PACIFIC JOURNAL OF MATHEMATICS
Vol. 15, No. 3, 1965

DEDEKIND DOMAINS: OVERRINGS AND SEMI-PRIME ELEMENTS

LUTHER CLABORN

This paper develops two themes: (1) the relation of the class group of a Dedekind domain A to that of an overring B and (2) the question of finding a nonzero, nonunit element x of a Dedekind domain A such that A/xA is regular. We obtain complete results in answer to the first question, giving a corollary concerning the realization of certain groups as class groups. We give various sufficient conditions in answer to the second question; some in terms of the class group, others concerning Dedekind domains which often arise in practice.

In § 1 of the present paper, we study the class group of an overring B of a Dedekind domain A and determine its class group in terms of that of A. We generalize and also strengthen the results of § 1 of an earlier article [1]. Combining several results, we obtain an interesting fact: if G is the class group of a Dedekind domain and G' is a homorphic image of G, then G' is the class group of a suitable Dedekind domain.

Section 2 introduces the question of finding a nonunit x in a Dedekind domain A for which A/xA is a direct sum of fields. Although we obtain no definitive result, various sufficient conditions are given. These require in part the developments of § 1. We also give examples Dedekind domains with "pathological" class groups.

1. We state two well known propositions which we will need by way of background.

PROPOSITION 1.1. *Let A be a Dedekind Domain with quotient field F. Let B be a ring such that $A \subseteq B \subset F$. Then $B = \cap A_p$ over those prime ideals P of A for which $B \subseteq A_p$.*

PROPOSITION 1.2. *Let A be a Dedekind domain with quotient field F. Let B be a ring such that $A \subseteq B \subset F$. Then B is a Dedekind domain.*

PROPOSITION 1.3. *Let A be a Dedekind domain with quotient field F and let B be a ring such that $A \subseteq B \subset F$. The assignment $I \rightarrow IB$ is a homomorphism of the set of fractionary ideals of A onto the set of fractionary ideals of B.*

Received August 27, 1964.

Proof. Let Q be a prime ideal of B and set $P = Q \cap A$. Then $PB = Q$. The inclusion $PB \subseteq Q$ is trivial, while $B_Q = A_p$ implies that $PB_Q = (PB)B_Q = QB_Q$. This yields $PB = Q$ if we know that PB is not contained in another prime ideal Q' of B. But then Q' would also lie over P, which is not the case by Prop. 1.1.

If I is a fractionary ideal of A, then there is a $d \neq 0$ in A such that $dI \subseteq A$. But then clearly $d(IB) \subseteq B$, so IB is a fractionary ideal of B. The mapping is clearly a homomorphism for multiplication. To see that the mapping is onto, let Q be a prime ideal of B. We have seen above that if $P = Q \cap A$, then $PB = Q$. Thus the mapping is onto the prime ideals of B, and these generate the group of fractionary ideals of B.

COROLLARY 1.4. *Let A be a Dedekind domain with quotient field F and let B be a ring such that $A \subseteq B \subset F$. The assignment $I \to IB$ of fractionary ideals of A onto fractionary ideals of B induces a homomorphism $\psi : \bar{I} \to \overline{IB}$ of the class group of A onto that of B.*

Proof. It is sufficient to note that if $I = xA$, then $IB = xB$.

PROPOSITION 1.5. The kernel of ψ is generated by all $\bar{P}_\alpha$, where P_α ranges over all prime ideals such that $P_\alpha B = B$.

Proof. Suppose $P_\alpha B = B$, and let I be a fractionary ideal such that $\bar{I} = \bar{P}_\alpha$, i.e. $I = xP_\alpha$ for $x \in F$. Then $IB = xP_\alpha B = xB$, so $\overline{IB}$ is the identity.

Suppose now that I is a fractionary ideal of A such that $IB = yB$ for $y \in F$. Then $yI^{-1}B = B$, showing that yI^{-1} is a product of primes P_α of A for which $P_\alpha B = B$, and this establishes the assertion.

COROLLARY 1.6. *Let A be a Dedekind domain and $W = \{P_\alpha\}$ be a collection of primes such that $\{\bar{P}_\alpha\}$ does not generate the full class group of A. Then there are an infinite number of prime ideals of A not in the set $\{P_\alpha\}$.*

Proof. Let $B = \bigcap_{P \notin W} A_p$. By Proposition 1.5, B is not a principal ideal domain. Therefore there are an infinite number of prime ideals of B, hence an infinite number of prime ideals of A which are not in W.

COROLLARY 1.7. *Let A be a Dedekind domain with class group*

G. Let H be any subgroup of G. Then there is a Dedekind domain whose class group is G/H.

Proof. In [1], we constructed the Dedekind domain $A' = A[X]_S$, where S denotes the set of all monic polynomials of $A[X]$. We showed that A has the same class group as A [1, Prop. 2.3] and also that A has a prime ideal in every class of the class group [1, Cor. 2–5]. Identify G and H at the class group and a subgroup of the class group of A'. For each class of H, choose a prime P' of A' in the given class. Let W denote the set $\{P'\}$ so chosen. Then $B = \bigcap_{Q \in W} A_Q$ has class group G/H by Proposition 1.5.

