这一章我们讲讲有限阿贝尔群。

有限阿贝尔群

我们将证明每个有限阿贝尔群是循环群的直和。首先让我们看看什么是直和。

定义 1外直和. 2个阿贝尔群S,T的外直和记为$S\times T$，其做基础的集合是S和T的笛卡尔积，我们定义运算为：$(s,t)+(s',t')=(s+s',t+t')$

定义 2（内直和）. 若S和T是阿贝尔群G的子群，则G是一个内直和，定义为$G=S\oplus T$，每一个$g\in G$可被唯一的表示$g=s+t$，其中$s\in S,t\in T$

若S，T是阿贝尔群G的子群，定义

$$S+T=\{s+t\colon s\in S\text{和}t\in T\}$$

则$S+T$总是G的子群。因为他就是$\langle S\cup T\rangle$，由S和T生成的子群。我们说$G=S+T$，这是在说每个$g\in G$能分解为$g=s+t$。其中$s\in S$和$t\in T$。而当我们说$G=S\oplus T$是在说这种表示唯一。

引理 3. 若S和T是阿贝尔群G的子群，则$G=S\oplus T$当且仅当$S+T=G$且$S\cap T=\{0\}$

证明. 设$G=S\oplus T$，每个$g\in G$都有唯一分解$g=s+t$。其中$s\in S,t\in T$。因此$G=S+T$。若$x\in S\cap T$，则x有两种分解,但由于表示唯一，那么$x=x+0=0+x$。x只能是0才满足上述关系，因此$S\cap T=\{0\}$

反之，设$G=S+T$，则每个$g\in G$都有形如$g=s+t$的分解。设$g=s+t=s'+t'$，它给出$s-s'=t'-t\in S\cap T=\{0\}$，因此$s=s',t=t'$证毕。 □

定义 4. 一个阿贝尔群G的子群S称为**直和**的，若这里存在G的子群T使得$G=S\oplus T$，因此$S+T=G$和$S\cap T=\{0\}$

注意$S\times T$不等于$S\oplus T$，因为S和T都不是$S\times T$的子群。实际上，他们甚至不是其笛卡尔积的子集。但这有解决的方法，只需要定义阿贝尔群S,T，定义其子群S^*,T^*的外直和为

$$S^*=\{(s,0)\colon s\in S\}\text{和}T^*=\{(0,t)\colon t\in T\}$$

$S\cong S^*$通过$s\mapsto(s,0)$和$T\cong T^*$由$t\mapsto(0,t)$定义而来。我们可以快速的检查$S\times T=S^*\oplus T^*$，对于$S^*+T^*=S\times T$，由于$(s,t)=(s,0)+(0,t)$且$S^*\cap T^*=\{(0,0)\}$，因此，其内直积可以被表示为外直积

引理 5. 令S和T是阿贝尔群G的子群使得$G=S+T$。若$G=S\oplus T$，则这里存在同构$\varphi\colon S\oplus T\to S\times T$使得$\varphi(S)=S^*$和$\varphi(T)=T^*$。

证明. 若$g\in S\oplus T$，则引理3告诉我们g是被唯一表示为$g=s+t$的。定义：$\varphi\colon S\oplus T\to S\times T$由$\varphi(g)=\varphi(s+t)=(s,t)$给出。唯一表示$g=s+t$可以推导出$\varphi$是定义良好的函数。另一方面，该函数告诉了我们$\varphi(S)=S^*,\varphi(T)=T^*$。我们现在来检查$\varphi$是同态。取另一个不同的元素$g'=s'+t'$，那么$(s,t)+(s',t')=(s+s',t+t')$。因此

$$\begin{aligned}\varphi(g+g') &= \varphi(s+s'+t+t')\\ &= (s+s',t+t')\\ &= (s,t)+(s',t')\\ &= \varphi(g)+\varphi(g')\end{aligned}$$

若$\varphi(g)=(s,t)=(0,0)$，则$s=0,t=0$且$g=s+t=0$。所以φ是单射的。最后，若$(s,t)\in S\times T$，则$\varphi(s+t)=(s,t)$是满射是容易得到的。 □

定义 6（外直和）. 阿贝尔群$S_1,\cdots S_n$的外直和是阿贝尔群$S_1\times\cdots\times S_n$，其做集合的基础也是由笛卡尔积得到的。且其运算由下给出：

$$(s_1,\cdots,s_n)+(s_1',\cdots,s_n')=(s_1+s_1',\cdots,s_n+s_n')$$

例如：n维空间$R^n=R\times R\times\cdots$，它是$R$和自身做了$n$次外直和得到的

定义 7(内直和). 若$S_1,\cdots,S_n$是阿贝尔群G的子群，则G的内直和记为

$$S_1\oplus\cdots\oplus S_n=G$$

即对每个$g\in G$都有唯一的$s_i\in S_i$使得$g=s_1+\cdots+s_n$

例 8.

