PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 139, Number 9, September 2011, Pages 3025–3038
S 0002-9939(2011)11053-0
Article electronically published on May 4, 2011

NONUNIQUE FACTORIZATION AND PRINCIPALIZATION IN NUMBER FIELDS

KIMBALL MARTIN

(Communicated by Matthew A. Papanikolas)

Abstract. Following what is basically Kummer's relatively neglected approach to nonunique factorization, we determine the structure of the irreducible factorizations of an element n in the ring of integers of a number field K. Consequently, we give a combinatorial expression for the number of irreducible factorizations of n in the ring. When K is quadratic, we show in certain cases how quadratic forms can be used to explicitly produce all irreducible factorizations of n.

1. Introduction

One of the basic issues in algebraic number theory is the fact that for a number field K, and an integer $n \in \mathcal{O}_K$, an irreducible factorization of n may not be unique (up to ordering and units). Historically, there were three major attempts to deal with this: Gauss's theory of binary quadratic forms for quadratic fields K, Kummer's theory of ideal numbers, and Dedekind's theory of ideals. Kummer's approach was largely abandoned in favor of Dedekind's powerful theory. Ideals lead naturally to the general notion of the class group $\mathcal{C}l_K$, which provides a way of measuring the failure of unique factorization in $\mathcal{O}_K$. In fact there are precise ways in which we can characterize the failure of unique factorization of $\mathcal{O}_K$ in terms of the class group. For instance, Carlitz [3] showed that every irreducible factorization of n over $\mathcal{O}_K$ has the same length for all $n \in \mathcal{O}_K$ if and only if the class number h_K of K is 1 or 2.

Nevertheless, the precise way in which the class group determines the irreducible factorizations of n is still not completely understood. Much of the research on nonunique factorizations to date has been devoted to the study of lengths of factorizations, motivated by [3], determining which elements have unique factorization, and related questions about asymptotic behavior. For an introduction to this subject, see [18], [11] or [7]. See [6] for a more comprehensive reference.

In this note we will give an explicit description of the structure of the irreducible factorizations of n in $\mathcal{O}_K$ in terms of the prime ideal factorization of (n) which depends only upon the class group $\mathcal{C}l_K$. Thus we have a very precise description of how the class group measures the failure of unique factorization in $\mathcal{O}_K$. For example, Carlitz's result is an immediate corollary. To do this, we use the idea of

Received by the editors February 23, 2010.
2010 *Mathematics Subject Classification.* Primary 11R27, 11R29.
Key words and phrases. Nonunique factorization, principalization, class group.

principalization, which is essentially Kummer's theory of ideal numbers, framed in the language of Dedekind's ideals. Specifically, we pass to an extension L which principalizes K; i.e., every ideal of K becomes principal in L. This means that all irreducible factorizations of $n \in \mathcal{O}_K$ come from different groupings of a single factorization in $\mathcal{O}_L$.

To understand the irreducible factorizations of n in a more quantitative way, one natural question is, what is the number $\eta_K(n)$ of (nonassociate) irreducible factorizations of n in $\mathcal{O}_K$? Of course if $h_K = 1$, then $\eta_K(n) = 1$ for all $n \in \mathcal{O}_K$. If $h_K = 2$, then Chapman, Herr and Rooney [4] established a formula for $\eta_K(n)$ in terms of the prime ideal factorization of (n) in $\mathcal{O}_K$. However, it is a rather complicated recursive formula on the number of prime ideal factors of (n). (In fact the work [4] treats the more general case of Krull domains.) For work on determining which n satisfy $\eta_K(n) = 1$, see [18]; for asymptotic results on $\eta_K(n)$, see [9], [10] or [6].

We obtain, for an arbitrary number field K and $n \in \mathcal{O}_K$, a relatively simple combinatorial expression for $\eta_K(n)$, which appears to be about as simple as one could hope for. This formula is particularly simple in the case $h_K = 2$, and we begin in Section 2 by explaining how to treat the standard class number 2 example of $K = \mathbb{Q}(\sqrt{-5})$. The expression we get for $\eta_K(n)$ is valid for any K with class number 2, and is considerably nicer than the formula in [4]. One can in fact treat the case of $K = \mathbb{Q}(\sqrt{-5})$ with quadratic forms, and this is what we do in Section 2. This yields, more than just the structure of the factorizations of n in $\mathcal{O}_K$, the explicit irreducible factorizations of n in terms of the representations of the primes dividing n (say if $n \in \mathbb{Z}$) by certain quadratic forms.

In Section 3, we treat the case of an arbitrary number field K and discuss some simple consequences. We remark that these results should in fact apply to more general Krull domains than $\mathcal{O}_K$ by the theory of type monoids [6, Section 3.5], but this is not our focus here. In Section 4, we revisit the approach using quadratic forms presented in Section 2 for quadratic fields K.

2. An example: Class number 2

Let $K = \mathbb{Q}(\sqrt{-5})$. This field has discriminant $\Delta = -20$ and class group $\mathcal{C}l_K \simeq \mathbb{Z}/2\mathbb{Z}$. Denote by $\mathfrak{C}_1$ the set of principal ideals in $\mathcal{O}_K$ and by $\mathfrak{C}_2$ the set of nonprinicpal ideals of $\mathcal{O}_K$. Now the reduced (positive binary quadratic) forms of discriminant Δ are $Q_1(x,y) = x^2 + 5y^2$ and $Q_2(x,y) = 2x^2 + 2xy + 3y^2$.

Let $\mathcal{P}_0$ denote the primes $p \in \mathbb{N}$ which are not represented by Q_1 or Q_2 and $\mathcal{P}_i$ denote the primes $p \in \mathbb{N}$ which are represented by Q_i for $i = 1, 2$. Then $\mathcal{P}_0$ is the set of inert primes in $K/\mathbb{Q}$, $\mathcal{P}_1$ is the set of primes p such that the ideal $p\mathcal{O}_K$ factors into two principal ideals in $\mathcal{O}_K$, and $\mathcal{P}_2$ is the set of primes p such that $p\mathcal{O}_K$ factors into two nonprincipal ideals of $\mathcal{O}_K$.

Set

$$\mathcal{P}_i^{ram} = \{p \in \mathcal{P}_i : p \text{ is ramified in } K\}, \text{ and}$$
$$\mathcal{P}_i^{unr} = \{p \in \mathcal{P}_i : p \text{ is unramified in } K\}.$$

Explicitly, we have $\mathcal{P}_0 = \{p : p \equiv 11, 13, 17, 19 \mod 20\}$, $\mathcal{P}_1^{ram} = \{5\}$, $\mathcal{P}_1^{unr} = \{p : p \equiv 1, 9 \mod 20\}$, $\mathcal{P}_2^{ram} = \{2\}$ and $\mathcal{P}_2^{unr} = \{p : p \equiv 3, 7 \mod 20\}$.

If $p \in \mathcal{P}_0 \cup \mathcal{P}_1$, then any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying above p is in $\mathfrak{C}_1$, and if $q \in \mathcal{P}_2$, then any prime ideal of $\mathcal{O}_K$ lying above q is in $\mathfrak{C}_2$. Specifically, if $q = 2 \in \mathcal{P}_2^{ram}$, then $q\mathcal{O}_K = \mathfrak{r}^2$, where $\mathfrak{r}$ is the prime ideal $(2, 1+\sqrt{-5})$ of $\mathcal{O}_K$, and if $q \in \mathcal{P}_2^{unr}$, then $q = \mathfrak{q}\bar{\mathfrak{q}}$, where $\mathfrak{q}$ and $\bar{\mathfrak{q}}$ are distinct prime ideals of $\mathcal{O}_K$. Here $\bar{\mathfrak{q}}$ denotes the conjugate ideal of $\mathfrak{q}$ in $K/\mathbb{Q}$.

