ON THE AUTOMORPHISMS OF A CERTAIN CLASS OF FINITE RINGS

By Mizue Moriya

The determination of the structure of finite rings is reduced to that of p-rings,[1] for every finite ring is a direct sum of p_i-rings where p_i are different primes.

Let R be a finite p-ring whose additive group $(R, +)$ is of type $(p^{e_1}, p^{e_2}, \cdots, p^{e_l})$, $e_1 \geqq e_2 \geqq \cdots \geqq e_l$. Then R can be identified with a subring of the endomorphism ring B of $(R, +)$. (If R does not contain an identity element, we replace $(R, +)$ by $(R^*, +)$, where R^* is the ring obtained by adjoining an identity 1 to R; here we may set $p^{e_1}1=0$.) The ring B can be considered as the ring of all $l \times l$ matrices $(a_{ij})\,(1 \leqq i, j \leqq l)$ of the form

$$a=(a_{ij})=\begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ p^{e_1-e_2}g_{21} & g_{22} & & g_{2n} \\ \vdots & & \ddots & \vdots \\ p^{e_1-e_n}g_{n1} & \cdots & & g_{nn} \end{bmatrix}, \qquad a_{ij}=\begin{cases} g_{ij} & (i \leqq j), \\ p^{e_j-e_i}g_{ij} & (i>j), \end{cases}$$

where g_{ij} are rational integers modulo p^{e_k}, $k=\max\{i, j\}$. (Shoda [2], Szele [3]).

Now, let λ be a positive integer $\leqq n=e_1$ and let β_λ be the number of λ's which appear among the set $\{e_i | i=1, 2, \cdots, l\}$. If $\beta_\lambda=0$ for some λ (i.e. if λ does not appear in $\{e_i\}$), we insert λ to $\{e_i\}$. After this for every λ with $\beta_\lambda=0$, we obtain a series of integers in which each positive integer not greater than $n(=e_1)$ appears at least once:

$$\underbrace{n, n, \cdots, n}_{\alpha_n}, \underbrace{n-1, \cdots, n-1}_{\alpha_{n-1}}, \cdots, \underbrace{i, \cdots, i}_{\alpha_i}, \cdots, \underbrace{1, \cdots, 1}_{\alpha_1}.$$

Here, $\alpha_\lambda=\beta_\lambda$ or $\alpha_\lambda=1$ according as $\beta_\lambda \neq 0$ or $\beta_\lambda=0$, respectively. We set $m=\alpha_1+\alpha_2+\cdots+\alpha_n$. Then the ring R can be imbedded in the endomorphism ring A of an abelian group of type $(p^n, \cdots, p^n, p^{n-1}, \cdots, p^{n-1}, \cdots, p, \cdots, p)$. We can identify A with the ring of all matrices of the form

$$a=\begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ pA_{21} & A_{22} & \cdots & A_{2n} \\ p^2A_{31} & pA_{32} & \cdots & A_{3n} \\ \cdots & \cdots & \cdots & \cdots \\ p^{n-1}A_{n1} & \cdots & \cdots & A_{nn} \end{bmatrix}$$

Received April 2, 1966.

1) A finite ring is called p-ring if the number of elements is a power of p.

where A_{ij} is an $\alpha_{n-i+1}\times\alpha_{n-j+1}$ matrix having the components of rational integers modulo p^{n-k+1}, $k=\max\{i,j\}$.

The finite ring A of this type is somewhat less general than the endomorphism ring B, which we have mentioned above. But we can still imbed an arbitrary finite p-ring R as a subring of such an A.

The present paper may be divided into two parts. In the first part we shall study the automorphisms of this type of finite rings. The second part is the discussion of a particular case where $\alpha_{n-i+1}=1$ $(1\leqq i\leqq n)$; there we shall also be concerned with the automorphisms of the radical of the ring. In any case, the radical of the ring as above can be seen to be (in a sense) a generalization of a total nilpotent algebra[2] over $GF(p)$, whose structure (the automorphisms and ideals in particular) is thoroughly discussed by Dubisch-Perlis [1]. In the following some of their methods will be extended to our matrix rings.

The author wishes to express her hearty thanks to Professor H. Tôyama and Professor M. Okuzumi for their kind advices. She is also indebted to Dr. S. Asano for his encouragement and valuable suggestions.

1. Let A be a finite ring as in the introduction. Namely, A is the ring of all $m\times m$ matrices of the form

$$a=\begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ pA_{21} & A_{22} & \cdots & A_{2n} \\ p^2A_{31} & pA_{32} & \cdots & A_{3n} \\ \cdots & \cdots & \cdots & \cdots \\ p^{n-1}A_{n-1} & \cdots & \cdots & A_{nn} \end{bmatrix} \tag{1}$$

where A_{ij} is an $\alpha_{n-i+1}\times\alpha_{n-j+1}$ matrix having the components of rational integers modulo p^k, $k=\min\{n-i+1, n-j+1\}$.

