

About Number Fields with Pólya Group of Order ≤ 2

David Adam and Jean-Luc Chabert

Abstract Carlitz characterized the number fields K with class number ≤ 2 by the equality of the lengths of all the factorizations of every integer of K into irreducible elements. Analogously, we study the links between the order of the Pólya group $\mathcal{P}o(K)$ of a number field K and the factorizations into irreducible elements of some rational numbers. Our main results concern quadratic fields where we prove some equivalences between, on the one hand, $|\mathcal{P}o(K)| = 1$ and uniqueness of factorizations, on the other hand, $|\mathcal{P}o(K)| = 2$ and uniqueness of lengths of factorizations. We also show how analogous results may be formulated in the case of function fields.

1 Introduction

Let K be a number field. Denote its ring of integers by \mathcal{O}_K and its class group by $\mathcal{C}l(K)$. If the group $\mathcal{C}l(K)$ is trivial it means that \mathcal{O}_K is a principal ideal domain. As \mathcal{O}_K is a Dedekind domain, to be a principal ideal domain is equivalent to be a unique factorization domain. From this point of view, Carlitz [4] proved in a very short paper the following result which says that, to weaken the hypothesis by allowing $\mathcal{C}l(K)$ to have not one but two elements is equivalent to weaken the factorization property in \mathcal{O}_K in the following way:

Theorem 1 (Carlitz) *The class number of a number field K is ≤ 2 if and only if, for every integer x of K , all the factorizations of x into irreducible elements of \mathcal{O}_K have the same length.*

We are interested here in a subgroup of $\mathcal{C}l(K)$ called the Pólya group of K . Let us recall its definition.

D. Adam

GAATI, Université de la Polynésie Française, BP 6570, 98702 Faa'a, Tahiti, French Polynesia
e-mail: david.adam@upf.pf

J.-L. Chabert (✉)

LAMFA CNRS-UMR 7352, Université de Picardie, 80039 Amiens, France
e-mail: jean-luc.chabert@u-picardie.fr

Notation. If an integer q is the norm of at least one maximal ideal of \mathcal{O}_K , we denote by $\Pi_q(K)$ the ideal product of all maximal ideals of \mathcal{O}_K with norm q

$$\Pi_q(K) = \prod_{\substack{\mathfrak{m} \in \text{Max}(\mathcal{O}_K) \\ N_{K/\mathbb{Q}}(\mathfrak{m})=q}} \mathfrak{m}. \quad (1)$$

Definition 1 [3, Sect. II.3] The *Pólya group* of K is the subgroup $\mathcal{P}o(K)$ of the class group $\mathcal{C}l(K)$ of K generated by the classes of all the ideals $\Pi_q(K)$ defined by Formula (1).

The Pólya group could also be defined as the subgroup of the class group generated by the classes of Bhargava's factorial ideals (which are defined in [2]).

The idea for this article comes from a remark by Jesse Elliott: the hypothesis $\text{Card}(\mathcal{C}l(K)) \leq 2$ corresponds to an interesting property, it could also be the case for the similar hypothesis $\text{Card}(\mathcal{P}o(K)) \leq 2$. Noticing that the Pólya group of K is trivial, if and only if, for every $n \in \mathbb{N}$, the \mathcal{O}_K -module

$$\text{Int}_n(\mathcal{O}_K) = \{f \in \text{Int}(\mathcal{O}_K) \mid \deg(f) \leq n\}$$

is free [15, 16], Elliott [7] suggests the following conjecture:

Conjecture. For every number field K , if $\text{Card}(\mathcal{P}o(K)) \leq 2$, then

$$\overline{\lim}_{N \rightarrow +\infty} \frac{1}{N} \text{Card}\{n \leq N \mid \text{Int}_n(\mathcal{O}_K) \text{ is free}\} \geq \frac{1}{2}.$$

For our part, always with the assumption $\text{Card}(\mathcal{P}o(K)) \leq 2$, returning to the spirit of the result of Carlitz, we consider the factorizations of rational integers into irreducible elements of \mathcal{O}_K , because there are natural links between the rational integers and the ideals $\Pi_q(K)$ whose classes generate $\mathcal{P}o(K)$. We will see that we have to exclude the prime numbers which are decomposed in the extension K/\mathbb{Q} .

Recall that a prime number p is said to be *decomposed* in the number field K if there are at least two prime ideals of the ring of integers \mathcal{O}_K lying over p . Consequently, the prime p is *undecomposed* in K if and only if $p\mathcal{O}_K$ is a primary ideal of \mathcal{O}_K , that is, is a power of a maximal ideal of \mathcal{O}_K .

In Sect. 2, we prove that $|\mathcal{P}o(K)| = 1$ (resp., $|\mathcal{P}o(K)| \leq 2$) implies the uniqueness of the factorization (resp., of the length of the factorizations) into irreducible elements of \mathcal{O}_K of all products of undecomposed primes numbers (Theorem 2). In Sect. 3, we study the obstructions for the converses of the previous assertions. In Sect. 4, we obtain characterizations in the particular case of Galois number fields of odd prime degree. In Sect. 5, we obtain equivalences for quadratic number fields (Theorems 3 and 4). Finally, in the last section, we end with some analogous results in the function fields case.

2 The Hypothesis $\text{Card}(\mathcal{P}o(K)) \leq 2$

In this section, we describe consequences of the hypothesis $\text{Card}(\mathcal{P}o(K)) \leq 2$. We consider rational integers m which are product of primes which are themselves undecomposed in the extension K/\mathbb{Q} and the factorizations of these rational integers m into irreducible elements of \mathcal{O}_K .

Theorem 2 *Let K be a number field. We denote its ring of integers by \mathcal{O}_K and its Pólya group by $\mathcal{P}o(K)$. Let m be any rational integer which is a product of undecomposed primes.*

1. *If $|\mathcal{P}o(K)| = 1$, then the factorization of m into irreducible elements of \mathcal{O}_K is unique.*
2. *If $|\mathcal{P}o(K)| \leq 2$, then all the factorizations of m into irreducible elements of \mathcal{O}_K have the same length.*

Let us be precise: in ‘a product of primes’ the primes are not necessarily distinct, and ‘the uniqueness of a factorization’ in \mathcal{O}_K is always up to units of \mathcal{O}_K and up to the order of the elements in the product.

Proof Note first that, if the prime p is undecomposed in the extension K/\mathbb{Q} and if \mathfrak{p} denotes the unique prime ideal of \mathcal{O}_K lying over p , then

$$p\mathcal{O}_K = \mathfrak{p}^e, \quad [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p] = f \quad \text{where} \quad ef = [K : \mathbb{Q}], \quad \text{and} \quad \mathfrak{p} = \Pi_{p^f}(K).$$

Now, let

$$m = p_1^{h_1} \cdots p_k^{h_k}$$

where, for $i = 1, \dots, k$, the prime p_i lies under a unique maximal ideal \mathfrak{p}_i of \mathcal{O}_K . Let

$$p_i\mathcal{O}_K = \mathfrak{p}_i^{e_i} \quad \text{with} \quad e_i \geq 1.$$

Then,

$$m\mathcal{O}_K = \mathfrak{p}_1^{h_1 e_1} \cdots \mathfrak{p}_k^{h_k e_k}. \quad (2)$$

By hypothesis on m , the ideals \mathfrak{p}_i are the ideals $\Pi_{p_i}(K)$.

1- Assume that $|\mathcal{P}o(K)| = 1$ (in this case, K is called a *Pólya field* [20]). Then, the ideals $\mathfrak{p}_i = \Pi_{p_i}(K)$ are principal and $\mathfrak{p}_i = \pi_i\mathcal{O}_K$ where π_i is an irreducible element of \mathcal{O}_K . Consequently, $p_i\mathcal{O}_K = \pi_i^{e_i}\mathcal{O}_K$, that is, $p_i = u_i\pi_i^{e_i}$ where u_i is a unit in \mathcal{O}_K . Finally,

$$m = u\pi_1^{h_1 e_1} \cdots \pi_k^{h_k e_k} \quad \text{where} \quad u \in \mathcal{O}_K^\times.$$

If π is an irreducible element of \mathcal{O}_K which divides m , then

$$\pi\mathcal{O}_K = \prod_{j \in J} \mathfrak{p}_j^{\gamma_j} = \prod_{j \in J} \pi_j^{\gamma_j} \mathcal{O}_K \quad \text{where} \quad J \subseteq \{1, \dots, k\} \quad \text{and} \quad 1 \leq \gamma_j \leq h_j e_j.$$

The irreducibility of π implies the existence of some index $j \in \{1, \dots, k\}$ such that $\pi \mathcal{O}_K = \mathfrak{p}_j = \pi_j \mathcal{O}_K$, that is, such that π and π_j are associated. One may easily conclude by iteration that the factorization of m is unique.