Now let $n \in \mathcal{O}_K$ be a nonzero nonunit and write the prime ideal factorization of (n) as

$$(n) = \mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_r^{d_r} \mathfrak{q}_1^{e_{11}} \bar{\mathfrak{q}}_1^{e_{12}} \cdots \mathfrak{q}_s^{e_{1s}} \bar{\mathfrak{q}}_s^{e_{2s}} \mathfrak{r}^f,$$

where each $\mathfrak{p}_i \in \mathfrak{C}_1$, $\mathfrak{q}_j \in \mathfrak{C}_2$ with conjugate $\bar{\mathfrak{q}}_j$, and the $\mathfrak{p}_i$'s, $\mathfrak{q}_j$'s, $\bar{\mathfrak{q}}_j$'s and $\mathfrak{r}$ are all distinct. Since each $\mathfrak{p}_i = (\pi_i)$ for some irreducible π_i of $\mathcal{O}_K$, any irreducible factorization of n must contain (up to units) $\pi_1^{d_1} \cdots \pi_r^{d_r}$. Thus it suffices to consider irreducible factorizations of $n' = n/(\pi_1^{d_1} \cdots \pi_r^{d_r})$.

Let q_j be the prime in $\mathbb{N}$ such that $\mathfrak{q}_j$ lies above q_j. Since $\mathfrak{q}_j$ is nonprincipal, we must have that $q_j \in \mathcal{P}_2$, i.e., q_j is represented by Q_2. Note that we can factor the quadratic form into linear factors

$$Q_2(x,y) = (\sqrt{2}x + \frac{\sqrt{2}+\sqrt{-10}}{2}y)(\sqrt{2}x + \frac{\sqrt{2}-\sqrt{-10}}{2}y) \tag{1}$$

over the field $L = K(\sqrt{2})$. Hence, while q_j is irreducible over $\mathcal{O}_K$ (otherwise the prime ideal factors of $q_j\mathcal{O}_K$ would be principal), the fact that $q_j = Q_2(x,y)$ for some x, y gives us a factorization $q_j = \alpha_{1j}\alpha_{2j}$ in L, where $\alpha_{1j} = \sqrt{2}x + \frac{\sqrt{2}+\sqrt{-10}}{2}y$ and $\alpha_{2j} = \sqrt{2}x + \frac{\sqrt{2}-\sqrt{-10}}{2}y$. Since $\sqrt{2}, \frac{\sqrt{2}\pm\sqrt{-10}}{2} \in \mathcal{O}_L$, we have $\alpha_{ij} \in \mathcal{O}_L$ (in fact irreducible).

Observing that α_{1j} and α_{2j} are conjugate with respect to the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$, the ideals $(\alpha_{1j}) \cap \mathcal{O}_K$ and $(\alpha_{2j}) \cap \mathcal{O}_K$ must be conjugate ideals of $\mathcal{O}_K$ which divide q_j, and hence in some order equal $\mathfrak{q}_j$ and $\bar{\mathfrak{q}}_j$. Thus, up to a possible relabeling, we can write $\mathfrak{q}_j\mathcal{O}_L = (\alpha_{1j})$ and $\bar{\mathfrak{q}}_j\mathcal{O}_L = (\alpha_{2j})$. Similarly $\mathfrak{r}\mathcal{O}_L = (\sqrt{2})$. To simplify notation below, we set $\alpha_{00} = \sqrt{2}$ and $e_{00} = f$.

This means the following. If $n' = \prod \beta_k$ is any irreducible factorization of n' in $\mathcal{O}_K$, we have $(n') = \mathfrak{q}_1^{e_{11}} \bar{\mathfrak{q}}_1^{e_{12}} \cdots \mathfrak{q}_s^{e_{1s}} \bar{\mathfrak{q}}_s^{e_{2s}} \mathfrak{r}^{e_{00}} = \prod (\beta_k)$ as ideals of $\mathcal{O}_K$. By unique factorization of prime ideals, any $(\beta_k) = \mathfrak{q}^{g_{11}} \bar{\mathfrak{q}}_1^{g_{12}} \cdots \mathfrak{q}_s^{g_{1s}} \bar{\mathfrak{q}}_s^{g_{2s}} \mathfrak{r}^{g_{00}}$, where $0 \le g_{ij} \le e_{ij}$. Passing to ideals of $\mathcal{O}_L$, we see that each β_k is a product of the α_{ij}. In other words, all the irreducible factorizations of n' in $\mathcal{O}_K$, up to units, come from different groupings of the factorization $n' = u \prod \alpha_{ij}^{e_{ij}}$ in $\mathcal{O}_L$, where u is a unit of $\mathcal{O}_K$.

Thus to determine the factorizations of n' in $\mathcal{O}_K$, it suffices to determine when a product of the α_{ij} is an irreducible element of $\mathcal{O}_K$. But this is simple! Note from the factorization of $Q_2(x,y)$ in (1), we see that each $\alpha_{ij} \in \sqrt{2}K$. Hence the product of any two α_{ij} lies in K, and therefore $\mathcal{O}_K$, and must be irreducible since no individual $\alpha_{ij} \in \mathcal{O}_K$. What we have done, together with the fact that the α_{ij}'s are all nonassociate (they generate different ideals), proves the following.

If $\{a_i\}$ is a collection of distinct objects, denote the multiset containing each a_i with cardinality m_i by $\{a_i^{(m_i)}\}$.

Proposition 1. *Let $K = \mathbb{Q}(\sqrt{-5})$, $L = K(\sqrt{2})$ and $n \in \mathcal{O}_K$ be a nonzero nonunit. Write the prime ideal factorization of (n) in $\mathcal{O}_K$ as $(n) = \prod \mathfrak{p}_i^{d_i} \prod \mathfrak{q}_j^{e_j}$, where each $\mathfrak{p}_i \in \mathfrak{C}_1$, $\mathfrak{q}_j \in \mathfrak{C}_2$ and the $\mathfrak{p}_i$'s and $\mathfrak{q}_j$'s are all distinct. Let $\pi_i \in \mathcal{O}_K$ and $\alpha_j \in \mathcal{O}_L$ such that $\mathfrak{p}_i = (\pi_i)$ and $\mathfrak{q}_j\mathcal{O}_L = (\alpha_j)$. Then the irreducible nonassociate factorizations of n are precisely $n = u \prod \pi_i^{d_i} \prod \beta_k$, where u is a unit, each β_k is a product of two (not necessarily distinct) α_j's and $\prod \beta_k = \prod \alpha_j^{e_j}$.*

In particular $\eta_K(n)$ is the number of ways we can arrange the multiset $\{\alpha_j^{(e_j)}\}$ in pairs, i.e., the number of partitions of this multiset into submultisets of size 2. In other words, if the number of distinct $\mathfrak{q}_j$'s is m, then $\eta_K(n)$ is the coefficient of $\prod x_j^{e_j}$ in the formal power series expansion of $\prod_{i \leq j} \frac{1}{1-x_i x_j}$ in $\mathbb{Z}[[x_1, x_2, \ldots, x_m]]$.

Note the final sentence is essentially a tautology.

Thus, in addition to $\eta_K(n)$, we have provided an explicit determination of the irreducible factorizations of an arbitrary $n \in \mathcal{O}_K$, provided one knows the (irreducible) factorization in $\mathcal{O}_L$. (The point is that there is a choice of which of α_{1j} and α_{2j} is $\mathfrak{q}_j \mathcal{O}_L$ and which is $\bar{\mathfrak{q}}_j \mathcal{O}_L$ in the above argument.) However if $n \in \mathbb{Z}$, then it suffices to know the prime factorization $n = 2^f \prod p_k'^{d_k'} \prod p_i^{d_i} \prod q_j^{e_j}$ in $\mathbb{Z}$, where each $p_k' \in \mathcal{P}_0$, $p_i \in \mathcal{P}_1$, $q_j \in \mathcal{P}_2^{unr}$ and they are all distinct. For then each p_k' is irreducible in $\mathcal{O}_K$, the irreducible factorization each of p_i in $\mathcal{O}_K$ is given by solving $p_i = x^2 + 5y^2 = (x + \sqrt{-5}y)(x - \sqrt{-5}y)$, and the factorization $q_j = \alpha_{1j}\alpha_{2j}$ in $\mathcal{O}_L$ above is given by solving $q_j = 2x^2 + 2xy + 3y^2$. Here there is no need to worry which of α_{1j} and α_{2j} correspond to which of $\mathfrak{q}_j$ and $\bar{\mathfrak{q}}_j$ since both $\mathfrak{q}_j$ and $\bar{\mathfrak{q}}_j$ occur to the same exponent e_j.