We write the matrix of A, which has (s,t) component 1 or p^{i-j}, and 0 elsewhere, as $e_{s,t}$ or $p^{i-j}e_{s,t}$ $(1\leqq s,t\leqq m)$; here, (s,t) is one of the subscripts associated to a block A_{ij} $(i\leqq j)$ or $p^{i-j}A_{ij}$ $(i>j)$, respectively, in the expression (1). (We shall say that $e_{s,t}$ $[p^{i-j}e_{s,t}]$ *belongs to the block* A_{ij} $[p^{i-j}A_{ij}]$).

A is generated by e_{ii} $(i=1,\cdots,m)$, $e_{j,j+1}$ $(j=1,\cdots,m-1)$, $e_{k+1,k}$ $(k\neq\sum_{i=1}^{f}\alpha_{n-i+1}$, $f=1,\cdots,n)$ and $pe_{k+1,k}$ $(k=\sum_{i=1}^{f}\alpha_{n-i+1}, f=1,\cdots,n)$.

The radical of A is the set of all matrices whose components of diagonal blocks A_{ii} $(i=1,\cdots,n)$ are divisible by p.

Let N be the radical of A. N and N^i, the powers of N, are characteristic ideals of A. Also, there are some other kinds of characteristic ideals in A. We

2) A total nilpotent algebra of degree n over a field F is defined to be any isomorphic copy of the algebra of $n\times n$ matrices over F with zeros on and above the diagonal.

list them as follows:

(a) $$Q^{(d)}=\{a|p^d a=0, a\in A\}.$$

It is clear that $Q^{(d)}$ is a characteristic ideal.

(b) $$P^{(d)}=\{b|bQ^{(d)}=0, b\in A\}.$$

We have $(bx)a=b(xa)=0$, $(xb)a=x(ba)=0$ for $x\in A$, $b\in P^{(d)}$ and $a\in Q^{(d)}$. Thus $P^{(d)}$ is an ideal. For every automorphism σ of A, $a\in Q^{(d)}$ and $b\in P^{(d)}$, we have $b^\sigma a^\sigma=(ba)^\sigma=0=ba$. As $Q^{(d)}$ is characteristic, a^σ varies over every element of $Q^{(d)}$, and so $b^\sigma\in P^{(d)}$. Thus $P^{(d)}$ is also characteristic. $P^{(d)}$ is the set of all matrices of A such that all the components are divisible by p^d. We write $P^{(1)}=P$. Clearly $P^{(d)}=P^d$. The matrices of $P^{(d)}$ are of the following form:

$$\begin{array}{l} \\ d+1 \text{ blocks} \end{array}\left\{\begin{array}{c} \overbrace{}^{d \text{ blocks}} \\ \left[\begin{array}{cccccc} p^dA_{11} & \cdots & p^dA_{1,n-d+1} & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p^dA_{d+1,1} & \cdots & \cdots & \cdots & \cdots & \cdots \\ p^{d+1}A_{d+2,1} & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p^{n-1}A_{n1} & \cdots & \cdots & 0 & \cdots & 0 \end{array}\right] \end{array}\right.$$

(c) $$U^{(d)}=\{a|N^d a\subset P\}.$$

$U^{(d)}$ is the set of all elements of A whose components in the blocks A_{ij}, $i>d$, are divisible by p.

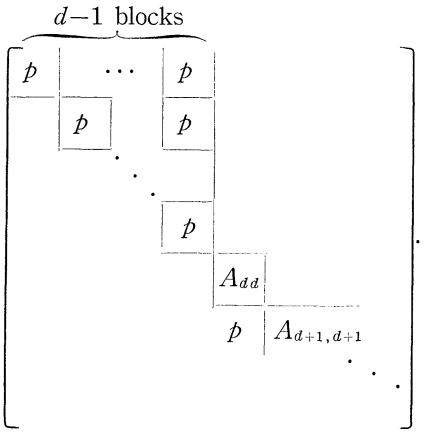
$$d \text{ blocks}\left\{\left[\begin{array}{c|c|c|c|c} A_{11} & & & & \\ \hline p & A_2 & & & \\ \hline & \ddots & \ddots & & \\ \hline & & p & & \\ \hline & & & p & A_{dd} \\ \hline & & & p & p\cdots p \end{array}\right]\right.$$

(The letter p means "divisible by p".)

(d) $$R^{(d)}=\{a|aU^{(d)}\subset P\}.$$

3) The arguments in this section is similar to that of Dubisch-Perlis [1].

