

**ORDERS OF $\text{END}_D(M)$ AND $U(\text{END}_D(M))$
FOR *f. g.* TORSION MODULE M OVER *p. i. d.* D**

EUNG TAI KIM

1. Introduction

In this paper we find the orders of the endomorphism ring $\text{End}_D(M)$ and its unit group $U(\text{End}_D(M))$ for the finitely generated torsion module over the principal ideal domain D whose residue class fields modulo prime ideals in D are all finite.

If $M(\neq 0)$ is a finitely generated module over the *p. i. d.* D , M is the direct sum of cyclic modules: $M = Dz_1 \oplus \cdots \oplus Dz_s$ such that

$$\text{ann } z_1 \supseteq \text{ann } z_2 \supseteq \cdots \supseteq \text{ann } z_s, \text{ ann } z_i \neq D$$

and the ideals $\text{ann } z_i$ are unique for module M . If the module M is the torsion module and if we put $\text{ann } z_i = (d_i)$, d_i are nonzeros, nonunits and $d_1 | d_2 | \cdots | d_s$. We call d_1, d_2, \dots, d_s the *invariant factors* of the torsion module M . If $d_i = p_{i,1}^{e_{i,1}} p_{i,2}^{e_{i,2}} \cdots p_{i,t_i}^{e_{i,t_i}}$ is the prime-power decomposition of d_i , then there exist $x_{i,1}, x_{i,2}, \dots, x_{i,t_i} \in M$ such that

$$Dz_i = Dx_{i,1} \oplus \cdots \oplus Dx_{i,t_i}, \text{ ann } x_{i,j} = (p_{i,j}^{e_{i,j}}).$$

We call $p_{i,j}^{e_{i,j}} (1 \leq i \leq s, 1 \leq j \leq t_i)$ the *elementary divisors* of M .

Now let D be a principal ideal domain. We denote the cardinal number of the residue class ring $D/(a)$ modulo ideal $(a) \subseteq D$ by $N(a)$ (the *norm* of a). Then it is easily verified that $N(a)N(b) = N(ab)$ for any $a, b \in D$, and $N(ab)$ is finite if and only if $N(a)$ and $N(b)$ are finite.

The following lemma can be found in [2].

LEMMA 1.1. *Let p be a prime element in *p. i. d.* D and let e be a positive integer. Suppose that $N(p)$ is finite. Then the order of the general linear group $\text{GL}(n, D/(p^e))$ is given by*

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

Received December 11, 1985.

2. Endomorphism ring $\text{End}_D(M)$

We consider the problem of explicitly determining the ring $\text{End}_D(M)$ of endomorphisms of finitely generated module M over *p.i.d.D.* and we will find the order of $\text{End}_D(M)$ when M is the torsion module.

THEOREM 2.1. *Let $M = Dz_1 \oplus \dots \oplus Dz_s$, where the order ideals $\text{ann } z_i = (d_i)$ satisfy $\text{ann } z_1 \supseteq \text{ann } z_2 \supseteq \dots \supseteq \text{ann } z_s$ and $\text{ann } z_i \neq 0$ for $i \leq r$ but $\text{ann } z_i = 0$ if $i > r$. Then the ring $\text{End}_D(M)$ is isomorphic to R/K where R is the ring of matrices $A \in \text{Mat}_s(D)$ of the form*

$$(*) \quad A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1r} & a_{1r+1} & \dots & a_{1s} \\ a_{21}d_2/d_1 & a_{22} & \dots & a_{2r} & a_{2r+1} & \dots & a_{2s} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{r1}d_r/d_1 & a_{r2}d_r/d_2 & \dots & a_{rr} & a_{rr+1} & \dots & a_{rs} \\ 0 & 0 & \dots & 0 & a_{r+1r+1} & \dots & a_{r+1s} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & a_{sr+1} & \dots & a_{ss} \end{pmatrix}, \quad a_{ij} \in D$$

whose lower left-hand corner consists of 0's, all the indicated a_{ij} are arbitrary, and the (i, j) entry for $j < i \leq r$ is $a_{ij}d_i/d_j$, and K is the ideal in R of the matrices of the form

$$(**) \quad B = \begin{pmatrix} b_{11}d_1 & b_{12}d_1 & \dots & b_{1r}d_1 & \dots & b_{1s}d_1 \\ b_{21}d_1 & b_{22}d_2 & \dots & b_{2r}d_2 & \dots & b_{2s}d_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ b_{r1}d_1 & b_{r2}d_2 & \dots & b_{rr}d_r & \dots & b_{rs}d_r \\ 0 & 0 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 0 \end{pmatrix}, \quad b_{ij} \in D$$

whose (i, j) entry is 0 if $i > r$, $b_{ij}d_i$ if $i \leq r$ and $i \leq j \leq s$, $b_{ij}d_j$ if $j < i \leq r$, and all the indicated b_{ij} are arbitrary.

