서울大學校 師大論叢 第31輯(1985. 12. 30)

The Orders of End(G) and Aut(G) for Finite Abelian Group G

Eung Tai Kim
(Department of Mathematics Education)

I. Preliminaries

In this paper we represent the endomorphism ring End(G) and the unit group of the ring End(G), *i.e.*, Aut(G), by matrices with integral elements for finite abelian group G and we give the orders of End(G) and Aut(G).

The following lemmas are used to prove the main theorems.

Lemma 1. *Let G be a finite abelian group.* Then,

(1) *There is a unique list of positive integers $m_1, m_2, \cdots, m_t$ such that $1<m_1|m_2|\cdots|m_t$ and*

$$G\cong \boldsymbol{Z}_{m_1}\oplus\boldsymbol{Z}_{m_2}\oplus\cdots\oplus\boldsymbol{Z}_{m_t}.$$

(2) *There is a list of positive integers $p_1^{s_1}, p_2^{s_2}, \cdots, p_k^{s_k}$, which is unique except for the order of its members, such that $p_1, p_2, \cdots, p_k$ are primes, $s_1, s_2, \cdots, s_k$ are positive integers and*

$$G\cong \boldsymbol{Z}_{p_1^{s_1}}\oplus\boldsymbol{Z}_{p_2^{s_2}}\oplus\cdots\oplus\boldsymbol{Z}_{p_k^{s_k}}.$$

This lemma is the structure theorem for finite abelian groups which is called *Fundamental Theorem for Finite Abelian Groups.* The uniquely determined integers $m_1, m_2, \cdots, m_t$ in Lemma 1(1) are called *the invariant factors of G*, and the uniquely determined prime powers in Lemma 1(2) are called *the elementary divisors of G.*

Lemma 2. *Let $G_1, G_2, \cdots, G_t$ be finite abelian additive groups which have the orders relatively prime in pairs. Then we have*

$$\mathrm{End}(G_1\oplus G_2\oplus\cdots\oplus G_t)\cong \mathrm{End}(G_1)\oplus\cdots\oplus\mathrm{End}(G_t),$$
$$\mathrm{Aut}(G_1\oplus G_2\oplus\cdots\oplus G_t)\cong \mathrm{Aut}(G_1)\times\cdots\times\mathrm{Aut}(G_t).$$

Proof. Let φ be an elment of End($G_1\oplus\cdots\oplus G_t$) and let $n_i=o(G_i)$ be the order of G_i. For arbitrary element a_i of G_i, we put

$$\varphi(0, \cdots, 0, a_i, 0, \cdots, 0)=(b_1, \cdots, b_i, \cdots, b_t).$$

Then,

$$\begin{aligned}(0,\cdots,0,\cdots,0)&=\varphi(0,\cdots,n_ia_i,\cdots,0)\\&=n_i\varphi_i(0,\cdots,a_i,\cdots,0)\\&=n_i(b_1,\cdots,b_i,\cdots,b_t)\\&=(n_ib_1,\cdots,0,\cdots,n_ib_t).\end{aligned}$$

Therefore $n_ib_j=0$ for all $j\neq i$ and $o(b_j)\mid n_i$ where $o(b_j)$ is the order of b_j. Hence $o(b_j)=1$, since $o(b_j)$ is a divisor of n_j and $(n_i,n_j)=1$ for $j\neq i$. That is $b_j=0$ for $j\neq i$ and

$$\varphi(0,\cdots,a_i,\cdots,0)=(0,\cdots,b_i,\cdots,0).$$

Therefore we may define a homomorphism $\varphi_i: G_i\to G_i$ by $\varphi_i(a_i)=b_i$ where a_i and b_i are elements of G_i such that $\varphi(0,\cdots,a_i,\cdots,0)=(0,\cdots,0,b_i,0,\cdots,0)$.

Now we define a mapping $F:\mathrm{End}(G_1\oplus\cdots\oplus G_t)\to\mathrm{End}(G_1)\oplus\cdots\oplus\mathrm{End}(G_t)$ by $F(\varphi)=(\varphi_1,\cdots,\varphi_t)$. Then it is easily seen that F is a ring isomorphism of $\mathrm{End}(G_1\oplus\cdots\oplus G_t)$ onto $\mathrm{End}(G_1)\oplus\cdots\oplus\mathrm{End}(G_t)$ and the restriction $F|_{\mathrm{Aut}(G_1\oplus\cdots\oplus G_t)}$ is a group isomorphism of $\mathrm{Aut}(G_1\oplus\cdots\oplus G_t)$ onto $\mathrm{Aut}(G_1)\times\cdots\times\mathrm{Aut}(G_t)$.

