Amitsur, S. A.
Osaka Math. J.
15 (1963), 59-69.

REMARKS ON PRINCIPAL IDEAL RINGS

To Prof. K. Shoda

By

Shimshon A. AMITSUR

The study of non commutative (associative) principal ideal rings and its unique factorization has been carried out extensively by Asano [1] and others and was almost completely summarized by Jacobson in [3] (Ch. 3). The motivation to this study was the factorization of differential polynomials which constitute a non-commutative principal ideal ring (Ore [4]) and the factorization of elements in algebras, in particular in matrices with integral elements, or in general commutative principal ideal rings (e.g. Dickson, "Algebras and their arithmetics", Chicago 1923). The latter is closely connected with the subject of elementary divisors and invariant factors.

The present paper contains two additional notes to this subject and a generalization of a notion of local rings, which appears in arithmetical considerations of commutative rings. The first section deals with modules over locally principal ideal rings and applies the result to obtain some consequences in the direction of Hermite-ring which are stronger than obtained in [2]. In the second section, it is shown that the unique factorization theorem, in the sense of [4] or [5] (Ch. 3) holds in some more general principal ideal rings and this is applied to obtain a straightforward proof of Nakayama's theorem ([5]) on the uniqueness of the elementary divisors of matrices over principal ideal rings. The last part deals with a generalized notion of local rings of principal ideals ring at a prime p, and it is shown that such a ring exists if one takes into consideration all the primes equivalent to p.

1. Matrices and modules over principal ideal rings

Let R be an associative (not necessarily commutative) ring with a unit 1, and R_n be the ring of all $n\times n$ matrices over R.

We shall deal with rings R satisfying the following:

(R1) Every *finitely generated* right ideal is a principal right ideal.

(R2) For a left zero divisor $a \in R$, the right ideal $(0:a)=\{x \mid ax=0\}$ is a finitely generated ideal.

Our first result is:

Theorem 1.1. *Let R satisfy the conditions* (R1) *and* (R2), *then every finitely generated right ideal in the matrix ring R_n is a principal right ideal* (*i.e. R_n satisfies* (R1)); *furthermore, these ideals are generated by triangular matrices.*

To prove the theorem we begin with a lemma which is interesting by itself.

Lemma 1.2. *Let $V=v_1R+\cdots+v_nR$ be a free right R-module generated by n elements $v_1, \cdots, v_n$; and R be satisfying* (R1) *and* (R2)*-then every finitely generated submodules $W \subseteq V$ is generated by at most n element. Moreover, the generators of W can be chosen to be of the form: $w_k = v_kr_{kk}+\cdots+v_nr_{kn}$, $k=1, 2, \cdots, n$.*

Proof. Put $V^{(k)}=v_kR+\cdots+v_nR$, and let $I^{(k)}$ be the right ideal in R consisting of all $r_k \in R$ for which there exist $v \in V^{(k)} \cap W$ of the form $v=v_kr_k+\cdots+v_nr_n$. Clearly, $I^{(k)}$ is a right ideal.

First we note that if W is generated by the elements $u_1, \cdots, u_m$ then $I^{(1)}$ is a right ideal generated by the m coefficients of v_1 in the expression of $\{u_j\}$. Thus, it follows by (R1) that $I^{(1)}=r_{11}R$, and that there exists $w_1 \in W$ for which $w_1=v_1r_{11}+\cdots+v_nr_{1n}$. The definition of $I^{(1)}$ yields immediately that for every $v \in W$ there exists $x \in R$ such that $v-w_1x \in V^{(2)}$.

Next we assert that $V^{(2)} \cap W$ is also finitely generated. Indeed, let $w \in V^{(2)} \cap W$ and choose $x_i \in R$ for which $u_i-w_1x_i \in V^{(2)}$. Then, since $\{u_i\}$ generates W, we have:

$$w = \sum u_iy_i = \sum (u_i-w_1x_i)y_i+w_1 \cdot \sum x_iy_i$$

Since $w \in V^{(2)}$ the coefficient of v_1 in the w is zero, and thus the coefficient of v_1 in the right side is $r_{11}\cdot\sum x_iy_i=0$, i.e. $\sum x_iy_i \in (0:r_{11})$. Furthermore, if $a \in (0:r_{11})$ then $wa \in V^{(2)} \cap W$. Hence, $V^{(2)} \cap W$ is generated by the finite set $\{u_1-w_1x_1, \cdots, u_m-w_1x_m, w_1m_1, \cdots, w_1m_t\}$ where $m_1, \cdots, m_t$ are the finite set of generators (by (R2)) of $(0:r_{11})$.