Except for the explicit factorization we get from the quadratic forms Q_1 and Q_2 above, all of this is true for arbitrary number fields with class number 2.

Proposition 2. *If K is a number field with class number 2, and $n \in \mathcal{O}_K$ is a nonzero nonunit, write the prime ideal factorization of (n) as $(n) = \prod \mathfrak{p}_i^{d_i} \prod_{j=1}^m \mathfrak{q}_j^{e_j}$, where each $\mathfrak{p}_i$ is principal, $\mathfrak{q}_j$ is nonprincipal, and the $\mathfrak{p}_i$'s and $\mathfrak{q}_j$'s are all distinct. Consider the formal power series $f(x_1, \ldots, x_m) \in \mathbb{Z}[[x_1, \ldots, x_m]]$ formally given by $f(x_1, \ldots, x_m) = \prod_{i,j} \frac{1}{1-x_i x_j}$. Then $\eta_K(n)$ is the number of ways we can arrange the multiset $\{x_j^{(e_j)}\}$ in pairs, i.e., the coefficient of $\prod x_j^{e_j}$ in $f(x_1, \ldots, x_m)$.*

One can either conclude this result from the work of [4] together with our example of $K = \mathbb{Q}(\sqrt{-5})$ or observe that it is a special case of our main result, Theorem 1, below. In [4], the authors prove a recursive formula for $\eta_K(n)$, being recursive on the number of nonprincipal prime ideal factors of (n), which is independent of the field K (in fact it is valid more generally for Krull domains also, but we will not stress this). As the formula in [4] is rather complicated, we will not state their complete formula here, but just give the first two cases to give the reader an idea of the form of their expressions. In the notation of the corollary above, they show, assuming $e_1 \leq e_2 \leq \cdots \leq e_m$, that $\eta_K(n) = \eta_{\mathbb{X}_{m+1}}(e_1, e_2, \ldots, e_m, \frac{e_1 + \ldots + e_m}{2})$, where

$$\eta_{\mathbb{X}_2}(x_1, x_2) = \lfloor \frac{\min(x_1, x_2)}{2} \rfloor + 1,$$
$$\eta_{\mathbb{X}_3}(x_1, x_2, x_3) = \sum_{j=0}^{\lfloor \frac{x_1}{2} \rfloor} \sum_{k=0}^{x_1 - 2j} \eta_{\mathbb{X}_2}(x_2 - k, x_3 - x_1 + 2j + k),$$

and the expression for $\eta_{\mathbb{X}_{m+1}}$ involves an m-fold summation over $\eta_{\mathbb{X}_m}$.

Hence our approach of principalization and factoring the form $Q_2(x, y)$ in $K(\sqrt{2})$ provides a much nicer combinatorial answer to the question of what is $\eta_K(n)$. We now proceed to see what our result says in some simple cases. For the rest of this section, we maintain the notation of Proposition 2.

The first thing we observe is that $\sum e_i$ must be even.

Corollary 1. *An irreducible factorization of n is unique, i.e., $\eta_K(n) = 1$, if and only if (i) there is at most one nonprincipal prime ideal dividing (n), or (ii) $(n) = \prod \mathfrak{p}_i^{d_i} \cdot \mathfrak{q}_1^e \mathfrak{q}_2$, where the $\mathfrak{p}_i$'s are principal, the $\mathfrak{q}_i$'s are nonprincipal, and e is odd.*

In particular, to return to the original example of $K = \mathbb{Q}(\sqrt{-5})$, if $n \in \mathbb{Z}$, then $\eta_K(n) = 1$ if and only if (i) it is not divisible by any primes in $\mathcal{P}_2^{unr}$, i.e., any primes of the form $q \equiv 3, 7 \mod 20$, or (ii) $n = q \prod p_i^{d_i}$, where the p_i's and q are primes with $q \equiv 3, 7 \mod 20$ and each $p_i \in \mathcal{P}_0 \cup \mathcal{P}_1$, i.e., $p_i \not\equiv 3, 7, \mod 20$ and p_i odd. This classification of $n \in \mathbb{N}$ with $\eta_{\mathbb{Q}(\sqrt{-5})}(n) = 1$ was previously established by Fogels using an approach similar in spirit to ours in [5], where he used this to show that "almost all" $n \in \mathbb{N}$ do not have unique factorization.

Corollary 2. *If $m = 2$, then $\eta_K(n) = \lfloor \frac{\min(e_1, e_2)}{2} \rfloor + 1$.*

Note that this matches with the formula for $\eta_{\mathbb{X}_2}(x_1, x_2)$ in [4]. This was observed earlier in the case of elementary abelian 2-class groups ([10, Example 1]).

Proof. We want to count the number of ways we can pair e_1 x_1's and e_2 x_2's. This is simply determined by the number of x_1's which are paired up with x_2's. This can be any number k between 0 and $\min(e_1, e_2)$ such that $e_i - k$ is even. □

In the special case $K = \mathbb{Q}(\sqrt{-5})$, this means if $q \in \mathcal{P}_2^{unr}$, then $h_K(q^e) = \lfloor \frac{e}{2} \rfloor + 1$.

Corollary 3. *If $e_1 = e_2 = \cdots = e_m = 1$, then $\eta_K(n) = (m-1)!!$.*

Proof. This is just the number of ways in which we can arrange the set $\{x_1, \ldots, x_m\}$ in pairs, which is $(m-1)!! = (m-1)(m-3)\cdots 1$. □

When $K = \mathbb{Q}(\sqrt{-5})$ and $q_1, \ldots, q_k$ are distinct primes in $\mathcal{P}_2^{unr}$, this means $h_K(q_1 \cdots q_k) = (2k-1)!!$.

3. General number fields

Let K be an arbitrary number field and let $Cl_K = \{\mathfrak{C}_i\}$ be the ideal class group of K. Denote the class of principal ideals in $\mathcal{O}_K$ by $\mathfrak{I}$.

We say that K_i is a *principalization field* for $\mathfrak{C}_i$ if K_i is an extension of K such that every ideal in $\mathfrak{C}_i$ becomes principal in $\mathcal{O}_{K_i}$. Such a field always exists. For example, if $\mathfrak{C}_i$ has order m, then for any ideal $\mathfrak{a} \in \mathfrak{C}_i$, we have that $\mathfrak{a}^m$ is principal. Say $\mathfrak{a}^m = (a)$. Consequently $\mathfrak{a}$, and therefore every ideal in $\mathfrak{C}_i$, becomes principal in the field $K_i = K(\sqrt[m]{a})$.

We say that L is a *prinicpalization field* for K if every ideal in $\mathcal{O}_K$ becomes principal in $\mathcal{O}_L$. For instance if K_i is a principalization field for $\mathfrak{C}_i$ for each $\mathfrak{C}_i \in Cl_K$, then the compositum $L = \prod K_i$ is a principalization field for K. By the principal ideal theorem of class field theory, the Hilbert class field of K is a principalization field for K.

If $\alpha, \beta \in \mathcal{O}_K$ and $\alpha = u\beta$ for a unit $u \in \mathcal{O}_K$, i.e., if α and β are associates, write $\alpha \sim \beta$.