Lemma 3. *Let p be a prime and let $GL(n,\boldsymbol{Z}_{p^e})$ be the general linear group of degree n over the ring $\boldsymbol{Z}_{p^e}$. Then the order of $GL(n,\boldsymbol{Z}_{p^e})$ is given by*

$$p^{en^2}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right)\cdots\left(1-\frac{1}{p^n}\right).$$

The proof of this lemma can be found in [1].

II. The Ring $\mathfrak{M}(p;e_1,e_2,\cdots,e_r)$

Let p be a prime and $e_1,e_2,\cdots,e_r$ be positive integers such that $1\leqslant e_1\leqslant e_2\leqslant\cdots\leqslant e_r$ and let $\mathfrak{M}=\mathfrak{M}(p;e_1,e_2,\cdots,e_r)$ be the set of all matrices of the form

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r-1} & a_{1r}\\ p^{e_2-e_1}a_{21} & a_{22} & \cdots & a_{2r-1} & a_{2r}\\ p^{e_3-e_1}a_{31} & p^{e_3-e_2}a_{32} & \cdots & a_{3r-1} & a_{3r}\\ & & \cdots & & \\ p^{e_r-e_1}a_{r1} & p^{e_r-e_2}a_{r2} & \cdots & p^{e_r-e_{r-1}}a_{rr-1} & a_{rr}\end{pmatrix},$$

$a_{ij}\in\boldsymbol{Z}$. Then it is easy to verify that $\mathfrak{M}(p;e_1,e_2,\cdots,e_r)$ is a ring with unit element I. Now, we define the relation $\sim$ on $\mathfrak{M}(p;e_1,\cdots,e_r)$ by

$$A\sim B\leftrightarrows c_{ij}\equiv d_{ij}\bmod p^{e_i}\text{ for }A=[c_{ij}]\text{ and }B=[d_{ij}],\ 1\leq i,j\leq r,$$

where $c_{ij}=p^{e_i-e_j}a_{ij}$ and $d_{ij}=p^{e_i-e_j}b_{ij}$ for $i>j$. Incidentally we see that for $i>j$,

$$c_{ij}\equiv d_{ij} \bmod p^{e_i} \Leftrightarrow a_{ij}\equiv b_{ij} \bmod p^{e_i}.$$

Then the relation $\sim$ is an equivalence relation on $\mathfrak{M}(p;e_1,\cdots,e_r)$. Let $\bar{A}$ be the equivalence class containing matrix A and let $\mathfrak{M}/\sim$ be the set of all equivalence classes.

Now we define addition and multiplication on $\mathfrak{M}/\sim$ by

$$\bar{A}+\bar{B}=\overline{A+B},\quad \bar{A}\bar{B}=\overline{AB}.$$

Then we can easily verify that the addition and multiplication are well defined and $(\mathfrak{M}/\sim,+,\cdot)$ is a ring with unit element $\bar{I}$.

By the definition of the relation $\sim$, the equivalence class $\bar{A}$ is represented by unique matrix whose (i,j) element a_{ij} is an element in the prescribed complete set of residues modulo p^{e_i} if $i\leq j$ and modulo p^j if $i>j$ respectively.

Therefore, since the number of choices of a_{ij} is p^{e_i} if $i\leq j$ and p^{e_j} if $i>j$ respectively, the order of $\mathfrak{M}/\sim$ is

$$(p^{e_1})^r(p^{e_2})^{r-1}\cdots(p^{e_{r-1}})^2p^{e_r}(p^{e_1})^{r-1}(p^{e_2})^{r-2}\cdots(p^{e_{r-2}})^2p^{e_{r-1}}=p^{k^{\sum_1^r(2r-2k+1)e_k}}.$$

Thus we get

Lemma 4. *The order of the ring $\mathfrak{M}(p;e_1,\cdots,e_r)/\sim$ is given by*

$$p^{\sum_{k=1}^{r}(2r-2k+1)e_k}.$$

Now we determine the unit group $U(\mathfrak{M}/\sim)$ of the ring $\mathfrak{M}/\sim$. If $\bar{A}\in U(\mathfrak{M}/\sim)$, there exists $\bar{B}\in\mathfrak{M}/\sim$ such that $\overline{AB}=\bar{A}\bar{B}=\bar{B}\bar{A}=\overline{BA}=\bar{I}$, *i.e.*,

$$AB=I+\begin{pmatrix} p^{e_1}f_{11} & p^{e_1}f_{12} & \cdots\cdots & p^{e_1}f_{1r}\\ p^{e_1}f_{21} & p^{e_2}f_{22} & \cdots\cdots & p^{e_2}f_{2r}\\ & & \cdots\cdots & \\ p^{e_1}f_{r1} & p^{e_2}f_{r2} & \cdots\cdots & p^{e_r}f_{rr}\end{pmatrix}.$$