The rest of the proof follows now easily by induction on n.

We turn now to the proof of the theorem; let I be a finitely generated ideal in R_n. Let V be the free module generated by all $1 \times n$ columns and $W=W(I)$ be the submodule of V generated by all columns of the matrices appearing in I. Since I is finitely generated so is W, and thus if $v_1=(1, 0, \cdots, 0)^*, \cdots, v_n=(0, 0, \cdots, 0, 1)^*$ [1], then it follows by the pre-

[1] A^* denotes the transpose matrix of A.

vious lemma that W is generated by: $w_1=(r_{11},\cdots,r_{n1})^*,\cdots,w_k=(0,\cdots,r_{kk},\cdots,r_{nk})^*,\cdots,w_n=(0,\cdots,0,r_{nn})^*$. Let $P=(w_1,w_2,\cdots,w_n)^*$ the triangular matrix formed by the columns w_j. We wish to show that $I=PR_n$; let E_{ik} be the matrix of R_n containing 1 in i-th row and k-th column and zero elsewhere. As $w_j\in W$ it follows that for some matrix $P_j\in I$ w_j appears in the $k=k(j)$ row of P_j; then, clearly, $P=\sum P_jE_{kj}\in I$. Now for every $Q\in I$, the j-th column of Q is a linear combination $\sum w_ir_{ij}$; hence, $QE_{jj}=P(r)_j$ where $(r)_j$ is the matrix containing $(r_{1j},\cdots,r_{nj})^*$ as the j-th column and zero elsewhere. Consequently $Q=\sum QE_{jj}=P(r_{ij})$, and the proof is completed.

Notice that the preceding proof actually yields

Corollary 1.3. *Let A be an $n\times m$ matrix over a ring R satisfying* (R1) *and* (R2), *then there exists a triangular $n\times m$ matrix D and two matrices P, Q such that $AP=D$ and $DQ=A$.*

REMARK. It is probable that (R2) need not hold in the matrix ring R_n even if R satisfies both (R1) and (R2). In order to get conditions for R which would be inherited to R_n one needs to require a stronger condition about finiteness of the generation of more general of ideal quotients.

We turn now to apply the preceding result to the case of Hermite-rings (Kaplansky [2]):

A ring R is called a *right-Hermite ring* if every 1×2 matrix (a, b) admits a diagonal reduction. Namely, there exists a 2×2 unimodular matrix Q such that $(ab)Q=(d0)$, and in this case every matrix has a triangular reduction. In view of corollary 1.3, we prove:

Theorem 1.4. *A ring R without zero divisors is a right-Hermite ring if and only if every finitely generated right ideal is principal.*

Proof. If R is right-Hermite, then it was already pointed out in [2, p. 465] that $aR+bR=dR$ where $(ab)Q=(d0)$.

To prove the converse, we first note that the assumpition of the theorem yields that any two non zero elements $a, b\in R$ have a common right multiple. Indeed, let $aR+bR=dR$ then $ax+by=d$ and $a=du$, $b=dv$; thus $byu=a(1-xu)$, and if $y=0$ the proof is evident. Consequently, R satisfies the Ore-condition for the embeddability of R in a division ring D, and hence $R_n\subseteqq D_n$. From which we deduce that if $PQ=1$ in R_n then $QP=1$, since it holds in D_n.

