JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Amandine LERICHE

Pólya fields, Pólya groups and Pólya extensions: a question of capitulation

Tome 23, n° 1 (2011), p. 235-249.

<http://jtnb.cedram.org/item?id=JTNB_2011__23_1_235_0>

Journal de Théorie des Nombres
de Bordeaux **23** (2011), 235-249

Pólya fields, Pólya groups and Pólya extensions: a question of capitulation

par Amandine LERICHE

Résumé. Un corps de nombres K, d'anneau des entiers $\mathcal{O}_K$, est dit de Pólya lorsque la $\mathcal{O}_K$-algèbre des polynômes à valeurs entières sur $\mathcal{O}_K$ possède une base régulière. Ces corps sont caractérisés par le fait que les idéaux caractéristiques sont principaux. Par analogie avec le problème de plongement dans un corps de nombres de classes égal à un, lorsque K n'est pas un corps de Pólya, on tente de le plonger dans un corps qui est de Pólya. Dans cet article nous étudions deux notions qui peuvent être considérées comme des mesures de l'obstruction pour un corps au fait d'être de Pólya : les extensions de Pólya L/K où les idéaux caractéristiques de K étendus à L deviennent principaux, et le groupe de Pólya qui est un sous-groupe du groupe de classes engendré par les idéaux caractéristiques.

Abstract. A number field K, with ring of integers $\mathcal{O}_K$, is said to be a Pólya field when the $\mathcal{O}_K$-algebra formed by the integer-valued polynomials on $\mathcal{O}_K$ admits a regular basis. It is known that such fields are characterized by the fact that some characteristic ideals are principal. Analogously to the classical embedding problem in a number field with class number one, when K is not a Pólya field, we are interested in the embedding of K in a Pólya field. We study here two notions which can be considered as measures of the obstruction for K to be a Pólya field: the Pólya extensions L/K where the characteristic ideals of K extended to L become principal, and the Pólya group which is the subgroup of the class group generated by the classes of the characteristic ideals.

1. The regular bases problem: Pólya fields and Pólya extensions

Let K be an algebraic number field and denote by $\mathcal{O}_K$ its ring of integers. We first recall two notions, the integer-valued polynomials and the regular basis, which were introduced by Pólya:

Definition 1.1. [12] An *integer-valued polynomial* on $\mathcal{O}_K$ is a polynomial $P \in K[X]$ such that $P(\mathcal{O}_K) \subseteq \mathcal{O}_K$.

Notations. The set formed by the integer-valued polynomials on $\mathcal{O}_K$ is an $\mathcal{O}_K$-algebra denoted by:

$$\mathrm{Int}(\mathcal{O}_K) = \{P \in K[X] \,|\, P(\mathcal{O}_K) \subseteq \mathcal{O}_K\}.$$

For each $n \in \mathbb{N}$, let $\mathfrak{I}_n(\mathcal{O}_K)$ be the subset of K formed by 0 and the leading coefficients of the polynomials in $\mathrm{Int}(\mathcal{O}_K)$ with degree n. This is a fractional ideal of $\mathcal{O}_K$ called the *characteristic ideal of index n* of $\mathcal{O}_K$ [5, Prop I.3.I].

Recall that $\mathrm{Int}(\mathcal{O}_K)$ is a free $\mathcal{O}_K$-module [5, Rem. II.3.7]: there is an $\mathcal{O}_K$-module isomorphism from $\mathrm{Int}(\mathcal{O}_K)$ onto $\oplus_{n=0}^{\infty}\mathfrak{I}_n(\mathcal{O}_K)$, consequently, $\mathrm{Int}(\mathcal{O}_K)$ is a non-finitely projective module; according to [3], it is a free module. But a basis may be difficult to describe. Thus, Pólya tried to characterize the fields K such that $\mathrm{Int}(\mathcal{O}_K)$ admits a "regular basis":

Definition 1.2. [12] A basis $(f_n)_{n\in\mathbb{N}}$ of the $\mathcal{O}_K$-module $\mathrm{Int}(\mathcal{O}_K)$ is said to be a *regular basis* if, for each n, the polynomial f_n has degree n.

There exist fields K such that $\mathrm{Int}(\mathcal{O}_K)$ has no regular basis and Zantema introduced the following definition:

Definition 1.3. [15] A number field K is said to be a *Pólya field* if the $\mathcal{O}_K$-module $\mathrm{Int}(\mathcal{O}_K)$ admits a regular basis.

Recall that $\mathrm{Int}(\mathcal{O}_K)$ has a regular basis if and only if the characteristic ideals $\mathfrak{I}_n(\mathcal{O}_K)$ are principal and we obtain a regular basis of $\mathrm{Int}(\mathcal{O}_K)$ when we choose, for each n, a polynomial f_n of $\mathrm{Int}(\mathcal{O}_K)$ with degree n whose leading coefficient generates the ideal $\mathfrak{I}_n(\mathcal{O}_K)$ [5, II.1.4]. In particular, if $\mathcal{O}_K$ is a principal ideal domain, $\mathrm{Int}(\mathcal{O}_K)$ has a regular basis. However, there exist rings of integers $\mathcal{O}_K$ which are not principal ideal domain but such that $\mathrm{Int}(\mathcal{O}_K)$ has a regular basis. For instance, that is the case for $K = \mathbb{Q}[\sqrt{-23}]$. Its class number is 3 but it is a Pólya field [5, II.4.5]. The hypothesis "K is a Pólya field" is weaker than the hypothesis "$\mathcal{O}_K$ is a principal ideal domain".

We know the classical embedding problem:

Is every number field contained in a field with class number one?

In 1964, Golod and Schafarevitch [9] gave a negative answer to this question. But, if we reformulate this question with a weaker hypothesis, here comes the natural question:

Is every number field contained in a Pólya field?

The counter-example given by Golod and Schafarevitch for the classical embedding problem (an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ with $d = 2\times3\times5\times7\times11\times13$) is not a counter-example for the embedding problem in a Pólya field since every quadratic field is contained in a cyclotomic field

which is always a Pólya field (see example 1). For a field K the embedding problem in a Pólya field L is equivalent to the following question:

Is there a field L containing K such that all the ideals $\mathfrak{I}_n(\mathcal{O}_L)$ are principal?

