Pólya and pre-Pólya Groups in Dihedral Number Fields

Abbas Maarefparvar

School of Mathematics

IPM

April 26, 2021

Outline

Outline

1. A brief historical background
    1. Integer valued polynomials

Outline

1. A brief historical background
    1. Integer valued polynomials
    2. Pólya fields

Outline

1. A brief historical background
    1. Integer valued polynomials
    2. Pólya fields
    3. Pólya groups

Outline

1. A brief historical background
    1. Integer valued polynomials
    2. Pólya fields
    3. Pólya groups
2. Pólya groups in “odd prime degree” dihedral fields

Outline

1. A brief historical background
    1. Integer valued polynomials
    2. Pólya fields
    3. Pólya groups
2. Pólya groups in “odd prime degree” dihedral fields
    1. An exact sequense of Pólya groups

Outline

Outline

1. A brief historical background
   1. Integer valued polynomials
   2. Pólya fields
   3. Pólya groups
2. Pólya groups in “odd prime degree” dihedral fields
   1. An exact sequense of Pólya groups
   2. Maximum ramification
   3. Divisibility of class numbers

Outline

1. A brief historical background
   1. Integer valued polynomials
   2. Pólya fields
   3. Pólya groups
2. Pólya groups in “odd prime degree” dihedral fields
   1. An exact sequense of Pólya groups
   2. Maximum ramification
   3. Divisibility of class numbers
3. Relative Pólya group

Outline

1. A brief historical background
    1. Integer valued polynomials
    2. Pólya fields
    3. Pólya groups
2. Pólya groups in “odd prime degree” dihedral fields
    1. An exact sequense of Pólya groups
    2. Maximum ramification
    3. Divisibility of class numbers
3. Relative Pólya group
    1. Generalization of Zantema’s exact sequence

Outline

1. A brief historical background
   1. Integer valued polynomials
   2. Pólya fields
   3. Pólya groups
2. Pólya groups in “odd prime degree” dihedral fields
   1. An exact sequense of Pólya groups
   2. Maximum ramification
   3. Divisibility of class numbers
3. Relative Pólya group
   1. Generalization of Zantema’s exact sequence
4. Non-Galois extensions

Outline

1. A brief historical background
    1. Integer valued polynomials
    2. Pólya fields
    3. Pólya groups
2. Pólya groups in “odd prime degree” dihedral fields
    1. An exact sequense of Pólya groups
    2. Maximum ramification
    3. Divisibility of class numbers
3. Relative Pólya group
    1. Generalization of Zantema’s exact sequence
4. Non-Galois extensions
    1. pre-Pólya group

Outline

1. A brief historical background
   1. Integer valued polynomials
   2. Pólya fields
   3. Pólya groups
2. Pólya groups in “odd prime degree” dihedral fields
   1. An exact sequense of Pólya groups
   2. Maximum ramification
   3. Divisibility of class numbers
3. Relative Pólya group
   1. Generalization of Zantema’s exact sequence
4. Non-Galois extensions
   1. pre-Pólya group
   2. Even dihedral extensions of $\mathbb{Q}$

Outline

1. A brief historical background
   1. Integer valued polynomials
   2. Pólya fields
   3. Pólya groups
2. Pólya groups in "odd prime degree" dihedral fields
   1. An exact sequense of Pólya groups
   2. Maximum ramification
   3. Divisibility of class numbers
3. Relative Pólya group
   1. Generalization of Zantema's exact sequence
4. Non-Galois extensions
   1. pre-Pólya group
   2. Even dihedral extensions of $\mathbb{Q}$
   3. Maximum ramification in Pólya D_4-fields

Integer Valued Polynomials in $\mathbb{Q}[X]$

Theorem (Pólya, 1919)

For a polynomial $f(X) \in \mathbb{Q}[X]$, we have $f(\mathbb{Z}) \subseteq \mathbb{Z}$ if and only if it can be written as a $\mathbb{Z}$-linear combination of the polynomials

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

▸ regular basis

Replace $\mathbb{Q}$ with K

Definition (Ring of integer valued polynomials)

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

$\mathfrak{J}_n(K) = \{\text{leading coefficients of } \quad f(X) \in \mathrm{Int}(\mathscr{O}_K), \deg(f) = n\} \cup \{0\}$.

Proposition

$\mathrm{Int}(\mathscr{O}_K) \simeq \bigoplus_{n=0}^{\infty} \mathfrak{J}_n(K)$ (as $\mathscr{O}_K$-module).

Replace $\mathbb{Q}$ with K

Definition (Ring of integer valued polynomials)

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

$\mathfrak{I}_n(K) = \{\text{leading coefficients of} \quad f(X) \in \mathrm{Int}(\mathcal{O}_K), \deg(f) = n\} \cup \{0\}$.

Proposition

$\mathrm{Int}(\mathcal{O}_K) \simeq \bigoplus_{n=0}^{\infty} \mathfrak{I}_n(K)$ (as $\mathcal{O}_K$-module).

Replace $\mathbb{Q}$ with K

Definition (Ring of integer valued polynomials)

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

$\mathfrak{I}_n(K) = \{\text{leading coefficients of} \quad f(X) \in \mathrm{Int}(\mathcal{O}_K), \deg(f) = n\} \cup \{0\}$.

Proposition

$\mathrm{Int}(\mathcal{O}_K) \simeq \bigoplus_{n=0}^{\infty} \mathfrak{I}_n(K)$ (as $\mathcal{O}_K$-module).

$\mathrm{Int}(\mathscr{O}_K)$ is a free $\mathscr{O}_K$-module

Definition

If $\mathrm{Int}(\mathscr{O}_K)$ has an $\mathscr{O}_K$ basis with exactly one member from each degree, we say that $\mathrm{Int}(\mathscr{O}_K)$ has a regular basis.

$\mathrm{Int}(\mathcal{O}_K)$ is a free $\mathcal{O}_K$-module

Definition

If $\mathrm{Int}(\mathcal{O}_K)$ has an $\mathcal{O}_K$ basis with exactly one member from each degree, we say that $\mathrm{Int}(\mathcal{O}_K)$ has a regular basis.

Example

By Pólya's result, $\{\binom{X}{n}\}_{n\geq 0}$ is a regular basis for $\mathrm{Int}(\mathbb{Z})$.

Go back

Existence of a regular basis

Theorem (Pólya, 1919)

$\mathrm{Int}(\mathscr{O}_\mathrm{K})$ has a regular basis iff all the ideals $\mathfrak{J}_\mathrm{n}(\mathrm{K})$'s are principal.

Existence of a regular basis

Theorem (Pólya, 1919)

$\mathrm{Int}(\mathscr{O}_K)$ has a regular basis iff all the ideals $\mathfrak{J}_n(K)$'s are principal.

Proposition (Bhargava, 1997)

$$n!_{\mathscr{O}_K} = \mathfrak{J}_n(K)^{-1}.$$

Ostrowski Ideals

Theorem(Ostrowski, 1919)

Int $(\mathscr{O}_K)$ has a regular basis if and only if all the ideals

Ostrowski Ideals

Theorem(Ostrowski, 1919)

Int $(\mathscr{O}_K)$ has a regular basis if and only if all the ideals

$$\Pi_q(K) =: \prod_{\substack{\mathfrak{m}\in \mathrm{Max}(\mathscr{O}_K) \\ \mathscr{N}_{K/\mathbb{Q}}(\mathfrak{m})=q}} \mathfrak{m}$$

Ostrowski Ideals

Theorem(Ostrowski, 1919)

Int $(\mathscr{O}_K)$ has a regular basis if and only if all the ideals

$$\Pi_q(K) =: \prod_{\substack{\mathfrak{m} \in \mathrm{Max}(\mathscr{O}_K) \\ \mathscr{N}_{K/\mathbb{Q}}(\mathfrak{m}) = q}} \mathfrak{m}$$

are principal.

Ostrowski Ideals

Theorem(Ostrowski, 1919)

Int $(\mathscr{O}_K)$ has a regular basis if and only if all the ideals

$$\Pi_q(K) =: \prod_{\substack{\mathfrak{m}\in \mathrm{Max}(\mathscr{O}_K)\\ \mathscr{N}_{K/\mathbb{Q}}(\mathfrak{m})=q}} \mathfrak{m}$$

are principal.

Ostrowski Ideals

Theorem (Ostrowski, 1919)

Int $(\mathscr{O}_K)$ has a regular basis if and only if all the ideals

$$\Pi_q(K) =: \prod_{\substack{\mathfrak{m} \in \mathrm{Max}(\mathscr{O}_K) \\ \mathscr{N}_{K/\mathbb{Q}}(\mathfrak{m}) = q}} \mathfrak{m}$$

are principal.

Convention

If p^f is not the norm of any maximal ideal of $\mathscr{O}_K$, put $\Pi_{p^f}(K) = \mathscr{O}_K$.

Definition (Zantema, 1982)

A number field K is called a Pólya field, if the following equivalent conditions hold:

- $\mathrm{Int}(\mathscr{O}_K)$ has a regular basis;
- All the characteristic ideals $\mathfrak{J}_n(K)$'s are principal;
- All the Ostrowski ideals $\Pi_q(K)$'s are principal;
- All the Bhargava factorial ideals of K are principal.

