



Sidi Mohamed Ben
Abdellah university
Faculty of Sciences Dhar
El Mahraz



Recent results in the study of monogenity and indices in number fields

Hamid Ben Yakkou

beyakouhamid@gmail.com

Number Theory Seminar, University of Debrecen

June 09, 2023

- 1 Introduction, Notations
- 2 Some previous explicit works
- 3 Prime ideal factorization via Newton polygon techniques
- 4 Monogeneity of certain pure number fields
- 5 Monogeneity and indices of certain number fields defined by trinomials
- 6 Thanks

- 1 Introduction, Notations
- 2 Some previous explicit works
- 3 Prime ideal factorization via Newton polygon techniques
- 4 Monogeneity of certain pure number fields
- 5 Monogeneity and indices of certain number fields defined by trinomials
- 6 Thanks

Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a root α of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$ of degree n and \mathbb{Z}_K its ring of integers.

Theorem

The ring \mathbb{Z}_K is a free- \mathbb{Z} -module of rank n .

- Any \mathbb{Z} -basis $(\omega_1, \omega_2, \dots, \omega_n)$ of the free \mathbb{Z} -module \mathbb{Z}_K is called an integral basis of K .
- For any primitive element θ of \mathbb{Z}_K (that is $\theta \in \mathbb{Z}_K$ and $K = \mathbb{Q}(\theta)$), the abelian group $\mathbb{Z}_K/\mathbb{Z}[\theta]$ is finite, its order is called the index of $\mathbb{Z}[\theta]$ (shortly, the index of θ), and is denoted by $(\mathbb{Z}_K : \mathbb{Z}[\theta])$.

Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a root α of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$ of degree n and \mathbb{Z}_K its ring of integers.

Theorem

The ring \mathbb{Z}_K is a free- \mathbb{Z} -module of rank n .

- Any \mathbb{Z} -basis $(\omega_1, \omega_2, \dots, \omega_n)$ of the free \mathbb{Z} -module \mathbb{Z}_K is called an integral basis of K .
- For any primitive element θ of \mathbb{Z}_K (that is $\theta \in \mathbb{Z}_K$ and $K = \mathbb{Q}(\theta)$), the abelian group $\mathbb{Z}_K/\mathbb{Z}[\theta]$ is finite, its order is called the index of $\mathbb{Z}[\theta]$ (shortly, the index of θ), and is denoted by $(\mathbb{Z}_K : \mathbb{Z}[\theta])$.

Definition : Monogenic number field

A number field K is called monogenic if \mathbb{Z}_K admits a power integral basis of the form $(1, \theta, \dots, \theta^{n-1})$ for some primitive element θ in \mathbb{Z}_K . This means that $\mathbb{Z}_K = \mathbb{Z}[\theta]$. In this case, we call θ a generator of a power integral basis of K (or shortly, a monogenerator).

If \mathbb{Z}_K has no power integral basis, we say that K is not monogenic.

Let

$$m(K) = \min\{(\mathbb{Z}_K : \mathbb{Z}[\theta]), \theta \in \mathbb{Z}_K, \text{ and } K = \mathbb{Q}(\theta)\}$$

be the minimal index of K .

- K monogenic $\Leftrightarrow (\mathbb{Z}_K : \mathbb{Z}[\theta]) = 1$ for some primitive element θ in \mathbb{Z}_K .
- K monogenic $\Leftrightarrow m(K) = 1$.

Definition : Monogenic number field

A number field K is called monogenic if \mathbb{Z}_K admits a power integral basis of the form $(1, \theta, \dots, \theta^{n-1})$ for some primitive element θ in \mathbb{Z}_K . This means that $\mathbb{Z}_K = \mathbb{Z}[\theta]$. In this case, we call θ a generator of a power integral basis of K (or shortly, a monogenerator).

If \mathbb{Z}_K has no power integral basis, we say that K is not monogenic.

Let

$$m(K) = \min\{(\mathbb{Z}_K : \mathbb{Z}[\theta]), \theta \in \mathbb{Z}_K, \text{ and } K = \mathbb{Q}(\theta)\}$$

be the minimal index of K .

- K monogenic $\Leftrightarrow (\mathbb{Z}_K : \mathbb{Z}[\theta]) = 1$ for some primitive element θ in \mathbb{Z}_K .
- K monogenic $\Leftrightarrow m(K) = 1$.

- Every quadratic number field $K = \mathbb{Q}(\sqrt{d})$, with $d \neq 1$ and square-free, has ring of integers given by

$$\mathbb{Z}_K = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{if } d \equiv 2, 3 \pmod{4}, \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

Thus, every quadratic number field is monogenic.

- If $K = \mathbb{Q}(\xi_n)$ is any cyclotomic number field, where $n \in \mathbb{Z}$ and ξ_n is a primitive n th root of unity, then $\mathbb{Z}_K = \mathbb{Z}[\xi_n]$.
So, every cyclotomic number field is monogenic.

- Every quadratic number field $K = \mathbb{Q}(\sqrt{d})$, with $d \neq 1$ and square-free, has ring of integers given by

$$\mathbb{Z}_K = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{if } d \equiv 2, 3 \pmod{4}, \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

Thus, every quadratic number field is monogenic.