Recall that the Hilbert class field of an algebraic number field K is the maximal unramified abelian extension of K. We denote it by H_K. We know that the Galois group of the extension H_K/K is isomorphic to $Cl(K)$, the class group of K. Consequently, the degre $[H_K : K]$ is equal to the class number h_K of K. We also know that the ideals of $\mathcal{O}_K$ become principal by extension to $\mathcal{O}_{H_K}$ (the capitulation's theorem). In other words, for every ideal $\mathfrak{I}$ of $\mathcal{O}_K$, $\mathfrak{I}\mathcal{O}_{H_K}$ is principal. But, the ring $\mathcal{O}_{H_K}$ itself is not necessarily a principal ideal domain. By analogy, we introduce the following notion:

Definition 1.4. An extension L/K is said to be a *Pólya extension* if all the characteristic ideals $\mathfrak{I}_n(\mathcal{O}_K)$ extended to $\mathcal{O}_L$ are principal.

Remarks.
(1) If K is a Pólya field, then every extension L/K is a Pólya extension.
(2) If L/K is a Pólya extension, then every extension M of L is a Pólya extension of K.
(3) For every number field K, H_K/K is a Pólya extension.

The minimal degree of a Pólya extension of the field K could be a measure of the gap for K with being a Pólya field.

In order to justify the terminology of Pólya extension, we link its definition with integer-valued polynomials. First, we extend the previous notions:

Definitions 1.1. Let L/K be a finite extension of K.

(1) The set of *integer-valued polynomials on $\mathcal{O}_K$ relatively to $\mathcal{O}_L$* is:

$$\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L) = \{P \in L[X] \,|\, P(\mathcal{O}_K) \subseteq \mathcal{O}_L\}.$$

(2) The *characteristic ideal of index n of $\mathcal{O}_K$ relatively to $\mathcal{O}_L$* is the set $\mathfrak{I}_n(\mathcal{O}_K, \mathcal{O}_L)$ formed by the leading coefficients of the polynomials in $\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$ with degree n.

Proposition 1.1. *The $\mathcal{O}_L$-module generated by* $\mathrm{Int}(\mathcal{O}_K)$ *is equal to the set* $\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$. *In particular,*

$$\mathfrak{I}_n(\mathcal{O}_K)\,\mathcal{O}_L = \mathfrak{I}_n(\mathcal{O}_K, \mathcal{O}_L).$$

Proof. As $\mathrm{Int}(\mathcal{O}_K) \subseteq \mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$, the $\mathcal{O}_L$-module generated by $\mathrm{Int}(\mathcal{O}_K)$ is contained in $\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$. We will prove the inverse containment. In order to simplify, we note $A = \mathcal{O}_K$ and $B = \mathcal{O}_L$. Let $f \in \mathrm{Int}(A, B)$ with degree d. Let $\mathfrak{m}$ be a maximal ideal of A. As $A_{\mathfrak{m}}$ is a discrete valuation domain with a finite residue field, there exists a sequence $(a_n)_{n\in\mathbb{N}}$ in A

such that the following polynomials $(f_n)_{n\in\mathbb{N}}$ form a regular basis of the $A_{\mathfrak{m}}$-module $\mathrm{Int}(A_{\mathfrak{m}})$ [5, Thm. II.2.7]:

$$f_n(X) = \prod_{k=0}^{n-1} \frac{X - a_k}{a_n - a_k}.$$

The sequence $(f_n)_{n\in\mathbb{N}}$ is especially a basis of the L-vector space $L[X]$. Consequently, there exist $\alpha_0, \ldots, \alpha_d \in L$ such that

$$f(X) = \sum_{k=0}^{d} \alpha_k f_k(X).$$

As $f_k(a_j) \in A_{\mathfrak{m}}$ for $0 \leq j, k \leq d$, $f_k(a_j) = 0$ for $0 \leq j \leq d$, $f_k(a_k) = 1$, $f(a_j) \in B$ for $0 \leq j \leq d$, the $d+1$ coefficients α_k satisfy a system of $d+1$ linear equations whose matrix is triangular, unimodular with coefficients in $A_{\mathfrak{m}}$ and whose all the second members are in B. As a consequence, the α_k are in $B_{\mathfrak{m}}$ and the B-module $\mathrm{Int}(A, B)$ is contained in the $B_{\mathfrak{m}}$-module generated by $\mathrm{Int}(A)$. Since this happens for every maximal ideal $\mathfrak{m}$ of A, $\mathrm{Int}(A, B)$ is contained in the B-module generated by $\mathrm{Int}(A)$. □

As a consequence, we have:

Proposition 1.2. *The extension L/K is a Pólya extension if and only if the $\mathcal{O}_L$-module $\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$ has a regular basis.*

Proof. L/K is a Pólya extension if and only if the characteristic ideals $\mathfrak{I}_n(\mathcal{O}_K)$ extended to $\mathcal{O}_L$ are principal. By proposition 1.1, this is equivalent to the fact that $\mathfrak{I}_n(\mathcal{O}_K, \mathcal{O}_L)$ is principal. Analogously to $\mathrm{Int}(\mathcal{O}_K)$, $\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$ admits a regular basis if and only if the ideals $\mathfrak{I}_n(\mathcal{O}_K, \mathcal{O}_L)$ are principal. □

2. Factorial groups and Pólya groups

Here is another way of measuring the obstruction for a field K to be a Pólya field. We introduce the group of factorial ideals and the Pólya group of the field K.

Definition 2.1. The *factorial group* of K is the subgroup $Fact(K)$ of the nonzero fractional ideal group $\mathrm{I}(K)$ of $\mathcal{O}_K$ generated by the characteristic ideals of $\mathcal{O}_K$.

The factorial group is named by this way because the characteristic ideals are the inverse of the factorial ideals introduced by Bhargava [1], [2]:

$$(n!)_{\mathcal{O}_K} = \mathfrak{I}_n(\mathcal{O}_K)^{-1}.$$

Remarks. (1) For $K = \mathbb{Q}$, $(n!)_{\mathbb{Z}} = (n!)\,\mathbb{Z}$.

(2) For all $m, n \in \mathbb{N}$, the ideal $(n!)_{\mathcal{O}_K}(m!)_{\mathcal{O}_K}$ divides $((n+m)!)_{\mathcal{O}_K}$.

