ON RINGS WITH A CERTAIN DIVISIBILITY PROPERTY

Hiroshi Gunji and Donald L. McQuillan

1. INTRODUCTION

Let θ be the ring of algebraic integers in an algebraic number field k. It is well known (and easily proved, usually by means of the zeta-function [4]) that if L is a finite Galois extension of k, then infinitely many prime ideals of θ split completely in L. In this paper we consider this property, in another formulation (see Proposition 8 in Section 3), for arbitrary integral domains (hereafter simply called rings).

DEFINITION. *Let* R *be a ring whose field of fractions is* K. *We call* R *a* D-*ring if whenever* f(x) *and* g(x) *are polynomials in* R[x] *with the property that* f(a) *divides* g(a) *in* R *for almost all elements* a *in* R, *then* f(x) *divides* g(x) *in* K[x].

We note first of all that it is unrealistic to demand here that f(x) divide g(x) in R[x], as the example f(x) = 2 and g(x) = x^2 - x in $\mathbb{Z}$[x] shows. For a discussion of polynomials $\phi(x)$ in K[x] such that $\phi(R) \subset R$, see [1], [2], [6], [7] and [8]; for generalizations, see [3].

We note next that if R is the ring of algebraic integers in an algebraic number field, then R is a D-ring. An easy proof goes as follows: Suppose that to the contrary f(a) divides g(a) in R for almost all elements a in R, but that f(x) does not divide g(x) in K[x]. Then we can assume that f(x) and g(x) are relatively prime in K[x] and that f(x) is not constant. Then there exist polynomials u(x) and v(x) in R[x] and a nonzero element d in R such that u(x)f(x) + v(x)g(x) = d. We conclude that f(a) divides d for almost all elements a in R. But this is a contradiction, since there are infinitely many prime ideals $\mathfrak{p}$ in R such that the congruence $f(x) \equiv 0 \pmod{\mathfrak{p}}$ has a solution in R.

It is clear that a field is not a D-ring, and it is easy to see that a ring that is not semisimple can not be a D-ring. Indeed, if R is not semisimple, then the polynomial f(x) = 1 + mx, where m is in the Jacobson radical and $m \neq 0$, has the property that f(a) divides 1 for all elements a in R.

Section 2 is devoted to results on general D-rings. We give several equivalent formulations of the concept, and from these we deduce that D-rings have some pleasant "going-up" properties:

Suppose S *is an over-ring of* R *that is integral over* R. *If* R *is a* D-*ring, then* S *is a* D-*ring.*

Suppose S *is an over-ring of* R, *finitely generated over* R. *Then* S *is a* D-*ring if either*

(i) R *is a* D-*ring or*

(ii) S *contains an element that is transcendental over* R.

Received December 4, 1974.

Michigan Math. J. 22 (1975).

We shall show by examples that in the second of these statements we cannot omit the "finitely generated", and also that the corresponding "going-down" result does not hold.

It is clear that the group U of units of R plays a role in all this. Let T be the torsion subgroup of U, and let C be a complete set of representatives of the cosets of T in U. We show that R *is not a* D-*ring if and only if for every subring* S *of* R, *the ring* S[C] *is not a* D-*ring.*

From this we deduce that *if the rank of* U *is finite, then* R *is a* D-*ring.* (This result was originally conjectured by C. Sundberg in a private communication. Sundberg proved a special case of it by using Theorem 7 in Chapter 7 of [5].)

In this connection we also prove the following. *Suppose that* $\mathbb{F}$ *is the prime field of* K. *If* R *is not a* D-*ring, then* K *is a purely inseparable extension (possibly infinite) of* $\mathbb{F}(U)$; *in particular, if the characteristic is* 0, *then* $K = \mathbb{F}(U)$.

In Section 3, we treat the special case of Dedekind rings. We mention here two results:

Let R be a Dedekind ring of characteristic 0. Then R is a D-ring if and only if whenever L is a finite Galois extension of K, infinitely many primes of R split completely in L.

Let R be a Dedekind ring of characteristic 0. Suppose the units of R have finite rank. Then, whenever L is a finite Galois extension of K, there are infinitely many primes of R that split completely in L.

The last result generalizes the statement on algebraic number fields given at the beginning of this section.

2. D-RINGS

Throughout this section, R is a ring and K is its field of fractions. If A and B are subsets of K and there is a finite set C in K such that $A \subset B \cup C$, we write $A < B$. The words "prime ideal of R" will always mean "nonzero prime ideal of R". We also fix the following notation and terminology.

(a) If $f = f(x)$ is a polynomial in $R[x]$, we denote by S(f) the set of prime ideals $\mathfrak{p}$ of R with the property that the congruence $f(x) \equiv 0 \pmod{\mathfrak{p}}$ has a solution in R. In particular, if c is an element of R, then S(c) is precisely the set of prime ideals of R that contain c.

(b) An over-ring S of R will be called *almost finitely generated over* R if $S \subset S_1$ and S_1 is a ring that is finitely generated over R (as a ring).

PROPOSITION 1. *Let* R *be a ring, and let* K *be the field of fractions of* R. *The following statements about* R *are equivalent:*

(i) R *is a* D-*ring.*

(ii) *There exists no nonconstant polynomial* f *in* $R[x]$ *such that* $f(R) < U_R$.