Clearly, R satisfies the conditions of corollary 1.3, hence considering the matrix $A=\begin{pmatrix} a & b \\ 0 & 1\end{pmatrix}$, we obtain $P, Q\in R_2$ for which

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} P = \begin{pmatrix} d & 0 \\ u & v \end{pmatrix}; \quad \begin{pmatrix} d & 0 \\ u & v \end{pmatrix} Q = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}.$$

To prove that (ab) admits the reduction to $(d\,0)$, it remains to prove that P is unimodular, since it also holds that $(a\,b)P=(d\,0)$. Indeed, we readily obtain that $APQ=A$ and if $a\neq 0$, A is not a zero divisor so $PQ=1$ and, consequently, $QP=1$ i.e. P is unimodular. The case $a=0$ is self evident.

In view of [2] lemma 3. 3, it follows now that:

Corollary 1. 5. *If in a ring R without zero divisors, the union of two principal right ideals is principal then the intersection of two principal right ideals is principal.*

This strengthen theorem 3. 4 of [2].

2. Unique factorization

For reasons of adhering to certain relations between the ring R and the matrix ring R_n — we use the following notations:

1) Two elements $a, b\in R$ are (right) equivalent if $R-aR\cong R-bR$ as right R-modules[2]. This is equivalent to the existence of elements $x, y, \cdots$ satisfying

$$\begin{aligned} xa &= by\,, & xu+bv &= 1 \\ ub &= aw\,, & ux+at &= 1 \end{aligned} \tag{2.1}$$

The relation of equivalency between elements will be denoted by $a\cong b$.

2) An element $a\in R$ is regular if it is neither right nor left zero divisor in R.

In the present section we deal with rings which satisfy some more restricted conditions than those of the preceding section. Namely,

(R3) a) Every right ideal which contains a regular element is a principal right ideal.

b) If $a\in R$ is regular and $b\in R$ arbitrary, then there exists $ax=by$ with y regular[3].

[2] This relation is called 'similarity' in ([4], [3] ch 3). This has its origin in the theory of differential polynomials. Since similarity is used in matrix ring for the relation $a=ubu^{-1}$, we prefer to call the present relation by 'equivalency' which is the natural generalization of classical equivalency i.e. $a=pbq$ with p, q invertible.

[3] The existence of a right common multiple follows as in the preceding section, the present condition emphasizes the regularity of y.

c) The right invertible elements of R form a group: the regular elements form a multiplicative semigroup and the factors of regular elements are regular.

The last condition will always be in the case:

Lemma 2.1. *If R can be embedded in a ring D with the same unit such that the (left) right zero divisors of R are also (right) left zero divisor in D, and such that the regular elements of R are also regular in D, then R satisfies* (R3c).

Indeed, if $ab=1$ then b is not a left zero divisor, since $bx=0$ implies $0=abx=x$. Thus b is not also a right zero divisor. Hence, $(ba-1)b=0$ implies that $ba=1$. This proves the first part of (R3c). The rest follows from the fact that our condition implies that all multiples of zero divisors are also zero divisors at least in D; hence cannot be regular in R.

A simple example of rings R satisfying lemma 2.1 are rings with a quotient ring in a matrix ring over division rings.

Condition (R3a) is less restrictive than the principal ideal requirement and we shall call a ring R a *regular-principal-right ideal ring* (r-pri ring) if it satisfies the three condition of (R3).

A r-pri ring R will be refered to as a *ring with factorization* if it satisfies also:

(R4) Every regular element in R can be written as a product of a finite number of prime elements.

One of the aims of the present section is to show that in a great many cases this property is inherited to R_n. Condition (R4) is generally proved if R is both right and left principal ideal ring ([3] p. 31). Nevertheless, some of the differential rings defined by Ore ([4]) are right but not left principal ideal ring but satisfy (R4).

It is well known that commutative principal ideal rings have unique factorization. The case of non-commutative right and left principal ideal rings without zero divisors is dealt extensively in [1] and [3]. The basic tools in the study of factorizations in rings is the application of the Jordan-Hölder theorem and the Krull-Schmidt-Remak factorization theorem for the R-module $R-aR$, for $a\in R$.