Some Families of Pólya Fields

Example

The following number fields are Pólya fields:

1. Class number one number fields (Obviously, but not conversely!);
2. Cyclotomic fields (Zantema, 1982);
3. Abelian number fields with only one ramified prime (Zantema, 1982);
4. Hilbert class field of a number field (Leriche, 2014).
5. Genus field of an abelian number field (Leriche, 2014).

measure of the obstruction for K to be Pólya

Definition(Cahen-Chabert, 1997)

The Pólya group of K is the subgroup **Po**(K) of the class group **Cl**(K) generated by the classes of the ideals $\Pi_{p^f}(K)$:

$$\mathbf{Po}(K) = < \left[\Pi_{p^f}(K)\right] : p \in \mathbb{P}, f \in \mathbb{N} > .$$

measure of the obstruction for K to be Pólya

Definition(Cahen-Chabert, 1997)

The Pólya group of K is the subgroup $\mathbf{Po}(K)$ of the class group $\mathbf{Cl}(K)$ generated by the classes of the ideals $\Pi_{p^f}(K)$:

$$\mathbf{Po}(K) = < \left[\Pi_{p^f}(K)\right] : p \in \mathbb{P}, f \in \mathbb{N} > .$$

Remark (Ostrowski)

For a Galois extension $K/\mathbb{Q}$,

$$\mathbf{Po}(K) = < \left[\Pi_{p^f}(K)\right] : p \text{ is a ramified prime in } K, f \in \mathbb{N} > .$$

Non-Galois case

Galois action on ideal class group

Proposition(Brumer-Rosen, 1963)

For a Galois extension $K/\mathbb{Q}$, $\mathscr{P}o(K)$ and the group of strongly ambiguous ideal classes in K, coincide.

Example(Hilbert, 1897)

Let K be a quadratic field and denote the number of ramifid primes in $K/\mathbb{Q}$ by s_K. Then

$$|\mathscr{P}o(K)| = \begin{cases} 2^{s_k - 2} & : K \text{ is real and } N_{K/\mathbb{Q}}(\mathscr{O}_K^\times) = \{1\} \\ 2^{s_k - 1} & : \text{Otherwise} \end{cases}$$

Ramification is very restricted

Proposition (Zantema, 1982)

Let $K/\mathbb{Q}$ be a Galois extension with Galois group G. Then the following sequence is exact:

$$\{0\} \to H^1(G, U_K) \to \bigoplus_{p \text{ prime}} \mathbb{Z}/e(p)\mathbb{Z} \to \mathscr{P}o(K) \to \{0\}$$

where $e(p)$ denotes the ramification index of p in $K/\mathbb{Q}$.

Corollary

For a Galois extension $K/\mathbb{Q}$, if $\gcd(h_K, [K:\mathbb{Q}]) = 1$ then K is Pólya; but not converesely.

relative case | Max ramification in S_3-extensions | Improving Ishida's result

Relative Pólya group

Definition (-, A. Rajaei, 2020 & Chabert, 2019)

For a finite extension K/P of number fields, relative Pólya group $\mathbf{Po}(K/P)$, is defined as follows:

$$\mathbf{Po}(K/P) = < \left[\Pi_{\mathfrak{P}^f}(K/P) = \prod_{\substack{\mathfrak{M} \in \mathrm{Max}(\mathcal{O}_K) \\ N_{K/P}(\mathfrak{M}) = \mathfrak{P}^f}} \mathfrak{M} \right] : \mathfrak{P} \text{ is a prime of } P, f \in \mathbb{N} > .$$

In particular, $\mathbf{Po}(K/\mathbb{Q}) = \mathbf{Po}(K)$ and $\mathbf{Po}(K/K) = \mathbf{Cl}(K)$.

Theorem (-, A. Rajaei, J. Number Theory, 2020)

Let K/P be a finite Galois extension of number fields with Galois group G. Then we have an exact sequence as follows:

$$\{0\} \to \mathrm{Ker}(\varepsilon_{K/P}) \to H^1(G, U_K) \to \bigoplus_{\mathfrak{P}\text{ a prime of } P} \mathbb{Z}/e_{\mathfrak{P}}\mathbb{Z} \to \frac{\mathrm{Po}(K/P)}{\varepsilon_{K/P}(\mathrm{Cl}(P))} \to \{0\},$$

where $\varepsilon_{K/P} : [\mathfrak{a}] \in \mathrm{Cl}(P) \mapsto [\mathfrak{a}\mathscr{O}_K] \in \mathrm{Cl}(K)$ denotes the transfer of ideal classes, and $e_{\mathfrak{P}}$ denotes the ramification index of $\mathfrak{P}$ in K/P. ◂ Zantema's exact sequence

▸ even dihedral fields

Corollary

For a finite Galois extension K/P, if $\gcd(h_K, [K:P]) = 1$, then $\mathrm{Po}(K/P) = \varepsilon_{K/P}(\mathrm{Cl}(P))$. ▸ even dihedral fields

Lemma (-, A. Rajaei, J. Number Theory, 2020)

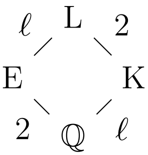
Let $P \subseteq K \subseteq L$ be a tower of finite extensions of number fields.

(i) If K/P and L/P are Galois extensions, then $\varepsilon_{L/K}(\mathbf{Po}(K/P)) \subseteq \mathbf{Po}(L/P)$.

(ii) If L/K is a Galois extension, then $\mathbf{Po}(L/P) \subseteq \mathbf{Po}(L/K)$.

even dihedral fields

Pólya odd prime dihedral extensions of $\mathbb{Q}$



$\mathrm{Gal}(L/\mathbb{Q}) \simeq D_\ell$, ℓ an odd prime

Lemma (-, A. Rajaei, J. Number Theory, 2020)

Let K be a D_ℓ-field with Galois closure L, and denote by E the unique quadratic subfield of L. For each ramified prime p in $L/\mathbb{Q}$:

1. if $p\mathcal{O}_L = (\gamma_1\gamma_2\ldots\gamma_\ell)^2$, then $p\mathcal{O}_K = \beta_1\beta_2^2\ldots\beta_{\frac{\ell+1}{2}}^2$, and

$$\Pi_p(L) \text{ is principal} \Leftrightarrow \Pi_p(E) \text{ is principal}$$

proof for maximum ramification

Lemma (-, A. Rajaei, J. Number Theory, 2020)

Let K be a D_ℓ-field with Galois closure L, and denote by E the unique quadratic subfield of L. For each ramified prime p in $L/\mathbb{Q}$:

1. if $p\mathscr{O}_L = (\gamma_1\gamma_2\ldots\gamma_\ell)^2$, then $p\mathscr{O}_K = \beta_1\beta_2^2\ldots\beta_{\frac{\ell+1}{2}}^2$, and

$$\Pi_p(L) \text{ is principal} \Leftrightarrow \Pi_p(E) \text{ is principal}$$

2. If $p\mathscr{O}_L = \gamma^\ell$ or $p\mathscr{O}_L = (\gamma_1\gamma_2)^\ell$, then $p\mathscr{O}_K = \beta^\ell$, and

$$\Pi_p(L) \text{ is principal} \Leftrightarrow \Pi_p(K) \text{ is principal}$$

proof for maximum ramification

Lemma (-, A. Rajaei, J. Number Theory, 2020)

Let K be a D_ℓ-field with Galois closure L, and denote by E the unique quadratic subfield of L. For each ramified prime p in $L/\mathbb{Q}$:

1. if $p\mathscr{O}_L = (\gamma_1\gamma_2\ldots\gamma_\ell)^2$, then $p\mathscr{O}_K = \beta_1\beta_2^2\ldots\beta_{\frac{\ell+1}{2}}^2$, and

$$\Pi_p(L) \text{ is principal} \Leftrightarrow \Pi_p(E) \text{ is principal}$$

2. If $p\mathscr{O}_L = \gamma^\ell$ or $p\mathscr{O}_L = (\gamma_1\gamma_2)^\ell$, then $p\mathscr{O}_K = \beta^\ell$, and

$$\Pi_p(L) \text{ is principal} \Leftrightarrow \Pi_p(K) \text{ is principal}$$

3. If $p\mathscr{O}_L = \gamma^{2\ell}$, then $p = \ell$, $\ell\mathscr{O}_K = \beta^\ell$ and

$$\Pi_\ell(L) \text{ is principal} \Leftrightarrow \Pi_\ell(K) \text{ and } \Pi_\ell(E) \text{ are principal}$$

proof for maximum ramification

Theorem (-, A. Rajaei, J. Number Theory, 2020)

Let K be a D_ℓ-field with Galois closure L, and denote by E the unique quadratic subfield of L. Then we have an exact sequence as follows:

$$\{0\} \longrightarrow \mathscr{P}o(E) \xrightarrow[{[\mathfrak{a}]\mapsto[\mathfrak{a}\mathscr{O}_L]}]{\epsilon_{L/E}} \mathscr{P}o(L) \xrightarrow{\mathscr{N}_{L/K}\circ\pi_\ell} \mathscr{P}o(K).$$

Moreover, $(\mathscr{P}o(L))_2 \simeq \mathscr{P}o(E)$ and $(\mathscr{P}o(L))_\ell \hookrightarrow \mathscr{P}o(K)$.

proof for maximum ramification | Improving Ishida's result

$(\mathscr{P}o(L))_2 \simeq \mathscr{P}o(E)$ and $(\mathscr{P}o(L))_\ell \hookrightarrow \mathscr{P}o(K)$

Example

Let $K = \mathbb{Q}(\boldsymbol{\theta})$, where $\boldsymbol{\theta}$ is a root of

$$f(X) = X^5 - 2X^4 + 7X^3 - 11X^2 + 5X + 1.$$

Then

- K is a D_5-field;
- $\mathrm{disc}(K) = 1367^2$;
- $h_K = 4$;
- $E = \mathbb{Q}(\sqrt{-1367})$ is the unique quadratic subfield of Galois closure L of K.

$$(\mathscr{P}o(L))_2 \simeq \mathscr{P}o(E) \text{ and } (\mathscr{P}o(L))_\ell \hookrightarrow \mathscr{P}o(K)$$

Example

Let $K = \mathbb{Q}(\theta)$, where θ is a root of

$$f(X) = X^5 - 2X^4 + 7X^3 - 11X^2 + 5X + 1.$$

Then

- K is a D_5-field;
- $\mathrm{disc}(K) = 1367^2$;
- $h_K = 4$;
- $E = \mathbb{Q}(\sqrt{-1367})$ is the unique quadratic subfield of Galois closure L of K.