令k是域和$G=k^n$是k自身做n次外直和得到的。那么令$e_1,\cdots,e_n$是一组基。其中$e_i=(0,\cdots,0,1,0,\cdots,0)$是第$i$个系数为1且其他系数为0的。若$V_i$是由$e_i$生成的一维子空间，那么$V_i=\{a\,e_i:a\in k\}$，则$k^n$是$k^n=V_1\oplus\cdots\oplus V_n$的内直和得到的。且对每个向量是有唯一表示的基的线性组合。

引理 9. 令$G=S_1+\cdots+S_n$，其中S_i是子群，因此，每个$g\in G$都有唯一表示：

$$g=s_1+s_2+\cdots+s_n$$

其中对i，$s_i\in S_i$。则下列条件是等价的。

1. $G=S_1\oplus S_2\oplus\cdots\oplus S_n$，对每个$g\in G$有表示$g=s_1+\cdots+s_n$。其中$s_i\in S_i$是唯一的。

2. 存在同构$\varphi\colon G\to S_1\times S_2\times\cdots\times S_n$，其中$\varphi(S_i)=S_i^*$对每个$i$成立

3. 若定义$G_i=S_1+\cdots+\hat{S}_i+\cdots+S_n$，其中$\hat{S}_i$的意思从和中省略$S_i$，这意味着$S_i\cap G_i=\{0\}$对每个$i$成立。

证明. 我们先从1推到2。若$g\in G$且$g=s_1+\cdots+s_n$。我们定义$\varphi\colon G\to S_1\times\cdots\times S_n$由$\varphi(g)=\varphi(s_1+\cdots+s_n)=(s_1,\cdots,s_n)$决定的。由于$g$是唯一表示的，这说明$\varphi$是定义良好的，这足以证明$\varphi$是同构使得$\varphi(S_i)=S_i^*$对每个$i$成立

然后是2到3,。若$g\in S_i\cap G_i$，则$\varphi(g)\in S_i^*\cap(S_1^*+\cdots+\hat{S}_i+\cdots+S_n)$。但由定义，第$i$个元素的是0。若$\varphi(g)\in S_i^*$，则其除了第$i$位元素其他都不为0。另一个方面，$\varphi(g)\in(S_1^*+\cdots+\hat{S}_i+\cdots+S_n)$，这意味着$\varphi(g)=0$。由于$\varphi$是同构，所以$g=0$

最后我们从3推到1。令$g\in G$，且设

$$g=s_1+\cdots+s_n=t_1+\cdots+t_n$$

其中对每个i，$t_i,s_i\in S_i$。对每个i，由上述式子我们有$s_i-t_i=\sum_{j\neq i}(t_j-s_j)$,左边在$S_i$中，但等式右边则没有第$i$项。即$s_i-t_i=\sum_{j\neq i}(t_j-s_j)\in S_i\cap G_i=S_1+\cdots+\hat{S}_i+\cdots+S_n=\{0\}$。因此$s_i=t_i$对每个$i$成立。 □

记法 10. 我们在以后都使用记号$S_1\oplus\cdots\oplus S_n$表示任意一种直和、内直和、和外直和。因为我们的直和几乎都是指向内直和，我们将记

$$\bigoplus_{i=1}^{n}S_i=S_1\oplus\cdots\oplus S_n$$

用$G=\sum_{i=1}^{n}S_i$来缩写$G=S_1+\cdots S_n=\langle S_1\cup\cdots\cup S_n\rangle$。因此，若其中每个$g\in G$都可以表示为$g=\sum_{i=1}^{n}s_i$，则若$G=\sum_{i=1}^{n}S_i$，且若g的分解表示唯一，则$G=\bigoplus S_i$

定义 11. 若p是素数，则一阿贝尔群G是$p-$准素的。若它对每个$a\in G$，存在$n\geq 1$使得$p^n a=0$

若G是容易阿贝尔群，则它的$p-$准素分支是

$$G_p=\{a\in G\colon p^n a=0\text{对某个}n\geq 1\}$$

若我们不特指一个素数p，我们说阿贝尔群G是准素的（而不是$p-$准素的）。准素分支明显的是一个子群。但在非阿贝尔群中是不成立的。例如：若$G=S_3$，则$G_2=\{(1),(1\,2),(1\,3),(2\,3)\}$，但它不是$S_3$的子群，因为$(1\,2)(1\,3)=(1\,3\,2)\notin G_2$

定理（准素分解） 12.