One can show easily that the same methods work as well for some general cases like matrix rings over principal ideal rings ([1]). Without additional efforts one can carry out the proofs also for the regular elements of an r-pri ring R with factorization. We shall summarise this result in the next theorem for further reference:

Theorem 2.2. *Let R be a r-pri ring with factorization and $a\in R$ be* *a regular element, then*:

1) *R-aR is R-irreducible if and only if a is prime.*
2) *The factorization $a=p_1, \cdots, p_n$ into prime factors holds in R and is unique up to equivalency.*
3) *The decomposition $a=[a_1, \cdots, a_m]$, $(a_i, [a_1, \cdots, \hat{a}_i, \cdots, a_m])=1$ into indecomposable factors is possible in R, and it is unique up to equivalency*[4].

Part (2) of the theorem is the Jordan-Holder theorem ([3] p. 34) and (3) is the Schmidt-Remak theorem ([3] ibid) and ([2]).

The following is an important class of r-pri ring:

Theorem 2. 3. *Let R be a (r-)pri ring without zero divisors then R_n is also an r-pri ring.*

Proof. Similar to the proof of theorem 1. 1 one verifies that every right ideal in R_n is a principal right ideal generated by a triangular matrix, and thus R_n satisfies (a) of (R3).

To prove (b) of (R3) we note that R can be embedded in a division ring D whose elements are of the form ab^{-1}, with $0 \neq b \in R$, $a \in R$, and hence it follows readily that every matrix $T \in D_n$ can be written as $T=T_0 \cdot t^{-1}$, where $T_0 \in R_n$, $t \in R$. Thus, for $A \in R_n$ regular and B arbitrary, we have in D_n the relation $A^{-1}B=T_0 t^{-1}$ for some $T_0 \in R_n$, $t \in R$. Consequently, $AT_0=B(t \cdot 1)$ and $t \cdot 1$ is regular.

The last requirement (c) of (R3) follows from lemma 2. 1.

It remains now to prove that R_n is a ring with factorization, and we note first that a diagonal matrix $D=\sum d_i e_{ii}$ is prime if and only if one d_j is prime in R and the rest of the d_j are invertible elements (Hilfsatz 3, § 6 is [1])[5]. Next, one verifies that triangular matrices can be written as a product of diagonal matrices and invertible elements, e.g.:

$$\begin{pmatrix} a_{11} & 0 & \cdots 0 \\ a_{12} & a_{22} & \\ & & \ddots \\ a_{1n} & & a_{nm} \end{pmatrix} = \begin{pmatrix} a_{11} & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & 1 \end{pmatrix} \begin{pmatrix} 1 & & 0 \\ a_{21} & 1 & \\ \vdots & & \ddots \\ a_{1n} & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & & 0 \\ & a_{22} & \\ & & \ddots \\ 0 & & 1 \end{pmatrix} \cdots$$

Rings R which are both right and left principal ideal rings have the property that for every matrix $A \in R_n$ there exist two invertible matrices

[4] $[a, b]$ denotes the least common right multiple of a, b and it exists in an r-pri ring R if both a and b are regular. (a, b) denotes the greatest common left divisor of a, b and it exists under the same condition. $\hat{a}_i$ denote the omission of a_i.

[5] The proof of this Hilfsatz assumes that R is both right and left principal ideal ring, but actually it uses only the possibility of triangular reduction in R_n which is valid in our case.

P, Q such that $PAQ=D$ and $D=\sum d_i e_{ii}$ is a diagnal matrix; and each d_i is a total divisor of d_{i+1} ([3] Theorem 10, ch. 3). This includes the fact that d_i is bounded by an element d_i^*, in the sense that d_i^*R is a the maximal two sided ideal containing d_i, and $d_iR \supseteqq d_i^*R \supseteqq d_{i+1}R$. The uniqueness of the invariant factors d_i (up to equivalency) was proved by Nakayama using properties of the factorizations and enumeration of prime factors of bounded elements (e.g. [3], theorem 31, p. 49). The present proof is a straight forward proof using factorization properties of r-pri rings with zero divisors, in particular R_n.

The following lemma for rings R of the type of theorem 2 will be used in the proof.