$R^{(d)}$ is the set of all elements of A whose components of the blocks $A_{ij}, j<d$, are divisible by p.



In the same way as in (b), we can see that $U^{(d)}$ and $R^{(d)}$ are characteristic ideals.

LEMMA 1. *When $e_{s,t}$ belongs to the block A_{ij} $(i\leqq j)$ $[p^{i-j}e_{s,t}$ to the block $p^{i-j}A_{ij}$ $(i>j)]$, then for every automorphism σ of A we have*

$$e_{s,t}^{\sigma}\in U^{(i)}\frown R^{(j)} \qquad [(p^{i-j}e_{s,t})^{\sigma}\in P^{i-j}-P^{i-j+1}].$$

The residue class ring A/P of A with respect to the characteristic ideal P is isomorphic to the matrix algebra over $GF(p)$ of the following form

$$(*) \qquad \bar{a}=\begin{bmatrix} \bar{A}_{11} & \bar{A}_{12} & \cdots & \bar{A}_{1n} \\ & \bar{A}_{22} & \cdots & \bar{A}_{2n} \\ 0 & & \ddots & \vdots \\ & & & \bar{A}_{nn} \end{bmatrix}$$

where the block $\bar{A}_{ij}$ is an $\alpha_{n-i+1}\times\alpha_{n-j+1}$ matrix with the components of rational integers modulo p.

We consider, in general, a ring R of matrices of the form (*) over an arbitrary field F. We write the matrix of R which has (s,t) component 1 and has 0 elsewhere as $e_{s,t}$. Also we write the set of matrices of R whose components are all zero except for components of the block R_{ij} ($\bar{A}_{ij}$, in (*)) as $R_{[i,j]}$.

The radical $N(R)$ of R is the set of all matrices whose components of R_{ii} $(i=1,2,\cdots,n)$ are all zero. We can find characteristic ideals of R in the same way as before:

(a′) $$U^{(d)}=\{a|N(R)^d a=0\},$$

(b′) $$V^{(d)}=\{a|aU^{(d)}=0\}.$$

$U^{(d)}$ is the set of all matrices whose components of the blocks R_{ij}, $i>d$, are zero, and $V^{(d)}$ is the set of all matrices whose components belonging to the blocks R_{ij}, $j>d$, are zero.

If the matrix $e_{s,t}$ belongs to $R_{[i,j]}$, then for every automorphism σ of R, $e_{s,t}{}^{\sigma}\in U^{(i)}\frown V^{(j)}$.

THEOREM 1. *Let R be the ring of all matrices of the form* (*) *over a field F. If σ is an automorphism of R, then σ is inner.*[4]

Proof. (i) Let σ be an automorphism of R and let $a_{[k,k]}$ be a matrix of $R_{[k,k]}$. Then we have, as mentioned above,

$$a_{[k,k]}{}^{\sigma}=\sum_{\substack{i\leqq k\\ j\geqq k}} b_{[i,j]}=b_{[k,k]}+r_k,$$

where $b_{[i,j]}\in R_{[i,j]}$ and $r_k\in N(R)$. Hence $R_{[k,k]}$ is mapped in itself mod $N(R)$ by σ.

By the well known theorem of algebra, we see that there exists an inner automorphism I_a: $x\to a^{-1}xa$ ($x\in R$) of R which has the same effect as $\bar{\sigma}$ on $R_{[k,k]}$ mod $N(R)$.

Now set $\tau=\sigma I_a{}^{-1}$. The automorphism τ fixes the elements of $R_{[k,k]}$ ($k=1,\cdots,n$) mod $N(R)$. This implies that τ satisfies $x^{\tau}-x\in N(R)$ for all $x\in R$.

