

Troisième Rencontre Internationale sur les Polynômes à Valeurs Entières

Rencontre organisée par : Sabine Evrard

29 novembre-3 décembre 2010

Amandine Leriche **Pólya fields and Pólya numbers** Vol. 2, n° 2 (2010), p. 21-26. <http://acirm.cedram.org/item?id=ACIRM_2010__2_2_21_0>

> Centre international de rencontres mathématiques U.M.S. 822 C.N.R.S./S.M.F. Luminy (Marseille) FRANCE

cedram

Texte mis en ligne dans le cadre du Centre de diffusion des revues académiques de mathématiques http://www.cedram.org/

Pólya fields and Pólya numbers

Amandine LERICHE

Abstract

A number field K, with ring of integers \mathcal{O}_K , is said to be a Pólya field if the \mathcal{O}_K -algebra formed by the integer-valued polynomials on \mathcal{O}_K admits a regular basis. In a first part, we focus on fields with degree less than six which are Pólya fields. It is known that a field K is a Pólya field if certain characteristic ideals are principal. Analogously to the classical embedding problem, we consider the embedding of K in a Pólya field. We give a positive answer to this embedding problem by showing that the Hilbert class field H_K of K is a Pólya field. Finally, we give upper bounds for the minimal degree po_K of a Pólya field containing K, namely the Pólya number of K.

1. INTRODUCTION: PÓLYA FIELDS AND THE EMBEDDING PROBLEM

In this paper, we state main results from our thesis¹[9].

Let K be an algebraic number field and denote by \mathcal{O}_K its ring of integers. Consider the ring of integer-valued polynomials on \mathcal{O}_K , that is,

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

One knows that $\operatorname{Int}(\mathcal{O}_K)$ is a free \mathcal{O}_K -module [1, Rem. II.3.7], but, describing a basis often constitutes an arduous task. After the seminal work of Pólya [12] and Ostrowski, [11], where they tried to characterize the fields K such that $Int(\mathcal{O}_K)$ admits a "regular basis", Zantema [14] introduced the following definition:

Definition 1.1. [14] A number field K is said to be a *Pólya field* if the \mathcal{O}_K -module Int (\mathcal{O}_K) admits a regular basis, that is, a basis $(f_n)_{n \in \mathbb{N}}$ such that, for each n, the polynomial f_n has degree n.

For instance, every cyclotomic field is a Pólya field (see [14]).

For each $n \in \mathbb{N}$, we denote by $\mathfrak{I}_n(K)$ the subset of K formed by 0 and the leading coefficients of the polynomials in Int (\mathcal{O}_K) with degree n. This is a fractional ideal of \mathcal{O}_K called the *characteristic* ideal of index n of K [1, Prop I.3.I]. Recall that K is a Pólya field if and only if the characteristic ideals $\mathfrak{I}_n(K)$ are principal [1, II.1.4]. In particular, if \mathcal{O}_K is a principal ideal domain, then K is a Pólya field. The converse, however, is false. Thus, the condition "K is a Pólya field" is weaker than the condition "K has a class number equal to one".

One knows the classical embedding problem:

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

Golod and Schafarevitch [8] gave a negative answer to this question in 1964. With a weaker hypothesis, however, a natural question arises:

Is every number field contained in a Pólya field?

Text presented during the meeting "Third International Meeting on Integer-Valued Polynomials" organized by Sabine Evrard. 29 novembre-3 décembre 2010, C.I.R.M. (Luminy).

²⁰⁰⁰ Mathematics Subject Classification. 11R04, 13F20, 11R16, 11R37.

Key words. Pólya fields, Hilbert class field, genus field, integer-valued polynomials. ¹The thesis was defended at the C.I.R.M. during the Entcounter.

Amandine Leriche

The counter-example given by Golod and Schafarevitch is not a counter-example for this new embedding problem.

We undertook the study of this question in [10] and pursued it in our thesis [9]. As mentioned, we wish to state here some results contained in this thesis. We start by determining number fields which are already themselves Pólya fields. Quadratic Pólya fields were completely characterized [1], we do the same for several families of fields with degree less than six. Then we give a positive answer to our "new embedding problem": the Hilbert class field H_K of any number field K is a Pólya field. It is not, however, generally the smallest Pólya field containing K. Thus, we try to give upper bounds for the minimal degree po_K of a Pólya field containing K, that we call the Pólya number of K.

2. Families of Pólya fields with small degree

2.1. **Presentation.** We recall the notion of Pólya group which can be considered as a measure of the obstruction for a field K to be a Pólya field. 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 2.1. [1] The *Pólya group of* K is the subgroup Po(K) of Cl(K) generated by the classes of the characteristic ideals $\mathfrak{I}_n(K)$ of K.