2- Assume that $|\mathcal{P}o(K)| \leq 2$. Then, for each i , either the ideal \mathfrak{p}_i is principal, or the ideal \mathfrak{p}_i^2 is principal. Let π be an irreducible of \mathcal{O}_K which divides m and consider the factorization of the ideal $\pi \mathcal{O}_K$ in a product of maximal ideals of \mathcal{O}_K . If in this factorization there is an ideal \mathfrak{p}_i which is principal, then necessarily $\pi \mathcal{O}_K = \mathfrak{p}_i$. Otherwise, there are at least two maximal ideals (not necessarily distinct) \mathfrak{p}_i and \mathfrak{p}_j which are not principal and the hypothesis on $\mathcal{P}o(K)$ implies that $\mathfrak{p}_i \mathfrak{p}_j$ is principal, and hence, necessarily $\pi \mathcal{O}_K = \mathfrak{p}_i \mathfrak{p}_j$.

Finally, the number of irreducible elements which appear in the factorization of m may be computed in the following way: if ν denotes the number of principal ideals \mathfrak{p}_i which appear in the right hand side of Eq.(2) taking into account their multiplicity and if μ denotes the number of nonprincipal ideals \mathfrak{p}_i still taking into account their multiplicity, then the number of irreducible elements in a factorization of m is necessarily $\nu + \frac{1}{2}\mu$, which is a fixed integer for a given m .

The following examples show that we cannot admit decomposed primes in Theorem 2, neither when $|\mathcal{P}o(K)| = 1$, nor when $|\mathcal{P}o(K)| \leq 2$.

Example 1 Let $K = \mathbb{Q}(\sqrt{-31})$. We know that $|\mathcal{P}o(K)| = 1$ (see for instance [3, Corollary II.4.5]). On the other hand, $5\mathcal{O}_K = \mathfrak{p}\mathfrak{q}$ where \mathfrak{p} and \mathfrak{q} are not principal (there are no integers of \mathcal{O}_K with norm 5). Consequently, 5 is irreducible in \mathcal{O}_K and the order of the classes of \mathfrak{p} and \mathfrak{q} is 3 (the class number of K is 3). In other words, $\mathfrak{p}^3 = \pi \mathcal{O}_K$ and $\mathfrak{q}^3 = \pi' \mathcal{O}_K$ where π and π' are irreducible. Finally, we have

$$5^3 \mathcal{O}_K = \pi \pi' \mathcal{O}_K$$

with 3 irreducible elements on the left side and 2 on the right side.

Example 2 Even in the cyclotomic case, one has to exclude the decomposed primes. For instance, let $K = \mathbb{Q}(\zeta_{39})$ where $\zeta_{39} = e^{2i\pi/39}$. Then, $\mathcal{P}o(K)$ is trivial as for every cyclotomic number field [20, Proposition 2.6]. Let us consider the factorization of 13 in \mathcal{O}_K : $e_{K/\mathbb{Q}}(13) = 12$ and $f_{K/\mathbb{Q}}(13) = 1$ since $13 \equiv 1 \pmod{3}$, and hence,

$$13 \mathcal{O}_K = (\mathfrak{q}\mathfrak{q}')^{12}.$$

We show now that the ideals \mathfrak{q} and \mathfrak{q}' are not principal by considering the containments $\mathbb{Q} \subset \mathbb{Q}(\sqrt{-39}) \subset K$. For instance, if \mathfrak{q} were a principal ideal, then the ideal

$$N_{K/\mathbb{Q}(\sqrt{-39})}(\mathfrak{q}) = (\mathfrak{q} \cap \mathcal{O}_{\mathbb{Q}(\sqrt{-39})})^{f_{K/\mathbb{Q}(\sqrt{-39})}(\mathfrak{q})} = \mathfrak{q} \cap \mathcal{O}_{\mathbb{Q}(\sqrt{-39})},$$

which is the prime ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{-39})}$ lying over 13, would be principal, but it is not. On the other hand, $h_K = 2$, and hence, $\mathfrak{q}^2 = \pi \mathcal{O}_K$, $\mathfrak{q}'^2 = \pi' \mathcal{O}_K$, $\mathfrak{q}\mathfrak{q}' = \sigma \mathcal{O}_K$, and π, π', σ are irreducible elements of \mathcal{O}_K . The equality $(\mathfrak{q}\mathfrak{q}')^2 = \mathfrak{q}^2 \mathfrak{q}'^2$ leads to two distinct factorizations $\sigma^2 \mathcal{O}_K = \pi \pi' \mathcal{O}_K$.

3 Toward Reciprocal Assertions

Note that the uniqueness of the factorization (resp., the uniqueness of the length of the factorizations) of the products of undecomposed primes is equivalent to the uniqueness of the factorization (resp., the length of the factorizations) of the products of undecomposed primes which are (at least partially) ramified.

Indeed, an undecomposed prime p which is not ramified is totally inert, and hence, $p\mathcal{O}_K$ is a prime ideal, which means that p is not only an irreducible element of \mathcal{O}_K , but it is a prime element of \mathcal{O}_K . Consequently, if such an element p appears in some factorization of an integer m , necessarily it appears in all the factorizations of m .

3.1 Counterexamples

The converse of both implications in Theorem 2 are false as shown by the following examples of quadratic fields.

Example 3 The field $K = \mathbb{Q}(\sqrt{-5})$ is an example of a non-Pólya field whereas the factorizations are unique. The ramified primes are 2 and 5. Let $2\mathcal{O}_K = \mathfrak{p}^2$ and $5\mathcal{O}_K = \mathfrak{q}^2$. Then, $\mathfrak{q} = \sqrt{-5}\mathcal{O}_K$ while \mathfrak{p} is not principal. Consequently, on the one hand 2 is irreducible in \mathcal{O}_K , on the other hand $\mathcal{P}o(K)$ is not trivial. Let us prove the uniqueness of the factorization of every product $m = p_1 \dots p_k$ of undecomposed primes. As previously said, we may assume for our proof that all the p_i 's are ramified, that is, that the product is of the form $m = 2^a 5^b$. Clearly, m admits the unique factorization $2^a (\sqrt{-5})^{2b}$.

Example 4 The field $K = \mathbb{Q}(\sqrt{-21})$ is an example where $|\mathcal{P}o(K)| = 4$ while the factorizations have the same length. The ramified primes are 2, 3, and 7. Let

$$2\mathcal{O}_K = \mathfrak{p}^2, \quad 3\mathcal{O}_K = \mathfrak{q}^2 \text{ and } 7\mathcal{O}_K = \mathfrak{r}^2. \quad (3)$$

The ideals \mathfrak{p} , \mathfrak{q} , and \mathfrak{r} are not principal. Consequently, 2, 3, and 7 are irreducible elements of \mathcal{O}_K . Since the field K is not real, we know with Hilbert [12] that the relations between the classes of \mathfrak{p} , \mathfrak{q} , and \mathfrak{r} are all given by relations (3) and by

$$\mathfrak{q}\mathfrak{r} = \sqrt{-21}\mathcal{O}_K. \quad (4)$$

The Pólya group of K which is generated by the classes of \mathfrak{p} , \mathfrak{q} , and \mathfrak{r} is then of order 4. Let us prove that all the factorizations of every product $m = p_1 \dots p_k$ of undecomposed primes have the same length. We still assume that all the p_i 's are ramified, and hence, that $m = 2^a 3^b 7^c$. Then, one has

$$m\mathcal{O}_K = 2^a 3^b 7^c \mathcal{O}_K = \mathfrak{p}^{2a} \mathfrak{q}^{2b} \mathfrak{r}^{2c}.$$

The only irreducibles which can divide m are 2, 3, 7 and $\sqrt{-21}$, and hence, the factorizations of m into irreducible elements are of the form $m = u 2^\alpha 3^\beta 7^\gamma \sqrt{-21}^\delta$ where $u \in \mathcal{O}_K^\times$, $\alpha = a$, $2\beta + \delta = 2b$ and $2\gamma + \delta = 2c$. Consequently, $\alpha + \beta + \gamma + \delta = a + b + c$ and the lengths of all the factorizations of m are equal.

These examples show that the hypotheses $|\mathcal{P}o(K)| = 1$ and $|\mathcal{P}o(K)| \leq 2$ are too strong.

