# Hilbert Class Fields and Embedding Problems

(Lethbridge Number Theory and Combinatorics Seminar)

Abbas Maarefparvar

Department of Mathematics & Computer Science

University of Lethbridge

February 14, 2024

# Outline

# Preliminaries

**Definition**

A number field is a finite extension $K$ of $\mathbb{Q}$, i.e., a $\mathbb{Q}$-vector space of finite dimension. We denote this dimension by $[K : \mathbb{Q}]$ and call it the degree of $K$ over $\mathbb{Q}$.

## Definition

A number field is a finite extension $K$ of $\mathbb{Q}$, i.e., a $\mathbb{Q}$-vector space of finite dimension. We denote this dimension by $[K : \mathbb{Q}]$ and call it the degree of $K$ over $\mathbb{Q}$.

## Example

For $d$, a square-free integer, the number field

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \, : \, a, b \in \mathbb{Q}\}$$

is called a quadratic field.

### Definition

A number field is a finite extension $K$ of $\mathbb{Q}$, i.e., a $\mathbb{Q}$-vector space of finite dimension. We denote this dimension by $[K:\mathbb{Q}]$ and call it the degree of $K$ over $\mathbb{Q}$.

### Example

For $d$, a square-free integer, the number field

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \,:\, a, b \in \mathbb{Q}\}$$

is called a quadratic field.

### Example

Let $\zeta_n = \exp(\frac{2\pi i}{n})$ be a primitive $n^{\text{th}}$ root of unity. The number field

$$\mathbb{Q}(\zeta_n) = \{a_{m-1}\zeta_n^{m-1} + \cdots + a_1\zeta_n + a_0 \,:\, a_i \in \mathbb{Q}, \forall i\}$$

is a cyclotomic field of degree $m = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

**Definition**

Let $K$ be a number field of degree $n$. An element $\alpha \in K$ is called an algebraic integer, if it is a root of a monic polynomial $f(X) \in \mathbb{Z}[X]$.

### Definition

Let $K$ be a number field of degree $n$. An element $\alpha \in K$ is called an algebraic integer, if it is a root of a monic polynomial $f(X) \in \mathbb{Z}[X]$.

### Example

The number $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is an algebraic integer, since it is a root of $X^2 - 2$.

## Definition

Let $K$ be a number field of degree $n$. An element $\alpha \in K$ is called an algebraic integer, if it is a root of a monic polynomial $f(X) \in \mathbb{Z}[X]$.

## Example

The number $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is an algebraic integer, since it is a root of $X^2 - 2$.

## Example

The number $\zeta_n = \exp(\frac{2\pi i}{n}) \in \mathbb{Q}(\zeta_n)$ is an algebraic integer, since it is a root of $X^n - 1$.

## Definition

The set of all algebraic integers of a number field $K$ is denoted by $\mathcal{O}_K$. In fact, $\mathcal{O}_K$ is a ring which is called the ring of integers of $K$.

## Example

Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial. By a theorem of Gauss,

$$\text{if} \quad \frac{a}{b} \in \mathbb{Q},\ f(\frac{a}{b}) = 0 \ \Rightarrow b = \pm 1.$$

Hence the ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$.

## Example

Let $d$ be a square-free integer. Then

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \,:\, a, b \in \mathbb{Z}\}, & d \equiv 2, 3 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \{a + b(\frac{1+\sqrt{d}}{2}) \,:\, a, b \in \mathbb{Z}\}, & d \equiv 1 \pmod 4. \end{cases}$$

## Proposition

Let $K$ be a number field. Then every nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ can be written uniquely in the form

$$\mathfrak{a} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g},$$

where $\mathfrak{P}_i$'s are distinct prime ideals of $\mathcal{O}_K$ and $e_i$'s are positive integers.

## Proposition

Let $K$ be a number field. Then every nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ can be written uniquely in the form

$$\mathfrak{a} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g},$$

where $\mathfrak{P}_i$'s are distinct prime ideals of $\mathcal{O}_K$ and $e_i$'s are positive integers.

