Some Pólya Fields of Small Degrees

(Lethbridge Number Theory and Combinatorics Seminar)

Abbas Maarefparvar

Department of Mathematics & Computer Science

University of Lethbridge

November 7, 2023

Proceedings of the Royal Society of Edinburgh, **149**, 1421–1433, *2019*
DOI:10.1017/prm.2018.86

Pólya S_3-extensions of $\mathbb{Q}$

Abbas Maarefparvar and Ali Rajaei
Department of Mathematics, Tarbiat Modares University,
Tehran 14115-134, Iran (a.maarefparvar@modares.ac.ir;
alirajaei@modares.ac.ir)

(MS received 10 May 2017; accepted 27 September 2017)

A number field K with a ring of integers $\mathcal{O}_K$ is called a Pólya field, if the $\mathcal{O}_K$-module of integer-valued polynomials on $\mathcal{O}_K$ has a regular basis, or equivalently all its Bhargava factorial ideals are principal [1]. We generalize Leriche's criterion [8] for Pólya-ness of Galois closures of pure cubic fields, to general S_3-extensions of $\mathbb{Q}$. Also, we prove for a real (resp. imaginary) Pólya S_3-extension L of $\mathbb{Q}$, at most four (resp. three) primes can be ramified. Moreover, depending on the solvability of unit norm equation over the quadratic subfield of L, we determine when these sharp upper bounds can occur.

Theorem (Pólya, 1919)

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

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

Replace $\mathbb{Q}$ with an arbitrary number field K

Definition (Ring of integer valued polynomials)

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

Replace $\mathbb{Q}$ with an arbitrary number field K

Definition (Ring of integer valued polynomials)

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

Proposition (Pólya, 1919)

$\mathrm{Int}(\mathcal{O}_K) \simeq \bigoplus_{n=0}^{\infty} \mathfrak{J}_n(\mathcal{O}_K)$ (as $\mathcal{O}_K$-module), where

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

denotes the n^{th} characteristic ideal of K.

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

Definition

If Int($\mathcal{O}_K$) has an $\mathcal{O}_K$-basis, say $\{f_n\}_n$, with exactly one member from each degree, i.e., $\deg(f_n) = n$, we say that Int($\mathcal{O}_K$) has a regular basis.

Example

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

Existence of a regular basis

Theorem (Pólya, 1919)

$\mathrm{Int}(\mathcal{O}_K)$ has a regular basis if and only if for every integer $n \geq 0$, the ideal $\mathfrak{J}_n(\mathcal{O}_K)$ is principal.

Existence of a regular basis

Theorem (Pólya, 1919)

$\mathrm{Int}(\mathcal{O}_K)$ has a regular basis if and only if for every integer $n \geq 0$, the ideal $\mathfrak{J}_n(\mathcal{O}_K)$ is principal.

Theorem (Ostrowski, 1919)

$\mathrm{Int}(\mathcal{O}_K)$ has a regular basis 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 (Zantema, 1982)

A number field K is called a Pólya field, if any of the following equivalent conditions holds:

1. $\mathrm{Int}(\mathcal{O}_K)$ has a regular basis;
2. All the characteristic ideals $\mathfrak{J}_n(\mathcal{O}_K)$'s are principal;
3. All the Ostrowski ideals $\Pi_q(K)$'s are principal;

Definition (Zantema, 1982)

A number field K is called a Pólya field, if any of the following equivalent conditions holds:

1. $\mathrm{Int}(\mathcal{O}_K)$ has a regular basis;
2. All the characteristic ideals $\mathfrak{J}_n(\mathcal{O}_K)$'s are principal;
3. All the Ostrowski ideals $\Pi_q(K)$'s are principal;

Remark

1. If $h_K = 1$, then K is a Pólya field. But not conversely, for instance, every cyclotomic field is a Pólya field (Zantema, 1982);
2. If $K/\mathbb{Q}$ is a Galois extension, the ideals $\Pi_{p^t}(K)$'s for all unramified primes p ($t \in \mathbb{N}$) are principal.

Pólya quadratic fields

Theorem (Zantema, 1982)

A quadratic number field $E = \mathbb{Q}(\sqrt{d})$ 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 prime numbers, and $E = \mathbb{Q}(\sqrt{d})$ has no units of negative norm.

