COLLOQUIUM MATHEMATICUM

VOL. XLV 1981 FASC. 2

A PURE ARITHMETICAL CHARACTERIZATION FOR CERTAIN FIELDS WITH A GIVEN CLASS GROUP

BY

J. KACZOROWSKI (POZNAŃ)

1. Let us denote by K, R_K, $H(K)$, and $h(K)$, an algebraic number field, its ring of integers, the class group, and class number, respectively.

It is well known that R_K is a unique factorization domain if and only if $h(K) = 1$ and that every element from R_K has all irreducible factorizations of the same length if and only if $h(K) \leqslant 2$ (see [1]).

It is an interesting question to give a pure arithmetical characterization for the fields with a given class group or class number.

One of the possible approaches to this problem was given by Śliwa in [3].

The aim of this note is to give an arithmetical characterization of the fields with the cyclic class group or with the class group of the form C_p^k, where p is a prime number. Our method is not a generalization of the method used in [1] and [3].

2. Let us begin with the following pure group theoretical lemma:

LEMMA. *Let G be a finite abelian group and let $s(G)$ be the maximal number of elements in the family $\{H_1, \ldots, H_n\}$ of non-trivial subgroups of G such that for every $i \neq j$ we have $H_i \cap H_j = \{e\}$, where e is the unit element of G. Let*

$$G = \bigoplus_{p \mid |G|} G_p = \bigoplus_{p \mid |G|} \bigoplus_{k=1}^{\nu(p)} C_{p^{a_k(p)}},$$

where G_p denotes the maximal p-group contained in G. Then

$$s(G) = \sum_{p \mid |G|} \frac{p^{\nu(p)}-1}{p-1}.$$

Proof. Let $n = s(G)$ and let $J = \{H_1, \ldots, H_n\}$ be a maximal system of subgroups with the prescribed property. For $i = 1, \ldots, n$ let H_i' be a non-trivial subgroup of H_i. The set $\{H_1', \ldots, H_n'\}$ has the same cardinality as J and the same property. Thus we can choose J in such a way that every

H_i is a cyclic group of prime order. Conversely, if J is a set of cyclic subgroups with prime orders, then for every $H_1, H_2 \in J$, $H_1 \neq H_2$, we have $H_1 \cap H_2 = \{e\}$. Hence

$$s(G) = \sum_{p \mid |G|} \sum_{\substack{H \leqslant G \\ |H| = p}} 1 = \sum_{p \mid |G|} \frac{1}{p-1} \sum_{\substack{g \in G_p \\ \operatorname{ord} g = p}} 1 = \sum_{p \mid |G|} \frac{p^{\nu(p)}-1}{p-1}.$$

3. An element d from R_K is said to be *completely irreducible* if it is irreducible and d^n has a unique factorization for every natural n.

PROPOSITION 1. (i) *$d \in R_K$ is completely irreducible if and only if there exists a prime ideal $\mathfrak{p}$ such that $dR_K = \mathfrak{p}^{\operatorname{ord}[\mathfrak{p}]}$, where $[\mathfrak{p}]$ denotes the class from $H(K)$ to which $\mathfrak{p}$ belongs.*

(ii) *There exists a natural number M such that, for every a from R_K, a^M has a factorization into completely irreducible numbers. Let $m(K)$ be the least such number M. If $H(K) = C_{n_1} \oplus \ldots \oplus C_{n_k}$, where $n_1 \mid \ldots \mid n_k$, then $m(K) = n_k$.*

(iii) *The factorization of $a \in R_K$ into completely irreducible integers is unique.*

Proof. The sufficiency of the condition contained in (i) is obvious. To show the necessity let us consider the factorization of dR_K into prime ideals $dR_K = \mathfrak{p}_1 \ldots \mathfrak{p}_t$. We have

$$(1) \qquad d^{n_k} R_K = (\mathfrak{p}_1^{\operatorname{ord}[\mathfrak{p}_1]})^{n_k/\operatorname{ord}[\mathfrak{p}_1]} \ldots (\mathfrak{p}_t^{\operatorname{ord}[\mathfrak{p}_t]})^{n_k/\operatorname{ord}[\mathfrak{p}_t]}.$$

Let d_i be any generator of $\mathfrak{p}_i^{\operatorname{ord}[\mathfrak{p}_i]}$. All d_i are irreducible and we have

$$d^{n_k} = u d_1^{n_k/\operatorname{ord}[\mathfrak{p}_1]} \ldots d_t^{n_k/\operatorname{ord}[\mathfrak{p}_t]}, \qquad u \in U(K).$$

But d^{n_k} is an element with the unique factorization, so $\mathfrak{p}_1 = \ldots = \mathfrak{p}_t$ and $t = \operatorname{ord}[\mathfrak{p}_1]$. This completes the proof of (i).

The inequality $m(K) \leqslant n_k$ follows from (1) and (i). To show that $m(K) = n_k$ we consider the class X from $H(K)$ such that $\operatorname{ord} X = n_k$ and two prime ideals $\mathfrak{p} \in X$, $\mathfrak{P} \in X^{-1}$. The integer $a \in R_K$ defined by $aR_K = \mathfrak{p}\mathfrak{P}$ is irreducible and one can easily see that the minimal number M such that a^M has the factorization into completely irreducible numbers is equal to n_k. Hence (ii) is proved.

(iii) follows from the fact that the representation of every non-trivial ideal is unique as a product of prime ideals.

Thus the proof of our proposition is complete.

In the following proposition we give another arithmetical characterization of $m(K)$.