(iii) *If* f *is a nonconstant polynomial in* $R[x]$, *then* S(f) *is not empty.*

(iv) *If* f *is a nonconstant polynomial in* $R[x]$, *then* S(f) *is infinite.*

(v) *If* f *is a nonconstant polynomial in* $R[x]$ *and* c *is a nonzero element of* R, *then* S(f) - S(c) *is infinite.*

(vi) *If* f *and* c *are as in* (v) *then* S(f) - S(c) *is not empty.*

(vii) *Each subring* T *of* K *that is almost finitely generated over* R *is a* D*-ring.*

Proof. The proof is cyclic: (i) implies (ii) because if there exists a nonconstant polynomial f(x) in R[x] such that $f(R) < U_R$, then f(a) divides 1 in R for almost all a in R, but f(x) does not divide 1 in K[x]. This contradicts (i). Assume now that (ii) holds but that there exists a nonconstant f(x) in R[x] such that S(f) is empty. Then $f(R) \subset U_R$, which contradicts (ii). We show that (iv) follows from (iii). Let f(x) be nonconstant in R[x], and suppose that S(f) is finite, say $S(f) = \{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r\}$. There are two cases. Suppose first that f(0) = 0, so that $f(a) \in aR$ for all a in R. Then S(f) consists of all prime ideals of R, and therefore our assumption that S(f) is finite means in particular that R is not semisimple. If m is a nonzero element of the Jacobson radical, then $\psi(x) = 1 + mx$ has the property that $\psi(R) \subset U_R$, that is, $S(\psi) = \emptyset$. This contradicts (iii). Suppose then that $f(0) = a_0 \neq 0$. Take a nonzero element c in $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \cdots \cdot \mathfrak{p}_r$, and define g(x) in R[x] by the relation $a_0 g(x) = f(a_0 cx)$. Then $S(g) \subset S(f)$, g(0) = 1, and every other coefficient of g(x) is in $cR \subset \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \cdots \cdot \mathfrak{p}_r$. This forces S(g) to be empty, which contradicts (iii).

We show that (iv) implies (v). Let c be a nonzero element of R, and let f(x) be a nonconstant polynomial of R[x]. Suppose first that f(0) = 0. Then S(f) consists of all prime ideals of R, and thus if (v) does not hold, we can assume that c belongs to all but a finite number of prime ideals of R, say $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$. Take a nonzero element b in $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \cdots \cdot \mathfrak{p}_r$. Then bc is not zero and belongs to all prime ideals of R. In particular, bc is in the Jacobson radical of R, and if g(x) = 1 + bcx, then $S(g) = \emptyset$, which contradicts (iv). Suppose then that $f(0) = a_0 \neq 0$. Define g(x) in R[x] by the relation $a_0 g(x) = f(a_0 cx)$. Then g(0) = 1, all other coefficients of g(x) are divisible by c, and $S(g) \subset S(f)$. But S(g) is infinite, by (iv), and the result follows at once.

Now (v) implies (vi) and (vii) implies (i) trivially. It remains to show that (vi) implies (vii). Let T be a subring of K that is almost finitely generated over R. Then $T \subset R[1/v]$ for some v in R. Now R[1/v] is not a field (in other words, it is not K), since by (vi) there exists a prime ideal $\mathfrak{p}$ of R such that $v \notin \mathfrak{p}$ and therefore $\mathfrak{p}R[1/v]$ is a nontrivial ideal in R[1/v]. Thus T is not a field (that is, T is not K). Now suppose that f(x) and g(x) are in T[x] and that f(a) divides g(a) for almost all elements a of T. We show that f(x) divides g(x) in K[x]. Now we can assume that f(x) and g(x) are relatively prime in K[x]. Then we must show that f(x) is a constant. Suppose to the contrary that deg f(x) > 0. Now we can also suppose that f(x) and g(x) belong to R[x], and therefore we can find polynomials u(x) and w(x) in R[x] and a nonzero element c in R such that u(x)f(x) + w(x)g(x) = c. Then f(a) divides c for almost all a of T. By (vi), we can find a prime ideal $\mathfrak{p}$ of R and an element a of R such that $f(a) \in \mathfrak{p}$ and $cv \notin \mathfrak{p}$. But since c/f(a) is in T and therefore in R[1/v], we can write $c = f(a)b/v^N$, where $b \in R$ and $N \geq 0$. Thus $cv^N = f(a)b$. Reducing this equation modulo $\mathfrak{p}$, we get a contradiction. The proof is complete.

Examining the proof, we get the following reformulation:

PROPOSITION 2. *The preceding proposition remains true if we replace "prime ideal" everywhere by "maximal ideal".*

We give some easy consequences.

COROLLARY 1. R *is not a* D*-ring if and only if there exists a nonconstant polynomial* f(x) *in* R[x] *that is irreducible in* K[x] *and such that* $f(R) < U_R$.

Proof. If such a polynomial exists then R is not a D-ring, by Proposition 1. Conversely, if R is not a D-ring, there exists a nonconstant polynomial f(x) in R[x] such that $f(R) < U_R$. If f(x) is irreducible in K[x], we have finished. If f(x) is reducible in K[x], then there exist a nonzero element d in R and a polynomial g(x) in R[x], irreducible in K[x], such that g(x) divides df(x) in R[x]. Therefore g(a) divides d in R for almost all elements a in R. If d is a unit in R, the proof is complete. Otherwise, let $a_0 = g(0)$ and define $h(x) = a_0^{-1} g(a_0 dx)$. Then h(a) divides d for almost all a, h(x) is in R[x], h(x) is irreducible in K[x], and $h(x) = 1 + d\phi(x)$, where $\phi(x)$ is in R[x]. Then $1 = h(a) + d\phi(a)$, so that h(a) divides 1 for almost all a; that is, $h(R) < U_R$.

COROLLARY 2. *Let* R *be a ring that is not a field. Then* R *is not a* D*-ring if and only if there exists a nonconstant polynomial* f(x) *in* R[x] *such that* $f(R) \subset U_R$.