2. DEFINITION 2.1. Let A be a Dedekind domain. An element x of A which is not zero and not a unit will be said to be semi-prime if A/xA is a regular ring.

REMARK 2.2. This condition is equivalent to (1) A/xA is a direct sum of fields, or (2) xA is not contained in the square of any prime ideal of A.

In what follows, sufficient conditions will be given for A to contain semi-prime elements. If A has only a finite number of prime ideals, then A is a principal domain and obviously A contains semi-prime elements. This case (A has only a finite number of prime ideals) will be excluded from the developments which follow.

PROPOSITION 2.3. If A has a finite class group, then there are semi-prime elements in A.

Proof. Since we are assuming that A has infinitely many prime ideals, there must be at least one class of the class group containing an infinite set $\{P_i\}$ of the prime ideals. If n is the class number of A, then $P_1 \cdots P_n$ must be principal, say $xA = P_1 \cdots P_n$. x is then a semi-prime element.

PROPOSITION 2.4. Let A be a Dedekind domain, and suppose that every class of the class group (except possibly the principal class) contains a prime ideal. Then A contains a semi-prime element.

Proof. If A is a principal ideal domain, then there is nothing to prove. Otherwise let P be a nonprincipal prime ideal and let Q be a prime in the class of P^{-1}. Then PQ is principal, say $PQ = xA$, and x will be semi-prime unless $P = Q$. We are therefore done unless every class has exponent 2 and there is only one prime in each class.

Choose P to represent one nonprincipal class and Q to represent a different nonprincipal class. Choose a prime ideal R in the class of PQ. Obviously $R \neq P$, $R \neq Q$, while PQR is principal. This gives a semi-prime element in A.

We can actually prove a little more.

PROPOSITION 2.5. Let A be a Dedekind domain, and suppose that for every prime ideal P there is a prime of A in the class of P^{-1}. Then A contains a semi-prime element.

Proof. As in the proof Proposition 2.4 we may assume that every class has exponent 2. The class group of A may therefore be regarded as a vector space over the field with 2 elements. Since the prime ideals of A generate the class group, we may choose a basis $\{\bar{P}_\alpha\}$ for the class group consisting of classes of prime ideals. Let P be any prime ideal of A and let $\bar{P}$ be its class. Let $\bar{P} = \bar{P}_{\alpha_1} \cdots \bar{P}_{\alpha_k}$ be its representation in terms of the given basis. Thus $PP_{\alpha_1} \cdots P_{\alpha_k}$ is principal and we get a semi-prime element unless P is in the set $\{P_\alpha\}$. We may assume then that the set $\{P_\alpha\}$ contains all prime ideals of A. But this contradicts Corollary 1.6, and the proposition is established.

Before giving an example violating the hypothesis of Proposition 2.5, we present a lemma which will be useful in constructing such an example and in a later proof.

LEMMA 2.6. *Let F be a field of characteristic p such that $[F^{1/p} : F] = p$. Let K be a separable extension of F; then $[K^{1/p} : K] = p$.*

Proof. Since K is a separable extension of F, we have $K = F(K^p)$ [3, Thm. 8, p. 69]. Thus $K^{1/p} = F^{1/p}(K)$. But $F^{1/p}$ and K are linearly disjoint [3, Thm. 35, p. 111], so we get $[K^{1/p} : K] = [F^{1/p}(K) : K] = [F^{1/p} : F] = p$.

EXAMPLE 2.7. Let $F' = Z/3Z(a)$ where Z denotes the integers and a is indeterminant. Let F be the separable closure of F' in its algebraic closure. By Lemma 2.6, $[F^{1/3} : F] = 3$. Consider the integral closure A of $F[X]$ in the field $F(X, Y)$, where $Y^3 = aX^3 + X$. It is not difficult to show by a direct computation that $A = F[X, Y]$, but it is easier to notice that since the matrix of partial derivatives of the equation $Y^3 - aX^3 - X$ has always rank 1, $F[X, Y]$ is regular [2, Thm. 1. p. 201]. Over each prime ideal of $F[X]$ there lies only one prime ideal of A and for the relative degree f of the residue field and the ramification index e we have $e = 3$, $f = 1$ or $e = 1$, $f = 3$ [3, Thm. 22, p. 289]. We show first that for all nonlinear prime elements of $F[X]$, we get $e = 1$, $f = 3$, so these remain principal. Let Q be a prime ideal of $F[X]$ generated by a nonlinear element; $Q = X^q - t$, where q is a power of 3 and $t \in F$. The residue field $F[X]/(X^q - t)$ is $F[t^{1/q}]$, while the residue field relative to A will be $F[t^{1/q}, w]$, where $w^3 = at^{3/q} + t^{1/q}$. Since $[F^{1/3} : F] = 3$, we have $F^{1/3} \subseteq F[t^{1/q}]$, hence $a^{1/3} \in F[t^{1/q}]$. Thus $at^{3/q}$ is a cube in $F[t^{1/q}]$. But $t^{1/q}$ is not a cube in $F[t^{1/q}]$, so $[F[t^{1/q}, w] : F[t^{1/q}]] = 3$. That is, $f = 3$, $e = 1$; thus we see that nonlinear prime elements of $F[X]$ remain prime in A.

