由交换环的2阶元诱导的群的同构类

邓江流[1]　雨辰[2]

1.贵阳职业技术学院装备制造分院；2.遵义市〇六一基地

[摘　要]通过中国剩余定理（=CRT）考虑了剩余类环$\mathbb{Z}/m\mathbb{Z}$所诱导的剩余类乘法群$(\mathbb{Z}/m\mathbb{Z})^*$的2阶元个数问题，并给出了相应的计数定理.具体地说，$(\mathbb{Z}/m\mathbb{Z})^*$的2阶元个数可以通过$m$的素因子分解$m=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$决定：当$p_1\geq 3$时，或者当$p_1=2,\alpha_1=2$时，2阶元个数是$2^r-1$；当$p_1=2,\alpha_1=1$时，2阶元个数是$2^{r-1}-1$；当$p_1=2,\alpha_1\geq 3$时，2阶元个数大于$2^r-1$.该计数定理可以用于判定剩余类乘法群所在的Abel群同构类.

[关键词]近世代数；Abel群；有限群分类；中国剩余定理；同余；阶

【DOI】10.12252/j.issn.2096-6261.2021.09.889

记号约定以及预备知识

本文通过计算由含幺交换环所决定的商群的2阶元个数来完成一些群的分类问题.简便起见，对本文中所使用的记号我们进行如下约定：

●对乘法群$G=(G,\cdot)$，其上的单位元记作1_G；

●对环$R=(R,+,\cdot)$，其上的零元（即加法单位元）记作0_R，特别地若R是含幺环，即R有幺元（即乘法单位元），记此幺元为1_R.如无特殊说明，本文所说的环均是含幺环；

●对任意集合S，$\sharp S$表示S的元素个数；

●令$\mathbb{Z}$表示整数环$\mathbb{Z}=(\mathbb{Z},+,\cdot)$，$\mathbb{Z}/m\mathbb{Z}$是其剩余类环，则对任意$n\in\mathbb{Z}/m\mathbb{Z}$，$n$是$\mathbb{Z}/m\mathbb{Z}$的乘法可逆元，即存在$n'\in\mathbb{Z}/m\mathbb{Z}$使得$nn'=n'n=1_{\mathbb{Z}/m\mathbb{Z}}$，当且仅当$m$，$n$互素，即$\gcd(m,n)=1$（见本文的命题1）；

●由上，全部$\mathbb{Z}/m\mathbb{Z}$的乘法可逆元组成了$\mathbb{Z}/m\mathbb{Z}$的子集，记作$(\mathbb{Z}/m\mathbb{Z})^*$，它是群，群运算取剩余类乘法.

群分类问题一直是代数学的基本问题.至1955年起，群分类问题就成为群论的重要问题之一.最先发起的分类问题是有限单群分类，而Abel群的完全分类则通过其结构定理给出，具体地说，任意Abel群在同构意义下形如$\mathbb{Z}\times\mathbb{Z}/p\ \mathbb{Z}\times\cdots\times\mathbb{Z}/p\ \mathbb{Z}$，其中，$r\in\mathbb{N}$，$p_i$是素数，$\alpha_i\in\mathbb{N}^+$.这一经典结果在诸多群论文献中都有提及，例如[1].