- If $K = \mathbb{Q}(\xi_n)$ is any cyclotomic number field, where $n \in \mathbb{Z}$ and ξ_n is a primitive n th root of unity, then $\mathbb{Z}_K = \mathbb{Z}[\xi_n]$.
So, every cyclotomic number field is monogenic.

The first example of a non-monogenic number field

In 1878, R. Dedekind showed that the cubic number field $K = \mathbb{Q}(\alpha)$, where α is a root of $x^3 + x^2 - 2x + 8$ is not monogenic.



R. Dedekind, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, *Göttingen Abhandlungen*, **23**, (1878), 1–23.

How can one check the monogeneity of a given number field K and how to construct a power integral basis for it when it is monogenic?

Monogeneity of number fields is a classical problem of algebraic number theory, going back to **Dedekind, Hasse, and Hensel**. In the last five decades, there are extensive theoretical and computational results in the literature of testing monogeneity of number fields and constructing power integral bases.

M. Ahmed, S. Akhtari, T. Arnóczy, S. Arpin, M. Ayad, A. Bayad, H. Ben Yakkou, Y. Bilu, K. Blair, S. Bolzee, B. Boudine, A. Bremner, M.-L. Chang, M. E. Charkani, A. Chillali, H. Choulli, C. T. Davis, J. Didi, D. S. Dummit, El Fadil, J.-H. Evertse, T. Funakura, I. Gaál, T. A. Gassert, M.-N. Gras, J. Guàrdia, K. Győry, M. Hall, A. Hameed, L. Herr, J. G. Huard, J. G. Huard, R. H. Hudson, S. M. Husnine, R. Ibarra, B. Jadrijević, A. Jakhar, B. Jhorar, L. Jones, A. C. Kable, O. Kchit, S. K. Khanduja, N. Khan, O. Kihel, H. H. Kim, H. Kisilevsky, Y. Kôhno, S. Kuar, S. Kumar, H. Lembeck, G. Lettl, M. J. Lavalley, Y. Motoda, J. Montes, D.G.-Muños, Nakahara, E. Nart, G. Nyul, P. Olajos, M. Ozaslan, A. Pethő, G. Petrányi, T. Phillips, M. Pohst, L. Remete, M. Sahnoudi, N. Sangwan, M. Seddik, H. Smith, A. Soullami, B. K. Spearman, K. E. Stange, M. Sultan, F. Tanoé, M. Tinková, P. Teibekabe, D. White, K. S. Williams, Z. Wolske, Q. Yang, J. Yoo...

There are several methods to study the monogeneity of number fields, mainly :

- **The resolution of index form equations :**

I. Gaál, K. Győry, A. Pethő, M. Pohst and their collaborators, and others.

- **Relative power integral bases :**

S. Ahmed, M.-N. Gras, A. Hameed, S. M. Husnine, T. Nakahara...

- **Dedekind's criterion or its equivalent versions :**

T. A. Gassert, L. Jones, S. K. Khanduja, T. Phillips, M. Sahmoudi...

- **Prime ideal factorization :**

L. Carlitz, N. Khan, T. Nakahara, H. Sekigueli...

- **Prime ideal factorization via Newton polygon techniques :**

H. Ben Yakkou, H. Choulli, J. Didi, L. El Fadil, T. A. Gassert, J. Guàrdia, A. Jakhar, O. Kchit, J. Montes, S. Kuar, S. Kumar, E. Nart, H. Smith...

Let $(1, \omega_2, \dots, \omega_n)$ be an arbitrary integral basis of K and $L(x) = x_1 + x_2\omega_2 + \dots + x_n\omega_n$ be the fundamental form defined by this basis, where $x = (x_1, x_2, \dots, x_n) \in \mathbb{Z}^n$. Then

$$D_{K/\mathbb{Q}}(L(x)) = \prod_{1 \leq i < j \leq n} (L^{(j)}(x) - L^{(i)}(x))^2 = I(x_2, \dots, x_n)^2 D_K,$$

where $I(x_2, \dots, x_n)$ is an homogeneous form of degree $\frac{n(n-1)}{2}$ in $n - 1$ variables with coefficients in \mathbb{Z} , called the index form corresponding to the integral basis $(1, \omega_2, \dots, \omega_n)$.

It follows that if $\theta = x_1 + x_2\omega_2 + \cdots + x_n\omega_n \in \mathbb{Z}_K$ for some x_1, \dots, x_n in \mathbb{Z} , then

$$(\mathbb{Z}_K : \mathbb{Z}[\theta]) = |I(x_2, x_3, \dots, x_n)|.$$

Therefore, θ generates a power integral basis of K if and only if (x_2, x_3, \dots, x_n) satisfies the index form equation

$$I(x_2, x_3, \dots, x_n) = \pm 1 \quad (\text{IFE})$$

In a series of his papers, Győry (1973, 1974, 1976, 1978a, 1978b) gave general effective finiteness results for :

- monic polynomials with given discriminant (1973).
- integral elements in a number field with given discriminant/index (1973) (independently, in case of discriminant, an **ineffective** finiteness result was obtained by Birch and Merriman in 1972)
- He provided the first general algorithms for deciding whether K is monogenic or not and for determining all power integral bases in \mathbb{Z}_K .
- He gave the first explicit upper bounds for the absolute values of the solutions of an index form equation. These bounds imply, in an effective form, that there are only finitely many generators of a power integral basis.

