Math. Proc. Camb. Phil. Soc. (1983), **94**, 23
Printed in Great Britain

An arithmetic characterization of algebraic number fields with a given class group

By DAVID E. RUSH
University of California, Riverside

(*Received* 22 *December* 1982)

Let R be the ring of integers of a number field K with class group G. It is classical that R is a unique factorization domain if and only if G is the trivial group; and the finite abelian group G is generally considered as a measure of the failure of unique factorization in R. The first arithmetic description of rings of integers with non-trivial class groups was given in 1960 by L. Carlitz (1). He proved that G is a group of order $\leqslant$ two if and only if any two factorizations of an element of R into irreducible elements have the same number of factors. In ((6), p. 469, problem 32) W. Narkiewicz asked for an arithmetic characterization of algebraic number fields K with class numbers $\neq 1, 2$. This problem was solved for certain class groups with orders $\leqslant 9$ in (2), and for the case that G is cyclic or a product C_p^k of k copies of a group of prime order in (5). In this note we solve Narkiewicz's problem in general by giving arithmetical characterizations of a ring of integers whose class group G is any given finite abelian group.

As one would expect, the proof proceeds by describing arithmetically what it means for the class group G to have subgroups of certain kinds and for G to be a direct sum of them. Therefore several purely arithmetic properties must be formulated but it is hoped that these will seem fairly natural after they are translated into properties of the class group in the lemmas which follow.

In this note K will be a number field with integers R and class group G. The set of maximal ideals of R will be denoted $\max(R)$ and, if $p \in \max(R)$, $[p]$ denotes the ideal class of G containing p. The identity of G will be denoted by E. If $X_1, X_2, \ldots, X_n \in G$, then $\langle X_1, \ldots, X_n \rangle$ denotes the subgroup of G generated by $X_1, \ldots, X_n$. We will write C_n for the cyclic group of order n. If $a, b \in R$ or if $a, b \in Z$, we will write $a|b$ for 'a divides b in R' or 'a divides b in Z'. The context will make the meaning clear. A non-zero non-unit $a \in R$ is called *irreducible* if $a = bc \Rightarrow b$ or c is a unit. The element a is called *prime* if aR is a prime ideal. Following (5) we will say that $a \in R$ is *completely irreducible* if it is irreducible and every power a^n of a has a unique factorization. It was proved in (5) that $a \in R$ is completely irreducible if and only if $aR = p^{\mathrm{ord}\,[p]}$, where $p \in \max(R)$ and $\mathrm{ord}\,[p]$ denotes the order, or period, of $[p] \in G$. We will abuse language slightly and call p the radical of a. Elements $a, b \in R$ are coprime if $aR + bR = R$. If a, b are completely irreducible this just means that a and b are not associates, or equivalently, a and b have distinct radicals. If S is a set of completely irreducible elements we will say that a completely irreducible element $a \in R$ is coprime to S if it is coprime to each element of S. We will write $\sup A$ for the supremum of a set A of integers.

Definition. If $a \in R$ is completely irreducible and not prime, the *period of* a, denoted $P(a)$, is the greatest integer n such that $ab = c^n$ for some $b, c \in R$ with b completely

https://doi.org/10.1017/S0305004100060886 Published online by Cambridge University Press

irreducible and c irreducible. If a is prime we define $P(a) = 1$. If $S \subseteq R$ is a set of completely irreducible elements the period of S is defined as $P(S) = \sup\{P(a) | a \in S\}$.

LEMMA 1. *If $a \in R$ is completely irreducible, $aR = p^{\mathrm{ord}\,[p]}$, $p \in \max(R)$, then*

$$P(a) = \mathrm{ord}\,[p].$$

Proof. If a is not prime let $q \in [p]^{-1} \cap \max(R)$. Then $\mathrm{ord}\,[p] = \mathrm{ord}\,[q]$, and if $b, c \in R$ are such that $bR = q^{\mathrm{ord}\,[q]}$ and $cR = pq$, then b is completely irreducible, c is irreducible, and $abu = c^{\mathrm{ord}\,[p]}$ for some unit u of R. Thus $P(a) \geqslant \mathrm{ord}\,[p]$. To show $P(a) \leqslant \mathrm{ord}\,[p]$ let $ab = c^m$ with $b, c \in R$, b completely irreducible, c is irreducible, say $bR = q^{\mathrm{ord}\,[q]}$, $q \in \max(R)$. Then from $ab = c^m$ we get $cR = p^r q^s$, with $r + s \geqslant 1$. Thus