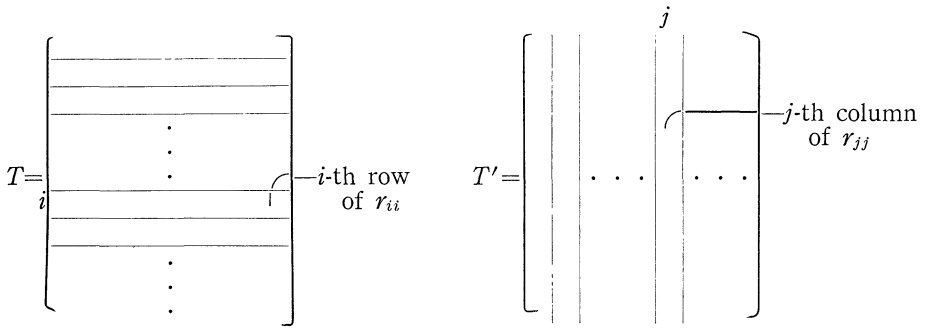
(ii) Let τ be as above: $x^{\tau}-x\in N(R)$ for all x. Let $e_{s,t}$ be a matrix unit in $R_{[i,i+1]}$ ($1\leqq i\leqq n-1$). Since $e_{s,s}{}^{\tau}e_{s,t}{}^{\tau}e_{t,t}{}^{\tau}=e_{s,t}{}^{\tau}$ we have $e_{s,s}e_{s,t}{}^{\tau}e_{t,t}\equiv e_{s,t}{}^{\tau}(N(R)^2)$. This means $e_{s,t}{}^{\tau}\equiv c_{s,t}e_{s,t}$ $(N(R)^2)$ with some $c_{s,t}\in F$. Next suppose that $e_{u,v}$ is another matrix unit in $R_{[i,i+1]}$. Then $e_{u,v}=e_{u,s}e_{s,t}e_{t,v}$, where $e_{u,s}\in R_{[i,i]}$ and $e_{t,v}\in R_{[i+1,i+1]}$. From $e_{u,v}{}^{\tau}=e_{u,s}{}^{\tau}e_{s,t}{}^{\tau}e_{t,v}{}^{\tau}$ we have $c_{u,v}=c_{s,t}$. Thus for each $R_{[i,i+1]}$ there exists a (non-zero) element c_i in F with $x^{\tau}\equiv c_i x$ $(N(R)^2)$ for all $x\in R_{[i,i+1]}$. We now set $D=E_1+c_1E_2+c_1c_2E_3+\cdots+c_1c_2\cdots c_{n-1}E_n$, whers E_i is the unit element of the subring $R_{[i,i]}$. The inner automorphism I_D by D clearly satisfies $x^{\tau}\equiv c_i x=x^{I_D}$ $(N(R)^2)$ for all $x\in R_{[i,i+1]}$, and hence $x^{\tau}\equiv x^{I_D}$ $(N(R)^2)$ for all $x\in N(R)$. Set $\rho=\tau I_D{}^{-1}$; it is easy to see that $x^{\rho}\equiv x$ $(N(R))$ for all $x\in R$ and $x^{\rho}\equiv x$ $(N(R)^2)$ for all $x\in N(R)$.

(iii) We proceed to show that the automorphism ρ is inner. Thus put $e_{s,t}{}^{\rho}=e_{s,t}+r_{s,t}$; we know that $r_{s,t}\in N(R)$ always and that $r_{s,t}\in N(R)^2$ if $e_{s,t}\in N(R)$. From $e_{k,k}{}^{\rho}=e_{k,k}{}^{\rho}e_{k,k}{}^{\rho}$ we have $r_{k,k}\equiv e_{k,k}r_{k,k}+r_{k,k}e_{k,k}$ $(N(R)^2)$. Hence the components of the matrix $r_{k,k}$ is zero mod $N(R)^2$ except for its k-th row and k-th column. Also, from $e_{i,j}{}^{\rho}=e_{i,i}{}^{\rho}e_{i,j}{}^{\rho}e_{j,j}{}^{\rho}$ we get $r_{i,j}\equiv e_{i,j}r_{j,j}+r_{i,i}e_{i,j}$ $(N(R)^2)$, which implies that the components of $r_{i,j}$ is zero mod $(N(R)^2)$ except for its i-th row and j-th column; moreover, the i-th row is congruent to the j-th row of $r_{j,j}$ and the j-th column to the i-th column of $r_{i,i}$ (mod $N(R)^2$). Finally, from $e_{i,i}{}^{\rho}e_{j,j}{}^{\rho}=0$ $(i\neq j)$, we have $r_{ii}e_{jj}+e_{ii}r_{jj}$

4) When α_{n-k+1} are all 1, this theorem is reduced to the Theorem 8 of [1].

$\equiv 0\,(N(R)^2)$. This shows that the (i, j) components $r_{(i,i)i,j}$, $(r_{j,j})_{i,j}$ (of $r_{i,i}$ and $r_{j,j}$ respectively) satisfy $(r_{i,i})_{i,j}+(r_{j,j})_{i,j}=0$ if the position (i, j) is such that $e_{i,j}\notin N(R)^2$.

Now define a matrix T as follows: The i-th row of T is that of r_{ii} $(i=1, 2, \cdots, m)$ Then, if T' is a matrix defined similarly by column (i.e., the j-th column of T' is that of $r_{j,j}$ $(j=1, 2, \cdots, m)$), we have $T+T'\equiv 0\,(N(R)^2)$ by what we have seen. Clearly $T\equiv T'\equiv 0\,(N(R))$.



