抽象代数习题答案

四川大学数学学院，四川成都，610064

彭联刚

§1 群论

9.设G是群，k为正整数. 记$G^k=\{a^k|a\in G\}$. 证明：G循环$\Leftrightarrow G$的每个非平凡子群具有形式G^k，对某个k.

证明: "$\Rightarrow$"：显然.

"$\Leftarrow$"：由条件易知G的每个子群都是正规子群. 如果G中有$x\neq e$且x有有限阶，不妨设为n. 设$\langle x\rangle=G^k$（某个k），那么对任意$y\in G$，有$y^k\in\langle x\rangle$. 故$y^{nk}=e$，即y的阶小于或等于nk. 故G中每个元都是有限阶的，并且阶有上界nk. 设$a,b\in G$的阶分别为s,t，且$(s,t)=1$，设ab的阶为m，由$\langle b\rangle$正规知$a\langle b\rangle=\langle b\rangle a$，故$ab=b^ja$，于是$e=(ab)^m=b^la^m$（对某个$l$），即$a^{-m}=b^l$，故$s|m$，类似$t|m$，从而$st|m$. 由此易知，若设$c\in G$的阶$r$最大（由阶有限知这样的$c$存在），那么$G$中任意元的阶整除$r$. 设$\langle c\rangle=G^{k'}$（某个$k'$），故存在$d\in G$使得$c=d^{k'}$. 由$r$的最大性知$d$的阶也为$r$，从而$(r,k')=1$. 任取$g\in G$，其阶为$r'$，那么$r'|r$知$(r',k')=1$. 故$\langle g\rangle=\langle g^{k'}\rangle=\langle c\rangle$，即$g\in\langle c\rangle$. 故$G=\langle c\rangle$.

如果G中所有非单位元的阶都无限. 对任意的$a,b\in G$，且$b\neq e$. 由$\langle b\rangle$正规知$ab=b^ja$，设$\langle b\rangle=G^k$（某个k）. 那么$a^k=b^i$，从而$b^{ji}=(aba^{-1})^i=ab^ia^{-1}=a^k=b^i$. 有$b$的阶无限知$j=1$. 故$ab=ba$，即$G$为交换群. 又存在$c\in G$使得$b=c^k$，故$a^k=b^i=c^{ik}$，由交换性和非单位元阶无限知$a=c^i\in\langle c\rangle$，由$a$的任意性知$G=\langle c\rangle$. ■

12.当$n>2$时，证明A_n由$(1\,2\,3)$和$(1\,2\,\cdots\,n)$生成(当n是奇数时)，A_n由$(1\,2\,3)$和$(2\,3\,\cdots\,n)$生成(当n是偶数.)

证明: 注意A_n由所有的3-轮换生成，而$(i\,j\,k)=(i\,j)(j\,k)=(1\,i)(1\,j)(1\,i)(1\,j)(1\,k)(1j)=(i\,1\,j)(i\,1\,j)(k\,1\,j)$. 故$A_n$由$(1\,i\,j),\forall i,j$生成.

当n为奇数时，设$H=<(1\,2\,3),(1\,2\,\cdots n)>$.考虑$(1\,i\,j),j\geq 3$.注意易知$(3\,4\,5)\in H$. 故$(3\,4\,5)(1\,2\,3)(3\,4\,5)^{-1}=(1\,2\,4)\in H$.归纳易知$(1\,2\,j)\in H,j\geq 3$. 又考虑$(1\,i\,j),2\leq i<j$. 若$i>2$, 由$(i-1\,i\,i+1)\in H$知$\sigma:=(i\,i-1\,i+1)=(i-1\,i\,i+1)^2\in H$,而$\sigma(1\,i\,j)\sigma^{-1}=(1\,i-1\,\sigma(j))\in H$（对$i$进行归纳可得）. 故$(1\,i\,j)\in H$，从而$H=A_n$.

当n为偶数时，设$H=<(1\,2\,3),(2\,3\,\cdots n)>$, 那么$(1\,i\,i+1)\in H,2\leq i\leq n-1$. 由$(2\,3\,4)=(2\,3)(3\,4)=(2\,1)(1\,3)(2\,1)(3\,1)=(2\,1\,3)(2\,1\,3)(4\,1\,3)=(1\,2\,3)(1\,3\,4)\in H$, 类似于$n$为奇数的证明可知对于任意的$i<j,(1\,i\,j)\in H$，故$H=A_n$. ■

14.在S_5中确定每个共轭类的一个代表元及每个共轭类包含元素的个数. 由此证明S_5只有三个正规子群$\{e\}$，A_5，S_5.

证明: 共轭类的代表元分别为$e,(12),(12)(34),(12)(345),(123),(1234),(12345)$，它们所在共轭类的元素个数分别为$1,10,15,20,20,30,24$.

设$H\lhd G$且H不为$\{e\}$，A_5，S_5. 那么H不包含(12)和(123). H也不可能同时包含$(12)(34)$和(12345)，否则包含(245). 但$15,20,30$中任意多个不同的和再加1都不是$5!$的因子. 而$20,30,24$中任意多个不同的和再加1也不是$5!$的因子，从而这样的H不存在. ■

18.设G有限群，$H<G$是$[G:H]=n>1$，证明：或者存在某个正规子群$K\lhd G$使得$[G:K]|n!$，或者G同构于S_n的一个子群.

证明: G自然地左乘作用在G/H上，而$Sym(G/H)=S_n$. 故有群同态$G\to S_n$. 其核记为$K\lhd G$，于是$[G:K]=|G/K|\,||S_n|=n!$. 当$K=\{e\}$时，有G到S_n的嵌入. ■

19.设G为有限群且p为$|G|$的最小素因子. 若存在子群H使得$[G:H]=p$，则$H\lhd G$.

证明: 由上题的证明知存在$K\lhd G$且$K<H$使得$[G:K]|p!$，由p的定义知$[G:K]=p$. 故$H=K\lhd G$. ■

21.证明任一非交换的6阶群同构于S_3.

证明: 设H和H'分别是G的2-sylow子群和3-sylow子群，由G在左陪集G/H上的左乘作用知有同态$G\to Sym(G/H)=S_3$. 其核$K\le H$，如果$K\ne\{e\}$，则$H=K\lhd G$，由上题（或sylow定理）知$H'\lhd G$. 但$H\cap H'=\{e\}$，故$G=H\oplus H'$，从而G交换，矛盾. 所以$K=\{e\}$，即上面的同态单，但$|G|=6=|S_3|$，故有同构$G\simeq S_3$. ■

23.给出全部互不同构的10阶群G.

证明: 若G的2-sylow子群和5-sylow子群都正规，则G交换且为10阶循环群. 若2-sylow子群不正规，记$\langle a\rangle,\langle b\rangle$分别为2-sylow子群和5-sylow子群. 则$\langle b\rangle\lhd G$，从而$a\langle b\rangle=\langle b\rangle a$. 于是$ab=b^ia$，注意$a^2=e$，故$b=ab^ia=b^{i^2}a^2=b^{i^2}$，由$5|i^2-1$，$1<i\le 4$，故$i=4$. 故$ab=b^4=b^{-1}$. 从而$G$与二面体群$D_5$同构，即在同构意义下，10阶群为循环群或$D_5$. ■

25.设p,q为不同的整数，证明p^2q阶群G必包含一个正规的sylow子群.

证明: 设S和H 分别是G的$p-$sylow子群和$q-$sylow子群. 若$q>p^2$，则$H\lhd G$，故设$q<p^2$. 若$q<p$，则$S\lhd G$，故设$p<q<p^2$. 假设S和H都不正规，则$q-$sylow子群个数为p^2个，它们两个的交为$\{e\}$，故G中q阶元的个数为$p^2(q-1)$. 而$p-$sylow子群子群的个数为q，故阶为p或p^2的元的个数大于等于$(p^2-1)+1=p^2$，故G中阶大于1的元素个数大于等于$p^2(q-1)+p^2=p^2q$，矛盾. 故S和H之一正规. ■

26.举出两个有限的非交换群G，分别适合：(1) $a^3=e,\forall a\in G$；(2) $a^4=e,\forall a\in G$.

解: （1）设$p\geq 3$是素数，$\mathbb{F}_p$是$p-$元域. 记$UT(3,\mathbb{F}_p)=\left\{\left.\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\right|a,b,c\in\mathbb{F}_p\right\}$，它自然是一个群，且非交换，如：$\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}\cdot\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$，而

$$\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}\cdot\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}=\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}$$

又$\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}^p=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}+\begin{pmatrix}0&a&b\\0&0&c\\0&0&0\end{pmatrix}^p=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$.特别地，取$p=3$即可.

（2）之一为四元数群$\{1,i,j,k,-1,-i,-j,-k\}$，有关系$ij=k,jk=i,ki=j,i^2=j^2=k^2=-1$. 之二为$D_4=\{b,b^2,b^3,b^4,ab,ab^2,ab^3,ab^4\}$有关系$a^2=b^4=1,aba=b^3$(8元群非交换，故非循环，从而元素的阶至多为4). **注:** 上述两个例子不同构!■

27.设$H,K<G$，$a\in G$. 证明：$|HaK|=|H|[K:a^{-1}Ha\cap K]$.

证明: H自然在$\{haK|h\in H\}=S$上有左乘作用. $stab(aK)=\{h\in H|haK=aK\}=\{h\in H|a^{-1}ha\in K\}=H\cap aKa^{-1}$，故$|HaK|=|S|.|K|=(|H|/|H\cap aKa^{-1}|).|K|=|H|.|K|/|a^{-1}Ha\cap K|=|H|[K:a^{-1}Ha\cap K]$.

另证：$|HaK|=|a^{-1}HaK|=|a^{-1}Ha|.|K|/|a^{-1}Ha\cap K|=|H|.[K:a^{-1}Ha\cap K]$. ■

30.设H是有限群G的真子群，证明：$G\neq\bigcup_{g\in G}gHg^{-1}$.

证明: G共轭作用在$\{gHg^{-1}|g\in G\}=S$上，$Stab(H)=N(H)$（H的正规化子）. 显然$H\lhd N(H)$，若$N(H)=G$，显然$G\neq H=\bigcup_{g\in G}gHg^{-1}$，故$N(H)\neq G$，$1<|S|=[G:N(H)]\leq[G:H]$. 知$|\bigcup_{g\in G}gHg^{-1}|<|S|.|H|\leq[G:H]|H|=|G|$. 故$G\neq\bigcup_{g\in G}gHg^{-1}$. ■

31.决定S_4的2-sylow子群和3-sylow子群.

解:3-sylow子群4个：$\langle(123)\rangle,\langle(124)\rangle,\langle(234)\rangle,\langle(134)\rangle$.

2-sylow子群3个：$\{e,(1234),(1234)^2,(1234)^3,(13),(13)(1234),(13)(1234)^2,(13)(1234)^3\}$
$=\{e,(1234),(13)(24),(1432),(13),(12)(34),(24),(14)(23)\}$;

$$\{e,(1324),(12)(34),(1423),(12),(13)(24),(34),(14)(23)\}$$

以及

$$\{e,(1243),(14)(23),(1342),(14),(12)(34),(23),(13)(24)\}.$$

它们都与二面体D_4同构，如第一个令$a=(13),b=(1234)$，则$aba=(1432)=b^{-1}$. ■

32.证明不存在56阶和148阶单群.

证明: 若群G的阶为$148=37\times 2^2$，显然37-sylow子群为正规子群（也见25题），从而G不单.

若群G的阶为$56=7\times 2^3$. 若7-sylow子群不正规，则有8个，它们两两相交为$\{e\}$，故G中7阶元的个数为$8\times(7-1)=48$个，若2-sylow子群也不正规，则有7个，故G中阶为2, 4或8的元素个数至少有8个，故G中阶大于1的元素个数大于等于$8+48=56=|G|$，矛盾，故G至少有一个sylow子群正规，从而G不是单群. ■

33.设G为有限群，$N\lhd G$，P为N的一个sylow子群，$T=N(P)$是P在G中的正规化子. 证明$G=NT$.

证明: 对任意的$g\in G$，有$gPg^{-1}\leq gNg^{-1}=N$，故gPg^{-1}也是N的sylow子群，故存在$h\in N$使得$gPg^{-1}=hPh^{-1}$，从而$h^{-1}g\in T$，即$g\in hT\leq NT$，故$G=NT$. ■

34.设G为有限群，P是G的$p-$sylow子群，$N\lhd G$，证明$P\cap N$是N的$p-$sylow子群且PN/N是G/N的$p-$sylow子群.

证明: 设P'是N的$p-$sylow子群，那么存在$g\in G$，使得$gP'g^{-1}\leq P$，而$gP'g^{-1}\leq N$也是N的$p-$sylow子群且$gP'g^{-1}\leq P\cap N$，后者是$p-$群，故$P\cap N=gPg^{-1}$是N的sylow子群.

设$|G|=p^rm$，$p\nmid m$和$|N|=p^{r'}m'$，$r'\leq r, m'|m$. 那么$|P|=p^r$且$|\overline{P}|=|PN/N|=|P/P\cap N|=|P|/|P\cap N|$. 而$P\cap N$是$N$的$p-$sylow子群，故$|P\cap N|=p^{r'}$，从而$|\overline{P}|=p^{r-r'}$，由$|\overline{G}|=p^{r-r'}(\frac{m}{m'})$知$\overline{P}$是$\overline{G}$ 的$p-$sylow子群. ■

36.设p为素数，$\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$，$G=GL_n(\mathbb{F}_p)$具体写出$G$的一个$p-$sylow子群，算出他的阶以及$G$的全部$p-$sylow子群的个数.