## Definition

Let $K/F$ be a finite extension of number fields. A prime ideal $\mathfrak{p}$ of $F$ will factor in $\mathcal{O}_K$, say $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$ ($e_i \geq 1$). The exponents $e_i$'s are called the ramificaton indices of $\mathfrak{p}$ in $K$.

## Proposition

Let $K$ be a number field. Then every nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ can be written uniquely in the form

$$\mathfrak{a} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g},$$

where $\mathfrak{P}_i$'s are distinct prime ideals of $\mathcal{O}_K$ and $e_i$'s are positive integers.

## Definition

Let $K/F$ be a finite extension of number fields. A prime ideal $\mathfrak{p}$ of $F$ will factor in $\mathcal{O}_K$, say $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$ $(e_i \geq 1)$. The exponents $e_i$'s are called the ramificaton indices of $\mathfrak{p}$ in $K$.

- If $e_i > 1$, for at least one $i$, then we say $\mathfrak{p}$ is ramified in $K$;

## Proposition

Let $K$ be a number field. Then every nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ can be written uniquely in the form

$$\mathfrak{a} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g},$$

where $\mathfrak{P}_i$'s are distinct prime ideals of $\mathcal{O}_K$ and $e_i$'s are positive integers.

## Definition

Let $K/F$ be a finite extension of number fields. A prime ideal $\mathfrak{p}$ of $F$ will factor in $\mathcal{O}_K$, say $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$ ($e_i \geq 1$). The exponents $e_i$'s are called the ramificaton indices of $\mathfrak{p}$ in $K$.

- If $e_i > 1$, for at least one $i$, then we say $\mathfrak{p}$ is ramified in $K$;
- If $e_1 = g = 1$, then $\mathfrak{p}$ is said to be inert in $K$;

## Proposition

Let $K$ be a number field. Then every nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ can be written uniquely in the form

$$\mathfrak{a} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g},$$

where $\mathfrak{P}_i$'s are distinct prime ideals of $\mathcal{O}_K$ and $e_i$'s are positive integers.

## Definition

Let $K/F$ be a finite extension of number fields. A prime ideal $\mathfrak{p}$ of $F$ will factor in $\mathcal{O}_K$, say $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$ $(e_i \geq 1)$. The exponents $e_i$'s are called the ramificaton indices of $\mathfrak{p}$ in $K$.

- If $e_i > 1$, for at least one $i$, then we say $\mathfrak{p}$ is ramified in $K$;
- If $e_1 = g = 1$, then $\mathfrak{p}$ is said to be inert in $K$;
- If $g > 1$, and $e_1 = \cdots = e_g = 1$, then $\mathfrak{p}$ is said to split in $K$. If also $f_i := [\frac{\mathcal{O}_K}{\mathfrak{P}_i} : \frac{\mathcal{O}_F}{\mathfrak{p}}] = 1$ for all $i$, $\mathfrak{p}$ is said to split completely in $K$.

### Example

Let $K = \mathbb{Q}(i)$, where $i^2 = -1$. Then $\mathcal{O}_K = \mathbb{Z}[i]$ (The Gaussian integers). We have

- $2\mathcal{O}_K = (1+i)^2$, so 2 ramifies in $\mathbb{Q}(i)$;

## Example

Let $K = \mathbb{Q}(i)$, where $i^2 = -1$. Then $\mathcal{O}_K = \mathbb{Z}[i]$ (The Gaussian integers). We have

- $2\mathcal{O}_K = (1+i)^2$, so 2 ramifies in $\mathbb{Q}(i)$;
- $3\mathcal{O}_K$ is a prime ideal in $\mathbb{Z}[i]$, so 3 is inert in $\mathbb{Q}(i)$;

## Example

Let $K = \mathbb{Q}(i)$, where $i^2 = -1$. Then $\mathcal{O}_K = \mathbb{Z}[i]$ (The Gaussian integers). We have

- $2\mathcal{O}_K = (1+i)^2$, so 2 ramifies in $\mathbb{Q}(i)$;
- $3\mathcal{O}_K$ is a prime ideal in $\mathbb{Z}[i]$, so 3 is inert in $\mathbb{Q}(i)$;
- $5\mathcal{O}_K = (2+i)(2-i)$, so 5 splits (completely) in $\mathbb{Q}(i)$.

