$

♡

Proof 考虑$\sigma:R\to R/I_1\oplus\cdots\oplus R/I_n\quad x\mapsto(x+I_1,\cdots,x+I_n)$
则显然 Ker$\sigma=I_1\cap\cdots I_n$
而由中国剩余定理，任意$(\overline{r_1},\overline{r_2},\cdots,\overline{r_n})\in R/I_1\oplus\cdots\oplus R/I_n$，存在$x\in R$使得$\sigma(x)=(\overline{r_1},\overline{r_2},\cdots,\overline{r_n})$
故σ为满同态，因此由环的同态基本定理即证

Theorem 3.16

Let R be a ring and $I_1,I_2,\ldots,I_n$ be two ideal elements of R such that $I=I_1\cap I_2\cap\cdots\cap I_n$. We have the following result:
Let $\gamma:R\to R/I_1\oplus R/I_2\oplus\cdots\oplus R/I_n$, where $\gamma(a)=(a+I_1,a+I_2,\ldots,a+I_n)$. The mapping γ is surjective.

Proof By the result , we only need to prove that the following condition holds:

$$\gamma:R\to R/I_1\oplus R/I_2\oplus\cdots\oplus R/I_n,\quad \gamma(a)=(a+I_1,\ldots,a+I_n).$$

According to the previous reasoning, for any index j where $1\leq j\leq n$, there exist ideals I_j and $\ell_j\in I_1\ldots I_{j-1}I_{j+1}\ldots I_n$ such that $s_j+\ell_j=1$. Therefore, we have the following relation:

$$\ell_j+I_k=\begin{cases}1+I_k, & \text{if } k=j,\\ \ell_k, & \text{if } k\neq j.\end{cases}$$

Then, for any $(a+I_1,\ldots,a+I_n)\in R/I_1\oplus\cdots\oplus R/I_n$, we have:

$$a=a_1\ell_1+\cdots+a_n\ell_n\quad\text{where}\quad a=a_1\ell_1+\cdots+a_n\ell_n=0+0+a_k\cdot1+0+\cdots+0\equiv a_k\pmod{I_k}.$$

Thus, we conclude that:

$$\gamma(a)=(a+I_1,\ldots,a+I_n)=(a_1+I_1,\ldots,a_n+I_n).$$

Theorem 3.17

If $m_1,m_2,\ldots,m_n\in\mathbb{Z}$ are coprime, and $m=m_1m_2\ldots m_n$, then the following holds:

$$Z_m\cong Z_{m_1}\oplus Z_{m_2}\oplus\cdots\oplus Z_{m_n},\quad [a]\mapsto([a]_{m_1},[a]_{m_2},\ldots,[a]_{m_n}).$$

Proof By the previous theorem, the general solution to the equation is the following:

$$Z_m\cong Z_{m_1}\oplus\cdots\oplus Z_{m_n},\quad [a]\mapsto([a]_{m_1},\ldots,[a]_{m_n}).$$

Theorem 3.18 (Euler's Function)

Let $m = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$, then by the previous proposition, $Z_m \cong Z_{p_1^{n_1}} \oplus Z_{p_2^{n_2}} \oplus \cdots \oplus Z_{p_k^{n_k}}$, we get

$$Z_m^\times \cong Z_{p_1^{n_1}}^\times \oplus Z_{p_2^{n_2}}^\times \oplus \cdots \oplus Z_{p_k^{n_k}}^\times .$$

Proof Thus, we have:

$$\varphi(m) = \varphi(p_1^{n_1})\varphi(p_2^{n_2}) \dots \varphi(p_k^{n_k}).$$

Now, we only need to prove that for $\varphi(p^n) = p^{n-1}(p-1)$ for p prime: we know every number that less than p^n can be expressed as

$$ap + b, \quad a = 0, 1, \dots, p^{n-1} - 1, \quad b = 0, 1, \dots, p - 1.$$

Hence,such number is coprime with p if and only if $b = 1, 2, \dots, p-1$, so there are $p-1$ such numbers for each fixed a. Therefore, we have

$$\varphi(p^n) = p^{n-1}(p-1).$$

3.6 整环上的因子分解

Definition 3.18 (整除与因子)

设R为一个整环，$a,b\in R$，若存在$c\in R$使得$a=bc$，称a能被b整除，这时也称b为a的因子.

Definition 3.19 (相伴)

设R为整环，$a,b\in R$，若存在R中的单位（乘法可逆元）u，使得$a=ub$，则称a与b相伴，记为$a\sim b$

Definition 3.20 (平凡因子与真因子)

设R为一个整环，$a\in R^*$则单位与a相伴的元都称为a的平凡因子

真因子：a的除单位，除与a相伴的元

Definition 3.21 ((不) 可约元素与素元素)

设R为整环，$a\in R^*-U$

1.若a不存在真因子(或其因子只有平凡因子)，则称a为不可约元素，反之，则称a为可约元素

2.$p\in R^*-U$，如果对任何$a,b\in R, p\mid ab$蕴含$p\mid a$或者$p\mid b$，则称p为素元素.

Definition 3.22 (因子与公因子)

对R中n个元素$a_1,a_2,\cdots,a_n$，若c均能整除它们，称为其的一个公因子

若它们的一个公因子d满足能被其任何一个公因子整除，则称为其的一个最大公因子

Definition 3.23 (真因子链)

若R中的一个元素序列$a_1,a_2,\cdots$满足对任何$l\geq 1, a_{l+1}$为a_l的真因子，则称其为真因子链

Proposition 3.18

1.a相伴于$b\iff a\sim b\iff a|b$且$b|a\iff \exists u\in U$使得$a=ub$

2.相伴是R中的等价关系且是R^*中幺半群对于乘法的同余关系

3.a为单位$\iff a\sim 1$　且单位可作为任何元素的因子

4.单位没有真因子，单位不会有不可约元作为因子　单位的因子只有单位

5.真因子链中不会出现单位，且0元若出现也只会出现在第一个位置

6.a与b的最大公因子在相伴意义下唯一，记为(a,b)

7.$(0,a)=a$　u为单位$(u,a)=u$

8.整环中任意有限个元素的最大公因子存在，且在相伴意义下$(a,b,c)=(a,(b,c))$

9.对于任何的a,b,c属于整环R，则$c\,(a,b)\sim(ca,cb)$

10.对于任何的a,b,c属于整环R，若$(a,b)\sim 1,(a,c)\sim 1$则$(a,bc)\sim 1$

11.若$a\in R^*-U$且$a=pq$其中p为a的真因子则q也为a的真因子

12.乘单位不改变 (不) 可约性与 (不) 素性

13.整环R中，k为不可约元素，则k不可能写为两个非单位的乘积

14.c为不可约元$\iff c=ab$蕴含着a,b其中至少一个为单位

15.由14.素元一定是不可约元

Proof 4.假设单位u有一个真因子a此时若$a\mid u$但是$a=u\cdot u^{-1}a$矛盾

假设有一个不可约元p使得$p\mid u$与此同时$u\mid p\Longrightarrow u\sim p$故$p$也为单位

但是p为不可约元属于R^*-U矛盾

5.若单位的位次为 $\geqslant 2$时单位不是前一个的真因子，故单位不会出现在真因子链中
若单位的位次为1，则位次为2的a_2的作为单位的因子也只能为单位 (4.) 但是a_2为单位不能作为真因子出现在链中
故真因子链中不会出现单位
若0出现在链条中 $\geqslant 2$的位次，则前面的都为0但是0与0可以看作只相差一个单位，故非真因子
故0不会出现在链中 $\geqslant 2$位次

6.若对于a与b的最大公因子有两个记为d与k那么由最大公因子定义知道
$d \mid k$且$k \mid d \Longrightarrow d$相伴$k$

8.记 $(a,b,c)=d_1$记 $(a,(b,c))=d_2$则
$d_1 \mid a,b,c \Longrightarrow d_1 \mid (b,c) \Longrightarrow d_1 \mid d_2 \quad d_2 | a$且$d_2 \mid (b,c) | b,c$故$d_2$是$a,b,c$的公因子故$d_2 \mid d_1$
故在相伴意义下$d_1=d_2$

9.下面证明：对任何$a,b,c \in R_1, c(a,b) \sim (ca,cb)$
无妨设a,b,c都不为零．设 $(a,b)=d_1$，$(ca,cb)=d_2$
$WTS: cd_1 \sim d_2$
由$d_1 | a, d_1 | b$，我们得$cd_1 | ca \quad cd_1 | cb$，故$cd_1 \mid d_2$
由 $(ca,cb)=d_2 \Longrightarrow$ 设$ca=u_1 d_2$
由$cd_1 \mid d_2 \Longrightarrow d_2=u_2 cd_1$
则我们有$ca=u_1u_2cd_1$，从而$a=u_1u_2d_1$，故$u_2d_1 \mid a$，同样$u_2d_1 \mid b \Longrightarrow u_2d_1 \mid d_1$又$d_1 \mid u_2d_1$
$\Longrightarrow u_2d_1 \sim d_1$，故$u_2$是单位
由$d_2=u_2cd_1 \Longrightarrow$ 故$cd_1 \sim d_2$.

Proposition 3.19

1. $a \in R^{\times} \Longleftrightarrow Ra=R.$
2. $a \sim b \Longleftrightarrow Ra=Rb.$
3. $b \mid a \Longleftrightarrow a \in Rb \Longleftrightarrow Ra \subseteq Rb.$
4. b 是 a 的真约元 $\Longleftrightarrow Ra \subsetneq Rb \subsetneq R.$
5. a 是不可约元 $\Longleftrightarrow Ra$ 是 R 的极大的主理想。
6. a 是素元 $\Longleftrightarrow Ra$ 是 R 的非零素理想。

Proposition 3.20 (整环中的各个条件)

素条件：每个不可约元均为素元素
公因子条件：R中任何两个元都有最大公因子
因子链条件：任何一条真因子链均只有有限长度
有限分解条件：R^*-U中任何一个元素a，a均可写为有限个不可约元素的乘积
分解唯一条件：若$a=p_1p_2\cdots p_r=q_1q_2=\cdots q_s \Longrightarrow r=s$且在允许调换顺序的情况下使得$p_i \sim q_i$

Definition 3.24 (唯一分解整环 UFD)

设整环R满足有限分解条件，且满足分解唯一性，即对任何$a \in R^*-U$
如果a有两种分解：$a=p_1p_2\cdots p_r=q_1q_2\cdots q_s$其中$p_1,p_2,\cdots,p_r,q_1,q_2,\cdots,q_s$为不可约元素，则有$r=s$
而且适当交换顺序可以使得$p_i \sim q_i, 1 \leqslant i \leqslant r$，则称$R$为唯一分解整环.

Proposition 3.21

在任何整环中，素元素一定是不可约元素

Proof 设整环R，任取$p \in R^* - U$为一个素元素，设a为p的一个因子：WTS：a为p的平凡因子即可
此时不妨设$p = ab$且能够有$p \mid a$或$p \mid b$
若$p \mid a \Longrightarrow p \sim a$则$a$为$p$的相伴元因子，为平凡因子
若$p \mid b \Longrightarrow p \sim b$则$p = ub$带入得到$a = u$也为平凡因子

Lemma 3.5 (有限分解条件与因子链条件等价)

一个整环满足有限分解条件 $\Longleftrightarrow$ 其满足因子链条件

Proof 先假设整环R满足有限分解条件.
如果$a_1, a_2, \cdots$为R的真因子链，而且是无限的，则由于对任何$l \geqslant 1, a_{l+1}$都是a_l的真因子
a_l可以分解为$a_l = a_{l+1}b_{l+1}$，其中b_{l+1}也是a_l的真因子 (可用反证法)
这说明a存在一种分解方式，可以一直分解下去，与有限分解条件矛盾. 因此R满足因子链条件

反之，设R满足因子链条件来证明：R满足有限分解条件
先断言：$a \in R^* - U$, 先断言a有不可约元作为因子 (称为不可约因子)
若a为不可约元则其本身就作为a的不可约因子
若a可约，则$a = a_1b_1$ (其中a_1, b_1为a的真因子)
若a_1, b_1有一个不可约则证毕
若a_1, b_1都可约则可以设$a_1 = a_2b_2$ (a_2, b_2都为a_1的真因子)
若a_2, b_2有一个不可约则证毕
若a_2, b_2都可约类似的下去若无穷操作
我们可以得到一串真因子链：$a, a_1, a_2 \cdots$与因子链条件矛盾故断言成立

接下来：设$a = p_1a_1$ (其中p_1是不可约元, $p_1 \notin U$) 因为$a \in R^* - U$故$a_1 \neq 0$
若$a_1 \in U$则$a = (p_1a_1)$ (利用不可约元的相伴元仍然为不可约元) 则已经将a写为了一个不可约元的乘积
若$a_1 \in R^* - U$则同样利用断言得到$a_1 = p_2a_2$ (其中p_2是不可约元, $p_2 \notin U$)
此时能得到p_1为a的真因子 (利用反证法) 故立马得知a_1也为a的真因子，且$a_2 \neq 0$
若$a_2 \in U$则$a = p_1 (p_2a_2)$ 就写为了两个不可约元的乘积
若$a_2 \in R^* - U$则同样利用断言得到$a_2 = p_3a_3$ (其中p_3是不可约元, $p_3 \notin U$)
此时能得到p_2为a_1的真因子 (利用反证法) 故立马得知a_2也为a_1的真因子，且$a_3 \neq 0$
以此类推若此过程能无穷下去则有一串真因子链：$a, a_1, a_2 \cdots$
与因子链条件矛盾故上述操作在某一刻停止，此时整合起来就把a写为了若干个有限个不可约元的乘积

Lemma 3.6 (公因子条件能推出素条件)

整环R满足公因子条件 $\Longrightarrow$ R满足素条件

Proof 取$p \in R^* - U$且p为一个不可约元素，想要说明p为素元素WTS即：$p \mid ab \Longrightarrow p \mid a$或$p \mid b$
反证法若$p \nmid a$且$p \nmid b$此时又p为一个不可约元素
$(p, a) = d_1$则d_1作为p的因子所以只能是单位或者是p的相伴元
若d_1为p的相伴元up, 则$up \mid a \Longrightarrow a = upt \Longrightarrow p \mid a$矛盾
则d_1为单位则 $(p, a) \sim 1$同理 $(p, b) \sim 1$故 $(p, ab) \sim 1$
由于$p \mid ab \Longrightarrow (p, ab) = p \Longrightarrow p \sim 1 \Longrightarrow p$为单位矛盾

Lemma 3.7

设R为整环，则R为唯一分解整环(有限分解条件，唯一分解性) $\Longrightarrow$ R满足因子链条件与素条件

Proof 由前面的$lemma$知道唯一分解条件 $\Longleftrightarrow$ 因子链条件

故仅需证明R满足素条件.

设$p \in R^* - U$为不可约元素，且$p \mid ab$，则存在$c \in R$使得$ab = pc$. 我们需要证明$p \mid a$或$p \mid b$

我们将证明分成下面三种情形来完成

(i)若a, b中有一个等于0，结论是显然的

(ii)若a, b中有一个是单位，例如b为单位，则$a = abb^{-1} = pcb^{-1}$，因此$p \mid a$，结论也成立

(iii)设$a, b \in R^* - U$. 我们先说明$c \in R^* - U$

一方面：显然$c \neq 0$因为若$c = 0 \Longrightarrow ab = 0$因为整环满足无零因子性这与$a \neq 0$且$b \neq 0$矛盾

再者：若c为单位，则pc作为p的相伴元且p不可约 $\Longrightarrow$ pc为不可约元素，而它可以写成两个非单位的元素a, b的乘积，这是矛盾

$\Longrightarrow$ 故$c \in R^* - U$

那么由于已经满足的是有限分解条件与分解唯一条件

$\Longrightarrow$ 那么存在$R^* - U$中不可约元素$p_i (1 \leqslant i \leqslant t)$使得$c = p_1 p_2 \cdots p_t$

此外，a, b也有分解：$a = q_1 q_2 \cdots q_r$； $b = q_1' q_2' \cdots q_s'$其中$q_1, q_2, \cdots, q_r$，$q_1', q_2, \cdots, q_s'$为不可约元素

由$pc = ab$我们得到$q_1 q_2 \cdots q_r q_1' q_2' \cdots q_s' = p p_1 p_2 \cdots p_t$

由于分解的唯一性成立，p必与某一个q_i或某一个q_i'相伴

若$p \sim q_i$，则$p = q_i \varepsilon$，$\varepsilon \in U$，故$a = q_1 \cdots q_i \varepsilon \varepsilon^{-1} q_{i+1} \cdots q_r = p\left(\varepsilon^{-1} q_1 \cdots q_{i-1} q_{i+1} \cdots q_r\right)$即$p \mid a$

同理，若p与某个q_i'相伴，则$p \mid b$

即p必能整除a, b中的某一个. 因而p是素元素

Lemma 3.8

R为整环，R满足因子链条件与素条件 $\Longrightarrow$ R满足因子链条件与公因子条件

Proof 设R满足因子链条件与素条件进而可以得到R满足有限分解条件，我们只需证明R满足公因子条件

只需证：设$a, b \in R$，我们证明a, b存在最大公因子

我们同样将证明分下面几种情形来完成

(i)若a, b中有一个为零，例如，$a = 0$，则$(a, b) = (0, b) = b$是a, b的最大公因子

(ii)若a, b中有一个是单位，例如，a是单位，则a是a, b的最大公因子

(iii)设$a, b \in R^* - U$. 因为R满足因子链条件，从而满足有限分解条件

故a, b都存在分解$a = q_1 q_2 \cdots q_r$， $b = q_1' q_2' \cdots q_s'$其中$q_i, q_j' (i = 1, 2, \cdots, r \quad j = 1, 2, \cdots, s)$是不可约元素，即素元素

现在我们将出现在上述分解中的互相相伴的元写在一起，可以统一写成

$a = \varepsilon_a p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$， $b = \varepsilon_b p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n}$ (其中p_i为不可约为素元素且互不相伴，k_i与$l_i \geqslant 0$ ε_a与ε_b为单位)

令$m_i = \min(k_i, l_i), i = 1, 2, \cdots, n$ 令$d = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$

由定义显然$d \mid a$且$d \mid b$，即d是a, b的公因子

WTS：d为最大公因子，故任取c为公因子想说明$c \mid d$

假定c也是a, b的公因子，则显然$c \neq 0$(否则$a = b = 0$)

若c是单位，则显然$c \mid d$

若c不是单位，则$c \in R^* - U$则由有限分解条件 $\Longrightarrow$ 存在分解$c = p_1' p_2' \cdots p_t'$其中$p_i'$是素元素 (不可约元)

由于$c \mid a$，故$p_1' p_2' \cdots p_t' \mid \varepsilon_a p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n} \Longrightarrow p_i' \mid \varepsilon_a p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$

因为满足素条件故p_i'应该整除$\varepsilon_a p_1 p_2 \cdots p_n$当中的某一个，但是单位不可能有一个不可约元作为因子

于是p_i'必能整除某一个p_j，$p_i' \mid p_j$

由于p_j为不可约元素，故p_i'作为p_j的因子只能为单位或者p_j的相伴元，又p_i'不可约$\in R^* - U$

故p_i'与p_j它们相伴

类似的考虑p'_{i+1}等等
$\Longrightarrow c$也可以写成$c=\varepsilon_c p_1^{h_1}p_2^{h_2}\cdots p_n^{h_n}$其中$\varepsilon_c$是单位
此时由于c为a，b的公因子$\Longrightarrow c\mid a$
$\Longrightarrow \varepsilon_c p_1^{h_1}p_2^{h_2}\cdots p_n^{h_n}\mid \varepsilon_a p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n}$
$\Longrightarrow \varepsilon_a p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n}=\varepsilon_c p_1^{h_1}p_2^{h_2}\cdots p_n^{h_n}\times t$
断言$h_i\leqslant k_i$
因为若$h_1>k_1$则$\varepsilon_a p_2^{k_2}\cdots p_n^{k_n}=\varepsilon_c p_1^{h_1-k_1}p_2^{h_2}\cdots p_n^{h_n}\times t$
$\Longrightarrow p_1\mid \varepsilon_a p_2^{k_2}\cdots p_n^{k_n}\Longrightarrow p_1$整除$\varepsilon_a p_2\cdots p_n$某一个
但是ε_a作为单位不能有不可约元作为因子，且p_1与$p_2,p_3,\cdots p_n$互不相伴矛盾
故$h_i\leqslant k_i$
同理，由$c\mid b$也可推出$h_i\leqslant l_i$．故$h_i\leqslant m_i$
即$c\mid d$．故d是a,b的最大公因子．至此证明了R满足公因子条件．

Lemma 3.9

R为整环，R满足因子链条件与素条件$\Longrightarrow R$满足有限分解条件与唯一分解条件

Proof 因为因子链条件$\Longleftrightarrow$有限分解条件所以我们进行证明唯一分解条件
设$a\in R^*-U$，则a有分解$a=p_1p_2\cdots p_r$（p_i是不可约元素）．假定a还有另一个分解$a=q_1q_2\cdots q_s$（q_i是不可约元素）
我们证明$r=s$且适当交换顺序可使$p_i\sim q_i,1\leqslant i\leqslant r=s$
为此对r用归纳法
当$r=1$时$a=p_1=q_1q_2\cdots q_s$.
若$s>1$，则$p_1=q_1(q_2\cdots q_s)$.这说明p_1可以写成两个非单位的乘积，这是不可能的．故这时$r=s=1,p_1=q_1$
现在假定结论对$r=k-1$成立
当$r=k$时有$a=p_1p_2\cdots p_k=q_1q_2\cdots q_s.\Longrightarrow$于是$p_1\mid q_1q_2\cdots q_s$
由于满足素条件则R中不可约元素都是素元素，我们得到p_1必能整除q_j，$j=1,2,\cdots,s$中的某一个，通过交换顺序，无妨设$p_1\mid q_1$
由于p_1,q_1都是不可约的，故$p_1\sim q_1$．设$p_1=\varepsilon q_1$，其中ε是单位
则$(\varepsilon p_2)\cdots p_k=q_2q_3\cdots q_s$
由归纳假设$k-1=s-1=r-1$，且适当交换顺序可以使得$p_j\sim q_j,j=2,3,\cdots,r$且$p_1\sim q_1$
这说明结论对$r=k$也成立．至此定理证毕．

Theorem 3.19 (唯一分解整环 UFD 的若干等价条件)

设R为整环，则下面三个条件等价
（1）R为唯一分解整环
（2）R满足因子链条件和素条件
（3）R满足因子链条件和公因子条件.

Example 3.14 整环中不可约元素未必是素元素且未必存在最大公因子

1.是复数环的子环即可.
2.定义范数N：$N(\alpha)=N\left(a+b\sqrt{-5}\right)=a^2+5b^2$且范数满足$N(\alpha)\geqslant 0$且$N(\alpha\beta)=N(\alpha)N(\beta)$
3.求：$\mathbb{Z}\left[\sqrt{-5}\right]$的单位群$U$
$\forall\alpha\in U$则$\alpha\alpha^{-1}=1\Longrightarrow N(\alpha)N\left(\alpha^{-1}\right)=N(1)=1\Longrightarrow N(\alpha)=1\Longrightarrow a^2+5b^2=1\Longrightarrow a=\pm1,b=0\Longrightarrow\alpha=\pm1$
容易验证$\alpha=\pm1$为可逆元
故$U=\{\pm1\}$
4.说明3是$\mathbb{Z}\left[\sqrt{-5}\right]$的不可约元但不是素元素
设$\alpha=a+b\sqrt{-5}$为3的一个因子WTS：α只能是单位或者3的相伴元

有$3=\alpha\beta\Longrightarrow N(3)=9=N(\alpha)N(\beta)$于是$N(\alpha)=9$或者3或者1

若$N(\alpha)=9$则$N(\beta)=1\Longrightarrow\beta=\pm1\Longrightarrow\alpha\sim3$

若$N(\alpha)=3$则$a^2+5b^2=3$且$a,b\in\mathbb{Z}$无解

若$N(\alpha)=1$则α为单位

$\Longrightarrow$ 3是一个不可约元

我们知道$3\mid\left(2+\sqrt{-5}\right)\left(2-\sqrt{-5}\right)$但是$3\nmid2+\sqrt{-5}$且$3\nmid2-\sqrt{-5}$

反证若$3\mid2+\sqrt{-5}\Longrightarrow2+\sqrt{-5}=3\cdot\beta\Longrightarrow N\left(2+\sqrt{-5}\right)=N(3)N(\beta)\Longrightarrow9=9N(\beta)\Longrightarrow\beta=\pm1$

于是$2+\sqrt{-5}=\pm3$矛盾

5.说明$\alpha=6+3\sqrt{-5}$与$\beta=9$不存在最大公因子

若设d为最大公因子，此时发现3是$\alpha\beta$的一个公因子则$3\mid d$

设$d=3\left(a+b\sqrt{-5}\right)$则存在$c+d\sqrt{-5}$使得$3\left(a+b\sqrt{-5}\right)\left(c+d\sqrt{-5}\right)=9$

$$\Longrightarrow\begin{cases}ac-5bd=3\\ad+bc=0\end{cases}\quad(*)$$

取范数有$a^2+5b^2\mid9\Longrightarrow a^2+5b^2=1$或者3或者$9\Longrightarrow a+b\sqrt{-5}=\pm1$或者$\pm3$或者$\pm2\pm\sqrt{-5}$

若$a+b\sqrt{-5}=\pm2\pm\sqrt{-5}$带入$(*)$方程组无解

若$a+b\sqrt{-5}=\pm3$则$d=\pm9$此时就应该有$\pm9\mid6+3\sqrt{-5}$同理可列出相应的$(*)$类似的方程组无解

若$a+b\sqrt{-5}=\pm1$则$d=\pm3$则在相伴意义下最大公因子可取为3

此外发现$\alpha=6+3\sqrt{-5}=3\cdot\left(2+\sqrt{-5}\right)$且$\beta=9=\left(2+\sqrt{-5}\right)\left(2-\sqrt{-5}\right)$于是$\left(2+\sqrt{-5}\right)$为一个公因子

则应该有$\left(2+\sqrt{-5}\right)\mid3$同样列出$(*)$类似的方程组矛盾

故$\alpha=6+3\sqrt{-5}$与$\beta=9$不存在最大公因子

6.$\mathbb{Z}\left[\sqrt{-5}\right]$满足因子链条件

反证法，若不满足因子链条件，从而存在无限长的真因子链$a_1,a_2,\cdots,a_n,\cdots$，且$a_{i+1}$均为$a_i$的真因子

故$N(a_{i+1})$为$N(a_i)$的真因子，这表明正整数列$N(a_1),N(a_2),\cdots,N(a_n),\cdots$严格递减，矛盾！

3.7 素理想与极大理想

Note 让我们回忆一下,性质较好的环一般是整环甚至是域,因此找出构造这两种环的方法是重要的.
一般来说,我们遇到的很多例子都是交换么环.一个交换么环如果不是整环,那么就含有零因子.
这表明这个环太大了,因此需要模掉一个理想来得到整环或域.
设R为交换么环,I是R的理想.如果商环R/I是整环,那么就由$(a+I)(b+I)=0+I, a,b\in R$,可以推出$a+I=0+I$或$b+I=0+I$.
这就要求I满足条件$ab\in I\Rightarrow a\in I$或$b\in I$.这引导我们给出下面的定义.

Definition 3.25 (素理想定义)

设I为环R的理想,$I\neq R$,如果由$ab\in I$可以推出$a\in I$或$b\in I$,则称I为R的一个素理想.
有些书上也把单位理想包含进来

Proposition 3.22 (整数环中的素理想)

考虑整数环$R=\mathbb{Z}$.我们知道,R的任何理想都具有$m\mathbb{Z}, m\geqslant 0$的形式.
作为平凡的情形,零理想当然是R的素理想.
如果$m\neq 0$,则$m\mathbb{Z}$为素理想当且仅当$ab\in m\mathbb{Z}\Rightarrow a\in m\mathbb{Z}$或$b\in m\mathbb{Z}$,这也就是$m|ab\Rightarrow m|a$或$m\mid b$,亦即$m$为素数.
因此$m\mathbb{Z}$为素理想当且仅当$m=0$或m为素数.

Problem 3.4

考虑剩余类环$R=\mathbb{Z}_4$.容易看出,R只有三个理想:$\{\bar{0}\}, I=\{\bar{0},\bar{2}\}$和$R$本身.
因为R有零因子$\bar{2}$,所以$\{\bar{0}\}$不是R的素理想
.现在考虑I,若$a,b\in\{0,1,2,3\}$,且$\bar{a}\bar{b}\in I$,则a,b中必有一个为0或2,因此有$\bar{a}\in I$或$\bar{b}\in I$,从而I为素理想.

Theorem 3.20 (素理想与整环定理)

设R是交换么环,I是R的一个理想,$I\neq R$,则I是素理想$\Longleftrightarrow R/I$为整环.

Proof 因为R/I为整环.$(a+I)(b+I)=0+I\Longrightarrow a+I$或$b+I$为$0+I\Longrightarrow a$或$b$属于$I$
若I为素理想,因R是交换么环,R/I也是交换么环.在商环R/I中,若$(a+I)(b+I)=0+I$,则有$ab+I=0+I$,因此$ab\in I$.
由于I是素理想,故$a\in I$或$b\in I$.这说明$a+I=0+I$或$b+I=0+I$,因此R/I中没有零因子,从而是整环.

Corollary 3.6

注意到任何环R都同构于自身的商环$R/\{0\}$
设R是交换么环,则R是整环的充分必要条件是$\{0\}$为R的素理想.

Proposition 3.23 (素理想在同态下的性质)

设f是环R_1到R_2的满同态,I是R_1中包含$K=\mathrm{Ker}f$的一个素理想,则$f(I)$是R_2的素理想.

Proof 由理想在同态下的性质,$f(I)$为R_2的理想.
设$a_2,b_2\in R_2$,且$a_2b_2\in f(I)$,则存在$c\in I$使得$a_2b_2=f(c)$.因f为满同态,存在$a_1,b_1\in R_1$使得$f(a_1)=a_2, f(b_1)=b_2$.
这样就有$f(a_1)f(b_1)=f(c)$.由f为同态,有$f(a_1b_1-c)=f(a_1)f(b_1)-f(c)=0$,于是$a_1b_1-c\in K\subseteq I$.
由此我们得到$a_1b_1\in I$.利用假设I为素理想,得到$a_1\in I$或$b_1\in I$.故有$a_2=f(a_1)\in f(I)$或$b_2=f(b_1)\in f(I)$.这说明$f(I)$为素理想.

Note 设A,B为交换幺环R的两个非空子集,记$AB=\{\sum a_ib_i \mid a_i\in A,b_i\in B\}$,其中的和号代表有限和.
容易证明,如果A,B都是R的子环 (理想),那么AB也是R的子环 (理想).

