From Pólya fields to Pólya groups

Jean-Luc Chabert Université de Picardie France

Graz, February 2018

One century ago: the notion of Pólya field

Pólya & Ostrowski. Let K be a number field and

$$\mathrm{Int}(\mathcal{O}_K) = \{f(X) \in K[X] \mid f(\mathcal{O}_K) \subseteq \mathcal{O}_K\}.$$

Does this $\mathcal{O}_K$-module admits a basis with one polynomial of each degree?

Example ($\mathrm{Int}(\mathbb{Z})$: $\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!}$ $(n \geq 0)$.)

Theorem (Pólya & Ostrowski 1919)

$\mathrm{Int}(\mathcal{O}_K)$ *admits such a basis if and only if for every positive integer q the product of all the maximal ideals of $\mathcal{O}_K$ with norm q is a principal ideal.*

Definition (Zantema, 1982)

A Pólya field *is a number field K such that $\mathrm{Int}(\mathcal{O}_K)$ admits a basis with one polynomial of each degree, equivalently, such that*

$$\forall q \qquad \Pi_q(K) = \prod_{\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K), |\mathcal{O}_K/\mathfrak{p}|=q} \mathfrak{p} \quad \text{is principal.}$$

Twenty years ago: Pólya groups

Integer-valued polynomials, 1997:
The Pólya group is a measure of the obstruction for K to be a Pólya field.

Definition

The Pólya group *of a number field K is the subgroup $\mathcal{P}o(K)$ of the class group $Cl(K) = \mathcal{I}_K/\mathcal{P}_K$ generated by the classes of the $\Pi_q(K)$'s.*

$$K \text{ is a Pólya field } \Leftrightarrow \mathcal{P}o(K) = \{1\}$$

Proposition (Hilbert, 1897)

Let $K = \mathbb{Q}(\sqrt{d})$ and let t be the number of ramified primes. Then,

$$|\mathcal{P}o(K)| = \begin{cases} 2^{t-2} & \text{if } K \text{ is real and } N(\mathcal{O}_K^\times) = \{1\} \\ 2^{t-1} & \text{in the other cases} \end{cases}$$

Application: the list of the quadratic Pólya number fields (cf. Zantema).

The aim of my talk

$$K \text{ is a Pólya field } \Leftrightarrow \mathcal{P}o(K) = \{1\}$$

Each assertion about Pólya groups implies a result concerning Pólya fields.

Proposition

If $[K : \mathbb{Q}] = p$ (p odd) with t ramified primes, then $|\mathcal{P}o(K)| = p^{t-1}$

Corollary

If $[K : \mathbb{Q}] = p$ (p odd), then: K is Pólya $\Leftrightarrow$ only one prime is ramified.

Conjecture

An assertion on Pólya fields is the evidence of a statement on Pólya groups

Example (Zantema)

If $K/\mathbb{Q}$ is a non-galoisian cubic extension, then: K is Pólya $\Leftrightarrow h_K = 1$.

The aim of my talk

$$K \text{ is a Pólya field } \Leftrightarrow \mathcal{P}o(K) = \{1\}$$

Each assertion about Pólya groups implies a result concerning Pólya fields.

Proposition

If $[K : \mathbb{Q}] = p$ (p odd) with t ramified primes, then $|\mathcal{P}o(K)| = p^{t-1}$

Corollary

If $[K : \mathbb{Q}] = p$ (p odd), then: K is Pólya $\Leftrightarrow$ only one prime is ramified.

An assertion on Pólya fields is the evidence of a statement on Pólya groups

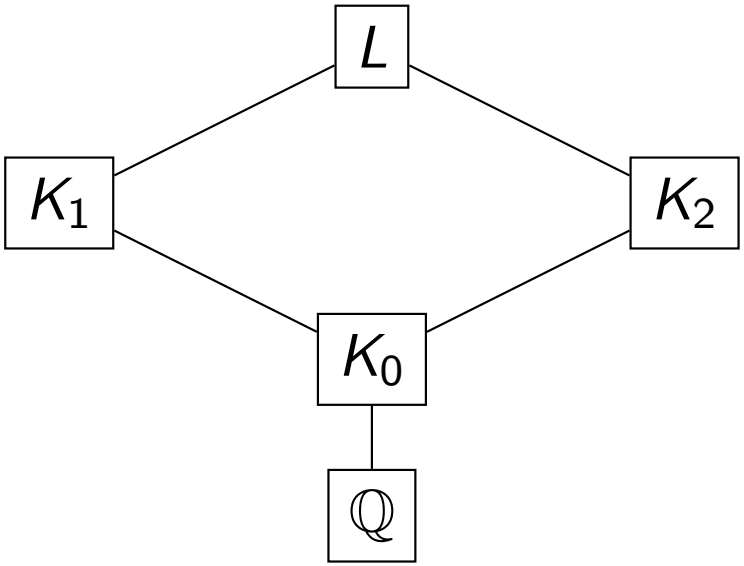
Example (Zantema)

If $K/\mathbb{Q}$ is a non-galoisian cubic extension, $\mathcal{P}o(K) = \{1\} \Leftrightarrow \mathcal{C}l(K) = \{1\}$

Conjecture

If $K/\mathbb{Q}$ is a non-galoisian cubic extension, then $\mathcal{P}o(K) = \mathcal{C}l(K)$.

