Chapter 1

基本概念

1.1 二元运算与同余关系

1. 试问下列关系是否为等价关系?并验证.
   1) 在$\mathbf{R}$中, $x\,R\,y$, 若$x \geq y$;
   2) 在$\mathbf{R}$中, $x\,R\,y$, 若$|x| = |y|$;
   3) 在$\mathbf{R}$中, $x\,R\,y$, 若$|x - y| \leq 3$;
   4) 在$\mathbf{Z}$中, $x\,R\,y$, 若$x - y$为奇数;
   5) 在$\mathbf{C}_{n\times n}$(复数域$\mathbf{C}$上n阶方阵的集合)中,$A\,R\,B$,若有可逆矩阵P,Q使$A = PBQ$;
   6) 在$\mathbf{C}_{n\times n}$中,$A\,R\,B$,若有可逆矩阵P,Q使$A = PBQ$;
   7) 在$\mathbf{C}_{n\times n}$中,$A\,R\,B$,若有可逆矩阵P使$A = P^{-1}BP$.

   解 1) 不等价，不满足对称性.
   2) 是等价关系.
   a) $\forall x \in \mathbf{R}, |x| = |x|$.
   b) 若$|x| = |y|$,则$|y| = |x|$.
   c) 若$|x| = |y|, |y| = |z|$,则$|x| = |z|$.
   3) 不等价，不满足传递性.
   4) 不是等价关系.对$x \in \mathbf{Z}, x - x = 0$为偶数,则$x\,\overline{R}\,x$,$R$不满足自反性.
   5) 等价；自反性：$A = IAI$;对称性：若$A = PBQ$（p,Q可逆），则$B = P^{-1}AQ^{-1}$;传递性：若$A = P_1BQ_1, B = P_2CQ_2$,则$A = P_1P_2CQ_2Q_1$,即$A\,R\,C$.
   （事实上，这是矩阵秩的等价关系）.
   6) 不是等价关系.取$A = 0, B$为非零矩阵,则有$P = 0, Q$,使$A = PBQ = 0$,而不存在矩阵P,Q,使$B = PAQ$.不满足对称性.
   7) 等价.（这是高等代数中的相似关系）. ■

2. 假设R是非空集合A中的一个等价关系,且有对称性和传递性.有人断定R是一个等价关系.其推理如下:“对$a, b \in A$,从$a\,R\,b$得$b\,R\,a$.又从传递

性得$a\,R\,a$.因而R有自反性,故为等价关系."他的推理对吗?

解 不对.集合A的任意元素a都要满足自反性，如果上述关系中存在$a\in A$,对任意的$b\in A, a\,R\,b$不成立,则a无自反性. ■

3. 设R是非空集合A中的一个关系,再定义A中等价关系R_1, R_2分别为$x\,R_1\,y$,当$x=y, x\,R\,y$与$y\,R\,x$三者之一成立;
$x\,R_2\,y$,若有$x_0, x_1, \cdots, x_n$使
$x_0=x, x_n=y$,且$x_0\,R_1\,x_1, x_1\,R_1\,x_2, \cdots, x_{n-1}\,R_1\,x_n$.
1) 证明R_2是一个等价关系;
2) 证明若R是等价关系,则$R_2=R$,即$x\,R_2\,y$ iff $x\,R\,y$.
3) 令$A=\mathbf{Z}, n$为一固定整数.R定义为:$x\,R\,y$,当$x-y=n$.求关系R_1与R_2.

解 1) R_1有自反性，对称性.从而R_2有自反性，对称性.R_2的定义决定了R_2有传递性.故R_2是等价关系.
2) 若$x\,R\,y$,则$x\,R_1\,y, x\,R_2\,y$,若$x\,R_2\,y$,则有$x_0, x_1, \cdots, x_n$使得$x=x_0, x_n=y$且$x_0\,R_1\,x_1, x_1\,R_1\,x_2, \cdots, x_{n-1}\,R_1\,x_n$,由于$R$是等价关系，及$R_1$的定义知$x_0\,R\,x_1, x_1\,R\,x_2, \cdots, x_{n-1}\,R\,x_n$.从而$x_0\,R\,x_n$即$x\,R\,y$,所以$R_2=R$.
3) $x\,R_1\,y\Longleftrightarrow x-y=0, m, -m$.
$x\,R_2\,y\Longleftrightarrow x\equiv y(\mathrm{mod}m)$. ■

4. 试问下面的二元运算$*$哪些满足交换律，哪些满足结合律?
1) 在$\mathbf{Z}$中，$a*b=a-b$;
2) 在$\mathbf{Q}$中，$a*b=ab+1$;
3) 在$\mathbf{Q}$中，$a*b=ab/2$;
4) 在$\mathbf{N}$中，$a*b=2^{ab}$;
5) 在$\mathbf{N}$中，$a*b=a^b$.

解 1) 不满足结合律，不满足交换律.
2) a) $\because b*a=ba+1=a*b, \forall a,b\in\mathbf{Q}$.$\therefore$满足交换律. b) $(a*b)*c=(ab+1)*c=(ab+1)c+1, a*(b*c)=a*(bc+1)=a(bc+1)+1$,当$a\neq c$时，$(a*b)*c\neq a*(b*c)$,.$\therefore$不满足结合律.
3) a) $b*a=ba/2=a*b, \forall a,b\in\mathbf{Q}$.$\therefore$满足交换律；b) $(a*b)*c=ab/2*c=abc/4, a*(b*c)=a*bc/2=abc/4, \forall a,b,c\in\mathbf{Q}$,满足结合律.
4) a) $b*a=2^{ba}=a*b, \forall a,b\in\mathbf{N}$满足交换律；b) $(a*b)*c=2^{ab}*c=2^{2^{ab}c}, a*(b*c)=a*2^{bc}=2^{2^{bc}a}$,取$a=1, b=c=2$,则$(a*b)*c=2^8, a*(b*c)=2^{16}$,故$(a*b)*c\neq a*(b*c)$,所以不满足结合律.
5) 不满足交换律和结合律. ■

5. 设$m\in\mathbf{Z}, m\neq 0$. 在$\mathbf{Z}$中定义关系$\backsim$:
$a\backsim b$,若$a\equiv b(\mathrm{mod}\ \ m)$.
将$\mathbf{Z}$对此关系的商集合记为$\mathbf{Z}_m$(或$\mathbf{Z}/m\mathbf{Z}$).试求

1) $\mathbf{Z}_m$中元素个数;
2) 由$\mathbf{Z}$导出的$\mathbf{Z}_3$的加法和乘法;
3) 由$\mathbf{Z}$导出的$\mathbf{Z}_6$的加法和乘法.

解 易知，关系$\backsim$是等价关系且对于加法和乘法都是同余关系，$\mathbf{Z}_m$中共有m个元素，分别为$\overline{0},\overline{1},\overline{2},\cdots,\overline{m-2},\overline{m-1}$,在$\mathbf{Z}_3$中，有三个元素$\overline{0},\overline{1},\overline{2},\overline{0}+\overline{0}=\overline{0},\overline{0}+\overline{1}=\overline{1},\overline{0}+\overline{2}=\overline{2},\overline{1}+\overline{1}=\overline{2},\overline{1}+\overline{2}=\overline{0},\overline{2}+\overline{2}=\overline{1},\overline{0}\times\overline{0}=\overline{0},\overline{0}\times\overline{1}=\overline{0},\overline{0}\times\overline{2}=\overline{0},\overline{1}\times\overline{1}=\overline{1},\overline{1}\times\overline{2}=\overline{2},\overline{2}\times\overline{2}=\overline{2}$.
$\mathbf{Z}_m$中加法与乘法都有交换性.$\mathbf{Z}_6$中的加法与乘法.（略） ■

1.2 幺半群 群

1. 验证下列集合及所给的二元运算$*$是否合理.若合理，问哪些是半群，幺半群及群，或三种都不是?
   1) $\mathbf{Z}, a*b=ab$;
   2) $\mathbf{Z}, a*b=a-b$;
   3) $\mathbf{R}^+=\{x\in\mathbf{R}|x>0\}, a*b=ab$;
   4) $\mathbf{Q}-\{0,1\}, a*b=ab$;
   5) $[0,1], a*b=\delta_{1a}b+\delta_{1b}a-\delta_{1a}\delta_{1b}$.这里$\delta_{1a}=0$,若$a\neq 1\delta_{1a}=1$,若$a=1$,$\delta_{1b}$类似.
   6) $\mathbf{Z}, a*b=a+b-ab$.

   解 1) 二元运算定义合理，对此运算构成群.
   2) 二元运算定义合理，对此运算不构成半群.这是因为此运算不满足结合律.
   3) 二元运算定义合理，对此二元运算构成群.
   4) 不合理.$\because 2,0.5\in\mathbf{Q}, 2*0.5=1\in\mathbf{Q}, \therefore$二元运算不合理;
   5) 合理.$\because a*b=0, a\neq 1, b\neq 1; a*b=1, a=1=b; a*b=a, a\neq 1, b=1; a*b=b, a=1, b\neq 1. \therefore$ 满足封闭律，而$(a*b)*c\neq a*(b*c), \therefore$不满足结合律，$\therefore$三种都不是.
   6) 合理.$\because \mathbf{Z}$对$*$有封闭性，

   $$(a*b)*c=(a+b-ab)*c=a+b-ab+c-c(a+b-ab)=a+b+c-ca-bc+abc,$$

   $$a*(b*c)=a*(b+c-bc)=a+b+c-bc-a(b+c-bc)=a+b+c-ab-bc-ac+abc.$$

   $\therefore$满足结合律.$\forall c\in\mathbf{Z}, 0*c=0+c-0c=c, \therefore 0$是左幺元,同理,0是右幺元,所以$c$是幺元,
   $\forall d\in\mathbf{Z}, d*1=d+1-d1=1\neq 0, \therefore 1$没有幺元,所以$\mathbf{Z}$是幺半群 ■

2. 在$\mathbf{Z}\times\mathbf{Z}$中定义乘法为
   $(x_1,x_2)(y_1,y_2)=(x_1y_1+2x_2y_2, x_1y_2+x_2y_1)$. 证明:

1) $\mathbf{Z}\times\mathbf{Z}$对此乘法为交换幺半群.
2) 当$(x_1,x_2)\neq(0,0)$时，则由$(x_1,x_2)(y_1,y_2)=(x_1,x_2)(z_1,z_2)$可得$(y_1,y_2)=(z_1,z_2)$.

证明 1) 显然，此二元运算定义合理.
$((x_1,x_2)(y_1,y_2))(z_1,z_2)=(x_1y_1+2x_2y_2,x_1y_2+x_2y_1)(z_1,z_2)=(x_1y_1z_1+2(x_2y_2z_1+y_2z_2x_1+z_2x_2y_1),x_1y_1z_2+y_1z_1x_2+z_1x_1y_2+2x_2y_2z_2)=(x_1,x_2)((y_1,y_2(z_1,z_2)$
二元运算满足结合律.
$x_1,x_2)(y_1,y_2)=(y_1,y_2)(x_1,x_2)$
二元运算满足交换律.
$(1,0)(x_1,x_2)=(x_1,x_2)=(x_1,x_2)(1,0)$.
故$(1,0)$为此交换半群幺元.$\mathbf{Z}\times\mathbf{Z}$对此乘法为交换幺半群. 2) $\because$
$(x_1,x_2)(y_1,y_2)=(x_1,x_2)(z_1,z_2)$,
$\therefore x_1(y_1-z_1)+2x_2(y_2-z_2)=0,x_1(y_2-z_2)+x_2(y_1-z_1)=0$,
$\because(x_1,x_2)\neq(0,0)$,
$\therefore y_1-z_1=0,y_2-z_2=0$.
$\therefore(y_1,y_2)=(z_1,z_2)$. ■

3. 在$\mathbf{S}=\{x|x\in\mathbf{R},x\neq-1\}$中定义运算“$*$”为$a*b=a+b+ab$.试证$\mathbf{S}$对$*$是一个群.并求方程$2*x*3=7$的解.

证明

(a) $\because a\neq-1$且$b\neq1$时,$a*b\neq-1,\therefore S$对$*$有封闭律;

(b) $(a*b)*c=(a+b+ab)*c=a+b+ab+c+ac+bc+abc$
$a*(b*c)=a*(b+c+bc)=a+b+c+ab+ac+bc+abc$
所以满足结合律;

(c) $\forall c\in S,0*c=c$,0为左幺元;

(d) $\forall d\in S,\dfrac{-d}{d+1}\neq-1$为$d$的左逆元.

所以S对$*$是一个群.
$2*x*3=(2+x+2x)*3=12x+11=7,\therefore x=-\frac{1}{3}$ ■

4. 证明若有限半群$\mathbf{G}$满足消去律，即
$ax=ay\Longrightarrow x=y;xa=ya\Longrightarrow x=y$，则$\mathbf{G}$为群.
此结论对无限半群成立吗?

证明 引理：若半群G满足$\forall a,b\in G$,方程$xa=b,ax=b$均有解，则G为群.
引理的证明：$xa=a$有解，记为e_a,则$e_aa=a$,对任意$c\in G,ax=c$有

解，记为d,则$ad=c$,则$e_ac=e_a(ad)=ad=c$,$\therefore$ G存在幺元；$\forall f\in G, xf=e_a$有解，x为f的左逆元.综上，G是群.
$\forall a\in G,\because ax=ay\Leftrightarrow x=y$,且$|G|$有限知$aG=G$,从而$\forall a,b\in G, ax=b$有解，同理$xa=b$有解.从而命题得证.
此结论对无限半群不成立，反例$\{\mathbf{N},+\}$. ■

5. 如果在半群$\mathbf{G}$中还有一个“一元运算”（即$\mathbf{G}$到$\mathbf{G}$的一个映射：$a\longrightarrow a'$），且满足
$a'(ab)=(ba)a', \forall a,b\in\mathbf{G}$.
证明此半群必为群.

证明 $\forall a,b,c\in G, a'ac=c=b'bc$,再利用题目条件可得$a'a=a'acc'=b'bc'=b'b$.令$e=a'a$, 则$e$为$G$得左幺元，$a'$为$a$得左逆元.
$\therefore$ G是群. ■

6. 如果半群$\mathbf{G}$有左幺元e，对$\forall a\in\mathbf{G}$，有右逆元（即有$a'\in\mathbf{G}$使$aa'=e$）.问$\mathbf{G}$一定是群吗？

解 不一定是群.反例：
$G=\left\{\begin{pmatrix}1&1\\0&0\end{pmatrix},\begin{pmatrix}1&-1\\0&0\end{pmatrix},\begin{pmatrix}-1&-1\\0&0\end{pmatrix},\begin{pmatrix}-1&1\\0&0\end{pmatrix}\right\}$
易知G是半群.左幺元为$\begin{pmatrix}1&1\\0&0\end{pmatrix}$,
$\begin{pmatrix}1&1\\0&0\end{pmatrix}$的右逆元是$\begin{pmatrix}1&1\\0&0\end{pmatrix}$,
$\begin{pmatrix}1&-1\\0&0\end{pmatrix}$的右逆元是$\begin{pmatrix}1&1\\0&0\end{pmatrix}$,
$\begin{pmatrix}-1&-1\\0&0\end{pmatrix}$的右逆元是$\begin{pmatrix}-1&-1\\0&0\end{pmatrix}$,
$\begin{pmatrix}-1&1\\0&0\end{pmatrix}$的右逆元是$\begin{pmatrix}-1&-1\\0&0\end{pmatrix}$ ■

7. 设$P(X)$为非空集合X的幂集（即X的所有子集的集合）.
1) 试证$P(X)$对于对称差$\triangleleft(A\triangleleft B=(A-B)\cup(B-A), \forall A,B\in P(X))$构成一个群；每个非幺元的阶为2.
2) 试求$P(X)$的阶.

证明 1) 封闭性显然.
$(A\triangle B)\triangle C=A\triangle(B\triangle C)$,左幺元是$\varnothing$,左逆元$A^{-1}=A$,$A\triangle A=\varnothing$,所以阶为2.
2) $|P(X)|=2^{|X|}$. ■

8. 设群$\mathbf{G}$中每个非幺元的阶为2.试证$\mathbf{G}$为Abel群.

证明 $\forall a,b\in\mathbf{G},a^2=b^2=e,(ab)(ab)=e=a^2$由消去律知$bab=a,\therefore$. $b(bab)=ba$由$b^2=e$知$ab=ba,\therefore$. G为Abel群. ■

9. 确定$\mathbf{S}_5$中元素$\sigma\tau,\sigma^{-1}\tau\sigma,\sigma^2,\sigma^3$.其中
$\sigma=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix},\tau=\begin{pmatrix}1&2&3&4&5\\3&4&1&5&2\end{pmatrix}$.

解

$$\sigma\tau=\begin{pmatrix}1&2&3&4&5\\1&5&2&4&3\end{pmatrix},\sigma^{-1}\tau\sigma=\begin{pmatrix}1&2&3&4&5\\5&3&2&1&4\end{pmatrix}$$
$$\sigma^2=\begin{pmatrix}1&2&3&4&5\\3&1&2&4&5\end{pmatrix},\sigma^3=\begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix}$$

■

10. 列出$\mathbf{S}_3$的群表.

解 设$X=\{a,b,c\},\mathbf{S}_3=\{\tau_1,\tau_2,\tau_3,\tau_4,\tau_5,\tau_6\},\tau_1=\begin{pmatrix}a&b&c\\a&b&c\end{pmatrix},\tau_2=\begin{pmatrix}a&b&c\\a&c&b\end{pmatrix},\tau_3=\begin{pmatrix}a&b&c\\b&a&c\end{pmatrix},\tau_4=\begin{pmatrix}a&b&c\\b&c&a\end{pmatrix},\tau_5=\begin{pmatrix}a&b&c\\c&a&b\end{pmatrix},\tau_6=\begin{pmatrix}a&b&c\\c&b&a\end{pmatrix}$,

群表为:

$\cdot$	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6
τ_1	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6
τ_2	τ_2	τ_1	τ_5	τ_6	τ_3	τ_4
τ_3	τ_3	τ_4	τ_1	τ_2	τ_6	τ_5
τ_4	τ_4	τ_3	τ_6	τ_5	τ_1	τ_2
τ_5	τ_5	τ_6	τ_2	τ_1	τ_4	τ_3
τ_6	τ_6	τ_5	τ_4	τ_3	τ_2	τ_1

■

11. $\mathbf{N}$的所有变换组成的幺半群$\mathbf{M}(\mathbf{N})$中元素f定义为:
$f(n)=n+1,\forall n\in\mathbf{N}$
证明f有无穷多个左逆元，但无右逆元.

证明 令$g_k(n)=n-1,n\geq 2;g_k(1)=k,k\in\mathbf{N}$,则$\forall k,g_k$都是$f$的左逆元，假设$h$是$f$的右逆元，则$fh(1)=h(1)+1,\because h(1)\geq 1,\therefore fh(1)\geq 2$,与$fh(1)=1$矛盾.从而命题得证. ■

12. 设$\mathbf{M}$为幺半群，$m\in\mathbf{M}$.在$\mathbf{M}$中定义乘法“$*$”：$a*b=amb$. 1) 试证$\mathbf{M}$对$*$为半群. 2) 试问在什么情况下，$\mathbf{M}$对$*$为幺半群?

证明 1) 封闭性显然.
$(a*b)*c=ambmc=a*(b*c)$,故M对$*$为半群.
2) m可逆时. ■

1.3 子群与商群

1. 设$\mathbf{H}$是群$\mathbf{G}$的子群.证明$\{\mathbf{H}a\}$是$\mathbf{G}$的分划，且对应的等价关系$\mathbf{R}_1$为$a\,\mathbf{R}_1\,b$,当$ba^{-1}\in\mathbf{H}$.

   证明 首先证明R_1是等价关系.
   $e=aa^{-1}\in H\Rightarrow aR_1a,\forall a\in G$,又设$aR_1b$,则$ab^{-1}\in H$,故$ba^{-1}=(a^{-1}b)^{-1}\in H$,即$bR_1a$,再设$aR_1b,bR_1c$即$ab^{-1},bc^{-1}\in H$,故$ac^{-1}=(ab^{-1})(bc_{-1})\in H$,即$aR_1c$.
   所以R_1是等价关系.
   又由$aR_1b\Leftrightarrow ba^{-1}\in H\Leftrightarrow b\in aH$
   故b所在的等价类为aH.从而知$\{aH\}$为G的一个分划. ■

2. 设$\mathbf{H}$是$\mathbf{Z}$的一个子群.证明必有非负整数m使$\mathbf{H}=m\mathbf{Z}$.
   证明 令$m=\min\{|n||n\in H,n\neq 0\}$,若有$mz_0+r\in H,0\leq r<m,r\in N,\because mz_0\in H$,知$r\in H$,由$m$的定义知$r=0$,从而$H=m\mathbf{Z}$. ■

3. 写出$\mathbf{S}_3$的全部子群及其左右陪集.并指出哪些子群是正规子群.
   解 设$X=\{a,b,c\},\mathbf{S}_3=\{\tau_1,\tau_2,\tau_3,\tau_4,\tau_5,\tau_6\},\tau_1=\begin{pmatrix}a&b&c\\a&b&c\end{pmatrix},\tau_2=\begin{pmatrix}a&b&c\\a&c&b\end{pmatrix},\tau_3=\begin{pmatrix}a&b&c\\b&a&c\end{pmatrix},\tau_4=\begin{pmatrix}a&b&c\\b&c&a\end{pmatrix},\tau_5=\begin{pmatrix}a&b&c\\c&a&b\end{pmatrix},\tau_6=\begin{pmatrix}a&b&c\\c&b&a\end{pmatrix}$
   $H_1=\{\tau_1\},H_2=\{\tau_1,\tau_2\},H_3=\{\tau_1,\tau_3\},H_4=\{\tau_1,\tau_6\},H_5=\{\tau_1,\tau_4,\tau_5\}$,
   $H_6=\{\tau_1,\tau_2,\tau_3,\tau_4,\tau_5,\tau_6\}$
   $\therefore H_1,H_2,H_3,H_4,H_5,H_6$是$\mathbf{S}_3$的全部子群，其中$H_1,H_5,H_6$是正规子群. ■

4. 设$\mathbf{H}$是群$\mathbf{G}$的子群，且$[\mathbf{G}:\mathbf{H}]=2$.试证$\mathbf{H}\lhd\mathbf{G}$.
   证明 $\because[G:H]=2,\therefore,\exists a\in G$,且$a^{-1}\in H$,使$G=eH\cup aH$且$eH\neq aH$
   $\forall h,g\in H$,有$ghg^{-1}\in H$
   $\forall h\in H,g\in aH,\exists h_1\in H$,使$g=ah_1,ghg^{-1}=ah_1hh_1^{-1}a^{-1}$
   $\because ghg^{-1}\in G$.若$ghg^{-1}\in H$,则必有$ghg^{-1}\in aH$,从而$\exists h_2\in H$,使$ghg^{-1}=ah_2$即$ah_1hh_1^{-1}a^{-1}=ah_2$，
   由消去律有$h_1hh_1^{-1}=h_2\Rightarrow h_2^{-1}h_1hh_1^{-1}=a\Rightarrow a\in H$.
   $\because H$是G的子群,$\therefore a^{-1}\in H$与前提$a^{-1}\in H$矛盾
   $\therefore ghg^{-1}\in H$,即对$\forall h\in H,g\in G,ghg^{-1}$成立.
   $\therefore H\lhd G$. ■

5. 设$\mathbf{H}_1,\mathbf{H}_2$是群$\mathbf{G}$的两个有限子群.证明
   $|\mathbf{H}_1\mathbf{H}_2|=[\mathbf{H}_1:1][\mathbf{H}_2:1]/[\mathbf{H}_1\cap\mathbf{H}_2:1]$.

证明 考虑左陪集$aH_2, a \in H_1$,则$\{aH_2\}$是H_1H_2的一个分划.
1) 若有$aH_2 = bH_2, a, b \in H_1$,则有$ab^{-1} \in H_2$,从而$ab^{-1} \in H_1 \cap H_2, b \in a(H_1 \cap H_2)$.
2) $\forall b \in a(H_1 \cap H_2)$,有$aH_2 = bH_2$,
$\therefore |H_1H_2| = [H_1 : 1][H_2 : 1]/[H_1 \cap H_2 : 1]$ ■

6. 设$\mathbf{G}$为Abel群，$n \in \mathbf{N}$.试证$\{g \in \mathbf{G} | g^n = 1\}$是$\mathbf{G}$的子群.
证明 令$H = \{g \in G | g^n = 1\}, \forall g_1, g_2 \in H, (g_1g_2^{-1})^n = g_1^n(g_2^n)^{-1} = e, \therefore H < G$ ■

7. 证明群$\mathbf{G}$不能写成两个真子群的并.
证明 若有$H_1 < G, H_2 < G, H_1 \neq G, H_2 \neq G, H_1 \cup H_2 = G$,取$a \in H_1, b \in H_2$,且$a \in H_2, b \in H_1$,则$ab \in H_1, ab \in H_2$, 从而$ab \in G$,矛盾！ ■

8. 设设$\mathbf{H}, \mathbf{K}$是群$\mathbf{G}$的两个正规子群，且$\mathbf{H} \cap \mathbf{K} = \{1\}$.试证$hk = kh, \forall h \in \mathbf{H}, k \in \mathbf{K}$.
证明 $\because (kh)^{-1}hk = h^{-1}k^{-1}hk, h^{-1}k^{-1}h \in K, \forall h \in H, k \in K$,故$(kh)^{-1}hk \in K, \because k^{-1}hk \in H, \therefore h^{-1}k^{-1}hk \in H, \because H \cap K = \{1\}, \therefore (kh)^{-1}hk = 1, \therefore kh = hk.$ ■

9. 设$\mathbf{H}$是群$\mathbf{G}$的正规子群.证明$\mathbf{G}/\mathbf{H}$是Abel群的充要条件是$gkg^{-1}k^{-1} \in \mathbf{H}, \forall g, k \in \mathbf{G}$.
证明 G/H是Abel群$\iff gHkH = kHgH \iff gkH = kgH \iff gk(kg)^{-1} = gkg^{-1}k^{-1} \in H$ ■

10. 设$\mathbf{H}, \mathbf{K}$是二群.在$\mathbf{H} \times \mathbf{K} = \{(h, k) | h \in \mathbf{H}, k \in \mathbf{K}\}$中定义乘法为$(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$.试证：
1) $\mathbf{H} \times \mathbf{K}$是一个群（称为$\mathbf{H}$与$\mathbf{K}$的**外直积**）.
2) $\mathbf{H}_1 = \{(h, 1') | h \in \mathbf{H}, 1'$为$\mathbf{K}$的幺元$\}$和$\mathbf{K}_1 = \{(1, k) | k \in \mathbf{H}, 1$为$\mathbf{H}$的幺元$\}$为$\mathbf{H} \times \mathbf{K}$的正规子群.
3) $\mathbf{H}_1 \cap \mathbf{K}_1 = \{(1, 1')\}; \mathbf{H} \times \mathbf{K} = \mathbf{H}_1\mathbf{K}_1$.（$\mathbf{H} \times \mathbf{K}$称为$\mathbf{H}_1$与$\mathbf{K}_1$的**内直积**.）
证明 1) 设e_h为H的幺元，e_k是K的幺元，则$(e_h, e_k) \in \mathbf{H} \times \mathbf{K}$
$\therefore \mathbf{H} \times \mathbf{K}$是非空集合，
$\forall (h_1, k_1), (h_2, k_2) \in \mathbf{H} \times \mathbf{K}, (h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2) \in \mathbf{H} \times \mathbf{K}$,
$\therefore \mathbf{H} \times \mathbf{K}$对乘法有封闭律；
$\forall (h_1, k_1), (h_2, k_2), (h_3, k_3) \in \mathbf{H} \times \mathbf{K}, ((h_1, k_1)(h_2, k_2))(h_3, k_3) = (h_1h_2, k_1k_2)(h_3, k_3) = (h_1h_2h_3, k_1k_2k_3) = (h_1, k_1)((h_2, k_2)(h_3, k_3)) = (h_1, k_1)((h_2, k_2)(h_3, k_3))$
$\therefore \mathbf{H} \times \mathbf{K}$对乘法有结合律
$\forall (h, k) \in \mathbf{H} \times \mathbf{K}, (e_h, e_k)(h, k) = (h, k)$,
$\therefore (e_h, e_k)$是左幺元；

$\forall (h,k)\in \mathbf{H}\times\mathbf{K}, (h^{-1},k^{-1})(h,k)=(e_h,e_k)$,
$\therefore (h^{-1},k^{-1})\in \mathbf{H}\times\mathbf{K}$为左逆元
$\therefore \mathbf{H}\times\mathbf{K}$是一个群.
2) $\because (e_h,1')\in H_1, \therefore H_1$是$\mathbf{H}\times\mathbf{K}$的非空子集.$\forall (h_1,1')\in H_1,(h_2,1')\in H_1,(h_1,1')(h_2,1')^{-1}=(h_1,1')(h_2^{-1},1')=(h_1h_2^{-1},1')\in H_1$,
$\therefore H_1$是$\mathbf{H}\times\mathbf{K}$的子群;
$\forall (h_1,1')\in H_1,(h,k)\in \mathbf{H}\times\mathbf{K}$
$(h,k)(h_1,1')(h,k)^{-1}=(hh_1h^{-1},kk^{-1})=(hh_1h^{-1},1')\in H_1,\therefore$ H_1是$\mathbf{H}\times\mathbf{K}$的正规子群;
同理可证K_1是$\mathbf{H}\times\mathbf{K}$的正规子群.
3) 设$(h,k)\in H_1$且$(h,k)\in K_1$,则$k=1',h=1,\therefore H_1\cap K_1=\{(1,1')\}$
若$(h,k)\in \mathbf{H}\times\mathbf{K}$,则$(h,k)=(h,1')(1,k)\in H_1K_1,\therefore \mathbf{H}\times\mathbf{K}\subseteq H_1K_1$
若$(h_1,1')\in H_1,(1,k_1)\in K_1$，则$(h_1,1')(1,k_1)\in H_1K_1$,且$(h_1,1')(1,k_1)=(h_1,k_1)$,
$\therefore H_1K_1\subseteq \mathbf{H}\times\mathbf{K}$
$\therefore \mathbf{H}\times\mathbf{K}=H_1K_1$. ■

11. 幺半群$\mathbf{M}$中的元素a称为**可逆的**，如$\exists a^{-1}\in\mathbf{M}$使$aa^{-1}=a^{-1}a=1$.试证以下结论：
1) 设$a\in\mathbf{M}$，若$\exists b,c\in\mathbf{M}$使$ba=ac=1$则a可逆，且$a^{-1}=b=c$;（因而称a^{-1}为a的逆元.）
2) 可逆元的逆元唯一;
3) 若a可逆，则$b=a^{-1}$的充要条件是$aba=a, ab^2a=1$;
4) $\mathbf{M}$中非空子集$\mathbf{G}$为群的充要条件是$\mathbf{G}$中每个元素都可逆且$\forall g_1,g_2\in\mathbf{G}$有$g_1g_2\in\mathbf{G}$;
5) $\mathbf{M}$中所有可逆元素构成一群.
证明 1) $b=bac=c$,故a可逆，且$a^{-1}=b=c$.
2) 设b_1,b_2均为a的逆元，则$b_1=b_1ab_2=b_2$.
3) “$\Rightarrow$”显然.
“$\Leftarrow$”:$ab=abaa^{-1}=aa^{-1}=1, ba=a^{-1}aba=a^{-1}a=1,\therefore b=a^{-1}$.
4) “$\Leftarrow$”显然.
“$\Rightarrow$”封闭性，结合律，逆元存在是显然的.$\forall g\in G$,必有$g^{-1}\in G$,从而$1=gg^{-1}\in G$
5) 若g_1,g_2可逆，则$(g_1g_2)(g_2^{-1}g_1^{-1})=1$,故$g_1g_2$可逆，由上一结论知此成立. ■

1.4 环与域

1. 在$\mathbf{Z}\times\mathbf{Z}$中定义加法与乘法如下：
$(a,b)+(c,d)=(a+c,b+d)$;

$(a,b)(c,d)=(ac,bd),\forall(a,b),(c,d)\in\mathbf{Z}\times\mathbf{Z}$.
证明：$\mathbf{Z}\times\mathbf{Z}$是一个有零因子的交换幺环.
证明

(a) $\mathbf{Z}\times\mathbf{Z}$对加法显然是Abel群.

(b) $((a,b)(c,d))(e,f)=(ac,bd)(e,f)=(ace,bdf)=(a,b)(ce,df)=(a,b)((c,d)(e,f))$;
且$(a,b)(c,d)=(ac,bd)=(ca,db)=(c,d)(a,b).\forall(a,b),(c,d),(e,f)\in\mathbf{Z}\times\mathbf{Z}$. 故$\mathbf{Z}\times\mathbf{Z}$对乘法为交换半群.

(c) $(a,b)((c,d)+(e,f))=(a,b)(c+e,d+f)=(ac,bd)+(ae,bf)=(a,b)(c,d)+(a,b)(e,f)$;
同样的$((c,d)+(e,f))(a,b)=(c,d)(a,b)+(e,f)(a,b)$ 因此$\mathbf{Z}\times\mathbf{Z}$在加法与乘法间有分配律.

综上$\mathbf{Z}\times\mathbf{Z}$是一个交换环.
$\because(1,1)(a,b)=(a,b)=(a,b)(1,1),\therefore$对乘法是幺半群.
$\because(0,1)\neq0,(0,1)\neq0,(0,1)(1,0)=(0,0)=0$
因此$\mathbf{Z}\times\mathbf{Z}$是一个有零因子的交换幺环. ■

2. 设C为$(-\infty,+\infty)$上实函数的集合，在C中定义加法与乘法为
$(f+g)(x)=f(x)+g(x)$;
$(fg)(x)=f(g(x)),\forall f,g\in C,x\in(-\infty,+\infty)$.
试问C对这种加法与乘法是否构成环？
解 令$f(x)=x,g(x)=x^2,h(x)=x^2$,所以有$h(f+g)(x)=(x+x^2)^2,hf(x)+hg(x)=x^2+x^4$, 因此不够成环. ■

3. 设在非空集合R中定义了加法与乘法两种运算.且
1) R对加法为群；
2) R对乘法为幺半群；
3) 加法与乘法间有分配律.
证明R为幺环.
证明 $\forall a,b\in R,(a+1)(b+1)=a(b+1)+b+1=ab+a+b+1,(a+1)(b+1)=(a+1)b+a+1=ab+b+a+1,\therefore a+b=b+a$,所以$R$为幺环. ■

4. 设R是无零因子环，且只有有限个元素.证明R是体.
证明 因为R是无零因子环，所以$\forall a\in R,a\neq0,ab=ac\Leftrightarrow b=c$,所以$aR=R,Ra=R,\therefore ax=b,xa=b,b\in R$在$R$中均有解，所以$R$对乘法构成群，所以$R$是体. ■

5. 证明有理数加法群$\mathbf{Q}$对整数加法群$\mathbf{Z}$的商群$\mathbf{Q}/\mathbf{Z}$只能是零环的加法群.
证明 $\forall a,b\in\mathbf{Q}/\mathbf{Z}$,若$a,b$中有一个为$\overline{0}$,则$ab=\overline{0}$,若$a\neq\overline{0},b\neq\overline{0}$,记$a=\overline{\frac{q_1}{p_1}},b=\overline{\frac{q_2}{p_2}}$,则$ab=\overline{\frac{q_1}{p_1}}\overline{\frac{q_2}{p_2}}=\overline{\frac{q_1}{p_1}\frac{p_1q_2}{p_1p_2}}=\overline{\frac{q_1}{p_1}}p_1\overline{\frac{q_2}{p_1p_2}}=p_1\overline{\frac{q_1}{p_1}\frac{q_2}{p_1p_2}}=\overline{0}$. 因此命题成立. ■

6. 若环R的非零元素e满足$e^2=e$，则称e为**幂等元**.证明若无零因子环R有幂等元e，则R为整环，且e为R的幺元.
证明 $\because e(ea-a)=ea-ea=0$而R是无零因子环，故$ea=a$
同理可证$ae=a$
$\therefore$R为整环，且e为R的幺元. ■

7. 证明一个环R如果只有一个左幺元1_l（即$1_la=a,\forall a\in R$).则R为幺环，且$1_l=1$.
证明 $(ae-a+e)b=b\Rightarrow ae-a+e=e\Rightarrow ae=a$ ■

8. 设R为幺环.$u\in R,u$有右逆元，即有$v\in R$使$uv=1$.证明下列三个条件等价：
1) u的右逆元不唯一；
2) u不是可逆元；
3) u是一个左零因子.
证明 1⇒2: 设u是可逆元，设w使$wu=uw=1$,则$wuv=v$,另一方面$wuv=w(uv)=w,\therefore v=w$,所以$u$的右逆元唯一，与1矛盾. 所以$u$不是可逆元.
2⇒3:因为u不是可逆元，所以$vu\neq1$,即$vu-1\neq0$
而$u(vu-1)=(uv)u-u=u-u=0$
$\therefore u$是一个左零因子.
3⇒ 1:$\because u$是一个左零因子
$\therefore\exists w\neq0$,使$uw=0,\therefore w\neq v$
即$v-w\neq0$,而$u(v-w)=uv-uw=1$
$\therefore v-w$也是u的右逆元，且$v-w\neq v$
$\therefore u$的右逆元不唯一. ■

9. 证明在幺环中如果一元素的右逆元存在但不唯一，则此元素有无穷多个右逆元.
证明 假设u有右逆元为v_1,构造$v_{n+1}=v_1-v_nu+1$,则容易验证v_n都是u的右逆元，若有w使$wu=0$,则$w=w(uv_1)=wuv_1=0$,而且有上题可知$v_1u\neq1$,即$v_1u-1\neq0$,由此可检验$v_{n+1}\neq v_1,n\geqslant1$,若$v_{n+1}=v_{m+1}(m<n)$,则可推出$v_n=v_m$,从而由数学归纳法可得到，当$n\neq m$时，就有$v_n\neq v_m$,因此结论成立. ■

10. 设R为幺环，$a,b\in R$.证明$1-ab$可逆当且仅当$1-ba$可逆.
证明 设$1-ab$可逆，c为其可逆元，令$d=1+bca$,则$(1-ba)d=$

$(1-ba)(1+bca)=1-ba+(1-ba)bca=1-ba+b(1-ab)ca=1-ba+ab=1, d(1-ab)=(1+bca)(1-ba)=1-ba+bca(1-ba)=1-ba+bc(1-ab)a=1-ba+ba=1,\therefore 1-ba$可逆.同样可证明若$1-ba$可逆，则$1-ab$可逆. ■

11. 设R是幺环，a,b及$ab-1$都可逆.证明
1) $a-b^{-1},(a-b^{-1})^{-1}-a^{-1}$都可逆；
2) **华罗庚等式**成立：
$((a-b^{-1})^{-1}-a^{-1})^{-1}=aba-a$
证明 1) $a-b^{-1}=abb^{-1}-b^{-1}=(ab-1)b^{-1},\because b,ab-1$可逆，故$a-b^{-1}$可逆，且$(a-b^{-1})^{-1}=b(ab-1)^{-1}$.
2) $(a-b^{-1})^{-1}-a^{-1}=b(ab-1)^{-1}-a^{-1}=a^{-1}(ab(ab-1)^{-1}-1)=a^{-1}(ab-(ab-1))(ab-1)^{-1}=a^{-1}(ab-1)^{-1},\therefore((a-b^{-1})^{-1}-a^{-1})^{-1}=(ab-1)a=aba-a.$ ■

12. 试问$\mathbf{Z}_m$中元素$\overline{n}=n+m\mathbf{Z}$为零因子或可逆元的充要条件各是什么？并确定$\mathbf{Z}_m$中零因子与可逆元的个数.
解 若$(n,m)=1,\exists u,v\in\mathbf{Z}$,使得$nu+mv=1\Rightarrow\overline{nu}=\overline{1}$,从而$\overline{n}$可逆，若$(n,m)=k\neq1$,则$\overline{n}\overline{\frac{m}{k}}=0$从而$\overline{n}$为零因子.$\therefore\overline{n}$可逆$\Leftrightarrow(n,m)=1$,可逆元个数$\varphi(m)$,$\varphi$为欧拉函数，$\overline{n}$为零因子$\Leftrightarrow(n,m)\neq1$,零因子个数是$m-\varphi(m)$. ■

13. 设$m_1,m_2\in\mathbf{Z}$.确定$\langle m_1,m_2\rangle$（即由m_1与m_2生成的理想）.
解 易知$\langle m_1,m_2\rangle=\{um_1+vM_2|u,v\in\mathbf{Z}\}$,由数论知识知$\langle m_1,m_2\rangle=\langle d\rangle,d=(m_1,m_2)$. ■

14. 举例说明，一个无零因子环R的商环R/I(I为R的理想)可能有零因子.
解 $\mathbf{Z}$为无零因子环，$6\mathbf{Z}$为$\mathbf{Z}$的理想，$\mathbf{Z}/6\mathbf{Z}=\mathbf{Z}_6,\mathbf{Z}_6$中$\overline{23}=0$. ■

15. 设R是环.$a\in R$.若$\exists m\in\mathbf{N}$使$a^m=0$,则称a是一个**幂零元**.证明交换环R的幂零元集合是R的理想.
证明 令$R_1=\{a|\exists m\in\mathbf{N},a^m=0\},\forall a,b\in R_1,\exists m,n\in\mathbf{N}$,使得$a^m=0,b^n=0$,则$(a-b)^{m+n}=\sum_{k=0}^{m+n}a^k(-b)^{m+n-k}=0,(ab)^m=a^mb^m=0.\forall r\in R,(ar)^m=a^mr^m=0.\therefore R_1$是$R$的理想. ■

16. 设K是体.$R=K_{n\times n}$.令$C_i=\{a\in R|\mathrm{col}_j(a)=0,j\neq i\};R_i=\{a\in R|\mathrm{row}_j(a)=0,j\neq i\},1\leq n$.证明
1) C_i是R的**极小左理想**（即若A为R的左理想且$A\subseteq C_i$，则$A=\{0\}$或$A=C_i$）；
2) R_i是R**极小右理想**；
3) R无非平凡理想.
证明 1) $\forall\alpha,\beta\in C_i,\mathrm{col}_j(\alpha-\beta)=0,j\neq i;\mathrm{col}_j(\alpha\beta)=0,j\neq i;\forall c\in$

$K, \mathrm{col}_j(c\alpha) = 0, j \neq i. \therefore C_i$是$R$的左理想.
若A为R的左理想，且$A \subseteq C_i, A \neq \{0\}$,则有$\alpha \in A$,不妨设$\alpha_{j_0 l} \neq 0$,则有$l \neq i, j_0 \neq i, \therefore E_{jl} \in C_i, E_{jl} = \alpha_{j_0 l}^{-1} E_{jj_0} \alpha \in A, \therefore A = C_i, \therefore C_i$是$R$的极小左理想.
2) 同上可得R_i是R的极小右理想.
3) 设R'为R的非零理想，则$\exists \alpha \in R', \alpha \neq 0$,不妨设$\alpha_{i_0 j_0} \neq 0$,则$E_{ij} = \alpha_{i_0 j_0}^{-1} E_{ii_0} \alpha E_{j_0 j} \in R', \therefore R' = R$.所以$R$无非平凡理想. ■

1.5 同态与同构

1. 设A是一个Abel群，其运算记为加法，以$\mathrm{End}\, A$表示A的**自同态**（即A到A的同态）的集合.在$\mathrm{End}\, A$中有乘法，再定义加法

$$(\sigma + \tau)(\alpha) = \sigma(\alpha) + \tau(\alpha), \forall \sigma, \tau \in End\, A, \alpha \in A.$$

试证$\mathrm{End}\, A$是幺环（称为A的**自同态环**）.
证明 对于加法，验证封闭律，结合律，幺元律（幺元为0）和逆元律；对于乘法，验证封闭律，结合律，幺元律（幺元为id）；对于加法和乘法，验证分配律. ■

2. 设$\mathbf{S}_3$是三个文字的对称群，试证

$$\mathrm{Aut}\, \mathbf{S}_3 = \mathrm{Int}\, \mathbf{S}_3 \simeq \mathbf{S}_3.$$

证明 $\because C(\mathbf{S}_3) = \mathrm{id}, \therefore \mathbf{S}_3 \cong \mathrm{Int}\, \mathbf{S}_3$,又$\mathbf{S}_3 = < \{(1,2),(1,3),(2,3)\} >$,自同构一定把2阶元变成2阶元，$\therefore |\mathrm{Aut}\, \mathbf{S}_3| \leq 3! = 6, \because \mathrm{Int}\, \mathbf{S}_3 \lhd \mathrm{Aut}\, \mathbf{S}_3, |\mathrm{Int}\, \mathbf{S}_3| = 6, \therefore |\mathrm{Aut}\, \mathbf{S}_3| = 6, \therefore \mathrm{Aut}\, \mathbf{S}_3 = \mathrm{Int}\, \mathbf{S}_3$. ■

3. 设a, b是两个实数，定义R的变换

$$T_{(a,b)} : T_{(a,b)}(x) = ax + b, \forall x \in R.$$

试证下列结论：
1) $a \neq 0$时，$T_{(a,b)}$是一一对应；
2) $G = \{T_{(a,b)} | a \neq 0\}$是一群；
3) $H = \{T_{(1,b)} | b \in R\}$是$G$的正规子群；（$T_{(1,b)}$称为由$b$决定的**平移**.）
4) $G/H \simeq R^*$（R^*为非零实数乘法群.）
证明 1) 若$x = y$,则$T_{(a,b)}(x) = ax + b = ay + b = T_{(a,b)}(y), \therefore T_{(a,b)}$是映射.
若$T_{(a,b)}(x) = Y_{(a,b)}(y)$,则$ax + b = ay + b$,由$a \neq 0$知$x = y, \therefore T_{(a,b)}$是单

射.
$\forall x \in \mathbf{R}, \exists x' = \dfrac{x-b}{a} \in \mathbf{R}, T_{(a,b)}(x') = ax' + b = x, \therefore T_{(a,b)}$是满射.
$\therefore a \neq 0$时，$T_{(a,b)}$是一一对应.

2) $\forall T_{(a_1,b_1)}, T_{(a_2,b_2)} \in G, T_{(a_1,b_1)}T_{(a_2,b_2)} = T_{(a_1,b_1)}(a_2x + b_2) = a_1(a_2x + b_2) + b_1 = T_{(a_1a_2,b_1b_2)}(x)$,且$a_1a_2 \neq 0, \therefore T_{(a_1a_2,b_1b_2)} \in G \therefore G$满足封闭律；$\forall (T_{(a_1,b_1)}T_{(a_2,b_2)})T_{(a_3,b_3)} = T_{(a_1,b_1)}(T_{(a_2,b_2)}T_{(a_3,b_3)}) \therefore G$满足结合律；$\forall T_{(a,b)} \in G, T_{(1,0)}T_{(a,b)} = T_{(a,b)} \therefore T_{(1,0)}$为$G$的左幺元；$\forall T_{(a,b)} \in G, T_{(\frac{1}{a},-\frac{b}{a})}T_{(a,b)} = T_{(1,0)} \therefore T_{(\frac{1}{a},-\frac{b}{a})}$为$T_{(a,b)}$的左逆元.$\therefore G$是群.

3) 显然H是G的非空子集，$\forall T_{(1,a)}, T_{(1,b)} \in H, T_{(1,a)}T_{(1,b)}^{-1} = T_{(1,a)}T_{(1,-b)} = T_{(1,a-b)} \in H \therefore H < G, \forall T_{(1,b)} \in H, T_{(a,c)} \in G, T_{(a,c)}T_{(1,b)}T_{(a,c)}^{-1} = T_{(a,ab+c)}T_{(\frac{1}{a},\frac{-c}{a})} = T_{(1,ab)} \in H \therefore H \lhd G.$

4) 令$\varphi : G \longrightarrow \mathbf{R}^*, \varphi(T_{(a,b)}) = a, \forall a \in \mathbf{R}^*, \exists T_{(a,b)} \in G$,使$\varphi(T_{(a,b)}) = a, \therefore \varphi$是满射. $\forall T_{(a_1,b_1)}, T_{(a_2,b_2)} \in G, \varphi(T_{(a_1,b_1)}T_{(a_2,b_2)} = \varphi(T_{(a_1a_2,a_1b_2+b_1)}) = a_1a_2 = \varphi(T_{(a_1,b_1)})\varphi(T_{(a_2,b_2)}) \therefore \varphi$是满同态. $\therefore G/\ker\varphi \cong \mathbf{R}^* \forall T_{(a,b)} \in \ker\varphi, \varphi(T_{(a,b)}) = 1 \Rightarrow a = 1 \Rightarrow T_{(a,b)} \in H, \forall T_{(1,b)} \in H, \varphi(T_{(1,b)}) = 1, \therefore T_{(a,b)} \in \ker\varphi, \therefore H = \ker\varphi, \therefore G/H \cong \mathbf{R}^*$ ∎

4. 在集合$G = \{e, a, b, c\}$中定义二元运算如下表.试证G是一个群，且Aut G及G的外自同构群均与$\mathbf{S}_3$同构.

（此群称为**Klein四元素群**，以K_4表示.）

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

证明

(a) 从运算中可看出G对此二元运算封闭；

(b) 对于a, b, c,有$(ab)c = cc = e, a(bc) = aa = e$,
$\therefore (ab)c = a(bc)$
当a, b, c中有相同得元素或有元素e时，都容易验证$(ab)c = a(bc)$,则结合律成立；

(c) e左乘G中任何元素结果是元素本身
$\therefore e$是G的左幺元；

(d) $aa = bb = cc = e$,
$\therefore a, b, c$分别是自身的左逆元.