For every maximal ideal $\mathfrak{m}$ of $\mathcal{O}_K$, $(\mathcal{O}_K)_{\mathfrak{m}}$ is a discrete valuation domain. We denote by $v_{\mathfrak{m}}$ the corresponding valuation and by $N(\mathfrak{m})$ the norm of $\mathfrak{m}$ (which is the cardinality of the residue field $\mathcal{O}_K/\mathfrak{m}$) and we consider the arithmetic fonction $w_{\mathfrak{m}}$ defined by

$$w_{\mathfrak{m}}(n) = w_{N(\mathfrak{m})}(n) = \sum_{k=1}^{\infty} \left[\frac{n}{N(\mathfrak{m})^k} \right].$$

Remark. When $K = \mathbb{Q}$ et $\mathfrak{m} = p\mathbb{Z}$, we have

$$w_p(n) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right] = v_p(n!).$$

We find in [5] and [12] the decomposition of the characteristic ideals as a product of maximal ideals:

Proposition 2.1. [12, Pólya] *For each $n \in \mathbb{N}$ and for every maximal ideal $\mathfrak{m}$ in $\mathcal{O}_K$,*

$$v_{\mathfrak{m}}\left(\mathfrak{I}_n(\mathcal{O}_K)\right) = -w_{\mathfrak{m}}(n)$$

Notation. For each $q \geq 2$, let $\Pi_q(K)$ be the product of all the maximal ideals of $\mathcal{O}_K$ with norm q:

$$\Pi_q(K) = \prod_{\substack{\mathfrak{m} \in Max(\mathcal{O}_K) \\ N(\mathfrak{m}) = q}} \mathfrak{m}.$$

If q is not the norm of an ideal, then $\Pi_q(K) = \mathcal{O}_K$

We deduce easily from the equality:

$$(n!)_{\mathcal{O}_K} = \Pi_n(K) \times \prod_{2 \leq q < n} \Pi_q(K)^{w_q(n)}$$

that:

Proposition 2.2. *$Fact(K)$ is a free abelian subgroup of $I(K)$ and the nontrivial ideals $\Pi_q(K)$ form a basis of this subgroup.*

Recall that the class group of $\mathcal{O}_K$ is the quotient $Cl(K) = I(K)/P(K)$ of the group of fractional ideals $I(K)$ of K by the group $P(K)$ of nonzero principal ideals.

Definition 2.2. [5] The *Pólya-Ostrowski group* or *Pólya group* is the image $Po(K)$ of the factorial group $Fact(K)$ in the ideal class group $Cl(K)$:

$$Po(K) = Fact(K)/P(K) \cap Fact(K).$$

In other words, the Pólya group of K is the subgroup of $Cl(K)$ generated by the classes of the characteristic ideals $\mathfrak{I}_n(\mathcal{O}_K)$ or by the classes of the ideals $\Pi_q(K)$. Now, we have several ways to say that the field K is a Pólya field.

Proposition 2.3. *The field K is a Pólya field if and only if one of the following assertions is satisfied:*

(1) $\mathrm{Int}\,(\mathcal{O}_K)$ *has a regular basis,*
(2) *for each* $n \in \mathbb{N}$, *the ideal* $(n!)_{\mathcal{O}_K}$ *is principal,*
(3) *for each* $q \geq 2$, $\Pi_q\,(K)$ *is principal,*
(4) $Po\,(K) = \{1\}$.

Example 1. [15] *Every cyclotomic field is a Pólya field.*

Let $m \in \mathbb{N}$ and $K = \mathbb{Q}(\zeta_m)$ where ζ_m denotes a m-th primitive root of unity. There is an explicit expression of a generator of $(n!)_{\mathcal{O}_K}$. Let p be prime number. Recall that [10, Proposition 6.4.8]:

$$f_p = \min\left\{f \geq 1 \mid p^f \equiv 1 \pmod{\frac{m}{p^{v_p(m)}}}\right\} \text{ and } e_p = \varphi\left(p^{v_p(m)}\right).$$

Following the decomposition of a prime number in a cyclotomic field we have:

$$(n!)_{\mathcal{O}_K} = \prod_{q \leq n} \Pi_q(K)^{w_q(n)} = \prod_{p \nmid m} p^{w_{pf_p}(n)} \times \prod_{p \mid m} \left(1 - \zeta_m^{\left(\frac{m}{p^{v_p(m)}}\right)}\right)^{w_{pf_p}(n)} \mathbb{Z}\left[\zeta_m\right].$$

Consequently, by the Kronecker-Weber theorem:

Corollary 2.1. *Every finite abelian extension of* $\mathbb{Q}$ *is contained in a Pólya field.*

This is a positive answer to the embedding problem in a Pólya field in the case of an abelian extension of $\mathbb{Q}$.

Remark. Recall that if K is a galoisian extension of $\mathbb{Q}$, an ambiguous ideal of K is an ideal which is invariant under the action of the Galois group $Gal(K/\mathbb{Q})$, so that, if $K/\mathbb{Q}$ is a galoisian extension, the factorial group of K is the group of ambiguous ideals of K. Actually, the subgroup $I(K)^G$ formed by the ideals which are invariant under the action of $G = Gal(K/\mathbb{Q})$ is generated by the $\Pi_q\,(K)$. Then

$$\begin{aligned} Fact(K) &= I(K)^G, \\ Fact(K) \cap P(K) &= I(K)^G \cap P(K) = P(K)^G, \\ Po(K) &= I(K)^G/P(K)^G. \end{aligned}$$

Thus, $Po(K)$ is the subgroup of $Cl(K)$ generated by the classes of the ambiguous ideals of K. Hilbert describes this subgroup in the case when K is a quadratic field:

Proposition 2.4. [8, §75] *Let* $K = \mathbb{Q}[\sqrt{d}]$ *be a quadratic field where* d *is a squarefree integer. Then, let* s *be the number of primes which are ramified in the extension* $K/\mathbb{Q}$*:*

(1) *If K is a real quadratic field whose fondamental unit has norm $+1$, then $Po(K)$ has $s-2$ independent generators and 2^{s-2} elements.*
(2) *In the other cases (K is an imaginary quadratic field or a real quadratic field whose fondamental unit has norm -1), $Po(K)$ has $s-1$ independent generators and 2^{s-1} elements.*

We come back to Pólya extensions. Analogously, we introduce the following definition.

