ON THE DISTRIBUTION OF PRIME IDEALS WITHIN THE IDEAL CLASS GROUP

Robert Gilmer, William Heinzer, and William W. Smith

Abstract. For a countably generated group K and a function Δ on K taking values that are either nonnegative integers or ∞, we determine in Theorem 8 equivalent conditions for there to exist a Dedekind domain D with class group K such that, for each k in K, exactly $\Delta(k)$ maximal ideals of D belong to k.

1. Introduction.

Suppose D is a Dedekind domain with class group K. Work on this paper was motivated by the following question (Q) of Scott Chapman in a communication that, in turn, was motivated by work of Chapman and Franz Halter-Koch on factorization in Dedekind domains.

(Q) *Is it possible for a nonidentity element k of K to contain exactly one maximal ideal of D?*

We show in Example 6 that (Q) has an affirmative answer. In fact, if K is the infinite cyclic group, it is possible for each element of K to contain a unique maximal ideal of D. Our investigation of the distribution of maximal ideals within the elements of K extends beyond (Q). There are two basic questions related to the distribution problem:

(1) If K is an abelian group and S is a subset of K, under what conditions on S does there exist a Dedekind domain D with class group K such that S is the set of elements of K that contain maximal ideals of D?
(2) Given a subset S as in (1), to what extent can the distribution of maximal ideals of D within elements of S be specified?

We will formulate the two questions in terms of a function Δ on K, where $\Delta(k)$ represents the number of maximal ideals of the Dedekind domain in the class k. (We note that $\Delta(k)$ may be zero, finite positive, or infinite, and the set S of Questions (1) and (2) consists of all elements k of K such that $\Delta(k) \neq 0$.) The main result of this paper (Theorem 8) gives a definitive answer to both (1) and (2) in the case where K is countably generated. (We restrict ourselves to this case throughout.)

Question (1) was originally investigated by Grams [Gr]. Since every nonzero ideal of a Dedekind domain can be expressed as a product of maximal ideals, the condition that S generates K as a group is obviously necessary. In [Gr, Th. 1.4], Grams formulates a second condition on S that, together with the generating property, yields necessary and sufficient conditions for S to satisfy the condition in (1); this second condition is obtained via the approximation theorem for Dedekind domains [B, p. 497]. In later works, Skula [S] and Michel and Steffan [MS] give similar necessary and sufficient conditions on S. The article of Michel and Steffan [MS] also contains results regarding (2). However, we believe the approach to this question taken here is more direct. Theorem 8 shows that if S generates K as a monoid and if $S = B \cup C$ is a partition of S with the property that $B^* \cup C$

generates K as a monoid for each cofinite subset B^* of B, then there exists a Dedekind domain D with class group K such that S is precisely the set of classes of K that contain maximal ideals, C is the set of classes each of which contains infinitely many maximal ideals, and B is the set of classes each of which contains a finite number of maximal ideals. Moreover, the (finite positive) number of maximal ideals in the elements of B can be specified arbitrarily.

Throughout the paper we use $\mathbb{Z}$ to denote the integers, $\mathbb{Z}_0$ the set of nonnegative integers, and $\mathbb{Z}^+$ the set of positive integers.

2. Results.

Let $G = \mathbb{Z}^\infty$ be the free abelian group on a countably infinite set. We consider elements of G alternately as sequences $\{n_i\}_{i=1}^\infty$ over $\mathbb{Z}$ that are finitely nonzero or as functions $f : \mathbb{Z}^+ \to \mathbb{Z}$ that are finitely nonzero. If x_i is the characteristic function of $\{i\}$, then $\{x_i\}_{i=1}^\infty$ is a basis for G. Let P be the subset of G consisting of all sequences $\{n_i\}_{i=1}^\infty$ such that $n_i \geq 0$ for all i. Following Grams (see also [C2, p. 249]), we say that a subset S of P is *dense* in G if for any $t \in \mathbb{Z}^+$ and any $n_1, \ldots, n_t \in \mathbb{Z}_0$, S contains an element of the form $\sum_{i=1}^{t} n_i x_i + \sum_{j=1}^{v} n_{t+j} x_{t+j}$ for some $v \in \mathbb{Z}_0$ and some non-negative integers $n_{t+1}, \ldots, n_{t+v}$.

If K is a group, if $\beta = \{n_i\} \in G$, and if $\alpha = \{a_i\}_{i=1}^\infty$ is any sequence over K, define $\beta \cdot \alpha$ to be the element $\sum_{i=1}^{\infty} n_i a_i$ of K; the summation is finite since β is finitely nonzero. It is easy to verify that $(\beta_1 \pm \beta_2) \cdot \alpha = \beta_1 \cdot \alpha \pm \beta_2 \cdot \alpha$ and $\theta \cdot \alpha = 0$ for all $\beta_1, \beta_2 \in G$ and each sequence α over K (θ denotes the zero element of G).