$\therefore G$是一个群.
令$\varphi : \varphi(\mathcal{A}) = \mathcal{A}|_X$,其中$\forall \mathcal{A} \in$ Aut $G, X = \{a, b, c\}$,因为自同构把不同

的二阶元变为不同的二阶元，所以$\mathcal{A}|_X \in \mathbf{S}_3$,且$\mathcal{A}(e) = e$,
则φ是$\operatorname{Aut} G \longrightarrow \mathbf{S}_3$的满映射，若$\mathcal{A}|_X = \mathcal{B}|_X$,又$\mathcal{A}(e) = \mathcal{B}(e) = e \Rightarrow \mathcal{A} = \mathcal{B}$
$\therefore \varphi$是单射,
$\therefore \varphi$是双射，
$\forall \mathcal{A}, \mathcal{B} \in \operatorname{Aut} G, \varphi(\mathcal{AB}) = \mathcal{AB}|_X = \mathcal{A}|_X\mathcal{B}|_X = \varphi(\mathcal{A})\varphi(\mathcal{B})$
$\therefore \varphi$是同构，
$\therefore \operatorname{Aut} G \cong \mathbf{S}_3$;
令$\sigma : \operatorname{Aut} G \longrightarrow \operatorname{Aut} G/\operatorname{Inn} G, \sigma(\mathcal{A}) = \mathcal{A}\operatorname{Inn} G$,显然$\sigma$是满映射，因为$G$是可交换的，所以$\operatorname{Inn} G = \{\mathrm{id}_G\}, \therefore \sigma$是同构.
$\therefore \operatorname{Aut} G \cong \operatorname{Aut} G/\operatorname{Inn} G \cong \mathbf{S}_3$. ■

5. 设G是一个群.证明
1) $a \to a^{-1}$是G的自同构当且仅当G是交换群；
2) 又若G是交换群，则$\forall k \in \mathbf{Z}, a \to a_k$是$G$的自同态.（即$G$到$G$的同态.）
证明 1) $\forall a \in G, \varphi(a) = a^{-1}, \because a^{-1} \in G, \therefore \varphi$是$G \longrightarrow G$的变换，$\varphi$是映射,
若$\forall a \in G$,有$\varphi(a^{-1}) = a, \therefore \varphi$是满射，
若$\varphi(a) = \varphi(b)$，则$a^{-1} = b^{-1} \Rightarrow a = b$
$\therefore \varphi$是单射;
由上知φ是一一对应.
“$\Leftarrow$”: $\forall a, b \in G, \varphi(ab) = (ab)^{-1} = b^{-1}a^{-1}$,由$G$是Abel群，知$\varphi(ab) = \varphi(a)\varphi(b)$,
$\therefore \varphi$是同态，
$\therefore \varphi$是自同构.
“$\Rightarrow$”: $\forall a, b \in G, \varphi(a^{-1}b^{-1}) = (b^{-1}a^{-1})^{-1} = ba$,
$\because \varphi$是同构，
$\therefore \varphi(a^{-1}b^{-1}) = \varphi(a^{-1})\varphi(b^{-1}) = ab$,
$\therefore ab = ba$,
$\therefore G$是Abel群.
2) 设$\varphi : \varphi(a) = a^k, k \in \mathbf{Z}$,则$\varphi$是$G \longrightarrow G$的映射，
$\forall a, b \in G, G$是Abel群，$\varphi(ab) = (ab)^k = a^kb^k = \varphi(a)\varphi(b)$,
$\therefore \varphi$是G的自同态. ■

6. 设a是群G的自同构，且满足

$$a(g) = g \Rightarrow g = 1.$$

证明下列结论
1) $g \rightharpoonup a(g)g^{-1}$是一一的；

2) 若G是有限群，则G的每个元素均可写成$a(g)g^{-1}$形式；
3) 又若$a^2 = \mathrm{id}_G$,则G为奇数阶交换群.
证明 1) 设$\varphi : \varphi(g) = a(g)g^{-1}, \varphi$是$G \longrightarrow G$的映射，
若$\varphi(g_1) = \varphi(g_2)$,即$a(g_1)g_1^{-1} = a(g_2)g_2^{-1} \Rightarrow a(g_1)^{-1}a(g_2) = g_1^{-1}g_2^{-1} \Rightarrow a(g_1^{-1}g_2) = g_1^{-1}g_2 \Rightarrow g_1^{-1}g_2 = 1 \Rightarrow g_1 = g_2$,
$\therefore \varphi$是一一的；
2) $\because G$是有限群，G是一一的，$\therefore \varphi$必为一一对应，且$\varphi : G \longrightarrow G$.
$\therefore G$中每个元素作为像可写成$a(g)g^{-1}$形式；
3) $\forall g \in G, \exists g_1 \in G$,使$g = a(g_1)g_1^{-1}$,
$a(g) = a(g_1)^2a(g_1^{-1}) = g_1a(g_1^{-1}) = g^{-1}$,
$\forall a, b \in G$,一方面$a(a^{-1}b^{-1}) = a(a^{-1})a(b^{-1}) = ab$,另一方面$a(a^{-1}b^{-1}) = (a^{-1}b^{-1})^{-1} = ba$,
$\therefore ab = ba$,
$\therefore G$为Abel群.
$\forall g \in G$,若$g = g^{-1}$,则$a(g) = g^{-1} = g \Rightarrow g = 1$
$\therefore \forall a \in G, a \neq 1, a$和$a^{-1}$是$G$中两不同元素，
再考虑到$1 \in G$,
$\therefore G$为奇数阶. ■

7. 设G是一个群，$K \lhd G$,又H_a是含K的子群族（即H_a是G的子群.且$H_a \supseteq K$），证明

$$\bigcap_a (H_a/K) = (\bigcap_a H_a)/K.$$

证明 一方面：$gk \in \bigcap_a (H_a/K) \Rightarrow gk \in H_\alpha K(\forall \alpha) \Rightarrow \forall \alpha, \exists g_\alpha \in H_\alpha$使得$gK = g_\alpha K \Rightarrow g^{-1}g_\alpha \in K \Rightarrow g \in H_\alpha(\forall \alpha) \Rightarrow g \in \bigcap_\alpha H_\alpha \Rightarrow \bigcap_a (H_a/K) \subseteq (\bigcap_a H_a)/K$.
另一方面，显然$(\bigcap_a H_a)/K \subseteq \bigcap_a (H_a/K)$. ■

8. 在$\mathbf{Z}$中定义二元运算“$\circ$”为

$$a \circ b = a + b - ab, \forall a, b \in \mathbf{Z},$$

则$(\mathbf{Z}, \circ)$是一个幺半群，且与$\mathbf{Z}$对乘法的幺半群同构.
证明 结合律：$a \circ (b \circ c) = a \circ (b+c-bc) = a+b+c-bc-a(b+c-bc) = a+b+c-ab-bc-ca+abc, (a \circ b) \circ c = (a+b-ab) \circ c = a+b+c-ab-bc-ca-abc, \therefore a \circ (b \circ c) = (a \circ b) \circ c, a \circ 0 = 0, 0 \circ a = 0, \therefore (\mathbf{Z}, \circ)$是幺半群，0为幺元.
令$f : (\mathbf{Z}, \cdot) \longrightarrow (\mathbf{Z}, \circ), f(a) = 1 - a$,显然$f$是双射，而$f(ab) = 1 - ab =$

$(1-a)+(1-b)-(1-a)(1-b)=f(a)+f(b)-f(a)f(b)=f(a)\circ f(b),\therefore$ $(\mathbf{Z},\circ)\cong(\mathbf{Z},\cdot)$. ■

9. 证明整数加法群的自同态环与整数环同构.
证明 $T:\operatorname{End}\mathbf{Z}\longrightarrow\mathbf{Z},T(\sigma)=\sigma(1),\forall\sigma\in\operatorname{End}\mathbf{Z},\forall m\in\mathbf{Z},\exists\sigma\in\operatorname{End}\mathbf{Z}$,使得$\sigma(1)=m,\sigma(n)=mn(n\in\mathbf{Z}),\therefore T$是满射.又$\forall\sigma,\tau\in\operatorname{End}\mathbf{Z},\sigma(1)\neq\tau(1)$,则$\sigma\neq\tau,\therefore T$是单射，$\therefore T$是双射.
又$\forall\sigma,\tau\in\operatorname{End}\mathbf{Z},T(\sigma+\tau)=\sigma(1)+\tau(1)=T(\sigma)+T(\tau),T(\sigma\tau)=\sigma\tau(1)=\sigma(\tau(1))=\sigma(1)\tau(1)=T(\sigma)T(\tau),\therefore T$是$\operatorname{End}\mathbf{Z}\longrightarrow\mathbf{Z}$的同构. ■

10. **H**如例1.4.8所述，令

$$1=\begin{pmatrix}1&0\\0&1\end{pmatrix},i=\begin{pmatrix}\sqrt{-1}&0\\0&-\sqrt{-1}\end{pmatrix}$$

,

$$j=\begin{pmatrix}0&1\\-1&0\end{pmatrix},k=\begin{pmatrix}0&\sqrt{-1}\\\sqrt{-1}&0\end{pmatrix}$$

证明下列结论
1) $\forall a\in\mathbf{H}$,存在唯一的一组$(a,b,c,d)\in\mathbf{R}^{(1)}$，使得$a=a+bi+cj+dk$.
2) **H**的变换σ:

$$\sigma(a+bi+cj+dk)=a-bi-cj-dk,$$

是**H**的一个对合.
证明 1) 显然.
2) $\forall\alpha,\beta\in H,\alpha=a_1+b_1i+c_1j+d_1k,\beta=a_2=a_2+b_2i+c_2j+d_2k,\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta),\sigma(\alpha\beta)=\sigma(\beta)\sigma(\alpha),\sigma(\alpha)^2=\alpha,\therefore\sigma$是$H$的一个对合. ■

11. （**华罗庚定理**）设σ为环R到环R'的一个映射，对$\forall a,b\in R$满足
1) $\sigma(a+b)=\sigma(a)+\sigma(b)$,
2) $\sigma(ab)=\sigma(a)\sigma(b)$或$\sigma(ab)=\sigma(b)\sigma(a)$.
则σ为同态或反同态.试证明.
证明 设σ不是反同态，下证σ必为同态映射.由于σ不是反同态，故$\exists c,d\in R$,使得

$$\sigma(cd)=\sigma(c)\sigma(d)\neq\sigma(d)\sigma(c)$$

首先证明$\forall x\in R$,都有

$$\sigma(cx)=\sigma(c)\sigma(x),\sigma(xd)=\sigma(x)\sigma(d)$$

事实上，若有

$$\sigma(cx) = \sigma(x)\sigma(c)$$

则

$$\sigma(c(d+x)) = \sigma(cd+cx) = \sigma(c)\sigma(d) + \sigma(x)\sigma(c) \tag{1.1}$$

另一方面，若

$$\sigma(c(d+x)) = \sigma(d+x)\sigma(c) = \sigma(d)\sigma(c) + \sigma(x)\sigma(c) \tag{1.2}$$

(1.2)式与(1.1)式比较得

$$\sigma(c)\sigma(d) = \sigma(d)\sigma(c)$$

矛盾.
故必有

$$\sigma(c(d+x)) = \sigma(c)\sigma(d) + \sigma(c)\sigma(x) \tag{1.3}$$

(1.3)式与(1.1)式比较得

$$\sigma(x)\sigma(c) = \sigma(c)\sigma(x)$$

即对$\forall x \in R$,都有

$$\sigma(cx) = \sigma(c)\sigma(x)$$

同理可得

$$\sigma(xd) = \sigma(x)\sigma(d)$$

对$\forall x, y \in R$,若有

$$\sigma(xy) = \sigma(y)\sigma(x)$$

同上证明知$\forall z \in R$,有

$$\sigma(xz) = \sigma(x)\sigma(z)$$

$$\sigma(zy) = \sigma(z)\sigma(y)$$

则

$$\sigma((x+c)(y+d)) = \sigma(y)\sigma(x) + \sigma(x)\sigma(d) + \sigma(c)\sigma(y) + \sigma(c)\sigma(d) \tag{1.4}$$

另一方面，若有

$$\sigma((x+c)(y+d)) = \sigma(y+d)\sigma(x+c) = \sigma(y)\sigma(x)+\sigma(d)\sigma(x)+\sigma(y)\sigma(c)+\sigma(d)\sigma(c) \tag{1.5}$$

$\because \sigma(x)\sigma(d) = \sigma(d)\sigma(x), \sigma(c)\sigma(y) = \sigma(y)\sigma(c)$
$\therefore$由(1.4)，(1.5)得

$$\sigma(c)\sigma(d) = \sigma(d)\sigma(c)$$

矛盾.
故必有

$$\sigma((x+c)(y+d)) = \sigma(x+c)\sigma(y+d) = \sigma(x)\sigma(y)+\sigma(x)\sigma(d)+\sigma(c)\sigma(y)+\sigma(c)\sigma(d) \tag{1.6}$$

由(1.4),(1.6)得

$$\sigma(x)\sigma(y) = \sigma(y)\sigma(x)$$

∴此时σ是R的一个同态映射. ■

12. 设R是一个无零因子环，且R的每个加法子群都是R的左理想，证明R或与$\mathbf{Z}_p$（p为素数）同构，或与$\mathbf{Z}$的一个子环同构.

13. 设R是一个环，令$G(R)$为R的自同构与反自同构的集合.Aut R为R的自同构集合.证明$G(R)$对映射的乘法构成一个群，且$[G(R) : \text{Aut } R]$的值为1或2.
证明 (1):封闭性，$\forall \sigma, \eta \in G(R)$.
若σ是自同构，η是反自同构，则$\sigma\eta$是反自同构;
若σ是反自同构，η是自同构，则$\sigma\eta$是反自同构;
若σ, η都是自同构，或都是反自同构，则$\sigma\eta$是自同构.
结合律显然.
幺元律：$\sigma\text{id} = \sigma = \text{id}\sigma$.
逆元律：$\sigma\sigma^{-1} = \text{id}$.
(2):显然Aut R是$G(R)$的正规子群.$\forall \sigma, \eta \in G(R), \sigma\text{Aut } R = \eta\text{Aut } R \Leftrightarrow \eta^{-1}\sigma \in \text{Aut } R$,即$\sigma, \eta$同为自同构，或同为反自同构.
若$G(R) = \text{Aut } R$,则$[G(R) : \text{Aut } R] = 1$;
若$\text{Aut } R \subset G(R)$,则$[G(R) : \text{Aut } R] = 2$. ■

1.6 模

1. 设R是幺环，M是一个Abel群.假设存在R到End M的同态u,使$u(1) = \text{id}_M$.证明$R \times M$到M的映射$(a, x) \to ax = u(a)(x), a \in R, x \in M$使$M$成为$R-$模.
证明 $\forall x, y \in M, a, b \in R$,则$u(a) \in \text{End } M$;

   (a) $a(x+y) = u(a)(x+y) = u(a)(x) + u(a)(y) = ax + ay$;

   (b) $(a+b)x = u(a+b)(x) = (u(a) + u(b))(x) = u(a)(x) + u(b)(x) = ax + bx$;

   (c) $(ab)x = u(ab)(x) = (u(a)u(b))(x) = u(a)(u(b)(x)) = u(a)(bx) = a(bx)$;

   (d) $1x = u(1)(x) = \text{id}_M(x) = x$.

$\therefore$在此映射下M成为$R-$模. ■

2. 设R是幺环，M是$R-$模.证明有R到$\mathrm{End}\,M$的同态f使$f(1)=\mathrm{id}_M$.
证明 作$f: R\longrightarrow \mathrm{End}\,M, \forall a\in R, f(a)=a\mathrm{id}_M$,则易知$f(1)=\mathrm{id}_M, f$是$R$到$\mathrm{End}\,M$的同态. ■

3. 设R,S都是幺环，$1',1$分别为S与R的幺元，映射$f: S\to R$是同态，且$f(1')=1$.又设M是一个$R-$模.证明：$S\times M$到M的映射$(s,x)\to f(s)x, s\in S, x\in M$使$M$成为$S-$模.
证明 $\forall s,s_1,s_2\in S, x,x_1,x_2\in M$
$1): (s_1+s_2,x)=f(s_1+s_2)x=[f(s_1)+f(s_2)]x=f(s_1)x+f(s_2)x=s_1x+s_2x$;
$2): (s,x_1+x_2)=f(s)(x_1+x_2)=f(s)x_1+f(s)x_2$;
$3): (s_1s_2,x)=f(s_1s_2)x=f(s_1)f(s_2)x=(s_1,(s_2,x))$;
$4): (1',x)=f(1')x=1x=x$.
$\therefore f$使M成为$s-$模. ■

4. 设R是交换幺环，M是$R-$模，且$a\in R$.令$aM=\{ax|x\in M\}, M(a)=\{x|x\in M, ax=0\}$.证明$aM$与$M(a)$都是$M$的子模.
证明 $1):\forall x_1,x_2\in M, ax_1,ax_2\in aM$,则$ax_1-ax_2=a(x_1-x_2)\in aM.\forall x\in M, r\in R, r(ax)=a(rx)\in aM, \therefore aM$是$M$的子模.
$2):\forall x_1,x_2\in M(a), ax_1=ax_2=0$,则$ax_1-ax_2=a(x_1-x_2)=0, \therefore x_1-x_2\in M(a).\forall x\in M(a), r\in Ra(rx)=r(ax)=0, \therefore rx\in M(a), \therefore M(a)$是$M$的子模. ■

5. 设$n\in\mathbf{N}, a,b\in\mathbf{Z}, n=ab, (a,b)=1$,又$\mathbf{Z}_n$为$\mathbf{Z}-$模.试证$a\mathbf{Z}_n=\mathbf{Z}_n(b)$.
证明 $\mathbf{Z}_n=\{\overline{0},\overline{1},\overline{2},\cdots,\overline{n-1}\}, \forall\overline{x}\in\mathbf{Z}_n(b)\Leftrightarrow n|bx\Leftrightarrow a|x(\because n=ab,(a,b)=1)\Leftrightarrow x\in a\mathbf{Z}_n$ ■

6. 无非平凡子模的$R-$模M称为单模.试证M为单模当且仅当对$\forall x\in M, x\neq 0$有$M=Rx$.
证明 “$\Rightarrow$”:$\forall x\in M, x\neq 0$,显然有$\{0\}\subset Rx\subseteq M, \forall ax\in Rx, bx\in Rx$,其中$a,b\in R, ax-bx=(a-b)x\in Rx$,
$\therefore Rx<M$.（Rx不空是显然的）
$\forall r\in R, ax\in Rx, r(ax)=(ra)x\in Rx$,
$\therefore Rx$是M的子模. $\because M$是单模，
$\therefore Rx$是M的平凡子模. $\therefore M=Rx$.
“$\Leftarrow$”:设N为M的子模，$N\neq\{0\}$,则$RN\subseteq N, \forall x\in N, x\neq 0$,有$Rx\subseteq RN$.
上述$x\in M, x\neq 0, \therefore$由条件有$M=Rx$,
$\therefore M=Rx\subseteq RN\subseteq N$.
从而$M=N, \therefore M$只有平凡子模.
$\therefore M$为单模. ■

7. 试证幺环R（至少有两个元素）为单R—模当且仅当R为体.
证明 “$\Leftarrow$”:若R为体，则R只有平凡理想，且$I \lhd R \Leftrightarrow I$是$R$的子模.
$\therefore R$只有平凡子模，
$\therefore R$为单模.
“$\Rightarrow$”:若R为单模，由第6题结论知$\forall x \in R, x \neq 0$,有$R = Rx$.
故$\forall x \in R, x \neq 0, \exists r \in R$,使得$1 = rx$.
$\therefore x$有左逆元，又R已是幺环，
$\therefore \{R^*; \cdot\}$成群，即$R$为体. ■

8. 设M是R—模，S是M的非空子集.S在R中的**零化子**定义为

$$\operatorname{ann}_R S = \{a \in R | ax = 0, \forall x \in S\}$$

证明下列结论:
1) $\operatorname{ann}_R S$是R的左理想（M为右R—模时，相应地为右理想）;
2) 若S是M的子模，则$\operatorname{ann}_R S$是R的理想.
证明 1) $\forall a, b \in \operatorname{ann}_R S$,有$ax = bx = 0, \forall x \in S$,从而$ax - bx = (a-b)x = 0, \forall x \in S, \therefore a - b \in \operatorname{ann}_R S$.
$\forall a \in \operatorname{ann}_R S, r \in R, rax = 0, \forall x \in S, \therefore ra \in \operatorname{ann}_R S$.综上$\operatorname{ann}_R S$是$R$的左理想.
2) $\forall a \in \operatorname{ann}_R S, r \in R, x \in S, \because S$是$M$的子模，$\therefore rx \in S, \therefore arx = a(rx) = 0, \therefore ar \in \operatorname{ann}_R S, \therefore \operatorname{ann}_R S$是$R$的理想. ■

9. 求$\mathbf{Z}$—模$\mathbf{Z}_m$在$\mathbf{Z}$中的零化子$\operatorname{ann}_Z \mathbf{Z}_m$及$\mathbf{Z}/\operatorname{ann}_Z \mathbf{Z}_m$.
解 $k \cdot \overline{n} = \overline{0}, \forall \overline{n} \in \mathbf{Z}_m, k \in \mathbf{Z} \Leftrightarrow k \in m\mathbf{Z}$. $\therefore \operatorname{ann}_{\mathbf{Z}} \mathbf{Z}_m = m\mathbf{Z}, \mathbf{Z}/\operatorname{ann}_{\mathbf{Z}} \mathbf{Z}_m = \mathbf{Z}_m$. ■

10. 设R为幺环.试证明：
1) 左R—模R的自同态环$\operatorname{End}_L R$与R反同构；
2) 右R—模的自同态环$\operatorname{End}_R R$与R同构.
证明 由例1.6.14知$\operatorname{End}_L R \cong R_r$反同构于$R$,$\operatorname{End}_R R \cong L_r \cong R$,($R_r$表示$R$右乘变换，$L_r$表示$R$左乘变换.) ■

11. 设V是数域$\mathbf{P}$上的线性空间，$\mathcal{A}$是V的一个线性变换，定义$\mathbf{P}[\lambda] \times V$到$V$的映射为$(f(\lambda), x) \to f(\mathcal{A})x, f(\lambda) \in \mathbf{P}[\lambda], x \in V$.于是$V$是一个$\mathbf{P}[\lambda]$—模.试证：
1) $\operatorname{End}_{p[\lambda]} V = \{\varphi \in \operatorname{End}(V) | \varphi\mathcal{A} = \mathcal{A}\varphi\}$,其中$\operatorname{End}(V)$是$V$的线性变换的集合；
2) $\operatorname{ann}_p[\lambda] V = \{f(\lambda) \in \mathbf{P}[\lambda] | f(\mathcal{A}) = 0\} = \langle g(\lambda) \rangle$,其中$g(\lambda)$是$\mathcal{A}$ 的极小多项式.
证明 1) 一方面，$\forall \varphi \in \operatorname{End}_{p[\lambda]} V$,有$\varphi(x+y) = \varphi(x) + \varphi(y), \forall x, y \in V. \varphi(ax) = a\varphi(x), \forall a \in \mathbf{P}, x \in V. \therefore \varphi \in \operatorname{End}(V)$.

又$\varphi(\lambda x)=\lambda\varphi(x),\forall x\in V,\therefore \varphi\mathcal{A}=\mathcal{A}\varphi$.
另一方面，$\forall\varphi\in \mathrm{End}(V),\varphi\mathcal{A}=\mathcal{A}\varphi$,显然有$\varphi(x+y)=\varphi(x)+\varphi(y),\forall x,y\in V,\varphi(f(\lambda)x)=\varphi(f(\mathcal{A})x)=f(\mathcal{A})\varphi(x)=f(\lambda)\varphi(x),\forall f(x)\in P[\lambda],x\in V,\therefore \mathrm{End}_{p[\lambda]}V=\{\varphi\in \mathrm{End}(V)|\varphi\mathcal{A}=\mathcal{A}\varphi\}$.
2) $f(\lambda)\in \mathrm{ann}_p[\lambda]V\Leftrightarrow f(\mathcal{A})x=0,\forall x\in V\Leftrightarrow f(\mathcal{A})=0\Leftrightarrow g(\lambda)|f(\lambda)\Leftrightarrow f(\lambda)\in\langle g(\lambda)\rangle,\therefore \mathrm{ann}_p[\lambda]V=\{f(\lambda)\in P[\lambda]|f(\mathcal{A})=0\}=\langle g(\lambda)\rangle$. ■

12. 设V是复数域$\mathbf{C}$上的n维线性空间，试证由V的线性变换$\mathcal{A}$定义的$\mathbf{C}[\lambda]$－模V为循环模的充要条件是$\mathcal{A}$的极小多项式为$(\lambda-\lambda_0)^n,\lambda_0\in\mathbf{C}$.

1.7 同态基本定理

1. 下列各题中，φ是群G到H的映射，判断φ是否为同态映射.若是，求$\ker\varphi$.
1) $G=R,H=\mathbf{Z}$为加法群，$\varphi(x)=[x]$（x的整数部分函数，即小于或等于x的最大整数）；
2) $G=\mathbf{R}^*,H=\mathbf{R}^*$为乘法群，$\varphi(x)=|x|$;
3) $G=\mathbf{S}_n,H=\{1,-1\},\varphi(\sigma)=\mathrm{sgn}\,\sigma$;
4) $G=GL(n,\mathbf{P}),H=\mathbf{P}^*$（$\mathbf{P}$是数域）,$\varphi(A)=\det A$;
5) $G=O(n,\mathbf{P}),H=\{1,-1\},\varphi(A)=\det A$;
6) $G=\mathbf{Z}_9,H=\mathbf{Z}_2,\varphi(x)$为$x$除以2的余数.
解 1) 不是. $\varphi(1.5+0.5)=\varphi(2)=2,\varphi(1.5)+\varphi(0.5)=1+0=1$
2) 是. $\ker\varphi=\{1,-1\}$
3) 是. $\ker\varphi=A_n$.
4) 是. $\ker\varphi=\{A|\det A=1\}$.
5) 是. $\ker\varphi=SO(n,p)$.
6) 不是. $\varphi(\overline{4})=0,\varphi(\overline{5})=1,\varphi(\overline{4}+\overline{5})=\varphi(\overline{0})=0$. ■

2. 设G_1,G_2与H都是群，且f_i是G_i到H上的同态，$i=1,2$.又有$\ker f_1\simeq\ker f_2$.问G_1与G_2是否同构？
解 不一定.$G_1=\mathbf{S}_3,f_1:\mathbf{S}_3\longrightarrow\mathbf{Z}_2,\ker f_1=\langle(1,2,3)\rangle$,
$G_2=\mathbf{Z}_6,f_2:\mathbf{Z}_6\longrightarrow\mathbf{Z}_2,\ker f_2=\langle\overline{2}\rangle=\{\overline{0},\overline{2},\overline{4}\}\mathbf{Z}_6$是循环群，$\mathbf{S}_3$不是循环群，因此$\mathbf{S}_3$不同构于$\mathbf{Z}_6$. ■

3. 设$\mathbf{R}$为实数加法群，$\mathbf{C}^*$为非零复数的乘法群.$\mathbf{R}$到$\mathbf{C}^*$的映射φ定义为

$$\varphi(x)=\cos x+\sqrt{-1}\sin x,\forall x\in R.$$

证明φ是一个同态，并求$\ker\varphi$.

证明 $\forall x,y\in\mathbf{R},\varphi(x+y)=\cos(x+y)+\sqrt{-1}\sin(x+y)$,
$\varphi(x)\varphi(y)=(\cos x+\sqrt{-1}\sin x)(\cos y+\sqrt{-1}\sin y)=\cos x\cos y-\sin x\sin y+\sqrt{-1}(\sin x\cos y+\cos x\sin y)=\cos(x+y)+\sqrt{-1}\sin(x+y)$,
$\therefore\varphi(x+y)=\varphi(x)+\varphi(y)$,
$\therefore\varphi$是一个同态.
$\mathbf{C}^*$中的幺元是1,若$\varphi(x)=1$即$\cos x+\sqrt{-1}\sin x=1$,则$x=2k\pi,(k\in\mathbf{Z})$
$\therefore\ker\varphi=\{x|x=2k\pi,k\in\mathbf{Z}\}$. ■

4. 设G是n个文字对称群$\mathbf{S}_n$的一个子群，且G中包含有奇置换.试证G中必有一个子群H满足$[G:H]=2$.

证明 令$H=\{\sigma\in G|\sigma$为偶置换$\}$,
$\because\mathrm{id}\in H$,
$\therefore H$是G的非空子集.
$\forall\sigma_1,\sigma_2\in H,\sigma_1\sigma_2^{-1}\in G$且为偶置换，
$\therefore\sigma_1\sigma_2^{-1}\in H$,
$\therefore H<G$.
取奇置换$\tau\in G$,则$\forall\tau_1\in G,\tau_1$为奇置换，有$\tau^{-1}\tau_1\in H,\therefore\tau H=\tau_1 H$.
取偶置换$\mathrm{id}\in G$,则$\forall\tau_2\in G,\tau_2$为偶置换，有$\mathrm{id}^{-1}\tau_2\in H$,
$\therefore\mathrm{id}\,H=\tau_2 H$.
$\therefore[G:H]=2$. ■

5. 设G,G'都是群，且$H\lhd G,H'\lhd G'$,又设φ是G到G'上的同态，证明若$\varphi(H)\subseteq H'$,则φ可导出G/H到G'/H'上的一个同态φ^*.对于环‘模叙述相应命题，并证明之.

证明

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \pi\downarrow & & \downarrow\pi' \\ G/H & \xrightarrow{\varphi'} & G'/H' \end{array}$$

令$\varphi'\pi(g)=\pi'\varphi(g)$.
下证φ'是映射.
$\forall g_1,g_2\in G,\pi(g_1)=\pi(g_2)$,有$g_1^{-1}g_2\in H$,从而$\varphi(g_1^{-1}g_2)\in H'.\pi'\varphi(g_1^{-1}g_2)=1\Rightarrow\pi'\varphi(g_1)=\pi'\varphi(g_2)$,从而$\varphi'(\pi(g_1))=\varphi'(\pi(g_2)),\varphi'$同态是显然的.
环的叙述：R,R'都是环，K,K'分别是R,R'的理想，又设φ是R到R'上的环同态，证明若$\varphi(K)\subseteq K'$,则φ可诱导出R/K到R'/K'上的一个环同态φ'.
模的叙述：M,M'都是幺环R上的模，N,N'分别是M,M'的子模，又设φ是M到M'上的模同态，证明若$\varphi(N)\subseteq N'$,则φ可诱导出M/N到M'/N'上的一个模同态φ'. ■

6. 设K是一个体，$K_{n\times n}$为K上n阶方阵所构成的环，确定$K_{n\times n}$的同态象.
解 由1.4第16题知$K_{n\times n}$无非平凡理想，所以$K_{n\times n}$的同态像只能为$K_{n\times n}$或$\{0\}$. ■

7. 证明$\mathbf{R}$上一元多项式环$\mathbf{R}[x]$对由x^2+1生成的理想的商环$\mathbf{R}[x]/\langle x^2+1\rangle$与复数域$\mathbf{C}$同构.
证明 作$\varphi: R[x]\longrightarrow \mathbf{C}, \varphi(f(x))=f(\sqrt{-1}), \forall f(x)\in R[x]$. ■

8. 设R是一个环，在$\mathbf{Z}\times R$中定义加法与乘法为

$$(m,a)+(n,b)=(m+n,a+b),$$
$$(m,a)(n,b)=(mn,na+mb+ab), m,n\in\mathbf{Z}, a,b\in R$$

证明$\mathbf{Z}\times R$是一个幺环，且有一双边理想与R同构.
证明 易证$\mathbf{Z}\times R$是一个环，幺元是$(1,0),(0,R)$是一双边理想且与R同构. ■

9. 证明环R一定与某Abel群的自同态环的一个子环同构.
证明 考虑R作为加法运算为Abel群的自同态环$\mathrm{End}\,R$,设L_R为R左乘变换的集合，易知$L_R\subseteq \mathrm{End}\,R$.又$\because \forall a_R,b_R\in L_R, \forall x\in R, (a_R-b_R)x=(a-b)_R x, \therefore a_R-b_R\in L_R. \because (a_Rb_R)x=(ab)_R x, \therefore a_rb_R\in L_R. \therefore L_R$是$\mathrm{End}\,R$的子环.
由Cayley定理可得$R\cong L_R$. ■

10. 设R是一个无零因子环，且每个加法子群都是R的左理想.证明R或与$\mathbf{Z}_p$（p为素数）同构，或与$\mathbf{Z}$的一个子环同构.

11. 试证无零因子幺环R中含幺元e的最小子环必与$\mathbf{Z}_p$（p为素数）或$\mathbf{Z}$同构.（前一情形称R的**特征**为p, 后一情形称R的**特征**为0.）
证明 引理：无零因子环R中每个元素关于加法的阶或者都为∞,或者都为p（p为素数）.
证明：若R中所有元素的阶都为∞,则命题得证.
若$\exists a\in R, a$的阶$m, ma=0$,则对$\forall b\in R, 0=(ma)b=a(mb), \because R$是无零因子环，$\therefore mb=0$,同理，设$b$的阶为$n, nb=0$,则$m\geq n, na=0, \therefore n\geq m, \therefore m=n$
若m不是素数，则$m=m_1m_2, m_1m_2\neq 1, 0=mab=(m_1a)(m_2b), \because R$无零因子，$\therefore m_1a=0$或$m_2b=0$.矛盾.所以$m$为素数.
对正题的证明：包含e的最小子环为$\{me|m\in\mathbf{Z}\}=R_1$,作$f: R_1\longrightarrow \mathbf{Z}, f(me)=m$.易证$f$是同态.由引理知，当$R$的特征为0时，易证$f$是同构，$R_1\cong\mathbf{Z}$.
当R的特征为p时，$\ker f=p\mathbf{Z}, R_1\cong\mathbf{Z}/p\mathbf{Z}=\mathbf{Z}_p$. ■

12. 举例说明一个环R的两个子环H,K的和$H+K$不一定是R的子环.
解 $\mathbf{Q},\mathbf{Z}[\sqrt{-1}]$是$\mathbf{C}$的子环，但$\mathbf{Q}+\mathbf{Z}[\sqrt{-1}]$不是$R$的子环. ■

13. 设有$R-$模与$R-$同态的序列如下：

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \cdots .$$

若$f_{i-1}(M_{i-1})=\ker f_i, \forall i \in \mathbf{Z}$，则称此序列为**正合序列**.
设f是M到N的$R-$同态，O表示由一个元素构成的$R-$模.同时约定，$O \to M$表示将O映射到M的零元素的$R-$同态，$N \to O$为将N的所有元素映到O的$R-$同态，试证：
1) f是一一同态当且仅当序列$O \to M \xrightarrow{f} N$是正合的；
2) f是满同态当且仅当序列$M \xrightarrow{f} N \longrightarrow O$是正合的；
3) f是同构当且仅当序列$O \longrightarrow M \xrightarrow{f} N \longrightarrow O$是正合的.
证明 1) f是一一同态$\Leftrightarrow \ker f=\{0\}=g(0) \Leftrightarrow 0 \xrightarrow{g} M \xrightarrow{f} N$是正合的.
2) f是满同态$\Leftrightarrow \ker g=N=f(M) \Leftrightarrow M \xrightarrow{f} N \longrightarrow 0$是正合的.
3) 由1，2知3成立. ■

14. 一个$R-$模M若无非平凡子模，则称为单模（或不**可约模**）.设M为$R-$模，则下列条件等价：
1) M是单模；
2) 若映射$f: M \to N$是非零同态，则序列$O \to M \xrightarrow{f} N$是正合的；
3) 若映射$g: N \to M$是非零同态，则序列$N \xrightarrow{g} M \longrightarrow O$是正合的.
证明 M是单模$\Leftrightarrow \ker f=\{0\}$（$\because f$是非零同态）$\Leftrightarrow 0 \longrightarrow M \xrightarrow{f} N$是正合的.
$\therefore 1 \Leftrightarrow 2.$
M是单模$\Leftrightarrow g(N)=M$（$\because g$是非零同态）$\Leftrightarrow N \xrightarrow{g} M \longrightarrow 0.$
$\therefore 1 \Leftrightarrow 3.$
因此得证. ■

1.8 循环模

1. 设G是有限群，G的任何真子群都是循环群，试问G一定是循环群吗？
解 不一定.反例Klein四元素群. ■

2. 设G是一个群，$a \in G, \langle a\rangle$是$G$中唯一的二阶子群.证明：$ax=xa, \forall x \in G$.

证明 $\langle a\rangle$是G中唯一的二阶子群，则$\langle a\rangle$是G的正规子群.

$\forall x\in G, x^{-1}ax=a$或$e$,显然$ax\neq x$,否则$a=e,\therefore x^{-1}ax=a$即$ax=xa$. ■

3. 举例说明定理1.8.3对非循环的有限群不成立.
解 反例：设$X=\{1,2,3,4\}, A_4$为其偶置换群，
$A_4=\{(1),(12)(34),(13)(24),(14)(23),(123),(124),$
$(132),(134),(142),(143),(234),(243)\}, |A_4|=12$,,则可验证$A_4$无6阶子群. ■

4. 设p,q是素数，且$p\neq q$,试问$\mathbf{Z}_{pq}$有多少个生成元？
解 $pq(1-\frac{1}{p})(1-\frac{1}{q})$. ■

5. 设p是素数，整数$r\geq 1$.试问$\mathbf{Z}_{p^r}$有多少个生成元？
解 $p^r(1-\frac{1}{p})$. ■

6. 设G是Abel群，H,K,是G中的循环子群，它们的阶分别为r,s试证：
1) 若$(r,s)=1$，则G中有rs阶循环子群；
2) G中包含一个$[r,s]$阶的循环子群.
证明 设$H=\langle a\rangle, K=\langle b\rangle$,设$ab$的阶为$k$,则$(ab)^k=a^kb^k,\therefore s|k,t|k,\therefore [r,s]|k$.
另一方面，$(ab)^{[r,s]}=a^{[r,s]}b^{[r,s]}=1,\therefore k=[r,s].\therefore \langle ab\rangle$是$G$中的$[r,s]$阶循环子群.由2易推出1成立. ■

7. 设G是n阶群，且其不同的子群有不同的阶.试证：
1) G的任何子群都是正规子群；
2) G的子群与商群的不同子群也有不同的阶；
3) G是循环群.
证明 1) 设$H<G$,则$\forall g\in G, g^{-1}Hg<G$.又$|g^{-1}Hg|=|H|,\therefore g^{-1}Hg=H,\therefore H\lhd G$.
2) $\because \forall H<G, H$的子群也是G的子群.$\therefore H$的不同子群有不同的阶.G/H的子群与G中包含H的子群一一对应.G的不同子群有不同的阶，G/H的不同子群也有不同的阶. ■

8. 设群G只有有限个子群.证明G必为有限群.
证明 反设G为无限群，若$\exists g\in G, g$的阶为∞,则$\langle g\rangle\backsimeq\mathbf{Z}, \mathbf{Z}$有无限多个子群.矛盾！$\therefore G$中每个元素的阶有限，从而取$a\in G, \exists b\in G, b\in\langle a\rangle, \exists c\in G, c\in\langle a\rangle, c\in\langle b\rangle,\cdots$,依此类推，$G$有无限个子群，$\therefore G$必为有限群. ■

Chapter 2

环

2.1 分式域

1. 试问一个域作为整环其分式域是什么?

   解 这个域本身. ■

2. 令$\mathbf{Z}[\sqrt{-1}]=\{m+n\sqrt{-1}\mid m,n\in\mathbf{Z}\}$.证明$\mathbf{Z}[\sqrt{-1}]$是一个交换整环,并确定$\mathbf{Z}[\sqrt{-1}]$的分式域($\mathbf{Z}[\sqrt{-1}]$称为Gauss整数环).

   证明 易证$\mathbf{Z}[\sqrt{-1}]$是一个幺环,又因为$\mathbf{Z}[\sqrt{-1}]\subseteq\mathbf{C},\mathbf{C}$是域,从而$\mathbf{Z}[\sqrt{-1}]$是一个交换整环.设其分式域为$F$,显然$\mathbf{Q}[\sqrt{-1}]\subseteq F$,对任意$a,b,c,d\in\mathbf{Z}$,有:

   $$\frac{a+\sqrt{-1}\,b}{c+\sqrt{-1}\,d}=\frac{(a+\sqrt{-1}\,b)(c-\sqrt{-1}\,d)}{c^2+d^2}\in\mathbf{Q}[\sqrt{-1}],$$

   从而$\mathbf{Q}[\sqrt{-1}]\supseteq F$,所以$\mathbf{Q}[\sqrt{-1}]=F$ ■

3. 证明: $\mathbf{Z}[\sqrt{2}]=\{m+n\sqrt{2}\mid m,n\in\mathbf{Z}\}$是一个交换整环,并确定它的分式域.

   证明 易证$\mathbf{Z}[\sqrt{2}]$是一个幺环,又因为$\mathbf{Z}[\sqrt{2}]\subseteq\mathbf{C},\mathbf{C}$是域,从而$\mathbf{Z}[\sqrt{2}]$是一个交换整环.设其分式域为$F$,显然$\mathbf{Q}[\sqrt{2}]\subseteq F$,对任意$a,b,c,d\in\mathbf{Z}$,有:

   $$\frac{a+\sqrt{2}\,b}{c+\sqrt{2}\,d}=\frac{(a+\sqrt{2}\,b)(c-\sqrt{2}\,d)}{c^2+d^2}\in\mathbf{Q}[\sqrt{2}],$$

   从而$\mathbf{Q}[\sqrt{2}]\supseteq F$,所以$\mathbf{Q}[\sqrt{2}]=F$ ■

4. 设D是一个交换整环,$m,n\in\mathbf{N},(m,n)=1$.证明: $a,b\in D$满足$a^m=b^m,a^n=b^n$的充要条件是$a=b$.

证明 充分性显然,下证必要性:
因为$(m,n)=1$,所以$\exists s,t\in\mathbf{Z}$, 使得$ms+nt=1$,
故$a=a^1=a^{ms+nt}=b^{ms+nt}=b^1=b$. ■

5. 证明一个交换幺半群若满足消去律(即从$ab=ac$可推出$b=c$),则可嵌入到一个Abel群中.此命题对满足消去律的交换半群成立吗?

证明 同定理2.1.1的方法.定理2.1.1中,只考虑R的乘法,则R关于乘法成交换半群.证明过程中只用到了R满足消去律. 于是R便可嵌入到一Abel群中.知此结论成立.且对满足消去律的交换半群亦成立. ■

6. 设D为整环,$D^*=D-\{0\}$.若$\forall a,b\in D^*,\exists a_1,b_1\in D^*$ 使$ab_1=ba_1$,则称D满足右公倍性质,且称$m=ab_1=ba_1$为a,b的一个右公倍元.又设D为满足右公倍性质的整环.在$D\times D^*$中定义关系$\sim$: $(a,b)\sim(c,d)$,若有$d_1,b_1\in D^*$使$db_1=bd_1$,则有$ad_1=cb_1$.试证下列命题:
1) 关系$\sim$是等价关系
2) 以$\frac{a}{b}$表示(a,b)的等价类.若在商集合$F=D\times D^*/\sim$中定义加法与乘法如下:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad_1+cb_1}{m}$$

(其中$m=bd_1=db_1$为b,d的右公倍元),

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac_2}{db_2}$$

(其中b_2,c_2满足$b_2\in D^*,c_2\in D,cb_2=bc_2$).则$F$是一个体.
3) D与F的一个子环D'同构.
4) $\forall x\in F,\exists a',b'\in D'$使$x=a'(b')^{-1}$.

7. 设R是交换环,S是R的乘法子半群,且S中任何元素都不是零因子.在$R\times S$中可如定理2.1.1一样定义同余关系.商集合记为RS^{-1}(或$Q(R,S)$).试证:
1) RS^{-1}为交换幺环;
2) R可嵌入RS^{-1}中;
3) $\forall a\in S\subseteq RS^{-1}$,$a$为可逆元.

证明 1)由定理2.1.1的证明知,只需验证加法,乘法定义的合理性.
$\forall s_1,s_2\in S,r_1,r_2\in R$,

$$\frac{r_1}{s_1}+\frac{r_2}{s_2}=\frac{r_1s_2+r_2s_1}{s_1s_2}\in RS^{-1}$$

$$\frac{r_1}{s_1}\cdot\frac{r_2}{s_2}=\frac{r_1r_2}{s_1s_2}\in RS^{-1}$$

所以RS^{-1}为交换幺环.

2),3)则需把R改为交换幺环才是正确的. ■

8. 令$R=\mathbf{Z}_4, S=\{1,3\}$.求$RS^{-1}$.

   解 $RS^{-1}=\{0,1/1,2/1,3/1,1/3,2/3,3/3\}$, 由于$2/1=2/3, 1/1=3/3, 3/1=1/3$. 故$RS^{-1}$与$\mathbf{Z}_4$同构. ■

9. 令$R=\mathbf{Z}, S=\{2^n \mid n\in\mathbf{N}$.求$RS^{-1}$.

   解 $RS^{-1}=\{\frac{k}{2^n}|k\in\mathbf{Z},(2,k)=1,n\in\mathbf{N}\}$ ■

10. 令$R=3\mathbf{Z}, S=\{6^n \mid n\in\mathbf{N}\}$.证明$RS^{-1}$与$\mathbf{R}$中子环$\{\frac{m}{6^n} \mid m\in\mathbf{Z}, n\in\mathbf{Z}^+\}$同构.

    证明 作$\varphi: RS^{-1}\to\{\frac{m}{6^n}|m\in\mathbf{Z},n\in\mathbf{Z}^+\}$, 满足
    $\varphi((3x,6^n))=\dfrac{3x}{6^n}, \quad \forall x\in\mathbf{Z}, n\in\mathbf{N}$. 显然$\varphi$是单同态.
    $\forall m\in\mathbf{Z}, n\in\mathbf{Z}^+, \varphi((3\cdot 2m, 6^{n+1}))=\dfrac{m}{6^n}$.
    所以φ是满同态.
    综上RS^{-1}与$\{\frac{m}{6^n} \mid m\in\mathbf{Z}, n\in\mathbf{Z}^+\}$ ■

11. 设R是交换环,R_1为R的非零因子的集合.又若另一交换环$K\supseteq R$,且$\forall a\in R_1, a$在K中有逆元素,证明RR_1^{-1}一定与K中一个子环同构.

    证明 $\forall r\in R, a\in R_1$, 定义同态$\varphi: r/a\to ra^{-1}\in K$. 由于$a^{-1}=0$.
    从而φ是一个单同态,故RR_1^{-1}与K的一个子环同构. ■

2.2 多项式环

1. 设R是交换整环,$R[x]$是R上的一元多项式环,$f,g\in R[x]$.证明:

   $$\deg(fg)=\deg f+\deg g.$$

   (试问对一般的交换幺环,上式是否成立?)

   证明 令$f(x)=\sum\limits_{i=0}^{n}a_ix^i, g(x)=\sum\limits_{j=0}^{m}b_jx^j, (a_n,b_m\neq 0)$. 此时$\deg f=n, \deg g=m$. 则$f(x)g(x)=\sum\limits_{i=0}^{n}\sum\limits_{j=0}^{m}a_ib_jx^{i+j}=\sum\limits_{k=0}^{m+n}(\sum\limits_{i+j=k}a_ib_jx^k)$. 若$R$是交换整环,$a_nb_m\neq 0$, 从而$\deg(fg)=m+n$. 所以$\deg(fg)=\deg f+\deg g$.
   若R是交换幺环,取a_n使得$a_nb_m=0$, 此时$\deg(fg)\leq m+n$. 所以交换幺环上不成立. ■

2. 设R是交换整环,F是R的分式域,$F[x]$是F上一元多项式环.证明$R[x]$是R上的一元多项式环,且$R[x]$与$F[x]$有相同的分式域.

证明 设$R[x],F[x]$的分式域分别为K,E. 我们已知$E=F(x),K\subseteq E$. 为证$E\subseteq K$, 取$f,g\in F[x]$, 则$\frac{f(x)}{g(x)}\in E$. 由于f,g中系数都是$\frac{r}{s},r,s\in R$的形式,故存在$r_0,s_0\in R$, 使得$f(x)=\frac{f_1(x)}{r_0},g(x)=\frac{g_1(x)}{s_0},f_1(x),g_1(x)\in R[x],\frac{f(x)}{g(x)}=\frac{s_0f_1(x)}{r_0g_1(x)},s_0f_1(x),r_0g_1(x)\in g[x]$. 于是$E\subseteq K$. 综上$E=K$. ■

3. 设$\mathbf{Q}$为有理数域.证明$\omega=-1/2+\sqrt{-3}/2$在Q上是代数的,且$\mathbf{Q}[\omega]\simeq\mathbf{Q}[x]/\langle x^2+x+1\rangle$.

   证明 作$\varphi:\mathbf{Q}[x]\to\mathbf{Q}[\omega]$, 使得$\varphi(f(x))=f(\omega),\forall f(x)\in\mathbf{Q}[x]$, 易证$\varphi$是满同态,且$\ker\varphi=\langle x^2+x+1\rangle$, 所以$\mathbf{Q}[\omega]\simeq\mathbf{Q}[x]/\langle x^2+x+1\rangle$. ■

4. 证明$u=\sqrt{2}+\sqrt{3}$在Q上代数的,并求Q[x]中理想I,使得$\mathbf{Q}[u]\simeq\mathbf{Q}[x]/I$.

   证明 因为$u^4-10u^2+1=0$, 所以u在$\mathbf{Q}$上是代数元.
   作$\varphi:\mathbf{Q}[x]\to\mathbf{Q}[u]$, 使得$\varphi(f(x))=f(u),\forall f(x)\in\mathbf{Q}[x]$, 易证$\varphi$是满同态,且$\ker\varphi=\langle x^4-10x^2+1\rangle,(x^4-10x^2+1$是$\mathbf{Q}$中不可约多项式), 所以$\mathbf{Q}[u]\simeq\mathbf{Q}[x]/\langle x^4-10x^2+1\rangle$. ■

5. 设I是交换幺环R的理想.令$I[x_1,x_2,\ldots,x_n]$是$R[x_1,x_2,\ldots,x_n]$中系数在I中的多项式集合.证明:
   1) $I[x_1,x_2,\ldots,x_n]$是$R[x_1,x_2,\ldots,x_n]$的理想;
   2) $R[x_1,x_2,\ldots,x_n]/I[x_1,x_2,\ldots,x_n]\simeq(R/I)[y_1,y_2,\ldots,y_n]$, 这里$y_1,y_2,\ldots,y_n$ 在R/I上代数无关.

   证明 1)由多项式运算法则,$I[x_1,\cdots,x_n]$构成环是显然的.现对于$f\in R[x_1,\cdots,x_n],g\in[x_1,\cdots,x_n]$, 则$fg$各项系数将有形式
   $c=\sum\limits_{1\le i_s,j_t\le n}a_{i_1\cdots i_n}b_{j_1\cdots j_n}$.
   由于$a_{i_1\cdots i_n}\in R,b_{j_1\cdots j_n}\in I$, 故$c\in I,fg\in I[x_1,\cdots,x_n]$.

   2)设$f=\sum\limits_{i_1\cdots i_n}a_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}\in R[x_1,\cdots,x_n]$, 其中$a_{i_1\cdots i_n}\in R$,记$a_{i_1\cdots i_n}$ 在R/I中像为$\overline{a_{i_1\cdots i_n}}$.
   则作$\varphi:R[x_1,\cdots,x_n]\to(R/I)[y_1,\cdots,y_n],\varphi(x_i)=y_i,\varphi(r)=\overline{r},\forall r\in R$. φ显然是一个满同态.若$f\in\operatorname{Ker}\varphi$, 由于$y_i$在$R/I$上代数无关,必有$\overline{a_{i_1\cdots i_n}}=0$, 即$a_{i_1\cdots i_n}\in I,\forall 1\le i_1,\cdots,i_n\le n$, 亦即$f\in I[x_1,\cdots,x_n]$. 由于上述过程反之亦成立.故$\operatorname{Ker}\varphi=I[x_1,\cdots,x_n]$, 综上知
   $R[x_1,x_2,\ldots,x_n]/I[x_1,x_2,\ldots,x_n]\simeq(R/I)[y_1,y_2,\ldots,y_n]$. ■

6. 设R是一个环.令

$$R\langle x\rangle=\left\{(a_0,a_1,\ldots,a_n,\ldots)=\sum_{n=0}^{\infty}a_nx^n\mid a_n\in\mathbf{R}\right\}$$

在$R\langle x\rangle$中定义加法与乘法如下:

$$\left(\sum_{n=0}^{\infty}a_nx^n\right)+\left(\sum_{n=0}^{\infty}b_nx^n\right)=\left(\sum_{n=0}^{\infty}(a_n+b_n)x^n\right);$$

$$\left(\sum_{n=0}^{\infty}a_nx^n\right)\cdot\left(\sum_{n=0}^{\infty}b_nx^n\right)=\sum_{n=0}^{\infty}\left(\sum_{i+j=n}a_ib_j\right)x^n.$$

证明$R\langle x\rangle$是一个环(称为R上的**形式幂级数环**).

证明 验证$R\langle x\rangle$对加法成Abel群,对乘法成半群.加法与乘法间满足分配律即可,这些都是显然的. ■

7. 设M是一个幺半群,R是交换幺环.令

$$R[M]=\{f\mid f:M\to R,\mid M-f^{-1}(0)\mid<\infty\}.$$

在$R[M]$中定义加法与乘法如下:

$$(f+g)(m)=f(m)+g(m),$$

$$(f\cdot g)(m)=\sum_{p\,q=m}f(p)g(q).$$

证明$R[M]$为一环(称为M在R上的**幺半群环**或**幺半群代数**).

证明 $R[M]$实为M上只有有限点取值非零的R函数的全体.从而若$f,g\in R[M],f-g,fg$ 也$\in R[M]$, 逐一验证环的条件可证. ■

8. 设R为交换幺环,M为非负整数对加法构成的幺半群.证明M在R上的幺半群环$R[M]$与R上一元多项式环$R[x]$同构.

证明 $\forall f\in R[M]$, 设f取非零值的整数为$c_1,\cdots,c_n$, 令$a_i=f(c_i)$, $f(c)=0,c\neq c_i(i=1,2,\cdots,n)$. 则作映射:$f\to\sum a_ix^i$. 由$R[M]$ 中运算法则知此映射为环同态. 由$R[M]$定义知,此映射是满射.面若$a_i=0,\forall i$, 则$f\equiv0$为$R[M]$中零元,故此映射是单射,综上知$R[M]\simeq R[x]$. ■

2.3 对称多项式

1. 将Newton对称幂和s_1,s_2,s_3,s_4与s_5用初等对称多项式表示出来.