## Example

Let $K = \mathbb{Q}(i)$, where $i^2 = -1$. Then $\mathcal{O}_K = \mathbb{Z}[i]$ (The Gaussian integers). We have

- $2\mathcal{O}_K = (1+i)^2$, so 2 ramifies in $\mathbb{Q}(i)$;
- $3\mathcal{O}_K$ is a prime ideal in $\mathbb{Z}[i]$, so 3 is inert in $\mathbb{Q}(i)$;
- $5\mathcal{O}_K = (2+i)(2-i)$, so 5 splits (completely) in $\mathbb{Q}(i)$.

## Remark

In fact, one can show that for an odd prime $p$:

$$p \text{ splits in } \mathbb{Z}[i] \iff p \equiv 1 \pmod 4 \iff p = a^2 + b^2, \text{ for some } a, b \in \mathbb{Z}$$

Let $K$ be a number field and denote its ring of integers by $\mathcal{O}_K$.

- A fractional ideal of $K$, is a non-zero $\mathcal{O}_K$-submodule $\mathfrak{a}$ of $K$ for which there exists an element $0 \neq d \in \mathcal{O}_K$ such that

$$d\mathfrak{a} = \{dx : x \in \mathfrak{a}\} \subseteq \mathcal{O}_K.$$

We denote by $I(K)$ the set of all the fractional ideals of $K$.

Let $K$ be a number field and denote its ring of integers by $\mathcal{O}_K$.

- A fractional ideal of $K$, is a non-zero $\mathcal{O}_K$-submodule $\mathfrak{a}$ of $K$ for which there exists an element $0 \neq d \in \mathcal{O}_K$ such that

$$d\mathfrak{a} = \{dx : x \in \mathfrak{a}\} \subseteq \mathcal{O}_K.$$

  We denote by $I(K)$ the set of all the fractional ideals of $K$.

- A principal fractional ideal of $K$ is of the form

$$\langle b \rangle = b\mathcal{O}_K = \{bx : x \in \mathcal{O}\}$$

  for some $0 \neq b \in K$. We denote by $P(K)$ the set of all the principal fractional ideals of $K$.

Let $K$ be a number field and denote its ring of integers by $\mathcal{O}_K$.

- A fractional ideal of $K$, is a non-zero $\mathcal{O}_K$-submodule $\mathfrak{a}$ of $K$ for which there exists an element $0 \neq d \in \mathcal{O}_K$ such that

$$d\mathfrak{a} = \{dx : x \in \mathfrak{a}\} \subseteq \mathcal{O}_K.$$

  We denote by $I(K)$ the set of all the fractional ideals of $K$.

- A principal fractional ideal of $K$ is of the form

$$\langle b \rangle = b\mathcal{O}_K = \{bx : x \in \mathcal{O}\}$$

  for some $0 \neq b \in K$. We denote by $P(K)$ the set of all the principal fractional ideals of $K$.

- The ideal class group of $K$, denoted by $\mathrm{Cl}(K)$, is defined as

$$\mathrm{Cl}(K) = \frac{I(K)}{P(K)}.$$

### Theorem

Let $K$ be a number field. Then the ideal class group $\mathrm{Cl}(K)$ is a finite abelian group.

### Definition

The class number $h_K$ of $K$ is the order of $\mathrm{Cl}(K)$.

## Theorem

Let $K$ be a number field. Then the ideal class group $\mathrm{Cl}(K)$ is a finite abelian group.

## Definition

The class number $h_K$ of $K$ is the order of $\mathrm{Cl}(K)$.