Definition 3.26

设I是交换幺环R的真理想,则I是R的素理想当且仅当对任何理想A,B,由$AB\subseteq I$可推出$A\subseteq I$或$B\subseteq I$.

Proof 必要性设I是R的素理想,A,B是R的理想且$AB\subseteq I$.
采用反证法,假设A,B都不包含于I,则存在$a\in A,b\in B$使得$a\notin I,b\notin I$.但是由条件我们又有$ab\in AB\subseteq I$,这与I是素理想矛盾.
充分性我们同样采用反证法,假设I满足定理的条件但不是素理想,则存在$a,b\in R$,使得$ab\in I$但$a\notin I,b\notin I$.作理想$A=\langle a\rangle,B=\langle b\rangle$.
由R是交换幺环,容易看出$AB=\langle ab\rangle\subseteq I$,这与所给的条件矛盾.因此$I$是素理想.

Proposition 3.24

设R为唯一分解整环,$p\in R$则p为不可约元素 (素元素)$\iff\langle p\rangle$主理想为素理想

Proof 若R为UFD
1.若p为素元素,若$ab\in\langle p\rangle\Longrightarrow p\mid ab\Longrightarrow p\mid a$或者$p\mid b\Longrightarrow p\in\langle a\rangle$ 或者$p\in\langle b\rangle$
2.若$\langle p\rangle$为素理想,且$p\mid ab\Longrightarrow ab\in\langle p\rangle\Longrightarrow a\in\langle p\rangle$或者$b\in\langle b\rangle\Longrightarrow p\mid a$或者$p\mid b$

Note 下面介绍极大理想的概念.我们继续上面素理想定义以前的分析.
一个交换幺环R不能成为域,原因还是R太大了,即包含的元素太多,因此需要模掉一个理想.
设I为R的理想,让我们看看商环R/I成为域的条件
首先我们当然需要$I\neq R$.其次,如果R/I为域,那么对于任何$a\notin I,a+I$在R/I中存在逆元$b+I$
因此有$(a+I)(b+I)=1+I$,即$1-ab\in I$.特别地,如果I_1为R的理想,$I\subset I_1$且$I_1\neq I$,那么就存在$a\in I_1-I,b\in R$使得$1-ab\in I$.
于是对任何$c\in R$,有$c=(1-ab+ab)c=(1-ab)c+(ab)c=(1-ab)c+a(bc)$.
因I为理想且$1-ab\in I$,有$(1-ab)c\in I\subseteq I_1$;又由$I_1$为理想,且$a\in I_1$,有$a(bc)\in I_1$.于是得到$c\in I_1$.这说明$I_1=R$.由此我们引入.

Definition 3.27 (极大理想定义)

设R环.R的理想I称为极大理想,若$I\neq R$,且包含I的R的理想只有I和R本身.

Proposition 3.25 (整数环的极大理想)

考虑例2.6.2中的整数环$R=\mathbb{Z}$.我们现在确定R的所有极大理想.
首先,$\{0\}$自然不是极大理想.
其次,如果$m\geqslant 2$且不是素数,则存在$n\geqslant 2$使得$n\mid m$且$n\neq m$,这样就有$m\mathbb{Z}\subset n\mathbb{Z}$且$m\mathbb{Z}\neq n\mathbb{Z},n\mathbb{Z}\neq R$,因此$m\mathbb{Z}$也不是极大理想.
下面我们证明,若p为素数,则$\langle p\rangle$是R的极大理想.事实上,设A是R的理想,且$\langle p\rangle\subset A,\langle p\rangle\neq A$,则存在$k\in A$,使得$k\notin\langle p\rangle$.
由p是素数,p,k互素.于是存在整数a,b使$ap+bk=1$.这样我们就得到$1\in A$.
于是对任何整数$l,l=l\times 1\in A$,从而$A=R$.因此$\langle p\rangle$是R的极大理想.故R的所有极大理想为$p\mathbb{Z}$,其中p为素数.

Lemma 3.10 (域与除环中极大理想的结构)

1.域 (除环) 中没有非零的真理想I
2.域 (除环) 中极大理想为$\{0\}$
3.对于域 (整环) 上的非零且不可逆元a,$\langle a\rangle$为一个非平凡理想

Proof 1.$\forall 0\neq a\in I$则$a\cdot a^{-1}=1\in I\Longrightarrow I=R$

2.任取域(除环)的极大理想I显然若$I\neq\{0\}\Longrightarrow I=R$与极大理想定义矛盾故$I=\{0\}$

3.显然$a\neq 0\Longrightarrow\langle a\rangle\neq\{0\}$且断言$\langle a\rangle\neq R$否则的话$ap=1\Longrightarrow a$可逆矛盾

Theorem 3.21 (极大理想与域)

设R为交换幺环,M为R的理想,则M是R的极大理想$\Longleftrightarrow$商环R/M是一个域.

Proof 设M为R的极大理想,我们证明商环R/M是域.为此只需证明R/M中每个非零元都是单位.

设$a+M\neq 0+M$,则$a\notin M$.考虑理想$I=\langle M\cup\{a\}\rangle$,则由$M$为极大理想有$I=R$.

因此存在$a_i\in M, r_i\in R, 1\leqslant i\leqslant n, r\in R$使得$\sum_{i=1}^{n}a_ir_i+ar=1$.两边取等价类得$(a+M)(r+M)=1+M$,因此在商环$R/M$中$a+M$可逆.

于是R/M是一个域.

反之,设R/M是域,则$\{0+M\}$是R/M的极大理想.

设A为R中包含M的理想,则A/M是R/M的理想,故$A/M=\{0+M\}$或$A/M=R/M$,即$A=M$或$A=R$.故M为极大理想.

Corollary 3.7

1.若R为交换幺环,则$\{0\}$是R的一个极大理想$\Longleftrightarrow R/\{0\}=R$是域

2.设F为一个非零整环,则F是域$\Longleftrightarrow F$仅有平凡理想

♡

Theorem 3.22 (极大理想是素理想)

因为域是整环故交换幺环 R 上M为极大理想$\Longleftrightarrow R/M$是域$\Longrightarrow R/M$是整环$\Longleftrightarrow M$为素理想

Proposition 3.26

设N为环R的理想,且R/N是除环

1.N为极大理想

2.$\forall a\in R$由$a^2\in N\Longrightarrow a\in N$

Proof(1)由R/N为除环,从而$\{0+N\}$是R/N的极大理想,从而任意I为R中包含N的理想,则I/N是R/N中包含$\{0+N\}$的理想

从而$I/N=\{0+N\}$或R/N,这表明$I=N$或R,从而N为极大理想

(2)反证法,若$a\notin N$,则由R/N为除环,故存在$b\notin N$,使得$(a+N)(b+N)=e+N$,进而

$a+N=(a+N)(e+N)=\left(a^2+N\right)(b+N)=0+N$,这表明$a\in N$,矛盾!从而$a\in N$

Example 3.15 是素理想但不是极大理想反例

$\varphi:\mathbb{Z}[x]\to\mathbb{Z}\quad f(x)\to f(0)\quad Ker\varphi=\langle x\rangle\Longrightarrow\mathbb{Z}\simeq\mathbb{Z}[x]/(x)$

整数环$\mathbb{Z}$是整环,但不是域$\Longrightarrow\mathbb{Z}[x]/(x)$是整环,但不是域.

所以(x)是素理想,但不是极大理想.

Proposition 3.27 (整数环中理想的结构)

至今我们总结一下:$\mathbb{Z}$整数环中的理想结构

1.所有的理想均为$m\mathbb{Z}$的形式

2.所有的理想均为主理想

3.所有的素理想为$\{0\}$;$p\mathbb{Z}\left(p\text{为素数}\right)$;若计算单位理想也可以加入$\mathbb{Z}$

4.所有的极大理想为$p\mathbb{Z}\left(p\text{为素数}\right)$

Proposition 3.28 ($\mathbb{Z}_m$中理想与素理想与极大理想的结构)

1.若m为质数那么$\mathbb{Z}_m$为域.而域中没有真理想,在这里我们讨论的素理想与极大理想并不包括R

此时我们来考察唯一剩下的可能零理想$\{0\}$.显然因为$\mathbb{Z}_m$是域$\Longrightarrow \{0\}$既是素理想又是极大理想(推论3.6)

所以$Z/(m)$的素理想与极大理想都是$\{\overline{0}\}$。

2.若m为合数,$\mathbb{Z}_m$是$\mathbb{Z}/\langle m\rangle$商环.

根据同构定理我们知道环R，I为理想，则R/I的理想的结构为J/I；其中J是环R的理想且J包含I

R包含I的素理想与R/I的素理想一一对应;R包含I的极大理想与R/I的极大理想形成了一一对应

此时：针对该情形我们就去考虑$\mathbb{Z}$中包含了$\langle m\rangle$的素理想与极大理想即可

而$\mathbb{Z}$是主理想整环其中的素理想与极大理想都形如$p\mathbb{Z}=\langle p\rangle$的形式

所以若$\langle m\rangle\subset\langle p\rangle\Longrightarrow p|m$;设$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$

那么所以$Z/(m)$的素理想和极大理想都是:$(p_i)/(m)=p_iZ/(m)=p_iZ_m, i=1,2,...,k$，都是$k$个

比如$m=18=2\cdot 3^2$，$Z/(m)$的素理想和极大理想都是:$2Z_{18}=\{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8},\overline{10},\overline{12},\overline{14},\overline{16}\}$　$3Z_{18}=\{\overline{0},\overline{3},\overline{6},\overline{9},\overline{12},\overline{15}\}$

3.更一般地，$Z/(m)$的理想有$\prod_{i=1}^{k}(\alpha_i+1)$个，即$m$的因数^{a}个数

Proposition 3.29 ($\mathbb{R}[x]$ 上的极大理想)

设$p(x)\in\mathbb{R}[x]$，那么设其全体不可约因式为$p_1(x),\cdots,p_m(x)$

下证：$\mathbb{R}[x]/\langle p(x)\rangle$的全体极大理想为$\langle p_k(x)\rangle/\langle p(x)\rangle$，其中$1\le k\le m$

$\mathbb{R}[x]$是ED，自然为PID，我们可得$\mathbb{R}[x]/\langle p(x)\rangle$的极大理想与$\mathbb{R}[x]$中包含$\langle p(x)\rangle$的极大理想一一对应

设I为极大理想且$\langle p(x)\rangle\subseteq I$，一方面$I$为主理想，从而存在$q(x)$使得$I=\langle q(x)\rangle$，这意味着$q(x)\mid p(x)$

另一方面$\langle q(x)\rangle$为极大理想，从而$q(x)$是$\mathbb{R}[x]$中的不可约多项式(可用反证法)，即证

Problem 3.5

设$R=\boldsymbol{Z}[x,y]$,证明$\langle x,y\rangle$是R的素理想

Proof 因为R是整系数$\boldsymbol{Z}$上的二元多项式环,它是一个有单位元的交换环,所以,

$(x,y)=(x)+(y)=\{xf(x,y)\mid f(x,y)\in\boldsymbol{Z}x,y]\}+\{yg(x,y)\mid g(x,y)\in\boldsymbol{Z}x,y]\}=\{\boldsymbol{Z}[x,y]$上常数为零的多项式全体$\}$。

因为任意两个常数项都不为零的二元多项式的乘积一定是常数项不为零的,所以,(x,y)是R的素理想。

Problem 3.6

设R是偶数环,p是素数,$(2p)$是不是R的极大理想?是不是R的素理想?

Proof 先证$(2p)$是R的极大理想.

因为R是一个没有单位元的交换环,所以$(2p)=\{r(2p)+n(2p)\mid r\in R,n\in\boldsymbol{Z}\}=\{n(2p)\mid n\in\boldsymbol{Z}\}$

由$2\in R$,但$2\notin(2p)$,得$R\neq(2p)$.

如果有R的理想M,使得$(2p)\subsetneq M\subseteq R$,

则存在$a\in M, a=2k$,但$a\notin(2p)$,得$2k$不是$2p$的倍数,即k不是p的倍数,众而由p为素数得$(a,p)=1$

因此,存在整数s,t,使得$sa+tp=1$,则$(2s)a+\lambda(2p)=2\in M$,从而证得$M=R$

所以,$(2p)$是R的极大理想

再考虑素理想

当p为偶素数2时,则有$(2p)=(4)=4\boldsymbol{Z}$,因为$2\notin(2p)$,但$2\times 2=4\in(2p)$,所以,当$p=2$时,$(2p)$不是R的素理想

当p为奇素数时,如果$a,b\in R$,即存在$k,l\in\boldsymbol{Z}$,使得$a=2k$,　$b=2l$,如果$ab=4kl\in(2p)$,即$2p\mid 4kl$,即$p\mid 2kl$

由于p是奇素数,所以有$p\mid k$或$p\mid l$,即$2p\mid 2k$或$2p\mid 2l$,从而得$a=2k\in(2p)$或$b=2l\in(2p)$

所以,当p为奇素数时,$(2p)$是R的素理想。

Problem 3.7

在$\boldsymbol{Z}[x]$中, 证明 : (x,n)是极大理想的充分必要条件是n为素数

Proof 因为$\boldsymbol{Z}[x]$是有单位元的交换环，因此, 我们只需证明 : $\boldsymbol{Z}[x]/(x,n)$是一个域的充分必要条件为n是素数

因为

$(x,n)=(x)+(n)=\{xf(x)\mid f(x)\in \boldsymbol{Z}[x]\}+\{ng(x)\mid g(x)\in \boldsymbol{Z}[x]\}=\{\text{常数项为}n\text{的倍数的整系数多项式}\},\forall f(x)\in \boldsymbol{Z}[x]$

如果$f(x)$的常数项为$a_0\in \boldsymbol{Z}$, 则由带余除法得$a_0=nq+r$, 其中$0\leqslant r<n$, 那么

$f(x)+(x,n)=[f(x)-a_0]+a_0+(x,n)=a_0+(x,n)=nq+r+(x,n)=r+(x,n)=\bar{r},$

所以, $\boldsymbol{Z}[x]/(x,n)=\{\overline{0},\overline{1},\cdots,\overline{n-1}\}\cong \boldsymbol{Z}_n$

因为$\boldsymbol{Z}_n$为域当且仅当n为素数, 所以, $\boldsymbol{Z}x]/(x,n)$是域当且仅当n为素数, 从而证得(x,n)是极大理想的充分必要条件n为素数。

Problem 3.8

设$M_2(\boldsymbol{Q})$是$\boldsymbol{Q}$上的二阶矩阵环

证明 : $M_2(\boldsymbol{Q})$只有零理想与单位理想, 但不是一个除环, 由此说明 : 关于有单位元的环R的极大理想M, 其商环R/M未必是除环

Proof 由本章4知$M_2(Q)$不存在真理想, 即$M_2(\boldsymbol{Q})$只有零理想与单位理想, 从而得零理想$\{0\}$是$M_2(\boldsymbol{Q})$的极大理想

我们在环$M_2(\boldsymbol{Q})$中取极大理想$M=\{0\}$, 则$R/M=R/\{0\}=R$

因为$M_2(\boldsymbol{Q})$是 – 个有零因子的环, 它不是一个除环, 所以, R/M不是除环。

3.8 主理想整环与欧几里得环

Definition 3.28 (主理想整环（PID）：*Principal Ideal Domain*)

如果一个交换么环的每个理想都是主理想，则称其为主理想环，若其还为整环，则称为主理想整环.

Proposition 3.30 ($\mathbb{Z}[x]$ 不是一个主理想整环)

反证法若是一个主理想整环则，$\langle 2, x^2+1\rangle = \langle g(x)\rangle$

则$2 \in \langle g(x)\rangle \Longrightarrow g(x) \mid 2 \Longrightarrow g(x) = \pm 1$或者$\pm 2$

且$g(x) \in \langle 2, x^2+1\rangle \Longrightarrow g(x) = 2h(x) + (x^2+1)k(x)$

令$x = 1$得到$2 \mid g(x)$ 所以$g(x) = \pm 2$

则 $\langle g(x)\rangle$ 为系数全为偶数的整系数多项式但是$x^2+1 \notin \langle g(x)\rangle$ 矛盾

Lemma 3.11

1.设$I_i, i = 1, 2, \cdots$为R中的一个升理想序列，即满足任意j，有$I_j \subset I_{j+1}$，则$I = \bigcup_{i=11}^{\infty} I_i$是$R$的理想.

2.若$a \sim 1 \Longleftrightarrow \langle a\rangle = R$

3.$a \mid b \Longleftrightarrow \langle b\rangle \subseteq \langle a\rangle$

4.$a \sim b \Longleftrightarrow \langle a\rangle = \langle b\rangle$

Lemma 3.12

设R为主理想整环则设p为一个不可约元(后我们知道亦即素元)，p生成的主理想为极大理想

Proof 设$\langle p\rangle$为p生成的主理想且设I为一个包含$\langle p\rangle \subsetneq I$的理想，下面说明$I = R$

因为R为主理想整环则$I = \langle r\rangle$则$\langle p\rangle \subsetneq \langle r\rangle \Longrightarrow r \mid p$又$p$不可约则$r \sim p$或$r$为单位

又$\langle p\rangle \subsetneq \langle r\rangle$故$r$只能为单位故$I = R$

Theorem 3.23

主理想整环$PID \Longrightarrow$唯一分解整环UFD

Proof 我们只需证明主理想整环满足因子链条件和素条件

(1) 先证明主理想整环满足因子链条件，即考虑R的一个序列$a_1, a_2, \cdots, a_n, \cdots$，其中$a_{k+1}$是$a_k$的真因子

则进而考虑a_k生成的主理想$\langle a_k\rangle$，从而不难看见$I_k \subset I_{k+1}$，故由引理$I = \cup_k I_k$为理想，进而为主理想

从而存在$d \in R$使得$\langle d\rangle = I$，从而由$d \in I$，故存在m使得$d \in I_m = \langle a_m\rangle$

我们断言a_m是序列中的最后一个元素

若不然存在a_m的真因子a_{m+1}，则由$a_{m+1} \in \langle d\rangle$，则$a_m | d | a_{m+1}$，矛盾！故可知$R$满足因子链条件

(2) 再证明主理想整环满足素条件

这部分证明的核心在于不可约元素生成的主理想为极大理想，那么利用模掉极大理想的商环是域就不难证明

设p为一个不可约元素且设$p \mid ab$

则在商环$R/\langle p\rangle$中有$(a + \langle p\rangle)(b + \langle p\rangle) = ab + \langle p\rangle = 0 + \langle p\rangle$，由引理$\langle p\rangle$为极大理想知$R/\langle p\rangle$为域进而为整环

从而不妨$a + \langle p\rangle = 0 + \langle p\rangle$，进而$p \mid a$，即证$p$为素元素，故满足素条件.

Theorem 3.24 (主理想整环的*Bezout*定理)

设R为主理想整环，$a, b \in R$，且d为a, b的一个最大公因子，则存在$u, v \in R$使得$d = ua + vb$

Proof 由R为主理想整环，从而存在d_1使得$\langle d_1\rangle = \langle a, b\rangle$，故有$d_1 \mid a, b$，从而$d_1 \mid d$

又$d_1 \in \langle a, b\rangle$，从而存在$u_1, v_1$使得$d_1 = u_1 a + v_1 b \Longrightarrow$可知$d \mid a, b$进而$d \mid d_1$

故$d \sim d_1$，进而存在单位ε使得$d = u_1 \varepsilon a + v_1 \varepsilon b = ua + vb$，即证.

Theorem 3.25 (主理想整环上的素理想与极大理想的等价)

主理想整环上(交换幺环+理想都为主理想),有素理想 $\Longleftrightarrow$ 极大理想

Proof 原因非常简单仅仅只需以下几条：1. a 是不可约元 $\Longleftrightarrow$ Ra 是 R 的极大的主理想。2. a 是素元 $\Longleftrightarrow$ Ra 是 R 的非零素理想。

Proof 对任意素理想 (a)，注意这里a一定为素元，因此任意 $(a)\subseteq(b)$，则$b\mid a$，因此$b=a$或为单位
这即表明任何一个比 (a)大的理想只能是 (a)或者R，即证.

Proposition 3.31 (PID 上等价性质)

R 为 PID，$0\neq a\in R, I=Ra$, 则下列命题等价：

1. I 为极大理想；
2. I 为素理想；
3. a 为素元
4. a 是不可约元

Theorem 3.26

UFD是PID $\Longleftrightarrow$ UFD中每个素理想是极大理想

Proof 一方面是显然的我们主要来证明：UFD+素理想是极大理想能够推出UFD是PID
先证明：两个素元(不可约元) p,q要么$p\sim q$要么$\exists a,b\in R$使得$ap+bq=1$(这也等价于 $(p,q)=1$)
若$p\nsim q$，能够断言 $\langle p\rangle$ 与 $\langle q\rangle$ 无包含关系，此时 $\langle p\rangle$ $\langle q\rangle$ 均为素理想亦是极大理想
此时 $\langle q\rangle\subsetneq\langle p,q\rangle$ 由 $\langle q\rangle$ 是极大理想那么 $\langle p,q\rangle=R\Longrightarrow\exists a,b\in R$使得$ap+bq=1$

再证明：对于$c,d\in R^*-U$，若c与d的因子分解中，c的不可约因子与d的不可约因子互不相伴
则存在a,b使得$ac+bd=1$
我们只需证明：对于不可约元p_1,p_2,q若 $(p_1,q)=1$且 $(p_2,q)=1\Longrightarrow(p_1p_2,q)=1$这利用 (等价于 $(p,q)=1$) 即可
那么再将上一行的结论应用于c，d的因子分解归纳下去即可

最后来证明R是一个PID，令I是一个理想若I为零理想则可写为 $\langle 0\rangle$，若I不为零理想，从I中挑选一个x
使得x有数目最少的素因子，我们说明$I=\langle x\rangle$
若能够取到$y\in I-\langle x\rangle$ 则$y\nsim x$，令$d=(x,y)$，$x=dx_d$且$y=dy_d$且x_d,y_d无公共的素因子那么
就有$ax_d+by_d=1\Longrightarrow ax+by=d$又$x\in I$，$y\in I\Longrightarrow d\in I$与$x$的定义矛盾

Definition 3.29 (欧几里得环（ED）：$Euclidean\ Domain$)

设R为整环，如果存在从R^*到$\mathbb{N}$(包含0) 的一个映射δ
使$\forall a,b\in R,b\neq 0$，存在$q,r\in R$使得$a=qb+r$，其中$r=0$或$\delta(r)<\delta(b)$，则称 (R,δ)为欧几里得环.

Note 你可能在其他书上看到的要求还有额外一条那就是要求 $\delta(a)\leqslant\delta(ab)$ 对所有 $a,b\in R^*$ 成立。但是事实上我们可以没有强制必要要求有这一条，如果我们有我们的 ED 的定义，我们可以造出一个新的映射 δ^* 满足我们的要求：

$$\delta^*(a)=\min\{\delta(ab)\mid b\in R^*\}$$

显然 δ^* 也是从 R^* 到 $\mathbb{N}\cup\{0\}$ 的映射，并且对于任意的 $a,b\in R^*$，我们有

$$\delta^*(ab)=\min\{\delta(abc)\mid c\in R^*\}\geqslant\min\{\delta(ac)\mid c\in R^*\}=\delta^*(a)$$

因此 δ^* 满足额外的要求，并且我们也可以验证 (R,δ^*) 仍然是一个欧几里得环。

Theorem 3.27

欧几里得环一定是主理想整环进而是唯一分解整环

Proof 设I为欧几里得环R的理想，δ为定义中的映射

若I只包含零元，则$I=\langle 0\rangle$

若I包含非零元，则非负整数的集合$\{\delta(x)\mid x\in I,x\neq 0\}\subseteq\mathbb{N}\cup\{0\}$中必存在最小者

设$a\in R^*\cap I$且$\delta(a)$达到最小值，则对任何$x\in I,x\neq 0$有$\delta(x)\geqslant\delta(a)$

由定义对任何$b\in I$，存在$q,r\in R$使得$b=qa+r$，其中$r=0$或$\delta(r)<\delta(a)$．由于$a,b\in I$，故$r=b-qa\in I$

若$r\neq 0$，则$r\in I$且$\delta(r)<\delta(a)$，与a的取法矛盾

故$r=0$，即$b=qa$

由b的任意性我们得$I=\langle a\rangle$。故R是主理想整环．

Proposition 3.32

*Gauss*整数环是欧几里得环

Proof 对于$\beta=a+b\sqrt{-1}\in\mathbb{Z}[\sqrt{-1}]$，定义$\delta(\beta)=|\beta|^2=a^2+b^2$

设$\beta=a_1+b_1\sqrt{-1}\neq 0$，则对任何$c_1+d_1\sqrt{-1}$，有$\dfrac{c_1+d_1\sqrt{-1}}{a_1+b_1\sqrt{-1}}=s+t\sqrt{-1}$其中$s,t\in\mathbb{Q}$

故存在$c_2,d_2\in\mathbb{Z}$使$|c_2-s|\leqslant\dfrac{1}{2},|d_2-t|\leqslant\dfrac{1}{2}$

令$q=c_2+d_2\sqrt{-1}$，$r=c_1+d_1\sqrt{-1}-q\beta$，则$c_1+d_1\sqrt{-1}=q\beta+r$，且

$$\begin{aligned}\delta(r)&=\delta(\beta(s+t\sqrt{-1})-q\beta)\\&=\delta(\beta)\delta(s+t\sqrt{-1}-q)\\&\leqslant\left(\frac{1}{4}+\frac{1}{4}\right)\delta(\beta)<\delta(\beta).\end{aligned}$$

Proposition 3.33

1.$\mathbb{Z}$是一个欧几里得环其中$\delta:\mathbb{Z}^*\to\mathbb{N}\cup\{0\}\quad\delta(m)=|m|$

2.设$\mathbb{P}$为数域，则$\mathbb{P}$上的一元多项式环$\mathbb{P}[x]$是欧几里得环其中$\delta(f(x))=\deg f(x)\ (f(x)\neq 0)$

3.9 环上的多项式

3.9.1 一般环上的多项式

Definition 3.30

设$1 \in R \subseteq R_1$都为交换幺环，设$u \in R_1$，此时有包含R与u的最小的R_1的子环称之为添加u的R的环

且有$R[u] = \left\{a_0 + a_1u + a_2u^2 + \cdots + a_nu^n | a_i \in R\right\}$

Definition 3.31

若R上有有限个元$a_0, a_1 \cdots a_n$不全为零，使得$a_0 + a_1u + \cdots + a_nu^n = 0$

此时称u为R上的代数元，像这样的组合可能并不唯一，次数最小的称为该代数元在R上的次数

Definition 3.32

若$a_0 + a_1u + \cdots + a_nu^n = 0 \Longrightarrow a_i = 0\,(\forall i)$则称为$u$为$R$上的代数元

Definition 3.33

设$1 \in R \subseteq R_1$都为交换幺环，设$u \in R_1$，此时有包含R与u的最小的R_1的子环称之为添加u的R的环

且有$R[u] = \left\{a_0 + a_1u + a_2u^2 + \cdots + a_nu^n | a_i \in R\right\}$

当u为不定元时则称$R[u] = \left\{a_0 + a_1u + a_2u^2 + \cdots + a_nu^n | a_i \in R\right\}$为环上的$u$的多项式

Proposition 3.34

两个环上的多项式相等当且仅当其系数全部的相等，这里利用超越元即可

Theorem 3.28 (交换幺环诱导多项式环的存在性)

设R为可交换幺环，则环上的$R[u]$多项式环必定存在

Proof 构造集合$S = \left\{(a_0, a_1 \cdots a_n \cdots) | a_i \in R$且只有有限个$a_i \neq 0\right\}$

定义

$f = \{a_0, a_1, a_2, \cdots\}, g = \{b_0, b_1, b_2, \cdots\},$

$f + g = \{a_0 + b_0, a_1 + b_1, a_2 + b_2, \cdots\}$

$fg = \{a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \cdots\} = \{c_k\}$其中$c_k = \sum_{i+j=k} a_ib_j, \quad k = 0, 1, 2, \cdots$

则容易证明，S在上述加法和乘法下构成一个环

若R是么环，则S也是么环；若R是交换环，则S也是交换环

S的零元是$\{0, 0, 0, \cdots\}$，而$f = \{a_0, a_1, a_2, \cdots\}$的负元是$-f = \{-a_0, -a_1, -a_2, \cdots\}$

如果1是R的么元，则$\{1, 0, 0, \cdots\}$是S的么元

取$R_0 = \{(a_0, 0, 0 \cdots) | a_0 \in R\}$于是$R_0$为$S$的子交换幺环

构造$\varphi : R_0 \to R \quad (a_0, 0, 0 \cdots) \to a_0$为一个环同构映射

取$u = (0, 1, 0 \cdots)$此时其作为R上的不定元　不难发现$u^k = \left(\underbrace{0 \cdots 0}_{k\text{个}}, 1, 0 \cdots\right)$

$\left(\text{若} a_0 + a_1u + \cdots + a_nu^n = 0 \Longrightarrow (a_0, a_1 \cdots a_n) = 0 \Longrightarrow a_i = 0\right)$

且易知$R_0[u] = S$

Theorem 3.29 (可交换幺环的诱导多项式环同态)

设R, S为可换幺环，且φ为R到S的环同态，$\varphi(1_R) = 1_S = 1'$，任取$u \in S$

则φ可唯一的扩充为$R[x]$到S的一个环同态φ_u，$\varphi_u(x) = u$且$\varphi_u|_R = \varphi$

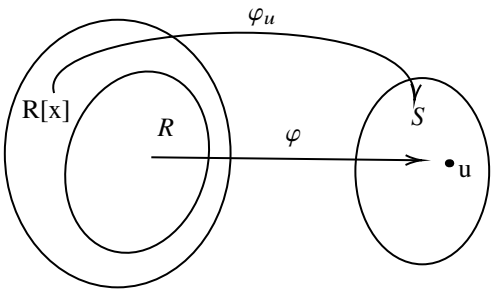
Proof $\forall a_0+a_1x+\cdots+a_nx^n\in R[x]$ 其中$a_i\in R$

$\varphi_u(a_0+a_1x+\cdots+a_nx^n)=\varphi_u(a_0)+\varphi_u(a_1)\varphi_u(x)+\cdots+\varphi_u(a_n)\varphi_u(x^n)=\varphi(a_0)+\varphi(a_1)u+\cdots+\varphi(a_n)u^n$

因此满足条件的映射是唯一的

构造φ_u即为$\varphi_u(a_0+a_1x+\cdots+a_nx^n)=\varphi(a_0)+\varphi(a_1)u+\cdots+\varphi(a_n)u^n$

不难说明φ_u是$R[x]$到S的一个环同态φ_u，且$\varphi_u|_R=\varphi$，$\varphi_u(x)=\varphi_u(1\cdot x)=1'u=u$



