On Factorization into Prime Ideals

ROBERT GILMER [1])

Let r be a regular element of the commutative ring R. It is well known that if r can be written as a finite product of prime elements of R, then this representation is unique. We consider here the corresponding question for ideals:

If A is a regular ideal of R such that A can be represented as a finite product of prime ideals of R, is this representation unique?

We begin by listing some observations concerning this question.

(1) Without the assumption that A is regular, the answer to the question is negative, even if R is Noetherian with identity. For example, (0) is prime in R for any integral domain R, and yet $(0)=[(0)]^n$ for each positive integer n. If R is the direct sum of two fields F_1 and F_2, then $P=F_1\oplus(0)$ is maximal in R, and $P=P^n$ for each positive integer n.

(2) Even with the assumption that A is regular, the answer to the question is negative, even if R is an integral domain with identity. For instance, $P_1=P_1P_2$ for any prime ideals P_1, P_2 of a valuation ring R with $P_1\subset P_2$; more generally the equality $P_1=P_1P_2$ holds for any prime ideals P_1, P_2 of a Prüfer domain with $P_1\subset P_2$ [1, Theorem 19.3].

(3) The following result appears as Theorem 30.13 of [1]:

Let A be a nonzero ideal of a Noetherian domain D such that A can be expressed as a finite product of prime ideals of D. Then this representation is unique if D contains no identity, and is unique to within factors of D if D contains an identity.

(4) By examining the proof of Theorem 30.13, we can see that the following result, which we label as (*), is valid.

(*) *Let A be a regular ideal of a commutative ring R such that A can be expressed as a finite product of finitely generated prime ideals of R. Then this representation is unique if R contains no identity, and is unique to within factors of R of R contains an identity.*

In this paper we exted (*) to the case where A is finitely generated, but the prime factors of A need not be finitely generated (Theorems 1 and 2). In Proposition 1, we prove that our results are stronger than (*) by proving that for any positive integers

[1]) During the writing of this paper, the author received partial support from National Science Foundation Grant GP-19406.

k and n, there is an integral domain D_k with identity containing prime ideals $P_1, \ldots, P_n$ such that $P_1^{e_1} P_2^{e_2} \ldots P_n^{e_n}$ is finitely generated if and only if $e_1 + \cdots + e_n \geqslant k$. Our proofs of Theorems 1 and 2 are independent of (*) and the result cited in (3). Moreover, our proofs are more elementary than the proof of (30.13) in [1]; these proofs rest on the following facts.

OBSERVATION 1. *If $\{A_i\}_1^n$ is a finite family of ideals of the commutative ring R, then $A_1 A_2 \ldots A_n$ is regular if and only if each A_i is regular.*

OBSERVATION 2. *If A is a regular ideal of the commutative ring R and if N is a multiplicative system in R, then the extension of A to the ring of quotients R_N is regular in R_N.*

RESULT 1. [1, Corollary 5.2] *If A and B are ideals of the commutative ring R such that $AB = B$, where B is finitely generated, then there is an element x of A such that $xb = b$ for each b in B: if B is regular, then R has an identity element and $A = R$.*

LEMMA 1. *Assume that A and B are ideals of the commutative ring R, where B is proper, finitely generated, and regular. Moreover, assume that $\{P_1, \ldots, P_m\}$ and $\{Q_1, \ldots, Q_n\}$ are two families of proper prime ideals of R such that $B = AP_1^{s_1} \ldots P_m^{s_m} = AQ_1^{t_1} \ldots Q_n^{t_n}$, where each s_i and each t_i is positive. Then each minimal element of the set $\{P_1, \ldots, P_m, Q_1, \ldots, Q_n\}$ occurs both as a P_i and as a Q_j, and the corresponding exponents s_i and t_j are equal.*

Proof. We assume that the labeling is such that P_1 is a minimal element of $\{P_i\}_1^m \cup \{Q_j\}_1^n$. If '$e$' denotes extension of ideals with respect to the quotient ring R_{P_1}, then

$$B^e = A^e (P_1^e)^{s_1} = A^e (Q_j^e)^{wt_j},$$

where $w = 0$ if $P_1 \notin \{Q_j\}_1$, while $w = 1$ and $P_1 = Q_j$ otherwise. The assumption $w = 0$ would lead to the equation

$$B^e = B^e (P_1^e)^{s_1},$$

where B^e is finitely generated, regular, and proper, and $(P_1^e)^{s_1}$ is proper in R_{P_1}, in contradiction to Result 1. Hence $w = 1$ and

$$B^e = A^e (P_1^e)^{s_1} = A^e (P_1^e)^{t_j}.$$

Again, if $t_j > s_1$, we obtain a contradiction, as above, from the equation

$$B^e = B^e (P_1^e)^{t_j - s_1}.$$

Therefore $s_1 = t_j$, and our proof is complete.

