ON A CLASSICAL THEOREM OF NOETHER IN IDEAL THEORY

ROBERT W. GILMER

A classical result in the ideal theory of commutative rings is that an integral domain D with unit is a Dedekind domain if and only if D is noetherian, of dimension less than two, and integrally closed. [8; 275]. The statement of this theorem is due essentially to Noether [6; 53], though the present statement is a refined version of Noether's theorem. (See Cohen [1; 32] for the historical development of the theorem above.) Noether did not, in fact, require that the domain D contain a unit element. By imposing greater restrictions on the prime ideal factorization of each ideal, she showed that D must contain a unit element.

This paper considers an integral domain J with Property C: Every ideal of J may be expressed as a product of prime ideals.

In particular, it is shown that an integral domain J with property C need not contain a unit element. However, factorization of an ideal as a product of prime ideals is unique and J is noetherian, of dimension less than two, and integrally closed.[1] A domain without unit having these three properties need not have property C. If J does not contain a unit element, J is the maximal ideal of a discrete valuation ring V of rank one such that V is generated over J by the unit element e, and conversely. The structure of all such valuation rings V is known. [4; 62].

If J is an integral domain with quotient field k, then J^* will denote the subring of k generated by J and the unit element e of k. We will assume that all domains considered contain more than one element.

If D is an integral domain, not necessarily containing a unit, and if k is the quotient field of D, the definitions of fractionary ideals of D, of sums, products and quotients of fractionary ideals, and of the fractionary ideal $(u_1, u_2, \cdots, u_t)$ of D generated by finitely many elements $u_1, u_2, \cdots, u_t$ of k, are generalized in the obvious ways. In particular, D^* is a fractionary ideal of D and if $\mathscr{S}$ is the collection of all nonzero fractionary ideals of D, $\mathscr{S}$ is an abelian semigroup under multiplication with unit element D^*. A fractionary ideal F of

Received January 22, 1963. This research was supported by the Office of Naval Research under contract number NONR G 00099-62.

[1] A domain D with quotient field k is integrally closed if D contains every element x of k with the following property: There exist elements $d_0, d_1, \cdots, d_n$ of D such that $x^{n+1} + d_n x^n + \cdots + d_1 x + d_0 = 0$.

D is said to be invertible if F has an inverse when considered as an element of $\mathscr{S}$. A nonzero principal fractionary ideal is invertible and $(d)^{-1} = (1/d)$. A product of fractionary ideals is invertible if and only if each of the factors is invertible. [8; 271].

The following two lemmas may be proved by making minor changes in the usual proofs given in the case of a domain with unit. [8; 272-273]. While the proof of Theorem 1 is definitely a modification of the usual proof for a domain with unit, the author feels enough difficulties arise to prove Theorem 1 here.

LEMMA 1. *If A is an invertible fractional ideal of the integral domain D, then $A^{-1} = D^*: A$. Further, A has a finite module basis over D.*

LEMMA 2. *Suppose A is a proper ideal of the domain D such that A may be expressed as a product of invertible prime ideals of D. This representation is unique if $D \subset D^*$, or unique to within factors of D if $D = D^*$.*

Henceforth in this paper, J will denote an integral domain without unit such that J has property C.

THEOREM 1. *Every nonzero proper prime ideal of J is invertible and maximal.*

Suppose first that there exists a nonzero proper invertible prime ideal P of J such that P is not maximal. We chose a such that $P \subset P + (a) \subset J$. We express $P + (a)$ and $P + (a^2)$ as products of prime ideals: $P + (a) = J^k P_1 \cdots P_r$, $P + (a^2) = J^t Q_1 \cdots Q_s$ where each P_i and each Q_j is a proper ideal of J. In $\bar{J} = J/P$ we have: $(\bar{a}) = \bar{J}^k \bar{P}_1 \cdots \bar{P}_r$, $(\bar{a})^2 = \bar{J}^t \bar{Q}_1 \cdots \bar{Q}_s$. By Lemma 2, $s = 2r$ and by proper labeling $P_i = Q_{2i-1} = Q_{2i}$. If $\bar{J}$ does not contain a unit element, then Lemma 2 implies also that $t = 2k$ so that $P + (a^2) = [P + (a)]^2$. If $\bar{J}$ contains a unit, then $(\bar{a}) = \bar{J}^k \bar{P}_1 \cdots \bar{P}_r$ so that r is positive and $(\bar{a}) = \overline{P_1 \cdots P_r}$. Similarly, $(\bar{a})^2 = \overline{Q_1 \cdots Q_s}$. Therefore $[P + (a)]^2 = P_1^2 \cdots P_r^2 = P + (a^2)$. For either case, therefore, $P + (a^2) = [P + (a)]^2$. The remainder of the proof of the theorem is the same as the proof appearing in [8; 273].