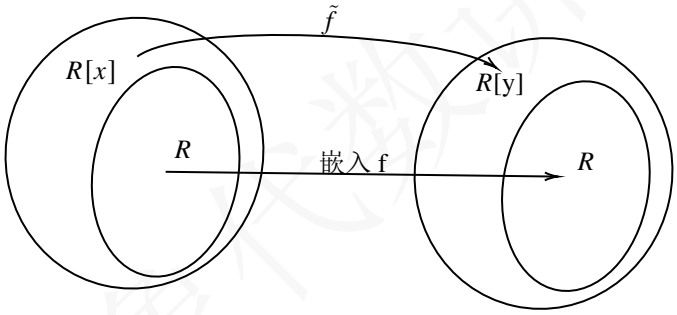
Corollary 3.8 (可交换幺环多项式环的唯一性)

设R为可换幺环，$R[x],R[y]$都是R上的一元多项式环则$R[x]\cong R[y]$

考察嵌入映射$f:R\to R\subseteq R[y]$

那么由定理知道f可唯一扩充为$\widetilde{f}:R[x]\to R[y]$的环同态且$\widetilde{f}(x)=y$且$\widetilde{f}|_R=f$

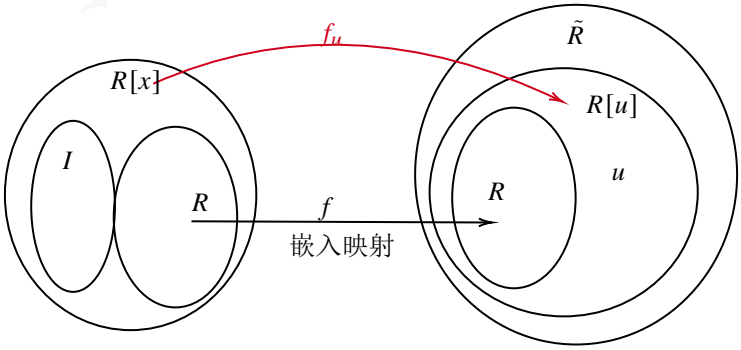
下说明$\widetilde{f}$即为环同构就说明单满射，满射是显然的，单射也显然



Corollary 3.9

设R为可换幺环，$\widetilde{R}$也为可换幺环且$1\in R\subseteq\widetilde{R}$，且$u\in\widetilde{R}$

证明：存在$R[x]$上的理想I使得$I\cap R=\{0\}$使得$R[u]\cong R[x]/I$，且u为R的代数元$\iff I\neq\{0\}$



Proof 考察R到$R\subseteq\widetilde{R}$的嵌入映射f由定理知道，存在唯一的f_u是$R[x]$到$\widetilde{R}$的环同态，$f_u(x)=u$且$f_u|_R=f$

我们考察$f_u:R[x]\to R[u]$这就为一个满同态，令$I=\mathrm{Ker}f_u$

则由环同构基本定理$R[u]\cong R[x]/I$，且$\forall a\in I\cap R$有$a=f(a)=f_u(a)=0\Longrightarrow I\cap R=\{0\}$

u为R上代数元$\iff$存在不全为零的$a_0,a_1\cdots a_n$使得$a_0+a_1u+\cdots+a_nu^n=0$

$\iff 0\neq a_0+a_1x+\cdots+a_nx^n\in I\iff I\neq\{0\}$

Corollary 3.10

设R为可换幺环, $R[x]$为R的一元多项式环，且I是$R[x]$的理想且$I \cap R = \{0\}$且$I \neq \{0\}$

证明：$R[x]/I$是R上添加一个代数元所构成的环

Proof 构造$\pi : R[x] \to R[x]/I$为自然同态且$\mathrm{Ker}\pi = I$

此时$\pi|_R : R \to \pi(R) \subseteq R[x]/I$为满同态且$\mathrm{Ker}\pi|_R = R \cap I = \{0\}$故$\pi|_R$为同构映射$\Longrightarrow R \cong \pi(R)$

令$u = \pi(x)$

因为$I \neq \{0\} \Longrightarrow$所以$I$中存在非零元素$0 \neq a_0 + a_1 x + \cdots a_n x^n \in I$(即$a_0 \sim a_n$不全为0)

又因为$R \cong \pi(R)$故$\pi(a_0) \sim \pi(a_n)$不全为零$\Longrightarrow \pi(a_0) + \pi(a_1)u + \cdots + \pi(a_n)u^n = 0 \Longrightarrow u$为代数元

$R[x]/I = \pi(R[x]) = \pi(R)[\pi(x)] = \pi(R)[u]$证毕

Theorem 3.30 (整环上的次数公式与带余除法)

1.设R为整环，$f(x), g(x) \in R[x]$设$g(x)$的首项系数不是零因子则$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$

2.设R为整环，$f(x), g(x) \in R[x]$.且$g(x) \neq 0$又$g(x)$的首项系数为R中乘法可逆元，进一步其实 R 为交换幺环，g 的首项系数为非

$\Longrightarrow$存在唯一多项式$q(x), r(x)$使得$f(x) = q(x)g(x) + r(x)$且$\deg(r(x)) < \deg(g(x))$

Corollary 3.11

Let R be a commutative ring, and let $f(x) \in R[x]$, $r \in R$. Then there exists a unique $q(x) \in R[x]$ such that

$$f(x) = (x - r)q(x) + f(r).$$

Proof Since $x - r$ is a monic polynomial, by the division algorithm 3.4.2, there exists a unique $q(x) \in R[x]$ and $s \in R$ such that

$$f(x) = (x - r)q(x) + s.$$

Substituting $x = r$, we get $f(r) = s$.

Proposition 3.35

1.R为交换幺环$\Longleftrightarrow R[x]$为交换幺环

2.R为整环$\Longleftrightarrow R[x]$为整环

3.设R为交换幺环，$f(x), g(x) \in R[x]$

若$f, g \in R[x], \deg f(x) = m, \deg g(x) = n$，则

(1) $\deg(f+g) \leqslant \max(m, n)$

(2) $\deg(fg) \leqslant \deg f(x) + \deg g(x)$，等号成立当且仅当$f$的首项系数$a_m$与$g$的首项系数$b_n$的乘积$a_m b_n$不为零

4.R为交换幺环，且$g(x)$首项系数不是零因子则：$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$

5.R为整环则$R[x]$中的单位就是R中的单位

Corollary 3.12

Let R be a ring. Let $f(x), g(x) \in R[x]$, and assume $\deg f(x) = n \geq 0$, $\deg g(x) \leq n$.

1. If $r_1, \ldots, r_k \in R$ are distinct roots of $f(x)$, then
$$f(x) = (x - r_1)(x - r_2)\cdots(x - r_k)g(x).$$
2. The function $f(x)$ has at most n distinct roots in R.
3. If there are $n+1$ distinct elements $r_1, \ldots, r_n, r_{n+1} \in R$ such that
$$f(r_i) = g(r_i), \quad i = 1, \ldots, n, n+1,$$
then in $R[x]$, $f(x) = g(x)$.

Proof (1). For $k=1$, this is the result from the previous proposition. Let $f(x)=(x-r_1)q(x)$; for $j\neq 1$, we have

$$(r_j-r_1)q(r_j)=f(r_j)=0,$$

but $r_j-r_1\neq 0$, so

$$q(r_j)=0,\quad j=2,\dots,k.$$

By induction, $q(x)=(x-r_2)\cdots(x-r_k)g(x)$; hence

$$f(x)=(x-r_1)(x-r_2)\cdots(x-r_k)g(x).$$

(2). If $f(x)$ has $n+1$ distinct roots $r_1,\dots,r_n,r_{n+1}$ in R, by the previous result, we have

$$f(x)=(x-r_1)\cdots(x-r_n)(x-r_{n+1})g(x).$$

Then $\deg f(x)\geq n+1$.

(3). Let $h(x)=f(x)-g(x)\in R[x]$. Then $\deg h(x)\leq n$, and by the condition

$$h(r_j)=0,\quad j=1,\dots,n+1,$$

this implies $h(x)=0$. Therefore, $f(x)=g(x)$.

3.9.2 域上的多项式

Theorem 3.31 (域上的多项式的带余除法与性质)

1.设F为域，$F[x]$中任一$f(x),g(x)\neq 0$必定存在唯一的$q(x),r(x)$使得$f(x)=q(x)g(x)+r(x)$
其中$\deg r(x)<\deg g(x)$
2.$F[x]$为欧几里得环其中$\delta:F[x]\to\mathbb{N}\cup\{0\}\quad f(x)\to 2^{\deg f(x)}$
3.$F[x]$进而为PID为UFD

Proposition 3.36

1.$f_1(x)\equiv f_2(x)(\mathrm{mod}\,g(x))\Longleftrightarrow g(x)\mid f_1-f_2$
2.$f(x)\in F(x)$，$c\in F$则$f(x)\equiv f(c)(\mathrm{mod}\,(x-c))$
3.在$F[x]$上考虑有：若$c_1\sim c_k$是$f(x)$互不相等的根，则$(x-c_1)\cdots(x-c_k)\mid f(x)$从而$k\leqslant\deg f(x)$
4.设R为交换幺环，且$R\subseteq S$其中S为无零因子交换环，则$f(x)$在S中的不同根的个数不超过$\deg f(x)$
其注意上述无零因子交换环无法去掉例如：$x^2-1\in\mathbb{Z}_8[x]$取$S=R=\mathbb{Z}_8[x]$有根$\bar{1}\bar{3}\bar{5}\bar{7}$
例如可换也无法去掉例如四元数体x^2+1
5.那么作为4.的推论取$R=S$为整环，则有$f(x)$在R上的根的个数不超过$\deg f(x)$

Proof 2.由带余除法$f(x)=q(x)(x-c)+r$
考察$F\to F$的嵌入映射从而对于$c\in F$诱导出$F[x]\to F$的同态φ且$\varphi(x)=c$
从而$\varphi(f(x))=f(c)$从而用φ作用得到$f(c)=q(c)(c-c)+r\Longrightarrow f(c)=r$
从而由1.即可

3.一反面：$x-c_1$的因子只可能为零次或者一次的，则$x-c_1=g(x)h(x)$则$g(x),h(x)$次数要么零要么1
则要么相伴与$x-c_1$要么为单位
此时由带余除法$f(x)=(x-c_1)q(x)+r\Longrightarrow$带入$c_1$得到$x-c_1\mid f(x)\Longrightarrow f(x)=q_1(x)(x-c_1)$
同理得到$f(x)=q_2(x)(x-c_2)\Longrightarrow q_1(x)(x-c_1)=q_2(x)(x-c_2)$
$\Longrightarrow x-c_1\mid q_2(x)(x-c_2)$又互不相伴且$F[x]$为$UFD$则$x-c_1\mid q_2(x)$

同理类似下去得到 $(x-c_1)\cdots(x-c_k)\,|f(x)$ 从而 $k\leqslant \deg f(x)$

4.设 F 为 S 的分式域则 $f(x)\in R[x]\subseteq F[x]$ 则根据3.知道 $f(x)$ 在 F 中不同根的个数不超过 $\deg f(x)$
那么在 S 中更不超过了

Theorem 3.32

设 R 为一整环，$R^*=R-\{0\}$ 构成了交换幺半群，则 R^* 的任一有限子群是循环群

Proof 1.设 G 为 R^* 的一个有限子群，G 为 $Abel$ 群，对每个正整数 m 根据命题知道 x^m-1 在 R 上最多有 m 个根
由群论习题知道 G 为循环群

2.设 G 为 R^* 的一个有限子群，G 为 $Abel$ 群，取 g 为 G 中阶最大的元素设 $o(g)=m$
$\langle g\rangle=\left\{1,g\cdots g^{n-1}\right\}\subseteq G$ 其次 $\forall h\in G$ 设 $o(h)=m_1$
$WTS:h$ 为 x^m-1 的根而我们知道 x^m-1 在 R 上最多有 m 个根，而 $\left\{1,g\cdots g^{n-1}\right\}$ 已经是 m 个根了
则 $G\subseteq\langle g\rangle$ 从而完成证明
$h^m=e\Longleftrightarrow m_1\mid m$
反证 $m_1\nmid m$ 则必有素数 p 使得 $m_1=p^sl$ 且 $m=p^rk$ 且 $(p,l)=(p,k)=1\Longrightarrow(p,lk)=1$
且有 $s>r$ 或者 $l>k$ 严格成立
若 $s>r$ 则 $o\left(h^l\right)=p^s$ 且 $o\left(g^{p^r}\right)=k$ 因为可换与互素 $\Longrightarrow o\left(h^lg^{p^r}\right)=p^sk>m$
这与 g 的取法矛盾
若 $l>k$ 则 $o\left(h^{p^s}\right)=l$ 且 $o\left(g^k\right)=p^r$ 则 $o\left(g^kh^{p^s}\right)=p^rl>m$
同样与 g 的取法矛盾
故证毕

Proposition 3.37

设 F 为数域，$f(x)\in F[x]$ 为不可约多项式，则 $\langle f(x)\rangle$ 为极大理想，因此 $F[x]/\langle f(x)\rangle$

Theorem 3.33 (Newton-Lagrange Interpolation Theorem)

Let F be a field, let $a_1,\ldots,a_k\in F$ be pairwise distinct, and set $t(x)=\prod_{i=1}^k(x-a_i)$. Then for any $b_1,\ldots,b_k\in F$ there exists a unique polynomial $h(x)\in F[x]$ of degree $<k$ such that:

(1) $h(a_i)=b_i, i=1,\ldots,k$.

(2) If $f(x)\in F[x]$ satisfies $f(a_i)=b_i, i=1,\ldots,k$, then there exists a unique $g(x)\in F[x]$ such that $f(x)=h(x)+g(x)t(x)$.

Proof For $i\neq j$, we have $(x-a_i)-(x-a_j)=a_j-a_i\neq 0$; hence

$$1=(a_j-a_i)^{-1}(a_j-a_i)=(a_j-a_i)^{-1}\big((x-a_i)-(x-a_j)\big)\in F[x](x-a_i)+F[x](x-a_j).$$

Thus $F[x](x-a_i)+F[x](x-a_j)=F[x]$; i.e., the ideals $F[x](x-a_i)$ and $F[x](x-a_j)$ are coprime.

By the definition of $t(x)$, the ideal it generates satisfies $F[x]t(x)\subseteq F[x](x-a_i)$ for $i=1,\ldots,k$; hence $F[x]t(x)\subseteq\bigcap_{i=1}^k F[x](x-a_i)$. Conversely, suppose $f(x)\in\bigcap_{i=1}^k F[x](x-a_i)$. Then for each $1\leq i\leq k$, we have $f(x)\in F[x](x-a_i)$, so we may write $f(x)=h_i(x)(x-a_i)$, whence $f(a_i)=0$. By Corollary 3.4.6(1), there exists $g(x)\in F[x]$ such that $f(x)=g(x)t(x)$. Therefore $f(x)\in F[x]t(x)$. Combining the inclusions we obtain

$$F[x]t(x)=\bigcap_{i=1}^k F[x](x-a_i).$$

By the Chinese Remainder Theorem we obtain a ring isomorphism:

$$F[x]/F[x]t(x)\xrightarrow{\cong}F[x]/F[x](x-a_1)\oplus\cdots\oplus F[x]/F[x](x-a_k),$$

$$f(x)+F[x]t(x)\longmapsto \big(f(x)+F[x](x-a_1),\dots,f(x)+F[x](x-a_k)\big).$$

So there exists a $g(x)\in F[x]$,such that $g(x)+F[x](x-a_i)=b_i+F[x](x-a_i)$. Hence $g(a_i)=b_i$ for $i=1,\dots,k$.Then we use division , $g(x)=q(x)t(x)+r(x)$ and $deg(r(x))<deg(t(x)=k), r(a_i)=b_i$.

Now we have shown the existance of such a polynomial $h(x)$. To show uniqueness, suppose there are two such polynomials $h_1(x)$ and $h_2(x)$ of degree $<k$ satisfying $h_1(a_i)=b_i$ and $h_2(a_i)=b_i$ for $i=1,\dots,k$. Then the polynomial $h_1(x)-h_2(x)$ has degree $<k$ and has k distinct roots $a_1,\dots,a_k$. By Corollary ,this implies that $h_1(x)-h_2(x)=0$, hence $h_1(x)=h_2(x)$. This completes the proof.

Note

For $(b_1,\dots,b_k)\in \mathbb{F}\oplus\cdots\oplus\mathbb{F}$, how can we concretely find a polynomial $h(x)$ satisfying conditions (1) and (2) of the interpolation theorem? From the Chinese Remainder Theorem, the key is to find polynomials $\ell_i(x)$ such that

$$\ell_i(x)\equiv\begin{cases}1 \pmod{x-a_j}, & \text{if } i=j,\\ 0 \pmod{x-a_j}, & \text{if } i\neq j.\end{cases}$$

Let $t_i(x)=t(x)/(x-a_i)$, where $t(x)$ is as in the theorem, then $t_i(a_i)\neq 0$. The following polynomials, called Lagrange polynomials, satisfy the above requirements:

$$\ell_i(x)=\frac{t(x)}{t_i(a_i)}=\frac{\prod_{j\neq i}(x-a_j)}{\prod_{j\neq i}(a_i-a_j)},\quad i=1,\dots,k;$$

then

$$h(x)=\sum_{i=1}^{k}b_i\ell_i(x).$$

3.9.3 唯一分解整环与域上的多项式

Definition 3.34

1.设R为UFD则$f(x)=\sum_{k=0}^{n}a_kx^k\in R[x]$，称$c(f)=(a_0,a_1\cdots a_n)$为$f$的容度

2.设$0\neq f(x)\in R[x]$且$c(f)\sim 1$则称f为本原多项式

Proposition 3.38

设R为UFD且记S为$R[x]$中所有本原多项式的集合

1.$0\neq f(x)\in R[x]$则有$d\in R^*, f_1(x)\in S$,使得$f(x)=df_1(x)$，且该分解在相伴意义下唯一

2.若$f(x)$为不可约元且$degf>0$则$f(x)$为本原多项式,但反之不对例如x^2-1

3.两个本原多项式乘积仍然为本原多项式

Proof 1.$f(x)=\sum_{k=0}^{n}a_kx^k=c(f)\sum_{k=0}^{n}a_k'x^k=df_1(x)$此时$c(f)=d$断言不会等于0因为首项系数一定不会为0

这就说明了分解的存在性

其次，若$f(x)=d_1f_1(x)=d_2f_2(x)$其中$d_1,d_2\in R^*, f_1(x), f_2(x)\in S$

则$c(f)=d_1c(f_1)=d_2c(f_2)\Longrightarrow d_1\sim d_2$故$d_1=ud_2\Longrightarrow uf_1(x)=f_2(x)\Longrightarrow f_1\sim f_2$

2.设$d=c(f)$，则$f(x)=df_1(x)$且$d\in R^*, f_1(x)\in S$此时d为f的真因子，由f不可约则$d\sim 1$故$f\in S$

3.仿照高等代数$Gauss$引理证明

Proposition 3.39

设R为UFD且记S为$R[x]$中所有本原多项式的集合，记F为R的分式域，则$R[x]\subseteq F[x]$

记$R[x]$中相伴为$\underset{R}{\sim}$,记$F[x]$的相伴为$\underset{F}{\sim}$,显然相伴$\underset{R}{\sim}$一定为相伴$\underset{F}{\sim}$

1.$0\neq f(x)\in F[x]$，必定存在$g(x)$为$R[x]$的本原多项式使得$f(x)\underset{F}{\sim}g(x)$且$g(x)$在相伴$\underset{R}{\sim}$下唯一

且若有两个非零多项式$h(x),k(x)\in F[x]$使得$h(x)\underset{F}{\sim}k(x)\Longrightarrow k(x)\underset{R}{\sim}h(x)$

2.设$f_1(x),f_2(x)\in F[x]$且$g(x),g_1(x),g_2(x)$为$R[x]$的本原多项式

若$f_1\underset{F}{\sim}g_1$，$f_2\underset{F}{\sim}g_2$，$f_1f_2\underset{F}{\sim}g\Longrightarrow g_1g_2\underset{R}{\sim}g$

3.$f(x)\in R[x]$且$deg f(x)>1$，$f(x)$在$R[x]$中不可分解为两个次数较低的多项式乘积

则$f(x)$在$F[x]$也不可分解为两个次数较低的多项式乘积

Proof 1.$f(x)=\sum_{k=0}^{n}\frac{a_k}{b_k}x^k=\frac{1}{b_1\times\cdots\times b_n}\sum_{k=0}^{n}a_1b_2\cdots b_nx+\cdots=\underbrace{\frac{o(*)}{b_1\times\cdots\times b_n}}_{\neq 0且\in F即F中的平凡因子}\underbrace{\sum_{k=0}^{n}\underbrace{h_kx^k}_{\in S}}_{称为g(x)}$

故$f(x)\underset{F}{\sim}g(x)$,若有$f(x)\underset{F}{\sim}g_1(x)$，此时$g(x)\underset{F}{\sim}g_1(x)$即存在$\frac{v}{u}\in F^*$使得$g(x)=\frac{v}{u}g_1(x)$

$\Longrightarrow ug(x)=vg_1(x)$左右两端就是$R[x]$中的，再由上个命题的1得到$\underset{R}{\sim}$相伴

2.此时相伴关系为同余关系则$g_1g_2\underset{F}{\sim}g$,而$g_1$本原$g_2$本原由上个命题知道$g_1g_2$本原，且$g$本原

由本命题1.知道$\underset{R}{\sim}$相伴

3.反证法若$f(x)$在$F[x]$可分解为两个次数较低的多项式乘积，$f(x)=f_1f_2$其中$f_1\in F[x],f_2\in F[x]$

由本命题1.知道$f_1\underset{F}{\sim}g_1$且$f_2\underset{F}{\sim}g_2$且$f(x)\underset{F}{\sim}g(x)$其中$g_1,g_2,g$为$R[x]$中的本原多项式

且相伴不改变次数故g_1g_2次数与f_1f_2一样都是比f低的

由相伴关系为同余关系$\Longrightarrow g(x)\underset{F}{\sim}g_1g_2\Longrightarrow g(x)\underset{R}{\sim}g_1g_2\Longrightarrow g(x)=ug_1(x)g_2(x)\quad u\in R^*$

由上个命题1.知道$f(x)=dg(x)$其中$d\in R^*,g(x)$为$R[x]$中的本原多项式

注意上一行从$f(x)\underset{F}{\sim}g(x)$是只看到$F$相伴为什么$R$相伴还是$g(x)$因为上个命题的1.说明分解在$R$相伴下唯一

故$f(x)=dg(x)=(dug_1(x))g_2(x)$故$f$在$R[x]$上分解成了两个次数较低的多项式的乘积

Theorem 3.34

设R为UFD则$R[x]$也是UFD，S为$R[x]$上的本原多项式集合

Proof 1.有限分解条件：若$f(x)$次数等于零则$f(x)\in R$则可以有限分解故不妨设$f(x)$次数大于零

由命题$f(x)=dg(x)$其中$d\in R^*,g(x)\in S$

不妨假设$d\notin U$否则放着与后面$g(x)$的因子配对，则$d\in R^*-U$

$\Longrightarrow d=p_1\cdots p_t$其中$p_i$为$R$中不可约元自然也为$R[x]$中不可约元

记F为R的分式域，在$F[x]$中$g(x)$可分解为$g(x)=g_1(x)\cdots g_r(x)$其中$g_i(x)$是$F[x]$中不可约元

由命题知$g_i(x)\underset{F}{\sim}p_i(x)$其中$p_i(x)\in S$，而$g_i(x)$在$F[x]$中不可约自然相伴的$p_i(x)$在$F[x]$中不可约

$\Longrightarrow g(x)\underset{F}{\sim}p_1(x)\cdots p_r(x)\Longrightarrow g(x)\underset{R}{\sim}p_1(x)\cdots p_r(x)\Longrightarrow g(x)=up_1(x)\cdots p_r(x)$其中$u\in R^*$

且$p_i(x)\in S$且$p_i(x)$在$F[x]$中不可约$\Longrightarrow p_i(x)$在$R[x]$中不可约(这里推出的条件要注意例如$3x^2+6$在$\mathbb{Z}[x]$)

于是$f(x)=p_1\cdots p_t(up_1(x))\cdots p_r(x)$

2.唯一分解条件：若有$f(x)=q_1\cdots q_{t'}q_1(x)\cdots q_s(x)=p_1\cdots p_tp_1(x)\cdots p_r(x)$

$q_i(x)$为$R[x]$上不可约元，且$q_i(x)$次数大于0由引理知道$q_i(x)\in S$(该性质对于$p_i(x)$一样)

根据命题我们就知$q_1\cdots q_{t'}\underset{R}{\sim}p_1\cdots p_t$且$p_1(x)\cdots p_r(x)\underset{R}{\sim}q_1(x)\cdots q_s(x)$

故不妨设$p_1\cdots p_t=q_1\cdots q_{t'}$在$R$为$UFD$上有$t=t'$且在相差一个置换下$R$相伴

同理不妨设$p_1(x)\cdots p_r(x)=q_1(x)\cdots q_s(x)$

由$q_i(x)$为$R[x]$上不可约元，$\deg q_i(x)>0$，$q_i(x)\in S$故命题知道$q_i(x)$在$R[x]$上不可分解为两个次数较低的多项式的乘积

则$q_i(x)$在$F[x]$上不可分解为两个次数较低的多项式乘积$\Longrightarrow q_i(x)$在$F[x]$上不可约

$p_1(x)\cdots p_r(x)=q_1(x)\cdots q_s(x)$ 在$F[x]$上就是两种分解故由$F[x]$为UFD知道$r=s$且在置换下$p_i(x)\underset{F}{\sim}q_i(x)$
又他们本原故$p_i(x)\underset{R}{\sim}q_i(x)$

3.10 常见的环的性质讨论

Theorem 3.35

$\mathbb{Z}_{pq} \simeq \mathbb{Z}_p \oplus \mathbb{Z}_q \Longleftrightarrow p$和$q$互素

Proof 若p,q互素我们下面就来证明：$\mathbb{Z}_{pq} \cong \mathbb{Z}_p \oplus \mathbb{Z}_q$

事实上此时$\mathbb{Z}_{pq} \cong \mathbb{Z}_p \oplus \mathbb{Z}_q$都是环实际上为环同构

构造映射$\varphi : \mathbb{Z}_{pq} \to \mathbb{Z}_p \oplus \mathbb{Z}_q \quad \bar{a} \mapsto (\widetilde{x}, \widetilde{y})$ 其中$\widetilde{x} \equiv a \bmod (p)$ 且$\widetilde{y} \equiv a \bmod (q)$

首先我们来说明映射的合理性对于$a_1 = k_1 pq + a$与$a_2 = k_2 pq + a$于是$\widetilde{x_1} = a \bmod (p) = \widetilde{x_2}$

注意到：$\left|\mathbb{Z}_{pq}\right| = \left|\mathbb{Z}_p \oplus \mathbb{Z}_q\right| = pq$故我们只需要说明$\varphi$为单射就可以顺带带出满射从而是双射

$\overline{a_1} = \overline{a_2} \Longleftrightarrow pq \mid a_1 - a_2 \Longrightarrow p \mid a_1 - a_2$与$q \mid a_1 - a_2 \Longleftrightarrow \widetilde{x_1} = \widetilde{x_2}$与$\widetilde{y_1} = \widetilde{y_2}$

且注意到p,q互素故上行的$\Longrightarrow$可以进一步改为$\Longleftrightarrow$

故$\overline{a_1} = \overline{a_2} \Longleftrightarrow \widetilde{x_1} = \widetilde{x_2}$与$\widetilde{y_1} = \widetilde{y_2}$至此说明了单射从而为双射

下面说明同态：$\varphi(\overline{a_1 a_2}) = \varphi(\overline{a_1 a_2}) = (\overline{x_1 x_2}, \overline{y_1 y_2}) = (\overline{x_1}, \overline{y_1})(\overline{x_2}, \overline{y_2}) = \varphi(\overline{a_1})\varphi(\overline{a_2})$

同理$\varphi(\overline{a_1} + \overline{a_2}) = \varphi(\overline{a_1}) + \varphi(\overline{a_2})$故为环同构

另一方面：若$\mathbb{Z}_{pq} \simeq \mathbb{Z}_p \oplus \mathbb{Z}_q$我们就知道了$\mathbb{Z}_p \oplus \mathbb{Z}_q$是一个循环群我们去证明若$p,q$不互素，则$\mathbb{Z}_p \oplus \mathbb{Z}_q$不是循环群

证它的逆否命题：设$(m_1, m_2) \neq 1$，去证群$(\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}, +)$不是循环群.

只要证$(\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}, +)$的任一元素$\left(\tilde{a}_1, \tilde{\tilde{a}}_2\right)$的阶都小于群$(\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}, +)$的阶$m_1 m_2$就可以了.

设$(m_1, m_2) = d > 1$，则$m_1 = k_1 d, 1 \leqslant k_1 < m_1; m_2 = k_2 d, 1 \leqslant k_2 < m_2$.由于$(\mathbb{Z}_{m_1}, +)$是$m_1$阶循环群，因此$\tilde{1}$的阶为$m_1$.

同理，$\tilde{\tilde{1}}$的阶为m_2.于是有

$$
\begin{aligned}
k_1 d k_2 \left(\tilde{a}_1, \tilde{\tilde{a}}_2\right) &= \left(k_1 d k_2 \tilde{a}_1, k_1 d k_2 \tilde{\tilde{a}}_2\right) = \left(k_2 m_1 \tilde{a}_1, k_1 m_2 \tilde{\tilde{a}}_2\right) \\
&= \left(k_2 m_1 \tilde{1} \tilde{a}_1, k_1 m_2 \tilde{\tilde{1}} \tilde{\tilde{a}}_2\right) = \left(k_2 \tilde{0} \tilde{a}_1, k_2 \tilde{\tilde{0}} \tilde{\tilde{a}}_2\right) = (\tilde{0}, \tilde{0}).
\end{aligned}
$$

从而$\left(\tilde{a}_1, \tilde{\tilde{a}}_2\right)$的阶$s \mid k_1 d k_2$.由于$k_1 d k_2 = m_1 k_2 < m_1 m_2$，因此$s < m_1 m_2$.于是$(\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}, +)$不是循环群.

Lemma 3.13

1.一个至少含有两个元素且无零因子的有限环是一个除环

2.有限整环为域

3.有限无零因子环为除环

4.$\mathbb{Z}_p$为无零因子环$\Longleftrightarrow p$为一个素数

5.$\mathbb{Z}_p$为域$\Longleftrightarrow p$为一个素数

Proof 1.设$(R, +, \cdot)$是一个至少含有两个元素且无零因子的有限环

要证它是一个除环，只需证$(R^*, \cdot)$是一个群.因为R中至少含有两个元素，所以，R^*是一个非空集合.

又因为R中无零因子，所以，$\forall a, b \in R^*$，即$a \neq 0, b \neq 0$，得$ab \neq 0$，也就是说，R^*关于乘法运算是封闭的.