Therefore $(\mathrm{Det}(A))(\mathrm{Det}(B))=\mathrm{Det}(AB)=1+pk$ for some $k\in\boldsymbol{Z}$, hence $(\mathrm{Det}(A),p)=1$.

Conversely, suppose that $(\mathrm{Det}(A),p)=1$ for $\bar{A}\in\mathfrak{M}/\sim$. It is easily shown that the adjoint of A, *i.e.*, $\mathrm{Adj}(A)$, is also an element of $\mathfrak{M}$ for any $A\in\mathfrak{M}$, and

$$\mathrm{Adj}(A)A=A\mathrm{Adj}(A)=\mathrm{Det}(A)I.$$

Since $(\mathrm{Det}(A),\ p^{e_r})=1$, there exist $u,v\in\boldsymbol{Z}$ such that $\mathrm{Det}(A)u-p^{e_r}v=1$ and

$$u\mathrm{Adj}(A)A=A(u\mathrm{Adj}(A))=u\mathrm{Det}(A)I=(1+p^{e_r}v)I=I+p^{e_r}vI\sim I.$$

Therefore, $\overline{u\mathrm{Adj}(A)}\bar{A}=\bar{A}\,\overline{u\,\mathrm{Adj}(A)}=\bar{I}$, that is,

$$\bar{A}^{-1}=\overline{u\,\mathrm{Adj}(A)}\in\mathfrak{M}/\sim.$$

Thus we have proved

Lemma 5. *The element* $\bar{A}\in\mathfrak{M}/\sim$ *is unit if and only if* $(\mathrm{Det}(A),p)=1$, *that is,*

$$U(\mathfrak{M}/\sim)=\{\bar{A}\in\mathfrak{M}/\sim\mid A\in\mathfrak{M}\ \textit{and}\ (\mathrm{Det}(A),p)=1\}.$$

Now suppose that

$$1\leq e_1=\cdots=e_{k_1}<e_{k_1+1}=\cdots=e_{k_1+k_2}<\cdots<e_{k_1+\cdots+k_{s-1}+1}=\cdots=e_{k_1+\cdots+k_s}=e_r.$$

If we denote $e_{k_1}=f_1, e_{k_1+k_2}=f_2, \cdots, e_{k_1+\cdots+k_s}=f_s$, then every matrix A of $\mathfrak{M}(p;e_1,\cdots,e_r)$ has the following form

$$A=\begin{pmatrix} A_{11} & A_{12}\cdots\cdots A_{1s-1} & A_{1s}\\ p^{f_2-f_1}A_{21} & A_{22}\cdots\cdots A_{2s-1} & A_{2s}\\ p^{f_3-f_1}A_{31} & p^{f_3-f_2}A_{32}\cdots\cdots A_{3s-1} & A_{3s}\\ & \cdots\cdots\cdots & \\ p^{f_s-f_1}A_{s1} & p^{f_s-f_2}A_{s2}\cdots p^{f_s-f_{s-1}}A_{ss-1} & A_{ss}\end{pmatrix},$$

where A_{ij} is $k_i\times k_j$ matrix. Thus we may write $A=A_0+P$ where

$$A_0=\begin{pmatrix} A_{11} & A_{12}\cdots\cdots A_{1s}\\ 0 & A_{22}\cdots\cdots A_{2s}\\ & \cdots\cdots & \\ 0 & 0\cdots\cdots A_{ss}\end{pmatrix},\qquad P=\begin{pmatrix} 0 & 0\cdots\cdots 0\\ p^{f_2-f_1}A_{21} & 0\cdots\cdots 0\\ & \cdots\cdots & \\ p^{f_s-f_1}A_{s1} & p^{f_s-f_2}A_{s2}\cdots\cdots 0\end{pmatrix}.$$

Then, we have

$$\bar{A}\in U(\mathfrak{M}/\sim)\Leftrightarrow(\mathrm{Det}(A),p)=1\Leftrightarrow(\mathrm{Det}(A_0),p)=1$$
$$\Leftrightarrow(\mathrm{Det}(A_{ii}),p)=1,\quad 1\leq i\leq s,$$

since p is prime, $1\leq f_1<f_2<\cdots<f_s$ and $\mathrm{Det}(A_0)=\prod_{i=1}^{s}\mathrm{Det}(A_{ii})$.