Proof. If $f(R) \subset U_R$, then certainly R is not a D-ring, by Proposition 1. Conversely, suppose R is a D-ring. Then, by Proposition 1, there exists a nonconstant polynomial f(x) in R[x] such that $S(f) = \emptyset$. Then $f(R) \subset U_R$. If $f(R) \not\subset U_R$, then f(a) is not a unit for some a in R, and therefore $f(a) \in \mathfrak{p}$ for some prime ideal $\mathfrak{p}$, since R is not a field. This means that $S(f) \neq \emptyset$, which is a contradiction.

COROLLARY 3. *Suppose* $R \subset S \subset K$, *where* S *is a ring, and suppose* $dS \subset R$ *for some nonzero element* d *in* R. *Then* R *is a* D*-ring if and only if* S *is a* D*-ring.*

Proof. $S \subset R[1/d]$, and thus, if R is a D-ring, so is S, by Proposition 1. Conversely, suppose S is a D-ring. If R is not a D-ring, then $f(R) < U_R$, where f(x) is a nonconstant polynomial in R[x]. Write g(x) = f(dx). Then g(x) is in S[x] and $g(S) = f(dS) \subset f(R) < U_R \subset U_S$. This is a contradiction.

The next corollary is a "going-up" result for non-D-rings. It will be shown later by an example that the stated condition on prime ideals can not be left out.

COROLLARY 4. *Let* S *be a subring of* K *that is almost finitely generated over* R. *Suppose that prime ideals of* R *are maximal. Then, if* R *is not a* D*-ring, neither is* S.

Proof. If we assume S is a D-ring, we get a contradiction as follows. Since $S \subset R[1/v]$ for some v in R, we see that $S[1/v] = R[1/v]$. Since S is a D-ring, so is S[1/v], by Proposition 1; that is, R[1/v] is a D-ring. Therefore we may assume from the beginning that $S = R[1/v]$. Now let f(x) be a nonconstant polynomial in R[x]. We verify statement (iii) of Proposition 1 to get the required contradiction. Consider f(x) in S[x]. By Proposition 1, there exist a prime ideal $\mathfrak{p}_1$ of S and an element a in S such that $f(a) \equiv 0 \pmod{\mathfrak{p}_1}$. Let $\mathfrak{p} = \mathfrak{p}_1 \cap R$. It is clear that $\mathfrak{p}$ is not (0) and thus $\mathfrak{p}$ is a maximal ideal by our assumption. Now v is not in $\mathfrak{p}$, and therefore $uv \equiv 1 \pmod{\mathfrak{p}}$ for some u in R. If $a = b/v^N$, define $a_1 = bu^N$. Then a_1 is in R and $a_1 \equiv a \pmod{\mathfrak{p}_1}$. It follows that $f(a_1) \equiv 0 \pmod{\mathfrak{p}_1}$, and hence $f(a_1) \equiv 0 \pmod{\mathfrak{p}}$. This completes the proof.

COROLLARY 5. *A polynomial ring in any number of indeterminates over an arbitrary ring is a* D*-ring.*

Proof. This is clear from (ii) of Proposition 1.

We next prove the "going-up" results mentioned in the introduction.

PROPOSITION 3. *Let* S *be an over-ring of* R *that is integral over* R. *If* R *is a* D*-ring, then* S *is a* D*-ring.*

Proof. Suppose first that S is finitely generated as a ring over R. Then S is finitely generated as a module over R, say $S = \sum_i Rw_i$. If S is not a D-ring, then

by Proposition 1 there exists a nonconstant polynomial $f(x)$ in $S[x]$ such that $f(S) < U_S$. Let L be the field of fractions of S, and write $F(x) = N_{L/K}f(x) \in K[x]$. Then $1/F(x)$ maps almost all elements of R into $N_{L/K}(U_S) \subset N_{L/K}\left(\sum_i Rw_i\right)$. It follows that $1/F(x)$ maps almost all elements of R into a finitely generated R-module, $\sum_j Ru_j$ say, in K. Pick a nonzero element d in R such that du_j is in R for each j and $F_1(x) = dF(x)$ is in $R[x]$. Then $F_1(a)$ divides d^2 for almost all elements a in R. This contradicts the fact that R is a D-ring.

If S is not finitely generated over R, we proceed as follows. We take a nonconstant polynomial $f(x)$ in $S[x]$ and verify statement (iii) of Proposition 1. Write $f(x) = \sum_{i=0}^{n} a_i x^i$, and set $S_1 = R[a_0, a_1, \cdots, a_n]$. Now $f(x)$ is in $S_1[x]$ and S_1 is a D-ring, by the first part of the proof. Therefore, by Proposition 2, there exist a maximal ideal $\mathfrak{p}_1$ in S_1 and an element a in S_1 such that $f(a) \equiv 0 \pmod{\mathfrak{p}_1}$. Now there exists a maximal ideal $\mathfrak{p}$ of S over $\mathfrak{p}_1$. Therefore $f(a) \equiv 0 \pmod{\mathfrak{p}_1}$, and the proof is complete.

COROLLARY 1. *Let* R *be a ring consisting of algebraic integers. Then* R *is a* D*-ring.*

Proof. It is easy to see, from statement (ii) of Proposition 1, for instance, that $\mathbb{Z}$ is a D-ring. The result follows at once.

COROLLARY 2. *Let* S *be an over-ring of* R *that is finitely generated over* R. *Then* S *is a* D*-ring if* R *is a* D*-ring. The same conclusion holds for* S *even if* R *is not a* D*-ring, provided that some element of* S *is transcendental over* R.

Proof. In either case, we can assume R is a D-ring and S is algebraic over R (use Corollary 5 of Proposition 1). Say

$$S = R\left[\frac{a_1}{v}, \frac{a_2}{v}, \cdots, \frac{a_n}{v}\right],$$

where each a_i is integral over R and v is in R. Then

$$R[a_1, a_2, \cdots, a_n] \subset S \subset R\left[\frac{a_1}{v}, \frac{a_2}{v}, \cdots, \frac{a_n}{v}\right],$$

and thus S is a D-ring, by Propositions 1 and 3.