从而得到$(R^*, \cdot)$是一个满足消去律的有限半群，得(R^*)是一个群。所以，R是一个除环

2.3.利用有限半群满足消去律为群

4.$\Longrightarrow$：显然若n不为素数那么就有$n = ab$；所以$\bar{a}\bar{b} = \bar{0}$

$\Longleftarrow$：若$\bar{a}\bar{b} = \bar{0}$且$\bar{a} \neq \bar{0}$且$\bar{b} \neq \bar{0}$那么有$p \mid ab$又因为p为素数那么$p \mid a$或者$p \mid b$此时但a与b小于p矛盾

5.利用3.4.就知道$\mathbb{Z}_p$为整环，除环，域

Proposition 3.40 (整数环的讨论)

$(\mathbb{Z}, +, \cdot)$：

1.无零因子环　交换性　具有乘法幺元

2.整环
3.非除环　非域

Proposition 3.41 (模 n 整数环的讨论)

$(\mathbb{Z}_n,+,\cdot)$ (n为一个合数)：$\begin{cases} \text{交换性} \\ \text{具有乘法幺元} \end{cases}$

1.交换性　具有乘法幺元
2.非整环　是一个非无零因子环　不是域

Proposition 3.42 (模 p 整数环的讨论)

$(\mathbb{Z}_p,+,\cdot)$ (p为一个素数)
1.交换性　具有乘法幺元　无零因子环
2.整环　除环　域
3.$\mathbb{Z}_p$上的自同态只有零同态和id

Proof 3.若$p=2$显然下设p为一个奇素数　设$f:\mathbb{Z}_p\to\mathbb{Z}_p$，则$f(0)=0$，设$f(1)=k\in\{0,1,\cdots,p-1\}$
则$f(2)=\overline{2k}, f(2)=f(1)f(2)=\overline{2k^2}$，即$2k^2\equiv 2k(\mathrm{mod}p)\Longrightarrow p\mid k^2-k\Longrightarrow$则可知$k=0$或1
故f为零同态或恒等同态，即证

第 4 章 模论

4.1 模的基础概念

Definition 4.1

设R为么环，M是一个交换群（其运算用加法表示），如果有一个从$R\times M$到M的映射$(a,x)\mapsto ax$满足条件

（1）对任何$a,b\in R$及$x\in M,(a+b)x=ax+bx$

（2）对任何$a\in R$及$x,y\in M,a(x+y)=ax+ay$

（3）对任何$x\in M,1x=x$，其中1为R的么元

（4）对任何$a,b\in R$及$x\in M,a(bx)=(ab)x$

则称M为一个左R模。

Remark 一般的在本章中若无特殊指出 若R为交换环，则我们直接定义右R模：$xa:=ax$ (其中$x\in M,a\in R$)

若R不是交换环，则说M是一个R模意思是左R模

Note 1.任何域F上的线性空间V一定是F作为么环上的左模

事实上，线性空间定义中的前四个条件恰好说明V本身具有交换群的结构，而后面的四个条件正好是左模定义中的条件

2.设G为一个交换群，定义$\mathbb{Z}\times G$到G的映射：$(m,x)\mapsto mx$

则容易验证上述映射满足条件这样任何一个交换群就可以看成整数环上的左模

这一观点将导出有限生成交换群的分类

3.任何一个环R都可以看成一个R—模

事实上，如果我们只考虑加法，则$M=\{R;+\}$成为一个交换群，而通过环的乘法就可以将交换群M看成环R上的模

4.在1.中说明任何域F上的线性空间V都可以看成F上的模

现在我们给定V上的一个线性变换$\mathcal{A}$，则可以将V看成F上的一元多项式环$F[\lambda]$上的左模

事实上，对任何多项式$f(\lambda)$以及V中的一个向量v，定义$f(\lambda)v=f(\mathcal{A})(v)$则容易验证模的条件全部是成立的

因此V成为$F[\lambda]$上的一个模．这一观点将导出一般域上线性空间上的线性变换的标准形理论．

Proposition 4.1

1.设M为R模，此时$\forall a\in R$有$a0_M=0_M$

2.设M为R模，此时$\forall x\in M$有$0_RM=0_M$

3.有$a(-x)=(-a)x=-(ax)$

4. $\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{m}x_j\right)=\sum_{i=1}^{n}\sum_{j=1}^{m}a_ix_j$

Definition 4.2 (子模)

1.设R为么环，R上的模M的一个非空子集N称为M的子模，如果N在M的加法运算和R与M的纯量乘法运算下成为一个R模

Proposition 4.2

N为M的子模的充分必要条件是：（1）N是加法群M的子群；（2）对任何$a\in R,x\in N$，有$ax\in N$

Proof 一方面若N为M的子模，则已经蕴含着N是一个交换群且N是M的子集，故N是M的子群，且由模的定义

纯量乘法：$R\times N\to N$故$a\in R,x\in N$，有$ax\in N$

另一方面：若N是加法群M的子群；对任何$a\in R,x\in N$，有$ax\in N$

此时$\forall x,y\in N,\forall a,b\in R$则

$a(x+y)=ax+ay$其中能写出等号是将x,y看成M上的元素，其次利用(2)ax,ay就属于N，又N为M子群故$ax+ay\in N$

$(a+b)x=ax+bx$同理

$1_R x=x$同理

$a(bx)=(ba)x$同理

Note（1）域F上线性空间V的一个非空子集W是子模当且仅当W是V的线性子空间

（2）交换群G的非空子集H是G作为$\mathbb{Z}$一模的子模当且仅当H是G的子群

（3）将环R看成R一模，则R的非空子集R_1是子模当且仅当R_1是R的左理想

（4）如果$\mathcal{A}$是域F上线性空间V上的线性变换，且将V看成$F[\lambda]$一模，则V的非空子集W是子模，当且仅当W是$\mathcal{A}$的不变子空间

Proposition 4.3 (子模的和与交)

1.给定R一模M的两个子模M_1,M_2，容易看出交集$M_1\cap M_2$也是M的子模

2.如果定义$M_1+M_2=\{x_1+x_2\mid x_1\in M_1,x_2\in M_2\}$则$M_1+M_2$也是$M$的子模，称为子模$M_1$与$M_2$的和

值得注意的是，任意多个（可以无穷）子模的交一定是子模，而关于子模的和的结论只能推广到任何有限多个子模的和的情形

Definition 4.3

现设$S\subset M$为一个非空子集，则M中所有包含S的子模（例如，M本身就是一个）的交还是M的一个子模，称为由S生成的子模，

一般地，如果$[S]=M$，则称S为M的一个生成组

如果模M中存在一个元素y使得$[y]=M$，则称M为循环模

模M称为有限生成的，如果存在M中的一个有限子集S_1，使得$[S_1]=M$

显然，一个交换群G作为$\mathbb{Z}$一模是循环模当且仅当G是循环群；而G作为$\mathbb{Z}$一模是有限生成模当且仅当G是有限生成群

Proposition 4.4

试证明$[S]=\left\{\sum_{i=1}^{m}a_i y_i\mid m\in\mathbb{N},a_i\in R,y_i\in S\right\}$．特别地$S=\{x_1\cdots x_k\}$有$[S]=Rx_1+\cdots+Rx_k$

Definition 4.4 (模的内直和)

设M的子模$M_1,M_2,\cdots,M_s$满足$M=M_1+M_2+\cdots+M_s$

任意M中元素u表示成$u=a_1+a_2+\cdots+a_s,a_i\in M_i$的方法是唯一的

则称M为$M_1,M_2,\cdots,M_s$的（内）直和，记为$M=M_1\oplus M_2\oplus\cdots\oplus M_s$

Theorem 4.1

设$M_i,1\leqslant i\leqslant s$为模$M$的子模，且$M=M_1+M_2+\cdots+M_s$，则下面三个条件等价

（1）$M=M_1\oplus M_2\oplus\cdots\oplus M_s$

（2）如果$a_i\in M_i,1\leqslant i\leqslant s$使得$a_1+a_2+\cdots+a_s=0$，则$a_1=a_2=\cdots=a_s=0$，简言之，0的表示法唯一.

（3）对任何i，我们有$M_i\cap\left(\sum_{j\neq i}M_j\right)=\{0\}$.

Definition 4.5 (模的外直和)

设$N_1,N_2,\cdots,N_n$为R一模，在直积集合$N=N_1\times N_2\times\cdots\times N_n$上定义加法以及$R$与$N$的纯量乘法如下

$(x_1,\cdots,x_n)+(y_1,\cdots,y_n)=(x_1+y_1,\cdots,x_n+y_n)$

$a(x_1,\cdots,x_n)=(ax_1,\cdots,ax_n),\quad x_i,y_i\in N_i,\quad 1\leqslant i\leqslant n,\quad a\in R$

则N成为一个R—模，称为$N_1, N_2, \cdots, N_n$的外直和，记为$N = N_1 \otimes \cdots \otimes N_n$

Theorem 4.2

设$N = N_1 \otimes N_2 \otimes \cdots \otimes N_n$为$R$模$N_1, N_2, \cdots, N_n$的外直和

令$N_i' = \{(0, 0, \cdots, 0, x_i, 0, \cdots, 0) \in N \mid x_i \in N_i\}$则$N_i'$为$N$的子模，而且$N$是$N_1', N_2', \cdots, N_n'$的内直和

Proof 显然，对任何$\alpha_1, \alpha_2 \in N_i'$，有$\alpha_1 - \alpha_2 \in N_i'$，因此$N_i'$是$N$的加法子群

此外，对任何$a \in R, x_i \in N_i$，有$a(0, \cdots, 0, x_i, 0, \cdots, 0) = (0, \cdots, 0, ax_i, 0, \cdots, 0) \in N_i'$，因此$N_i'$是$N$的子模

又对任何$x_i \in N_i, 1 \leqslant i \leqslant n$，$(x_1, \cdots, x_n) = (x_1, 0, \cdots, 0) + \cdots + (0, \cdots, 0, x_n)$因此$N = N_1' + N_2' + \cdots + N_n'$

此外，条件显然成立，因此$N = N_1' \oplus N_2' \oplus \cdots \oplus N_n'$.

Definition 4.6 (商模)

设N为R—模M的子模，则作为加法群N为M的正规子群，因此商群M/N是交换群

现在定义R与M/N的纯量乘法如下

$a(x + N) = ax + N, \quad a \in R, x \in M$则$M/N$在上述两种运算下成为一个$R$—模，称为$M$对$N$的商模

Proof 我们先验证纯量乘法的定义是合理的．事实上，如果$x_1, x_2 \in M$，使得$x_1 + N = x_2 + N$，则$x_1 - x_2 \in N$

因N为子模，故$\forall a \in R, a(x_1 - x_2) = ax_1 - ax_2 \in N$，从而$ax_1 + N = ax_2 + N$．这证明了纯量乘法的合理性

容易验证定义中的条件（1）—（4）成立，因此M/N是R—模。

Definition 4.7 (模同态与模同构)

设M_1, M_2为两个R—模，一个由M_1到M_2的映射ϕ称为模同态，如果ϕ满足条件

（1）对任何$x, y \in M_1$，有$\phi(x + y) = \phi(x) + \phi(y)$

（2）对任何$a \in R$及$x \in M_1$有$\phi(ax) = a\phi(x)$

条件（1）说明ϕ是加法群M_1到M_2的群同态．如果一个模同态ϕ是满射，则称ϕ为满同态；如果模同态ϕ为双射，则称ϕ为模同构

显然，两个模同态的复合映射是模同态，一个模同构的逆映射也是模同构

如果模M_1与M_2之间存在一个同构，则称M_1与M_2是同构的，记为$M_1 \simeq M_2$．显然，同构关系是R—模的集合中的一种等价关系．

Proposition 4.5

设R为幺环，M_1，M_2都为R模，$\varphi : M_1 \to M_2$为模同态

1.Kerφ为M_1子模

2.Imφ为M_2子模

Theorem 4.3 (模同态基本定理)

设R为幺环，M_1，M_2都为R模，且φ为$M_1 \to M_2$的满模同态

1.$M_1/\mathrm{Ker}\varphi \cong M_2$

2.φ建立了M_1中包含 Kerφ的子模与M_2中子模的一一对应

且若H为子模且 Ker$\varphi \subseteq H$则$M_1/H \cong M_2/\varphi(H)$

3.若H为M_1的子模，则$H + \mathrm{Ker}\varphi$是$\varphi(H)$的完全原像且$\varphi(H) = \varphi(H + \mathrm{Ker}\varphi)$

4.$H/H \cap \mathrm{Ker}\varphi \cong \varphi(H) = \varphi(H + \mathrm{Ker}\varphi)$

Note [由一个交换群确定一个模]

对于任意的交换群G，定义由该群结构唯一确定的环.

设G为一加法交换群，记 End(G)为G上所有自同态的集合，并在其上定义$\forall x \in G$

$(f + g)(x) := f(x) + g(x) \quad (fg)(x) := f(g(x))$

则 $\mathrm{End}(G)$ 为一个幺环.

1.加法幺元为G上的零同态，f的加法逆元为 $-f$其中 $(-f)(x)=-f(x)$

2.乘法幺元为G上的id

此时我们可以将G看成 $\mathrm{End}(G)$ 上的模

Definition 4.8 (模的自同态环)

现在考虑已知一个幺环R，设M为R上的模，则考察所有模M上的自同态集合记为 $\mathrm{End}_{\mathrm{R}}(G)$

1.由模同态定义知道 $\mathrm{End}_{\mathrm{R}}(G)\subseteq\mathrm{End}(G)$

2.其次 $\mathrm{End}_{\mathrm{R}}(G)$ 为 $\mathrm{End}(G)$ 的幺子环

$\forall f,g\in\mathrm{End}_{\mathrm{R}}(G)$ 与$\forall x,y\in G$与$\forall a\in R$此时

断言$f-g\in\mathrm{End}_{\mathrm{R}}(G)$

因为 $(f-g)(x+y)=f(x+y)-g(x+y)=f(x)-g(x)+f(y)-g(y)=f(x+y)-g(x+y)$

这实际上是有$f,g\in\mathrm{End}(G)$继承过来的

且另外，$(f-g)(ax)=f(ax)-g(ax)=af(x)-ag(x)=a(f-g)(x)$

断言$fg\in\mathrm{End}_R(G)$这是因为，$fg(x+y)=f(g(x+y))=f(g(x)+g(y))=f(g(x))+f(g(y))=fg(x)+fg(y)$

另外$fg(ax)=f(g(ax))=f(ag(x))=af(g(x))=a(fg)(x)$

故 $\mathrm{End}_{\mathrm{R}}(G)$ 为 $\mathrm{End}(G)$ 的幺子环

4.2 自由模与其线性代数

Definition 4.9 (模上线性无关)

设R为幺环，M为一个R模，若存在M中元素$u_1\cdots u_n$满足

$$\sum_{i=1}^{n} a_i u_i = 0 \Longleftrightarrow a_i = 0 a_i \in R$$

则称$u_1\cdots u_n$线性无关

Definition 4.10 (模上的基)

设R为幺环，M为一个R模，若存在M中元素$u_1\cdots u_n$满足

1.$u_1,\cdots u_n$生成M，有：$M = Ru_1 + Ru_2 + \cdots + Ru_n$亦即$M = \langle u_1\cdots u_n\rangle$

2.$u_1\cdots u_n$线性无关

则我们称$u_1\cdots u_n$$R$模$M$上的一组基

Corollary 4.1

此时我们类似于线性空间的知识能够知道模 M 的元素在选定基底下的表法唯一

Note 设R为幺环，定义集合$R^{(n)} = R\times R\cdots\times R = \{(a_1, a_2\cdots a_n)\ \ |a_i \in R\}$

定义：$(a_1, a_2\cdots a_n) + (b_1, b_2\cdots b_n) = (a_1 + b_1, a_2 + b_2\cdots a_n + b_n)$ 与$k \in R$且$k\ (a_1, a_2\cdots a_n) = (ka_1, ka_2\cdots ka_n)$

1.$R^{(n)}$是$Abel$群

2.$R^{(n)}$是一个左R模

3.$R^{(n)}$上有基$\{e_1\cdots e_n\}$其中$e_i = (0,\cdots 0, 1, 0\cdots 0)$

Definition 4.11 (自由模)

设幺环R，若幺环R上的模M与$R^{(n)}$同构，我们则称模M为秩为n的自由模

Theorem 4.4

设R为幺环，则M为秩为n的自由模 $\Longleftrightarrow$ M中存在$u_1\cdots u_n$作为M的一组基

Proof 一方面：若M为秩为n的自由模，则$M \cong R^{(n)}$设$R^{(n)}$到M的模同构为φ

则容易验证$\varphi\ (e_1)\cdots\varphi\ (e_n)$为$M$的一组基

另一方面：若M中有基$\{u_1\cdots u_n\}$，那么构造映射$\varphi : M \to R^{(n)}$ $\varphi\left(\sum_{i=1}^{n} a_i u_i\right) = \sum_{i=1}^{n} a_i e_i$

此时容易验证该映射是模同态 + 满射 + 单射

Theorem 4.5

设R为幺环，M是R模，$u_1\cdots u_n$为M中n个元素

则M是秩为n的自由模，且一组基为$u_1\cdots u_n$

$\Longleftrightarrow$ 对于任一R模N及任意n个$v_1\cdots v_n$为N中元素，存在唯一的M到N的模同态φ使得$\varphi\ (u_1) = v_i$

Proof 先证必要性：已知M是秩为n的自由模，且一组基为$u_1\cdots u_n$.此时对于任一R模N及任意n个$v_1\cdots v_n$为N中元素

先来说明唯一性，$\forall x \in M$不妨设$x = \sum_{i=1}^{n} a_i u_i$那么$\varphi\ (x) = \varphi\left(\sum_{i=1}^{n} a_i u_i\right) = \sum_{i=1}^{n} a_i v_i$

故若这样的φ同态是存在的则其一定为如上形式

下证存在性，构造φ：$M \to N$ $\sum_{i=1}^{n} a_i u_i \mapsto \sum_{i=1}^{n} a_i v_i$

1.φ的确为一映射，因为$\forall x \in M$则x在基$u_1\cdots u_n$下的系数是唯一的，则在φ下的像亦唯一

2.φ保持加法
3.φ保持乘法运算
4.φ把u_i映到v_i
这都是非常容易验证的

再来证明充分性：已知对于任一R模N及任意n个$v_1\cdots v_n$为N中元素，存在唯一的M到N的模同态φ使得$\varphi(u_1)=v_i$
根据上个定理知道，我们只需证明$u_1\cdots u_n$为M的一组基即可
1.说明$u_1\cdots u_n$生成M即可，令$M_1=\langle u_1\cdots u_n\rangle$，下说明$M_1=M$
根据题意存在唯一的模同态$\mathscr{A}$：$M\to M_1$且选取M_1当中的元素恰为$u_1\cdots u_n$
又设$inclusion$ $\mathscr{L}$为M_1到M中的嵌入映射
则$\mathscr{L}\mathscr{A}$为M到M的模同态且$\mathscr{L}\mathscr{A}(u_i)=u_i$
但我们知道M到M自然有恒等映射id，则根据题目条件就知道若取特殊的N恰为M本身就有
$\mathscr{L}\mathscr{A}=id\Longrightarrow\mathscr{L}$为满射故$M_1=M$
2.下说明$u_1\cdots u_n$线性无关
对于任一线性组合$\sum\limits_{i=1}^{n}a_iu_i=0$此时根据题干取特殊的$N$为$R^{(n)}$特殊的$v_i$就为$e_i$
ψ模同态：$M\to R^{(n)}$　$\psi(u_i)=e_i$
则$\sum\limits_{i=1}^{n}a_iu_i=0\Longrightarrow\psi\left(\sum\limits_{i=1}^{n}a_iu_i\right)=0\Longrightarrow\sum\limits_{i=1}^{n}a_ie_i=0\Longrightarrow a_i=0$证毕

Note 设交换幺环 R，且 M 为 R 上的 n 秩自由模，取定 M 上的一组基记为 $\{u_1\cdots u_n\}$，此时对于任意 M 中元素 x，x 可以被基底唯一表出并且可以形式记作 $x=(u_1\cdots u_n)(a_1\cdots a_n)^T$ 我们类似的将 $(a_1\cdots a_n)^T$ 称之为坐标向量，且坐标向量显然是唯一的。类似的我们也有两组基之间的过渡矩阵的说法，且关于行列式的计算可以平行的推广到这里来。

Theorem 4.6

设R是交换幺环，M是自由R模，$u_1,u_2,\cdots,u_n$与$v_1,v_2,\cdots,v_m$是M的两组基，则$m=n$

Proof 因为$u_1,u_2,\cdots,u_n$为基．作R上的$n\times m$矩阵$\boldsymbol{A}$满足$(v_1\cdots v_m)=(u_1\cdots u_n)A$
同理$(u_1\cdots u_n)=(v_1\cdots v_m)B$
$\Longrightarrow(u_1\cdots u_n)=(u_1\cdots u_n)AB\Longrightarrow AB=I_n$同理$BA=I_m$
假设$n<m$．作m阶方阵$\boldsymbol{A}_1$，满足$\operatorname{row}_i\boldsymbol{A}_1=\begin{cases}\operatorname{row}_i\boldsymbol{A}, & 1\leqslant i\leqslant n\\ 0, & n+1\leqslant i\leqslant m\end{cases}$　即$\boldsymbol{A}_1=\begin{pmatrix}\boldsymbol{A}\\ \boldsymbol{O}\end{pmatrix}$
再作m阶方阵$\boldsymbol{B}_1$满足$\operatorname{col}_i\boldsymbol{B}_1=\begin{cases}\operatorname{col}_i\boldsymbol{B}, & 1\leqslant i\leqslant n\\ 0, & n+1\leqslant i\leqslant m\end{cases}$　即有$\boldsymbol{B}_1=\begin{pmatrix}\boldsymbol{B} & \boldsymbol{O}\end{pmatrix}$
于是有$\boldsymbol{B}_1\boldsymbol{A}_1=\boldsymbol{B}\boldsymbol{A}=\boldsymbol{I}_m$与数域P上方阵的行列式一样，可定义$R$上的方阵的行列式，并有相应的性质
于是$\det\boldsymbol{B}_1\cdot\det\boldsymbol{A}_1=1$但是$\det\boldsymbol{B}_1=\det\boldsymbol{A}_1=0$，矛盾，故$n\geqslant m$．类似可证$m\geqslant n$，故$m=n$．

Corollary 4.2

设R为交换幺环，M与N都为R上的自由模，则$M\cong N\Longleftrightarrow M$与$N$有相同的秩

Proposition 4.6

$\mathbb{Z}$为秩为1的自由$\mathbb{Z}$模，且1是基，但是对于元素2来说其是线性无关的，但是并不是基
$\mathbb{Z}$为秩为1的自由$\mathbb{Z}$模，且1是基，$\{2\}$是线性无关的且$\{1,2\}$是线性相关的，但是1不能由2线性表出

Theorem 4.7

设R为交换幺环，M为R上的秩为n的自由模，则$End_R(M)\cong M_n(R)$为环同构，其中$M_n(R)$为环R上的n阶矩阵环

Proof 取定M的基$\{u_1\cdots u_n\}$，取定$\varphi\in End_R(M)$，则我们有φ在基下的表示阵$M(\varphi)$这由φ唯一确定

即$\varphi(u_1\cdots u_n)=(u_1\cdots u_n)M(\varphi)$

故上述过程确定了一个映射$\sigma:End_R(M)\to M_n(R)\quad \varphi\mapsto M(\varphi)$

接下去需要说明上述σ为双射且为一个环同态

1.单射，若$M(\varphi_1)=M(\varphi_2)$，那么我们就知道$\varphi_1$与$\varphi_2$在基$\{u_1\cdots u_n\}$下的像是一样的

故$\forall x\in M$故φ_1与φ_2在x下的像都一样故$\varphi_1=\varphi_2$

2.满射：取定$A\in M_n(R)$，则存在$v_1\cdots v_n\in M$使得$(v_1\cdots v_n)=(u_1\cdots u_n)A$

那么由自由模泛性质的刻画知：对于R上的自由模M及其$v_1\cdots v_n$，存在唯一的M到M的模同态ψ使得$\psi(u_i)=v_i$

故$\psi(u_1\cdots u_n)=(u_1\cdots u_n)A$故满射证毕

3.下说明σ是一个环同态

设$\eta,\xi\in End_R(M)$，说明$\sigma(\eta+\xi)=\sigma(\eta)+\sigma(\xi)$与$\sigma(\eta\xi)=\sigma(\eta)\sigma(\xi)$

对于任意的u_i我们有$(\eta+\xi)(u_i)=\eta(u_i)+\xi(u_i)\Longrightarrow(\eta+\xi)(u_1\cdots u_n)=\eta(u_1\cdots u_n)+\xi(u_1\cdots u_n)$

$\Longrightarrow(u_1\cdots u_n)M(\eta+\xi)=(u_1\cdots u_n)M(\xi)+(u_1\cdots u_n)M(\eta)\Longrightarrow M(\eta+\xi)=M(\xi)+M(\eta)\Longrightarrow\sigma(\eta+\xi)=\sigma(\eta)+\sigma(\xi)$

再者$(\eta\xi)(u_i)=\eta(\xi(u_i))=\eta((u_1\cdots u_n)\mathrm{col}_iM(\xi))=(\eta(u_1)\cdots\eta(u_n))\mathrm{col}_iM(\xi)=(u_1\cdots u_n)M(\eta)\mathrm{col}_iM(\xi)$

则有$\mathrm{col}_i(M(\eta\xi))=M(\eta)\mathrm{col}_iM(\xi)=\mathrm{col}_i(M(\eta)M(\xi))\Longrightarrow M(\eta\xi)=M(\eta)M(\xi)$

证毕

Theorem 4.8

设R为可换幺环，M为R上的n秩自由模，$\{u_1\cdots u_n\}$为M的一组基，且$\varphi\in End_R(M)$，那么有等价论断

1.φ为可逆映射

2.φ为M上的模自同构

3.$\varphi(u_1)\cdots\varphi(u_n)$为一组基

4.$M(\varphi)$为可逆阵

5.$\det(M(\varphi))$为R上可逆元

Proof 1.$\Longrightarrow$2.显然

2.$\Longrightarrow$3.反证法若$\varphi(u_1)\cdots\varphi(u_n)$并非为一组基，那么就$\varphi(u_1)\cdots\varphi(u_n)$要么线性相关要么生成不出$M$

3.$\Longrightarrow$4.此时φ在基下的矩阵即两组基之间的过渡矩阵，而过渡矩阵是可逆的

4.$\Longrightarrow$5.$M(\varphi)$可逆阵则存在$M(\varphi)B=I_n$取行列式$\Longrightarrow\det(M(\varphi))\cdot\det(B)=1\Longrightarrow\det(M(\varphi))$为$R$上可逆元

5.$\Longrightarrow$4.构造类似的伴随矩阵即可

4.$\Longrightarrow$1.根据$End_R(M)\cong M_n(R)$此时，则有$M(\varphi)B=I_n\Longleftrightarrow\varphi\psi=id$故$\varphi$为可逆映射

4.3 模的直和

Definition 4.12 (外直和)

设R为幺环，且$M_1 \sim M_n$为R上的模，构造乘积集合

$M = M_1 \times \cdots \times M_n := \{(x_1, \cdots x_n) : x_i \in M_i\}$并在该集合上定义如下的运算

$(x_1 \cdots x_n), (y_1 \cdots y_n) \in M$，$a \in R$

$(x_1 \cdots x_n) + (y_1 \cdots y_n) = (x_1 + y_1, \cdots x_n + y_n)$

$a(x_1 \cdots x_n) = (ax_1 \cdots ax_n)$

容易验证M为R上的模，将其称之为M_i的外直和记作$M = \bigoplus_{i=1}^{n} M_i$

若记$M_1^* := \{(x_1, 0, \cdots, 0) : x_1 \in M_1\}$类似的定义$M_2^* \cdots$

此时容易验证M_i^*为M的子模，且构造映射$\varphi : M_1^* \to M_1 \quad (x_1, 0, \cdots, 0) \mapsto x_1$易知有模同构$M_1^* \cong M_1$

Theorem 4.9 (外直和的泛性质)

设R为幺环，$M_1 \sim M_n$都为R上的模，N也为R模，且M_i到N有模同态φ_i

则存在唯一的模同态φ：$M = \bigoplus_{i=1}^{n} M_i \to N \quad$ 且$\varphi((0, \cdots x_i, 0 \cdots 0)) = \varphi_i(x_i)$

Proof 先证明唯一性：若存在这样的模同态，则$\forall (x_1 \cdots x_n) \in M$

此时$\varphi(x_1 \cdots x_n) = \varphi\left(\sum_{i=1}^{n} x_i^*\right) = \sum_{i=1}^{n} \varphi_i(x_i)$故说明了$\varphi$的作用像是不依赖于$\varphi$的故唯一性证毕

存在性只需定义φ的作用即为$\sum_{i=1}^{n} \varphi_i(x_i)$即可

Definition 4.13 (内直和)

设R为幺环，M为R上的模，$N_1 \sim N_k$为M的子模，且有

1.$M = N_1 + N_2 + \cdots + N_k$

2.$N_i \cap (N_1 + \cdots + N_{i-1} + N_{i+1} + \cdots + N_k) = \{0\} \ (\forall 1 \leqslant i \leqslant k)$

则称M为$N_1 \sim N_k$的内直和

Theorem 4.10

设R为幺环，M为R上的模，$N_1 \sim N_k$为M的子模，且满足

1.$M = N_1 + N_2 + \cdots + N_k$

2.$N_i \cap (N_1 + \cdots + N_{i-1} + N_{i+1} + \cdots + N_k) = \{0\} \ (\forall 1 \leqslant i \leqslant k)$

此时构造如下的映射

φ：$\bigoplus_{i=1}^{k} N_i \to M \quad (x_1 \cdots x_k) \mapsto x_1 + \cdots + x_k$ 则φ建立了模同构$\bigoplus_{i=1}^{k} N_i \cong M$

Proof 一方面满射显然有内直和的1.保证

另一方面若$x_1 + \cdots + x_k = y_1 + \cdots + y_k \Longrightarrow x_1 - y_1 = y_2 - x_2 + \cdots + y_k - x_k$

$\Longrightarrow LHS \in N_1; RHS \in N_2 + \cdots + N_k \Longrightarrow x_1 - y_1 = y_2 - x_2 + \cdots + y_k - x_k = 0$

$\Longrightarrow x_1 = y_1$且有$x_2 + \cdots + x_k = y_2 + \cdots + y_k$类似的下去得到所有$x_i = y_i$

再者模同态容易验证

Definition 4.14 (模无关的定义)

设R为幺环，设$M_1 \sim M_n$为R上的模，若$M_i \cap (M_1 + \cdots + M_{i-1} + M_i + \cdots + M_n) = \{0\}\ (\forall 1 \leqslant i \leqslant n)$

则称$M_1 \sim M_n$这些模是无关的

Proposition 4.7

设R为幺环，M是R模，若$x_1 \cdots x_n$是M中n个线性无关的向量

则Rx_i是M的子模，且是无关的。但是逆命题不对

Proof 先证明Rx_i是子模，有定义$Rx_i := \{rx_i : r \in R\}$

此时$r_1x_i - r_2x_i = (r_1 - r_2)\,x_i \in Rx_i$且$r_1 \cdot r_2x_i = (r_1r_2)\,x_i \in Rx_i$

所以Rx_i是M的子模

此时$\forall x \in Rx_1 \cap (Rx_2 + \cdots + Rx_n)$；故不妨设$x = r_1x_1 = r_2x_2 + \cdots + r_nx_n$

$\Longrightarrow r_1x_1 - r_2x_2 - \cdots - r_nx_n = 0 \Longrightarrow r_1 = r_2 = \cdots = r_n = 0$故此时$x = 0$类似的可以证明其他交也为零

但是逆命题不对，例如增加一个$x_{n+1} = 0$, 此时Rx_i仍然后无关的，但是$x_1 \cdots x_n, x_{n+1}$显然是线性相关的

Corollary 4.3

但是把上述命题的 R 幺环改为域则此时子模无瓜与向量线性无关就等价了

Proposition 4.8

设R为幺环，M_1, M_2为R上自由模

1.$M = M_1 \oplus M_2$为自由R模且"和的秩 = 秩的和"。和的基 = 基的并

Theorem 4.11

设M为模，$M_1 \sim M_s$为M的子模且$M = \bigoplus_{i=1}^{s} M_i$，又$N$为$M$的子模，且$N = \bigoplus_{i=1}^{s} N_i$且$N_i \subseteq M_i$

则$M/\bigoplus_{i=1}^{s} N_i = \bigoplus_{i=1}^{s} M_i/\bigoplus_{i=1}^{s} N_i \cong \bigoplus_{i=1}^{s} (M_i/N_i)$

4.4 主理想整环上的有限生成模

4.4.1 p.i.d 上的有限生成模结构 1

Example 4.1一般环上的自由模的子模未必是自由模

例如$\mathbb{Z}_6$上的模$\mathbb{Z}_6$,是自由模因为有基$\{\bar{1}\}$,但其子模$\langle\bar{2}\rangle=\{\bar{0},\bar{2},\bar{4}\}$并不是自由模

一方面：$\langle\bar{2}\rangle=\{\bar{0},\bar{2},\bar{4}\}$并不是零模，且也不是秩大于等于1的自由模，因为若是必然有线性无关的元素

但是$\bar{3}$乘去全为$\bar{0}$

Proposition 4.9

主理想整环上的自由模的子模必定是自由模，而且子模的秩不超过模本身的秩.