Definitions

- Two monic polynomials $F(x), G(x) \in \mathbb{Z}[x]$ are \mathbb{Z} -equivalent if $G(x) = F(x + a)$ for some $a \in \mathbb{Z} \implies D(F) = D(G)$
- Two integral elements $\theta_1, \theta_2 \in \mathbb{Z}_K$ are \mathbb{Z} -equivalent if $\theta_2 = \theta_1 + a$ for some $a \in \mathbb{Z} \implies D_{K/\mathbb{Q}}(\theta_1) = D_{K/\mathbb{Q}}(\theta_2)$ and $(\mathbb{Z}_K : \mathbb{Z}[\theta_1]) = (\mathbb{Z}_K : \mathbb{Z}[\theta_2])$.

Theorem (Györy 1973)

Let D be a non-zero rational integer. Apart from \mathbb{Z} -equivalence, there are only finitely many monic polynomials $F(x)$ in $\mathbb{Z}[x]$ with $D(F) = D$, and a full set of representatives of such polynomials $F(x)$ can be effectively determined.

- In 1976, Györy proved that for given non-zero integer l , any index form equation

$$l(x_2, x_3, \dots, x_n) = l \text{ in } x_2, \dots, x_n \in \mathbb{Z}$$

has only finitely many integral solutions, and there is an effectively computable C such that $|x_i| \leq C$ for all $2 \leq i \leq n$ (quantitative version).






⇒ For $l = \pm 1$, decide effectively whether K is monogenic or not.

⇒ Up to translations by elements of \mathbb{Z} , there are only finitely many θ such that $(\mathbb{Z}_K : \mathbb{Z}[\theta]) = 1$.

⇒ Determine a full set of representative of inequivalent monogenerators of \mathbb{Z}_K .

- In 1978, 1981, Györy provided several effective finiteness results concerning the monogeneity of relative extensions and relative power integral bases of relative extensions.

Main steps in the proof : Reduction to systems of unit equations and application of Baker's method to these unit equations.

-  K.Győry, Sur les polynômes à coefficients entiers et de discriminant donné, *Acta Arithmetica* **23(4)** (1973), 419–426.
-  K.Győry, Sur les polynômes à coefficients entiers et de discriminant donne III, *Publ. Math. Debrecen.* **23** (1976), 141–165.
-  K.Győry, On polynomials with integer coefficients and given discriminant, IV, *Publ. Math. Debrecen.* **25** (1978), 155–167.
-  K.Győry, On discriminants and indices of integers of an algebraic number field, *J.Reine Angew. Math.* **324**(1981), 114–126.
-  K.Győry, Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains, *Acta Math. Hungar.* **42** (1983), 45-80.

Monogenic polynomials

For $K = \mathbb{Q}(\alpha)$ with $F(\alpha) = 0$, among the candidates which can generate a power integral basis of \mathbb{Z}_K is α .

Definition : Monogenic polynomial

Let $F(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n . The polynomial $F(x)$ is said to be monogenic if it is irreducible and $(1, \alpha, \dots, \alpha^{n-1})$ is a power integral basis of \mathbb{Z}_K , where $K = \mathbb{Q}(\alpha)$ and $F(\alpha) = 0$.

- A number field K defined by a non-monogenic polynomial can be monogenic.

Theorem : Dedekind's criterion

Let p be a rational prime. If $F(x)$ is the minimal polynomial for α , $K = \mathbb{Q}(\alpha)$, and $F(x) \equiv \prod_{i=1}^t \phi_i^{e_i}(x) \pmod{p}$, with $\phi_1(x), \dots, \phi_t(x)$ being irreducible polynomials and distinct modulo p , then set

$$M(x) = \frac{1}{p} \left(F(x) - \prod_{i=1}^t \phi_i^{e_i}(x) \right),$$

then p does not divide the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ if and only if $\phi_i(x)$ does not divide $M(x)$ modulo p for every $1 \leq i \leq t$ with $e_i \geq 2$.

The discriminant-index relation

For any primitive element $\theta \in \mathbb{Z}_K$ with minimal polynomial $F(x)$, we have

$$D(F) = D_{K/\mathbb{Q}}(\theta) = (\mathbb{Z}_K : \mathbb{Z}[\theta])^2 D_K,$$

where D_K is the discriminant K . This relation was established by **Dedekind**.
 \implies The candidates rational primes to divide the index of θ (in particular, the index of α) (**called singularities**) are

$$S_F = \{p, \text{ rational prime, } p^2 \text{ divides } D(F)\}$$

. • The discriminant $D(F)$ of F is calculable (resultant, formulas, programs (e.g. Maple)).

- 1 Introduction, Notations
- 2 Some previous explicit works**
- 3 Prime ideal factorization via Newton polygon techniques
- 4 Monogeneity of certain pure number fields
- 5 Monogeneity and indices of certain number fields defined by trinomials
- 6 Thanks

There are a great number of results regarding the monogeneity of several classes of numbers fields. Let us recall some of them.

- In 1989, **Gaál and Schulte** gave an efficient method for the computation of power integral bases of cubic number fields and performed it for all cubic fields with discriminant in the range $[-300, 3137]$.



I. Gaál and N. Schulte, Computing all power integral bases of cubic number fields, *Math. Comput.*, **53**, (1989), 689–696.