Now, every $\bar{A}\in U(\mathfrak{M}/\sim)$ is represented by unique matrix $A\in\mathfrak{M}$ which has elements a_{ij} in prescribed complete set of residues modulo p^{e_i} for $i\leq j$ and modulo p^{e_j} for $i>j$ respectively. Hence every $k_i\times k_i$ matrix A_{ii} is considered as matrix in the general linear group $GL(k_i,\boldsymbol{Z}_{p^{f_i}})$ and every $k_i\times k_j$ matrix A_{ij} is considered as matrix in $\mathrm{Mat}_{k_i\times k_j}(\boldsymbol{Z}_{p^{f_i}})$ for $i\leq j$ and as matrix in $\mathrm{Mat}_{k_i\times k_j}(\boldsymbol{Z}_{p^{f_j}})$ for $i>j$ respectively. Therefore, since the order of $GL(k_i,\boldsymbol{Z}_{p^{f_i}})$ is given by $p^{f_ik_i^2}Q_{k_i}(p)$ where

$$Q_{k_i}(p)=\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right)\cdots\left(1-\frac{1}{p^{k_i}}\right)$$

and the number of choices for A_{ij} is $p^{f_ik_ik_j}$ for $i<j$ and $p^{f_jk_ik_j}$ for $i>j$ respectively, it

follows that the order of $U(\mathfrak{M}/\sim)$ is given by $p^{\alpha}\prod_{i=1}^{s}Q_{k_i}(p)$ where

$$\alpha=\sum_{i<j}f_ik_ik_j+\sum_{i>j}f_jk_ik_j+\sum_{i=1}^{s}f_ik_i^2=\sum_{i=1}^{s}\sum_{j=1}^{s}f_{min(i,j)}k_ik_j$$

$$=\sum_{s=1}^{s}\sum_{j=1}^{s}e_{k_1+\cdots+k_{min(i,j)}}k_ik_j.$$

Thus we have proved

Lemma 6. *The order of the unit group $U(\mathfrak{M}/\sim)$ is given by*

$$p^{\alpha}\prod_{i=1}^{s}Q_{k_i}(p),$$

where

$$\alpha=\sum_{i=1}^{s}\sum_{j=1}^{s}e_{k_1+\cdots+k_{min(i,j)}}k_ik_j,$$

$$Q_{k_i}(p)=\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right)\cdots\left(1-\frac{1}{p^{k_i}}\right).$$

Ⅲ. Orders of End(G) and Aut(G)

Let G be a finite abelian p-group which has the elementary divisors

$$p^{e_1}, p^{e_2}, \cdots, p^{e_r}\quad (1\leq e_1\leq e_2\leq\cdots\leq e_r).$$

Then,

$$G=V=V_1\oplus V_2\oplus\cdots\oplus V_r$$

where V_i is the cyclic group of order p^{e_i} generated by an element v_i, that is, V_i is the cyclic $\boldsymbol{Z}$-module of order p^{e_i} generated by v_i. Thus for any element $v\in V$, we may write

$$v=a_1v_1+a_2v_2+\cdots+a_rv_r,\quad a_i\in\boldsymbol{Z}$$

and $a_1v_1+\cdots+a_rv_r=b_1v_1+\cdots+b_rv_r$ if and only if $a_i\equiv b_i \bmod p^{e_i}$ $(1\leq i\leq r)$.

We now introduce a homomorphism from $\mathfrak{M}=\mathfrak{M}(p;e_1,\cdots,e_r)$ to End(V). Let

$$A=\begin{pmatrix} a_{11} & a_{12}\cdots\cdots\cdots\cdots\cdots a_{1r-1} & a_{1r}\\ p^{e_2-e_1}a_{21} & a_{22}\cdots\cdots\cdots\cdots\cdots a_{2r-1} & a_{2r}\\ p^{e_3-e_1}a_{31} & p^{e_3-e_2}a_{32}\cdots\cdots\cdots\cdots a_{3r-1} & a_{3r}\\ & \cdots\cdots\cdots\cdots & \\ p^{e_r-e_1}a_{r1} & p^{e_r-e_2}a_{r2}\cdots\cdots p^{e_r-e_{r-1}}a_{rr-1} & a_{rr}\end{pmatrix}$$

be a matrix in $\mathfrak{M}$. We shall define a homomorphism

$$\varphi_A : V\to V$$

depending on A. For any $v=a_1v_1+a_2v_2+\cdots+a_rv_r\in V$ and its coordinate $X=[a_1,\cdots,a_r]^T$, we put $AX=[x_1,\cdots,x_r]^T$ and we define $\varphi_A : V\to V$ by the rule $\varphi_A(v)=x_1v_1+\cdots+x_rv_r$.