Pólya cubic fields

Theorem(Zantema, 1982)

A cubic number field K is a Pólya field if and only if

- for $K/\mathbb{Q}$ Galois, it is ramified at only one prime;
- for $K/\mathbb{Q}$ non-Galois, K has class number one.

Remark

Let $K = \mathbb{Q}(\theta)$ be a cubic field, where θ is a root of $X^3 + aX + b$, for some $a, b \in \mathbb{Z}$. Then $K/\mathbb{Q}$ is Galois if and only if $-4a^3 - 27b^2$ is square.

Pólya cubic fields

Theorem(Zantema, 1982)

A cubic number field K is a Pólya field if and only if

- for $K/\mathbb{Q}$ Galois, it is ramified at only one prime;
- for $K/\mathbb{Q}$ non-Galois, K has class number one.

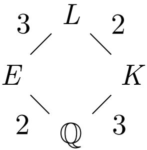
Remark

Let $K = \mathbb{Q}(\theta)$ be a cubic field, where θ is a root of $X^3 + aX + b$, for some $a, b \in \mathbb{Z}$. Then $K/\mathbb{Q}$ is Galois if and only if $-4a^3 - 27b^2$ is square.

There are some results concerning Pólya quartic and Pólya quintic fields (Zantema, Chabert, Leriche, M.).

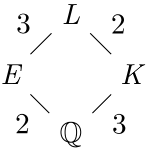
Pólya Galois number fields of degree 6

For $L/\mathbb{Q}$ a Galois extension with $[L:\mathbb{Q}] = 6$ (the non-Galois case is much more complicated!), consider the following diagram



Pólya Galois number fields of degree 6

For $L/\mathbb{Q}$ a Galois extension with $[L:\mathbb{Q}] = 6$ (the non-Galois case is much more complicated!), consider the following diagram

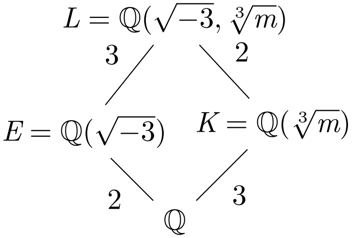


Theorem(Zantema, 1982)

If $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$, i.e., $K/\mathbb{Q}$ is Galois, then L is a Pólya field if and only if both E and K are Pólya fields.

Motiviation!

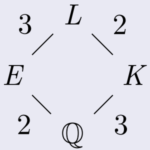
For $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$, when is L a Pólya field?



Theorem (Leriche, 2013)

The number field $L = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{m})$, for m a cube-free integer, is Pólya iff:

- when $m^2 \not\equiv 1 \pmod 9$, for each prime p dividing $3m$, the ideal $\Pi_p(K)$ is principal;
- when $m^2 \equiv 1 \pmod 9$, for each prime p dividing m, the ideal $\Pi_p(K)$ is principal.



$$\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$$

Theorem (M. - Rajaei, 2019)

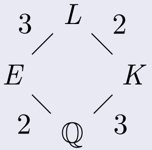
The number field L is Pólya field iff for each ramified prime p in $L/\mathbb{Q}$:

(a) if $e_{p(L/\mathbb{Q})} = 2$, then the ideal $\Pi_p(E)$ is principal;

(b) if $e_{p(L/\mathbb{Q})} = 3$, then the ideal $\Pi_p(K)$ is principal;

(c) if $e_{p(L/\mathbb{Q})} = 6$, then both the ideals $\Pi_p(E)$ and $\Pi_p(K)$ are principal,

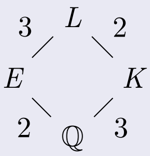
where $e_{p(L/\mathbb{Q})}$ denotes the ramification index of p in $L/\mathbb{Q}$.



$$\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$$

Corollary (M. - Rajaei, 2019)

1. If $3 \nmid h_K$ and E is Pólya, then L is a Pólya field. In particular, if E and K are Pólya, then so is L.
2. If L is Pólya, then E is also Pólya.
3. If all the finite primes of E are unramified in L, and E is Pólya, then L is also a Pólya field.



$$\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$$

Corollary (M. - Rajaei, 2019)

1. If $3 \nmid h_K$ and E is Pólya, then L is a Pólya field. In particular, if E and K are Pólya, then so is L.
2. If L is Pólya, then E is also Pólya.
3. If all the finite primes of E are unramified in L, and E is Pólya, then L is also a Pólya field.