Proposition 1. *Let $\alpha = \{a_i\}_{i=1}^\infty$ be a sequence over the group K. The mapping $\phi_\alpha : G \to K$ defined by $\phi_\alpha(\beta) = \beta \cdot \alpha$ is a homomorphism* *from G into K with kernel $G_\alpha = \{\beta \in G : \beta \cdot \alpha = 0\}$. The image of ϕ_α is the subgroup of K generated by $\{a_1, a_2, \dots\}$. Each homomorphism of G into K is of the form ϕ_γ for some sequence γ over K.*

Proof. The statement concerning ϕ_α is clear. Since $\{x_i\}_{i=1}^\infty$ generates G, $\{\phi_\alpha(x_i)\}_{i=1}^\infty$ generates $\operatorname{Im}\phi_\alpha$. But $\phi_\alpha(x_i) = a_i$, so $\{a_1, a_2, \dots\}$ generates Im ϕ_α. If $\phi : G \to K$ is any homomorphism from G into K, we show that $\phi = \phi_\gamma$, where $\gamma = \{\phi(x_i)\}_{i=1}^\infty$. This is practically the definition: if $g \in G$, then $g = \sum_1^\infty n_i x_i$ for some n_i, so $\phi(g) = \sum_1^\infty n_i \phi(x_i) = g \cdot \gamma$. □

With notation as in Proposition 1, we are interested in determining conditions under which $G_\alpha \cap P$ is dense in G. For reasons that will become apparent later, we restrict our attention to sequences $\{a_i\}$ over K such that $\{a_1, a_2, \dots\}$ generates K *as a monoid*; if K is a torsion group this is, of course, equivalent to the condition that $\{a_1, a_2, \dots\}$ generates K as a group.

Theorem 2. *Assume that $\alpha = \{a_i\}_{i=1}^\infty$ is a sequence over the group K such that α generates K as a monoid. With notation as in the statement of Proposition 1, $G_\alpha \cap P$ is dense in G if and only if $\{a_t, a_{t+1}, \dots\}$ generates K as a monoid for each $t \in \mathbb{Z}^+$.*

Proof. Assume first that $G_\alpha \cap P$ is dense in P, and choose $t \in \mathbb{Z}^+$. If $x \in K$, then $-x$ is a nonnegative linear combination of the elements a_i, say $-x = \sum_{i=1}^{s} n_i a_i$, where we may assume that $s \geq t$. Since $G_\alpha \cap P$ is dense in G, there exists an element $g = \{n_1, \dots, n_u, 0, 0, \dots\}$ in $G_\alpha \cap P$, where $n_i \geq 0$ for each i and $u \geq s$. Thus $0 = \sum_1^u n_i a_i = -x + \sum_{i=s+1}^{u} n_i a_i$, and hence $x = \sum_{i=s+1}^{u} n_i a_i$ belongs to the monoid generated by $\{a_s, a_{s+1}, \ldots\}$, which is contained in the monoid generated by $\{a_t, a_{t+1}, \ldots\}$.

Conversely, if $\{a_t, a_{t+1}, \ldots\}$ generates K as a monoid for each $t \in \mathbb{Z}^+$, consider any finite sequence $n_1, \ldots, n_r$ of nonnegative integers. The element $s = -\sum_{i=1}^{r} n_i a_i$ of K belongs to the monoid generated by $\{a_{r+1}, a_{r+2}, \ldots\}$, so $s = \sum_{i=1}^{v} n_{r+i} a_{r+i}$ for some v and some integers $n_{r+i} \geq 0$. Then $\{n_1, \ldots, n_{r+v}, 0, 0, \ldots\} \in G_\alpha \cap P$ and the first r coordinates of this sequence are $n_1, \ldots, n_r$. Therefore $G_\alpha \cap P$ is dense in G. □

Henceforth we call a sequence $\{a_i\}_{i=1}^{\infty}$ over a group K *acceptable* if it satisfies the condition of Theorem 2 — that is, if $\{a_t, a_{t+1}, \ldots\}$ generates K as a monoid for each $t \in \mathbb{Z}^+$.

Proposition 3. (**Grams**, [Gr, Lemma 1.3]) *If H is a subgroup of G such that $H \cap P$ is dense in G, then $H \cap P$ generates H as a group.*

If D is a Dedekind domain, we denote by $\mathcal{C}(D)$ the class group of D and by $\overline{F}$ the element of $\mathcal{C}(D)$ determined by the nonzero fractional ideal F of D.