Proof 以主理想整环设为D设M为D上的自由模，设其秩为$r(M)$，M的子模记为N

我们对$r(M)$做归纳法，当$r(M)=0$时，此时$N\subseteq M=\{0\}$，故$r(N)=0$为零模

假设$r(M)=n-1$时成立，此时当$r(M)=n$时

取定M的一组基$\{e_1\cdots e_n\}$，构造集合$I=\left\{a_1\in D:\ \sum_{i=1}^{n}a_ie_i\in N\right\}$(即$N$中元素写成基表示之后$e_1$的系数)

断言I是D上的理想原因如下：

1.$\forall a_1,a_1^*\in I$则存在两个元素$a_1e_1+a_2e_2+\cdots+a_ne_n$与$a_1^*e_1+a_2^*e_2+\cdots+a_n^*e_n$都属于$N$

此时相减得到$(a_1-a_1^*)e_1+\cdots+(a_n-a_n^*)e_n$由$N$为子模知道$(a_1-a_1^*)e_1+\cdots+(a_n-a_n^*)e_n\in N$

故$a_1-a_1^*\in I$

2.$\forall d\in D$与$a_1\in I$此时存在元素$a_1e_1+a_2e_2+\cdots+a_ne_n$属于$N$,

此时由于N是子模知：$d(a_1e_1+a_2e_2+\cdots+a_ne_n)\in N\Longrightarrow da_1\in I$

故I是D上的理想

故有$d\in D$使得$\langle d\rangle=I$

若$d=0$则$I=0$，这也意味着N中元素拆为基底表示后e_1前系数均为0，则$N\subseteq\langle e_2\cdots e_n\rangle$

利用归纳假设知，N为自由模，且N的秩小于等于$n-1$进而小于等于n

若$d\neq0$，那么$d\in I$就知道存在元素$f=de_1+\cdots+d_ne_n\in N$其中$d\neq0$,此时自然$f\neq0$

那么$f\notin\langle e_2\cdots e_n\rangle$

下面断言$N=Df\oplus(N\cap\langle e_2\cdots e_n\rangle)$

先说明$N=Df+(N\cap\langle e_2\cdots e_n\rangle)$

1.$RHS\subseteq LHS$显然

2.$\forall g\in N$不妨设$g=a_1e_1+\cdots+a_ne_n\quad a_1\sim a_n\in D$

其中$a_1\in I=\langle d\rangle$故有$a_1^*\in D$使得$a_1^*d=a_1$

故$g-a_1^*f=(a_2-a_1^*d_2)e_2+(a_3-a_1^*d_3)e_3+\cdots+(a_n-a_1^*d_n)e_n$

此时$g\in N$且$f\in N\Longrightarrow g-a_1^*f\in N\Longrightarrow(a_2-a_1^*d_2)e_2+(a_3-a_1^*d_3)e_3+\cdots+(a_n-a_1^*d_n)e_n\in N$

且$(a_2-a_1^*d_2)e_2+(a_3-a_1^*d_3)e_3+\cdots+(a_n-a_1^*d_n)e_n\in\langle e_2\cdots e_n\rangle$

故$(a_2-a_1^*d_2)e_2+(a_3-a_1^*d_3)e_3+\cdots+(a_n-a_1^*d_n)e_n\in(N\cap\langle e_2\cdots e_n\rangle)$

故$g=a_1^*f+(a_2-a_1^*d_2)e_2+(a_3-a_1^*d_3)e_3+\cdots+(a_n-a_1^*d_n)e_n\in Df+(N\cap\langle e_2\cdots e_n\rangle)$

这就说明了$LHS\subseteq RHS$故$N=Df+(N\cap\langle e_2\cdots e_n\rangle)$

3.在说明$Df+(N\cap\langle e_2\cdots e_n\rangle)$的和是直和

$\forall x\in Df\cap(N\cap\langle e_2\cdots e_n\rangle)$则可以设$x=hf=b_2e_2+\cdots+b_ne_n$(其中$h,b_2\sim b_n$均属于$D$)

$\Longrightarrow hde_1+hd_2e_2+\cdots+hd_ne_n=b_2e_2+\cdots+b_ne_n\Longrightarrow$又$\{e_1\cdots e_n\}$为一组基$\Longrightarrow hd=0$

$\Longrightarrow d\neq0$且D为主理想整环自然是无零因子环故$h=0$

$\Longrightarrow x=0$故为直和

综上$N=Df\oplus(N\cap\langle e_2\cdots e_n\rangle)$
此时Df即为1秩自由模，$N\cap\langle e_2\cdots e_n\rangle\subseteq\langle e_2\cdots e_n\rangle$
利用归纳假设故$N\cap\langle e_2\cdots e_n\rangle$为一个自由模且其秩小于等于$n-1$
再利用自由模的直和为自由模且和的秩等于秩的和与和的基等于基的并
证毕

Corollary 4.4

主理想整环有限生成模的子模仍然是有限生成模

Proof 设D为主理想整环，D上的一有限生成模M，其子模N
下说明N也是有限生成的
设M的一有限的生成组为$\{g_1\cdots g_n\}$则$\langle g_1\cdots g_n\rangle=M$
构造自由模D^n并设其一组基$e_1\cdots e_n$，由自由模的泛性质知道存在唯一的模同态φ使得$\varphi(e_i)=g_i$
且因为$g_1\cdots g_n$为M的生成组，故很简单知道φ还是满同态
由模同构基本定理知道，φ建立了D^n中包含 Kerφ的子模与M中子模的一一对应
故φ建立了$\varphi^{-1}(N)$与N的对应.而由上个命题PID上的自由模的子模仍然是自由模，且秩变小
故$\varphi^{-1}(N)$是D^n的子模，是一个自由模，且其秩小于等于n，不妨设其一组基为$f_1\cdots f_r$
此时$\varphi(f_1)\cdots\varphi(f_r)$就生成了$N$
因为$\forall x\in N$其$\varphi^{-1}(x)\in\varphi^{-1}(N)=\langle f_1\cdots f_r\rangle$故$\varphi^{-1}(x)=a_1f_1+\cdots+a_rf_r\Longrightarrow x=a_1\varphi(f_1)+\cdots+a_r\varphi(f_r)$
故N也是有限生成的证毕

Definition 4.15

1.设R为幺环，设M为R上的模，设$x\in M$
若存在$0\neq a\in R$使得$ax=0$则称x为扭元(显然0为扭元)
若不存在这样的$0\neq a$或者说只有零元能做到则称x为非扭元(自由元)
2.设R为幺环，设M为R上的模
若M中每个元素都是扭元则称扭模
若M中每个非零元素都是自由元则称无扭模
3.设R为幺环，M为R上的模，$x\in M$则记
$annihilator(x)=ann(x)=\{a\in R:\ ax=0\}$为$x$的零化子
显然$ann(x)$为R的左理想，且若R可换则为双边理想，且$x\neq0$此时x为扭元$\Longleftrightarrow ann(x)\neq\{0\}$
4.设R为整环，M为R模，
若R为交换环，M为R模则设所有扭元集合构成$torison\ submodel$为M的子模$Tor(M)$　$Tor(M)$　=
$\{x\in M:\ \exists a\in R$使得$ax=0\}$
若R为交换环且为无零因子环(进一步为整环)则且商模$M/Tor(M)$为无扭模

Problem 4.1 1.M为有限$Abel$群，则M作为$\mathbb{Z}$模是扭模
2.设M为域F上的线性空间，则M作为F模是无扭模
3.设V是域F上的有限维线性空间，$\mathscr{A}$是V上的线性变换，$F[\lambda]$是F上的一元多项式环，
$f(\lambda)\in F[\lambda]$则$f(\lambda)(\alpha):=f(\mathscr{A})(\alpha)$，此时$V$为扭模
4.整环R上的自由模一定为无扭模(设一组基证)
5.有理数加群$\mathbb{Q}$作为$\mathbb{Z}$模是无扭模，但不是$\mathbb{Z}$上的自由模(可看为4.的逆命题不真)
(无扭模显然，且容易证明$\mathbb{Q}$中任意两个元素都是线性相关，故若是自由模则秩小于等于2，且$\mathbb{Q}$中有非零元
故$\mathbb{Q}$的秩为1，设$\mathbb{Q}=\left\langle\frac{q}{p}\right\rangle$,则$\frac{q}{p}+\frac{1}{2p}$不能由其表示矛盾)

Lemma 4.1

设M为主理想整环D上的有限生成的无扭模，则M为D上的自由模

Proof 不妨设M的生成组为：$x_1\cdots x_m\in M$且x_i均不为0有$\langle x_1\cdots x_m\rangle=M$

显然$\{x_1\}$一定线性无关否则x_1即为扭元矛盾，那么类似于极大线性无关组的想法

(这里利用无扭模证明了极大无关组的存在性)

我们可以不妨设极大无关组为$\langle x_1\cdots x_r\rangle$此时有

$\sum_{k=1}^{r}a_{kj}x_k+a_jx_j=0\ (\forall r+1\leqslant j\leqslant m且a_{kj}与0\neq a_j\in D)$

记作$a=a_{r+1}\times\cdots\times a_m$因为$D$无零因子则$a\neq 0$

构造映射φ：$M\to M\quad x\mapsto ax$

容易验证φ为模同态则$\varphi:M\to\eta(M)$为一满同态故$M/\mathrm{Ker}\varphi\cong\varphi(M)$

而$\mathrm{Ker}\varphi=\{x\in M:\ \varphi(x)=0\}=\{x\in M:\ ax=0\}\overset{因为无扭模}{=\!=\!=}\{0\}$故$M\cong\varphi(M)$

我们希望$\varphi(M)$即为D上的自由模即可

而我们知道主理想整环上的自由模的子模是自由模所以我们希望$\varphi(M)$是某一个D上的自由模的子模

令$N=\langle x_1\cdots x_r\rangle=Dx_1+\cdots+Dx_r$下面说明$\varphi(M)$是$N$的子模即可

而模同态像仍为模，故$\varphi(M)$是模只需证明$\varphi(M)\subseteq N$即可

注意到$x_1\cdots x_m$是M的生成组故$\varphi(x_1)\cdots\varphi(x_m)$是$\varphi(M)$生成组

所以要证明$\varphi(M)\subseteq N$只需证明$\varphi(x_1)\cdots\varphi(x_m)\in N=\langle x_1\cdots x_r\rangle$

而$\varphi(x_1)=ax_1\cdots\cdots\varphi(x_r)=ax_r\in N$

但是$\varphi(x_{r+1})=ax_{r+1}=a_{r+1}\times\cdots\times a_mx_{r+1}=a_{r+2}\times\cdots\times a_m(-a_{1r+1}x_1-\cdots-a_{rr+1}x_r)=\widehat{a_{r+1}}\times\cdots\times a_m\times\left(-\sum_{k=1}^{r}a_{kr+1}x_k\right)\in N$

一般的对于$r+1\leqslant j\leqslant m$有$\varphi(x_j)=a_{r+1}\times\cdots\widehat{a_j}\times\cdots a_m\times\left(-\sum_{k=1}^{r}a_{kj}x_k\right)\in N$

Theorem 4.12 (主理想整环上有限生成模的分解结构 1)

设D为一个主理想整环，M是有限生成的D模，则存在M的自由子模N使得$M=TorM\oplus N$

且N在同构意义下唯一

Proof 令$\widetilde{M}=M/TorM$由前文知道这是一个无扭模　设M的生成组为$x_1\cdots x_m$则有$\langle x_1\cdots x_m\rangle=M$

设π为M到$\widetilde{M}$的自然映射，于是$\pi(x_1)\cdots\cdots\pi(x_m)$为$\widetilde{M}$的生成组，

则由引理知道PID上有限生成的无扭模是自由模即$\widetilde{M}$是自由模

故存在$e_1\cdots e_r\in M$使得$\pi(e_1)\cdots\pi(e_r)$是$\widetilde{M}$的一组基

令$N=\langle e_1\cdots e_r\rangle=De_1+\cdots+De_r$

此时断言$e_1\cdots e_r$线性无关

若$a_1e_1+\cdots+a_re_r=0\Longrightarrow a_1\pi(e_1)+\cdots+a_r\pi(e_r)=\bar{0}\Longrightarrow a_1=a_2=\cdots=a_r=0$

故N是一个r秩自由模

下说明$M=TorM+N$

一方面$RHS\subseteq LHS$,另一方面$\forall x\in M$则$\pi(x)\in M/TorM$

$\Longrightarrow\pi(x)=b_1\pi(e_1)+\cdots+b_r\pi(e_r)\Longrightarrow x+TorM=b_1e_1+\cdots+b_re_r+TorM$

$\Longrightarrow x-b_1e_1-\cdots-b_re_r\in TorM$故$LHS\subseteq RHS$

再者，$\forall z\in TorM\cap N$，因为$z\in TorM$故z为M中扭元，

且$z\in N=\langle e_1\cdots e_r\rangle$即$N$是主理想整环上的自由模一定为无扭模

故z在N中只有零是扭元故$z=0$故为直和
其次若存在这样的N则有$N\cong M/TorM$

4.4.2 p.i.d 上有限生成的扭模结构

Note 在上文我们已经清楚了
若D为一$p.i.d.$且M为D上有限生成模，则存在M的自由子模N与M上的有限生成扭模$TorM$
成立$M=TorM\oplus N$故我们希望搞清楚主理想整环上有限生成的扭模结构

Definition 4.16

设D为$p.i.d.$且M是D上有限生成的扭模，$\forall a\in D$
定义：$M(a)=\{x\in M:\ ax=0\}$

1.$M(a)$为M的子模$(关键是利用系数环的交换性)$且$M(0)=M$且若a为系数环的可逆元则$M(a)=\{0\}$
2.若$a|b\Longrightarrow M(a)\subseteq M(b)$
3.$M(a)\cap M(b)=M(gcd(a,b))$$(利用2.与p.i.d上存在Bezout定理)$
4.若$(a,b)=1\Longrightarrow M(ab)=M(a)\oplus M(b)$
5.若a相伴$b\Longrightarrow M(a)=M(b)$

Proposition 4.10

设D为$p.i.d$且M为D上有限生成的扭模，又$a\in D^*-U$
并设a的素因子分解：$a=up_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$$(u为D中可逆元，p_i互不相伴)$
则$M(a)=M\left(p_1^{n_1}\right)\oplus M\left(p_2^{n_2}\right)\oplus\cdots\oplus M\left(p_r^{n_r}\right)$

Proof 利用归纳法不难证明

Definition 4.17 (模的 p 分支)

设D为$p.i.d$且p为D上一个素元素，模M为D上的模
称$M_p=\bigcup_{i=1}^{\infty}M\left(p^i\right)$为模$M$的$p$分支又若$M=M_p$则称$M$为$p$模

1.$M\left(p^i\right)\subseteq M\left(p^{i+1}\right)\subseteq\cdots\cdots$
2.M_p是M的子模
3.p模的子模和商模都是p模

Definition 4.18 (子模的零化子)

设R为幺环，M是R模，R的子集$annM:=\{a\in R:\ ax=0,\forall x\in M\}$称为$M$的零化子
1.$annM=\bigcap_{x\in M}annx$
2.$annM$是R的理想$(一般是左模对应左理想)$
3.N_1，N_2均是M的子模则$N_1\subseteq N_2\Longrightarrow annN_2\subseteq annN_1$
4.若R是可交换环，则$\forall x\in M$有$annx=annRx$

Lemma 4.2

设D为$p.i.d$，M为D上的扭模

1.$\forall x\in M$，$\exists a_x\in D$使得$annx=\langle a_x\rangle$且在相伴意义下a_x被x唯一确定

又$\exists a_M\in D$使得$annM=\langle a_M\rangle$在相伴意义下a_M被M唯一确定，a_M是$\{a_x:\ x\in M\}$的最小公倍式

2.$M=M(a_M)=\{x\in M:\ a_Mx=0\}$

3.若$M\neq\{0\}$且M是由$x_1\cdots x_r$有限生成的，则$a_M=[a_{x_1}\cdots a_{x_r}]$且$annM$是$D$的非平凡理想

Proof 1.$\forall x\in M$，$annx$为D的理想，则D为主理想整环则$\exists a_x\in D$使得$annx=\langle a_x\rangle$

且因为M是扭模故$annx\neq\{0\}\Longrightarrow a_x\neq 0$则若有$annx=\langle a_x\rangle=\langle a'_x\rangle$

$\Longrightarrow a_x=a'_xs\quad a'_x=a_xt\Longrightarrow a_x=a'_xts\Longrightarrow ts=1\Longrightarrow a_x$与$a'_x$相伴

同理$annM=\langle a_M\rangle$此时若有$annM=\langle a_M\rangle=\langle a'_M\rangle$再分情况讨论若$annM=\{0\}$则$a_M=a'_M=0$则二者显然相伴

若$annM\neq\{0\}$则$a_M\neq 0,a'_M\neq 0$同理可以证a_M与a'_M相伴

此时显然有$annM\subseteq annx\Longrightarrow\langle a_M\rangle\subseteq\langle a_x\rangle\Longrightarrow a_x|a_M\Longrightarrow a_M$是$\{a_x:\ x\in M\}$的公倍式

此时任取s为$\{a_x:\ x\in M\}$的公倍式故s能够把所有$x\in M$化零，故$s\in\langle a_M\rangle\Longrightarrow s=a_Mt\Longrightarrow a_M|s$

故为最小公倍式

2.显然$M(a_M)\subseteq M$此时$\forall x\in M$,因为$annM=\langle a_M\rangle$则a_M是能够把M中所有元素化零

而$M(a_M)=\{x\in M:\ a_Mx=0\}$故$M(a_M)=M$

3.同理由1.a_M是将M中所有元素化零的，所以a_M同理亦为$a_{x_1}\cdots a_{x_r}$的公倍式

其次任取c为$a_{x_1}\cdots a_{x_r}$的公倍式，$\forall x\in M$则$x=b_1x_1+\cdots+b_rx_r$

$cx=b_1(cx_1)+\cdots+b_r(cx_r)=0$故$c\in\langle a_M\rangle\Longrightarrow a_M|c\Longrightarrow a_M=[a_{x_1}\cdots a_{x_r}]$

下面说明$annM=\langle a_M\rangle$是D的非平凡理想

一方面说明$annM=\langle a_M\rangle\neq\{0\}$只要说明$a_M\neq 0$只要说明$a_M=[a_{x_1}\cdots a_{x_r}]\neq 0$

只要说明$a_{x_1}\cdots a_{x_r}$都$\neq 0$而$annx_1=\langle a_{x_1}\rangle$因为$M$是扭模故$annx_1\neq\{0\}$故$a_{x_1}\neq 0$其余同理

再者说明$annM\neq D$反证法若$annM=D$，此时$1\in annM=\langle a_M\rangle\Longrightarrow a_M\times h=1\Longrightarrow a_M$为单位

$\Longrightarrow M(a_M)=\{0\}=M$这与已知矛盾

Theorem 4.13 (主理想整环上有限生成扭模的分解形式 1)

设D为$p.i.d$，M为D上有限生成的扭模，且$annM=\langle a_M\rangle,a_M=up_1^{n_1}\cdots p_r^{n_r}$

其中u为D上单位，$p_1\cdots p_r$为素元素且互不相伴，则有

1.$\forall p$为D中素元素，则模M的p分支$M_p=\bigcup_{k=1}^{\infty}M(p^k)=\bigcup_{k=1}^{\infty}\{x\in M:\ p^kx=0\}=\begin{cases}M(p_i^{n_i}) & p\text{与}p_i\text{相伴}\\ \{0\} & p\text{与诸}p_i\text{均不相伴}\end{cases}$

2.$M=M_{p_1}\oplus\cdots\oplus M_{p_r}$

Proof 设D为$p.i.d$，M为D上有限生成的扭模，且$annM=\langle a_M\rangle,a_M=up_1^{n_1}\cdots p_r^{n_r}$

其中u为D上单位，$p_1\cdots p_r$为素元素且互不相伴，则有

1.$\forall p$为D中素元素，则模M的p分支$M_p=\bigcup_{k=1}^{\infty}M(p^k)=\bigcup_{k=1}^{\infty}\{x\in M:\ p^kx=0\}=\begin{cases}M(p_i^{n_i}) & p\text{与}p_i\text{相伴}\\ \{0\} & p\text{与诸}p_i\text{均不相伴}\end{cases}$

2.$M=M_{p_1}\oplus\cdots\oplus M_{p_r}$

Corollary 4.5

设D为$p.i.d$且M为D上有限生成的扭模，设N为M的子模,$annM=\langle a_M\rangle,a_M=up_1^{n_1}\cdots p_r^{n_r}$(标准分解)

则有$N=\bigoplus_{i=1}^{r}N_{p_i}$，$N_{p_i}=N\cap M_{p_i}$.其中$M_{p_i},N_{p_i}$都为模分支

Proof 设$annN=\langle b\rangle$,则由于$N\subseteq M$知$annM\subseteq annN\Longrightarrow\langle a_M\rangle\subseteq\langle b\rangle\Longrightarrow b|a_M$

故$b=u^*p_1^{k_1}\cdots p_r^{k_r}$的形式，其中$u^*$为单位,$0\leqslant k_1\cdots k_r\leqslant n_1\cdots n_r$

仿照上个定理同样可以证明$N=\bigoplus_{i=1}^{r}N_{\boldsymbol{p_i}}$

这里的$N_{p_i}=N\left(p_i^{k_i}\right)$所以当$k_i=0$时$N_{p_i}=N\left(p_i^{k_i}\right)=N(1)=\{0\}$不影响

接下来说明$N_{p_i}=N\cap M_{p_i}$

$N\cap M_{p_i}=N\cap\bigcup_{k=1}^{\infty}M\left(p_i^k\right)=N\cap\left\{x\in M:\ \exists k\in\mathbb{Z}^+\text{使得}p_i^kx=0\right\}\overset{N\subseteq M}{=\!=\!=}\left\{x\in N:\ \exists k\in\mathbb{Z}^+\text{使得}p_i^kx=0\right\}=N_{p_i}$

故证毕

4.4.3 p.i.d 上有限生成的 p 模结构

Note 于是我们对于$p.i.d$上的有限生成的扭模得到了一个分解，其中$M_{p_i}=M\left(p_i^{n_i}\right)$为$M$的子模

若将M_{p_i}看成新的完整模有$M_{p_i}=\bigcup_{k=1}^{\infty}M\left(p_i^k\right)$，则$M_{p_i}$为一个$p$模，所以我们接下来继续思考$p.i.d$上有限生成的$p$模结构

Lemma 4.3

设D为$p.i.d$，且M为D上n秩自由模，N是M的子模，商模M/N为p模

则存在M的基$\{e_1\cdots e_n\}$以及非负整数组$k_1\cdots k_n$使得$p^{k_1}e_1\cdots p^{k_n}e_n$为$N$的一组基

Proof 我们对秩n做数学归纳法

当$n=1$时，设e为M的基生出M，故$\bar{e}=e+N$是M/N的生成元，又因为M/N是p模

故存在p的某个方幂把$\bar{e}$化零，可设$ann\bar{e}=\left\langle p^k\right\rangle$，其中$k\geqslant 0$(取能够把$\bar{e}$化零的最小的$k$)

下说明$\left\{p^ke\right\}$为N的基

一方面p^ke线性无关，若$ap^ke=0\overset{e线性无关}{\Longrightarrow}ap^k=0\overset{整环}{\Longrightarrow}a=0$

另一面p^ke生出N，因为$N\subseteq M=\langle e\rangle$故取$N$中任何一元素形如$ae$

$ae\in N$取等价类则$a\bar{e}=\bar{0}\Longrightarrow a\in ann\bar{e}=\left\langle p^k\right\rangle\Longrightarrow a=p^k\times t\Longrightarrow N$中任何一元素$ae=t\cdot\left(p^ke\right)$

故当$n=1$证毕

下设当秩为$n-1$成立去证明秩为n情况

取M的一组基$\{f_1\cdots f_n\}$

构造集合$I_i=\left\{a_i:\ x\in N,x=\sum_{i=1}^{n}a_if_i\right\}$

不难证明I_i为D的理想，而D为主理想整环$\Longrightarrow I_i=\langle c_i\rangle$

因为M/N为p模故存在$p^{n_i}\overline{f_i}=\bar{0}\Longrightarrow p^{n_i}\left(f_i+N\right)=0+N\Longrightarrow p^{n_i}f_i\in N\Longrightarrow p^{n_i}\in I_i=\langle c_i\rangle$

$\Longrightarrow c_i|p^{n_i}\overset{素元素方幂的因子}{\Longrightarrow}c_i\sim p^{l_i}$(相伴)$\Longrightarrow I_i=\langle c_i\rangle=\left\langle p^{l_i}\right\rangle$

$\Longrightarrow I_i=\left\{a_i:\ x\in N,x=\sum_{i=1}^{n}a_if_i\right\}=\left\langle p^{l_i}\right\rangle$

不妨设l_1是诸位l_i中最小的则有$p^{l_1}|p^{l_*}|\cdots\cdots$

此时$p^{l_1}\in I_1$故存在N中元素$g=p^{l_1}f_1+a_2f_2+\cdots+a_nf_n\in N$

此时$a_2\sim a_n\in I_2\sim I_n$故$a_2\sim a_n\in\left\langle p^{l_2}\right\rangle\sim\left\langle p^{l_n}\right\rangle$故$a_2\sim a_n$是$p^{l_2}\sim p^{l_n}$的倍式更是$p^{l_1}$的倍式

$\Longrightarrow g=p^{l_1}\left(f_1+a_1'f_2+\cdots+a_n'f_n\right):=p^{l_1}e_1$(其中$e_1=f_1+a_1'f_2+\cdots+a_n'f_n$)

此时$(e_1,f_1,f_2\cdots f_n)=(f_1,f_2\cdots f_n)\begin{pmatrix}1&0&0&0\\a_1'&1&0&0\\\vdots&\vdots&\vdots&\vdots\\a_n'&0&0&1\end{pmatrix}$

$\Longrightarrow\{e_1,f_1\cdots f_n\}$为$M$的一组基

$M=\langle e_1,f_1\cdots f_n\rangle=De_1\oplus Df_1\oplus\cdots\oplus Df_n$

故令$M_1=Df_1\oplus\cdots\oplus Df_n$并且记$N_1=N\cap M_1$则$N_1$是$M_1$的子模

由模同构基本定理：$M_1/N_1=M_1/(M_1\cap N)\cong(M_1+N)/N\subseteq M/N$

而M/N是p模且p模的子模是p模则M_1/N_1是p模

下证：$N=Dg\oplus N_1$

(因为我们利用归纳假设思路就是要$M=De_1\oplus M_1,N=Dg\oplus N_1$对应的基是$e_1,f_1\cdots f_n$与$g=p^{l_1}e_1\cdots\cdots$)

显然$g\in N$故$Dg\in N,N_1\subseteq N$故$Dg+N_1\subseteq N$

此时$\forall x\in N\quad x=b_1f_1+\cdots+b_nf_n$此时想去说明$x-g$的倍式在$N_1$里且$g=p^{l_1}\left(f_1+a_1'f_2+\cdots+a_n'f_n\right)$且$b_1\in I_1$

不妨设$x=tp^{l_1}f_1+b_2f_2+\cdots+b_nf_n$

所以$x-tg=\left(b_2-tp^{l_1}a_2'\right)f_2+\cdots+\left(b_n-tp^{l_1}a_n'\right)f_n$想去说明$x-tg\in N_1=M_1\cap N$

一方面$x\in N,g\in N\Longrightarrow x-tg\in N$,且$x-tg\in\langle f_2\cdots f_n\rangle=M_1$

故$N=Dg+N_1$

下证$Dg+N_1=Dg\oplus N_1$

此时$Dg\cap N_1\subseteq De_1\cap N_1\subseteq De_1\cap M_1=\{0\}$

故：$N=Dg\oplus N_1$

利用归纳假设针对M_1，N_1，M_1/N_1利用归纳假设

由M_1的一组基$\{e_2\cdots e_n\}$,N_1的一组基$\{p^{m_2}e_2\cdots\cdots p^{m_n}e_n\}$

所以M得一组基为$\{e_1,e_2\cdots e_n\}$,N的一组基为$\{g,p^{m_2}e_2\cdots p^{m_n}e_n\}=\left\{p^{l_1}e_1,p^{m_2}e_2\cdots p^{m_n}e_n\right\}$