3.2 Nontrivial Relations in $\mathcal{P}o(K)$

The following notation will be used in the sequel.

Notation. Denote by p_1, \dots, p_t the prime numbers which are undecomposed and ramified in the extension K/\mathbb{Q} , and by $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ the corresponding prime ideals of \mathcal{O}_K lying over these p_j . For $1 \leq j \leq t$, we have $p_j \mathcal{O}_K = \mathfrak{p}_j^{e_j}$ where $e_j = e_{K/\mathbb{Q}}(p_j)$ and $|\mathcal{O}_K/\mathfrak{p}_j| = p_j^{f_j}$ where $f_j = f_{K/\mathbb{Q}}(p_j)$. Clearly, $e_j \times f_j = [K : \mathbb{Q}]$.

Since $\mathfrak{p}_j = \Pi_{p_j}(K)$, we are interested in the relations between the classes $\bar{\mathfrak{p}}_j$ of the \mathfrak{p}_j 's in $\mathcal{P}o(K)$. Finally, denote by ε_j the order of $\bar{\mathfrak{p}}_j$. Clearly, ε_j divides e_j and $\mathfrak{p}_j^{e_j} = \pi_j \mathcal{O}_K$ where π_j is an irreducible element of \mathcal{O}_K . The relation $\bar{\mathfrak{p}}_j^{\varepsilon_j} = 1$ in $\mathcal{P}o(K)$ will be said to be *trivial* and we introduce the following definition:

Definition 2 We say that there is a *non-trivial relation* in $\mathcal{P}o(K)$ between the classes $\bar{\mathfrak{p}}_j$ if there exists a sequence $\alpha_1, \dots, \alpha_t$ of integers such that

$$\mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_t^{\alpha_t} = y \mathcal{O}_K \quad (5)$$

for some $y \in \mathcal{O}_K$, where $0 \leq \alpha_j < \varepsilon_j$, and where at least two α_j are nonzero. Moreover, we say that such a nontrivial relation is *minimal* if there is no other nontrivial relation with exponents β_j such that $0 \leq \beta_j \leq \alpha_j$ with $\beta_{j_0} < \alpha_{j_0}$ for at least one j_0 .

Proposition 1 *The factorization into irreducible elements of every product of undecomposed primes is unique if and only if there is no nontrivial relation between the classes $\bar{\mathfrak{p}}_j$.*

Proof Assume that there exists a nontrivial relation of the form (5). Clearly, $\alpha_j \neq 0$ implies that the ideal \mathfrak{p}_j is not principal, that is, $\varepsilon_j \neq 1$. Let us prove that $m = \prod_{j=1}^t p_j^{\frac{n}{\varepsilon_j} \alpha_j}$ where $n = [K : \mathbb{Q}]$ admits two distinct factorizations. First,

$$m \mathcal{O}_K = \prod_{j=1}^t p_j^{\frac{n}{\varepsilon_j} \alpha_j} \mathcal{O}_K = \prod_{j=1}^t \mathfrak{p}_j^{n \times \alpha_j} = y^n \mathcal{O}_K.$$

Using a factorization of y , we will obtain a factorization for m in product of irreducible elements whose exponents are nonzero multiples of n .

On the other hand, we have the equality

$$m\mathcal{O}_K = \prod_{j=1}^t (\mathfrak{p}_j^{\varepsilon_j})^{\frac{n}{\varepsilon_j}\alpha_j} = \left(\prod_{j=1}^t \pi_j^{\frac{n}{\varepsilon_j}\alpha_j} \right) \mathcal{O}_K.$$

Assume, for instance, that $\alpha_1 \neq 0$, and hence, that $1 \leq \alpha_1 < \varepsilon_1$. Then, we have another factorization of m where the exponent of π_1 is $< n$.

Conversely, assume that there is no nontrivial relation. Then, the only irreducible elements which can divide $m = p_1^{h_1} \dots p_t^{h_t}$ are the π_j 's. Thus, we have the uniqueness of the factorization of m .

Proposition 2 *The lengths of the factorizations into irreducible elements of every product of undecomposed primes are equal if and only if, for every minimal nontrivial relation of the form (5), we have*

$$\sum_{j=1}^t \frac{\alpha_j}{\varepsilon_j} = 1. \quad (6)$$

Proof Assume that there exists a nontrivial relation of the form (5) and consider such a minimal relation. Then, $\mathfrak{p}_1^{\alpha_1} \mathfrak{p}_2^{\alpha_2} \dots \mathfrak{p}_t^{\alpha_t} = y\mathcal{O}_K$ and the minimality of the relation implies the irreducibility of y . With the notation of the previous proof, we have

$$m\mathcal{O}_K = y^n \mathcal{O}_K = \left(\prod_{j=1}^t \pi_j^{\frac{n}{\varepsilon_j}\alpha_j} \right) \mathcal{O}_K.$$

The uniqueness of the length of the factorizations implies equality (6).

Conversely, assume that every minimal nontrivial relation of the form (5) satisfies equality (6). Let us consider these relations

$$\mathfrak{p}_1^{\alpha_{1,k}} \mathfrak{p}_2^{\alpha_{2,k}} \dots \mathfrak{p}_t^{\alpha_{t,k}} = \sigma_k \mathcal{O}_K \quad (1 \leq k \leq s)$$

where the elements σ_k are irreducible in \mathcal{O}_K . Let $m = p_1^{h_1} \dots p_t^{h_t}$. The only irreducible elements which can divide m are the π_j 's ($1 \leq j \leq t$) and the σ_k 's ($1 \leq k \leq s$). From

$$m\mathcal{O}_K = \prod_{j=1}^t \mathfrak{p}_j^{\beta_j} = \prod_{j=1}^t \pi_j^{\gamma_j} \times \prod_{k=1}^s \sigma_k^{\delta_k} \mathcal{O}_K,$$

we deduce:

$$\beta_j = h_j e_j = \varepsilon_j \gamma_j + \sum_{k=1}^s \alpha_{j,k} \delta_k \quad (1 \leq j \leq t).$$

Thus,

$$\sum_{j=1}^t \frac{\beta_j}{\varepsilon_j} = \sum_{j=1}^t h_j \frac{e_j}{\varepsilon_j} = \sum_{j=1}^t \gamma_j + \sum_{k=1}^s \left(\sum_{j=1}^t \frac{\alpha_{j,k}}{\varepsilon_j} \right) \delta_k = \sum_{j=1}^t \gamma_j + \sum_{k=1}^s \delta_k$$

which shows that the number of irreducible elements in the factorization, that is, $\sum_j \gamma_j + \sum_k \delta_k$ is a constant equal to $\sum_j h_j \frac{e_j}{\varepsilon_j}$ which depends only on m .

3.3 Factorizations in Monoids

While our aim was to emphasize on the group $\mathcal{P}o(K)$ and, in the spirit of Carlitz' theorem, to find links with factorizations of rational integers, the previous propositions show that we have the uniqueness of factorizations or of the lengths of the factorizations only by considering relations between the classes of the ramified primes which are not decomposed. As the classes of ramified primes which are decomposed may take part to the group $\mathcal{P}o(K)$, we understand that the sufficient conditions $|\mathcal{P}o(K)| = 1$ or $|\mathcal{P}o(K)| \leq 2$ may be not necessary for the uniqueness.

Let us consider for a while the question of the uniqueness from the point of view of the factorization theory in commutative monoids (see [8]). We said that the Pólya group is generated by the classes of the ideals $\Pi_q(K)$ (given by formula (1)). Let us consider the ideals $\Pi_q(K)$ themselves, they generate a free submonoid of the monoid of nonzero ideals of \mathcal{O}_K , and the undecomposed ramified primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ (which are some particular ideals $\Pi_q(K)$) generate a smaller free submonoid F :

$$F = \{\mathfrak{p}_1^{\beta_1} \cdots \mathfrak{p}_t^{\beta_t} \mid \beta_1, \dots, \beta_t \in \mathbb{N}\}.$$

Now we introduce the following submonoid of the monoid $\mathcal{O}_K^* = \mathcal{O}_K \setminus \{0\}$:

$$H = \{\alpha \in \mathcal{O}_K^* \mid \alpha \mathcal{O}_K \in F\}$$

As H is divisor-closed [$\forall \alpha \in H \forall \beta \in \mathcal{O}_K (\beta | \alpha \Rightarrow \beta \in H)$], the factorization of an element $\alpha \in H$ into irreducible elements of \mathcal{O}_K is the same as the factorization into irreducible elements of H . Recall that the monoid H is said to be factorial if the factorization of every element of H into irreducible elements of H is unique up to the units. Then, we may formulate a stronger version of Proposition 1

Proposition 3 *The monoid H is factorial if and only if there is no nontrivial relation between the classes $\bar{\mathfrak{p}}_j$.*

The fact that the condition is necessary follows from Proposition 1, while the proof of the fact that the condition is sufficient is similar to those given in the proof of Proposition 1. We can made analogous remarks with respect to Proposition 2.