解 $s_1=p_1,\quad s_2=p_1^2-2p_2,\quad s_3=p_3-3p_1p_2+3p_3,$
$s_4=p_1^4-4p_1^2p_2+2p_2^2+4p_1p_3-4p_4.$ ■

2. 设s_k为Newton对称幂和,p_i为初等对称多项式.又

$$s_k = \sum a_{\lambda_1\lambda_2\cdots\lambda_n} p_1^{\lambda_1} p_2^{\lambda_2}\cdots p_n^{\lambda_n}, \sum_{j=1}^{n} j\lambda_j = k.$$

1) 试求出关于$a_{\lambda_1,\lambda_2\cdots\lambda_n}$的递推公式.

$$a_{\lambda_1\lambda_2\cdots\lambda_n} = a_{(\lambda_1-1)\lambda_2\cdots\lambda_n} - a_{\lambda_1(\lambda_2-1)\cdots\lambda_n} + \cdots[+(-1)^{k-1}k];$$

(此处方括号内的项仅在$\lambda_k = 1, \lambda_i = 0, i \neq k$时才出现,而且作为单独一项出现,令一切具有负下标的a等于零.)

2) 证明这个递推关系式的解是

$$a_{\lambda_1\lambda_2\cdots\lambda_n} = (-1)^{\lambda_2+\lambda_4+\lambda_6+\cdots} k(\lambda_1+\lambda_2+\cdots+\lambda_{n-1})/\lambda_1!\lambda_2!\cdots\lambda_n!$$

3. 设环$R \subseteq \mathbf{C}$.证明Newton对称幂和$s_1, s_2, \ldots, s_n$是代数无关的.且$R[p_1, p_2, \cdots, p_n] = R[s_1, s_2, \cdots, s_n]$. 这里$p_1, p_2, \cdots, p_n$是初等对称多项式.

证明 设有$a_1, \cdots, a_n \in R$, 使得$a_1s_1+\cdots+a_ns_n = 0$, 则由于$x_1, \cdots, x_n$无关,有$a_1x_1+a_2x_2+\cdots+a_nx_n = 0, 1 \leq i \leq n$. 从而易知$a_i = 0, 1 \leq i \leq n$, 即$s_1, s_2, \cdots, s_n$ 在R上代数无关.对后一断言,只要证明$p1, \cdots, pn$与$s_1, \cdots, s_n$ 可以相互表出,而这已经由定理2.3.3和Newton公式所保证. ■

4. 设$n > 4$.用初等对称多项式表示$s(x_1^2x_2), s(x_1^2x_2^2)$.再用Newton对称幂和$s_k$表示它们.

解 $s(x_1^2x_2) = \sum_{i=1}^{2}(p_1 - x_i) = p_1\sum_{i=1}^{n} x_i^2 - \sum_{i=1}^{n} x_i^3 = s_1s_2 - s_3$

$s(x_1^2x_2^2) = \frac{1}{2}\sum_{i=1}^{n} x_i^2(s_2 - x_i^2) = \frac{1}{2}\sum_{i=1}^{n} x_i^2 - \frac{1}{2}\sum_{i=1}^{n} x_i^4 = \frac{1}{2}s_2^2 - \frac{1}{2}s_4.$ ■

5. 证明$D = \prod_{1\leq i\leq j\leq n}(x_i - x_j)^2$是对称函数.当$n = 2, 3$时,用初等对称多项式表示$D$.

证明 显然D是对称函数.

$n = 2$时, $D = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = p_1^2 - 4p_2$

$n = 3$时, $D = (x_1 - x_2)^2(x_2 - x_3)^2(x_1 - x_3)^2 = p_1^2p_2^2 - 4p_1^3p_3 - 4p_2^3 + 27p_1p_2p_3 - 27p_3^2$ ■

6. 证明:当$R = \mathbf{R}, x_1, x_2, \cdots, x_n \leq 0$时,$p_k \leq p_1^k/k_1$.

证明 使用数学归纳法:显然$p_1 = p_1$,假设$p_1^{(k-1)} \geq (k-1)!p_{k-1}$, 则$p_1^k = p_1^{(k-1)}p_1 \geq (k-1)!p_{k-1}p_1 \geq (k-1)!(kp_k) = k!p_k$. ■

7. 任给n个非负实数$a_1, a_2, \cdots, a_n$,试证

$$\left(\prod_{j=1}^{n}(1+a_j)\right)^{1/n} \leq 1+\left(\prod_{j=1}^{n} a_j\right)^{1/n}$$

证明 只需证$\prod j=1^n(1+a_j) \geq (1+(\prod_{j=1}^{n} a_j)^{\frac{1}{n}})^n = \sum_{k=0}^{n} C_n^k(p_n)^{\frac{k}{n}}$
注意到$\prod j=1^n(1+a_j) = 1+\sum_{k=1}^{n} p_k$, 只需证$p_k \geq C_n^k(p_n)^{\frac{k}{n}}$, 由均值不等式,得证. ■

8. 证明:$x^n+x^{-n}=f(y)$,其中$y=x+x^{-1}, f(y)\in \mathbf{Z}[y]$.

证明 $n=1$时,$f_1(y)=y$,
$n=2$时, $f_2(y)=y^2-2$
假设$n\leq N$时, $f_n(y)\in \mathbf{Z}[y]$.
因为$f_N(y)f_1(y)=f_{(N+1)}(y)-f_{(N-1)}(y)$
所以$f_{(N+1)}(y)=f_N(y)f_1(y)-f_{(N-1)}(y)$,
所以$f_{(N+1)}(y)\in \mathbf{Z}[y]$,得证. ■

9. 令$s_{-k}=\sum_{i=1}^{n} x_i^{-k}, k=1,2,\cdots$.试建立$s_{-k}$与初等对称多项式$p_1, p_2, \ldots p_n$间的关系.

10. 证明三次方程$x^3+a_1x^2+a_2x+a_3=0$的三个根为等差数列的条件是$2a_1^3-9a_1a_2+27a_3=0$.

证明 记方程的三个根为x_1, x_2, x_3,由韦达定理知

$$\begin{cases} x_1+x_2+x_3 &= -a_1 \\ x_1x_2+x_2x_3+x_3x_1 &= a_2 \\ x_1x_2x_3 &= -a_3 \end{cases} \tag{2.1}$$

令$f=2a_1^3-9a_1a_2+27a_3$,将(2.1)代入f得
$f=(x_1+x_2-2x_3)(x_1+x_3-2x_2)(x_2+x_3-2x_1)$
"$\Rightarrow$" x_1, x_2, x_3成等差数列,所以$f=0, \Rightarrow 2a_1^3-9a_1a_2+27a_3=0$
"$\Leftarrow$" $2a_1^3-9a_1a_2+27a_3=0$,即$f=0$,所以$x_1+x_2=2x_3, x_1+x_3=2x_2, x_2+x_3=2x_1$至少有一个成立.所以$x_1, x_2, x_3$成等差数列. ■

2.4 唯一析因环

1. 证明$\mathbf{Z}[\sqrt{-5}]$满足因子链条件.

证明 定义范数$N(a+b\sqrt{-5})=a^2+5b^2,(a,b\in\mathbf{Z})$, 则$\forall\, x,y\in\mathbf{Z}[\sqrt{-5}]$, $x|y\Leftrightarrow N(x)|N(y)$, 故因子链条件成立. ■

2. 证明$\mathbf{Z}[\sqrt{-3}]$满足因子链条件但非唯一析因环.

证明 定义范数$N(a+b\sqrt{-3})=a^2+3b^2,(a,b\in\mathbf{Z})$, 则$\forall\, x,y\in\mathbf{Z}[\sqrt{-3}]$, $x|y\Leftrightarrow N(x)|N(y)$, 故因子链条件成立.
因为$4=(1+\sqrt{-3})(1-\sqrt{-3})=2\times 2$, 易证, $1+\sqrt{-3},1-\sqrt{-3},2$ 都是$\mathbf{Z}[\sqrt{-3}]$中的不可约元素,且2与$1+\sqrt{-3}$不相伴, 故$\mathbf{Z}[\sqrt{-3}]$ 不是唯一析因环. ■

3. 证明$\mathbf{Z}[\sqrt{10}]$不是唯一析因环.

证明 定义范数$N(a+b\sqrt{10})=|a^2-10b^2|,(a,b\in\mathbf{Z})$. 则$\forall\, x,y\in\mathbf{Z}[\sqrt{10}],x|y\Leftrightarrow N(x)|N(y)$. 显然$31=(3+2\sqrt{10})(3-2\sqrt{10})=(11+3\sqrt{10})(11-3\sqrt{10})$. 因为$N(3+2\sqrt{10})=N(3-2\sqrt{10})=N(11+3\sqrt{10})=N(11-3\sqrt{10})=31$, 所以$3+2\sqrt{10},3-2\sqrt{10},11+3\sqrt{10},11-3\sqrt{10}$是不可约元素. 因为$\frac{11+3\sqrt{10}}{3+2\sqrt{10}},\frac{11-3\sqrt{10}}{3+2\sqrt{10}}\notin\mathbf{Z}[\sqrt{10}]$, 所以$3+2\sqrt{10}$与$11+3\sqrt{10},11-3\sqrt{10}$ 都不相伴, 故$\mathbf{Z}[\sqrt{10}]$ 不是唯一析因环. ■

4. 证明在$\mathbf{Z}[\sqrt{-3}]$中4与$2(1+\sqrt{-3})$无最大公因子.

证明 反设其最大公因子为d. $2,1+\sqrt{-3}$ 都是4与$(1+\sqrt{-3})$ 的公因子,则$2|d,1+\sqrt{-3}|d$. 因为$2,1+\sqrt{-3}$ 是$\mathbf{Z}[\sqrt{-3}]$ 中不相伴的不可约元素.所以$2(1+\sqrt{-3})|d$. 但$2(1+\sqrt{-3})\nmid 4$, 矛盾.所以4与$2(1+\sqrt{-3})$无最大公因子. ■

5. 证明$\sqrt{-3}$是$\mathbf{Z}[\sqrt{-3}]$的素元素.

证明 定义范数$N(a+b\sqrt{-3})=a^2+3b^2,(a,b\in\mathbf{Z})$, 若$\sqrt{-3}|ab,a,b\in\mathbf{Z}[\sqrt{-3}]$, 则$3|N(a)N(b)$, 从而$3|N(a)$ 或$3|N(b)$. $\mathbf{Z}[\sqrt{-3}]$中范数为3的只有$\sqrt{-3}$ 或$-\sqrt{-3}$, 所以$\sqrt{-3}|a$ 或$\sqrt{-3}|b$.
所以$\sqrt{-3}$ 是$\mathbf{Z}[\sqrt{-3}]$的素元素. ■

6. 设F是一个域.令

$$A=\left\{\sum_{i=1}^{n}a_ix^{\alpha_i}\,\middle|\,a_i\in F,\alpha_i\in\mathbf{Q},\alpha_i\geq 0,1\leq i\leq n\right\}$$

在A中定义加法和乘法如下:

$$\left(\sum_{i=1}^{n}a_ix^{\alpha_i}\right)+\left(\sum_{i=1}^{n}b_ix^{\beta_i}\right)=\sum_{i=1}^{n}a_ix^{\alpha_i}+b_ix^{\beta_i}$$

$$\left(\sum_{j=1}^{n}a_ix^{\alpha_j}\right)\cdot\left(\sum_{k=1}^{n}b_ix^{\beta_k}\right)=\sum_{j=1}^{n}\sum_{k=1}^{n}a_jb_kx^{\alpha_j+\beta_k}$$

证明A是交换整环,但不满足有限析因条件.

证明 A关于加法成Abel群,关于乘法成交换幺半群,加法与乘法间满足分配律是显然的.若$\sum\limits_{j=1}^{n} a_j x^{\alpha_j}, \sum\limits_{k=1}^{n} b_k x^{\beta_k} \in A$, 且$\sum\limits_{k=1}^{n} b_k x^{\beta_k} \neq 0$.

若$0 = (\sum\limits_{j=1}^{n} a_j x^{\alpha_j})(\sum\limits_{k=1}^{n} b_k x^{\beta_k})$

$= \sum\limits_{j=1}^{n}\sum\limits_{k=1}^{n} a_j b_k x^{\alpha_j+\beta_k} = \sum\limits_{j=1}^{n} a_j x^{\alpha_j} \sum\limits_{k=1}^{n} b_k x^{\beta_k}$,

则$a_j = 0, j = 1, 2, \cdots, n$. 所以$\sum\limits_{j=1}^{n} a_j x^{\alpha_j} = 0$. 所以$A$无零因子,$A$是交换整环. $(x-1) = (x^{\frac{1}{2}}+1)(x^{\frac{1}{4}}+1)(x^{\frac{1}{8}}+1)\cdots(x^{\frac{1}{2^n}}+1)(x^{\frac{1}{2^n}}-1)$, 而由分析知识知$\dfrac{1}{(x^{\frac{1}{2^n}}+1)} \notin A$, 所以$(x^{\frac{1}{2^n}}+1) \notin$ U.所以$x-1$ 无限析因,A不满足有限析因条件. ■

7. 设R是UFD,$a, b \in R^*$.如$m \in R$满足:
1) m是a, b的公倍式,即$a \mid m, b \mid m$;
2) 若n也是a, b的公倍式.则$m \mid n$.
m称为a, b的**最小公倍式**.试证下列结论:
1) 若m是a, b的最小公倍式,则当且仅当$m_1 \sim m$时,m_1也是a, b的最小公倍式;
2) R^*中任意两个元素都有最小公倍式;
3) 以$[a, b]$表示a, b的一个最小公倍式,则有
$[(a, b)[a, b] \sim ab, \quad [a, (b, c)] \sim ([a, b], [a, c])$.

证明 1) "⇒" 因为m是a, b的公倍式,所以$a|m, b|m$,由$m_1 \sim m$知$m|m_1$从而$a|m_1, b|m_1$,所以m_1是a, b的公倍式.
a, b的任一公倍式m',有$m|m'$(m是最小公倍式),由$m_1 \sim m$知$m_1|m$, 从而$m_1|m'$,所以m_1是a, b的最小公倍式.
"⇐" m_1是a, b的最小公倍式,m是a, b的最小公倍式,所以$m_1|m$.
m是a, b的最小公倍式,m_1是a, b的最小公倍式,所以$m|m_1$.
所以$m_1 \sim m$.

2) $\forall a, b \in R^*$,若$a \in$ **U**,则b为a, b 的最小公倍式.若$b \in$ **U**,则a为a, b的最小公倍式.若$a, b \in R^* -$ **U**,由R是UFD知a有分解:
$a = uP_1^{n_1}P_2^{n_2}\cdots P_r^{n_r}$,同样有$b = vP_1^{m_1}P_2^{m_2}\cdots P_r^{m_r}$,其中$u, v \in$ **U**,
$P_1, P_2, \ldots, P_r$ 为互不相伴的不可约元素,n_i, m_i为非负整数.取
$k_i = \max(n_i, m_i)$,易知$m = P_1^{k_1}P_2^{k_2}\cdots P_r^{k_r}$为$a, b$的最小公倍式.

3)$(a, b)[a, b] \sim ab$. 只需证
$\min(m, n)\max(m, n) = mn$, 这显然$[a, (b, c)] \sim ([a, b], [a, c])$, 只需证$\max[k, \min(m, n)] = \min[\max(k, m), \max(k, n)]$. 讨论$k \geq m \geq$

$n, m \geq k \geq n, m \geq n \geq k$ 这三种情况,结果相等.得证. ■

8. 证明$\mathbf{Z}$上一元多项式环$\mathbf{Z}[x]$是UFD.

证明 唯一析因环上的多项式环是唯一析因环. ■

9. 设R, R'都是交换整环,R是UFD,又φ是R到R'上的同态.试问R'是否UFD? 若是,请证明;若不是,请举例说明.

解 R'不一定是UFD.反例:
设$R = \mathbf{Z}[x], R' = \mathbf{Z}[\sqrt{-3}], \varphi'$是$\mathbf{Z} \to \mathbf{Z}[\sqrt{-3}]$的嵌入映射为同态,且$\varphi'(1) = 1$, 所以$\varphi'$ 可唯一地扩充为$\varphi : \mathbf{Z}[x] \to \mathbf{Z}[\sqrt{-3}]$ 的同态,使$\varphi(x) = \sqrt{-3}$. 且$\forall\, a + b\sqrt{-3} \in \mathbf{Z}[\sqrt{-3}]$有原象$a + bx \in \mathbf{Z}[x]$. 所以$\varphi$是$\mathbf{Z}[x] \to \mathbf{Z}[\sqrt{-3}]$的满同态. 由本节第8题知$\mathbf{Z}[x]$是UFD,
而$\mathbf{Z}[\sqrt{-3}]$不是UFD. ■

2.5 主理想整环与Euclid环

1. 设R是一个主理想整环,$a \in R$,且$a \neq 0$.证明:
1) 当a为素元素时$R/\langle a\rangle$是域;
2) 当a不是素元素是$R/\langle a\rangle$不是整环.

证明 1)考虑$R/\langle a\rangle$的理想,它们与R中包含$\langle a\rangle$的理想一一对应,如存在I满足$\langle a\rangle \subset I \subset R$,设$I = \langle b\rangle$,则有$b|a$,于是$b = 1$或$b = a$,故$R/\langle a\rangle$只有二个理想,从而是域.

2)设$a = bc,\ b, c \notin U$.则$(b + \langle a\rangle) \cdot (c + \langle a\rangle) = 0$,从而$R/\langle a\rangle$不是整环. ■

2. 设R是主理想整环,R_1是交换整环,且$R_1 \supseteq R$.又设$a, b \in R^*$,d为a, b在R中最大公因子.证明d也是a, b在R_1中最大公因子.

证明 记d是a, b在R 中的最大公因子,则在R中$d|a, d|b$.所以d也是a, b在R 中的最大公因子. 下设c是a, b在R_1中的任一公因子.因为R是p.i.d.,所以$\exists u, v \in R \subseteq R_1$,使得$d = ua + vb$.因为$c|a, c|b$,所以$c|d$,所以$d$是$a, b$ 在R_1中的最大公因子. ■

3. 设R主理想整环,I是R的理想,且$I \neq \{0\}$.试证:
1) R/I的每个理想都是主理想;
(问R/I是主理想整环吗?)
2) R/I中仅有有限多个理想.

证明 1)设$I = \langle a\rangle, a \in R, R/I$的每个理想与$R$中包含$\langle a\rangle$的理想一一对应.若$\langle a\rangle \subseteq \langle b\rangle$, 则有$b|a$,则$\langle b\rangle/I$是$R/I$的理想.显然$\langle b\rangle/I = \langle b + I\rangle$,所以$R/I$的每个理想都是主理想.

但是R/I不一定是主理想整环.由习题1.2)可知,取a不是素元素,即可得$R/\langle a\rangle$不是整环.

2)由1)知R/I的理想$\langle b+I\rangle$,必有$b|a$,由于R是UFD,故a在相伴意义下只有有限个因子,所以R/I仅有有限多个理想. ■

4. 设R是交换整环,但不是域.证明$R[x]$不是主理想整环.

证明 设$a\in R$无逆元,则$\langle a,x\rangle\subset R[x]$不是主理想. ■

5. 求$\mathbf{Z}[\sqrt{-1}]$中的单位.并把$2,3$与5在$\mathbf{Z}[\sqrt{-1}]$中分解为素元素的乘积.

解 设$\alpha=a+b\sqrt{-1}\in\mathbf{U}$.则$\alpha\cdot\alpha^{-1}=1$.两边取范数,有$N(\alpha)\cdot N(\alpha^{-1})=1$.因为$N(\alpha)$为非负整数,所以$N(\alpha)=1$,即$a^2+b^2=1,a,b\in\mathbf{Z}$.所以$\alpha=\pm1,\pm\sqrt{-1}$,且$\pm1,\pm\sqrt{-1}$均为可逆元.
故$\mathbf{U}=\{1,-1,\sqrt{-1},-\sqrt{-1}\}$.

1) $2=(1+\sqrt{-1})(1-\sqrt{-1})$.因为$\mathbf{Z}[\sqrt{-1}]$为Euclid环,所以$\mathbf{Z}[\sqrt{-1}]$为唯一析因环,故素元素与不可约元素是等价的,且2的"分解"唯一.下证$1+\sqrt{-1}$和$1-\sqrt{-1}$均为不可约元素:
反设$1+\sqrt{-1}$为可约元素,则必有非平凡真因子$a+b\sqrt{-1}$.使$1+\sqrt{-1}=(a+b\sqrt{-1})\cdot\beta,\beta\in\mathbf{Z}[\sqrt{-1}]$.两边取范数后可知:$(a^2+b^2)\cdot N(\beta)=2$.所以$a^2+b^2$知可能为$1,2$.
若$a^2+b^2=1$,则$a+b\sqrt{-1}\in\mathbf{U}$, 为平凡因子,矛盾;
若$a^2+b^2=2$,则$N(\beta)=1$,则$\beta\in\mathbf{U}$,从而$a+b\sqrt{-1}\sim1+\sqrt{-1}$.不是真因子,矛盾.所以$1+\sqrt{-1}$为不可约元素.完全类似知$1-\sqrt{-1}$也是不可约元素.

2) $5=(2+\sqrt{-1})(2-\sqrt{-1})$.与上面类似地,只需证$2\pm\sqrt{-1}$为不可约元素.反设$2+\sqrt{-1}$为可约元素,则必有非平凡真因子$a+b\sqrt{-1}$,使$2+\sqrt{-1}=(a+b\sqrt{-1})\cdot\beta,\beta\in\mathbf{Z}[\sqrt{-1}]$.两边取范数有$5=(a^2+b^2)N(\beta)$.所以$a^2+b^2$只可能是1或5.若$a^2+b^2=1$,则$a+b\sqrt{-1}\in\mathbf{U}$为平凡因子,矛盾.若$a^2+b^2=5$,则$N(\beta)=1\Rightarrow\beta\in\mathbf{U}$. 从而$a+b\sqrt{-1}$不是真因子,矛盾.所以$2+\sqrt{-1}$不可约.同理,$2-\sqrt{-1}$不可约.

3) 3是素元素.反设3为可约元素,则必有非平凡真因子$a+b\sqrt{-1}$使$3=(a+b\sqrt{-1})\beta,\beta\in\mathbf{Z}[\sqrt{-1}]$. 两边取范数,$9=(a^2+b^2)N(\beta)$,$a^2+b^2$只可能是$1,3,9$.若$a^2+b^2=1$,则$a+b\sqrt{-1}$为平凡因子,矛盾.

若$a^2+b^2=9$,则$\beta\in\mathbf{U}$,所以$a+b\sqrt{-1}$不是真因子,矛盾.若$a^2+b^2=3,a,b\in\mathbf{Z}$时无解.所以3为不可约元素,即为素元素. ■

6. 证明$R=\{a+\frac{b}{2}(1+\sqrt{-3})\mid a,b\in\mathbf{Z}\}$为Euclid 环.

证明 定义δ为:$\delta(a+\frac{b}{2}(1+\sqrt{-3}))=a^2+b^2$.对于$\alpha=a+\frac{b}{2}(1+\sqrt{-3}),\beta=c+\frac{d}{2}(1+\sqrt{-3}),\alpha\beta^{-1}\in\mathbf{Q}(\sqrt{-3})$,记$\alpha\beta^{-1}=u+v\sqrt{-3}$, 则取$e,f\in$

$\mathbf{Z}$,使$|u-e| \leq \frac{1}{2}, |v-f| \leq \frac{1}{2}$, 则$\alpha = \beta(e + \frac{f}{2}(\sqrt{-3}+1) = c\epsilon - d\eta + \frac{d\eta+c\eta+d\epsilon}{2}(1+\sqrt{-3})$. 记右边为$\gamma$, 则$\delta(\gamma) < \delta(\beta)$. 得证$R$为Euclid环. ■

7. 设R为Euclid环,且$\delta(ab) = \delta(a)\delta(b)$.证明$a \in U \Leftrightarrow \delta(a) = \delta(1)$.

   证明 $\forall b \in R, \delta(b) = \delta(1)\delta(b)$,因为$\delta \neq 0$,所以$\delta(1) = 1$
   "$\Rightarrow$"$\forall a \in U, \delta(a)\delta(a^{-1}) = \delta(1) = 1$,所以$\delta(a) = \delta(1) = 1$.
   "$\Leftarrow$" 若$\delta(a) = \delta(1) = 1$, 因为$0 = 0 \cdot 1 + 0$. 所以$1 = \delta(1) > \delta(0)$, 所以$\delta(0) = 0$.
   由Euclid环的定义知$\delta(b) = 0 \Leftrightarrow b = 0, \exists a, r \in R$ 满足$1 = q \cdot a + r, 1 = \delta(a) > \delta(r)$, 从而$r = 0$. a可逆. ■

8. 设R为Euclid环,且$\delta(ab) = \delta(a)\delta(b), \delta(a+b) \leq \max\{\delta(a), \delta(b)\}$.证明$R$或为一个域,或为一个域上的一元多项式环.

   证明 取$R_0 = \{a|\delta(a) \equiv 1\}$.则$\forall b \in R_0, \delta(-b) = \delta(-1)\delta(b) = 1, \delta(a+b) \leq \max\{\delta(a), \delta(b)\} = 1$. 所以$R_0 \cup \{0\}$是一个域.
   若$R = R_0$,则R是个域.否则取$x = \{b|\delta(b) = \min(\delta(a)), \delta(a) > 1\}$, 则$\forall a \in R, a \neq 0, \exists a_0, a_1$, 使得$a = a_1 x + a_0, \delta(a_0) < \delta(x)$. 从而$a_0 \in R_0 \cup \{0\}$.
   又因为$\delta(a_1)\delta(x) = \delta(a_1 x), \delta(a - a_0) \leq \max\{\delta(a), \delta(a_0)\} \leq \delta(a)$, 所以$\delta(a_1) < \delta(a)$.
   依此类推,直到$\delta(a_n) = 1$或0, 此时R是一个域上的一元多项式环(x是R上的超越元是显然的). ■

9. 证明任何一个域都是Euclid环.

   证明 设F为一个域,定义映射$\delta : F \to \mathbf{N} \bigcup \{0\}, \delta(0) = 0, \delta(a) = 1, \forall a \in F$ 且$a \neq 0$.则$\forall a, b \in F, b \neq 0, \exists ab^{-1} \in F$,使得$a = (ab^{-1})b + 0, \delta(0) < \delta(b)$.所以$F$是Euclid环. ■

10. 设R是一个环.称R中理想的**升链条件**成立(ACC),若任何R的严格递增的理想序列$N_1 \subset N_2 \subset N_3 \subset \cdots$是有限长的;称$R$中关于理想的**极大条件**成立(MC),如果$R$中每个理想的非空集合$S$包含一个理想,这个理想不真包含在$S$中的其它任何理想中; 称$R$中关于理想的**有限基条件**成立(FBC),如果R中每个理想N是有限生成的,即$N = \langle b_1, b_2, \cdots, b_n \rangle$.
    证明:ACC,MC与FBC三条件等价.

    证明 (ACC)$\Rightarrow$(MC): (MC)的逆命题就是存在这样的$S, \forall I \in S, \exists J \in S$, 使$I \subset J$, 但这显然会产生一个无限的理想升链,与(ACC)矛盾.
    (MC)$\Rightarrow$(FBC): 若I是不能被有限生成的,则必存在$\{a_i\}_{i \geq 1} \subset I$使$\langle a_1, \cdots, a_n \rangle \subset \langle a_1, \cdots, a_{n+1} \rangle$, 则$S = \{\langle a_1, \cdots, a_n \rangle | n \geq 1\}$构成了(MC) 的反例.

(FBC)⇒(ACC): 若有一个无限长的升链,则这个链的并不能被有限生成,却还是一个理想. ■

11. 若环R中严格递降理想序列$N_1 \supset N_2 \supset N_3 \supset \cdots$是有限长,则称$R$满足**降链条件**(DCC).若环$R$的一个理想的集合$S$中有一个理想不真包含$S$中任何理想,则称$R$满足**极小条件**(mC).证明:DCC与mC等价.

证明 与上题只是采用了不同的序关系,没有本质的不同. ■

12. 举一个满足ACC但不满足DCC的环的例子.

解 整数环$\mathbf{Z}$.
$\mathbf{Z}$是主理想整环,显然满足ACC,$\langle 2\rangle \supset \langle 2^2\rangle \supset \langle 2^3\rangle \supset \cdots \supset \langle 2^n\rangle \cdots$ 不满足DCC. ■

2.6 域上一元多项式环

1. $x^4+4 \in \mathbf{Z}_4[x]$,将其分解为不可约因式的积.

解 $x^4+4 = x^4-1 = (x^2+1)(x^2-1) = (x^2-4)(x^2-1)$
$= (x-1)(x-2)(x+1)(x+2)$. ■

2. 试问x^3+2x+8是$\mathbf{Q}[x]$中的不可约多项式吗?作为$\mathbf{Z}_5[x]$中的多项式是否不可约?若可约,试将它分解为不可约因式的积.

解 $x^3+2x+3 = (x+1)(x^2-x+3)$,其中$x+1, x^2-x+3$均为$\mathbf{Q}[x]$站的不可约多项式,故$x^2+2x+3$不是$\mathbf{Q}[x]$中的不可约多项式.从而它在$\mathbf{Z}_5[x]$中必可约(第6题结论).在$\mathbf{Z}_5[x]$中分解为$x^3+2x+3 = (x+1)(x^2-x+3) = (x+1)^2(x-2)$. ■

3. 证明$\forall\, a \in \mathbf{Z}$,($p$为素数),$x^p+a$在$\mathbf{Z}_p[x]$中都可约.

证明 $x^p+a = (x+a)^p$. ■

4. 求所有奇素数p,使得在$\mathbf{Z}_p[x]$中有
$x+2 \mid x^4+x^3+x^2-x+1$.

解 $\mathbf{Z}_p = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{p-1}\}$.当且仅当$x = \overline{p-2}$时$x+\overline{2} = \overline{0}$.所以$x+\overline{2} \mid x^4+x^3+x^2-x+\overline{1} \Longleftrightarrow (\overline{p-2})^4+(\overline{p-2})^3+(\overline{p-2})^2-\overline{p-2}+\overline{1} = \overline{0} \Longleftrightarrow \overline{p[(p-2)^2(p-3)+3p-13]+15} = \overline{0} \Longleftrightarrow p \mid 15$. 由于$p$为素数,所以$p=3$或$p=5$. ■

5. 设F是一个域,$f(x), g(x) \in F[x]$.证明
$N = \{u(x)f(x)+v(x)g(x) \mid u(x), v(x) \in F[x]\}$
是$F[x]$的理想,又若$\deg f(x) \neq \deg g(x), N \neq F[x]$,则$f(x), g(x)$至少有一个可约.

证明 $\forall u_1(x)f(x)+v_1(x)g(x), u_2(x)f(x)+v_2(x)g(x)\in N$,有
$(u_1(x)-u_2(x))f(x)+(v_1(x)-v_2(x))g(x)\in N$.
$\forall h(x)\in F(x), \forall u(x)f(x)+v(x)g(x)\in N$,有
$h(x)(u(x)f(x)+v(x)g(x))=(h(x)u(x))f(x)+(h(x)v(x))g(x)\in N$.
因为$F[x]$是可换环,所以$(u(x)f(x)+v(x)g(x))h(x)=$
$(u(x)h(x))f(x)+(v(x)h(x))g(x)\in N$.
所以N是$F[x]$的理想.

反设$f(x),g(x)$均不可约.若$f(x)\mid g(x)$.则$f(x)\in F^*$或$f(x)\sim g(x)$.当$f(x)\in F^*$时,取$v(x)=0$,则$N\subseteq\{u(x)f(x)\mid u(x)\in F[x]\}$,由此$N=F[x]$,矛盾;当$f(x)\sim g(x)$时,则$\deg f(x)=\deg g(x)$,也矛盾.故$f(x)\nmid g(x)$,同理$g(x)\nmid f(x)$.故$f(x)$与$g(x)$互素.所以存在$u_0(x),v_0(x)\in F[x]$,使$u_0(x)f(x)+v_0(x)g(x)=1$,故$1\in N$.因为$N$是理想,所以$\forall f(x)\in F[x]$,有$1\cdot f(x)\in N$,故$F[x]\subseteq N$,所以$N=F[x]$,矛盾.所以$f(x),g(x)$至少有1个可约. ■

6. 设$f[x]\in\mathbf{Z}[x]$.证明若$f(x)$作为$\mathbf{Z}_p[x]$中多项式不可约,则$f(x)$作为$\mathbf{Q}[x]$中多项式也不可约.

   证明 若$f(x)$作为$\mathbf{Q}[x]$上多项式可约,则$f(x)$作为$\mathbf{Z}[x]$上多项式可约,从而$f(x)$作为$\mathbf{Z}_p[x]$多项式可约.矛盾. ■

7. 设F是一个域,$f(x)\in F[x]$.证明$f(x)$含有一个非平凡的**平方因子**(即$\exists f_1(x)\in F[x]$,且$\deg f_1(x)>0$使$f_1^2(x)\mid f(x)$)的充要条件是$F[x]/\langle f(x)\rangle$含有非零的幂零元.

   证明 必要性: 设$f(x)$有平方因子$f_1(x)$,则$f(x)/f_1(x)$在$F[x]/\langle f(x)\rangle$中幂零.
   充分性: 设$g(x)+\langle f(x)\rangle$在$F[x]/\langle f(x)\rangle$中幂零,即有自然数$n>1, g^n(x)\subset\langle f(x)\rangle$,即$f(x)|g^n(x)$. 但同时又有$f(x)\nmid g(x)$.
   则$g(x)/[f(x),g(x)]$是$f(x)$的平方因子. ■

8. 设p是一个素数,$a_n\not\equiv 0(\mathrm{mod}\ p)$.证明同余式:
   $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv 0(\mathrm{mod}\ p)$
   在$\mathbf{Z}$中至多有n个非同余的解.

   证明 原命题等价于:$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$作为$\mathbf{Z}_p[x]$中多项式在$\mathbf{Z}_p$中至多有$n$个根. 由定理2.6.1推论3知这是显然的. ■

9. 设域F中只有q个元素$a_1,a_2,\cdots,a_q$.求证在$F[x]$中有
   $x^q-x=(x-a_1)(x-a_2)\cdots(x-a_q)$.

   证明 显然,$\forall i$,有$a_i^q=a_i$, 由上题,同余式$x^q-x\equiv 0(\mathrm{mod}\ p), (p=\mathrm{Ch}\ F)$仅有$a_1,\cdots,a_q$这$q$个根,故在$F$中,$x^q-x=(x-a_1)\cdots(x-a_q)$. ■

10. (**Wilson定理**)设p是素数,求证
$(p-1)!=-1(\mathrm{mod}\ p)$.

证明 由上题,在$E_p[x]$中,有$x^p-x=x(x-1)\cdots(x-p+1)$. 比较两边一次项系数即得结论. ■

11. 验证x^3-x在$\mathbf{Z}_6$中有6个根.

证明 $(\overline{0})^3-\overline{0}=\overline{0},(\overline{1})^3-\overline{1}=\overline{0},(\overline{2})^3-\overline{2}=\overline{0}$
$(\overline{3})^3-\overline{3}=\overline{0},(\overline{4})^3-\overline{4}=\overline{0},(\overline{5})^3-\overline{5}=\overline{0}$
所以$\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5}$都是$x^3-x$在$\mathbf{Z}_6$中的根. ■

12. 求多项式x^5-3x^3+2x在$\mathbf{Z}_{30}$中的根.

解 x^5-3x^3+2x
在$\mathbf{Z}_2$中的根为$\overline{0},\overline{1}$;
在$\mathbf{Z}_3$中的根为$\overline{0},\overline{1},\overline{2}$;
在$\mathbf{Z}_5$中的根为$\overline{0},\overline{1},\overline{4}$.
故x^5-3x^3+2x在$\mathbf{Z}_{30}$中的根为$\overline{0},\overline{1},\overline{4},\overline{5},\overline{6},\overline{9},\overline{10},\overline{11},\overline{14},\overline{15},$
$\overline{16},\overline{19},\overline{20},\overline{21},\overline{24},\overline{25},\overline{26},\overline{29}$. ■

13. 证明x^2+1在四元数体$\mathbf{H}$中有无穷多个根.

证明 $H=\left\{\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}\middle|\alpha,\beta\in\mathbf{C}\right\}$.设$\alpha=ae^{i\alpha},\beta=be^{i\beta}\in\mathbf{C}$.
令$\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}^2+1=0,$
则只要取$\alpha=ia,\beta=b,a^2+b^2=1$ 即可.这样的(α,β)有无限多组. ■

14. 设域F上多项式$f(x)=a_0x^2+a_1x+a_2,g(x)=b_0x^2+b_1x+b_2$.证明:
$4R(f,g)=(2a_0b_2-a_1b_1+2a_2b_0)^2-(4a_0a_2-a_1^2)(4b_0b_2-b_1^2)$.

证明 $R(f,g)=\begin{vmatrix}a_0 & a_1 & a_2 & 0\\ 0 & a_0 & a_1 & a_2\\ b_0 & b_1 & b_2 & 0\\ 0 & b_0 & b_1 & b_2\end{vmatrix}$
$=a_0^2b_2^2+a_0a_2b_1^2-2a_0a_2b_0b_2-a_0a_1b_1b_2+a_1^2b_0b_2+a_2^2b_0^2-a_1a_2b_0b_1$
$(2a_0b_2-a_1b_1+2a_2b_0)^2-(4a_0a_2-a_1^2)(4b_0b_2-b_1^2)$
$=4a_0^2b_2^2+4a_0a_2b_1^2-8a_0a_2b_0b_2-4a_0a_1b_1b_2+4a_1^2b_0b_2+4a_2^2b_0^2-4a_1a_2b_0b_1$
比较各项系数知:
$4R(f,g)=(2a_0b_2-a_1b_1+2a_2b_0)^2-(4a_0a_2-a_1^2)(4b_0b_2-b_1^2)$. ■

15. 求$f(x)=x^{n-1}+x^{n-2}+\cdots+x+1$与$g(x)=x^m-1$的结式$R(f,g)$.

16. 求$f(x)=x^{n-1}+x^{n-2}+\cdots+x+1$与$g(x)=x^{m-1}+x^{m-2}+\cdots+x+1$的结式$R(f,g)$.

2.7 唯一析因环的多项式环

1. 证明$x^4+1, x^6+x^3+1, x^4-x^3-2x^+1$都是整数环$\mathbf{Z}$上的一元多项式环$\mathbf{Z}[x]$中的不可约多项式.

   证明 1)若x^4+1可约.因为± 1不是x^4+1的根,所以x^4+1只能分解成两个二次多项式的乘积. 不妨设$x^4+1=(x^2+ax\pm 1)(x^2+bx\pm 1)$ 考察一次项与二次项系数得: $\pm(a+b)=0, ab\pm 2=0,$ 这与$a,b\in\mathbf{Z}$矛盾.所以x^4+1不可约.

   2)令$x=y+1$ 则$x^6+x^3+1=(y+1)^6+(y+1)^3+1$
   $=y^6+6y^5+15y^4+21y^3+18y^2+9y+3.$ 由Eisenstein判别法知$(y+1)^6+(y+1)^3+1$ 不可约,从而x^6+x^3+1 不可约.

   3)仿1)可得± 1不是x^4-x^3-2x+1的根,所以若x^4-x^3-2x+1可约,可分解成两个二次多项式乘积,仿1)即可得出矛盾. ■

2. 设$p_1,p_2,\cdots,p_r$是r个不同的素数,$m>1$.证明$(p_1p_2\cdots p_r)^{1/m}$是无理数.

   证明 若是有理数,设$(p_1p_2\cdots p_r)^{\frac{1}{m}}=\frac{a}{b}$ 既约,则$p_1p_2\cdots p_rb^m=a^m$. 则$p_1|a,$ 从而$p_1^m|a^m, p|b,$ 这与$\frac{a}{b}$既约矛盾. ■

3. 设$a_1,a_2,\cdots,a_n$是不同的整数.证明
   $(x-a_1)(x-a_2)\cdots(x-a_n)-1,$
   $(x-a_1)(x-a_2)\cdots(x-a_n)+1, \quad (n>4)$
   是$\mathbf{Q}[x]$中不可约多项式.

   证明 只须证原式在$\mathbf{Z}[x]$中不可约即可.
   设$(x-a_1)\cdots(x-a_n)-1=f(x)g(x), \quad f(x),g(x)\in\mathbf{Z}[x].$ 我们不妨假定$\deg(f(x))\leq 2$ 则$\forall 1\leq i\leq n, f(a_i)g(a_i)=-1,$ 则$f(a_i)=\pm 1$,即$f^2(x)=1$有n个不同的根,这是不可能的.
   同理可证$(x-a_1)(x-a_2)\cdots(x-a_n)+1$是$\mathbf{Q}[x]$中不可约多项式. ■

4. 设$f(x)$是$\mathbf{Z}[x]$中的首一多项式,α是$f(x)$的一个有理根.证明α是整数.

   证明 本题是下题的直接推论. ■

5. 设F是唯一析因环R的分式域,$f(x)$是$R[x]$中的首一多项式,又$g(x)$是$F[x]$ 中的首一多项式,且$g(x)\mid f(x)$.证明$g(x)\in R[x]$.

   证明 因为$g(x)|f(x)$,所以存在$h(x)\in F[x],$ 使得$f(x)=g(x)h(x).$ 由定理2.7.2,存在$g_1(x),h_1(x)\in R[x],$ 且$g_1(x)\overset{F}{\sim}g(x), h_1(x)\overset{F}{\sim}h(x),$
   $f(x)=g_1(x)h_1(x).$ 由$f(x)$首一,我们可假设此时$g_1(x),h_1(x)$也是首一多项式.因为$g_1(x)\overset{F}{\sim}g(x)$ 且都是首一多项式,故$g(x)=g_1(x)\in R[x].$ ■

6. 设π是$\mathbf{Z}$到$\mathbf{Z}_m$的自然同态,定义$\mathbf{Z}[x]$到$\mathbf{Z}_m[x]$的映射$\overline{\pi}$为

$$\overline{\pi}\left(\sum_{k=0}^{n} a_k x^k\right) = \sum_{k=0}^{n} \pi(a_k) x^k.$$

证明下列结论:
1) $\overline{\pi}$是同态映射.
2) 设$f(x) \in \mathbf{Z}[x], \deg f(x) = n$.又$\overline{\pi}(f(x))$在$\mathbf{Z}_m[x]$中不能分解为两个次数小于$n$的多项式的积, 则$f(x)$是$\mathbf{Q}[x]$中不可约多项式.
3) $x^3 + 17x + 36$在$\mathbf{Q}[x]$中不可约.

证明 1) $\forall f(x) = \sum\limits_{k=0}^{n} a_k x^k, g(x) = \sum\limits_{k=0}^{n} b_k x^k \in \mathbf{Z}[x]$ a_k, b_k可以为0.

$$\overline{\pi}(f(x)+g(x)) = \overline{\pi}(\sum_{k=0}^{n}(a_k+b_k)x^k) = \sum_{k=0}^{n}\pi(a_k+b_k)x^k$$
$$= \sum_{k=0}^{n}\pi(a_k)x^k + \sum_{k=0}^{n}\pi(b_k)x^k = \overline{\pi}(f(x)) + \overline{\pi}(g(x)).$$
$$\overline{\pi}(f(x)g(x)) = \overline{\pi}(\sum_{k=0}^{n}(\sum_{j+i=k} a_j b_i)x^k) = \sum_{k=0}^{n}\pi(\sum_{j+i=k} a_j b_i)x^k$$
$$= \sum_{k=0}^{n}(\sum_{j+i=k}\pi(a_j)\pi(b_i))x^k = \sum_{k=0}^{n}\pi(a_k)x^k \cdot \sum_{k=0}^{n}\overline{\pi}(b_k)x^k$$
$$= \overline{\pi}(f(x)) \cdot \overline{\pi}(g(x))$$
所以$\overline{\pi}$是同态映射.

2) 反设$f(x)$在$\mathbf{Q}[x]$中可约.由于Q是域,所以$\mathbf{U} = \mathbf{Q}^*$.故$f(x)$可分解为2个次数小于$n$的多项式的乘积, 即$\exists f_1(x), f_2(x) \in \mathbf{Z}[x]$,
$1 \le \deg f_i(x) < n, i = 1, 2$, 使$f(x) = f_1(x)f_2(x)$.则
$\overline{\pi}(f(x)) = \overline{\pi}(f_1(x)f_2(x)) = \overline{\pi}(f_1(x))\overline{\pi}(f_2(x))$.
于是$\overline{\pi}(f(x))$在$\mathbf{Z}_m[x]$中可以分解为2个次数小于n的多项式的积,矛盾.
所以$f(x)$是$\mathbf{Q}[x]$中不可约多项式.

3) 取$m = 5$,则
$\overline{\pi}(f(x)) = \overline{\pi}(x^3 + 17x + 36) = x^3 + 2x + 1$, $\mathbf{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$
若$x^3 + 2x + 1$在$\mathbf{Z}_5[x]$中可分解为两次数小于3的多项式积,则必有1次因式,设为$x - c$. 则有$c^3 + 2c + 1 = 0, c \in \mathbf{Z}_5$.即
$5 \mid c^3 + 2c + 1, c = 0, 1, 2, 3, 4$.这显然是不可能的.
所以$x^3 + 2x + 1$在$\mathbf{Z}_5[x]$中不可分解为次数低于3的多项式.
所以$x^3 + 17x + 36$在$\mathbf{Q}[x]$中不可约. ■

7. 证明$xy + y + 1, xy + x$在$\mathbf{Q}$上是互素的.但不存在$\mathbf{Q}$上多项式f与g使$f(x, y)(xy + y + 1) + g(x, y)(xy + x) = 1$.

证明 设$d = (xy + y + 1, xy + x) = (x(y + 1), y - x + 1)$, 故在相伴意义下,$d$只能是$1, x, y + 1$或$xy + x$. 因为$x \nmid y - x + 1, y + 1 \nmid y - x + 1$, 所

以$d=1$. 反设存在$f(x,y),g(x,y)\in\mathbf{Q}[x,y]$ 使得$f(x,y)(xy+y+1)+g(x,y)(xy+x)=1$. 令$x=0$ 得$f(0,y)(y+1)=1$, 右边次数为0,左边次数≥ 1. 矛盾. ■

8. 试证n^2元多项式

$$\begin{vmatrix} x_{11} & x_{12} & \cdot & x_{1n} \\ x_{21} & x_{22} & \cdot & x_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ x_{n1} & x_{n2} & \cdot & x_{nn} \end{vmatrix}$$

是整环$R[x_{11},x_{12},\cdots,x_{1n}\cdots,x_{n1},x_{n2},\cdots,x_{nn}]$中的不可约多项式.

证明 当$n=1$时,结论显然成立.假设$n=k-1$时结论成立.当$n=k$时,x_{kk}的系数是$\begin{vmatrix} x_{11} & x_{12} & \cdot & x_{1,k-1} \\ x_{21} & x_{22} & \cdot & x_{2,k-1} \\ \cdot & \cdot & \cdot & \cdot \\ x_{k-1,1} & x_{k-1,2} & \cdot & x_{k-1,k-1} \end{vmatrix}=A$, 则原多项式为$Ax_{kk}+B(B$中不含$x_{kk})$. 若多项式可约,$A|B$. 令$x_{ij}=1\quad(1\leq i,j\leq k-1)$ 则$A=0,Ax_{kk}+B\equiv 0$. 但原行列式显然$\neq 0$, 矛盾.所以原多项式不可约. ■

9. 设F是一个域.$S\subseteq F\times F\times\cdots\times F(n$个).试证$F[x_1,x_2,\cdots,x_n]$中子集$\{f(x_1,x_2,\cdots,x_n)\mid f(a_1,a_2,\cdots,a_n)=0,(a_1,a_2,\cdots,a_n)\in S\}$是一个理想.

证明 令$A=\{f(x_1,x_2,\cdots,x_n)|f(a_1,a_2,\cdots,a_n)=0,(a_1,a_2,\cdots,a_n)\in S\}$.
$\forall\, f(x_1,x_2,\cdots,x_n),g(x_1,x_2,\cdots,x_n)\in A$,
$h(x_1,x_2,\cdots,x_n)\in F[x_1,x_2,\cdots,x_n]$,
因为$f(a_1,a_2,\cdots,a_n)-g(a_1,a_2,\cdots,a_n)=0$
$h(a_1,a_2,\cdots,a_n)\cdot f(a_1,a_2,\cdots,a_n)=h(a_1,a_2,\cdots,a_n)\cdot 0=0$
所以$f(a_1,a_2,\cdots,a_n)-g(a_1,a_2,\cdots,a_n)\in A$
$h(x_1,x_2,\cdots,x_n)\cdot f(x_1,x_2,\cdots,x_n)\in A$. 所以$A$是$F[x_1,x_2,\cdots,x_n]$的理想. ■

10. 确定$\mathbf{Z}_2[x],\mathbf{Z}_3[x]$中所有次数为2与3的不可约多项式.

解 $\mathbf{Z}_2=\{\overline{0},\overline{1}\}$,次数为2的多项式为:$ax^2+bx+c,\quad a,b,c\in\mathbf{Z}_2$
若$c=\overline{0}$,则必可约,所以$c=\overline{1},a\neq\overline{0}$.次数为2的不可约多项式可能为$x^2+x+1,x^2+1$.而$x^2+1=(x+1)(x-1)$,故所有不可约多项式为$x^2+x+1$.

同样推导,可能的3次不可约多项式有:$x^3+1,x^3+x^2+x+1,x^3+x^2+1,x^3+x+1$.而$x^3+1,x^3+x^2+x+1$显然可约. 由于3次多项式若可约必有一次因式,且$\mathbf{Z}_2[x]$中一次因式只有$x,x+1$,显然它们均不

是x^3+x^2+1, x^3+x+1的因式.
所以3次不可约多项式有x^3+x^2+1, x^3+x+1 ■

11. 在$\mathbf{Z}_2[x], \mathbf{Z}_3[x]$中分解$f(x)=x^5+x^4+x^2+x+2$.

解 $\mathbf{Z}_3[x]$ 2次不可约多项式:
$x^2+1, \quad 2x^2+x+1, \quad 2x^2+2x+1.$
3次不可约多项式:
$x^3+2x+1, x^3+x^2+x+1, x^3+2x^2+1,$
$2x^3+2x+1, 2x^3+x^2+x+1, 2x^3+2x^2+1.$ ■

12. 在$\mathbf{Z}[x]$中分解$f(x)=x^5+x^4+x^2+x+2$.

解 $f(x)=x^5+x^4+x^2+x+2.$ ■

2.8 素理想与极大理想

1. 设R是一个环,R的理想$M \neq R$称为**极大理想**,如果不存在R的理想A使$M \subset A \subset R$.试证M是R的极大理想当且仅当R/M是**单环**(即不包含非平凡理想的环).

证明 由环同态基本定理,因为R中包含M的理想与R/M的理想一一对应,所以M是极大理想当且仅当R/M是单环. ■

2. 设M是整环R的理想.试证若R/M为体则M为极大理想.

证明 R/M的理想与R中包含M的理想一一对应,因为R/M 是体,所以R/M 只有两个理想$0, R/M$. 所以R中包含M 的理想只有M 与R,所以M 为极大理想. ■

3. 试证$\langle x\rangle$是$\mathbf{Z}[x]$中的素理想而非极大理想.

证明 因为x是$\mathbf{Z}[x]$中的素元素,所以$\langle x\rangle$是$\mathbf{Z}[x]$的素理想.
因为$\mathbf{Z}[x]/\langle x\rangle \simeq \mathbf{Z}$,$\mathbf{Z}$ 不是域,所以$\langle x\rangle$不是$\mathbf{Z}[x]$的极大理想. ■

4. 取$m \in \mathbf{N}, m>1$,令$A=\{f(x) \mid f(x) \in \mathbf{Z}[x], m \mid f(0)\}$.
证明A是$\mathbf{Z}[x]$的理想,且$\langle x\rangle \subset A \subset \mathbf{Z}[x]$.并问在什么情况下$A$是素理想?