Now we shall show that φ_A is a well defined homomorphism on V. If $v=a_1v_1+\cdots+a_rv_r=b_1v_1+\cdots+b_rv_r=w$, then $b_i=a_i+p^{e_i}k_i$ for some $k_i\in\boldsymbol{Z}$. If we put $X=[a_1,\cdots,a_r]^T$, $Y=[b_1,\cdots,b_r]^T$ and $AX=[x_1,\cdots,x_r]^T$, $AY=[y_1,\cdots,y_r)^T$, then

$$\begin{aligned}y_i&=p^{e_i-e_1}a_{i1}b_1+\cdots+p^{e_i-e_{i-1}}a_{ii-1}b_{i-1}+a_{ii}b_i+\cdots+a_{ir}b_r\\&=p^{e_i-e_1}a_{i1}(a_1+p^{e_1}k_1)+\cdots+p^{e_i-e_{i-1}}a_{ii-1}(a_{i-1}+p^{e_{i-1}}k_{i-1})\\&\quad+a_{ii}(a_i+p^{e_i}k_i)+\cdots+a_{ir}(a_r+p^{e_r}k_r)\\&=(p^{e_i-e_1}a_{i1}a_1+\cdots+p^{e_i-e_{i-1}}a_{ii-1}a_{i-1}+a_{ii}a_i+\cdots+a_{ir}a_r)\\&\quad+(p^{e_i}a_{i1}k_1+\cdots+p^{e_i}a_{ii-1}k_{i-1}+p^{e_i}a_{ii}k_i+\cdots+p^{e_r}a_{ir}k_r)\\&=x_i+p^{e_i}h_i,\quad(h_i\in\boldsymbol{Z}),\end{aligned}$$

i.e., $y_i\equiv x_i \bmod p^{e_i}$, $1\leq i\leq r$.

Hence $\varphi_A(v)=x_1v_1+\cdots+x_rv_r=y_1v_1+\cdots+y_rv_r=\varphi_A(w)$. Clearly for arbitrary $v,w\in V$, and $a,b\in\boldsymbol{Z}$, we have $\varphi_A(av+bw)=a\varphi_A(v)+b\varphi_A(w)$.

Therefore φ_A is a well defined homomorphism on V. Now we have the well defined mapping

$$F : \mathfrak{M}\to \mathrm{End}(V)$$

such that $F(A)=\varphi_A$ for any $A\in\mathfrak{M}$. We can easily see that the mapping F is a ring homomorphism.

We shall show that F is surjective. Let φ be an arbitrary element of $\mathrm{End}(V)$, and let

$$\varphi(v_j)=c_{1j}v_1+c_{2j}v_2+\cdots+c_{rj}v_r,\quad 1\leq j\leq r.$$

Then, since the order of v_j is p^{e_j} and $1\leq e_1\leq e_2\leq\cdots\leq e_r$,

$$\begin{aligned}0=\varphi(0)=\varphi(p^{e_j}v_j)&=p^{e_j}\varphi(v_j)\\&=p^{e_j}c_{1j}v_1+\cdots+p^{e_j}c_{rj}v_r\\&=p^{e_j}c_{j+1j}v_{j+1}+\cdots+p^{e_j}c_{rj}v_r.\end{aligned}$$

Hence $p^{e_i}\mid p^{e_j}c_{ij}$, *i.e.*, $p^{e_i-e_j}\mid c_{ij}$ for all $i>j$. That is, $c_{ij}=p^{e_i-e_j}a_{ij}$ for some $a_{ij}\in\boldsymbol{Z}$ if $i>j$. Thus, if we denote $c_{ij}=a_{ij}$ for $i\leq j$

$$\varphi(v_j)=a_{1j}v_1+\cdots+a_{jj}v_j+p^{e_{j+1}-e_j}a_{j+1j}v_{j+1}+\cdots+p^{e_r-e_j}a_{rj}v_r.$$