Theorem 1. *Let K be a number field and $Cl_K = \{\mathfrak{C}_i\}$. Let $n \in \mathcal{O}_K$ be a nonzero nonunit. Suppose the prime ideal factorization of $n\mathcal{O}_K$ is $(n) = \prod_{(i,j) \in T} \mathfrak{p}_{ij}$, where the $\mathfrak{p}_{ij}$'s are (not necessarily distinct) prime ideals such that $\mathfrak{p}_{ij} \in \mathfrak{C}_i$, and T is some finite index set. Let K_i be a principalization field for $\mathfrak{C}_i$, so $\mathfrak{p}_{ij}\mathcal{O}_{K_i} = (\alpha_{ij})$ for some $\alpha_{ij} \in \mathcal{O}_{K_i}$. Let $L = \prod K_i$.*

Then the irreducible factorizations of n in $\mathcal{O}_K$ are precisely the factorizations of the form $n = \prod \beta_l$, where $\prod \beta_l \sim \prod \alpha_{ij}$ in $\mathcal{O}_L$ and each β_l is of the form $\beta_l \sim \prod_{(i,j)\in S} \alpha_{ij}$ in $\mathcal{O}_L$ for S a minimal (nonempty) subset of T such that $\prod_{(i,j)\in S} \mathfrak{C}_i = \mathfrak{I}$. (Here each β_l is irreducible in $\mathcal{O}_K$.)

In other words, all irreducible factorizations n in $\mathcal{O}_K$ come from different groupings of the factorization $n \sim \prod \alpha_{ij}$ in $\mathcal{O}_L$. Now a grouping of terms of this factorization in $\mathcal{O}_L$ gives an irreducible factorization in $\mathcal{O}_K$ if and only if every group of terms gives an irreducible element of $\mathcal{O}_K$ (possibly up to a unit in $\mathcal{O}_L$). (We will call such a grouping *irreducible.*) A product of α_{ij}'s gives an element of $\mathcal{O}_K$ if and only if the corresponding product of ideal classes $\mathfrak{C}_i$ is trivial in $\mathcal{C}l_K$, and this element of $\mathcal{O}_K$ will be irreducible if and only if no proper subproduct of the corresponding ideal classes is trivial.

It should be clear that this theorem gives a precise way that the class group measures the failure of unique factorization in $\mathcal{O}_K$. In particular, the larger the class group, the more complicated the structure of the irreducible factorizations of an element can become. Simple explicit examples are given at the end of Section 4. This theorem also connects Kummer's and Dedekind's approaches to resolving nonunique factorization in $\mathcal{O}_K$.

We also remark that one could take each $K_i = L$ for any principalization field L of K, but we will see in the next section reasons why one may not always want to do this. In fact, for specific n, L need not be a principalization field for K, but just for the ideal classes containing ideals dividing $n\mathcal{O}_K$.

Proof. Suppose $n = \prod \beta_l$ is an irreducible factorization of n in $\mathcal{O}_K$, i.e., each β_l is a (nonunit) irreducible. By unique factorization of prime ideals, each (β_l) is a subproduct of $\prod \mathfrak{p}_{ij}$. Write $(\beta_l) = \prod_{(i,j)\in S} \mathfrak{p}_{ij}$, where $S \subseteq T$. Since (β_l) is principal, the subproduct of prime ideals yielding (β_l) must be trivial in the class group, i.e., $\prod_{(i,j)\in S} \mathfrak{C}_i = \mathfrak{I}$. Further, S must be minimal such that the corresponding product in the class group is trivial; otherwise, we would be able to write (β_l) as a product of two principal ideals, contradicting irreducibility.

Write $S = \{(i_1, j_1), (i_2, j_2), \ldots, (i_r, j_r)\}$, so that

$$(\beta_l) = \mathfrak{p}_{i_1 j_1} \mathfrak{p}_{i_2 j_2} \cdots \mathfrak{p}_{i_r j_r}$$

Observe

$$\beta_l \mathcal{O}_{K_{i_1}} = (\alpha_{i_1 j_1}) \mathfrak{P}_{i_2 j_2} \cdots \mathfrak{P}_{i_r j_r},$$

where $\mathfrak{P}_{i_i j_i} = \mathfrak{p}_{i_i j_i} \mathcal{O}_{K_{i_1}}$. Passing to $\mathcal{O}_{K_{i_1} K_{i_2}}$ and using the fact that $\mathfrak{p}_{i_2 j_2} = (\alpha_{i_2 j_2})$ in $\mathcal{O}_{K_{i_2}}$, we see that

$$\beta_l \mathcal{O}_{K_{i_1} K_{i_2}} = (\alpha_{i_1 j_1})(\alpha_{i_2 j_2}) \mathfrak{P}^{(2)}_{i_3 j_3} \cdots \mathfrak{P}^{(2)}_{i_r j_r},$$

where $\mathfrak{P}^{(2)}_{i_i j_i} = \mathfrak{P}_{i_i j_i} \mathcal{O}_{K_{i_1} K_{i_2}}$. Proceeding inductively, we obtain

$$(\beta_l) = (\alpha_{i_1 j_1})(\alpha_{i_2 j_2}) \cdots (\alpha_{i_r j_r})$$

as ideals in $\mathcal{O}_L$, yielding (ii) as asserted in the theorem.

This proves that any irreducible factorization of n in $\mathcal{O}_K$ is of the form stated above, namely that any irreducible factorization of n is obtained from a grouping of the terms in the (not necessarily irreducible) factorization $n = u \prod \pi_i \prod \alpha_{ij}$ in $\mathcal{O}_L$ such that each group of terms is minimal so that the corresponding product in the class group $\mathcal{C}l_K$ is trivial. (Here u is some unit.) It remains to show that any such grouping gives an irreducible factorization of $\mathcal{O}_K$.

It suffices to show that if S is a minimal subset of T such that $\prod_{(i,j)\in S} \mathfrak{C}_i = \mathfrak{I}$, then $u\prod_{(i,j)\in S} \alpha_{ij}$ is an irreducible element of $\mathcal{O}_K$ for some unit $u \in \mathcal{O}_L$. Suppose S is such a subset. Then $\prod_{(i,j)\in S} \mathfrak{q}_{ij} = (\beta)$ for some $\beta \in \mathcal{O}_K$. As above, looking at ideals in $\mathcal{O}_L$, we see that $\beta \sim \prod_{(i,j)\in S} \alpha_{ij}$; hence the product on the right is, up to a unit of $\mathcal{O}_L$, an element of $\mathcal{O}_K$. If β were reducible, say $\beta = \gamma\gamma'$, where $\gamma, \gamma' \in \mathcal{O}_K$ are nonunits, then by unique factorization into prime ideals, we would have $(\gamma) = \prod_{(i,j)\in S'} \mathfrak{q}_{ij}$, where S' is a proper subset of S, i.e., $\prod_{(i,j)\in S'} \mathfrak{C}_i = \mathfrak{I}$, contradicting the minimality of S. □

Corollary 4. *Let K be a number field and $\mathcal{C}l_K = \{\mathfrak{C}_i\}$. Let $n \in \mathcal{O}_K$ be a nonzero nonunit. Suppose $(n) = \prod_{(i,j)\in T} \mathfrak{p}_{ij}^{e_{ij}}$, where the $\mathfrak{p}_{ij}$'s are distinct prime ideals, each $\mathfrak{p}_{ij} \in \mathfrak{C}_i$, and T is some index set. Let U be the multiset $U = \{(i,j)^{(e_{ij})} : (i,j) \in T\}$. Then $\eta_K(n)$ is the coefficient of $\prod x_{ij}^{e_{ij}}$ in the formal power series*

$$f(x_{ij}) = \prod_S \frac{1}{1 - \prod_{(i,j)\in S} x_{ij}} \in \mathbb{Z}[[x_{ij}]] , \quad (i,j) \in T,$$

where S runs over all minimal sub-multisets of U such that the product $\prod_{(i,j)\in S} \mathfrak{C}_i = \mathfrak{I}$. Combinatorially, $\eta_K(n)$ is the number of ways one can partition the multiset $\{x_{ij}^{e_{ij}}\}$ into minimal subsets V such that $\prod_{x_{ij}\in V} \mathfrak{C}_i = \mathfrak{I}$.