We now give two examples that deal with the case when S is not finitely generated over R. The third example below is related to Corollary 4 of Proposition 1. It shows that the condition on prime ideals can not be omitted from that statement.

Example 1. Let V be the set of rational primes consisting of 2 and all odd primes p such that $p \equiv 1 \pmod 4$. Let W consist of all p^{-1} ($p \in V$). Then $S = \mathbb{Z}[W]$ is not a D-ring. Indeed, we show that if $f(x) = x^2 + 1$, $f(S) \subset U_S$ (the set of units of S). Let $\alpha = a/b$ be in S, where $a, b \in \mathbb{Z}$ and $(a, b) = 1$. Then $f(\alpha) = (a^2 + b^2)/b^2$, and it is clear that the only primes that can divide $a^2 + b^2$ are primes $p \in V$. Thus $f(\alpha) \in U_S$ and S is a non-D-ring.

Example 2. Let V be a set of rational primes p such that $\sum_{p \in V} 1/p$ converges, or more generally, such that V has Dirichlet density zero. Let W be the set of all p^{-1} ($p \in V$). Then $S = \mathbb{Z}[W]$ is a D-ring. If not, then there exists a nonconstant polynomial $f(x)$ in $S[x]$ such that $f(S) < U_S$. By Corollary 1 of Proposition 1, we can take $f(x)$ to be irreducible in $\mathbb{Q}[x]$. Now $f(\mathbb{Z}) < dU_S$ for some

rational integer d, and thus if the equation $f(x) \equiv 0 \pmod{p}$ has a solution in $\mathbb{Z}$, then $p \mid d$ or $p \in V$. It follows that if α is a root of $f(x)$, then the primes of $\mathbb{Z}$ that are covered in $\mathbb{Q}(\alpha)$ by a prime ideal of degree 1 are precisely the primes in V, with at most finitely many exceptions. Let L be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Let $N = [L:\mathbb{Q}]$. Now, if S is the set of primes of $\mathbb{Z}$ that split completely in L, then $S \subset V \cup S_0$, where S_0 is a finite set, and it is well-known that S has Dirichlet density $1/N$. This is impossible, since V has Dirichlet density zero.

Example 3. We give an example of a ring R and an element v in R ($v \neq 0$) such that R is a non-D-ring and $R[1/v]$ is a D-ring.

Let k be an algebraically closed field, and let z and x be two indeterminates over k. In the polynomial ring $k[z, x]$ let A be the multiplicative set consisting of polynomials $f(z, x)$ with the property that $f(0, x)$ is a nonzero constant in k. It is clear that A is saturated, in other words, that if f and g belong to $k[z, x]$ and $f \cdot g$ is in A, then both f and g are in A.

Set $R = A^{-1}k[z, x]$. We show that R is a non-D-ring but $R[1/z]$ is a D-ring.

Now the maximal ideals of $k[z, x]$ are the ideals of the form

$$M_{\alpha,\beta} = (z - \alpha, x - \beta),$$

where $\alpha, \beta \in k$. Note that our multiplicative set A is simply $k[z, x] - \bigcup_{\beta \in k} M_{0,\beta}$ so that the ideals $M_{0,\beta}R$ are maximal ideals in R. Conversely, every maximal ideal of R has this form. Indeed, let M be a maximal ideal of R, and set $\mathfrak{p} = M \cap k[z, x]$. Then $(\mathfrak{p}, z)$ is a proper ideal in $k[z, x]$, for otherwise we have a relation of the form $1 = p(z, x) + z \cdot g(z, x)$, where $p(z, x) \in \mathfrak{p}$ and $g(z, x) \in k[z, x]$. Hence $p(0, x) = 1$, so that $p(z, x) \in A$. This is impossible, since $p(z, x)$ is also in M. Thus $(\mathfrak{p}, z)$ belongs to a maximal $M_{0,\beta}$ and thus $M \subset M_{0,\beta}R$; that is, $M = M_{0,\beta}R$. But then the Jacobson radical of R, which is $\bigcap_{\beta \in k} M_{0,\beta}R$, contains z. Therefore R is a non-D-ring, by Corollary 1 of Proposition 1.

We show now that $R[1/z]$ is a D-ring. First we show that the units of $R[1/z]$ consist of all elements of the form $\frac{u(z, x)}{v(z, x)} \cdot z^r$, where $u(z, x)$ and $v(z, x)$ are in A, and r is an integer. A typical element of $R[1/z]$ looks like $\frac{f(z, x)}{g(z, x)} \cdot z^n$, where $n \leq 0$, $f(z, x) \in k[z, x]$, and $g(z, x) \in A$. After factoring out a z^s from $f(z, x)$, we can assume that $f(0, x) \neq 0$ and $n \in \mathbb{Z}$. If this element is a unit, then

$$\frac{f}{g} z^n \cdot \frac{f_1}{g_1} z^{n_1} = 1$$

for some elements f_1, g_1 and n_1 that satisfy conditions like those of f, g, and n, respectively. Then $f \cdot f_1 z^{n+n_1} = g g_1$. Evaluating at $z = 0$, we see that $n + n_1 = 0$. Therefore $f \cdot f_1 = g \cdot g_1 \in A$, and thus $f, f_1 \in A$, since A is saturated. Our statement on units is now clear.