Consider the inner automorphism I_{1+T} by $1+T$. then $e_{i,j}{}^{I_{1+T}}=(1+T)^{-1}e_{i,j}(1+T)$ $\equiv(1-T)e_{i,j}(1+T)\equiv(1+T')e_{i,j}(1+T)\equiv e_{i,j}+T'e_{i,j}+e_{i,j}T=e_{i,j}+r_{i,i}e_{i,j}+e_{i,j}r_{j,j}\equiv e_{i,j}$ $+r_{i,j}$ $(N(R)^2)$. Hence $e_{i,j}{}^{\rho}\equiv e_{i,j}{}^{I_{1+T}}$ for all $e_{i,j}$. We set $\mu=\rho I_{1+T}^{-1}$ Then $x^{\mu}\equiv x$ $(N(R)^2$ for all $x\in R$.

(iv) Let $e_{s,t}\in R_{[i,i+1]}$. From $e_{s,s}{}^{\mu}e_{s,t}{}^{\mu}e_{t,t}{}^{\mu}=e_{s,t}{}^{\mu}$ and from (iii) $(x^{\mu}\equiv x\ (N(R)^2)$ if $x\in R)$ one verifies easily that $e_{s,t}{}^{\mu}\equiv e_{s,t}(N(R)^3)$. Hence we have $x^{\mu}\equiv x\ (N(R)^3)$ for all $x\in N(R)$. By constructing a similar inner automorphism as in (iii) we see $x^{\mu}\equiv x^{I_{1+T_2}}$ $(N(R))$ for all $x\in R$, where T_2 is a matrix in $N(R)$. In the similar way we can construct successively the inner automorphisms I_{1+T_1}, I_{1+T_2}, $\cdots$, I_{1+T_n} such that $x^{\rho I_{1+T_1}^{-1}I_{1+T_2}^{-1}\cdots I_{1+T_n}^{-1}}-x\in N(R)^n$. Since $N(R)^n=0$ we must have $\rho=I_{1+T_n}I_{1+T_{n-2}}\cdots I_{1+T_1}$; this shows that ρ is inner and, at the same time, σ is an inner automorphism. This completes the proof of Theorem 1.

Let σ be an automorphism of A. σ induces an automorphism $\bar{\sigma}$ of A/P. By Theorem 1, $\bar{\sigma}$ is an inner automorphism of A/P: $\bar{x}^{\bar{\sigma}}=\bar{x}^{I_{\bar{a}}}=\bar{a}^{-1}\bar{x}\bar{a}$, for $\bar{x}\in A/P$.

Let a be an element of the class $\bar{a}\in A/P$. The automorphism $\sigma I_a{}^{-1}$: $x^{\sigma I_a{}^{-1}}=ax^{\sigma}a^{-1}$ satisfies $x^{\sigma I_a{}^{-1}}-x\in P$. By constructing matrices M_i successively, similarly as in the proof of Theorem 1, we can prove that $\tau=\sigma I_a{}^{-1}$ is inner: $\sigma I_a{}^{-1}=I_{M_1}\cdots I_{M_{n-1}}$.

Thus we have the following

THEOREM 2. *All automorphisms of A are inner.*

2. Now, we consider the case where e_i $(i=1, \cdots, n)$ are different each other. In this case, we can imbed the ring in the ring A whose elements are the matrices of the form

$$a=\begin{bmatrix} g_{11} & g_{12} & \cdots & \cdots & g_{1n} \\ pg_{21} & g_{22} & \cdots & \cdots & g_{2n} \\ p^2g_{31} & pg_{32} & g_{33} & \cdots & g_{3n} \\ \cdots & & & \ddots & \\ p^{n-1}g_{n1} & p^{n-2}g_{n2} & \cdots & \cdots & g_{nn} \end{bmatrix}$$

where g_{ij} are rational integers mod p^{n-k+1}, $k=\max\{i,j\}$.

The radical of A is the totality of the matrices whose diagonal components are divisible by p. We denote it as N. N is generated by the elements $e_{k,k+1}$ and $pe_{j+1,j}$ $(k,j=1,2,\cdots,n-1)$. We can find characteristic ideals of N corresponding to those of A. These are the intersections of N and those of A.

The residue class ring N/P is a total nilpotent algebra over the prime field of characteristic p.

The automorphisms of a total nilpotent algebra are determined explicitly by Dubisch-Perlis [1]: The automorphism group of N/P, which we denote $\mathfrak{G}=\mathfrak{G}(N/P)$, has the suructure $\mathfrak{G}=\mathfrak{D}\mathfrak{M}=\mathfrak{M}\mathfrak{D}$, where $\mathfrak{D}$ is the group of diagonal automorphisms, and $\mathfrak{M}$ the group of monic automorphisms. Besides, $\mathfrak{M}$ has the structure $\mathfrak{M}=\mathfrak{N}\times\mathfrak{I}$ where $\mathfrak{N}$ is the group of nil automorphisms and $\mathfrak{I}$ the group of inner automorphisms.