E is Pólya and $5 \nmid h_K \implies$ L is a Pólya D_5-extension of $\mathbb{Q}$.

$$\{0\} \longrightarrow \mathscr{P}o(E) \longrightarrow \mathscr{P}o(L) \longrightarrow \mathscr{P}o(K).$$

Corollary (-, A. Rajaei, J. Number Theory, 2020)

Let K be a D_ℓ-field with Galois closure L, and denote the unique quadratic subfield of L by E. If either

- $\ell \nmid h_K$;
- or L/E is unramified,

then $Po(L) \simeq Po(E)$.

Corollary (-, A. Rajaei, J. Number Theory, 2020)

With the above notations, if L is the splitting field of an irreducible polynomial

$$f(X) = X^\ell + a_2X^{\ell-2} + a_3X^{\ell-3} + \cdots + a_{\ell-1}X + a_\ell, \quad a_i \in \mathbb{Z}$$

over $\mathbb{Q}$. If $\gcd(a_2, a_3, \ldots, a_{\ell-1}, \ell.a_\ell) = 1$, then $Po(E) \simeq Po(L)$.

$$\{0\} \longrightarrow \mathscr{P}o(E) \longrightarrow \mathscr{P}o(L) \longrightarrow \mathscr{P}o(K).$$

Corollary (-, A. Rajaei, J. Number Theory, 2020)

Let K be a D_ℓ-field with Galois closure L, and denote the unique quadratic subfield of L by E. If either

- $\ell \nmid h_K$;
- or L/E is unramified,

then $\mathbf{Po}(L) \simeq \mathbf{Po}(E)$.

Corollary (-, A. Rajaei, J. Number Theory, 2020)

With the above notations, if L is the splitting field of an irreducible polynomial

$$f(X) = X^\ell + a_2X^{\ell-2} + a_3X^{\ell-3} + \cdots + a_{\ell-1}X + a_\ell, \quad a_i \in \mathbb{Z}$$

over $\mathbb{Q}$. If $\mathbf{gcd}(a_2, a_3, \ldots, a_{\ell-1}, \ell.a_\ell) = 1$, then $\mathbf{Po}(E) \simeq \mathbf{Po}(L)$.

Theorem (A. Leriche, J. Number Theory, 2013)

Let $M/\mathbb{Q}$ be a Pólya Galois extension of degree n, and denote the number of ramified primes in $M/\mathbb{Q}$ by s_M. Then

$$s_M \leq \sum_{p|n} n\left(\frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^{v_p(n)}}\right) + v_p(n)$$

Example

For $[M:\mathbb{Q}] = 2\ell$ (ℓ an odd prime), $s_M \leq \ell + 4$. D_ℓ-extensions

Theorem (A. Leriche, J. Number Theory, 2013)

Let $M/\mathbb{Q}$ be a Pólya Galois extension of degree n, and denote the number of ramified primes in $M/\mathbb{Q}$ by s_M. Then

$$s_M \leq \sum_{p|n} n\left(\frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^{\nu_p(n)}}\right) + \nu_p(n)$$

Example

For $[M:\mathbb{Q}] = 2\ell$ (ℓ an odd prime), $s_M \leq \ell + 4$. ▸ D_ℓ-extensions

Maximum ramification in Pólya S_3-extensions of $\mathbb{Q}$

Theorem (-, A. Rajaei, Proc. Roy. Soc. Edinburgh Sect. A, 2019)

Let K be a non-Galois cubic field with Galois closure L and $E = \mathbb{Q}(\sqrt{\operatorname{disc}(K)})$. Denote by s_L the number of ramified primes in $L/\mathbb{Q}$. If L is Pólya,

Maximum ramification in Pólya S_3-extensions of $\mathbb{Q}$

Theorem (-, A. Rajaei, Proc. Roy. Soc. Edinburgh Sect. A, 2019)

Let K be a non-Galois cubic field with Galois closure L and $E = \mathbb{Q}(\sqrt{\mathrm{disc}(K)})$. Denote by s_L the number of ramified primes in $L/\mathbb{Q}$. If L is Pólya,

1. for L real, $s_L \leq 4$ and this is sharp. Moreover, if $\varepsilon_E \in \mathrm{Norm}_{L/E}(U_L)$ where ε_E is the fundamental unit of E, then $s_L \leq 3$.

Maximum ramification in Pólya S_3-extensions of $\mathbb{Q}$

Theorem (-, A. Rajaei, Proc. Roy. Soc. Edinburgh Sect. A, 2019)

Let K be a non-Galois cubic field with Galois closure L and $E = \mathbb{Q}(\sqrt{\mathrm{disc}(K)})$. Denote by s_L the number of ramified primes in $L/\mathbb{Q}$. If L is Pólya,

1. for L real, $s_L \leq 4$ and this is sharp. Moreover, if $\varepsilon_E \in \mathrm{Norm}_{L/E}(U_L)$ where ε_E is the fundamental unit of E, then $s_L \leq 3$.
2. for L imaginary:

Maximum ramification in Pólya S_3-extensions of $\mathbb{Q}$

Theorem (-, A. Rajaei, Proc. Roy. Soc. Edinburgh Sect. A, 2019)

Let K be a non-Galois cubic field with Galois closure L and $E = \mathbb{Q}(\sqrt{\mathrm{disc}(K)})$. Denote by s_L the number of ramified primes in $L/\mathbb{Q}$. If L is Pólya,

1. for L real, $s_L \leq 4$ and this is sharp. Moreover, if $\varepsilon_E \in \mathrm{Norm}_{L/E}(U_L)$ where ε_E is the fundamental unit of E, then $s_L \leq 3$.
2. for L imaginary:
   1. for non-pure K, $s_L \leq 2$ and this is sharp;

Maximum ramification in Pólya S_3-extensions of $\mathbb{Q}$

Theorem (-, A. Rajaei, Proc. Roy. Soc. Edinburgh Sect. A, 2019)

Let K be a non-Galois cubic field with Galois closure L and $E = \mathbb{Q}(\sqrt{\mathrm{disc}(K)})$. Denote by s_L the number of ramified primes in $L/\mathbb{Q}$. If L is Pólya,

1. for L real, $s_L \leq 4$ and this is sharp. Moreover, if $\varepsilon_E \in \mathrm{Norm}_{L/E}(U_L)$ where ε_E is the fundamental unit of E, then $s_L \leq 3$.
2. for L imaginary:
    1. for non-pure K, $s_L \leq 2$ and this is sharp;
    2. for pure K, $s_L \leq 3$ and this is sharp. Moreover, if $\zeta_3 \in \mathrm{Norm}_{L/E}(U_L)$ where ζ_3 is a primitive third root of unity, then $s_L \leq 2$.

Proof.

Using ◂ Zantema's exact sequence we find

$$\#H^1(G, U_L) = \prod_{p \mid \mathrm{disc}(L)} e(p); \qquad G = \mathrm{Gal}(L/\mathbb{Q})$$

Proof.

Using ◂ Zantema's exact sequence we find

$$\#H^1(G, U_L) = \prod_{p \mid \mathrm{disc}(L)} e(p); \qquad G = \mathrm{Gal}(L/\mathbb{Q})$$

For $G_2 = \mathrm{Gal}(L/K)$ and $G_3 = \mathrm{Gal}(L/E)$

$$\mathrm{res} : H^1(G, U_L) \to H^1(G_2, U_L),$$

and

$$\mathrm{res} : H^1(G, U_L) \to H^1(G_3, U_L),$$

are injective on the 2-primary and 3-primary part of $H^1(G, U_L)$, respectively.

Proof.

Using ◂ Zantema's exact sequence we find

$$\#H^1(G, U_L) = \prod_{p|\mathrm{disc}(L)} e(p); \qquad G = \mathrm{Gal}(L/\mathbb{Q})$$

For $G_2 = \mathrm{Gal}(L/K)$ and $G_3 = \mathrm{Gal}(L/E)$

$$\mathrm{res} : H^1(G, U_L) \to H^1(G_2, U_L),$$

and

$$\mathrm{res} : H^1(G, U_L) \to H^1(G_3, U_L),$$

are injective on the 2-primary and 3-primary part of $H^1(G, U_L)$, respectively.

$$\Rightarrow \#H^1(G, U_L) \mid \#H^1(G_2, U_L).\#H^1(G_3, U_L).$$

Proof.

Using ◂ Zantema's exact sequence we find

$$\#H^1(G, U_L) = \prod_{p \mid disc(L)} e(p); \qquad G = Gal(L/\mathbb{Q})$$

For $G_2 = Gal(L/K)$ and $G_3 = Gal(L/E)$

$$res : H^1(G, U_L) \to H^1(G_2, U_L),$$

and

$$res : H^1(G, U_L) \to H^1(G_3, U_L),$$

are injective on the 2-primary and 3-primary part of $H^1(G, U_L)$, respectively.

$\Rightarrow \#H^1(G, U_L) \mid \#H^1(G_2, U_L).\#H^1(G_3, U_L).$

Proof.

Using Herbrand quotient for the cyclic extensions L/K and L/E, we have:

Proof.

Using Herbrand quotient for the cyclic extensions L/K and L/E, we have:

$$Q(G_2, U_L) = \frac{\#\hat{H}^0(G_2, U_L)}{\#H^1(G_2, U_L)} = \begin{cases} \frac{1}{2} & : \text{L is real}, \\ 1 & : \text{L is imaginary}, \end{cases}$$

$$Q(G_3, U_L) = \frac{\#\hat{H}^0(G_3, U_L)}{\#H^1(G_3, U_L)} = \frac{1}{3}$$

Proof.