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

$$\Pi_{q}\left(K\right) = \prod_{\substack{\mathfrak{m}\in Max(\mathcal{O}_{K})\\N(\mathfrak{m})=q}}\mathfrak{m}.$$

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

In fact we know that Po(K) is also the subgroup of Cl(K) generated by the classes of the ideals $\Pi_q(K)$. We can thus characterize the Pólya fields in several ways:

Proposition 2.2. The field K is a Pólya field if and only if one of the following assertions is satisfied:

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

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 that we have $e_p f_p g_p = [K : \mathbb{Q}]$ then

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

Thus we obtain the following result due to Ostrowski:

Proposition 2.3. [11] Let K be a finite galoisian extension of \mathbb{Q} . The group 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}

If K is a galoisian extension of \mathbb{Q} , then Po(K) is the subgroup of Cl(K) generated by the classes of the ambiguous ideals of K, where an ambiguous ideal of K is an ideal which is invariant under the action of the Galois group $Gal(K/\mathbb{Q})$. Hilbert [7, §75] described this subgroup in the case where K is a quadratic field and from this description, Zantema [14] deduced the characterization of the quadratic Pólya fields (see [1, Cor. II.4.5]):

Proposition 2.4. A quadratic field $\mathbb{Q}[\sqrt{d}]$ is a Pólya field if and only if d is of one of the following forms (p and q denote two distinct odd prime numbers):

- (1) d = 2,
- (2) d = -1,
- (3) d = -2,

- (4) d = -p with $p \equiv 3 \pmod{4}$,
- (5) d = p,
- (6) d = 2p and if $p \equiv 1 \pmod{4}$ then the fundamental unit has norm 1,
- (7) d = pq with $pq \equiv 1 \pmod{4}$ and if $p \equiv 1 \pmod{4}$ then the fundamental unit has norm 1.

We believe this is the only characterization of Pólya fields of a given degree to be found in the literature. We would like to give similar results for number fields of higher degrees.

2.2. Cyclic number fields. Recall a result which gives explicitly the cardinality of the Pólya group of a cyclic field:

Proposition 2.5. [2, Cor. 3.11] Let K/\mathbb{Q} be a cyclic extension of degree n. Then:

- (1) If K is real and the norm of every unit is 1, then $|Po(K)| = \frac{1}{2n} \times \prod_{p} e_{p}$.
- (2) In all other cases, $|Po(K)| = \frac{1}{n} \times \prod_{p} e_{p}$.

Thus, one deduces easily the following property:

Proposition 2.6. Let K/\mathbb{Q} be a cyclic extension of degree q, with q an odd prime number. Then $|Po(K)| = q^{s-1}$ where s is the number of primes which are ramified in K/\mathbb{Q} . In particular, K is a Pólya field if and only if there is exactly one prime which ramifies in K/\mathbb{Q} .

First, we apply this proposition to cubic cyclic fields. Following the description of such fields given in [3, Lemma 6.4.5], we have:

Proposition 2.7. Let K be a cubic cyclic field. Then K is a Pólya field if and only if $K = \mathbb{Q}(\theta)$ where θ is a root of a polynomial P such that :

$$P = X^3 - 3X + 1$$

or,

$$P = X^3 - 3pX - pu$$

where p is a prime such that $p = \frac{u^2 + 27w^3}{4}$ with $u \equiv 2 \pmod{3}$ and $w \in \mathbb{N}^*$.

Next, we carry on the study with quartic cyclic fields. We find a complete description of quartic cyclic fields in [6] and their discriminants are computed in [13]. Using Proposition 2.5, we may prove the following result:

Proposition 2.8. Let $K = \mathbb{Q}\left(\sqrt{A(D+B\sqrt{D})}\right)$ be a quartic cyclic field where A, B, C, D are integers such that A is squarefree and odd, $D = B^2 + C^2$ is squarefree, B > 0, C > 0, and gcd(A, D) = 1. Then K is a Pólya field if and only if one of the following conditions is satisfied (p and q denote distinct odd prime numbers):

(1)
$$K = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$$
 or $K = \mathbb{Q}\left(i\sqrt{2+\sqrt{2}}\right)$.