1. 每个有限阿贝尔群G是一些p-准素分支的直和

$$G=\bigoplus_p G_p$$

2. 两个有限阿贝尔群G,G'同构当且仅当$G_p\cong G'_p$对每个素数p成立。

证明.

1. 令$x\in G$非零，再设它的阶为d。利用算术基本定理，则它被分解为不同素数$p_1\cdots p_n$和正指数$e_1\cdots e_n$有：

$$d=p_1^{e_1}\cdots p_n^{e_n}$$

定义$r_i=d/p_i^{e_i}$，那么$p_i^{e_i}r_i=d$。那么我们进一步得到$r_i x\in G_{p_i}$对每个i成立。但$r_1,\cdots r_n$的gcd是1。那么就存在整数$s_1,\cdots,s_n$使得$\sum_i s_i r_i=1$成立。因此

$$x=\sum_i s_i r_i x\in G_{p_1}+\cdots+G_{p_n}$$

我们像引理9的命题3一样简单记$H_i=G_{p_1}+\cdots+\widehat{G_{p_i}}+\cdots G_{p_n}$。只需证明，若

$$x\in G_{p_i}\cap H_i$$

则$x=0$即可。由于$x\in G_{p_i}$和$x\in H_i$。第一方面，我们有$p_i^\ell x=0$对某个$\ell\geq 0$成立，另一方面，又因为$x\in H_i$，那么就有$\mathrm{ux}=0$，其中$u=\Pi_{j\neq i}\, p_j^{g_j}, g_j\geq 0$。由于$p_i^\ell$和$u$是互素的，那就存在一些整数$s,t$使得$1=\mathrm{sp}_i^\ell+\mathrm{tu}$成立。从而

$$x=(\mathrm{sp}_i^\ell+\mathrm{tu})\,x=0$$

2. 若$f\colon G\to G'$是同态，则$f(G_p)\subseteq G'_p$对某个p成立。若$p^\ell a=0$，则$0=f(p^\ell a)=p^\ell f(a)$。但$f$是同构，则$f^{-1}\colon G'\to G$也是同构（古早前证明过）那么$f^{-1}(G'_p)\subseteq G_p$。这说明，如果我们对定义域限制。$f|\,G_p\colon G_p\to G'_p$是同构。逆为$f^{-1}|\,G'_p$

   反之，若对所有的p存在同构$f_p\colon G_p\to G'_p$，则存在一个同构$\varphi\colon\bigoplus_p G_p\to\bigoplus_p G'_p$由$\sum_p a_p\mapsto\sum_p f_p(a_p)$给出。

□

记法 13. 若G是阿贝尔群且m是整数，则

$$mG=\{ma\colon a\in G\}$$

可以验证$m\,G$是G的子群。

定义 14. 令p是素数和令G是$p-$准素阿贝尔群。一个子群$S\subseteq G$是纯子群，若对所有$n\geq 0$有

$$S\cap p^nG=p^nS$$

$S\cap p^nG\supseteq p^nS$对每个$S\supseteq G$成立。所以上述结论的反包含才有比较重要的意义。我们说$s\in S$满足等式$s=p^nx$可以解出$x\in G$，则对$x\in S$也是有解的。

引理 15. 若p是素数且$G\neq\{0\}$是有限$p-$准素阿贝尔群，则G有非零的纯循环子群。

证明. 令$G=\langle x_1,\cdots,x_q\rangle$。对所有的i，$x_i$的阶是$p^{n_i}$。由于$G$是p准素的。若$x\in G$,则$x=\sum_i a_ix_i$，其中$a_i\in\mathrm{Z}$。若$\ell$是$n_i$中最大的那项。则$p^\ell x=0$。我们选择任意$y\in G$，它的阶是$p^\ell$。我们讲$S=\langle y\rangle$是$G$的纯子群。现在来证明它