Theorem 4. *Let $\alpha = \{a_i\}_{i=1}^{\infty}$ be a sequence over a group K such that α generates K as a monoid and $G_\alpha \cap P$ is dense in G. Then there exists a Dedekind domain D with family $\{M_i\}_{i=1}^{\infty}$ of maximal ideals such that $\mathcal{C}(D)$ is isomorphic to K under a mapping that sends $\overline{M_i}$ to $a_i \in K$ for each $i \in \mathbb{Z}^+$.*

Proof. Since $G_\alpha \cap P$ is dense in G, it follows from Proposition 3 that $G_\alpha \cap P$ generates G_α as a group, and Claborn's Theorem 2.1 [C2] shows that there exists a Dedekind domain D whose class group

$\mathcal{C}(D)$ is isomorphic to G/G_α under an isomorphism that maps $\overline{M}_i$ to $x_i + G_\alpha$ for each i. On the other hand, since α generates K as a group, the mapping $\beta \to \beta \cdot \alpha$ is a surjection of G onto K, and Proposition 1 shows that G/G_α is isomorphic to K under an isomorphism mapping $x_i + G_\alpha$ to $x_i \cdot \alpha = a_i \in K$. The composite of these two isomorphisms yields an isomorphism of $\mathcal{C}(D)$ onto K that maps $\overline{M}_i$ to a_i for each i. □

Theorem 5. *Let K be a countably generated group and let S be a nonempty subset of K. In order that there exists a Dedekind domain D with class group K such that $S = \{\overline{M} : M \in \mathrm{Spec}(D)\}$, it is necessary and sufficient that S generates K as a monoid.*

Proof. Assume first that $\mathcal{C}(D) = K$ and $S = \{\overline{M} : M \in \mathrm{Spec}(D)\}$. Let T be the submonoid of K generated by S and let $g \in K$. Since S generates K as a group, $g = a - b$ for some $a, b \in T$. We write $b = \overline{I}$, where I is an integral ideal with prime factorization $I = P_1^{e_1} \cdots P_k^{e_k}$, $P_i \in \mathrm{Spec}(D)$. If $d \in I - \{0\}$, then $(d) = IJ$ for some ideal J of D, and hence, in additive notation, $-b = -\overline{I} = \overline{J} \in T$. Therefore $g = a + (-b) \in T$ and $K = T$, as we wished to show.

For the converse we first note that K, and hence S, is countable. Let $\alpha = \{a_i\}_{i=1}^{\infty}$ be a sequence in K such that each a_i is in S and each element of S occurs an infinite number of times in α; such a sequence α exists since a countable union of countable sets is countable. By Theorem 2, $G_\alpha \cap P$ is dense in G, and hence by Theorem 4 there exists a Dedekind domain D with family $\{M_i\}_{i=1}^{\infty}$ of maximal ideals such that $\mathcal{C}(D)$ is isomorphic to K under an isomorphism that maps $\overline{M}_i$ to a_i for each i. Since the distinct elements of α are precisely the elements of S, it follows that S is the set of classes of K determined by maximal ideals of D. □

In the case of a torsion group K, the condition on S in Theorem 5 is the same as the condition of Grams in [Gr, Cor. 1.5]. But for a non-torsion group K, the condition of Theorem 5 is easier to apply than the two conditions on S of [Gr, Th.1.4]. Nevertheless, the main value of Theorem 5 to us is its application, in combination with Theorem 4, to the question of possible distribution of maximal ideals within the ideal classes of a Dedekind domain. For example, we can immediately provide an answer to question (Q).

Example 6. If α is the sequence $\{0, 1, -1, 2, -2, \ldots\}$ over $\mathbb{Z}$, then α is acceptable, and Theorem 4 shows that there exists a Dedekind domain D with class group $\mathbb{Z}$ such that each element of $\mathcal{C}(D)$ is represented by exactly one maximal ideal of D. Thus Chapman's question (Q) has an affirmative answer. If M_i is the unique maximal ideal of D in the class of i for each i in $\mathbb{Z}$, then from the known theory concerning the class groups of overrings of a Dedekind domain (see [C1], [G1, Th. 40.4]), $E = \cap_{i \neq 0} D_{M_i}$ is the unique proper overring of D with class group $\mathbb{Z}$. Each proper overring of D distinct from E has finite cyclic class group, and each finite cyclic group can be realized in this way. □

Proposition. (**Michel-Steffan**, [MS, Ex., p. 86]) *Let K be a countably infinite abelian group. There exists a Dedekind domain D with class group K such that each element of K is the class of a unique maximal ideal of D.*