- (2) $K = \mathbb{Q}\left(\sqrt{q(2+\sqrt{2})}\right)$ and the norm of every unit is 1.
- (3) $K = \mathbb{Q}\left(\sqrt{p + B\sqrt{p}}\right)$ with $p \equiv 1 \pmod{4}, B \equiv 0 \pmod{4}$, and $p = B^2 + C^2$.
- (4) $K = \mathbb{Q}\left(i\sqrt{p+B\sqrt{p}}\right)$ with $p \equiv 1 \pmod{4}, B \equiv 2 \pmod{4}$, and $p = B^2 + C^2$.
- (5) $K = \mathbb{Q}\left(\sqrt{p + B\sqrt{p}}\right)$ with $p \equiv 1 \pmod{4}$, $B \equiv 1, 2, 3 \pmod{4}$, $p = B^2 + C^2$ and the norm of every unit is 1.
- (6) $K = \mathbb{Q}\left(\sqrt{q(p+B\sqrt{p})}\right)$ with $p \equiv 1 \pmod{4}$, $p = B^2 + C^2$, $q+B \equiv 1 \pmod{4}$, and the norm of every unit is 1.

2.3. Compositum of linearly disjoined galoisian extensions.

Notation. For every finite finite extension L/K, the injective morphism defined by:

$$j_{K}^{L}: \mathcal{I} \in I\left(K\right) \mapsto \mathcal{IO}_{L} \in I\left(L\right)$$

induces a morphism

$$\epsilon_{K}^{L}:\overline{\mathcal{I}}\in Cl\left(K\right)\mapsto\overline{\mathcal{IO}_{L}}\in Cl\left(L\right).$$

Proposition 2.9. [10, Prop. 4.2] Let K, K_1 and K_2 be galoisian extensions of \mathbb{Q} such that $K_1 \cap K_2 = K$ and denote by $L = K_1K_2$ the compositum of K_1 and K_2 . If, for each prime ideal \mathfrak{p} of the ring of integers \mathcal{O}_K of K, the indices of ramification $e_{K_1/K}(\mathfrak{p})$ and $e_{K_2/K}(\mathfrak{p})$ are coprime, then:

 $\epsilon_{K_{1}}^{L}\left(Po\left(K_{1}\right)\right).\epsilon_{K_{2}}^{L}\left(Po\left(K_{2}\right)\right)=Po\left(L\right).$

In particular, if K_1 et K_2 are Pólya fields, L is a Pólya field too.

Consequently, we are able to prove that some fields obtained by composition are Pólya fields. For instance:

Proposition 2.10. Sextic cyclic Pólya fields are exactly those which are the compositum of a quadratic Pólya field and a cubic cyclic Pólya field.

The case of biquadratic fields, compositum of two quadratic extension K_1/K and K_2/K , is more difficult to study because the indices of ramification $e_{K_1/K}(\mathfrak{p})$ and $e_{K_2/K}(\mathfrak{p})$ of some prime \mathfrak{p} may not be coprime (both being equal to 2). We may however prove the following result:

Theorem 2.11. Let m and n be two squarefree integers such that $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$ are quadratic Pólya fields. The biquadratic field $\mathbb{Q}[\sqrt{m}, \sqrt{n}]$ is a Pólya field except for the following fields, where p and q are odd primes such that $p \equiv 3 \pmod{4}$:

- (1) $\mathbb{Q}[i\sqrt{2},\sqrt{p}]$ is not a Pólya field;
- (2) $\mathbb{Q}[i, \sqrt{2q}]$ is not a Pólya field;
- (3) If Q[√p, √2q] is a Pólya field, then :
 (a) either p ≡ -1 (mod 8) and q ≡ 1, -1 (mod 8)
 - (b) or $p \equiv 3 \pmod{8}$ and $q \equiv 1, 3 \pmod{8}$.

Remark. The conditions given in (3) are necessary but not sufficient. For example, the fields $\mathbb{Q}[\sqrt{7}, \sqrt{62}], \mathbb{Q}[\sqrt{7}, \sqrt{82}]$ and $\mathbb{Q}[\sqrt{3}, \sqrt{34}]$ are not Pólya fields. However, there are no such examples for $p, q \equiv 3 \pmod{8}$: one may compute that, for $p, q < 100, \mathbb{Q}[\sqrt{p}, \sqrt{2q}]$ is always a Pólya field.