解: 可以计算$|G|=(p^n-1)(p^n-p)\dots(p^n-p^{n-1})=p^{\frac{n(n-1)}{2}}(p^n-1)(p^{n-1}-1)\dots(p-1)$（也见第一章44题（ii）），

记$\mathcal{T}$是G中严格上三角矩阵的集合，那么$E+\mathcal{T}=\{E+T|T\in\mathcal{T}\}\subseteq G$是子群且$|E+\mathcal{T}|=|\mathcal{T}|=p^{\frac{n(n-1)}{2}}$. 故$E+\mathcal{T}$是$G$的一个$p-$sylow子群.

记$Stab(E+\mathcal{T})=\{A\in G|A(E+\mathcal{T})A^{-1}=E+\mathcal{T}\}$，那么$G$的$p-$sylow子群的个数为$|G|/|Stab(E+\mathcal{T})|$. 现计算$|Stab(E+\mathcal{T})|$，注意$A\in Stab(E+\mathcal{T})$当且仅当$A\mathcal{T}A^{-1}=\mathcal{T}$. 设这样的$A=(a_{ij})$, $A^{-1}=(b_{ij})$. 那么对任意的上三角矩阵单位E_{st}（$s<t$），有$AE_{st}A^{-1}$为严格上三角矩阵，但

$$AE_{st}A^{-1}=\begin{pmatrix} 0 & \dots & 0 & a_{1s} & 0 & \dots & 0 \\ 0 & \dots & 0 & a_{2s} & 0 & \dots & 0 \\ & \dots & & \dots & & \dots & \\ 0 & \dots & 0 & a_{ns} & 0 & \dots & 0 \end{pmatrix}.(b_{ij})=\begin{pmatrix} a_{1s}b_{t1} & a_{1s}b_{t2} & \dots & a_{1s}b_{tn} \\ a_{2s}b_{t1} & a_{2s}b_{t2} & \dots & a_{2s}b_{tn} \\ \dots & \dots & \dots & \dots \\ a_{ns}b_{t1} & a_{ns}b_{t2} & \dots & a_{ns}b_{tn} \end{pmatrix}$$

从而最后一行为0，但某个$b_{ti}\neq 0$，故$a_{ns}=0$. 由s,t的任意性且$s<t$知$a_{nj}=0$，$j=1,2,\dots,n-1$，从而对n归纳可知$a_{ij}=0$，$\forall i>j$. 即$A\in G$为上三角矩阵，反之，对任意上三角矩阵$A\in G$，显然有$A\mathcal{T}A^{-1}\subseteq\mathcal{T}$. 故$stab(E+\mathcal{T})=\{A\in G|A$为上三角矩阵$\}$，从而$|Stab(E+\mathcal{T})|=|\{A\in G|A$为对角矩阵$|.|\mathcal{T}|=p^{\frac{n(n-1)}{2}}(p-1)^n$. 所以$G$的全部$p-$sylow子群个数为$(p^n-1)(p^{n-1}-1)\dots(p-1)/(p-1)^n$. ■

38.设G为群且$|G|=p^n$（p为素数），$N\lhd G$且$|N|=p$，证明：$N<Z(G)$（中心）.

证明: 注意$Z(G)\neq\{e\}$，故归纳可知$\overline{N}$含于$\overline{G}=G/Z(G)$的中心，故对任意的$h\in N,g\in G$，有$\overline{hgh^{-1}g^{-1}}=\{e\}$，故$hgh^{-1}g^{-1}\in Z(G)$，但$gh^{-1}g\in N$，故$hgh^{-1}g^{-1}\in N\cap Z(G)$，假设$N\cap Z(G)=\{e\}$，则$hg=gh$，故$N\subseteq Z(G)$，矛盾，从而$N\cap Z(G)\neq\{e\}$，但$|N|=p$，故$N\subseteq Z(G)$. ■

40.证明任一有限群G同构于A_n的一个子群，n为一个适当的正整数.

证明: 设$|G|=m$, X是一个二元集合，并且群G平凡的作用在X上，同时考虑G在G本身上的左乘作用. 则这两个群的作用可自然导出群G在笛卡儿积(X,G)上的作用. 对每个$e\neq g\in G$，设g的阶为s，那么$s|m$，注意到$|(X,G)|=2m$，而$|(X,G)|/|\langle g\rangle|=2m/s$为偶数，从而$g$作为$S_{2m}$中元作用在笛卡儿积$(X,G)$上是偶数（$|(X,G)|/|\langle g\rangle|$）个$s-$轮换的乘积，为偶置换. 故$G$同构于$A_{2m}$的子群. ■

48.证明四元群$V=\{e,(12)(34),(13)(24),(14)(23)\}$的自同构群与$S_3$同构.

证明: 自然视S_3为S_4的子群，那么S_3中每个元π在S_4上的共轭作用σ_π（为内自同构）保持V不变，即σ_π是V的一个自同构，如果σ_π保持V中元不变，那么由$\pi(4)=4$易知π保持$\{1,2,3,4\}$中元都不动，即$\pi=e\in S_3$. 故$S_3\mapsto Aut(V)$，$\pi\to\sigma_\pi$为单射. 从而$|S_3|\leq|Aut(V)|$.

另一方面，对任意的$\phi\in Aut(V)$，有$\phi(e)=e$，故ϕ是$V\setminus\{e\}$的一个双射，若ϕ保持$V\setminus\{e\}$中元不动，则ϕ在V上恒等，即$\phi=1\in Aut(V)$. 故有单射$Aut(V)\to S_3$. 从而$|S_3|\geq|Aut(V)|$. 故上面的单射为同构，即$Aut(V)\simeq S_3$. ■

注:V同构于Klein四元群，故Klein四元群的自同构群为S_3.

49.称一个群G为完全群，如果G的中心为e且$Aut(G)\simeq Inn(G)$（内自同构群），证明S_3,S_4都是完全群.

证明: 首先易证S_n（$n\geq3$）的中心为e，故$S_n=Inn(S_n)$.

考虑S_3：对任意$\phi\in Aut(S_3)$，有ϕ保持元素的阶，而S_3中二阶元只有对换，由ϕ保持$\{(12),(23),(13)\}$，且ϕ使得每个对换不动当且仅当$\phi=1\in Aut(S_3)$（$(12),(23)$是生成元）. 故有单态$Aut(S_3)\to S_3\simeq Inn(S_3)$. 从而$Aut(G)=Inn(G)$.

考虑S_4：对任意$\phi\in Aut(S_4)$，由ϕ保持元的阶知ϕ保持所有3-轮换的集合，故$\phi(A_4)=A_4$. 从而ϕ把对换变为对换，故ϕ也保持$V=\{e,(12)(34),(13)(24),(14)(23)\}$，从而有同态$Aut(G)\to S_3$，注意$(14)=(13)(34)(13)$和$(23)=(12)(13)(12)$，故若$\phi$保持$V$中元都不动，则$\phi$ 由在$(12),(34),(13),(24)$上的作用确定,且$\phi((12)),\phi((34))\in\{(12),(34)\}$和$\phi((13)),\phi((24))$ $\{(13),(24)\}$. 可见保持V中元都不动的ϕ至多有四个，故$|Aut(G)|\leq|S_3|.4=4!$，但$S_4=Inn(S_4)<Aut(S_4)$，从而只能是$S_4\simeq Inn(S_4)=Aut(S_4)$. ■

补充:有一般性的结果:对$n\geq3$，如果$n\neq6$，那么S_n为完全群. 对于证明，先证几个引理（某些有独立意义）.

引理 1.0.1 对任意$\phi\in Aut(S_n)$，有$\phi(A_n)=A_n$.

证明: 注意ϕ保持元素的阶（当$n \le 5$时，ϕ把3-轮换映到3-轮换，故$\phi(A_n) = A_n$. 当$n > 5$时，有$\phi(A_n) \lhd S_n$，由A_n单且$|S_n/A_n| = 2$知$\phi(A_n) \cap A_n = A_n$，故$\phi(A_n) = A_n$.）而ϕ映3-轮换为不相交的3-轮换的乘积. 即$\phi(A_n) \subseteq A_n$，$\phi(A_n) = A_n$. ■

引理 1.0.2 当$n \ge 4$时，A_n在S_n中的中心化子为$\{e\}$.

证明: 设$\pi \in S_n$属于A_n的中心化子，$\pi(1, 2, \ldots, i-1, i+1, \ldots, n)\pi^{-1} = (1, 2, \ldots, i-1, i+1, \ldots, n)$，故$\pi(i) = i$，由$i$的任意性可知$\pi = \{e\}$. ■

引理 1.0.3 设$x = (abc)$和$y = (a'b'c')$是两个3-轮换，记$X = \{a, b, c\}$和$Y = \{a', b', c'\}$，考虑xy的不相交轮换分解.（1）如果$X = Y$，那么$y = (abc)$或(acb)，从而$xy = (acb)$或$\{e\}$.

（2）如果$|X \cap Y| = 2$，不妨设$\{a, b\} = \{a', b'\}$，但$c \ne c'$，那么$y = (abc')$或(bac')，从而$xy = (ac)(bc')$或$(ac'c)$.

（3）如果$|X \cap Y| = 1$，不妨设$a = a'$，但$\{b, c\} \cap \{b', c'\} = \emptyset$，那么$xy = (cbab'c')$. ■

以下设$C \subseteq S_n$是所有3-轮换的集合.

引理 1.0.4 设$n \ne 6$，$n \ge 3$，$C' \subseteq S_n$满足条件: C'对元素的共轭类封闭，C'中每个元的阶为3，并且对任意$x, y \in C'$，有xy的阶为1，2，3或5.那么$C' = C$.

证明: 当$n < 6$时，阶为3的元是3-轮换，那么$C' \subseteq C$，但C'对共轭类封闭，故$C' = C$.

当$n > 6$时，假设$C' \ne C$，那么C'中存在一个元是至少两个不相交3-轮换的乘积（因为阶为3，故C'中元是3-轮换的乘积）. 由C'对共轭类封闭，可不妨设C'中存在元$x = (253)(467)\ldots$和$y = (137)(254)\ldots$. 那么$xy = (123456\ldots)\ldots$，故$xy$的阶大于5，矛盾. 从而$C = C'$. ■

以下记$\Omega = \{1, 2, \ldots, n\}$，对$a, b \in \Omega$，且$a \ne b$，记$L(a, b) = \{(abc) | c \in \Omega \setminus \{a, b\}\}$.

引理 1.0.5 $L(a, b)$是C中满足下列条件的极大集: 对$x, y \in L(a, b), x \ne y$，有$xy$的阶为2，反之，$C$中任意满足上述条件的极大子集具有形式$L(a, b)$.

证明: 由引理1.0.3（2）知$L(a, b)$满足题中条件，设$L(a, b) \subseteq S \subseteq C$且$S$满足题中条件，若$S \ne L(a, b)$，那么存在$(a'b'c') \in S \setminus L(a, b)$，记$Y = \{a', b', c'\}$，如果$Y \cap \{a, b\} = 2$，不妨设$\{a', b'\} = \{a, b\}$，取$c = c'$，那么有$(abc) \in L(a, b) \subseteq S$且由引理1.0.3（1）知$(abc)(a'b'c')$的阶为3或1，矛盾. 如果$|Y \cap \{a, b\}| = 1$，不妨设$a' = a$，取$c = b'$，那么由引理1.0.3（2）知$(abc)(a'b'c')$的阶为3，矛盾. 如果$Y \cap \{a, b\} = \emptyset$，$c = a'$，那么由引理1.0.3（3）知$(abc)(a'b'c')$的阶为5，也矛盾，故有$S = L(a, b)$.

反之，设$S \subseteq C$是满足题中条件的极大集，设$x = (abc) \in S$，那么对$x \ne (a'b'c') \in S$，由$x(a'b'c')$的阶为2和引理1.0.3知$|\{a, b, c\} \cap \{a', b', c'\}| = 2$，不妨设$\{a, b\} = \{a', b'\}$，那么进一步知$(a'b'c') = (abc') \in L(a, b)$，即$a' = a, b' = b$. 记$y = (a'b'c') \in S$. 那么对任

意$z=(a''b''c'')\in S$，设$z\neq x$，$z\neq y$. 那么类似有$|\{a,b,c\}\cap\{a'',b'',c''\}|=2=|\{a',b',c'\}\cap\{a'',b'',c''\}|$，假设$c\in\{a'',b'',c''\}$，不妨设$c''=c$，那么$|\{a,b\}\cap\{a'',b''\}|=1$，如果$a=a''$，即$z=(ab''c)$，由$c\notin\{a,b,c'\}$知$b''=b$或$c'$，由$z\neq x$知$z=(ac'c)$，那么$yz=(abc')(ac'c)$，阶为5，矛盾. 如果$a=b''$，则$z=(a''bc)$，那么$xz$的阶为5，也矛盾. 故$c\notin\{a'',b'',c''\}$，故$\{a,b\}\subseteq\{a'',b'',c''\}$，不妨设$\{a,b\}=\{a'',b''\}$，由$xz$阶为2又知$z=(abc'')$，可见$S\subseteq L(a,b)$，由$S$的极大性知$S=L(a,b)$. ■

引理 1.0.6 当$n\geq 4$时，对$\phi\in Aut(S_n)$，如果$\phi|_{A_n}=1$，则$\phi=1$.