$$p^{\mathrm{ord}\,[p]} q^{\mathrm{ord}\,[q]} = (p^r q^s)^m \Rightarrow \mathrm{ord}\,[p] \geqslant m.$$

Definition. Let $S \subseteq R$ be a set of completely irreducible elements of R. A completely irreducible element $d \in R$ which is coprime to S is said to be *dependent on S* if there exist pairwise coprime elements $d_1, \ldots, d_n \in S$ and an element $a \in R$ such that $a | (dd_1 d_2 \ldots d_n)$, $d | a^{P(d)}$ and $d \nmid a^{P(d)-1}$. The set S is said to be *saturated* if there are no completely irreducible elements of R dependent on S.

Remarks. (i) If $d, d_1, d_2, \ldots, d_n$ are pairwise coprime completely irreducible elements and d is prime, then d is dependent on $\{d_1, \ldots, d_n\}$.

(ii) If $d, d_1, d_2, \ldots, d_n$ are pairwise coprime completely irreducible elements with d dependent on $\{d_1, \ldots, d_n\}$ and d_n prime, then d is dependent on $\{d_1, \ldots, d_{n-1}\}$. Further, if all of the d_i are prime, then d is prime.

If S is a set of completely irreducible elements of R we let

$$M(S) = \{p \in \max(R) | aR = p^{\mathrm{ord}\,[p]} \text{ for some } a \in S\}.$$

LEMMA 2. *Let $d, d_1, \ldots, d_n$ be pairwise coprime completely irreducible elements of R, with radicals $p, p_1, \ldots, p_n$ respectively. Then d is dependent on $\{d_1, \ldots, d_n\}$ if and only if $[p] \in \langle [p_1], \ldots, [p_n] \rangle$.*

Proof. We may assume d is not prime by remark (i) above. If d is dependent on $d_1, d_2, \ldots, d_n$, then $dd_1 d_2 \ldots d_n = ab$ with $d | a^{P(d)}$, $d \nmid a^j$ for $1 \leqslant j < P(d)$. Thus we have $aR = pp_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$ where $0 \leqslant r_i \leqslant \mathrm{ord}\,[p_i]$, and hence $E = [p][p_1]^{r_1} \ldots [p_n]^{r_2}$. Therefore $[p] = [p_1]^{\mathrm{ord}\,[p_1]-r_1} [p_2]^{\mathrm{ord}\,[p_2]-r_2} \ldots [p_n]^{\mathrm{ord}\,[p_2]-r_n}$.

Conversely, if $[p] = [p_1]^{s_1} [p_2]^{s_2} \ldots [p_n]^{s_n}$ with $0 \leqslant s_i \leqslant \mathrm{ord}\,[p_i]$, then if $r_i + s_i = \mathrm{ord}\,[p_i]$ for $i = 1, 2, \ldots, n$, then $E = [p][p_i]^{r_1} \ldots [p_n]^{r_n}$ and hence $pp_1^{r_1} \ldots p_n^{r_n} = aR$ for some $a \in R$. Then $a | (dd_1 d_2 \ldots d_n)$, $d | a^{P(d)}$ and $d \nmid a_j$ for $1 \leqslant j < P(d)$.

LEMMA 3. *Let $S \subseteq R$ be a saturated set of completely irreducible elements, and let $H \subseteq G$ be the subgroup generated by $\{[p] | p \in M(S)\}$. Then $M(S) = \{p \in \max(R) | [p] \in H\}$.*

Proof. It suffices to show the inclusion $\supseteq$. If $p \in \max(R)$, $[p] \in H$, and $p \notin M(S)$, then there exist distinct primes $p_1, p_2, \ldots, p_n \in S$ such that $[p] \in \langle [p_1], \ldots, [p_n] \rangle$. Let $dR = p^{\mathrm{ord}\,[p]}$, $d_i = p^{\mathrm{ord}\,[p_i]}$. Then, by the above lemma, d is dependent on $d_1, \ldots, d_n$ and hence $d \in S$ since S is saturated. But then $p \in M(S)$, a contradiction.