Lemma 2.4. *Let $a=[a_1, \cdots, a_n]$, $b=[b_1, \cdots, b_n]$ be the decomposition of a and b, regular elements, into indecompasable factors, such that $a_i \cong b_i$, $i=1, \cdots, n$ then $a \cong b$.*

This is a simple consequence of the fact that $R-aR=R_1 \oplus \cdots \oplus R_n$ with $R_i \cong R-a_iR$, and $R-bR$ has a similar decomposition with isomorphic factors.

Lemma 2.5. *Let a, b be regular: if $a=[a_1, a_2]$, $b=[b_1, b_2]$ with $(a_1, a_2)=(b_1, b_2)=1$ and such that $a \cong b$ and $a_1 \cong b_1$ then $a_2 \cong b_2$.*

Indeed, we use the decomposition of $a_1=[a_{i1}, \cdots, a_{ir_i}]$, $i=1, 2$ into indecomposable factors to obtain a decomposition of a, and similarly one obtains the decomposition of b. The condition that $a \cong b$ and the uniqueness of the decomposition together with $a_1 \cong b_1$ yields readily that the elements a_{1j} and b_{1j} can be paired into equivalent pairs, hence the preceding lemma yields that $a_2 \cong b_2$.

Lemma 2.6. *Let $a \in R$ be regular and c^* a regular bound element (i.e. $c^*R=Rc^*$) and let $a=(c^*, a)q$, $b=(c^*, b)p$, then $a \cong b$ implies that $(c^*, a) \cong (c^*, b)$ and $q \cong p$.*

Proof. $a \cong b$ means that $R-aR \cong R-bR$. In this isomorphism two-sided ideals are mapped on themselves, for if $1+aR \rightarrow x+bR$, and I is two sided then $I+aR \rightarrow xI+bR \subseteqq I+bR$, and isomorphism yields the equality of the image. In particular, for $I=c^*R$ we get that the preceding isomorphism yields that $(c^*R+aR)-aR \cong (c^*R+bR)-bR$ and $R-(c^*R+aR) \cong R-(c^*R+bR)$. The rest follows since $c^*R+aR=(c^*, a)R$ and $(c^*, a)R-aR \cong R-qR$ (by mapping $(c^*, a)+aR \leftrightarrow 1+qR$) etc. $\cdots$.

We need some additional properties of the matrix ring R_n. The proofs of which follow easily by (2.1):

Lemma 2. 7. *a) Let* $A=\begin{pmatrix}A_1 & 0\\ 0 & 0\end{pmatrix}$, $B=\begin{pmatrix}B_1 & 0\\ 0 & 0\end{pmatrix}$, *$A$ and $B \in R_n$ and $A_1, B_1 \in R_s$ then $A \cong B$ if and only if $A_1 \cong B_1$*

b) $A=\begin{pmatrix}A_1 & 0\\ 0 & 1\end{pmatrix}$, $B=\begin{pmatrix}B_1 & 0\\ 0 & 1\end{pmatrix}$ *of the same type of (a) then $A \cong B$ if and only if $A_1 \cong B_1$.*

We are now in position to prove:

Theorem 2. 8. (Nakayama) *Let R be a r-pri ring without zero divisors and $A \in R_n$. If $A \cong D = \sum d_iE_{ii}$ and d_i is total divisor of d_{i+1} for $i \geqslant 1$ then the d_i's and their bounds are uniquely determined up to equivalency. That is the elementary divisors of A, if they exists, are unique up to equivalency.*

By (*a*) of lemma 2. 7 we can reduce the problem to regular matrices A, i.e. $d_i \neq 0$.

Proof. Let $l(A)$ denote the number of prime factors of A in the factorization of A into prime factors; by the uniqueness of this number and the factorization of diagonal matrices as given in the proof of theorem 2. 3, it follows that $l(A)=l(D)=\sum l(d_i)$. The proof of the theorem will be induction on the triple $(n, l(D), l(d_1))$ arranged lexicographically.

Suppose $A \cong \sum e_iE_{ii} = E_i$ is a diagonal matrix such that e_i a total divisor of e_{i+1}, then $l(A)=l(D)=l(E)$.