## Remark

The structure of $\mathrm{Cl}(K)$ indicates how far $\mathcal{O}_K$ is from being a unique factorization domain:

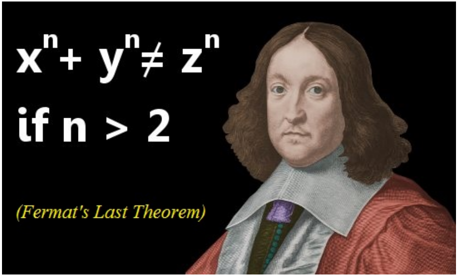
$$h_K = 1 \iff \mathcal{O}_K \text{ is PID} \iff \mathcal{O}_K \text{ is UFD}$$

## Example

The quadratic field $K = \mathbb{Q}(\sqrt{-5})$ has class number 2. Its ring of integers is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ in which we have

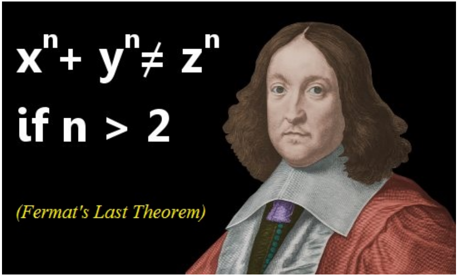
$$6 = 2.3 = (1+\sqrt{-5}).(1-\sqrt{-5}).$$

# The Classical Embedding Problem




### Lamé observation (1847)

Fermat's Last Theorem would be proven if the $p^{\text{th}}$ cyclotomic fields $\mathbb{Q}(\zeta_p)$ had class number 1 for odd primes $p$.




### Lamé observation (1847)

Fermat's Last Theorem would be proven if the $p^{\text{th}}$ cyclotomic fields $\mathbb{Q}(\zeta_p)$ had class number 1 for odd primes $p$.

However, Ernst Kummer had shown three years earlier that this is false for most primes $p$, with $p = 23$ being the famous first example.


## Gauss' class number one problems for quadratic fields (1801)

1. An imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ has class number one, if and only if $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.


### Gauss' class number one problems for quadratic fields (1801)

1. An imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ has class number one, if and only if $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.
   - This problem was solved by Heegner (1954), Baker (1966), and Stark (1967).


## Gauss' class number one problems for quadratic fields (1801)

1. An imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ has class number one, if and only if $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.
   - This problem was solved by Heegner (1954), Baker (1966), and Stark (1967).

2. There are infinitely many real quadratic number fields with class number one
   - This is still an open problem! ▸ quadratic Pólya fields

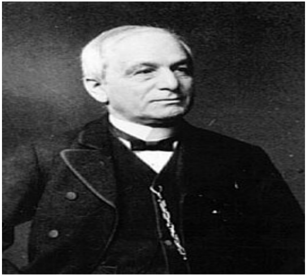
## The classical embedding problem

For $K$, a number field, does exist a finite extension $L/K$ with $h_L = 1$?

## The classical embedding problem

For $K$, a number field, does exist a finite extension $L/K$ with $h_L = 1$?

Kummer didn't have the tools to answer this embedding question; but his work has led to the foundation of class field theory (the study of abelian extensions of arbitrary number fields).

## Kronecker-Weber Theorem

Let $K/\mathbb{Q}$ be a finite abelian extension. Then $K \subseteq \mathbb{Q}(\zeta_n)$ for some positive integer $n$.

## Conjecture (Hilbert, 1902)

For any number field $K$, there exists a unique finite extension $H(K)$ of $K$ such that principal prime ideals $\mathfrak{p}$ of $K$ split completely in $H(K)$:

$$\mathfrak{p}\mathcal{O}_{H(K)} = \mathfrak{P}_1 \dots \mathfrak{P}_g,$$

where $\mathfrak{P}_i$'s are distinct prime ideals of $H(K)$ and $g = [H(K) : K]$.

**Theorem (Furtwängler, 1925)**

Let $K$ be an arbitrary number field. Then there exists a unique finite extension $H(K)$ of $K$ such that the extension $H(K)/K$ is

- unramified (for every prime ideal $\mathfrak{p}$ of $K$, the ideal $\mathfrak{p}\mathcal{O}_{H(K)}$ either remains prime or splits completely in $H(K)$);
- abelian (a finite Galois extension whose Galois group is abelian);
- maximal respect to the above properties.

### Definition

The Hilbert class field of a number field $K$, denoted by $H(K)$, is the maximal abelian unramified extension of $K$.