Recall that, if H is group and $x \in H$, the *period of x* is the least positive integer n such that $x^n = e$ = identity element of H. We will call $\sup\{\text{period of } x | x \in H\}$ the period of H.

https://doi.org/10.1017/S0305004100060886 Published online by Cambridge University Press

LEMMA 4. *If $S \subseteq R$ is a saturated set of completely irreducible elements of R and $H \subseteq G$ is the subgroup generated by $\{[p] | p \in M(S)\}$, then $P(S) =$ period of H.*

Proof. This is immediate from Lemmas 1 and 3.

LEMMA 5. *Let $d_1, d_2, \ldots, d_n$ be non-prime pairwise coprime completely irreducible elements of R with radicals $p_1, p_2, \ldots, p_n$ respectively. Then the product $d_1 d_2 \ldots d_n$ has a unique factorization if and only if the sum $\langle [p_1] \rangle + \ldots + \langle [p_n] \rangle = H \subseteq G$ is direct.*

Proof. If $d_1 d_2 \ldots d_n = \alpha_1 \ldots \alpha_r$ with $\alpha_i \in R$ irreducible and some

$$\alpha_i R \notin \{d_1 R, d_2 R, \ldots, d_n R\},$$

then we have $\alpha_i R = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$ with $0 \leqslant r_i < \operatorname{ord}[p_i]$. But this factorization gives $E = [p_1]^{r_1} [p_2]^{r_2} \ldots [p_n]^{r_n}$ and so the sum $\langle [p_1] \rangle + \ldots + \langle [p_n] \rangle$ is not direct.

Conversely, if the sum is not direct then we get $aR = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$ with

$$0 \leqslant r_i < \operatorname{ord}[p_i] \quad \text{and} \quad \sum_{i=1}^{n} r_i > 0.$$

But then an irreducible factor of a is an irreducible factor of $d_1 \ldots d_n$ which is not an associate of any of the d_i. Thus $d_1 \ldots d_n$ does not have unique factorization.

Before giving our first arithmetical characterization we need a simple result on finite abelian groups from (5).

Definition. If H is a finite abelian group let $s(H)$ be the greatest integer n such that there exists a set $\{H_1, H_2, \ldots, H_n\}$ of non-trivial subgroups of H such that $H_i \cap H_j = \{e\}$ for $i \neq j$.

LEMMA 6. (5) *Let H be an abelian group of order n with decomposition into cyclic groups of prime power order:*

$$H = \bigoplus_{p|n} H_p = \bigoplus_{p|n} \bigoplus_{i=1}^{v(p)} C_{p^{n(p,i)}}$$

where H_p denotes the maximal p-subgroup of H. Then

$$s(H) = \sum_{p|n} \frac{p^{v(p)} - 1}{p - 1}.$$

It follows immediately from the above lemma that, if H is a finite abelian group and $m =$ the period of H, then $H \cong C_m$ if and only if $s(H) =$ number of prime integers dividing m.

The following definition will be convenient for interpreting $s(H)$ for $H \subseteq G$ in terms of the arithmetic of R.

Definition. The *spread* $s(T)$ of a saturated set T of completely irreducible elements of R is $\sup\{n \in Z |$ there exists non-prime, pairwise coprime elements $d_1, d_2, \ldots, d_n \in T$ such that $d_i d_j$ has a unique factorization for $i \neq j\}$.