3. The Pólya number po_K of a number field

3.1. The answer to the embedding problem: the Hilbert class field. We come back to the embedding problem in a Pólya field. The question of embedding every algebraic number field in a Pólya field is equivalent to the following one:

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 degree $[H_K : K]$ 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 theorem). In other words, for every ideal \mathfrak{I} of \mathcal{O}_K , \mathfrak{IO}_{H_K} is principal. But, the ring \mathcal{O}_{H_K} itself is not necessarily a principal ideal domain. By analogy, we have the following notion:

Definition 3.1. [10] An extension L/K is said to be a *Pólya extension* if the following equivalent assertions are satisfied:

- (1) The extension of every characteristic ideals $\mathfrak{I}_n(K)$ to \mathcal{O}_L is principal.
- (2) The ring of integer-valued polynomials on \mathcal{O}_K relatively to \mathcal{O}_L , that is,

Int $(\mathcal{O}_K, \mathcal{O}_L) = \{P \in L[X] | P(\mathcal{O}_K) \subseteq \mathcal{O}_L\}$ admits a regular basis as an \mathcal{O}_L -module.

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.

When we work with galoisian extensions of \mathbb{Q} , the Pólya groups behave nicely with respect to morphisms introduced in §2.3:

Proposition 3.2. [2] If K and L are two galoisian extensions of \mathbb{Q} such that $K \subseteq L$ then $\epsilon_K^L(Po(K)) \subseteq Po(L)$

Corollary 3.3. 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 $\epsilon_K^L(Po(K))$ is trivial in Po(L).
- (2) If L is a Pólya field, then L/K is a Pólya extension.

Notice that a Pólya extension is not necessarily a Pólya field. For instance, $\mathbb{Q}[\sqrt{-5}, \sqrt{2}]/\mathbb{Q}[\sqrt{-10}]$ is a Pólya extension but $\mathbb{Q}[\sqrt{-5}, \sqrt{2}]$ is not a Pólya field (see Theorem 2.11). We have however a partial converse assertion:

Proposition 3.4. Assume K/\mathbb{Q} and L/\mathbb{Q} are two galoisian extensions such that $K \subseteq L$. If L/K is a Pólya extension such that all finite places are unramified, then L is a Pólya field.

In the particular case $L = H_K$, thanks to the capitulation theorem, we can forget the hypothesis " K/\mathbb{Q} is a galoisian extension" and we obtain the following theorem:

Theorem 3.5. Let K be a number field. Then the Hilbert class field H_K of K is a Pólya field.

Consequently, the embedding problem in a Pólya field has a positive answer :

Every number field may be embedded in a Pólya field, namely its Hilbert class field.

Remark. We know that a positive answer to the classical embedding problem is equivalent to a finite Hilbert class field tower. Although we have defined the notion of Pólya extension following the capitulation property of Hilbert class fields and we have answered positively the new embedding problem, we are able to construct infinite Pólya extensions towers.

3.2. The genus field. We are interested in the genus field because, under particular conditions, some ideals of K become principal by extension to the genus field Γ_K of K. First, recall the definition of the genus field:

Definition 3.6. Assume that K is an abelian number field. The genus field Γ_K of K is the maximal abelian extension of \mathbb{Q} containing K such that Γ_K/K is unramified.

Obviously, $\Gamma_K \subseteq H_K$.

Proposition 3.7. [4] Let K be an abelian extension of \mathbb{Q} . The extension of every ambiguous ideal of \mathcal{O}_K is principal in the genus field Γ_K of K.

Corollary 3.8. If K is an abelian number field then the genus field Γ_K of K is a Pólya extension of K.

It then follows from Proposition 3.4 that:

Proposition 3.9. The genus field of an abelian number field is a Pólya field.

Now, we know that H_K and Γ_K are both Pólya fields and Pólya extensions of each abelian field K. Moreover, we have the inclusion $\Gamma_K \subseteq H_K$. Consequently we are interested in the determination of minimal Pólya fields.

3.3. The Pólya number of a number field.

Definition 3.10. Let K be an algebraic number field.

- (1) A minimal Pólya field over K is a finite extension L of K which is a Pólya field and such that no intermediate extension $K \subseteq M \subsetneq L$ is Pólya field.
- (2) The Pólya number of K is the following integer

$$po_K = \min_{K \subset L} \{ [L:K] \mid K \subseteq L, L \text{ Pólya field} \}.$$

There are several questions about minimal Pólya field over K. For example, we can prove that there is no uniqueness for such minimal extension. However we do not know whether they all have the same degree. Now, we will see some upper bounds for the minimal degree of these minimal extensions.

From Theorem 3.5 we deduce that

$$po_K \leq h_K.$$

For an abelian number field K, since the genus field of K is a Pólya field, we have

 $po_K \leq g_K$ where $g_K = [\Gamma_K : K]$.

For a non abelian number field K, one may also define a genus field. In this case however the genus field is not generally a minimal Pólya field over K.