Galoisian extensions



$K_1/\mathbb{Q}$ et $K_2/\mathbb{Q}$ Galois

$L = K_1 \cdot K_2$

$K_0 = K_1 \cap K_2$

Proposition (Zantema) (Hyp: $\forall p \;\; e_p(K_1/\mathbb{Q}), e_p(K_2/\mathbb{Q})) = 1$)

K_1 *and* K_2 *Pólya* $\Rightarrow$ L *Pólya*

Notation: $\varepsilon_{K_i}^{L} : \overline{\mathfrak{a}} \in Cl(K_i) \mapsto \overline{\mathfrak{a}\,\mathcal{O}_L} \in Cl(L)$ $\qquad$ $\varepsilon_{K_i}^{L}(\mathcal{P}o(K_i)) \subseteq \mathcal{P}o(L)$

Proposition (Revisited) (Hyp: $\forall p \;\; e_p(K_1/\mathbb{Q}), e_p(K_2/\mathbb{Q})) = 1$)

$$\mathcal{P}o(L) = \varepsilon_{K_1}^{L}(\mathcal{P}o(K_1)) + \varepsilon_{K_2}^{L}(\mathcal{P}o(K_2))$$

The reverse implication

Proposition (Zantema)

If K_0 is Pólya and if $([K_1 : K_0], [K_2 : K_0]) = 1$, then:

$$L \text{ Pólya } \Leftrightarrow K_1 \text{ and } K_2 \text{ Pólya}$$

Proposition (Revisited)

If K_0 is Pólya and if $([K_1 : K_0], [K_2 : K_0]) = 1$, then:

$$\mathcal{P}o(L) \simeq \mathcal{P}o(K_1) \oplus \mathcal{P}o(K_2)$$

Proposition (Zantema)

If $[K_1 : K_0], [K_2 : K_0]$ and $[K_0 : \mathbb{Q}]$ are pairwise relatively prime, then:

$$L \text{ Pólya } \Leftrightarrow K_1 \text{ and } K_2 \text{ Pólya}$$

Proposition (Revisited)

If $[K_1 : K_0], [K_2 : K_0]$ and $[K_0 : \mathbb{Q}]$ are pairwise relatively prime, then:

$$\mathcal{P}o(L) \simeq \mathcal{P}o(K_0) \oplus \mathcal{P}o(K_1)/\varepsilon_{K_0}^{K_1}(\mathcal{P}o(K_0)) \oplus \mathcal{P}o(K_2)/\varepsilon_{K_0}^{K_2}(\mathcal{P}o(K_0))$$

Non Galoisian extensions

$[K : \mathbb{Q}] = n \geq 3$, N_K normal closure of K over $\mathbb{Q}$, $G = \mathrm{Gal}(N_K/\mathbb{Q})$

Theorem (Zantema)

If $G = \mathcal{S}_n$ $(n \neq 4)$, or $G = \mathcal{A}_n$ $(n \neq 3, 5)$, or G is a Frobenius group, the following assertions are equivalent:

(i) all the $\Pi_{p^f}(K)$ where p is not ramified are principal

(ii) all the $\Pi_q(K)$ are principal, i.e., K is Pólya.

(iii) all the ideals of $\mathcal{O}_K$ are principal, i.e., $h_K = 1$.

$$\mathcal{P}o(K) = \langle \overline{\Pi_{p^f}(K)} \mid p \in \mathbb{P}, f \in \mathbb{N}^* \rangle \quad \mathcal{P}o(K)_{nr} = \langle \overline{\Pi_{p^f}(K)} \mid p \text{ not ramif.} \rangle$$

$$\mathcal{P}o(K)_{nr} \subseteq \mathcal{P}o(K) \subseteq \mathcal{C}l(K)\,.$$

Theorem (Zantema's theorem in other words)

If $G = \mathcal{S}_n$ $(n \neq 4)$, or $G = \mathcal{A}_n$ $(n \neq 3, 5)$, or G is a Frobenius group, then

$$\mathcal{P}o(K)_{nr} = \{1\} \Leftrightarrow \mathcal{P}o(K) = \{1\} \Leftrightarrow \mathcal{C}l(K) = \{1\}$$

