Topology Vol. 3, Suppl. 1, pp. 113–118. Pergamon Press. 1964. Printed in Great Britain

ON A SPECIAL CLASS OF DEDEKIND DOMAINS

OSCAR GOLDMAN

(*Received* 17 *May* 1963)

§1. INTRODUCTION

WE ARE interested in Dedekind domains R which have the following two properties:

F1: $R/\mathfrak{P}$ is a finite field for every maximal ideal $\mathfrak{P}$

F2: The group $U(R)$ of units of R is finitely generated.

The ring of integers of an algebraic number field and the Dedekind domains associated to curves over finite fields are examples of rings having the properties listed above. It is the main purpose of this note to show that there are many other examples and that, in fact, the quotient field of such a ring may have arbitrary, but finite, transcendence degree over the prime field. The particular manner in which these domains are constructed (§3) suggests that they may have some geometric significance; but that interpretation must be left for another occasion.

Certain elementary facts about the relation between units and ideal classes of a Dedekind domain seem not to have appeared in the literature. Since we shall need to use some of these facts, we shall include them here.

§2. UNITS AND IDEAL CLASSES

We begin by recalling some well-known facts. If R is a Dedekind domain with quotient field K and $\mathfrak{P}$ is a maximal ideal of R, then $R_{\mathfrak{P}}$ is a discrete rank one valuation ring and R is the intersection of all these $R_{\mathfrak{P}}$. Furthermore, $\cap R_{\mathfrak{P}} = R$ only if every prime ideal of R is included in forming the intersection. If S is a subring of K which contains R, then S is also a Dedekind ring. Furthermore, if $\mathfrak{P}$ is a prime ideal of R for which $\mathfrak{P}S$ is not S itself, then $\mathfrak{P}S$ is a maximal ideal of S and all maximal ideals of S arise in this way. Finally, the ring of quotients of S with respect to $\mathfrak{P}S$ (when $\mathfrak{P}S \neq S$) coincides with $R_{\mathfrak{P}}$.

If A is a set of maximal ideals of R, we denote by R^A the intersection of all $R_{\mathfrak{P}}$, as $\mathfrak{P}$ ranges over the prime ideals not in A. Then $\mathfrak{P}R^A = R^A$ is equivalent with $\mathfrak{P} \in A$.

PROPOSITION (1). *Let A be a finite set of maximal ideals of R. Then $U(R^A)/U(R)$ is a free abelian group whose rank does not exceed the cardinality of A. Equality holds if, and only if, the ideal class of each $\mathfrak{P} \in A$ is a torsion element of the ideal class group of R.*

Proof. A non-zero element x of K is a unit in R^A if, and only if, the decomposition of xR as a product of prime ideals contains only ideals of the set A. Thus, $U(R^A)/U(R)$ may be identified with a subgroup of the group of ideals generated by the primes in the set A. The assertions of the proposition follow immediately.

COROLLARY (1). *The following two statements are equivalent:*

(a) *Every subring of K which contains R is a ring of quotients of R;*

(b) *The ideal class group of R is a torsion group.*

Proof.

(a) $\rightarrow$ (b)

Let $\mathfrak{P}$ be a prime ideal of R; form R^A with A the set consisting of $\mathfrak{P}$ alone. Since R^A is a ring of quotients of R and $R^A \neq R$, there is a non-unit in R which is a unit in R^A. It follows from the proposition that the ideal class of $\mathfrak{P}$ is a torsion element. Since this is the case for every prime ideal of R, we see that the ideal class group of R is a torsion group.

(b) $\rightarrow$ (a)

Suppose S is a subring of K which contains R. Let M be the set of elements of R which are units in S, i.e., $M = R \cap U(S)$. M is then a multiplicative set, and we shall show that $S = R_M$. Clearly we have $R_M \subset S$. Let x be any element of S and set $xR = \mathfrak{A}\mathfrak{B}^{-1}$ where $\mathfrak{A}$ and $\mathfrak{B}$ are integral ideals of R with $\mathfrak{A} + \mathfrak{B} = R$. Then, $\mathfrak{A}S + \mathfrak{B}S = S$, while $\mathfrak{A}S = x\mathfrak{B}S \subset \mathfrak{B}S$ since $x \in S$. Hence $\mathfrak{B}S = S$. Now, under the assumption that the ideal class group of R is a torsion group, we have $\mathfrak{B}^n = bR$ with n some positive integer. Hence, from $\mathfrak{B}S = S$ we get $bS = S$, i.e., $b \in M$. But $x\mathfrak{B} = \mathfrak{A} \subset R$, so that $xb \in R$, i.e., $x \in R_M$. Thus $S = R_M$ and the proof is complete.