证明 $\forall f_1(x), f_2(x) \in A$,则$m \mid f_1(0), m \mid f_2(0)$,于是$m \mid f_1(0)-f_2(0)$,所以$f_1(x)-f_2(x) \in A$.
$\forall g(x) \in \mathbf{Z}[x], f(x) \in A$,则$m \mid f(0)$,于是$m \mid f(0)g(0)$,所以$f(x)\cdot g(x) \in A$.同理$g(x)\cdot f(x) \in A$.所以$A$是$\mathbf{Z}[x]$的理想.

$\langle x\rangle = \{x\cdot f(x) \mid f(x) \in \mathbf{Z}[x]\}, \forall x\cdot f(x) \in \langle x\rangle$ 有$m \mid 0\cdot f(0)$,故$x\cdot f(x) \in A$,所以$\langle x\rangle \subseteq A$. 而$x+m \in A$,但$x+m \notin \langle x\rangle$,所以$\langle x\rangle \neq A$.又因为$1 \in \mathbf{Z}[x], m \nmid 1$,所以$1 \notin A$,所以$A \neq \mathbf{Z}[x]$.故$\langle x\rangle \subset A \subset \mathbf{Z}[x]$.

m是素数,则A是素理想$\Longleftrightarrow \mathbf{Z}[x]/A$为整环. ■

5. 试问$\mathbf{Z}_m(m>1)$有多少理想?有多少素理想?有多少极大理想?

解 由环同态基本定理,$\mathbf{Z}\to\mathbf{Z}_m$ 的自然同态把包含$m\mathbf{Z}$的理想对应到$\mathbf{Z}_m$的理想, 把包含$m\mathbf{Z}$的素(极大)理想对应到$\mathbf{Z}_m$的素(极大)理想. $\mathbf{Z}$中包含$m\mathbf{Z}$ 的理想为$m_1\mathbf{Z}(m_1|m)$. $\mathbf{Z}$中包含$m\mathbf{Z}$ 的素(极大)理想为$d\mathbf{Z}(d|m$为互数). 设m有标准分解:$m=p_1^{t_1}p_2^{t_2}\cdots p_n^{t_n}$. 则知$\mathbf{Z}$中包含$m\mathbf{Z}$的理想个数为$\prod_{i=1}^n(t_i+1)$, 包含$m\mathbf{Z}$的素(极大)理想个数为$n$. 从而$\mathbf{Z}$中理想个数为$\prod_{i=1}^n(t_i+1)$, 素理想个数为$n$. ■

6. 设R为交换整环,P是R的素理想.证明下列结论:
   1) $S=R-P$是R的乘法幺半群.
   2) 仿2.1的方法,以S代替R^*可构造R的一个扩环,记为$S^{-1}R=T\supseteq R$.
   3) $\forall\, s\in S$是T中可逆元.
   4) P在T中生成的理想$P'=S^{-1}P$为T的极大理想.

证明 1)$\forall\, a,b\in S$, 则$a,b\notin P$. 因为P是R的素理想,所以$ab\notin P$, 即$ab\in S$. 又显然$1\notin P$, 否则$P=R$,所以$1\in S$. 故S是R的幺半群.

2)由定理2.1.1的证明知,此处只需证$S^{-1}R$对乘法和加法的封闭性. $\forall\, a,b\in R,\forall\, c,d\in S$ $\frac{a}{c}+\frac{b}{d}=\frac{ad+bc}{cd}$, $\frac{a}{c}\cdot\frac{b}{d}=\frac{ab}{cd}$. 由1)知$cd\in S$. 所以$\frac{a}{c}+\frac{b}{d},\frac{a}{c}\cdot\frac{b}{d}\in S^{-1}R=T\supseteq R$.

3)$\forall\, s\in S$,则$s\cdot\frac{1}{s}=1$, 所以s是T中可逆元.

4)$\forall\, p_1,p_2\in P,s_1,s_2\in S$, $\frac{p_1}{s_1}-\frac{p_2}{s_2}=\frac{p_1s_2-p_2s_1}{s_1s_2}$. 因为$P$是$R$的理想,所以$p_1s_2-p_2s_1\in P$, 所以$fracp_1s_1-\frac{p_2}{s_2}\in S^{-1}P$ $\forall p\in P,r\in R,s_1,s_2\in S$, $\frac{r}{s_1}\cdot\frac{p}{s_2}=\frac{rp}{s_1s_2}\in S^{-1}P$. 所以$S^{-1}P$是$T$的理想.接下来证$S^{-1}R/S^{-1}P$是域.

$\forall r\in R,s\in S$, 若$\overline{(\frac{r}{s})}\in S^{-1}R/S^{-1}P$,且$\overline{(\frac{r}{s})}\neq 0$, 可设$r\notin P$, 即$r\in S$, 所以$\overline{(\frac{s}{r})}\in S^{-1}R/S^{-1}P$, 所以$\overline{(\frac{s}{r})}\cdot\overline{(\frac{r}{s})}=1$,所以$\overline{(\frac{r}{s})}$ 是可逆元. 故$S^{-1}P$是极大理想. ■

7. 设R是一个无限的主理想整环.试证若R中只有有限个可逆元,则R中有无限多个素理想.

证明 先证R中有无限个互不相伴的素元素.若不然,出于R中只有有限个可逆元,故R中素元素存在, 设R中只有有限个互不相伴的素元素$p_1,p_2,\cdots,p_n$, 令$\pi_k=(\prod_{i=1}^n p_i)^k+1$, 若存在$k,m$ 使得$u\pi_k=\pi_m,(u\in\mathbf{U})$, 则$u(\prod_{i=1}^n p_i)^{k-m}=0$, 矛盾.故$\{\pi_k\}$互不相等$(k=1,2,\cdots,n\cdots)$. 又因为$p_i\nmid\pi_k(i=1,2,\cdots,n,k=1,2,\cdots,n\cdots)$ 且R中只有有限个可逆元. 所以$\{\pi_k\}$中有无限多个素元素.这与假设矛盾. 主理想整环R的互不相伴的素元素,生成不同的素理想,故R中有无限多个素理想. ■

8. 证明$\mathbf{Z}_p[x]$(p为素数)有无限多个不可约多项式.

证明 由上题知,$\mathbf{Z}_p[x]$中有无限多个互不相伴的素元素,故$\mathbf{Z}_p[x]$中有无限多个不可约多项式. ■

Chapter 3

域

3.1 域的单扩张

1. 设域**F**的特征为$p>0$,证明在**F**中有以下公式：
   1) $(a\pm b)^{p^n}=a^{p^n}\pm b^{p^n}$, $\forall n\in N$;
   2) $(a_1+a_2+\cdots+a_r)^p=a_1^p+a_2^p+\cdots+a_r^p$;
   3) $(a-b)^{p-1}=\sum_{j=0}^{p-1}a^jb^{p-j-1}$.

   证明 1) 据二项式展开：$(a\pm b)^{p^n}=\sum_{k=0}^{p^n}C_{p^n}^k a^{p^n-k}(\pm b)^k$. $C_{p^n}^k$能被p整除$\Leftrightarrow$ $k\neq 0$且$k\neq p^n$.(p为素数）。而域F的特征为p,则$px=0$, $\forall x\in F$.故$C_{p^n}^k a^{p^n-k}(\pm b)^k=0 \Leftrightarrow k\neq 0$且$k\neq p^n$.另外，$(-b)^p=-b^p$在$p=2$时也对，是因为此时$1=-1$. 故$(a\pm b)^{p^n}=a^{p^n}\pm b^{p^n}$, $\forall n\in N$.
   2)由1)知，$(a_1+a_2+\cdots+a_r)^p=(a_1+a_2+\cdots+a_{r-1})^p+a_r^p=(a_1+a_2+\cdots+a_{r-2})^p+a_{r-1}^p+a_r^p=\cdots=a_1^p+a_2^p+\cdots+a_r^p$.
   3)$\because (a-b)^p=a^p-b^p=(a-b)\sum_{j=0}^{p-1}a^jb^{p-j-1}$
   $\therefore (a-b)^{p-1}=\sum_{j=0}^{p-1}a^jb^{p-j-1}$.证闭 ∎

2. 证明下列各商环是域，并求其特征：
   1) $Z\left[\sqrt{-1}\right]/\langle 7\rangle$;
   2) $Z\left[\sqrt{-1}\right]/\langle 3\rangle$;
   3) $Z\left[\sqrt{-1}\right]/\langle 2+\sqrt{-1}\rangle$;
   4) $Z\left[\sqrt{-1}\right]/\langle 1+\sqrt{-1}\rangle$.

   证明 1) $Z\left[\sqrt{-1}\right]=\{a+b\sqrt{-1}|a,b\in Z\}$. 若$\alpha\in U$,有$\alpha\alpha^{-1}=1$,故$N(\alpha)=1$.设$\alpha=a+b\sqrt{-1}$, 则$a^2+b^2=1$,故$\alpha=\pm 1$或$\pm\sqrt{-1}$.同时可以验证$\pm 1,\pm\sqrt{-1}$都是可逆元，故$U=\{1,-1,\sqrt{-1},-\sqrt{-1}\}$.
   $7\in Z\left[\sqrt{-1}\right]-U$.设$7=(a+b\sqrt{-1})\beta$.两边取范数：$49=(a^2+b^2)N(\beta)$.则$a^2+b^2$只可能是1,7,49. 若$a^2+b^2=1$,则$a+b\sqrt{-1}\in U$,为平凡

因子；若$a^2+b^2=7$,无解；若$a^2+b^2=49$,则$N(\beta)=1$,从而β是平凡因子。故7是不可约元素. 而$Z\left[\sqrt{-1}\right]$是UFD, 故7是素元素.又$Z\left[\sqrt{-1}\right]$是p.i.d.,故$\langle 7\rangle$是极大理想，$\Rightarrow Z\left[\sqrt{-1}\right]/\langle 7\rangle$是域.
又$\forall(a+b\sqrt{-1})+\langle 7\rangle \in Z\left[\sqrt{-1}\right]/\langle 7\rangle$.有$7((a+b\sqrt{-1})+\langle 7\rangle)=7(a+b\sqrt{-1})+\langle 7\rangle=0+\langle 7\rangle$.故特征为7.
2),3),4)事实上，$7,3,2+\sqrt{-1},1+\sqrt{-1}$都是$Z\left[\sqrt{-1}\right]$中的素元素，从而$Z\left[\sqrt{-1}\right]/\langle 7\rangle, Z\left[\sqrt{-1}\right]/\langle 3\rangle, Z\left[\sqrt{-1}\right]/\langle 2+\sqrt{-1}\rangle, Z\left[\sqrt{-1}\right]/\langle 1+\sqrt{-1}\rangle$都是域.
判断乘法幺元关于加法的阶，可知$Z\left[\sqrt{-1}\right]/\langle 7\rangle$的特征为7，$Z\left[\sqrt{-1}\right]/\langle 3\rangle$的特征为3,$Z\left[\sqrt{-1}\right]/\langle 2+\sqrt{-1}\rangle$特征为5,$Z\left[\sqrt{-1}\right]/\langle 1+\sqrt{-1}\rangle$特征为2. ■

3. 证明习题2中四个域对它们所包含的素域是单代数扩张.

证明 验证$Z\left[\sqrt{-1}\right]/\langle 7\rangle = Z_7\left[\sqrt{-1}\right]$
$Z\left[\sqrt{-1}\right]/\langle 3\rangle = Z_3\left[\sqrt{-1}\right]$
$Z\left[\sqrt{-1}\right]/\langle 2+\sqrt{-1}\rangle = Z_5\left[\sqrt{-1}\right]$
$Z\left[\sqrt{-1}\right]/\langle 1+\sqrt{-1}\rangle = Z_2\left[\sqrt{-1}\right]$即可. ■

4. 设Γ是一个域，Z是不定元，又$\Sigma=\Gamma(Z)$,即Σ是$\Gamma(Z)$的分式域，$\Delta=\Gamma\left(\frac{Z^3}{1+Z}\right)$,证明$\Sigma$是$\Delta$的单代数扩张，并求$\mathrm{Irr}(Z,\Delta)$.

证明 注意到：$\Delta(Z)=\Gamma\left(\frac{Z^3}{1+Z}\right)(Z)=\Gamma(Z)\left(\frac{Z^3}{1+Z}\right)=\Gamma(Z)$.故$\Sigma=\Gamma(Z)=\Delta(Z)$.
由$y=\frac{Z^3}{1+Z}$得$y(1+Z)=Z^3$,从而$Z^3-yZ-y=0$,故Z是$\Delta=\Gamma(y)$上多项式$x^3-yx-y=0$的根.故Z是代数元.
最后证明$\mathrm{Irr}(Z,\Delta)=x^3-yx-y$.
y是Γ上的超越元.反设$f\left(\frac{Z^3}{1+Z}\right)=0$.$f$是$m$次的，两边同乘以$(1+Z)^m$,则得$Z$是$\Gamma$上的代数元，与已知矛盾；$\Gamma[y]$中$y$是不可约元，是素元，用艾森斯坦因定理，可证$x^3-yx-y$是$\Delta[x]$即$\Gamma(y)[x]$中不可约多项式. ■

5. 设K是有限域，Z_p是K中素域，则$\forall\alpha\in K$，α在Z_p上是代数元.

证明 $\because K^*=K-\{0\}$关于乘法是循环群.
$\therefore \forall\alpha\in K^*$,必$\exists n\in N$,使得$a^n=1$.
$\therefore \alpha$是Z_p上代数元.
又0显然是Z_p上代数元.证闭. ■

6. 设θ是$x^4+1\in Q[x]$的一根.在$Q[\theta]$中将x^4+1分解为不可约因式之积.

解 $\theta^4+1=0.\Rightarrow 1=-\theta^4$.故$x^4+1=x^4-\theta^4=(x^2-\theta^2)(x^2+\theta^2)=(x+\theta)(x-\theta)(x^2-\theta^4\theta^2)=(x+\theta)(x-\theta)(x-\theta^3)(x+\theta^3)$. ■

7. 设$\Delta = Z_p(x)$为Z_p上一元多项式环的分式域.
1) 证明$z^p - x \in \Delta[Z]$是不可约多项式;
2) 又设θ是$z^p - x$的一个根，试将$z^p - x$在$\Delta(\theta)$上分解为不可约多项式的积.

证明 1)$\because x$是$Z_p(x)$上的素元素，由Eisenstein判别法可得.
2)$\because \theta^p - x = 0, \therefore z^p - x = z^p - \theta^p = (z-\theta)^p$. ■

8. 证明$x^2+x+1 \in Z_2[x]$是不可约多项式.若θ是x^2+x+1的一个根，再证明$Z_2(\theta)$含有4个元素，并写出$Z_2(\theta)$的加法表与乘法表.求x^2+x+1的另一个根.

证明 $\because (0)^2+0+1=1, (1)^2+1+1=1.$
$\therefore x^2+x+1$是$Z_2[x]$上不可约多项式.
若θ是x^2+x+1的一个根，由韦达定理$1-\theta$也是x^2+x+1的根，易知$\theta \neq 1-\theta$. 又$\because \deg(\theta, Z_2) = 2, \therefore Z_2(\theta)$含有个$2^2 = 4$个元素$0, 1, \theta, 1-\theta$.
$1+\theta = 1-\theta,$
$1+(1-\theta) = -\theta = \theta,$
$\theta + (1-\theta) = 1,$
$\theta \cdot (1-\theta) = \theta - \theta^2 = \theta - 1 - \theta = 1$.证闭. ■

9. 对下列每个$\alpha \in \mathbf{C}$,求$\mathrm{Irr}(\alpha, \mathbf{Q})$:
1) $1+\sqrt{2}$; 2) $\sqrt{2}+\sqrt{3}$;
3) $\sqrt{1+\sqrt[3]{2}}$; 4) $\sqrt{\sqrt[3]{2}-\sqrt{-1}}$.

解 2) $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}, (\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2}+9\sqrt{3}, (\sqrt{2}+\sqrt{3})^4 = 49+20\sqrt{6}$. 则$(\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 + 1 = 0$.故$x^4 - 10x^2 + 1 \in Q[x]$是$\alpha$的零化多项式.假设还有次数更低的零化多项式，设为$f(x) = ax^3+bx^2+cx+d,\ a,b,c,d \in Q$.则$a(11\sqrt{2}+9\sqrt{3})+b(5+2\sqrt{6})+c(\sqrt{2}+\sqrt{3})+d = 0. \Rightarrow 11a+c = 0, 9a+c = 0, 2b = c, 5b+d = 0. \Rightarrow a = b = c = d = 0$,则$f(x)$不是零化多项式，矛盾！故$x^4 - 10x^2 + 1$就是所求的$\mathrm{Irr}(\alpha, Q)$.
1)$\mathrm{Irr}(1+\sqrt{2}, Q) = x^2 - 2x + 1.$
3)$\mathrm{Irr}(\sqrt{1+\sqrt[3]{2}}, Q) = x^4 - 10x^2 + 1.$
4)$\mathrm{Irr}(\sqrt{\sqrt[3]{2}-\sqrt{-1}}, Q) = x^{12} + 3x^8 - 4x^6 + 3x^4 + 12x^2 + 5$
1),3),4)具体的证明可参照1). ■

10. 设K是F的扩域，证明K中元素α, β对F共轭的充要条件是存在$F(\alpha)$到$F(\beta)$的$F-$同构η使$\eta(\alpha) = \beta$.

证明 “$\Rightarrow$” 由α, β对F共轭，知：$\mathrm{Irr}(\alpha, F) = \mathrm{Irr}(\beta, F) = p(x)$，则：
$\exists$同构$f : F(\alpha) \to F[x]/\langle p(x)\rangle$ 使得$F(\alpha) = x + \langle p(x)\rangle$
$\exists$同构$\varphi : F(\beta) \to F[x]/\langle p(x)\rangle$ 使得$\varphi(\beta) = x + \langle p(x)\rangle$
令:$\eta = \phi_{-1} f : F(\alpha) \to F(\beta)$

则η是$F(\alpha)$到$F(\beta)$的同构，使得:$\eta(\alpha)=\beta$
"$\Leftarrow$" 设$\mathrm{Irr}(\alpha,F)=p_1(x),\mathrm{Irr}(\beta,F)=p_2(x)$
则$p_1(\alpha)=0,p_2(\beta)=0.$
$\because 0=\eta(p_1(\alpha))=p_1(\beta),\therefore p_2(x)\mid p_1(x)$
$\because 0=\eta^{-1}(p_2(\beta))=p_1(\alpha),\therefore p_1(x)\mid p_2(x)$
$\therefore p_1(x)=p_2(x),\therefore \alpha,\beta$对$F$共轭. ■

11. 设$m\in\mathbf{N}$,求$\mathbf{C}$中所有对于$\mathbf{Q}$与$\exp(2\pi\sqrt{-1}/m)$共轭的数.

解 $\alpha=\exp(2\pi\sqrt{-1}/m)$是$x^m-1$的根.
x^m-1的所有根是:$\alpha,\alpha^2\cdots,\alpha^m=1.$
若α^k与α共轭,则$(k,m)=1.$
(否则$(\alpha^k)^{\frac{m}{(k,m)}}=1$,而$\alpha^{\frac{m}{(k,m)}}\neq 1$).
易证存在$\mathbf{Q}(\alpha)$到$\mathbf{Q}(\alpha^k)$的$\mathbf{Q}$自同构σ,使得$\sigma(\alpha)=\sigma(\alpha^k).$
综上若$(k,m)=1$则α^k与α共轭.
$\therefore$与$\exp(2\pi\sqrt{-1}/m)$共轭的数共有$\varphi(m)$个. ■

12. 设K是F的扩域，$\alpha\in K^*$,α是F上的代数元，且$\mathrm{Irr}(\alpha,F)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$.证明$\alpha^{-1}$也是$F$上代数元，且
$\mathrm{Irr}(\alpha^{-1},F)=x^n+a_{n-1}a_n^{-1}x^{n-1}+\cdots+a_1a_n^{-1}x+a_n^{-1}.$

证明 令：$g(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$
$f(x)=x^n+a_{n-1}a_n^{-1}x^{n-1}+\cdots+a_1a_n^{-1}x+a_n^{-1}$
$\because \mathrm{Irr}(\alpha,F)=g(x),\therefore \alpha^n+a_1\alpha^{n-1}+\cdots+a_{n-1}\alpha+a_n=0$
两边同乘以$a_n^{-1}(\alpha^{-1})^n$, 得：
$(\alpha^{-1})^n+a_{n-1}a_n^{-1}(\alpha^{-1})^{n-1}+\cdots+a_1a_n^{-1}\alpha^{-1}+a_n^{-1}=0$
$\therefore \mathrm{Irr}(\alpha^{-1},F)\mid f(x)$
若$f(x)$可约,有$f(x)=f_1(x)f_2(x)$
则有$g(x)=a_nx^nf(\frac{1}{x})=a_nx^nf_1(\frac{1}{x})f_2(\frac{1}{x})$
$=a_nx_1^nf_1(\frac{1}{x})x_2^nf_2(\frac{1}{x})=a_ng_1(x)g_2(x)$
(这里$n_i=Deg(f_i(x))$),从而$g(x)$可约，矛盾.
$\therefore \mathrm{Irr}(\alpha^{-1},F)=f(x).$ ■

3.2 有限扩张

1. 求下列域扩张的次数：
1) $[\mathbf{Q}(\sqrt{2}+\sqrt{3}):\mathbf{Q}]$;
2) $[\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q}]$;
3) $[\mathbf{Q}(\sqrt{2},\sqrt[3]{5}):\mathbf{Q}]$;
4) $[\mathbf{Q}(\sqrt[3]{2},\sqrt[3]{6},\sqrt[3]{24}):\mathbf{Q}]$;
5) $[\mathbf{Q}(\sqrt{2},\sqrt{6}):\mathbf{Q}(\sqrt{3})]$;
6) $[\mathbf{Q}(\sqrt{2}+\sqrt{3}):\mathbf{Q}(\sqrt{3})]$;

7) [$\mathbf{Q}(\sqrt{2},\sqrt{3})$:$\mathbf{Q}(\sqrt{2}+\sqrt{3})$];
8) [$\mathbf{Q}(\sqrt{2},\sqrt{6}+\sqrt{10})$:$\mathbf{Q}(\sqrt{3}+\sqrt{5})$].

解 2) $\mathrm{Irr}(\sqrt{2},Q)=x^2-2$.所以$[Q(\sqrt{2}):Q]=2$.基为$\{1,\sqrt{2}\}$ $\mathrm{Irr}(\sqrt{3},Q(\sqrt{2}))=x^2-3$.（须证）.所以[$\mathbf{Q}(\sqrt{2},\sqrt{3})$:$\mathbf{Q}(\sqrt{2})$] = 2. 基为$\{1,\sqrt{3}\}$.所以$[Q(\sqrt{2},\sqrt{3}):Q]=[Q(\sqrt{2},\sqrt{3}):Q(\sqrt{2})][Q(\sqrt{2}:Q]=2*2=4$，且合起来基为$\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$.
4) $\mathrm{Irr}(\sqrt[3]{2},Q)=x^3-2$.所以$[Q(\sqrt[3]{2}):Q]=3$.基为$\{1,\sqrt[3]{2},\sqrt[3]{4}\}$. 可证$\mathrm{Irr}(\sqrt[3]{6},Q(\sqrt[3]{2}))=x^3-6$.反设$(a_1+b_1\sqrt[3]{32}+c_1\sqrt[3]{34})(\sqrt[3]{6})^2+(a_2+b_2\sqrt[3]{32}+c_2\sqrt[3]{34})\sqrt[3]{6}+a_3+b_3\sqrt[3]{32}+c_3\sqrt[3]{34}=0$. $a_i,b_i,c_i\in Q,i=1,2,3.\Rightarrow a_i=b_i=c_i=0.\ i=1,2,3$.故$\mathrm{Irr}(\sqrt[3]{6},Q(\sqrt[3]{2}))\geq 3$. 又$x^3-6$能被$\sqrt[3]{6}$化零，则$\mathrm{Irr}(\sqrt[3]{6},Q(\sqrt[3]{2}))=x^3-6$. 故$[Q(\sqrt[3]{2},\sqrt[3]{6}):Q(\sqrt[3]{2})]=3$.基为$\{1,\sqrt[3]{6},\sqrt[3]{36}\}$. 故$Q(\sqrt[3]{2},\sqrt[3]{6})$作为$Q$上线性空间的基为$\{1,\sqrt[3]{2},\sqrt[3]{4},\sqrt[3]{6},\sqrt[3]{12},\sqrt[3]{24},\sqrt[3]{36},\sqrt[3]{72},\sqrt[3]{144}\}$.故$\sqrt[3]{24}\in Q(\sqrt[3]{2},\sqrt[3]{6})$. 故$\mathrm{Irr}(\sqrt[3]{24},Q(\sqrt[3]{2},\sqrt[3]{6}))=x-\sqrt[3]{24}$. 所以$[Q(\sqrt[3]{2},\sqrt[3]{6},\sqrt[3]{24}):Q(\sqrt[3]{2},\sqrt[3]{6})]=1$. 故$Q(\sqrt[3]{2},\sqrt[3]{6},\sqrt[3]{24})=Q(\sqrt[3]{2},\sqrt[3]{6})$. 故$[Q(\sqrt[3]{2},\sqrt[3]{6},\sqrt[3]{24}):Q]=[Q(\sqrt[3]{2},\sqrt[3]{6},\sqrt[3]{24}):Q(\sqrt[3]{2},\sqrt[3]{6})][Q(\sqrt[3]{2},\sqrt[3]{6}):Q(\sqrt[3]{2})][Q(\sqrt[3]{2}):Q]=1*3*3=9$. 且$Q(\sqrt[3]{2},\sqrt[3]{6},\sqrt[3]{24})$作为$Q$上线性空间的基为$\{1,\sqrt[3]{2},\sqrt[3]{4},\sqrt[3]{6},\sqrt[3]{12},\sqrt[3]{24},\sqrt[3]{36},\sqrt[3]{72},\sqrt[3]{144}\}$.
1)4, 3)6, 5)2, 6)2, 7)1, 8)2.证明方法同2),4). ■

2. 求习题1中各扩域对给定域的基.

解 2) 由上题过程中已求得，基为$\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$.
4) 由上题过程中已求得，基为$\{1,\sqrt[3]{2},\sqrt[3]{4},\sqrt[3]{6},\sqrt[3]{12},\sqrt[3]{24},\sqrt[3]{36},\sqrt[3]{72},\sqrt[3]{144}\}$.
1)$\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$.
3)$\{1,\sqrt{2},\sqrt[3]{5},\sqrt[3]{25},\sqrt{2}\sqrt[3]{5},\sqrt{2}\sqrt[3]{25}\}$.
5)$\{1,\sqrt{2}\}$.
6)$\{1,\sqrt{2}\}$.
7)$\{1\}$.
8)$\{1,\sqrt{2}\}$. ■

3. 设K是F的扩域，且$[K:F]=p$为素数，证明$K=F(\alpha),\ \forall\alpha\in K-F$.

证明 任取$\alpha\in K-F$,则$F\subseteq F(\alpha)\subseteq K$
$\because [K:F]=p$为素数,$\therefore F$与K之间无中间域.
$\therefore K=F(\alpha)$. ■

4. 设K是F的扩域，$\alpha,\beta\in K$都是F上的代数元，假设$\deg(\alpha,F)$与$\deg(\beta,F)$互素.证明$\mathrm{Irr}(\alpha,F)$是$F(\beta)[x]$中不可约多项式，从而
$[F(\alpha,\beta):F]=\deg(\alpha,F)\deg(\beta,F)$.

证明 首先有$[F(\alpha,\beta):F]=[F(\alpha,\beta):F(\beta)][F(\beta):F]=[F(\alpha,\beta):F(\alpha)][F(\alpha):F]$. 因为$[F(\beta):$

$F]$与$[F(\alpha):F]$互素，有$[F(\alpha):F]|[F(\alpha,\beta):F(\beta)]$，即$\deg(\alpha,F)|\deg(\alpha,F(\beta))$.又$\mathrm{Irr}(\alpha,F(\beta))|\mathrm{Irr}(\alpha,F)$. 故$\deg(\alpha,F(\beta))\leq\deg(\alpha,F)$,所以有$\deg(\alpha,F(\beta))=\deg(\alpha,F)$故$[F(\alpha,\beta):F]=[F(\alpha):F][F(\beta):F]=\deg(\alpha,F)\deg(\beta,F)$. 且$\mathrm{Irr}(\alpha,F)\sim\mathrm{Irr}(\alpha,F(\beta))$是$F(\beta)[x]$中不可约的.证毕. ■

5. 设K是F的扩域，$\alpha\in K$是F上的代数元，且$\deg(\alpha,F)$为奇数，证明:$F(\alpha^2)=F(\alpha)$.

证明 因为$F(\alpha^2)\subseteq F(\alpha)$,故只要证$[F(\alpha):F(\alpha^2)]=1$,就有$F(\alpha)=F(\alpha^2)$. 设法转化成单代数扩张，$[F(\alpha):F(\alpha^2)]=[F(\alpha^2)(\alpha):F(\alpha^2)]=\deg(\alpha,F(\alpha^2))$.
$x^2-\alpha^2$是α在$F(\alpha^2)$上的零化多项式. $[F(\alpha):F]=[F(\alpha):F(\alpha^2)][F(\alpha^2):F]$是奇数. 所以$[F(\alpha):F(\alpha^2)]$一定是奇数. 所以$[F(\alpha):F(\alpha^2)]$只能是1.故$F(\alpha^2)=F(\alpha)$.证毕. ■

6. 证明若$\sqrt{a}+\sqrt{b}\neq 0$,则$\mathbf{Q}(\sqrt{a},\sqrt{b})=\mathbf{Q}(\sqrt{a}+\sqrt{b})$, $\forall a,b\in\mathbf{Q}$.

证明 若$a=b$,显然.
设$a\neq b$,$\because(\sqrt{a}+\sqrt{b})^2=a+b+2\sqrt{a}\sqrt{b}$,$\therefore\sqrt{a}\sqrt{b}\in\mathbf{Q}(\sqrt{a}+\sqrt{b})$.
又$\because(\sqrt{a}+\sqrt{b})^3=a\sqrt{a}+b\sqrt{b}+3\sqrt{a}\sqrt{b}(\sqrt{a}+\sqrt{b})$,
$\therefore a\sqrt{a}+b\sqrt{b}\in\mathbf{Q}(\sqrt{a}+\sqrt{b})$
$\because a\sqrt{a}+b\sqrt{b}=a\sqrt{a}+b\sqrt{b}-b\sqrt{a}+b\sqrt{a}$
$=\sqrt{a}(\sqrt{a}-\sqrt{b})+b(\sqrt{a}+\sqrt{b})$.
$\therefore\sqrt{a}\in\mathbf{Q}(\sqrt{a}+\sqrt{b})$.
同理：$\sqrt{b}\in\mathbf{Q}(\sqrt{a}+\sqrt{b})$.
显然$\sqrt{a}+\sqrt{b}\in\mathbf{Q}(\sqrt{a},\sqrt{b})$.
$\therefore\mathbf{Q}(\sqrt{a},\sqrt{b})=\mathbf{Q}(\sqrt{a}+\sqrt{b})$. ■

7. 设K是F的有限扩张，且整环D满足$F\subseteq D\subseteq K$.证明D是域.

证明 只需证D中任意非零元可逆.
$\forall\alpha\in D-\{0\}$,,α是F上的代数元.
从而有$\sum_{i=1}^{n}a_i\alpha^i=1$,即:
$\alpha\sum_{i=1}^{n}a_i\alpha^{i-1}=1$.
$\therefore\alpha$可逆,$\therefore D$是域. ■

8. 设K是有限域，而$\mathrm{Ch}\ K=p>0$,试证K中包含p^n个元素$(n\in N)$.

证明 设$[K:Z_p]=n,\{x_1,x_2,\cdots x_n\}$是$K$作为$Z_p$上线形空间的一组基.
则$\forall\alpha\in K$,有$\alpha=\alpha_1x_1+\alpha_2x_2\cdots\alpha_nx_n.(\alpha_i\in Z_p,i=1,2,\cdots n)$
$\therefore|K|=P^n$. ■

3.3 分裂域 正规扩张

1. 求下列$\mathbf{Q}[x]$中的多项式的分裂域及该分裂域的$\mathbf{Q}$-自同构的个数.
   1) x^2+3; 2) x^5-1;
   3) $(x^2-2)(x^3-2)$; 4) x^5-3.

   解 3) 设ϵ为3次本原单位根，则$(x^2-2)(x^3-2)$的根为$\pm\sqrt{2}, \sqrt[3]{2}\epsilon^0, \sqrt[3]{2}\epsilon^1, \sqrt[3]{2}\epsilon^2$. 故$E = Q(-\sqrt{2}, \sqrt{2}, \sqrt[3]{2}\epsilon^0, \sqrt[3]{2}\epsilon^1, \sqrt[3]{2}\epsilon^2) = Q(\sqrt{2}, \sqrt[3]{2}, \epsilon)$.即为分裂域.
   注意到$(x^2-2)(x^3-2)$不可约因式无重根，故该分裂域的$Q-$自同构个数$= [E:Q]$. 下求$[E:Q]$.
   $[E:Q] = [Q(\sqrt{2}, \sqrt[3]{2}, \epsilon) : Q(\sqrt{2}, \sqrt[3]{2})][Q(\sqrt{2}, \sqrt[3]{2}) : Q(\sqrt{2})][Q(\sqrt{2}) : Q]$.
   1. $\mathrm{Irr}(\sqrt{2}, Q) = x^2-2$.故$[Q(\sqrt{2}) : Q] = \deg(\sqrt{2}, Q) = 2$.
   2. $\mathrm{Irr}(\sqrt[3]{2}, Q) = x^3-2$.$Q(\sqrt{2}, \sqrt[3]{2})$是$Q$的扩域.$\sqrt{2}, \sqrt[3]{2} \in Q(\sqrt{2}, \sqrt[3]{2})$都是$Q$上的代数元.$\deg(\sqrt{2}, Q)$与$\deg(\sqrt[3]{2}, Q)$互素，则$\mathrm{Irr}(\sqrt[3]{2}, Q)$是$Q(\sqrt{2})[x]$中不可约多项式（由125页第四题）. 故$\mathrm{Irr}(\sqrt[3]{2}, Q(\sqrt{2})) = \mathrm{Irr}(\sqrt[3]{2}, Q) = x^3-2$. 故$[Q(\sqrt{2}, \sqrt[3]{2}) : Q(\sqrt{2})] = \deg(\sqrt[3]{2}, Q(\sqrt{2})) = 3$.
   3. $\mathrm{Irr}(\epsilon, Q) = x^2+x+1$.$Q(\sqrt{2}, \sqrt[3]{2}, \epsilon)$是$Q(\sqrt{2})$的扩域，$\sqrt[3]{2}, \epsilon \in Q(\sqrt{2}, \sqrt[3]{2}, \epsilon)$是$Q(\sqrt{2})$上的代数元. $\deg(\sqrt[3]{2}, Q(\sqrt{2})) = 3.\deg(\epsilon, Q(\sqrt{2})) = 2$ 故.$\deg(\sqrt[3]{2}, Q(\sqrt{2}))$与$\deg(\epsilon, Q(\sqrt{2}))$互素.所以$\mathrm{Irr}(\epsilon, Q(\sqrt{2}))$是$Q(\sqrt{2}, \sqrt[3]{2})[x]$中不可约多项式. 故$\mathrm{Irr}(\epsilon, Q(\sqrt{2}, \sqrt[3]{2})) = \mathrm{Irr}(\epsilon, Q(\sqrt{2})) = x^2+x+1$. 从而$[Q(\sqrt{2}, \sqrt[3]{2}, \epsilon) : Q(\sqrt{2}, \sqrt[3]{2})] = 2$. 综上1.2.3,有$[E:Q] = 2*3*2 = 12$.
   1)$Q(\sqrt{-3}), Q$自同构个数：2.
   2)$Q(\omega)$(ω为5次本原单位根）,Q自同构个数：4.
   4)$Q(\sqrt[5]{3}, \omega)$(ω为5次本原单位根）,Q自同构个数：$5*4 = 20$. ■

2. 设p是素数，$Z_p(\alpha)$是Z_p的单超越扩张.求$x^p-\alpha \in Z_p(\alpha)[x]$的分裂域$K$及其$Z_p(\alpha)-$自同构的个数.

   解 1) 因为α是Z_p的超越元，所以α是$Z_p[\alpha]$中不可约多项式，所以α是$Z_p[\alpha]$中的素元素. 由艾森斯坦因定理知$x^p-\alpha$是$Z_p(\alpha)[x]$中不可约多项式.
   2) 设θ是$x^p-\alpha$在某一扩域中的根，则$\theta^p-\alpha = 0$.从而$\alpha = \theta^p$. 所以$x^p-\alpha = x^p-\theta^p = (x-\theta)^p \Rightarrow x^p-\alpha$的$p$个根都是$\theta$.故$K = Z_p(\alpha, \theta)$.
   3) $[K : Z_p(\alpha)] = [Z_p(\alpha, \theta) : Z_p(\alpha)] = p$.
   4) K的$Z_p(\alpha)-$自同构的个数$\leq [K : Z_p(\alpha)] = p$.等号不成立.故个数$< p$. 设$\sigma$是一个$K$的$Z_p(\alpha)$自同构，且$\sigma|_{Z_p(\alpha)} = \mathrm{id}_{Z_p(\alpha)}$. 因为$K = Z_p(\alpha, \theta)$,所以$\sigma$的不同仅在于$\sigma(\theta)$的不同. θ是$x^p-\alpha \in Z_p(\alpha)[x]$的一个根$\Rightarrow \sigma(\theta)$一定是$x^p-\alpha$的一个根.$\Rightarrow \sigma(\theta) = \theta$. $\Rightarrow \sigma = \mathrm{id}_K$. $\Rightarrow \sigma$只有一个.故K的$Z_p(\alpha)-$自同构的个数为1. ■

3. 证明域F的二次扩张K是F的正规扩张.

   证明 可设$K=F(\alpha)$,则$\mathrm{Irr}(\alpha,F)=x^2+bx+c,(b,c\in F.$
   有韦达定理知：$x^2+bx+c=(x-\alpha)(x-\frac{c}{\alpha})$.
   $\because \frac{c}{\alpha}\in F(\alpha),\therefore K$是$F$关于多项式$x^2+bx+c$的分裂域.
   $\therefore K$是F的正规扩张. ■

4. 证明$\mathbf{Q}(\sqrt[3]{5})$不是$\mathbf{Q}$的正规扩张.

   证明 $\mathrm{Irr}(\sqrt[3]{5},\mathbf{Q})=x^3-5=(x-\sqrt[3]{5})(x-\sqrt[3]{5}\omega)(x-\sqrt[3]{5}\omega^2)$.
   (ω是3次本原单位根)
   易知，$\omega\overline{\in}\ \mathbf{Q}(\sqrt[3]{5}),\therefore \mathbf{Q}(\sqrt[3]{5})$不是$\mathbf{Q}$的正规扩张. ■

5. 设K,E都是域F的扩域，且$F\subseteq E\subseteq K$,又K是F的正规扩张，则K也是E的正规扩张.

   证明 因为K是F的正规扩张，所以K是F的代数扩张，即$\forall\alpha\in K,\exists 0\neq f(x)\in F[x]$,使得$f(\alpha)=0$. 因为$F\subseteq E$,所以$f(x)\in E[x]$.从而$\alpha$是$E$上代数元，所以$K$是$E$的代数扩张. 任一$p(x)\in E[x],p(x)$不可约，设$\alpha$是$p(x)$在$K$中一根，去证$p(x)$的任一根$\beta$也在$K$中. 显然，$\alpha,\beta$都是$E$上代数元，故$\exists!\sigma:E(\alpha)\to E(\beta)$的同构，使得$\sigma(\alpha)=\beta$,且$\sigma|_E=\mathrm{id}_E$.由$\alpha\in K$知$\alpha$是$F$上代数元，设$g(x)=\mathrm{Irr}(\alpha,F)$,则$g(\alpha)=0$，从而$\sigma g(\alpha)=g(\sigma(\alpha))=g(\beta)=0$.从而$\beta$也是$g(x)=\mathrm{Irr}(\alpha,F)$的根. 因为$K$是$F$的正规扩张，$g(x)\in F[x]$不可约，$\alpha$是$g(x)$的一个在$K$中的根，故$g(x)$所有根在$K$中，所以$\beta\in K$.从而$K$是$E$的正规扩张.证毕. ■

6. 设K,E都是域F的扩域，且$F\subseteq E\subseteq K$,又E是F的正规扩张，σ是K的$F-$自同构，则$\sigma(E)=E$.

   证明 先证：$\sigma(E)\subseteq E.\forall\alpha\in E$, 记$p(x)=\mathrm{Irr}(\alpha,F).\Rightarrow\sigma(\alpha)$也是$p(x)$的一个根.$\Rightarrow\sigma(\alpha)\in E$.故$\sigma(E)\subseteq E$.
   再证：$E\subseteq\sigma(E)$. σ^{-1}也是K的$F-$自同构.$\Rightarrow\sigma^{-1}(E)\subseteq E\Rightarrow E\subseteq\sigma(E)$.证毕. ■

7. 设K是F的有限正规扩张，E_1,E_2是两个中间域，则E_1,E_2对F共轭的充要条件是存在K的$F-$自同构σ,使$\sigma(E_1)=E_2$.

   证明 “$\Leftarrow$”去证$\sigma|_{E_1}$是$E_1\to E_2$的$F-$同构.首先σ在K上保持加法，乘法.所以$\sigma|_{E_1}$保持加法，乘法. $\sigma|_{E_1}(E_1)=E_2$.所以是满的同态.由于σ在K是单射，所以$\sigma|_{E_1}$是单射. 所以$\sigma|_{E_1}$是$E_1\to E_2$的同构.且$\sigma|_F=\mathrm{id}_F$.所以E_1,E_2共轭.
   “$\Rightarrow$”由已知K是$f(x)\in F[x]$的分裂域$\Rightarrow k$是$f(x)\in E_1[x]$,也是$f(x)\in E_2[x]$的分裂域.因为E_1,E_2共轭，所以存在σ_1是$E_1\to E_2$的$F-$同构，$\sigma_1|_F=\mathrm{id}_F$.所以$\sigma_1$可开拓为$K\to K$的同构$\sigma$,$\sigma|_{E_1}=\sigma_1$.所

以$\sigma|_F = \sigma_1|_F = \mathrm{id}_F$. 所以$\sigma$是$K$的$F-$自同构，且$\sigma(E_1) = \sigma|_{E_1}(E_1) = \sigma_1(E_1) = E_2$.证毕. ■

8. 设K是F的正规扩张，且$[K:F] < +\infty$,则$\alpha, \beta \in K$对F共轭的充要条件是存在K的$F-$自同构σ使$\sigma(\alpha) = \beta$.

证明 “ $\Rightarrow$ ” $\alpha, \beta \in K$对F共轭，则α, β同是$p(x) \in F[x]$（不可约）的根.由定理知：id_F可唯一开拓为$\sigma_1 : F(\alpha) \to F(\beta)$的同构，且$\sigma_1(\alpha) = \beta$.因为$F \subseteq F(\alpha) \subseteq K$,又$K$是$F$的正规扩张，所以$K$也是$F(\alpha)$的正规扩张（由上题）.又$[K:F] = [K:F(\alpha)][F(\alpha):F] < +\infty$, 故$[K:F(\alpha)] < +\infty$.从而$K$可看作$F(\alpha)[x]$上某一多项式的分裂域. 同理$K$也可看作$F(\beta)[x]$上某一多项式的分裂域.由定理3.3.3知：$\sigma_1$可同构开拓为$\sigma : K \to K$且$\sigma|_F(\alpha) = \sigma_1$.又$\sigma_1|_F = \mathrm{id}_F$,故$\sigma$是$K$的$F-$自同构.且$\sigma(\alpha) = \sigma_1(\alpha) = \beta$.
“ $\Leftarrow$ ” 因为K是F的正规扩张，所以K是F的代数扩张，所以α, β都是F上的代数元.设$g(x) = \mathrm{Irr}(\alpha, F)$,则$\sigma(g(\alpha)) = g(\sigma(\alpha)) = g(\beta) = 0$,所以$g(x)$是$\beta$的零化多项式，所以$\mathrm{Irr}(\beta, F)|g(x)$. 因为$g(x)$是$F[x]$中不可约多项式，所以$\mathrm{Irr}(\alpha, F) = \mathrm{Irr}(\beta, F)$, 故$\alpha, \beta$对$F$共轭.证毕. ■

9. 设C_0是$\mathbf{Q}$在$\mathbf{C}$中的代数闭包（称为代数数域）.证明C_0是$\mathbf{Q}$的正规扩张，且$[C_0 : \mathbf{Q}] = +\infty$.

证明 $\forall \alpha \in C_0$,令$\mathrm{Irr}(\alpha, \mathbf{Q}) = p(x)$.
则由C_0的定义知$p(x)$的所有根$\in C_0$.
$\therefore C_0$是$\mathbf{Q}$的正规扩张.
反设$[C_0 : \mathbf{Q}] = \mathbf{n}$,
由Eisenstein判别法知：$x^{n+1} - 2$是$\mathbf{Q}$ $[x]$中不可约多项式.
$2^{\frac{1}{n+1}} \in C_0$,而$[\mathbf{Q}\ (2^{\frac{1}{n+1}}) : \mathbf{Q}] = n+1$.
矛盾.$\therefore [C_0 : \mathbf{Q}] = +\infty$. ■

3.4 可分多项式 完备域

1. 设F是一个域，$F[x]$到自身的映射D如果满足：
$D(f(x)+g(x)) = D(f(x)) + D(g(x))$;
$D(f(x)g(x)) = D(f(x))g(x) + f(x)D(g(x))$;
$D(a) = 0,\ \forall a \in F$.
那么称D是$F[x]$上的一个**导子**.证明:
1) $D(af(x)) = aD(f(x)),\ \forall a \in F, f(x) \in F[x]$;
2) $D(f(x)^m) = mf(x)^{m-1}D(f(x)),\ \forall f(x) \in F[x], m \in N$.

证明 1)$\forall a \in F, f(x) \in F[x]$,
$D(af(x)) = D(a)f(x) + aD(f(x)) = aD(f(x))$.
2)$m = 1$时结论显然成立.假设$m = k$结论成立,即:

$D(f(x)^k) = kf(x)^{k-1}D(f(x))$
$m = k+1$时:
$D(f(x)^{k+1}) = D(f(x))f(x)^k + D(f(x)^k))f(x)$
$= f(x)^k D(f(x)) + kf(x)^{k-1}D(f(x))f(x) = (k+1)f(x)^k D(f(x))$.
证毕. ■

2. 令Der$F[x]$为$F[x]$的导子集合.在Der$F[x]$中定义加法：$(D_1 + D_2)(f(x)) = D_1(f(x)) + D_2(f(x))$; 再定义$F[x]$中元素与Der$F[x]$中元素的乘法：$(f(x)D)(g(x)) = f(x)D(g(x))$. 证明Der$F[x]$是一个左$F[x]-$模，且与左$F[x]-$模$F[x]$同构.

证明 (1)乘法定义合理性:
$\forall f(x), g(x), h(x) \in F[x], D \in \mathrm{Der}F[x]$,
$(f(x)D)(g(x) + h(x)) = (f(x))(D(g(x) + h(x)))$
$= f(x)(D(g(x)) + D(h(x))) = (f(x)D)(g(x)) + (f(x)D)(h(x))$.
$(f(x)D)(g(x)h(x)) = f(x)(D(g(x)h(x)))$
$= f(x)(D(g(x))h(x) + g(x)D(h(x))) = (f(x)D)g(x))h(x) + (f(x)D)h(x))g(x)$.
(2)Der$F[x]$是一个左$F[x]-$模.
$\forall f(x), g(x), h(x) \in F[x], D, D_1, D_2 \in \mathrm{Der}F[x]$,
$(f(x)(D_1 + D_2))g(x) = f(x)((D_1 + D_2)g(x))$
$= f(x)(D_1 g(x) + D_2 g(x)) = f(x)(D_1 g(x)) + f(x)(D_2 g(x))$
$= (f(xD_1 + f(x)D_2))g(x)$.
$((f(x) + g(x))D)h(x) = (f(x) + g(x))(Dh(x))$
$= f(x)(Dh(x)) + g(x)(Dh(x)) = (f(x)D + g(x)D)h(x)$.
$(f(x)g(x)D)h(x) = (f(x)g(x))(Dh(x)) = f(x)((g(x)D)h(x))$.
$(1 \cdot D)f(x) = 1 \cdot (Df(x)) = Df(x)$.
(3)作$\varphi : \mathrm{Der}F[x] \to F[x]$, 使得$\varphi(D) = D(x)$.
则易证φ是Der$F[x] \to F[x]$的同态.
易验证$\exists D_0 \in \mathrm{Der}F[x]$,使得:
$D_0(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)$
$= na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$.
此时,$D_0(x) = 1$
则$\forall f(x) \in F[x], \varphi(f(x)D_0) = f(x)$
从而是φ满射.
若$\varphi(D) = 0$,则$D(x) = 0$,
从而$D(x^n) = 0, D(f(x)) = 0(\forall f(x) \in F[x])$
$\therefore D = 0, Ker\varphi = 0$.
$\therefore \varphi$是单射.
$\therefore \mathrm{Der}F[x] \simeq F[x]$. ■

3. 设F是一个域，$f(x) \in F[x]$.$f(x)$在其分裂域K中有分解$f(x) = (x -$

$a_1)(x-a_2)\cdots(x-a_n)$.证明:$R(f,f')=\prod\limits_{1\le j<k\le n}(a_j-a_k)^2$,($R(f,f')$称为$f(x)$的判别式，记为$\Delta(f)$.)

证明 $f'(x)=\sum\limits_{i=1}^{n}\frac{f(x)}{x-\alpha_i}$.

$R(f,f')=\prod\limits_{j=1}^{n}(\sum\limits_{i=1}^{n}\frac{f(\alpha_j)}{\alpha_j-\alpha_i})=\prod\limits_{1\le j<k\le n}(a_j-a_k)^2$. ■

4. 设域F的特征为p，又$\alpha\in F$,而$\alpha\notin F^p$.$n\in Z$,且$n\ge 0$.证明$x^{p^n}-a$是$F[x]$中不可约多项式.

证明 $n=0$时，$x-a$是$F[x]$中不可约多项式，这是显然的.
下设$n>0$.设θ是$x^{p^n}-a$在其分裂域中的一个根，则$a=\theta^{p^n}$,有$x^{p^n}-a=(x-\theta)^{p^n}$. 反设$x^{p^n}-a$在$F[x]$中可约，则$\exists g(x),h(x)\in F[x],0<\deg g(x),\deg h(x)<p^n$,使得$x^{p^n}-a=g(x)h(x)$.于是在分裂域中$g(x)=(x-\theta)^{l_1},h(x)=(x-\theta)^{l_2}$. 若$(l_1,p)=1$,则$(l_1,p^n)=1$.$\exists u,v\in Z$,使得$ul_1+vl_2=1$.由于$g(x)\in F[x]$,所以$g(x)$的系数$\in F$.就有$(-\theta)^{l_1}\in F$.所以$\theta^{l_1}\in F$.又$\theta^{p^n}=a\in F$,故$\theta=\theta^{ul_1+vp^n}=(\theta^{l_1})^u(\theta^{p^n})^v\in F$.故$a=(\theta^{p^{n-1}})^p\in F^p$.与题设$a\notin F^p$矛盾！同理，$(l_2,p)=1$.也能推出矛盾.即必有$p|l_1,p|l_2$,故$(p^n,l_1)=p^l,0<l<n$.故$\exists u,v\in Z$,使得$up^n+vl_1=p^l$.所以$\theta^{p^l}=\theta^{up^n+vl_1}=(\theta^{p^n})^u(\theta^{l_1})^v\in F,0<l<n$.故$\theta^{p^{n-1}}\in F$.得到$a=(\theta^{p^{n-1}})^p\in F^p$.矛盾！故$x^{p^n}-a$是$F[x]$中不可约多项式.证毕. ■

5. 设F是一个域，$K=F(\alpha)$是$f(x)=\mathrm{Irr}(\alpha,F)$的分裂域，$K$的$F-$自同构的个数为$m$，试证$m=\mathrm{red}\ f(x)$.

