UNIQUE FACTORIZATION IN A PRINCIPAL RIGHT IDEAL DOMAIN[1]

R. E. JOHNSON

An integral domain with unity in which every right ideal is principal is called a pri-domain. The classical example of a pri-domain is the polynomial domain $F[x]=\{\sum x^i a_i \mid a_i \in F\}$ over a division ring F, where multiplication is defined by $ax = xa^\sigma + a^\delta$, $a \in F$, with σ a monomorphism and δ an associated derivation of F (see Ore, [1]).

In what follows, R is a pri-domain and L is its lattice of right ideals. Each $a \in R$ has dimension, dim a, defined to be the length of the longest chain in the interval $[aR, R]$ of L. The elements of dimension 1 are the primes of R. Although dim a is conceivably infinite[2] for some nonzero $a \in R$, we are only interested in those elements for which $\dim a < \infty$. For convenience, let $R^* = \{a \in R \mid a \neq 0,\ 0 < \dim a < \infty\}$.

Each $a \in R^*$ may be expressed as a product of primes, $a = p_1 \cdot p_2 \cdot \cdots \cdot p_n$, where $n = \dim a$. For if p_1 is a prime left factor of a and $a = p_1 a_1$, then $R - a_1 R \cong p_1 R - aR$ (as right R-modules) and therefore $\dim a_1 = n-1$. The factorization now follows by induction. Elements b and c of R^* are said to be similar, $b \sim c$, if $R - bR \cong R - cR$. It may be shown by the usual proof for pri- and pli-domains (see [2, p. 34]) that if $a = p_1 \cdot p_2 \cdot \cdots \cdot p_n = q_1 \cdot q_2 \cdot \cdots \cdot q_n$, where all p_i and q_i are primes, then there exists a permutation α of $(1, 2, \cdots, n)$ such that $q_i \sim p_{\alpha(i)}$, $i = 1, 2, \cdots, n$.

Whenever $a \in R$ is represented as a product $a = a_1 \cdot a_2 \cdot \cdots \cdot a_n$, then a can also be represented as a product

$$a = (a_1 u_1)(u_1^{-1} a_2 u_2) \cdots (u_{n-1}^{-1} a_n) \tag{1}$$

for any units $u_1, u_2, \cdots, u_{n-1}$ of R. Let us call a factorization $a = a_1 \cdot a_2 \cdot \cdots \cdot a_n$ of a as a product of elements of a stated type *unique* if every other representation of a as a product of elements of the stated type has the form (1) above. It is the purpose of this note to describe a particular type of unique factorization that occurs in R.

Associated with each $a \in R^*$ is the subset L_a of L defined by

$$L_a = \{B \in [aR, R] \mid [aR, R] = [aR, B] \cup [B, R]\}.$$

By a lattice-theoretic argument, it is easily demonstrated that L_a is

Received by the editors, December 18, 1963.

[1] Research supported by NSF grant G24155.

[2] No example is known to the author where $\dim a = \infty$.

a finite chain $aR=B_k<B_{k-1}< \cdots <B_0=R$ and that

$$[aR, R] = [B_k, B_{k-1}] \cup [B_{k-1}, B_{k-2}] \cup \cdots \cup [B_1, B_0].$$

Let us call $a\in R^*$ *simple* if $L_a=\{aR, R\}$. Clearly every prime is simple, and if a is simple and $b\sim a$, then b is also simple. If R is commutative, then $a\in R^*$ is simple if and only if either a is prime or a has two dissimilar prime factors.

If $a\in R^*$ and $L_a=\{B_0, B_1, \cdots, B_k\}$ as above, with $B_i=b_iR$ and $b_i=b_{i-1}a_i$, $i=1, 2, \cdots, k$, $b_0=1$ and $b_k=a$, then $B_{i-1}-B_i\cong R-a_iR$, $i=1, 2, \cdots, k$. Since the lattice $[B_i, B_{i-1}]$ is not a union of two proper intervals of L, evidently each a_i is simple. Thus, $a=a_1\cdot a_2\cdot \cdots \cdot a_k$ where each a_i is simple but no element of the form $a_i\cdot a_{i+1}\cdot \cdots \cdot a_j$, $i<j$, is simple. It is easy to see that this is the unique factorization of a associated with the lattice L_a.