Proof. List the elements of K in a sequence $\alpha = \{a_i\}_{i=1}^{\infty}$ without repetition. In view of Theorems 2 and 4, it suffices to show that α is acceptable. Let n be a positive integer, let $\beta = \{a_{n+i}\}_{i=1}^{\infty}$, and let x be an element of K. As y ranges over the terms of β, we obtain infinitely many elements of K of the form $x - y$. Choose y so that

$z = x - y$ is a term of β. Then $x = y + z$, and hence x is in the monoid generated by β. Therefore α is acceptable. $\square$

Combining Theorems 2 and 4, we see that examples illustrating various distributions of maximal ideals within elements of the class group can easily be constructed simply by constructing acceptable sequences for the group in question. This is particularly easy for torsion groups (as noted earlier) and for the case $K = \mathbb{Z}$. Conditions for a sequence to generate $\mathbb{Z}$ as a monoid are well-known [H], [G2, Th. 2.4 and 2.6]: $\{b_i\}_{i=1}^{\infty}$ generates $\mathbb{Z}$ as a monoid if and only if $\gcd\{b_i\} = 1$ and $\{b_i\}$ contains both positive and negative integers.

Example 7. We indicate the wide range of variations where the class group is $\mathbb{Z}$ with the following four examples:

A) Let $\alpha = \{1, -1, 1, -1, \cdots\}$. For a Dedekind domain D associated with α via Theorem 4, each of the classes 1 and -1 contains infinitely many maximal ideals and no other class contains a maximal ideal. That is to say, for this example $\Delta(-1) = \Delta(1) = \infty$ and $\Delta(k) = 0$ for $k \neq \pm 1$. Each proper overring of D is a PID (cf. [C2, Ex.3-2]).

B) Let $\alpha = \{2, 2, 2, 3, -4, 5, -4, 5, \cdots\}$. For a Dedekind domain D associated with this sequence, $\Delta(2) = 3, \Delta(3) = 1$, and $\Delta(-4) = \Delta(5) = \infty$. Again each proper overring of D has finite cyclic class group, but the only cyclic groups that arise in this case are those of orders 1, 2, 3, 4 and 5.

C) Let $\alpha = \{-1, 1, -1, 2, -1, 3, \cdots\}$. For this sequence we have $\Delta(-1) = \infty, \Delta(k) = 1$ for $k \geq 1$, and $\Delta(0) = \Delta(k) = 0$ for $k < -1$.

D) Let $\alpha = \{2, -3, 5, -7, 11, -13, \cdots\}$. By using the sequence of primes we have one maximal ideal in each of the classes represented by a term of α. If D is a Dedekind domain associated with α, then for each prime integer p there exists a unique overring E_p of D whose class group is cyclic of order p. Each proper overring of D distinct from each E_p is a PID.

Examples 6 and 7 illustrate the alternative formulation of the main result in terms of the function Δ which counts the number of maximal ideals in each class. The statement of Theorem 8 uses the following terminology. Let K be a countably generated group and let $\Delta : K \to \mathbb{Z}_0 \cup \{\infty\}$ be a function. We say that Δ is *realizable* if there exists a Dedekind domain D with class group K such that the class of k contains exactly $\Delta(k)$ maximal ideals for each k in K.

Theorem 8. *Let K be a countably generated group and let $\Delta : K \to \mathbb{Z}_0 \cup \{\infty\}$ be a function. Let $B = \Delta^{-1}(\mathbb{Z}^+)$ and let $C = \Delta^{-1}(\infty)$. Then Δ is realizable if and only if $C \cup B^*$ generates K as a monoid for each cofinite subset B^* of B. In other words, if $B = \{b_1, b_2, \ldots\}$, then Δ is realizable if and only if $C \cup \{b_n, b_{n+1}, \ldots\}$ generates K as a monoid for each $n \in \mathbb{Z}^+$.* [Note: Either B or C may be empty or finite nonempty.]