Then, we get a matrix

$$A=\begin{pmatrix}a_{11} & a_{12} & \cdots\cdots\cdots & a_{1r}\\ p^{e_2-e_1}a_{21} & a_{22} & \cdots\cdots\cdots & a_{2r}\\ & & \cdots\cdots\cdots & \\ p^{e_r-e_1}a_{r1} & p^{e_r-e_2}a_{r2} & \cdots\cdots & a_{rr}\end{pmatrix}$$

which belongs to $\mathfrak{M}$. Then, the mapping φ_A on V defined by this matrix is clearly the same as φ, *i.e.*, $F(A)=\varphi_A=\varphi$. Therefore the homomorphism F is surjective. The kernel of F is the set of all matrices of the form

$$\begin{pmatrix} p^{e_1}k_{11} & p^{e_1}k_{12} & \cdots\cdots & p^{e_1}k_{1r} \\ p^{e_2}k_{21} & p^{e_2}k_{22} & \cdots\cdots & p^{e_2}k_{2r} \\ & & \cdots\cdots & \\ p^{e_1}k_{r1} & p^{e_2}k_{r2} & \cdots\cdots & p^{e_r}k_{rr} \end{pmatrix}.$$

Therefore,

$$\mathfrak{M}/\sim=\mathfrak{M}/\ker F\cong \mathrm{End}(V).$$

If we make use of Lemma 4 and Lemma 6, we get

Theorem 1. *Let G be a finite abelian p-group which has the elementary divisors*

$$p^{e_1}, p^{e_2}, \cdots, p^{e_r} \quad (1\leq e_1\leq e_2\leq\cdots\leq e_r),$$

then we have

(1) $\mathrm{End}(G)\cong\mathfrak{M}(p;e_1,\cdots,e_r)/\sim$. *That is, every element of* $\mathrm{End}(G)$ *is uniquely represented by an $r\times r$ matrix of the form*

$$\begin{pmatrix} a_{11} & a_{12} & \cdots\cdots & a_{1r-1} & a_{1r} \\ p^{e_2-e_1}a_{21} & a_{22} & \cdots\cdots & a_{2r-1} & a_{2r} \\ & & \cdots\cdots & & \\ p^{e_r-e_1}a_{r1} & p^{e_r-e_2}a_{r2} & \cdots\cdots & p^{e_r-e_{r-1}}a_{rr-1} & a_{rr} \end{pmatrix}$$

where a_{ij} is an integer in the prescribed complete set of residues modulo p^{e_i} for $i\leq j$ and modulo p^{e_j} for $i>j$ respectively.

The order of $\mathrm{End}(G)$ *is given by*

$$p^{\sum_{k=1}^{r}(2r-2k+1)e_k}.$$

(2) $\mathrm{Aut}(G)\cong U(\mathfrak{M}(p;e_1,\cdots,e_r)/\sim)$. *If* $1\leq e_1=\cdots=e_{k_1}<e_{k_1+1}=\cdots=e_{k_1+k_2}<\cdots<e_{k_1+\cdots+k_{s-1}+1}=\cdots=e_{k_1+\cdots+k_s}=e_r$, *and if we put* $e_{k_1}=f_1$, $e_{k_1+k_2}=f_2,\cdots$, $e_{k_1+k_2+\cdots+k_s}=f_s$, *every element of* $\mathrm{Aut}(G)$ *is uniquely represented by a matrix of the form*

$$\begin{pmatrix} A_{11} & A_{12} & \cdots\cdots & A_{1s-1} & A_{1s} \\ p^{f_2-f_1}A_{21} & A_{22} & \cdots\cdots & A_{2s-1} & A_{2s} \\ & & \cdots\cdots & & \\ p^{f_s-f_1}A_{s1} & p^{f_s-f_2}A_{s2} & \cdots\cdots & p^{f_s-f_{s-1}}A_{ss-1} & A_{ss} \end{pmatrix}$$

where A_{ij} is a $k_i\times k_j$ matrix with elements in the prescribed complete set of residues modulo

p^{f_i} for $i\leq j$, modulo p^{f_j} for $i>j$ respectively and the determinant of A_{ii} is relatively prime to p for every i.