Proof. Let K_i be a principalization field for $\mathfrak{C}_i$, and write $\mathfrak{p}_{ij}\mathcal{O}_{K_i} = (\alpha_{ij})$. Set $L = \prod K_i$. Then we have $n \sim \prod_T \alpha_{ij}^{e_{ij}} = \prod_U \alpha_{ij}$ over $\mathcal{O}_L$. By the theorem, the irreducible factorizations of n in $\mathcal{O}_K$ correspond to the partitions of U into minimal sub-multisets S such that $\prod_S \mathfrak{C}_i = \mathfrak{I}$. Hence it remains to show that any two distinct partitions give nonassociate factorizations of n.

It suffices to prove that if $\prod_S \alpha_{ij} \sim \prod_{S'} \alpha_{ij}$ over $\mathcal{O}_L$ for two sub-multisets S, S' of T, then $S = S'$. But this hypothesis means that

$$\prod_S \mathfrak{p}_{ij}\mathcal{O}_L = \prod_S \alpha_{ij}\mathcal{O}_L = \prod_{S'} \alpha_{ij}\mathcal{O}_L = \prod_{S'} \mathfrak{p}_{ij}\mathcal{O}_L.$$

Intersecting our ideals with $\mathcal{O}_K$ gives $\prod_S \mathfrak{p}_{ij} = \prod_{S'} \mathfrak{p}_{ij}$, which means that $S = S'$ by unique factorization into prime ideals. □

The current approach to investigating lengths and number of factorizations has primarily been through block and type monoids [6, Chapter 3]. Our theorem essentially gives the theory of block and type monoids in the case of rings of integers of number fields. In particular it can be used to provide new proofs of many known results in the theory of nonunique factorizations. Here we just illustrate the most basic example of Carlitz's result.

If n is a nonzero nonunit in $\mathcal{O}_K$ and $n = \prod \alpha_i$, where each α_i (not necessarily distinct) is a (nonunit) irreducible of $\mathcal{O}_K$, then we say that the number of α_i's occurring in this product (with multiplicity) is the *length* of this factorization.

Corollary 5 ([3])**.** *Let K be a number field. Every irreducible factorization of n in $\mathcal{O}_K$ has the same length for all nonzero nonunits $n \in \mathcal{O}_K$ if and only if $h_K \leq 2$.*

Proof. It is immediate from the theorem (or Proposition 2) that if $h_K \leq 2$, then every irreducible factorization of an element must have the same length. Suppose $h_K > 2$.

First suppose $\mathcal{C}l_K$ has an element $\mathfrak{C}$ of order $e > 2$. Then let $\mathfrak{p} \in \mathfrak{C}$ and $\mathfrak{q} \in \mathfrak{C}^{-1}$ be prime ideals of $\mathcal{O}_K$. Let $n \in \mathcal{O}_K$ such that $(n) = \mathfrak{p}^e\mathfrak{q}^e$. Then one irreducible factorization of n corresponds to the grouping $(n) = (\mathfrak{p}\mathfrak{q})(\mathfrak{p}\mathfrak{q})\cdots(\mathfrak{p}\mathfrak{q})$, which has length $e > 2$. Another irreducible factorization of n corresponds to the grouping $(n) = (\mathfrak{p}^e)(\mathfrak{q}^e)$, which has length 2.

Otherwise $\mathcal{C}l_K$ has at least three elements $\mathfrak{C}_1$, $\mathfrak{C}_2$ and $\mathfrak{C}_3 = \mathfrak{C}_1\mathfrak{C}_2$ of order 2. Let $\mathfrak{p}_i \in \mathfrak{C}_i$ be a prime ideal of $\mathcal{O}_K$ for each $i = 1, 2, 3$. Let $n \in \mathcal{O}_K$ such that $(n) = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2$. The two different groupings $(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)$ and $(\mathfrak{p}_1^2)(\mathfrak{p}_2^2)(\mathfrak{p}_3^2)$ give irreducible factorizations of n of lengths 2 and 3. □

This proof might be considered a slight simplification, but it does not differ in any essential way from Carlitz's original proof. However, looking at this proof suggests that if $\mathcal{C}l_K \simeq \mathbb{Z}/h\mathbb{Z}$, then the ratio of the maximal length of an irreducible factorization of n to a minimal length is bounded by $\frac{h}{2}$ for any nonzero nonunit $n \in \mathcal{O}_K$. In fact this is true, and the maximum value of this ratio is called the *elasticity* ρ_K of K. More generally, the *Davenport constant* $D(\mathcal{C}l_K)$ of $\mathcal{C}l_K$ is defined to be the maximal m such that there is a product of length m which is trivial in $\mathcal{C}l_K$ but no proper subproduct is. Then the above theorem can be used to provide a new proof of the known result (e.g., see [18]) that $\rho_K = D(\mathcal{C}l_K)/2$.

Specializing to certain cases, we can obtain simple formulas for $\eta_K(n)$ or criteria on when $\eta_K(n) = 1$. A few examples were given in the case of class number 2 in the previous section. Here we give two more simple examples for arbitrary class number.

Corollary 6. *Let K be a quadratic field and $p \in \mathbb{Z}$ a rational prime. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ above p, and let m be the order of $\mathfrak{p}$ in $\mathcal{C}l_K$. If $m = 1$ or p is ramified in $K/\mathbb{Q}$, then $\eta_K(p^n) = 1$ for all $n \in \mathbb{N}$. Otherwise, $\eta_K(p^n) = \lfloor \frac{n}{m} \rfloor + 1$.*

Proof. If $m = 1$, the statement is obvious. If p is ramified, then $p\mathcal{O}_K = \mathfrak{p}^2$, and again the result is immediate from our main result. Otherwise $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, where $\bar{\mathfrak{p}} \neq \mathfrak{p}$ and $\bar{\mathfrak{p}}$ is the inverse of $\mathfrak{p}$ in $\mathcal{C}l_K$. Then any irreducible of $\mathcal{O}_K$ dividing p corresponds to one of the groupings $\mathfrak{p}\bar{\mathfrak{p}}$, $\mathfrak{p}^m$ or $\bar{\mathfrak{p}}^m$. The number of times $\mathfrak{p}^m$ appears in an irreducible grouping of $\mathfrak{p}^n\bar{\mathfrak{p}}^n$ is the same as the number of times $\bar{\mathfrak{p}}^m$ will appear. Hence the irreducible factorizations of p^n in $\mathcal{O}_K$ are determined by the number of $\mathfrak{p}^m$'s which appear in an irreducible grouping of $\mathfrak{p}^n\bar{\mathfrak{p}}^n$. □

We remark that in [10], Halter-Koch showed that for any number field K and $x \in \mathcal{O}_K$ (or more generally a Krull monoid), $\eta_K(x^n) = An^d + O(n^{d-1})$ for some $A \in \mathbb{Q}$ and $d \in \mathbb{Z}$.

Corollary 7. *Let K be a number field and $\mathfrak{C} \in \mathcal{C}l_K$ be an ideal class of order m. Suppose $n \in \mathcal{O}_K$ such that $(n) = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_k$, where the $\mathfrak{p}_i$'s are distinct prime ideals in $\mathfrak{C}$. Then $\eta_K(n)$ is the number of partitions of $\{1, 2, \ldots, k\}$ into subsets of size m, i.e., $\eta_K(n) = \frac{k!}{(m!)^{k/m}(k/m)!}$.*

This is immediate from our main result and is a generalization of Corollary 3.

4. Explicit factorizations in quadratic fields

As we pointed out earlier, the approach via quadratic forms in Section 2 in some sense gives the irreducible factorizations of an element of $\mathcal{O}_K$ in a more explicit fashion. Specifically, one does not know *a priori* the elements α_{ij} occurring in

Theorem 1 explicitly. Therefore one might ask in what generality can one apply the prinicipalization argument from Section 2 using quadratic forms. First we must restrict to the case of quadratic fields.