The case $n=1$ is trivial. For $n>0$, if $l(D)=0$ then since $l(d_i) \geqslant 0$ it follows that all $l(d_i)=0$, i.e. d_i are invertible; similarly, since $l(D)=l(E)=\sum l(e_i)=0$, it follows that all $l(e_i)=0$, hence $d_i \cong e_i \cong 1$.

So let $n>0$, $l(D)>0$. If both $l(d_1)=l(e_1)=0$, then we may choose $d_1^*=e_1^*=1$ since both are invertible, and then by applying (*b*) of lemma 2. 7 we can reduce to the case of matrices of order $n-1$, since it follows by the lemma that $\sum_{i=2}^{n} e_iE_{ii} \cong \sum_{i=2}^{n} e_iE_{ii}$.

We shall denote the diagonal matrix $\sum u_iE_{ii}$ by $\mathrm{Diag}\,(u_1, \cdots, u_n)$.

Assume $l(d_1)>0$, and $l(d_1) \geqslant l(e_1)$ and consider the matrix $d_1^*1 = \mathrm{Diag}\,(d_1^*, d_1^*, \cdots, d_1^*)$[6] then we have $(D, d_1^*1) = \mathrm{Diag}\,(d_1, d_1^*, \cdots d_1^*)$ and $(\mathrm{Diag}\,(e_1, \cdots, e_n), d_1^*1) = \mathrm{Diag}\,((e_1, d_1^*), \cdots, (e_n, d_1^*))$ where (U, V) denotes the greatest common left divisor of U and V; and one readily shows that if $U=\mathrm{Diag}\,(u_1, \cdots, u_n)$, $V=\mathrm{Diag}\,(v_1, \cdots, v_n)$ $(U, V)=\mathrm{Diag}\,((u_1, v_1), \cdots, (u_n, v_n))$. It follows now by lemma 2. 6, since d^*1 is a bound in R_n, that $(D, d_1^*1) \cong (E, d_1^*1)$. If $l(D)>l\,[(D, d_1^*1)]$ then noticing that both (D, d_1^*1) and (E, d_1^*1) satisfy the condition that ths diagonal elements are total divisors of the ones following them — we can use the induction on

[6] 1 in the unit matrix in R_n.

$l(D, d_1^*1)$ and obtain for the first elementary divisor that $d_1 \cong (e_1, d_1^*)$. Consequently $l(e_1) \leqslant l(d_1) = l[(e_1, d_1^*)] \leqslant l(e_1)$; hence $l(d_1) = l(e_1)$, and $e_1 = (e_1, d_1^*)$ and thus $d_1 \cong e_1$. Now $D = [\text{Diag}\,(d_1, 1, \cdots, 1), \text{Diag}\,(1, d_2, \cdots, d_n)]$ and $E = [\text{Diag}\,(e_1, 1, \cdots, 1), \text{Diag}\,(1, e_2, \cdots, e_n)]$ (where $[U, V]$ denotes the least right common multiple of U, V). Since $D \cong E$ and $\text{Diag}\,(d_1, 1, \cdots, 1) \cong \text{Diag}\,(e_1, 1, \cdots, 1)$ it follows by lemma 2.5 that $\text{Diag}\,(1, d_2, \cdots, d_n) \cong \text{Diag}\,(1, e_2, \cdots, e_n)$ and by induction we get $d_i \cong e_i$ for $i \geqslant 2$. q.e.d.