Using Herbrand quotient for the cyclic extensions L/K and L/E, we have:

$$Q(G_2, U_L) = \frac{\#\hat{H}^0(G_2, U_L)}{\#H^1(G_2, U_L)} = \begin{cases} \frac{1}{2} & : L \text{ is real,} \\ 1 & : L \text{ is imaginary,} \end{cases}$$

$$Q(G_3, U_L) = \frac{\#\hat{H}^0(G_3, U_L)}{\#H^1(G_3, U_L)} = \frac{1}{3}$$

where

$$\hat{H}^0(G_2, U_L) = \frac{U_K}{\mathrm{Norm}_{L/K}(U_L)} \leq \frac{U_K}{U_K^2} \leq \begin{cases} \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} & : L \text{ is real} \\ \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} & : L \text{ is imaginary} \end{cases}$$

$$\hat{H}^0(G_3, U_L) = \frac{U_E}{\mathrm{Norm}_{L/E}(U_L)} \leq \frac{U_E}{U_E^3} \leq \frac{\mathbb{Z}}{3\mathbb{Z}}.$$

Proof.

$$\Rightarrow \prod_{p \mid disc(L)} e(p) = \#H^1(G, U_L) \mid \begin{cases} 2^4.3^2 & : L \text{ is real} \\ 2^2.3^2 & : L \text{ is imaginary} \end{cases}$$

Proof.

$$\Rightarrow \prod_{\mathrm{p}|\mathrm{disc}(\mathrm{L})} \mathrm{e(p)} = \#\mathrm{H}^1(\mathrm{G}, \mathrm{U_L}) \mid \begin{cases} 2^4.3^2 & : \mathrm{L \text{ is real}} \\ 2^2.3^2 & : \mathrm{L \text{ is imaginary}} \end{cases}$$

Since L is Pólya, by ◂ Theorem E is also Pólya.

Proof.

$$\Rightarrow \prod_{p|\mathrm{disc}(L)} e(p) = \#H^1(G, U_L) \mid \begin{cases} 2^4.3^2 & : L \text{ is real} \\ 2^2.3^2 & : L \text{ is imaginary} \end{cases}$$

Since L is Pólya, by ◂ Theorem E is also Pólya.

By ◂ Hilbert's result at most two primes ramify in $E/\mathbb{Q}$.

Proof.

$$\Rightarrow \prod_{p \mid \mathrm{disc}(L)} e(p) = \#H^1(G, U_L) \mid \begin{cases} 2^4.3^2 & : L \text{ is real} \\ 2^2.3^2 & : L \text{ is imaginary} \end{cases}$$

Since L is Pólya, by Theorem E is also Pólya.

By Hilbert's result at most two primes ramify in $E/\mathbb{Q}$.

For each ramified prime p in $E/\mathbb{Q}$, by Lemma $2 \mid e(p)$.

Proof.

$$\Rightarrow \prod_{p|\mathrm{disc}(L)} e(p) = \#H^1(G, U_L) \mid \begin{cases} 2^4.3^2 & : L \text{ is real} \\ 2^2.3^2 & : L \text{ is imaginary} \end{cases}$$

Since L is Pólya, by ◂ Theorem E is also Pólya.

By ◂ Hilbert's result at most two primes ramify in $E/\mathbb{Q}$.

For each ramified prime p in $E/\mathbb{Q}$, by ◂ Lemma $2 \mid e(p)$.

$$\Rightarrow \prod_{p|\mathrm{disc}(L)} e(p) = \#H^1(G, U_L) \mid \begin{cases} 2^2.3^2 & : L \text{ is real} \\ 2^1.3^2 & : L \text{ is imaginary} \end{cases}$$

Proof.

1. for L real and $\varepsilon_E \in \mathrm{Norm}_{L/E}(U_L)$,

$$\prod_{p \mid \mathrm{disc}(L)} e(p) = \#H^1(G, U_L) \mid 2^2.3^1;$$

2. for L real and $\varepsilon_E \notin \mathrm{Norm}_{L/E}(U_L)$,

$$\prod_{p \mid \mathrm{disc}(L)} e(p) = \#H^1(G, U_L) \mid 2^2.3^2.$$

Proof.

1. for L real and $\varepsilon_E \in \mathrm{Norm}_{L/E}(U_L)$,

$$\prod_{p|\mathrm{disc}(L)} e(p) = \#H^1(G, U_L) \mid 2^2.3^1;$$

2. for L real and $\varepsilon_E \notin \mathrm{Norm}_{L/E}(U_L)$,

$$\prod_{p|\mathrm{disc}(L)} e(p) = \#H^1(G, U_L) \mid 2^2.3^2.$$

Proof.

1. for L imaginary and K non-pure,

$$\prod_{p \mid \mathrm{disc}(L)} e(p) = \#H^1(G, U_L) \mid 2^1.3^1,$$

Proof.

1. for L imaginary and K non-pure,

$$\prod_{p|\mathrm{disc}(L)} e(p) = \#H^1(G, U_L) \mid 2^1.3^1,$$

2. for L imaginary and K pure,

Proof.

1. for L imaginary and K non-pure,

$$\prod_{p|\mathrm{disc}(L)} e(p) = \#H^1(G, U_L) \mid 2^1.3^1,$$

2. for L imaginary and K pure,
    1. if $\zeta_3 \in \mathrm{Norm}_{L/E}(U_L)$, then

$$\prod_{p|\mathrm{disc}(L)} e(p) = \#H^1(G, U_L) \mid 2^1.3^1;$$

Proof.

1. for L imaginary and K non-pure,

$$\prod_{p|\mathrm{disc}(L)} e(p) = \#H^1(G, U_L) \mid 2^1.3^1,$$

2. for L imaginary and K pure,
   1. if $\zeta_3 \in \mathrm{Norm}_{L/E}(U_L)$, then

$$\prod_{p|\mathrm{disc}(L)} e(p) = \#H^1(G, U_L) \mid 2^1.3^1;$$

   2. if $\zeta_3 \notin \mathrm{Norm}_{L/E}(U_L)$, then

$$\prod_{p|\mathrm{disc}(L)} e(p) = \#H^1(G, U_L) \mid 2^1.3^2.$$

L is real

Example

$K = \mathbb{Q}(\boldsymbol{\theta})$; $\boldsymbol{\theta}$ is a root of $f(X) = X^3 - 20X - 30$;

$\mathrm{disc}(K) = 2^2 \times 5^2 \times 7 \times 11$;

$L = K(\sqrt{77})$ and $E = \mathbb{Q}(\sqrt{77})$;

$h_K = 1$ and E is Pólya;

$\Rightarrow$ L is a real Pólya S_3-extension of $\mathbb{Q}$ with $s_L = 4$.

L is imaginary and K is pure

Example

$K = \mathbb{Q}(\sqrt[3]{10})$;

$\mathrm{disc}(K) = -3 \times 2^2 \times 5^2$;

$L = K(\sqrt{\zeta_3})$ and $E = \mathbb{Q}(\sqrt{\zeta_3})$;

$h_K = 1$ and E is Pólya;

$\Rightarrow$ L is an imaginary Pólya S_3-extension of $\mathbb{Q}$ with $s_L = 3$;

L is imaginary and K is not pure

Example

$K = \mathbb{Q}(\boldsymbol{\theta})$ where $\boldsymbol{\theta}$ is a root of $f(X) = X^3 + 5X + 5$;

$\mathrm{disc}(K) = -5^2 \times 47$;

$L = K(\sqrt{-47})$ and $E = \mathbb{Q}(\sqrt{-47})$; K is not pure;

$h_K = 1$ and E is Pólya;

$\Rightarrow$ L is an imaginary Pólya S_3-extension of $\mathbb{Q}$ with $s_L = 2$;

Maximum ramification in Pólya D_ℓ-extensions of $\mathbb{Q}$ for a prime $\ell > 3$

Theorem (-, A. Rajaei, J. Number Theory, 2020)

Let K be D_ℓ-field with Galois closure of L, for $\ell > 3$ an odd prime, and E be the unique quadratic subfield of L. Denote by s_L the number of ramified primes in $L/\mathbb{Q}$. If L is Pólya, then:

Maximum ramification in Pólya D_ℓ-extensions of $\mathbb{Q}$ for a prime $\ell > 3$

Theorem (-, A. Rajaei, J. Number Theory, 2020)

Let K be D_ℓ-field with Galois closure of L, for $\ell > 3$ an odd prime, and E be the unique quadratic subfield of L. Denote by s_L the number of ramified primes in $L/\mathbb{Q}$. If L is Pólya, then:

(i) For L real, if $\varepsilon_E \in \mathrm{Norm}_{L/E}(U_L)$ (resp. $\varepsilon_E \notin \mathrm{Norm}_{L/E}(U_L)$) then $s_L \leq 3$ (resp. $s_L \leq 4$), where ε_E is the fundamental unit of E.

Maximum ramification in Pólya D_ℓ-extensions of $\mathbb{Q}$ for a prime $\ell > 3$

Theorem (-, A. Rajaei, J. Number Theory, 2020)

Let K be D_ℓ-field with Galois closure of L, for $\ell > 3$ an odd prime, and E be the unique quadratic subfield of L. Denote by s_L the number of ramified primes in $L/\mathbb{Q}$. If L is Pólya, then:

(i) For L real, if $\varepsilon_E \in \mathrm{Norm}_{L/E}(U_L)$ (resp. $\varepsilon_E \notin \mathrm{Norm}_{L/E}(U_L)$) then $s_L \leq 3$ (resp. $s_L \leq 4$), where ε_E is the fundamental unit of E.

(ii) For L imaginary, $s_L \leq 2$.