Proof. Let $\eta \in \text{End}_D(M)$ and suppose $\eta(z_j) = w_j \in M$, $1 \leq j \leq s$.

Then if $x \in M$, $x = \sum_{i=1}^s a_i z_i$, $a_i \in D$ and hence

$$\eta(x) = \eta(\sum a_i z_i) = \sum a_i \eta(z_i) = \sum a_i w_i.$$

This shows that η is determined by its effect on the generators z_i of M . Moreover, $d_j w_j = d_j \eta(z_j) = \eta(d_j z_j) = 0$, which shows that $\text{ann } w_j \supseteq \text{ann } z_j$, so if $\text{ann } w_j = (g_j)$, then g_j is arbitrary if $j > r$, and $g_j | d_j$ if $j \leq r$.

Conversely, suppose that for all j we pick an element $w_j \in M$ such

that $\text{ann } w_j \supseteq \text{ann } z_j$. Suppose $x \in M$ and $x = \sum a_j z_j = \sum b_j z_j$ are two representations of x . Then we have $a_j - b_j \in \text{ann } z_j$. So $a_j - b_j \in \text{ann } w_j$ and consequently $\sum a_j w_j = \sum b_j w_j$. This shows that $\eta : \sum a_j z_j \longrightarrow \sum a_j w_j$ is a map of M into M . Direct verification shows that $\eta \in \text{End}_D(M)$.

Our result is the following. We have a bijection $\eta \longrightarrow (w_1, \dots, w_s)$ of the ring $\text{End}_D(M)$ onto the set of s -tuples of elements of M satisfying $\text{ann } w_j \supseteq \text{ann } z_j$. We now write $w_j = \sum_{i=1}^s c_{ij} z_i$, $c_{ij} \in D$ and we associate with the s -tuple (w_1, \dots, w_s) the matrix $A = [c_{ij}]$ in the ring $\text{Mat}_s(D)$ of $s \times s$ matrices with entries in D . This matrix may not be uniquely determined since c_{ij} may be replaced by c_{ij}' such that $c_{ij}' \equiv c_{ij} \pmod{d_i}$ if $i \leq r$. This is the only alternation which can be made without changing the w_j . The condition that $\text{ann } w_j \supseteq \text{ann } z_j$ is equivalent to

$$c_{ij} d_j \equiv 0 \pmod{d_i}.$$

This, of course, means that there exists $e_{ij} \in D$ such that $c_{ij} d_j = d_i e_{ij}$. Hence the above condition is equivalent to the following condition on the matrix A : there exists a matrix $E = [e_{ij}] \in \text{Mat}_s(D)$ such that

$$A \text{ diag } \{d_1, d_2, \dots, d_s\} = \text{diag } \{d_1, d_2, \dots, d_s\} E.$$

The set R of matrices A satisfying the above condition is a subring of $\text{Mat}_s(D)$. Any $A = [c_{ij}] \in R$ determines an $\eta \in \text{End}_D(M)$ such that $\eta(z_j) = \sum c_{ij} z_i$. It is easy to verify that the map $A \longrightarrow \eta$ is an epimorphism of R onto $\text{End}_D(M)$. It is clear that $\eta = 0$ if and only if $c_{ij} \equiv 0 \pmod{d_i}$ for $A = [c_{ij}]$. Hence the kernel K of our homomorphism is the set of matrices A such that

$$A = \text{diag } \{d_1, d_2, \dots, d_s\} Q$$

where $Q \in \text{Mat}_s(D)$, and $\text{End}_D(M) \cong R/K$.

Now a more explicit determination of the ring of matrices R can be made if we make use of the conditions on d_i that $d_i | d_j$ if $i \leq j \leq r$, and $d_i = 0$ if $i > r$. The conditions $c_{ij} d_j \equiv 0 \pmod{d_i}$ then imply:

- c_{ij} is arbitrary if $i \leq j$ since in this case $d_j \equiv 0 \pmod{d_i}$;
- $c_{ij} = 0$ if $i \geq r$ and $j \leq r$ since in this case $d_i = 0$ and $d_j \neq 0$;
- c_{ij} is arbitrary if $i, j > r$ since $d_i = d_j = 0$ in this case;
- $c_{ij} \equiv 0 \pmod{d_i/d_j}$ if $j < i \leq r$.