本文将通过中国剩余定理（=CRT）来计算群$(\mathbb{Z}/m\mathbb{Z})^*$的2阶元以获得相应的计数定理（见本文的定理2），并将此定理做到交换环上（见本文的定理3）.本文的最后会利用此计数定理以及Abel群的结构定理来实现对给定的$(\mathbb{Z}/m\mathbb{Z})^*$的同构类.为此先回忆一下CRT（=CRT）及其交换环上的一般形式.该定理是关于一次同余式方程组$(x\equiv a_j(\mathrm{mod}\,m_j))_{1\leq j\leq r}$的解的存在性定理：如果$m_1,\cdots,m_r$两两互素，则$(x\equiv a_j(\mathrm{mod}\,m_j))_{1\leq j\leq r}$对$x$有唯一解.由于$x\equiv a_j(\mathrm{mod}\,m_j)$可以看作是$\mathbb{Z}/m_j\mathbb{Z}$上的对$x$的一次方程$x\overset{\mathbb{Z}/m_j\mathbb{Z}}{=\!=}a_j$，该方程可以被理解为$a_j$是$x$在自然满同态$\pi_j:\mathbb{Z}\to\mathbb{Z}/m_j\mathbb{Z}$下的像，故此方程可以通过群同态写为$\pi_j(x)=a_j$.因此上述一次同余式方程组变成关于$x$的同态方程组$(\pi_j(x)=a_j)_{1\leq j\leq r}$.$m_j\mathbb{Z}$是$\mathbb{Z}=(\mathbb{Z},+,\cdot)$的理想，所以$(\pi_j)_{1\leq j\leq r}$给出了环的同态$\pi=(\pi_j)_{1\leq j\leq r}:\mathbb{Z}\to\bigoplus_{j=1}^r\mathbb{Z}/m_j\mathbb{Z}$，其满足$\pi(x)=(a_j)_{j=1}^r$.在此意义下，CRT可表述为，如果$m_1,\cdots,m_r$两两互素，则$\pi$是满同态，$\ker\pi=\bigcap_{j=1}^r m_j\mathbb{Z}$，且有环同构$\mathbb{Z}/m\mathbb{Z}\cong\bigoplus_{j=1}^r\mathbb{Z}/m_j\mathbb{Z}$，其中$m=m_1\cdots m_r$.CRT可以被推广到一般的交换环上：

定理1[2, 3, 4, etc].（中国剩余定理）令环$R=(R,+,\cdot)$是交换环，$I_1,\cdots,I_r$是R的理想，且两两互素，即$I_i+I_j=R,\forall i\neq j$，则自然满同态组$(\pi_j:R\to R/I_j)_{1\leq j\leq r}$诱导了商环的满同态$\pi=[\pi_j]_{1\leq j\leq r}:R\to\bigoplus_{j=1}^r R/I_j$使得$\ker\pi=\bigcap_{j=1}^r I_j$，且有环同构$R/\bigcap_{j=1}^r I_j\cong\bigoplus_{j=1}^r R/I_j$.

Abel群$(\mathbb{Z}/m\mathbb{Z})^*$的2阶元的个数

定义1.（Euler函数）本文中，我们始终定义函数$\varphi:\mathbb{N}^+\to\mathbb{N}^+$表示将$n\in\mathbb{N}^+$映射为小于$n$且与$n$互素的正整数个数，如果$n\geq 2$；而对$n=1$，我们定义$\varphi(1)=1$.

注记.若m有素因子分解$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$，则$\varphi(m)=m\prod_{j=1}^r(1-p_j^{-1})$.因此，若$\alpha_1=\alpha_2=\quad\alpha\quad$，则该式可以变化为（）$\prod$（　　）；特别地，若$m$是素数$p$，则$\varphi(m)=m-1$（这由$\varphi:\mathbb{N}^+\to\mathbb{N}^+$的定义直接得出）.

命题1[4, 5, etc].剩余类乘法群$(\mathbb{Z}/m\mathbb{Z})^*$的阶，即$\sharp(\mathbb{Z}/m\mathbb{Z})^*$，等于$\varphi(m)$.