Leriche's upper bound

Maximum ramification in Pólya D_ℓ-extensions of $\mathbb{Q}$ for a prime $\ell > 3$

Theorem (-, A. Rajaei, J. Number Theory, 2020)

Let K be D_ℓ-field with Galois closure of L, for $\ell > 3$ an odd prime, and E be the unique quadratic subfield of L. Denote by s_{L} the number of ramified primes in $\mathrm{L}/\mathbb{Q}$. If L is Pólya, then:

(i) For L real, if $\boldsymbol{\varepsilon}_{\mathrm{E}} \in \mathrm{Norm}_{\mathrm{L}/\mathrm{E}}(\mathrm{U}_{\mathrm{L}})$ (resp. $\boldsymbol{\varepsilon}_{\mathrm{E}} \notin \mathrm{Norm}_{\mathrm{L}/\mathrm{E}}(\mathrm{U}_{\mathrm{L}})$) then $s_{\mathrm{L}} \leq 3$ (resp. $s_{\mathrm{L}} \leq 4$), where $\boldsymbol{\varepsilon}_{\mathrm{E}}$ is the fundamental unit of E.

(ii) For L imaginary, $s_{\mathrm{L}} \leq 2$.

◂ Leriche's upper bound

Remark

For $\ell > 3$ and E imaginary, $\gcd(\#\mathrm{U}_{\mathrm{E}}, \#\frac{\mathrm{U}_{\mathrm{E}}}{\mathrm{U}_{\mathrm{E}}^{\ell}}) = 1 \Rightarrow \mathrm{U}_{\mathrm{E}} = \mathrm{Norm}_{\mathrm{L}/\mathrm{K}}(\mathrm{U}_{\mathrm{L}})$.

Theorem(Ishida, J. Number Theory, 1969)

For $K/\mathbb{Q}$ a non-pure extension of degree n, if

$$\#\{\text{primes ramify totally in } K\} > \text{rank}_{\mathbb{Z}}(\mathscr{O}_K^{\times}),$$

then $n \mid h_K$.

Theorem(Ishida, J. Number Theory, 1969)

For $K/\mathbb{Q}$ a non-pure extension of degree n, if

$$\#\{\text{primes ramify totally in K}\} > \operatorname{rank}_{\mathbb{Z}}(\mathscr{O}_K^{\times}),$$

then $n \mid h_K$.

Example

For a D_ℓ-field K (ℓ an odd prime), we have

$$\text{Signature of K} = \begin{cases} (\ell, 0): & \operatorname{disc}(K) > 0 \\ (1, \frac{\ell-1}{2}): & \operatorname{disc}(K) < 0 \end{cases}$$

$\Rightarrow$ for $\operatorname{disc}(K) > 0$ (resp. $\operatorname{disc}(K) < 0$) if at least ℓ (resp. $\frac{\ell+1}{2}$) primes ramify totally in K, then $\ell | h_K$.

Corollary (-, A. Rajaei, J. Number Theory, 2020)

Let K be a D_ℓ-field, where ℓ is an odd prime. Denote the number of totally ramified primes in K by t_K.

(i) If $\ell = 3$:

(i−1) for $\mathrm{disc}(K) > 0$ or K pure, if $t_K \geq 3$ then $3 \mid h_K$;

(i−2) for $\mathrm{disc}(K) < 0$ and K non-pure, if $t_K \geq 2$ then $3 \mid h_K$.

(ii) If $\ell > 3$:

(ii−1) for $\mathrm{disc}(K) > 0$, if $t_K \geq 3$ then $\ell \mid h_K$.

(ii−2) for $\mathrm{disc}(K) < 0$, if $t_K \geq 2$ then $\ell \mid h_K$.

Proof.

For instance, assume that K is a D_ℓ-field ($\ell > 3$ prime) with $\mathrm{disc}(K) > 0$ and denote its Galois closure by L.

If at least three distinct primes ramify totally in $K/\mathbb{Q}$, then

$$\ell^3 \mid \prod_{p \mid \mathrm{disc}(L)} e(p) \overset{\text{Zantema's exact sequence}}{=} \#H^1(\mathrm{Gal}(L/\mathbb{Q}), U_L).\#\mathscr{P}o(L).$$

$$\#H^1(\mathrm{Gal}(L/\mathbb{Q}), U_L) \mid 2^{\omega}.\ell^2 \ (\omega \in \mathbb{N}) \Rightarrow \ell \mid \#\mathscr{P}o(L).$$

$$\frac{\mathbb{Z}}{\ell\mathbb{Z}} \leq (\mathscr{P}o(L))_\ell \overset{\text{Theorem}}{\hookrightarrow} \mathscr{P}o(K) \overset{\text{Chabert-Halberstadt}}{=} Cl(K).$$

Proof.

For instance, assume that K is a D_ℓ-field ($\ell > 3$ prime) with $\mathrm{disc}(K) > 0$ and denote its Galois closure by L.

If at least three distinct primes ramify totally in $K/\mathbb{Q}$, then

$$\ell^3 \mid \prod_{p \mid \mathrm{disc}(L)} e(p) \overset{\text{Zantema's exact sequence}}{=} \#H^1(\mathrm{Gal}(L/\mathbb{Q}), U_L).\#\mathscr{P}o(L).$$

$$\#H^1(\mathrm{Gal}(L/\mathbb{Q}), U_L) \mid 2^\omega.\ell^2 \ (\omega \in \mathbb{N}) \Rightarrow \ell \mid \#\mathscr{P}o(L).$$

$$\frac{\mathbb{Z}}{\ell\mathbb{Z}} \leq (\mathscr{P}o(L))_\ell \overset{\text{Theorem}}{\hookrightarrow} \mathscr{P}o(K) \overset{\text{Chabert-Halberstadt}}{=} Cl(K).$$

Proof.

For instance, assume that K is a D_ℓ-field ($\ell > 3$ prime) with disc(K) > 0 and denote its Galois closure by L.

If at least three distinct primes ramify totally in $K/\mathbb{Q}$, then

$$\ell^3 \mid \prod_{p \mid \mathrm{disc}(L)} e(p) \overset{\text{Zantema's exact sequence}}{=} \#H^1(\mathrm{Gal}(L/\mathbb{Q}), U_L).\#\mathscr{P}o(L).$$

$$\#H^1(\mathrm{Gal}(L/\mathbb{Q}), U_L) \mid 2^{\omega}.\ell^2 \ (\omega \in \mathbb{N}) \Rightarrow \ell \mid \#\mathscr{P}o(L).$$

$$\frac{\mathbb{Z}}{\ell\mathbb{Z}} \leq (\mathscr{P}o(L))_\ell \overset{\text{Theorem}}{\hookrightarrow} \mathscr{P}o(K) \overset{\text{Chabert-Halberstadt}}{=} Cl(K).$$

Proof.

For instance, assume that K is a D_ℓ-field ($\ell > 3$ prime) with $\mathrm{disc}(K) > 0$ and denote its Galois closure by L.

If at least three distinct primes ramify totally in $K/\mathbb{Q}$, then

$$\ell^3 \mid \prod_{p \mid \mathrm{disc}(L)} e(p) \overset{\text{Zantema's exact sequence}}{=} \#H^1(\mathrm{Gal}(L/\mathbb{Q}), U_L).\#\mathscr{P}o(L).$$

$$\#H^1(\mathrm{Gal}(L/\mathbb{Q}), U_L) \mid 2^{\omega}.\ell^2 \ (\omega \in \mathbb{N}) \Rightarrow \ell \mid \#\mathscr{P}o(L).$$

$$\frac{\mathbb{Z}}{\ell\mathbb{Z}} \leq (\mathscr{P}o(L))_\ell \overset{\text{Theorem}}{\hookrightarrow} \mathscr{P}o(K) \overset{\text{Chabert-Halberstadt}}{=} Cl(K).$$

non-Galois extensions of $\mathbb{Q}$

Definition (Chabert-Halberstadt, J. Number Theory, 2020)

For a number field K, the subgroups $\mathbf{Po}(K)_{nr}$ (pre-Pólya group) and $\mathbf{Po}(K)_{nr1}$ of $\mathbf{Po}(K)$ are defined as follows:

$$\mathbf{Po}(K)_{nr} =< \left[\Pi_{p^f}(K)\right] : f \in \mathbb{N}, \text{p is a non-ramified prime in } K/\mathbb{Q} >,$$

$$\mathbf{Po}(K)_{nr1} =< \left[\Pi_{p^1}(K)\right] : \text{p is a non-ramified prime in } K/\mathbb{Q} > .$$

Polya group

Definition (Chabert-Halberstadt, J. Number Theory, 2020)

For a number field K, the subgroups $\mathrm{Po}(K)_{nr}$ (pre-Pólya group) and $\mathrm{Po}(K)_{nr1}$ of $\mathrm{Po}(K)$ are defined as follows:

$$\mathrm{Po}(K)_{nr} =< \left[\Pi_{p^f}(K)\right] : f \in \mathbb{N}, p \text{ is a non-ramified prime in } K/\mathbb{Q} >,$$

$$\mathrm{Po}(K)_{nr1} =< \left[\Pi_{p^1}(K)\right] : p \text{ is a non-ramified prime in } K/\mathbb{Q} > .$$

Polya group

Theorem (Chabert-Halberstadt, J. Number Theory, 2020)

For a D_n-field K with n an odd integer, we have:

$$\mathrm{Po}(K)_{nr1} = \mathrm{Po}(K)_{nr} = \mathrm{Po}(K) = \mathrm{Cl}(K).$$

Definition (Chabert-Halberstadt, J. Number Theory, 2020)

For a number field K, the subgroups $\mathbf{Po}(K)_{nr}$ (pre-Pólya group) and $\mathbf{Po}(K)_{nr1}$ of $\mathbf{Po}(K)$ are defined as follows:

$$\mathbf{Po}(K)_{nr} = < \left[\Pi_{p^f}(K)\right] : f \in \mathbb{N}, p \text{ is a non-ramified prime in } K/\mathbb{Q} >,$$

$$\mathbf{Po}(K)_{nr1} = < \left[\Pi_{p^1}(K)\right] : p \text{ is a non-ramified prime in } K/\mathbb{Q} > .$$

◂ Polya group

Theorem (Chabert-Halberstadt, J. Number Theory, 2020)

For a D_n-field K with n an odd integer, we have:

$$\mathbf{Po}(K)_{nr1} = \mathbf{Po}(K)_{nr} = \mathbf{Po}(K) = \mathbf{Cl}(K).$$

Motivation

We take K to be a D_n-field with $n \geq 4$ an even integer.