We wish to define the automorphisms of N corresponding to the monic, nil, diagonal and inner automorphisms of N/P. First we observe that the inner automorphisms are defined in the same way (footnote 6).

a) Automorphisms corresponding to $\mathfrak{M}$ (monic automorphisms).

For every automorphism σ of N, $e_{k,k+1}{}^{\sigma}$ is written as follows:

$$e_{k,k+1}{}^{\sigma}=\sum_{\substack{i\leqq k\\ j\geqq k+1}}\beta_{ij}{}^{(k)}e_{ij}+p,\quad p\in P,$$

since $e_{k,k+1}{}^{\sigma}\in N\frown U^{(k)}\frown R^{(k+1)}$. We can easily see that $\beta_{k,k+1}{}^{(k)}\neq 0$. When $\beta_{k,k+1}{}^{(k)}=1$, the set of these automorphisms correspond to the monic automorphisms of N/P.

b) Automorphisms corresponding to $\mathfrak{N}$ (nil automorphisms).

We call the element u satisfying $xu\in P$ $(ux\in P)$ for all $x\in N$ an absolute right (left) divisor of P, corresponding to the absolute divisor of zero in N/P. The absolute right (left) divisors of P are linear combinations of $e_{12}, e_{13}, \cdots, e_{1n}$ $(e_{1n}, e_{2n}, \cdots, e_{n-1,n})$ and

5) An automorphism μ of an arbitrary ring S is called *monic* in case $x-x\in S^{r+1}$ whenever x lies in S^r.

6) An *inner* automorphism λ of S is defined by the formula

$$x^{\lambda}=x+bx+xa+bxa$$

where a is an element of S such that there exists $b\in S$; $a+b+ab=a+b+ba=0$.

7) A *diagonal* automorphis δ of a matrix algebra over F is an automorphism $x^{\delta}=dxd^{-1}$ determined by a diagonal non-singular matrix $d=\sum d_ie_{ii}$, $d_i\in F$.

8) An automorphism ν of S is called *nil* if $u^{\nu}=u$ for every absolute right if $xu=0$ $(ux=0)$ for every $x\in S$.

the elements of P. The automorphisms which satisfy $u^p-u\in P$ correspond to the nil automorphisms of N/P.

c) Automorphisms corresponding to $\mathfrak{D}$ (diagonal automorphisms).

Let d_i be an unit of the ring of rational integers mod p^{n-i+1}. A diagonal matrix

$$d=\sum_{i=1}^{n} d_i e_{ii}$$

determines an automorphisms δ of A: $x^\delta=d^{-1}xd$, $x\in A$. The automorphisms of N induced by these δ's correspond to the diagonal automorphisms of N/P.

Let δ be such an automorphism. Then

$$e_{k,k+1}{}^\delta\equiv\alpha_k e_{k,k+1}(P),$$

where α_k are units (i.e. integers (considered mod p^{n-k}) relatively prime to p), and for $k<l$

$$\begin{aligned} e_{kl}{}^\delta&\equiv\alpha_{kl}e_{kl}(P),\\ \alpha_{kl}&\equiv\alpha_k\alpha_{k+1}\cdots\alpha_{l-1}, \end{aligned}\tag{4}$$

and

$$pe_{k+1,k}{}^\delta\equiv\alpha_k{}^{-1}pe_{k+1,k}\,(P^2),$$

For $k>l$

$$p^{k-l}e_{kl}{}^\delta\equiv p^{k-l}\alpha_{kl}{}^{-1}e_{kl}(P^{k-l+1}).\tag{5}$$

Conversely, arbitrary units α_i ($i=1,\cdots,n-1$) mod p^{n-i} and equations (4) and (5) determine a δ defined in (c) given by

$$d=e_{11}+\alpha_1e_{22}+\alpha_1\alpha_2e_{33}+\cdots+\alpha_1\alpha_2\cdots\alpha_{n-1}e_{nn}.$$

THEOREM 3. *The group $\mathfrak{G}$ of the automorphisms of N has the structure $\mathfrak{G}=\mathfrak{D}\mathfrak{M}=\mathfrak{M}\mathfrak{D}$ where $\mathfrak{D}$ and $\mathfrak{M}$ are the groups of automorphisms defined in* c) *and* a), *respectively.*

Proof. This is proved in the same way as in [1].

THEOREM 4. *All the automorphisms defined in* b) *are generated by*

$$e_{k,k+1}{}^\nu=e_{k,k+1}+\alpha_k e_{1n}+p,\quad \alpha_1=\alpha_{n-1}=0,\quad p\in P,\tag{7}$$

$$(pe_{k+1,k})^\nu=pe_{k+1,k}+p\gamma_k e_{1n-1}+p',\quad p'\in P^2.\tag{8}$$

Proof. From (7) it follows

$$e_{in}{}^{\nu}-e_{in}\in P,\quad e_{1j}{}^{\nu}-e_{1j}\in P\quad (i=1,\cdots,n-1;j=2,\cdots,n).$$

And, as P is characteristic, we have $a^{\nu}-a\in P$ for $a\in P$. Hence ν has the required property.