### Principal Ideal Theorem (Furtwängler, 1930)

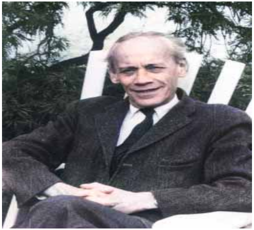
Every fractional ideal $\mathfrak{a}$ of $K$ becomes principal in $H(K)$.

## Definition

The Hilbert class field of a number field $K$, denoted by $H(K)$, is the maximal abelian unramified extension of $K$.

## Principal Ideal Theorem (Furtwängler, 1930)

Every fractional ideal $\mathfrak{a}$ of $K$ becomes principal in $H(K)$.



Artin's reciprocity law gives a canonical isomorphism $\mathrm{Gal}(H(K)/K) \simeq \mathrm{Cl}(K)$. In particular, $[H(K) : K] = h_K$.

## Example

Let $K = \mathbb{Q}(\sqrt{-5})$. Then $H(K) = \mathbb{Q}(\sqrt{-1}, \sqrt{-5})$. Also,

- $\mathrm{Gal}(H(K)/K) \simeq \mathrm{Cl}(K) =< (2, 1 + \sqrt{-5}) >\simeq \mathbb{Z}/2\mathbb{Z}$;
- $(2, 1 + \sqrt{-5})\mathcal{O}_{H(K)} = (1 + \sqrt{-1})$.

## Remark

The number field $K$ has class number 1 if and only if $H(K) = K$. In particular, if $h_K = 1$ then there exists no (non-trivial) abelian unramified extension of $K$.

## Class Field Tower Problem (Furtwängler, 1925)

Let $K = K_1$ be a number field. For every $n \geq 1$, let $K_{n+1}$ be the Hilbert class field of $K_n$. Decide whether the tower

$$K = K_1 \subseteq K_2 \subseteq K_3 \subseteq \dots \qquad \text{(Class Field Tower)}$$

can be infinite, or must always terminate with a field of class number 1 after a finite number of steps.

## Class Field Tower Problem (Furtwängler, 1925)

Let $K = K_1$ be a number field. For every $n \geq 1$, let $K_{n+1}$ be the Hilbert class field of $K_n$. Decide whether the tower

$$K = K_1 \subseteq K_2 \subseteq K_3 \subseteq \dots \qquad \text{(Class Field Tower)}$$

can be infinite, or must always terminate with a field of class number 1 after a finite number of steps.

## Remark

The Class Field Tower Problem is equivalent to the classical embedding problem.

## Example

The class field tower for $\mathbb{Q}(\sqrt{-5})$ is $\mathbb{Q}(\sqrt{-5}) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{-5})$.

For nearly 40 years, no counterexamples emerged, leading many to suppose that class field towers always terminated!

For nearly 40 years, no counterexamples emerged, leading many to suppose that class field towers always terminated!

**A counterexample for Class Field Tower Problem (Golod and Shafarevich, 1964)**

The class field tower for $\mathbb{Q}(\sqrt{-2 \times 3 \times 5 \times 7 \times 11 \times 13})$ is infinite. Equivalently, the quadratic field $\mathbb{Q}(\sqrt{-2 \times 3 \times 5 \times 7 \times 11 \times 13})$ is not contained in any number filed with class number one.

# The New Embedding Problem

# On Pólya fields and Pólya groups

**Theorem (Pólya, 1919)**

A polynomial $f(X) \in \mathbb{Q}[X]$ maps $\mathbb{Z}$ to $\mathbb{Z}$ if and only of it can be written as a finite $\mathbb{Z}$-linear combination of the polynomials

$$\binom{X}{n} = \frac{X(X-1)(X-2)\cdots(X-n+1)}{n!} \quad : \quad n = 0, 1, 2, \cdots .$$

**Definition (Zantema, 1982)**

A number field $K$, with ring of integers $\mathcal{O}_K$, is called a Pólya field, if the $\mathcal{O}_K$-module

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

has a regular basis. That is, an $\mathcal{O}_K$-basis $\{f_n\}_{n\geq 0}$ with $\deg(f_n) = n$.