Lemma (–, Int. J. Math, 2021)

Assume that $n \geq 4$ is an even integer, K is a D_n-field with the unique subfield F of degree $\frac{n}{2}$ over $\mathbb{Q}$. Then the norm map $\mathscr{N}_{K/F} : \mathbf{Cl}(K) \to \mathbf{Cl}(F)$ is surjective. In particular, $h_F | h_K$.

Proof.

Zantema proved K/F is not unramified. Hence $K \cap H(F) = F$. Surjectiveness of the norm map $\mathscr{N}_{K/F} : \mathbf{Cl}(K) \to \mathbf{Cl}(F)$ is a well known result in Class Field Theory. □

▸ proof of main theorem ▸ Corollary

Theorem (–, Int. J. Math, 2021)

Let K be a D_n-field, for $n \geq 4$ an even integer, and denote the unique subfield of K of degree $\frac{n}{2}$ (over $\mathbb{Q}$) by F. Then $Po(K)_{nr1} = Po(K)_{nr} = \varepsilon_{K/F}(Cl(F))$. ▸ Corollary ▸ Max ramification

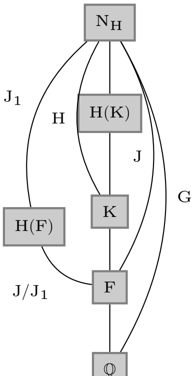
Theorem (–, Int. J. Math, 2021)

Let K be a D_n-field, for $n \geq 4$ an even integer, and denote the unique subfield of K of degree $\frac{n}{2}$ (over $\mathbb{Q}$) by F. Then $\mathrm{Po}(K)_{nr1} = \mathrm{Po}(K)_{nr} = \varepsilon_{K/F}(\mathrm{Cl}(F))$. Corollary Max ramification

Proof. Let N_H be the Galois closure of H(K) (over $\mathbb{Q}$) and:

- $G = \mathrm{Gal}(N_H/\mathbb{Q})$;
- $H = \mathrm{Gal}(N_H/K)$;
- $H_1 = \mathrm{Gal}(N_H/H(K))$;
- $J = \mathrm{Gal}(N_H/F)$;
- $J_1 = \mathrm{Gal}(N_H/H(F))$.

$$\Rightarrow H/H_1 \simeq \mathrm{Cl}(K),$$
$$J/J_1 \simeq \mathrm{Cl}(F).$$



$G = Gal(N_H/\mathbb{Q}),\ H = Gal(N_H/K),\ H_1 = Gal(N_H/H(K)),\ J = Gal(N_H/F),\ J_1 = Gal(N_H/H(F))$

Let $\Omega = \{Hs : s \in G\}$; $\Rightarrow \#\Omega = [K : \mathbb{Q}] = n$.

G acts transitively on Ω, as $(Hs)^g \mapsto Hsg^{-1}$, $\forall g, s \in G$.

By $S_\Omega \simeq S_n$, $g \longleftrightarrow \pi_1 \dots \pi_t$, where π_i's are disjoint cycles of orders f_i, and $f_i = 1$ for fixed points.

Let $Hs_i \in \Omega$ belongs to the orbit of π_i, i.e. Hs_i is permuted by π_i.

$G = \mathrm{Gal}(N_H/\mathbb{Q})$, $H = \mathrm{Gal}(N_H/K)$, $H_1 = \mathrm{Gal}(N_H/H(K))$, $J = \mathrm{Gal}(N_H/F)$, $J_1 = \mathrm{Gal}(N_H/H(F))$

Let $\Omega = \{Hs : s \in G\}$; $\Rightarrow \#\Omega = [K : \mathbb{Q}] = n$.

G acts transitively on Ω, as $(Hs)^g \mapsto Hsg^{-1}$, $\forall g, s \in G$.

By $S_\Omega \simeq S_n$, $g \longleftrightarrow \pi_1 \ldots \pi_t$, where π_i's are disjoint cycles of orders f_i, and $f_i = 1$ for fixed points.

Let $Hs_i \in \Omega$ belongs to the orbit of π_i, i.e. Hs_i is permuted by π_i.

$G = \mathrm{Gal}(N_H/\mathbb{Q})$, $H = \mathrm{Gal}(N_H/K)$, $H_1 = \mathrm{Gal}(N_H/H(K))$, $J = \mathrm{Gal}(N_H/F)$, $J_1 = \mathrm{Gal}(N_H/H(F))$

Let $\boldsymbol{\Omega} = \{Hs : s \in G\}$; $\Rightarrow \#\boldsymbol{\Omega} = [K:\mathbb{Q}] = n$.

G acts transitively on $\boldsymbol{\Omega}$, as $(Hs)^g \mapsto Hsg^{-1}$, $\forall g, s \in G$.

By $S_{\boldsymbol{\Omega}} \simeq S_n$, $g \longleftrightarrow \boldsymbol{\pi}_1 \ldots \boldsymbol{\pi}_t$, where $\boldsymbol{\pi}_i$'s are disjoint cycles of orders f_i, and $f_i = 1$ for fixed points.

Let $Hs_i \in \Omega$ belongs to the orbit of π_i, i.e. Hs_i is permuted by π_i.

$G = \mathrm{Gal}(N_H/\mathbb{Q})$, $H = \mathrm{Gal}(N_H/K)$, $H_1 = \mathrm{Gal}(N_H/H(K))$, $J = \mathrm{Gal}(N_H/F)$, $J_1 = \mathrm{Gal}(N_H/H(F))$

Let $\Omega = \{Hs : s \in G\}$; $\Rightarrow \#\Omega = [K : \mathbb{Q}] = n$.

G acts transitively on Ω, as $(Hs)^g \mapsto Hsg^{-1}$, $\forall g, s \in G$.

By $S_\Omega \simeq S_n$, $g \longleftrightarrow \pi_1 \ldots \pi_t$, where π_i's are disjoint cycles of orders f_i, and $f_i = 1$ for fixed points.

Let $Hs_i \in \Omega$ belongs to the orbit of π_i, i.e. Hs_i is permuted by π_i.

$G = \mathrm{Gal}(N_H/\mathbb{Q})$, $H = \mathrm{Gal}(N_H/K)$, $H_1 = \mathrm{Gal}(N_H/H(K))$, $J = \mathrm{Gal}(N_H/F)$, $J_1 = \mathrm{Gal}(N_H/H(F))$

Let $\Omega = \{Hs : s \in G\}$; $\Rightarrow \#\Omega = [K : \mathbb{Q}] = n$.

G acts transitively on Ω, as $(Hs)^g \mapsto Hsg^{-1}$, $\forall g, s \in G$.

By $S_\Omega \simeq S_n$, $g \longleftrightarrow \pi_1 \dots \pi_t$, where π_i's are disjoint cycles of orders f_i, and $f_i = 1$ for fixed points.

Let $Hs_i \in \Omega$ belongs to the orbit of π_i, i.e. Hs_i is permuted by π_i.

For a non-ramified prime p in $K/\mathbb{Q}$, a prime $\mathfrak{P}$ of N_H above p and $g = (\mathfrak{P}, N_H/\mathbb{Q})$, the Frobenius element of $\mathfrak{P}$ in $N_H/\mathbb{Q}$, we have

$$\left(\frac{\Pi_{p^f}(K)}{H(K)/K}\right) = \prod_{\{i | f_i = f\}} s_i g^{f_i} s_i^{-1} \bmod H_1,$$

where $\left(\frac{\Pi_{p^f}(K)}{H(K)/K}\right)$ is the Artin symbol of $\Pi_{p^f}(K)$.

$G = Gal(N_H/\mathbb{Q})$, $H = Gal(N_H/K)$, $H_1 = Gal(N_H/H(K))$, $J = Gal(N_H/F)$, $J_1 = Gal(N_H/H(F))$

Let $\Omega = \{Hs : s \in G\}$; $\Rightarrow \#\Omega = [K : \mathbb{Q}] = n$.

G acts transitively on Ω, as $(Hs)^g \mapsto Hsg^{-1}$, $\forall g, s \in G$.

By $S_\Omega \simeq S_n$, $g \longleftrightarrow \pi_1 \dots \pi_t$, where π_i's are disjoint cycles of orders f_i, and $f_i = 1$ for fixed points.

Let $Hs_i \in \Omega$ belongs to the orbit of π_i, i.e. Hs_i is permuted by π_i.

$$Cl(K) \simeq Gal(H(K)/K) \simeq H/H_1$$

$$Po(K)_{nr} = \left\langle \left[\Pi_{p^f}(K)\right] \right\rangle \overset{\simeq}{\longleftrightarrow} \left\langle \left(\frac{\Pi_{p^f}(K)}{H(K)/K} \right) \right\rangle \overset{\simeq}{\longleftrightarrow} \mathscr{A} = \left\langle \prod_{\{i|f_i=f\}} s_i g^{f_i} s_i^{-1} \bmod H_1 \right\rangle.$$

$G = \mathrm{Gal}(N_H/\mathbb{Q})$, $H = \mathrm{Gal}(N_H/K)$, $H_1 = \mathrm{Gal}(N_H/H(K))$, $J = \mathrm{Gal}(N_H/F)$, $J_1 = \mathrm{Gal}(N_H/H(F))$

Let $\Omega = \{Hs : s \in G\}$; $\Rightarrow \#\Omega = [K : \mathbb{Q}] = n$.

G acts transitively on Ω, as $(Hs)^g \mapsto Hsg^{-1}$, $\forall g, s \in G$.

By $S_\Omega \simeq S_n$, $g \longleftrightarrow \pi_1 \ldots \pi_t$, where π_i's are disjoint cycles of orders f_i, and $f_i = 1$ for fixed points.