证.为了文章的完整性，我们在这里将此命题予以证明.注意到$x\in(\mathbb{Z}/m\mathbb{Z})^*$当且仅当$xy\equiv 1(\mathrm{mod}\,m)$对y有解，所以命题等价于证明$\gcd(x,m)=1$当且仅当$xy\equiv 1(\mathrm{mod}\,m)$对$y$有解.关于充分性，$y$满足$xy\equiv 1(\mathrm{mod}\,m)$可知存在$t\in\mathbb{Z}$使得$xy-1=mt$，所以$xy+mt=1$，再用Bezout定理就知道$\gcd(x,m)=1,\gcd(y,t)=1$.反之，即必要性，若$\gcd(x,m)=1$，则存在$y,t\in\mathbb{Z}$使得$xy+mt=1$，所以$xy=1-mt\equiv 1(\mathrm{mod}\,m)$.□

引理1.令$x\in(\mathbb{Z}/m\mathbb{Z})^*$是$(\mathbb{Z}/m\mathbb{Z})^*$中的2阶元，则对任意$m$的每个奇数素因子$p\mid m$以及其此素因子对应的正整数$k$使得$p^k\mid m$且$p^{k+1}\nmid m$，始终有$\sharp\{x\in(\mathbb{Z}/m\mathbb{Z})^*\mid x^2\equiv 1(\mathrm{mod}\,p^j),1\leq x\leq m\}=2$对任意$1\leq j\leq k$成立.

证.因为x是$(\mathbb{Z}/m\mathbb{Z})^*$中的2阶元，所以$x^2=1_{(\mathbb{Z}/m\mathbb{Z})^*}$，即$x^2\equiv 1(\mathrm{mod}\,m)$（这里总假定$0\leq x\leq m-1$）.令$p$是$m$的奇数素因子，$k$是正整数使得$p^k\mid m$且$p^{k+1}\nmid m$，这意味着$m=p^km'$，其中$\gcd(p,m')=1$.则按$x^2\equiv 1(\mathrm{mod}\,m)$，可知对某个$t\in\mathbb{Z}$有$x^2-1=mt=p^km't\ \Rightarrow\ x\cdot x+(-m't)\cdot p^k=1$，即得$x^2\equiv 1(\mathrm{mod}\,p^j),\forall 1\leq j\leq k$.再者将$x^2\equiv 1(\mathrm{mod}\,p^j)$改写为$x^2-1=(x+1)(x-1)\equiv 0(\mathrm{mod}\,p^j)$，则有$p^j\mid(x+1)$或$p^j\mid(x-1)$，且由于$p\geq 3$，所以二者只能满足其一，这是因为，若$p^j\mid(x+1)$则$(x+1)=p^jt\Rightarrow x-1=p^jt-2\equiv -2(\mathrm{mod}\,p^j)$，得$p^j\nmid(x-1)$；反之若$p^j\mid(x-1)$则$p^j\nmid(x+1)$.从而$x^2\equiv 1(\mathrm{mod}\,p^j)$的解必满足$x\equiv -1(\mathrm{mod}\,p^j)$以及$x\equiv 1(\mathrm{mod}\,p^j)$.另一方面，根据$(p^j\pm 1)^2=p^{2j}\pm 2p^j+1\equiv 1(\mathrm{mod}\,p^j)$可知$x^2\equiv 1(\mathrm{mod}\,p^j)$在模$p^j$的完全剩余系中仅有解1和$p^j-1$.□

引理2.沿用引理1中的记号，若m的偶数素因子$2\mid m$满足$2^k\mid m$且$2^{k+1}\nmid m$，则$x\equiv\pm 1(\mathrm{mod}\,2^j)\ (1\leq j\leq k)$在$2^j$的剩余系下的解集是$\{1,2^j-1\}$当且仅当$j\in\{1,2\}$.

证.$x^2\equiv 1(\mathrm{mod}\,2^j)$可改写$x^2-1=(x+1)(x-1)\equiv 0(\mathrm{mod}\,2^j)$，而得$2^j\mid(x+1)(x-1)$，于是$\mid$　且$2\mid x-1$（因为$2\mid x+1$得到$x+1$是偶数，可知$x-1$也是，反之亦然）.对$j=1$的情形$x\equiv\pm 1(\mathrm{mod}\,2)$等价于$x\equiv 1(\mathrm{mod}\,2)$，它的解在完全剩余系$\{0,1\}$中有且仅有1个，是$x=1$；对$j=2$的情形，$x\equiv\pm 1(\mathrm{mod}\,2^2=4)$在完全剩余系$\{0,1,2,3\}$下只有1,3.（注意$k=1$的情形下必有$j=1$，此时是$x\equiv\pm 1\equiv 1(\mathrm{mod}\,2^1)$.）若$j\geq 3$，写$x=1+2^{j-1}$，总有：