证明: 对任意的$y\in S_n$和$x\in A_n$，有$yxy^{-1}\in A_n$. 故$yxy^{-1}=\phi(yxy^{-1})=\phi(y)x\phi(y)^{-1}$，从而$y^{-1}\phi(y)$属于$A_n$在$S_n$的中心化子，由引理1.0.2知$\phi(y)=y$，故$\phi=1$. ■

引理 1.0.7 对任意的$a,b\in\Omega$，A_n由$L(a,b)$生成.

证明: 由A_n中元对共轭类封闭，可不妨设$a=1,b=2$，对n归纳，即设A_{n-1}由$L(1,2)\cap A_{n-1}$生成，注意A_n由3-轮换生成，考虑(i,j,n)，若$\{i,j\}=\{1,2\}$，由$(12n)\in L(1,2)$和$(21n)=(12n)^2\in L(1,2)$知$(i,j,n)\in\langle L(1,2)\rangle$，若$|\{i,j\}\cap\{1,2\}|=1$，如果$i=1$，那么$(1jn)=(1n)(1j)=(n1)(12)(21)(1j)=(12n)(21j)\in\langle L(1,2)\rangle$. 如果$i=2$，那么$(2jn)=(n2)(2j)=(n2)(21)(12)(2j)=(21n)(12j)\in\langle L(1,2)\rangle$. 即有$(ijn)\in\langle L(1,2)\rangle$，可见总有$(ijn)\in\langle L(1,2)\rangle$，故$A_n=\langle L(1,2)\rangle$. ■

定理 1.0.8 当$n\geq 3$，且$n\neq 6$时，S_n是完全群.

证明: 注意S_n的中心总是$\{e\}$，故只需证对任意的$\phi\in Aut(S_n)$，ϕ是内自同态，$n=3$时易直接证（见49第一部分的证明）. 设$n\geq 4$且$n\neq 6$. 由C对共轭类封闭知$\phi(C)$也对共轭类封闭且满足引理1.0.4的条件，故$\phi(C)=C$，任取$L(a,b)\subseteq C$是满足引理1.0.5中条件的极大集，故$\phi(L(a,b))=L(a',b')$，令$\pi\in S_n$使得$\pi(a)=a'$，$\pi(b)=b'$. 且对任意的$c\in\Omega\setminus\{a,b\}$，若$\phi((abc))=(a'b'c')$，则$\pi(c)=c'$. 于是$\phi((abc))=\pi(abc)\pi^{-1}=\sigma_\pi((abc))$，$\forall(abc)\in L(a,b)$. 故$\phi^{-1}\sigma_\pi$在$\langle L(a,b)\rangle=A_n$上恒等，故由引理1.0.6可知$\phi^{-1}\sigma_\pi=1$，即$\phi=\sigma_\pi\in Inn(S_n)$. ■

注: 结论对$n=6$不成立，实际上有$Aut(S_6)/Inn(S_6)$的阶为2.（见[J.D.Dixon, B.Mortimer, Permutation Groups. P261练习8.2.5]）

50.设G为非交换单群，证明$Aut(G)$是完全群.

证明: 注意$Inn(G)=\{\sigma_a|a\in G\}\lhd Aut(G)$，且由$G$非交换单知$G\to Inn(G),a\mapsto\sigma_a$是同构，故$Inn(G)$是非交换单群. 任取$\Phi\in Aut(Aut(G))$，有$\Phi(Inn(G))$也是$Aut(G)$的正规子群，注意$Inn(G)$在$Aut(G)$中的中心化子为恒等变换和下面的引理，故$\Phi(Inn(G))=Inn(G)$，于是存在映射$\alpha:G\to G$使得若$\Phi(\sigma_a)=\sigma_{a'}$，则$\alpha(a)=a'$. 易知$\alpha$是群同构，即$\alpha\in Aut(G)$，故$\Phi(\sigma_a)=\alpha\sigma_a\alpha^{-1}=\Sigma_\alpha(\sigma_a)$，其中$\Sigma_\alpha$是$Aut(G)$上的内自同构，于是对于任意的$\beta\in Aut(G)$和$a\in G$，有$\sigma_{(\Phi(\beta)\alpha)(a)}=\Phi(\beta)\sigma_{\alpha(a)}\Phi(\beta)^{-1}=\Phi(\beta)\Phi(\sigma_a)\Phi(\beta)^{-1}=$

$\Phi(\beta\sigma_a\beta^{-1}) = \Phi(\sigma_{\beta(a)}) = \sigma_{\alpha\beta(a)}$ 从而$\Phi(\beta)\alpha(a) = \alpha\beta(a)$. 由$a$的任意性知$\Phi(\beta)\alpha = \alpha\beta$. 故$\Phi(\beta) = \Sigma_\alpha(\beta)$. 又由$\beta$的任意性知$\Phi = \Sigma_\alpha \in Inn(Aut(G))$，故$Inn(Aut(G)) = Aut(Aut(G))$.
■

引理 1.0.9 设G是群，如果$\phi \in Aut(G)$属于$Inn(G)$的中心化子，那么对任意的$a \in G$，有$a^{-1}\phi(a)$属于G 的中心，特别地，如果G的中心为$\{e\}$，那么$Inn(G)$在$Aut(G)$中的中心化子为恒等映射.

证明: 由$\phi\sigma_a = \sigma_a\phi$知$\sigma = \sigma_{\phi(a)}$，即$\sigma_{a^{-1}\phi(a)}$ =恒等. 故$a^{-1}\phi(a)$属于G的中心. ■

51.证明不存在群G使得$G > S_4$，且$G^{(1)} = S_4$.
证明: 假设上述群G存在，设$Z = \{g \in G|gx = xg, \forall x \in S_4\}$，即$S_4$在$G$中的中心化子. 注意$S_4 = G^{(1)} \lhd G$，故对任意$g \in G$，和$x \in S_4$有$gxg^{-1} \in S_4$，故$\sigma_g|_{S_4}$是$S_4$的自同构. 由49题的结果知存在$a \in S_4$，使得$\sigma_g|_{S_4} = \sigma_a|_{S_4}$. 故对任意的$x \in S_4$，有$gxg^{-1} = axa^{-1}$，故$a^{-1}g \in Z$，从而$g \in S_4Z$. 即$G = S_4Z$，于是$G^{(1)} = S_4^{(1)} = A_4$，矛盾. ■

56.证明阶为60的单群与A_5同构，而阶小于60的群为可解群.
证明: 设G是阶60的单群. 注意$60 = 2^2 \cdot 3 \cdot 5$. 故G的5-sylow子群的个数为6, 3-sylow子群的个数只能是4或10. 假设为4个，因为3-sylow子群彼此共轭，所以G共轭作用在所有3-sylow子群组成的集合上并且该作用迁移，从而$60 = |G|\,||S_4| = 4! = 24$矛盾. 故$G$的3-sylow子群的个数为10个，于是$G$中阶为1,3,5的元素个数共为$1 + (3-1) \times 10 + (5-1) \times 6 = 45$个. 设$X = \{g \in G|g$的阶不为1,3或5$\}$. 那么$|X| = 60 - 45 = 15$. 任取$x \in X$, 由$G$为单群且不交换(因为阶不是素数)知$x$不是中心元，故$x$所在的共轭类$[x]$中的元素个数大于1，从而由$G$共轭迁移作用在$[x]$上知$|[x]| \geq 5$. 如果$|[x]| = 5$，那么$G$到$S_5$有单同态，从而由$|S_5|/|G| = 2$知$G$可视为$S_5$的正规子群并且易知只能有$G \cap A_5 = G$, 故$G = A_5$. 注意也有$|[x]|$整除$|G|$. 如果$x$中每个元所在的共轭类中的元素个数都大于5，那么$X$中元只有一个共轭类，即$X = [g]$. 但$G$中有2阶元，故可设$y$的阶为2. 现在$G$共轭迁移作用在$X$上，故$stab(y) = 4$. 如果$S$是包含$y$的2-sylow, 注意$S$交换，那么$S \subseteq stab(y)$,从而$S = stab(y)$. 由此易知任意两个不同的2-sylow子群之交为$\{e\}$(否则它们有一个公共的2阶元属于X，它们都是这个2阶元的稳定化子，从而相等，矛盾.)但每个2-sylow含于$X \cup \{e\}$. 而不同的2-sylow子群的个数≥ 5, 从而只能有5个2-sylow子群，由G共轭迁移作用在2-sylow子群的集合上知也有G到S_5有单同态，故类似于上面知也有$G \simeq A_5$.

现在设G是阶小于60的群，下面证明G可解. 对$|G|$归纳，只需证G不是单群. 可设G不是$p-$群（否则G已经可解）. 也由24和25题可设G不具有形式pq或$p^2q(p, q$为不同的素数). 故G的素因子只能是7,5,3,2. 假设G是单群，如果$7||G|$, 那么$|G| = 7m, (1 < m \leq 8)$且$(7, m) = 1$. 若$m = 8$, 那么G的7-sylow子群的个数为8，从而7阶元的个数为$(7-1) \times 8 = 48$个. 从而阶不为1或7的元的个数为56-48-1=7，这些元所在的共轭类中的元的个数≥ 7, 故只能是7. 从而阶不为1或7的元只有一个共轭类且阶为2，即知每个2-sylow子群中的元的阶都为2，且G中阶为2的元的个数为7，可见至多有2个2-sylow子

群，但2个不可解，故只有一个2-sylow子群，正规，矛盾．若$m<8$，则7-sylow子群正规，矛盾．如果$|G|=5m$, $1<m$, $5\nmid m$且m的素因子只能为3或2，于是只有两种情形：$m=8$或$m=6$. 若$m=6$, 则5-sylow子群的个数为6个，而3-sylow子群的个数为10个，从而元素阶为1,3或5的元素的个数为$1+(3-1)\times 10+(5-1)\times 6=1+20+24>30$, 矛盾．若$m=8$, 则5-sylow子群的个数只有一个，故正规，也矛盾．故$|G|=3^j\cdot 2^i, j>1, i>1$. 若$|G|=3^3\cdot 2$, 则3-sylow子群正规，矛盾．若$|G|=3^2\cdot 2^2$, 则3-sylow子群个数为4，于是$G$到$S_4$有单同态，故$3^2||S_4|=4!$, 矛盾．若$|G|=3\cdot 2^i, i>2$, 则2-sylow子群个数为3，于是$G$到$S_3$有单同态，故$3\cdot 2^i|3!$, 矛盾．综上讨论知，若$G$的阶小于60，那么$G$可解．■

57. 证明：若群G有限生成，则它的指数有限的子群也是有限生成的．

证明： 设$G=\cup_{i=1}^m a_iH$,左陪集可解．$G=<g_1,\cdots,g_n>$. 记$K=<a_j^{-1}g_ia_k\in H>\subseteq H$. 现证反包含．任取$h\in H$, 那么$h=g_{i_1}g_{i_2}\cdots g_{i_s}$. 设$g_{i_s}\in a_iH$, 于是$a_i^{-1}g_{i_s}\in K$, 记$k'=(a_i^{-1}g_{i_s})^{-1}\in K$, 那么$hk'=g_{i_1}g_{i_2}\cdots g_{i_{s-1}}a_i$. 归纳可知存在$k''\in K$和$a_j$, 使得$hk'k''=g_{i_1}a_j$, 从而$g_{i_1}a_j\in K$, 故$h\in K$, 故$H=K$为有限生成．■

二．环论

•[丁-聂]第三章习题选．

1. 证明：在环R内，若$1-ab$有逆，则$1-ba$有逆．

证明： 由$b(1-ab)=b-bab=(1-ba)b$知$ba=(1-ba)b(1-ab)^{-1}a$. 从而直接计算可得$(1-ba)(1+b(1-ab)^{-1}a)=1$. 可见$1-ba$有逆$1-b(1-ab)^{-1}a$.

注：”设A,B是复数域C上的矩方阵，那么λ为AB的特征值$\Leftrightarrow\lambda$为BA的特征值“可由上述结论得到．

2.设环R中元u有右逆，证明下面三条等价：

(1)u有多于一个的右逆

(2)u是一个左零因子．

(3)u不是单位．

证明: $(1)\Rightarrow(2)\Rightarrow(3)$易得，现证$(3)\Rightarrow(1)$.设$x$是$u$的一个右逆，由$u$不是单位知$xu-1\neq 0$, 从而$xu-1+x\neq x$, 但$u(xu-1+x)=uxu-u+ux=ux=1$. 故$u$有多于一个的右逆.■

3. 在环R中，若元素u有多于一个的右逆，则u有无穷多个右逆．

证明: 设x是u的一个右逆，则$(xu-1)u^i+x$也是u的右逆，假如u的右逆个数有限，那么存在$i\neq j$，使得$(xu-1)u^i+x=(xu-1)u^j+x$, 即$(xu-1)u^i=(xu-1)u^j$. 不妨设$i>j$，则右乘x^j得$(xu-1)u^{i-j}=xu-1$, 注意$(xu-1)x=0$, 故再右乘x^{i-j}得$xu-1=0$. 故u是单位，从而右逆只有一个，矛盾.■

群，但2个不可解，故只有一个2-sylow子群，正规，矛盾. 若$m<8$，则7-sylow子群正规，矛盾. 如果$|G|=5m$, $1<m$, $5\nmid m$且m的素因子只能为3或2，于是只有两种情形：$m=8$或$m=6$. 若$m=6$, 则5-sylow子群的个数为6个，而3-sylow子群的个数为10个，从而元素阶为1,3或5的元素的个数为$1+(3-1)\times10+(5-1)\times6=1+20+24>30$, 矛盾. 若$m=8$, 则5-sylow子群的个数只有一个，故正规，也矛盾. 故$|G|=3^j\cdot2^i, j>1, i>1$. 若$|G|=3^3\cdot2$, 则3-sylow子群正规，矛盾. 若$|G|=3^2\cdot2^2$, 则3-sylow子群个数为4，于是$G$到$S_4$有单同态，故$3^2||S_4|=4!$, 矛盾. 若$|G|=3\cdot2^i, i>2$, 则2-sylow子群个数为3，于是$G$到$S_3$有单同态，故$3\cdot2^i|3!$, 矛盾. 综上讨论知，若$G$的阶小于60，那么$G$可解. ■

57. 证明：若群G有限生成，则它的指数有限的子群也是有限生成的.
证明: 设$G=\cup_{i=1}^{m}a_iH$,左陪集可解. $G=<g_1,\cdots,g_n>$. 记$K=<a_j^{-1}g_ia_k\in H>\subseteq H$. 现证反包含. 任取$h\in H$, 那么$h=g_{i_1}g_{i_2}\cdots g_{i_s}$. 设$g_{i_s}\in a_iH$, 于是$a_i^{-1}g_{i_s}\in K$, 记$k'=(a_i^{-1}g_{i_s})^{-1}\in K$, 那么$hk'=g_{i_1}g_{i_2}\cdots g_{i_{s-1}}a_i$. 归纳可知存在$k''\in K$和$a_j$, 使得$hk'k''=g_{i_1}a_j$, 从而$g_{i_1}a_j\in K$, 故$h\in K$, 故$H=K$为有限生成. ■

二. 环论

•[丁-聂]第三章习题选.