证明 $\because f$是K的$F-$自同构当且仅当$f(\alpha)=\alpha_i$.
(α_i是$\mathrm{Irr}(\alpha,F)$的根).
$\therefore m=\mathrm{red}\ f(x)$. ■

6. 设域F的特征$p\neq 0$.$F(\alpha_1,\alpha_2,\cdots,\alpha_n)$是$F$的扩域，$\alpha_1,\alpha_2,\cdots,\alpha_n$在$F$上代数无关，试证：
1) $[F(\alpha_1,\alpha_2,\cdots,\alpha_n):F(\alpha_1^p,\alpha_2^p,\cdots\alpha_n^p)]=p^n$;
2) $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$的$F(\alpha_1^p,\alpha_2^p,\cdots\alpha_n^p)-$自同构为恒等映射.

证明 1) 对n用归纳法.$n=1$时α_1是F上不定元，则α_1^p也是F上的不定元.若不然，则$\exists f(x)\in F[x]$,使$f(\alpha_1^p)=0$.其中$f(x)\neq 0$.同时$f(\alpha_1^p)$也可看作关于α_1的多项式. 因为α_1是F上的不定元，所以$f(x)=0$,矛盾！所以α_1^p是F上的超越元. 所以$x^p-\alpha_1^p$是$F(\alpha_1^p)[x]$中不可约多项式，α_1是它的根. 所以$\mathrm{Irr}(\alpha_1,F(\alpha_1^p))=x^p-\alpha_1^p$.故$[F(\alpha_1):F(\alpha_1^p)]=[F(\alpha_1^p)(\alpha):F(\alpha_1^p)]=p$. 下设$n-1$时成立，去证$n$时成立.
$[F(\alpha_1,\alpha_2,\cdots,\alpha_n):F(\alpha_1^p,\alpha_2^p,\cdots\alpha_n^p)]=[F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})(\alpha_n):F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})(\alpha_n^p)][F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})(\alpha_n^p):F(\alpha_1^p,\alpha_2^p,\cdots,\alpha_{n-1}^p)(\alpha_n^p)]=p*p^{n-1}=p^n$.

2) 设σ为任一个自同构，则$\sigma|_{F(\alpha_1^p,\alpha_2^p,\cdots\alpha_n^p)}$是恒等映射，所以$\sigma|_F = \mathrm{id}_F$.因$\sigma(\alpha_i^p) = (\sigma(\alpha_i))^p \Rightarrow \sigma(\alpha_i)^p = \alpha_i^p$.故$\sigma(\alpha_i)^p - \alpha_i^p = (\sigma(\alpha_i) - \alpha_i)^p = 0$. 故$\sigma(\alpha_i) = \alpha_i$.故$\sigma$只能是恒等映射.证毕. ■

7. 设F是q个元素的有限域，$E = F(t)$是F的单超越扩张，证明:
1) $\forall a \in F$,存在E的一个$F-$自同构σ_a使$\sigma_a(t) = t + a$;
2) $G = \{\sigma_a | a \in F\}$是一个群;
3) 令$K = \{x \in E | \sigma_a(x) = x, \ \forall a \in F\}$,则$K$是$E$的子域，且$K = F(t^q - t)$.

证明 1)令:$\sigma_{\alpha|F} = \mathrm{id}$,则$\sigma_\alpha(f(t)) = f(t + \alpha), \forall f(t) \in F(t)$
易证σ_α是同态.
$\because \forall x \in F(t), \sigma_\alpha(x) = 0 \Rightarrow x = 0$.
$\therefore \sigma_\alpha$是单射.
又$\forall f(x) \in F(t), \sigma_\alpha(f(t - \alpha)) = f(t)$.
$\therefore \sigma_\alpha$是满射.
$\therefore \sigma_\alpha$是$F-$自同构.
2)$\forall \alpha, \beta, \gamma \in F$,有:
封闭性：$\sigma_\beta\sigma_\alpha(t) = t + \alpha + \beta, \therefore \sigma_\beta\sigma_\alpha \in G$.
结合律：$\sigma_\alpha(\sigma_\beta\sigma_\gamma)(t) = t + \alpha + \beta + \gamma = (\sigma_\alpha\sigma_\beta)\sigma_\gamma(t)$.
幺元律：$\sigma_\alpha\sigma_0 = \sigma_\alpha = \sigma_0\sigma_\alpha$.
逆元律：$\sigma_\alpha\sigma_{-\alpha} = \sigma_0$.
$\therefore G$是一个群.
3)易证K是E的子域.
$\because (t + \alpha)^q - (t + \alpha) = t^q + \alpha^q - t - \alpha = t^q - t$.
$\therefore F(t^q - t) \subseteq K$.
又$\forall f(t) \in F[t]$且$f(t) \in K$,有$f(t + \alpha) = f(t), \forall \alpha \in F$.
令$g(t) = f(t) - f(0)$.
则$\forall \alpha \in F$是$g(t) = 0$的根.
由F^*是q阶循环群知：
$t(t^{q-1} - 1) \mid g(t)$,即：$t(t^{q-1} - 1) \mid f(t) - f(0)$.
从而$\frac{f(t)-f(0)}{t^q-t} \in F[t]$,且$\frac{f(t)-f(0)}{t^q-t} \in K$.
依上述方法类推，可得:$f(t) \in F[t^q - t]$.
$\forall \frac{f(t)}{g(t)} \in F(t)$,其中$f(t), g(t) \in F[t]$.
$\frac{f(t)}{g(t)} \in F(t) \Rightarrow \frac{f(t)}{g(t)} = \frac{f(t+\alpha)}{g(t+\alpha)} \Rightarrow f(t + \alpha) = f(t), g(t + \alpha) = g(t) \Rightarrow f(t), g(t) \in F[t^q - t] \Rightarrow \frac{f(t)}{g(t)} \in F(t^q - t)$.
$\therefore K \subseteq F(t^q - t)$.
$\therefore K = F(t^q - t)$. ■

8. 设E是域F的有限扩张，证明E是完备域的充要条件是F是完备域.

证明 “$\Leftarrow$” E是F的有限扩张$\Rightarrow$ E是F的代数扩张，又F是完备

域，故E是完备域.
“$\Rightarrow$”1) 若Ch $E=0$,则Ch $F=0$.F是完备域.
2) 令$\sigma: E\to E\ (a\mapsto a^p)$.因为$E$是完备域，所以$E=E^p=\sigma(E)$.($\sigma$是同构）. 现$\sigma|_F: F\to F\ (b\mapsto b^p)$.可知$\sigma|_F$是单射，同态.故$\sigma|_F$是$F\to\sigma(F)=F^p$的同构.$[\sigma(E):\sigma(F)]=[E:\sigma(F)]=[E:F][F:\sigma(F)]$. 现要证$F=\sigma(F)=F^p$,即证$[F:\sigma(F)]=1$,即证$[\sigma(E):\sigma(F)]=[E:F]$. 设$[E:F]=n.\alpha_1,\cdots,\alpha_n$是$E$作为$F$上线性空间的基. 去证$\sigma(\alpha_1),\cdots,\sigma(\alpha_n)$是$\sigma(E)$作为$\sigma(F)$上线性空间的基. $\alpha_1,\cdots,\alpha_n\in E$, 故$\sigma(\alpha_1),\cdots,\sigma(\alpha_n)\in\sigma(E)$. 设$a_1,\cdots,a_n\in\sigma(F)$且$a_1\sigma(\alpha_1)+\cdots+a_n\sigma(\alpha_n)=0$. $\exists b_1,\cdots,b_n\in F$,使$b_i^p=a_i$.即$\sum_{i=1}^n b_i^p\sigma(\alpha_i)=0$.即$\sum_{i=1}^n b_i^p\alpha_i^p=0$. 因为$b_i,\alpha_i\in E$且Ch $E=p$,所以$(\sum_{i=1}^n b_i\alpha_i)^p=0$.故$\sum_{i=1}^n b_i\alpha_i=0$. 因为$\alpha_1,\cdots,\alpha_n$是$E$作为$F$上线性空间的基，故$b_1,\cdots,b_n$均为0. 从而$a_1,\cdots,a_n$均为0，故$\sigma(\alpha_1),\cdots,\sigma(\alpha_n)$线性无关. $\forall e\in\sigma(E),\exists e'\in E$,使$e'^p=e$. 故$e=e'^p=(\sum_{i=1}^n e_i\alpha_1)^p=\sum_{i=1}^n e_i^p\alpha_i^p=\sum_{i=1}^n\sigma(e_i)\sigma(\alpha_i)$. 即$e$可被$\sigma(\alpha_1),\cdots,\sigma(\alpha_n)$线性表示. 故$\sigma(\alpha_1),\cdots,\sigma(\alpha_n)$是$\sigma(E)$的基.证毕. ■

3.5 可分扩张 本原元素

1. 求$Q(\sqrt{2},\sqrt{3})$对于Q的本原元素.

   解 注意到$\mathrm{Irr}(\sqrt{2},Q)=x^2-2=(x-\sqrt{2})(x+\sqrt{2})$. $\mathrm{Irr}(\sqrt{3},Q)=x^2-3=(x-\sqrt{3})(x+\sqrt{3})$. 据定理可取$\theta=\sqrt{2}+c\sqrt{3}$.其中$c\in Q, c\neq\frac{\pm\sqrt{2}-\sqrt{2}}{\sqrt{3}+\sqrt{3}}$.即$c\neq 0, c\neq-\sqrt{2}/\sqrt{3}$. 便有$Q(\sqrt{2},\sqrt{3})=Q(\theta)$,$\theta$是所求本原元素. ■

2. 设E是$x^5-2\in Q[x]$的分裂域，求θ使得$E=Q(\theta)$.

   解 设ϵ是5次本原单位根，则$E=Q(\sqrt[5]{2},\epsilon)$.令$\theta=\epsilon+c\sqrt[5]{2}, c\in Q$. $\mathrm{Irr}(\sqrt[5]{2},Q)=x^5-2$.根为$\sqrt[5]{2},\sqrt[5]{2}\epsilon,\sqrt[5]{2}\epsilon^2,\sqrt[5]{2}\epsilon^3,\sqrt[5]{2}\epsilon^4$. $\mathrm{Irr}(\epsilon,Q)=x^4+x^3+x^2+x+1$.根为$\epsilon,\epsilon^2,\epsilon^3,\epsilon^4$. $c\neq\frac{\epsilon^k-\epsilon}{\sqrt[5]{2}-\sqrt[5]{2}\epsilon^i}\quad k=1,2,3,4.\ i=1,2,3,4$.故$c$可取1.所以$\theta=\epsilon+\sqrt[5]{2}$是本原元素，即$E=Q(\sqrt[5]{2},\epsilon)=Q(\sqrt[5]{2}+\epsilon)$. ■

3. 设$Z_3(\alpha)=F$,且$\mathrm{Irr}(\alpha,Z_3)=x^2+1$.又设$F^*=F-\{0\}$,$<\alpha>$为$\alpha$生成的$F^*$的子群，证明$<\alpha>$是$F^*$的真子群，并求$\theta\in F^*$使得$F^*=<\theta>$.

   证明 1) 由$\mathrm{Irr}(\alpha,Z_3)=x^2+1$知，$[Z_3(\alpha):Z_3]=2$.即$F$是$Z_3$上二维线性空间，$\{1,\alpha\}$是一组基. 故$F$中元素形如$k_1*1+k_2*\alpha\ (k_i=0,1,2)$. F中共有9个元素.F^*中有8个元素.可证α对乘法是4阶元. 由于$\alpha^2=-1,\alpha^3=-\alpha\neq 1,\alpha^4=(-1)^2=1$.故$<\alpha>=\{1,\alpha,\alpha^2,\alpha^3\}$. 故$<\alpha>$是$F^*$的真子群. ■

解 2) F是有限域，所以F^*是对乘法的循环群，故只需找8阶元即为生成元. 因为$(2\alpha)^4 = 2^4\alpha^4 = 1$. $(\alpha+1)^2 = \alpha^2+2\alpha+1 = 2\alpha$. 故$(\alpha+1)^8 = (2\alpha)^4 = 1$.而$(\alpha+1)^i \neq 1,\ i = 1,\cdots,7$. 故$\theta = \alpha+1$即为所求. ■

4. 设$Z_p(\alpha,\beta)$是Z_p的扩域，且α,β在Z_p上代数无关，$F = Z_p(\alpha^p,\beta^p)$.试证：
1) $[Z_p(\alpha,\beta):F] = p^2$;
2) $Z_p(\alpha,\beta)$在F上无本原元素.

证明 1) $[Z_p(\alpha,\beta):F] = [Z_p(\alpha,\beta):Z_p(\alpha^p,\beta^p)] = [Z_p(\alpha,\beta):Z_p(\alpha^p,\beta)][Z_p(\alpha^p,\beta):Z_p(\alpha^p,\beta^p)]$. $x^p-\alpha^p \in Z_p(\alpha^p,\beta)[x]$是$\alpha$的零化多项式，又$\alpha^p$是$Z_p(\beta)$上的超越元.（若不然，有$f(x) \in Z_p(\beta)[x], f(x)\neq 0$,使$f(\alpha^p)=0$.同时也可看成$g(x)\in Z_p[x]$,使$g(\alpha,\beta) = f(\alpha^p) = 0$,与$\alpha,\beta$在$Z_p$上代数无关矛盾.）所以$\alpha^p$是$Z_p(\beta)[\alpha^p]$中素元素.由艾森斯坦因定理：$x^p-\alpha^p$是$Z_p(\alpha^p,\beta)[x]$中的不可约多项式.故$\mathrm{Irr}(\alpha,Z_p(\alpha^p,\beta)) = x^p-\alpha^p$.故$[Z_p(\alpha,\beta):Z_p(\alpha^p,\beta)] = [Z_p(\alpha^p,\beta)(\alpha):Z_p(\alpha^p,\beta)] = p$. $x^p-\beta^p \in Z_p(\alpha^p,\beta^p)[x]$是$\beta$的零化多项式，又$\beta^p$是$Z_p(\alpha^p)$中的超越元（同上）. 故$x^p-\beta^p$是$Z_p(\alpha^p,\beta^p)[x]$中不可约多项式，故$\mathrm{Irr}(\beta,Z_p(\alpha^p,\beta^p)) = x^p-\beta^p$. 故$[Z_p(\alpha^p,\beta):Z_p(\alpha^p,\beta^p)] = [Z_p(\alpha^p,\beta^p)(\beta):Z_p(\alpha^p,\beta^p)] = \deg(\beta,Z_p(\alpha^p,\beta^p)) = p$. 所以$[Z_p(\alpha,\beta):F] = [Z_p(\alpha,\beta):Z_p(\alpha^p,\beta)][Z_p(\alpha^p,\beta):Z_p(\alpha^p,\beta^p)] = p^2$.
2) 反设θ是本原元素，即$\theta \in Z_p(\alpha,\beta)$,且$Z_p(\alpha,\beta) = Z_p(\alpha^p,\beta^p)(\theta)$. 若$\theta \in Z_p(\alpha^p,\beta^p)$,则$Z_p(\alpha^p,\beta^p,\theta) = Z_p(\alpha^p,\beta^p) = Z_p(\alpha,\beta)$. 与$[Z_p(\alpha,\beta):F] = p^2$.矛盾！若$\theta \notin Z_p(\alpha^p,\beta^p)$,则由于$\theta \in Z_p(\alpha,\beta)$,所以$\exists c_{ij} \in Z_p$,使得$\theta = \sum_{i,j} c_{ij}\alpha^i\beta^j$或$(\sum_{i,j} c_{ij}\alpha^i\beta^j)^{-1}$ 所以$\theta^p = (\sum_{i,j} c_{ij}\alpha^i\beta^j)^p = \sum_{i,j} c_{ij}^p(\alpha^p)^i(\beta^p)^j \in Z_p(\alpha^p,\beta^p)$. 或$\theta^p = ((\sum_{i,j} c_{ij}\alpha^i\beta^j)^{-1})^p = (\sum_{i,j} c_{ij}^p(\alpha^p)^i(\beta^p)^j)^{-1} \in Z_p(\alpha^p,\beta^p)$.
故$x^p-\theta^p \in Z_p(\alpha^p,\beta^p)[x]$,且它是$\theta$的零化多项式.故$\deg(\theta,Z_p(\alpha^p,\beta^p)) \leq p$.而$[Z_p(\alpha,\beta):F] = [F(\theta):F] = \deg(\theta,Z_p(\alpha^p,\beta^p)) = p^2$.矛盾！
故这样的θ不存在.所以$Z_p(\alpha,\beta)$在F上无本原元素.证毕. ■

5. 设域F的特征$p \neq 0$,$F(\alpha,\beta)$是F的代数扩张，α可分，$\deg(\alpha,F) = n$,β不可分，$\deg(\beta,F) = p$.求$[F(\alpha,\beta):F]$.

证明 $\because \beta$可分，$\deg(\beta,F) = p$.
$\therefore \mathrm{Irr}(\beta,F) = (x-\beta)^p$.
又$\because F(\alpha)$是可分扩张,β不可分.
$\therefore \beta \overline{\in} F(\alpha)$.
同定理3.4.4的方法，可证:
$(x-\beta)^p$是$F(\alpha)[x]$上的不可约多项式.
$\therefore [F(\alpha)(\beta):F(\alpha)] = p$.
$\therefore [F(\alpha,\beta):F] = [F(\alpha)(\beta):F(\alpha)]\cdot[F(\alpha):F] = pn$. ■

6. 设E是域F的有限扩张，证明E中存在关于F的本原元素的充要条件是E与F间只有有限个中间域.

证明 “⇐”若F是有限域，则显然.若F是无限域，反设结论不成立,
则$\exists \alpha, \beta \in E$,使得$F(\alpha, \beta) \subseteq E$,且$F(\alpha, \beta)$不是$F$的单扩张，
显然$F(\alpha + x\beta) \subset F(\alpha, \beta) \forall x \in F$.
若$x_1, x_2 \in F, x_1 \neq x_2$.则$F(\alpha + x_1\beta) \neq F(\alpha + x_2\beta)$.
(否则$\alpha, \beta \in F(\alpha + x_1\beta) = F(\alpha + x_2\beta) = F(\alpha, \beta)$.矛盾)
此时，e与F之间有无限个中间域，矛盾.
“⇒”若$E = F(\alpha)$,令$\mathrm{Irr}(\alpha, F) = p(x)$.
若$F \subset K \subset E$,即K是与F的E中间域.
则$\mathrm{Irr}(\alpha, K) = p_1(x) \mid p(x)$,且$K(\alpha) = E$.
令K'为F上添加$P_1(x)$的系数生成的域,则$K' \subseteq K$.
又显然$\mathrm{Irr}(\alpha, K') \mid p_1(x)$,则$[E : K] \geq [E : K']$.
$\therefore K = K'$.由K'的取法知E与F间只有有限个中间域. ■

7. 设K是域F的代数扩张，Ch $F = p \neq 0$,证明K是F的可分扩张的充要条件是$K^p = \{\alpha^p | \alpha \in K\}$生成的$F$上的线性空间$K$的子空间为$K$.

8. 设K是域F的代数扩张，Ch $F = p \neq 0$,令K_0为K中（对F的）可分元素的集合（K_0称为F在K中的可分闭包）.试证明:
1) K_0是K的子域，且K是K_0的不可分扩张;
2) $\forall \alpha \in K - K_0$, $\exists e \in N$,使得$\alpha^{p^e} \in K_0$.

证明 1)$\forall \alpha, \beta \in K_0, \therefore \alpha, \beta$是可分元素.
$\therefore F(\alpha, \beta)$是$F$的可分扩张，
$\therefore \alpha - \beta, \alpha\beta^{-1} \in F(\alpha, \beta) \subseteq K_0$
$\therefore K_0$是K的子域.
若$\exists \alpha \in K - k_0$是对$K_0$的可分元素，则$K_0(\alpha)$是$K_0$的可分扩张，又$\because$ K_0是F的可分扩张，$K(\alpha)$是F的可分扩张，
$\therefore \alpha$是F的可分元素，矛盾.
2)$\forall \alpha \in K - K_0$,则$\alpha$是$F$上的不可分元素，
E是$\mathrm{Irr}(\alpha, F)$的分裂域，则$\mathrm{Irr}(\alpha, F)$在E中有分解:
$\mathrm{Irr}(\alpha, F) = (x - \alpha)^{p^e}(x - \alpha_1)^{p^e} \cdots (x - \alpha)^{p^e}$.
且$h(x) = (x - \alpha^{p^e})(x - \alpha_1^{p^e}) \cdots (x - \alpha^{p^e})$是$F[x]$中可分的不可约多项式.
从而是K中（对F的）可分元素，$\therefore \alpha^{p^e} \in K_0$. ■

9. 设K是域F的代数扩张，Ch $F = p \neq 0$, 对$\alpha \in K$,若有整数$e \geq 0$使得$\alpha^{p^e} \in F$,则称α是F上的纯不可分元素.若K中每个元素都是F上的纯不可分元素，则称K为F的纯不可分扩张，试证：
1) $\alpha \in K$为F上纯不可分元素的充要条件是：$\mathrm{red}(\mathrm{Irr}(\alpha, F)) = 1$;
2) 若$\alpha \in K$在F上既是可分的又是纯不可分的，则$\alpha \in F$;
3) 设K_0为F在K中的可分闭包，则K是K_0的纯不可分扩张.

证明 1)$\alpha \in K$为F上纯不可分元素
$\Leftrightarrow \exists e$,使得$\mathrm{Irr}(\alpha, F) = (x-\alpha)^{p^e}$
$\Leftrightarrow \mathrm{red}(\mathrm{Irr}(\alpha, F)) = 1$;
2)$\alpha \in K$在F上既是可分的又是纯不可分得:
$\mathrm{Irr}(\alpha, F) = (x-\alpha)$.
$\therefore \alpha \in F$;
3)$\forall \alpha \in K_0$,有$\alpha \in k$,
$\forall \alpha \in K - K_0, \exists e \in N$,使得$\alpha^{p^e} \in K_0$.(第8题结论)
$\therefore K$是K_0的纯不可分扩张. ■

10. 设域F的特征$p \neq 0$,E, K都是F的代数扩张，且$F \subset E \subset K$,证明K是F的纯不可分扩张当且仅当E是F的纯不可分扩张且K是E的纯不可分扩张.

证明 "⇒"若K是F的纯不可分扩张.
$\because \alpha \in K, \therefore \exists e \geq 0$,使得$\alpha^{p^e} \in F \subseteq E$,
$\therefore K$是E的纯不可分扩张.
$\because \alpha \in E \subseteq K, \therefore \exists e \geq 0$,使得$\alpha^{p^e} \in F$,
$\therefore E$是F的纯不可分扩张.
"⇐"$\forall \alpha \in K, \exists e_1 \geq 0$,使得$\alpha^{p^{e_1}} \in E$,
$\exists e_2 \geq 0$,使得$(\alpha^{p^{e_1}})^{e_2} = \alpha^{p^{(e_1+e_2)}} \in F$.
$\therefore K$是F的纯不可分扩张. ■

11. 设K是域F的有限扩张，Ch $F = p \neq 0$, K_0为F在K中的可分闭包，试证存在整数$e \geq 0$使得$[E:F] = [K_0:F]p^e$.

12. 设K是域F的代数扩张，Ch $F = p \neq 0$,试证K中F上的纯不可分元素的集合E是一个中间域.

13. 设K是域F的有限纯不可分扩张，试问K有多少个$F-$自同构?

证明 若σ是K的$F-$自同构，
则$\forall \alpha \in K, \alpha(\alpha) = \alpha_i, \alpha_i$是$\mathrm{Irr}(\alpha, F)$的根.
而$\mathrm{Irr}(\alpha, F)$的根只有α,
$\therefore K$的$F-$自同构只有$\sigma = \mathrm{id}$. ■

14. 设K是域F的正规扩张，K_0是F在K中的可分闭包，试证K_0也是F的正规扩张.

证明 $\forall \alpha \in K_0, \mathrm{Irr}(\alpha, F)$在$K[x]$中的分解为:
$\mathrm{Irr}(\alpha, F) = (x-\alpha)(x-\alpha_1)\cdots(x-\alpha_m), i \neq j$时$\alpha \neq \alpha_i \neq \alpha_j$.
$\alpha_i (1 \leq i \leq m)$是$K$对$F$的可分元素.
$\therefore K_0$也是F的正规扩张. ■

Chapter 4

群

4.1 群的生成组

1. 设群G的阶为4.试证G为4阶循环群或与Klein四元素群K_4同构.
证明 方法甚多，例如把4阶群看作$\mathbf{S}_4$的子群来考虑.这里直接做了.
(i) G中有一个4阶元，则G是4阶循环群.
(ii) G中没有4阶元，那么$\forall a \in G, a^2 = e$.从而对$\forall a, b \in G, (ab)^2 = e$,,即$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$,故$G$是Abel群，易见$G \cong K_4$. ■

2. 设群G的阶为6.试证G为6阶循环群或与$\mathbf{S}_3$同构.
证明 G中必有一个3阶元，否则除幺元外都是2阶元，则必是Abel群，那么任取$a \neq b \in G$,且$a \neq e, b \neq e$,则$\langle a, b\rangle$是4阶群，矛盾.
G中必有一2阶元，否则除幺元外都是3阶元，那么$|G|$是奇数，矛盾.
取G中一2阶元a,一3阶元b.
1):a, b可换，则ab是6阶元，从而$G = \langle ab\rangle$是个6阶循环群.
2):a, b不可环，那么G中无6阶元.设G中k个3阶群，j个2阶群，则$2k + j + 1 = 6$,那么$(k, j) = (2, 1)$或$(1, 3)$.若$k = 2$,可令G中3阶元为$\{x, x^{-1}, y, y^{-1}\}$.易见xy不是3阶元和幺元，那么xy是唯一的2阶元，同样yx也是，故$xy = yx$,那么$\langle x, y\rangle$是9阶群，矛盾.故$(k, j) = (1, 3)$.我们知道存在G到$\mathbf{S}_6$的单同态φ,不妨设$\varphi(b) = (1, 2, 3)$,令$\varphi(a) = \sigma$. 由于G中有唯一的3阶群，而$\sigma(1, 2, 3)\sigma^{-1} = (\sigma(1), \sigma(2), \sigma(3))$,故$\{\sigma(1), \sigma(2), \sigma(3)\} = \{1, 2, 3\}$.由于$\sigma$与$(1, 2, 3)$不可换，故不能有$\sigma(1) = 1, \sigma(2) = 2, \sigma(3) = 3$,不妨令$\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 2$.设
$$\alpha = \begin{pmatrix} 4 & 5 & 6 \\ \sigma(4) & \sigma(5) & \sigma(6) \end{pmatrix}$$
那么$\sigma = (2, 3)\alpha$,且由$\sigma^2 = e$,知$\alpha^2 = e$.易得
$\langle \sigma, (1, 2, 3)\rangle = \{(1, 2, 3), (1, 3, 2), e, (2, 3)\alpha, (1, 2)\alpha, (3, 1)\alpha\}$同构于$\mathbf{S}_3$

所以$G \cong \mathbf{S}_3$. ■

3. 设G是$r = st$阶循环群，H是G的t阶子群.试证

$$H = \{g^s | g \in G\} = \{h \in G | h^{'} = e\}.$$

证明 设$G = \langle g_0 \rangle$,那么$\{g^s | g \in G\} = \{g_0^s, g_0^{2s}, \cdots, g_0^{ts}\}, \{h \in G | h^t = e\} = \{g_0^s, g_0^{2s}, \cdots, g_0^{ts}\}$,而$\{g_0^s, g_0^{2s}, \cdots, g_0^{ts}\}$是$G$的$t$阶子群，且循环群$G$的$t$阶子群唯一.故

$$G = \{g^s | g \in G\} = \{h \in G | h^t = e\}$$

■

4. 设G是一个群，$a, b \in G$.称$[a, b] = aba^{-1}b^{-1}$为a, b的**换位子**.由所有换位子$\{aba^{-1}b^{-1} | a, b \in G\}$生成的子群$G^{(1)}$称为$G$的**换位子群**.试证:
   1) 如果$\alpha \in \mathrm{Aut}\, G$,则$\alpha(G^{(1)}) = G^{(1)}$;
   2) 若$H \lhd G$.则G/HAbel群的充要条件是$H \supseteq G^{(1)}$.

   证明 1) $\alpha(G^{(1)}) = \alpha(\langle \{aba^{-1}b^{-1} | a, b \in G\} \rangle) = \langle \{\sigma(a)\sigma(b)\sigma(a)^{-1}\sigma(b)^{-1} | a, b \in G\} \rangle = G^{(1)}$.
   2) G/H为Abel群$\Leftrightarrow (G/H)^{(1)} = \{e\} \Leftrightarrow G^{(1)} \subseteq H$. ■

5. 设S是群G的生成组，又φ, ψ都是G到群H上的同态，若$\varphi(x) = \psi(x), \forall x \in S$.证明$\varphi = \psi$.

   证明 对$\forall a \in G$,由$G = \langle S \rangle$,可令$a = y_1 y_2 \cdots y_n$,且$y_i \in S$或$y_i^{-1} \in S$.而$\varphi(x) = \psi(x), \forall x \in S$,故$\varphi(x^{-1}) = \psi(x^{-1}), \forall x \in S$,从而$\varphi(y_i) = \psi(y_i), \forall 1 \leq i \leq n$,故$\varphi(a) = \psi(a)$,即$\varphi = \psi$. ■

6. 设H是群G的子群，且$H \neq G$.证明$G = \langle G - H \rangle$.

   证明 由$H \neq G$知$\exists a \in G$,且$G\overline{H}$,那么$aH \cap H = \varnothing$,而$\langle aH \rangle \supseteq H$,故$\langle G - H \rangle \supset H \cup (G - H) = G$,当然$G = \langle G - H \rangle$. ■

7. 设G是偶数阶群，证明G必有2阶元素.

   证明 设G中有k个m阶循环群（$m > 1$），则m阶元为$k\varphi(m)$个，这里φ是欧拉函数.若m是奇数，那么$\varphi(m)$为偶数，可见除幺元外奇数元的个数为偶数个.而$|G|$为偶数，故必有偶阶元，从而存在2阶元. ■

8. 将$\alpha \in \mathbf{S}_3$分解为不相交轮换之积.这里

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 5 & 4 & 8 & 2 & 7 & 1 \end{pmatrix}$$

   解 $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 5 & 4 & 8 & 2 & 7 & 1 \end{pmatrix} = (1358)(26)$. ■

9. 证明$\mathbf{S}_n = \langle\{(1\quad 2), (2\quad 3), \cdots, (n-1\quad n)\}\rangle$.
证明 用归纳法证明.当$n = 2$时，显然成立.假设$n = k$时成立.那么当$n = k+1$时，由归纳知

$$\langle\{(1\quad 2), \cdots, (k-1\quad k)\}\rangle = \mathbf{S}_k$$

而

$$(1\quad k)(k\quad k+1)(1\quad k) = (1\quad k+1)$$

故

$$\langle\{(1\quad 2), \cdots, (k-1\quad k), (k\quad k+1)\}\rangle = \langle\{(1\quad 2), \cdots, (1\quad k), (1\quad k+1)\}\rangle = \mathbf{S}_{k+1}$$

自然

$$\langle\{(1\quad 2), \cdots, (n-1\quad n)\}\rangle = \mathbf{S}_n$$

于是$n = k+1$时命题成立.从而对一切$n \in N$命题成立. ■

10. 证明$(i_1 i_2 \cdots i_r)^{-1} = (i_r i_{r-1} \cdots i_1)$.
证明

$$(i_1\quad \cdots\quad i_r)(i_r\quad i_{r-1}\quad \cdots\quad i_1) = e$$

■

11. 证明$\forall \sigma \in \mathbf{S}_n$,有

$$\sigma(i_1 i_2 \cdots i_r)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r)).$$

证明 对于$j = 1, 2, \cdots, r-1, (\sigma(i_1 i_2 \cdots i_r)\sigma^{-1})(\sigma(i_j)) = \sigma(i_1 i_2 \cdots i_r)(i_j) = \sigma(i_{j+1})$,
对于$j = r, (\sigma(i_1 i_2 \cdots i_r)\sigma^{-1})(\sigma(i_r)) = \sigma(i_1 i_2 \cdots i_r)(i_r) = \sigma(i_1)$,
对于$j = r+1, \cdots, n, (\sigma(i_1 i_2 \cdots i_r)\sigma^{-1})(\sigma(i_j)) = \sigma(i_1 i_2 \cdots i_r)(i_j) = \sigma(i_j)$,
$\therefore \sigma(i_1 i_2 \cdots i_r)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r))$. ■

12. 设群G的阶为$2k$,其中k是奇数且$k > 1$.试证G中必有指数为2的子群.
证明 由Cayley定理知：

$$G \backsimeq L_G$$

由$|G| = 2k$知存在2阶元$a \in G$,那么对$\forall x \in G, L_a(x)^2 = x$,可见$L_a$是$k$个对换之积，而$k$是奇数，从而$L_a$是奇置换，故$L_G$中存在指数为2的子群，自然$G$中也有. ■

13. 设σ是r－轮换.试问：
1) σ^k仍为轮换的冲要条件是什么？
2) 如果σ^k仍为轮换，σ^k的长是多少？

解 1) 由对称性知，σ^k仍为轮换$\Leftrightarrow$ σ^k的轮换长度为1或r $\Leftrightarrow$ σ^k的阶为1或r $\Leftrightarrow$ $(k,r)=1$或r.
2) 当$(k,r)=1$时,σ^k的长为r;当$(k,r)=r$时，σ^k的长为1. ■

14. 设σ是r－轮换，又$k|r$.证明σ^k分解为k个长为r/k的不相交到的轮换之积.

证明 设$n=r/k$,则$n\in\mathbf{N}$.,设$\sigma=(\alpha_1\alpha_2\cdots\alpha_r)=\begin{pmatrix}\alpha_1 & \alpha_2 & \cdots & \alpha_{r-1} & \alpha_r\\ \alpha_2 & \alpha_3 & \cdots & \alpha_r & \alpha_1\end{pmatrix}$
则$\sigma^k=\begin{pmatrix}\alpha_1 & \alpha_2 & \cdots & \alpha_{r-k} & \alpha_{r-k+1} & \cdots & \alpha_r\\ \alpha_{k+1} & \alpha_{k+2} & \cdots & \alpha_r & \alpha_1 & \cdots & \alpha_k\end{pmatrix}$
就有：$\sigma^k=(\alpha_1\alpha_{k+1}\alpha_{2k+1}\cdots\alpha_{(n-1)k+1(=r-k+1)})$
$(\alpha_2\alpha_{k+2}\alpha_{2k+2}\cdots\alpha_{(n-1)k+2(=r-k+2)})\cdots(\alpha_k\alpha_{2k}\cdots\alpha_{nk(=r)})$,显然上述各轮换不相交，且长均为$n$,即$r/k$,
$\therefore$ σ^k可分解为k个长为r/k的不相交的轮换之积. ■

4.2 群在集合上的作用

1. 设正方形$\square A_1A_2A_3A_4$的四条边分别为s_1,s_2,s_3,s_4.四条边的中点分别为M_1,M_2,M_3,M_4. 对边中点连线为m_1,m_2.对角线为d_1,d_2.中心为O.（见下图）G是使$\square A_1A_2A_3A_4$不变的保长变换的集合.用通常方式定义G在

$$X=\{A_i,M_i,s_i,m_i,d_i,O\}$$

上的作用.确定X的轨道分解.

解 使$\square A_1A_2A_3A_4$不变的保长变换即是正交变换（旋转和反射），并使$\square A_1A_2A_3A_4$不变（形状位置均不变，四顶点标号可变），以通常方式作用在X上即$\forall g\in G,g$为$\mathbf{R}^2$的一个保长变换，g将X中的点P变为变为$g(P)$.
$\therefore$ X的轨道分解为：

$$\{A_1,A_2,A_3,A_4\}\cup\{M_1,M_2,M_3,M_4\}\cup\{s_1,s_2,s_3,s_4\}\cup\{m_1,m_2\}\cup\{d_1,d_2\}\cup\{O\}.$$

其中G有8个元素，由$a=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$（绕$O$旋转$\pi/2$），$b=\{$关于$m_1$的反射$\}$生成，$a$ 的阶为4，b的阶为2. ■

2. 设群G作用在集合X上，Y是X的子集，令
$$F_Y = \{g \in G | g(Y) = Y\}$$
又对X的子集Z，若$\exists g \in G$使$Z = g(Y)$，则称Z与Y在G作用下共轭.试证
1) F_Y是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.
证明 1) $\forall g_1, g_2 \in F_Y$,那么$g_1 g_2^{-1}(Y) = g_1(Y) = Y$,故$g_1 g_2^{-1} \in F_Y$,即$F_Y$是$G$的子群.
2) $\forall g_1 \in F_Y$，那么$gg_1g^{-1}(g(Y)) = g(Y)$,故$F_{g(Y)} \supseteq \mathrm{ad}\, g(F_Y)$.同样$F_Y = F_{g^{-1}(g(Y))} \supseteq \mathrm{ad}\, g^{-1}(f_{G(Y)})$,即$F_{g(Y)} \subseteq \mathrm{ad}\, g(F_Y)$,从而$F_{g(Y)} = \mathrm{ad}\, g(F_Y)$.
3) 构造子集族$T = \{g(Y) | g \in G\}$.作G在T的作用：$\forall Z \in T, g(Z) = \{g(z) | z \in Z\}$.显然$Y$的迷向子群就为$F_Y, g$在$T$上可递，又$|G| < \infty$,故$X$中与$Y$共轭的子集个数为$|T| = [G : F_Y]$. ■

3. 设群G的子群H的指数为n.证明H中包含G的一个正规子群N且$[G : N] | n!$.
证明 考虑G在G/H上的左平移作用，诱导出G到$\mathbf{S}_n$上一个同态η,而$\ker \eta = \bigcap\limits_{x \in G/H} Fx$, 且$F_{eH} = H$,记$N = \ker \eta$.那么$N \subset H$,且$N \lhd G$,$[G : N] | n!$. ■

4. 设p是有限群G的阶的最小素因数，又H为G的子群且$[G : H] = p$.试证$H \lhd G$.
证明 由p是有限群G的解的最小素因数，知G的任一子集$K, [G : K]$中最小素因子不小于p,而由上题知存在G 的正规子群N,满足$N < H$,且$[G : H] | p!$,那么$[G : N] = p$,故$H = N$,即$H \lhd G$. ■

5. 设群G的每个元素都是有限阶元素（这样的群称为周期群），H为G的子群，$[G : H] = m$.又G中任何非幺元的阶不小于m.试证$H \lhd G$.
证明 令$d = \min\{o(g) | o(g)$为g的阶，$g \in G$,且$g \neq e\}$,显然d为素数，且$d \geq m$.若$m = 1$,自然$H \lhd G$.设$m > 1$,则有$g \in G$且$g \in H$,令$s = \min\{t | gt \in H\}$,可见$[G : H] \geq s$,且$(s, o(g)) > 1$,那么$s \geq d$!即$m \geq d$,从而m也是个素数，由题3可得$H \lhd G$. ■

6. 设G是一个群，试证：
1) 当且仅当$G = \{e\}$时，G在G上的伴随作用可递.
2) 当且仅当$C(G) = \{e\}$时，G在G上的伴随作用有效.
证明 1) 由$Oe = \{e\}$可知：G在G上的伴随作用可递$\Leftrightarrow G = \{e\}$.
2) 由定义易得. ■

7. 写出$\mathbf{S}_3, \mathbf{S}_4$的共轭类.

解 $\mathbf{S}_3$的共轭类有3种，分别以$(1), (12), (123)$为代表，$C_{(1)} = \{(1)\}, C_{(12)} = \{(12), (13), (23)\}, C_{(123)} = \{(123), (132)\}$. ■

8. 试证$\mathbf{S}_3$的共轭类与n的**分划**

$$n = n_1 + n_2 + \cdots + n_q, n_1 \geq n_2 \geq \cdots n_q \geq 1$$

间有一一对应关系.

证明 设$\sigma \in \mathbf{S}_n$,那么有

$$\sigma(i_1, \cdots, i_r)\sigma^{-1} = (\sigma(i_1), \cdots, \sigma(i_r))$$

可得$\sigma, \eta \in \mathbf{S}_n, \sigma$与$\eta$共轭当且仅当$\sigma, \eta$写成不相交的轮换之积的形状一致.我们作$\mathbf{S}_n$的共轭类到$n$的分划的对应：设$\sigma \in \mathbf{S}_n, \sigma = \sigma_1\sigma_2\cdots\sigma_k, \sigma_1, \sigma_2, \cdots, \sigma_k$是$k$个不相交的轮换.用$|\sigma_i|$表示轮换$\sigma_i$的长度，有

$$\sum_{i=1}^{k} |\sigma_i| = n$$

且$|\sigma_1| \geq |\sigma_2| \geq \cdots \geq |\sigma_k|$.那么降以$\sigma$为代表的共轭类映到这样的$n$的分划：

$$n = |\sigma_1| + |\sigma_2| + \cdots + |\sigma_k|.$$

显然这样的对应是一一的. ■

9. 设H是群G的子群.证明下列条件等价：

1) H是群G的正规子群；
2) $C_h \subseteq H$,若$h \in H$;
3) $C_g \cap H = \varnothing, g \overline{\in} H$.

证明 由定义易得. ■

10. 设H是群G的子群，试证：

1) 对$\forall g \in G, H_1 = gHg^{-1}$也是$G$的子群（称为$H$的**共轭子群**）.
2) 群G的子集$N_G(H) = \{g \in G | gHg^{-1} = H\}$也是$G$的子群且$H \lhd N_G(H)$.（$N_G(H)$称为$H$在$G$中的**正规化子**，也简称为$H$的正规划子.）3) G中与H共轭的子群的个数为$[G : N_G(H)]$.
4) $H \lhd G \iff N_a(H) = G$.

证明 1) $\because \operatorname{ad} g \in \operatorname{Int} G, \therefore$将子群$H$变成$G = ad\, gG$的子群$gHg^{-1}$.
2) 令$X = \{gHg^{-1} | g \in G\}$,考虑$G$到$X$上的一个作用：

$$g(K) = gKg^{-1}, \forall K \in X.$$

易见$N_G(H)=F_H$,而$H\lhd N_G(H)$是显然的.

3) 2中的作用显然是可递的，故G中与H共轭的子群的个数为

$$|X|=[G:N_G(H)].$$

4) $H\lhd G\Leftrightarrow|X|=1\Leftrightarrow[G:N_G(H)]=1\Leftrightarrow G=N_G(H)$. ■

11. 设H是有限群G的真子群（即$H\neq G$）.试证$G\neq\bigcup\limits_{g\in G}gHg^{-1}$.

证明 由上题3知$|\bigcup\limits_{g\in G}gHg^{-1}|\leq[G:N_G(H)](|H|-1)+1\leq[G:H]|H|+1-[G:H]=|G|+1-[G:H]<|G|$,故$G\neq\bigcup\limits_{g\in G}gHg^{-1}$. ■

12. 设H是群G的子群.G的子集

$$C_G(H)=\{g\in G|gh=hg,\forall h\in H\}$$

称为H在G中的**中心化子**,也简称为H的中心化子.试证:

1) $C_G(H)=\bigcap\limits_{h\in H}C_G(h)$;

2) $C_G(H)\lhd N_G(H)$.

证明 由定义易得. ■

13. 设H,K都是群G的子群.$\forall k\in K$,称kHk^{-1}与H是**K-共轭**的.证明H的不同**K**-共轭子群的个数恰为$[K:K\cap N_G(H)]$.

证明 将题10的2中的作用限制在K上，则$F_H=K\cap N_G(H)$,故H的不同$K-$共轭子群的个数恰为$[K:K\cap N_G(H)]$. ■

14. 设θ是群G的任一自同构,试证$\theta(C(G))=C(G)$.

证明 由定义易得. ■

15. 设$\mathrm{Aut}\,G$是群G的自同构群,$C(G)=\{e\}$(e为G的幺元).证明$C(\mathrm{Aut}\,G)=\{\mathrm{id}_G\}$.

证明 设$\theta\in C(\mathrm{Aut}\,G)$,那么对$\forall g\in G,af\,g\theta\mathrm{ad}\,g^{-1}=\theta$.从而对$\forall h\in G,\mathrm{ad}\,g\theta\mathrm{ad}\,g^{-1}(h)=\theta(h)$,即$(g\theta(g^{-1}))\theta(h)(g\theta(g^{-1}))^{-1}=\theta(h)$,故$\theta(g)=g$,即$\theta=\mathrm{id}_G$,从而

$$C(\mathrm{Aut}\,G)=\{\mathrm{id}_G\}.$$

■

16. 设a是有限群G的自同构.令$I=\{g\in G|\alpha(g)=g^{-1}\}$.试证:

1) 若$|I|>\frac{3}{4}|G|$,则G为Abel群;

2) 若$|I|=\frac{3}{4}|G|$,则G中一定包含一个指数为2的Abel子群.

17. 设群G作用在集合X上,若对$\forall x_1,x_2,y_1,y_2 \in X, x_1 \neq x_2, y_1 \neq y_2, \exists g \in G$使$y_1 = g(x_1), y_2 = g(x_2)$.则称$G$在$X$上的作用**双重可递**.
设$\Pi(X) = \{X_1, X_2, \cdots, X_k, \cdots\}$
是X的一个分划,令$g(\pi(X)) = \{g(X_1), g(X_2), \cdots, g(X_k), \cdots\}$,则$g(\pi(X)) = \pi(X)$的充要条件是$\pi(X) = \{X\}$ 或$\pi(X) = \{\{x\}|x \in X\}$.试证以上结论.
证明 充分性是显然的.
下证必要性.若有i使$|X_i| > 1$,不妨设$x_1, x_2 \in X_i$,那么$\forall y \neq x_1, x_2$,由G是X上的双重可递作用，故有g,使得$g(x_1) = x_1, g(x_2) = y$,而$g(\pi(X)) = \pi(X)$,故$y \in x_i$,从而$X_i = X$,即$\pi(X) = \{X\}$.若对$\forall i, |X_i| = 1$,即$\pi(X) = \{\{x\}|x \in X\}$. ■

18. 试证当$n \geq 2$时,$\mathbf{S}_n$在$\{1, 2, \cdots, n\}$上的作用是双重可递的.
证明 由$\mathbf{S}_n$的定义可得. ■

19. n满足什么条件时,A_n在$\{1, 2, \cdots, n\}$上的作用是双重可递?
解 当$n \neq 2, 3$时，A_n在$\{1, 2, \cdots, n\}$上的作用是双重可递的.
显然$n = 2$或3时，A_n在$\{1, 2, \cdots, n\}$上的作用不是双重可递的.$n = 1$时，显然是的.
当$n \geq 4$时，对$\forall x_1, x_2, y_1, y_2 \in \{1, 2, \cdots, n\}, x_1 \neq x_2, y_1 \neq y_2$,我们知存在$\sigma \in \mathbf{S}_n$使$y_1 = \sigma(x_1), y_2 = \sigma(x_2)$,取$x_3, x_4$使$x_1, x_2, x_3, x_4$互不相等，令$\sigma_1 = (\sigma(x_3), \sigma(x_4))\sigma$,那么$\sigma_1, \sigma_2$中必有一个属于$A_n$,且$\sigma(x_1) = y_1, \sigma(x_2) = y_2$,故$A_n$在$\{1, 2, \cdots, n\}$上的作用是双重可递的. ■

4.3 Sylow 子群

1. 设p是素数.证明p^2阶群一定是交换群.而且在同构意义下,仅有两类p^2阶群.
证明 由$C(G) \neq \{e\}$,可得p^2阶群一定是交换群.
1) G中有p^2阶元，则G是p^2阶循环群.
2) G中无p^2阶元，那么除了幺元外，其它的都是p阶元.任取$a \neq e$,那么有$b \in \langle a\rangle$,显然$G = \langle a\rangle \otimes \langle b\rangle \cong \mathbf{Z}_p \oplus \mathbf{Z}_p$.可见在同构意义下，仅有两类$p^2$阶群. ■

2. 设p是奇素数,$G =< a, b, c >$ .a, b, c满足

$$a^p = b^p = c^p = e, ab = ba, ac = ca, bc = cb$$

其中e为G的幺元.试证:G是一个p^3阶群, 且除幺元外的任何元素的阶均为p.

3. 设p为素数,F是p^{l-1}阶子群,证明$F \lhd G$.
证明 由上节第四题结论:"设p是有限群G的阶的最小素因数,又H为G的子群,且$[G:H]=p$,则$H \lhd G$".本题中p是有限群G的阶的最小素因数,$F<G$,且$[G:H]=|G|/|F|=p^l/p^{l-1}=p$.由此可知$F \lhd G$. ■

4. 写出$\mathbf{S}_4$的所有Sylow 3−子群.
解 $|\mathbf{S}_4|=24=3\times 2^3$,$\therefore$ $\mathbf{S}_4$的Sylow 3−子群是3阶子群,设有k个.则$k\equiv 1(\mathrm{mod}\ 3)$且$k|8$,从而$k$只可能是1或4.$(1\ 2\ 3)\in \mathbf{S}_4$,且$(1\ 2\ 3)$是一个3阶元,$\therefore$ $\langle(1\ 2\ 3)\rangle=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$是一个Sylow 3−子群.
$(1\ 4)\in \mathbf{S}_4$,由Sylow第二定理知$(1\ 4)\langle(1\ 2\ 3)\rangle(1\ 4)^{-1}=\{(1),(2\ 3\ 4),(2\ 4\ 3)\}$也是Sylow 3−子群.
同理,$(2\ 4)\langle(1\ 2\ 3)\rangle(2\ 4)^{-1}=\{(1),(1\ 3\ 4),(1\ 4\ 3)\}$,$(3\ 4)\langle(1\ 2\ 3)\rangle(3\ 4)^{-1}=\{(1),(1\ 2\ 4),(1\ 4\ 2)\}$都是Sylow 3−子群.
$\therefore k=4$.
$\mathbf{S}_4$的所有Sylow 3−子群为:

$$p_1=\{(1),(1\ 2\ 3),(1\ 3\ 2)\},p_2=\{(1),(2\ 3\ 4),(2\ 4\ 3)\},$$

$$p_3=\{(1),(1\ 3\ 4),(1\ 4\ 3)\},p_4=\{(1),(1\ 2\ 4),(1\ 4\ 2)\}$$

(注:直接找出4个3阶元$(1\ 2\ 3),(1\ 2\ 4),(1\ 3\ 4),(2\ 3\ 4)$即可.) ■

5. 证明阶为56或148的群不是单群.
证明 若群G的阶为56，设K为G中Sylow 7−子群的个数，于是$K\equiv 1(\mathrm{mod}\ 7)$且$K|8$,可得$K=1$或8.若$K=1$,则$G$非单；若$K=8$,那么7阶元为$8\times(7-1)=48$个，那么$G$中其他元为8个，而$G$中存在8阶的Sylow 2−子群，故这8个元组成唯一的Sylow 2−子群，故56阶群非单. 若$|G|=148=2^2\times 37$,易得Sylow37子群唯一，故148阶群非单. ■

6. 设群G的阶为35^3.则G有一个125阶的正规子群.
证明 由Sylow第三定理易得G中125阶的Sylow 5−子群唯一，故该125阶子群正规. ■

7. 设群G的阶为p^lm,p为素数,且$p>m(m\neq 1)$.证明G不是单群.
证明 考虑Sylow p−子群即可. ■

8. 设p,q都是素数,$p<q,p\nmid(q-1)$.证明pq阶群一定是循环群.
证明 由Sylow第三定理易得，p，q阶群唯一，从而它是个循环群. ■

9. 证明255阶群一定是循环群.
证明 $255=3\times 5\times 17$,用Sylow第三定理可得：Sylow 17−子群唯一，Sylow 5−子群1个或51个，Sylow 3−子群1个或85个.

令Sylow 17−子群为$P_{17}=\langle a\rangle$,任取Sylow 3−子群$P_3=\langle b\rangle$,Sylow 5−子群$P_5=\langle c\rangle$. 由于P_{17}是正规的，故$P_5\times P_{17}$是G的子群，再由上题知$P_5\times P_{17}$是循环群，自然a，c可换.那么$P_5\times P_{17}$中85阶元为64个，若Sylow 5−子群不唯一，则为51个，从而5阶元为4×51204个，从而64+204<255,矛盾.故Sylow 5−子群唯一. 同样由上题知$P_3\times P_5, P_3\times P_{17}$为循环群，从而a，b，c之间两两可换，那么$G=\langle abc\rangle$是个255阶循环群. ■

10. 设H是有限群G的正规子群,p是$|G|$的素因数,且$p\nmid[G:H]$.试证H包含G的所有Sylow p−子群.