COROLLARY (2). *There is a subring S of K which contains R, which has the same unit group as R and whose ideal class group is a torsion group.*

Proof. The set of subrings of K which contain R and which have the same group of units as R satisfies the requirements for the application of Zorn's lemma. Let S be a maximal element of this set. Then $U(S) = U(R)$, and if S' contains S properly, then $U(S')$ is properly larger than $U(S)$. Applying the proposition to S shows that the ideal class group of S is a torsion group.

§3. SPECIAL DEDEKIND DOMAINS

THEOREM. *Let R be a Dedekind domain, with field of quotients K, which satisfies the hypotheses* F1 *and* F2 *(of the Introduction). Let X be an indeterminate over K. Then, there is a Dedekind domain S with field of quotients $K(X)$, which contains $R[X]$ as subring, which satisfies* F1 *and whose unit group coincides with the unit group of R (so that S also satisfies* F2*).*

Proof. We dispose first of the case where R has only a finite number of maximal ideals. It follows from F2 that in this case the group K^* of non-zero elements of K is finitely generated, and this can occur only when K is a finite field. Thus, in this situation K and R coincide and we simply take for S the ring $K[X]$.

From now on we suppose that R has infinitely many maximal ideals. We apply corollary (2) of proposition (1); let R' be a ring between R and K with the same unit group as R and having a torsion ideal class group. If we replace R by R' in the statement of the theorem, and prove the existence of S relative to R', then that S would have the required properties relative to R. Thus we may and shall assume from now on that R has a torsion ideal class group.

We show first that K is countable. If $\mathfrak{A}$ is a non-zero integral ideal, it follows from F1 that $R/\mathfrak{A}$ is a finite ring. Denote, as usual, by $N\mathfrak{A}$ the number of elements of $R/\mathfrak{A}$. If m is any integer, the number of integral ideals $\mathfrak{A}$ for which $N\mathfrak{A} = m$ is finite. Namely, let $a_1, \ldots, a_{m+1}$ be distinct elements of R. If $N\mathfrak{A} = m$, then $a_i - a_j \in \mathfrak{A}$ for some pair of distinct indices i, j, so that $\mathfrak{A}$ is a divisor of $R(a_i - a_j)$. Since the number of such divisors is finite, it follows that the number of $\mathfrak{A}$ is finite. We conclude that the group of ideals of R is countable, which, when combined with the countability of $U(R)$, shows that K is countable.

The lemma which follows contains the crucial element of the proof of the theorem.

LEMMA (1). *Let $\mathfrak{N}$ be a maximal ideal in $R[X]$. Then there is a discrete rank one valuation ring V in $K[X]$, having the following properties:*

(a) $V \supset R[X]$;

(b) $\mathfrak{M} \cap R[X] = \mathfrak{N}$, *where $\mathfrak{M}$ is the ideal of non-units of V;*

(c) *$V/\mathfrak{M}$ is a finite field.*

Proof. The fact that R is a Dedekind domain with infinitely many maximal ideals implies in particular that R is a Hilbert ring. (See [1] for a discussion of those properties of Hilbert rings which are needed here.) Hence $\mathfrak{P} = \mathfrak{N} \cap R$ is a maximal ideal. Then, $\mathfrak{P}R[X] \subset \mathfrak{N}$ and $\mathfrak{N}/\mathfrak{P}R[X]$ is a maximal ideal in $R[X]/\mathfrak{P}R[X] \cong R/\mathfrak{P}[X]$. In particular, $\mathfrak{N}/\mathfrak{P}R[X] \neq 0$, and is a proper ideal. Since $R/\mathfrak{P}$ is a field, $\mathfrak{N}/\mathfrak{P}R[X]$ is a principal ideal. We choose an element f of $\mathfrak{N}$ whose image in $\mathfrak{N}/\mathfrak{P}R[X]$ generates that ideal. Furthermore, we may choose f to be monic. Certainly $f \notin R$. And finally it is clear that $\mathfrak{N} = \mathfrak{P}[RX] + fR[X]$.