PROPOSITION 2. *$m(K)$ is the minimal number M with the following property: if a^M has a unique factorization, then a^n has a unique factorization for every natural number n.*

Proof. We show that $m(K) = n_k$ (see Proposition 1). Assume that $X \in H(K)$ has order n_k. If $\mathfrak{p}$ is a prime ideal from X and $\mathfrak{P}$ is a prime ideal from X^{-1}, then the ideal $\mathfrak{p}\mathfrak{P}$ is principal, generated, e.g., by a and, obviously, a^n has a unique factorization for $n = 1, \ldots, n_k-1$, but not for $n = n_k$. This shows that $m(K) \geqslant n_k$.

To prove $m(K) \leqslant n_k$ let $a \in R_K$ be such that a^{n_k} has a unique factorization and let $a = d_1 \ldots d_s$ be a factorization of a into irreducible integers. By Proposition 1, a^{n_k} has a factorization into completely irreducible integers. Hence all d_i for $i = 1, \ldots, s$ are completely irreducible, say: $d_i R_K = \mathfrak{p}_i^{\operatorname{ord}[\mathfrak{p}_i]}$. If a^n has a non-unique factorization for a certain natural n, then in the set $\{[\mathfrak{p}_1], \ldots, [\mathfrak{p}_s]\}$ one can find a minimal equality (see [3]) different from $[\mathfrak{p}_i]^{\operatorname{ord}[\mathfrak{p}_i]} = E$, say

$$[\mathfrak{p}_1]^{c_1} \ldots [\mathfrak{p}_s]^{c_s} = E, \qquad \sum c_i \neq 0,\ 0 \leqslant c_i < \operatorname{ord}[\mathfrak{p}_i]$$

(this follows from (iii) of Proposition 1). The ideal $\mathfrak{p}_1^{c_1} \ldots \mathfrak{p}_s^{c_s}$ is principal, generated, say, by b, and b is an irreducible integer, but not a completely irreducible one. Moreover, b divides a, which shows that a does not have a unique factorization, and we obtain a contradiction.

Now we can find an arithmetical interpretation for the constant $s\big(H(K)\big)$ which we denote simply by $s(K)$.

Two non-unit integers a_1 and a_2 from R_K are called *completely relatively prime* if, for every natural number n, a_1^n and a_2^n have no common non-unit divisors. One can easily see that a_1 and a_2 are completely relatively prime if and only if every b dividing both $a_1^{m(K)}$ and $a_2^{m(K)}$ is a unit.

PROPOSITION 3. *$s(K)$ is the maximal natural number n such that there exists a set $\{a_1, \ldots, a_n\}$ with the following properties: for every $i = 1, \ldots, n$, a_i is not a product of prime elements* (π is *prime* if $\pi \mid ab$ implies $\pi \mid a$ or $\pi \mid b$), *a_i and a_j are completely relatively prime for $i \neq j$, and $(a_i a_j)^{m(K)}$ has a unique factorization.*

Proof. Let $a_1, \ldots, a_n$ be an arbitrary set of pairwise completely relatively prime integers satisfying the conditions given in the proposition. For $i = 1, \ldots, n$ let d_i be any completely irreducible element dividing $a_i^{m(K)}$, $d_i R_K = \mathfrak{p}_i^{\operatorname{ord}[\mathfrak{p}_i]}$, $[\mathfrak{p}_i] \neq E$.

For $i \neq j$ the elements d_i and d_j are distinct and $d_i d_j$ has a unique factorization. If now $\langle g \rangle$ denotes the cyclic group generated by g, then for $i \neq j$

$$\langle [\mathfrak{p}_i] \rangle \cap \langle [\mathfrak{p}_j] \rangle = E.$$

Hence $n \leqslant s(K)$.

But we can find $s(K)$ classes $\{X_1, \ldots, X_{s(K)}\}$, neither of them equal to the unit class, such that $\langle X_i \rangle \cap \langle X_j \rangle = E$ for $i \neq j$. Let $\mathfrak{p}_i$ be a prime ideal from X_i. The ideals $\mathfrak{p}_i^{\operatorname{ord}[\mathfrak{p}_i]}$ are all principal and generated, say, by d_i for $i = 1, \ldots, s(K)$. The set $\{d_1, \ldots, d_{s(K)}\}$ has $s(K)$ elements and $(d_i d_j)^{m(K)}$ has a unique factorization for every $i \neq j$. This completes the proof.

COROLLARY. *For every set A of completely irreducible but not prime numbers with* $\operatorname{card} A > s(K)$ *we can find two elements $d_1, d_2 \in A$ such that $d_1 d_2$ has a non-unique factorization and $s(K)$ is the minimal number with this property.*

From the Lemma and Proposition 1 we obtain the main theorem of our paper.

THEOREM. (i) $H(K) = C_n$ *if and only if*

$$m(K) = n \quad \text{and} \quad s(K) = \omega(n), \text{ where } \omega(n) = \sum_{p|n} 1.$$

(ii) $H(K) = C_p^k$ *if and only if*

$$m(K) = p \quad \text{and} \quad s(K) = \frac{p^k - 1}{p - 1}.$$

(iii) *$H(K)$ is a p-group if and only if $m(K) = p^k$ for a suitable natural number k.*

REFERENCES

[1] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proceedings of the American Mathematical Society 11 (1960), p. 391-392.

[2] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Chapter IX, Warszawa 1974.

[3] J. Śliwa, *Factorization of distinct lengths in algebraic number fields*, Acta Arithmetica 31 (1976), p. 399-417.

INSTITUTE OF MATHEMATICS
A. MICKIEWICZ UNIVERSITY
POZNAŃ

Reçu par la Rédaction le 14. 11. 1978;
en version modifiée le 20. 4. 1979