From now on, unless otherwise stated, let Δ be a fundamental discriminant and $K = \mathbb{Q}(\sqrt{\Delta})$ be the quadratic field of discriminant Δ. Suppose $Q(x, y) = ax^2 + bxy + cy^2$ is a primitive quadratic form of discriminant Δ. Then $Q(x, y)$ factors into linear factors

$$Q(x,y) = ax^2 + bxy + cy^2 = \left(\sqrt{a}x + \frac{b+\sqrt{\Delta}}{2\sqrt{a}}y\right)\left(\sqrt{a}x + \frac{b-\sqrt{\Delta}}{2\sqrt{a}}y\right) \tag{2}$$

over $K' = K(\sqrt{a})$. Clearly $\sqrt{a} \in \mathcal{O}_{K'}$. On the other hand, $\beta^{\pm} = \frac{b\pm\sqrt{\Delta}}{2\sqrt{a}} \in \mathcal{O}_{K'}$ if and only if the norm $N_{K'/K}(\beta^{\pm})$ and trace $\mathrm{Tr}_{K'/K}(\beta^{\pm})$ lie in $\mathcal{O}_K$.

Note that $K' = K$ if and only if $a = m^2$ or $a = m^2\Delta$ for some $m \in \mathbb{Z}$. The latter is not possible since Q is primitive. The former implies that $\beta^{\pm} \in \mathcal{O}_{K'} = \mathcal{O}_K$ if and only if $a = 1$.

Suppose $K' \neq K$ and write $\mathrm{Gal}(K'/K) = \{1, \sigma\}$. Then $\sigma(\beta^{\pm}) = -\beta^{\pm}$, so we always have $\mathrm{Tr}_{K'/K}(\beta^{\pm}) = 0 \in \mathcal{O}_K$. On the other hand, $N(\beta^{\pm}) = \frac{b(b\pm\sqrt{\Delta})}{2a} - c$, which lies in $\mathcal{O}_K$ if and only if $b|a$. If $b|a$, then $Q(x, y)$ is called *ambiguous.* Hence we have shown

Lemma 1. *Let $Q(x, y) = ax^2 + bxy + cy^2$ be a primitive form of discriminant Δ. Then Q factors into integral linear forms in $\mathbb{Q}(\sqrt{\Delta}, \sqrt{a})$ if and only if Q is ambiguous.*

In other words, we can use the factorization of a quadratic form to principalize the corresponding ideal class if and only if the quadratic form is ambiguous. This makes sense because an ideal class corresponds to an ambiguous form if and only if it has order ≤ 2 in the class group. On the other hand, the linear factorization of a binary quadratic form always happens over a quadratic extension, but one needs to use an extension of degree m to principalize an ideal class of order m in $\mathcal{C}l_K$.

To see this last assertion, suppose $\mathfrak{a}$ is an ideal of order m in $\mathcal{C}l_K$, so that $\mathfrak{a}^m = (\alpha)$. If L principalizes $\mathfrak{a}$, say $\mathfrak{a}\mathcal{O}_L = (\beta)$, then $\beta^m\mathcal{O}_L = \alpha\mathcal{O}_L$. Hence $\sqrt[m]{u\alpha} \in \mathcal{O}_L$ for some unit $u \in \mathcal{O}_K$. No k-th root of $u\alpha$ is contained in K for $1 \neq k|m$ since $\mathfrak{a}$ has order m. Therefore $m|[L : K]$.

We now set up our notation for the statement and proof of the main result of this section. Let $\mathfrak{I}$ be the class of principal ideals in $\mathcal{C}l_K$, and $\mathfrak{C}_1, \ldots, \mathfrak{C}_k$ be the ideal classes in $\mathcal{C}l_K$ of order 2. We assume $k \geq 1$.

If $Q(x, y) = ax^2 + bxy + cy^2$ is primitive of discriminant Δ, we define the ideal in $\mathcal{O}_K$ corresponding to Q to be $(a, \frac{b-\sqrt{\Delta}}{2})$. We will say that two forms are (weakly) equivalent if their corresponding ideals are equivalent, so that the equivalence classes of forms form a group isomorphic to $\mathcal{C}l_K$. It is easy to see that Q and $-Q$ correspond to the same ideal if Q is ambiguous.

Let $Q_j(x, y) = a_jx^2 + b_jxy + c_jy^2$ be an ambiguous form corresponding to an ideal in $\mathfrak{C}_j$. Set $K_j = K(\sqrt{a_j})$ and $L = K_1K_2 \cdots K_k$.

Lemma 2. *K_j is a principalization field for $\mathfrak{C}_j$. Hence L is a principalization field for $\mathfrak{C}_1, \ldots, \mathfrak{C}_k$.*

Proof. Let $\mathfrak{a}$ be the ideal of $\mathcal{O}_K$ corresponding to Q_j, and $\bar{\mathfrak{a}}$ be its conjugate. One easily checks that $\bar{\mathfrak{a}} = \mathfrak{a}$ and $\mathfrak{a}^2 = (a_j)$. Thus $\mathfrak{a}\mathcal{O}_{K_j} = (\sqrt{a_j})^2$. Since $\mathfrak{a} \in \mathfrak{C}_j$, K_j principalizes any ideal in $\mathfrak{C}_j$. □

Though we do not need this for the proposition below, it would be decent of us to determine the structure of L/K. This follows from the following.

Lemma 3. *Let $Q(x,y) = ax^2+bxy+cy^2$ and $R(x,y) = dx^2+exy+fy^2$ be primitive ambiguous forms of discriminant Δ. Let $\mathfrak{a} = (a, \frac{b-\sqrt{\Delta}}{2})$ and $\mathfrak{b} = (d, \frac{e-\sqrt{\Delta}}{2})$ be the ideals of $\mathcal{O}_K$ corresponding to Q and R. Then $K(\sqrt{a}) = K(\sqrt{d})$ implies that $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent.*

Proof. Write $b = ra$ and $e = sd$. Note that $b^2 - 4ac = \Delta$ then implies $a|\Delta$. Since Δ is either squarefree or 4 times a squarefree number, we have that a is either squarefree, 2 times a squarefree number or 4 times a squarefree number. On the other hand, if $4|a$, then $16|b^2-4ac = \Delta$, which is not possible. Hence a is squarefree. Similarly d is a squarefree divisor of Δ.

For any squarefree $n|\Delta$ and $m \in \mathbb{Z}$, we have $\sqrt{m} \in K(\sqrt{n})$ if and only if $m = a, \frac{\Delta}{a}, \Delta, \frac{\Delta}{4a}$ or $\frac{\Delta}{4}$. Set $\Delta' = \frac{\Delta}{4}$ if $4|\Delta$ and $\Delta' = \Delta$ otherwise. Thus $K(\sqrt{a}) = K(\sqrt{d})$ if and only if $d = a$ or $d = \frac{\Delta'}{a}$.

First suppose $d = a$. Note that dividing $r^2a^2 - 4ac = s^2a^2 - 4af$ by a implies that $r^2a \equiv s^2a \mod 4$, which implies that $r \equiv s \mod 2$ since $4 \nmid a$. But this means that the ideals $\mathfrak{a} = (a, \frac{ra-\sqrt{\Delta}}{2})$ and $\mathfrak{b} = (a, \frac{sa-\sqrt{\Delta}}{2})$ are in fact equal.

If $d = \frac{\Delta'}{a}$, we may replace $R(x,y)$ with the equivalent form $R(y,-x)$, thus interchanging d and f, and negating e. This means that both e and f are now divisible by $\frac{\Delta'}{a}$, so d cannot be by primitivity. This means that d must be $\pm a$, which we have just dealt with. (If $d = -a$, we can replace R by $-R$, which corresponds to the same ideal.) □

We remark that this lemma gives the following well-known result.