- In a series of their papers (1991, 1993, 1994, 1996, 1997), **Gaál, Pethő, and Pohst** gave efficient algorithms for several families of quartic number fields with not too large discriminant.



I. Gaál, A. Pethő and M. Pohst, On the resolution of index form equations in quartic number fields, *J. Symbolic Comput.*, **16**(1993), 563–584.

Method of proof : reduction to cubic/quartic Thue equations, application of Baker's method , and efficient reduction and enumeration algorithms

- In 1992, by reducing index form equations to system of unit equations, and using Baker's method and efficient reduction and enumeration algorithms, **Gaál and Győry** described an algorithm to solve index form equations in quintic fields. As application of their results, they computed all generators of power integral bases in totally real quintic fields with Galois group S_5 .



I. Gaál and K. Győry, Index form equations in quintic fields, *Acta Arithmetica*, **89(4)**, (1999), 379-396.

- In 2004, **Bilu, Gaál and Győry**, provided algorithms for sextic number fields and computed (with a hard computation) all generators of power integral bases in a totally real sextic number field with Galois group S_6 .



Y. Bilu, I. Gaál and K. Győry, Index form equations in sextic fields : a hard computation, *Acta Arithmetica* **115(1)** (2004), 85–96.

- In 2017, **Gaál and Remete** showed that if m is a square free rational integer such that $m \equiv 2$ or $3 \pmod{4}$, then the octic number field $K = \mathbb{Q}(i, \sqrt[4]{m})$ is not monogenic.








I. Gaál and L. Remete, Non-monogeneity in a family of octic fields, *Rocky Mountain J. Math*, **47(3)**, (2017), 817–824.

- In 2021, **Gaál** studied the multi-monogeneity of sextic number fields defined by trinomials of type $x^6 + ax^3 + b$.



I. Gaál, An experiment on the monogeneity of a family of trinomials, *JP Journal of Algebra Number Theory Appl*, **51(1)**, (2021), 97–111.

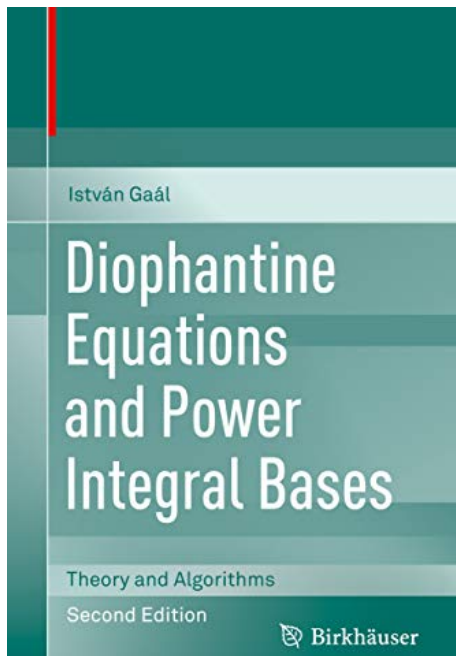
The following books give detailed surveys on discriminant and index form theory and its applications, including related Diophantine equations and monogeneity of number fields.

-  K. Győry, *Résultats effectifs sur la représentation des entiers par des formes décomposables*, Kingston, Canada, 1980.
-  W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers, 3rd edn.*, Springer Monographs in Mathematics (Springer-Verlag, Berlin, 2004).
-  J.-H. Evertse and K. Győry, *Unit Equations in Diophantine Number Theory*, Cambridge Univ. Press (2015).
-  J.-H. Evertse and K. Győry, *Discriminant Equations in Diophantine Number Theory*, Cambridge Univ. Press (2017).
-  I. Gaál, *Diophantine Equations and Power Integral Bases, Theory and algorithm, 2nd edn.*, Birkhäuser, (Boston, 2019).

New mathematical monographs: 32

Discriminant Equations in Diophantine Number Theory

Jan-Hendrik Evertse
and Kálmán Győry



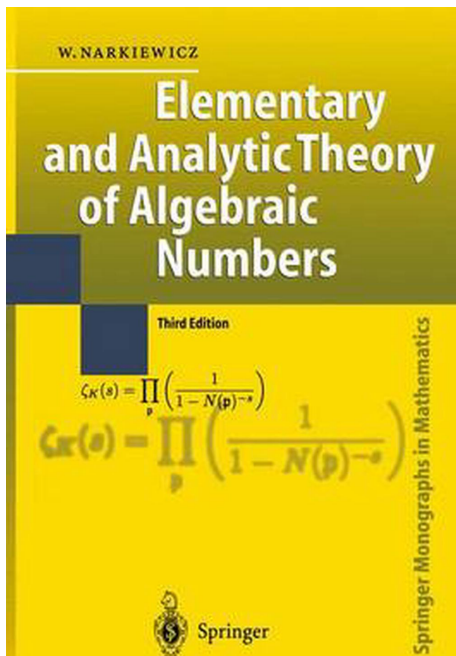
István Gaál

Diophantine Equations and Power Integral Bases

Theory and Algorithms

Second Edition

 Birkhäuser



- 1 Introduction, Notations
- 2 Some previous explicit works
- 3 Prime ideal factorization via Newton polygon techniques**
- 4 Monogeneity of certain pure number fields
- 5 Monogeneity and indices of certain number fields defined by trinomials
- 6 Thanks