1. 证明：在环R内，若$1-ab$有逆，则$1-ba$有逆.
证明: 由$b(1-ab)=b-bab=(1-ba)b$知$ba=(1-ba)b(1-ab)^{-1}a$. 从而直接计算可得$(1-ba)(1+b(1-ab)^{-1}a)=1$. 可见$1-ba$有逆$1-b(1-ab)^{-1}a$.
注：" 设A,B是复数域C上的矩方阵，那么λ为AB的特征值$\Leftrightarrow\lambda$为BA的特征值"可由上述结论得到.

2.设环R中元u有右逆，证明下面三条等价：

(1)u有多于一个的右逆

(2)u是一个左零因子.

(3)u不是单位.

证明: $(1)\Rightarrow(2)\Rightarrow(3)$易得，现证$(3)\Rightarrow(1)$.设$x$是$u$的一个右逆，由$u$不是单位知$xu-1\neq0$, 从而$xu-1+x\neq x$, 但$u(xu-1+x)=uxu-u+ux=ux=1$. 故$u$有多于一个的右逆.■

3. 在环R中，若元素u有多于一个的右逆，则u有无穷多个右逆.
证明: 设x是u的一个右逆，则$(xu-1)u^i+x$也是u的右逆，假如u的右逆个数有限，那么存在$i\neq j$，使得$(xu-1)u^i+x=(xu-1)u^j+x$, 即$(xu-1)u^i=(xu-1)u^j$. 不妨设$i>j$，则右乘x^j得$(xu-1)u^{i-j}=xu-1$, 注意$(xu-1)x=0$, 故再右乘x^{i-j}得$xu-1=0$. 故u是单位，从而右逆只有一个，矛盾.■

证明：设C_R是R在D中的中心化子，即$C_R = \{d \in D | dr = rd, \forall r \in R\}$,则$C_R$是$D$的一个子体(且$C \subseteq C_R$). 并且$R \subseteq C$当且仅当$C_R = D$.下面证明$D = R \cup C_R$, 从而$D = R$或$D = C_R$(故$R \subseteq C$). 任取$a \in D$, 若$a \notin R$,对任意的$0 \neq b \in R$,则由55题和$R$的正规性知$R \ni ((a-b^{-1})^{-1} - a^{-1})b(aba - a) = ((a-b^{-1})^{-1} - a^{-1})b(a-b^{-1})ba = (a-b^{-1})^{-1}b(a-b^{-1})ba - a^{-1}baba + a^{-1}ba = ((a-b^{-1})^{-1}b(a-b^{-1}) - a^{-1}ba)ba + a^{-1}ba$. 故$((a-b^{-1})^{-1}b(a-b^{-1}) - a^{-1}ba)ba \in R$. 注意$(a-b^{-1})b(a-b^{-1}) - a^{-1}ba \in R$. 若它不为0，则由$b \in R$知有$a \in R$,矛盾. 故只能有$(a-b^{-1})b(a-b^{-1}) - a^{-1}ba = 0$，即$(a-b^{-1})b(a-b^{-1}) = a^{-1}ba$，也即$b(1-b^{-1}a^{-1}) = (1-b^{-1}a^{-1})b$, 故$b - a^{-1} = b - b^{-1}a^{-1}b$, 从而$a^{-1} = b^{-1}a^{-1}b$. 故$ba^{-1} = a^{-1}b$. 即$ab = ba$. 由$0 \neq b \in R$的任意性知$a \in C_R$. 这就证明了$D = R \cup C_R$.■

注：H. Cartan对可除代数证明了上述结果. 证明复杂，用到了Galois理论，华的证明非常简单，只用了半页纸，(利用上述55题结论)，贝特曼用莎士比亚的≪罗密欧与朱丽叶≫中的一句诗句来赞美华的这一精妙的证明:“没有一口井那么深，也没有教堂门那么宽，绿茂丘两奥的伤口一样致命呀!”

12. 设S是四元数体H的子体.若对$\forall 0 \neq d \in H$都有$dSd^{-1} \subset S$, 则$S = H$或$S \subseteq R$(H的中心)。

证明: 证一：利用56题直接可得。

证二: 设$S \nsubseteq R$. 那么存在$\alpha = a+bi+cj+dk \notin R$, 不妨设$b \neq 0$, 注意$i^{-1} = -i$且$iji = j, iki = k$,于是由$i\alpha i^{-1} = a+bi-cj-dk \in S$,故$2(a+bi) \in S$, 从而$a+bi \in S(\because 2 \in S)$,于是又有$j(a+bi)(-j) = a-bi \in S$. 故$bi \in S$. 注意$(bi)^{-1} = -ib^{-1}$, 故对任意的$a, b \in R$, 由$(a_1+b_1j)^{-1} = \frac{a_1-b_1j}{a_1^2+b_1^2}$知$\frac{-b^{-1}i(a_1+b_1j)bi(a_1-b_1j)}{a^2+b^2} = \frac{(a_1-b_1j)^2}{a_1^2+b_1^2} = \frac{a_1^2-b_1^2-2a_1b_1j}{a_1^2+b_1^2} \in S$. 类似于上面的证明知$\frac{2a_1b_1}{a_1^2+b_1^2}j \in S$. 由$a_1, b_1 \in R$的任意性易知对$\forall x \in R, -1 \leq x \leq 1$, 有$xj \in S$. 故对$\forall y \in R$, 有$y_j \in S$, 即$Rj \subseteq S$. 同理$Rk \subseteq S$. 从而$R = (Rj)^2 \subseteq S, Ri = RjRk \subseteq S$,故$H \subseteq S$. ■

31. 设p为素数，n为整数，$R = \mathbb{Z}/(p^n)$, 试具体指出多项式环$R[x]$中那些是单位，零因子或幂零元。

解：先考虑幂零元。注意在交换环中幂零元的和还是幂零元。故对$f(x) \in R[x]$, 若$f(x)$的系数幂零，则$f(x)$幂零。反之，若$f(x)$幂零，则易知$f(x)$的最高次项a_mx^m幂零，故a_m幂零。从而$f(x) - a_mx^m$也幂零。对次数归纳可知$f(x)$的所有系数都幂零。即$I = \{f(x) \in R[x] | f(x)\text{的所有系数幂零}\}$是$R[x]$中所有幂零元的集合。

令$F = \mathbb{Z}/(p)$，则有自然的环满同态$\varphi: R[X] \twoheadrightarrow F[x], \Sigma a_ix^i \mapsto \Sigma\overline{a_i}x^i$. 且易知$ker\varphi = I$, 注意$F[x]$中的单位为$F^*$. 故易知$R[x]$中单位全体为$\{\overline{m} + f(m) | m = 1, 2, \cdots, p-1, f(x) \in I\}$. 另外，由同构$R[x]/I \simeq F[x]$ 知$R[x]$中零因子也为I. ■

15. 在域F上$n \times n(n > 1)$全矩阵环$M_n(F)$内寻找一个子环R使得R除了恒等同构而外没有其他反自同构。

解：令$R = \mathbb{Z}E$, 其中E为n阶单位矩阵。那么由自同构保持单位元知R的同构只有

恒等同构。由R交换知R也没有其他反自同构。■

注：该题的本意可能是另外的意思，即$M_n(F)$内寻找一个子环R使得R没有反自同构。这个结果在当$F \neq \mathbb{Z}\cdot 1$时成立。证明如下：

令$R = \begin{pmatrix}\mathbb{Z}\cdot 1 & F \\ 0 & F\end{pmatrix}$，是$M_2(F)$的子环，假如$R$有反自同构$\varphi$，由$\varphi$保持幂零元知$\varphi(\begin{pmatrix}0 & a \\ 0 & 0\end{pmatrix}$ $\begin{pmatrix}0 & x_a \\ 0 & 0\end{pmatrix}$. 令$\varphi(\begin{pmatrix}0 & 0 \\ 0 & y\end{pmatrix}) = \begin{pmatrix}l_y\cdot 1 & b_y \\ 0 & c_y\end{pmatrix}$，其中$l_y$为整数，那么$\begin{pmatrix}0 & x_a \\ 0 & 0\end{pmatrix} = \varphi(\begin{pmatrix}0 & 1 \\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & 0 \\ 0 & a\end{pmatrix})$ $\begin{pmatrix}l_a & b_a \\ 0 & c_a\end{pmatrix}\begin{pmatrix}0 & x_1 \\ 0 & 0\end{pmatrix} = \begin{pmatrix}0 & l_a x_1 \\ 0 & 0\end{pmatrix}$. 故$l_1 = 1$.

如果$\mathbb{Z}\cdot 1$有限，那么$\exists 0 \neq y \in F$使得$l_y \cdot 1 = 1$.故得$l_1 \cdot 1 = 0$.矛盾。

如果$\mathbb{Z}\cdot 1$无限，那么对$\forall x, y \in F$,易知$l_{xy} = l_x l_y$且$l_1 = 1$. 特别的，$l_x^{-1} = l_{x^{-1}}$为整数，从而$l_x = \pm 1, \forall 0 \neq x \in F$. 故也存在$0 \neq y \in F$使得$l_y = 0$.故$l_1 = 0$. 矛盾。这就说明了$R$没有反自同构。对一般的$n > 1$,令$R = \{\begin{pmatrix} m\cdot 1 & b & 0 & \cdots & 0 \\ 0 & a & 0 & \cdots & 0 \\ 0 & 0 & a & \cdots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & a\end{pmatrix} | a, b, m \in \mathbb{Z}\}$那么这个$R$与$n = 2$时的$R$环同构，故也没有反自同构。■

注：对$\begin{pmatrix}F & F \\ 0 & F\end{pmatrix}$总有反自同构$\begin{pmatrix}a & c \\ 0 & b\end{pmatrix} \mapsto \begin{pmatrix}b & c \\ 0 & a\end{pmatrix}$.

三. 整环

•[聂-丁]第四章习题选.

3. 设D是主理想整环R，且F是D的商域，设$D' \supseteq D$是F的子环，那么D'也是主理想整环且是D的一个分式环，反之，D的任一分式环是F的子环，从而是主理想整环.

证明： 首先证明，对$s, d \in D$且s与d互素，如果$s^{-1}d \in D'$, 那么$s^{-1} \in D'$.实际上，由D为主理想整环知存在$u, v \in D$,使得$1 = du + sv$, 故$s^{-1} = s^{-1}du + v \in D'$. 现在，设$I$是$D'$的理想，那么易知$I \cap D$是$D$的理想，从而$I \cap D = Da (a \in D)$. 对任意$x = s^{-1}d \in I$,其中$s, d \in D$互素，有$d \in I \cap D$,故$d = ba, b \in D$. 于是$x = s^{-1}ba$.由上面已证的结论知$s^{-1} \in D'$且$b \in D \subseteq D'$,故$s^{-1}b \in D'$.从而$x \in D'a$. 于是$I = D'a$为主理想. 另外，记$S = \{0 \neq s \in D | s^{-1} \in D'\}$,显然为$D$的一个乘法子集，且$s^{-1}D \subseteq D'$. 对$\forall y \in D'$,有$y = s^{-1}d, s, d \in D$且互素，故$s^{-1} \in D'$.从而$y \in s^{-1}D$,故$s^{-1}D = D'$.■

9.证明$\mathbb{Z}[x]$的任一主理想不极大.

证明： 设$f(x) \neq \pm 1$, 且$f(x) \neq 0$((0)显然不极大！)，若$f(x) = a$为常数，显然$(a) \subsetneq (a, x) \subsetneq \mathbb{Z}[x]$,如果$f(x)$不是常数，那么存在$n \in \mathbb{Z}$使得$f(n) \neq \pm 1, f(n) \neq 0$,显然$f(n) \notin (f(x))$,从而$(f(x)) \subsetneq (f(n), f(x))$, 又易知$1 \notin (f(n), f(x))$, (否则$f(n) | 1$), 故$f(x)$不极大.