Let $Hs_i \in \Omega$ belongs to the orbit of π_i, i.e. Hs_i is permuted by π_i.

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

$$\mathrm{Po}(K)_{nr} \overset{\simeq}{\longleftrightarrow} \mathscr{A} = \left\langle \prod_{\{i|f_i=f\}} s_i g^{f_i} s_i^{-1} \bmod H_1 \ : g \text{ has the orbit structure } 1,1,2,\ldots,2 \right\rangle$$

$G = \mathrm{Gal}(N_H/\mathbb{Q})$, $H = \mathrm{Gal}(N_H/K)$, $H_1 = \mathrm{Gal}(N_H/H(K))$, $J = \mathrm{Gal}(N_H/F)$, $J_1 = \mathrm{Gal}(N_H/H(F))$

g has the orbit structure $1, 1, 2, \ldots, 2 \iff p\mathscr{O}_K = \underbrace{(\beta_1.\beta_2)}_{\Pi_{p1}(K)}\underbrace{(\beta_3 \ldots \beta_t)}_{\Pi_{p2}(K)}$.

$G = \mathrm{Gal}(N_H/\mathbb{Q})$, $H = \mathrm{Gal}(N_H/K)$, $H_1 = \mathrm{Gal}(N_H/H(K))$, $J = \mathrm{Gal}(N_H/F)$, $J_1 = \mathrm{Gal}(N_H/H(F))$

$$g \text{ has the orbit structure } 1,1,2,\ldots,2 \Longleftrightarrow p\mathscr{O}_K = \underbrace{(\beta_1.\beta_2)}_{\Pi_{p1}(K)}\underbrace{(\beta_3\ldots\beta_t)}_{\Pi_{p2}(K)}.$$

$\mathrm{Po}(K)_{nr} \overset{\simeq}{\longleftrightarrow} \mathscr{A} = \langle s_1 g s_1^{-1} s_2 g s_2^{-1} \bmod H_1 \,:\, g \in H \text{ has the orbit structure } 1,1,2,\ldots,2\rangle$;
$\Longrightarrow \mathrm{Po}(K)_{nr} = \mathrm{Po}(K)_{nr1}$.

$G = \mathrm{Gal}(N_H/\mathbb{Q})$, $H = \mathrm{Gal}(N_H/K)$, $H_1 = \mathrm{Gal}(N_H/H(K))$, $J = \mathrm{Gal}(N_H/F)$, $J_1 = \mathrm{Gal}(N_H/H(F))$

$$g \text{ has the orbit structure } 1,1,2,\ldots,2 \iff p\mathscr{O}_K = \underbrace{(\beta_1.\beta_2)}_{\Pi_{p1}(K)}\underbrace{(\beta_3\ldots\beta_t)}_{\Pi_{p2}(K)}.$$

$$Po(K)_{nr} \overset{\simeq}{\longleftrightarrow} \mathscr{A} = \langle s_1 g s_1^{-1} s_2 g s_2^{-1} \bmod H_1 \;:\; g \in H \text{ has the orbit structure } 1,1,2,\ldots,2\rangle;$$

$$\Longrightarrow Po(K)_{nr} = Po(K)_{nr1}.$$

$$\overset{(J:H)=2}{\Rightarrow} J = \{s \in G \,|\, sgs^{-1} \in H, \text{ for all } g \in H \text{ with the orbit structure } 1,1,2,\ldots,2\},$$

$G=Gal(N_H/\mathbb{Q}),\ H=Gal(N_H/K),\ H_1=Gal(N_H/H(K)),\ J=Gal(N_H/F),\ J_1=Gal(N_H/H(F))$

$$g \text{ has the orbit structure } 1,1,2,\ldots,2 \Longleftrightarrow p\mathscr{O}_K=\underbrace{(\beta_1.\beta_2)}_{\Pi_{p1}(K)}\underbrace{(\beta_3\ldots\beta_t)}_{\Pi_{p2}(K)}.$$

$$Po(K)_{nr}\overset{\simeq}{\longleftrightarrow}\mathscr{A}=\langle s_1gs_1^{-1}s_2gs_2^{-1} \bmod H_1 : g\in H \text{ has the orbit structure } 1,1,2,\ldots,2\rangle;$$
$$\Longrightarrow Po(K)_{nr}=Po(K)_{nr1}.$$

$$\overset{(J:H)=2}{\Rightarrow} J=\{s\in G\,|sgs^{-1}\in H, \text{ for all } g\in H \text{ with the orbit structure } 1,1,2,\ldots,2\},$$

$$\overset{s_1=1,s_2\in J\backslash H}{\Rightarrow}$$
$$Po(K)_{nr}\overset{\simeq}{\longleftrightarrow}\mathscr{A}=\langle gsgs^{-1} \bmod H_1 : g\in H \text{ has the orbit structure } 1,1,2,\ldots,2 \text{ and } s\in J\backslash H\rangle.$$

$G = \mathrm{Gal}(N_H/\mathbb{Q})$, $H = \mathrm{Gal}(N_H/K)$, $H_1 = \mathrm{Gal}(N_H/H(K))$, $J = \mathrm{Gal}(N_H/F)$, $J_1 = \mathrm{Gal}(N_H/H(F))$

$$\Rightarrow \mathrm{Po}(K)_{nr} \simeq \mathrm{Ver}\,(i(H/H_1))\,,$$

where $i : H/H_1 \to J/J_1$ induced by the inclusion map is surjective by ◂ Lemma,
and $\mathrm{Ver} : J/J_1 \to H/H_1$ is the transfer map.

$G = \mathrm{Gal}(N_H/\mathbb{Q})$, $H = \mathrm{Gal}(N_H/K)$, $H_1 = \mathrm{Gal}(N_H/H(K))$, $J = \mathrm{Gal}(N_H/F)$, $J_1 = \mathrm{Gal}(N_H/H(F))$

$$\Rightarrow \mathrm{Po}(K)_{nr} \simeq \mathrm{Ver}\left(i(H/H_1)\right),$$

where $i : H/H_1 \to J/J_1$ induced by the inclusion map is surjective by Lemma,
and $\mathrm{Ver} : J/J_1 \to H/H_1$ is the transfer map.

Using the following commutative diagram

$$\begin{array}{ccc} \mathrm{Cl}(F) & \xrightarrow{\varepsilon_{K/F}} & \mathrm{Cl}(K) \\ \downarrow & & \downarrow \\ J/J_1 & \xrightarrow{\mathrm{Ver}} & H/H_1 \end{array}$$

we have $\mathrm{Po}(K)_{nr} \simeq \mathrm{Ver}(J/J_1) \simeq \varepsilon_{K/F}(\mathrm{Cl}(F))$, where the vertical arrows are isomorphisms induced by the Artin map.

Corollary (–, Int. J. Math, 2021)

Let K be a D_n-field, for $n \geq 4$ an even integer, and denote the unique subfield of K of degree $\frac{n}{2}$ (over $\mathbb{Q}$) by F. If h_K is odd, then

$$\mathrm{Po}(K)_{nr1} = \mathrm{Po}(K)_{nr} = \mathrm{Po}(K) = \mathrm{Po}(K/F) \simeq \mathrm{Cl}(F).$$

Proof.

$$\varepsilon_{K/F}(\mathrm{Cl}(F)) \overset{\text{Theorem}}{=} \mathrm{Po}(K)_{nr} \subseteq \mathrm{Po}(K) \overset{\text{Lemma}}{\subseteq} \mathrm{Po}(K/F) \overset{\text{Corollary}}{=} \varepsilon_{K/F}(\mathrm{Cl}(F)).$$

by Lemma [Lemma] h(F) is odd. Hence $\mathcal{N}_{K/F} \circ \varepsilon_{K/F} : \bar{\mathfrak{a}} \in \mathrm{Cl}(F) \mapsto \bar{\mathfrak{a}}^2 \in \mathrm{Cl}(F)$ is injective, and so is $\varepsilon_{K/F}$. □

Example

Proposition (C. J. Parry, 1975)

For a prime $p \equiv 3 \pmod 8$, the pure quartic fields $\mathbb{Q}(\sqrt[4]{2p})$ and $\mathbb{Q}(\sqrt[4]{2p^2})$ have odd class numbers.

$\Rightarrow$ for $p \equiv 3 \pmod 8$ prime:

$$\mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p}))_{nr1} = \mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p}))_{nr} = \mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p})) = \mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p})/\mathbb{Q}(\sqrt{2p})) \simeq \mathrm{Cl}(\mathbb{Q}(\sqrt{2p}));$$

$$\mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p^2}))_{nr1} = \mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p^2}))_{nr} = \mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p^2})) = \mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p^2})/\mathbb{Q}(\sqrt{2})) \simeq \mathrm{Cl}(\mathbb{Q}(\sqrt{2})) = \{1\}.$$

For instance $\mathbb{Q}(\sqrt[4]{2.(59)^2})$ is a Pólya field with class number five.

Example

Proposition (C. J. Parry, 1975)

For a prime $p \equiv 3 \pmod 8$, the pure quartic fields $\mathbb{Q}(\sqrt[4]{2p})$ and $\mathbb{Q}(\sqrt[4]{2p^2})$ have odd class numbers.

$\Rightarrow$ for $p \equiv 3 \pmod 8$ prime:

$$Po(\mathbb{Q}(\sqrt[4]{2p}))_{nr1} = Po(\mathbb{Q}(\sqrt[4]{2p}))_{nr} = Po(\mathbb{Q}(\sqrt[4]{2p})) = Po(\mathbb{Q}(\sqrt[4]{2p})/\mathbb{Q}(\sqrt{2p})) \simeq Cl(\mathbb{Q}(\sqrt{2p}));$$

$$Po(\mathbb{Q}(\sqrt[4]{2p^2}))_{nr1} = Po(\mathbb{Q}(\sqrt[4]{2p^2}))_{nr} = Po(\mathbb{Q}(\sqrt[4]{2p^2})) = Po(\mathbb{Q}(\sqrt[4]{2p^2})/\mathbb{Q}(\sqrt{2})) \simeq Cl(\mathbb{Q}(\sqrt{2})) = \{1\}.$$

For instance $\mathbb{Q}(\sqrt[4]{2.(59)^2})$ is a Pólya field with class number five.