The maximal ideal $\mathfrak{P}$ of R defines a valuation of K; let Γ be the completion of K with respect to this valuation, and let $\mathfrak{O}$ be the ring of integers of Γ. Since $R/\mathfrak{P}$ is finite, $\mathfrak{O}$ is compact and hence, in particular, $\mathfrak{O}$ is not countable. Since K is countable, there are elements of $\mathfrak{O}$ which are transcendental over K and hence also non-units of $\mathfrak{O}$ which are transcendental over K. Let t be such a non-unit.

We introduce another indeterminate Y, and consider the polynomial $F(Y) = f(Y) - t \in \Gamma[Y]$. Then F is a monic polynomial, of positive degree, with coefficients in $\mathfrak{O}$. Let Ω be an extension of Γ of finite degree which contains a zero y_0 of F. Then, firstly y_0 is integral over $\mathfrak{O}$, and secondly, y_0 is still transcendental over K.

Because y_0 is transcendental over K, there is an imbedding of $K(X)$ into Ω in which X is mapped on y_0. The valuation of Γ extends (uniquely) to Ω, again with finite residue class field. The imbedding of $K(X)$ into Ω induces a valuation in $K(X)$; we denote its valuation

ring by V. Clearly V is a discrete rank one valuation ring with finite residue class field. Since y_0 is integral over $\mathfrak{O}$, we have $X \in V$ and hence $R[X] \subset V$. If $\mathfrak{M}$ is the ideal of non-units of V, then certainly $\mathfrak{P} \subset \mathfrak{M}$. Furthermore, under the imbedding of $K(X)$ into Ω, f maps into t which is in $\mathfrak{O}$ and is a non-unit in that ring. Hence $f \in \mathfrak{M}$, and therefore $\mathfrak{N} = \mathfrak{P}R[X] + fR[X] \subset \mathfrak{M} \cap R[X]$. However, $\mathfrak{N}$ is a maximal ideal so that we have $\mathfrak{N} = \mathfrak{M} \cap R[X]$ and the proof of the lemma is complete.

Denote by A the set of non-zero elements a of R which are such that rad (aR) is a prime ideal. Since the ideal class group of R is a torsion group, every maximal ideal of R has the form rad (aR), for some $a \in A$. Denote by A_0 a subset of A with the following property: every maximal ideal of R has the form rad (aR) for a unique $a \in A_0$.

If f is a non-zero element of $R[X]$, one calls the *content* of f the ideal $C(f)$ in R generated by the coefficients of f. It is well known that $C(fg) = C(f)C(g)$. Denote by B the set of all non-zero $f \in R[X]$ with the following properties:

(a) $f \notin R$;

(b) $C(f) = R$;

(c) rad $(fR[X])$ is a prime ideal of $R[X]$.

If f and g are elements of B, the equality rad $(fR[X])$ = rad $(gR[X])$ defines an equivalence relation in B. Denote by B_0 a subset of B which contains exactly one representative from each equivalence class of B. Note that because of (b), rad $(fR[X])$ is not the extension to $R[X]$ of an ideal of R.

Since K is countable, the same is the case for $K[X]$ so that both A_0 and B_0 are countable sets. Let $t_1, t_2, \ldots$ be an enumeration of the elements of $A_0 \cup B_0$.

LEMMA (2). *For each n, we have $t_1 t_2 \ldots t_{n-1} \notin$ rad $(t_n R[X])$.*

Proof. Note that rad $(t_n R[X])$ is a prime ideal in $R[X]$, so that we need only show that $t_m \notin$ rad $(t_n R[X])$ if $m \neq n$. But this follows directly from the definition of the sets A_0, B_0.

LEMMA (3.) *If y is a non-zero element of $R[X]$, then there is a positive integer h such that $y^h = u t_1^{h_1} t_2^{h_2} \ldots t_n^{h_n}$ with u a unit of R and $h_i \geqslant 0$.*

Proof. For a suitable non-zero element b of K we may write $y = b f_1 f_2 \ldots f_m$ with $f_i \in R[X]$ and f_i an irreducible polynomial viewed as an element of $K[X]$. Since the ideal class group of R is a torsion group, there is a positive integer r such that each of the ideals $C(f_1)^r$, $C(f_2)^r \ldots$, $C(f_m)^r$ is principal. Thus, $f_i^r = d_i g_i$, with $d_i \in R$ and $g_i \in R[X]$ such that $C(g_i) = R$. Furthermore, it is clear that $g_i \in B$. Thus, $y^r = d g_1 \ldots g_m$, with $d \in K^*$ and $g_i \in B$. And, since $C(g_i) = R$, actually $d \in R$.