设$s\in S$使得$s=\mathrm{mp}^ty$，其中$t\geq 0$且$p\nmid m$，且令

$$s=p^na$$

对某个$a\in G$成立。若$t\geq n$，定义$s'=\mathrm{mp}^{t-n}y\in S$，那么验证一下定义

$$p^ns'=p^n\mathrm{mp}^{t-n}y=\mathrm{mp}^ty=s$$

其次，若$t<n$，则

$$p^\ell a=p^{\ell-n}p^na=p^{\ell-n}s=p^{l-n}\mathrm{mp}^ty=\mathrm{mp}^{\ell-n+t}y$$

但由于$l-n+t<l$，因为里面-n+t<0，那么我们立刻就知道$p^\ell a\neq 0$，这样子的y是不存在的。与其是最大元矛盾。 □

引理 16. 若G是阿贝尔群和p是素数，则G/pG是$\mathbb{F}_p$上的线性空间，当G有限时它是有限维的

证明. 若$[r]\in\mathbb{F}_p$和$a\in G$，定义标量乘法

$$[r](a+\mathrm{pG})=\mathrm{ra}+\mathrm{pG}$$

若$k=r \bmod p$，则存在整数m使得$k=r+\mathrm{pm}$成立。那么

$$ka+pG=ra+pma+pG=ra+pG$$

因为$p\,\mathrm{ma}\in G$，我们可以来证明向量空间的公里成立。并且G是有限的，所以$G/p\,G$也是有限的且有有限基。 □

定义 17. 若p是素数和G是有限的$p-$准素阿贝尔群，则

$$d(G)=\dim(G/pG)$$

另外，d上的直和是可加的

$d(G\oplus H)=d(G)+d(H)$

定义$f\colon G\oplus H\rightarrow(G/p\,G)\times(H/p\,H)$，利用第一同构定理就有

$$\frac{G\oplus H}{p(G\oplus H)}\cong\frac{G}{pG}\oplus\frac{H}{pH}$$

用$G/p\,G$的一个基并上$H/p\,H$的一个基就可以得到$(G/p\,G)\oplus(H/p\,H)$的一个基，因此，上述等式左边的维数是$d(G\oplus H)$，右边是$d(G)+d(H)$

定理 18. 若G是$p-$准素阿贝尔群，则$d(G)=1$当且仅当G是循环群。

证明. 若G是循环的，则G的商群也是循环群，特别的$G/p\,G$也是循环群，因此dim(G/pG)=1。 □

反之，设$d(G)=1,$则$G/p\,G\cong\mathbb{I}_p$。由于$\mathbb{I}_p$是单群，它的正规子群只有单位和自身。由于$p\,G$也是子群，那么它是里面的一个极大子群。现在我们来证明$p\,G$是唯一的极大子群。令$L\subseteq G$是任意的极大子群，则$G/L\cong\mathbb{I}_p$，由于它是阶为p的方幂的单阿贝尔群。所以他的阶是p。因此，若$a\in G$，则在G/L中$p(a+L)=0$。因此$pa\in L$。由于$p\,G\subseteq L$。但pG是极大的，因此$pG=L$，由此可以得出G的每个真子群都被pG包含。现在，$G/pG\cong\mathbb{I}_p$是循环的。设对$z\in G$有$G/p\,G=\langle z+p\,G\rangle$，若$\langle z\rangle$是真子群，则$\langle z\rangle\subseteq p\,G$。但这就与$z+\mathrm{pG}$是$G/p\,G$的生成元矛盾了，为此$G=\langle z\rangle$。所以$G$是循环的。

引理 19. 令G是有限p-准素阿贝尔群，则

1. 若$S\subseteq G$，则$d(G/S)\leq d(G)$

2. 若S是G的纯子群，则

$$d(G)=d(S)+d(G/S)$$

证明. 由对应定理，$p(G/S)=(\mathrm{pG}+S)/S$，那么由第三同构定理有

$$(G/S)/p(G/S)=(G/S)/[(pG+S)/S]\cong G/(\mathrm{pG}+S)$$

由于$p\,G\subseteq p\,G+S$，那么这里存在满射同态

$$G/\,pG\to G/\,(pG+S)$$

也就是把$g+p\,G\mapsto g+(p\,G+S)$。商群G/pG的阶就是$|\,G|/|\,p\,G|$，因此我们有$\dim(G/\,p\,G)\geq\dim(G/\,(pG+S))$。利用定义17就有结论了。 □