Suppose now that $R[1/z]$ is not a D-ring. Then some polynomial $F(Y)$ in $R[1/z][Y]$ maps $R[1/z]$ to the units of $R[1/z]$. Multiplying through by a unit of the form $u(z, x) \cdot z^N$, where $u(z, x) \in A$, we can assume that $F(Y) \in k[z, x, Y]$. Write

$$F(Y) = F(z, x, Y) = \sum_{i=0}^{n} \left(\sum_{j=0}^{m_i} a_{ij} Y^j \right) x^i.$$

Here $a_{ij} = a_{ij}(z) \in k[z]$, and for each i we can assume that $a_{im_i} \neq 0$. Now choose N so big that for each i and for each $j > 0$, the function $a_{ij}(z)z^{-Nj}$ has a pole at $z = 0$ and for each i the pole of greatest order is achieved when $j = m_i$. Let ρ be the largest of the degrees of the poles of all the $a_{ij}z^{-Nj}$ at $z = 0$. Then for at least one i we know that $z^{\rho}a_{im_i}(z)z^{-Nm_i}$ is a polynomial in z that does not vanish at $z = 0$. Now choose $M > 0$ so that the integers $\{Mm_i + i\}_{i=0}^{n}$ are all distinct. Consider $F(z, x, x^M z^{-N})$, which by assumption is a unit in $R[1/z]$ and so has the form $\frac{u(z, x)}{v(z, x)}z^r$, where $u, v \in A$ and $r \in \mathbb{Z}$. Then the function $G(z, x) = z^{\rho}F(z, x, x^M z^{-N})$ also has this form $\frac{u}{v}z^r$. By our choices of M, N, and ρ, we know that $G(0, x)$ is a polynomial in x of positive degree. Evaluating $\frac{u}{v}\cdot z^r$ at $z = 0$, we get an immediate contradiction.

The preceding example shows that a result like Corollary 2 of Proposition 3 does not carry over, as it stands, to non-D-rings. Nevertheless, there is a natural generalization. We need some notation. For each positive integer n, let U_n denote the set of polynomials $f(x_1, x_2, \cdots, x_n)$ in $R[x_1, x_2, \cdots, x_n]$ with the property that $f(a_1, a_2, \cdots, a_n)$ is a unit in R for all $a_1, a_2, \cdots, a_n$ in R. Then U_n is a saturated multiplicative subset of $R[x_1, x_2, \cdots, x_n]$ that contains the units U of R.

LEMMA 1. *Let* n *be a positive integer. Let* R *be a ring that is not a field. Then* $U_n = U$ *if and only if* R *is a* D*-ring.*

Proof. If $n = 1$, the result follows from Corollary 2 of Proposition 1. Suppose that $n > 1$. Now, if R is not a D-ring, then $U_1 \neq U$, and therefore $U_n \neq U$. Suppose then that R is a D-ring. If $U_n \neq U$, we get a contradiction as follows. Take $f(x_1, x_2, \cdots, x_n)$ in U_n and suppose x_n actually appears in $f(x_1, x_2, \cdots, x_n)$. Since R is by assumption not finite, we can choose $a_1, a_2, \cdots, a_{n-1}$ in R so that $f(a_1, a_2, \cdots, a_{n-1}, x_n) = \phi(x_n)$ is a nonconstant polynomial in $R[x_n]$. But then $\phi(R) \subset U_R$, and we have contradicted the assumption that R is a D-ring.

Now let $\alpha_1, \alpha_2, \cdots, \alpha_n$ belong to an over-ring of R. We assume that $f(\alpha_1, \alpha_2, \cdots, \alpha_n) \neq 0$ for all $f(x_1, x_2, \cdots, x_n)$ in U_n. We write $A_n(\alpha)$ for the multiplicatively closed subset of $R[\alpha_1, \alpha_2, \cdots, \alpha_n]$ consisting of all $f(\alpha_1, \alpha_2, \cdots, \alpha_n)$, where $f(x_1, x_2, \cdots, x_n)$ is in U_n. We consider the ring $A_n(\alpha)^{-1}R[\alpha_1, \alpha_2, \cdots, \alpha_n]$.

PROPOSITION 4. *Let* R *be a ring that is not a field. Then* R *is a* D*-ring if and only if* $A_n(\alpha)^{-1}R[\alpha_1, \alpha_2, \cdots, \alpha_n]$ *is a* D*-ring.*

Proof. If R is a D-ring, then $U_n = U$, by the lemma, and therefore $A_n(\alpha) = U$. Thus $A_n(\alpha)^{-1}R[\alpha_1, \alpha_2, \cdots, \alpha_n] = R[\alpha_1, \alpha_2, \cdots, \alpha_n]$, and this is a D-ring, by Corollary 2 of Proposition 3. If R is not a D-ring, let f(x) be a nonconstant polynomial of degree m in $R[x]$ such that $f(R) \subset U$. We show that f(x) also maps $A_n(\alpha)^{-1}R[\alpha_1, \alpha_2, \cdots, \alpha_n]$ to the units of this ring. Let a/b belong to $A_n(\alpha)^{-1}R[\alpha_1, \alpha_2, \cdots, \alpha_n]$, where $a = g(\alpha_1, \alpha_2, \cdots, \alpha_n)$ and $b = h(\alpha_1, \alpha_2, \cdots, \alpha_n)$, and where $g(x_1, x_2, \cdots, x_n)$ is in $R[x_1, x_2, \cdots, x_n]$ and $h(x_1, x_2, \cdots, x_n)$ is in U_n. It is enough to show that $F(a, b) = b^m f(a/b)$ belongs to $A_n(\alpha)$, in other words, that $F(g(x_1, x_2, \cdots, x_n), h(x_1, x_2, \cdots, x_n))$ belongs to U_n. This amounts to showing that

$$F(g(a_1, a_2, \cdots, a_n), h(a_1, a_2, \cdots, a_n)) = h(a_1, a_2, \cdots, a_n)^m f\left(\frac{g(a_1, a_2, \cdots, a_n)}{h(a_1, a_2, \cdots, a_n)}\right)$$

is in U for all $a_1, a_2, \cdots, a_n$ in R. But this is clear from the definition of h and f. The proof is complete.