Conversely, let ν be an automorphism defined in b). By Theorem 3, $\nu=\delta\mu$, $\delta\in\mathfrak{D}$, $\mu\in\mathfrak{M}$. So we have

$$e_{k,k+1}{}^{\nu}=e_{k,k+1}{}^{\delta\mu}=(\alpha_k e_{k,k+1}+p_k)^{\mu}=\alpha_k e_{k,k+1}+c_k,$$

where $p_k\in P$, $c_k\in N^2\cup P$. As e_{12} is an absolute divisor of P, we have $\alpha_1=1$, $c_1\in P$. For $k<n$, we have

$$\begin{aligned}e_{1,k+1}{}^{\nu}&=e_{1k}{}^{\nu}e_{k,k+1}{}^{\nu}=(e_{1k}+p_k')e_{k,k+1}{}^{\delta\mu}=(e_{1k}+p_k')(\alpha_k e_{k,k+1}+c_k)\\&=\alpha_k e_{1,k+1}+e_{1k}c_k+p'=e_{1,k+1}+p_{k+1},\end{aligned}$$

where p_k', p', $p_{k+1}\in P$. From above, we see $\alpha_k=1$ and $e_{1k}c_k\in P$. For $j\neq k$, $1<j$ we have from $0=e_{1j}{}^{\nu}e_{k,k+1}{}^{\nu}$, $e_{1j}c_k\in P$. Therefore all the components of c_k except the first row are divisible by p. And for $k+1\neq j$, $j<n$ we have from $0=e_{k,k+1}{}^{\nu}e_{jn}{}^{\nu}$ and $e_{kn}{}^{\nu}=e_{k,k+1}{}^{\nu}e_{k+1,n}{}^{\nu}$, $c_k e_{jn}\in P$ and $c_k e_{k+1,n}\in P$. So all the components of c_k except $(1,n)$-component are divisible by p. We have

$$c_k=\gamma_k e_{1n}+p_k,\quad p_k\in P.$$

As $e_{n-1,n}{}^{\nu}-e_{n-1,n}\in P$, we have $\gamma_1=\gamma_{n-1}=0$. Thus we have proved (5).

As for $(pe_{k+1,k})^{\nu}$, we have from $(pe_{k+1,k})^{\nu}\in P-P^2$,

$$(pe_{k+1,k})^{\nu}\equiv\sum_{i=1}^{n-1}\alpha_i{}^{(k)}pe_{ii}+\sum_{i=1}^{n-1}\beta_i{}^{(k)}pe_{i+1,i}+\sum_{i<j}\gamma_{ij}{}^{(k)}pe_{ij}\ (P^2).$$

From $0=e_{1l}(pe_{k+1,k})^{\nu}\equiv e_{1l}(pe_{k+1,k})^{\nu}$ (P^2) $(1<l\neq k+1)$, and $pe_{1k}{}^{\nu}\equiv e_{1k+1}(pe_{k+1,k})^{\nu}$, we have

$$\alpha_l{}^{(k)}=\beta_{l-1}{}^{(k)}=\gamma_{lj}{}^{(k)}=0\ (1<l\neq k);\quad \alpha_{k+1}{}^{(k)}=\gamma_{k+1,j}{}^{(k)}=0,\quad \beta_k{}^{(k)}=1.$$

Also we get $\alpha_1{}^{(k)}=0$ from $0\equiv(pe_{k+1,k})^{\nu}e_{1l}$ $(k\neq 1)$ and $(pe_{2l})^{\nu}=(pe_{2l})^{\nu}e_{1l}{}^{\nu}$ $(l\geqq 2)$. So we have

$$(pe_{k+1,k})^{\nu}\equiv pe_{k+1,k}+\sum_{1<j}\gamma_{1j}{}^{(k)}pe_{1j}.$$

As $0=(pe_{k+1,k})^{\nu}(e_{l,l+1})^{\nu}$ $(l\neq k)$ and $pe_{k+1,k+2}\equiv(pe_{k+1,k+2})^{\nu}\equiv(pe_{k+1,k})^{\nu}(e_{k,k+2})^{\nu}$, we have

$$\gamma_{1j}=0\ (k\neq j,n-1),\qquad \gamma_{1k}{}^{(k)}=0\ (k<n-2).$$

Finally, from the congruence

$$0=(pe_{21}pe_{n-1,n-2})^{\nu}\equiv p^2\gamma_{1,n-2}^{(n-2)}e_{2,n-2}\ (P^3)$$

we get $\gamma_{1,n-2}^{(n-2)}=0$ (p).