LEMMA 7. *Let $T \subseteq R$ be a saturated set of completely irreducible elements of R and let $H \subseteq G$ be the subgroup generated by $\{[p] | p \in M(T)\}$. Then $s(H) = s(T)$.*

Proof. If $d_1, \ldots, d_n$ is a set of non-prime, pairwise coprime elements such that $d_i d_j$ has a unique factorization for $i \neq j$, then by Lemma 5 we have $\langle [p_i] \rangle \cap \langle [p_j] \rangle = \{E\}$ for $i \neq j$. Thus $s(T) \leqslant s(H)$.

https://doi.org/10.1017/S0305004100060886 Published online by Cambridge University Press

Conversely if $[p_1], \ldots, [p_k]$ are non-identity classes of H such that

$$\langle [p_i] \rangle \cap \langle [p_j] \rangle = \{E\}$$

for $i \neq j$, then $p_i \in M(T)$ by Lemma 3 and so $p_i^{\text{ord}\,[p_i]} = d_i R$ for $d_i \in T$. But then $\{d_1, \ldots, d_k\} \subseteq T$ is a family of non-prime, pairwise coprime elements and $d_i d_j$ has unique factorization for $i \neq j$ by Lemma 5. Thus $s(H) \leqslant s(T)$ and so $s(H) = s(T)$.

THEOREM 1. *R has class group $G = C_{n_1} \oplus C_{n_2} \oplus \ldots \oplus C_{n_k}$ where $n_1 | n_2 | \ldots | n_k$ if and only if there exist saturated subsets $I_1, I_2, \ldots, I_k$ of completely irreducible elements of R such that:*

(i) *$P(I_j) = n_j$ for $j = 1, 2, \ldots, k$.*

(ii) *$s(I_j) =$ the number of prime divisors of n_j for $j = 1, 2, \ldots, k$.*

(iii) *For any choice of pairwise coprime elements $d_j \in I_j$, $j = 1, 2, \ldots, k$, the product $d_1 d_2 \ldots d_k$ has a unique factorization.*

(iv) *If $d \in R - \cup_{j=1}^{k} I_j$ is completely irreducible then there exist $d_j \in I_j$, $j = 1, \ldots, k$, such that d is dependent on $\{d_1, \ldots, d_k\}$.*

Proof. Assume $I_1, I_2, \ldots, I_k$ are saturated subsets of completely irreducible elements satisfying the above properties. For $j = 1, 2, \ldots, k$ let H_j be the subgroup of G generated by $\{[p] | p \in M(I_j)\}$. Then H_j has period n_j by Lemma 4 and $s(H_j) =$ the number of primes dividing n_j by Lemma 7. Thus $H_j \cong C_{n_j}$ by the remark following lemma 6. Let $[p_j] \in H_j$ be a generator of $H_j \cong C_{n_j}$. Further, we may choose the primes $p_1, p_2, \ldots, p_k$ to be distinct ((6), p. 325, corollary 7). The sum $H_1 + \ldots + H_k = \langle [p_1] \rangle + \ldots + \langle [p_k] \rangle$ is direct by (iii) and Lemma 5. To show $H_1 + H_2 + \ldots + H_k = G$, let $[p] \in G$, $p \in \max(R)$. If $p \in M(I_j)$ for some j then $[p] \in H_j$. If $p \notin \cup_{j=1}^{k} M(I_j)$ let $dR = p^{\text{ord}\,[p]}$. Then $\text{ord}\,[p] > 1$ and by (iv) there exist $d_i \in I_i$, $i = 1, 2, \ldots, k$, such that d is dependent on $\{d_1, \ldots, d_k\}$. Since d is not prime, then not all of the d_i are prime, and after possibly renumbering the I_j we may assume that $d_1, d_2, \ldots, d_t$ are not prime and $d_{t+1}, d_{t+2}, \ldots, d_k$ are prime (if $t < k$). Then d is dependent on $d_1 d_2, \ldots, d_t$. Let $p_i =$ radical of d_i, $i = 1, 2, \ldots, t$. Since $[p_i] \in H_i$ and $H_i \cap H_j = \{E\}$ for $i \neq j$, then $d_1, d_2, \ldots, d_t$ are pairwise coprime. Thus by Lemma 2 we have $[p] \in \langle [p_1], [p_2], \ldots, [p_t] \rangle \subseteq H_1 + \ldots + H_t$. Thus