It remains to consider the case $l(D) = l[(D, d_1^*1)]$, i.e. $D \cong \text{Diag}\,(d_1, d_1^*, \cdots, d_1^*)$ hence $l(D) = \sum l(d_i) = l(d_1) + (n-1)l(d_1^*)$ and since d_1^* is a divisor of d_1 we must have $l(d_i) = l(d_1^*)$, $i \geqslant 2$. Consequently, $d_i \cong d_1^*$; but then the preceding result yields that $E \cong (E, d_1^*1)$ and, therefore, $l(E) = \sum l(e_i) = \sum l[(e_i, d_1^*)] = l(D) = l(d_1) + (n-1)l(d_1^*)$. Since $l(e_i) \geqslant l[(e_i, d_1^*)]$ this could hold only if equality holds for all i and hence $e_i = (e_i, d_1^*)$. Consequently $l(e_i) \leqslant l[(e_i, d_1^*)] \leqslant l(d_1^*)$, but again the same reasoning yields that the equality holds for all $i \geqslant 2$, since by assumption $l(d_1) \geqslant l(e_1)$. Consequently $e_i \cong (e_i, d_1^*) \cong d_1^*$ for $i \geqslant 2$. Hence, $\text{Diag}\,(1, d_1^*, \cdots, d_1^*) \cong \text{Diag}\,(1, e_2, \cdots, e_n)$, and since $D = [\text{Diag}(d_1, 1, \cdots, 1), \text{Diag}(1, d_1^*, \cdots, d_1^*)] \cong [\text{Diag}\,(e_1, 1, \cdots, 1), \text{Diag}\,(1, e_2, \cdots, e_n)]$ it follows by lemma 2.5, that $\text{Diag}\,(d_1, 1, \cdots, 1) \cong \text{Diag}\,(e_1, 1, \cdots, 1)$ and, therefore, lemma 2.7 yields that $d_1 \cong e_1$ which completes the proof of the theorem.

3. Local quotients rings

In this section we denote by R a pri-ring without zero divisors and with factorization, and we deal with the existence of certain subrings of the quotient ring R, (which exists since they satisfy the Ore-condition) which behave like the local rings at a prime p of commutative ring.

Let D be the quotient ring of R containing all elements of the form ab^{-1}, $0 \neq b \in R$. Let p be a fixed prime element in R.

Let R_p be the set of all elements of R whose factors do not contain a prime $\cong p$; and we form $D_p = \{ab^{-1} \mid a \in R,\ b \in R_p\}$. Our main result is:

Theorem 3.1. *D_p is a proper pri-subring of D and all its primes are equivalent in D_p with p.*

Proof. To prove that D_p is a ring we first show that 1) R_p is a multiplicative set; and 2) for arbitrary $a \in R$, $b \in R_p$ there exist $x, y \in R$ such that $bx = ay$ and $y \in R_p$.

Indeed, let $a, b \in R_p$ and $a = p_1 \cdots p_n$, $b = q_1 \cdots q_m$ then $ab = p_1 \cdots p_n q_1 \cdots q_m$ is the factorization of ab and it does not contain factors $\cong p$; hence by the uniqueness of the factorization it follows that no factors of ab will be $\cong p$. The proof of the second part follows from the fact that if

$[a, b]=ay$ then $(aR+bR)-bR\cong aR-[a, b]R\cong R-yR$; on the other hand if $b=(a, b)\cdot c$ then $(aR+bR)-bR\cong(a, b)R-bR\cong R-cR$ so that $y\cong c$ but c is a factor of b hence $c\in R_p$ since its factors are not $\cong p$. Consequently $y\in R_p$.

The definitions of addition and multiplication in the quotient ring D, yields readily that D_p is a subring of D. For, if $b, d\in R_p$ then

$ab^{-1}+cd^{-1}=(a+cd^{-1}b)b^{-1}=(av+cu)(bv)^{-1}$ where $du=bv$ (i.e. $d^{-1}b=uv^{-1}$) and both $b, v\in R_p$ so $bv\in R_p$. Similarly $ab^{-1}\cdot cd^{-1}=(ax)(dy)^{-1}$ where $bx=cy$ and $b, y\in R_p$.

To complete the proof of the theorem, we consider a right ideal I in D_p. Let $I_0=I\cap R$, then I_0 is a right ideal in R and $I=I_0D_p$. Indeed, if $ab^{-1}\in I$ then $a=ab^{-1}\cdot b\in I\cap R=I_0$ and so $ab^{-1}\in I_0D_p$. Thus $I\subseteq I_0D_p\subseteq I$. Now let $I_0=qR$ then $I=qD_p$.