It is clear that every automorphism σ of N induces that of N/P.

And moreover all automorphisms of N/P are induced by those of N. To see this it suffices to prove the existence of an automorphism of N which induce each element of $\mathfrak{D}$, $\mathfrak{N}$ or $\mathfrak{I}$ of N/P. This is evident from the fact that the group $\mathfrak{G}$ of all automorphisms of N/P is decomposed into the product of these subgroups.

(i) Automorphisms inducing $\mathfrak{D}$.

Suppose δ of $\mathfrak{D}$ of N/P is given by the element $\bar{d}=\bar{e}_{11}+\bar{\alpha}_1\bar{e}_{22}+\cdots+\bar{\alpha}_{n-1}\bar{e}^{nn}$ of N/P. Then, the diagonal automorphism δ of N determined by the element $d=e_{11}+\alpha_1e_{22}+\cdots+\alpha_{n-1}e_{nn}$, $\alpha_i=\bar{\alpha}_i$ induces $\bar{\delta}$ itself on N/P.

(ii) Automorphisms inducing $\mathfrak{I}$.

For every inner automorphism $\bar{\tau}$ of N/P, $\bar{x}^{\bar{\tau}}=\bar{x}+b\bar{x}+\bar{x}\bar{a}+b\bar{x}\bar{a}$, we take an element a of N in the class $\bar{a}$ mod P and find b such that $a+b+ab=a+b+ba=0$. Then, the automorphism τ, $y^{\tau}=y+by+ya+bya$ induces $\bar{\tau}$ on N/P.

(iii) Automorphisms inducing $\mathfrak{N}$.

All nil automorphisms of N/P are generated by

$$\bar{e}_{k,k+1}{}^{\bar{\nu}}=\bar{e}_{k,k+1}+\bar{\gamma}_k\bar{e}_{1}{}^{n}. \qquad \bar{\gamma}_1=\bar{\gamma}_{n-1}=0. \quad [1]$$

In N we define a mapping ν as follows:

$$e_{k,k+1}{}^{\nu}=e_{k,k+1}+\gamma_k e_{1n}, \quad \gamma_k=\bar{\gamma}_k,$$
$$pe_{k,k+1}{}^{\nu}=pe_{k+1,k}.$$

It is clear that ν is an automorphism of N inducing $\bar{\nu}$ on N/P.

THEOREM 5. *The automorphisms of N which satisfy $x^{\sigma}-x\in P$ for $x\in N$ are inner.*

Proof. We put $e_{i,i+1}{}^{\sigma}-e_{i,i+1}=p_i$, $p_i\in P$. From $0=e_{i,i+1}{}^{\sigma}e_{j,j+1}{}^{\sigma}$ for $i+1\neq j$, we have

$$p_ie_{j,j+1}+e_{i,i+1}p_j\equiv 0 \quad (P^2),$$

that is

$$(p_i)_{i,j}+(p_j)_{i+1,j+1}\equiv 0 \quad (p^2).$$

Thus we know that the components of p_i are divisible by p^2 except the i-th row and the $(i+1)$-st column.

We construct a matrix Q in the same way as in the proofs of Theorems 1 and 2. We set

$$(Q)_{i+1,j}\equiv(p_i)_{i,j} \ (p^2) \quad (\text{for } i+1\neq j),$$

$$(Q)_{i,i}+(Q)_{i+1,i+1}\equiv(p_i)_{i,i+1}\ (p^2).$$

The inner automorphism induced from I_{1+Q}: $x^{I_{1+Q}}\equiv(1-Q)x(1+Q)\ (P^2)$ is the same one as $\sigma \bmod P^2$.

By the method similar to the proof of Theorem 1, we know σ is inner.

From Theorem 5 and the facts mentioned in (i), (ii), (iii) we have

THEOREM 6. *There is a natural mapping from the group of automorphisms of* N, $\mathfrak{G}(N)$ *onto the group of automorphisms of* N/P, $\mathfrak{G}(N/P)$. *And all automorphisms in the kernel of this mapping are inner.*

REFERENCES

[1] DUBISCH, R., AND S. PERLIS, On total nilpotent algebras. Amer. J. Math. **73** (1951), 439–452.

[2] SHODA, K., Über die Automorphismen einer endlichen Gruppe. Math. Ann. **100** (1928), 674–686.

[3] SZELE, T., Ein Satz über die Struktur der endlichen Ringe. Acta Univ. Szeged., Sect. Sci. Math. **2** (1948), 246–250.

DEPARTMENT OF MATHEMATICS,
TOKYO INSTITUTE OF TECHNOLOGY.