证明 由$P\nmid[G:H]$知H包含G中一个Sylow p−子群，设为P_1,又$H\lhd G$,故$gPg^{-1}\subseteq H,\forall g\in G$,从而$H$包含$G$所有的Sylow p−子群. ■

11. 设群G的阶为p^lm,p为素数,$(p,m)=1$,且$m<2p$.试证G中有正规Sylow p−子群或正规的p^{l-1}阶子群.

证明 取G中一个Sylow p−子群P,那么$[G:P]=m$,故P内有G的正规子群N使得$[G:N]|m!$, 即$[G:P][P:N]|m!$,由$[P:N]$是p次幂，而$p||m!$,故$[P:N]=1$或p, 从而G中有正规Sylow p−子群或正规的p^{l-1}阶子群. ■

12. 设素数p是有限群G的阶的因数,又P为G的一个Sylow p−子群.证明$N_G(N_G(P))=N_G(P)$.

证明 由题13可推出. ■

13. 设P是有限群G的Sylow p−子群.又G的子群$H\supseteq N_G(P)$.证明$N_G(H)=H$.

证明 设H中k个Sylow p−子群，设为$P,P_2,P_3,\cdots,P_k$. 设$g\in N_G(H)$,那么$gHg^{-1}=H$,自然$gPg^{-1}\subseteq H$,设$gPg^{-1}=P_j,h\in H$且$hPh^{-1}=P_j$,从而$(h^{-1}g)P(h^{-1}g)^{-1}=P$,那么$h^{-1}g\in N_G(P)\subseteq H$,故$g\in H, N_G(H)=H$. ■

14. 设G是非Abel p−群,证明$[G:C(G)]\geq p^2$.

证明 由G是非Abel p−群，故有$g\in G$,且$g\notin C_G(G)$. 显然$\langle g\rangle C(G)$是Abel群，故$[G:\langle g\rangle C(G)]\geq p$,又$[\langle g\rangle C(G):C(G)]\geq p$从而$[G:C(G)]\geq p^2$. ■

15. 设P是有限群G的Sylow p−子群，N是G的正规子群.试证$N\cap P, PN/N$分别为N与G/N的Sylow p−子群.

证明 设H是N的Sylow p−子群，那么有$g\in G$使得$gHg^{-1}\subseteq P$.由$N\lhd G$,可知$gHg^{-1}\subseteq N$,从而$gHg^{-1}\subseteq N\cap P$.再由$|H|=|N\cap P|$,可知$|N\cap P|=|H|$,从而$N\cap P$是$N$的一Sylow p−子群.

设$p^{l_1}|||N|, p^l||\ |G|$,那么$p^{l-l_1}||\ |G/N|$. 由同态基本定理知$PN/N \cong P/P\cap N$,可得$p^{l-l_1}||\ |PN/N|$,可知PN/N是PG/N的Sylow $p-$子群. 这里也能推出$p^{l-l_1}||\ |PN/N|$,那么$p^{l-l_1}||\ |P/P\cap N|$, 那么$p^{l_1}|\ |P\cap N|$,故$P\cap N$是N的Sylow $p-$子群. ■

4.4 有限单群

1. 设G是幺元为e的有限群，试证：

   (a) G中有子群序列

   $$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{n-1} \supset G_n = \{e\}$$

   使得a.$G_i \lhd G_{i-1}, 1 \le i \le n$; b.商群$G_{i-1}/G_i$是单群.

   (b) 若G是可换群，则G_{i-1}/G_i的阶为素数.

   证明 1)设$n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_k}^{\alpha_k}, p_i$为素数，令$l(n) = \alpha_1 + \cdots + \alpha_k$.注意到$(G_i/G_k)/(G_{i+1}/G_k) \cong G_i/G_{i+1}$, 对$l(|G|)$做归纳就可得.
   2)若G是可换群，那么G_{i-1}/G_i为Abel群，又G_{i-1}/G_i是单群，故G_{i-1}/G_i的阶为素数. ■

2. 设G是偶数阶Abel群，试证G一定有指数为2的子群.

   证明 设$n = |G|, n = 2^{l_0}{p_1}^{l_1}\cdots{p_k}^{l_k}, 2, p_1, \cdots, p_k$为不同的素因子.由上题知存在$G$的子群$H$,满足：$2^{l_0-1}||\ |H|$.设$P_i$为$G$的Sylow p_i-子群，$1 \le i \le k$.令$G_1 = HP_1\cdots P_k$,那么$[G : G_1] = 2$. ■

3. 求$(1\ 2\ 3)$在$\mathbf{A}_3$中的共轭类$C_{(1\ 2\ 3)}$.

   解 由于$\mathbf{A}_3 =< (1\ 2\ 3) >$,是个Abel群，故$C_{(1\ 2\ 3)} = \{(1\ 2\ 3)\}$. ■

4. 求$(1\ 2\ 3)$在$\mathbf{A}_4$中的共轭类$C_{(1\ 2\ 3)}$.

   解 首先，$(1\ 2\ 3)$在$\mathbf{S}_4$中的共轭类为与之有相同形式的置换的集合，即为$\{(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}$,记为$A$，则有$C_{(1\ 2\ 3)} \subseteq A$.
   其次，A中元素α属于$C_{(1\ 2\ 3)} \Leftrightarrow \exists\sigma \in \mathbf{A}_4$,使得$\sigma(1\ 2\ 3)\sigma^{-1} = \alpha$,即$(\sigma(1)\ \sigma(2)\ \sigma(3)) = \alpha$.
   显然，$(1\ 2\ 3) \in C_{(1\ 2\ 3)}$.
   若$(1\ 2\ 4) = (\sigma(1)\ \sigma(2)\ \sigma(3)) \Rightarrow \sigma = (3\ 4) \in \mathbf{A}_4, \therefore (1\ 2\ 4) \in C_{(1\ 2\ 3)}$.
   若$(1\ 4\ 2) = (\sigma(1)\ \sigma(2)\ \sigma(3)) \Rightarrow \sigma = (2\ 4\ 3) \in \mathbf{A}_4, \therefore (1\ 4\ 2) \in C_{(1\ 2\ 3)}$.
   同样可得出$(1\ 4\ 3), (1\ 3\ 2), (2\ 3\ 4) \in C_{(1\ 2\ 3)}$,
   $(1\ 3\ 4), (2\ 4\ 3) \in C_{(1\ 2\ 3)}$
   $\therefore C_{(1\ 2\ 3)} = \{(1\ 2\ 3), (1\ 4\ 2), (2\ 3\ 4), (2\ 4\ 3)\}$ ■

5. 设$n \geq 3, r, s$是$\{1, 2, \cdots, n\}$中有两个固定元素，证明

$$\mathbf{A}_n =< \{(r\ s\ t), t \neq r, s\} > .$$

证明 由引理知，当$n \geq 3$时，$\mathbf{A}_n$由所有3−轮换生成，故有$\mathbf{A}_n \supseteq <\{(r\ s\ t), t \neq r, s\} >$.
下面只需证$\mathbf{A}_n \subseteq <\{(r\ s\ t), t \neq r, s\} >$即可.
$\forall \alpha \in \mathbf{A}_n, \alpha$可表为偶数个对换之积，设$\alpha = \alpha_1\alpha_2\cdots\alpha_l$.其中每个$\alpha_i$为2个对换之积, $i = 1, 2, \cdots, l$.
有三种情形：
(1)

$$(i\ j)(i\ j) = \mathrm{id} = (r\ s\ t_0)^3, t_0 \neq r, s.$$
$$\therefore (i\ j)(i\ j) \in <\{(r\ s\ t), t \neq r, s\} > .$$

(2) $(i\ j)(i\ k) = (i\ j)(i\ r)(i\ r)(i\ k) = (i\ r\ j)(i\ k\ r) = (r\ i)(r\ j)(r\ k)(r\ i) = (r\ i)(r\ s)(r\ j)(r\ k)(r\ s)(r\ s)(r\ i) = (r\ s\ i)(r\ j\ s)(r\ s\ k)(r\ i\ s) = (r\ s\ i)(r\ s\ j)^2(r\ s\ k)(r\ s\ i)^2$,对于$i, j, k \neq r, s, (i\ j)(i\ k) \in <\{(r\ s\ t), t \neq r, s\} >$.
$(r\ j)(r\ k) = (r\ j)(r\ s)(r\ s)(r\ k) = (r\ s\ j)(r\ s\ k)^2$,其中$j, k \neq s$.
$(i\ r)(i\ k) = (i\ k\ r) = (r\ k)(r\ i) = (r\ k)(r\ s)(r\ s)(r\ i) = (r\ s\ k)(r\ s\ i)^2$,其中$k \neq s$.
$(i\ r)(i\ s) = (i\ s\ r) = (r\ s)(r\ i)(r\ s\ i)^2$,同理有$(s\ j)(s\ k), (i\ s)(i\ k) \in <\{(r\ s\ t), t \neq r, s\} >$.
综合以上各种情况有，对$\forall i, j, k, (i\ j)(i\ k) \in <\{(r\ s\ t), t \neq r, s\} >$. (3)
$(i\ k)(j\ l) = (i\ k)(i\ j)(j\ i)(j\ l)$,由第二种情况易得$\forall i, k, j, l, (i\ k)(j\ l) \in <\{(r\ s\ t), t \neq r, s\} >$.
综合以上三种情况，每个$\alpha_i \in <\{(r\ s\ t), t \neq r, s\} >$,
$\therefore \alpha \in <\{(r\ s\ t), t \neq r, s\} >$.
从而$\mathbf{A}_n \subseteq <\{(r\ s\ t), t \neq r, s\} >$. ■

6. 设G是非Abel有限单群，证明$|G| \geq 60$.

证明 设G是n阶群，且$n < 60$,且不是Abel群.由$2\times3\times5\times7 > 60$知n至多有3个不同的素因子.
1）n有一个素因子，可令$n = p^l$.由于G不是Abel群，故$l > 1, C(G) \neq G$,而$C(G) \lhd G$,故G非单.
2) n有2个不同的素因子，设$n = p^aq^b, p < q, p, q$为素数.
A) $p \geq 3$,由$60 > n > 3^{a+b}$,得$a + b \leq 3$. 当$a = 1$时，那么Sylow $q-$子群是唯一的，自然非单. 当$a = 2$时，$n = 3^2 * 5$,Sylow $5-$子群也唯一，G也非单.
B) $p = 2$.若$q > 7$,则$p^a < 60/11 < q$,故Sylow $q-$子群唯一.G非

单.若$q \geq 7$,即$q = 3, 5, 7$.我们知道，当$a = 1$时，Sylow $q-$子群唯一，G非单. 那么当$a \geq 2$时，n只有以下几种情况：$2^2 \times 3, 2^2 \times 3^2, 2^2 \times 5, 2^2 \times 7, 2^3 \times 3, 2^3 \times 5, 2^3 \times 7$.
当$n = 2^2 \times 5$或$2^2 \times 7$时，Sylow $q-$子群唯一，故G非单.
当$n = 2^2 \times 3$时，考虑3阶元的个数便知G非单.
当$n = 2^2 \times 3^2$或$2^3 \times 3$时，那么Sylow $3-$子群为4个或1个. 若为4个，设$X = \{P_1, P_2, P_3, P_4\}$为$G$的Sylow $3-$子群的集合，我们知道有G到X上的可递作用，那可诱导出G到$\mathbf{S}_{1\times 1}$的同态σ, 于是$G/\mathrm{Ker}\sigma$同构于$\mathbf{S}_4$的一个子群. 若$n = 2^2 \times 3^2$,那么由$|G/\mathrm{Ker}\sigma| \leq |\mathbf{S}_4| = 24$, 知$\mathrm{Ker}\sigma \neq \{e\}$.又$G$在$X$上作用可递，知$\mathrm{Ker}\sigma \neq G$, 故$\mathrm{Ker}\sigma$是$G$的非平凡正规子群.因而$G$非单. 若$n = 2^3 \times 3$,如果$\mathrm{Ker}\sigma \neq \{e\}$,同样知$G$非单；如果$\mathrm{Ker}\sigma = \{e\}$,从而$G \cong \mathbf{S}_4$,由$\mathbf{A}_4 \lhd G$可知$G$也非单.
当$n = 2^3 \times 5$时，可知Sylow $5-$子群唯一，故G非单.
当$n = 2^3 \times 7$时，也判断G非单.
由上知，当$|G|$仅有2个不同的素因子时，G非单.
3) n至少有3个不同的素因子.由$n/2 \times 3 \times 5 \leq 1, n < 3 \times 5 \times 7$, 知$n = 2qr, 2, q, r$为不同的素数.那么$2||n$, 故$G$必有正规子群$H$使得$[G : H] = 2$,从而$G$非单.
综上知：当$|G| < 60$,且非交换，则G不是单群. 当G是非Abel有限单群，有$|G| \geq 60$. ■

7. 设G是60阶的单群，证明G与$\mathbf{A}_5$同构.

证明 设H是G的一个子群，$X = \{gHg^{-1} | g \in G\}$,我们知道$G$在$X$上有一个自然的可递作用.由$G$是单的，知该作用是有效的. 令$n = [G : N_G(H)] = |X|$,那么$G$同构于$\mathbf{S}_n$的一个子群，故$n \geq 5, [G : H] \geq 5$.若$n = 5$,则$G$同构于$\mathbf{S}_n$的一个子群，那么$G \cong \mathbf{A}_5$.我们考虑$G$的Sylow $2-$子群，它的个数n_2可能为3，5，15个，由上知，$n_2 \geq 5$:若$n_2 = 5$,则$G \cong \mathbf{A}_5$,若$n_2 = 15$,由5阶元的个数为$6 \times (5-1) = 24$个知：必有2个Sylow $2-$子群的交不为$\{e\}$,而为2阶群A.由于$C_G(A)$包含这两个Sylow $2-$子群，故$4|C_G(A), |C_G(A)| > 4$,又$|G : C_G(A)| \geq 5$,从而$|C_G(A)| = 12, [G : C_G(A)] = 5$.再由$G$是单的，知$N_G(C_G(A)) = C_G(A)$,这样$[G : N_G(C_G(A))] = 5$ 故$G \cong \mathbf{A}_5$.综上可知$G \cong \mathbf{A}_5$. ■

8. 设G =SL$(3, \mathbf{Z}_2)$,即$\mathbf{Z}_2$上行列式值为1的3阶方阵的集合.证明G是一个168阶的单群.

证明 由$\mathbf{Z}_2$中只有1这个可逆元，知SL$(3, \mathbf{Z}_2)$ =GL$(3, \mathbf{Z}_2)$. 归纳可证$|\mathrm{GL}(n, \mathbf{Z}_p)| = \prod_{i=1}^{n-1}(p^n - p^i)$,那么$|G| = (2^3-1)(2^3-2)(2^3-2^2) = 168 = 2^3 \times 3 \times 7$.
易得$\mathbf{Z}_2$上次数不大于3的不可约多项式为：$x, x-1, x^2+x+1, x^3+x+1, x^3+x^2+1$. 那么由$\mathbf{Z}_2$上n阶方阵在相似下的分类定理

知，$\mathrm{SL}(3,\mathbf{Z}_2)$中有以下6种标准形：
$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}\begin{pmatrix}0&0&1\\1&0&1\\0&1&0\end{pmatrix}\begin{pmatrix}0&0&1\\1&0&0\\0&1&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&0&1\\0&1&1\end{pmatrix}$
分别记为A_1,A_2,A_3,A_4,A_5,A_6,其最低多项式分别为：$(x-1),(x-1)^2,(x-1)^3,x^3+x+1,x^3+x^2+1,(x-1)(x^2+x+1)$. 那么$G$中有以$A_1,A_2,\cdots,A_6$为代表的6个共轭类. 由$A_i$的最低多项式可知$A_1,A_2,\cdots,A_6$的阶分别为：1，2，4，7，7，3. 由第235页习题8知$\langle\{P(1\times i,j)|1\leq i,j\leq 3,i\neq j\}\rangle=G$. 由共轭类的分类知任意2个2阶元共轭，任意2个3阶元共轭. 设$H\lhd G$,且$H\neq G$，那么H中无2阶元.由于偶阶群，必有2阶元，故$|H|\ |3\times 7$.经计算得$|C(A_2)|=8,|C(A_3)|=4,|C(A_6)|=3$. 那么2阶元为168/8=21个,4阶元为42个，3阶元为56个，从而7阶元为$168-21-42-56-1=48$个.由Sylow $p-$子群之间共轭知：若H有一3阶元，则至少有56个3阶元；若H有7阶元，则至少有48个. 但$|H|\leq 21$,故$|H|=1$.故G是单群. ■

9. 假设有限群G的中心仅有G的幺元e，即$C(G)=\{e\}$.试证:$C(\mathrm{Aut}\,G)=\{\mathrm{id}\}$.

   证明 同2.15题. ■

10. 设G是非Abel有限单群，$A=\mathrm{Aut}\,G$.证明A的自同构都是内自同构.即$\mathrm{Aut}\,A=\mathrm{Int}\,A$.

4.5 群的直积

1. 设p,q是素数，且$p<q$.又群A是p阶群，群B是q阶群，G是A过B的扩张.试证：

   (a) G一定是A过B的非本质扩张；

   (b) 若q模p不等于1，则此扩张为平凡扩张，G为pq阶循环群；

   (c) 如果$q\equiv 1(\mathrm{mod}\ p)$,那么存在$A$过$B$的非平凡扩张$G$.此时$G$为非Abel群.

   证明 1) 设$N\lhd G$,且$N\cong B$.任取G内一个Sylow $p-$子群P，由$P\cap N=\{e\}$,知$PN=G$.故G一定是A过B的非本质扩张.
   2) 若$q\not\equiv 1(\mathrm{mod}\ p)$,那么Sylow $p-$子群也唯一，设为P,自然$P\lhd G$,又$PN=G$. 故此扩张为平凡扩张，G为pq阶循环群.
   3) ■

2. 设A，B分别为m,n阶循环群，试问A过B的非平凡扩张有多少个？（一个群若是循环群过循环群的扩张，则称为**亚循环群**.）

3. 若群A的中心$C(A)=\{1\}$,且$\mathrm{Aut}\,A=\mathrm{Int}\,A$,则称$A$为**完全群**. 试证任何群$B$过完全群$A$的扩张一定是平凡扩张.

   证明 由$C(A)=\{1\}$,知$C_G(A)\cap A=\{e\}$,而$\forall g\in G,\mathrm{ad}g\in\mathrm{Aut}\,A$;又$\mathrm{Aut}\,A=\mathrm{Int}\,A$,故有$a\in A$,使得$\mathrm{ad}g=\mathrm{ad}a$,即$a^{-1}g\in C_G(A)$.那么$G=C_G(A)A$.又由$C_G(A)$中元互换，知$C_G(A)\lhd G$,那么该扩张为平凡扩张. ■

4. 设$N_1,N_2,\cdots,N_k$是群G的子群，则G是$N_1,N_2,\cdots,N_k$的直积的充要条件是：

   (a) $G=N_1N_2\cdots N_k$;

   (b) $N_i\lhd G,1\le i\le k$;

   (c) $(\prod\limits_{j\neq i}N_j)\cap N_i=\{1\},1\le i\le k$.

   证明 充分性：根据定义可知在1，2已成立的情况下只须证$\forall g\in G,g=n_1n_2\cdots g_k,n_i\in N_i$表法唯一.假设有$m_i\in N_i$,使$g=n_1n_2\cdots g_k=m_1m_2\cdots m_k.(*)$
   则${m_1}^{-1}n_1=m_2m_3\cdots m_k{n_k}^{-1}n_{k-1}^{-1}\cdots{n_2}^{-1}=(m2\cdots m_k)(n_2\cdots n_k)^{-1}$.
   $\because N_i\lhd G,1\le i\le k$,
   $\therefore N_2N_3\cdots N_k\lhd G$,则由$m_2\cdots m_k\in N_2N_3\cdots N_k$,
   $n_2\cdots n_k\in N_2N_3\cdots N_k$,就有$(n_2\cdots n_k)^{-1}\in N_2\cdots N_k$,
   $\therefore(m_2\cdots m_k)(n_2\cdots n_k)^{-1}\in N_2\cdots N_k$,
   又${m_1}^{-1}n_1\in N_1,\therefore{m_1}^{-1}n_1\in N_1\cap(\prod\limits_{j\neq1}N_j)=\{1\}$.
   从而$n_1=m_1$.在$(*)$式两端消去n_1,m_1,再用类似的方法，依次得$n_2=m_2,n_3=m_3,\cdots,n_k=m_k$
   $\therefore g$的表法唯一，从而充分性得证.
   必要性：$\because G$是$N_1,N_2,\cdots,N_k$的直积，
   $\therefore$1,2成立.且有$\forall g\in G,g=n_1n_2\cdots N_k$表法唯一.设$a\in N_1\cap(\prod\limits_{j\neq1}N_j)$.则有$n_i\in N_i,i=1,2,\cdots,k$使$a=n_1=n_2\cdots n_k$,即$a=n_1\underbrace{1\cdot1\cdot1\cdots1}_{k-1}=1\cdot n_2n_3\cdots n_k$,由表法唯一立得$n_1=n_2=\cdots=n_k=1,\therefore a=1$即$N_1\cap(\prod\limits_{j\neq1}N_j)=\{1\}$.完全类似地有$N_i\cap(\prod\limits_{j\neq i}N_j)=\{1\},1\le i\le k$.即3成立. ■

5. 设$G=N_1N_2\cdots N_k$.证明$(\prod\limits_{j\neq i}N_j)\subseteq C_G(N_i)$.

证明 由$N_i \cap N_j = \{e\}, N_i \lhd N_iN_j, N_j \lhd N_iN_j$,知$N_i$与$N_j$中元两两互换，从而$(\prod_{j\neq i} N_j) \subseteq C_G(N_i)$. ■

6. 设$G = A \otimes B$,又$N \lhd B$.试证：

   (a) N是G的正规子群；

   (b) G/N与$A \times (B/N)$同构.

   证明

   (a) $\forall g \in G, n \in N$,由$G = A \otimes B$知$\exists a \in A, b \in B$.使$g = ab$.
   $\therefore gng^{-1} = abnb^{-1}a^{-1}, \because N \lhd B, \therefore bnb^{-1} \in N \subseteq B$.
   又由$G = A \otimes B$知$a(bnb^{-1}) = (bnb^{-1})a$,
   $\therefore gng^{-1} = bnb^{-1}aa^{-1} = bnb^{-1}aa^{-1} = bnb^{-1} \in N$,
   $\therefore N \lhd G$

   (b) 令$f : A \times (B/N) \longrightarrow G/N, f((a, bN)) = abN$.
   首先，若$(a, b_1N) = (a, b_2N)$,则${b_1}^{-1}a^{-1}ab_2 \in N$,即$(ab_1)^{-1}(ab_2) \in N, \therefore ab_1N = ab_2N$,
   $\therefore f$是映射.
   其次，若$f((a_1, b_1N)) = f((a_2, b_2N))$,即$a_1b_1N = a_2b_2N$,则$(a_1b_1)^{-1}a_2b_2 \in N, \exists n_1 \in N$,使${b_1}^{-1}{a_1}^{-1}a_2b_2 = n_1$.
   $\because G = A \otimes B, \therefore {b_1}^{-1}({a_1}^{-1}a_2) = ({a_1}^{-1}a_2){b_1}^{-1}$, 就有$({a_1}^{-1}a_2)({b_1}^{-1}b_2) = 1n_1$.其中$1 \in A, n_1 \in N \subseteq B$.由$G$中元素分解的唯一性知必有${a_1}^{-1}a_2 = 1, {b_1}^{-1}b_2 = n_1$, 即$a_1 = a_2, {b_1}^{-1}b_2 \in N$
   $\therefore b_1N = b_2N$,即$(a_1, b_1N) = (a_2, b_2N), \therefore f$是单射.
   再次，$\forall gN \in G/N, \exists a \in A, b \in B$,使$g = ab$,故$gN = abN$有原像$(a, bN), \therefore f$是满射.
   最后，$f((a_1, b_1N)(a_2, b_2N)) = f((a_1a_2, b_1b_2N)) = a_1a_2b_1b_2N$
   由A与B中元素可交换知$a_1a_2b_1b_2N = a_1b_1a_2b_2N = a_1b_1N \cdot a_2b_2N$
   即$f((a_1, b_1N)(a_2, b_2N)) = f((a_1, b_1N))f((a_2, b_2N)), \therefore f$是同态.
   综上可知f是$A \times B/N$到G/N的群同构，故$G/N \backsimeq A \times B/N$.

   ■

7. 设A, B是群G的正规子群，且$G = AB$.证明$G/(A \cap B) = A/(A \cap B) \otimes B/(A \cap B)$.

   证明 由A, B是G的正规子群，知$A/(A \cap B), B/(A \cap B)$也是$G/(A \cap B)$的正规子群，又$(A/(A \cap B)) \cap (B/(A \cap B)) = (A \cap B)/(A \cap B) = \{\mathrm{id}\}, A/(A \cap B) \times B/(A \cap B) = G/(A \cap B)$,故$G/(A \cap B) = A/(A \cap B) \otimes B/(A \cap B)$. ■

8. 设A,B是群G的正规子群,且$A\cap B=\{1\}$.证明G与$(G/A)\times(G/B)$的一个子群同构.

证明 令$fG\longrightarrow G/A\times G/Bf(g)=(gA,gB)$,则显然$f$是映射.
若$(g_1A,g_1B)=(g_2A,g_2B)$,则$g_1A=g_2A,g_1B=g_2B,\therefore {g_1}^{-1}g_2\in A\cap B$,
$\therefore {g_1}^{-1}g_2=1,\therefore g_1=g_2$.
从而f是单射，又$f(g_1g_2)=(g_1g_2A,g_1g_2B)=(g_1A,g_1B)(g_2A,g_2B)=f(g_1)f(g_2)$.
$\therefore f$是单同态.故$f:G\longrightarrow f(G)$是同构.
$\therefore G\backsimeq f(G)$.
而$f(G)$是$G/A\times G/B$的子群，故命题成立. ■

9. 设A,B是群G的正规子群,且$G=AB;ab=ba,\forall a\in A,b\in B$.证明存在群$A\times B$到$G$的同态映射.

证明 作映射$\sigma:\sigma(a,b)=ab$即可. ■

10. 设Y是集合X上的一个子集，令G,A,B分别为$P(X),P(Y),P(X-Y)$对于对称差“$\triangle$”所成的群（参见1.2习题7）.证明G与$A\times B$同构.

证明 令$f:G\longrightarrow A\times B,f(M)=(M\cap Y,M-Y)$.显然$f$是映射.
若$f(M)=f(N)$,则$(M\cap Y,M-Y)=(N\cap Y,N-Y)$,则$M\cap Y=N\cap Y,M-Y=N-Y$.
从而$M=(M\cap Y)\cup(M-Y)=(N\cap Y)\cup(N-Y)=N$,
$\therefore f$是单射.
又$\forall A_1\in A,B_1\in B$,令$M=A_1\cup B_1$,可知$M\in G,f(M)=(M\cap Y,M-Y)=(A_1,B_1)$.
即$\forall(A_1,b_1)\in A\times B$,有原象$A_1\cap B_1$.故$f$是满射.
$\forall M,N\in G,f(M\triangle N)=((M\triangle N)\cap Y,(M\triangle N)-Y)=((M\cap Y)\triangle(N\cap Y),(M-Y)\triangle(N-y)=$
$(M\cap Y,M-Y)\triangle(N\cap Y,N-Y)=f(M)\triangle f(N)$.
故f是同态.
$\therefore f$是同构.
$\therefore G\backsimeq A\times B$. ■

11. 设G是有限群，$|G|={p_1}^{a_1}{p_2}^{a_2}\cdots{p_k}^{a_k},p_1,p_2,\cdots,p_k$为互不相等的素数.又每个Sylow p_i-子群$P_i\lhd G$.试证$G=P_1\otimes P_2\otimes\cdots\otimes P_k$.

证明 运用结论：若$G=(\bigotimes_{i=1}^{s}N_i)\otimes(\bigotimes_{i=1}^{t}M_i)$, 则$G=N_1\otimes\cdots\otimes N_s\otimes\cdots\otimes M_t$. ■

4.6 可解群与幂零群

1. 证明：$n \leq 4$时，$\mathbf{S}_n$是可解群；$n \geq 5$时，$\mathbf{S}_n$是非可解群.

   证明 由有限群有合成序列以及小于60阶的单群都是Abel群，知小于60阶的群都是可解群. 那么当$n \leq 4$时，$|\mathbf{S}_n| < 60$,故$\mathbf{S}_n$可解. 当$n \geq 5$时，由于$\mathbf{A}_n$不可解，于是$\mathbf{S}_n$不可解. ■

2. 证明$\mathrm{GL}(2, \mathbf{Z}_2)$,$\mathrm{GL}(2, \mathbf{Z}_3)$是可解群.

   证明 仍用上题中提到的命题：由于$|\mathrm{GL}(2, \mathbf{Z}_2)| = |(2^2-1)(2^2-2)| < 60, |\mathrm{GL}(2, \mathbf{Z}_3)| = (3^2-1)(3^2-3) < 60$, 故$\mathrm{GL}(2, \mathbf{Z}_2)$,$\mathrm{GL}(2, \mathbf{Z}_3)$是可解群. ■

3. 设群G的阶为pqr,其中p, q, r是三个不同的素数.试证G为可解群.

   证明 我们知道pq型群是可解的，那么G中若有Sylow $q-$子群或Sylow $r-$子群,则G可解；若G中不存在Sylow $q-$子群以及Sylow $p-$子群，那么Sylow $r-$子群的个数为pq个，Sylow $q-$子群至少r个，这样r阶元以及q阶元至少为$pq(r-1)+r(q-1) \geq pqr - pq + rp > pqr = |G|$,矛盾.故$pqr$型群可解. ■

4. (a) 设H, K均为群G的可解正规子群，试证HK也是群G的可解正规子群.

   (b) 设R是群G（不是可解群）的极大可解正规子群，H为G的任一可解正规子群.证明$H \subseteq R$,且G/R无非平凡的可解正规子群.

   证明

   (a) 首先，$H \lhd G, K \lhd G \Rightarrow HK \lhd G$.再由49页定理1.7.3知$HK/K \backsimeq H/H \cap K$.
   $\because$ H是可解群，$\therefore$商群$H/H \cap K$也是可解群.从而HK/K是可解群.
   又K是可解群，故HK是可解群，即HK是群G的可解正规子群.

   (b) 由R和H均为G的可解正规子群，用结论1知HK是G的可解正规子群，反设$H \nsubseteq R$,则$R \subsetneq HR$,此与R是G的极大正规子群矛盾，$\therefore H \subseteq R$.
   令$\pi : G \longrightarrow G/R$为自然同态，$\therefore \ker\pi = R$.由定理知$\pi$建立了$G$中包含$R$的正规子群与$G/R$的正规子群之间的一一对应.下证这种对应把可解正规子群也仍对应为可解正规子群，任一$K \supseteq R, K \lhd G$,且K可解，则K对应为$\pi|_K(K)$.而$\pi|_K$是K到$\pi|_K(K)$的同态.
   $\therefore$ $\pi|_K(K)$可解.反之，$\because$ π是满射，$\therefore$任一G/R的可解正规子群可写成为$\pi|_K(K)$.其中$K \supseteq R$,且$K \lhd G$.而$\pi|_K(K) = K/R$可

解.又R可解，故K可解.所以G中包含R的可解正规子群与G/K中的可解正规子群是一一对应的. 设K是G/K的非平凡可解正规子群，则$K \neq R$.设K_1是与之对应的G中包含R的可解正规子群，则必有$K_1 \supsetneqq R$,且$\because G$不是可解群，$\therefore K_1 \subsetneqq G$.此与$R$是”$G$的极大可解正规子群“矛盾.
$\therefore G/R$无非平凡的可解正规子群.

■

5. 设G是一个有限群.则下列条件等价：

   (a) G是可解群；

   (b) $\forall H \lhd G, \exists H_1 \lhd H$使$H/H_1$有Abel正规子群$K \neq \{1\}$;

   (c) $\forall H \lhd G, G/H$有Abel正规子群$K \neq \{1\}$.

   证明 1) $\Rightarrow$ 2) $\Rightarrow$ 3)是显然的.
   3) $\Rightarrow$ 1) :
   取G的极大可解正规子群H，那么G/H无非平凡的可解正规子群.那么由3）可知$G = H$,故G可解. ■

6. 设H是G的极大可解子群.证明$N_G(H) = H$.

   证明 若$N_G(H) \neq H$,取$g \in N_G(H)$,但$g \notin H$.由$H \lhd N_G(H)$,可知$\langle g\rangle H$为一群.而$\langle g\rangle H/H \cong \langle g\rangle/(\langle g\rangle \cap H)$,那么$\langle g\rangle H/H$可解，从而$\langle g\rangle H$可解，且$\langle g\rangle H \supset H$,与$H$的极大性矛盾.故$N_G(H) = H$. ■

7. 设n是一个偶数，试证每个n阶群都是幂零群的充要条件是$n = 2^k, k \in \mathbf{N}$.

   证明 若n中有不同于2的素因子p,那么存在非Abel群$H : |H| = 2p$.由H只有一个非平凡正规子群，易得H不是幂零群.设$n = 2pk$, 再取一个k阶群K，令$G = H \times K$,由H不是幂零，知G不是幂零，故若每个n阶群都是幂零的，则$n = 2^k$.而当$n = 2^k$时，自然G是幂零的. ■

8. 设G是有限幂零群.H为G的极大子群.证明$N_G(H) \neq H$.

   证明 由G是幂零的，可取$k \in \mathbf{N}$,使得$T_k \neq H$,且$H \supset T_{k+1}$.由于$[T_k, H] \subseteq [T_k, G] = T_{k+1}$,故$T_k \subset N_G(H), H \neq N_G(H)$.（这里$G$可以是一般的幂零群）. ■

9. 设G是有限幂零群.M为G的极大子群.证明$M \lhd G$.且G的每个Sylow子群正规.

   证明 $\because M$是G的极大子群，$\therefore M$是G的真子群，又G是有限幂零群，就有M是$N_G(M)$的真子群.若$N_G(M) \neq G$，则$M \subsetneqq N_G(M) \subsetneqq$

G,此与M是G的极大子群矛盾.
$\therefore N_G(M)=G$,从而$M \lhd G$.
对于G的任一Sylow子群P,由163页第12题的结论知$N_G(N_G(P)) = N_G(P).(*)$
若$N_G(P) \neq G$,则$N_G(P)$是G的真子群，又G是有限幂零群，$\therefore N_G(P)$是$N_G(N_G(P))$的真子群，与$(*)$式矛盾.
$\therefore N_G(P)=G$.从而$P \lhd G$,即G的每个Sylow子群正规. ■

10. 证明有限群G为幂零群当且仅当对$\forall H \lhd G, C(G/H) \neq \{1\}$.

证明 若G幂零，那么升中心列长是有限的，那么当$H \neq G$且$H \lhd G$时，$C(G/H) \neq \{1\}$.
若$\forall H \lhd G, H \neq G$,有$C(G/H) \neq \{1\}$. 再由$|G| < +\infty$,知$G$的升中心列长是有限的，故$G$是幂零的. ■

4.7 Jordan-Hölder定理

1. 给出加群$\mathbf{Z}$的两个正规序列

$$\mathbf{Z} \supset 20\mathbf{Z} \supset 60\mathbf{Z} \supset \{0\},$$

$$\mathbf{Z} \supset 49\mathbf{Z} \supset 245\mathbf{Z} \supset \{0\}$$

的同构加细.

证明 取$\mathbf{Z} \supset 20\mathbf{Z} \supset 60\mathbf{Z} \supset \{0\}$与$\mathbf{Z} \supset 49\mathbf{Z} \supset 245\mathbf{Z} \supset \{0\}$ 的加细分别为：$\mathbf{Z} \supset 4\mathbf{Z} \supset 20\mathbf{Z} \supset 60\mathbf{Z} \supset 2940\mathbf{Z} \supset \{0\}, \mathbf{Z} \supset 49\mathbf{Z} \supset 245\mathbf{Z} \supset 980\mathbf{Z} \supset 2940\mathbf{Z} \supset \{0\}$. 显然它们是同构的. ■

2. 求$\mathbf{Z}_{60}$的所有合成序列，并验证它们都是同构的.

证明 验证很容易. ■

3. 设群G有次正规（正规）序列

$$G = G_1 \supset G_2 \supset \cdots \supset G_r = \{1\}.$$

又G_i/G_{i+1}的阶为$S_i, i = 1, 2, \cdots, r-1$.试证明$G$的阶为$S_1S_2\cdots S_{r-1}$.

证明 易得. ■

4. 证明Abel群G有合成序列当且仅当G是有限阶的.

证明 只要注意到有限群有合成序列以及无限Abel群有非平凡真子群. ■

5. 证明可解群G有合成序列当且仅当G是有限群.

证明 由可解群G存在次正规序列$G = G_1 \supset G_2 \ldots G_r = 1$, 且$G_i/G_{i+1}$为Abel群，$1 \leq i \leq r-1$.在由上题以及同态定理可知可解群$G$有合成序列当且仅当$G$是有限群. ■

6. 设$G = G_1 \supset G_2 \supset \cdots \supset G_r = \{1\}$为群$G$的合成序列，1为幺元，$N$是$G$是正规单子群.证明

$$G_1 \supseteq G_2N \supseteq \cdots \supseteq G_{r-1}N \supseteq G_rN \supseteq G_r = \{1\}$$

中不同的群也是G的合成序列.

证明 作G_i/G_{i+1}到$G_iN/G_{i+1}N$的同态φ: $\varphi(gG_{i+1}) = gG_{i+1}N, \forall g \in G_i$.由$G_i/G_{i+1}$的单性，知$G_iN/G_{i+1}N = \{1\}$或是单的.故$G_1 \supseteq G_2N \supseteq \ldots G_{r-1}N \supseteq G_rN = \{1\}$.中不同的群也是$G$的合成序列. ■

7. 设φ是群G到群H上的同态.又

$$G = G_1 \supset G_2 \supset \cdots \supset G_r = \{1\}$$

是G的合成序列.证明

$$H = H_1 \supseteq \varphi(G_2) \supseteq \cdots \supseteq \varphi(G_r) = \{1\}$$

中不同的子群也是H的合成序列.

证明 由G到H上的同态φ可诱导出G_i/G_{i+1}到$\varphi(G_i)/\varphi(G_{i+1})$的同态$\overline{\varphi}$: $\overline{\varphi}(gG_{i+}) = \varphi(g)\varphi(G_{i+1}), \forall g \in G_i$. 这样，由$G_i/G_{i+1}$的单性，知$\varphi(G_i)/\varphi(G_{i+1})\{1\}$或是单群.故$H = H_1 \supseteq \varphi(G_2) \supseteq \ldots \supseteq \varphi(G_r) = \{1\}$中不同的群也是$H$的合成序列. ■

8. R-模M的任一子模序列

$$L_1 \subseteq L2 \subseteq \cdots \subseteq L_n \subseteq \cdots$$

有n使$L_{n+i} = L_n, i = 1, 2, \cdots$.则称$M$满足**升链条件**，或称$M$为Noether模.
若R-模M的任子模序列

$$L_1 \supseteq L_2 \supseteq \cdots \supseteq L_n \cdots$$

有n使$L_{n+i} = L_n, i = 1, 2, \cdots$.则称$M$满足**降链条件**，或称$M$为Artin模.
证明R-模M有合成序列当且仅当M既是Noether模又是Artin模.

证明 若$R-$模M有合成序列，则M有有限个合成因子，那么M必既是Noether模又是Artin模. 若$R-$模既是Noether模又是Artin模，令$M_1 = M$.由M具有升链条件，知M_1有子模M_2使$M_1 \supseteq M_2$，且M_1/M_2使单模，依次寻找，再由M有降链条件，知存在R使得：$M = M_1 \supseteq M_2 \supseteq \ldots \supseteq M_r = \{0\}$, 且$M_i/M_{i+1}, i = 1, 2, \ldots, r-1$为单模，故$M$有合成序列. ■

4.8 自由幺半群与自由群

1. 设S, T是群G的子集，且$gSg^{-1} \subseteq S, \forall g \in G$.试证：

   (a) $< S > \lhd G$;

   (b) $< \bigcup\limits_{g\in G} gTg^{-1} >$是$G$中包含$T$的最小正规子群.

   证明 1) 由定义可得.

   2) 由$g(\bigcup\limits_{g\in G}(gTg^{-1}))g^{-1} = \bigcup\limits_{g\in G}(gTg^{-1}), \forall g \in G,$

   知$\langle \bigcup\limits_{g\in G}(gTg^{-1})\rangle$是$G$的正规子群，显然它也是包含$T$最小的. ■

2. 设$X = \{x_1, x_2, x_3\}$,求由$\{x_1^2, x_2^2, x_3^2\}$生成的$F(X)$的正规子群K在$F(X)$中的指数.

   解 由$F(X)/K$中的子集$G_1 = \{\overline{x_1}^{k_1}\overline{x_2}^{k_2}\overline{x_3}^{k_3} | 0 \leq k_1, k_2, k_3 \leq 1\}$为子群，且$\overline{x_1}, \overline{x_2}, \overline{x_3} \in G_1$,故$F(X)/K = G_1$,那么$[F(X) : K] \leq 8$. 考虑$F(X)$到$\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$的同态$\varphi$：

   $$\varphi(x_1) = (1, 0, 0), \varphi(x_2) = (0, 1, 0), \varphi(x_3) = (0, 0, 1).$$

   易见$\ker\varphi \supseteq \{x_1{}^2, x_2{}^2, x_3{}^2\}$,故$\ker\varphi \supseteq K$,，故$[F(X) : K] \geq 8$，从而$[F(X) : K] = 8$. ■

3. 设$\mathbf{S}_4 = \langle(1\ 2), (1\ 3), (1\ 4)\rangle, X = \{x_1, x_2, x_3\}$.试证$\mathbf{S}_4$的生成关系为$x_i^2, (x_ix_j)^3, (x_ix_jx_k)^2$. 其中$i, j, k$互不相等.

4. 设$\mathbf{S}_4 = \langle(1\ 2), (1\ 3), (1\ 4)\rangle, X = \{x_1, x_2, x_3\}$, 试证$\mathbf{S}_4$的生成关系为$x_i^2, (x_ix_{i+1})^3, (x_ix_j)^2$., 其中$j > i+1$.

5. 试将习题3中的命题推广到$\mathbf{S}_n$,并证明.

6. 试将习题4中的命题推广到$\mathbf{S}_n$,并证明.

Chapter 5

模

5.1 自由模

1. 设R为交换么环，η是$R^{(n)}$的自同态.
   1) 试证η若为满自同态则必为$R^{(n)}$的自同构.
   2) 若η是$R^{(n)}$的一一同态，试问η是否为$R^{(n)}$的自同构?

   证明 1) 取$R^{(n)}$中一组基$\{u_1, u_2, \cdots, u_n\}$，设

   $$(\eta(u_1), \cdots, \eta(u_n)) = (u_1, u_2, \cdots, u_n)A, \quad \text{其中} A \in M_n(R).$$

   由于η是满同态，那么有$v_i \in R^{(n)}$, $1 \leqslant i \leqslant n$，使得$\eta(v_i) = u_i$.
   设$(v_1, v_2, \cdots, v_n) = (u_1, u_2, \cdots, u_n)B$, $B \in M_n(R)$,
   那么：$(u_1, u_2, \cdots, u_n) = (\eta(v_1), \cdots, \eta(u_n))B = (u_1, u_2, \cdots, u_n)AB$,
   即有$AB = I_n$，$\det A \cdot \det B = 1 = \det B \cdot \det A$，故$\det A$是$R$中可逆元，从而$\eta$是$R^{(n)}$的自同构.

   2) 不一定. η是否是$R^{(n)}$的自同构，取决于R. 如果R是体，则η必然是自同构. 如果$R = \mathbf{Z}$; $\eta : \eta(m) = 2m$, $m \in \mathbf{Z}^{(n)}$，则由η不是满射知：η不是自同构. ∎

2. 设R为交换么环. M，N是R-模. 以$\mathrm{Hom}(M, N)$表示从M到N的同态集合. 对η，$\xi \in \mathrm{Hom}(M, N)$，由$(\xi + \eta)(x) = \xi(x) + \eta(x)$定义$\xi + \eta$. 对$a \in R$，由$(a\eta)(x) = \eta(ax)$定义$a\eta$. 试证明：
   1) $\xi + \eta$，$a\eta \in \mathrm{Hom}(M, N)$;
   2) 对上述加法及R与$\mathrm{Hom}(M, N)$的乘法，$\mathrm{Hom}(M, N)$也是R-模;
   3) 若M与N分别是秩为m，n的自由R-模，则$\mathrm{Hom}(M, N)$是秩mn的R-模.

   证明 1) 对$\forall x, y \in R$-模M，$a \in R$, $(\xi + \eta)(ax) = \xi(ax) + \eta(ax) = a(\xi(x)+\eta(x)) = a((\xi+\eta)(x))$; $(\xi+\eta)(x+y) = \xi(x)+\xi(y)+\eta(x)+\eta(y) =$

$(\xi+\eta)(x)+(\xi+\eta)(y)$，故$\xi+\eta\in \mathrm{Hom}(M,N)$. $a\eta\in \mathrm{Hom}(M,N)$，同样容易验证.

2) 按照模的定义，容易验证$\mathrm{Hom}(M,N)$是R-模.

3) 设$R_{n\times m}$是R上$n\times m$的矩阵，对于矩阵的加法及R与矩阵的乘法构成一个模，且是一个秩为$n\times m$的自由模. 设$\{u_1,u_2,\cdots,u_n\}$, $\{v_1,v_2,\cdots,v_n\}$分别是M,N的一组基，对任意$\eta\in \mathrm{Hom}(M,N)$，令:

$$(\eta(u_1),\cdots,\eta(u_m))=(v_1,v_2,\cdots,v_n)M(\eta),\quad M(\eta)\in R_{n\times m}.$$

作映射：$\eta\to M(\eta)$，容易验证$\eta\to M(\eta)$是$\mathrm{Hom}(M,N)$到$R_{n\times m}$的模同构，故$\mathrm{Hom}(M,N)$ 是秩mn的R-模. ■

3. 设R为交换整环，M是秩n的自由R-模，$u_1,u_2,\cdots,u_n$为一组基，$f_1,f_2,\cdots,f_n\in M$，$K=<f_1,f_2,\cdots,f_n>$是M的子模，证明K是秩n的自由R-模当且仅当

$$\det(\mathrm{crd}f_1,\mathrm{crd}f_2,\cdots,\mathrm{crd}f_n)\neq 0$$

且此时对$\forall x=x+K\in M/K$ 有

$$\det(\mathrm{crd}f_1,\mathrm{crd}f_2,\cdots,\mathrm{crd}f_n)\cdot x=0.$$

证明 若K是秩n的自由R-模，设$\{v_1,v_2,\cdots,v_n\}$是K的一组基，作K的自同态λ：$\lambda(v_i)=f_i$, $1\leqslant i\leqslant n$，则λ是满的，故λ是自同构，自然$\{f_i,1\leqslant i\leqslant n\}$是$K$的一组基. 可见，$K$是秩$n$的自由$R$-模$\Longleftrightarrow$对任意$x\in R^{n\times 1}$, $x\neq 0$, $(f_1,f_2,\cdots,f_n)X\neq 0$.

记$A=(\mathrm{crd}f_1,\mathrm{crd}f_2,\cdots,\mathrm{crd}f_n)$. 可知：$K$是秩$n$的自由$R$-模$\Longleftrightarrow AX\neq 0$, $\forall X\neq 0, X\in R^{n\times 1}$，而$R$是交换整环，则有$R$的分式域$F$. 由线性代数理论知：$\det A\neq 0\Longleftrightarrow AX\neq 0$, $\forall X\neq 0, X\in F^{n\times 1}$. 那么有$\det A\neq 0\Rightarrow AX\neq 0$, $\forall X\neq 0, X\in R^{n\times 1}$. 而若$\forall X\neq 0, X\in R^{n\times 1}$，有$AX\neq 0$，任取$X\in F^{n\times 1}, X\neq 0$，由$F$是$R$的分式域，可令$X=(b_1c_1^{-1},\cdots,b_nc_n^{-1})'$，那么$X\cdot c_1\cdots c_n\neq 0$，而$X\cdot c_1\cdots c_n\in R^{n\times 1}$，故$AX=A(X\cdot c_1\cdots c_n)\cdot(c_1\cdots c_n)^{-1}\neq 0$，从而$\det A\neq 0$.

综上可知：当R是交换整环时，$A\in M_n(R)$, $\det A\neq 0\Longleftrightarrow\forall X\neq 0, X\in R^{n\times 1}, AX\neq 0$. 从而：$K$是秩$n$的自由$R$-模当且仅当$\det(\mathrm{crd}f_1,\mathrm{crd}f_2,\cdots,\mathrm{crd}f_n)\neq 0$，此时，任取$x=(u_1,u_2,\cdots,u_n)X$, $X\in R^{n\times 1}, \det A\cdot x=(u_1,u_2,\cdots,u_n)(A\cdot A^*)\cdot X=((u_1,u_2,\cdots,u_n)A)(A^*\cdot X)=(f_1,f_2,\cdots,f_n)(A^*\cdot X)$，这里$A^*$是方阵$A$的伴随矩阵，故$\det A\cdot x\in K$，从而对任意$x=x+K\in M/K$，有$\det(\mathrm{crd}f_1,\mathrm{crd}f_2,\cdots,\mathrm{crd}f_n)\cdot x=0$. ■

4. 设R是交换么环，M为秩n的自由R-模，$f \in \mathrm{End}_R M$，试证f为一一的模同态当且仅当f不是环$\mathrm{End}_R M$的左零因子.

证明 “$\Longrightarrow$” 反设$f,,g \in \mathrm{End}_R M$,且$f \neq 0, g \neq 0$.有$f \cdot g = 0$.即对$\forall x \in M, f(g(x)) = 0$. $\because$ f是模同态 $\therefore$ $f(0) = 0$. 而$g \neq 0$ $\therefore$ $\exists x_0 \in M$,使$g(x_0) \neq 0$. 且$f(g(x_0)) = 0$.则有$f(0) = f(g(x_0))$, $g(x_0) \neq 0$与f是一一的矛盾. $\therefore$ f不是环$\mathrm{End}_R M$的左零因子.

“$\Longleftarrow$” 反设f不是一一的，则f在给定基$\{u_i\}$下的矩阵A不可逆. 故$\exists P, Q$可逆，使$PAQ = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$, 令$K = \begin{pmatrix} 0 & * \end{pmatrix}$, 其中$0 \in R^{n\times r}, * \neq 0, K \in R^{n\times n}$, 则$PAQK = 0$,两边乘以$P^{-1}$,$\therefore$ $A(QK) = 0$.由于$f \neq 0, \therefore$ $A \neq 0$. 若$QK = 0$,两边乘以Q^{-1}得到$K = 0$与K的形式矛盾. 所以$QK \neq 0$,故存在$g \in \mathrm{End}_R M$,使QK为g 在$\{u_i\}$下的矩阵. 则有$f \neq 0, g \neq 0$,但$f \cdot g = 0$.与f不是环$\mathrm{End}_R M$的左零因子矛盾. 所以f是一一的模同态. 证毕. ■

5. 设p是素数. 令$\mathbf{Q}_p = \{m/pk | m \in \mathbf{Z}\}$. 则$\mathbf{Q}_p$是加群$\mathbf{Q}$的子群. 且$\mathbf{Z} \subseteq \mathbf{Q}_p$. 于是商群$\mathbf{Q}_p/\mathbf{Z}$是一个$\mathbf{Z}$-模. 作映射$f$为$f(x) = p\,x$. $\forall x \in \mathbf{Q}_p/\mathbf{Z}$. 试证明：
1) $f \in \mathrm{End}_Z(\mathbf{Q}_p/\mathbf{Z})$;
2) f不是一一映射;
3) f不是环$\mathrm{End}_Z(\mathbf{Q}_p/\mathbf{Z})$的左零因子;
4) $\mathbf{Q}_p/\mathbf{Z}$不是自由$\mathbf{Z}$-模.