We now turn our attention to the role played by the units of R. Let T be the torsion subgroup of the group U of units of R. Let C be a complete set of representatives of the cosets of T in U.

PROPOSITION 5. *R is not a* D*-ring if and only if for every subring* S *of* R, *the ring* S[C] *is not a* D*-ring.*

Proof. If for every subring S of R, the ring S[C] is not a D-ring, then R = R[C] is clearly not a D-ring. Conversely, suppose R is not a D-ring. By Proposition 1, there is a nonconstant polynomial f(x) in R[x] such that $f(R) < U$. Let $f(x) = \sum_{i=0}^{n} a_i x^i$, and write $S_1 = S[a_0, a_1, \cdots, a_n]$. Then f(x) is in $S_1[U][x]$, the group U is the group of units of $S_1[U]$, and of course $f(S_1[U]) < U$. Thus, $S_1[U] = S[U][a_0, a_1, \cdots, a_n]$ is not a D-ring, by Proposition 1. Therefore S[U] is not a D-ring, by Corollary 2 of Proposition 3. But S[U] = S[C][T] is integral over S[C], and therefore S[C] is not a D-ring, by Proposition 3.

The next corollary follows at once.

COROLLARY 1. R *is a* D*-ring if there is a subring* S *of* R *such that* S[C] *is a* D*-ring.*

PROPOSITION 6. *Let* R *be a ring that is not a field. If the group* U *of units of* R *has finite rank, then* R *is a* D*-ring.*

Proof. If the rank of U is r, we can choose the representatives C of cosets of T in U so that they constitute a free subgroup of U on r generators $c_1, c_2, \cdots, c_r$. Let $\mathbb{P}$ be the prime ring of R. Then $\mathbb{P}[C] = \mathbb{P}[c_1, c_2, \cdots, c_r, c_1^{-1}, c_2^{-1}, \cdots, c_r^{-1}]$ is finitely generated over $\mathbb{P}$. If $\mathbb{P} = \mathbb{Z}$, then $\mathbb{P}[C]$ is a D-ring, by Corollary 2 of Proposition 3, and thus R is a D-ring, by the preceding corollary. If $\mathbb{P}$ is the Galois field $\mathbb{F}_p$ with p elements, there are two possibilities, namely $r > 0$ and $r = 0$. If $r > 0$, then each c_i must be transcendental over $\mathbb{F}_p$, and the same reasoning as before still works. Suppose then that r = 0, and that R is not a D-ring. We get a contradiction as follows. Let f(x) be a nonconstant polynomial in R[x] such that $f(R) \subset U = T$. If T is a finite group, it follows from this inclusion that R is also finite. But then R is a field, which contradicts our assumption. Suppose T is infinite. Let m = deg f(x) and $f(x) = \sum_{i=0}^{m} a_i x^i$. Choose m + 1 distinct elements $\alpha_0, \alpha_1, \cdots, \alpha_m$ in T. Say $f(\alpha_i) = \beta_i$ (in T). We can solve these m + 1 equations for the coefficients $a_0, a_1, \cdots, a_n$ to conclude that each a_i belongs to the field $\mathbb{F}_p[T]$. But then, if α is any element of R, we see that $f(\alpha) \in T$ and therefore α is algebraic over $\mathbb{F}_p[T]$. But then again we conclude that R is a field, and we have a contradiction.

Remark. Let R be a ring that is not a field. Let $\mathbb{P}$ be the prime ring of R. We can choose a set $\mathcal{J}$ of elements of R that are algebraically independent over $\mathbb{P}$ and maximal, in other words, such that R is algebraic over $P[\mathcal{J}]$. Let $\mathbb{P}_1$ be the integral closure of $\mathbb{P}[\mathcal{J}]$ in R. Then, applying our results, we deduce that $\mathbb{P}_1$ is a D-ring with the same field of fractions as R, and R is a D-ring if $\mathbb{P}_1[C]$ is finitely generated as a ring over $\mathbb{P}_1$ (the proof of this follows the lines of Proposition 6). The following question is therefore of interest: If R is a ring with field of fractions K and S is a ring such that $R \subset S \subset K$, under what conditions is S a D-ring? This question is answered in Section 3, for the special case when R is a Dedekind ring.

PROPOSITION 7. *Let* R *be a ring that is not a field. Denote by* $\mathbb{P}$ *the prime ring of* R, *by* K *the field of fractions of* R, *and by* $\mathbb{F}$ *the prime field of* K. *Let* p

($p \geq 0$) *be the characteristic of* R. *Suppose* R *is not a* D*-ring. Then there exist a nonnegative integer* m *and an element* c *in* $\mathbb{P}[U]$ *such that* $cR^{p^m} \subset \mathbb{P}[U]$. *In particular,* K *is a purely inseparable extension of* $\mathbb{F}(U)$.

Proof. By Corollary 1 of Proposition 1, there exists a nonconstant polynomial $f(x)$ in $R[x]$ such that $f(x)$ is irreducible in $K[x]$ and $f(R) \subset U$. Suppose first that $f(x)$ is separable. Now $\mathbb{P}[U]$ is infinite -- indeed, U is infinite, since otherwise the inclusion $f(R) \subset U$ would force R to be finite and R would then be a field. We can therefore choose α in $\mathbb{P}[U]$ so that $f'(\alpha) \neq 0$. Then $f_1(x) = f(x + \alpha)$ still maps R into U, and if $f_1(x) = \sum_{i=0}^{n} a_i x^i$, then $a_1 \neq 0$. Now let u be a unit such that $u^n \neq u$. Then

$$f(ux) - u^n f(x) = a_0(1 - u^n) + a_1(u - u^n)x + \cdots$$

is a polynomial in $R[x]$ that maps R into $\mathbb{P}[U]$ and is nonconstant. We can repeat this argument to arrive at a nonconstant polynomial $b_0 + b_1 x$ in $R[x]$ that maps R into $\mathbb{P}[U]$. Then $b_1 x$ maps $\mathbb{R}$ into $\mathbb{P}[U]$, and we have finished. If the original $f(x)$ is inseparable, then $f(x) = g(x^{p^m})$, where $g(y)$ is separable. If $g(y) = \sum_{i=0}^{t} a_i y^i$, then we can repeat the last part of the argument to get a polynomial $b_1 x^{p^m}$ that maps R into $\mathbb{P}[U]$. The proof is complete.