$$G = H_1 \oplus \ldots \oplus H_k \cong C_{n_1} \oplus \ldots \oplus C_{n_k}.$$

Conversely, assume that R has class group $G \cong C_{n_1} \oplus \ldots \oplus C_{n_k}$ with $n_1 | n_2 | \ldots | n_k$. Let $I_j = \{d \in R | dR = p^{\text{ord}\,[p]}$ for some $p \in \max(R)$ with $[p] \in C_{n_j}\}$, $j = 1, 2, \ldots, k$. To see that I_j is saturated let $d \in R$ be a completely irreducible element which is coprime to I_j and assume that there exist pairwise coprime elements $d_1, d_2, \ldots, d_n \in I_j$ with d dependent on $d_1, d_2, \ldots, d_n$. Let $p, p_1, p_2, \ldots, p_n$ be the radicals of $d, d_1, d_2, \ldots, d_n$ respectively. Then $[p] \in \langle [p_1], \ldots, [p_n] \rangle \subseteq C_{n_j}$ by Lemma 2 and hence $d \in I_j$. But this contradicts the assumption that d is coprime to I_j. Thus I_j is saturated. That (i) holds follows from Lemma 4, and property (ii) follows from Lemmas 6 and 7. To verify property (iii) let $d_j \in I_j$, $j = 1, 2, \ldots, k$, be pairwise coprime. After possibly renumbering the I_j we may assume that $d_1, d_2, \ldots, d_t$ are not prime and $d_{t+1}, \ldots, d_k$ are prime. Since any factorization of $d_1 d_2 \ldots d_k$ must clearly have associates of $d_{t+1}, d_{t+2}, \ldots, d_k$ among the factors it suffices to show that $d_1 d_2 \ldots d_t$ has a unique factorization, and this holds by Lemma 5. To verify property (iv) let $d \in R - \cup_{j=1}^{k} I_j$ be a completely irreducible element of R, and let $dR = p^{\text{ord}\,[p]}$. Then

$$[p] \in G = C_{n_1} \oplus \ldots \oplus C_{n_k} \Rightarrow [p] = [p_1]^{r_1} [p_2]^{r_2} \ldots [p_k]^{r_k}$$

https://doi.org/10.1017/S0305004100060886 Published online by Cambridge University Press

where the $[p_i]$, $p_i \in \max(R)$, are generators of C_{n_i}, and $0 \leqslant r_i < \operatorname{ord}[p_i] = n_i$, and since $C_{n_i} \cap C_{n_j} = \{E\}$ for $i \neq j$ the primes $p, p_1, p_2, \ldots, p_k$ are distinct. Thus if $d_i R = p_i^{\operatorname{ord}[p_i]}$, then $d_i \in I_i$ and d is dependent on $\{d_1, d_2, \ldots, d_k\}$ by Lemma 2.

Many variations of the above theorem are clearly possible. The above theorem uses the fact that each ideal class of an algebraic number field contains infinitely many prime ideals. The following variation may be preferred since it requires only that each ideal class of R contain at least one prime ideal. However, there are Dedekind domains with finite class group that do not satisfy this latter condition ((3), example 15.20). The above ideas can be applied to these domains if one is willing to adjoin an indeterminate as is discussed following the next theorem.

THEOREM 2. *R has class group $G = C_{n_1} \oplus C_{n_2} \oplus \ldots \oplus C_{n_k}$ where $n_1 | n_2 | \ldots | n_k$ if and only if there exist saturated subsets $I_1, I_2, \ldots, I_k$ of completely irreducible elements of R, and pairwise relatively prime elements $d_j \in I_j$, $j = 1, 2, \ldots, k$, such that*

(i) *$P(d_j) = n_j$.*

(ii) *Any element $d \in I_j$ is either an associate of d_j or is dependent on d_j.*

(iii) *The product $d_1 d_2 \ldots d_k$ has a unique factorization.*

(iv) *Any completely irreducible element $d \in R - \cup_{j=1}^{k} I_j$ which is coprime to the set $\{d_1, d_2, \ldots, d_k\}$ is dependent on $\{d_1, d_2, \ldots, d_k\}$.*