$$x^2=(1+2^{j-1})^2=1+2^j(1+2^{j-2})\equiv 1(\mathrm{mod}\,2^j).$$

此时$x^2\equiv 1(\mathrm{mod}\,2^j)$有除$x\equiv\pm 1(\mathrm{mod}\,2^j)$以外的解.□

命题2.设m的素因子分解是$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$，其中$3\leq p_1<p_2<\cdots<p_r$，则：

$\sharp\{x\in(\mathbb{Z}/m\mathbb{Z})^*\mid x^2=1_{(\mathbb{Z}/m\mathbb{Z})^*}\text{且}x\neq 1_{(\mathbb{Z}/m\mathbb{Z})^*}\}=2^r-1$.

证. 简便起见，用$\Omega(k_1,k_2,\cdots,k_r)$表示一次同余式方程组$(x\equiv k_j(\mathrm{mod}\,p_j^{\alpha_j}))_{1\le j\le r}$，$k_j\in\mathbb{Z},\forall 1\le j\le r$.

对任意$1\le j\le r$，根据引理1，我们有$p_j^{\alpha_j}\mid m$，$p_j^{\alpha_j+1}\nmid m$，且$x^2\equiv 1(\mathrm{mod}\,p_j^{\alpha_j})$在模$p_j^{\alpha_j}$的完全剩余系下有两个解$x\equiv 1(\mathrm{mod}\,p_j^{\alpha_j})$和$x\equiv -1(\mathrm{mod}\,p_j^{\alpha_j})$. 换言之，用所给记号，$(\mathbb{Z}/m\mathbb{Z})^*$的2阶元$x$总满足$\Omega(k_1,k_2,\cdots,k_r)$，这里对任意的$1\le j\le r$，总是有$k_j\in\{-1,1\}$. 根据CRT，$x$在模$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$的完全剩余系下有关于方程组$\Omega(k_1,k_2,\cdots,k_r)$的唯一解. 注意每个$(k_1,k_2,\cdots,k_r)$都对应了一组一次同余式方程组$\Omega(k_1,k_2,\cdots,k_r)$，所以：

$\sharp\{x\in(\mathbb{Z}/m\mathbb{Z})^*\mid x^2=1_{(\mathbb{Z}/m\mathbb{Z})^*},\}=\sharp\{(k_1,k_2,\cdots,k_r)\in\mathbb{Z}^r\mid k_j\in\{-1,1\}$ 对任意$1\le j\le r\}=(C_2^1)^r=2^r$.

特别地，$\Omega(1,1,\cdots,1)$对应平凡解$x=1_{(\mathbb{Z}/m\mathbb{Z})^*}$其不是$(\mathbb{Z}/m\mathbb{Z})^*$的2阶元，所以$(\mathbb{Z}/m\mathbb{Z})^*$的2阶元个数是$2^r-1$. □

注记. 注意在命题2中，若m素因子分解$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$（$p_1<p_2<\cdots<p_r$）满足$p_1=2$，则根据引理2，有

$$\sharp\{x\in(\mathbb{Z}/m\mathbb{Z})^*\mid x^2=1_{(\mathbb{Z}/m\mathbb{Z})^*}\text{且}x\neq 1_{(\mathbb{Z}/m\mathbb{Z})^*}\}=\begin{cases}2^{r-1}-1, & \alpha_1=1;\\ 2^r-1, & \alpha_1=2.\end{cases}$$

特别地，若$\alpha_1\ge 3$，则是：

$\sharp\{x\in(\mathbb{Z}/m\mathbb{Z})^*\mid x^2=1_{(\mathbb{Z}/m\mathbb{Z})^*}\text{且}x\neq 1_{(\mathbb{Z}/m\mathbb{Z})^*}\}>2^r-1$.