恒等同构。由R交换知R也没有其他反自同构。■

注：该题的本意可能是另外的意思，即$M_n(F)$内寻找一个子环R使得R没有反自同构。这个结果在当$F \neq \mathbb{Z}\cdot 1$时成立。证明如下：

令$R = \begin{pmatrix} \mathbb{Z}\cdot 1 & F \\ 0 & F \end{pmatrix}$，是$M_2(F)$的子环，假如$R$有反自同构$\varphi$，由$\varphi$保持幂零元知$\varphi(\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$
$\begin{pmatrix} 0 & x_a \\ 0 & 0 \end{pmatrix}$. 令$\varphi(\begin{pmatrix} 0 & 0 \\ 0 & y \end{pmatrix}) = \begin{pmatrix} l_y\cdot 1 & b_y \\ 0 & c_y \end{pmatrix}$，其中$l_y$为整数，那么$\begin{pmatrix} 0 & x_a \\ 0 & 0 \end{pmatrix} = \varphi(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}) =$
$\begin{pmatrix} l_a & b_a \\ 0 & c_a \end{pmatrix}\begin{pmatrix} 0 & x_1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & l_a x_1 \\ 0 & 0 \end{pmatrix}$. 故$l_1 = 1$.

如果$\mathbb{Z}\cdot 1$有限，那么$\exists 0 \neq y \in F$使得$l_y \cdot 1 = 1$.故得$l_1 \cdot 1 = 0$.矛盾。

如果$\mathbb{Z}\cdot 1$无限，那么对$\forall x, y \in F$,易知$l_{xy} = l_x l_y$且$l_1 = 1$. 特别的，$l_x^{-1} = l_{x^{-1}}$为整数，从而$l_x = \pm 1, \forall 0 \neq x \in F$. 故也存在$0 \neq y \in F$使得$l_y = 0$.故$l_1 = 0$. 矛盾。这就说明了$R$没有反自同构。对一般的$n > 1$,令$R = \{\begin{pmatrix} m\cdot 1 & b & 0 & \cdots & 0 \\ 0 & a & 0 & \cdots & 0 \\ 0 & 0 & a & \cdots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & a \end{pmatrix} | a, b, m \in \mathbb{Z}\}$那么这个$R$与$n = 2$时的$R$环同构，故也没有反自同构。■

注：对$\begin{pmatrix} F & F \\ 0 & F \end{pmatrix}$总有反自同构$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \mapsto \begin{pmatrix} b & c \\ 0 & a \end{pmatrix}$.

三. 整环

•[聂-丁]第四章习题选.

3. 设D是主理想整环R，且F是D的商域，设$D' \supseteq D$是F的子环，那么D'也是主理想整环且是D的一个分式环，反之，D的任一分式环是F的子环，从而是主理想整环.

证明: 首先证明，对$s, d \in D$且s与d互素，如果$s^{-1}d \in D'$, 那么$s^{-1} \in D'$.实际上，由D为主理想整环知存在$u, v \in D$,使得$1 = du + sv$, 故$s^{-1} = s^{-1}du + v \in D'$. 现在，设$I$是$D'$的理想，那么易知$I \cap D$是$D$的理想，从而$I \cap D = Da(a \in D)$. 对任意$x = s^{-1}d \in I$,其中$s, d \in D$互素，有$d \in I \cap D$,故$d = ba, b \in D$. 于是$x = s^{-1}ba$.由上面已证的结论知$s^{-1} \in D'$且$b \in D \subseteq D'$,故$s^{-1}b \in D'$.从而$x \in D'a$. 于是$I = D'a$为主理想. 另外，记$S = \{0 \neq s \in D | s^{-1} \in D'\}$,显然为$D$的一个乘法子集，且$s^{-1}D \subseteq D'$. 对$\forall y \in D'$,有$y = s^{-1}d, s, d \in D$且互素，故$s^{-1} \in D'$.从而$y \in s^{-1}D$,故$s^{-1}D = D'$.■

9.证明$\mathbb{Z}[x]$的任一主理想不极大.

证明: 设$f(x) \neq \pm 1$, 且$f(x) \neq 0$((0)显然不极大！)，若$f(x) = a$为常数，显然$(a) \subsetneq (a, x) \subsetneq \mathbb{Z}[x]$,如果$f(x)$不是常数，那么存在$n \in \mathbb{Z}$使得$f(n) \neq \pm 1, f(n) \neq 0$,显然$f(n) \notin (f(x))$,从而$(f(x)) \subsetneq (f(n), f(x))$, 又易知$1 \notin (f(n), f(x))$, (否则$f(n)|1$), 故$f(x)$不极大.

14. 设p为奇素数，证明：在$\mathbb{Z}$内，$x^2\equiv -1(mod\ p)$有解$\Leftrightarrow p\equiv 1(mod\ 4)$.

证. "$\Rightarrow$" 设$p=2n+1$,且存在$a\in\mathbb{Z}$使得$a^2\equiv -1(mod\ p)$. 但$1\equiv a^{p-1}=a^{2n}\equiv(-1)^n(mod\ p)$. 可见$n$是偶数，即$p\equiv 1(mod\ 4)$.

"$\Leftarrow$" 设$p=4m+1$,故对任意使得$p\nmid a$的$a\in\mathbb{Z}$,有$a^{4m}=a^{p-1}\equiv 1(modp)$，故$(a^{2m}-1)(a^{2m}+1)\equiv 0(modp)$.在$\mathbb{F}_p=\mathbb{Z}/\mathbb{Z}p$中，$x^{2m}-1$的根至多有$2m<4m=p-1$个。故存在某个$a\in\mathbb{Z}$,使得$p|a$且$a^{2m}\equiv 1(mod\ p)$, 故$a^{2m}\equiv -1(mod\ p)$.可见$a^m$是$x^2\equiv -1(mod\ p)$的解.■

16. 设p是素数，证明：

(i).若$p\equiv 1(mod\ 4)$, 则p在$R_{-1}=\mathbb{Z}\sqrt{-1}$内可分解为两个共轭的既约元的乘积，从而$p$是两个整数的平方和.

(ii).若$p\equiv -1(mod\ 4)$, 则p在R_{-1}既约.

(iii).z在R_{-1}内与一个既约元的平方和相伴. 即$z=(1+\sqrt{-1})(1-\sqrt{-1})=-\sqrt{-1}(1+\sqrt{-1})^2$，其中$1+\sqrt{-1}$既约.

证明: 注意R_{-1}的单位为$\pm 1,\pm\sqrt{-1}$.

(i)假如p在R_{-1}中既约，由R_{-1}是主理想整环(因为是Euclid环)知p是素元，p在R_{-1}中生成的理想(p)是R_{-1}中的极大理想. 从而$\overline{R_{-1}}=R_{-1}/(p)$是域. 由上面14题知存在整数$n$，使得在$\overline{R_{-1}}$中有$\overline{n}^2=\overline{-1}$,而$\overline{\sqrt{-1}}^2=\overline{-1}$在$\overline{R_{-1}}$中也成立，故在$\overline{R_{-1}}$有$(\overline{n}-\overline{\sqrt{-1}})(\overline{n}+\overline{\sqrt{-1}})=0$，故$\overline{n-\sqrt{-1}}=0$或$\overline{n+\sqrt{-1}}=0$.即存在$a+b\sqrt{-1}\in R_{-1}$(即$a,b\in\mathbb{Z}$)使得$n-\sqrt{-1}=p(a+b\sqrt{-1})$),于是$p|1$, 矛盾，故知$p$在$R_{-1}$中可约，于是$p=\alpha_1\alpha_2\cdots\alpha_r,\alpha_i\in R_{-1}$为既约元. 考虑范数知$p^2=N(P)=N(\alpha_1)\cdots$可见$r=2$, 又考虑共轭$p=\overline{p}=\overline{\alpha_1\alpha_1}$.由此也知$p$是两个整数的平方和.

(ii)若p可约，类似于(i)的证明可知$p=a^2+b^2,a,b\in\mathbb{Z}$，由$p$奇数，不妨设$a=2n,b=2m+1$, 则$p=4n^2+4m^2+4m+1$, 与$p\equiv -1(mod\ 4)$矛盾.

(iii)只需证$1+\sqrt{-1}$既约，但$N(1+\sqrt{-1})=1+1=2$是素数，故$1+\sqrt{-1}$既约.

注：本题的目标是刻画R_{-1}的所有既约元，具体结果如下：$\alpha=a+b\sqrt{-1}\in R_{-1}$既约$\Leftrightarrow$下列之一成立：

$(i)ab\neq 0$且$N(\alpha)=p$为素数,此时$p=2$或者$p\equiv 1(mod\ 4)$.

$(ii)\alpha=\pm p$或$\pm\sqrt{-1}$,此时p为素数且$p\equiv -1(mod\ 4)$. (在这种情况之下，$N(\alpha)=p^2$)

证明: "$\Leftarrow$" 显然. "$\Rightarrow$"注意$N(\alpha)=p$或p^2, p为某个素数，$N(\alpha)=p^2$.即$\alpha\overline{\alpha}=p^2$. 由唯一分解性知$p\sim\alpha$. 但$R_{-1}$的单位是$\pm 1$和$\pm\sqrt{-1}$,故$a$与$b$之一为0，此时$\alpha$只能是$(ii)$中的形式，这也说明，如果$ab\neq 0$,则$N(\alpha)=p$.■

25.在$R_{10}=\mathbb{Z}[10]$中证明：

(i) $\varepsilon=\sqrt{10}+3$是一个单位.

(ii) R_{10}的任一单位u都可写成$\pm\varepsilon^r,r\in\mathbb{Z}$的形式.

$(iii)R_{10}$不是唯一因式分解整环.

证明: $(i)N(\varepsilon)=9-10=-1$,故$\varepsilon$是单位，但$\varepsilon^{-1}=\sqrt{10}-3$.

(ii)设$u=a+b\sqrt{10}$是单位，如果$b=1$,那么由$N(u)=\pm1$知$a^2-10=\pm1$.可见只能有$a=\pm3$, 即$u=\varepsilon$或ε^{-1},对一般的b,不妨设$b>1$(否则考虑共轭$\overline{u}$). 也不妨设$a>0$,(否则考虑$-\overline{u}$). 那么$u\varepsilon^{-1}=(-3a+10b)+(a-3b)\sqrt{10})$也是单位. 假如$|a-3b|\geq b$,则$a-3b\geq b$或$a-3b\leq -b$, 从而$a\geq 4b$或$a\leq 2b$.于是$1=N(u)=a^2-10b^2\geq 16b^2-10b^2=6b^2$或$1=N(u)=a^2-10b^2\leq 4b^2-10b^2=-6b^2$, 都是矛盾. 故$|a-3b|<b$. 如果$a-3b\geq 0$,归纳可知$u\varepsilon^{-1}=\pm\varepsilon^r$,对某个$r\in\mathbb{Z}$成立，故$u=\pm\varepsilon^{r+1}$.如果$a-3b<0$,则$-u\varepsilon^{-1}=\pm\varepsilon^r, r\in\mathbb{Z}$, 故也有$u=\pm\varepsilon^{r+1}$.

(iii)首先证明$2\in R_{10}$是既约的，实际上，假如2可约，则存在R_{10}中既约元α,使得$2=\alpha\overline{\alpha}$. 记$\alpha=a+b\sqrt{10}, a,b\in\mathbb{Z}$, 那么$2=a^2-10b^2$,显然$5\nmid a$,若$a=5a'\pm1, a'\in\mathbb{Z}$,则$2=5^2a^2\pm2\times5a'+1-10b^2$,从而$5|2-1=1$，矛盾. 若$a=5a'\pm2$,则$2=(5a')^2\pm2(5a')+4-10b^2$,从而$5|-2=2-4$,矛盾. 可见2是既约的. 注意$2\cdot5=\sqrt{10}\cdot\sqrt{10}$,而5至多有两个互为共轭的既约因子，从而左边在$R_{10}$中至多3个既约因子，因而，如果$\sqrt{10}$既约，显然上面的分解不唯一. 如果$\sqrt{10}$可约，右边至少有4个既约因子，可见分解也不唯一.

30. 设P是R_m的非零素理想，证明：

(i) $P\cap\mathbb{Z}$是$\mathbb{Z}$的非零素理想，从而存在素数p，使得$P\cap Z=\mathbb{Z}p$(且p是含于P中的唯一素数)

(ii) 商环$F=R_m/p$包含$\mathbb{F}_p=\mathbb{Z}/\mathbb{Z}p$为子域.

(iii) $F=F_p[\alpha]$,α表示陪集$\frac{1}{2}(1+\sqrt{m}+P)$按照$m\equiv 2$或$3(mod4)$或$m\equiv 1(mod4)$而定。而且$\alpha$在$F_p$上的极小多项式是$x^2-m(modP)$的因子，或是$x^2-x+\frac{1}{4}(1-m)(modP)$的因子按上述两种情况而定。总之$F$是$p$个元素或$p^2$个元素的有限整环，因而$F$是一个域。由此可知，$R_m$的任一非零素理想是极大理想。

证： (i)易知$P\cap\mathbb{Z}$是$\mathbb{Z}$的非零素理想。故$P\cap\mathbb{Z}=\mathbb{Z}$(关于非零，若$\alpha\in P,\alpha\neq 0$则$N(\alpha)=\overline{\alpha}\alpha\in P\cap\mathbb{Z}$且$N(\alpha)\neq 0$).

(ii)$\mathbb{F}_p=\mathbb{Z}/\mathbb{Z}p\cong\mathbb{Z}+P/P\subseteq R_m/P=F$.