The fundamental method to test whether a number K field is monogenic or not and determine all the power integral bases is to solve an index form equation associated to an integral basis $\{1, \omega_1, \dots, \omega_n\}$ of K , which is very complicated for higher degree number fields. For a number field of degree n , an index form equation $I(x_2, x_3, \dots, x_n) = \pm 1$ is a Diophantine equation of degree $\frac{n(n-1)}{2}$ with $n - 1$ variables. To decide the monogeneity of K , we should solve this equation which is not easy to achieve. Indeed, one must use advanced techniques and methods in addition to computations using powerful computers and algorithms. Actually, for $n \geq 7$ we do not have any general practical procedure to solve the corresponding index form equations. To overcome part of this problem, we use the prime ideal factorization method as our approach. We determine the prime ideals factorization by using Newton polygon techniques. This method is efficient to investigate indices and monogeneity of several classes of number fields.

The index of a number field

As defined by **Dedekind**, the index of a field K is

$$i(K) = \gcd \{(\mathbb{Z}_K : \mathbb{Z}[\theta]) \mid K = \mathbb{Q}(\theta) \text{ and } \theta \in \mathbb{Z}_K\}$$

Monogenic fields have both $m(K) = 1$ and $i(K) = 1$, but the condition $i(K) = 1$ is not sufficient for the monogeneity of K . Also, if $i(K) > 1$, then K is not monogenic.

Definition : prime common index divisor

A rational prime p dividing $i(K)$ is called a prime common index divisor of K .

\implies A number field possessing a prime common index divisor is not monogenic.

• p divides $i(K) \Leftrightarrow f(x_2, \dots, x_n) \equiv 0 \pmod{p}$ has solutions.

Theorem

The ring \mathbb{Z}_K is a Dedekind domain.

Let

$$p\mathbb{Z}_K = \prod_{j=1}^g \mathfrak{p}_j^{e_j}$$

be the factorization of $p\mathbb{Z}_K$ into a product of powers of distinct prime ideals \mathbb{Z}_K .

- $e_j = e(\mathfrak{p}_j/p)$, $j = 1, \dots, g$ is the ramification index of p at \mathfrak{p}_j .
- $f_j = (\mathbb{Z}_K/\mathfrak{p}_j : \mathbb{Z}/p\mathbb{Z})$ is the residual degree of \mathfrak{p}_j over p .

By **Dedekind's** Theorem on decomposition of primes in \mathbb{Z}_K , we deduce the following result which gives a necessary and sufficient condition for a rational prime integer p to be a common divisor. **This condition depends the form of the factorization of $p\mathbb{Z}_K$.**

Lemma A

Let p be a rational prime and K be a number field. For every positive integer f , let $L_p(f)$ be the number of distinct prime ideals of \mathbb{Z}_K lying above p with residue degree f , and $N_p(f)$ the number of monic irreducible polynomials of $\mathbb{F}_p[x]$ of degree f . Then p is a common index divisor of K if and only if $L_p(f) > N_p(f)$, for some positive integer f .

The numbers $N_p(f)$ and $L_p(f)$

- To apply Lemma A, one needs to know the number $N_p(f)$.

$$N_p(f) = \frac{1}{f} \sum_{d|f} \mu(d) p^{\frac{f}{d}},$$

where μ is the Möbius function. This number was found by Gauss.

Examples :

- ✓ For $f = 1$, $N_p(1) = p$ for every rational prime p : the monic linear irreducible polynomials in $\mathbb{F}_p[x]$ are : $x, x - 1, \dots, x - p + 1$.
- ✓ For $f = 2$ and $p = 2$, $N_2(2) = 1$: the unique monic irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$ is $x^2 + x + 1$.
- ✓ For $p = 5$, $N_5(2) = 10$ and $N_5(3) = 40$.

⇒ The number $N_p(f)$ increases according to f ⇒ It is more practical to consider small values of f .

- To apply Lemma A, one needs to know the number $L_p(f) \Leftrightarrow$ Determine the form of the factorization of $p\mathbb{Z}_K$.

To factorize $p\mathbb{Z}_K$, we will use Newton polygons techniques. This method was introduced by Ore, and developed by Guàrdia, Montes and Nart.

Let p be a rational prime integer and ν_p the discrete valuation of $\mathbb{Q}_p(x)$ defined on $\mathbb{Z}_p[x]$ by

$$\nu_p\left(\sum_{i=0}^m a_i x^i\right) = \min\{\nu_p(a_i), 0 \leq i \leq m\}.$$

Let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial whose reduction modulo p is irreducible. Any monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$ admits a unique ϕ -adic development

$$F(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_n(x)\phi(x)^n,$$

with $\deg(a_i(x)) < \deg(\phi(x))$. For every $0 \leq i \leq n$, let $u_i = \nu_p(a_i(x))$.

Definition

- The ϕ -Newton polygon of $F(x)$ is the lower boundary convex envelope of the set of points $\{(i, u_i), 0 \leq i \leq n, a_i(x) \neq 0\}$ in the Euclidean plane, which we denote by $N_\phi(F)$.
- The polygon determined by the sides of negative slopes of $N_\phi(F)$ is called the ϕ -principal Newton polygon of $F(x)$ and will be denoted by $N_\phi^+(F)$.