Corollary 8. *If $\mathcal{C}l_K$ contains a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$, then Δ has at least $r+1$ distinct prime divisors.*

Proof. Since there must be at least 2^r pairwise equivalent ambiguous forms $a_ix^2 + b_ixy + c_iy^2$ of discriminant Δ, the above lemma and its proof imply that the a_i's and $\frac{\Delta}{a_i}$'s are distinct divisors of Δ. Each a_i is always squarefree, and if $\frac{\Delta}{a_i}$ is not squarefree, then $\frac{\Delta}{4a_i}$ is, and it is distinct from the other divisors. Thus Δ has at least 2^{r+1} distinct squarefree divisors, so it must have at least $r+1$ distinct prime factors. □

One could refine this had we been using the notion of proper equivalence classes of quadratic forms, which we do not need for our purpose. Precisely, if r is maximal so that $\mathcal{C}l_K$ contains a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$, then one can show that there are either $r+1$ or $r+2$ distinct prime divisors of Δ. The first case occurs when the extended genus field of K equals the genus field of K, and the second when they are different. (See, e.g., [15].)

However, our interest in the previous lemma is in the structure of L/K (which is closely related to the genus field and extended genus field of K, but different from both in general). We know that $\{\mathfrak{I}, \mathfrak{C}_1, \ldots, \mathfrak{C}_k\}$ is the subgroup of $\mathcal{C}l_K$ generated by all elements of order 2. We put r such that $2^r = k+1$ so that this subgroup is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$.

Corollary 9. *L is an abelian extension of K of degree 2^r and $\mathrm{Gal}(L/K) \simeq (\mathbb{Z}/2\mathbb{Z})^r$.*

Proof. Clearly $[L : K] \leq 2^r$ and is a power of 2 by construction. Moreover L/K is Galois and the Galois group is an elementary abelian 2-group because L is obtained from K by adjoining square roots of K. By the previous lemma, L/K has $2^r - 1$ subextensions of degree 2 over K, so $[L : K] = 2^r$. □

Proposition 3. *Let $n = \prod p_i^{d_i} \prod q_{jk}^{e_{jk}} \prod r_\ell^{f_\ell} \in \mathbb{N}$, where the p_i's are primes in $\mathbb{N}$ represented by the principal form $Q_0(x,y) = x^2 + b_0xy + c_0y^2$ of discriminant Δ, the q_{jk}'s are primes in $\mathbb{N}$ represented by Q_j and the r_ℓ's are primes in $\mathbb{N}$ not represented by any form of discriminant Δ. Write each $p_i = Q_0(u_i, v_i)$ and $q_{jk} = Q_j(x_{jk}, y_{jk})$ for $u_i, v_i, x_{jk}, y_{jk} \in \mathbb{Z}$. Let*

$$\alpha_i^\pm = u_i + \frac{b_0 \pm \sqrt{\Delta}}{2} v_i$$

and

$$\beta_{jk}^\pm = \sqrt{a}_j x_{jk} + \frac{b_j \pm \sqrt{\Delta}}{2\sqrt{a_j}} y_{jk}.$$

Then the irreducible factorizations of n in $\mathcal{O}_K$, up to units, are precisely given by the $\mathcal{O}_K$-irreducible groupings of the factorization

$$n = \prod_i (\alpha_i^+ \alpha_i^-)^{d_i} \prod_{jk} (\beta_{jk}^+ \beta_{jk}^-)^{e_{jk}} \prod r_\ell^{f_\ell}$$

in $\mathcal{O}_L$.

By an *$\mathcal{O}_K$-irreducible grouping* of a product $\prod \gamma$ in $\mathcal{O}_L$, we of course mean a grouping of the terms such that the product of each group of terms is (up to a unit of $\mathcal{O}_L$) an irreducible in $\mathcal{O}_K$. In the above proposition, each $\alpha_i^\pm$ and r_ℓ is already an irreducible of $\mathcal{O}_K$, and the elements $\beta_{jk}^\pm$ correspond to the ideal class $\mathfrak{C}_j$. A product of these $\beta_{jk}^\pm$'s is, up to a unit of $\mathcal{O}_L$, an irreducible in $\mathcal{O}_K$ if and only if the corresponding product of ideal classes is trivial but no proper subproduct is. In fact, such a product of $\beta_{jk}^\pm$'s must actually be an irreducible of $\mathcal{O}_K$, since the fact that $\beta_{jk}^\pm \in \sqrt{a_j}K$ implies that such a product lies in $\mathcal{O}_K$.

Proof. It is obvious that any prime p_i represented by Q_0 satisfies $p_i\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ for some principal prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of $\mathcal{O}_K$, since Q_0 factors over K. Further any prime q_{jk} represented by Q_j satisfies $q_{jk}\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ for some prime ideals $\mathfrak{q}_1, \mathfrak{q}_2 \in \mathfrak{C}_j$ (see [1, p. 143]). Lastly each r_ℓ is inert in $K/\mathbb{Q}$. Now apply Theorem 1. □

The above gives a complete answer for the factorization of rational integers n in $\mathcal{O}_K$ when $\mathcal{C}l_K \simeq (\mathbb{Z}/2\mathbb{Z})^r$, i.e., when there is one class per genus in the form class group, and a partial answer for other quadratic fields. We end with two examples and some remarks on principalization fields.

Example 1. Let $\Delta = -87$. Then $K = \mathbb{Q}(\sqrt{-87})$ has class number $h_K = 6$. The principal form is $Q_0(x,y) = x^2 + xy + 22y^2$ and there is one other ambiguous form up to equivalence, $Q_1(x,y) = 3x^2 + 3xy + 8y^2$. Let $n = 14145 = 3 \cdot 5 \cdot 23 \cdot 41$. We see that $3 = Q_1(1,0)$, $\left(\frac{-87}{5}\right) = -1$, so 5 is not represented by a form of discriminant Δ, $23 = Q_0(1,1)$ and $41 = Q_1(1,2)$. Let

$$\alpha^{\pm} = 1 + \frac{1 \pm \sqrt{-87}}{2} = \frac{3 \pm \sqrt{-87}}{2}, \beta_1 = \sqrt{3},$$
$$\beta_2^{\pm} = \sqrt{3} + 2\frac{3 \pm \sqrt{-87}}{2\sqrt{3}} = 2\sqrt{3} \pm \sqrt{-29}.$$

Then the irreducible factorizations of n in $\mathcal{O}_K$ are given by the $\mathcal{O}_K$-irreducible groupings of the factorization

$$n = \alpha^{+}\alpha^{-}\beta_1^2\beta_2^{+}\beta_2^{-} \cdot 5$$

in $\mathcal{O}_L$, where $L = K(\sqrt{3})$. Specifically, $\eta_K(n) = 2$ and the factorizations are

$$(\alpha^{+})(\alpha^{-})(\beta_1^2)(\beta_2^{+}\beta_2^{-})5 = \frac{3+\sqrt{-87}}{2} \cdot \frac{3-\sqrt{-87}}{2} \cdot 3 \cdot 41 \cdot 5,$$
$$(\alpha^{+})(\alpha^{-})(\beta_1\beta_2^{+})(\beta_1\beta_2^{-})5 = \frac{3+\sqrt{-87}}{2} \cdot \frac{3-\sqrt{-87}}{2}(6+\sqrt{-87})(6-\sqrt{87}) \cdot 5.$$

Example 2. Let $\Delta = -21$. Then $K = \mathbb{Q}(\sqrt{-21})$ has class group $\mathcal{C}l_K \simeq (\mathbb{Z}/2\mathbb{Z})^2$. We take for our ambiguous forms the principal form $Q_0(x,y) = x^2 + 21y^2$, $Q_1(x,y) = 2x^2 + 2xy + 11y^2$, $Q_2(x,y) = 3x^2 + 7y^2$ and $Q_3(x,y) = 14x^2 + 14xy + 5y^2$. (Note that all of these are reduced, except for Q_3, which is equivalent to the reduced form $5x^2 + 4xy + 5y^2$.)

A prime $p \in \mathbb{N}$ is represented by Q_0 if $p \equiv 1, 25, 37 \mod 84$, by Q_1 if $p = 2$ or $p \equiv 11, 23, 71 \mod 84$, by Q_2 if $p = 3, 7$ or $p \equiv 19, 31, 55 \mod 84$, and by Q_3 if $p \equiv 5, 17, 41 \mod 84$.