由此，我们得到了本文的主要结论：

定理2.（主定理1）令正整数m的素因子分解为$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$，其中$p_1<p_2<\cdots<p_r$，则：

（1）（见命题1）$(\mathbb{Z}/m\mathbb{Z})^*$的2阶元个数是$2^r-1$当且仅当下述情形之一满足：（i）$p_1\ge 3$；（ii）$p_1=2$且$\alpha_1=2$.

（2）（见命题1的注记）$(\mathbb{Z}/m\mathbb{Z})^*$的2阶元个数是$2^{r-1}-1$当且仅当$p_1=2$且$\alpha_1=1$.

（3）（见命题1的注记）$(\mathbb{Z}/m\mathbb{Z})^*$的2阶元个数$\ge 2^r$当且仅当$p_1=2$且$\alpha_1\ge 3$.

由商环诱导的乘法群的2阶元的个数

下面考虑更一般的情形，为此令R是交换环，并对R的理想I用记号$\bar{x}$表示x在环的自然满同态$R\to R/I$下的像. 再对R的两个元素x,a，用记号$x\equiv a(\mathrm{mod}\,I)$表示$x-a\in I$. 这一记号起源自$\mathbb{Z}$上的同余式. 如$I=m\mathbb{Z}$的情形，$x,a\in\mathbb{Z}$满足$x-a\in m\mathbb{Z}$意味着$x-a=mt$，其中$t\in\mathbb{Z}$，从而$x=mt+a\equiv a(\mathrm{mod}\,t)$；反之若有$x\equiv a(\mathrm{mod}\,t)$，就是$x-a\equiv(\mathrm{mod}\,t)$，即$x-a\in m\mathbb{Z}$.

引理3. 令R是交换环（乘法单位元记作1_R），$I_1,I_2,\cdots,I_r$是R的素理想，且两两互素，记$I=\cap_{j=1}^r I_j$. $(R/I)^*$表示R/I的全部非零因子做成的乘法群. 则$\bar{x}$是$(R/I)^*$中的2阶元，即x满足$x^2\equiv 1_R(\mathrm{mod}\,I)$，当且仅当对任意的$I_j$$(1\le j\le r)$，或者$x\equiv 1_R(\mathrm{mod}\,I_j)$，或者$x\equiv -1_R(\mathrm{mod}\,I_j)$.

证. 首先，$x^2\equiv 1_R(\mathrm{mod}\,I)$即$x^2-1_{R/I}\in I=\cap_{j=1}^r I_j$，这当且仅当$x^2-1_R=(x-1_R)(x+1_R)\in I_j$，$\forall 1\le j\le r$. 因为$I_j$是素理想，所以$x-1_R\in I_j$和$x+1_R\in I_j$至少有其一. 等价地，即$x\equiv 1_R(\mathrm{mod}\,I_j)$和$x\equiv -1_R(\mathrm{mod}\,I_j)$至少有其一. 反之，若$x\in(R/I)^*$满足$x\equiv 1_R(\mathrm{mod}\,I_j)$或$x\equiv -1_R(\mathrm{mod}\,I_j)$，$\forall 1\le j\le r$，则上面过程可逆. □

显然，引理1和引理2可以作为上述引理在$R=\mathbb{Z}$情形下的特例. 但是由于整数环$\mathbb{Z}$自身的特殊性，$I_1,I_2,\cdots,I_r$是素理想这一条件可以放宽为$\mathbb{Z}$中的素元的幂（即素数的幂）生成的$\mathbb{Z}$的主理想. 下面定理是定理1在交换环上的版本.