Each g_i is equivalent to some element of B_0. That is, $g_i^s = a \tau^k$ where s and k are positive integers, $a \in K^*$ and $\tau \in B_0$. Thus, with N a positive integer, we have $y^N = d' \tau_1 \ldots \tau_m$, where the τ_i are in B_0, and as above $d' \in R$.

Let $d'R = \mathfrak{P}_1 \ldots \mathfrak{P}_g$ be the factorization of the ideal $d'R$. Each $\mathfrak{P}_i$ when raised to a

suitable positive power is principal, and generated by an element of A_0. Hence $d'^M = v\alpha_1 \dots \alpha_j$, with $\alpha_i \in A_0$ and v a unit in R.

Assembling these facts shows that $y^h = ut_1^{h_1} \dots t_n^{h_n}$ with $h \geqslant 1$, $h \geqslant 0$ and u a unit in R. This completes the proof of Lemma (3).

Since R is a Hilbert ring, the same is the case for $R[X]$ so that, because of Lemma (2), there are maximal ideals $\mathfrak{N}_n$ in $R[X]$ such that:

(a) $t_n \in \mathfrak{N}_n$;

(b) $t_i \notin \mathfrak{N}_n$ for $i < n$.

Note in particular that the ideals $\mathfrak{N}_n$ are distinct.

We apply Lemma (1) to $\mathfrak{N}_n$. Thus, there is in $K(X)$ a discrete rank one valuation ring V_n with finite residue class field such that:

(a) $V_n \subset R[X]$;

(b) t_n is a non-unit in V_n;

(c) t_i is a unit in V_n for $i < n$,

Denote by $\mathfrak{M}_n$ the ideal of non-units of V_n, by S the intersection of all V_n, and set $\mathfrak{Q}_n = S \cap \mathfrak{M}_n$. We shall show that S is a Dedekind domain, whose maximal ideals are exactly the ideals $\mathfrak{Q}_1, \mathfrak{Q}_2, \dots$.

For this purpose it is sufficient to prove the following (see [2]):

1. if $m \neq n$, then $\mathfrak{Q}_m + \mathfrak{Q}_n = S$;

2. if y is a non-zero element of $R[X]$, then y is a unit in V_n for all but a finite number of n.

The first assertion is trivial. For $\mathfrak{N}_n \subset \mathfrak{O}_n$ and $\mathfrak{N}_m$ and $\mathfrak{N}_n$ are different maximal ideals in $R[X]$. Hence, we have $1 \in \mathfrak{N}_m + \mathfrak{N}_n$ and certainly therefore $1 \in \mathfrak{Q}_m + \mathfrak{Q}_n$.

To prove the second assertion we use Lemma (3):

$y^h = ut_1^{h_1} \dots t_n^{h_n}$ $h \geqslant 1$, $h_i \geqslant 0$, $u \in U(R)$. Clearly y^h and hence y is a unit in V_r for $r > n$.

Thus S is a Dedekind domain whose maximal ideals are the $\mathfrak{Q}_n$, and furthermore $S/\mathfrak{Q}_n = V_n/\mathfrak{M}_n$. S therefore has property F1. Clearly $R[X] \subset S$, so that certainly the quotient field of S is $K[X]$. There remains only the question of $U(S)$.

If w is a non-zero element of $K(X)$, Lemma (3) shows that $w^h = ut_1^{h_1} \dots t_n^{h_n}$ where $h \geqslant 1$, u is a unit in R and the h_i are integers (possibly negative). If w is itself not a unit in R, then some h_i must be non-zero; we suppose $h_n \neq 0$. But then $ut_1^{h_1} \dots t_{n-1}^{h_{n-1}}$ is a unit in V_n while $t_n^{h_n}$ is not a unit in V_n. Hence w is not a unit in V_n so that certainly w is not a unit in S. Hence we find $U(S) = U(R)$, and the proof of the theorem is complete.