Definition 2.3. For every finite extension L/K, the Pólya group of the set $\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$ is the subgroup of $Cl(L)$ generated by the classes of the ideals $\mathfrak{I}_n(\mathcal{O}_K, \mathcal{O}_L)$. We denote it by $Po(K, L)$.

Then, we generalize all the properties obtained on $\mathrm{Int}(\mathcal{O}_K)$:

Proposition 2.5. *The following asssertions are equivalent:*
(1) *L/K is Pólya extension.*
(2) *$\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$ has a regular basis.*
(3) *For each $n \in \mathbb{N}$ the fractional ideal $\mathfrak{I}_n(\mathcal{O}_K, \mathcal{O}_L)$ is principal.*
(4) *For every q, the ideal $\Pi_q(K)\mathcal{O}_L$ is principal.*
(5) *$Po(K, L)$ is trivial.*

Proof. The equivalence between (1) and (2) comes from Proposition 1.2. The equivalence between (2) and (3) is proved by the same way than the the assertion "$\mathrm{Int}(\mathcal{O}_K)$ has a regular basis if and only if the $\mathcal{O}_K$-modules $\mathfrak{I}_n(\mathcal{O}_K)$ are principal" [5, II.1.4]. Since $\mathfrak{I}_n(\mathcal{O}_K)\mathcal{O}_L = \mathfrak{I}_n(\mathcal{O}_K, \mathcal{O}_L)$ (Proposition 1.1), Proposition 2.2 gives the equivalence between (3) and (4). The equivalence (3)$\Leftrightarrow$(5) is deduced from Definition 2.3. □

3. Pólya groups in galoisian extensions of $\mathbb{Q}$

In this section, we study the Pólya group of galoisian extensions of $\mathbb{Q}$. We recall that, if K is a galoisian extension of $\mathbb{Q}$, for each prime number p, the g_p maximal ideals of $\mathcal{O}_K$ over p have the same ramification index e_p and the same residue degree f_p and we have :

$$e_p f_p g_p = [K : \mathbb{Q}].$$

Then

$$p\mathcal{O}_K = \prod_{\mathcal{M}|p} \mathcal{M}^{e_p} = \Pi_q(K)^{e_p} \text{ where } q = p^{f_p}.$$

Consequently, following Ostrowski:

Proposition 3.1. [11] *Let K be a finite galoisian extension of $\mathbb{Q}$. $Po(K)$ is generated by the classes of the ideals $\Pi_q(K)$ where $q = p^f$ and the prime number p is ramified in $K/\mathbb{Q}$*

Corollary 3.1. *$|Po(K)|$ divides $\prod_p e_p$.*

Corollary 3.2. *Let $K/\mathbb{Q}$ be a galoisian extension such that $[K:\mathbb{Q}] = q^n$ where q is a prime number. If $Cl_q(K)$ denote the q-class group of K, then we have the containment $Po(K) \subseteq Cl_q(K)$.*

Proof. According to the last corollary, the order of $Po\,(K)$ divides $\prod_p e_p$ but, since the extension $K/\mathbb{Q}$ is galoisian, for each prime number p ramified in $K/\mathbb{Q}$, $e_p \mid q^n$. □

Corollary 3.3. *Let K be a galoisian extension of $\mathbb{Q}$ with degree n and class number h_K. If n and h_K are relatively prime, then K is a Pólya field.*

Proof. $|Po(K)|$ divides a power of n and $|Cl(K)| = h_K$. □

Corollary 3.4. [15, Proposition 2.5] *Let $K/\mathbb{Q}$ be a finite abelian extension. If only one prime p is ramified in the extension then K is a Pólya field.*

Notation. Let L/K be a finite extension. Consider the norm morphism [14, Chap I. §5]:

$$N_L^K : I\,(L) \mapsto I\,(K)$$

which is determined by its value on the maximal ideals $\mathcal{N}$ of $\mathcal{O}_L$

$$N_L^K\,(\mathcal{N}) = \mathcal{M}^{f_{\mathcal{N}}(L/K)}$$

where $\mathcal{M} = \mathcal{N} \cap \mathcal{O}_K$ and $f_{\mathcal{N}}\,(L/K) = [\mathcal{O}_L/\mathcal{N} : \mathcal{O}_K/\mathcal{M}]$. The morphism N_L^K induces the morphism:

$$\nu_L^K : \overline{\mathcal{I}} \in Cl\,(L) \mapsto \overline{N_L^K\,(\mathcal{I})} \in Cl\,(K)\,.$$

On the other hand, the injective morphism:

$$j_K^L : \mathcal{I} \in I\,(K) \mapsto \mathcal{I}\mathcal{O}_L \in I\,(L)$$

induces the morphism

$$\epsilon_K^L : \overline{\mathcal{I}} \in Cl\,(K) \mapsto \overline{\mathcal{I}\mathcal{O}_L} \in Cl\,(L)\,.$$

We know that the morphism N_L^K generalizes the norm $N_{L/K}(x)$ of an element x and the absolute norm of an ideal :

$$N_L^K(x\mathcal{O}_L) = N_{L/K}(x)\mathcal{O}_K \text{ and } \left|N_K^{\mathbb{Q}}(I)\right| = Card(\mathcal{O}_K/I),$$

for every $x \in L$ and every entire ideal I of K. Moreover, since the extension L/K is separable, for each ideal of $I\,(K)$, we have:

$$N_L^K \circ j_K^L\,(\mathcal{I}) = \mathcal{I}^{[L:K]}.$$

We recall that, when we work with galoisian extensions of $\mathbb{Q}$, the factorial ideal groups and the Pólya groups behave nicely with respect to these morphisms:

Proposition 3.2. [6] *If K and L are two galoisian extensions of $\mathbb{Q}$ such that $K \subseteq L$ then*

(1) $j_K^L\left(Fact\left(K\right)\right) \subseteq Fact\left(L\right)$ *and* $\epsilon_K^L\left(Po\left(K\right)\right) \subseteq Po\left(L\right)$