(iii)由$\mathbb{F}_p\cong\mathbb{Z}+P/P\subset F$，易知第一个断言成立。当$m\equiv 2$ 或$3(mod4)$ 时，显然$\sqrt{m}+P$ 在$\mathbb{F}_p$上是$x^2-m(modp)$的根。当$m\equiv 1(mod4)$时，注意到$\frac{1}{4}(1-m)\in\mathbb{Z}$，故$x^2-x+\frac{1}{4}(1-m)$在$\mathbb{F}_p$上有意义。显然$\frac{1}{2}(1+\sqrt{m})$是$x^2-x+\frac{1}{4}(1-m)(modp)$的根。从而$(iii)$的断言都成立（注意$F$是整环，有限整环是域）。

31、设p是素数，p在R_m内生成的理想记为R_mp，证明：

i) $R_mp\cap\mathbb{Z}=\mathbb{Z}p$，且商环$R=R_m/R_mp$包含$\mathbb{F}_p=\mathbb{Z}/\mathbb{Z}p$为子域；

ii) $R=\mathbb{F}_p[\gamma]$，γ表示陪集$\sqrt{m}+R_mp$或陪集$\frac{1}{2}(1+\sqrt{m})+R_mp$按照$m\equiv 2$或$3(mod\ 4)$或$m=1(mod\ 4)$而定。并且在这两种情况之下，$\gamma$的极小多项式(在$\mathbb{F}_p$上)分别是$x^2-m(mod\ \mathbb{Z}p)$或$x^2-x+\frac{1}{4}(1-m)(mod\ \mathbb{Z}p)$。总之，$R$是含$p^2$个元素的有限环；

iii) 对$m\equiv 2$或$3(mod\ 4)$，设$x^2-m(mod\ \mathbb{Z}p)$可约。若

$$x^2-m\equiv(x-a)(x-b)(mod\ \mathbb{Z}p),$$

其中$a,b\in\mathbb{Z}$且$a\not\equiv b(mod\ \mathbb{Z}p)$，则$R_m$的理想

$$P_1=(p,\sqrt{m}-a),P_2=(p,\sqrt{m}-b)$$

是R_m的素理想，且$R_mp=P_1\cap P_2=P_1P_2$;

iv) 对$m\equiv 2$或$3(mod\ 4)$，设$x^2-m\equiv(x-a)^2(mod\mathbb{Z}p),a\in\mathbb{Z}$，则$P=(p,\sqrt{m}-a)$是$R_m$的素理想，且$R_mp=P^2$。这种情况仅当$p=2$或$p|m$时才能出现；

v) 对$m\equiv 2$或$3(mod\ 4)$，若$x^2-m(mod\mathbb{Z}p)$不可约，则R_mp是R_m的素理想；

vi) 对$m\equiv 1(mod\ 4)$，在情况$(iii)-(v)$中用$x^2-x+\frac{1}{4}(1-m)$替代x^2-m，结论仍然成立。此时(iv)仅当$p|m$时才能出现。因此，明显地决定了R_m的一切素理想。

证明： (i)易知对$\alpha\in R_m$，有$\alpha p\in\mathbb{Z}\Leftrightarrow\alpha\in\mathbb{Z}$。故$R_mp\cap\mathbb{Z}=\mathbb{Z}p$，于是$\mathbb{F}_p=\mathbb{Z}/\mathbb{Z}p\cong\mathbb{Z}+R_mp/R_mp\subset R$;

(ii)由$\mathbb{F}_p\cong\mathbb{Z}+R_mp/R_mp$易知第一个断言成立。显然$\gamma$是所给的2次多项式的根，且$\sqrt{m}\notin\mathbb{Z}+R_mp$和$\frac{1}{2}(1+\sqrt{m})\notin\mathbb{Z}+R_mp$(比较$\sqrt{m}$或$\frac{1}{2}(1+\sqrt{m})$的系数可知)，即$\gamma\notin\mathbb{F}_p$，从而所给的多项式是$\gamma$的极小多项式，从而$R$是含有$p^2$个元素的有限环(此时注意，$R$不一定是整环，从而极小多项式不一定既约，故有下面的$(iii)-(iv)$)。

(iii)注意在$\mathbb{Z}$上有$x^2-m=(x-a)(x-b)+pf(x),f(x)\in\mathbb{Z}[x]$，从而在$\mathbb{Q}[\sqrt{m}]$中有$0=(\sqrt{m}-a)(\sqrt{m}-b)+pf(\sqrt{m})$。易知$f(\sqrt{m})=c+d\sqrt{m},c,d\in\mathbb{Z}$。假如$1\in P_1$，那么存在$\alpha,\beta\in R_m$使得$1=\alpha p+\beta(\sqrt{m}-a)$。从而$\sqrt{m}-b=\alpha p(\sqrt{m}-$

$b)-\beta pf(\sqrt{m})$。注意$m\equiv 2$ 或$3(mod\ 4)$，故$R_m=\mathbb{Z}[\sqrt{m}]$，于是得到$p|1$在$\mathbb{Z}$中成立，矛盾。故$1\notin P_1$，即$P_1\cap\mathbb{Z}\subset\mathbb{Z}$。显然$\mathbb{Z}p\subset P_1\cap\mathbb{Z}$，由$\mathbb{Z}p$是$\mathbb{Z}$的极大理想知$\mathbb{Z}p=P_1\cap\mathbb{Z}$。从而$\mathbb{F}_p\cong\mathbb{Z}/\mathbb{Z}p\cong\mathbb{Z}+P_1/P_1\subseteq R_m/P_1$。但显然有$\sqrt{m}\in\mathbb{Z}+P_1$，从而$\mathbb{Z}+P_1/P_1$，即$R_m/P_1$是$p$元有限域，故$P_1$是$R_m$的极大理想，从而也是素理想。类似知$P_2$是$R_m$的极大理想。从而又由$x^2-m=(x-a)(x-b)(mod\,\mathbb{Z}p)$知$p|a+b,p|m+ab$。由$a\not\equiv b(mod\mathbb{Z}p)$知$p\neq 2$(否则$a$与$b$不同则$a+b$为奇数且2整除奇数，矛盾)。但$p(\sqrt{m}-a)\in P_1P_2$和$p(\sqrt{m}-b)\in P_1P_2$知$pa-pb\in P_1P_2$。又由$p|a+b$知$p(a+b)\in P_1P_2$，故$2ap,2bp\in P_1P_2$。注意$a$与$p$互素和$p\neq 2$知$2a$与$p$在$\mathbb{Z}$中互素。故存在$u,v\in\mathbb{Z}$使得$1=2au+pv$。故$p=2apu+p^2v\in P_1P_2$，从而$R_mp\subseteq P_1P_2\subseteq P_1\cap P_2$。反之，由$(\sqrt{m}-a)(\sqrt{m}-b)=-pf(\sqrt{m})\in R_mp$知$P_1P_2\subseteq R_mp$，从而$P_1P_2=R_mp$。

又假如$P_1\cap P_2=P_1$，则$\sqrt{m}-a=\alpha p+\beta(\sqrt{m}-b),\alpha,\beta\in R_m$，于是$(\sqrt{m}-a)^2=\alpha'p,\alpha'\in R_m$。从而易知$p|2a$，矛盾。即有$P_1\cap P_2\neq P_1$。类似地，$P_1\cap P_2\neq P_2$，从而$P_1\neq P_2$，由他们的极大性知$P_1+P_2=R_m$。故$P_1\cap P_2=(P_1\cap P_2)P_1+(P_1\cap P_2)P_2\subseteq P_1P_2=R_mp$。

(iv) 类似于(iii)的证明可得$P=(p,\sqrt{m}-a)$是R_m的极大理想，从而为素理想。由条件知$p|2a$且$p|m-a^2$，可见$p=2$或$p|a$，后者导出$p|m$。设$p=2$，如果a为偶数，那么m也为偶数。此时$P=(2,\sqrt{m})$，从而$m\in P^2$。设$m=2m'$，由m没有平方因子知m'为奇数，故$1=2u+m',u\in\mathbb{Z}$。从而$2=2^2u+2m'\in P^2$，即有$R_m2\subseteq P^2$。另外，由$\sqrt{m}\sqrt{m}=m\in R_m2$知$(2,\sqrt{m})^2\subset R_m2$，故$P^2=R_m2$。如果$a$为奇数，那么$m$也为奇数。故$m=4n-1$。但易知$P=(2,\sqrt{m}+1)$，故$P^2\ni(\sqrt{m}+1)^2=m+1+2\sqrt{m}$。由$m+1=4n\in P^2$知$2\sqrt{m}\in P^2$，但$P^2\ni 2(\sqrt{m}+1)=2\sqrt{m}+2$，故$2\in P^2$，即有$R_m2\subseteq P^2$。反之由$(\sqrt{m}+1)^2=4n+2\sqrt{m}$知$P^2\subset R_m2$，故$R_m2=P^2$。

设$p\neq 2$，则$p|a$，故$p|m$。于是$P=(p,\sqrt{m})$。从而由$\sqrt{m}\sqrt{m}=m\in R_mp$知$P^2\subseteq R_mp$。另一方面，设$m=pm',p\nmid m'$。由$m=\sqrt{m}\sqrt{m}\in P^2$和$1=pu+m'v,u,v\in\mathbb{Z}$知$p=p^2u+mv\in P^2$。故$R_mp\subseteq P^2$。从而$R_mp=P^2$。

(v)即证$R=R_m/R_mp$没有零因子。注意

$$R=\mathbb{F}_p[\gamma]=\{\bar{s}+\bar{t}\gamma|\bar{t},\bar{s}\in\mathbb{F}_p\}$$

（因为γ满足的极小多项式为2次）。假如存在$\bar{s}_1+\bar{t}_1\gamma\neq 0$和$\bar{s}_1+\bar{t}_2\gamma\neq 0$使得

$$(\bar{s}_1+\bar{t}_1\gamma)(\bar{s}_2+\bar{t}_2\gamma)=0.$$

注意$\gamma^2=\bar{m}$，从而$(\bar{s}_1\bar{s}_2+\bar{m}\bar{t}_1\bar{t}_2)+(\bar{s}_1\bar{t}_2+\bar{t}_1\bar{s}_2)\gamma=0$。故$\bar{s}_1\bar{s}_2+\bar{m}\bar{t}_1\bar{t}_2=0$和$\bar{s}_1\bar{t}_2+\bar{t}_1\bar{s}_2=0$。由$x^2-m(mod\ \mathbb{Z}p)$既约知$p\nmid m$。假如$\bar{t}_1=0$，则$\bar{s}_1\neq 0$，且$\bar{s}_1\bar{s}_2=0$。故$\bar{s}_2=0$，于是$\bar{s}_1\bar{t}_2=0$，从而$\bar{t}_2=0$，与$\bar{t}_2+\bar{s}_2\gamma\neq 0$矛盾。从而$\bar{t}_1\neq 0$，类似$t_2\neq 0$。故不妨假设$\bar{t}_1=\bar{1},\bar{t}_2=\bar{1}$。即有$\bar{s}_1\bar{s}_2+\bar{m}=0,\bar{s}_1+\bar{s}_2=0$。于是$(x+\bar{s}_1)(x+\bar{s}_2)=x^2+\bar{s}_1\bar{s}_2=x^2-\bar{m}$。故$x^2-m=(x+s_1)(x+s_2)(mod\ \mathbb{Z}p)$，矛盾。从而$R$没有零因子。

（vi）类似可证。

现在刻画R_m的所有非零素理想。设$m\equiv 2$或$3(mod\ 4)$，且设P是R_m的非零素理想，那么$P\cap\mathbb{Z}=\mathbb{Z}p$，$p$为素数。于是$P\supseteq R_mp$。如果$x^2-m(mod\mathbb{Z}p)$可约，那么由$(iii)$和$(iv)$知存在$R_m$的素理想$P_1,P_2$（可以有$P_1=P_2$），使得$R_mp=P_1P_2$。于是$P_1P_2\subseteq P$。由$P$素知$P_1\subseteq P$或$P_2\subseteq P$。但是$P_1,P_2$也是极大理想（30题），故$P=P_1$或$P=P_2$。可见$P=(p,\sqrt{m}-a)$，其中$x-a(mod\mathbb{Z}p)$是$x^2-m(mod\ \mathbb{Z}p)$的因子。如果$x^2-m(mod\mathbb{Z}p)$既约，那么$R_mp$素，从而由30题知$R_mp$极大，故$P=R_mp$。类似可以刻画$m=1(mod\ 4)$时$R_m$的素理想。 □

注：能否从上述角度考虑R_m的既约元，进一步考虑唯一分解性（可参见关于R_m的具体标准分解的相关内容）。

32、证明：

(i) 设d为正整数，则商环R_m/R_md是元素个数为d^2的有限环；

(ii) 设A是R_m的非零理想，则交$A\cap\mathbb{Z}$是$\mathbb{Z}$的非零理想。令$A\cap\mathbb{Z}=\mathbb{Z}d$，则商环$R_m/A$的元素个数小于或等于$d^2$；

(iii) R_m是Noether 环。

证： (i) 易知$R_md\cap\mathbb{Z}=\mathbb{Z}d$。故$\mathbb{Z}/\mathbb{Z}d\cong\mathbb{Z}+R_md/R_md\subseteq R_m/R_md$。类似于31题的证明知$R_m/R_md=\mathbb{Z}/\mathbb{Z}d[\gamma]$，$\gamma$表示陪集$\sqrt{m}+R_md$或$\frac{1}{2}(1+\sqrt{m})+R_md$按照$m\equiv 2$或$3(mod\,4)$或$m\equiv 1(mod\,4)$，并且直接验证可知$\gamma$是$x^2-m(mod\,\mathbb{Z}d)$或$x^2-x+\frac{1}{4}(1-m)(mod\,\mathbb{Z}d)$的根。从而$R_m/R_md$中的元形如$\bar{a}+\bar{b}\gamma,\bar{a},\bar{b}\in\mathbb{Z}/\mathbb{Z}d$。设$\bar{a}+\bar{b}\gamma=0$，当$m\equiv 2$或$3(mod\,4)$时，$R_m=\mathbb{Z}[\sqrt{m}]$。于是$a+b\sqrt{m}=\alpha d,\alpha=s+t\sqrt{m},s,t\in\mathbb{Z}$。可见$d|a,d|b$，即$\bar{a}=0,\bar{b}=0$。于是$R_m/R_md=\mathbb{Z}/\mathbb{Z}d[\gamma]$中元的个数为$d^2$。类似，当$m\equiv 1(mod\,4)$时，结论成立。