We end this section with an example to show that when the characteristic is positive, then K may indeed be different from $\mathbb{F}(U)$ and may even be an infinite extension of $\mathbb{F}(U)$.

Example 4. Let p be a prime, and let $S = \mathbb{F}_p[Y]$, where Y is transcendental over $\mathbb{F}_p$. Let R be the set of fractions $f(x)/g(x^p)$, where x is an indeterminate and $f(x)$ and $g(x)$ belong to $S[x]$ ($g(x) \neq 0$). Then U consists of all fractions $f(x^p)/g(x^p)$, where $f(x) \neq 0$ and $g(x) \neq 0$. Clearly, the polynomial $\phi(Z) = Z^p - Y$ maps R into U, and $[K : \mathbb{F}_p(U)] = p$. If we use infinitely many indeterminates $x_1, x_2, x_3, \cdots$, we get an example where $[K : \mathbb{F}_p(U)]$ is infinite.

3. DEDEKIND RINGS

We consider now the relation between Dedekind rings and D-rings.

PROPOSITION 8. *Let* R *be a Dedekind ring of characteristic* 0, *and let* K *be the field of fractions of* R. *Then* R *is a* D*-ring if and only if whenever* L *is a finite Galois extension of* K, *there are infinitely many prime ideals of* R *that split completely in the integral closure of* R *in* L.

Proof. Use a well-known theorem of Kummer (see Theorem 34 in Chapter 5 of [9]), together with statement (iv) of Proposition 1.

PROPOSITION 9. *Let* R *be a Dedekind ring of characteristic* 0, *and let* K *be the field of fractions of* R. *Suppose that the group of units of* R *has finite rank. Then, whenever* L *is a finite Galois extension of* R, *there are infinitely many prime ideals of* R *that split completely in the integral closure of* R *in* L.

Proof. This result follows from the preceding proposition together with Proposition 6.

Now let R be an arbitrary Dedekind ring, and let K be its field of fractions. We consider rings between R and K (see Examples 1 and 2 in Section 2), and we shall give a necessary and sufficient condition for such a ring to be a D-ring. We first

recall some well-known facts about these rings. Let $R \subset T \subsetneq K$. Then T is a Dedekind ring, and we can associate with T a family $S = \mathcal{S}(T)$ of prime ideals $\mathfrak{p}$ of R as follows: $\mathfrak{p} \in S$ if and only if there exists an element α in T such that $\mathrm{ord}_{\mathfrak{p}}(\alpha) < 0$. Conversely, if S is a family of prime ideals of R (with at least one prime ideal of R not in S), we can define a ring $T = \mathcal{T}(S)$ between R and K as follows: T consists of all elements α in K such that $\mathrm{ord}_{\mathfrak{p}}(\alpha) \leq 0$ for all $\mathfrak{p}$ in S. Now $\mathcal{S}(\mathcal{T}(S)) = S$ and $\mathcal{T}(\mathcal{S}(T)) = T$, and if T and S correspond in this way, we write $T = S^{-1}R$. We recall that if $T = S^{-1}R$, then the prime ideals of T are the ideals $\mathfrak{p}T$, where $\mathfrak{p}$ is a prime ideal of R and $\mathfrak{p} \notin S$.

We shall use the following notation:

(i) If S_1 and S_2 are families of prime ideals of R and there is a finite set S_0 of prime ideals of R such that $S_1 \subset S_2 \cup S_0$, then we write $S_1 < S_2$.

(ii) If $S_1 < S_2$ and $S_2 < S_1$, we write $S_1 \sim S_2$.

PROPOSITION 10. *Let* R *be a Dedekind ring, and let* K *be its field of fractions. Let* T *be a ring such that* $R \subset T \subsetneq K$. *Then* T *is a non-*D*-ring if and only if there exists a nonconstant polynomial* f(x) *in* R[x] *such that* $S(f) < \mathcal{S}(T)$.

LEMMA 1. *Suppose* $R \subset T_i \subset K$ (i = 1, 2). *Let* $T_i = S_i^{-1}R$, *and suppose* $S_1 \sim S_2$. *Then* T_1 *is a* D*-ring if and only if* T_2 *is a* D*-ring.*

Proof. Put $S_3 = S_1 \cap S_2$, so that $S_1 - S_3$ and $S_2 - S_3$ are both finite. Let $T_3 = S_3^{-1}R$. It is enough to show that T_3 is a D-ring if and only if T_i is a D-ring for i = 1, 2. In view of our remarks above, we can thus limit ourselves to proving this: R is a D-ring if and only if $S^{-1}R$ is a D-ring, where S is finite. Say $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r\}$, and let $v \in \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \cdots \cdot \mathfrak{p}_r$, $v \neq 0$. Then $S^{-1}R \subset R[1/v]$, and the result follows from Proposition 1 (vii) and Corollary 3 of that proposition.