Proof. Suppose Δ is realizable and let D be a Dedekind domain by which Δ is realized in the sense above. By definition of Δ, $C \cup B$ is the set of classes of D that contain maximal ideals of D. Therefore $C \cup B$ generates K as a monoid. If $\{b_i\}_{i=1}^m$ is a finite subset of B and if $B^* = B - \{b_i\}_{i=1}^m$, we show that $C \cup B^*$ generates K as a monoid. Let $\{P_i\}_{i=1}^s$ be the (finite) set of maximal ideals of D that belong to some b_j, $1 \le j \le m$. It suffices to show that each $\overline{P}_i$ belongs to the monoid generated by $C \cup B^*$. If v_i is the normed valuation associated with P_i for $1 \le i \le s$ and if v_P is the normed valuation associated with P for $P \in \operatorname{Spec}(D) - \{P_i\}_{i=1}^s$, then the approximation theorem for Dedekind domains [B, p. 497] implies that there exists an element x in the quotient field of D such that $v_i(x) = -1$, $v_j(x) = 0$ for $j \neq i$, and $v_P(x) \ge 0$ for all P. It follows that $Dx = P_i^{-1} Q_1^{e_1} \ldots Q_w^{e_w}$ for some

$Q_1, \ldots, Q_w$ in $\mathrm{Spec}(D) - \{P_i\}_{i=1}^s$ and some $e_i \in \mathbb{Z}_0$. In the class group, using additive notation, this yields a relation $\overline{P}_i = \sum_{j=1}^{w} e_j \overline{Q}_j$, where $\overline{Q}_j \notin \{b_t\}_{t=1}^m$ for each j. Consequently, each $\overline{Q}_j$ is in $C \cup B^*$ and $\overline{P}_i$ belongs to the monoid generated by $C \cup B^*$, as we wished to show.

Conversely, if $C \cup B^*$ generates K as a monoid for each cofinite subset B^* of B, let $\alpha = \{a_i\}_{i=1}^\infty$ be a sequence in which each element y of $C \cup B$ appears exactly $\Delta(y)$ times. Such a sequence exists because a countable union of countable sets is countable. The hypothesis on $C \cup B$ implies that $\{a_t, a_{t+1}, \ldots\}$ generates K as a monoid for each $t \in \mathbb{Z}^+$. Therefore Theorems 2 and 4 show that there exists a Dedekind domain D with family $\{M_i\}_{i=1}^\infty$ of maximal ideals such that $\mathcal{C}(D)$ is isomorphic to K under a mapping that sends $\overline{M}_i$ to a_i for each i. By choice of α, it follows that D is a realization of Δ. $\square$

In view of Theorem 8, the problem of determining the possible distribution of maximal ideals within classes of a countably generated class group K is reduced to the problem of determining what sequences $\{a_i\}_1^\infty$ in K satisfy the conditions of Theorem 2. For a torsion group K, the conditions are equivalent (as previosuly stated) to the condition that $\{a_t, a_{t+1}, \ldots\}$ generates K as a group for each $t \in \mathbb{Z}^+$. For a non-torsion group K, however, the problem of determining "useful" conditions for a given sequence $\{b_i\}_{i=1}^\infty$ to generate K as a monoid may be nontrivial. For example, if $K = \mathbb{Z}^n = \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$ (n summands), one way of viewing the monoid-generation problem amounts to asking for conditions under which certain systems of linear Diophantine equations in n variables are solvable in nonnegative integers. Because K is finitely generated as a monoid (for example, by $\{\pm e_1, \ldots, \pm e_n\}$, where $\{e_1, \ldots, e_n\}$ is the canonical basis for K as a group), the number of systems to be considered can be limited to at most $2n$.

References

[B] N. Bourbaki, *Commutative algebra*, Addison-Wesley, Reading, Mass., 1972.

[C1] L. Claborn, *Dedekind domains: overrings and semi-prime elements*, Pacific J. Math. **15** (1965), 799–804.

[C2] ____, *Specified relations in the ideal class group*, Michigan Math. J. **15** (1968), 249–255.

[G1] R. Gilmer, *Multiplicative ideal theory*, Queen's Papers Pure Appl. Math. Vol. 90, Kingston, Ont., 1992.

[G2] ____, *Commutative semigroup rings*, Univ. Chicago Press, Chicago, 1984.

[Gr] A.P. Grams, *The distribution of prime ideals of a Dedekind domain*, Bull. Austral. Math. Soc. **11** (1974), 429–441.

[H] J.C. Higgins, *Representing N-semigroups*, Bull. Austral. Math. Soc. **1** (1969), 115–125.

[MS] D. Michel and J. Steffan, *Repartition des ideaux premiers parmi les classes d'ideaux dans un anneau de Dedekind et equidecomposition*, J. Algebra **98** (1986), 82–94.

[S] L. Skula, *On c-semigroups*, Acta Arith. **31** (1976), 247–257.

Department of Mathematics 3027, Florida State University, Tallahassee, Florida, 32306-3027
email: gilmer@math.fsu.edu

Department of Mathematics, Purdue University, West Lafayette, Indiana 47907-1395
email: heinzer@math.purdue.edu

Department of Mathematics, University of North Car-

olina, Chapel Hill, North Carolina 27599-3250
email: wwsmith@math.unc.edu