Recall that the monoid H is said to be half-factorial if the factorizations of every element of H into irreducible elements have the same length.

Proposition 4 *The monoid H is half-factorial if and only if relation (6) is satisfied by every minimal nontrivial relation of the form (5).*

Proof Let $G_0 = \{\bar{p}_1, \dots, \bar{p}_r\} \subseteq \mathcal{Cl}(K)$ and let $\mathcal{B}(G_0)$ be the block monoid of G_0 , that is, the free abelian monoid formed by the sums $\beta_1 \bar{q}_1 + \dots + \beta_r \bar{q}_r$ (where $\bar{q}_1, \dots, \bar{q}_r$ denote the distinct elements of G_0) such that $\bar{q}_1^{\beta_1} \dots \bar{q}_r^{\beta_r} = 1$. Clearly, the canonical homomorphism of monoids $H \rightarrow \mathcal{B}(G_0)$ is surjective; in fact it is a transfer homomorphism. Thus, H is half-factorial if and only if $\mathcal{B}(G_0)$ is half-factorial and, by Zacks-Skula theorem, $\mathcal{B}(G_0)$ is half-factorial if and only if every irreducible block in $\mathcal{B}(G_0)$ has cross-number 1 (see [8, Proposition 6.7.3]), this is just relation (6).

Putting together Propositions 1 and 3 on the one hand, and Propositions 2 and 4 on the other hand, we have:

Corollary 1 *Let K be a number field. The following assertions are equivalent:*

- (i) *For every rational integer m which is not a multiple a prime number decomposed in \mathcal{O}_K , the factorization (resp., the lengths of the factorizations) of m into irreducible elements of \mathcal{O}_K is unique (resp., are equal).*
- (ii) *For every algebraic integer α of \mathcal{O}_K not contained in a prime ideal of K lying over a decomposed prime number, the factorization (resp., the lengths of the factorizations) of α into irreducible elements of \mathcal{O}_K is unique (resp., are equal).*

Proof In fact, this corollary is obvious. Let H_0 denote the submonoid of H formed by the rational integers which are product of undecomposed primes. The corollary says that H is factorial (resp., half-factorial) if and only if H_0 is factorial (resp., half-factorial). This is a clear consequence of the fact that $H_0 \subset H$ and, for each $\alpha \in H$, $\alpha^{[K:\mathbb{Q}]}$ is in H_0 .

3.4 Tame Ramification

Back to classical algebraic number theory, we consider now a case where there does exist a nontrivial relation. Noticing that in both examples of Sect. 3.1, the prime 2 is ramified with ramification index 2, we may try to exclude this case by assuming that ramifications are tame, that is, no ramified prime divides one of its ramification indices. With such an hypothesis and assuming moreover that the extension K/\mathbb{Q} is Galois, we know that the different δ_K of K is equal to

$$\delta_K = \prod_{\mathfrak{p} \in \text{Max}(\mathcal{O}_K)} \mathfrak{p}^{e_{K/\mathbb{Q}}(\mathfrak{p})-1} = \prod_{j=1}^w \Pi_j^{e_j-1} = \prod_{j=1}^w p_j \times \prod_{j=1}^w \Pi_j^{-1} \quad (7)$$

where p_1, \dots, p_w denotes the ramified primes in the extension K/\mathbb{Q} and Π_1, \dots, Π_w the corresponding ideals $\Pi_q(K)$, that is the products of the maximal ideals of \mathcal{O}_K lying over p_j . As a consequence, we have

Proposition 5 *Let K be a Galois number field with tame ramifications. The ideal $\prod_{j=1}^w \Pi_j$ is principal if and only if the different δ_K is principal. This is the case, in particular, either if the \mathbb{Z} -algebra \mathcal{O}_K is monogenic, or if the exponent of $\mathcal{P}o(K)$ is ≤ 2 .*

Proof The fact that $\prod_{j=1}^w \Pi_j$ is principal if and only if δ_K is principal is an obvious consequence of (7). Assume first that the \mathbb{Z} -algebra \mathcal{O}_K is monogenic, that is, that \mathcal{O}_K is of the form $\mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. Then, the ideal δ_K is principal since $\delta_K = f'(\alpha) \mathcal{O}_K$ where f denotes the minimal polynomial of α over \mathbb{Q} .

Assume now that the exponent of $\mathcal{P}o(K)$ is ≤ 2 . We know that the class of δ_K in the class group $\mathcal{C}l(K)$ is a square (see [19, Chap. XIII, Theorem 13]). As, by (7), the class of δ_K belongs to $\mathcal{P}o(K)$, we may conclude.

In order to be able to obtain links between the equivalences given by Propositions 1 and 2 and conditions on the Pólya group, we have to avoid the ramified primes which are decomposed. Thus, we restrict our study to Galois number fields K of prime degree.

4 Galois Number Fields of Prime Degree

From now on, we assume that K is a Galois number field of prime degree l . Then, every prime p is either totally ramified, or totally inert, or totally decomposed. Consequently, if p is ramified, $p\mathcal{O}_K = \mathfrak{p}^l$ and $\Pi_p(K) = \mathfrak{p}$ is maximal; if p is decomposed, $p\mathcal{O}_K = \mathfrak{p}_1 \dots \mathfrak{p}_l = \Pi_p(K)$ and $\Pi_p(K)$ is principal; and if p is inert, $p\mathcal{O}_K = \mathfrak{p}$, and $\Pi_p(K)$ is both maximal and principal. As we do not want to consider decomposed primes p , we only have to consider ideals $\Pi_q(K)$ which are maximal. Moreover, if p is inert, p is a prime element of \mathcal{O}_K , thus it cannot lead to distinct factorizations of products of undecomposed primes. Thus, we have

Lemma 1 *If K is a Galois number field of prime degree l , the following assertions are equivalent:*

- (i) *For every rational integer which is a product of undecomposed primes, the factorization (resp., the length of the factorizations) into irreducible elements of \mathcal{O}_K is unique.*
- (ii) *For every rational integer whose radical divides the discriminant d_K of K , the factorization (resp., the length of the factorizations) into irreducible elements of \mathcal{O}_K is unique.*

About the Pólya group, we have the following:

Proposition 6 *Let K be a Galois number field of prime degree l . Then,*

$$|\mathcal{P}o(K)| = \begin{cases} 2^{t-2} & \text{if } l = 2, K \subset \mathbb{R}, N_{K/\mathbb{Q}}(\mathcal{O}_K^\times) = \{+1\} \\ l^{t-1} & \text{otherwise} \end{cases} \quad (8)$$

where t denotes the number of ramified primes.

Proof Recall that, in a cyclic extension K/\mathbb{Q} of degree n where there are t ramified primes p_1, \dots, p_t with ramification indices e_1, \dots, e_t , the order of the Pólya group satisfies

$$|\mathcal{P}o(K)| = \frac{\prod_{i=1}^t e_i}{n} \text{ or } \frac{\prod_{i=1}^t e_i}{2n} \quad (\text{cf. [5, Corollary 3.11]})$$

and the second equality occurs exactly when K is real and $N_{K/\mathbb{Q}}(\mathcal{O}_K^\times) = \{+1\}$. Here, we may conclude since the ramification indices are necessarily equal to l .

We denote by p_1, \dots, p_t the primes which are ramified in the extension K/\mathbb{Q} and by $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ the corresponding prime ideals of \mathcal{O}_K . Clearly, $\mathfrak{p}_j \mathcal{O}_K = \mathfrak{p}_j^l$ for $1 \leq j \leq t$. The following morphism is well defined and surjective:

$$\varphi : (\overline{k_1}, \dots, \overline{k_t}) \in (\mathbb{Z}/l\mathbb{Z})^t \mapsto \overline{\mathfrak{p}_1}^{k_1} \cdots \overline{\mathfrak{p}_t}^{k_t} \in \mathcal{P}o(K). \quad (9)$$

If $l \neq 2$, it follows from Proposition 6 that $\text{Ker}(\varphi)$ is of order l . Consequently,

Corollary 2 *If K is a Galois number field of odd prime degree l , then one and only one of the following assertions holds: either the kernel of the morphism φ defined in (9) is generated by one class $\overline{\mathfrak{p}_j}$, that is, \mathfrak{p}_j is principal (and this is the only ramified prime ideal which is principal), or $\text{Ker}(\varphi)$ is generated by a nontrivial relation.*

Proposition 7 *Let K be a Galois number field of odd prime degree l . The following assertions are equivalent:*

- (i) *Every rational integer which is a product of undecomposed primes admits a unique factorization into irreducible elements of \mathcal{O}_K .*
- (ii) *There is a ramified prime ideal of \mathcal{O}_K which is principal.*

Proof By Proposition 1, assertion (i) is equivalent to the nonexistence of nontrivial relation between the $\overline{\mathfrak{p}_j}$ and, by Corollary 2, this nonexistence is equivalent to the existence of a principal ramified prime ideal.