### Theorem (Ostrowski, 1919)

A number field $K$ is a Pólya field if and only if for every $q$, a prime power, the ideal

$$\Pi_q(K) := \prod_{\substack{\mathfrak{p}\in\mathbb{P}_K \\ N_{K/\mathbb{Q}}(\mathfrak{p})=q}} \mathfrak{p} \qquad \text{(Ostrowski ideal)}$$

is principal (If $q$ is not the norm of any prime ideal of $\mathcal{O}_K$, set $\Pi_q(K) = \mathcal{O}_K$).

**Definition(Cahen-Chabert, 1997)**

The *Pólya group* of a number field $K$, denoted by $\mathrm{Po}(K)$, is the subgroup of $\mathrm{Cl}(K)$ defined as follows

$$\mathrm{Po}(K) = \langle [\Pi_q(K)] \,:\, q \text{ is a prime power} \rangle.$$

relative Pólya group

## Definition(Cahen-Chabert, 1997)

The *Pólya group* of a number field $K$, denoted by $\mathrm{Po}(K)$, is the subgroup of $\mathrm{Cl}(K)$ defined as follows

$$\mathrm{Po}(K) = \langle [\Pi_q(K)] \,:\, q \text{ is a prime power} \rangle.$$

▸ relative Pólya group

## Remark

The number field $K$ is Pólya if and only if $\mathrm{Po}(K) = 0$. In particular, if $h_K = 1$ then $K$ is a Pólya field.

### Theorem (Zantema, 1982)

A quadratic number field $K = \mathbb{Q}(\sqrt{d})$ is a Pólya field if and only if one of the following conditions holds:

- $d = -1, -2, -p$, where $p \equiv 3 \pmod 4$ is a prime number;
- $d = p$, where $p$ is a prime number;
- $d = 2p, pq$, where $p \equiv q \pmod 4$ are primes, and $x^2 - y^2 d = -1$ has no solution in $\mathcal{O}_K$.

◂ Gauss' conjecture

**Theorem (Zantema, 1982)**

Every cyclotomic field $\mathbb{Q}(\zeta_n)$ is a Pólya field.

**Theorem (Zantema, 1982)**

Every cyclotomic field $\mathbb{Q}(\zeta_n)$ is a Pólya field.

**The Kronecker-Weber Theorem**

Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.

## Theorem (Zantema, 1982)

Every cyclotomic field $\mathbb{Q}(\zeta_n)$ is a Pólya field.

## The Kronecker-Weber Theorem

Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.

## Corollary

The quadratic field $\mathbb{Q}(\sqrt{-2 \times 3 \times 5 \times 7 \times 11 \times 13})$ is contained in a Pólya field.

## The New Embedding Problem (Leriche, 2014)

Is a number field $K$ contained in a Pólya field?

## Theorem (Leriche, 2014)

Let $K$ be a number field. Then the Hilbert class field of $K$, i.e., $H(K)$, is Pólya field. In particular, $K$ is contained in a Pólya field, namely its Hilbert class field.

# The Relativized Version of New Embedding Problem

# Relative Pólya group

**Definition (M.-Rajaei, 2020 & Chabert 2019)**

Let $L/K$ be a finite extension of number fields. The *relative Pólya group* of $L/K$, denoted by $\mathrm{Po}(L/K)$, is defined as

$$\mathrm{Po}(L/K) = \left\langle \left[ \overbrace{\Pi_{\mathfrak{p}^f}(L/K)}^{\text{relative Ostrowski ideals}} = \prod_{\substack{\mathfrak{P}\in\mathbb{P}_L \\ N_{L/K}(\mathfrak{P})=\mathfrak{p}^f}} \mathfrak{P} \right] : \mathfrak{p}\in\mathbb{P}_K\,,\, f\in\mathbb{N} \right\rangle.$$

In particular, $\mathrm{Po}(L/\mathbb{Q}) = \mathrm{Po}(L)$ and $\mathrm{Po}(L/L) = \mathrm{Cl}(L)$. ◂ Pólya group