证明. 我们分析$(p\,G+S)/\,p\,G$，它是函数$G/\,p\,G\to G/\,(p\,G+S)$的核。由第二同构定理有

$$(pG+S)\,/\,(pG)\cong S/\,(S\cap pG)$$

由于S是纯子群，$S\cap p\,G=p\,S$。因此

$$(pG+S)\,/\,pG\cong S/\,pS$$

那么利用定义17就有$\dim[\,(p\,G+S)\,/\,p\,G]=d(S)$。但是，若$W$是向量空间$V$的一个子空间，那么我们知道$\dim(V)=\dim(W)+\dim(V/\,W)$，然后带入$V=G/\,p\,G$和$W=(pG+S)\,/\,p\,G$，就得到

$$d(G)=d(S)+d(G/\,S)$$ □

定理(基定理) 20. 每个有限阿贝尔群G是一些准素循环群的直和

证明. 利用准素分解定理，我们可以假设G是一个$p-$准素群。我们通过对$d(G)\geq 1$归纳证明G是一些循环群的直和。基本步骤就是我们的定理18，当$d(G)=1$时G是循环群。当对$d(G)>1$做验证时，注意到$G/\,pG$是一个F_p上的向量空间，我们在做的事情就是在验证，当我们拓展G时，我们要验证其基和元素做运算时依然是循环元。并利用其生成循环群。

其次，利用定理19，我们就有$d(G/\,S)<d(G)$，这对下一步至关重要。那么由于S是G的子群，则有

$$d(G/\,S)=d(G)-d(S)=d(G)-1<d(G)$$

由归纳法，$d(G/\,S)$刚刚好就是满足归纳法的群。那么它就是一些循环群的直和，记为

$$G/\,S=\bigoplus_{i=1}^{q}\langle\bar{x_i}\rangle$$

其中$\bar{x_i}=x_i+S$

现在，令$x\in G$和$\bar{x}$的阶为p^ℓ，其中$\bar{x}=x+S$。我们证明$z\in G$使得$z+S=\bar{x}=x+S$且$\bar{x}$和z是有相同的阶的。设x的阶为p^n，其中$n\geq\ell$。但$p^\ell(x+S)=p^\ell\bar{x}=0\in G/\,S$，那么这里就存在一些$s\in S$使得$p^\ell x=s$。由纯的定义，这里就有一些$s'\in S$有$p^\ell x_i=p^\ell s'$。然后我们定义$z=x-s'$，则$z+S=x+S$且$p^\ell z=0$，所以，若$m\,\bar{x}=0\in G/\,S$，那么有$p^\ell|\,m$，有$\mathrm{mz}=0\in G$。

对每个i，选择$z_i\in G$使得$z_i+S=x_i+S=\bar{x}$。且有z_i的阶等于$\bar{x_i}$，令$T=\langle z_1,\cdots,z_q\rangle$。那么现在$S+T=G$，由于$G$是由$S$和$z_i$生成的。为了证明$G=S\oplus T$。我们得证明$S\cap T=\{0\}$。若$y\in S\cap T$，则$y=\sum_i m_i z_i$，其中$m_i\in\mathbb{Z}$。其次，也有$y=\sum_i m_i\bar{x_i}=0$∈G/S成立。由于这是一个直和，每个$m_i\bar{x_i}=0$。最后，对每个i有

$$-m_i\bar{x_i}=\sum_{i\neq j}m_j\bar{x_j}\in\langle\bar{x_i}\rangle\cap\left(\langle\bar{x_1}\rangle+\cdots\widehat{\langle\bar{x_i}\rangle}+\cdots+\langle\bar{x_q}\rangle\right)=\{0\}$$

因此$y=0$。

最后，$G=S\oplus T$意味着$d(G)=d(S)+d(T)=1+d(T)<d(G)$，由归纳假设，$T$是循环群的直和，我们也完成了证明。 $\square$

什么时候两个有限阿贝尔群G,G'是同构的呢？由基定理，这些群是一些循环群的直和，那么我们的直觉告诉我们也许$G\cong G'$意味着它们同类型的循环群的数量是一样的。但这个不成立，因为$\mathbb{I}_{m\times n}\cong\mathbb{I}_m\times\mathbb{I}_n$当且仅当$m,n$是互素的。所以我们转而尝试计算其准素循环项的个数，但是如何计算呢？但这又有另一个问题，也就是是否存在唯一的分解定理。