Therefore changing the notation slightly we see that the matrix A of R has the above form (*) in the theorem.

Now let $A = [c_{ij}] \in K \subseteq R$ and A is the matrix of the form (*). Then every entry of i -th row of A is a multiple of d_i , so if $i > r$ every (i, j)

$$M = M(p_1) \oplus \cdots \oplus M(p_r).$$

In this case, it is easy to verify that

$$\begin{aligned} \text{End}_D(M) &\cong \text{End}_D(M(p_1)) \oplus \cdots \oplus \text{End}_D(M(p_r)), \\ U(\text{End}_D(M)) &\cong U(\text{End}_D(M(p_1))) \times \cdots \times U(\text{End}_D(M(p_r))) \end{aligned}$$

Now assume that every element of the module M has order ideal which is a power of the fixed prime element p in D . Then M is a direct sum of cyclic D -modules of order ideals $(p^{n_1}), \dots, (p^{n_r})$ respectively, where $1 \leq n_1 \leq n_2 \leq \cdots \leq n_r$, that is,

$$\begin{aligned} M &= Dz_1 \oplus \cdots \oplus Dz_r, \\ \text{ann } z_i &= (p^{n_i}), 1 \leq i \leq r. \end{aligned}$$

Then by Theorem 2.1 $\text{End}_D(M)$ is isomorphic onto the ring R/K where R is the ring of matrices of the form

$$(*) \quad A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ p^{n_2-n_1}a_{21} & a_{22} & \cdots & a_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ p^{n_r-n_1}a_{r1} & p^{n_r-n_2}a_{r2} & \cdots & a_{rr} \end{pmatrix}, \quad a_{ij} \in D$$

and K is the ideal of R of matrices of the form

$$(**) \quad B = \begin{pmatrix} p^{n_1}b_{11} & p^{n_1}b_{12} & \cdots & p^{n_1}b_{1r} \\ p^{n_1}b_{21} & p^{n_2}b_{22} & \cdots & p^{n_2}b_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ p^{n_1}b_{r1} & p^{n_2}b_{r2} & \cdots & p^{n_r}b_{rr} \end{pmatrix}, \quad b_{ij} \in D.$$

LEMMA 3.1. *Let p be a prime element of *p. i. d. D*, n_1, n_2, \dots, n_r be positive integers such that $n_1 \leq n_2 \leq \cdots \leq n_r$. Let R be the ring of matrices of the above form (*) and let K be the ideal of R of matrices of the above form (**). Then for an element $\bar{A} = A + K \in R/K$, $\bar{A} \in U(R/K)$ if and only if $(\text{Det}(A), p) = 1$.*

Proof. If $\bar{A} \in U(R/K)$ there exists $\bar{B} \in U(R/K)$ such that $\bar{A}\bar{B} = \bar{A}\bar{B} = \bar{B}\bar{A} = \bar{I}$, i. e.,

$$AB = I + \begin{pmatrix} p^{n_1}b_{11} & p^{n_1}b_{12} & \cdots & p^{n_1}b_{1r} \\ p^{n_1}b_{21} & p^{n_2}b_{22} & \cdots & p^{n_2}b_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ p^{n_1}b_{r1} & p^{n_2}b_{r2} & \cdots & p^{n_r}b_{rr} \end{pmatrix}$$

Therefore $(\text{Det}(A))(\text{Det}(B)) = \text{Det}(AB) = 1 + pc$ for some $c \in D$ hence $(\text{Det}(A), p) = 1$. Conversely suppose $(\text{Det}(A), p) = 1$ for $\bar{A} \in R/K$. We

We may write $A=A_0+P$ where

$$A_0 = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1s} \\ 0 & A_{22} & \cdots & A_{2s} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & A_{ss} \end{pmatrix}, \quad P = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ p^{l_2-l_1}A_{21} & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ p^{l_s-l_1}A_{s1} & p^{l_s-l_2}A_{s2} & \cdots & 0 \end{pmatrix}$$

Then utilizing Lemma 3.1 for $\bar{A} \in R/K$, we have

$$\begin{aligned} \bar{A} \in U(R/K) &\iff (\text{Det}(A), p) = 1 \iff (\text{Det}(A_0), p) = 1 \\ &\iff (\text{Det}(A_{ii}), p) = 1 \text{ for all } i, \end{aligned}$$

since p is a prime element in D , $1 \leq l_1 < l_2 < \cdots < l_s$, and $\text{Det}(A_0) =$

$\prod_{i=1}^s \text{Det}(A_{ii})$. Thus if $\bar{A} \in U(R/K)$, every $k(i) \times k(i)$ matrix A_{ii} is regarded as a matrix in the general linear group $\text{GL}(k(i), D/p^{l_i})$.