Finally, the following proposition shows that the genus field is not generally a minimal Pólya field over an abelian field.

Proposition 3.11. Let $K = \mathbb{Q}[\sqrt{d}]$ (where $d \in \mathbb{Z}$ is a squarefree integer) a quadratic number field. Denote by σ (resp. τ) the number of odd prime divisors of d congruent to 3 (mod 4) (resp. 1 (mod 4)). We have the following bounds:

- (1) If $d \equiv 1 \pmod{4}$, $po_K \leq 2^{\frac{\sigma}{2}+\tau-1}$ if d > 0 and $2^{\frac{\sigma-1}{2}+\tau}$ if d < 0.
- (2) If $d \equiv 3 \pmod{4}$, $po_K \leq 2^{\frac{\sigma-1}{2}+\tau}$ if d > 0 and $2^{\frac{\sigma}{2}+\tau}$ if d < 0.
- (3) If $d \equiv 2 \pmod{8}$, $po_K \leq 2^{\frac{\sigma}{2}+\tau}$ if d > 0 and $2^{\frac{\sigma-1}{2}+\tau+1}$ if d < 0.
- (4) If $d \equiv 6 \pmod{8}$, $po_K \leq 2^{\frac{\sigma-1}{2}+\tau}$ if d > 0 and $2^{\frac{\sigma}{2}+\tau}$ if d < 0.

Comparing this bounds with the genus number of quadratic fields [5, §4.2.9], we obtain:

Corollary 3.12. Let $K = \mathbb{Q}[\sqrt{d}]$ (where $d \in \mathbb{Z}$ is a squarefree integer) a quadratic number field. Denote by σ the number of primes $p \equiv 3 \pmod{4}$ which are ramified in K/\mathbb{Q} , then:

$$\frac{g_K}{po_K} \ge 2^{\frac{\sigma}{2}-2} \text{ if } d \text{ is even,}$$
$$\frac{g_K}{po_K} \ge 2^{\frac{\sigma+1}{2}-2} \text{ if } d \text{ is odd }.$$

It follows that, for $\sigma \geq 4$, Γ_K is not a minimal Pólya field over K.

References

- P.J. Cahen, J.L. Chabert, *Integer-valued polynomials*, Mathematical Surveys and Monographs, vol 48, Amer. Math. Soc., Providence (1997).
- [2] J.L Chabert, Factorial Groups and Pólya groups in Galoisian Extension of Q, Proceedings of the fourth international conference on commutative ring theory and applications (2002), 77-86.
- [3] H. Cohen, A Course in Computational Algebraic Number Theory, Springer, 2000.
- [4] H. Furuya, Principal ideal theorem in the genus field for absolutely abelian extensions, J. Number Theory 9 (1977), 4-15.
- [5] G. Gras, Class Field Theory, Springer, 2005.
- [6] K. Hardy, R.H. Hudson, D. Richman, K.S. Williams and N.M. Holtz, Calculation of Class Numbers of Imaginary Cyclic Quartic Fields, *Carleton-Ottawa Mathematical Lecture Note Series* 7 (1986), 201 pp.
- [7] D. Hilbert, Die Theorie der algebraischen Zahlkörper, Jahresbericht der Deutschen Mathematiker-Vereinigung 4 (1894-95), 175-546.
- [8] E.S. Golod, I.R. Shafarevich, On the class field tower, Izv. Akad. Nauk 28 (1964), 261-272.
- [9] A. Leriche, Groupes, Corps et Extensions de Pólya : une question de capitulation, PhD thesis, Université de Picardie Jules Verne (Décembre 2010).
- [10] A. Leriche, Pólya fields, Pólya groups and Pólya extensions: a question of capitulation, Journal de Théorie des Nombres de Bordeaux, 23, (2011), 235-249.
- [11] A. Ostrowski, Über ganzwertige Polynome in algebraischen Zahlkörpren, J. Reine Angew. Math. 149 (1919), 117-124.
- [12] G. Pólya, Über ganzwertige Polynome in algebraischen Zahlkörpern, J. Reine Angew. Math. 149 (1919), 97-116.
- [13] K.S. Williams, Integers of biquadratic fields, Canad. Math. Bull. 13 (1970), 519-526.
- [14] H. Zantema, Integer valued polynomials over a number field, Manusc. Math. 40 (1982), 155-203.

LAMFA, CNRS UMR 6140 Université de Picardie Jules Verne 33, rue Saint-Leu 80039 Amiens & École Centrale de Lille Cité Scientifique 59650 Villeneuve d'Ascq France • amandine.leriche@ec-lille.fr