Let $n = 46189 = 11 \cdot 13 \cdot 17 \cdot 19$, so $2 = Q_1(1,0)$, $11 = Q_1(0,1)$, 13 is not represented by a form of discriminant Δ, $17 = Q_3(1,-3)$ and $19 = Q_2(2,1)$. Set

$$\beta_1^{\pm} = \frac{2 \pm 2\sqrt{-21}}{2\sqrt{2}} = \frac{1 \pm \sqrt{-21}}{\sqrt{2}},$$
$$\beta_2^{\pm} = 2\sqrt{3} \pm \sqrt{-7},$$
$$\beta_3^{\pm} = \sqrt{14} - 3 \cdot \frac{14 \pm 2\sqrt{-21}}{2\sqrt{14}} = \frac{-\sqrt{7} \pm 3\sqrt{-3}}{\sqrt{2}}.$$

Then the irreducible factorizations of n in $\mathcal{O}_K$ are given by the $\mathcal{O}_K$-irreducible groupings of the factorization

$$n = \beta_1^{+}\beta_1^{-}\beta_2^{+}\beta_2^{-}\beta_3^{+}\beta_3^{-} \cdot 13$$

in $\mathcal{O}_L$, where $L = K(\sqrt{2}, \sqrt{3}, \sqrt{14})$. Precisely, there are $\eta_K(n) = 5$ of them and they are $13(\beta_1^{+}\beta_1^{-})(\beta_2^{+}\beta_2^{-})(\beta_3^{+}\beta_3^{-}) = 13 \cdot 11 \cdot 19 \cdot 17$, $13(\beta_1^{+}\beta_2^{+}\beta_3^{+})(\beta_1^{-}\beta_2^{-}\beta_3^{-})$, $13(\beta_1^{+}\beta_2^{+}\beta_3^{-})(\beta_1^{-}\beta_2^{-}\beta_3^{+})$, $13(\beta_1^{+}\beta_2^{-}\beta_3^{+})(\beta_1^{-}\beta_2^{+}\beta_3^{-})$, and $13(\beta_1^{+}\beta_2^{-}\beta_3^{-})(\beta_1^{-}\beta_2^{+}\beta_3^{+})$.

Final remarks. In the case that K is a quadratic field with class group $\mathcal{C}l_K \simeq (\mathbb{Z}/2\mathbb{Z})^r$, we have constructed a principalization field L which is Galois over K and $\mathrm{Gal}(L/K) \simeq \mathcal{C}l_K$. Further, L is unramified outside of any primes dividing 2Δ. In fact, by using $K_j = K(\sqrt{-a_j})$ instead of $K(\sqrt{a_j})$ when $a_j \equiv 3 \mod 4$, we can ensure that $L = \prod K_j$ is unramified outside of any (finite) primes dividing Δ. Moreover, this is not equal to the Hilbert class field H of K in general, as our earlier example of $K = \mathbb{Q}(\sqrt{5})$ shows. (It is of course closely related to H, and more generally to the genus field of K.)

In general for a number field K it is natural to ask, what can we say about the minimal abelian extensions L which principalize K? By the remarks after Lemma 1, we know that $m|[L : K]$ for every cyclic group of order m contained in $\mathcal{C}l_K$. One might be tempted to posit that $[L : K] \geq h_K$, or even that $\mathrm{Gal}(L/K)$ contains $\mathcal{C}l_K$, but this turns out to be false. For instance, the Hilbert class field H of K is an abelian extension of K with $\mathrm{Gal}(L/K) \simeq \mathcal{C}l_K$ and always principalizes K, but proper subextensions of H may also principalize K ([12], [13], [14]). We will not survey the literature on principalization, but refer to the expositions [16], [17] and [19], as well as point out the recent works [8] and [2] which study extensions of K not contained in Hilbert class field H.

Acknowledgements

We would like to thank Daniel Katz for helpful comments and for suggesting the use of formal power series. We also appreciate the comments provided by the referee after a careful reading of the manuscript.

References

[1] Borevich, A. I.; Shafarevich, I. R. Number theory. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20, Academic Press, New York-London, 1966. MR0195803 (33:4001)

[2] Bosca, Sébastien. Principalization of ideals in abelian extensions of number fields. (English summary), Int. J. Number Theory 5 (2009), no. 3, 527–539. MR2529089 (2010d:11127)

[3] Carlitz, L. A characterization of algebraic number fields with class number two. Proc. Amer. Math. Soc. 11 (1960), 391–392. MR0111741 (22:2603)

[4] Chapman, Scott T.; Herr, Jeremy; Rooney, Natalie. A factorization formula for class number two. J. Number Theory 79 (1999), no. 1, 58–66. MR1724253 (2001d:11105)

[5] Fogels, E. Zur arithmetik quadratischer Zahlenkörper. (German. Latvian summary), Univ. Riga. Wiss. Abh. Kl. Math. Abt. 1 (1943), 23–47. MR0022231 (9:175g)

[6] Geroldinger, Alfred; Halter-Koch, Franz. Non-unique factorizations. Algebraic, combinatorial and analytic theory. Pure and Applied Mathematics (Boca Raton), 278. Chapman & Hall/CRC, Boca Raton, FL, 2006. MR2194494 (2006k:20001)

[7] Geroldinger, Alfred; Halter-Koch, Franz. Non-unique factorizations: a survey. Multiplicative ideal theory in commutative algebra, 207–226, Springer, New York, 2006. MR2265810 (2007h:20065)

[8] Gras, Georges. Principalisation d'idéaux par extensions absolument abéliennes. (French. English summary) [Principalization of ideals by absolutely abelian extensions], J. Number Theory 62 (1997), no. 2, 403–421. MR1432784 (98j:11087)

[9] Halter-Koch, Franz. Chebotarev formations and quantitative aspects of nonunique factorizations. Acta Arith. 62 (1992), no. 2, 173–206. MR1183988 (93m:11119)

[10] Halter-Koch, Franz. On the asymptotic behaviour of the number of distinct factorizations into irreducibles. Ark. Mat. 31 (1993), no. 2, 297–305. MR1263556 (94m:11128)

[11] Halter-Koch, Franz. Non-unique factorizations of algebraic integers. Funct. Approx. Comment. Math. 39 (2008), part 1, 49–60. MR2490087 (2009m:11185)

[12] Heider, Franz-Peter; Schmithals, Bodo. Zur Kapitulation der Idealklassen in unverzweigten primzyklischen Erweiterungen. (German) [The capitulation of ideal classes in unramified prime-cyclic extensions], J. Reine Angew. Math. 336 (1982), 1–25. MR671319 (84g:12002)

[13] Iwasawa, Kenkichi. A note on capitulation problem for number fields. Proc. Japan Acad. Ser. A Math. Sci. 65 (1989), no. 2, 59–61. MR1010815 (90k:11136)

[14] Iwasawa, Kenkichi. A note on capitulation problem for number fields. II. Proc. Japan Acad. Ser. A Math. Sci. 65 (1989), no. 6, 183–186. MR1011867 (90k:11139)

[15] Janusz, Gerald J. Algebraic number fields. Second edition. Graduate Studies in Mathematics, 7. American Mathematical Society, Providence, RI, 1996. MR1362545 (96j:11137)

[16] Jaulent, J.-F. L'état actuel du problème de la capitulation. (French) [The current state of the capitulation problem], Séminaire de Théorie des Nombres, 1987–1988, Exp. No. 17, 33 pp., Univ. Bordeaux I, Talence.

[17] Miyake, Katsuya. On the capitulation problem. Hey, class field theory is waking up. Sugaku Expositions 1 (1988), no. 2, 175–194. MR855006 (88j:11081)

[18] Narkiewicz, Wladyslaw. Elementary and analytic theory of algebraic numbers. Third edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004. MR2078267 (2005c:11131)

[19] Suzuki, Hiroshi. On the capitulation problem. Class field theory—its centenary and prospect (Tokyo, 1998), 483–507, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001. MR1846474 (2002k:11207)

Department of Mathematics, University of Oklahoma, Norman, Oklahoma 73011
E-mail address: kmartin@math.ou.edu