THEOREM 2. *J is a noetherian domain.*

We first show that J is finitely generated. Thus if J contains a proper nonzero prime ideal P, then $P = (p_1, \cdots, p_s)$ is maximal and finitely generated by Theorem 1 and Lemma 1. Therefore if $d \in J$, $d \notin P$, then $J = (p_1, \cdots, p_s, d)$. If (0) is the only proper prime ideal of J, then given $d \in J$, $d \neq 0$, $(d) = J^k$ for some integer $k \geqq 1$. Then J is invertible, and hence finitely generated.

It follows that every prime ideal of J is finitely generated. Since J has property C, every ideal of J is finitely generated.

THEOREM 3. *Every nonzero ideal of J is a power of J and, in fact, J is a principal ideal domain.*

Since J is noetherian and $J \subset J^*$, $J^2 \subset J$. [5; 172–73]. We choose $x \in J$, $x \notin J^2$. Because J has property C, (x) is prime. We shall show that $(x) = J$. We suppose that $(x) \subset J$. Because (x) is invertible and $J \subset J^*$, $(x) \supset (x)J \supset (x^2)$. If A is any ideal such that $(x) \supset A \supset (x^2)$ and if P is a prime factor of A, then $P \supseteqq (x)$ so that $P = (x)$ or $P = J$. Because $(x) \supset A \supset (x^2)$, $A = (x)J^k$ for some $k \geqq 1$. But $x \notin J^2$ so that $x^2 \notin (x)J^k$ for $k \geqq 2$. Therefore $k = 1$ and $(x)J$ is the unique ideal properly between (x) and (x^2).

We next show that (x^2) is a primary ideal. Thus if $a, b \in J$, $ab \in (x^2)$, and $a \notin (x)$, then $b \in (x)$. Hence $(x^2) \subseteqq (x^2, b) \subseteqq (x)$. Now (x) is maximal and prime in J so that $J/(x)$ contains a unit element $\bar{u}$. Because $a \notin (x)$, $ua \notin (x)$ so that $uax \notin (x^2)$ and therefore $ux \notin (x^2, b)$. This means $(x^2, b) \not\supseteqq (x)J$ so that $(x^2, b) = (x^2)$ by the preceding paragraph. Hence $b \in (x^2)$ and (x^2) is primary.

Now $ua - a \in (x)$ so that $(ua - a)^3 \in (x^2)$. If $z \in J$, then $z(ua - a)^3 = a^3(tz - z) \in (x^2)$ where t is a fixed element of J independent of z. Since $a^3 \notin (x)$ and (x^2) is primary, $tz - z \in (x^2)$ for each $z \in J$—i.e., $J/(x^2)$ contains a unit element. This means, however, that $V = (x)/(x^2)$ is a vector space over the field $J/(x)$. There is a one-to-one correspondence between subspaces of V and ideals of J between (x) and (x^2). Hence V has exactly one nonzero proper subspace, which is impossible. Therefore $J = (x)$ as asserted.

If P is a proper prime ideal of J, the argument above shows that $P \subseteqq J^2 = (x^2)$. This means for some ideal A of J, $P = A(x)$. Since P is prime, $P = A$. Now $(x) = J \subset J^*$ so that P is not invertible and thus $P = (0)$. Hence J is the only nonzero prime ideal of J. Therefore if A is a nonzero ideal of J, $A = J^k = (x^k)$ for some positive integer k.

A ring R with at most two prime ideals is called a *primary ring*. Theorem 3 shows that J is a primary domain. The author has investigated primary rings in [3].

THEOREM 4. *J^* is a discrete valuation ring of rank one. Conversely if D is a discrete valuation ring of rank one with maximal* *ideal M and if $D = M^*$, then M is a domain without unit having property C.*

The proof will use the following.

LEMMA 3. *Suppose S is a ring with unit e and that R is a subring of S such that S is generated by R and e. A subset of R is an ideal of S if and only if it is an ideal of R. S is noetherian if and only if R is noetherian.*

For the proof of the lemma, see [3].

To prove the theorem, we let $\xi \in k$, the quotient field of J^*. For some elements a and b of J, $\xi = a/b$. By Theorem 3 the ideals (a) and (b) of J compare—i.e. $a/b \in J^*$ or $b/a \in J^*$. Therefore, J^* is a valuation ring. Because J^* is noetherian, J^* is discrete and of rank one. [9; 41].

If M is the maximal ideal of J^* then $J = M^r$ for some r. Then $M^{r+1} \subset J$ implies $M^{r+1} = (M^r)^s$ for some integer s so that $r + 1 = rs$ and $r = 1$ – i.e., $J = M$. Hence J^*/J is a field. Because J^* is generated over J by e, $J^*/J = Z/(p)$ for some prime integer p.