# Relative Pólya group

**Definition (M.-Rajaei, 2020 & Chabert 2019)**

Let $L/K$ be a finite extension of number fields. The *relative Pólya group* of $L/K$, denoted by $\mathrm{Po}(L/K)$, is defined as

$$\mathrm{Po}(L/K) = \left\langle \left[ \overbrace{\Pi_{\mathfrak{p}^f}(L/K)}^{\text{relative Ostrowski ideals}} = \prod_{\substack{\mathfrak{P}\in\mathbb{P}_L \\ N_{L/K}(\mathfrak{P})=\mathfrak{p}^f}} \mathfrak{P} \right] : \mathfrak{p} \in \mathbb{P}_K\,,\, f \in \mathbb{N} \right\rangle.$$

In particular, $\mathrm{Po}(L/\mathbb{Q}) = \mathrm{Po}(L)$ and $\mathrm{Po}(L/L) = \mathrm{Cl}(L)$. ◂ Pólya group

**Theorem (M.-Rajaei, 2020)**

Let $F \subseteq K \subseteq L$ be a tower of finite extensions of number fields. If $L/K$ is Galois, then $\mathrm{Po}(L/F) \subseteq \mathrm{Po}(L/K)$. In particular,

$$\mathrm{Po}(L) = \mathrm{Po}(L/\mathbb{Q}) \subseteq \mathrm{Po}(L/K).$$

### The relativized version of new embedding problem

Is every number field $K$ contained in a number field $L$ with $\mathrm{Po}(L/K) = 0$?

## The relativized version of new embedding problem

Is every number field $K$ contained in a number field $L$ with $\mathrm{Po}(L/K) = 0$?

### Theorem (M.-Rajaei, 2020)

Let $L/K$ be a finite Galois extension of number fields. Then there exists a surjective map

$$\psi : \bigoplus_{\mathfrak{p} \in \mathbb{P}_K} \frac{\mathbb{Z}}{e_{\mathfrak{p}(L/K)}\mathbb{Z}} \to \frac{\mathrm{Po}(L/K)}{\epsilon_{L/K}(\mathrm{Cl}(K))},$$

where $e_{\mathfrak{p}(L/K)}$ denotes the ramification index of $\mathfrak{p}$ in $L/K$, and $\epsilon_{L/K} : [\mathfrak{a}] \in \mathrm{Cl}(K) \to [\mathfrak{a}\mathcal{O}_L] \in \mathrm{Cl}(L)$ denotes the *capitulation map*.

### Theorem (M.-Rajaei, 2020)

Let $L/K$ a finite Galois extension of number fields. If $L/K$ is unramified at all prime ideals of $K$, then $\mathrm{Po}(L/K) = \epsilon_{L/K}(\mathrm{Cl}(K))$.

### Corollary (M.-Rajaei, 2020)

Let $K$ be a number field, and denote its Hilbert class field by $H(K)$. Then $\mathrm{Po}(H(K)/K) = 0$. In particular, $K$ is contained in a number field with trivial relative Pólya group (over $K$).

Proof. Since $H(K)/K$ is unramified, $\mathrm{Po}(H(K)/K) = \epsilon_{H(K)/K}(\mathrm{Cl}(K))$. By the Principal Ideal Theorem, $\epsilon_{H(K)/K}(\mathrm{Cl}(K)) = 0$.

- Since
$$\mathrm{Po}(H(K)) = \mathrm{Po}(H(K)/\mathbb{Q}) \subseteq \mathrm{Po}(H(K)/K) = 0,$$
we obtain Leriche's result on Pólya-ness of Hilbert Class Fields.

- Since
$$\mathrm{Po}(H(K)) = \mathrm{Po}(H(K)/\mathbb{Q}) \subseteq \mathrm{Po}(H(K)/K) = 0,$$
we obtain Leriche's result on Pólya-ness of Hilbert Class Fields.
- Let
$$K = K_1 \subseteq K_2 = H(K_1) \subseteq K_3 = H(K_2) \subseteq \dots,$$
be the class field tower of $K$. Then
$$\mathrm{Po}(K_i/K) = 0, \quad \forall i = 2, 3 \dots.$$

For instance, for $K = \mathbb{Q}(\sqrt{-2 \times 3 \times 5 \times 7 \times 11 \times 13})$, there are infinitely many number fields, containing $K$, whose relative Pólya groups over $K$ are trivial.


Happy
Valentine's
Day!