证明 1) 由于对任意$a \in \mathbf{Z}, x, y \in \mathbf{Q}_p/\mathbf{Z}$，有: $f(x+y) = p(x+y) = f(x) + f(y), f(ax) = p(ax) = af(x)$，故$f \in \mathrm{End}_{\mathbf{Z}}(\mathbf{Q}_p/\mathbf{Z})$.

2) 由$f(\frac{1}{p} + \mathbf{Z}) = f(0 + \mathbf{Z})$，可得$f$不是一一映射.

3) 实际上，我们可以证明：$\mathrm{End}_{\mathbf{Z}}(\mathbf{Q}_p/\mathbf{Z})$是整环.

对任意非零元$\lambda \in \mathrm{End}_{\mathbf{Z}}(\mathbf{Q}_p/\mathbf{Z})$，令$d = \sup\{l | \frac{1}{p^l} + \mathbf{Z} \in \lambda(\mathbf{Q}_p/\mathbf{Z})\}$，如果$d = \infty$，显然$\lambda$是满射.若$d < +\infty$，由$\mathbf{Q}_p/\mathbf{Z} = \bigcup_{k=1}^{\infty} \langle \frac{1}{p^k} + \mathbf{Z} \rangle$，知：$\{l | \varphi(\frac{m_l}{p^l} + \mathbf{Z}) = \frac{1}{p^d} + \mathbf{Z}, p \nmid m_l\}$是无穷集，则可取$l_1, l_2 \in \mathbf{N}$，且$l_2 > l_1$，$\varphi(\frac{m_{l_2}}{p^{l_2}} + \mathbf{Z}) = \frac{1}{p^d} + \mathbf{Z}$, $\varphi(\frac{m_{l_1}}{p^{l_1}} + \mathbf{Z}) = \frac{1}{p^d} + \mathbf{Z}$，由$(m_{l_2}, p^{l_2}) = 1$，可取$n \in \mathbf{Z}$，使$n \cdot m_{l_2} \equiv 1 \pmod{p^{l_2}}$，从而：$\varphi(\frac{m_{l_1}}{p^{l_1}} + \mathbf{Z}) = \varphi(m_{l_1} \cdot p^{l_2 - l_1} \cdot n \cdot (\frac{m_{l_2}}{p^{l_2}} + \mathbf{Z})) = \frac{m_{l_1} \cdot n}{p^{d-(l_2-l_1)}} + \mathbf{Z} \neq \frac{1}{p^d} + \mathbf{Z}$，矛盾！故$d = \infty$，从而$\lambda$一定是满射.那么$\mathrm{End}_Z(\mathbf{Q}_p/\mathbf{Z})$上任两非零元$\lambda, \mu, \lambda \cdot \mu$仍是满

射，故$\lambda \cdot \mu \neq 0$，可见$\mathrm{End}_Z(\mathbf{Q}_p/\mathbf{Z})$中无零因子，且又是么环，故$\mathrm{End}_Z(\mathbf{Q}_p/\mathbf{Z})$是整环.

4) 反设$\mathbf{Q}_p/\mathbf{Z}$是自由$\mathbf{Z}$-模，且设$\{\frac{m_k}{p^{l_k}}+\mathbf{Z}|m_k\in\mathbf{Z},l_k\in\mathbf{N},1\leqslant k\leqslant n\}$是$\mathbf{Q}_p/\mathbf{Z}$的一组基. 可令$d=\max\{p^{l_k}|1\leqslant k\leqslant n\}$，但$\frac{1}{p^{d+1}}+\mathbf{Z}\notin\langle\frac{m_k}{p^{l_k}}+\mathbf{Z}|1\leqslant k\leqslant n\rangle$，矛盾！故$\mathbf{Q}_p/\mathbf{Z}$不是自由$\mathbf{Z}$-模. ■

6. 设M是R-模，$f\in\mathrm{End}_RM$.
1) 证明若f是满同态，则f不是环End_RM的右零因子.
2) 试举例说明1)的逆命题不成立.

证明 1) 反设$g,f\neq 0,g,f\in\mathrm{End}_RM$,有$g\cdot f=0$,即对任意$x\in M,(g\cdot f)(x)=g(f(x))=0$. 因为$f$是满同态，所以$f(x)$在对$x$任取时可以取遍$M$中任一元素. 故对任意$y\in M,g(y)=0$.从而$g=0$.与假设矛盾. 所以$f$不是环$\mathrm{End}_RM$的右零因子.

2) $\mathbf{Z}^{(1)}$是$\mathbf{Z}$-模, $\forall n\in\mathbf{Z}^{(1)},f(n)=2n$. 若$g\neq 0,g\cdot f=0$,则$\forall n\in\mathbf{Z}^{(1)},(g\cdot f)(n)=g(f(n))=g(2n)=2g(n)=0$.故$g(n)=i,\forall n\in\mathbf{Z}^{(1)}$.从而$g=0$.矛盾.所以$f$不是环$\mathrm{End}_RM$的右零因子，而$f$不是满同态. ■

7. 设M是R-模. $x_1,x_2,\cdots,x_n\in M$称作线性无关的，如果对R中任意n个不全为零的元素$a_1,a_2,\cdots,a_n$，有$\sum_{i=1}^{n}a_ix_i\neq 0$. 否则称为线性相关的.
设R是交换么环，I是R的理想，于是I是R-模. 试证$n>2$时，$x_1,x_2,\cdots,x_n\in I$一定是线性相关的.

证明 取$a_1=-x_2,a_2=x_1,a_i=0,i\geqslant 3$，那么$\sum_{i=1}^{n}a_ix_i=0$，故$x_1,x_2,\cdots,x_n$线性相关. ■

8. 设R为交换么环，R的每个理想是自由R-模. 试证R是主理想整环.

证明 设I是R的一个理想,由上题可知I是一维的自由R-模,则可令$I=\langle a\rangle$, $a\in R$,可见R是主理想整环. ■

5.2 模的直和

1. 设V是域F上的线性空间. 试证：
1) 非零向量$x_1,x_2,\cdots,x_n$线性无关当且仅当子空间Fx_i无关，$i=1,2,\cdots,n$.
2) $x_1,x_2,\cdots,x_n$是V的基当且仅当$V=Fx_1\oplus Fx_2\oplus\cdots\oplus Fx_n$.

证明 1) $Fx_i, 1 \leqslant i \leqslant n$无关$\Longleftrightarrow$ 对任意$1 \leqslant k \leqslant n, \sum\limits_{i\neq k} a_i x_i = a_k x_k$，$\Longleftrightarrow a_i = 0, 1 \leqslant i \leqslant n \Longleftrightarrow x_1, x_2, \cdots, x_n$线性无关.

2) $x_1, x_2, \cdots, x_n$是V的基$\Longleftrightarrow F = \langle x_1, x_2, \cdots, x_n\rangle = Fx_1 + \cdots + Fx_n$，且$x_1, x_2, \cdots, x_n$线性无关$\Longleftrightarrow F = Fx_1 \bigoplus \cdots \bigoplus Fx_n$. ■

2. 设R-模M的一组子模$M_i(1 \leqslant i \leqslant n)$，满足$M = \sum\limits_{i=1}^{n} M_i$，并满足$M_1 \cap M_2 = 0, (M_1 + M_2) \cap M_3 = 0, \cdots, (\sum\limits_{i=1}^{n-1} M_i) \cap M_n = 0$. 证明$M = \bigoplus\limits_{i=1}^{n} M_i$.

证明 归纳证明.当$n = 2$时，显然成立.假设$n = k$时，命题成立.当$n = k + 1$时，由归纳知：$\bigoplus\limits_{i=1}^{n-1} M_i$，又$(\bigoplus\limits_{i=1}^{n-1} M_i) \bigcap M_n = 0$，故$(\bigoplus\limits_{i=1}^{n-1} M_i) \bigoplus M_n = M$，从而$M = \bigoplus\limits_{i=1}^{n} M_i$. ■

3. 一个模若不是两个非零子模的直和，则称为**不可分解模**. 否则称为**可分解模**.

1) 设$n = p^e$，p是素数，$e > 0$. 证明$\mathbf{Z}$-模$\mathbf{Z}_n$是不可分解模.

2) 试问$\mathbf{Z}$与一般的$\mathbf{Z}$作为$\mathbf{Z}$-模是否可分解?

证明 1) （这里$\langle\bar{1}\rangle = \mathbf{Z}_n$，我们应当考虑这个么元）反设$\mathbf{Z}_n$可分解，且设$\mathbf{Z}_n = A \bigoplus B$，那么有$\bar{x} \in A, \bar{y} \in B$，使$\bar{x} + \bar{y} = \bar{1}$，显然$(x, p) = 1$，那么有$a \in \mathbf{Z}$，使$\overline{ax} = \bar{1}$，这样$A = \mathbf{Z}_n$，矛盾!

2) 反设$\mathbf{Z}$是可分解模，且设$\mathbf{Z}$分解成A, B两个非零子模的直和，设$x \in A, y \in B$，那么$xy \in A \bigcup B$，故$A \bigcup B \neq \Phi$，矛盾! 故$\mathbf{Z}$不可分解. 可证$\mathbf{Z}_n$可分解$\Longleftrightarrow n$中含有不同的素因子. 由1)知，若$\mathbf{Z}_n$可分解，则n中必含有不同的素因子，而当n中含有不同的素因子时，则有$a, b \in \mathbf{N}$，且$(a, b) = 1, n = a \cdot b$. 令$A = \{\overline{ta} | t \in \mathbf{Z}\} = \langle\bar{a}\rangle, B = \langle\bar{b}\rangle$，显然$A \bigcup B = 0$，由$(a, b) = 1$，知存在$u, v \in \mathbf{Z}$，使$ua + vb = 1$，自然$A \bigoplus B = \mathbf{Z}$. ■

4. 证明 若$M = M_1 \oplus M_2$，则$M_1 \backsimeq M/M_2, M_2 \backsimeq M/M_1$.

证明 作M_1到M/M_2的映射φ : $\varphi(x) = x + M_2$，易证$M_1 \backsimeq M/M_2$.同理可证$M_2 \backsimeq M/M_1$. ■

5. 证明 $\mathbf{Z}$-模$\mathbf{Q}_p/\mathbf{Z}$（参见5.1习题5）是不可分解的.

证明 反设$\mathbf{Q}_p/\mathbf{Z} = A \oplus B$,$A, B$非空.则可作$\mathbf{Q}_p/\mathbf{Z}$的自同态$\varphi_A, \varphi_B$: $\varphi_A(x + y) = x$, $x \in A, y \in B$; $\varphi_B(x + y) = y$, $x \in A, y \in B$. 虽然$\varphi_A \cdot \varphi_B = \varphi_B \cdot \varphi_A = 0$,但$\mathrm{End}_{\mathbf{Z}}(\mathbf{Q}_p/\mathbf{Z})$是整环!故$\mathbf{Q}_p/\mathbf{Z}$不可解. ■

6. 设R-模M有直和分解$M=\bigoplus\limits_{i=1}^{n}M_i$，又设$N_i$是$M_i$的子模，$1\leqslant i\leqslant n$．$N=\sum\limits_{i=1}^{n}N_i$．试证：

1) $N=\bigoplus\limits_{i=1}^{n}N_i$；

2) $M/N\backsimeq\bigoplus\limits_{i=1}^{n}M_i/N_i$.

证明 1) 设$x\in N_i\cap(N_1+N_2+\cdots+N_{i-1}+N_{i+1}+\cdots+N_n)$，则$x\in M_i\cap(M_1+M_2+\cdots+M_{i-1}+M_{i+1}+\cdots+M_n)$. 因为$M$有直和分解$M=\bigoplus\limits_{i=1}^{n}M_i$，所以$x=0$，故$N_i\cap(N_1+N_2+\cdots+N_{i-1}+N_{i+1}+\cdots+N_n)=0$，又已知$N=\sum\limits_{i=1}^{n}N_i$，所以$N=\bigoplus\limits_{i=1}^{n}N_i$

2) 将$\bigoplus\limits_{i=1}^{n}M_i/N_i$看作外直和$M_1/N_1\times M_2/N_2\times M_n/N_n$. 对任意的$m\in M$，$m$有唯一分解$m=m_1+m_2+\cdots+m_n$，$m_i\in M_i$，$i=1,2,\cdots,n$. 令$\varphi$:

$$M\longrightarrow M_1/N_1\times M_2/N_2\times M_n/N_n$$

$$m\longmapsto(m_1+M_1,m_2+M_2,\cdots,m_n+M_n)$$

由于m分解唯一，故φ是映射. 且对于$M_1/N_1\times M_2/N_2\times M_n/N_n$中的任一元素$(x_1+N_1,x_2+N_2,\cdots,x_n+N_n)$，$x_i\in M_i$，$i=1,2,\cdots,n$.存在$x=\sum\limits_{i=1}^{n}x_i\in M$是其原象，所以$\varphi$是满射.

对于任意的$m,n\in M,m,n$各有唯一分解$m=\sum\limits_{i=1}^{n}m_i,n=\sum\limits_{i=1}^{n}n_i$，$m_i,n_i\in M_i,i=1,2,\cdots,n$. $\varphi(m+n)=\varphi(\sum\limits_{i=1}^{n}(m_i+n_i))=((m_1+n_1)+N_1,(m_2+n_2)+N_2,\cdots,(m_n+n_n)+N_n)=(m_1+N_1,\cdots,m_n+N_n)+(n_1+N_1,\cdots,n_n+N_n)=\varphi(m)+\varphi(n)$.对于任意的$m\in M$,有上述分解$m=\sum\limits_{i=1}^{n}m_i,m_i\in M_i,i=1,2,\cdots,n$,对于任意的$a\in R,\varphi(am)=\varphi(\sum\limits_{i=1}^{n}am_i)=(am_1+N_1,\cdots,am_n+N_n)=a(m_1+N_1,\cdots,m_n+N_n)=a\varphi(m)$.所以$\varphi$是模同态，所以$\varphi$是满同态. 又$\varphi(m)=(m_1+N_1,\cdots,m_n+N_n)=(0+N_1,\cdots,0+N_n)\Leftrightarrow m_1\in N_1,\cdots,m_n\in N_n\Leftrightarrow m\in N$,所以$\ker\varphi=N$由同态基本定理，$M/N\backsimeq$

$M_1/N_1 \times M_2/N_2 \times \cdots \times M_n/N_n$.由于外直和$\backsimeq$内直和，所以$M/N \backsimeq \bigoplus_{i=1}^{n} M_i/N_i$. ■

7. 设R-模M有有限长的合成序列（参见4.7）. 又如$f \in \mathrm{End}_R M$，则存在$n \in \mathbf{N}$，使得

$$M = \mathrm{Im} f^n \oplus \ker f^n.$$

证明 由归纳易证: $\mathrm{Im} f^k \supseteq \mathrm{Im} f^{k+1}$, $\ker f^k \subseteq \ker f^{k+1}$. 再由$R$-模$M$有有限长的合成序列,知存在$N$,使得$\ker f^N = \ker f^{N+1}$, $\mathrm{Im} f^N = \mathrm{Im} f^{N+1}$,从而对一切$n_1, n_2 \geqslant N$,有: $\ker f^{n_1} = \ker f^{n_2}$, $\mathrm{Im} f^{n_1} = \mathrm{Im} f^{n_2}$.那么对$\forall x \in M$,有$y \in M$,使$f^{2N}(y) = f^N(x)$,即$f^N(x - f^N(y)) = 0$,从而$x - f^N(y) \in \ker f^N$,而$f^N(y) \in \mathrm{Im} f^N$,故$x \in \mathrm{Im} f^N + \ker f^N$.设$x \in \mathrm{Im} f^N \cap \ker f^N$,那么有$y \in M$,使$f^N(y) = x$,且$f^N(x) = 0$, 这样$f^{2N}(y) = 0$,再由$\ker f^N = \ker f^{2N}$知$x = 0$,故 $M = \mathrm{Im} f^N \oplus \ker f^N$. ■

注: 如果取f是满同态,则$\mathrm{Im} f^k = M$, $k \in \mathbf{N}$,而$\ker f^k \subseteq \ker f^{k+1}$, 故$\ker f = 0$, 可见$f$也是单同态,从而是个自同构.

8. 设M是R-模，$f \in \mathrm{End}_R M$，满足$M = \mathrm{Im} f \oplus \ker f$. 试证

$$\mathrm{Im} f = \mathrm{Im} f^2.$$

证明 对于任意的$y \in \mathrm{Im} f$,存在$x \in M$,使$f(x) = y$.因为$M = \mathrm{Im} \oplus \ker f$,故$x$唯一分解为$x = x_1 + x_2, x_1 \in \mathrm{Im} f, x_2 \in \ker f$.所以$y = f(x) = f(x_1 + x_2) = f(x_1) + f(x_2) = f(x_1)$.因为$x_1 \in \mathrm{Im} f$,所以存在$x_1' \in M$,使$f(x_1') = x_1$,所以$y = f^2(x_1') \in \mathrm{Im} f^2$,所以$\mathrm{Im} f \subseteq \mathrm{Im} f^2$.对于任意的$y \in \mathrm{Im} f^2$,存在$x \in M$,使$f^2(x) = y$.因为$f(x) \in M$,所以$y = f(f(x)) \in \mathrm{Im} f$,所以$\mathrm{Im} f^2 \subseteq \mathrm{Im} f$,所以$\mathrm{Im} f = \mathrm{Im} f^2$,证明完毕. ■

5.3 主理想整环上的有限生成模

1. 设N是$\mathbf{Z}^{(3)}$中子模，且N有生成元：$f_1 = (1, 0, -1), f_2 = (2, -3, 1), f_3 = (0, 3, 1), f_4 = (3, 1, 5)$. 求$N$的一组基.

解 我们先来研究一些一般主理想整环D上的问题.
设N是$D^{(n)}$的子模,且$N = \langle x_1, x_2, \cdots, x_k \rangle$, $f_i = (a_{i1}, \cdots, a_{in})$, $1 \leqslant i \leqslant k$. 求$N$的一组基.

令$d_1 = (a_{11}, a_{21}, \cdots, a_{k1})$,则有$u_1, u_2, \cdots, u_k \in D$使$d_1 = \sum_{i=1}^{k} a_{i1} u_i$,记$e_1 = \sum_{i=1}^{k} f_i u_i$,由$d_1 | a_{i1}$,可设$a_{i1} = b_{i1} d_1$,那么

$$N = \langle e_1, f_1 - d_1 \cdot b_{11}, \cdots, f_k - d_1 \cdot b_{k1} = \langle e_1 \rangle \oplus \langle f_1 - d_1 \cdot b_{i1}, \cdots, f_k - d_1 \cdot b_{k1} \rangle$$

重复上作法就能得到一组基.

就这题而言, $e_1=f_1, N=\langle e_1\rangle\oplus\langle(0,1,8),(0,3,1),(0,-3,3)\rangle, e_2=\langle(0,1,8)\rangle, N=\langle e_1\rangle\oplus\langle e_2\rangle\oplus\langle(0,0,-23),(0,0,27)\rangle, e_3=\langle(0,0,1)\rangle, N=\langle e_1\rangle\oplus\langle e_2\rangle\oplus\langle e_3\rangle$, 可见$\{e_1,e_2,e_3\}$为$N$的一组基. ■

注: N中一组基不一定能从一生成组中找出,比如这个例子就不行.因为这里$N=\mathbf{Z}^{(3)}$,倘若能从$\{f_1,f_2,f_3,f_4\}$中找出一组基, 设为$\{f_i,f_j,f_k\}$, 作N的自同态φ : $\varphi(1,0,0)=f_i,\varphi(0,1,0)=f_j,\varphi(0,0,1)=f_k$.则$M(\varphi)=({f_i}^T,{f_j}^T,{f_k}^{T)}$,但易验证$M(\varphi)$不是可逆的.矛盾! 故$\{f_i,f_j,f_k\}$不可能构成一组基!

2. 求$\mathbf{Q}[\lambda]^{(3)}$中由$f_1=(2\lambda-1,\lambda,\lambda^2+3), f_2=(\lambda,\lambda,\lambda^2), f_3=(\lambda+1,2\lambda,2\lambda^2-3)$生成的子模$N$的一组基.

解 令$e_1=f_3-f_2=(1,\lambda,\lambda^2-3)$,那么$\langle f_1,f_2,f_3\rangle=\langle e_1\rangle\oplus\langle(0,\lambda-\lambda^2,-\lambda^3+\lambda^2+3\lambda),(0,2\lambda-2\lambda^2,-2\lambda^3+2\lambda^2+6\lambda)\rangle=\langle e_1\rangle\oplus\langle(0,\lambda-\lambda^2,-\lambda^3+\lambda^2+3\lambda)\rangle$. 故$\{(1,\lambda,\lambda^2-3),(0,\lambda-\lambda^2,-\lambda^3+\lambda^2+3\lambda)\}$为$\langle f_1,f_2,f_3\rangle$的一组基. ■

3. 令$N=\{(x_1,x_2,x_3)|(x_1,x_2,x_3)\in\mathbf{Z}^{(3)}, x_1+2x_2+3x_3=0, x_1+4x_2+9x_3=0\}$. 求$N$的一组基.

解 易得$x_1=3x_3, x_2=-3x_3$,故易得N的一组基$\{(3,-3,1)\}$. ■

注: 可研究一下一般主理想整环上线性方程组的解空间.

4. 设R是整环, M,N是R-模, $f\in\mathrm{Hom}_R(M,N)$. 试证明:
1) 若N是无扭模, 则$\mathrm{Tor}M\subseteq\ker f$;
2) 若M是扭模, 则$\mathrm{Im}f\subseteq\mathrm{Tor}N$.

证明 1) 对于任意的$x\in\mathrm{Tor}M$,有$a\in R^*$,使$ax=0$,则$af(x)=f(ax)=0(\because f\in\mathrm{Hom}_R(M,N))$从而$f(x)$是$N$中的扭元, 因为$N$是无扭模, 所以$f(x)=0$,故$x\in\ker f$, 所以$\mathrm{Tor}M\subseteq\ker f$.

2) 对于任意的$y\in\mathrm{Im}f$,存在$x\in M$, 使$f(x)=y$, 因为M是扭模, 所以存在$a\in R^*$, 使得$ax=0$.所以$ay=af(x)=f(ax)=0$,所以y是N中扭元, 所以$y\in\mathrm{Tor}N$,$\mathrm{Im}f\subseteq\mathrm{Tor}N$. ■

5. 设V是域F上线性空间, $V\neq0$, 而且V只有一组基. 证明$\dim V=1$, 且$F\backsimeq\mathbf{Z}_2$.

证明 反设$\dim V\geqslant2$,则有一组基$\{\alpha_1,\alpha_2,\cdots,\alpha_n\}, n\geqslant2$.
下证$\{\alpha_1,\alpha_2+\alpha_2,\alpha_3,\cdots,\alpha_n\}$也为一组基.首先,若有$k_i\in F, i=1,2,\cdots,n$.
使$k_1\alpha_1+k_2(\alpha_1+\alpha_2)+\cdots+k_n\alpha_n=0$,由$\alpha_1,\alpha_2,\cdots,\alpha_n$是基, 所以$k_1=k_2=\cdots=k_n=0$,故$\alpha_1,\alpha_2+\alpha_2,\alpha_3,\cdots,\alpha_n$线性无关, 且任意$V$中元

素x可表为$x=\sum_{i=1}^{n}t_i\alpha_i=(t_1-t_2)\alpha 1+t_2(\alpha_1+\alpha_2)+\cdots+t_n\alpha_n$.即$x$能被$\{\alpha_1,\alpha_2+\alpha_2,\alpha_3,\cdots,\alpha_n\}$线性表出，故$\{\alpha_1,\alpha_2+\alpha_2,\alpha_3,\cdots,\alpha_n\}$也为一组基.因为$V$只有一组基，故必有$\alpha_1+\alpha_2=\alpha_2\Rightarrow\alpha_1=0\Rightarrow\alpha_1,\cdots,\alpha_n$必线性相关，矛盾.所以$\dim V=1$.设$0\neq\alpha\in V$是$V$的一组基，对于任意的$f\in F^*$,有$f\alpha\in V$且$f\alpha\neq 0$.因为$f\alpha$能被$\alpha$线性表出，又$\alpha=f^{-1}f\alpha$,即$\alpha$也能被$f\alpha$线性表出，故$\alpha$与$f\alpha$等价.所以$f\alpha$也是$V$的一组基，从而$f\alpha=\alpha$($V$只有一组基.). $\Rightarrow f=1$. 所以域F中的非零元只有1，故$F=\{0,1\}$.又$z_2=\{\bar{0},\bar{1}\}$ 显然有$F\backsimeq\mathbf{Z}_2$. ■

6. 设V是域$\mathbf{Z}_p$上的n维线性空间．又设$1\leqslant m\leqslant n$．证明V中包含m个元素的线性无关组的个数是

$$\frac{1}{m!}\prod_{l=0}^{m-1}(p^n-p^l).$$

证明 我们先将这m个元素排个序. 由于前k个元素能生成p^k个元素,故第$k+1$个元素有p_n-p_k种选法,从而共有$\prod_{i=0}^{m-1}(p_n-p_i)$种.那么$m$个元素的线性无关组的个数为$\frac{1}{m!}\prod_{i=0}^{m-1}(p^n-p^i)$.(由于$\mathbf{Z}_p$上$n$阶可逆方阵,当且仅当$n$个行向量是一线性无关组,可见$\mathbf{Z}_p$上$n$阶可逆方阵的个数为$\frac{1}{m!}\prod_{i=0}^{m-1}(p^n-p^i)$). ■

5.4 主理想整环上的有限生成扭模

1. 设R是交换么环，N是循环R-模，f是N到N的映射．证明$f\in\mathrm{End}_R N$当且仅当$\exists\lambda\in R$ 使得$f(x)=\lambda x,\forall x\in N$.

证明 “$\Longrightarrow$” 设$N=Rx_0$,因为f是$N\to N$的映射，所以存在$\lambda\in R,\lambda x_0\in N$,使$f(x_0)=\lambda x_0$.对于任意的$x\in N,\exists r\in R$,使$x=rx_0$.由$f\in\mathrm{End}_R N$,所以$f(x)=f(rx_0)=rf(x_0)=r\lambda x_0=\lambda(rx_0)=\lambda x$.即$\exists\lambda\in R$使得$f(x)=\lambda x,\forall x\in N$.

“$\Longleftarrow$” $\forall y\in N,(x+y)=\lambda x+\lambda y=f(x)+f(y)$.$\forall r\in R,\forall x\in N,f(rx)=\lambda rx=r(\lambda x)=rf(x)$.所以$f\in\mathrm{End}_R N$, 证毕. ■

2. 设D是一个p. i. d.，M是有限生成D-模，且$M=\bigoplus_{i=1}^{t}Dx_i$，$\mathrm{ann}\,x_1\subseteq\mathrm{ann}\,x_2\subseteq\cdots\subseteq\mathrm{ann}\,x_t$．设$1\leqslant i\leqslant j\leqslant t$，证明存在唯一的$f_{ij}\in\mathrm{Hom}(Dx_i,Dx_j)$使$f_{ij}(x_i)=x_j$.

证明 定义$f_{ij}:Dx_i\to Dx_j$. $\forall dx_i\in Dx_i, f_{ij}(dx_i)=dx_j$.取$d=1$,则$f_{ij}(x_i)=x_j$. 若$d_1x_i=d_2x_i$则$d_1-d_2\in\operatorname{ann}x_i\subseteq\operatorname{ann}x_j$.故$d_1x_j=d_2x_j$,即$f_{ij}(d_1x_i)=f_{ij}(d_2x_i)$. 故$f_{ij}$是映射.$\forall d_1x_i,d_2x_i\in Dx_i, f_{ij}(d_1x_i+d_2x_i)=(d_1+d_2)x_j=f_{ij}(d_1x_i)+f_{ij}(d_2x_i)$.$\forall d_1x_i\in Dx_i,\forall d_1\in D, f_{ij}(d_1dx_i)=d_1dx_j=d_1f_{ij}(dx_i)$，故$f_{ij}\in\operatorname{Hom}(Dx_i,Dx_j)$,满足$f_{ij}(x_i)=x_j$,存在性得证.

若另有$f'_{ij}\in\operatorname{Hom}(Dx_i,Dx_j), f'_{ij}(x_i)=x_j$,则$\forall dx_i\in Dx_i$，有$f'_{ij}(dx_i)=df'_{ij}(dx_i)=df'_{ij}(x_i)=dx_j=f_{ij}(dx_i)$. 所以$f'_{ij}=f_{ij}$，唯一性得证. ■

3. 设D是p. i. d.，M是有限生成的p-模．试确定$M(p)$的结构，并证明$M(p)$可看作域$D/\langle p\rangle$上有限维线性空间.

解 $M(p)$是M的子模,自然也是有限生成的模. 由分解定理可知:$M(p)=\bigoplus_{i=1}^{m}Dy_i$,且$\operatorname{ann}y_i=\langle p\rangle$.由$M(p)$模很自然的定义域$D/\langle p\rangle$与Abel群$M(p)$的乘积: $a\cdot x=ax$.易验证在该乘积下,$M(p)$是$D/\langle p\rangle$上的线性空间且$\{y_1,y_2,\cdots,y_m\}$是一组基.故$M(p)$可看作域$D/\langle p\rangle$上有限维线性空间. ■

4. 设D是p. i. d.，M是D上扭模．证明M为循环D-模当且仅当有互不相伴的素元素$p_1,p_2,\cdots,p_k$使得M的初等因子为${p_1}^{n_1},{p_2}^{n_2},\cdots,{p_k}^{n_k}$.

证明 由定理5.4.7, 5.4.8, 5.4.9易得. ■

5. 设M是$\mathbf{Q}[\lambda]$上的扭模，且$M=\bigoplus_{i=1}^{4}\mathbf{Q}[\lambda]x_i,\operatorname{ann}x_i$分别是由$(\lambda-1)^3,(\lambda^2+1)^2,(\lambda-1)(\lambda^2+1)^4,(\lambda+2)(\lambda^2+1)^2$生成的理想．确定$M$的初等因子组和不变因子组.

解 首先$\mathbf{Q}$是域，故$\mathbf{Q}[\lambda]$是Euclid环，从而$\mathbf{Q}[\lambda]$是p. i. d.，又x_1,x_2,x_3,x_4是M的生成元，故M是p. i. d.$\mathbf{Q}[\lambda]$上的有限生成模，所以可以利用相关的定理.

令$y_1=x_1$，则$\operatorname{ann}y_1=\operatorname{ann}x_1=\langle(\lambda-1)^3\rangle$. 令$y_2=x_2$，则$\operatorname{ann}y_2=\operatorname{ann}x_2=\langle(\lambda^2+1)^2\rangle$. 存在$y_3,y_4\in M$.使

$$x_3=y_3+y_4,\mathbf{Q}[\lambda]x_3=\mathbf{Q}[\lambda]y_3\bigoplus\mathbf{Q}[\lambda]y_4,\operatorname{ann}y_3=\langle\lambda-1\rangle,\operatorname{ann}y_4=\langle(\lambda^2+1)^4\rangle;$$

存在$y_5,y_6\in M$.使

$$x_4=y_5+y_6,\mathbf{Q}[\lambda]x_4=\mathbf{Q}[\lambda]y_5\bigoplus\mathbf{Q}[\lambda]y_6,\operatorname{ann}y_5=\langle\lambda+2\rangle,\operatorname{ann}y_6=\langle(\lambda^2+1)^2\rangle;$$

则$M=\bigoplus_{i=1}^{6}\mathbf{Q}[\lambda]y_i$，零化子$\operatorname{ann}y_i$如上述，则初等因子组如下：$\{(\lambda-1)^3,\lambda-1,(\lambda^2+1)^2,(\lambda^2+1)^4,(\lambda^2+1)^2,\lambda+2\}$，再结合成不变因子

组：$d_1 = 1 \times (\lambda^2+1)^2 \times 1 = (\lambda^2+1)^2, d_2 = (\lambda-1) \times (\lambda^2+1)^2 \times 1 = (\lambda-1)(\lambda^2+1)^2, d_3 = (\lambda-1)^3 \times (\lambda^2+1)^4 \times (\lambda+2) = (\lambda-1)^3(\lambda^2+1)^4(\lambda+2)$.

所以不变因子组为$\{d_1, d_2, d_3\}$，其中$d_1 = (\lambda^2+1)^2, d_2 = (\lambda-1)(\lambda^2+1)^2, d_3 = (\lambda-1)^3(\lambda^2+1)^4(\lambda+2)$. ■

6. 设D是p. i. d.，M是D上的扭模．试证明：
1) M是单模当且仅当$M = Dz, \operatorname{ann} z = \langle p \rangle, p$是素数；（参见1.6习题6）．
2) 若M有限生成，则M不可分解当且仅当$M = Dz, \operatorname{ann} z = \langle p^n \rangle, n \in \mathbf{N}$，$p$为素元素．

证明 1) 若M是单模,则$M = Dz$,令$\langle a \rangle = \operatorname{ann} z$,故$\operatorname{ann} M = \langle a \rangle$. 任取$a$的一个因子$b$,则$D(bz) = Dz$,设$a = bc$,那么$\operatorname{ann} M = \langle c \rangle$,从而$c \sim a$,故$a$不可约,自然也是个素元素.

若$M = Dz$, $\operatorname{ann}, z = \langle p \rangle$,$p$是个素元素.设$M_1$是$M$的非零子模,任取$M_1$的非零元$x = \lambda z$,则$(a, p) = 1$,故有$u\lambda + vp = 1$,那么$z = (u\lambda + vp)z = ux$,可见$M_1 = M$;从而$M$是单模.

2) 只需注意到定理5.4.7的分解是"最细"的. ■

7. 设D是p. i. d.，M是有限生成的D-模，$M \backsimeq D^{(n)}/K$．又N是M的子模．证明

$$\operatorname{rank} M = n - \operatorname{rank} K = \operatorname{rank} N + \operatorname{rank}(M/N).$$

证明 我们先来证明下面这个命题:

设M是p. i. d. D上的有限生成模,$\{x_1, x_2, \cdots, x_r\}$是$M$上的极大线性无关组,则$r = \operatorname{rank} M$.

若M是无扭模,则由定理5.3.2知:$\eta(M) \cong M$,而$\eta(M) \subseteq N$(符号同定理5.3.2).从而$r(N) \geqslant r(M)$, 而$r(M) \geqslant r(N)$,故$r(M) = r(N) = r$.对于一般的模M,可令$\overline{M} = M/\operatorname{Tor} M, N = \langle x_1, x_2, \cdots, x_r \rangle = Dx_1 \oplus \cdots \oplus Dx_r$.易证$\{\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_r\}$是$N + \operatorname{Tor} M/\operatorname{Tor} M$的一组基,且是$\overline{M}$的极大线性无关组.故$r = \operatorname{rank} \overline{M} = \operatorname{rank} M$. 证毕.

现在回到原来的题目.

设$\{x_1, x_2, \cdots, x_r\}$是$N$的极大线性无关组,自然也是$M$的线性无关组,自然可扩充为$M$的极大线性无关组,设为$\{x_1, \cdots, x_r, \cdots, x_s\}$.可证$\{\overline{x_{r+1}}, \cdots, \overline{x_s}\}$在$M/N$上线性无关,否则有不全为0的$a_{r+1}, \cdots, a_s$使$a_{r+1}\overline{x_{r+1}} + \cdots + a_s\overline{x_s} = 0$,即$a_{r+1}x_{r+1} + \cdots + a_s x_s \in N$, 则$\{x_1, \cdots, x_r, a_{r+1}x_{r+1} + \cdots + a_s x_s\}$在$N$内线性无

关,与极大性矛盾!故$\overline{x_{r+1}},\cdots,\overline{x_s}$在$M/N$上线性无关,反证易知也是极大的.故

$$\mathrm{rank}M = s = r + (s-r) = \mathrm{rank}N + \mathrm{rank}(M/N)$$

取$M = D^{(n)}, N = K$,则$n = \mathrm{rank}D^{(n)} = \mathrm{rank} + \mathrm{rank}(D^{(n)}/K)$,即$\mathrm{rank}M = n - \mathrm{rank}K$. ■

8. 设D是p. i. d.，M是D上扭模，又$\overline{M}$是M的同态像，且有不变因子$d_1, d_2, \cdots, d_s$满足$d_i | d_{i+1}, 1 \leqslant i \leqslant s-1$. 证明$\overline{M}$也是扭模，其不变因子$\overline{d_1}, \overline{d_2}, \cdots, \overline{d_t}$（其中$\overline{d_j} | \overline{d_{j+1}}, 1 \leqslant j \leqslant t-1$）满足$t \leqslant s$及$\overline{d_j} | d_{s-t+j}, 1 \leqslant j \leqslant t$.

5.5 主理想整环上有限生成模的应用

1. 设$n = {p_1}^{m_1}{p_2}^{m_2}\cdots{p_s}^{m_s}, p_1, p_2, \cdots, p_s$为互不相等的素数，$m_i \in \mathrm{N}$. 以$\gamma(n)$表示互不同构的$n$阶Abel群的同构类数. 证明:

   1) $\gamma(n) = \prod_{i=1}^{s} \gamma({p_i}^{m_i})$;

   2) $\gamma({p_i}^{m_i}) = \rho(m_i)$，其中$\rho(m_i)$表示$m_i$的不同分划的个数.

   证明 1) 设n阶Abel群为G,令P_i为Sylow p_i-群,则$G = \bigoplus_{i=1}^{m} P_i$, 故$\gamma(n) = \prod_{i=1}^{s} \gamma({p_i}^{m_i})$.

   2) 那么$P_i = \bigoplus \mathbf{Z}_{K_{ti}}$, $\sum K_{ti} = m_i$,可见$\gamma({p_i}^{m_i}) = \rho(m_i)$. ■

2. 1) 求$\rho(m), 1 \leqslant m \leqslant 7$.

   2) 对于$k \leqslant 12$，求最小正整数n_k使得$\gamma(n_k) = k$.

   3) 证明$\forall n \in \mathbf{N}, \gamma(n) \neq 13$.

   4) 求$\gamma(n), n = 360, 1000, 1001, 1000000$.

   解 1) $\rho(1) = 1, \rho(2) = 2, \rho(3) = 3, \rho(4) = 5, \rho(5) = 7, \rho(6) = 11, \rho(7) = 15$.

   2) 易得$\gamma(1) = 1, \gamma(2) = 2, \gamma(3) = 3, \gamma(4) = 5, \gamma(5) = 7, \gamma(6) = 11, \gamma(7) > 12$,故$n_1 = 1, n_2 = 2, n_3 = 3, n_5 = 4, n_7 = 5, n_{11} = 6$,其它无解.

   3) 设$n = {p_1}^{m_1}{p_2}^{m_2}\cdots{p_s}^{m_s}, p_1, p_2, \cdots, p_s$为互不相等的素数，$m_1, \cdots, m_s$为正整数. 反设$\gamma(n) = 13$,则$\gamma(n) = \prod_{i=1}^{s} \rho(m_i) = 13$.因为13是素数，所以必有某$m_i$，使$\rho(m_i) = 13$.而$\rho(m)$关于$m$严格单

增，由$\rho(6) < \rho(m_i) < \rho(7)$知$6 < m_i < 7$，与$m_i$是整数矛盾.所以$\forall n \in N, \gamma(n) \neq 13$.

4) $360 = 2^3 \times 3^2 \times 5$，所以$\gamma(360) = \rho(3) \times \rho(2) \times \rho(1) = 6$.

$1000 = 2^3 \times 5^3$，所以$\gamma(1000) = \rho(3) \times \rho(3) = 9$.

$1001 = 7 \times 11 \times 13$，所以$\gamma(1001) = \rho(1)^3 = 1$.

$1000000 = 2^6 \times 5^6$，所以$\gamma(1000000) = \rho(6) \times \rho(6) = 121$. ■

3. 证明有限Abel p-群由它的最高阶元素生成.

证明 似乎说的不对,除非它是循环群. ■

4. 设Abel群G的扭系数为p^2, p^8. 问G中包含多少个p^2阶子群?

解 p^2阶子群共两类:$\mathbf{Z}_p \bigoplus \mathbf{Z}_p$与$\mathbf{Z}_{p^2}$,其中$\mathbf{Z}_p \bigoplus \mathbf{Z}_p$为1个,$\mathbf{Z}_{p^2}$为$p^2 + p$个,共计$p^2 + p + 1$. ■

5. 举出两个包含$p^2 + p + 1$个p阶子群的Abel p-群的例子.

解 包含$p^2 + p + 1$个p阶子群,即相当于有$p^3 - 1$个p阶元.设$G = \mathbf{Z}_{p^{k_1}} \bigoplus \cdots \bigoplus \mathbf{Z}_{p^{k_l}}$,则$G$中$p$阶元为$p^l - 1$,故当且仅当$l = 3$时,$G$有$p^2 + p + 1$个$p$阶子群. ■

6. 设A是域F上n阶方阵. 证明A为幂零方阵当且仅当A相似于准对角方阵

$$\mathrm{diag}(N_1, N_2, \cdots, N_s),$$

其中N_i形如

$$\begin{pmatrix} 0 & 0 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ 1 & 0 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 1 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 0 & 0 & \cdot & \cdot & \cdot & 1 & 0 \end{pmatrix}.$$

证明 设V是域F上的n维线性空间，则存在线性变换$\mathcal{A}$，使$\mathcal{A}$在某组基下的矩阵为A. 把V看作由$\mathcal{A}$定义的$F[\lambda]$-模，据“第二标准分解式”，有$V = \bigoplus_{i=1}^{s} P[\lambda]x_i$,

$\mathrm{ann}\, x_i = \langle d_i(\lambda) \rangle, d_i(\lambda) | d_{i+1}(\lambda)$，且$d_i(\lambda)$为首一多项式，$i = 1, 2, \cdots, s$.则$\mathcal{A}$的第I型有理标准形如：$\mathrm{diag}(N_1, N_2, \cdots, N_s)$,其中$N_i$是$d_i(\lambda)$对应的伴侣方阵.

设$d_i(\lambda)=\lambda^{n_i}+a_{n_i-1}^{(i)}\lambda^{n_i-1}+\cdots+a_1^{(i)}\lambda+a_0^{(i)}$.则$N_i$形如

$$\begin{pmatrix} 0 & 0 & \cdot & \cdot & \cdot & 0 & -a_0^{(i)} \\ 1 & 0 & \cdot & \cdot & \cdot & 0 & -a_1^{(i)} \\ 0 & 1 & \cdot & \cdot & \cdot & 0 & -a_2^{(i)} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & 0 & -a_{n_i-2}^{(i)} \\ 0 & 0 & \cdot & \cdot & \cdot & 1 & -a_{n_i-1}^{(i)} \end{pmatrix}.$$

“$\Longleftarrow$” 若A相似于题设准对角方阵，则此方阵必定就是第I型有理标准形，所以$-a_0^{(i)}=\cdots=-a_{n_i-1}^{(i)}=0$. 所以$d_i(\lambda)=\lambda^{n_i},i=1,2,\cdots,s$所以$mathcal A$的极小多项式为$d_s(\lambda)$即$\lambda^{n_s}$.故$A$的极小多项式为$\lambda^{n_s}$，即$A^{n_s}=0$，所以$A$为幂零方阵.

“$\Longrightarrow$” 若A是幂零方阵，则存在n使$A^n=0$.而A的零化多项式必是$d_s(\lambda)$的倍式，所以$d_s(\lambda)|\lambda^n$, 所以$d_s(\lambda)=\lambda^{n_s},n_s\leqslant n$,即$-a_0^{(s)}=\cdots=-a_{n_s-1}^{(s)}=0$. 又$d_i|d_s(\lambda),i=1,2,\cdots,s-1$,所以$-a_0^{(i)}=\cdots=-a_{n_i-1}^{(i)}=0,i=1,2,\cdots,s-1$.所以$A$的第I型有理标准形为$\mathrm{diag}(N_1,N_2,\cdots,N_s)$,其中$N_i$形如

$$\begin{pmatrix} 0 & 0 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ 1 & 0 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 1 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 0 & 0 & \cdot & \cdot & \cdot & 1 & 0 \end{pmatrix}.$$

故A相似于准对角方阵

$$\mathrm{diag}(N_1,N_2,\cdots,N_s),$$

其中N_i形如

$$\begin{pmatrix} 0 & 1 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 0 & 1 & \cdot & \cdot & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & \cdot & \cdot & 0 & 1 \\ 0 & 0 & 0 & \cdot & \cdot & \cdot & 0 & 0 \end{pmatrix}.$$

证毕. ■

7. 域$\mathbf{C}$上n阶方阵相似于对角阵的充要条件是A的极小多项式无重根.

证明 “$\Longrightarrow$” 设A相似于$\mathrm{diag}\{\lambda_1,\lambda_2,\cdots,\lambda_n\}$，即为$A$的Jordan标准形，从而$\lambda_i\neq\lambda_j$，当$i\neq j$时．所以初等因子组为$\{\lambda-\lambda_1,\lambda-\lambda_2,\cdots,\lambda-\lambda_n\}$. 所以存在不变因子$d(\lambda)$为$A$的极小多项式．无重根．

“$\Longleftarrow$” 若A的极小多项式无重根，设A的不变因子组为$\{d_1,d_2,\cdots,d_s\}$

$\because d_i|d_s,\ i=1,2,\cdots,s-1.\quad\therefore d_i$无重根，$i=1,2,\cdots,s-1.$

从而A的所有初等因子都是一次多项式，所以A的Jordan标准形是对角矩阵，即A相似于对角阵．证毕. ■

8. 设A,B均为$\mathbf{C}$上n阶方阵．试证A,B相似的充要条件是

$$\mathrm{rank}(aI_n-A)^k=\mathrm{rank}(aI_n-B)^k,\quad\forall a\in\mathbf{C},k\in\mathbf{N}.$$

证明 若A,B相似,自然有$M_n(\mathbf{C})$上可逆矩阵P,使$PAP^{-1}=B$,自然$\mathrm{rank}(aI_n-B)^k=\mathrm{rank}P(aI_n-A)^kP^{-1}=\mathrm{rank}(aI_n-A)^k,\forall a\in\mathbf{C},k\in\mathbf{N}$.记$m$阶方阵

$$\begin{pmatrix}0&&&0\\1&\ddots&&\\&\ddots&\ddots&\\0&&1&0\end{pmatrix}$$

为C_m.假设A,B的特征向量值集为$\{\lambda_1,\lambda_2,\cdots,\lambda_n\}$，可令$A,B$都是Jordan标准形．设$A,B$中$\lambda_1$对应的Jordan块共$l$块，Jordan块分别为$k_1\leqslant k_2\leqslant\cdots\leqslant k_l$阶，$A,B$中$k_i$阶对应的Jordan块个数分别为：$n_i,\ m_i$.由$n-\sum\limits_{i=1}^{l}n_i=\mathrm{rank}(\lambda_1I_n-A)=\mathrm{rank}(\lambda_1I_n-B)=n-\sum\limits_{i=1}^{l}m_i$，可得$\sum\limits_{i=1}^{l}n_i=\sum\limits_{i=1}^{l}m_i$. $n-\sum\limits_{i=1}^{s}n_i\cdot k_i-k_{s+1}\sum\limits_{i=s+1}^{l}n_i=\mathrm{rank}(aI_n-A)^{k_{s+1}}=\mathrm{rank}(aI_n-B)^{k_{s+1}}=n-\sum\limits_{i=1}^{s}m_i\cdot k_i-k_{s+1}\sum\limits_{i=s+1}^{l}m_i$

故$(n_s-m_s)\cdot k_s+(\sum\limits_{i=s+1}^{l}n_i-\sum\limits_{i=s+1}^{l}m_i)k_{s+1}=0$，从而$(n_s-m_s)(k_s-k_{s+1})=0$，即$n_s=m_s,\ 1\leqslant s\leqslant l$.

同样可证在A,B中λ_i对应的Jordan块是相同一致的，故A,B相似. ■

9. 证明$\mathbf{Z}_p$（p为素数）上的p阶方阵

$$\begin{pmatrix}0&0&0&\cdots&0&1\\1&0&0&\cdots&0&0\\0&1&0&\cdots&0&0\\\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&0&\cdots&1&0\end{pmatrix}.$$

$$\begin{pmatrix} 1 & 0 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 1 & 1 & \cdot & \cdot & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & \cdot & \cdot & 1 & 1 \end{pmatrix}.$$

相似.

证明 可算出第一个矩阵对应的线性变换的不变因子为：$x^p-1=(x-1)^p$，第二个矩阵对应线性变换的初等因子为：$(x-1)^p$，自然不变因子为：$(x-1)^p$，那么这两个矩阵是相似的. ■

10. 证明$\mathbf{R}$上的n阶方阵一定相似于一个准对角方阵$\mathrm{diag}(B_1,B_2,\cdots,B_k)$，其中$B_i$为下面两种形式之一：

$$\begin{pmatrix} r & 0 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ 1 & r & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 1 & r & \cdot & \cdot & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & \cdot & \cdot & 1 & r \end{pmatrix}.$$

$$\begin{pmatrix} C & 0 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ I_2 & C & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & I_2 & C & \cdot & \cdot & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & \cdot & \cdot & I_2 & C \end{pmatrix}.$$

其中

$$C=\begin{pmatrix} 0 & -b \\ 1 & a \end{pmatrix} \text{且} a^2<4b, \quad I_2=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

证明 设R上的n阶方阵对应于n维线性空间V上的线性变换$\mathcal{A}$.我们知道$R[\lambda]$上不可约因子共2种，为：$\lambda-\lambda_i$，$\lambda^2-a\lambda+b\ (a^2<4b)$.由$\mathcal{A}$定义的$R[\lambda]$-模$V$可按初等因子可分解成循环子模的直和：$V=\bigoplus_{i=1}^{t} R[\lambda]y_i$，满足$\mathrm{ann}\, y_i=\langle(\lambda-\lambda_i)^{r_i}\rangle$或$\langle(\lambda^2-a\lambda+b)^{r_i}\rangle\ (a^2<4b)$, $1\leqslant i\leqslant t$.于是$V_i=R[\lambda]y_i$是$\mathcal{A}$的不变子空间. 若$\mathrm{ann}\, y_i=\langle(\lambda-\lambda_i)^{r_i}\rangle$，则

$$y_i,\ (\mathcal{A}-\lambda_i\mathrm{id})y_i,\ \cdots,\ (\mathcal{A}-\lambda_i\mathrm{id})^{r_i-1}\cdot y_i$$

是V_i的一组基，易得$\mathcal{A}|_{V_i}$在上述基下的矩阵为第一种形式.
若$\mathrm{ann}\, y_i=\langle(\lambda^2-a\lambda+b)^{r_i}\rangle$，记$\mathcal{B}=\mathcal{A}^2-a\mathcal{A}+b\mathrm{id}$，那么

$$y_i,\mathcal{A}y_i,\mathcal{B}y_i,\mathcal{A}\mathcal{B}y_i,\mathcal{B}^2y_i,\mathcal{A}\mathcal{B}^2y_i,\cdots,\mathcal{B}^{r_i-1}y_i,\mathcal{A}\mathcal{B}^{r_i-1}y_i$$

是V_i的一组基，易得$\mathcal{A}|_{V_i}$在上述基下的矩阵为第二种形式. ■

5.6 主理想整环上的矩阵

1. 求$\mathbf{Z}$上下列矩阵的标准形：

1) $\begin{pmatrix} 6 & 2 & 3 & 0 \\ 2 & 3 & -4 & 1 \\ -3 & 3 & 1 & 2 \\ -1 & 2 & -3 & 5 \end{pmatrix}$；　　2) $\begin{pmatrix} 1 & 2 & 3 & -2 \\ 2 & -2 & 1 & 3 \\ 3 & 0 & 4 & 1 \end{pmatrix}$.