在学习下一个定理之前，我们先来回忆一些定义

$$d(G)=\dim(G/pG)$$

特别的，$d(p\,G)=\dim(p\,G/p^2G)$。我们就有更一般的定理

$$d(p^n\,G)=\dim(p^nG/p^{n+1}G)$$

引理 21. 令G是有限$p-$准素阿贝尔群，其中p是素数。再令$G=\bigoplus_j C_j$，其中C_j是循环群。若b_n是阶为p^n的群C_j的直和项个数。则这里对某个$t\geq 1$有

$$d(p^nG)=b_{n+1}+b_{n+2}+\cdots+b_t$$

证明. 令B_n是全部阶为p^n的C_j的直和，那么就存在某个t使得

$$G=B_1\oplus B_2\oplus\cdots\oplus B_t$$

由于对所有$j\leq n$都存在$p^nB_j=\{0\}$，那么

$$p^nG=p^nB_{n+1}\oplus\cdots\oplus p^nB_t$$

类似的

$$p^{n+1}G=B_{n+2}\oplus\cdots\oplus p^{n+1}B_t$$

我们引入如下定理辅助证明：

> **定理.** 设G,G'是群，且$K\lhd G$和$K'\lhd G'$是正规子群，则$K\times K$是$G\times G'$的正规子群且存在同构
>
> $$(G\times G)/(K\times K')\cong(G/K)\times(G'/K')$$

那么就有$p^nG/p^{n+1}G$同构于

$$[p^nB_{n+1}/p^{n+1}B_{n+1}]\oplus[p^nB_{n+2}/p^{n+1}B_{n+2}]\oplus\cdots\oplus[p^nB_t/p^{n+1}B_t]$$

d在直和上是可相加的，那么就有

$$d(p^nG)=b_{n+1}+\cdots+b_t$$ $\square$

定义 22. 若G是有限$p-$准素阿贝尔群，其中p是素数，则

$$U_p(n,G)=d(p^nG)-d(p^{n+1}G)$$

引理21告诉了我们一些事情，那么

$$d(p^nG)=b_{n+1}+\cdots+b_t$$

和

$$d(p^{n+1}G)=b_{n+2}+\cdots+b_t$$

因此$U_p(n,G)=b_{n+1}$

定理 23. 若p是素数，则对于有限$p-$准素阿贝尔群G的任意两种化为循环群直和的分解，它们每种类型的循环直和项个数是相同的。准确的说，对每个$n\geq 0$循环直和项其阶是p^{n+1}，它是U_p (n, G)

证明. 由基定理，这里就存在一些循环群C_i使得$G=\bigoplus_j C_j$，利用引理21，阶为p^{n+1}的C_j个数就是$U_p(n,G)$。这是与循环直和分解无关的数。因此，若存在另一个分解$G=\bigoplus_j D_j$，其中每个D_j是循环的、则阶为p^{n+1}的循环直和项也是$U_p(n,G)$ □

推论 24. 若G,G'是有限$p-$准素阿贝尔群，则$G\cong G'$当且仅当$U_p(n,G)=U_p(n,G')$对每个$n\geq 0$都成立。

证明. 设φ:$G\to G'$是同构，则$\varphi(p^nG)=p^nG'$对所有$n\geq 0$成立。因此它引出了在F_p上的线性空间$p^nG/p^{n+1}G\cong p^nG'/p^{n+1}G'$。由于他们的维数相同，就有$U_p(n,G)=U_p(n,G')$

反之，设$U_p(n,G)=U_p(n,G')$对所有$n\geq 0$成立。若$G=\bigoplus_i C_i$和$G'=\bigoplus_j C_j'$是循环的，由定理21，这里每种类型的直和数量相同，那么就可以建立在上面的一个同构$G\to G'$ □

定义 25. 若G是$p-$准素阿贝尔群，则G的初等因子是一些数p^{n+1}，每一个重复$U_p(n,G)$次。

若G是有限阿贝尔群，则G的初等因子就是所有准素分支的初等因子。

例如：阿贝尔群$\mathbb{I}_2\oplus\mathbb{I}_2\oplus\mathbb{I}_2$的初等因子就是$(2,2,2)$，而$\mathbb{I}_6$是$(2,3)$，因为可以看成是$\mathbb{I}_2\oplus\mathbb{I}_3$

有限阿贝尔群的基本定理 26. 有限阿贝尔群G,G'同构当且仅当它们有相同的初等因子，也就是G, G'的任两个准素循环群的直和分解中每个阶的直和项数相同。

证明. 利用定理24，G,G''同构当且仅当对每个p，它们的准素分支是同构的。然后利用定理23,即可证明完毕。 □

这个章节的结论告诉我们，一个阿贝尔群G叫做有限生成的，若存在有限个元素$a_i,i=1,2,\cdots,n$使得每个元素$x\in G$都是一个线性组合，即$x=\sum m_ia_i$，对所有$m\in Z$成立。