(ii)设$0\neq\alpha\in A$，则$N(\alpha)=\bar{\alpha}\alpha\in A\cap\mathbb{Z}$且$N(\alpha)\neq 0$，故$A\cap\mathbb{Z}=\mathbb{Z}d$。于是$R_md\subseteq A$，从而$R_m/R_md$到$R_m/A$有自然地环满同态，故$R_m/A$中元素的个数$\leq d^2$。

(iii)设$A_1\subseteq A_2\subseteq A_3\cdots$是$R_m$的一个理想升链。那么$R_m/A_n$到$R_m/A_{n+1}$有满同态，且若为同构当且仅当$A_n=A_{n+1}$。故$|R_m/A_{n+1}|\leq|R_m/A_n|\leq\cdots|R_m/A_1|$，而$|R_m/A_1|$有限，故当$n>>0$时，有$|R_m/A_{n+1}|=|R_m/A_n|$，即$A_n=A_{n+1}$。 □

补充1、求$y^2+2=x^3$的整数解（右边的3次方也可以是其他次方，如5次方时没有整数解）。

证明：易知$\mathbb{Z}[\sqrt{-2}]$是欧式整环，从而唯一因式分解，且易知单位为±1。设有整数解，那么在$\mathbb{Z}[\sqrt{-2}]$中有$(y+\sqrt{-2})(y-\sqrt{-2})=x^3$。对$x$的任一既约因子$\alpha$，有$\bar{\alpha}$也是$x$的既约因子。假如$\alpha\sim\bar{\alpha}$，那么$\alpha=\bar{\alpha}$或$\alpha=-\bar{\alpha}$，故$\alpha$为整数或$\alpha=\pm\sqrt{-2}$。若为前者，由$\alpha|y+\sqrt{-2}$或$\alpha|y-\sqrt{-2}$知$\alpha=\pm1$，矛盾。若为后者，则由$\alpha^3|x^3$知，2是$x^3$在$\mathbb{Z}[\sqrt{-2}]$中的因子，从而也是$\mathbb{Z}$中的因子，故$x$为偶数，易知不可能。于是$\alpha$与$\bar{\alpha}$不相伴。故若$\alpha|y+\sqrt{-2}$，则$\bar{\alpha}\nmid y+\sqrt{-2}$，否则由$\alpha\neq\bar{\alpha}$知$\alpha\bar{\alpha}|y+\sqrt{-2}$，知$\alpha\bar{\alpha}=\pm1$，与$\alpha$既约矛盾。由此可知$y+\sqrt{-2}=\varepsilon(a+b\sqrt{-2})^3,\varepsilon=\pm1,a,b\in\mathbb{Z}$。不妨设$\varepsilon=1$，故$y+\sqrt{-2}=a^3+3a^2b\sqrt{-2}-6ab^2-2b^3\sqrt{-2}$，故$1=3a^2b-2b^3$，于是$b=\pm1$。当$b=-1$时，有$1=-3a^2+2$，即$3a^2=1$，不可能。故$b=1$，此时$a^2=1$，经计算可得$y=\pm5,x=3$，验证可知这是解。 □

四、域的基本定理

4、设K是F上的域扩张。证明：如果$u\in K$是F上的奇次代数元，那么u^2也是F上的奇次代数元且$F(u)=F(u^2)$。

证： 设u在F上的极小多项式为$f(x)$。注意u是$F(u^2)$上多项式x^2-u^2的根。假如x^2-u^2是$F(u^2)$上u的极小多项式，那么在$F(u^2)$上有$x^2-u^2|f(x)$，从而$-u$也是$f(x)$的根。但$deg\,f(x)$为奇数，而u满足F上的多项式$f(x)+f(-x)$，而$deg\,(f(x)+f(-x))<deg\,f(x)$。故$f(x)=-f(-x)$。特别地，$f(x)$的常数项为0。由$f(x)$既约知$f(x)=x$，与$x^2-u^2|f(x)=x$矛盾。故$x^2-u^2$在$F(u^2)$上可约，而它的分解只能是$x^2-u^2=(x-u)(x+u)$。故$u\in F(u^2)$，从而$F(u)=F(u^2)$，这说明$u^2$是$F$上的奇次代数元。

另证：$f(x)=xg(x^2)+h(x^2)$，而$g(x)\neq 0,g(u^2)\neq 0$，故$u=-\frac{h(u^2)}{g(u^2)}\in F(u^2)$。 □

8、设L和M为域扩张K/F的中间域。记LM是K中包含L和M的最小的子域（也是F的中间域）。证明：

(i) $[LM:F]$有限当且仅当$[L:F]$和$[M:F]$都有限；

注：能否从上述角度考虑R_m的既约元，进一步考虑唯一分解性（可参见关于R_m的具体标准分解的相关内容）。

32、证明：

(i) 设d为正整数，则商环R_m/R_md是元素个数为d^2的有限环；

(ii) 设A是R_m的非零理想，则交$A\cap\mathbb{Z}$是$\mathbb{Z}$的非零理想。令$A\cap\mathbb{Z}=\mathbb{Z}d$，则商环$R_m/A$的元素个数小于或等于$d^2$；

(iii) R_m是Noether 环。

证： （i）易知$R_md\cap\mathbb{Z}=\mathbb{Z}d$。故$\mathbb{Z}/\mathbb{Z}d\cong\mathbb{Z}+R_md/R_md\subseteq R_m/R_md$。类似于31题的证明知$R_m/R_md=\mathbb{Z}/\mathbb{Z}d[\gamma]$，$\gamma$表示陪集$\sqrt{m}+R_md$或$\frac{1}{2}(1+\sqrt{m})+R_md$按照$m\equiv 2$或$3(mod\,4)$或$m\equiv 1(mod\,4)$，并且直接验证可知$\gamma$是$x^2-m(mod\,\mathbb{Z}d)$或$x^2-x+\frac{1}{4}(1-m)(mod\,\mathbb{Z}d)$的根。从而$R_m/R_md$中的元形如$\bar{a}+\bar{b}\gamma,\bar{a},\bar{b}\in\mathbb{Z}/\mathbb{Z}d$。设$\bar{a}+\bar{b}\gamma=0$，当$m\equiv 2$或$3(mod\,4)$时，$R_m=\mathbb{Z}[\sqrt{m}]$。于是$a+b\sqrt{m}=\alpha d,\alpha=s+t\sqrt{m},s,t\in\mathbb{Z}$。可见$d|a,d|b$，即$\bar{a}=0,\bar{b}=0$。于是$R_m/R_md=\mathbb{Z}/\mathbb{Z}d[\gamma]$中元的个数为$d^2$。类似，当$m\equiv 1(mod\,4)$时，结论成立。

(ii)设$0\neq\alpha\in A$，则$N(\alpha)=\bar{\alpha}\alpha\in A\cap\mathbb{Z}$且$N(\alpha)\neq 0$，故$A\cap\mathbb{Z}=\mathbb{Z}d$。于是$R_md\subseteq A$，从而$R_m/R_md$到$R_m/A$有自然地环满同态，故$R_m/A$中元素的个数$\le d^2$。

(iii)设$A_1\subseteq A_2\subseteq A_3\cdots$是$R_m$的一个理想升链。那么$R_m/A_n$到$R_m/A_{n+1}$有满同态，且若为同构当且仅当$A_n=A_{n+1}$。故$|R_m/A_{n+1}|\le|R_m/A_n|\le\cdots|R_m/A_1|$，而$|R_m/A_1|$有限，故当$n>>0$时，有$|R_m/A_{n+1}|=|R_m/A_n|$，即$A_n=A_{n+1}$。 □

补充1、求$y^2+2=x^3$的整数解（右边的3次方也可以是其他次方，如5次方时没有整数解）。

证明：易知$\mathbb{Z}[\sqrt{-2}]$是欧式整环，从而唯一因式分解，且易知单位为±1。设有整数解，那么在$\mathbb{Z}[\sqrt{-2}]$中有$(y+\sqrt{-2})(y-\sqrt{-2})=x^3$。对$x$的任一既约因子$\alpha$，有$\bar{\alpha}$也是$x$的既约因子。假如$\alpha\sim\bar{\alpha}$，那么$\alpha=\bar{\alpha}$或$\alpha=-\bar{\alpha}$，故$\alpha$为整数或$\alpha=\pm\sqrt{-2}$。若为前者，由$\alpha|y+\sqrt{-2}$或$\alpha|y-\sqrt{-2}$知$\alpha=\pm1$，矛盾。若为后者，则由$\alpha^3|x^3$知，2是$x^3$在$\mathbb{Z}[\sqrt{-2}]$中的因子，从而也是$\mathbb{Z}$中的因子，故$x$为偶数，易知不可能。于是$\alpha$与$\bar{\alpha}$不相伴。故若$\alpha|y+\sqrt{-2}$，则$\bar{\alpha}\nmid y+\sqrt{-2}$，否则由$\alpha\neq\bar{\alpha}$知$\alpha\bar{\alpha}|y+\sqrt{-2}$，知$\alpha\bar{\alpha}=\pm1$，与$\alpha$既约矛盾。由此可知$y+\sqrt{-2}=\varepsilon(a+b\sqrt{-2})^3,\varepsilon=\pm1,a,b\in\mathbb{Z}$。不妨设$\varepsilon=1$，故$y+\sqrt{-2}=a^3+3a^2b\sqrt{-2}-6ab^2-2b^3\sqrt{-2}$，故$1=3a^2b-2b^3$，于是$b=\pm1$。当$b=-1$时，有$1=-3a^2+2$，即$3a^2=1$，不可能。故$b=1$，此时$a^2=1$，经计算可得$y=\pm5,x=3$，验证可知这是解。 □

四、域的基本定理

4、设K是F上的域扩张。证明：如果$u\in K$是F上的奇次代数元，那么u^2也是F上的奇次代数元且$F(u)=F(u^2)$。

证： 设u在F上的极小多项式为$f(x)$。注意u是$F(u^2)$上多项式x^2-u^2的根。假如x^2-u^2是$F(u^2)$上u的极小多项式，那么在$F(u^2)$上有$x^2-u^2|f(x)$，从而$-u$也是$f(x)$的根。但$deg\,f(x)$为奇数，而u满足F上的多项式$f(x)+f(-x)$，而$deg\,(f(x)+f(-x))<deg\,f(x)$。故$f(x)=-f(-x)$。特别地，$f(x)$的常数项为0。由$f(x)$既约知$f(x)=x$，与$x^2-u^2|f(x)=x$矛盾。故$x^2-u^2$在$F(u^2)$上可约，而它的分解只能是$x^2-u^2=(x-u)(x+u)$。故$u\in F(u^2)$，从而$F(u)=F(u^2)$，这说明$u^2$是$F$上的奇次代数元。

另证：$f(x)=xg(x^2)+h(x^2)$，而$g(x)\neq0,g(u^2)\neq0$，故$u=-\frac{h(u^2)}{g(u^2)}\in F(u^2)$。 □

8、设L和M为域扩张K/F的中间域。记LM是K中包含L和M的最小的子域（也是F的中间域）。证明：

(i) $[LM:F]$有限当且仅当$[L:F]$和$[M:F]$都有限；

(ii) $[LM:F]\le[L:F][M:F]$;

(iii) 若$[L:F]$与$[M:F]$互素，则(ii)中等式成立;

(iv) 若L/F和M/F都是代数元，则LM/F也是代数元。

证: (i)"$\Rightarrow$"由$[LM:F]=[LM:L][L:F]$知$[L:F]$有限，类似$[M:F]$有限。

"$\Leftarrow$" 我们证明$[LM:L]\le[M:F]$。实际上，设$u_1,\cdots,u_m$是M的一组F-基。记$L<u_1,\cdots,u_m>$为由$u_1,\cdots,u_m$张成的L上的向量空间。由$u_iu_j\in M$可由$u_1,\cdots,u_m$在F上从而在L上线性表出知$L<u_1,\cdots,u_m>$为K的子环。故

$$L[u_1,\cdots,u_m]=L<u_1,\cdots,u_m>.$$

但$u_1,\cdots,u_m$都是F上，从而是L上的代数元知$L[u_1,\cdots,u_m]=L(u_1,\cdots,u_m)$，但

$$M\subseteq F<u_1,\cdots,u_m>\subseteq L<u_1,\cdots,u_m>=L(u_1,\cdots,u_m).$$

故$LM\subseteq L(u_1,\cdots,u_m)\subseteq LM$。从而$LM=L(u_1,\cdots,u_m)=L<u_1,\cdots,u_m>$。由定义知$[L(u_1,\cdots,u_m):L]\le m=[M:F]$，故

$$[LM:F]=[LM:L][L:F]=[L<u_1,\cdots,u_m>:L][L:F]\le[M:F][L:F]$$

有限。

(ii)由(i)的"$\Leftarrow$"证明已得。

(iii)注意$[M:F]$和$[L:F]$都是$[LM:F]$的因子，由它们互素知$[M:F][L:F]|[LM:F]=[LM:L][L:F]$。但$[LM:L]\le[M:F]$，故$[LM:L]=[M:F]$，从而$[LM:F]=[M:F][L:F]$。