Note that if all the finite primes of E are unramified in L, then $3 \mid h_E$.

Theorem (Honda, 1970)

Let $L/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$. Suppose that L is the splitting field of the polynomial

$$f(X) = X^3 + aX + b, \quad a, b \in \mathbb{Z}.$$

If $gcd(a, 3b) = 1$, then $L/\mathbb{Q}(\sqrt{-4a^3 - 27b^2})$ is unramified at all finite primes.

Theorem (Honda, 1970)

Let $L/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$. Suppose that L is the splitting field of the polynomial

$$f(X) = X^3 + aX + b, \quad a, b \in \mathbb{Z}.$$

If $gcd(a, 3b) = 1$, then $L/\mathbb{Q}(\sqrt{-4a^3 - 27b^2})$ is unramified at all finite primes.

Corollary (M. - Rajaei, 2019)

Let $L/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$. Suppose that L is the splitting field of the polynomial

$$f(X) = X^3 + aX + b, \quad a, b \in \mathbb{Z}.$$

If $gcd(a, 3b) = 1$, and $\mathbb{Q}(\sqrt{-4a^3 - 27b^2})$ is a Pólya field, then so is L.

Example

$K = \mathbb{Q}(\alpha)$; α is a root of $X^3 + 10X + 1$;

Example

$K = \mathbb{Q}(\alpha)$; α is a root of $X^3 + 10X + 1$;

$disc(K/\mathbb{Q}) = -4027$, $L = K(\sqrt{-4027})$ an S_3-extension of $\mathbb{Q}$;

Example

$K = \mathbb{Q}(\alpha)$; α is a root of $X^3 + 10X + 1$;

$disc(K/\mathbb{Q}) = -4027$, $L = K(\sqrt{-4027})$ an S_3-extension of $\mathbb{Q}$;

$gcd(10, 3) = 1$ and $\mathbb{Q}(\sqrt{-4027})$ is Pólya;

Example

$K = \mathbb{Q}(\alpha)$; α is a root of $X^3 + 10X + 1$;

$disc(K/\mathbb{Q}) = -4027$, $L = K(\sqrt{-4027})$ an S_3-extension of $\mathbb{Q}$;

$gcd(10, 3) = 1$ and $\mathbb{Q}(\sqrt{-4027})$ is Pólya;

$\Rightarrow$ L is a Pólya field;

Example

$K = \mathbb{Q}(\alpha)$; α is a root of $X^3 + 10X + 1$;

$disc(K/\mathbb{Q}) = -4027$, $L = K(\sqrt{-4027})$ an S_3-extension of $\mathbb{Q}$;

$gcd(10, 3) = 1$ and $\mathbb{Q}(\sqrt{-4027})$ is Pólya;

$\Rightarrow$ L is a Pólya field;

$h_K = 6$ and K is not Pólya;

Example

$K = \mathbb{Q}(\alpha)$; α is a root of $X^3 + 10X + 1$;

$disc(K/\mathbb{Q}) = -4027$, $L = K(\sqrt{-4027})$ an S_3-extension of $\mathbb{Q}$;

$gcd(10, 3) = 1$ and $\mathbb{Q}(\sqrt{-4027})$ is Pólya;

$\Rightarrow$ L is a Pólya field;

$h_K = 6$ and K is not Pólya;

While the ideal $\Pi_{4027}(K)$ is principal (This can only happen for non-Galois number fields).

Example

$K = \mathbb{Q}(\alpha)$; α is a root of $X^3 + 10X + 1$;

$disc(K/\mathbb{Q}) = -4027$, $L = K(\sqrt{-4027})$ an S_3-extension of $\mathbb{Q}$;

$gcd(10, 3) = 1$ and $\mathbb{Q}(\sqrt{-4027})$ is Pólya;

$\Rightarrow L$ is a Pólya field;

$h_K = 6$ and K is not Pólya;

While the ideal $\Pi_{4027}(K)$ is principal (This can only happen for non-Galois number fields).

Remark

All the above results concerning Pólya S_3-extensions of $\mathbb{Q}$ can be generalized to D_ℓ-extensions of $\mathbb{Q}$ for ℓ an odd prime number (M.-Rajaei, 2020).


THANK YOU
Any Questions?