(2) $N_L^K\left(Fact\left(L\right)\right) \subseteq Fact\left(K\right)$ *and* $\nu_L^K\left(Po\left(L\right)\right) \subseteq Po\left(K\right)$

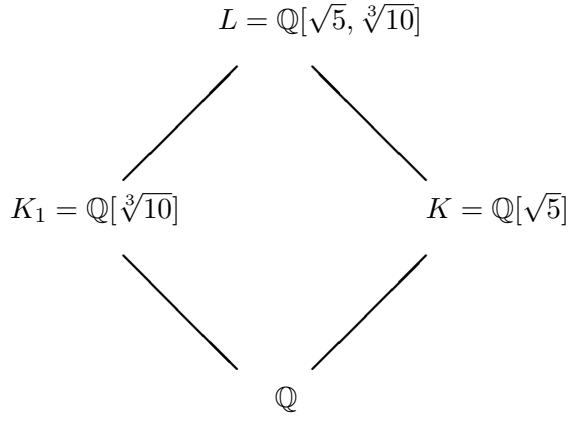
Remark. Notice that, under the hypothesis of the previous proposition, $\epsilon_K^L\left(Po(K)\right)$ is the subgroup of $Cl(L)$ we have denoted by $Po(K,L)$.

Corollary 3.5. *Let K and L be two galoisian extensions of $\mathbb{Q}$ such that $K \subseteq L$.*

(1) *The extension L/K is a Pólya extension if and only if the image $\epsilon_K^L\left(Po\left(K\right)\right)$ is trivial in $Po\left(L\right)$.*
(2) *If L is a Pólya field, then L/K is a Pólya extension.*

Remark. When L/K is not a galoisian extension, the containments given in Proposition 3.2 are not always true as shown by the following example: $\mathbb{Q}[\sqrt{5}, \sqrt[3]{10}]/\mathbb{Q}[\sqrt{5}]$

Example 2. *Let $K_1 = \mathbb{Q}[\sqrt[3]{m}]$ be a pure cubic field where m is cubefree and not equal to ± 1. Write $m = ab^2$ where a and b are squarefree and coprime. Then, according to* [7, Thm 6.4.16]*, 3 is partially ramified in $K_1/\mathbb{Q}$ if and only if $a^2 \equiv b^2 \pmod 9$.*
For our example, we choose $K_1 = \mathbb{Q}[\sqrt[3]{10}]$ and $K = \mathbb{Q}[\sqrt{5}]$. Then 3 is partially ramified in $K_1/\mathbb{Q}$ and inert in $K/\mathbb{Q}$. Let L be the compositum of K and K_1:



Then,

$$3\mathcal{O}_K = \mathfrak{m} \text{ where } N(\mathfrak{m}) = 3^2,$$

and

$$3\mathcal{O}_{K_1} = \mathfrak{m}_1\mathfrak{m}_2^2 \text{ where } N(\mathfrak{m}_i) = 3.$$

Consequently,

$$3\mathcal{O}_L = \mathfrak{n}_1\mathfrak{n}_2^2 \text{ where } N(\mathfrak{n}_i) = 3^2.$$

According to these equalities, we have

$$\Pi_9(L) = \mathfrak{n}_1\mathfrak{n}_2.$$

and

$$\Pi_9(K)\mathcal{O}_L = \mathfrak{m}\mathcal{O}_L = 3\mathcal{O}_L = \mathfrak{n}_1\mathfrak{n}_2^2.$$

If the containement $j_K^L(Fact(K)) \subseteq Fact(L)$ *was true, we would have* $\mathfrak{n}_2 \in Fact(L)$. *As* $N(\mathfrak{n}_2) = 3^2$, $\mathfrak{n}_2$ *would be a power of* $\Pi_q(L)$. *This is impossible.*

Here is the reason why $j_K^L(Fact(K)) \not\subseteq Fact(L)$ in the previous example:

Proposition 3.3. *Let* $K/\mathbb{Q}$ *be a galoisian extension and consider an extension* L/K. *We have the containment*

$$j_K^L(Fact(K)) \subseteq Fact(L)$$

if and only if, for all maximal ideals $\mathfrak{p}_1, \mathfrak{p}_2$ *of* $\mathcal{O}_L$ *lying over a same prime number,*

$$(f_{\mathfrak{p}_1}(L/K) = f_{\mathfrak{p}_2}(L/K)) \Rightarrow (e_{\mathfrak{p}_1}(L/K) = e_{\mathfrak{p}_2}(L/K))$$

Proof. Let p be a prime number. Let $e = e_p(K/\mathbb{Q})$ and $f = f_p(K/\mathbb{Q})$. We have

$$p\mathcal{O}_K = \Pi_{p^f}(K)^e.$$

Suppose that for all maximal ideals $\mathfrak{p}_1, \mathfrak{p}_2$ of $\mathcal{O}_L$ lying over p, we have $(f_{\mathfrak{p}_1}(L/K) = f_{\mathfrak{p}_2}(L/K)) \Rightarrow (e_{\mathfrak{p}_1}(L/K) = e_{\mathfrak{p}_2}(L/K))$. Denote by $f_1, \ldots, f_r$ the distincts residue degrees in the extension L/K of the maximal ideals of $\mathcal{O}_L$ lying over p and denote by $e_1, \ldots, e_r$ the corresponding ramification indices. Then,

$$\Pi_{p^f}(K)\mathcal{O}_L = \left(\Pi_{p^{ff_1}}(L)\right)^{e_1} \ldots \left(\Pi_{p^{ff_r}}(L)\right)^{e_r}$$

and

$$j_K^L(Fact(K)) \subseteq Fact(L)$$

Conversely, suppose that $j_K^L(Fact(K)) \subseteq Fact(L)$. Then, there exist $\alpha_1, \ldots, \alpha_s \in \mathbb{Z}$ and $f_1, \ldots, f_s \in \mathbb{N}$ such that

$$\Pi_{p^f}(K)\mathcal{O}_L = \left(\Pi_{p^{ff_1}}(L)\right)^{\alpha_1} \ldots \left(\Pi_{p^{ff_s}}(L)\right)^{\alpha_s}.$$