Proof. Let $I_1, \ldots, I_k$ and $d_j \in I_j$, $j = 1, \ldots, k$, satisfy the above properties. Let H_j be the subgroup of G generated by $\{[p] | p \in M(I_j)\}$ and let $p_j =$ radical of d_j for $j = 1, 2, \ldots, k$. Then H_j is cyclic with generator $[p_j]$ by lemma 2. The sum $H_1 + H_2 + \ldots + H_k$ is direct by (iii) and lemma 5, and $H_1 + H_2 + \ldots + H_k = G$ by (iv) and Lemma 2.

Conversely, if $G = C_{n_1} \oplus \ldots \oplus C_{n_k}$ with $n_1 | n_2 \ldots | n_k$ let $I_j = \{d \in R | dR = p^{\operatorname{ord}[p]}$ for some $p \in \max(R)$ with $[p] \in C_{n_j}\}$, $j = 1, 2, \ldots, k$. Then I_j is saturated as in the above proof and if $[p_j] \in C_{n_j}$ is a generator of C_{n_j} and $d_j R = p_j^{\operatorname{ord}[p_j]}$ then $I_1, I_2, \ldots, I_k$ and $d_1, d_2, \ldots, d_k$ satisfy the properties (i)–(iv).

Remarks. (*a*) If D is a Dedekind and X is an indeterminate let $D_1 = S^{-1}D[X]$ where $S =$ the set of monic polynomials in $D[X]$. Then D_1 is a Dedekind domain and the induced map of class groups $C(D) \to C(D_1)$ is an isomorphism. Further, each ideal class of D_1 contains a prime ideal ((4), theorem 40·6). Thus D has class group $G = C_{n_1} \oplus C_{n_2} \oplus \ldots \oplus C_{n_k}$ with $n_1 | n_2 | \ldots | n_k$ if and only if there exist saturated subsets $I_1, I_2, \ldots, I_k$ of completely irreducible elements of D_1 and pairwise relatively prime elements $d_j \in I_j, j = 1, 2, \ldots, k$, satisfying properties (i)–(iv) of theorem 2.

(*b*) We have chosen to work with the invariant factor decomposition of G in the above theorems. However, any representation of G as a direct sum of cyclic groups would work just as well.

(*c*) If D is a Dedekind domain with finite class group then it is well known that $D = D_1 \cap D_2$ where D_1 and D_2 are overrings which are principal ideal domains ((4), p. 505, exercise 4). It follows from the above theorems that, if R is the ring of integers of a number field, then any decomposition $C(R) \cong C_{n_1} \oplus \ldots \oplus C_{n_k}$ of the class group of R as a direct sum of cyclic groups corresponds to a representation $R = \cap_{i=1}^{k} R_i$ of R as an intersection of overrings with $C(R_i) \cong C_{n_i}$ and such that the induced map $C(R) \to \oplus_{i=1}^{k} C(R_i)$ is an isomorphism.

(*d*) Much of the above work carries over to Krull domains.

https://doi.org/10.1017/S0305004100060886 Published online by Cambridge University Press

REFERENCES

(1) CARLITZ, L. A characterization of algebraic number fields with class number two. *Proc. Amer. Math. Soc.* **11** (1960), 391–392.
(2) CZOGALA, A. Arithmetic characterization of algebraic number fields with small class numbers. *Math. Z.* **176** (1981), 247–253.
(3) FOSSUM, R. M. *The divisor class group of a Krull domain* (Springer-Verlag, New York, 1973).
(4) GILMER, R. *Multiplicative ideal theory* (Marcel Dekker, Inc., New York, 1972).
(5) KACZOROWSKI, J. A pure arithmetical characterization for certain fields with a given class group. *Colloq. Math.* **45** (1981), 327–330.
(6) NARKIEWICZ, W. *Elementary and analytic theory of algebraic numbers* (PWN-Polish Scientific Publishers, Warszawa, 1974).

https://doi.org/10.1017/S0305004100060886 Published online by Cambridge University Press