定理3.（主定理2）令R是交换环（乘法单位元记作1_R），$I_1,I_2,\cdots,I_r$是R的素理想，且两两互素，记$I=\cap_{j=1}^r I_j$. $(R/I)^*$表示R/I的全部非零因子做成的乘法群，称之为非零因子群. 则$(R/I)^*$的2阶元的个数不超过2^r-1. 特别地，若$2\cdot 1_R$不属于任何一个I_j，此个数等于2^r-1.

证. 从引理3的还证明可知$x\in(R/I)^*$满足方程$x^2\equiv 1_R(\mathrm{mod}\,I)$当且仅当满足方程组$(x^2\equiv 1_R(\mathrm{mod}\,I_j))_{1\le j\le r}$，该方程组的每个方程$x^2\equiv 1_R(\mathrm{mod}\,I_j)$等价于$x\equiv 1_R(\mathrm{mod}\,I_j)$或$x\equiv -1_R(\mathrm{mod}\,I_j)$，那么上述方程组实对应了一个方程组族$\{(x\equiv k_j(\mathrm{mod}\,I_j))_{1\le j\le r}\}_{k_j\in\{-1_R,1_R\},\forall j}$. 用环同态的语言来说，对每组$k_1,k_2,\cdots,k_r$，每个方程组都可以写为$(\pi_j(x)=k_j)_{1\le j\le r}$，其中$\pi_j:R\to R/I_j$是自然满同态. 因此，如果写$\pi=[\pi_j]_{1\le j\le r}:R\to\oplus_{j=1}^r R/I_j$，每个方程组可进一步改写为$\pi(x)=[\pi_j(x)]_{1\le j\le r}=[k_j]_{1\le j\le r}$. 根据CRT知$\pi$满，其诱导了$R/I\cong\oplus_{j=1}^r R/I_j$，所以唯一存在$\bar{x}\in R/I$使得$\pi(x)=[k_j]_{1\le j\le r}$. 注意对$k_1,k_2,\cdots,k_r$的不同选择可能得到不同的方程组，不同的方程组可以诱导出不同的$\bar{x}$（事实上，$\bar{x}$对某个I_j同时满足$x-1_R\in I_j$和$x+1_R\in I_j$导致$(x+1_R)-(x-1_R)=2\cdot 1_R\in I_j$，此时$x-1_R\in I_j$，从而$x-1_R+2\cdot 1_R=x+1_R\in I_j$，导致$\pi_j(x)=1_R$和$\pi_j(x)=-1_R$是同一方程），由此得满足$x^2\equiv 1_R(\mathrm{mod}\,I)$的$\bar{x}$的个数等于方程组族中方程组的个数（相同方程组只计算1次），该个数$\le 2^r$. 除去$k_1=k_2=\cdots=k_r=1_R$所对应的$x=1_R$平凡情形，其余的$\bar{x}$都是2阶元. 综上，$(R/I)^*$的2阶元个数$\le 2^r-1$. 特别地，若$2\cdot 1_R\notin I_j$，则$x-1_R\in I_j$和$x+1_R\in I_j$只能满足其一. 这时$\pi_j(x)=1_R$和$\pi_j(x)=-1_R$总是不同的. 此时若对每个理想I_j都有$2\cdot 1_R\notin I_j$，那么2阶元个数等于2^r-1. □

下面的两个例子提供了定理2（即主定理1）在Abel群分类问题上的一个应用.