(iv)记

$$\begin{aligned}L(M) &= \{\frac{f(\alpha_1,\cdots,\alpha_n)}{g(\beta_1,\cdots,\beta_m)}|n,m\ge1,\alpha_1,\cdots,\alpha_n,\beta_1,\cdots,\beta_m\in M,\\ &\quad f(x_1,\cdots,x_n)\in L[x_1,\cdots,x_n],g(x_1,\cdots,x_m)\in L[x_1,\cdots,x_m],g(\beta_1,\cdots,\beta_m)\ne0\}.\end{aligned}$$

注意有$L[x_1]\subseteq L[x_1,x_2]\subseteq\cdots\subseteq L[x_1,\cdots,x_i]\subseteq\cdots$，易知$L(M)$是$K$的子域。显然$L\subseteq L(M)\subset LM$和$M\subseteq L(M)\subseteq LM$，故$LM\subseteq L(M)\subseteq LM$，特别地，$L(M)=LM$。如果$L/F$和$M/F$都是代数的，那么$f(\alpha_1,\cdots,\alpha_n)$和$g(\beta_1,\cdots,\beta_m)$都是$F$上的代数元，从而它们相除也是$F$上的代数元，即$L(M)$中任意元都是$F$上的代数元，故$LM/F$是代数的。 □

19、设E/F是有限正规扩张，$f(x)\in F[x]$在F上既约（首1）。证明:

i) 在E上，有$f(x)=(f_1(x)\cdots f_r(x))^{p^e}$，$e\ge0$ 且$f_i(x)\in E(x)$是E上不同的首1的既约多项式，并且当$char\ F=0$时，$e=0$;

ii) 设E的全部F-自同构组成的群为G。令$H=\{\sigma\in G|f_1^\sigma(x)=f_1(x)\}$。于是令$G=\sigma_1H\cup\sigma_2H\cup\cdots\cup\sigma_{r'}H,\sigma_1=1$，则有

$$f(x)=(\prod_{i=1}^{r'}f_1^{\sigma_i}(x))^{p^e}.$$

从而$r'=r$。

证: (i)设K是$f(x)$在E上的分裂域。设$f(s)=f_1(x)^{m_1}\cdots f_r(x)^{m_r}$是$f(x)$在$E$上的标准既约分解。由$f(x)$首1不妨设既约多项式$f_i(x)$也首1。从而$f_i(x)$互不相伴当且仅当它们互不相同。故在$K$中，若$i\ne j$，则$f_i(x)$与$f_j(x)$没有公共根(否则它们都是一个$\alpha\in K$在$E$上的极小多项式，从而相伴，矛盾)。于是由$f_i(x)$在$K$中可完全分解和$f(x)$在$K$中完全分解且根的重数相等都为$m$知$m_1=\cdots=m_r$。当$char\ F=0$时，$m=1$。当$char\ F=p$时，$m=p^e,e\ge1$。故结论成立。

(ii)显然H是G的子群，故有陪集分解$G=\sigma_1H\cup\sigma_2H\cup\cdots\cup\sigma_rH,\sigma_1=1$。注意$\sigma_i$是$E$的$F$-自同构，故$f^{\sigma_i}(x)=f(x)$且$f_1^{\sigma_i}(x)$也是$E$上的首1的既约多项式。从而$f_1^{\sigma_i}(x)$也是$f(x)$在$E$上的既约因子，故$f_1^{\sigma_i}(x)=f_j(x)$，某个$j$。由$f_1^{\sigma_i}(x)=f_1^{\sigma_j}(x)$当且仅当$f_1^{\sigma_i^{-1}\sigma_j}(x)=f_1(x)$当且仅当$\sigma_i^{-1}\sigma_j\in H$知当$i\neq j$时，有$f_1^{\sigma_i}(x)\neq f_1^{\sigma_j}(x)$。

另一方面，记K是$f(x)$在E上的分裂域，即$K=E(\alpha_1,\cdots,\alpha_n)$，其中$\alpha_1,\cdots,\alpha_n$是$f(x)$的所有根，那么$K'=F(\alpha_1,\cdots,\alpha_n)$是$f(x)$在$F$上的分裂域。由$E$是$F$上的有限正规扩张知，存在$F$上的多项式$g(x)$，使得$E=F(\beta_1,\cdots,\beta_m)$，其中$\beta_1,\cdots,\beta_m$是$g(x)$的所有根。那么$K=E(\alpha_1,\cdots,\alpha_n)=F(\beta_1,\cdots,\beta_m,\alpha_1,\cdots,\alpha_n)$是$F$上多项式$g(x)f(x)$的分裂域，从而$K/F$也是有限正规扩张。现在，对任一$f_t(x)$，设$\alpha$与$\beta\in K$分别是$f_1(x)$与$f_t(x)$的一个根，那么它们都是$F$上既约多项式$f(x)$的根。从而存在$F$自同构$\sigma:F(\alpha)\to F(\beta)$，由$K/F$有限正规知$\sigma$可扩张为$K$的$F$自同构，仍记为$\sigma$，使得$\sigma(\alpha)=\beta$。但$E/F$正规且$E\subseteq K$，故$\sigma(E)=E$(见15题)，从而$\sigma|_E\in G$，于是$\sigma|_E\in\sigma_iH$，某个$i$。于是$f_1^{\sigma}(x)=f_1^{\sigma_i}(x)$。但$0=\sigma(f_1(\alpha))=f_1^{\sigma}(\beta)=f_1^{\sigma_i}(\beta)$。故$\beta$是$E$上既约多项式$f_t(x)$与$f_1^{\sigma_i}(x)$的根，故$f_t(x)$和$f_1^{\sigma_i}(x)$相伴。由他们都是首1知$f_1^{\sigma_i}(x)=f_t(x)$。可见$r=r'$且$f(x)=(\prod_{i=1}^r f_1^{\sigma_i}(x))^{p^e}$。 □

22、设$f(x)\in\mathbb{F}_p[x]$是次数为$n(n\geq 1)$的既约多项式。记$P_n(x)$是$\mathbb{F}_p[x]$中所有首1的n次既约多项式的乘积。证明：

i) $f(x)|x^{p^m}-x\Leftrightarrow n|m$;
ii) $x^{p^n}-x|x^{p^m}-x\Leftrightarrow n|m$;
iii) $x^{p^n}-x=\prod_{d|n}P_d(x)$;
iv) $P_n(x)=\prod_{d|n}(x^{p^d}-x)^{\mu(\frac{n}{d})}$，其中$\mu$为Möbius函数;
v) $\mathbb{F}_p$上的n次既约多项式（互不相伴）的个数为$N_n=\frac{1}{n}\sum_{d|n}\mu(\frac{n}{d})p^d$。

证: (i)设$\mathbb{F}_p(\alpha)$是单扩域且α在$\mathbb{F}_p$上的极小多项式为$f(x)$，那么$[\mathbb{F}_p(\alpha):\mathbb{F}_p]=n$，故$\mathbb{F}_p(\alpha)=\mathbb{F}_{p^n}$。由$\mathbb{F}_{p^n}$是$x^{p^n}-x$的分裂域知$\mathbb{F}_{p^n}/\mathbb{F}_p$正规，从而$f(x)$在$\mathbb{F}_p(\alpha)$上完全可分解，故$\mathbb{F}_p(\alpha)$也是$f(x)$的分裂域。

"$\Rightarrow$" 由$f(x)|x^{p^m}-x$知在$x^{p^m}-x$的分裂域$\mathbb{F}_{p^m}$中存在$f(x)$的根，不妨设为上述α。那么$\mathbb{F}_p(\alpha)\subseteq\mathbb{F}_{p^m}$。故$\mathbb{F}_{p^n}\subseteq\mathbb{F}_{p^m}$。从而$n|m$（因为$m=[\mathbb{F}_{p^m}:\mathbb{F}_p]=[\mathbb{F}_{p^m}:\mathbb{F}_{p^n}][\mathbb{F}_{p^n}:\mathbb{F}_p]=[\mathbb{F}_{p^m}:\mathbb{F}_{p^n}]n$）。

"$\Leftarrow$"由$n|m$知$\mathbb{F}_{p^n}\subseteq\mathbb{F}_{p^m}$，即$\mathbb{F}_p(\alpha)\subseteq\mathbb{F}_{p^m}$。从而$\alpha$也是$x^{p^m}-x$的根，但$\alpha$在$\mathbb{F}_p$上的极小多项式为$f(x)$，故$f(x)|x^{p^m}-x$。

(ii)由$(x^{p^n}-x)'=-1$知$x^{p^n}-x$在$\mathbb{F}_p$上的分裂域中没有重根，故$x^{p^n}-x$的既约因式的重数为1。设$g(x)$是$x^{p^n}-x$的任一既约因式且次数为d，由(i)知$d|n$。

"$\Rightarrow$"设$\mathbb{F}_{p^n}(\alpha_1,\cdots,\alpha_{p^m})$是$x^{p^m}-x$在$\mathbb{F}_{p^n}$上的分裂域，其中$\alpha_1,\cdots,\alpha_{p^m}$为$x^{p^m}-x$的所有根，注意$\mathbb{F}_{p^n}$中的元都是$x^{p^n}-x$的根，从而是$x^{p^m}-x$的根。于是$\mathbb{F}_{p^n}\subset\{\alpha_1,\cdots,\alpha_{p^m}\}$。故$\mathbb{F}_{p^n}(\alpha_1,\cdots,\alpha_{p^m})=\mathbb{F}_p(\alpha_1,\cdots,\alpha_{p^m})$是$x^{p^m}-x$在$\mathbb{F}_p$上的分裂域。从而$\mathbb{F}_{p^n}$是$\mathbb{F}_{p^m}$的子域，故$n|m$。

"$\Leftarrow$"(讲义先证$\mathbb{F}_{p^n}$是$\mathbb{F}_{p^m}$的子域，再由带余除法$x^{p^m}-x=(x^{p^n}-x)g(x)+r(x)$推出$\mathbb{F}_{p^n}$中的元都是$r(x)$的根，从而$r(x)=0$。以下是另一个证明)

对上述d，由$n|m$和$d|n$知$d|m$。故由(i)知$g(x)|x^{p^m}-x$。由$g(x)$作为$x^{p^n}-x$的既约因式的任意性以及$x^{p^n}-x$只有单重既约因式知$x^{p^n}-x|x^{p^m}-x$。

(iii)对任意的d，设$g(x)\in\mathbb{F}_p[x]$是d次既约多项式，那么由(i)知$g(x)|x^{p^n}-x\Leftrightarrow d|n$。从而$x^{p^n}-x=\prod_{d|n}P_d(x)$。

(iv)由(iii)，利用Möbius反演公式可得。

(v) 由 (i) 知 $\mathbb{F}_{p^n}=\cup_{d|n}M_d$，其中 $M_d=\{\alpha\in\mathbb{F}_{p^n}|\alpha$的极小多项式为$d$次$\}$。这是不交并，故

$$p^n=\Sigma_{d|n}|M_d|,$$

而任意d次既约多项式在$\mathbb{F}_{p^n}$中有d个根且不相伴的既约多项式没有公共根，故$|M_d|=dN_d$。即$p^n=\Sigma_{d|n}dN_d$。故由Möbius反演公式知$nN_n=\Sigma_{d|n}\mu(\frac{n}{d})p^d$。 □

23、(原书中结论有误，修改如下)：设p为素数且整数$n\geq 1$。如果$n\nmid p^n$，那么$x^{p^n}-x-a\in\mathbb{F}_p[x]$可约。

证： 设K是$x^{p^n}-x-a$在$\mathbb{F}_p$上的分裂域，E是$x^{p^n}-x$在K上的分裂域。记$\alpha\in K$是$x^{p^n}-x-a$的根，那么$x^{p^n}-x$在E中的任一根β，有$(\alpha+\beta)^{p^n}-(\alpha+\beta)-a=0$，即有$\alpha+\beta$也是$x^{p^n}-x-a$的根。故$\alpha+\beta\in K$，从而$\beta\in K$。故$E=K$。

假如$x^{p^n}-x-a$在$\mathbb{F}_p$上既约，那么由上题(i)的证明知$\mathbb{F}_{p^{p^n}}=\mathbb{F}_p(\alpha)$是$x^{p^n}-x-a$的分裂域。即$K=\mathbb{F}_{p^{p^n}}$。但$x^{p^n}-x$在$\mathbb{F}_p$上的分裂域$\mathbb{F}_{p^n}$是$E$的子域，从而是$E=K$的子域，即$\mathbb{F}_{p^n}\subseteq\mathbb{F}_{p^{p^n}}$，故$n|p^n$，矛盾。 □

24、证明有限域F的每个元可表成两个元的平方和。

证： 注意在F中$\alpha^2=\beta^2\Leftrightarrow\alpha=\pm\beta$，而$\alpha=-\alpha\Leftrightarrow 2\alpha=0$。故$|F^2|\geq\frac{|F|+1}{2}$，其中$F^2=\{a^2|a\in F\}$。于是对$\forall a\in F$，由$|a-F^2|=|F^2|$知$|a-F^2|+|F^2|\geq|F|+1\geq|F|$知$(a-F^2)\cap F^2\neq\emptyset$。设$b^2\in F^2\cap(a-F^2)$，则存在$c^2\in F^2$，使得$b^2=a-c^2$。故$a=b^2+c^2$。 □