THEOREM 1. *Let B be a proper, finitely generated regular ideal of the commutative ring R such that B is a product of proper prime ideals of R. Then the representation of B as a finite product of proper prime ideals is unique.*

Proof. Let

$$B = P_1^{e_1} \dots P_m^{s_m} \quad \text{and} \quad B = Q_1^{t_1} \dots Q_n^{t_n}$$

be two representations of B as a finite product of proper prime ideals. From the proof of Lemma 1, it follows that the set S of primes P_i such that $P_i = Q_j$ for some j, and $s_i = t_j$, is nonempty. We assume that $S = \{P_1, \dots, P_r\}$, where $r \leqslant m$ and where $P_i = Q_i$ for $1 \leqslant i \leqslant r$. Setting $A = P_1^{s_1} \dots P_r^{s_r}$, we have

$$B = AP_{r+1}^{s_{r+1}} \dots P_m^{s_m} = AQ_{r+1}^{t_{r+1}} \dots Q_n^{t_n},$$

and the assumption $r < m$ or $r < n$ would lead to a contradiction of Lemma 1. Hence $r = m = n$, and this completes the proof of Theorem 1.

THEOREM 2. *Suppose that R is a commutative ring without identity and that B is a finitely generated regular ideal of R that is representable as a finite product of prime ideals of R. Then this representation is unique.*

Proof. We consider first the case when $B = R^n$ is a power of R. It is clear that R is the only prime factor of B. Hence we need only prove in this case that $R^n = R^m$ implies that $m = n$. Since R is a ring without identity, this follows immediately from Result 1.

If B is not a power of R, then we write

$$B = R^s P_1^{s_1} \dots P_m^{s_m} = R^t Q_1^{t_1} \dots Q_n^{t_n},$$

where $\{P_i\}_1^m$ and $\{Q_i\}_1^n$ are sets of m and n proper prime ideals of R, where s_i and t_j are positive, and s and t are nonnegative ($R^0 U$, for U an ideal of R, is defined to be U). If $N = R - [(\cup_1^m P_i) \cup (\cup_1^n Q_i)]$, and if '$e$' denotes extension of ideals of R to the quotient ring R_N, then

$$B^e = (P_1^e)^{s_1} \dots (P_m^e)^{s_m} = (Q_1^e)^{t_1} \dots (Q_n^e)^{t_n}$$

in R_N. By Theorem 1, $m = n$ and, by proper labeling, $P_i^e = Q_i^e$ and $s_i = t_i$ for $1 \leqslant i \leqslant m$. It follows that $P_i = Q_i$ for $1 \leqslant i \leqslant n$, and we have

$$B = R^s P_1^{s_1} \dots P_m^{s_m} = R^t P_1^{s_1} \dots P_m^{s_m}.$$

As before, the assumption $s > t$ would lead to the equation $R^{s-t} B = B$, and to a contradiction of the assumption that R does not contain an identity.

It is clear that Theorems 1 and 2 imply (*). It is conceivable, however, that Theorems 1 and 2 are not actually stronger than (*). That is, if the following statement (**) were true, then (*) would imply Theorems 1 and 2.

(**) *If* $\{P_i\}_1^m$ *is a finite family of regular prime ideals of the commutative ring* R, *and if* $e_1, \ldots, e_m$ *are positive integers such that* $P_1^{e} \ldots P_m^{e_m}$ *is finitely generated, then each* P_i *is finitely generated.*

We proceed to show that a very strong negation of (**) is, in fact, true.

PROPOSITION 1. *Let* k *and* n *be positive integers, where* $k \geqslant 1$. *There is an integral domain with identity containing prime ideals* $P_1, P_2, \ldots, P_n$ *such that the product* $P_1^{e_1} P_2^{e_2} \ldots P_n^{e_n}$ *is finitely generated if and only if* $\sum_{i=1}^n e_i \geqslant k$.

Proof. Let D be a non-Noetherian domain with identity containing distinct ideals $A_1, A_2, \ldots, A_n$ such that $A_{i_1} + A_{i_2} + \cdots + A_{i_r}$ is not finitely generated for any nonempty subset $\{i_1, i_2, \ldots, i_r\}$ of $\{1, 2, \ldots, n\}$[2]. Let t be an indeterminate over D, and let E_k be the subring $D[t^{k+1}, t^{k+2}, \ldots, t^{2k+1}]$ of $D[t]$; E_k is a graded ring with gradation D, Dt^{k+1}, $Dt^{k+2}, \ldots$. We set

$$A = (t^{k+1}, t^{k+2}, \ldots, t^{2k+1}), \qquad B = (t^{k+1}, t^{k+2}).$$

It is straightforward to verify that

$$A^n = (t^{n(k+1)}, t^{n(k+1)+1}, \ldots, t^{n(k+1)+k})$$

for any positive integer n,

$$A^n = B^n \quad \text{for } n \geqslant k, \quad \text{and}$$
$$B^r = (t^{r(k+1)}, t^{r(k+1)+1}, \ldots, t^{r(k+1)+r}) \quad \text{for } r < k.$$