Corollary 3 *Let K be a Galois number field of odd prime degree l . Assume that the prime l is not ramified in K and that the different δ_K is a principal ideal. Then, the following assertions are equivalent:*

- (i) *Every product of undecomposed primes admits a unique factorization into irreducible elements of \mathcal{O}_K .*
- (ii) $|\mathcal{P}o(K)| = 1$.

Here the fact that $|\mathcal{P}o(K)| = 1$ is equivalent to the fact that there is only one ramified prime.

Proof (i) \Rightarrow (ii): The ramifications are tame since we assume that l is not ramified, then, by Proposition 5, the ideal $\mathfrak{p}_1 \dots \mathfrak{p}_t$ is principal. By Proposition 1, if (i) holds, this relation is trivial, that is, all the ramified prime ideals \mathfrak{p}_j are principal. (In fact, by Corollary 2, there is exactly one ramified prime.)

(ii) \Rightarrow (i) follows from Theorem 2.

Example 5 Following [6, Theorem 6.4.6], the field $K = \mathbb{Q}(\theta)$ where θ is a root of the equation

$$X^3 - 57X + 19 = 0$$

is a cyclic cubic field where the ramified primes are 3 and 19. Clearly, θ is a generator of the prime ideal \mathfrak{p} lying over 19. This is an example where we have the uniqueness of the factorizations (cf. Proposition 7) while K is not a Pólya field (cf. Proposition 6).

Proposition 8 *Let K be a Galois number field of odd prime degree l . The following assertions are equivalent:*

- (i) *All the factorizations into irreducible elements of \mathcal{O}_K of a rational integer which is a product of undecomposed primes have the same lengths.*
- (ii) *Either there is a ramified prime ideal which is principal, or there is a nontrivial relation between the classes of ramified prime ideals of the form $\bar{\mathfrak{p}}_1^{\alpha_1} \dots \bar{\mathfrak{p}}_t^{\alpha_t} = 1$ with $\alpha_j \geq 0$ where $\sum_{j=1}^t \alpha_j = l$.*

Proof By Corollary 2, either there is a ramified prime ideal which is principal, or there is a nontrivial relation between the classes of ramified prime ideals. In this latter case, by Proposition 2, if (i) holds, such a minimal nontrivial relation satisfies $\sum_j \frac{\alpha_j}{\varepsilon_j} = 1$, which means here $\sum_j \alpha_j = l$.

Conversely, assume that (ii) holds. Taking into account Proposition 7, we may assume that the ideals \mathfrak{p}_i are not principal, and hence, that there is a relation $\mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_t^{\alpha_t} = w\mathcal{O}_K$ with $\alpha_j \geq 0$ where $\sum_{j=1}^t \alpha_j = l$. Clearly, this nontrivial relation is minimal and, by Proposition 2, (i) holds.

Corollary 4 *Let K be a Galois number field of odd prime degree l . Assume that l is not ramified and that the different δ_K is principal. The following assertions are equivalent:*

- (i) *All the factorizations into irreducible elements of \mathcal{O}_K of a rational integer which is a product of undecomposed primes have the same lengths.*
- (ii) $|\mathcal{P}o(K)| = 1$ or l^{l-1} or, equivalently, there are 1 or l ramified primes in K .

Proof This is an obvious consequence of Propositions 5 and 8.

Unfortunately, following [11], there are very few number fields K of prime degree l such that \mathcal{O}_K is monogenic. In particular, the only cyclic number fields of prime degree $l \geq 5$ are real subfields of cyclotomic fields. More precisely, if l is a Sophie

Germain's prime, that is, if l and $2l + 1$ are primes, the real subfield $\mathbb{Q}(\cos \frac{2\pi}{2l+1})$ of the cyclotomic field $\mathbb{Q}(e^{\frac{2\pi i}{2l+1}})$ is of degree l and its ring of integers $\mathbb{Z}[\cos \frac{2\pi}{2l+1}]$ is monogenic. We know that in this case $|\mathcal{P}o(\mathbb{Q}(\cos \frac{2\pi}{2l+1}))| = 1$ [20, Proposition 2.6].

On the other hand, there exist infinite families of cyclic cubic number fields whose ring of integers is monogenic (see [10]) and, of course, the ring of integers of every quadratic number field is monogenic.

5 Quadratic Number Fields

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field where d is a square-free integer. What about the converses of the implications in Theorem 2?

Let p_1, \dots, p_s be the prime numbers which divide d . The ramified primes are p_1, \dots, p_s , and 2 in the case where $d \equiv 3 \pmod{4}$. From $d = \pm p_1 \dots p_s$, we have $\sqrt{d}\mathcal{O}_K = \mathfrak{p}_1 \dots \mathfrak{p}_s$, which is a nontrivial relation between the \mathfrak{p}_j 's if and only if there are nonprincipal prime ideals dividing $d\mathcal{O}_K$. This leads us to introduce the following notation:

Notation. In this section, $\mathcal{P}o^*(K)$ denotes the subgroup of $\mathcal{P}o(K)$ generated by the classes of the \mathfrak{p}_j 's which divide d .

Theorem 3 *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field where d is a square-free integer. The following assertions are equivalent:*

- (i) *Every product of undecomposed primes admits a unique factorization into irreducible elements of \mathcal{O}_K .*
- (ii) *\mathcal{O}_K has at most one ramified prime ideal which is not principal.*
- (iii) *$|\mathcal{P}o^*(K)| = 1$.*

Proof Assume that (i) holds. Then, by Proposition 1, there is no nontrivial relation. Consequently, the relation $\sqrt{d}\mathcal{O}_K = \mathfrak{p}_1 \dots \mathfrak{p}_s$ implies that all the prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ are principal, that is, $|\mathcal{P}o^*(K)| = 1$. Thus, (i) implies (iii).

Clearly, (iii) implies (ii) since all the ramified primes divide d except when $d \equiv 3 \pmod{4}$: 2 is ramified and the corresponding prime ideal may be nonprincipal.

Finally, assume that (ii) holds. Then, all the prime ideals \mathfrak{p}_j dividing d are principal: $\mathfrak{p}_j = \pi_j\mathcal{O}_K$ where π_j is a prime element in \mathcal{O}_K . If $d \equiv 3 \pmod{4}$, 2 is ramified and the corresponding prime ideal may be nonprincipal, in this case 2 is an irreducible element of \mathcal{O}_K . Thus, if m denotes an integer whose radical divides the discriminant d_K of K ($d_K = d$ or $4d$), then all the irreducible elements of \mathcal{O}_K dividing m are prime elements except in the case where 2 is irreducible. Consequently, (i) holds.

Note that the field $\mathbb{Q}(\sqrt{-5})$ studied in Counterexample 3 corresponds to this case where 2 is irreducible in \mathcal{O}_K .

Theorem 4 *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field where d is a square-free integer. The following assertions are equivalent:*

- (i) All the factorizations into irreducible elements of \mathcal{O}_K of any product of undecomposed primes have the same lengths.
- (ii) Either $|\mathcal{P}o^*(K)| \leq 2$, or $|\mathcal{P}o^*(K)| = 4$ and there is a product of two ramified prime ideals which is a principal ideal.