The proof of the converse is an immediate consequence of Lemma 3 and of the fact that a discrete valuation ring of rank one is a Dedekind domain. [8; 278].

It is possible to classify all discrete valuation rings V of rank one such that $V = M^*$ where M is the maximal ideal of V, for if V has this property, so does the completion $\bar{V}$ of V. [2; 60]. If now p is a fixed prime, if Π denotes the prime field with p elements, x an indeterminate over π, if $V_1 = Z_{(p)}$ and $V_2 = (\Pi[x])_{(x)}$ then V_1 and V_2 are discrete valuation rings of rank one and with residue field Π. Further V_1 and V_2 are regular and *unramified* in Cohen's sense. [2; 88]. Thus $\bar{V}_1$ and $\bar{V}_2$ are so-called *p-adic* rings. [2; 59–60, 89]. Now $\bar{V}_1$ has characteristic zero (unequal characteristic case for $\bar{V}_1$ and its residue field) and $\bar{V}_2$ has characteristic p (equal characteristic case). The within isomorphism, $\bar{V}_1$ and $\bar{V}_2$ are the only two p-adic rings of dimension one having residue class field Π. [2; 89]. Now $\bar{V}_1$ is simply the domain of Hensel's p-adic integers and $\bar{V}_2$ is the domain of formal power series in one indeterminate over the field Π. [7; 242–243]. Finally, $\bar{V}$ is an Eisenstein extension of $\bar{V}_1$ or $\bar{V}_2$, and in case $\bar{V}$ has characteristic p, $\bar{V} \cong \bar{V}_2$. In short we have: If V has characteristic p, then to within isomorphism V is a ring between V_2 and $\bar{V}_2$. If V is unramified of characteristic 0, then $V_1 \subseteqq V \subseteqq \bar{V}_1$. If V is ramified of characteristic zero, then V is isomorphic to a valuation ring contained in an Eisenstein extension of $\bar{V}_1$. Conversely, if V is a ring having any of the three properties just described, V is a discrete valuation ring of rank one having residue field Π. [2; 59–60].

We add the following remarks:

In the last paragraph of the proof of Theorem 2, it is not necessary to use the fact that J has property C to conclude J is noetherian. That J is noetherian follows from a theorem of Cohen [1; 29] if all prime ideals of J are finitely generated.

In the proof of Theorem 3, it is not true in general that if $D/(x)$ is a field, that the ring $D/(x^2)$ contains a unit element, and hence that $(x)/(x^2)$ is a vector space over $D/(x)$. One can take D to be the ring of even integers and $x = 6$.

Theorem 3 implies that J is noetherian and of dimension less than two. Using Theorem 4, it is easily seen that J is integrally closed. That these three conditions do not imply that a domain D has property C may be seen by taking D to be the domain of even integers. Theorems 3 and 4 imply a bit more than the above. They even imply that J is a noetherian integrally closed primary domain. It can be shown that a noetherian integrally closed primary domain D without unit is the Jacobson radical of D^*, which is a semi-local ring, and that further, $D^*/D \cong Z/(p_1p_2 \cdots p_k)$ for some distinct primes $p_1, \cdots, p_k$. [3]. However, D need not have property C as can be seen by choosing D as the Jacobson radical of Z_M where M consists of all integers relatively prime to 6. An analog to the classical Noether theorem cited earlier in the case of a domain without unit, while obtainable, now seems not as desirable to the author as Theorem 4.

References

1. I. S. Cohen, *Commutative rings with restricted minimum condition*, Duke Math. J. **17** (1950), 27–42.
2. ———, *On the structure and ideal theory of complete local rings*, Trans. Amer. Math Soc., **59** (1946), 54–106.
3. R. W. Gilmer, *Commutative rings containing at most two prime ideals*, submitted to Michigan Math. J.
4. H. Hasse and F. K. Schmidt, *Die Struktur diskret bewerteter Korper*, J. Reine Angew. Math., **170** (1934), 4–63.
5. S. Mori, *Über Ringe, in denen die grossten primarkomponenten jedes Ideals eindeutig bestimmt sind*, J. Science Hiroshima U., Ser. A, 1, (1931), 160–193.
6. E. Noether, *Abstrakter aufbau der Idealtheorie in algebraischen zahl- und Funktionenkorpern*, Math., Ann., **96** (1927), 26–61.
7. B. L. van der Waerden, *Modern algebra*, v. 1. Ungar, New York, 1949.
8. O. Zariski and P. Samuel, *Commutative algebra* v. 1, von Nostrand, Princeton, 1958.
9. ———, *Commutative algebra*, V. 2, Von Nostrand, Princeton, 1960.