Example A

Consider the monic irreducible polynomial $F(x) = x^4 - 4x^3 + 12x^2 - 8x + 95$.
Let $p = 2$. The ϕ -adic development of $F(x)$ is

$$F(x) = \phi(x)^4 + 6\phi(x)^2 + 8\phi(x) + 96.$$

Here, we have :

$$a_0 = 96, a_1 = 8, a_2 = 6, a_3 = 0, a_4 = 1$$

$$\mu_0 = 5, \mu_1 = 3, \mu_2 = 1, \mu_3 = \infty, \mu_4 = 0.$$

Thus, $N_\phi^+(F) = S_1 + S_2$ with respect to ν_2 has two sides, with $d(S_1) = 2$,
 $d(S_2) = 1$, $\lambda_1 = -2$ and $\lambda_2 = \frac{-1}{2}$.

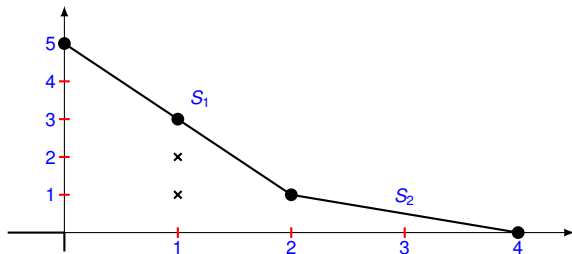


Figure – The ϕ -principal Newton polygon $N_\phi^+(F)$ with respect to ν_2 .

Let \mathbb{F}_ϕ be the finite field $\mathbb{Z}[x]/(\rho, \phi(x)) \simeq \mathbb{F}_\rho[x]/(\overline{\phi(x)})$.

• We attach to any abscissa $0 \leq i \leq l(N_\phi^+(F))$ the following residual coefficient $c_i \in \mathbb{F}_\phi$:

$$c_i = \begin{cases} 0, & \text{if } (i, u_i) \text{ lies strictly above } N_\phi^+(F), \\ \frac{a_i(x)}{\rho^{u_i}} \pmod{(\rho, \phi(x))}, & \text{if } (i, u_i) \text{ lies on } N_\phi^+(F). \end{cases}$$

• We attach to any side S of $N_\phi^+(F)$ of degree $d(S) = \frac{l(S)}{e(S)}$ the following residual polynomial :

$$R_\lambda(F)(y) = c_s + c_{s+e}y + \cdots + c_{s+(d-1)e}y^{d-1} + c_{s+de}y^d \in \mathbb{F}_\phi[y],$$

where s is the abscissa of the initial point of S ($d = d(S)$ and $e = e(S)$).

Let $K = \mathbb{Q}(\alpha)$ with $F(\alpha) = 0$.

- **Kummer** : Factorization of $p\mathbb{Z}_K$ when $p \nmid D(F)$.
- **Dedekind** : Factorization of $p\mathbb{Z}_K$ when $p \nmid (\mathbb{Z}_K : \mathbb{Z}[\alpha])$.
- **Ore** : Factorization of $p\mathbb{Z}_K$ when $F(x)$ is p -regular.

Definitions

- 1 *The polynomial $F(x)$ is ϕ -regular with respect to p if for each side S of $N_\phi^+(F)$, the associated residual polynomial $R_\lambda(F)(y)$ is separable in $\mathbb{F}_\phi[y]$.*
- 2 *The polynomial $F(x)$ is said to be p -regular if $F(x)$ is ϕ_i -regular for every $1 \leq i \leq t$, where $\overline{F(x)} = \prod_{i=1}^t \overline{\phi_i}^{l_i}$ is the factorization of $\overline{F(x)}$ into a product of powers of distinct irreducible polynomials in $\mathbb{F}_p[x]$.*
- 3 *The ϕ -index of $F(x)$, denoted by $\text{ind}_\phi(F)$, is $\deg(\phi)$ times the number of points with natural integer coordinates that lie below or on the polygon $N_\phi^+(F)$, strictly above the horizontal axis and strictly beyond the vertical axis.*

Ore's Theorem

- Let $\overline{F(x)} = \prod_{i=1}^t \overline{\phi_i(x)}^{l_i}$ be the factorization of $\overline{F(x)}$ into a product of powers of distinct irreducible polynomials in $\mathbb{F}_p[x]$.
- For every $i = 1, \dots, t$, let $N_{\phi_i}^+(F) = S_{i1} + \dots + S_{ir_i}$.
- For every $j = 1, \dots, r_i$, let $R_{\lambda_{ij}}(F)(y) = \prod_{s=1}^{S_{ij}} \psi_{ij_s}^{n_{ij_s}}(y)$ be the factorization of $R_{\lambda_{ij}}(F)(y)$ in $\mathbb{F}_{\phi_i}[y]$.

Theorem A : Ore's Theorem

With the notation as in above, we have :

1

$$\nu_p((\mathbb{Z}_K : \mathbb{Z}[\theta])) \geq \sum_{i=1}^t \text{ind}_{\phi_i}(F).$$

Moreover, the equality holds if $F(x)$ is p -regular.