Consider now a factorization $q=q_1\cdots q_n$ of q in R into prime factors: If $q_j\not\cong p$ then q_j is invertible in D_p; thus it suffices to show that $q_j\cong p$ in R holds also in D_p and that p (and therefore also q_j) are primes in D_p as well. Indeed, if $q_j\cong p$ in R then the conditions (2.1) for the equivalency remains valid also in D_p and hence $q_j\cong p$ also in D_p. Suppose now that $p=(ab^{-1})(cd^{-1})$ in D_p then $p=a(b^{-1}c)d^{-1}=auv^{-1}d^{-1}$ where $[b, c]=cv=bu$. Thus, $pdv=au$. Both $d, v\in R_p$ hence they both do not contain prime factors $\cong p$; consequently, au has only one prime factor $\cong p$. If this factor appears in a, then since $cv=bu$ and both $b, u\in R_p$ it follows that $c\in R_p$ and therefore cd^{-1} is invertible in D_p. On the other hand if this factor appears in u then $a\in R_p$ and consequently ab^{-1} is invertible in D_p. To end the proof that p is prime in D_p we show that $pD_p\neq D_p$. Indeed, if it is not true then $1=pab^{-1}$ and thus $b=pa$ but $b\in R_p$ and has no factor $\cong p$, which by the uniqueness of factorization leads to a contradiction.

The ring D_p seems to be proper generalization of the notion of local subring at p and it coincides with it if R is commutative.

EXAMPLE. Let $R=K[t]$ be the ring of polynomials in a commutative indeterminate t with coefficient in a division ring K. Let $p(t)=t-k$, $k\in K$, then all equivalent prime elements of $p(t)$ are of the form $t-xkx^{-1}$, $x\in K$. Thus $D_p=\{f(t)g(t)^{-1}\}$ where no factor of $g(t)$ is of the form $t-xkx^{-1}$.

If k is algebraic over the center K then D_p can be characterized as the set of all quotients $f(t)g^{-1}(t)$ where $g(t)$ is relatively prime to the minimal polynomial $z(t)$ of k.

Indeed, let $z(t)=t^m+z_1t^{m-1}+\cdots+z_m$ and $z_i\in$ Center of K. Then $K[t]-z(t)K[t]$ is a simple ring with minimun condition for right ideals, hence it is a total matrix ring over a division ring (which can be identified with the centralizer of k in K). Consequently. $\bar{g}=g(t)+z(t)K[t]$ is a invertible element in $K[t]-z(t)K[t]$ (i.e. $(z, g)=1$) if and only if it is not a zero divisor in this ring. Now let $g=g_1\cdots g_k$ be the factorization of $g(t)=g$ into prime factors, then g is a zero divisor in $K[t]-z(t)K[t]$ if and only if at least one of the factors is a zero divisor, i.e. $g_ih_i=z\cdot u$ and $h_i\not\equiv 0 \pmod{z(t)}$. Since g_i is irreducible, and z belongs to the center it follows that g_i must divide z. Otherwise g_i divides u and hence $h_i\equiv 0$ $\pmod{z(t)}$. Next we observe that $z(t)$ is the least common multiple of all $t-xkx^{-1}$ where x ranges over all non zero element of K, hence all its prime factors, like g_i must be of the form $\simeq t-xkx^{-1}$. Combining this remarks, we obtain that $(z, g)=1$ if and only if $g\in R_p$ with $p=t-k$ and our assertion is proved.

The proof of this example can be carried out, without any changes for pri-rings R and prime factors p which are bounded by p^*. Namely:

Corollary 3.2. *If R is a pri-ring without zero divisors and a prime bounded by p^* then $D_p=\{ab^{-1}|\,b, a\in R$, and $(b, p^*)=1\}$.*

HEBREW UNIVERSITY

(Received January 10, 1963)

References

[1] K. Asano: Nichtkommutative Hauptidealringe, Act. Sci. Ind. 696, Hermann Paris, 1938.

[2] I. Kaplansky: *Elementary divisors and modules,* Trans. Amer. Math. Soc. **66** (1949), 464-491.

[3] N. Jacobson: The theory of rings, Amer. Math. Soc. Survey No. II, 1943.

[4] O. Ore: *Theory of non-commutative polynomials,* Ann. of Math. **34** (1933), 480-508.

[5] Serbin: *Factorization in principal ideal rings,* Duke Math. J. **4** (1938), 656-663.