证毕

Theorem 4.14

设D是$p.i.d$，　M'是D上有限生成的p模

则$M'=\bigoplus_{i=1}^{m}Dy_i$　$ann\,(y_i)=\left\langle p^{k_i}\right\rangle$　$1\leqslant k_1\leqslant k_2\leqslant\cdots\leqslant k_m$且数$m$与$k_1\cdots k_m$唯一被$M'$确定

Proof 设M'的一组生成元为$\{x_1\cdots x_n\}$,构造D上的n秩自由模M一组基为$\{f_1\cdots f_n\}$

由自由模的泛性质知：存在唯一的$M\to M'$的模同态η使得$\eta\,(f_i)=x_i\,(\forall 1\leqslant i\leqslant n)$

由因为M'的一组生成元为$\{x_1\cdots x_n\}$，所以η为$M\to M'$的满模同态

$\Longrightarrow M/\mathrm{Ker}\eta\cong M'$并将 $\mathrm{Ker}\eta:=N$且M'是D上有限生成的p模$\Longrightarrow M/\mathrm{Ker}\eta$是$D$上有限生成的$p$模

故要去证明M'结构思考N结构

根据引理知道存在M的一组基$\{e_1\cdots e_n\}$使得$\{p^{m_1}e_1\cdots p^{m_n}e_n\}$为$N$的基

且不妨设$m_1\leqslant m_2\leqslant\cdots\leqslant m_n$

$\Longrightarrow M'\cong M/N=\bigoplus_{i=1}^{n}De_i/\bigoplus_{i=1}^{n}Dp^{m_i}e_i\cong\bigoplus_{i=1}^{n}De_i/Dp^{m_i}e_i$

发现当$m_i=0$时候，$p^{m_i}=p^0=1,De_i/Dp^{m_i}e_i=\{0\}$则在上行直和式中直和没有效果

把上述没有直和效果的删去，故可以设$m_1\sim m_n$中有m个不为0

设$0=m_1=m_2=\cdots=m_{n-m}<m_{n-m+1}\leqslant m_{n-m+2}\leqslant\cdots\leqslant m_n$

并记$m_{n-m+1}=k_1$，$m_{n-m+2}=k_2\cdots$，$m_n=k_m$，并记作$y_i'=e_{n-m+i}+Dp^{k_i}e_{n-m+i}$

故$\bigoplus_{i=1}^{n}\left(De_i/Dp^{m_i}e_i\right)=\underbrace{\bigoplus_{i=1}^{n}\left(De_{n-m+i}/Dp^{k_i}e_{n-m+i}\right)}=\bigoplus_{i=1}^{m}Dy_i'$

因为原来e_{n-m+i}是生成元故可以将e_{n-m+i}对应的左陪集作为商模的生成元

注意到$ann\,(y_i')=\left\langle p^{k_i}\right\rangle$

总结以上是有：$M'\cong\bigoplus_{i=1}^{m}Dy_i'$不妨设中的同构对应为$y_i\to y_i'$

于是$M'=\bigoplus_{i=1}^{m}Dy_i$且$ann\,(y_i)=\left\langle p^{k_i}\right\rangle$

唯一性略去看参考孟道骥老师之书

4.4.4 p.i.d 上的有限生成模的标准分解

Theorem 4.15 (标准分解形式 1)

设D为$p.i.d$且M为D上的有限生成模，则M可以分解为若干个循环模的直和

1.$M=TorM\oplus N$(此时N为M的自由子模其秩由M唯一确定)

2.并记作$ann(TorM)=\langle a\rangle$记$a=up_1^{n_1}\cdots p_r^{n_r}$(其中$a$元素与$p_1\cdots p_r$在相伴下与不计先后次序唯一确定)

此时$TorM=(TorM)_{p_1}\oplus(TorM)_{p_2}\oplus\cdots\oplus(TorM)_{p_r}=M_{p_1}\oplus M_{p_2}\oplus\cdots\oplus M_{p_r}$

3.$M_{p_i}=\bigoplus_{j=1}^{m_i}Dx_{ij}$其中$ann(x_{ij})=\left\langle p_i^{k_{ij}}\right\rangle$且不妨设$1\leqslant k_{im_i}\leqslant\cdots\leqslant k_{i2}\leqslant k_{i1}$(其中$m_i$与$k_{i1}\sim k_{im_i}$与$ann(x_{ij})$唯一确定)

4.将N的秩记为m_0一组基记为$\{x_{01}\cdots x_{0m_0}\}$其中$ann(x_{0i})=\{0\}(1\leqslant i\leqslant m_0)$

$\Longrightarrow M=\bigoplus_{i=0}^{r}\bigoplus_{j=1}^{m_i}Dx_{ij}$其中$ann(x_{ij})=\{0\}$或者为准素循环模

我们将$p_i^{k_{ij}}$称为初等因子，$\left\{p_i^{k_{ij}}\right\}(1\leqslant i\leqslant r,\ 1\leqslant j\leqslant m_i)$称为初等因子组

Lemma 4.4

设D为$p.i.d$且M是D上的模，且$x,y\in M$且$annx=\langle a\rangle$与$anny=\langle b\rangle$若有a,b互素

则$Dx\oplus Dy=D(x+y)$且$ann(x+y)=\langle ab\rangle$

推广：若$x_1\cdots x_r\in M$且$annx_i=\langle a_i\rangle$且$a_i$两两互素则$\bigoplus_{i=1}^{r}Dx_i=D(x_1+\cdots+x_r)$且$ann(x_1+\cdots+x_r)=\langle a_1\cdots a_r\rangle$

Proof 一方面$D(x+y)\subseteq Dx+Dy$显然

另一方面，$(a,b)=1\Longrightarrow ua+vb=1\Longrightarrow x=vbx\Longrightarrow x=vb(x+y)$

$\Longrightarrow x\in D(x+y)\Longrightarrow Dx\subseteq D(x+y)$同理$Dy\subseteq D(x+y)\Longrightarrow Dx+Dy\subseteq D(x+y)$

再者，有$Dx\cap Dy\subseteq M(a)\cap M(b)=M(gcd(a,b))=M(1)=\{0\}$故$Dx\cap Dy=\{0\}$

故$Dx\oplus Dy=D(x+y)$

其次，$ab(x+y)=0$故$ab\in ann(x+y)\Longrightarrow\langle ab\rangle\subseteq ann(x+y)$

且对于$\forall c\in ann(x+y)\Longrightarrow cx+cy=0\Longrightarrow 0=cx+cy\in Dx\oplus Dy\Longrightarrow cx=0$且$cy=0$

$\Longrightarrow c\in annx=\langle a\rangle$且$c\in anny=\langle b\rangle\Longrightarrow a|c$且$b|c\Longrightarrow ab|c\Longrightarrow c\in\langle ab\rangle\Longrightarrow ann(x+y)\subseteq\langle ab\rangle$

Theorem 4.16

设D为$p.i.d$且M是D上的有限生成模

则有$M=\bigoplus_{i=1}^{s}Dz_i$且$annz_s\subseteq annz_{s-1}\subseteq\cdots\subseteq annz_1$,且$annz_i\neq D$(为保证直和项都不是0)

并设$annz_i=\langle d_i\rangle$且有$d_i|d_{i+1}$，$\{\alpha_i\}$在相伴意义下由$M$唯一确定，其中$d_i$称为不变因子$\{d_i\}$为不变因子组

Proof 由于第一标准分解式：

$M=\bigoplus_{i=1}^{r}\bigoplus_{j=1}^{m_i}Dx_{ij}\oplus\bigoplus_{j=1}^{m_0}Dx_{0j}$其中$ann(x_{ij})=\left\langle p_i^{k_{ij}}\right\rangle$与$ann(x_{0j})=\{0\}$，$p_1\cdots p_r$为两两互不相伴的素元素

仿照高等代数利用初等因子写不变因子

令$m=\max\{m_1\cdots m_r\}$此时

对于$i=1\cdots r$，$j=m_i+1,m_i+2\cdots m$

定义$k_{ij}=0$与$Dx_{ij}=0(x_{ij}=1)$故$p_i^{k_{ij}}=1,ann(x_{ij})=\left\langle p_i^{k_{ij}}\right\rangle=\langle 1\rangle=D$

故令$d_1=p_1^{k_{1m}}p_2^{k_{2m}}\cdots p_r^{k_{rm}}\cdots\cdots\cdots d_m=p_1^{k_{11}}p_2^{k_{21}}\cdots p_r^{k_{r1}}$

则有$d_j|d_{j+1}(\forall j)$

令$z_1=x_{1m}+x_{2m}+\cdots+x_{rm}\cdots\cdots z_m=x_{11}+x_{21}+\cdots+x_{r1}$
且$p_1^{k_{1j}}\cdots p_r^{k_{rj}}\ (1\leqslant j\leqslant m)$两两互素则根据引理$Dz_1=Dx_{1m}\oplus\cdots\oplus Dx_{rm}\cdots\cdots Dz_m=Dx_{11}\oplus Dx_{21}\oplus\cdots\oplus Dx_{r1}$
且$annz_1=\left\langle p_1^{k_{1m}}\cdots p_r^{k_{rm}}\right\rangle=\langle d_1\rangle\cdots\cdots annz_m=\left\langle p_1^{k_{11}}\cdots p_r^{k_{r1}}\right\rangle=\langle d_m\rangle$且$annz_m\subseteq\cdots\subseteq annz_1$
再$z_{m+1}=x_{01}\cdots\cdots z_s=x_{0m_0}\ (s=m+m_0)$

$$M=\bigoplus_{i=1}^{r}\bigoplus_{j=1}^{m}Dx_{ij}\oplus\bigoplus_{j=1}^{m_0}Dx_{0j}=\bigoplus_{j=1}^{m}\bigoplus_{i=1}^{r}Dx_{ij}\oplus\bigoplus_{j=1}^{m_0}Dx_{0j}=\bigoplus_{j=1}^{m}Dz_{m+1-j}\oplus\bigoplus_{j=1}^{m_0}Dz_j$$

Proposition 4.11

1.$r(M)$与$\{d_j\}$是M的全系不变量
2.两种标准分解式直和项数相等当且仅当模M的扭模部分为零或者为p模
3.$annM=\bigcap\limits_{x\in M}annx=\bigcap\limits_{j=1}^{s}annz_j=annz_s=\begin{cases}0 & N\neq\{0\}\\ \langle d_m\rangle & N=0\end{cases}$(其中$N$为$M$的自由子模)

Lemma 4.5

设D为$p.i.d$，且M是D上的扭模，$x\in M$，$annx=\langle ab\rangle$且$(a,b)=1$
则存在$x_1,x_2\in M$使得$x=x_1+x_2$同时$Dx=Dx_1\oplus Dx_2$与$annx_1=\langle a\rangle$，$annx_2=\langle b\rangle$

Proof 由于$(a,b)=1\Longrightarrow\exists u,v\in D$使得$ua+vb=1\Longrightarrow x=uax+vbx$
故令$uax:=x_2$，$vbx:=x_1$即可
此时$annx_1=ann(vbx)$一方面显然$a\in ann(vbx)\Longrightarrow\langle a\rangle\subseteq ann(vbx)$
另一方面$ua+vb=1$故设$(a,v)=d\Longrightarrow d|a$且$d|v\Longrightarrow d|1\Longrightarrow d$单位故在相伴下$(a,v)=1$
$\forall c\in ann(vbx)\Longrightarrow cvbx=0\Longrightarrow cvb\in annx\Longrightarrow cvb=abt\Longrightarrow cv=at\Longrightarrow a|cv\Longrightarrow a|c\Longrightarrow c\in\langle a\rangle$
$ann(vbx)\subseteq\langle a\rangle$故$annx_1=\langle a\rangle$同理$annx_2=\langle b\rangle$
利用4.4.4节前一个引理即可

Note 设M是$\mathbb{R}[\lambda]$上的模，且$M=\bigoplus\limits_{i=1}^{6}\mathbb{R}[\lambda]x_i$且有如下零化子

$annx_1=\left\langle(\lambda+1)^2\left(\lambda^2+\lambda+1\right)\right\rangle\quad annx_2=\left\langle(\lambda-1)^2\left(\lambda^2-\lambda-1\right)^3\right\rangle$
$annx_3=\left\langle\left(\lambda^2+\lambda+1\right)^2\right\rangle\quad annx_4=\left\langle\left(\lambda^2-1\right)\left(\lambda^2+\lambda+1\right)\right\rangle$
$annx_5=annx_6=\langle 0\rangle$
求出M的初等因子组与不变因子组与标准分解式

显然$annx_i$并不是一个包含一个所以不会是第二标准分解，且生成元并非全是准素元与0也并非第一分解
故这是一个非标准分解，我们采用
非标准分解$\xrightarrow{\text{继续分解}}$第一标准分解$\xrightarrow{\text{写出}}$初等因子组$\xrightarrow{\text{结合}}$不变因子组$\xrightarrow{\text{写出}}$第二标准分解式子
$\mathbb{R}[\lambda]$上的素元素为一次与二次多项式且$\left(\lambda^2-\lambda-1\right)^3=\left(\lambda-\frac{1+\sqrt{5}}{2}\right)^3\left(\lambda-\frac{1-\sqrt{5}}{2}\right)^3$与$\left(\lambda^2-1\right)=(\lambda-1)(\lambda+1)$
存在y_1,y_2使得$x_1=y_1+y_2$且$\mathbb{R}[\lambda]x_1=\mathbb{R}[\lambda]y_1\oplus\mathbb{R}[\lambda]y_2$与$anny_1=\left\langle(\lambda+1)^2\right\rangle\quad anny_2=\left\langle\left(\lambda^2+\lambda+1\right)\right\rangle$
同理可得到其他的
故初等因子组为
$$\left\{(\lambda+1)^2,\lambda^2+\lambda+1,(\lambda-1)^2,\left(\lambda-\frac{1+\sqrt{5}}{2}\right)^3,\left(\lambda-\frac{1-\sqrt{5}}{2}\right)^3,\left(\lambda^2+\lambda+1\right)^2,(\lambda-1),(\lambda+1),\left(\lambda^2+\lambda+1\right)\right\}$$

4.5 p.i.d 上有限生成模的应用

4.5.1 有限生成的 Abel 群

Theorem 4.17

(1) 设G是有限生成的$Abel$群，群运算为加法，则存在整数$n \geqslant 0$以及正整数组$d_1 \cdots d_k$满足

1.$d_i | d_{i+1}\ (1 \leqslant i \leqslant k-1)$

2.$G \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n个} \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_k}$

其中n与$d_1 \cdots d_k$

(2) 设G为有限生成的$Abel$群，则$G \cong \bigoplus_{i,j} \mathbb{Z}_{d_{i,j}} \oplus \bigoplus_{i=1}^{n} \mathbb{Z}$其中$d_{i,j} = p_i^{k_{ij}}$，$p_i$为素数

Proof 1.将G看成$\mathbb{Z}$模，G为有限生成的，则由第二分解式子知

$$G = \underbrace{\bigoplus_{i=1}^{k} \mathbb{Z} y_i}_{\text{非自由模导出循环模}} \oplus \underbrace{\bigoplus_{i=k+1}^{k+n} \mathbb{Z} y_i}_{\text{自由模部分,1秩}} \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{d_i} \oplus \bigoplus_{i=k+1}^{k+n} \mathbb{Z}$$

其中$anny_i = \langle d_i \rangle\ (1 \leqslant i \leqslant k)$且$d_i | d_{i+1}$与$anny_i = \{0\}\ (k+1 \leqslant i \leqslant k+n)$

2.同理

Corollary 4.6

若G为有限阶的$Abel$群(自然就是有限生成的)，则G的同构式中$\bigoplus_{i=1}^{n} \mathbb{Z}$的部分是不存在的

Proof 这只需要对于我们定理中的同构式子取阶即可

Note 6000阶$Abel$群的结构在同构意义下有几种？

$6000 = 2^4 \times 3 \times 5^3$

则2的指数4的划分有$4=1+1+1+1$　$4=1+2+1$　$4=1+3$　$4=2+2$　$4=4$共计五种

则3的指数1的划分就1种

则5的指数3的划分就$3=1+1+1$　$3=1+2$　$3=3$共计3种

故根据定理的 (2) 形式共计$5 \times 3 \times 1 = 15$种

4.5.2 线性变换的标准型

Note 若$\mathscr{A}$是域F上n维线性空间V的线性变换

此时我们将V视作$F[\lambda]$模，其中模乘法$f(\lambda) \cdot x := f(\mathscr{A})(x)$，且有$Caley-Hamilton$定理知道为扭模

且V是有限生成的我们因为V的一组基即为生成组，系数为零次多项式自然也是属于$F[\lambda]$

且$F[\lambda]$的域上的一元多项式环为欧几里得环为主理想整环

故由$p.i.d$上有限生成模的结论我们自然知道

$V = \bigoplus_{i=1}^{s} F[\lambda] z_i$其中$z_i \in V$且$annz_i = \langle d_i(\lambda) \rangle$且$d_i(\lambda) | d_{i+1}(\lambda)\ (1 \leqslant i \leqslant s-1)$

不妨记$F[\lambda] z_i := V_i$　需要指出的是V_i为$\mathscr{A}$的不变子空间

一方面$f(\lambda) z_i$与$g(\lambda) z_i \in F[\lambda] z_i := V_i$则$f(\lambda) z_i + g(\lambda) z_i = f(\mathscr{A})(z_i) + g(\mathscr{A})(z_i) = (f(\mathscr{A}) + g(\mathscr{A}))(z_i) = (f(\lambda) + g(\lambda)) \cdot z_i$

另一方面$\forall a\in F$则$af(\lambda)z_i=af(\mathscr{A})(z_i)=(af(\mathscr{A}))(z_i)=(af(\lambda))\cdot z_i$

故V_i为子空间

此外$\mathscr{A}(f(\lambda)\cdot z_i)=\mathscr{A}(f(\mathscr{A})(z_i))=(\lambda f(\lambda))\cdot z_i$

故V_i为不变子空间我们将$\mathscr{A}|_{V_i}:=\mathscr{A}_i$

其中每一个V_i均为循环模，故我们寻找$\mathscr{A}$的标准型与基，只需观察每一个循环模V_i的结构

Lemma 4.6

设$\mathscr{A}$是域F上的线性空间V的线性变换．由$\mathscr{A}$定义的$F[\lambda]$模V的不变因子为$d(\lambda)$，即$V=F[\lambda]z,annz=\langle d(\lambda)\rangle$

则有下列结论

(1) $\deg d(\lambda)=\dim V$且$z,\mathscr{A}z,\cdots,\mathscr{A}^{n-1}z$为$V$的一组基

(2) 设$d(\lambda)=\lambda^n+a_{n-1}\lambda^{n-1}+\cdots+a_1\lambda+a_0$，则$\mathscr{A}$在上述基下的矩阵为$\boldsymbol{M}\left(\mathscr{A};z,\mathscr{A}z,\cdots,\mathscr{A}^{n-1}z\right)=\begin{pmatrix}0 & & & -a_0\\ 1 & 0 & & -a_1\\ & \ddots & & \vdots\\ & & 0 & -a_{n-2}\\ & & 1 & -a_{n-1}\end{pmatrix}$

(3) $\mathscr{A}$在V上的极小多项式与特征多项式相等

(4) 此时V称为循环空间，方阵称为$\mathscr{A}$在V上的友阵

Proof 因$\operatorname{ann}z=\langle d(\lambda)\rangle$，即$f(\lambda)z=0$当且仅当$d(\lambda)\mid f(\lambda)$，故$\deg f(\lambda)\geqslant\deg d(\lambda)=n$，于是$z,\mathscr{A}z,\cdots,\mathscr{A}^{n-1}z$线性无关

又设$x\in V$，由$V=F[\lambda]z$有$x=f(\lambda)z$．设$f(\lambda)=d(\lambda)\cdot q(\lambda)+r(\lambda)$，其中，$r(\lambda)=0$或$\deg r(\lambda)<\deg d(\lambda)$

于是$x=r(\lambda)z\in L\left(z,\mathscr{A}z,\cdots,\mathscr{A}^{n-1}z\right)$．结论1）得证

又因$\mathscr{A}\left(\mathscr{A}^kz\right)=\mathscr{A}^{k+1}z,\quad 0\leqslant k\leqslant n-2,$

$\mathscr{A}\left(\mathscr{A}^{n-1}z\right)=\mathscr{A}^nz=\left(d(\mathscr{A})-\sum_{k=0}^{n-1}a_k\mathscr{A}^k\right)z=-\sum_{k=0}^{n-1}a_k\eta^kz$故结论2）成立．

Theorem 4.18 (有理标准型 I)

设$\mathscr{A}$是域F上的线性空间V的线性变换

由$\mathscr{A}$定义的$F[\lambda]$模V的不变因子为$d_1(\lambda),d_2(\lambda),\cdots,d_s(\lambda),\quad d_i(\lambda)\mid d_{i+1}(\lambda),1\leqslant i\leqslant s-1$

即利用结论已知$V=\bigoplus_{i=1}^{s}F[\lambda]z_i\quad annz_i=\langle d_i(\lambda)\rangle\quad(d_i(\lambda)$也称为线性变换$\mathscr{A}$的不变因子）

则有下列结论

(1) V中存在一组基，使得$\mathscr{A}$在这组基下的矩阵为准对角$\operatorname{diag}(\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_s)$，其中，$\boldsymbol{B}_i$是$d_i(\lambda)$的友阵

(2) $\sum_{i=1}^{s}\deg d_i(\lambda)=\dim V$

(3) $\operatorname{ann}V=\langle d_s(\lambda)\rangle$，即$\mathscr{A}$的极小多项式是$d_s(\lambda)$

(4) $\mathscr{A}$的特征多项式为$f(\lambda)=\det(\lambda\mathrm{id}-\mathscr{A})=\prod_{i=1}^{s}d_i(\lambda)$

(5) $f(\mathscr{A})=0$

Proof 1）V作为由$\mathscr{A}$定义的$F[\lambda]$模有循环子模分解$V=\bigoplus_{i=1}^{s}F[\lambda]z_i$其中，$\operatorname{ann}z_i=\langle d_i(\lambda)\rangle,\quad d_i(\lambda)\mid d_{i+1}(\lambda),\quad i=1,2,\cdots,n-1$

$V_i=F[\lambda]z_i$是$\mathscr{A}$的不变子空间，$\mathscr{A}|_{V_i}=\mathscr{A}_i$，因而知在$V_i$中，$z_i,\mathscr{A}z_i,\cdots,\mathscr{A}^{n_i-1}z_i$（其中，$n_i=\deg d_i(\lambda)$）是基

$\mathscr{A}_i$在这组基下的矩阵为$d_i(\lambda)$的相伴矩阵由$V=V_1\oplus V_2\oplus\cdots\oplus V_s$知结论1）成立

2）$\dim V=\sum_{i=1}^{s}\dim V_i=\sum_{i=1}^{s}\deg d_i(\lambda).$

3）设$\operatorname{ann}V=\langle d(\lambda)\rangle$，则$d(\lambda)z_i=0$．因而$d(\lambda)\in\operatorname{ann}z_s=\langle d_s(\lambda)\rangle$，即$d_s(\lambda)\mid d(\lambda)$

另一方面，由$d_i(\lambda)\mid d_s(\lambda)(1\leqslant i\leqslant s)$知$d_s(\lambda)z_i=0(1\leqslant i\leqslant s)$，因而$d_s(\lambda)x=0(\forall x\in V)$，即$d_s(\lambda)\in\langle d(\lambda)\rangle$

由此知$d(\lambda)\mid d_s(\lambda)$，于是$d_s(\lambda)$是$\mathscr{A}$的极小多项式

4）$f(\lambda)=\det(\lambda\mathrm{id}-\mathscr{A})=\prod_{i=1}^{s}\det\left(\lambda\mathrm{id}_{V_i}-B_i\right)=\prod_{i=1}^{s}d_i(\lambda)$.

5）$f(\mathscr{A})=\prod_{i=1}^{s}d_i(\mathscr{A})=\left(\prod_{i=1}^{s-1}d_i(\mathscr{A})\right)d_s(\mathscr{A})=0$.

Theorem 4.19 (Jordan 标准型)

设F为代数封闭域，V是F上的有限维线性空间，$\mathscr{A}$是V上的线性变换

则存在V中一组基，使得$\mathscr{A}$在这组基下的矩阵为准对角阵$\mathrm{diag}\{C_1\cdots C_t\}$

其中$C_i=\begin{pmatrix}\lambda_i & & & & \\ 1 & \lambda_i & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda_i\end{pmatrix}$此时$\mathrm{diag}\{C_1\cdots C_t\}$称为$\mathscr{A}$的Jordan标准型

Proof 由于F为代数封闭域，即$F[\lambda]$的一个多项式的根一定都在F中，故$F[\lambda]$中素元素都是一次多项式

根据定理，由$\mathscr{A}$定义的$F[\lambda]$模V可分解成循环子模的直和，$V=\bigoplus_{i=1}^{t}F[\lambda]y_i$，$\mathrm{ann}y_i=\langle(\lambda-\lambda_i)^{r_i}\rangle$，$i=1,2,\cdots,t$

于是$V_i=F[\lambda]y_i$是$\mathscr{A}$的不变子空间，而y_i，$(\mathscr{A}-\lambda_i\mathrm{id})\,y_i$，$\cdots$，$(\mathscr{A}-\lambda_i\mathrm{id})^{r_i-1}y_i$是$V_i$的一组基．由

$\mathscr{A}(\mathscr{A}-\lambda_i\mathrm{id})^{k_i}y_i=\lambda_i(\mathscr{A}-\lambda_i\mathrm{id})^{k_i}y_i+(\mathscr{A}-\lambda_i\mathrm{id})^{k_i+1}y_i$，$1\leqslant k_i\leqslant r_i-2$,

$\mathscr{A}(\mathscr{A}-\lambda_i\mathrm{id})^{r_i-1}y_i=\lambda_i(\mathscr{A}-\lambda_i\mathrm{id})^{r_i-1}y_i$

得$\mathscr{A}|_{V_i}$在基$y_i,(\mathscr{A}-\lambda_i\mathrm{id})\,y_i,\cdots,(\mathscr{A}-\lambda_i\mathrm{id})^{r_i-1}y_i$下的矩阵为$\boldsymbol{C}_i$

因$V=V_1\oplus V_2\oplus\cdots\oplus V_t$，故在$V$中有基，使得$\mathscr{A}$在此基下的矩阵为Jordan标准形．

且在不计C_i次序的情况下$\mathscr{A}$的Jordan型是唯一的，这是因为$\mathscr{A}\Longleftrightarrow$不变因子组$\Longleftrightarrow$Joradan快$\Longleftrightarrow$Jordan标准型

Corollary 4.7

只要上述的所有的初等因子都是一次因式的方幂，尽管 F 不是代数封闭域，仍然可以得到上述 Jordan 标准型

4.6 p.i.d 上的矩阵

Definition 4.19

设D为$p.i.d$，$\boldsymbol{A},\boldsymbol{B}$是$D$上的$m\times n$矩阵．若有$D$上$m$阶可逆矩阵$\boldsymbol{P}$,$n$阶可逆矩阵$\boldsymbol{Q}$，使得$B=PAQ$,则称$\boldsymbol{A}$与$\boldsymbol{B}$相抵

容易知道相抵关系是一个等价关系

Note 先定义$D^*=D\backslash\{0\}$上的函数$l(a)$如下：$l(a)=\begin{cases}0, & a\text{ 可逆},\\ s, & a=p_1p_2\cdots p_s,p_i\text{ 为素元数}.\end{cases}$

显然有下列性质：

若a与b相伴，则$l(a)=l(b)$.

若$a\mid b$，但$b\nmid a$，则$l(a)<l(b)$.

若$a\mid b$，则$l(a)=l(b)$当且仅当a,b相伴

其次$\boldsymbol{E}_{ij}$表示第i行，第j列处为1，其余元素为0的方阵，即$\operatorname{ent}_{kl}\left(\boldsymbol{E}_{ij}\right)=\delta_{ki}\delta_{lj}$再令

$$\boldsymbol{P}(i,j)=\boldsymbol{E}_{ij}+\boldsymbol{E}_{ji}+\sum_{k\neq i,j}\boldsymbol{E}_{kk},$$

$$\boldsymbol{P}(i(c))=c\boldsymbol{E}_{ii}+\sum_{k\neq i}\boldsymbol{E}_{kk},\quad c\text{ 为}D\text{ 的可逆元},$$

$$\boldsymbol{P}(j,i(k))=\boldsymbol{I}+k\boldsymbol{E}_{ji},\boldsymbol{I}\text{ 为单位矩阵}.$$

显然这三个矩阵都可逆，而用它们左乘（或右乘）某一矩阵就是把该矩阵作相应的初等行（或列）变换

Lemma 4.7

设D为$p.i.d$，且A是D上$m\times n$阶的矩阵

则A相抵于$\begin{pmatrix}B & O\\ O & O\end{pmatrix}$其中$B=\begin{pmatrix}d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_r\end{pmatrix}$且$d_i\mid d_{i+1}$且$d_i\neq 0$这些$d_i$称之为$A$的不变因子

Lemma 4.8

设D为$p.i.d$．M为秩m的自由D模，N是M的子模，则存在M的一组基$e_1,e_2,\cdots,e_m$及D中r个非零元素$d_1,d_2,\cdots,d_r$满足

1）$d_i\mid d_{i+1},1\leqslant i\leqslant r-1$

2）$d_1e_1,d_2e_2,\cdots,d_re_r$是$N$的一组基（此时也称$d_1,d_2,\cdots,d_r$为$N$的不变量）

Proof 任取M的一组基$e_1',e_2',\cdots,e_m'$及N的一生成组$f_1',f_2',\cdots,f_n'$．于是有D上$m\times n$矩阵$\boldsymbol{A}_1$，使得$f_j'=\left(e_1',e_2',\cdots,e_m'\right)\operatorname{col}_j\boldsymbol{A}_1$.

由知有m阶可逆矩阵$\boldsymbol{P}$,n阶可逆矩阵$\boldsymbol{Q}$，使$\boldsymbol{A}=\boldsymbol{P}\boldsymbol{A}_1\boldsymbol{Q}$为标准形，而$(e_1,e_2,\cdots,e_m)=\left(e_1',e_2',\cdots,e_m'\right)\boldsymbol{P}^{-1}$仍为$M$的基

令$(f_1,f_2,\cdots,f_n)=\left(f_1',f_2',\cdots,f_n'\right)\boldsymbol{Q}$仍为$N$的生成组.