2 If $F(x)$ is p -regular, then

$$p\mathbb{Z}_K = \prod_{i=1}^t \prod_{j=1}^{r_i} \prod_{s=1}^{S_{ij}} \mathfrak{p}_{ij_s}^{e_{ij}},$$

where e_{ij} is the ramification index of the side S_{ij} and $f_{ij_s} = \deg(\phi_i) \times \deg(\psi_{ij_s})$ is the residue degree of \mathfrak{p}_{ij_s} over p .

Example A

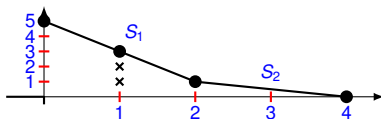


Figure – The ϕ -principal Newton polygon $N_{\phi}^{+}(F)$ with respect to ν_2 .

- Reducing modulo 2, we get $F(x) \equiv \phi(x)^4 \pmod{2}$, where $\phi = x - 1$. In this case, we have $D(F) = 2^{11} \cdot 3^3 \cdot 3457$ and $\overline{M(x)} = (x - 1)^2$
 \Rightarrow Neither **Dedekind's** nor **Kummer's** factorization theorem can be applied to factorize $2\mathbb{Z}_K$.
- The residual polynomials attached to the sides of $N_{\phi}^{+}(F)$ are $R_{\lambda_1}(F)(y) = 1 + y + y^2$ and $R_{\lambda_2}(F)(y) = 1 + y$, which are irreducible polynomials in $\mathbb{F}_{\phi}[y] \simeq \mathbb{F}_2[y]$. Thus, $F(x)$ is ϕ -regular, hence it is 2-regular. By Ore's Theorem (Theorem A),

$$\nu_2((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = \text{ind}_{\phi}(F) = \deg(\phi) \times 4 = 4$$

and

$$2\mathbb{Z}_K = \mathfrak{p}_1 \mathfrak{p}_2^2,$$

with respective residue degrees $f(\mathfrak{p}_1/2) = 2$ and $f(\mathfrak{p}_2/2) = 1$.




Newton polygons (the Montes algorithm) is an efficient tool compute discriminants and to determine p -integral bases of number fields which allows us to compute an integral basis. For every $1 \leq i \leq t$, $1 \leq j \leq l_i$, and $0 \leq k < m_i$, where $m_i = \deg(\phi_i)$, let $q_{i,j}(x)$ be the quotient of the Euclidean division of $F(x)$ by $\phi_i^j(x)$, $y_{i,j}$ the ordinate of $N_{\phi_i}^+(F)$ of abscissa j , and $\alpha_{i,j,k} = q_{i,j}(\alpha)\alpha^k$. The following Theorem gives explicitly a p -integral basis of K when the polynomial $F(x)$ is p -regular.





Theorem : Guàrdia, Montes and Nart, 2015

Under the above notations, if $F(x)$ is p -regular, then the family

$$\left\{ \frac{\alpha_{i,j,k}}{p^{\lfloor y_{i,j} \rfloor}}, 1 \leq i \leq t, 1 \leq j < l_i, 0 \leq k < m_i \right\}$$

is a p -integral basis of K .

-  P. Llorente, E. Nart and N. Vila, Discriminants of number fields defined by trinomials *Acta Arithmetica*, 1948.
-  L. Remete, Integral bases of pure fields with square free parameter, *Stud. Sci. Math. Hung.* **57(1)**, (2020), 91–115.
-  S. Kaur and S.K. Khanduja, Discriminant and integral basis of sextic fields defined by $x^6 + ax + b$. *Commun. in Algebra*. **50(10)**, (2022).

-  O. Ore, Newtonsche Polygone in der Theorie der algebraischen Körper, *Math. Ann.* **99** (1928), 84–117.
-  J. Montes and E. Nart, On theorem of Ore, *Journal of Algebra* **146(2)** (1992), 318–334.
-  J. Guàrdia, J. Montes and E. Nart, Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields, *Journal de théorie des nombres de Bordeaux* **23(7)** (2011), 667–669.
-  J. Guàrdia, J. Montes and E. Nart, Newton polygons of higher order in algebraic number theory, *Tran. Math. Soc. American* **364(1)**, (2012), 361–416.

- 1 Introduction, Notations
- 2 Some previous explicit works
- 3 Prime ideal factorization via Newton polygon techniques
- 4 Monogeneity of certain pure number fields**
- 5 Monogeneity and indices of certain number fields defined by trinomials
- 6 Thanks

Monogeneity of certain pure number fields

Let $K = \mathbb{Q}(\alpha)$ be a pure number field generated by a root α of a monic irreducible polynomial $F(x) = x^n - m$, \mathbb{Z}_K its ring of integers. There are several important and basic works concerning these fields. Let recall here some of them.

- In 2014, **S. Ahmad, T. Nakahara and S.M. Husnine** proved that if m is a square free rational integer such that $m \equiv 2, 3 \pmod{4}$ and $m \not\equiv \pm 1 \pmod{9}$, then the sextic pure field $K = \mathbb{Q}(\sqrt[6]{m})$ is monogenic.



S. Ahmad, T. Nakahara and S.M. Husnine, Power integral bases for certain pure sextic fields, *I. J. Number Theory*, **10(8)**, (2014), 2257–2265.

- In 2017, **Gassert** studied the monogeneity of the polynomial $x^n - m$ (The integrally closedness of $\mathbb{Z}[\alpha]$).