In order to deduce two curious corollaries from the theorem we first need a simple lemma.

LEMMA (4). *Let R be a Dedekind domain having property* F1, *and let K_1 be a subfield of K. Then $R_1 = R \cap K_1$ is again a Dedekind domain having property* F1.

Proof. Let a be a non-zero element of R_1. We note first that $aR_1 = K_1 \cap (aR)$. Namely,

aR_1 is certainly contained in $K_1 \cap (aR)$. On the other hand, if $b \in K_1 \cap (aR)$, then b/a is in R and is also in K_1, i.e., $b/a \in R_1$. It follows from this that R_1/aR_1 is a subring of R/aR. Because R has property F1, the ring R/aR is finite, so that also R_1/aR_1 is finite. As a result, if $\mathfrak{A}$ is any non-zero ideal of R_1, the $R_1/\mathfrak{A}$ is finite from which it follows immediately that R is noetherian and that every non-zero prime ideal of R is a maximal ideal. Since R_1 is obviously integrally closed we conclude that R_1 is a Dedekind domain. That R_1 has property F1 has already been proved above.

COROLLARY (1). *There exists a sequence* $S_1 \supset S_2 \supset \ldots \supset S_n \supset \ldots$ *of distinct Dedekind domains all having* $Q(X)$ *as quotient field, all of which contain* $Z[X]$, *all have property* F1 *and all have the same unit group which consists of* ± 1.

Proof. Applying the theorem to $R = Z$ gives a Dedekind domain $S \supset Z[X]$ having $Q(X)$ as quotient field, having property F1 and having $\{\pm 1\}$ as unit group. Let h be an integer with $h \geqslant 2$, set $K_n = Q(X^{h^n})$, $n \geqslant 0$. Also, set $T_n' = S \cap K_n$. By Lemma (4), T_n' is again a Dedekind domain with property F1; clearly $x^{h^n} \in T_n'$, so that the quotient field of T_n' is K_n. Let T_n be the integral closure of T_n' in $Q(X)$. Then T_n is again a Dedekind domain which is a finitely generated T_n' module. Each residue class field of T_n is an extension of finite degree of some residue class field of T_n', so that T_n also has property F1. We have $S = T_0 \supset T_1 \supset \ldots \supset T_n \supset \ldots$, and we shall show that not all the T_n coincide with S.

Let p be a rational prime number, so that p is not a unit in S. Suppose $T_n = S$ for some n. Set $pT_n' = \mathfrak{Q}_i^{b_1} \ldots \mathfrak{Q}_m^{b_m}$. Then $S/\mathfrak{Q}_i S$ is a vector space over $T_n'/\mathfrak{Q}_i$ of dimension $[Q(X):K_n] = h^n$. Now, $pS = (\mathfrak{Q}_1 S)^{b_1} \ldots (\mathfrak{Q}_m S)^{b_m}$, so that the number of elements in $S/\mathfrak{Q}_i S$ is not more than the number of elements in S/pS. But, the number of elements in $S/\mathfrak{Q}_i S$ is the h^n power of the number of elements in $T_n'/\mathfrak{Q}_i$. Thus, if $T_n = S$, then n is bounded, and therefore $T_n \neq S$ for some n.

Set $S_1 = S$ and $S_2 = T_n$ for some n such that $T_n \neq S$. We now repeat the whole of the above process, starting with S_2 instead of S, leading to a ring $S_3 \subset S_2$, $S_3 \neq S_2$. This procedure may be continued indefinitely, which completes the proof of the corollary.

COROLLARY (2). *There exists a Dedekind domain having properties* F1 *and* F2 *whose ideal class group is not a torsion group.*

Proof. We refer to the preceding corollary. Since S_2 is a proper subring of S_1, yet with $U(S_2) = U(S_1)$, it follows from Corollary (1) of proposition (1) that the ideal class group of S_2 cannot be a torsion group.

REFERENCES

1. O. GOLDMAN: Hilbert rings and the Hilbert Nullstelensatz, *Math. Z.* **54** (1951), 136–140.
2. K. MATUSITA: Über ein bewertungstheoretisches Axiomsystem für die Dedekind-Noetherschе Idealtheorie, *Jap. J. Math.* **19** (1944), 97–110.

University of Pennsylvania,
Philadelphia, Pa., U.S.A.