The order of $\mathrm{Aut}(G)$ *is given by*

$$p^{\beta}\prod_{i=1}^{s}Q_{k_i}(p)$$

where

$$\beta=\sum_{i=1}^{s}\sum_{j=1}^{s}e_{k_1+\cdots+k_{\min(i,j)}}k_ik_j,$$

$$Q_{k_i}(p)=\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right)\cdots\left(1-\frac{1}{p^{k_i}}\right).$$

Now let G be a finite abelian group with order n, and let $n=\prod_{\lambda=1}^{t}p_\lambda{}^{h_\lambda}$ be the prime-power decomposition of n where $p_1, p_2, \cdots, p_t$ are distinct primes and $h_\lambda\geq 1$ for all λ. Then

$$G\cong G_1\oplus G_2\oplus\cdots\oplus G_t$$

where every G_λ is the Sylow p_λ-subgroup of G with the order $p_\lambda{}^{h_\lambda}$, and we have

$$\mathrm{End}(G)\cong\mathrm{End}(G_1)\oplus\cdots\cdots\oplus\mathrm{End}(G_t),$$

$$\mathrm{Aut}(G)\cong\mathrm{Aut}(G_1)\times\cdots\times\mathrm{Aut}(G_t),$$

since the orders of $G_1, \cdots, G_t$ are relatively prime in pairs.

Suppose that the elementary divisors of G are

$$p_\lambda{}^{e_{\lambda^1}}, p_\lambda{}^{e_{\lambda^2}}, \cdots, p_\lambda{}^{e_{\lambda^{r_\lambda}}};\ \lambda=1, 2, \cdots, t$$

where $1\leq e_{\lambda,1}\leq e_{\lambda,2}\leq\cdots\leq e_{\lambda,r(\lambda)}$, and let $\sum_{\lambda=1}^{t}\mathfrak{M}_\lambda$ be the set of all matrices of the form

$$A_1\dot{+}A_2\dot{+}\cdots\dot{+}A_t=\begin{pmatrix} A_1 & 0 & \cdots\cdots & 0\\ 0 & A_2 & \cdots\cdots & 0\\ & & \cdots\cdots & \\ 0 & 0 & \cdots\cdots & A_t\end{pmatrix}$$

where $A_\lambda\in\mathfrak{M}_\lambda=\mathfrak{M}(p_\lambda; e_{\lambda,1}, \cdots, e_{\lambda,r(\lambda)})$. Then the system $(\sum_{\lambda=1}^{t}\mathfrak{M}_\lambda, +, \cdot)$ is a ring. Now we define relation on $\sum_{\lambda=1}^{t}\mathfrak{M}_\lambda$; $A\sim B$, for $A, B\in\sum_{\lambda=1}^{t}\mathfrak{M}_\lambda$, if and only if every (i, j) element of the i-th row of A_λ is congruent to the corresponding (i, j) element of the i-th row of B_λ modulo $p_\lambda{}^{e_{\lambda^i}}$ for each λ. Then the relation $\sim$ is an equivalence relation on $\sum_{\lambda=1}^{t}\mathfrak{M}_\lambda$ and the set of all equivalence classes $\sum_{\lambda=1}^{t}\mathfrak{M}_\lambda/\sim$ becomes a ring.

Now if we make use of Theorem 1, we get

Theorem 2. *Let G be a finite abelian group which has elementary divisors*

$$p_\lambda^{e_{\lambda 1}},\ p^{e_{\lambda 2}},\ \cdots,\ p_\lambda^{e_{\lambda r\lambda}},\quad 1\leq\lambda\leq t$$

where $p_1, p_2, \cdots, p_t$ are distinct primes and $1\leq e_{\lambda,1}\leq\cdots\leq e_{\lambda,r(\lambda)}$ for all λ. Then we have

(1) $\mathrm{End}(G)\cong\sum_{\lambda=1}^{t}\mathfrak{M}_\lambda/\sim$. *Every element of* End(G) *is uniquely represented by a matrix of the form*

$$A=A_1\dot{+}A_2\dot{+}\cdots\dot{+}A_t$$

where A_λ is the $r(\lambda)\times r(\lambda)$ matrix in $\mathfrak{M}(p_\lambda; e_{\lambda,1}, \cdots, e_{\lambda,r(\lambda)})$ whose elements of the i-th row are in the prescribed complete set of residues modulo $p_\lambda^{e_{\lambda i}}$ for every i.