LEMMA 2. *Let* R *be a Dedekind ring, and let* K *be its field of fractions. Let* $\mathfrak{p}$ *be a prime ideal of* R, *and let* $\alpha \in K$, $\alpha \neq 0$. *Then we can write* $\alpha = a/b$, *where* $a, b \in R$ *and either* $(a, \mathfrak{p}) = 1$ *or* $(b, \mathfrak{p}) = 1$.

Proof. Let $\alpha R = \mathfrak{a}/\mathfrak{b}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime integral ideals of R. Now there exists an element $a \in \mathfrak{a}$ $(a \neq 0)$ such that $((a)/\mathfrak{a}, \mathfrak{p}) = 1$. Let $\mathfrak{b} = (a)/\mathfrak{a}$. Then $\alpha R = \mathfrak{a}\mathfrak{b}/\mathfrak{b}\mathfrak{b} = (a)/\mathfrak{b}\mathfrak{b}$. Then $\mathfrak{b}\mathfrak{b}$ must be a principal integral ideal, say $\mathfrak{b}\mathfrak{b} = bR$. Then up to a unit $\alpha = a/b$, as required.

We now prove the proposition. Say $R \subset T \subsetneq K$. Suppose T is not a D-ring. Let $S = \mathcal{S}(T)$. There exists a nonconstant polynomial f(x) in T[x] such that $f(T) \subset U_T$. Choose d in R $(d \neq 0)$ so that $f_1(x) = df(x)$ is in R[x]. Then, if $a \in R$ we have the relation $f_1(a)R = (d)\mathfrak{a}/\mathfrak{b}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are integral ideals of R divisible only by prime ideals in S. It follows that if the equation $f(x) \equiv 0 \pmod{\mathfrak{p}}$ has a solution in R, then $\mathfrak{p}$ divides d or $\mathfrak{p} \in S$. Thus $S(f) < S$.

Conversely, suppose $S(f) < S = \mathcal{S}(T)$ for some nonconstant polynomial in R[x]. Write $f(x) = \sum_{i=0}^{n} a_i x^i$, where $n > 0$ and $a_n \neq 0$. Let S_0 be the finite set of primes $\mathfrak{p}$ such that $\mathfrak{p}$ divides a_n. Let S_1 be the finite set such that $S(f) \subset S \cup S_1$. Put $S_2 = S \cup S_0 \cup S_1$ and $T_2 = S_2^{-1}R$. We show that T_2 is a non-D-ring, from which it follows, by Lemma 1, that T is a non-D-ring. It is enough to show that $f(T_2) \subset U_{T_2}$. Let $\alpha \in T_2$. Then $f(\alpha) \in T_2$, and it will be enough to show that if $f(\alpha)R = \mathfrak{a}/\mathfrak{b}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are integral ideals of R, then the only prime ideals that divide $\mathfrak{a}$ belong to S_2. Let $\mathfrak{p}$ be a prime $(\mathfrak{p} \notin S_0)$. By Lemma 1, we can write $\alpha = a/b$, where $a, b \in R$ and either $(\mathfrak{p}, a) = 1$ or $(\mathfrak{p}, b) = 1$. Then

$$f(\alpha) = b^{-n}(a_0 b^n + a_1 ab^{n-1} + \cdots + a_n a^n).$$

If $\mathfrak{p}$ divides $a_0 b^n + a_1 ab^{n-1} + \cdots a_n a^n$, then $\mathfrak{p}$ cannot divide b, since otherwise $\mathfrak{p}$ divides $a_n a^n$, which is impossible. Thus b has an inverse, modulo $\mathfrak{p}$, and we have a solution of $f(x) \equiv 0 \pmod{\mathfrak{p}}$. It follows that $\mathfrak{p} \in S(f) \subset S_2$. Therefore $f(\alpha)$ is indeed a unit in T_2, and the proposition is proved.

COROLLARY 1. *Suppose* $R \subset T \subset K$. *If* T *is a non-*D*-ring, then so is every ring between* T *and* K. *If* T *is a* D*-ring, then so is every ring between* R *and* T.

COROLLARY 2. *Suppose* R *is the ring of algebraic integers of an algebraic number field* K. *Then, among the subrings of* K *that are infinitely generated over* R, *there are infinitely many* D*-rings and infinitely many non-*D*-rings.*

Proof. That there are infinitely many non-D-rings follows from the proposition. To show that there are infinitely many D-rings, do this. If f(x) is a nonconstant irreducible (in K[x]) polynomial in R[x], let S be any set of prime ideals $\mathfrak{p}$ of R such that $\mathfrak{p} \notin S(f)$. Then $S^{-1}R$ is a D-ring. For otherwise, $S(g) < S$ for some nonconstant polynomial g(x) in R[x], which can be assumed irreducible in K[x]. But then $S(f) \cap S(g)$ is finite, which is impossible.

REFERENCES

1. P. J. Cohen, *Polynômes à valeurs entières.* Canad. J. Math. 24 (1972), 747-754.
2. H. Gunji and D. L. McQuillan, *On a class of ideals in an algebraic number field.* J. Number Theory 2 (1970), 207-222.
3. ———, *On lattices over Dedekind rings* (to appear).
4. E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen.* Chelsea, New York, 1948.
5. S. Lang, *Diophantine geometry.* Interscience, New York, 1962.
6. A. Ostrowski, *Über ganzwertige Polynome in algebraischen Zahlkörpern.* J. Reine Angew. Math. 149 (1919), 117-124.
7. G. Pólya, *Über ganzwertige Polynome in algebraischen Zahlkörpern.* J. Reine Angew. Math. 149 (1919), 97-116.
8. Research Problems, Amer. Math. Monthly, Vol. 78 (1971), p. 179, and Vol. 80 (1973), p. 1124.
9. O. Zariski and P. Samuel, *Commutative algebra,* Vol. 1. Van Nostrand, Princeton, New Jersey, 1958.

University of Wisconsin
Madison, Wisconsin 53706