Example

Proposition (C. J. Parry, 1975)

For a prime $p \equiv 3 \pmod 8$, the pure quartic fields $\mathbb{Q}(\sqrt[4]{2p})$ and $\mathbb{Q}(\sqrt[4]{2p^2})$ have odd class numbers.

$\Rightarrow$ for $p \equiv 3 \pmod 8$ prime:

$$\mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p}))_{nr1} = \mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p}))_{nr} = \mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p})) = \mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p})/\mathbb{Q}(\sqrt{2p})) \simeq \mathrm{Cl}(\mathbb{Q}(\sqrt{2p}));$$
$$\mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p^2}))_{nr1} = \mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p^2}))_{nr} = \mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p^2})) = \mathrm{Po}(\mathbb{Q}(\sqrt[4]{2p^2})/\mathbb{Q}(\sqrt{2})) \simeq \mathrm{Cl}(\mathbb{Q}(\sqrt{2})) = \{1\}.$$

For instance $\mathbb{Q}(\sqrt[4]{2.(59)^2})$ is a Pólya field with class number five.

Maximum ramification in Pólya D_4-fields

Proposition (Zantema, 1982)

Let K be a Pólya D_4-field. Then at most five primes are ramified in $K/\mathbb{Q}$.

Maximum ramification in Pólya D_4-fields

Proposition (Zantema, 1982)

Let K be a Pólya D_4-field. Then at most five primes are ramified in $K/\mathbb{Q}$.

Example (Chabert-Halberstadt, 2020)

Let $K = \mathbb{Q}(\alpha)$, where α is a root of

$$f(X) = X^4 - 17X^2 + 31.$$

We have $\mathrm{disc}(K) = 2^4.3^2.5^2.11^2.31$, $h_K = 2$ and K is a Pólya D_4-field.

Lemma (–, Int. J. Math, 2021)

Let K be a Pólya D_4-field with the unique quadratic subfield F. Then

$$\mathrm{Po}(K/F) = \langle [\gamma] \in \mathbf{Cl}(K) : (\gamma \cap \mathbb{Z})\,\mathscr{O}_F = \beta_1\beta_2, \text{ and } \beta_i\text{'s ramify in } K \rangle.$$

▸ Maximum ramification

Lemma (–, Int. J. Math, 2021)

Let K be a Pólya D_4-field with the unique quadratic subfield F. Then

$$\mathrm{Po}(K/F) = \langle [\gamma] \in \mathbf{Cl}(K) : (\gamma \cap \mathbb{Z})\,\mathscr{O}_F = \beta_1\beta_2, \text{ and } \beta_i\text{'s ramify in } K\rangle\,.$$

▸ Maximum ramification

Proof.

By ◂ Theorem, $\mathrm{Po}(K)_{nr} = \varepsilon_{K/F}(\mathbf{Cl}(F))$ is trivial. Since K is Pólya, $\Pi_{\mathfrak{p}^f}(K/F)$ might not be principal only in the case that $(\mathfrak{p} \cap \mathbb{Z})\,\mathscr{O}_F = \beta_1\beta_2$, and β_i's ramify in K. □

Notation

For M/N a finite extension of number fields, we denote the number of ramified and totally ramified primes of N in M by $r_{M/N}$, $t_{M/N}$, respectively.

Lemma (–, Int. J. Math, 2021)

Let K be a Pólya D_4-field with the unique quadratic subfield F. Then

$$r_{K/\mathbb{Q}} = r_{K/F} + r_{F/\mathbb{Q}} - \left(t_{K/\mathbb{Q}} + u\right),$$

where $u = \#\{p \in \mathbb{Z} \text{ prime} : p\mathscr{O}_F = \beta_1\beta_2, \beta_i' \text{s ramify in } K\}$. ▸ Max ramification

Notation

For M/N a finite extension of number fields, we denote the number of ramified and totally ramified primes of N in M by $r_{M/N}$, $t_{M/N}$, respectively.

Lemma (–, Int. J. Math, 2021)

Let K be a Pólya D_4-field with the unique quadratic subfield F. Then

$$r_{K/\mathbb{Q}} = r_{K/F} + r_{F/\mathbb{Q}} - \left(t_{K/\mathbb{Q}} + u\right),$$

where $u = \#\{p \in \mathbb{Z} \text{ prime} : p\mathscr{O}_F = \beta_1\beta_2, \beta_i'\text{s ramify in } K\}$. ▸ Max ramification

Proof.

There exist $r_{K/F} - u$ primes of $\mathbb{Q}$ which are ramified in K/F (note that here we count the number of totally ramified primes in $K/\mathbb{Q}$). On the other hand, for a totally ramified prime p in $K/\mathbb{Q}p$ also ramifies in $F/\mathbb{Q}$. □

Theorem (–, Int. J. Math, 2021)

Let K be a Pólya D_4-field with the unique quadratic subfield F. Denote by $t_{K/\mathbb{Q}}$ and $p_{K/\mathbb{Q}}$ the number of totally and partially ramified primes in $K/\mathbb{Q}$.

(i) For F imaginary:

$$2t_{K/\mathbb{Q}} + p_{K/\mathbb{Q}} \leq \begin{cases} 2: & F \neq \mathbb{Q}(\sqrt{-1}) \text{ and } -1 \in N_{K/F}(U_K) \\ 3: & F \neq \mathbb{Q}(\sqrt{-1}) \text{ and } -1 \notin N_{K/F}(U_K) \\ 2: & F = \mathbb{Q}(\sqrt{-1}) \text{ and } \sqrt{-1} \in N_{K/F}(U_K) \\ 3: & F = \mathbb{Q}(\sqrt{-1}) \text{ and } \sqrt{-1} \notin N_{K/F}(U_K) \end{cases}$$

(ii) For F real, denote the fundamental unit of F by ε, and denote the number of infinite places of F ramified in K by s. Then:

$$2t_{K/\mathbb{Q}} + p_{K/\mathbb{Q}} \leq \begin{cases} 5: & N_{F/\mathbb{Q}}(\varepsilon) = +1, s = 0 \\ 4: & N_{F/\mathbb{Q}}(\varepsilon) = -1, s = 0 \\ 3: & N_{F/\mathbb{Q}}(\varepsilon) = +1, s = 2 \\ 2: & N_{F/\mathbb{Q}}(\varepsilon) = -1, s = 2 \end{cases}$$

Proof.

Since $\varepsilon_{K/F}(\mathrm{Cl}(F))$ is trivial, by Theorem for $G = \mathrm{Gal}(K/F)$ we have

$$\#\mathrm{Po}(K/F) = \frac{h_F \cdot \prod_{\mathfrak{P} \mid \mathrm{disc}(K/F)} e_{\mathfrak{P}}}{\#H^1(G, U_K)}.$$

Proof.

Since $\varepsilon_{K/F}(\mathbf{Cl}(F))$ is trivial, by Theorem for $G = \mathrm{Gal}(K/F)$ we have

$$\#\mathrm{Po}(K/F) = \frac{h_F \cdot \prod_{\mathfrak{P}|\mathrm{disc}(K/F)} e_{\mathfrak{P}}}{\#H^1(G, U_K)}.$$

By Lemma , $\mathbf{Po}(K/F)$ is an elementary abelian 2-group of rank at most u, where

$$u := \#\{p \in \mathbb{Z} \text{ prime} : p\mathscr{O}_F = \beta_1\beta_2,\ \beta_i' \text{s ramify in } K/F\}$$

Proof.

Since $\varepsilon_{K/F}(\mathbf{Cl}(F))$ is trivial, by Theorem for $G = Gal(K/F)$ we have

$$\#Po(K/F) = \frac{h_F \cdot \prod_{\mathfrak{P}|disc(K/F)} e_{\mathfrak{P}}}{\#H^1(G, U_K)}.$$

By Lemma , $\mathbf{Po}(K/F)$ is an elementary abelian 2-group of rank at most u, where

$$u := \#\{p \in \mathbb{Z} \text{ prime} : p\mathscr{O}_F = \beta_1\beta_2, \beta_i' \text{s ramify in } K/F\}$$

$$\implies \frac{h_F.2^{r_{K/F}}}{\#H^1(G, U_K)} \mid 2^u.$$

For F imaginary, $2^{r_{F/\mathbb{Q}}-1} | h_F \Longrightarrow \frac{2^{r_{K/F}+r_{F/\mathbb{Q}}-1}}{\#H^1(G,U_K)} \,|\, 2^u$.
Using Herbrand quotient we find

$$\#H^1(G,U_K) = 2.\left(U_F : N_{K/F}(U_K)\right) \mid 2^2.$$

Hence

$$r_{K/F} + r_{F/\mathbb{Q}} - u \leq \begin{cases} 2: & F \neq \mathbb{Q}(\sqrt{-1}) \text{ and } -1 \in N_{K/F}(U_K) \\ 3: & F \neq \mathbb{Q}(\sqrt{-1}) \text{ and } -1 \notin N_{K/F}(U_K) \\ 2: & F = \mathbb{Q}(\sqrt{-1}) \text{ and } \sqrt{-1} \in N_{K/F}(U_K) \\ 3: & F = \mathbb{Q}(\sqrt{-1}) \text{ and } \sqrt{-1} \notin N_{K/F}(U_K) \end{cases}$$

$$\Longrightarrow 2t_{K/\mathbb{Q}} + p_{K/\mathbb{Q}} = r_{K/\mathbb{Q}} + t_{K/\mathbb{Q}} \overset{\text{Lemma}}{=} r_{K/F} + r_{F/\mathbb{Q}} - u.$$

Thanks for your attention