Since all the maximal ideals of L lying over p are in this decomposition, necessarily, one has that, for all $\mathfrak{p}_1, \mathfrak{p}_2$ maximal ideals of $\mathcal{O}_L$ lying over p, $f_{\mathfrak{p}_1}(L/K) = f_{\mathfrak{p}_2}(L/K)$ implies $e_{\mathfrak{p}_1}(L/K) = e_{\mathfrak{p}_2}(L/K)$. □

Corollary 3.6. *Let $K_1 = \mathbb{Q}[\sqrt[3]{m}]$ be a pure cubic field such that $a^2 \not\equiv b^2 \pmod 9$ (where $m = ab^2$ with the notations of the previous example). Then, for every galoisian extension $K/\mathbb{Q}$, one has:*

$$j_K^{KK_1}\left(Fact\left(K\right)\right) \subseteq Fact\left(KK_1\right).$$

Proof. Following the description of the decomposition of a prime number in a pure cubic field of [7, Cor. 6.4.15, Thm. 6.4.16], the prime numbers p are never partially ramified except when $p = 3$. □

4. Linearly disjoined galoisian extensions

Let K be an algebraic number field and let K_1, K_2 be two finite extensions of K. Denote by K_1K_2 the field generated by K_1 and K_2. Recall that K_1 and K_2 are said to be linearly disjoined over K if a basis of K_1 over K is also a basis of K_1K_2 over K_2 [4].

If K_1 and K_2 are linearly disjoined over K, then $K_1 \cap K_2 = K$. The converse is false in general. But, if K_1/K is a galoisian extension and if $K_1 \cap K_2 = K$ then:

(1) K_1 and K_2 are linearly disjoined over K.
(2) K_1K_2/K_2 is a galoisian extension.
(3) $Gal(K_1K_2/K_2) \simeq Gal(K_1/K_1 \cap K_2)$

In particular, if K_1/K and K_2/K are galoisian extensions and $K_1 \cap K_2 = K$, then K_1K_2 is a galoisian extension of K and $Gal\left(K_1K_2\right) \simeq Gal\left(K_1\right) \times Gal\left(K_2\right)$.

The following result is proved in [6]:

Proposition 4.1. *Let K_1 and K_2 be two galoisian extensions of $\mathbb{Q}$ and $L = K_1K_2$. If $[K_1 : \mathbb{Q}]$ and $[K_2 : \mathbb{Q}]$ are relatively prime , then*

$$j_{K_1}^{L}\left(Fact\left(K_1\right)\right).j_{K_2}^{L}\left(Fact\left(K_2\right)\right) = Fact\left(L\right).$$

We are going to prove such a result but with a weaker hypothesis which concerns the ramification indices.

Notation for the section. Let K be a galoisian extension of $\mathbb{Q}$. Let K_1, K_2 be two galoisian extensions of K such that $K_1 \cap K_2 = K$ and $L = K_1K_2$. The extensions K_1 and K_2 are linearly disjoined over K. Let $\mathfrak{M}$ be a maximal ideal of L and

$$\mathfrak{P}_1 = \mathfrak{M} \cap K_1, \mathfrak{P}_2 = \mathfrak{M} \cap K_2 \text{ and } \mathfrak{p} = \mathfrak{M} \cap K$$

Remarks. (1) When $[K_1 : K]$ and $[K_2 : K]$ are relatively prime, it is easy to get the following equality :

$$e(\mathfrak{M}/\mathfrak{p}) = e(\mathfrak{P}_1/\mathfrak{p})e(\mathfrak{P}_2/\mathfrak{p}).$$

The residue degrees satisfy analoguous equalities.

(2) Clearly, without the hypothesis "$[K_1 : K]$ and $[K_2 : K]$ are relatively prime", this equality is not always true. For instance,

$$e_2\left(\mathbb{Q}(\sqrt{3})/\mathbb{Q}\right) = e_2\left(\mathbb{Q}(\sqrt{7})/\mathbb{Q}\right) = 2$$

and $e_2\left(\mathbb{Q}(\sqrt{3},\sqrt{7})/\mathbb{Q}\right) = 2$ since $e_2\left(\mathbb{Q}(\sqrt{21})/\mathbb{Q}\right) = 1$.

(3) This example contradicts Proposition 14.1.E of Ribenboim [13] which says that, with our hypothesis and notation:

$$I_{\mathfrak{M}}(L/K) \simeq I_{\mathfrak{P}_1}(K_1/K) \times I_{\mathfrak{P}_2}(K_2/K),$$

where $I_{\mathfrak{M}}(L/K)$ (resp. $I_{\mathfrak{P}_1}(K_1/K)$, $I_{\mathfrak{P}_2}(K_2/K)$) denotes the inertial group of $\mathfrak{M}$ (resp. $\mathfrak{P}_1$, $\mathfrak{P}_2$) in the extension L/K (resp. K_1/K, K_2/K). It is true that under our hypotheses,

$$Gal\,(L/K) \simeq Gal\,(K_1/K) \times Gal\,(K_2/K)$$

and the image of $I_{\mathfrak{M}}(L/K)$ in $Gal\,(K_1/K)$ is the subgroup $I_{\mathfrak{P}_1}(K_1/K)$ and in $Gal\,(K_2/K)$ the subgroup $I_{\mathfrak{P}_2}(K_2/K)$. However, we can not deduce from this Ribenboim's isomorphism. In the previous example, we have $I_{\mathfrak{P}_1}(K_1/K) \simeq I_{\mathfrak{P}_2}(K_2/K) \simeq \mathbb{Z}/2\mathbb{Z}$. The inertial group $I_{\mathfrak{M}}(L/K)$ is in fact the third subgroup of order 2 of $Gal\,(L/K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Lemma 4.1. *With the previous notation (but without the assumption that the extensions are galoisian), we have*

$$lcm\,(e(\mathfrak{P}_1/\mathfrak{p}), e(\mathfrak{P}_2/\mathfrak{p}))\,|e(\mathfrak{M}/\mathfrak{p}).$$

If one of the extensions K_1/K or K_2/K is galoisian, then

$$e(\mathfrak{M}/\mathfrak{p})|e(\mathfrak{P}_1/\mathfrak{p})e(\mathfrak{P}_2/\mathfrak{p}).$$