For the linear primes $X - t$, $t \varepsilon F$, we get $e = 1$, $f = 3$ if $at^3 + t$ is not a cube in F, while $e = 3$, $f = 1$ if $\mathrm{a}t^3 + t$ is a cube in F. Certainly we have the latter case at least for $t = 0$. Let P be a prime ideal of A lying over a linear prime ideal of $F[X]$ for which $e = 3$, $f = 1$. Then P is not principal. For if P were principal, say $P = (c_0(X) + c_1(X)Y + c_2(X)Y^2)$ we would get

$$P^3 = (c_0^3(X) + c_1^3(X)(aX^3 + X) + c_2^3(X)(a^2X^6 + 2aX^4 + X^2)\ .$$

But $P^3 = (x - t)$ for some $t \in F$. Comparing degrees and using the fact that $1, a, a^2$ are independent over F^3, we get a contradiction. Again let P be such a prime and suppose that the class of P^2 (which is the clsss of P^{-1}) contains a prime Q. Q is certainly not principal; therefore Q lies over a linear prime ideal of $F[X]$ and $e = 3$, $f = 1$ for Q. We also get that P^2Q^2 is principal, say

$$P^2Q^2 = (d_0(X) + d_1(X)Y + d_2(X)Y^2)\ .$$

Cubing, we get

$$(P^3)^2(Q^3)^2 = (d_0^3(X) + d_1^3(X)(aX^3 + X) + d_2^3(X)(a^2X^6 + 2aX^4 + X^2)).$$

On the left side of this equation we have a polynomial of degree 4, while on the right we have a polynomial whose degree is divisible by 3, a contradiction.

PROPOSITION 2.8. Let A be a principal ideal domain and let K be a finite separable extension of the quotient field F of A. Let B be the integral closure of A in K and let C be a ring such that $B \subseteq C \subset K$. Then C contains a semi-prime element.[1]

Proof. There are only a finite number of prime ideals $Q_1, \cdots, Q_k$ of B whose reduced ramification index is greater than 1 [3, Thm. 28, p. 302]. Let $P = \pi A$ be a prime ideal of A not lying under any $Q_1, \cdots, Q_k$. Then πB is a product of distinct primes and is a semi-

[1] The referee has kindly pointed out that this Proposition (and thus the following) hold when B is not necessarily integrally closed.

prime element in B. π will also be a semi-prime element in C unless all prime ideals of B dividing π generate C. The result now follows by Proposition 1.5 and Corollary 1.6.

PROPOSITION 2.9. Let A be the coordinate ring of an algebraic curve over a perfect ground field F. If A is a Dedekind domain, then A contains a semi-prime element.

Proof. $A = F[x_1, \cdots, x_n]$. Choose X in A such that A is integral over $F[X]$; this is possible by [2, Thm. 1, p. 22]. Since A is integrally closed in $K = F(x_1, \cdots, x_n)$, A is the integral closure of $F[X]$ in K. Let K' be the separable closure of $F(X)$ in K, and let A' be the integral closure of $F[X]$ in K. The conclusion holds for A' by Proposition 2.8.

Since $[F(X)^{1/p} : F(X)] = p$, we have $[K'^{1/p} : K'] = p$ by Lemma 2.6. K is a purely inseparable extension of K', so we may break the extension from K' to K into a chain of extensions each of which is pure inseparable of exponent p. This chain can only be

$$K' = K_0 \subset K_0^{1/p} \subset K_0^{1/p^2} \subset \cdots \subset K_0^{1/pm} = K .$$

But then we have an isomorphism of K onto K' given by $x \longrightarrow x^{pm}$ which induces an isomorphim of A onto A'. Since A' contained semi-prime elements, so does A.

REFERENCES

1. L. Claborn, *Dedekind domains and rings of quotients*, Pacific J. Math. **15** (1965), 59-64.
2. S. Lang, *Introduction to Algebraic Geometry*, New York, Interscience Publishers, Inc. (1958).
3. O. Zariski and P. Samuel, *Commutative Algebra*, Vol. I, Princeton, D. Van Nostrand Company (1958).

CORNELL COLLEGE