Proof We first recall Formula (8) in the case of quadratic number fields:

$$|\mathcal{P}o(K)| = \begin{cases} 2^{t-2} & \text{if } K \subset \mathbb{R} \text{ and } N_{K/\mathbb{Q}}(\mathcal{O}_K^\times) = \{+1\} \\ 2^{t-1} & \text{otherwise} \end{cases}$$

where t denotes the number of ramified primes (see [12, Sect. 73] or [3, Sect. II.4]). Recall also that we have

$$d = \pm p_1 \dots p_s \text{ with } p_i \mathcal{O}_K = \mathfrak{p}_i^2.$$

First case: $|\mathcal{P}o(K)| = 2^{t-1}$

The relations between the classes of the \mathfrak{p}_i 's are all deduced from (see also [12, Sect. 73]):

$$\mathfrak{p}_i^2 = p_i \mathcal{O}_K \quad (1 \leq i \leq t) \text{ and } \mathfrak{p}_1 \dots \mathfrak{p}_s = \sqrt{d} \mathcal{O}_K.$$

By Proposition 2, assertion (i) means that either there is no nontrivial relation between the \mathfrak{p}_j 's, that is $s \leq 1$, or every minimal nontrivial relation satisfies (6), that is here, $s = 2$ (since $\alpha_j = 1$ and $\varepsilon_j = 2$). Finally, (i) $\Leftrightarrow s \leq 2 \Leftrightarrow |\mathcal{P}o^*(K)| \leq 2$.

Second case: $|\mathcal{P}o(K)| = 2^{t-2}$

There is another fundamental relation between the classes of the \mathfrak{p}_j 's ($1 \leq j \leq t$).

The first subcase. The prime 2 does not divide d , but is ramified and the prime ideal lying over 2 is principal. Then, the relations between the \mathfrak{p}_j ($1 \leq j \leq s$) are as in the first case and, analogously, we may conclude (i) $\Leftrightarrow s \leq 2 \Leftrightarrow |\mathcal{P}o^*(K)| \leq 2$.

The other subcase. The other relation is then between the prime ideals which divide d . Thus, by renumbering the \mathfrak{p}_i 's, it may be written (see [12, Sect. 73]):

$$\alpha \mathcal{O}_K = \mathfrak{p}_1 \dots \mathfrak{p}_r \text{ with } 1 \leq r \leq \frac{s}{2}.$$

Then, the relations between the classes of the \mathfrak{p}_i 's are all deduced from

$$\mathfrak{p}_i^2 = p_i \mathcal{O}_K \quad (1 \leq i \leq t), \quad \alpha \mathcal{O}_K = \mathfrak{p}_1 \dots \mathfrak{p}_r \text{ and } \beta \mathcal{O}_K = \mathfrak{p}_{r+1} \dots \mathfrak{p}_s.$$

By Proposition 2, assertion (i) means that either there is no nontrivial relation or each minimal nontrivial relation is a product of two prime ideals, equivalently, either $s \leq 3$, or $s = 4$ and $r = 2$. These latter assertions mean that either $|\mathcal{P}o^*(K)| = 2$, or $|\mathcal{P}o^*(K)| = 4$ and there is a product of two prime ideals which is principal.

Finally, we have proved that (i) implies (ii). To be sure that (ii) implies (i), it remains to see that the assertion ' $|\mathcal{P}o^*(K)| = 4$ and there is a product of two primes which is principal' may only occur in the second subcase. Indeed, if we are not in the

second subcase, $|\mathcal{P}o^*(K)| \leq 4$ implies $s \leq 3$. If $s = 3$, the fact that there is a product of two prime ideals which is principal implies that the third prime ideal dividing d is principal, which itself implies that $|\mathcal{P}o^*(K)| \leq 2$. Finally, $s \leq 2$ and $|\mathcal{P}o^*(K)| \leq 2$.

Note that, for the field $\mathbb{Q}(\sqrt{-21})$ studied in Example 4, we have $|\mathcal{P}o^*(K)| = 2$ while $|\mathcal{P}o(K)| = 4$. The following example shows that we may have $|\mathcal{P}o^*(K)| = 4$ with a product of two prime ideals which is principal, while $|\mathcal{P}o(K)| = 8$.

Example 6 Let $K = \mathbb{Q}(\sqrt{3 \times 7 \times 17 \times 79})$. Since $28203 \equiv 3 \pmod{4}$, one has $\mathcal{O}_K = \mathbb{Z}[\sqrt{28203}]$. The group $\mathcal{P}o^*(K)$ is generated by the classes of ideals $\mathfrak{P}_3, \mathfrak{P}_7, \mathfrak{P}_{17}$ and \mathfrak{P}_{79} where \mathfrak{P}_p denotes the prime ideal of \mathcal{O}_K above the prime p . As ± 3 and ± 79 are not quadratic residues modulo 17, the ideals \mathfrak{P}_3 and \mathfrak{P}_{79} are not principal. The equality $168^2 - 28203 \times 1^2 = 21$ implies that $\mathfrak{P}_3\mathfrak{P}_7 = (168 + \sqrt{28203})\mathcal{O}_K$ is principal. From the equality $\sqrt{28203}\mathcal{O}_K = \mathfrak{P}_3\mathfrak{P}_7\mathfrak{P}_{17}\mathfrak{P}_{79}$, one deduces that $\mathfrak{P}_{17}\mathfrak{P}_{79}$ is principal. Finally, $\mathfrak{P}_3\mathfrak{P}_{17}$ is not principal because the equality $x^2 - 28203y^2 = 51$ is impossible (modulo 4), while the equality $x^2 - 28203y^2 = -51$ is impossible (modulo 7). Then we may conclude that

$$\mathcal{P}o^*(K) = \{\overline{\mathcal{O}_K}, \overline{\mathfrak{P}_3}, \overline{\mathfrak{P}_{17}}, \overline{\mathfrak{P}_3\mathfrak{P}_{17}}\}$$

is of order 4. Moreover, since -1 is not a square modulo 3, the norm of the fundamental unit of K is 1 and, as 2 is ramified, Formula (8) gives $|\mathcal{P}o(K)| = 8$.

6 A Few Words About the Function Fields Case

Let q be a power of a prime p and $K/\mathbb{F}_q(T)$ be a finite extension of function fields. Denote the integral closure of $\mathbb{F}_q[T]$ in K by \mathcal{O}_K . Analogously to Definition 1, one defines the Pólya group of \mathcal{O}_K

Definition 3 The Pólya group of \mathcal{O}_K is the subgroup $\mathcal{P}o(\mathcal{O}_K)$ of the class group $\mathcal{C}l(\mathcal{O}_K)$ of \mathcal{O}_K generated by the classes of the ideals $\Pi_{q^r}(\mathcal{O}_K)$ defined by

$$\Pi_{q^r}(\mathcal{O}_K) = \prod_{\substack{\mathfrak{m} \in \text{Max}(\mathcal{O}_K) \\ N(\mathfrak{m}) = q^r}} \mathfrak{m}.$$

The following proposition shows that the naive function field analog of Theorem 2 does not hold.

Proposition 9 Assume that q is odd and let $\beta \in \mathbb{F}_q \setminus \mathbb{F}_q^2$.

- (1) Let $K := \mathbb{F}_q(T)[y]$ where $y^2 = \beta T(T+1)$. Then $|\mathcal{P}o(\mathcal{O}_K)| = 1$, while $T(T+1)$ admits two distinct factorizations into irreducible elements of \mathcal{O}_K .
- (2) Let $K := \mathbb{F}_q(T)[y]$ where $y^2 = \beta T(T+1)Q(T)$ and $Q(T) \in \mathbb{F}_q[T]$ is a monic irreducible polynomial of degree 2. Then $|\mathcal{P}o(\mathcal{O}_K)| = 2$, while $T(T+1)Q(T)$ admits two factorizations into irreducible elements of \mathcal{O}_K with different lengths.

Proof In both cases, the extension $K/\mathbb{F}_q(T)$ is an imaginary extension. As a consequence $\mathcal{O}_K^\times = \mathbb{F}_q^*$ (see [17]).

(1) The fact that $|\mathcal{P}o(K)| = 1$ is a consequence of [1, Theorem 12]. It follows from [18, Proposition VI.3.1] that the ramified prime ideals of \mathcal{O}_K are the ideals \mathfrak{p}_T and \mathfrak{p}_{T+1} lying over T and $T + 1$ respectively. Thus, $y\mathcal{O}_K = \mathfrak{p}_T\mathfrak{p}_{T+1}$. The ideal \mathfrak{p}_T is not principal. Indeed, assume that $\mathfrak{p}_T = \alpha\mathcal{O}_K$ with $\alpha = A + yB$ ($A, B \in \mathbb{F}_q[T]$). This implies that $A^2 - \beta T(T + 1)B^2 = vT$ where $v \in \mathbb{F}_q^*$, that is $A^2 = T(v + \beta(T + 1)B^2)$. Obviously, $B = 0$ is impossible. The comparison of the leading coefficients of both sides leads to a contradiction since $\beta \notin \mathbb{F}_q^2$. In the same way, one could show that \mathfrak{p}_{T+1} is not principal. Consequently y , T and $T + 1$ are irreducible elements of \mathcal{O}_K , and $y^2 = \beta T(T + 1)$ are two different factorizations into irreducible elements of \mathcal{O}_K .