We set $C_i = B + A_i t^{k+3}$ for $1 \leqslant i \leqslant n$. Each C_i is a homogeneous ideal of E_k, and $B \subset C_i \subset A$ for each i. Hence

$$C_1^{e_1} C_2^{e_2} \ldots C_n^{e_n} = A^{e_1 + \cdots + e_n} = B^{e_1 + \cdots + e_n}$$

if $e_1 + \cdots + e_n \geqslant k$, and $C_1^{e_1} C_2^{e_2} \ldots C_n^{e_n}$ is finitely generated.

If $e = e_1 + \cdots + e_n < k$, then $C_1^{e_1} C_2^{e_2} \ldots C_n^{e_n}$ is a homogeneous ideal of E_k, and its homogeneous component in $Dt^{e(k+1)+(e+1)}$ is

$$(A_{i_1} + A_{i_2} + \cdots + A_{i_r})\, t^{e(k+1)+(e+1)},$$

where $\{i_1, i_2, \ldots, i_r\}$ is the set of integers j such that $e_j \neq 0$. Because E_k is a graded ring and $A_{i_1} + A_{i_2} + \cdots + A_{i_r}$ is not finitely generated as an ideal of D, it follows that $C_1^{e_1} C_2^{e_2} \ldots C_n^{e_n}$ is not finitely generated as an ideal of E_k.

The ideals C_i of E_k are not prime in E_k. To obtain our desired example, we let D_k be the subring of $E = E_k[X_1, \ldots, X_n]$ consisting of all polynomials f such that the

---

[2]) Take, for example, $D = Z[\{X_j\}_{j=1}^{\infty}]$, and for $1 \leqslant i \leqslant n$, take $A_i = (\{X_j \mid j \in S_i\})$, where $S_1, \ldots, S_n$ are distinct infinite subsets of N, the set of positive integers.

coefficient of $X_1^{e_1} X_2^{e_2} \dots X_n^{e_n}$ in f is in $A_1^{e_1} A_2^{e_2} \dots A_n^{e_n}$ for each $e_1, e_2, \dots, e_n \geq 0$. Again D_k is a graded ring with gradation

$$E_k, \sum A_i X_i, \sum A_i^{e_i} A_j^{2-e_i} X_i^{e_i} X_j^{2-e_i}, \dots;$$

in fact, D_k is a graded subring of E, where E has the usual gradation by degree. The ideal $X_i E \cap D_k = P_i$ is a homogeneous prime ideal of D_k: in fact,

$$P_i = A_i X_i + A_i A_j X_i X_j + \cdots = A_i X_i D_k .$$

Hence

$$P_1^{e_1} P_2^{e_2} \dots P_n^{e_n} = A_1^{e_1} A_2^{e_2} \dots A_n^{e_n} X_1^{e_1} X_2^{e_2} \dots X_n^{e_n} D_k$$

is the set of polynomials f in D_k such that the coefficient of $X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$ in f is zero if $i_j < e_j$ for some j, and is in $A_1^{i_1} A_2^{i_2} \dots A_n^{i_n}$ otherwise. Hence $P_1^{e_1} P_2^{e_2} \dots P_n^{e_n}$ is finitely generated if and only if $e_1 + \cdots + e_n \geqslant k$.

We remark that the prime ideals P_i of Proposition 1 extend to maximal ideals of the quotient ring $(D_k)_S$, where $S = D_k - (\cup_1^n P_i)$. But $(D_k)_S$ is a quotient ring of $L[X_1, \dots, X_n]$, where L is the quotient field of E_k, and hence $(D_k)_S$ is Noetherian.

We have no counterexample to (**) in the case where the ideals P_i are maximal in R. In particular, we know of no example of a regular maximal ideal M of a commutative ring S with identity such that M is not finitely generated, but some power of M is finitely generated. If such M and S exist, then they also exist with M maximal in a quasi-local ring S.

The author acknowledges several discussions with Tom Parker concerning factorization into prime ideals. These discussions were helpful in the preparation of this paper.

REFERENCES

[1] Gilmer, R., *Multiplicative Ideal Theory* (Queen's University, Kingston, Ontario, 1968).
[2] Ribenboim, P., *Anneaux de Rees integralement clos*, J. Reine Angew. Math. *204* (1960), 99–107.

Florida State University, Tallahassee

Received July 13, 1971