但是

$$\begin{aligned}(f_1,f_2,\cdots,f_n)&=\left(e_1',e_2',\cdots,e_m'\right)\boldsymbol{A}_1\boldsymbol{Q}\\&=(e_1,e_2,\cdots,e_m)\boldsymbol{P}\boldsymbol{A}_1\boldsymbol{Q}\\&=(e_1,e_2,\cdots,e_m)\boldsymbol{A},\end{aligned}$$

即$f_i=d_ie_i,1\leqslant i\leqslant r,\quad f_i=0,i>r$,于是$d_1e_1,d_2e_2,\cdots,d_re_r$生成$N$.

显然由$e_1,e_2,\cdots,e_m$线性无关可得到$d_1e_1,d_2e_2,\quad\cdots,d_re_r$线性无关．故$d_1e_1,d_2e_2,\cdots,d_re_r$是$N$的基．

Theorem 4.20

设D为$p.i.d$，M'为D上有限生成模

则$M'=\bigoplus_{i=1}^{r}Dy_i\oplus\bigoplus_{i=r+1}^{m}Dy_i$且$anny_1\supseteq\cdots\supseteq anny_r$且$anny_{r+1}=\cdots=anny_m=\{0\}$

并且记$anny_1 \sim anny_r = \langle d_1 \rangle \sim \langle d_r \rangle$且$d_1, \cdots, d_r \neq 0$

Proof 设M'的一组生成组为$M' = \langle x_1 \cdots x_m \rangle$
构造D上的m秩自由模$M = \langle e_1' \cdots e_m' \rangle$由自由模泛性质知
存在模同态$\eta : M \to M'$使得$\eta(e_i') = x_i$这是个满同态故记作$N = \mathrm{Ker}\eta$
则有$M/N \cong M'$
设N的一组生成组为$N = \langle f_1' \cdots f_n' \rangle$
不妨设$(f_1' \cdots f_n') = (e_1' \cdots e_m') A^{m\times n}$
令$(e_1 \cdots e_m) = (e_1' \cdots e_m') P^{-1}$为$M$的一组新基
令$(f_1 \cdots f_n) = (f_1' \cdots f_n') Q$为$N$的一组新生成组
$\Longrightarrow (f_1 \cdots f_n) = (f_1' \cdots f_n') Q = (e_1' \cdots e_m') A^{m\times n} Q = (e_1 \cdots e_m) PAQ$
$\Longrightarrow f_1 = d_1 e_1 \cdots f_r = d_r e_r,\ f_{r+1} = \cdots = f_n = 0$
故N的一组基为$f_1 \cdots f_r$，$N = \langle f_1 \cdots f_r \rangle$

令$(y_1 \cdots y_m) = \eta(e_1 \cdots e_m) = \eta(e_1' \cdots e_m') P^{-1} = (x_1 \cdots x_m) P^{-1}$
因为η是满射且$e_1 \cdots e_m$是M的一组基故$y_1 \cdots y_m$为M'的一组生成组
$M' = \langle y_1 \cdots y_m \rangle = Dy_1 + \cdots + Dy_m$

下算零化子
当$1 \leqslant i \leqslant r$时，
$d_i y_i = d_i \eta(e_i) = \eta(d_i e_i) = \eta(f_i) \xlongequal{f_i \in N = \mathrm{Ker}\eta} 0 \Longrightarrow d_i \in anny_i \Longrightarrow \langle d_i \rangle \subseteq anny_i$
$\forall a \in anny_i \Longrightarrow ae_i \in N = \mathrm{Ker}\eta = \langle f_1 \cdots f_r \rangle = \langle d_1 e_1 \cdots d_r e_r \rangle \Longrightarrow ae_i = \sum_{j=1}^{r} b_j d_j e_j \Longrightarrow a = b_i d_i \Longrightarrow a \in \langle b_i \rangle$
故$anny_i = \langle d_i \rangle$
当$r+1 \leqslant i \leqslant m$时
$\forall a \in anny_i \Longrightarrow ae_i \in N = \mathrm{Ker}\eta = \langle f_1 \cdots f_r \rangle = \langle d_1 e_1 \cdots d_r e_r \rangle \Longrightarrow ae_i = \sum_{j=1}^{r} b_j d_j e_j \Longrightarrow a = 0$
故$anny_i = \{0\}$

再证直和，只需证明零向量分解唯一
若$\sum_{i=1}^{m} c_i y_i = 0$此时$\sum_{i=1}^{m} c_i y_i \in N = \mathrm{Ker}\eta = \langle d_1 e_1 \cdots d_r e_r \rangle$
$\Longrightarrow \sum_{i=1}^{m} c_i y_i = \sum_{j=1}^{r} l_j d_j e_j \Longrightarrow c_i = l_i d_i\ (1 \leqslant i \leqslant r)$且$c_i = 0\ (i \geqslant r+1)$
故每一项$c_i y_i$要么直接为零要么$c_i y_i = l_i d_i y_i \xlongequal{\langle d_i \rangle = anny_i} 0$故证毕

Corollary 4.8

$r(M/N) = r(M') = m - r = r(M) - r(N)$ ♡

Proposition 4.12

设D为$p.i.d$，A与B都是D上$m \times n$阶矩阵，若A与B相抵，则在相伴意义下A与B有相同的行列式因子

设D是$p.i.d$，$\boldsymbol{A}$是D上的$m \times n$矩阵
若$d_1, d_2, \cdots, d_r$是$\boldsymbol{A}$的不变因子．$D_k(\boldsymbol{A})$是$\boldsymbol{A}$的k级行列式因子，则有

1）$d_k \sim D_k(\boldsymbol{A})/D_{k-1}(\boldsymbol{A}), k=1,2,\cdots,r$

2）$d_1, d_2, \cdots, d_r$在相伴的意义下唯一

3）如果$\boldsymbol{B}$也是D上的$m\times n$矩阵，那么$\boldsymbol{B}$与$\boldsymbol{A}$等价当且仅当$\boldsymbol{A}$与$\boldsymbol{B}$有相同的不变因子，当且仅当$\boldsymbol{A}$与$\boldsymbol{B}$有相同的行列式因子.

第 5 章 域论

5.1 扩域的基本概念

Definition 5.1

只有有限个元素的域称为有限域或者为 Galois 域，显然对于素数 p，$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 为一个有限域

Definition 5.2

设F, E为域，称映射$\varphi : F \to E$为域同态，如果φ是一个环同态，即

$\varphi(\alpha+\beta) = \varphi(\alpha)+\varphi(\beta),\quad \varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta),\quad \alpha, \beta \in F$而且满足$\varphi(1_F) = 1_E$其中$1_F, 1_E$分别是$F, E$的乘法幺元

在不会混淆的情况下，我们省略下标. 域同态的全体记作 $\mathrm{Hom}(F, E)$

称域同态φ是域同构，如果φ是双射。如果$F = E$，则称φ为E的自同态

进一步，若φ还是同构，则称φ为自同构. 记 $\mathrm{Aut}(E)$为E的所有自同构的全体

注意到域同态的复合仍是域同态，即若$\varphi : F \to E, \psi : E \to K$都是域同态，则$\psi \circ \varphi : F \to K$也是域同态

特别地，容易验证 $\mathrm{Hom}(E, E)$是一个幺半群，而 $\mathrm{Aut}(E)$是一个群，称为E的自同构群.

Note 由环的同态基本定理，域同态$\varphi : F \to E$的核 $\mathrm{Ker}\varphi$是F的理想，故 $\mathrm{Ker}\varphi$只能为F和$\{0\}$

若 $\mathrm{Ker}\varphi = \{0\}$，必有$\varphi(1_F) = 1_E$

若 $\mathrm{Ker}\varphi = F$，则φ是个零映射，这是平凡的情况，因此我们在定义中增加了$\varphi(1_F) = 1_E$，排除了这种情形

Proposition 5.1

域同态$\varphi : F \to E$ 一定是单射.

Definition 5.3 (扩域与扩张)

设E是一个域，F是E的一个子集

若F在E的运算下也是一个域，则称F是E的子域，E为F的扩域或扩张，记作E/F

Definition 5.4 (素域)

容易验证，域E的任意多个子域的交仍是E的子域

特别地，域E的所有子域的交是E的唯一的最小子域

这个最小子域没有任何非平凡子域。我们称不包含任何非平凡子域的域为素域

Theorem 5.1 (素域分类)

1.$\mathbb{Z}_p$ (p为素数)，$\mathbb{Q}$有理数域都为素域

2.任取素域M都有$M \cong \mathbb{Z}_p$或者$M \cong \mathbb{Q}$

Proof 1.任取$\mathbb{Z}_p$的非零子域F，我们证明$F = \mathbb{Z}_p$即可说明$\mathbb{Z}_p$为素域

而F作为子域，自然作为加法的子群，故F的元素个数自然整除p，故F的元素个数要么为1，要么为零

为1即为 $\{0\}$ 与取法矛盾，故$F = \mathbb{Z}_p$

任取$\mathbb{Q}$的非零子域F，则F作为$\mathbb{Q}$的加法乘法子群至少含有 $\{0, 1\} \Longrightarrow$ 经过运算即可得到$\mathbb{Z} \subseteq F$

且F为域故ab^{-1} $(a \in \mathbb{Z}, b \in \mathbb{Z})$ 也在F中即$\mathbb{Z}$的分式域也在F中即$\mathbb{Q} \subseteq F \Longrightarrow F = \mathbb{Q}$

2.任取素域M，取e为幺元，构造$\mathbb{Z}e := \{ne | n \in \mathbb{Z}\}$ 显然$\mathbb{Z}e$为M的子环，且是整环 (交换与无零因子性继承M)

φ: $\mathbb{Z} \to \mathbb{Z}e \quad n \to ne$

那么$\mathbb{Z}/\mathrm{Ker}\varphi \cong \mathbb{Z}e$且$\mathrm{Ker}\varphi$为$\mathbb{Z}$的理想，因而$\mathrm{Ker}\varphi$为素理想才能得到$\mathbb{Z}e$为整环，且$\mathbb{Z}$为主理想整环

$\Longrightarrow \mathrm{Ker}\varphi = \langle p\rangle$ p为零或者素数

若p为素数，则$\mathbb{Z}_p \cong \mathbb{Z}e$则$M$中有一个子域$\mathbb{Z}e$由$M$的素域条件 $\Longrightarrow M = \mathbb{Z}e \cong \mathbb{Z}_p$

若p为零，则$\mathbb{Z}e \cong \mathbb{Z}$又$M$为域故$ab^{-1}$形式也在$M$中，故$\mathbb{Z}e$的分式域 $\cong \mathbb{Z}$的分式域 $= \mathbb{Q}$ 也在M中

故M中包含一个子域，其为$\mathbb{Z}e$的分式域，由M的素域条件知道$M = \mathbb{Z}e$的分式域 $\cong \mathbb{Z}$的分式域 $= \mathbb{Q}$

Definition 5.5

如果F包含的素域与$\mathbb{Q}$同构，则F的特征为零；如果F包含的素域与$\mathbb{F}_p$同构，则F的特征为p.

Note 对于任何域同态$\sigma : F \to E, \sigma$自然建立了F的素域与E的素域之间的同构，因此F与E具有相同的特征

特别地，不妨设F和E都是同一个素域Π上的扩张，由$\varphi(1) = 1$及Π是素域，我们有如下结论

设E和F都是素域Π的扩张，$\varphi : F \to E$为域同态，则对任意$a \in \Pi$有$\varphi(a) = a$，即 $\varphi|_\Pi = \mathrm{id}_\Pi$.

5.2 域的单扩张

Definition 5.6

域$F\subseteq$域K，S为K中一个集合，域F上添加S集合所生成的域即包含F又包含S的最小的域记为$F(S)$

Theorem 5.2 ($F(S)$ 的构造)

记$F[S]=\left\{\sum a_{i_1\cdots i_n}\alpha_1^{i_1}\cdots\alpha_n^{i_n}\mid n\in\mathbb{N},i_1\cdots i_n\text{为非零整数},\alpha_j\in S,a_{i_1\cdots i_n}\in F\right\}$

不妨记$\sum a_{i_1\cdots i_n}\alpha_1^{i_1}\cdots\alpha_n^{i_n}=f(\alpha_1\cdots\alpha_n)$　$F[S]$的分式域$=\left\{\dfrac{f(\alpha_1\cdots\alpha_n)}{g(\beta_1\cdots\beta_m)}\mid f(\alpha_1\cdots\alpha_n)\text{且}g(\beta_1\cdots\beta_m)\in F[S]\right\}$

$\Longrightarrow F(S)$是$F[S]$的分式域

Proof $F[S]$是整环显然所以能够构造分式域

一方面：$F(S)$又包含F又包含S则$f(\alpha_1\cdots\alpha_n)\in F(S)$且$g(\beta_1\cdots\beta_m)^{-1}\in F(S)\Longrightarrow\dfrac{f(\alpha_1\cdots\alpha_n)}{g(\beta_1\cdots\beta_m)}\in F(S)$

因此$F[S]$的分式域$\subseteq F(S)$

另一方面$F[S]$的分式域，包含F也包含S，而$F(S)$是包含F与S的最小的域故$F(S)\subseteq F[S]$的分式域

$\Longrightarrow F(S)$是$F[S]$的分式域

Proposition 5.2

设E为域F的扩域，$S\subset E$，则

（1）$F(S)=\bigcup\limits_{S'\subset S}F(S')$，其中$S'$取遍$S$的所有有限子集

（2）若$S=S_1\cup S_2$，则$F(S)=F(S_1)(S_2)=F(S_2)(S_1)$

Proof（1）显然对任何有限子集$S'\subset S$，有$F(S')\subseteq F(S)$. 故$\bigcup_{S'\subset S}F(S')\subseteq F(S)$

反之，对任意$a\in F(S)$，存在$f,g\in F[S],g\neq 0$，使得$a=fg^{-1}$

由于f,g的表达式都是有限和的形式，因此存在S的有限子集S'使得$f,g\in F[S']$。于是$a\in F(S')$. 故（1）成立

（2）只需证明$F(S)=F(S_1)(S_2)$. 由于域$F(S_1)(S_2)$包含F,S_1,S_2，而$F(S)$是E中包含F,S的最小子域，故$F(S)\subseteq F(S_1)(S_2)$

另一方面，$F(S_1)(S_2)$是包含$F(S_1),S_2$的最小子域，而域$F(S_1\cup S_2)$显然包含$F(S_1),S_2$，故$F(S_1)(S_2)\subseteq F(S_1\cup S_2)$

于是（2）成立

Corollary 5.1

$F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$.

Definition 5.7 (单扩张与单代数扩张与单超越扩张)

K为F的扩域，$\alpha\in K$则$F(\alpha)$就称为F的一个单扩张

若α为F上的代数元则称为F的单代数扩张，若α为F上的超越元则称为F的单超越扩张

Theorem 5.3 (单超越扩张结构 I)

K为F的扩域，$\alpha\in K$且为F上的超越元，则$F[\alpha]$即为F上的一元多项式环，

而我们知道$F[\alpha]$在同构意义下唯一，故$F(\alpha)$是$F[\alpha]$的分式域故在同构意义下也唯一

Lemma 5.1

Suppose α is a algebraic element over a field F. And $0 \neq p(x) \in F[x]$. Then we have the following three equivalent statements:

1. $p(x)$ is the minimal polynomial of α over F.
2. $p(\alpha) = 0$ and for any $g(x) \in F[x]$, if $g(\alpha) = 0$, then $p(x) \mid g(x)$.
3. $p(\alpha) = 0$ and $p(x)$ is irreducible in $F[x]$.

Proof 1.$\Longrightarrow$2. Suppose $g(\alpha) = 0$. By the division algorithm, we can write

$$g(x) = q(x)p(x) + r(x)$$

where $q(x), r(x) \in F[x]$ and either $r(x) = 0$ or $\deg(r) < \deg(p)$. Since $p(\alpha) = 0$ and $g(\alpha) = 0$, we have

$$0 = g(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha).$$

If $r(x) \neq 0$, then by the minimality of the degree of $p(x)$, we must have a contradiction. Therefore, $r(x) = 0$, which implies that $p(x) \mid g(x)$.

2.$\Longrightarrow$3. Suppose that for any $g(x) \in F[x]$, if $g(\alpha) = 0$, then $p(x) \mid g(x)$. Let us assume that there exist polynomials $f_1, f_2 \in F[x]$ such that $p = f_1 f_2$. Then $f_1(\alpha) f_2(\alpha) = p(\alpha) = 0$. Since F is a field, at least one of $f_1(\alpha)$ or $f_2(\alpha)$ must be zero. Without loss of generality, suppose $f_1(\alpha) = 0$. Then by our assumption, $p \mid f_1$, so there exists some polynomial h such that $f_1 = hp$. But then

$$p = f_1 f_2 = (hp) f_2 = h(p f_2),$$

which means that h is a unit in $F[x]$, i.e., it's a constant polynomial. This shows that one of the factors is a unit, hence p is irreducible.

3.$\Longrightarrow$1. Suppose $p(\alpha) = 0$ and $p(x)$ is irreducible in $F[x]$. Then$F[x](x) \subset Ker\varphi_\alpha \subsetneqq F[x]$.And because $p(x)$ is irreducible, we have $F[x]p(x)$ is the maximal ideal of $F[x]$.Thus $Ker\varphi_\alpha = F[x]p(x)$.Therefore, for any polynomial $g(x) \in F[x]$ such that $g(\alpha) = 0$, we have $g(x) \in Ker\varphi_\alpha$, which implies that $p(x) \mid g(x)$.This shows that $p(x)$ is the minimal polynomial of α over F.

Theorem 5.4 (单代数扩张的结构)

K为F的扩域，$\alpha \in K$且为F上的代数元 $\Longleftrightarrow F(\alpha) = F[\alpha]$

$$F(\alpha) = F[\alpha] = \left\{ f(\alpha) = \sum_{n=0}^{m} a_n \alpha^n \mid \ a_n \in F \right\}$$

Proof 考察F到K的嵌入映射f，则f可唯一的扩充到$F[x]$到K上的同态$\widetilde{f}$，且$\widetilde{f}_{F=}f$且$\widetilde{f}(x) = \alpha$

则$\widetilde{f}$将$F[x]$的多项式$g(x)$映为$g(\alpha) \in F[\alpha]$

故考察$\widetilde{f}$从$F[x]$到$F[\alpha]$的同态即为一个满同态

于是$\widetilde{f}/\mathrm{Ker}\widetilde{f} \cong F[\alpha]$又$\mathrm{Ker}\widetilde{f}$为$F[x]$上的一个理想，但是域上的一元多项式环是$ED$为$PID$

故可设$\mathrm{Ker}\widetilde{f} = \langle p(x) \rangle$故$\widetilde{f}/\langle p(x) \rangle \cong F[\alpha]$

此外由$F[\alpha]$为K的子环为整环，则$\langle p(x) \rangle$自然为$F[x]$上的素理想，该多项式为素元素也为不可约元素

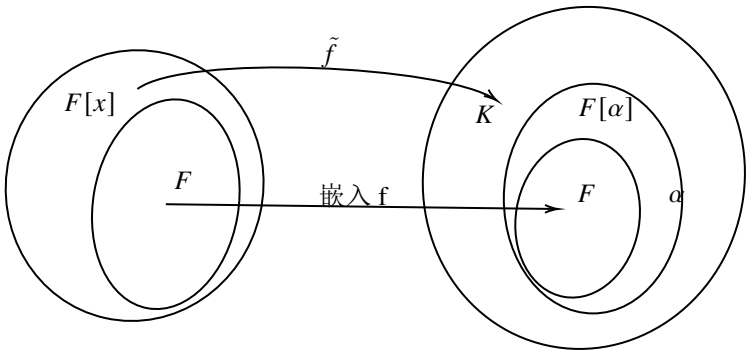
而$F[x]$为PID素理想因而等价与极大理想$\Longrightarrow \widetilde{f}/\langle p(x) \rangle \cong F[\alpha] \Longrightarrow F[\alpha]$为域

故则其分式域自然为自己故$F(\alpha) = F[\alpha]$

另一方面已知α为F上的代数元我们想要推出$F[\alpha] = F(\alpha)$一样的我们只需要说明$F[\alpha] = 0$

设α在F上的极小多项式为$\mathrm{Irr}(\alpha, F)$则由引理知道其为不可约多项式且由映射知道

$F[x]/\langle \mathrm{Irr}(\alpha, F) \rangle \cong F[\alpha]$而左边为域(模掉不可约生成的极大理想)，因此$F[\alpha]$为域



Corollary 5.2

1. $\langle p(x)\rangle = \mathrm{Ker}\tilde{f}$ 则 $\tilde{f}(p(x)) = p(\alpha) = 0$ 且 $p(x)$ 为 $F[x]$ 上的不可约多项式
$\Longrightarrow$ $p(x)$ 为 α 的零化多项式且设其首一
2. 这样的首一不可约零化多项式被 α 唯一确定，因为若 $p_1(\alpha) = p_2(\alpha) = 0$
且则 $(p_1(x), p_2(x)) \neq 1$ 又他们不可约 $\Longrightarrow$ $p_1 \sim p_2$ 又首一故 p_1, p_2
3. 则 $\forall\alpha$ 的零化多项式 $g(x)$，$g(x) \in \mathrm{Ker}\tilde{f} = \langle p(x)\rangle$ 故 $p(x)$ 是零化多项式次数最小的一个
故 $p(x)$ 为极小多项式

Definition 5.8 (极小多项式)

K 为 F 的扩域，$\alpha \in K$ 且为 F 的代数元，则 $F[x]$ 中以 α 为根的不可约首一多项式 $f(x)$
称为 $f(x)$ 为 α 在 F 上的极小多项式记作 $\mathrm{Irr}(\alpha, F)$，且极小多项式的次数就称为 α 在 F 上的次数记为 $\deg(\alpha, F)$

Lemma 5.2

E 为 F 的扩域，显然 E 是 F 上的线性空间

Theorem 5.5 (单代数扩张的结构 II)

设 $F(\alpha)$ 是域 F 的单代数扩张，且 $\deg(\alpha, F) = n$ 则 $F(\alpha)$ 是 F 上的 n 维线性空间，且 $1, \alpha\cdots\alpha^{n-1}$ 为一组基

Proof $F(\alpha) = F[\alpha] = \left\{\sum_{k=0}^{n} a_k\alpha^k \middle| n\text{为非负整数}, a_k \in F\right\}$
线性空间容易证明此时 $1, \alpha\cdots\alpha^{n-1}$ 为一组基
若 $1, \alpha\cdots\alpha^{n-1}$ 线性相关则存在不全为零的系数使得线性组合为零，则与 $\deg(\alpha, F) = n$
α 的极小多项式次数为 n 矛盾
再者，$\forall f(\alpha) = \sum_{k=0}^{n} a_k\alpha^k$ 其中 n 为非负整数，$a_k \in F$，记 $f(x) = \sum_{k=0}^{n} a_k x^k$
且 $f(x) = q(x)\,\mathrm{Irr}(\alpha, F) + r(x)$ 其中 $r(\alpha) = 0$ 或者 $\deg r(x) < \deg\mathrm{Irr}(\alpha, F) = n \Longrightarrow f(\alpha) = r(\alpha)$
故 $f(\alpha) = r(\alpha)$ 可以由 $1, \alpha\cdots\alpha^{n-1}$ 表出

Corollary 5.3

1. α 为 F 上的代数元，此时 $F(\alpha) = F[\alpha]$ 中的元素结构变为 $\sum_{k=0}^{n-1} a_k x^k$
2. 注意线性空间上的乘法与 $F(\alpha)$ 的乘法不一样！

Definition 5.9

设K_1与K_2都是F的扩域，且存在同构映射φ：$K_1 \to K_2$且$\varphi|_F = id_F$

称为K_1，K_2是F的等价扩张

Corollary 5.4

$F(\alpha), F(\beta)$是域F上的单超越扩张，则$F(\alpha) \cong F(\beta)$故是等价扩张

Proposition 5.3

设$F(\alpha), F(\beta)$是F的单代数扩张，且$\operatorname{Irr}(\alpha, F) = \operatorname{Irr}(\beta, F)$则$F(\alpha)$与$F(\beta)$是过$F$的等价扩张

Proof 记$n = \deg(\operatorname{Irr}(\alpha, F)) = \deg(\operatorname{Irr}(\beta, F))$

记$\varphi : F(\alpha) \to F(\beta)$ $\sum_{k=0}^{n-1} a_k \alpha^k \to \sum_{k=0}^{n-1} a_k \beta^k$

容易验证φ是$F(\alpha)$与$F(\beta)$作为F的线性空间的同构

还需验证φ是$F(\alpha)$与$F(\beta)$的域上的乘法保持这就需要用到 Irr 极小多项式相等

且$\forall a_0 \in F$有$\varphi(a_0) = \underbrace{\varphi\left(\sum_{k=0}^{n-1} a_k \alpha^k\right)}_{\text{其中}a_1 \cdots = 0} = \sum_{k=0}^{n-1} a_k \beta^k = a_0$故$\varphi|_F = id_F$

Corollary 5.5

1.单代数扩张$F(\alpha)$本质上在F等价扩张的意义下取决于$\operatorname{Irr}(\alpha, F)$

2.若$F(\alpha), F(\beta)$是F的等价的单代数扩张，是否$\operatorname{Irr}(\alpha, F) = \operatorname{Irr}(\beta, F)$

$\left(\mathbb{R}\sqrt{-1}\text{与}\mathbb{R}\left(1+\sqrt{-1}\right)\right)$

Definition 5.10

域K中子域F，F有两个扩张K_1与K_2且全都$\subseteq K$且K_1，K_2为过F等价则称K_1，K_2为共轭子域

$\alpha, \beta \in K$且α在F上的极小多项式$= \beta$在F上的极小多项式则称α，β为共轭元素

5.3 代数扩张与有限扩张

Definition 5.11 (代数扩张与有限扩张定义)

1.设K为域F的扩张，将K看成F上的线性空间

若 $\dim K = +\infty$则称K为F的无限扩张，反之则称为有限扩张且记扩张次数 $\dim K = [K:F]$

2.设K为域F的扩张，$\forall \alpha \in K$

若对于任取的α，α都是F上的代数元，则称K为F的代数扩张

若存在$\alpha \in K$，使得α是F上的超越元，则称K为F的超越扩张

Theorem 5.6

有限扩张一定是代数扩张

Proof 设K为域F的有限扩张，故不妨记作 $[K:F] = \dim K = n$，此时将K看成F上的线性空间

故此时$\forall \alpha \in K$有 $\{1, \alpha \cdots \alpha^n\}$ 这$n+1$个元素必定是线性相关的，故$\exists a_0 \sim a_n \in F$使得

$a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_n \cdot \alpha^n = 0$故$\alpha$为$F$上的代数元

Lemma 5.3

$$K\text{为域}F\text{的扩张} \Longrightarrow \begin{cases} \text{若}\alpha\text{是}F\text{上的代数元，则}F(\alpha)\text{是}F\text{的有限扩张} \\ \text{若}\alpha\text{是}F\text{上的超越元，则}F(\alpha)\text{是}F\text{的无限扩张} \end{cases}$$

Proof 利用单代数扩张的第二结构，我们得到$F(\alpha)$可看为F上的线性空间，其中一组基为 $\{1, \alpha \cdots \alpha^{n-1}\}$

其中$n = \deg(\alpha, F) = \deg \mathrm{Irr}(\alpha, F)$ 且n由α唯一确定

故$F(\alpha)$是F的有限扩张

若α是F上的超越元，且$F(\alpha)$是F的有限扩张，而有限扩张一定为代数扩张

则$\alpha \in F(\alpha)$一定为F上的代数元，矛盾

Corollary 5.6 (单扩张的代数扩张与有限扩张的关系)

下述三条等价$F(\alpha)$是F的代数扩张，α为F的代数元，$F(\alpha)$是F的有限扩张

Theorem 5.7 (二次有限扩张)

设有扩张链：$F \subseteq E \subseteq K$，则 $[K:F] < \infty \Longleftrightarrow [K:E] < \infty$且$[E:F] < \infty$

且当 $[K:F] < \infty$时，$[K:F] = [K:E] \times [E:F]$

$\Longrightarrow$ 得到有限扩张的有限扩张仍然为有限扩张

Proof 利用线性空间的知识

K看成E的线性空间有一组基 $\{\alpha_1 \cdots \alpha_s\}$，$E$看成$F$上的线性空间一组基为 $\{\beta_1 \cdots \beta_l\}$

则 $\{\alpha_i \beta_j\}$ 为K看成F上的线性空间的一组基，于是可证毕

Corollary 5.7

若域的扩张次数为素数，则两个域之间并无真正的中间域

Theorem 5.8 (有限扩张与单代数扩张升链)

设K为F的有限扩张，则存在单代数扩张链$F := F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r := K$

其中F_{i+1}对于F_i都是单代数扩张

反之，K对F有单代数扩张升列，则K是F的有限扩张进而为代数扩张

Proof 不妨设$K \neq F$否则平凡，故取$\alpha \in K - F$
且K为F的有限扩张一定为代数扩张故α为F上的代数元做$F_1 = F(\alpha)$
则$F := F_0 \subseteq F_1$且F_1为F_0的单代数扩张，且$[F_1 : F_0] > 1$,
以此类推讨论F_1是否相等于K，若$F_1 \neq K$,则取$\beta \in K - F_1$
β为F上的代数元，由$F \subseteq F_1$,故β也为F_1上的代数元故做$F_2 = F_1(\beta)$以此类推……
因为K对F是有限扩张，则$[K : F] = [F_r : F_{r-1}] \times \cdots \times [F_1 : F_0]$
且每一$[F_{i+1} : F_i] > 1$故这个步骤必将在有限步停止，存在单代数扩张链$F := F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r := K$
其中F_{i+1}对于F_i都是单代数扩张

反之K对F有单代数扩张升列，$F := F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r := K$
因为对于单扩张而言，代数扩张已经证明了等价于有限扩张，故也可看为有限扩张升链
故K对F为有限扩张的复合仍然为有限扩张

Theorem 5.9

设有扩张列$F \subseteq E \subseteq K$且每一层都为代数扩张，则$K$对$F$是代数扩张
$\Longrightarrow$ 代数扩张的代数扩张仍然为代数扩张

Proof $\forall \alpha \in K$，α为E上代数元设$\operatorname{Irr}(\alpha, E) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$其中$a_i \in E$
此时$\operatorname{Irr}(\alpha, E) \in F(a_0, a_1 \cdots a_{n-1})[x]$
此时$a_0 \in E$而E/F为代数扩张，a_0为F上的代数元故有单代数扩张$F \subseteq F(a_0)$
进一步$a_1 \in E \Longrightarrow a_1$为$F$上的代数元$\Longrightarrow a_1$为$F(a_0)$上的代数元……
故有单代数扩张列$F \subseteq F(a_0) \subseteq F(a_0)(a_1) \subseteq \cdots \subseteq F(a_0)(a_1)\cdots(a_{n-1}) \subseteq F(a_0, a_1 \cdots a_{n-1})(\alpha)$
最后一步是因为α在$F(a_0)(a_1)\cdots(a_{n-1})$中有多项式将其化零正是$\operatorname{Irr}(\alpha, E)$
则由有限扩张与单代数扩张列知道$F(a_0, a_1 \cdots a_{n-1})(\alpha)$对于$F$为代数扩张
$\Longrightarrow \alpha \in F(a_0, a_1 \cdots a_{n-1})(\alpha) \Longrightarrow \alpha$是$F$上的代数元
证毕