Thus, if moreover $(e(\mathfrak{P}_1/\mathfrak{p}), e(\mathfrak{P}_2/\mathfrak{p})) = 1$, then

$$e(\mathfrak{M}/\mathfrak{p}) = e(\mathfrak{P}_1/\mathfrak{p})e(\mathfrak{P}_2/\mathfrak{p}).$$

Proof. From the relation $e(\mathfrak{M}/\mathfrak{p}) = e(\mathfrak{M}/\mathfrak{P}_1)e(\mathfrak{P}_1/\mathfrak{p})$, we deduce that lcm $(e(\mathfrak{P}_1/\mathfrak{p}), e(\mathfrak{P}_2/\mathfrak{p}))$ divides $e(\mathfrak{M}/\mathfrak{p})$. If for instance, the extension K_2/K is galoisian, then L/K_1 is also galoisian. The image of the inertial group $I_{\mathfrak{M}}(L/K_1)$ by the restriction isomorphism:

$$\sigma \in Gal(L/K_1) \mapsto \sigma_{|K_2} \in Gal(K_2/K)$$

is a subgroup of the inertial group $I_{\mathfrak{P}_2}(K_2/K)$. Consequently, $e(\mathfrak{M}/\mathfrak{p})$ divides $e(\mathfrak{P}_2/\mathfrak{p})$. Then, $e(\mathfrak{M}/\mathfrak{p})$ divides $e(\mathfrak{P}_1/\mathfrak{p})e(\mathfrak{P}_2/\mathfrak{p})$.

□

Proposition 4.2. *Let K, K_1 and K_2 be galoisian extensions of $\mathbb{Q}$ such that $K_1 \cap K_2 = K$, and let $L = K_1K_2$. If, for all prime ideal $\mathfrak{p}$ of K, $(e_{K_1/K}(\mathfrak{p}), e_{K_2/K}(\mathfrak{p})) = 1$ then*

$$j_{K_1}^L\left(Fact\left(K_1\right)\right).j_{K_2}^L\left(Fact\left(K_2\right)\right) = Fact\left(L\right),$$
$$j_{K_1}^L\left(Fact\left(K_1\right)\right) \cap j_{K_2}^L\left(Fact\left(K_2\right)\right) = j_K^L\left(Fact(K)\right),$$
$$\epsilon_{K_1}^L\left(Po\left(K_1\right)\right).\epsilon_{K_2}^L\left(Po\left(K_2\right)\right) = Po\left(L\right).$$

Proof. Fix a prime ideal $\mathfrak{p}$ of K. Suppose that $N(\mathfrak{p}) = p^\alpha$. Let $e_i = e_{K_i/K}(\mathfrak{p})$, $f_i = f_{K_i/K}(\mathfrak{p})$ and $\varphi_i = f_{L/K_i}(\mathfrak{p})$ for $i \in 1, 2$. According to the previous lemma, $e_{L/K}(\mathfrak{p}) = e_1e_2$. The extension $L/\mathbb{Q}$ is galoisian, $f_{L/K}(\mathfrak{p}) = f_1\varphi_1 = f_2\varphi_2$.

Denote by $\Pi_i = \Pi_{p^{\alpha f_i}}\left(K_i\right)$ and $\Pi = \Pi_{p^{\alpha f_i\varphi_i}}\left(L\right)$. We have

$$\mathfrak{p}\mathcal{O}_{K_i} = \Pi_i^{e_i}, \mathfrak{p}\mathcal{O}_L = \Pi^{e_1e_2}, \Pi_i\mathcal{O}_L = \Pi^{e_{3-i}}\left(i = 1, 2\right).$$

We obtain

$$\langle\Pi_1\mathcal{O}_L, \Pi_2\mathcal{O}_L\rangle = \langle\Pi^{e_2}, \Pi^{e_1}\rangle = \left\langle\Pi^{gcd(e_1,e_2)}\right\rangle.$$

As $gcd(e_1, e_2) = 1$, $\langle\Pi_1\mathcal{O}_L, \Pi_2\mathcal{O}_L\rangle = \langle\Pi\rangle$. The first equality is proved.

Let $I \subseteq j_{K_1}^L\left(Fact\left(K_1\right)\right) \cap j_{K_2}^L\left(Fact\left(K_2\right)\right)$. Without lost of generality, we may assume that: $I = \Pi_{p^{\alpha f_i}}\left(K_i\right)^{k_i}\mathcal{O}_L \in j_{K_i}^L\left(Fact\left(K_i\right)\right)$, i.e $I = \Pi_i^{k_i}\mathcal{O}_L$, $k_i \in \mathbb{Z}$ for $i \in \{1, 2\}$. As a consequence, $I = \Pi_1^{k_1}\mathcal{O}_L = \Pi_2^{k_2}\mathcal{O}_L$, $\Pi^{k_1e_2} = \Pi^{k_2e_1}$, then $I \subseteq \left\langle\Pi^{lcm(e_1,e_2)}\right\rangle$. If $gcd(e_1, e_2) = 1$, $I \subseteq \langle\Pi^{e_1e_2}\rangle = \langle\Pi_{p^\alpha}(K)\mathcal{O}_L\rangle$. The second equality is proved. The third follows from the first one. □

Remark. The previous proof shows that, with the same notation, if for some fixed prime ideal $\mathfrak{p}$ of K one has $(e_{K_1/K}(\mathfrak{p}), e_{K_2/K}(\mathfrak{p})) = 1$, then Π is principal of $\mathcal{O}_L$ if and only if and if the extended ideals $\Pi_i\mathcal{O}_L$ are also principal.

Corollary 4.1. *Let K, K_1 and K_2 be galoisian extensions of $\mathbb{Q}$ such that $K_1 \cap K_2 = K$ and let $L = K_1K_2$. Assume that, for each ideal $\mathfrak{p}$ of K, $(e_{K_1/K}(\mathfrak{p}), e_{K_2/K}(\mathfrak{p})) = 1$, then :*

(1) *L is a Pólya field if and only if L/K_i are Pólya extensions.*
(2) *If K_1 and K_2 are Pólya fields, then K_1K_2 is a Pólya field.*

As a corollary, we obtain Zantema's result [15, Thm 3.4]: let $K_1/\mathbb{Q}$ and $K_2/\mathbb{Q}$ be two galoisian extensions whose degrees are relatively prime, if K_1 and K_2 are Pólya fields, then K_1K_2 is a Pólya field.