(2) Analogously, the ramified prime ideals of \mathcal{O}_K are the ideals \mathfrak{p}_T , \mathfrak{p}_{T+1} , and \mathfrak{p}_Q lying over T , $T + 1$, and $Q(T)$ respectively. Clearly, $\mathcal{P}o(\mathcal{O}_K)$ is generated by the classes of $\mathfrak{p}_T\mathfrak{p}_{T+1}$ and of \mathfrak{p}_Q . From the equalities

$$T(T + 1)\mathcal{O}_K = \mathfrak{p}_T^2\mathfrak{p}_{T+1}^2, \quad y\mathcal{O}_K = (\mathfrak{p}_T\mathfrak{p}_{T+1})\mathfrak{p}_Q, \quad Q\mathcal{O}_K = \mathfrak{p}_Q^2,$$

one deduces that $\mathcal{P}o(\mathcal{O}_K) = \{[\mathcal{O}_K], [\mathfrak{p}_Q]\}$. As in (1), one proves that the six ideals \mathfrak{p}_T , \mathfrak{p}_{T+1} , \mathfrak{p}_Q , $\mathfrak{p}_T\mathfrak{p}_{T+1}$, $\mathfrak{p}_T\mathfrak{p}_Q$, and $\mathfrak{p}_{T+1}\mathfrak{p}_Q$ are not principal. Consequently, $T + 1$, T , Q , and y are irreducible elements of \mathcal{O}_K . The equality

$$y^2 = \beta T(T + 1)Q(T)$$

corresponds to two factorizations with different lengths.

Nevertheless, the introduction of Sect. 3 and the whole Sect. 3.2 are still true when we replace ‘prime number’ by ‘irreducible polynomial’ (in $\mathbb{F}_q[T]$). In particular, Propositions 1 and 2 still hold for any extension $K/\mathbb{F}_q(T)$. But, to go further and in order to retrieve in the function fields case other results analogous to those of the zero characteristic, we are led to consider the group of classes of ambiguous ideals instead of the Pólya group.

Definition 4 Let $K/\mathbb{F}_q(T)$ be a Galois extension with Galois group G .

1. An ideal I of \mathcal{O}_K is said to be *ambiguous* if for every $\sigma \in G$, $\sigma(I) = I$.
2. A class \mathcal{C} of $\mathcal{C}l(\mathcal{O}_K)$ is said to be *ambiguous* if, for every $\sigma \in G$, one has $\sigma(\mathcal{C}) = \mathcal{C}$, that is, for every ideal $I \in \mathcal{C}$, one has $\sigma(I) \in \mathcal{C}$.
3. A class \mathcal{C} of $\mathcal{C}l(\mathcal{O}_K)$ is said to be *strongly ambiguous* if \mathcal{C} contains an ambiguous ideal I .

One denotes by $\mathcal{A}m_{str}(K)$ the subgroup of $\mathcal{C}l(\mathcal{O}_K)$ formed by the strongly ambiguous classes.

Remark 1 1. Clearly, a strongly ambiguous class is an ambiguous class, but the converse does not hold: [21, Theorem 2] shows that in the class group of the

field $\mathbb{F}_3(T)[y]$ with $y^2 = -(T^2 + 1)(T^2 + 2T + 2)$ there exists a class that is ambiguous but not strongly ambiguous.

2. When the extension of function fields $K/\mathbb{F}_q(T)$ is Galois, the group $\mathcal{A}m_{str}(K)$ is generated by the classes of the following ideals:

$$\prod_{\substack{\mathfrak{p} \in \text{Max}(\mathcal{O}_K) \\ \mathfrak{p}|P}} \mathfrak{p} \quad (P \in \mathbb{F}_q[T] \text{ ramified in } K).$$

Then, we have the containments

$$\mathcal{P}o(K) \subseteq \mathcal{A}m_{str}(K) \subseteq \mathcal{C}l(K)$$

which may be strict, while for a Galois number field K we have

$$\mathcal{P}o(K) = \mathcal{A}m_{str}(K) \subseteq \mathcal{C}l(K).$$

Thus, from now on, we assume that the extension of function fields $K/\mathbb{F}_q(T)$ is Galois with Galois group G . Since the proofs follow closely those of the characteristic zero case, we will sketch them only. Here is an analog of Theorem 2.

Theorem 5 *Let $K/\mathbb{F}_q(T)$ be a Galois extension of function fields. Let m be a product of irreducible polynomials of $\mathbb{F}_q[T]$ which are undecomposed in the extension.*

- (1) *If $|\mathcal{A}m_{str}(K)| = 1$, the factorization of m into irreducible elements of \mathcal{O}_K is unique.*
- (2) *If $|\mathcal{A}m_{str}(K)| \leq 2$, all the factorizations of m into irreducible elements of \mathcal{O}_K have the same length.*

Proof If $P \in \mathbb{F}_q[T]$ is an irreducible polynomial which is undecomposed in the extension, then there exists only one maximal ideal \mathfrak{p} of \mathcal{O}_K lying over P , and hence, for every $\sigma \in \text{Gal}(K/\mathbb{F}_q(T))$, one has $\mathfrak{p}^\sigma = \mathfrak{p}$. The proof ends as in Theorem 2.

Now, we prove the converses of Theorem 5 for quadratic separable extensions $K/\mathbb{F}_q(T)$. In this case, the group of classes of ambiguous ideals is generated by the ramified primes of \mathcal{O}_K . Recall that a quadratic extension of function fields $K/\mathbb{F}_q(T)$ is said to be *real* if the infinite place $(\frac{1}{T})$ of $\mathbb{F}_q(T)$ is split in K . Recall also

Proposition 10 *Let $K/\mathbb{F}_q(T)$ be a quadratic extension. If t denotes the number of ramified primes in the extension, then one has*

$$|\mathcal{A}m_{str}(K)| = \begin{cases} q \text{ odd} & \begin{cases} 2^{t-2} & \text{if } K \text{ real and } N_{K/\mathbb{F}_q(T)}(\mathcal{O}_K^\times) = \mathbb{F}_q^{*2} \\ 2^{t-1} & \text{otherwise} \end{cases} \\ q \text{ even} & \begin{cases} 2^{t-1} & \text{if } K \text{ real} \\ 2^t & \text{otherwise.} \end{cases} \end{cases} \quad \begin{array}{l} \text{(see [21])} \\ \text{(see [13])} \end{array}$$

Theorem 3 about the uniqueness of the factorizations translates into the two following theorems.

Theorem 6 *If q is odd and if $K/\mathbb{F}_q(T)$ is a quadratic extension, then the following assertions are equivalent:*

- (i) *Every product of irreducible polynomials of $\mathbb{F}_q[T]$ which are undecomposed in the extension admits a unique factorization into irreducible elements of \mathcal{O}_K .*
- (ii) *All the ramified prime ideals of \mathcal{O}_K are principal.*
- (iii) *$|\mathcal{A}m_{str}(K)| = 1$.*

Proof One can write $K := \mathbb{F}_q(T)[y]$ with $y^2 = D(T)$ where $D(T) \in \mathbb{F}_q[T]$ is square-free. Assume that D owns $t \geq 2$ primes divisors P_1, \dots, P_t in $\mathbb{F}_q[T]$. The following equality holds:

$$\sqrt{D}\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_t, \quad (10)$$

where each $\mathfrak{p}_i \in \text{Max}(\mathcal{O}_K)$ divides P_i . Analog of Proposition 1 proves that (i) implies (ii). Clearly, (ii) \Leftrightarrow (iii), and (iii) \Rightarrow (i) follows from Theorem 5.

Theorem 7 *If q is even and $K/\mathbb{F}_q(T)$ is a quadratic separable extension, then the following assertions are equivalent:*

- (i) *Every product of irreducible polynomials of $\mathbb{F}_q[T]$ which are undecomposed in the extension admits a unique factorization into irreducible elements of \mathcal{O}_K .*
- (ii) *Denoting by t the number of ramified primes, either $|\mathcal{A}m_{str}(K)| = 2^t$, or $|\mathcal{A}m_{str}(K)| = 2^{t-1}$ and \mathcal{O}_K has a principal ramified prime ideal.*

Proof By Proposition 10, the equality $|\mathcal{A}m_{str}(K)| = 2^t$ is obviously equivalent to the nonexistence of trivial relations in \mathcal{O}_K . On the other hand, the equality $|\mathcal{A}m_{str}(K)| = 2^{t-1}$ holds if and only if there exists a nontrivial relation in \mathcal{O}_K or one ramified prime ideal of \mathcal{O}_K is principal.