Definition 5.12

设有域扩张列$F \subseteq K$，并将K中所有是F上的代数元的元素集合叫做F在K中的代数闭包
1.若K为F的代数扩张，则自然$\bar{F} = K$

Theorem 5.10

设K为F的扩张，$\bar{F}$是F在K中的代数闭包
则$\bar{F}$是包含F又含于K的最大的代数扩张且$\forall \gamma \in K - \bar{F}$,$\gamma$是$\bar{F}$上的超越元

Proof 我们要说明$\bar{F}$是域，即加法构成$Abel$群，$\bar{F}\backslash\{0\}$构成乘法$Abel$群
而这些运算律都继承来源于域K，我们仅需要说明$\forall \alpha, \beta$使得$\alpha \pm \beta, \alpha\beta, \alpha\beta^{-1} \in \bar{F}$即可
$\alpha \in \bar{F}$则α是F上的代数元，则由单代数扩张$F \subseteq F(\alpha)$，再代数扩张$F \subseteq F(\alpha) \subseteq F(\alpha)(\beta)$
则$F(\alpha)(\beta)$关于F是代数扩张，而$\alpha \pm \beta, \alpha\beta, \alpha\beta^{-1} \in F(\alpha)(\beta)$
$\Longrightarrow \alpha \pm \beta, \alpha\beta, \alpha\beta^{-1}$是$F$上的代数元即$\alpha \pm \beta, \alpha\beta, \alpha\beta^{-1} \in \bar{F}$

此时$\forall \gamma \in K - \bar{F}$,$\gamma$是$F$上的超越元是显然的，这是由代数闭包的定义
但是我们要说明γ为$\bar{F}$上的超越元，若γ是$\bar{F}$上的代数元
则做单代数扩张$\bar{F} \subseteq \bar{F}(\gamma) \Longrightarrow$ 则$F \subseteq \bar{F} \subseteq \bar{F}(\gamma) \Longrightarrow \bar{F}(\gamma)$关于$F$为代数扩张
$\Longrightarrow \gamma \in \bar{F}(\gamma) \Longrightarrow \gamma$是$F$上的代数元$\Longrightarrow \gamma \in \bar{F}$与$\gamma$取法矛盾

5.4 分裂域

Definition 5.13

设$F[x]$是F域的一元多项式环，$f(x)\in F[x],\deg f(x)=n$. 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，$f(x)=c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$

2）$K=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，则称$K$是$f(x)$的分裂域

Lemma 5.4

设不可约多项式$p(x)\in F[x]$，则必定存在F的扩张E，使得$p(x)$在E中有根

Proof 若$p(x)$为$F[x]$上的常数即零次多项式，那么显然取$E=F$即可多项式为$x-c$类型

故不妨设非常数多项式$p(x)=\sum_{i=0}^{n}a_ix^i$其中$a_i\in F$

作自然映射$\pi:F[x]\longrightarrow F[x]/\langle p(x)\rangle$

考察$\pi|_F$这是一个单同态显然，则$F\cong\pi(F)\subseteq F[x]/\langle p(x)\rangle$

且因为$p(x)$为不可约多项式，则$\langle p(x)\rangle$为极大理想$F[x]/\langle p(x)\rangle$为域

故在同构下，只需在$F[x]/\langle p(x)\rangle$中找到一个元素，使得在$p(x)$下为0

考察$x+\langle p(x)\rangle$在$p(x)$下有$\sum_{i=0}^{n}a_i(x+\langle p(x)\rangle)^i=\sum_{i=0}^{n}a_ix^i+\langle p(x)\rangle=p(x)+\langle p(x)\rangle=\bar{0}$

故证毕

Corollary 5.8

设域F，设首一不可约多项式$f(x)$其根为$\alpha\in E/F$的扩张，此时$\mathrm{Irr}(\alpha,F)=f(x)$

$F[x]/f(x)\cong F(\alpha)$

Theorem 5.11

设$f(x)$是域F上的一元多项式且$\deg f(x)>0$，则$f(x)$的分裂域存在，且在f的分裂域中有f的n个根

Proof 对$\deg f(x)$用数学归纳法证明

当$\deg f(x)=1$时不妨设$f(x)=ax+b$其中$a,b\in F$，F本身就是$f(x)$的分裂域

且$f(x)$的根$-a^{-1}b\in F$

假设当$\deg f(x)=n-1$时结论成立

设$\deg f(x)=n>1,p(x)$是$f(x)$的一个不可约因子

由引理知有F的单代数扩张$F_1=F(\alpha_1)$，其中，α_1满足$p(\alpha_1)=0$，故$f(\alpha_1)=0$

$f(x)$作为$F_1[x]$内的多项式则有分解$f(x)=(x-\alpha_1)f_1(x),\quad\deg f_1(x)=\deg f(x)-1$

因而有$f_1(x)$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$K=F_1(\alpha_2,\alpha_3,\cdots,\alpha_n)=F(\alpha_1)(\alpha_2,\alpha_3,\cdots,\alpha_n)=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，故$K$是$f(x)$对$F$的分裂域

Corollary 5.9

1.设K是$f(x)\in F[x]$的分裂域且$\deg f(x)=n$，则$[K:F]\leqslant n!$

2.设K是$f(x)\in F[x]$的分裂域，又E是F与K的中间域，则K也是$f(x)\in E[x]$的分裂域.

Proof .事实上，$[K:F]=[F(\alpha_1,\cdots\alpha_n):F(\alpha_1\cdots\alpha_{n-1})]\times\cdots\times[F(\alpha_1):F]$

但是$[F(\alpha_1):F]$为$\deg\mathrm{Irr}(\alpha_1,F)$极小多项式的次数而这一定小于等于零化多项式的次数，

α_1在F上的一个零化多项式不就是$f(x)$，故$[F(\alpha_1):F]\leqslant n$

类似的$f(x)=(x-\alpha_1)f_1(x)$其中的$f_1(x)$就是α_2在$F(\alpha_1)$上的一个零化多项式

以此类推

2.事实上，若$K=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，则有$K=F(\alpha_1,\alpha_2,\cdots,\alpha_n)\subseteq E(\alpha_1,\alpha_2,\cdots,\alpha_n)\subseteq K$故$K=E(\alpha_1,\alpha_2,\cdots,\alpha_n)$.

Definition 5.14

设σ是环R_1到环R_2上的同构，又K_i是R_i的扩张，$i=1,2$.η是K_1到K_2上的同构且满足$\eta|_{R_1}=\sigma$，则称η是σ的开拓

特别地，若K_1,K_2都是域F的扩域，η是K_1到K_2上的F同构，则η是id_F的开拓.

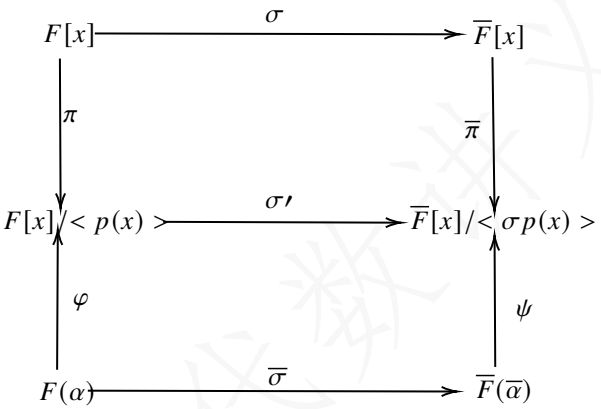
Lemma 5.5

设σ是F到$\bar{F}$上的域同构，则

1）σ可开拓为$F[x]$到$\bar{F}[x]$上的同构，仍记为σ,$p(x)\in F[x]$不可约当且仅当$\sigma p(x)\in\bar{F}[x]$不可约

2）又若$K,\bar{K}$分别为$F,\bar{F}$的扩域且$p(x)\in F[x]$不可约，而$\alpha\in K,\bar{\alpha}\in\bar{K}$分别为$p(x),\sigma p(x)$的根

则σ可开拓为$F(\alpha)$到$\bar{F}(\bar{\alpha})$上的同构$\bar{\sigma}$，使得$\bar{\sigma}(\alpha)=\bar{\alpha}$.



Proof 1）设$f(x)\in F[x]$且$f(x)=\sum_{i=0}^{n}a_ix^i$

令σ为由$\sigma(f(x))=\sum_{i=0}^{n}\sigma(a_i)x^i$定义的从$F[x]$到$\bar{F}[x]$的映射，由$\sigma$是$F$到$\bar{F}$上的同构，可直接验证开拓后的$\sigma$是$F[x]$到$\bar{F}[x]$上的同构

于是$p(x)\in F[x]$不可约当且仅当$\sigma p(x)\in\bar{F}[x]$不可约.

(2) 作如图的π与$\bar{\pi}$的自然映射

做$\sigma':F[x]/\langle p(x)\rangle\longrightarrow\bar{F}[x]/\langle\sigma p(x)\rangle\quad f(x)+\langle p(x)\rangle\mapsto\sigma f(x)+\langle\sigma p(x)\rangle$

容易验证σ'是合理定义的映射且为同态与单射，且在运算法则下容易验算上述图为交换图

故$\sigma'\pi=\bar{\pi}\sigma$因为$\sigma$是开拓到$F[x]$到$\bar{F}[x]$的同构自然为满射，自然映射$\bar{\pi}$自然为满射$\Longrightarrow\sigma'$为满射

故σ'为同构

且根据引理知道$F[x]/\langle p(x)\rangle\cong F(\alpha)\quad\bar{F}[x]/\langle\sigma p(x)\rangle\cong\bar{F}(\bar{\alpha})$

故令φ为$F(\alpha)$到$F[x]/\langle p(x)\rangle$的映射且ψ为$\bar{F}[x]/\langle\sigma p(x)\rangle$到$\bar{F}(\bar{\alpha})$的映射

于是令$\bar{\sigma}:=\psi\sigma'\varphi$显然这是一个同构映射

且容易验算$\bar{\sigma}(\alpha)=\bar{\alpha}$且$\bar{\sigma}|_F=\sigma$

Lemma 5.6

若$\varphi:F\to\bar{F}$的域同构，$F(\alpha)/F$是单代数扩张，记$p(x)=\mathrm{Irr}(\alpha,F)$，$\bar{p}(x)=\varphi(p(x))$

若$\bar{E}$为$\bar{F}$的扩张，且$\bar{p}(x)$在$\bar{E}$中分裂

则存在域同态$\psi:F(\alpha)\to\bar{E}$使得$\psi|_F=\varphi$且这样域同态的个数$\leqslant[F(\alpha):F]$等号成立当且仅当$p(x)$在E中无重根

Proof 由题易知$p(\alpha)=0\Longrightarrow\varphi(p(\alpha))=0\Longrightarrow\bar{p}(\varphi(\alpha))=0\Longrightarrow\varphi(\alpha)$为$\bar{p}(x)$的根

故根据上文的定理就知道φ可延拓为$F(\alpha)\to\bar{F}(\varphi(\alpha))$的同构进而可视为$\psi:F(\alpha)\to\bar{E}$使得$\psi|_F=\varphi$
此时这样的域同态个数$\leqslant \deg\bar{p}(x)=\deg p(x)=[F(\alpha):F]$

Theorem 5.12

设σ是域F到域$\bar{F}$上的同构．σ开拓为$F[x]$到$\bar{F}[x]$上的同构仍记为σ
又设$E,\bar{E}$分别为$f(x)\in F[x]$和$\sigma f(x)\in\bar{F}[x]$的分裂域
则σ可开拓为E到$\bar{E}$的同构．σ的不同开拓的个数$n_\sigma\leqslant[\bar{E}:\bar{F}]=[E:F]$
而且当且仅当$\sigma f(x)$中每一个不可约因子在$\bar{E}$中无重根时等号成立．

Proof 设$f(x)$在E中分裂为$(x-\alpha_1)\cdots(x-\alpha_n)$且$E=F(\alpha_1\cdots\alpha_n)$同理设$\sigma f(x)=(x-\bar{\alpha}_1)\cdots(x-\bar{\alpha}_n)$
记作$p_1(x)=\mathrm{Irr}(\alpha_1,F)$且$\bar{p}_1(x)=\sigma(p(x))$且$p_1(x)\mid f(x)$那么由引理知道
$\bar{p}_1(x)$为$\bar{F}[x]$上的不可约因式，且$\sigma(\alpha_1)$为$\bar{p}_1(x)$的根不妨设它为$\bar{\alpha}_1$
此时就有σ可延拓到$F(\alpha_1)$到$\bar{F}(\bar{\alpha}_1)$的同构，且这样的同构个数$\leqslant[F(\alpha_1):F]$
以此类推……
最终有σ可延拓到$F(\alpha_1\cdots\alpha_n)$到$\bar{F}(\bar{\alpha}_1\cdots\bar{\alpha}_n)$的同构即$E$与$\bar{E}$的同构
同构的开拓个数$\leqslant[F(\alpha_1):F]\cdot[F(\alpha_1)(\alpha_2):F(\alpha_1)]\cdots\cdots[F(\alpha_1\cdots\alpha_n):F(\alpha_1\cdots\alpha_{n-1})]=[E:F]$
等号成立当且仅当任何一个$\bar{p}_i(x)$在$\bar{E}$中无重根故等号成立当且仅当$\sigma f(x)$中每一个不可约因子在$\bar{E}$中无重根时等号成立．

Corollary 5.10

1.设F为域，$f(x)\in F[x],\deg f(x)>0$，则$f(x)$的任意两个分裂域E，$\bar{E}$是F同构的．
2.特别地，当E与$\bar{E}$都是F的同一扩域K的子域时，即$F\subseteq E\subseteq K$，$F\subseteq\bar{E}\subseteq K$，则$E=\bar{E}$
3.设K为域F的扩域，E是$f(x)\in F[x]$的分裂域且$E\subseteq K$，则对K的任意F自同构σ有$\sigma E=E$

Proof 在定理中取$F=\bar{F}$与$\sigma=\mathrm{id}_F$即得此推论的前一结论．至于后一结论，有
$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)\quad\alpha_i\in E\subseteq K,$
$f(x)=(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n)\quad\beta_i\in\bar{E}\subseteq K$
由于$x-\alpha_i,x-\beta_i\in K[x]$不可约因此在$K[x]$该$UFD$上有
$\exists\tau\in S_n$，使得$\alpha_i=\beta_{\tau(i)}$，故$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F\left(\beta_{\tau(1)},\beta_{\tau(2)},\cdots,\beta_{\tau(n)}\right)=\bar{E}$

证将σ在$K[x]$上的开拓仍记为σ.$f(x)$在$K[x]$中有分解$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),\quad\alpha_i\in E\subseteq K,$
于是由$f(x)\in F[x],\sigma|_F=\mathrm{id}_F$有$f(x)=\sigma f(x)=(x-\sigma(\alpha_1))(x-\sigma(\alpha_2))\cdots(x-\sigma(\alpha_n))$
因而$\exists\tau\in S_n$，使$\sigma(\alpha_i)=\alpha_{\tau(i)}$，所以$\sigma E=\sigma(F(\alpha_1,\alpha_2,\cdots,\alpha_n))=F\left(\sigma_{\tau(1)},\sigma_{\tau(2)},\cdots,\sigma_{\tau(n)}\right)=E$

5.5 正规扩张与可分多项式与完备域

Definition 5.15

域F的一个代数扩张K称为F的正规扩张

若$F[x]$中一个不可约多项式$p(x)$在K中有一个根，则$p(x)$在$K[x]$中可分解为一次因式之积

亦即若$p(x)$在K中有一个根，则$p(x)$的所有根都在K中.

Theorem 5.13

域F的有限扩张K为F的正规扩张 $\Longleftrightarrow$ K是$F[x]$中一个多项式的分裂域

Proof 必要性. 由K是F的有限扩张，故$\exists \alpha_1, \alpha_2, \cdots, \alpha_r \in K$，使得$K = F(\alpha_1, \alpha_2, \cdots, \alpha_r)$

令$f(x) = \operatorname{Irr}(\alpha_1, F) \operatorname{Irr}(\alpha_2, F) \cdots \operatorname{Irr}(\alpha_r, F)$ 由K是F的正规扩张，$\operatorname{Irr}(\alpha_i, F)$ 在K中有根α_i

故$f(x)$在$K[x]$中有分解$f(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_n)$ 而$E = F(\beta_1, \beta_2, \cdots, \beta_n)$ 为$f(x)$的分裂域

且$\alpha_1 \cdots \alpha_r \subseteq \{\beta_1 \cdots \beta_n\}$ 故$K = F(\alpha_1, \alpha_2, \cdots, \alpha_r) \subseteq F(\beta_1, \beta_2, \cdots, \beta_n) \subseteq K$

$\Longrightarrow F(\alpha_1, \alpha_2, \cdots, \alpha_r) = F(\beta_1, \beta_2, \cdots, \beta_n) \Longrightarrow$ 显然$E = K$，即K是$f(x)$的分裂域

充分性. 设K是$f(x) \in F[x]$的分裂域，自然$[K:F] < +\infty, K$是代数扩张

设$p(x) \in F[x]$不可约且$\exists \alpha \in K$，使$p(\alpha) = 0$

任取β为$p(x)$的一个根，要证$\beta \in K$

令E为$p(x) \in K[x]$的分裂域，因而$E \supseteq K \supseteq F$且$K(\alpha) = K$

令$g(x) = p(x)f(x) \in F[x]$ 于是E是$g(x) \in F[x]$的分裂域

那么根据分裂域同构定理由id_F可开拓为$K \to K$的自同构φ且$\varphi|_F = id_F$且$\varphi(\alpha) = \beta$

故根据推论我们知道$\varphi(K) = K$且$\alpha \in K \Longrightarrow \varphi(\alpha) = \beta \in K$

Proposition 5.4

1. $a' = 0, \forall a \in F$，而且当 $\operatorname{ch}F = 0$时有$f'(x) = 0 \Longleftrightarrow f(x) \in F$.
2. $x' = 1$
3. $(f(x) + g(x))' = f'(x) + g'(x)$.
4. $(cf(x))' = cf'(x), \forall c \in F$.
5. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$

Lemma 5.7

设K是$f(x) \in F[x]$的分裂域，$\alpha \in K$是$f(x)$的一个k重根.

1）若 $\operatorname{ch}F \nmid k$，则$\alpha$是$f'(x)$的$k-1$重根

2）若 $\operatorname{ch}F \mid k$，则$\alpha$是$f'(x)$的至少$k$重根

Proof 在$K[x]$中，$f(x)$有分解$f(x) = (x-\alpha)^k g(x), \quad g(\alpha) \neq 0$

于是由微商的性质有

$$f'(x) = k(x-\alpha)^{k-1} g(x) + (x-\alpha)^k g'(x)$$

$$= (x-\alpha)^{k-1}(kg(x) + (x-\alpha)g'(x))$$

当 $\operatorname{ch}F \nmid k$时，$k \neq 0$且$kg(\alpha) + (\alpha - \alpha)g'(\alpha) = kg(\alpha) \neq 0$，故$\alpha$是$f'(x)$的$k-1$重根

当 $\operatorname{ch}F \mid k$时，即$kg(x) = 0$有$f'(x) = (x-\alpha)^k g'(x)$，因而$\alpha$是$f'(x)$的至少$k$重根.

Theorem 5.14

设K是$f(x)\in F[x]$的分裂域，则$f(x)$在K中无重根的充分必要条件是$(f(x),f'(x))=1$

Proof 设$f(x)$在K中无重根，故有$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$其中，$n=\deg f(x)$
当$i\neq j$时，$\alpha_i\neq\alpha_j(1\leqslant i,j\leqslant n)$于是由定理知$\alpha_i$不是$f'(x)$的根，$i=1,2,\cdots,n$，故$(f(x),f'(x))=1$
反之，若$f(x)$在K中有重根α，设重数为$k(k>1)$．于是$f'(x)$至少有$k-1$重根α
因而在$K[x]$中有$(x-\alpha)^{k-1}\left|f'(x),(x-\alpha)^{k-1}\right|f(x)$。由此知$\deg(f(x),f'(x))\geqslant 1$，即$(f(x).f'(x))\neq 1$.

Corollary 5.11

设$p(x)$是$F[x]$中的不可约多项式，则$p(x)$在其分裂域K中有重根$\Longleftrightarrow p'(x)=0$

Proof 由定理知当且仅当$(p(x),p'(x))=d(x)\neq 1$时，$p(x)$在K中有重根，由于$p(x)$不可约，$d(x)\neq 1$
且$d(x)\mid p(x)$知$\deg d(x)=\deg p(x)$．又$\deg p'(x)<\deg p(x)$，$d(x)\mid p'(x)$,故$p'(x)=0$.

Corollary 5.12

若F的特征$\mathrm{ch}F=0$，则$F[x]$中任一不可约多项式在其分裂域中无重根

Proof 由$\mathrm{ch}F=0$得$F[x]$中不可约多项式$p(x)$满足$\deg p'(x)=\deg p(x)-1\geqslant 0$故$p'(x)\neq 0$
由推论知$p(x)$在其分裂域中只有单根.

Definition 5.16

设F是一个域，若$F[x]$中不可约多项式$p(x)$在其分裂域中只有单根则称$p(x)$为F上可分的不可约多项式
若$F[x]$中不可约多项式$f(x)$的每个不可约因式都是可分的，则称$f(x)$为F上可分多项式.

Corollary 5.13

1.$F[x]$中不可约多项式$p(x)$可分当且仅当$p'(x)\neq 0$
2.若$\mathrm{ch}F=0$，则$F[x]$的任何多项式$f(x)$都是可分的．因而只有在$\mathrm{ch}F=p>0$时，$F[x]$才可能有不可分多项式.

Lemma 5.8

设F的特征$chF=p>0,f(x)\in F[x]$为一不可约多项式
则$f(x)$不可分$\Longleftrightarrow$∃不可约多项式$g(x)\in F[x]$使得$f(x)=g(x^p)$

Proof 先证明充分性：设$g(x)=\sum_{i=0}^{n}a_ix^i$进一步$f(x)=\sum_{i=0}^{n}a_ix^{ip}$

$f'(x)=\sum_{i=0}^{n}ipa_ix^{ip-1}=0\Longrightarrow$且$f(x)$不可约$f(x)$不可分

再证明必要性：记$f(x)=\sum_{i=0}^{n}a_ix^i\Longrightarrow f'(x)=0\Longrightarrow\sum_{j=0}^{n}a_jjx^{j-1}=0$

要么$a_j=0$要么$a_j\neq 0$但有$p|j$

故只有$p|j$的那些j对应的a_j才有可能$\neq 0$即只有$a_0,a_p\cdots a_{mp}$可能$\neq 0$

$\Longrightarrow f(x)=\sum_{i=0}^{m}a_{ip}x^{ip}=\sum_{i=0}^{m}a_{ip}(x^p)^i$故令$g(x)=\sum_{i=0}^{m}a_{ip}x^i$即可

下说明$g(x)$不可约若$g(x)=g_1g_2\Longrightarrow f(x)=g_1(x^p)g_2(x^p)$矛盾

Theorem 5.15

设F的特征 $\mathrm{ch}F=p>0, f(x)$是$F[x]$中不可分不可约多项式，K是$f(x)$的分裂域

则在$K[x]$中$f(x)$有分解$f(x)=c\left(x-\alpha_1\right)^{p^e}\left(x-\alpha_2\right)^{p^e}\cdots\left(x-\alpha_r\right)^{p^e}$ 其中，当$i\neq j$时，$\alpha_i\neq\alpha_j, 1\leqslant i,j\leqslant r, e\in\mathrm{N}$

而且$h(x)=c\left(x-\alpha_1^{p^e}\right)\left(x-\alpha_2^{p^e}\right)\cdots\left(x-\alpha_r^{p^e}\right)$是$F[x]$中可分的不可约多项式，并有$f(x)=h\left(x^{p^e}\right)$.

Proof 因为$f(x)$为不可分不可约多项式，则由引理知道存在不可约的多项式$g_1(x)\in F[x]$使得$f(x)=g_1\left(x^p\right)$

若$g_1(x)$为可分的则我们就找到了所要证的$h(x)$

若$g_1(x)$是不可分的那么针对$g_1(x)$又可以用引理$g_1(x)=g_2\left(x^p\right)\Longrightarrow f(x)=g_2\left(x^{p^2}\right)$

上述过程导致了：$\deg f(x)>\deg g_1(x)>\deg g_2(x)>\cdots\cdots$无穷递降法知道这样的过程不可能无限下去

故存在一有限的正整数e使得$f(x)=h\left(x^{p^e}\right)$其中$h(x)$为$F[x]$上一可分的不可约多项式

因为$h(x)$可分，故$h(x)$在其分裂域K上可分解为$h(x)=c\left(x-\beta_1\right)\cdots\left(x-\beta_r\right)$其中$\beta_i\neq\beta_j\ (i\neq j)$

故$f(x)=c\left(x^{p^e}-\beta_1\right)\cdots\left(x^{p^e}-\beta_r\right)$取$x^{p^e}-\beta_1=0$的一个根$\alpha_1\cdots\cdots$

故$f(x)=c\left(x-\alpha_1\right)^{p^e}\left(x-\alpha_2\right)^{p^e}\cdots\left(x-\alpha_r\right)^{p^e}$，其中，当$i\neq j$时，$\alpha_i\neq\alpha_j, 1\leqslant i,j\leqslant r$

否则的话若$\alpha_i=\alpha_j\Longrightarrow\beta_i=\beta_j$矛盾

Definition 5.17

设F是一个域，若$F[x]$中每个多项式都是可分多项式，则称F是完备域

考虑完备域需要考察可分性即不可约因子在分裂域中是否无重根，故可以只考虑不可约多项式

从上述讨论知特征为0的域都是完备域，因而只需讨论特征 $\mathrm{ch}F=p>0$的域何时是完备域

Theorem 5.16

设F的特征 $\mathrm{ch}F=p>0$，则F是完备域$\Longleftrightarrow\forall a\in F,\exists b\in F$，使$a=b^p$。或者简记为$F^p=\{a^p\mid a\in F\}=F$

Proof 先证明充分性

设$F^p=F$，而$f(x)$为$F[x]$中不可分的不可约多项式，则由定理知

存在$F[x]$中可分的不可约多项式$h(x)$，使$f(x)=h\left(x^{p^e}\right)(e>1)$.

设$h(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_0$由$F^p=F$知$\exists a_i\in F$，使$a_i^{p^e}=b_i$，其中，$i=1,2,\cdots,m$

于是$f(x)=h\left(x^{p^e}\right)=\sum_{k=0}^{m}a_i^{p^e}\left(x^i\right)^{p^e}=\left(\sum_{k=0}^{m}a_ix^i\right)^{p^e}$ 这与$f(x)$的不可约性矛盾，由此知F是完备域.

在证明必要性

$\forall a\in F$要证明$\exists b\in F$使得$b^p=a$我们只需要说明$x^p-a=0$该方程有一个F中的根

$f(x)=x^p-a$且$f'(x)=0$ 此时若$f(x)$不可约且$f'(x)=0$则$f(x)$就为一不可分多项式

但是必要性条件已经知道F为完备域任何一多项式$f(x)$为可分多项式，矛盾

故$f(x)$可约，故设$f(x)=g(x)h(x)$其中$g(x),h(x)\in F[x]$，不妨设$\deg g(x)=0<r<p$

取$x^p-a=0$在$f(x)\in F[x]$的分裂域K上的一个根θ，即$a=\theta^p$

则$f(x)=x^p-\theta^p=(x-\theta)^p$又$g(x)h(x)=f(x)$

故$g(x)=(x-\theta)^r$且$g(x)\in F[x]\Longrightarrow\theta^r\in F$且$a=\theta^p\in F$

又$(r,p)=1\Longrightarrow ur+vp=1\Longrightarrow\theta^{ur+vp}=\theta\in F$证毕

Corollary 5.14

1.有限域是完备域

2.完备域的代数扩张也是完备域

Proof 1.设F为有限域，$\mathrm{ch}F=p>0$

作F到自身的映射$\sigma:\sigma(a)=a^p(\forall a\in F)$。显然$(ab)^p=a^pb^p(\forall a,b\in F)$

由 $\mathrm{ch}F = p > 0$，故 $(a+b)^p = a^p + b^p$，进而有$a^p = b^p \Longleftrightarrow a = b$
又F有限知σ是F的自同构，因而$\sigma(F) = F^p = F$，所以F是完备域.

2.若$chK = chF = 0$此时显然F与K都是完备域，不妨设$chK = chF = p > 0$
$\forall \alpha \in K$要证存在$\beta \in K$使得$\beta^p = \alpha$
设映射$\varphi : K \to K \quad a \mapsto a^p$容易证明$\varphi$为域同态且为单射　并且构造$E = F(\alpha)$
此时$\varphi|_E$刻画了同构$E \cong \varphi(E)$
下面我们就来证明$\varphi(E) = E$从而$\exists \beta \in E \subseteq K$使得$\beta^p = \alpha$从而证毕
$\varphi(E) = \varphi(F(\alpha)) = F(\alpha^p) \subseteq F(\alpha) = E$
进而得到$F \subseteq F(\alpha^p) = \varphi(E) \subseteq E$
故有 $[E:F] = [E:\varphi(E)]\,[\varphi(E):F]$
而 $[\varphi(E):\varphi(F)] = [\varphi(E):F] \Longrightarrow [E:\varphi(E)] = 1 \Longrightarrow \varphi(E) = E$

5.6 可分扩张

Definition 5.18 (可分扩张与可分元素)

1.设K是域F的扩域，$\alpha \in K$是F上的代数元．如果$\mathrm{Irr}(\alpha, F)$可分，那么称α是F上的可分元素

如果$\mathrm{Irr}(\alpha, F)$不可分，那么称α是F上的不可分元素

容易知道当且仅当$\mathrm{Irr}(\alpha, F)' \neq 0$时，$\alpha$是可分元素

2.设K是域F的代数扩张．如果K中每个元素都是F上的可分元素，那么称K是F的可分扩张，否则称为不可分扩张．

Proposition 5.5

1.完备域F的任何代数扩张K都是F的可分扩张

这是因为$\alpha \in K, \mathrm{Irr}(\alpha, F)$是$F[x]$上的不可约多项式，又由$F$为完备域知$\alpha$是$F$上的可分元素，故$K$是$F$的可分扩张

2.有限域F的任何代数扩张K都是可分扩张。因为有限域是完备域，故结论显然成立

3.若域F的特征为0，则F的任何代数扩张都是可分扩张

由特征为0的域是完备域即得．