Remark. Taking into account the remark following the proof of Proposition 4.2, the previous corollary may be refined in the following way:

Let $K \subseteq L$ be two galoisian extensions of $\mathbb{Q}$. If for every prime ideal $\mathfrak{p}$ of K, there exist two galoisian extensions K_1 and K_2 of $\mathbb{Q}$ such that:

(1) K_1 and K_2 are linearly disjoined over K and $L = K_1K_2$,
(2) $(e_{K_1/K}(\mathfrak{p}), e_{K_2/K}(\mathfrak{p})) = 1$,
(3) K_1 and K_2 are Pólya fields,

then L is a Pólya field.

Application to biquadratic fields. We may apply the previous corollary to biquadratic fields. Let K_1 and K_2 be two quadratic fields and $L = K_1K_2$. Denote by D_{K_i} the discriminant of K_i. The assumption "for each ideal $\mathfrak{p}$ of K $(e_{K_1/K}(\mathfrak{p}), e_{K_2/K}(\mathfrak{p})) = 1$" is obviously equivalent to " $(D_{K_1}, D_{K_2}) = 1$". Even if this condition is not satisfied, the previous technical remark leads us to consider the third quadratic subfield of L:

Proposition 4.3. *If $\mathbb{Q}[\sqrt{a}]$ and $\mathbb{Q}[\sqrt{b}]$ are two disctinct quadratic Pólya fields such that 2 is ramified in at most two of the three extensions $\mathbb{Q}[\sqrt{a}]$, $\mathbb{Q}[\sqrt{b}]$, $\mathbb{Q}[\sqrt{ab}]$, then the biquadratic field $\mathbb{Q}[\sqrt{a}, \sqrt{b}]$ is a Pólya field.*

Then, using the following characterization of the quadratic Pólya fields (see Proposition 2.4 and [5, Cor. II.4.5]), we can conclude that many biquadratic fields are Pólya fields.

Proposition 4.4. [5, Cor. II.4.5] *A quadratic field $\mathbb{Q}[\sqrt{d}]$ is a Pólya field if and only if d is of one of the following forms where p and q denote two distinct odd prime numbers:*

(1) *$d = -1$, or $d = -2$, or $d = -p$ where $p \equiv 3 \pmod 4$, or $d = p$,*
(2) *$d = 2p$, or $d = pq$ where $pq \equiv 1 \pmod 4$ and, in both cases, the fondamental unit has norm 1 if $p \equiv 1 \pmod 4$.*

Proposition 4.5. *Let p, q, r be three distinct odd primes. The following biquadratic real fields are Pólya fields:*

(1) $\mathbb{Q}[\sqrt{p}, \sqrt{q}]$,
(2) $\mathbb{Q}[\sqrt{p}, \sqrt{qr}]$ *with $qr \equiv 1 \pmod 4$.*

Proof. (1) If $p \equiv q \equiv 3 \pmod 4$ then 2 is not ramified in the extension $\mathbb{Q}(\sqrt{pq})/\mathbb{Q}$: we conclude with Proposition 4.3. If $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then 2 is not ramified in $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ or $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$.
(2) As $qr \equiv 1 \pmod 4$, 2 is not ramified in $\mathbb{Q}(\sqrt{qr})/\mathbb{Q}$.

□

More generally, we may verify that: if $\mathbb{Q}[\sqrt{a}]$ and $\mathbb{Q}[\sqrt{b}]$ are two distinct quadratic Pólya fields, then the biquadratic field $\mathbb{Q}[\sqrt{a}, \sqrt{b}]$ is a Pólya field except perhaps for $(a, b) = (-1, 2)$, $(-1, 2q)$, $(2, p)$, $(-2, p)$, $(p, 2q)$ where p and q denote two distinct odd primes with $p \equiv 3 \pmod 4$.

To know wether these exceptions are Pólya fields or not, we would have to look at them separately.

References

[1] M. Bhargava, *P-orderings and polynomial functions on arbitrary subsets of Dedekind rings*. J. Reine Angew. Math. **4**90 (1997), 101–127.

[2] M. Bhargava, *Generalized factorials and fixed divisors over subsets of a Dedekind domain*. J. Number Theory **7**2 (1998), 67–75.

[3] H. Bass, *Big projective modules are free*. Illinois J. Math. **7** (1963), 24–31.

[4] N. Bourbaki, *Algèbre*, Chapitre V. Masson, Paris, 1981.

[5] P.J. Cahen, J.L. Chabert, *Integer-valued polynomials*. Mathematical Surveys and Monographs **4**8, Amer. Math. Soc., Providence, 1997.

[6] J.L Chabert, *Factorial Groups and Pólya groups in Galoisian Extension of* $\mathbb{Q}$. Proceedings of the fourth international conference on commutative ring theory and applications (2002), 77–86.

[7] H. Cohen, *A Course in Computational Algebraic Number Theory*. Springer, 2000.

[8] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*. Jahresbericht der Deutschen Mathematiker-Vereinigung **4** (1894-95), 175–546.

[9] E.S. Golod, I.R. Shafarevich, *On the class field tower*. Izv. Akad. Nauk, **2**8 (1964).

[10] H. Koch, *Number Theory*. Graduate Studies in Mathematics, A.M.S., 2000.

[11] A. Ostrowski, *Über ganzwertige Polynome in algebraischen Zahlkörpren*. J. reine angew. Math. **1**49 (1919), 117–124.

[12] G. Pólya, *Über ganzwertige Polynome in algebraischen Zahlkörpern*. J. Reine Angew. Math. **1**49 (1919), 97–116.

[13] P. Ribenboim, *Classical Theory of Algebraic Numbers*. Springer, 2000.

[14] J.P Serre, *Corps Locaux*. Hermann, Paris, 1962.

[15] H. Zantema, *Integer valued polynomials over a number field*. Manusc. Math. **4**0 (1982), 155–203.

Amandine Leriche
LAMFA, CNRS UMR 6140
Université de Picardie Jules Verne
33, rue Saint-Leu
80039 Amiens, France
E-mail: amandine.leriche@u-picardie.fr