解　1)　方法同2)，略

2)　初等变换法：$\begin{pmatrix} 1 & 2 & 3 & -2 \\ 2 & -2 & 1 & 3 \\ 3 & 0 & 4 & 1 \end{pmatrix} \xrightarrow{2\times 1+1}$

$\begin{pmatrix} 3 & 0 & 4 & 1 \\ 2 & -2 & 1 & 3 \\ 3 & 0 & 4 & 1 \end{pmatrix} \xrightarrow{1\times(-1)+3} \begin{pmatrix} 3 & 0 & 4 & 1 \\ 2 & -2 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{2\times 1+1}$

$\begin{pmatrix} 3 & 0 & 4 & 1 \\ 0 & -2 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{2\times 1+4} \begin{pmatrix} 3 & 0 & 4 & 1 \\ 0 & -2 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{4\times(-1)+3}$

$\begin{pmatrix} 3 & 0 & 3 & 1 \\ 0 & -2 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{1\times(-1)+3} \begin{pmatrix} 3 & 0 & 0 & 1 \\ 0 & -2 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{4\times(-3)+1}$

$\begin{pmatrix} 0 & 0 & 0 & 1 \\ -3 & -2 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{1\times(-1)+2} \begin{pmatrix} 0 & 0 & 0 & 1 \\ -3 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{2\times 3+1}$

$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{2\times(-1)+4} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow[[1,4]]{} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

即为标准形. ■

2. 求$\mathbf{Q}[\lambda]$上4阶方阵

$$A = \begin{pmatrix} \lambda-17 & 8 & 12 & -14 \\ -46 & \lambda+22 & 35 & -41 \\ 2 & -1 & \lambda-4 & 4 \\ -4 & 2 & 2 & \lambda-3 \end{pmatrix}$$

的标准形，并求可逆矩阵P, Q，使PAQ为标准形.

解　$A = \begin{pmatrix} \lambda-17 & 8 & 12 & -14 \\ -46 & \lambda+22 & 35 & -41 \\ 2 & -1 & \lambda-4 & 4 \\ -4 & 2 & 2 & \lambda-3 \end{pmatrix} \xrightarrow[[2\times 1+1]]{}$

$$\begin{pmatrix} \lambda-9 & 8 & 12 & -14 \\ \lambda-24 & \lambda+22 & 35 & -41 \\ 1 & -1 & \lambda-4 & 4 \\ -2 & 2 & 2 & \lambda-3 \end{pmatrix} \xrightarrow[[1\times1+2][1\times(4-\lambda)+3][1\times(-4)+4]]{}$$

$$\begin{pmatrix} \lambda-9 & \lambda-1 & -\lambda^2+13\lambda-24 & -4\lambda+22 \\ \lambda-24 & 2\lambda-2 & -\lambda^2+28\lambda-61 & -4\lambda+55 \\ 1 & 0 & 0 & 0 \\ -2 & 0 & 2\lambda-6 & \lambda+5 \end{pmatrix} \xrightarrow{[1,3]}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ \lambda-24 & 2\lambda-2 & -\lambda^2+28\lambda-61 & -4\lambda+55 \\ \lambda-9 & \lambda-1 & -\lambda^2+13\lambda-24 & -4\lambda+22 \\ -2 & 0 & 2\lambda-6 & \lambda+5 \end{pmatrix} \xrightarrow[[1\times(24-\lambda)+2][1\times(9-\lambda)+3][1\times2+4]]{}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2\lambda-2 & -\lambda^2+28\lambda-61 & -4\lambda+55 \\ 0 & \lambda-1 & -\lambda^2+13\lambda-24 & -4\lambda+22 \\ 0 & 0 & 2\lambda-6 & \lambda+5 \end{pmatrix} \xrightarrow{[3\times(-1)+2]}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \lambda-1 & 15\lambda-37 & 33 \\ 0 & \lambda-1 & -\lambda^2+13\lambda-24 & -4\lambda+22 \\ 0 & 0 & 2\lambda-6 & \lambda+5 \end{pmatrix} \xrightarrow[[2\times(-15)+3]]{}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \lambda-1 & -22 & 33 \\ 0 & \lambda-1 & -\lambda^2-2\lambda-9 & -4\lambda+22 \\ 0 & 0 & 2\lambda-6 & \lambda+5 \end{pmatrix} \xrightarrow[[4\times1+3][3\times(-3)+4]]{}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \lambda-1 & 11 & 0 \\ 0 & \lambda-1 & -\lambda^2-6\lambda+13 & 3\lambda^2+14\lambda-17 \\ 0 & 0 & 3\lambda-1 & -8\lambda+8 \end{pmatrix} \xrightarrow{[3\times\frac{1}{11}]}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \lambda-1 & 1 & 0 \\ 0 & \lambda-1 & \frac{1}{11}(-\lambda^2-6\lambda+13) & 3\lambda^2+14\lambda-17 \\ 0 & 0 & \frac{1}{11}(3\lambda-1) & -8\lambda+8 \end{pmatrix} \xrightarrow[[3\times(1-\lambda)+2][2,3]]{}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & \frac{1}{11}(-\lambda^2-6\lambda+13) & \frac{1}{11}(\lambda-1)(\lambda^2+6\lambda-2) & 3\lambda^2+14\lambda-17 \\ 0 & \frac{1}{11}(3\lambda-1) & \frac{1}{11}(3\lambda-1)(1-\lambda) & -8\lambda+8 \end{pmatrix}$$

$$\xrightarrow[[2\times\frac{1}{11}(-\lambda^2-6\lambda+13)+3][2\times\frac{1}{11}(3\lambda-1)+4]]{}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{11}(\lambda-1)(\lambda^2+6\lambda-2) & 3\lambda^2+14\lambda-17 \\ 0 & 0 & \frac{1}{11}(3\lambda-1)(1-\lambda) & -8\lambda+8 \end{pmatrix} \xrightarrow[[3\times 11]]{}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (\lambda-1)(\lambda^2+6\lambda-2) & 3\lambda^2+14\lambda-17 \\ 0 & 0 & (3\lambda-1)(1-\lambda) & -8\lambda+8 \end{pmatrix} \xrightarrow[[4\times\frac{1}{8}(1-3\lambda)+3][3\times 8]]{}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -(\lambda-1)^2(\lambda+1) & 3\lambda^2+14\lambda-17 \\ 0 & 0 & 0 & -8\lambda+8 \end{pmatrix} \xrightarrow{[4\times\frac{3}{8}\lambda+3]}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -(\lambda-1)^2(\lambda+1) & 17\lambda-17 \\ 0 & 0 & 0 & -8\lambda+8 \end{pmatrix} \xrightarrow{[4\times\frac{17}{8}\lambda+3]}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -(\lambda-1)^2(\lambda+1) & 0 \\ 0 & 0 & 0 & -8\lambda+8 \end{pmatrix} \xrightarrow[[3\times(-1)][4\times(-\frac{1}{8})]]{}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (\lambda-1)^2(\lambda+1) & 0 \\ 0 & 0 & 0 & \lambda-1 \end{pmatrix} \xrightarrow[[3\times(-1)][4\times(-\frac{1}{8})]]{}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (\lambda-1)^2(\lambda+1) & 0 \\ 0 & 0 & 0 & \lambda-1 \end{pmatrix} \xrightarrow[[3,4]]{[3,4]}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \lambda-1 & 0 \\ 0 & 0 & 0 & (\lambda-1)^2(\lambda+1) \end{pmatrix}.$$ 即为标准形.

其中 $P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \frac{17}{8} \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \frac{3}{8}\lambda \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & \frac{1}{11}(1-3\lambda) & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & \frac{1}{11}(\lambda^2+6\lambda-13) & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\cdot$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 9-\lambda & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 24-\lambda & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 0 & 1 & 0 \\ -1 & 1 & 15 & 0 \\ \frac{1}{11}(3\lambda-1) & \frac{1}{11}(1-3\lambda) & \frac{1}{11}(37-45\lambda) & 1 \\ \frac{1}{88}(\lambda^2+175) & \frac{-1}{88}(\lambda^2+87) & \frac{-1}{88}(15\lambda^2+22\lambda+139) & \frac{1}{8}(3\lambda+17) \end{pmatrix}.$$

$$Q = \cdots = \begin{pmatrix} 1 & \frac{-1}{11}(\lambda+15) & -\frac{1}{8}(3\lambda+41) & \lambda^2+8\lambda-9 \\ 1 & \frac{-1}{11}(\lambda+30) & -\frac{1}{8}(3\lambda+86) & \lambda^2+23\lambda-22 \\ 0 & \frac{1}{11} & \frac{3}{8} & -\lambda-5 \\ 0 & \frac{1}{11} & \frac{1}{4} & 2\lambda-6 \end{pmatrix}.$$

■

3. 令$\mathbf{C}_3[\lambda] = \{f(\lambda)|f(\lambda) \in \mathbf{C}[\lambda], \deg f(\lambda) \leqslant 3\}$. 又$D$是微分映射，即$D(f(\lambda)) = f'(\lambda)$. 确定$D$的Jordan标准形.

解 $\{1, \lambda, \lambda^2, \lambda^3\}$是$\mathbf{C}_3[\lambda]$的一组基，$D$在这组基下的矩阵$A$为：

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

通过求$\lambda I - A$的不变量，可得A的Jordan标准形.这里A很简单，直接构造就行了：由$A \sim A'$，设D在基$\{u_1, u_2, u_3, u_4\}$下的矩阵为A'，那么在基$\{u_1, u_2, 2u_3, 6u_4\}$下的矩阵为：

$$\begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ & 1 & 0 & \\ & & 1 & 0 \end{pmatrix}$$

故D的Jordan标准形是一个4阶Jordan块. ■

4. 用行列式因子确定矩阵

$$\begin{pmatrix} \lambda+1 & 2 & -6 \\ 1 & \lambda & -3 \\ 1 & 1 & \lambda-4 \end{pmatrix}$$

的不变因子.

解 $D_3(A)=\det A=(\lambda-1)^3, D_2(A)=\lambda-1, D_1(A)=1.$ 故不变因子$d_1=D_1(A)=1.\ d_2=D_2/D_1=\lambda-1.\ d_3=D_3/D_2=(\lambda-1)^2.$ 所以不变因子组为$\{1,\ \lambda-1,\ (\lambda-1)^2\}.$ ■

5. A为$\mathbf{R}$上的7阶方阵，极小多项式为$(\lambda^2+2)(\lambda+3)^3$，求$A$所有可能的有理标准形.

解 极小多项式即为最后一个不变因子，$d_s(\lambda)=(\lambda^2+2)(\lambda+3)^3$对应一个5阶相伴方阵.

(1) $d_1(\lambda)=\lambda^2+2,\ d_2(\lambda)=(\lambda^2)(\lambda+3)^3$，相应标准形为：

$$\begin{pmatrix} 0 & -2 & & & & \\ 1 & 0 & & & & \\ & & 0 & & & -54 \\ & & 1 & 0 & & -54 \\ & & & 1 & 0 & -45 \\ & & & & 1 & -9 \end{pmatrix}$$

(2) $d_1(\lambda)=(\lambda+3)^3,\ d_2(\lambda)=(\lambda^2+2)(\lambda+3)^3$，相应标准形为：

$$\begin{pmatrix} 0 & -9 & & & & \\ 1 & -6 & & & & \\ & & 0 & & & -54 \\ & & 1 & 0 & & -54 \\ & & & 1 & 0 & -45 \\ & & & & 1 & -9 \end{pmatrix}$$

(3) $d_1(\lambda)=\lambda+3,\ d_2(\lambda)=\lambda+3,\ d_3(\lambda)=(\lambda^2+2)(\lambda+3)^3$，相应标准形为：

$$\begin{pmatrix} -3 & & & & & \\ & -3 & & & & \\ & & 0 & & & -54 \\ & & 1 & 0 & & -54 \\ & & & 1 & 0 & -45 \\ & & & & 1 & -9 \end{pmatrix}$$

■

6. 用χ_A, Δ_A分别表示矩阵A的特征多项式与极小多项式，在下列条件下分别求A的所有可能的Jordan标准形：
1) $\chi_A=(\lambda-7)^5$, $\Delta_A=(\lambda-7)^2$;
2) $(\lambda-3)^4(\lambda-5)^4$, $\Delta_A=(\lambda-3)^2(\lambda-5)^2$.

解 设A的不变因子组为$\{d_1(\lambda),d_2(\lambda),\cdots,d_s(\lambda)\}$，则$\chi_A=\prod_{i=1}^{s}d_i(\lambda)$, $\Delta_A=d_s(\lambda)=(\lambda-7)^2$.从而$\prod_{i=1}^{s-1}d_i(\lambda)=(\lambda-7)^3$, $d_s(\lambda)=(\lambda-7)^2$. 且$d_i(\lambda)|d_{i+1}$, $i=1,2,\cdots,s-1$.
1) $d_1(\lambda)=\lambda-7$, $d_2(\lambda)=(\lambda-7)^2$, $d_3(\lambda)=(\lambda-7)^2$，则初等因子组为$\{\lambda-7,\ (\lambda-7)^2,\ (\lambda-7)^3\}$，相应的Jordan标准形为：

$$\begin{pmatrix} 7 & & & & \\ & 7 & & & \\ & 1 & 7 & & \\ & & & 7 & \\ & & & 1 & 7 \end{pmatrix}$$

2) $d_1(\lambda)=\lambda-7$, $d_2(\lambda)=\lambda-7$, $d_3(\lambda)=\lambda-7$, $d_4(\lambda)=(\lambda-7)^2$，则初等因子组为$\{\lambda-7,\ \lambda-7,\ \lambda-7,\ (\lambda-7)^2\}$，相应的Jordan标准形为：

$$\begin{pmatrix} 7 & & & & \\ & 7 & & & \\ & & 7 & & \\ & & & 7 & \\ & & & 1 & 7 \end{pmatrix}$$

■

7. $\alpha,\beta,\gamma\in\mathbf{R}$. 证明当且仅当$\alpha=0$时下面矩阵能对角化：

$$A=\begin{pmatrix} 2 & 0 & 0 \\ \alpha & 2 & 0 \\ \beta & \gamma & -1 \end{pmatrix}.$$

证明 矩阵A能对角化$\Longleftrightarrow$ A的最低多项式可分解为$(\lambda-\lambda_i)$的乘积，且无重根$\Longleftrightarrow$ A的不变因子是$(\lambda-\lambda_i)$的乘积形式，且无重根.
易得$D_1(\lambda I_3-A)=1$, $D_3(\lambda I_3-A)=(\lambda-2)^2(\lambda+1)$，那么若$\alpha=0$，则$(\lambda-2)|D_2(\lambda I_3-A)$，故$d_i$无重根，$d_i$当然也是一阶因式的乘积，故$A$能对角化.
若A能对角化，那么由$d_3=D_3/D_2$无重根知$(\lambda-2)|D_2$.而$\begin{pmatrix} -\alpha & 0 \\ -\beta & \lambda+1 \end{pmatrix}=(-\alpha)(\lambda+1)$，故$\alpha=0$. ■

8. 设D为Euclid环．$c,\ k\in D$，且$c\neq 0$．试证：
1)　$A\in M_n(D)$可逆当且仅当A可表示为$P(i,j),P(c,i),P(k\cdot i,j)$型的矩阵的乘积；
2)　$P(i,j)$可表示为$P(c,i),P(k\cdot i,j)$的乘积．

证明　1) 若A可表示为$P(i,j),P(c,i),P(k\cdot i,j)$型的矩阵的乘积，自然可逆．
若A可逆，则有$P_1,\ P_2,\ \cdots,\ P_k,Q_1,\ Q_2,\ \cdots,\ Q_k$，使得

$$P_1\cdots P_kAQ_1\cdots Q_k=I_n$$

故$A={P_k}^{-1}{P_{k-1}}^{-1}\cdots{P_1}^{-1}{Q_1}^{-1}{Q_k}^{-1}$，可见$A$能表示为$P(i,j),P(c,i),P(k\cdot i,j)$的乘积．

2) $P(i,j)=P(-1,i)P(-j,i)P(1\cdot i,j)P(-i,j)$. ■

9. 设F是域，$A\in M_n(F)$．证明当且仅当A可表示为$P(k\cdot i,\ j)$型的矩阵乘积时A可逆，这里$k\in F$．

证明　这个似乎不对，因为$P(k\cdot i,j)$的行列式为1，这样A可逆当且仅当$\det A=1$，但是，行列式不为1的可逆矩阵是存在的． ■

10. 设D是p. i. d.，$a_i\in D,\ i=1,\ 2,\ \cdots,\ n$．又$d$为$a_1,a_2,\cdots,a_n$的最大公因式．证明存在$M_n(D)$中可逆矩阵$Q$使得

$$(a_1,a_2,\cdots,a_n)Q=(d,0,\cdots,0).$$

证明　当$d=(a_1,a_2,\cdots,a_n)$，我们知存在可逆矩阵P,Q_1使得$P(a_1,a_2,\cdots,a_n)Q_1=(d,0,\cdots,0)$，设$P=(C)$，那么$(a_1,a_2,\cdots,a_n)(Q_1C)=(d,0,\cdots,0)$.取$Q=CQ_1$即可． ■

11. 设D是p. i. d.，$a_i\in Di=1,2,\cdots,n$，且有$(a_1,a_2,\cdots,a_n)=1$．证明：存在$M_n(D)$中的可逆矩阵A，使$\mathrm{row}_1A=(a_1,a_2,\cdots,a_n)$.

证明　由$(a_1,a_2,\cdots,a_n)=1$，可知存在可逆矩阵Q使得$(a_1,a_2,\cdots,a_n)Q=(1,0,\cdots,0)$，即$(a_1,a_2,\cdots,a_n)=(1,0,\cdots,0)Q^{-1}$，那么取$A=I_nQ^{-1}$，有$\mathrm{row}_1A=(a_1,a_2,\cdots,a_n),\ A=Q^{-1}$自然可逆． ■

12. 设D为Euclid环，$A\in M_n(D)$，$\det A\neq 0$．证明存在$M_n(D)$中可逆矩阵P使得

$$PA=\begin{pmatrix} d_1 & & & * \\ & d_2 & & \\ & & \ddots & \\ 0 & & & d_n \end{pmatrix},$$

其中$d_i \neq 0$，且$\delta(\mathrm{ent}_{ji}(PA)) < \delta(d_i), \quad j < i.$

证明 归纳证明. $n = 1$时，显然成立,假设$n = k$时成立.当$n = k+1$时，由定理5.6.1的证明知存在可逆矩阵P_1，使得

$$P_1 A = \begin{pmatrix} d_1 & \alpha \\ 0 & Q \end{pmatrix}$$

由$\det A \neq 0$，知$d_1 \det Q = P_1 A \neq 0$，那么$\det Q \neq 0$.由归纳假设知存在可逆矩阵$P_0$使得

$$P_0 Q = \begin{pmatrix} d_2 & & * \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$$

且$\delta(\mathrm{ent}_{ji}(P_0 Q)) < \delta(d_i), 2 \leqslant j < i \leqslant n, d_i \neq 0.$ 记$P_2 = \begin{pmatrix} 1 & 0 \\ 0 & P_0 \end{pmatrix}$，那么$P_2 P_1 A = \begin{pmatrix} d_1 & \alpha \\ 0 & P_0 Q \end{pmatrix}$. 令$\alpha = (a_{12}, a_{13}, \cdots, a_{1n})$，由$d_2 \neq 0$，可知存在$q_2, r_2$，使$a_{12} = q_2 d_2 + r_2$，且$\delta(r_2) < \delta(d_2)$，对$P_2 P_1 A$作行操作$P(-q_2 \cdot 2, 1)$，这样$P(-q_2 \cdot 2, 1) P_2 P_1 A$的前两列满足题中条件，依次操作，就使$n$列都满足了. ■

Chapter 6

Galois理论

6.1 Galois基本理论

1. 设K是$x^3-2\in\mathbf{Q}[x]$ 的分裂域，求Gal$(K/\mathbf{Q})$的所有子群以及对应的子域，并证明Gal$(K/\mathbf{Q})\simeq S_3$.

   解 令$\theta=e^{2\pi\sqrt{-1}/3}$.那么$[K:\mathbf{Q}]=[K:\mathbf{Q}(\theta)][\mathbf{Q}(\theta):\mathbf{Q}]\leq 6$. 由$[\mathbf{Q}(\theta):\mathbf{Q}]|[K:\mathbf{Q}]$,得$2|[K:\mathbf{Q}]$; 由$[\mathbf{Q}(\sqrt[3]{2}):\mathbf{Q}]|[K:\mathbf{Q}]$,知$3|[K:\mathbf{Q}]$,故$|\mathrm{Gal}(K/\mathbf{Q})|=6$. 由$(3t+1)|2$当且仅当$t=0$，知$G=\mathrm{Gal}(K/\mathbf{Q})$中有唯一的3阶子群$G_1$,而$[K:\mathbf{Q}(\theta)]=3$, 故Inv $G_1=\mathbf{Q}(\theta)$.那么有$\tau\in G_1$,使$\langle\tau\rangle=G_1$,且τ满足：

   $$\tau(\theta)=\theta,\tau(\sqrt[3]{2})=\theta\sqrt[3]{2}.$$

   由$\mathbf{Q}(\theta^{i-1}\sqrt[3]{2}),1\leq i\leq 3$,是3个不同的中间域，且$[K:\mathbf{Q}(\theta^{i_1}\sqrt[3]{2})]=2$,故$G$上至少有3个2阶子群；又由Sylow定理知：$G$上至多有3个2阶群，从而$G$上恰有3个2阶群。设$P_i=\mathrm{Inv}^{-1}\mathbf{Q}(\theta^{i-1}\sqrt[3]{2})$,我们可取$\tau_i\in P_i$,
   $1\leq i\leq 3$,使$\langle\tau_i\rangle=G$,且τ_i满足：

   $$\tau_i(\theta_{i-1}\sqrt[3]{2})=\theta_{i-1}\sqrt[3]{2},\tau_i(\theta)=\theta^2.$$

   这样，我们就求出了Gal$(K/\mathbf{Q})$的所有子群以及所对应的子域。
   如下表：

子群	G	$G_1=\langle\tau\rangle$	$P_i=\langle\tau_i\rangle,1\leq i\leq 3$	id
阶数	6	3	2	1
不变子域	$\mathbf{Q}$	$\mathbf{Q}(\theta)$	$\mathbf{Q}(\theta^{i-1}\sqrt[3]{2})$	K

   令$X=\{P_1,P_2,P_3\}$,那么有G在X上的可递作用，从而诱导出G到$S_{|X|}$的同态η,那么$G/\ker\eta$同构于S_3的子群。由于G的正规子群

为id, G_1, G，而G在
X上的作用可递，故$\ker\eta = \mathrm{id}$，从而$G \simeq S_3$. ■

2. 设$K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. 求$\mathrm{Gal}(K/\mathbf{Q})$的所有子群以及对应的子域。

解 设$\theta \in \mathrm{Gal}(K/F)$,则$\theta(x) = \pm x, x \in \{\sqrt{2}, \sqrt{3}, \sqrt{5}\}$,那么$\theta^2(x) = x$,从而$\theta^2(x) = x, \forall x \in K$.即$\theta^2 = e$，从而$G = \mathrm{Gal}(K/\mathbf{Q})$是Abel群。
易得$[K : \mathbf{Q}] = 8$,那么$|G| = 8$.且$G \simeq \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$.那么$G$ 有7个2阶群，7个4阶群。
从$\mathrm{Inv}^{-1}\mathbf{Q}(\sqrt{3}, \sqrt{5}), \mathrm{Inv}^{-1}\mathbf{Q}(\sqrt{2}, \sqrt{5}), \mathrm{Inv}^{-1}\mathbf{Q}(\sqrt{3}, \sqrt{2})$中分别取出生成元$\sigma, \tau, \eta$,那么$G = \langle\sigma\rangle \otimes \langle\tau\rangle \otimes \langle\eta\rangle$.那么我们易算得$\mathrm{Gal}(K/\mathbf{Q})$的所有子群以及对应的不变子域。
见下表：

子群	G	id	$\langle\sigma\rangle$	$\langle\tau\rangle$
阶数	20	1	2	2
不变子域	$\mathbf{Q}$	K	$\mathbf{Q}(\sqrt{3}, \sqrt{5})$	$\mathbf{Q}(\sqrt{2}, \sqrt{5})$

$\langle\eta\rangle$	$\langle\sigma\tau\rangle$	$\langle\sigma\eta\rangle$	$\langle\eta\tau\rangle$	$\langle\eta\sigma\tau\rangle$
2	2	2	2	2
$\mathbf{Q}(\sqrt{2}, \sqrt{3})$	$\mathbf{Q}(\sqrt{6}, \sqrt{5})$	$\mathbf{Q}(\sqrt{3}, \sqrt{10})$	$\mathbf{Q}(\sqrt{2}, \sqrt{15})$	$\mathbf{Q}(\sqrt{6}, \sqrt{15})$

$\langle\tau, \eta\rangle$	$\langle\sigma, \eta\rangle$	$\langle\sigma, \tau\rangle$	$\langle\sigma\tau, \eta\rangle$	$\langle\sigma\eta, \tau\rangle$	$\langle\tau\eta, \sigma\rangle$	$\langle\sigma\tau, \sigma\eta\rangle$
4	4	4	4	4	4	4
$\mathbf{Q}(\sqrt{2})$	$\mathbf{Q}(\sqrt{3})$	$\mathbf{Q}(\sqrt{5})$	$\mathbf{Q}(\sqrt{6})$	$\mathbf{Q}(\sqrt{10})$	$\mathbf{Q}(\sqrt{15})$	$\mathbf{Q}(\sqrt{30})$

■

3. 设r是$x^3 + x^2 - 2x - 1 \in \mathbf{Q}[x]$的一个根，证明：$r^2 - 1$也是一个根；$\mathbf{Q}(r)$是$\mathbf{Q}$上的正规扩张, 并求$\mathrm{Gal}(\mathbf{Q}(r)/\mathbf{Q})$。

证明 易得r^2-1是一根，且$r^2-1 \neq r$.那么$r, r^2-1, 1/(r^3-r)$是方程的根，可见$\mathbf{Q}(r)$是$\mathbf{Q}$上多项式x^3+x^2-2x-1的分裂域，从而$\mathbf{Q}(r)$是$\mathbf{Q}$上的正规扩张。由于该多项式无重根，知$[\mathbf{Q}(r) : \mathbf{Q}] = 3$,从而$|\mathrm{Gal}(\mathbf{Q}(r)/\mathbf{Q})| = 3$.令$\sigma \in \mathrm{Gal}(\mathbf{Q}(r)/\mathbf{Q})$,且$\sigma$满足：

$$\sigma(r) = r^2 - 1.$$

那么$\mathrm{Gal}(\mathbf{Q}(r)/\mathbf{Q}) = \langle\sigma\rangle$. ■

4. 设域F的特征是p。试证$x^p - x - a \in F[x]$或者不可约，或者为一次因式的乘积。又设K为$x^p - x - a$的分裂域，求$\mathrm{Gal}(K/F)$。

证明 设$\alpha \in K$是x^p-x-a的一个根，那么$x^p-x-a=\prod_{k=0}^{p-1}(x-\alpha-k)$.可见该多项式要么可约，要么为一次因式的乘积。
若$x^p-a-x \in F[x]$,不可约，那么$|\mathrm{Gal}(K/F)|=p$.令$\sigma \in \mathrm{Gal}(K/F)$,且满足：$\sigma(\alpha)=\alpha+1$.可见$\mathrm{Gal}(K/F)=\langle\sigma\rangle$.
若$x^p-x-a \in F[x]$可约，则$K=F, \mathrm{Gal}(K/F)=\mathrm{id}$. ■

5. 设K是域F的有限可分扩张，K_1, K_2是两个中间域。以$K_1 \bigvee K_2$表示包含K_1与K_2的最小子域（称为K_1与K_2和域）。又设G_1, G_2是$G=\mathrm{Gal}(K/F)$的两个子群。试证：
1) $\mathrm{Inv}\,(G_1 \cap G_2)=\mathrm{Inv}\,G_1 \bigvee \mathrm{Inv}\,G_2$;
2) $\mathrm{Inv}\,(\langle G_1, G_2\rangle)=\mathrm{Inv}\,G_1 \cap \mathrm{Inv}\,G_2$.

证明 由定义易得。 ■

6. 设$\sigma_1, \sigma_2, \ldots, \sigma_n$ 是域K的自同构，且$i \neq j$时，$\sigma_i \neq \sigma_j$.试证：
1) K中子集$F=\{x \in K | \sigma_i(x)=x, 1 \leq i \leq n\}$是$K$中的子域；
2) $\sigma_i(1 \leq i \leq n)$是线性空间$K$中的线性变换；
3) $\sigma_1, \sigma_2, \ldots, \sigma_n$是线性无关的线性变换组；
4) $[K:F] \geq n$.

证明 1) 易得。
2) 由F的定义可知，$\sigma_i(1 \leq i \leq n)$可看成$F$上的线性空间$K$中的线性变换。
3) 若$\sigma_1, \sigma_2, \ldots, \sigma_n$线性相关，则有$s$满足：
$\sigma_1, \ldots, \sigma_s$线性无关，$\sigma_1, \ldots, \sigma_{s+1}$线性相关。
于是σ_{s+1}可唯一地表示成：

$$\sigma_{s+1}=a_1\sigma_1+\ldots+a_s\sigma, a_i \in F, 1 \leq i \leq s.$$

由$\sigma_{s+1} \neq \sigma_1$,知存在$a \in K$使$\sigma_{s+1}(a) \neq \sigma_1(a)$, 那么

$$\sigma_{s+1}(ax)=a_1\sigma_1(ax)+\ldots+a_s\sigma(ax),$$

$$\sigma_{s+1}=a_1 \cdot \frac{\sigma_1(a)}{\sigma_{s+1}(a)}\sigma_1+\ldots+a_s \cdot \frac{\sigma_s(a)}{\sigma_{s+1}(a)}\sigma.$$

但$a_1 \cdot \frac{\sigma_1(a)}{\sigma_{s+1}(a)} \neq a_1$,这样与$\sigma_{s+1}$的表示唯一矛盾。故$\sigma_1, \ldots, \sigma_n$线性无关。
4) 令$F_1=\mathrm{Inv}\,(\mathrm{Gal}(K/F))$。我们知$K$是$F_1$上的Galois扩张。如果$[K:F]<n$,那么$[K:F_1] \leq [K:F]<n$;又$[K:F_1]=|\mathrm{Gal}(K/F_1)|=$

$|\mathrm{Gal}(K/F)|$,但$|\mathrm{Gal}(K/F)| \geq n$,这样$[K:F_1] \geq n$,矛盾。故$[K:F] \geq n$. ■

7. 设K是F的扩域，又$G = \mathrm{Gal}(K/F)$.试证：
$|\mathrm{Gal}(K/F)| = [K : \mathrm{Inv}(\mathrm{Gal}(K/F))]$.
又问K是否为$\mathrm{Inv}(\mathrm{Gal}(K/F))$上的Galois扩张？

证明 令$F_1 = \mathrm{Inv}(\mathrm{Gal}(K/F))$.由$\mathrm{Gal}(K/F_1) = \mathrm{Gal}(K/F)$,易得$K$是$F_1$上的Galois扩张。 ■

8. 设K是域F的有限可分正规扩张，又K_1, K_2是两个之间域。证明：
1) $K_1 \bigvee K_2 = K \iff \mathrm{Gal}(K/K_1) \bigcap \mathrm{Gal}(K/K_2) = \mathrm{id}$;
2) 又若K_1是F的正规扩张，则$\mathrm{Gal}(K/K_2)$ 与$\mathrm{Gal}(K/K_1)$的一个子群同构。

证明 1) 由K是F上的有限Galois扩张，知K也是K_1, K_2上的Galois扩张，那么$K_i = \mathrm{Inv}(\mathrm{Gal}(K/F_i)), i = 1, 2$.再由题5(1)可知命题是显然成立的。

2) 令$H_i = \mathrm{Gal}(K/K_i), i = 1, 2$,那么$H_1 \cap H_2 = \mathrm{id}$.再由$K_1$是$F$的正规扩张知：$H_1 \lhd G$.由同态基本定理可知：$H_1H_2/H_1 \simeq H_2$,而$\mathrm{Gal}(K_1/F) = G/H_1$,故$\mathrm{Gal}(K/K_2)$与$\mathrm{Gal}(K_1/F)$的一个子群同构。 ■

9. 设K是F的有限可分正规扩张，$G = \mathrm{Gal}(K/F)$. 又设E是一个中间域，$\overline{E}$是K中包含E的F的最小正规扩张。
证明：
1) $\mathrm{Gal}(K/\overline{E}) = \bigcap\limits_{\sigma \in G} \sigma \mathrm{Gal}(K/E)\sigma^{-1}$;
2) $\overline{E} = \bigvee\limits_{\sigma \in G} \sigma(E)$.

证明 1) 由Galois基本定理知：$\overline{E}$是K中包含E的F的最小正规扩张$\Leftrightarrow \mathrm{Gal}(K/\overline{E})$ 是$\mathrm{Gal}(K/E)$内G的最大正规子群。自然$\mathrm{Gal}(K/\overline{E}) = \bigcap\limits_{\sigma \in G} \sigma \mathrm{Gal}(K/E)\sigma^{-1}$.

2) 题5(1)中的结论可推广到有限情形。那么$\overline{E} = \mathrm{Inv}(\mathrm{Gal}(K/\overline{E})) = \bigvee\limits_{\sigma \in G} \mathrm{Inv}(\sigma \mathrm{Gal}(K/E)\sigma^{-1}) = \bigvee\limits_{\sigma \in G} \sigma(E)$. ■

6.2 一个方程的群

1. 设F是域，$\mathrm{Ch}\, F \neq 2$.又$x_1, x_2, \ldots, x_n$是不定元，$p_1, p_2, \ldots, p_n$为$x_1, x_2, \ldots, x_n$的初等对称多项式，记$\mathrm{Gal}(F(x_1, x_2, \ldots, x_n)/F(p_1, p_2, \ldots, p_n))$为$S_n$。证明$\mathrm{Inv}\, A_n = F(p_1, p_2, \ldots, p_n, \Delta)$.其中$\Delta = \prod\limits_{i<j}(x_i - x_j)$.

证明 令$F_1 = F(p_1, p_2, \ldots, p_n)$.由Ch $F \neq 2$,知$\Delta \notin F_1$,又$\Delta^2 \in F_1$, 故$[F_1(\Delta) : F_1] = 2$.那么$[\mathrm{Gal}(K/F_1) : \mathrm{Gal}(K/F_1(\Delta)] = 2$,则$\mathrm{Gal}(K/F_1(\Delta)) = A_n$.故Inv $A_n = F(p_1, p_2, \ldots, p_n, \Delta)$. ■

2. 设G是有限群，证明存在域F及其Galois扩张K,使得$\mathrm{Gal}(K/F) \simeq G$.

证明 我们选取域F_1及其Galois扩张K，使得$\mathrm{Gal}(K/F_1) \simeq S_n, n = |G|$.由于$G$同构于$S_n$的一个子群，于是存在中间域$F$，使得$\mathrm{Gal}(K/F) \simeq G$. ■

3. 设F是域，$f(x) \in F[x]$无重根，又K为$f(x)$的分裂域，$u_1, u_2, \ldots, u_n, (n = \deg f(x))$是不定元。记$\overline{F} = F(u_1, u_2, \ldots, u_n), \overline{K}$为$f(x) \in \overline{F}[x]$的分裂域，证明$\mathrm{Gal}(\overline{K}/\overline{F})$与$\mathrm{Gal}(K/F)$同构。

证明 我们可取$\overline{K} = K(u_1, u_2, \ldots, u_n)$.对$\forall \sigma \in \mathrm{Gal}(K/F), \sigma$可自然开拓成$\overline{K}$上的自同构，记为$\overline{\sigma}$,显然$\overline{\sigma} \in \mathrm{Gal}(\overline{K}/\overline{F})$.作$\mathrm{Gal}(K/F)$到$\mathrm{Gal}(\overline{K}/\overline{F})$上的映射$\varphi : \varphi(\sigma) = \overline{\sigma}$.显然，$\varphi$是同构映射，即$\mathrm{Gal}(\overline{K}/\overline{F}) \simeq \mathrm{Gal}(K/F)$. ■

4. 在上题假设下，又设$a_1, a_2, \ldots, a_n$,为$f(x)$的根，记$v_1 = u_1a_1 + u_2a_2 + \ldots + u_na_n$.对$\sigma \in S_n$，定义$\sigma(v_1) = \sum_{i=1}^{n-1} u_i a_{\sigma(i)}$.

证明：

1) $\tau, \sigma \in S_n, \tau = \sigma \iff \tau(v_1) = \sigma(v_1)$.

2) 令$\overline{f}(x) = \prod_{\sigma \in S_n} (x - \sigma(v_1))$.则$\overline{f}(x) \in \overline{F}[x]$,且系数在$F[u_1, u_2, \ldots, u_n]$中。

3) 设$\overline{f}(x)$在$F[u_1, u_2, \ldots, u_n]$上有不可约因式分解：$\overline{f}(x) = \overline{f}_1(x)\overline{f}(x_2)\ldots$,其中$\overline{f}_1(v_1) = 0$，则$\sigma \in \mathrm{Gal}(K/F) \iff \overline{f}_1(v_1) = 0$.$\overline{f}_1$称为$f(x)$的Galois预解析式，且有$\overline{K} = \overline{F}(v_1)$.

证明 ■

5. 设p是素数，$f(x) \in \mathbf{Z}[x]$.将$f(x)$作为$\mathbf{Z}_p$上的多项式时记为$\overline{f}(x)$.若$\overline{f}(x)$无重根，则$G(\overline{f}, \mathbf{Z}_p)$与$G(f, \mathbf{Q})$的一个子群同构。试证明。

证明 ■

6. 利用上题证明$G(x^5 - x - 1, \mathbf{Q}) = S_5$.

解 ■

7. 求$G(2x^5 - 5x^4 + 5, \mathbf{Q})$.

解 ■

8. 设$f(x)=x^7+22x^5-776x^3+2688x-2$.试证$G(f,\mathbf{Q})=S_7$.

解 ■

6.3 分圆域二项方程

1. 设$m,n\in N$,且$(m,n)=1$.证明$\varphi(mn)=\varphi(m)\varphi(n)$.

证明 令$s=\varphi(m),t=\varphi(n),x_1,x_2,\dots,x_s$为小于$m$且与$m$互素的$s$个正整数，$y_1,\dots,y_t$为小于$n$且与$n$互素的$t$个互不相同的正整数。由$(m,n)=1$,知$nx_i+my_j,1\le i\le s,1\le j\le t$,为与$mn$互素且互不同余。而任意与$mn$互素的数$k$，有$a,b\in\mathbf{Z}$使$am+bn=k$,那么$(a,n)=(b,m)=1$.即有$x_i,y_j$使$x_i\equiv b(\mod m),y_i\equiv a(\mod n)$,那么$nx_i+my_i\equiv k(\mod mn)$.故$\varphi(mn)=\varphi(m)\varphi(n)$. ■

2. 设p是素数，证明$\varphi(p^k)=p^{k-1}(p-1)$,从而
$\varphi(p_1^{k_1}p_2^{k_2}\dots p_s^{k_s})=\prod_{i=1}^{s}(p_i-1)p_i^{k_i}$.
$p_1,p_2,\dots,p_n$是互不相同的素数。

证明 由上题可得。 ■

3. 定义N上的函数$\mu(n)$为
$$\mu(n)=\begin{cases}1, & \text{当}n=1;\\ 0, & \text{当}n>1,\text{且有平方因子;}\\ (-1)^l, & \text{当}n=p_1p_2\dots p_l,p_1,p_2,\dots,p_l\text{是互不相同的素数;}\end{cases}$$
$\mu(n)$称为Mobius函数。证明
1) 若$(m,n)=1$,则$\mu(mn)=\mu(m)\mu(n)$;
2) $\sum_{d|n}\mu(d)=\delta_{1n}$.

证明 1) 由定义可得。
2) 若$n=1$,显然成立；若$n>1$,令$n=p^lm,(m,p)=1$.那么$\sum_{d|n}\mu(d)=\sum_{k=0}^{l}(\sum_{d|m}\mu(dp^k))=\delta_{1n}$. ■

4. 证明$\Phi_n(x)=\prod_{d|n}(x^2-1)^{\mu(n/2)}$.

证明 由$x^d-1=\prod_{k|d}\Phi_k(x)$,知
$\prod_{d|n}(x^d-1)^{\mu(\frac{n}{d})}=\prod_{k|n}\Phi_k(x)^{l(k)}$,这里$l(k)=\sum_{k|d}\mu(\frac{n}{d})=\sum_{d|\frac{n}{k}}\mu(\frac{n}{kd})=\delta_{1\frac{n}{k}}$,
故$\Phi_n(x)=\prod_{d|n}(x^d-1)^{\mu(\frac{n}{d})}$. ■

5. 设$(m,n)=1$.证明$x^{mn}-1\in\mathbf{Q}[x]$的分裂域与$(x^m-1)(x^n-1)\in\mathbf{Q}[x]$的分裂域相同。

   证明 令$x^{mn}-1\in\mathbf{Q}[x],(x^m-1)(x^n-1)\in\mathbf{Q}[x]$的分裂域分别为$E,F$。由$(x^m-1)|(x^{mn}-1),(x^n-1)|(x^{mn}-1)$,可知$E\supseteq F$.又$[E:\mathbf{Q}]=\varphi(mn)=\varphi(m)\varphi(n)=[F:\mathbf{Q}]$,故$E=F$. ■

6. 设$(m,n)=1$.证明$G(x^{mn}-1,\mathbf{Q})$同构于$G(x^m-1,\mathbf{Q})$与$G(x^n-1,\mathbf{Q})$的直积。

   证明 设θ_1为m次单位原根，θ_2为n次单位原根，那么${\theta_1}^n{\theta_2}^m$为mn次单位原根。任取$\sigma\in G(x^m-1,\mathbf{Q}),\tau\in\mathrm{Gal}(x^n-1,\mathbf{Q})$,可诱导出$\mathrm{Gal}(x^{mn}-1,\mathbf{Q})$中元$\sigma\otimes\tau:\sigma\otimes\tau({\theta_1}^n{\theta_2}^m)=\sigma(\theta_1)^n\tau(\theta_2)^m$.那么可作$G(x^m-1,\mathbf{Q})\otimes G(x^n-1,\mathbf{Q})$到$G(x^{mn}-1,\mathbf{Q})$的映射$\varphi:\varphi(\sigma,\tau)=\sigma\otimes\tau$.显然$\varphi$是$G(x^m-1,\mathbf{Q})\otimes G(x^n-1,\mathbf{Q})$到$G(x^{mn}-1,\mathbf{Q})$的同构映射。 ■

7. 设$n=p_1^{k_1}p_2^{k_2},\ldots,p_t^{k_t},i$为互不相同的素数，则证明
   $U_n=U_{p_1^{k_1}}\times U_{p_2^{k_2}}\times\ldots\times U_{p_t^{k_t}}$.

   证明 我们知道$G(x^n-1,\mathbf{Q})$与U_n之间有一个自然的群同态，再由上题可得：如果$(n,m)=1$,那么$U_{mn}\simeq U_m\times U_n$.从而$U_n=U_{p_1^{k_1}}\times U_{p_2^{k_2}}\times\ldots\times U_{p_t^{k_t}}$. ■

8. 设域F的特征$p>0,p\neq n$.试求x^n-1对F的群。

   解 ■

9. 设F是域，p是素数，且$p\neq\mathrm{Ch}\,F,a\in F$, 证明$x^p-a$ 或为$F[x]$中不可约多项式，或在F中有根。

   证明 设ξ是x^p-a的根，θ是p次单位原根。若$x^p-a\in F[x]$可约，设$x^p-a=h(x)k(x),1\leq\deg h(x)<p$.那么$h(x)$的常数项可设为$\xi^k\theta^t$,且$(k,p)=1$,则有$u$使$uk\equiv1(\mod p)$.这样$(\xi^k\theta^t)^u\in F$,那么$\xi\theta^{tu}\in F$, 但$\xi\theta^{tu}$是$x^p-a$的根。可见$x^p-a$在$F$上要么不可约，要么有根。 ■

10. 设x^p-a为$\mathbf{Q}[x]$中不可约多项式，证明$G(x^p-a,\mathbf{Q})$ 与$\mathbf{Z}_p$中的变换群$\{\sigma_{kl}|k\neq0\}$同构，其中$\sigma_{kl}(y)=ky+l,\forall y\in\mathbf{Z}_p$.

    证明 ■

11. 设p是素数，F是域，$p\neq\mathrm{Ch}\,F$,且F包含p次单位根，$a\in F$,求x^p-a对F的群。

    解 我们知x^p-a 对F 的群$G(x^p-a,F)$与p阶循环群的子群同构，那么$|G(x^p-a,F)|=1$或p.再由题9可得：

若x^p-a在F上不可约，则$|G(x^p-a,F)|>1$,于是$G(x^p-a,F)\simeq \mathbf{Z}_p$.

若x^p-a在F上不可约，则$|G(x^p-a,F)|=1$,于是$G(x^p-a,F)\simeq \{\mathrm{id}\}$. ■

6.4 方程的根式解

1. 用根式解下列$\mathbf{Q}$上方程：

1) $x^3-2x+4=0$;

2) $x^3-15x+4=0$.

解 运用公式就可得。 ■

2. 设$x_i,1\leq i\leq 4$ 是域F上的不定元，在多项式$\prod_{i=1}^{4}(x-x_i)=x^4-t_1x^3+t_2x^2-t_3x+t_4$中用$y_i=x_i-t_1/4$代替$x_i$,得方程$f(y)=y^4+py^2+8y+r=0$.

1) 求p,q,r与t_1,t_2,t_3,t_4的关系。

2) 证明$G(f(y),F(t_1,t_2,t_3,t_4))=S_4$.

3) 求证：S_4的序列

$S_4\supset A_4\supset K_4\supset \mathbf{Z}\supset \mathrm{id}$,其中$\mathbf{Z}=\mathrm{id},(12)(34)$.

对应的不变子域为

$\mathrm{Inv}\,S_4=F(t_1,t_2,t_3,t_4)$;

$\mathrm{Inv}\,A_4=F(t_1,t_2,t_3,t_4,\sqrt{D})$;

$\mathrm{Inv}\,K_4=F(t_1,t_2,t_3,t_4,\sqrt{D})(\theta_1)=F(t_1,t_2,t_3,t_4,\theta_1,\theta_2,\theta_3)$,

θ_i 是$z^3-2pz^2+(p^2-4r)z+q^2=0$ 的根，$1\leq i\leq 3$.

$\mathrm{Inv}\,\mathbf{Z}=F(t_1,t_2,t_3,t_4,\sqrt{D},\theta_1,\sqrt{-\theta_1})$;

$D=16p^4r-4p^3q^2-12qp^2r^2+144q^2r-27q^4+256r^3$.

4) 求$x_i,1\leq i\leq 4$.

证明 1) 经计算可得p,q,r与t_1,t_2,t_3,t_4的关系为：

$p=t_2+\frac{3}{16}{t_1}^2$,

$q=-t_3+\frac{t_1t_2}{2}-\frac{3}{16}{t_1}^3$,

$r=t_4-\frac{t_1t_3}{4}+\frac{{t_1}^2t_2}{16}-\frac{3{t_1}^4}{256}$.

2) 令$E=F(t_1,t_2,t_3,t_4)$.由$G(\prod_{i=1}^{4}(x-x_i),E)=G(f(y),E)$,可得$G(f(y),F(t_1,t_2,t_3,t_4))=S_4$.

3) 由计算可得$D=\Delta^2$,其中$\Delta=\prod_{i<j}4(x_i-x_j)$.由$\Delta\notin E,D=\Delta^2\in E$,可得$\mathrm{Inv}\,A_4=E(\sqrt{D})$.

由$\prod_{1\leq i<j\leq 4}(y-y_i-y_j)$是对称多项式,知$\prod_{1\leq i<j\leq 4}(y-y_i-y_j)\in$

$E(y)$.而$\prod_{1\le i<j\le 4}(y-y_i-y_j)=[y^2-(y_1+y_2)^2][y^2-(y_1+y_3)^2][y^2-(y_1+y_4)]$,那么$[y+(y_1+y_2)^2][y+(y_1+y_3)^2][y+(y_1+y_4)]\in E(y)$,把该方程记为$h(y)$,经计算得$h(y)=z^3-2pz^2+(p^2-4r)z+q^2$,那么$E(\sqrt{D},\theta_1)\subset \mathrm{Inv}\,K_4, E(\theta_1,\theta_2,\theta_3)\subset \mathrm{Inv}\,K_4$.由$[E(\sqrt{D},\theta_1):E)=6=[\mathrm{Inv}\,K_4:E]$,可得$E(\sqrt{D},\theta_1)=\mathrm{Inv}\,K_4$;由于$E(\theta_1,\theta_2,\theta_3)$是$h(y)\in E(y)$上的分裂域，那么$E(\theta_1,\theta_2,\theta_3)$是$E$上的正规扩张，那么$\mathrm{Gal}(F(x_1,x_2,x_3,x_4)/E(\theta_1,\theta_2,\theta_3))$是$S_4$上的正规扩张，而$S_4$,只有2个非平凡正规子群$K_4, A_4$,那么$E(\theta_1,\theta_2,\theta_3)=\mathrm{Inv}\,K_4$.
由$\sqrt{-\theta_1}\notin \mathrm{Inv}\,K_4, (\sqrt{-\theta_1})^2\in \mathrm{Inv}\,K_4$，又，$E(\sqrt{D},\theta_1,\sqrt{-\theta_1})\subset \mathrm{Inv}\,\mathbf{Z}$,可得$E(\sqrt{D},\theta_1,\sqrt{-\theta_1})=\mathrm{Inv}\,\mathbf{Z}$.

4) 从求证$E(\theta_1,\theta_2,\theta_3)=\mathrm{Inv}\,K_4E(\sqrt{D},\theta_1$的过程中，我们知$y_1=\frac{\theta_1+\theta_2+\theta_3}{2}$,那么我们用三次方程的求根公式算出$\theta_1,\theta_2,\theta_3$;再由$x_1=y_1+\frac{t_1}{4}$,我们可算出$x_1$.同样可算出$x_2,x_3,x_4$. ■

6.5 圆规直尺作图

1. 设有$\mathbf{Q}$的二次扩域序列

$$K_0=\mathbf{Q}\subset K_1\subset K_2\subset\ldots\subset K_n$$

其中$[K_i:K_{i-1}]=2, 1\le i\le n$,证明有$\mathbf{Q}$的正规扩张$\overline{K_m}$满足$K_n\subset\overline{K_m}$,且
$\overline{K_0}=\mathbf{Q}\subset\overline{K_1}\subset\overline{K_2}\subset\ldots\overline{K_m}, [\overline{K_j}:\overline{K_{j-1}}]=2.$

证明 证法类似于定理6.4.1的。 ■

2. 已知一正立方体的边长a。试证不可能用圆规直尺作图的方法作一正方体使其体积为$2a^3$.

证明 要做出体积为$2a^3$的正方体等价于作出长度$\sqrt[3]{2}$,但$\deg(\sqrt[3]{2},\mathbf{Q})=3$! ■

3. 由圆周率π对$\mathbf{Q}$是超越数，证明不可能用圆规直尺作出一正方形使其面积为π.

证明 由$\deg(\pi,\mathbf{Q})=\infty$可得。 ■

4. 设$n\in N$,且$n=2^m p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$.其中$p_i, 1\le i\le s$是互不相同的奇素数。证明能用圆规直尺作出正$n$边形的充要条件是$p_i$为Fermat素数，且$k_i=1, i=1,2,\ldots,s$.

证明 由p^m阶群G是可解群，知G存在次正规序列

$$G=G_1\supset G_2\supset\ldots\supset G_s=\{\mathrm{id}\},$$

且$|G_i/G_{i+1}| = p$.再由题1可得结论：

$\gamma \in \mathbf{C}$可用圆规直尺作出$\Leftrightarrow$ 存在$\mathbf{Q}$的正规扩张K,满足$\gamma \in K$,且$2^n = [K : \mathbf{Q}]. \Leftrightarrow G(Irr(\gamma, \mathbf{Q}), \mathbf{Q}) = 2^n$.

在单位圆内作出正n边形，即作出n次单位原根θ.我们知$[\mathbf{Q}(\theta) : \mathbf{Q}] = \varphi(n), \mathbf{Q}(\theta)$是$\mathbf{Q}$的可分正规扩张。故能用圆规直尺作出正$n$边形的充要条件是$\varphi(n)$只含有素因子2，即$i$为Fermat素数，$k_i = 1, i = 1, 2, \ldots, s$. ■

5. 讨论正五边形的做法。

解 仿照例6.5.3的方法。 ■