Non Galoisian extensions

$[K : \mathbb{Q}] = n \geq 3$, N_K normal closure of K over $\mathbb{Q}$, $G = \mathrm{Gal}(N_K/\mathbb{Q})$

Theorem (Zantema)

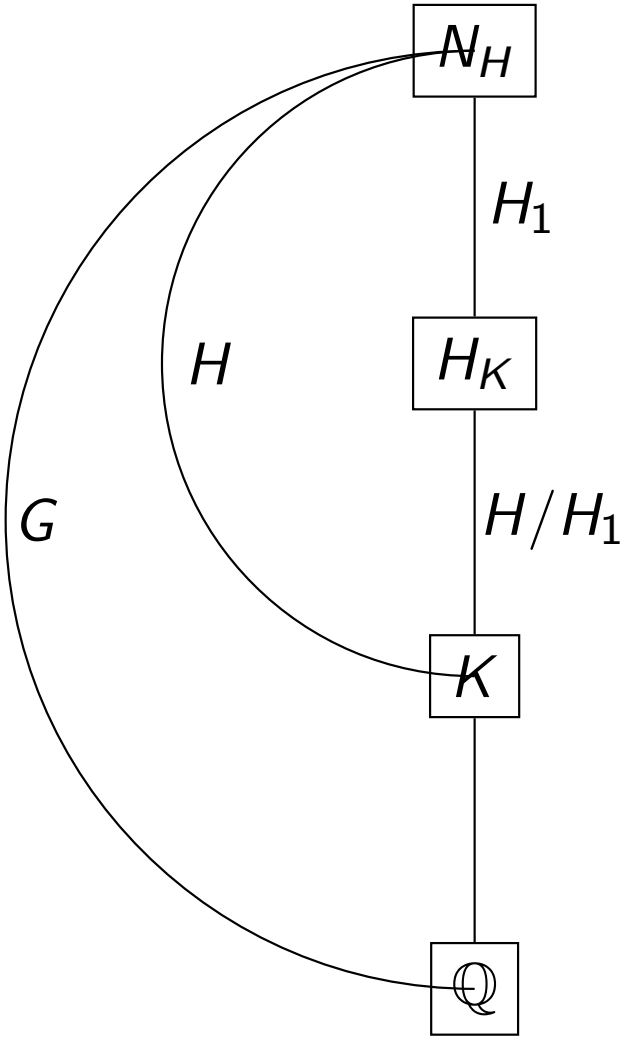
If $G = \mathcal{S}_n$ $(n \neq 4)$, or $G = \mathcal{A}_n$ $(n \neq 3, 5)$, or G is a Frobenius group, then

$$\mathcal{P}o(K)_{nr} = \{1\} \Leftrightarrow \mathcal{P}o(K) = \{1\} \Leftrightarrow \mathcal{C}l(K) = \{1\}$$

My Unreasonable Conjecture

If $G = \mathcal{S}_n$ $(n \neq 4)$, or $G = \mathcal{A}_n$ $(n \neq 3, 5)$, or G is a Frobenius group, then

$$\mathcal{P}o(K)_{nr} = \mathcal{P}o(K) = \mathcal{C}l(K)$$



N_H normal closure of H_K over $\mathbb{Q}$

H_K class field of K

$$H/H_1 = \mathrm{Gal}(H_K/K) \simeq Cl(K)$$

$$\gamma_K : \overline{\mathfrak{a}} \in Cl(K) \mapsto (\mathfrak{a}, H_K/K) \in \mathrm{Gal}(H_K/K)$$

Artin's symbol $(\mathfrak{a}, H_K/K)$ is defined linearly from its values on the primes

$\sigma = (\mathfrak{p}, H_K/K)$ characterized by $\sigma(a) \equiv a^q \pmod{\mathfrak{p}\mathcal{O}_{H_K}}$ with $q = |\mathcal{O}_K/\mathfrak{p}|$

The action of G on the right cosets of H in G

H has n right cosets in G of the form Hs_i $(1 \leq i \leq n)$

By its action on these cosets, G is isomorphic to a subgroup of $\mathcal{S}_n$

Let T be the set formed by the elements of H whose action on the cosets has no fixed point except H itself.