Remark 2 Both cases may occur

(1) The field $\mathbb{F}_2(T)[y]$ with $y^2 + y = \frac{T^3+T^2+1}{T(T+1)}$ is an imaginary function field (see [13]). The ramified irreducible polynomials of $\mathbb{F}_2[T]$ are T and $T + 1$ (see [9, Chap. III]). Clearly,

$$\mathcal{A}m_{str}(K) = \{1, [\mathfrak{p}_T], [\mathfrak{p}_{T+1}], [\mathfrak{p}_T\mathfrak{p}_{T+1}]\},$$

where \mathfrak{p}_T and \mathfrak{p}_{T+1} are the primes ideals of \mathcal{O}_K above T and $T + 1$.

(2) The field $\mathbb{F}_2(T)[y]$ with $y^2 + (T + 1)^2y = T(T + 1)$ is a real function field. There is a ramified prime ideal in \mathcal{O}_K , the ideal lying over $T + 1$. Moreover $\mathcal{C}l(\mathcal{O}_K)$ is trivial (see [14]).

The uniqueness of the length of the factorizations is characterized by the following theorems:

Theorem 8 *If q is odd and $K/\mathbb{F}_q(T)$ is a quadratic extension, the following assertions are equivalent:*

- (i) *All the factorizations into irreducible elements of \mathcal{O}_K of any product of undecomposed primes of $\mathbb{F}_q[T]$ have the same lengths.*
- (ii) *Either $|\mathcal{A}m_{str}(K)| \leq 2$, or $|\mathcal{A}m_{str}(K)| = 4$ and there is a product of two ramified prime ideals which is a principal ideal.*

Proof Write $K = \mathbb{F}_q(T)[y]$ with $y^2 = D(T)$ where $D \in \mathbb{F}_q[T]$ is squarefree with prime factorization $D = P_1 \cdots P_t$. Adapting the proof of Theorem 4, Proposition 2, and Equality (10) lead to the result.

Theorem 9 *If q is even and $K/\mathbb{F}_q(T)$ is a quadratic separable extension, the following assertions are equivalent:*

- (i) *All the factorizations into irreducible elements of \mathcal{O}_K of any product of undecomposed primes of $\mathbb{F}_q[T]$ have the same lengths.*
- (ii) *Denoting by t the number of ramified prime ideals of \mathcal{O}_K , either $|\mathcal{A}m_{str}(K)| = 2^t$, or $|\mathcal{A}m_{str}(K)| = 2^{t-1}$ and there is a principal ramified prime ideal of \mathcal{O}_K or a product of two ramified prime ideals of \mathcal{O}_K which is a principal ideal.*

Proof By Theorem 7, one can assume that $|\mathcal{A}m_{str}(K)| = 2^{t-1}$ and there is no ramified principal prime ideal of \mathcal{O}_K . Since all the orders of the classes in $\mathcal{A}m_{str}(K)$ of the ramified prime ideals are equal to 2, there is a relation between the ramified prime ideals \mathfrak{p}_i ($1 \leq i \leq t$) of \mathcal{O}_K which can be written as

$$\prod_{i=1}^t [\mathfrak{p}_i]^{\alpha_i} = 1 \quad (\alpha_i \in \{0, 1\}),$$

with at least two nonzero α_i 's. By Proposition 4, if we consider such a minimal nontrivial relation, assertion (i) holds if and only if there are exactly two nonzero α_i 's.

Remark 3 Here is an example where $|\mathcal{A}m_{str}(K)| = 2^{t-1}$ and there is a product of two ramified prime ideals which is a principal ideal. Let $K := \mathbb{F}_2(T)[y]$ with $y^2 + y = \frac{1}{T(T+1)}$ (K is an elliptic field following [9]). The ramified prime ideals of \mathcal{O}_K are the primes ideals \mathfrak{p}_T and \mathfrak{p}_{T+1} above T and $T+1$, and they are not principal. Indeed, assume (for instance) that \mathfrak{p}_T is principal. Obviously $\sigma(\mathfrak{p}_T) = \mathfrak{p}_{T+1}$, where σ is the automorphism of K defined by $\sigma(y) = y$ and $\sigma(T) = T+1$. Hence \mathfrak{p}_{T+1} is also principal and $\mathcal{A}m_{str}(K) = \{1\}$. This is a contradiction. Moreover, we have $y^{-1}\mathcal{O}_K = \mathfrak{p}_T\mathfrak{p}_{T+1}$.

Acknowledgments The authors want to thank the anonymous referee who suggested to study the problem in the framework of the theory of factorization in monoids and proposed almost everything that is contained in Sect. 3.3.

References

1. D. Adam, Pólya and Newtonian function fields. *Math. Manuscr.* **126**(2), 231–246 (2008)
2. M. Bhargava, Generalized factorials and fixed divisors over subsets of a Dedekind domain. *J. Number Theory* **72**, 67–75 (1998)
3. P.-J. Cahen, J.-L. Chabert, *Integer-Valued Polynomials*, vol. 48, American Mathematical Society Surveys and Monographs (American Mathematical Society, Providence, 1997)
4. L. Carlitz, A characterization of algebraic number fields with class number two. *Proc. Am. Math. Soc.* **11**, 391–392 (1960)
5. J.-L. Chabert, Factorial groups and Pólya groups in Galoisian extensions of \mathbb{Q} , *Commutative Ring Theory and Applications*, vol. 231, Lecture Notes in Pure and Applied Mathematics (Marcel Dekker, New York, 2003), pp. 77–86
6. H. Cohen, *A Course in Computational Algebraic Number Theory* (Springer, New York, 1993)
7. J. Elliott, The probability that $\text{Int}_n(D)$ is free, *Commutative Algebra, Recent Advances in Commutative Rings, Integer-Valued Polynomials, and Polynomial Functions* (Springer, New York, 2014), pp. 133–151
8. A. Geroldinger, F. Halter-Koch, *Non-Unique Factorizations, Algebraic, Combinatorial and Analytic theory* (Chapman & Hall, Boca-Raton, 2006)
9. D. Goldschmidt, *Algebraic Functions and Projective Curves*, vol. 215, Graduate Texts in Mathematics (Springer, New York, 2002)
10. M.-N. Gras, Sur les corps cubiques cycliques dont l’anneau des entiers est monogène. *C. R. Acad. Sci. Paris Sér. A* **278**, 59–62 (1974)
11. M.-N. Gras, Non monogénéité de l’anneau des entiers des extensions cycliques de \mathbb{Q} de degré premier $l \geq 5$. *J. Number Theory* **23**, 347–353 (1986)
12. D. Hilbert, Die Theorie der algebraischen Zahlkörper. *Jahresbericht der Deutschen Mathematiker-Vereinigung* **4**(1894–95), 175–546 (1897)
13. S. Hu, Y. Li, The genus fields of Artin-Schreier extensions. *Finite Fields Appl.* **16**(4), 255–264 (2010)
14. D. Lebrigand, Real quadratic extensions of the rational function field in characteristic two, arithmetic, geometry and coding theory (AGCT 2003), *Séminaires et Congrès*, vol. 11 (2005), pp. 143–169
15. A. Ostrowski, Über ganzwertige Polynome in algebraischen Zahlkörpern. *J. reine angew. Math.* **149**, 117–124 (1919)
16. G. Pólya, Über ganzwertige Polynome in algebraischen Zahlkörpern. *J. reine angew. Math.* **149**, 97–116 (1919)
17. M. Rosen, *Number Theory in Function Fields*, vol. 210, Graduate Texts in Mathematics (Springer, New York, 2002)
18. H. Stichtenoth, *Algebraic Function Fields and Codes, Universitext* (Springer, New York, 1993)
19. A. Weil, *Basic Number Theory* (Springer, New York, 1967)
20. H. Zantema, Integer valued polynomials over a number field. *Manuscr. Math.* **40**, 155–203 (1982)
21. X. Zhang, Ambiguous classes and 2-rank of class group of quadratic function fields. *J. China Univ. Sci. Technol.* **17**(4), 425–431 (1987)

Multiplicative Ideal Theory and Factorization Theory
Commutative and Non-commutative Perspectives
Chapman, S.; Fontana, M.; Geroldinger, A.; Olberding, B.
(Eds.)
2016, XIV, 407 p. 4 illus., Hardcover
ISBN: 978-3-319-38853-3