Let $a\in R^*$ and $a=a_1\cdot a_2\cdot \cdots \cdot a_k$ be the unique factorization of a associated with L_a as above. If $a_1=g\cdot h$ for some g, $h\in R^*$ and $c=h\cdot a_2\cdot \cdots \cdot a_k$, then $gc=a$. Since $[cR, R]\cong[aR, gR]$ and $[aR, gR] > [aR, a_1R]$, evidently $[cR, R]=[cR, c_{k-1}R]\cup[c_{k-1}R, c_{k-2}R]\cup \cdots \cup[c_1R, R]$ where $c_i=h\cdot a_2\cdot \cdots \cdot a_i$, $i>1$, and $c_1=h$. Each of the intervals $[c_iR, c_{i-1}R]$ is irreducible (i.e., not the union of two intervals) with the possible exception of $[c_1R, R]$. Hence, the factorization of c associated with L_c has the form $c=h_1\cdot \cdots \cdot h_r\cdot a_2\cdot \cdots \cdot a_k$ where $h=h_1\cdot \cdots \cdot h_r$ is the factorization of h associated with L_h.

A factorization of $a\in R^*$ into simple elements $a=a_1\cdot a_2\cdot \cdots \cdot a_k$ is called *irredundant* if no sub-product $a_i\cdot a_{i+1}\cdot \cdots \cdot a_j$, $i<j$, of a is simple. The main result of the paper is as follows.

THEOREM. *Each $a\in R^*$ has a unique irredundant factorization into simple elements.*

PROOF. The theorem is true if dim $a=1$. Assume that the theorem is true for every element of R^* of dimension less than n, and let $a\in R^*$ have dimension $n>1$. We know that a has an irredundant factorization into simple elements associated with L_a, say $a=a_1\cdot a_2\cdot \cdots \cdot a_k$. If $k=1$, then the factorization clearly is unique, so let us assume that $k>1$. Also assume that $a=c_1\cdot c_2\cdot \cdots \cdot c_m$, $m>1$, is an irredundant factorization of a into simple elements.

Since $c_1R\in[aR, R]=[aR, a_1R]\cup[a_1R, R]$, either $c_1R<a_1R$ or $c_1R\geqq a_1R$. If $c_1R<a_1R$ then $[c_1R, R]=[c_1R, a_1R]\cup[a_1R, R]$ contrary to the simplicity of c_1. Hence, $c_1R\geqq a_1R$. If $c_1R=a_1R$ then a has unique factorization by induction.

Finally, if $c_1R>a_1R$ then $a_1=c_1h$ for some $h\in R^*$ and $b=c_2\cdot \cdots \cdot c_m = h\cdot a_2\cdot \cdots \cdot a_k$. By a previous remark, the irredundant factorization of b into simple elements associated with L_b has the form $b=h_1\cdot \cdots \cdot h_r\cdot a_2\cdot \cdots \cdot a_k$. Since dim $b<n$, this must be the unique factorization of b into simple elements. Therefore, $c_2\cdot \cdots \cdot c_{r+1}=h_1\cdot \cdots \cdot h_r\cdot u$ for some unit u. However, then $c_1\cdot c_2\cdot \cdots \cdot c_{r+1}=a_1\cdot u$ contrary to the assumption that $c_1\cdot c_2\cdot \cdots \cdot c_{r+1}$ is not simple. This proves the theorem.

Let us call $a\in R^*$ *primary* if $[aR, R]$ is a chain. The above theorem has the following form for primary elements.

COROLLARY. *An element a of R^* is primary if and only if a has a unique representation as a product of primes.*

If R is commutative, then our definition of primary agrees with the usual one; $a\in R^*$ is primary if $a=p^n u$ for some prime p and some unit u.

Our results on simple elements of R^* are too fragmentary to present at this time.

We close this note with an example. Let $F=Z_2(t)$ be a transcendental extension of the integers modulo 2, $R=F[x]=\{\sum x^i a_i \mid a_i\in F\}$, $F\to^\sigma F$ be the monomorphism $a^\sigma=a^2$, and $\delta=0$. Thus, $ax=xa^2$ for every $a\in F$. The ring R is a pri-domain, but not a pli-domain. An unusual feature of R is that $x+a\sim x+b$ for all nonzero $a, b\in F$. The following statements can be verified by some elementary computations. x^2+a is prime if and only if $\sqrt[3]{a}\notin F$; x^2+t^n is prime if and only if $(n, 3)=1$; if $a=b^3\neq 0$, then x^2+a has the unique factorization $x^2+a=(x+b)(x+a/b)$; thus, x^2+a is always primary; $(x+a)^2$ is not primary if $a+ab=b^2\neq 0$ for some $b\in F$, for then $(x+a)^2=(x+b)(x+a^2/b)$; x^2+xt is primary; $(x+1)(x^2+t)$ is primary.

BIBLIOGRAPHY

1. O. Ore, *Theory of non-commutative polynomials*, Ann. Math. **34** (1933), 480–508.

2. N. Jacobson, *The theory of rings*, Math Surveys No. 2, Amer. Math. Soc., Providence, R. I., 1943.

UNIVERSITY OF ROCHESTER