The order of the ring End(G) *is given by* $\prod_{\lambda=1}^{t}p_\lambda^{\alpha_\lambda}$ *where*

$$\alpha_\lambda=\sum_{k=1}^{r(\lambda)}(2r(\lambda)-2k+1)e_{\lambda,k}\ .$$

(2) $\mathrm{Aut}(G)\cong U(\prod_{\lambda=1}^{t}\mathfrak{M}_\lambda/\sim)$. *Every element of* Aut(G) *is uniquely represented by a matrix of the same form as A in the above* (1) *where the determinant of A_λ is relatively prime to p_λ for every λ. If*

$$1\leq e_{\lambda,1}=\cdots=e_{\lambda,k(\lambda,1)}<e_{\lambda,k(\lambda,1)+1}=\cdots=e_{\lambda,k(\lambda,2)}<\cdots$$
$$<e_{\lambda,k(\lambda,1)+\cdots+k(\lambda,s(\lambda)-1)+1}=\cdots=e_{\lambda,k(\lambda,1)+\cdots+k(\lambda,s(\lambda))}=e_{\lambda,r(\lambda)},$$

then the order of Aut(G) *is given by* $\prod_{\lambda=1}^{t}p_\lambda^{\beta\lambda}(\prod_{j=1}^{s(\lambda)}Q_{\lambda,k(\lambda,j)}(p_\lambda))$ *where*

$$\beta_\lambda=\sum_{i=1}^{s(\lambda)}\sum_{j=1}^{s(\lambda)}e_{\lambda,k(\lambda,1)+\cdots+k(\lambda,\min(i,j))}k(\lambda,i)k(\lambda,j),$$

$$Q_{\lambda,k(\lambda,j)}(p_\lambda)=\left(1-\frac{1}{p_\lambda}\right)\left(1-\frac{1}{p_\lambda^2}\right)\cdots\left(1-\frac{1}{p_\lambda^{k(\lambda,j)}}\right)\ .$$

References

1. Newman, M. (1972). *Integral Matrices*, Academic Press.
2. _____. (1963). Normal Congruence Subgroups of the t×t Modular Group, *Bull. Amer. Math. Soc.* 69, 619-620.
3. _____. (1962). Some Free Product of Cyclic Groups, *Michigan Math. J.* 9, 369-373.
4. Taussky, O. (1960). Matrices of Rational Integers, *Bull. Amer. Math. Soc.* 66, 327-345.

〈要 約〉

有限 可換群 G에 대한 End(G)와 Aut(G)의 位數

金 應 泰
(數學敎育科)

이 論文에서 有限可換群 G의 準同型寫像 전체의 環 End(G)와 그 單元群 U(End(G)) 즉 Aut(G)의 位數를 결정하는 다음 定理를 증명하였다.

定理 2. G를 有限可換群이라 하고 그 單因子를

$$p_\lambda{}^{e_{\lambda^1}},\ p_\lambda{}^{e_{\lambda^2}}\cdots,\ p_\lambda{}^{e_{\lambda^r\lambda}},\ 1\leq\lambda\leq t$$

라 하자. 단, $p_1, p_2, \cdots, p_k$는 서로 다른 素數이고, 모든 λ에 대하여 $1\leq e_{\lambda,1}\leq e_{\lambda,2}\leq\cdots\leq e_{\lambda,r(\lambda)}$ 이다. 이때,

(1) End(G)의 位數는 $\prod_{\lambda=1}^{t} p_\lambda{}^{\alpha_\lambda}$ 이다. 단,

$$\alpha_\lambda=\sum_{k=1}^{r(\lambda)}(2r(\lambda)-2k+1)e_{\lambda,k}.$$

(2) 單因子 $p_\lambda{}^{e_{\lambda i}}$들에 대하여,

$$1\leq e_{\lambda,1}=\cdots=e_{\lambda,k(\lambda,1)}<e_{\lambda,k(\lambda,1)+1}=\cdots=e_{\lambda,k(\lambda,1)+k(\lambda,2)}<\cdots$$
$$\cdots<e_{\lambda,k(\lambda,1)+\cdots+k(\lambda,s(\lambda)-1)+1}=\cdots=e_{\lambda,k(\lambda,1)+\cdots+k(\lambda,s(\lambda))}=e_{\lambda,r(\lambda)}$$

일 때, Aut(G)의 位數는 $\prod_{\lambda=1}^{t} p_\lambda{}^{\beta_\lambda}\left(\prod_{j=1}^{s(\lambda)} Q_{\lambda,k(\lambda,j)}(p_\lambda)\right)$ 이다. 단,

$$\beta_\lambda=\sum_{i=1}^{s(\lambda)}\sum_{j=1}^{s(\lambda)} e_{\lambda,k(\lambda,1)+\cdots+k(\lambda,\min(i,j))}\,k(\lambda,i)\,k(\lambda,j),$$

$$Q_{\lambda,k(\lambda,j)}(p_\lambda)=\left(1-\frac{1}{p_\lambda}\right)\left(1-\frac{1}{p_\lambda{}^2}\right)\cdots\left(1-\frac{1}{p_\lambda{}^{k(\lambda,j)}}\right).$$