Now suppose that $N(p)$ is finite. Then, since the order of group $\text{GL}(k(i), D/(p^{l_i}))$ is given by $N(p)^{l_i k(i)^2} Q_{k(i)}(p)$ where $Q_{k(i)}(p) = \left(1 - \frac{1}{N(p)}\right) \left(1 - \frac{1}{N(p)^2}\right) \cdots \left(1 - \frac{1}{N(p)^{k(i)}}\right)$ by Lemma 1.1, and the number of choices for A_{ij} is $N(p)^{l_i k(i) k(j)}$ when $i < j$ and $N(p)^{l_j k(i) k(j)}$ when $i > j$ respectively, it follows that the order of $U(R/K)$ is given by

$$\prod_{i < j} N(p)^{l_i k(i) k(j)} \prod_{i > j} N(p)^{l_j k(i) k(j)} \prod_{i=1}^s N(p)^{l_i k(i)^2} Q_{k(i)}(p) = N(p)^\alpha \prod_{i=1}^s Q_{k(i)}(p)$$

where

$$\begin{aligned} \alpha &= \sum_{i < j} l_i k(i) k(j) + \sum_{i > j} l_j k(i) k(j) + \sum_{i=1}^s l_i k(i)^2 \\ &= \sum_{i=1}^s \sum_{j=1}^s l_{\min(i,j)} k(i) k(j) = \sum_{i=1}^s \sum_{j=1}^s n_{k(1)+\cdots+k(\min(i,j))} k(i) k(j). \end{aligned}$$

THEOREM 3.3. *Let M be a finitely generated torsion module over a p . i. d. D which has elementary divisors*

$$p_\lambda^{n_{\lambda,1}}, p_\lambda^{n_{\lambda,2}}, \dots, p_\lambda^{n_{\lambda,r_\lambda}}, \quad 1 \leq \lambda \leq t,$$

where p_1, p_2, \dots, p_t are nonassociate prime elements in D such that $N(p_1), N(p_2), \dots, N(p_t)$ are all finite and $1 \leq n_{\lambda,1} \leq \dots \leq n_{\lambda,r_\lambda}$ for all λ .

Assume that

$$\begin{aligned} 1 \leq n_{\lambda,1} = \dots = n_{\lambda,k(\lambda,1)} < n_{\lambda,k(\lambda,1)+1} = \dots = n_{\lambda,k(\lambda,1)+k(\lambda,2)} < \dots \\ \dots < n_{\lambda,k(\lambda,1)+\dots+k(\lambda,s_\lambda-1)+1} = \dots = n_{\lambda,k(\lambda,1)+\dots+k(\lambda,s_\lambda)} = n_{\lambda,r_\lambda} \end{aligned}$$

Then the order of $U(\text{End}_D(M))$ is given by

$$\prod_{\lambda=1}^t N(p_\lambda)^{\alpha_\lambda} \left(\prod_{j=1}^{s_\lambda} Q_{\lambda, k(\lambda, j)}(p_\lambda) \right)$$

where

$$\alpha_\lambda = \sum_{i=1}^{s_\lambda} \sum_{j=1}^{s_\lambda} n_{\lambda, k(\lambda, 1) + \dots + k(\lambda, \min(i, j))} k(\lambda, i) k(\lambda, j),$$

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

Proof. Let $M(p_\lambda) = \{z \in M \mid \text{ann } z = (p_\lambda^m) \text{ for some integer } m \geq 1\}$. Then

$$M = M(p_1) \oplus M(p_2) \oplus \cdots \oplus M(p_t),$$

$$\text{End}_D(M) \cong \text{End}_D(M(p_1)) \oplus \cdots \oplus \text{End}_D(M(p_t)),$$

$$U(\text{End}_D(M)) \cong U(\text{End}_D(M(p_1))) \times \cdots \times U(\text{End}_D(M(p_t))),$$

and $p_\lambda^{n_{\lambda, 1}}, \dots, p_\lambda^{n_{\lambda, r_\lambda}}$ are elementary divisors of $M(p_\lambda)$ for each λ . Therefore by Theorem 3.2, we have the desired order of the unit group $U(\text{End}_D(M))$.

References

1. L. Dornhoff, *Group representation theory*, Marcel Dekker, Inc., New York, 1972.
2. M. Newmann, *Integral matrices*, Academic Press, 1972.
3. _____, *The structure of some subgroups of the modular group*, Illinois J. Math. **6**, 480-487(1962).

Seoul National University
Seoul 151, Korea