例. 用定理2说明$(\mathbb{Z}/100\mathbb{Z})^*\cong(\mathbb{Z}/110\mathbb{Z})^*$. 首先$\sharp(\mathbb{Z}/100\mathbb{Z})^*=\varphi(100)=40=\varphi(110)=\sharp(\mathbb{Z}/110\mathbb{Z})^*$，所以$(\mathbb{Z}/100\mathbb{Z})^*$和$(\mathbb{Z}/110\mathbb{Z})^*$都是40阶Abel群. 注意$40=2^3\cdot 5$给出了40阶Abel群在同构意义下的完全分类是$A_1=\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z}$，$A_2=\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z}$，以及$A_3=(\mathbb{Z}/2\mathbb{Z})^{\oplus 3}\oplus\mathbb{Z}/5\mathbb{Z}$. 易见$A_1$，$A_2$，$A_3$的2阶元的个数分别是1，3，7（注意5阶循环群内没有2阶元）. 而，利用命题1的注记，$100=2^2\cdot 5^2$得到$(\mathbb{Z}/100\mathbb{Z})^*$的2阶元个数是$2^2-1=3$，所以必有$(\mathbb{Z}/100\mathbb{Z})^*\cong A_2$. 同理$110=2\cdot 5\cdot 11$可知，仍利用命题1的注记，$(\mathbb{Z}/110\mathbb{Z})^*$的2阶元的个数是$2^{3-1}-1=3$，从而也有$(\mathbb{Z}/110\mathbb{Z})^*\cong A_2$. 故根据Abel群的结构定理得$(\mathbb{Z}/100\mathbb{Z})^*\cong(\mathbb{Z}/110\mathbb{Z})^*$.

例. 利用定理2说明$(\mathbb{Z}/100\mathbb{Z})^*\cong(\mathbb{Z}/110\mathbb{Z})^*\cong A_2\ncong(\mathbb{Z}/132\mathbb{Z})^*$. 由$\sharp(\mathbb{Z}/132\mathbb{Z})^*=\varphi(132)=40=\sharp A_2$得到$(\mathbb{Z}/132\mathbb{Z})^*$也是40阶Abel群. 但$132=12\cdot 11=2^2\cdot 3\cdot 11$，根据命题1的注记，也即定理2的（1），得$(\mathbb{Z}/132\mathbb{Z})^*$有$2^3-1=7$个2阶元，所以$(\mathbb{Z}/132\mathbb{Z})^*\cong A_3\ncong A_2$.

下面，我们再于一元多项式环上给出一个例子，其作为定理3（即主定理2）的一个应用.

例. 取$\mathbb{R}[x]$和它的两个理想$\langle x-1\rangle$和$\langle x-2\rangle$，易见$\langle x-1\rangle\cap\langle x-2\rangle=\langle(x-1)(x-2)\rangle$. 则商环$\frac{\mathbb{R}[x]}{(x-1)(x-2)}$诱导的乘法群$G=(\frac{\mathbb{R}[x]}{(x-1)(x-2)})^*$有$2^2-1=3$个2阶元. 这是因为$\langle x-1\rangle$和$\langle x-2\rangle$都是素理想，且$2\notin\langle x-1\rangle\cap\langle x-1\rangle$. 事实上，$\frac{\mathbb{R}[x]}{(x-1)(x-2)}$中的元素形如$ax+b,a,b\in\mathbb{R}$，因此若其是$G$的2阶元，当且仅当$(ax+b)^2$形如$P(x)\cdot(x-1)(x-2)+1$，$P(x)\in\mathbb{R}[x]$. 若$a\neq 0$，则$(ax+b)^2=a^2(x^2+2\cdot\frac{b}{a}x+\frac{b^2-1}{a^2})+1$. 得$a=-2,b=3$；或$a=2,b=-3$. 得$G$的两个2阶元$-2x+3$和$2x-3$. 若$a=0$，则有两解$-1$和$1$，后者是$G$的单位元.

参考文献

[1]Atiyah.M..Macdonald Introduction to Commutative Algebra.Universitat Politècnica de Catalunya，2011.

[2]柯召，孙琦.数论讲义（上册）[M].第二版：高等教育出版社，2001.

[3]孙智伟.基础数论入门[M].哈尔滨工业大出版社，2014.4，ISBN：9978-7-5603-4189-7.

[4]聂灵沼，丁石孙.代数学引论[M].第二版：高等教育出版社，2000.

[5]杨子胥.近世代数[M].第四版：高等教育出版社，2003.