Recall that $$\gamma_K : Cl(K) \xrightarrow{\sim} \mathrm{Gal}(H_K/K) = H/H_1$$

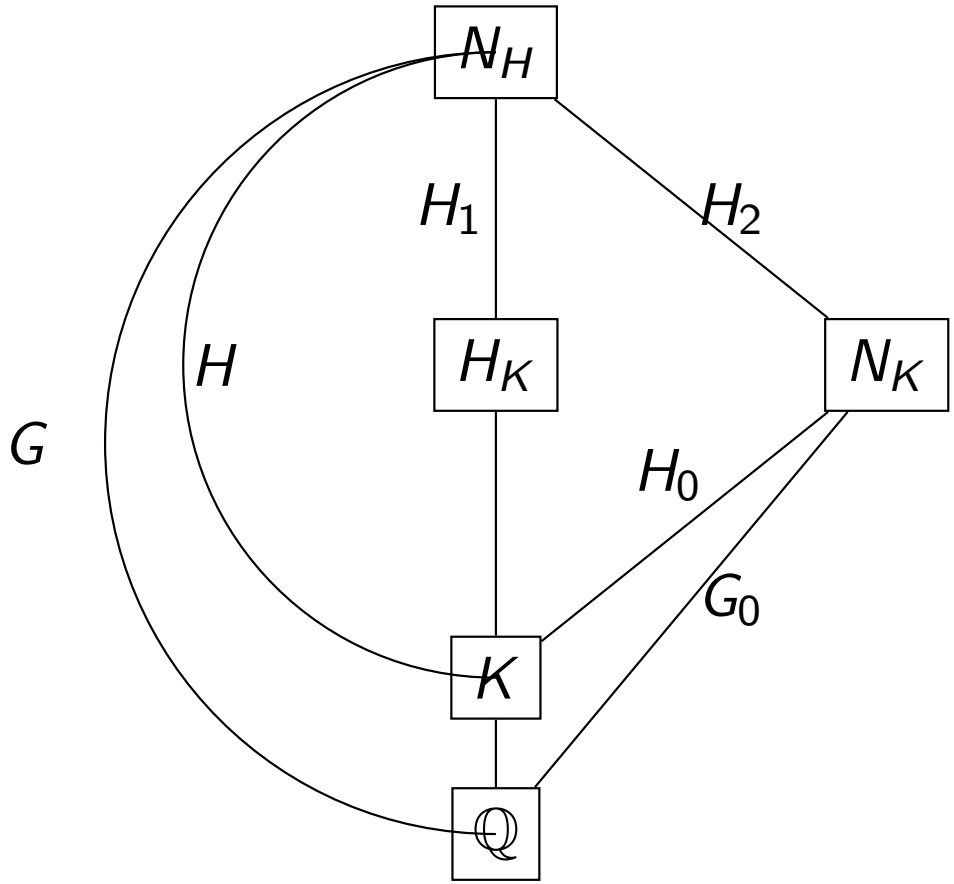
Thanks to $\begin{cases} \text{the properties of Artin's symbols} \\ \text{the decomposition of permutations in disjoint cycles} \end{cases}$

one may prove that:

Lemma (A) ($\gamma_K(\mathcal{P}o(K)_{nr}) \supseteq T \bmod H_1$)

Lemma (B) ($H = \langle T, H_1 \rangle \Rightarrow \mathcal{P}o(K)_{nr} = \mathcal{P}o(K) = Cl(K)$)

The normal closure of K



$$\mathrm{Gal}(N_H/N_K) = H_2$$

$$\mathrm{Gal}(N_K/\mathbb{Q}) = G_0 = G/H_2$$

$$\mathrm{Gal}(N_K/K) = H_0 = H/H_2$$

$$(G, H, T) \mapsto (G_0, H_0, T_0)$$

Lemma C. $T_0 \neq \emptyset \Rightarrow T \neq \emptyset \Rightarrow H_2 \subseteq \langle T \rangle$

Lemma D. $T_0 \neq \emptyset$ and $H_0 = \langle T_0, H_0' \rangle$) $\Rightarrow H = \langle T, H_1 \rangle$

Conclusion

Theorem (Let K be a number field of degree $n \geq 3$)

Let N_K be the normal closure of K, $G_0 = \mathrm{Gal}(N_K/\mathbb{Q})$, $H_0 = \mathrm{Gal}(N_K/K)$, and T_0 be the set formed by the elements of H whose action on the cosets of H_0 in G_0 admits only one fixed point, namely H_0.

If $T_0 \neq \emptyset$ and $H_0 = \langle T_0, H_0' \rangle$, then $\mathcal{P}o(K)_{nr} = \mathcal{P}o(K) = \mathcal{C}l(K)$.

Corollary (The unreasonable conjecture is true)

If $G = \mathcal{S}_n$ $(n \neq 4)$, or $G = \mathcal{A}_n$ $(n \neq 3, 5)$, or G is a Frobenius group, then

$$\mathcal{P}o(K)_{nr} = \mathcal{P}o(K) = \mathcal{C}l(K).$$

(♡) **For any number field K chosen at random, with probability 1**

$\mathrm{Gal}(N_K/\mathbb{Q}) \simeq \mathcal{S}_n$, and hence, $\mathcal{P}o(K) = \mathcal{C}l(K)$.

The End