T. A. Gassert, A note on the monogeneity of power maps, *Albanian J. Math*, **11**(2017), 3–12.

- In 2017, **Gaál and Remete** answered completely to the problem of monogeneity of pure number fields $K = \mathbb{Q}(\sqrt[n]{m})$, where $m \neq \pm 1$ is a square free rational integer and $3 \leq n \leq 9$.



I. Gaál and L. Remete, Power integral bases and monogeneity of pure fields, *J. of Number Theory*, **173**, (2017), 129–146.

- Between 2020-2022, **El Fadil** based on prime ideal factorization via Newton polygon techniques, he studied the monogeneity of several pure number fields of fixed degrees, namely of degrees 6, 12, 18, 20, 24...



L. El Fadil, On Power integral bases for certain pure sextic fields, *Bol. Soc. Paran. Math*, (2020), doi :10.5269/bspm.42373.



L. El Fadil, On power integral basis for certain pure number fields defined by $x^{36} - m$, *Stud. Sci. Math. Hung*, **58(3)**, (2021).



L. El Fadil, On power integral bases for certain pure number fields defined by $x^{18} - m$, *Commentationes Mathematicae Universitatis Carolinae*, (2022).

Monogeneity of pure number fields of degrees p^f

The majority of available works regarding the problem of monogeneity of K consider only pure number fields of small fixed degrees n , namely $3 \leq n \leq 9$.

- In 2021, Ben Yakkou and El Fadil studied the monogeneity of certain pure number fields of degree p^f .



H. Ben Yakkou and L. El Fadil, On monogeneity of certain pure number fields defined by $x^{p^f} - m$, *I. J. of Number theory*, 17 (10) (2021), 2235–2242. DOI : <https://doi.org/10.1142/S1793042121500858>.

Based on prime ideal factorization via Newton polygon techniques, mainly, Ore's Theorem (Theorem A), Lemma A (prime common index divisor), and using some technical results such as the following lemma which allows to evaluate the p -adic valuation of the Binomial coefficient :

Lemma B

Let p be a rational prime integer and r be a positive integer. Then

$$\nu_p \left(\binom{p^f}{j} \right) = r - \nu_p(j)$$

for any integer $j = 1, \dots, p^f - 1$.

we obtain some new results on the monogeneity of these pure number fields.

The following theorem is an improvement of Gassert's result for $n = p^r$. Recall also that Gassert used Dedekind's criterion to show her result, but we used the Index Theorem of Ore to prove our result.

Theorem 1 (Ben Yakkou and El Fadil, 2021)

Let $n = p^r$, with p a prime rational integer, and r a positive integer, then $\mathbb{Z}[\alpha]$ is the ring of integers of K if and only if $\nu_p(m^p - m) = 1$.

Notice that by the above theorem, if $\nu_p(m^p - m) \geq 2$, then $\mathbb{Z}[\alpha]$ is not the ring of integers of K . Henceforth, It can not decide on the monogeneity of K . The following theorem gives a partial answer.

Theorem 2 (Ben Yakkou and El Fadil, 2021)

For $n = p^r$, with p an odd prime integer not dividing m . If $m^{p-1} \equiv 1 \pmod{p^{p+1}}$ and $r \geq p$, then K is not monogenic.

We proved that p is a common index divisor of K .

- $\overline{F(x)} = (x - m)^{p^r}$ in $\mathbb{F}_p[x]$.
- Using Binomial Theorem, we get

$$F(x) = (x - m)^{p^r} + \sum_{j=1}^{p^r-1} \binom{p^r}{j} m^{p^r-j} (x - m)^j + m^{p^r} - m.$$

Let $\phi = x - m$ and $\nu = \nu_p(m^{p^r} - m)$.

- $\nu = \nu_p(m^{p^r} - m) = \nu_p(m^{p-1} - 1)$.
- $\nu > p$ and $r \geq p + 1$ Applying Lemma B \Rightarrow

$$N_{\phi}^+(F) = S_1 + \cdots + S_{t-p+1} + \cdots + S_t$$

has t -distinct sides of degree 1 each, with $t \geq p + 1$.

$\Rightarrow F(x)$ is p -regular + Applying Ore's Theorem $\Rightarrow L_p(1) \geq p + 1$. But $N_p(1) = p$ + Applying Lemma A $\Rightarrow p$ divides $i(K)$.

The case $p = 2$ is different to the case when p is odd ; the first side of $N_{\phi}^{+}(F)$ can have degree 2 which can induces non separable residual polynomial.

Theorem 3 (Ben Yakkou and El Fadil, 2021)

Assume that $n = 2^r$ ($p=2$).

- 1 If $r = 2$ and $m \equiv 1 \pmod{16}$, then the pure quartic number field K is not monogenic.
- 2 If $r \geq 3$ and $m \equiv 1 \pmod{32}$, then K is not monogenic.

This result is partially complete the work of A. Hameed, T. Nakahara, S. M. Husnine, and S. Ahmed when they proved that for $n = 2^r$, if $m \equiv 2$ or $3 \pmod{4}$, then $\mathbb{Z}[\alpha]$ is the ring of integers of K for every natural integer r .



A. Hameed, T. Nakahara, S. M. Husnine, and S. Ahmed, On existence of canonical number system in certain classes of pure algebraic number fields, *J. Prime Res. Math*, **7** (2011), 19–24.

Our second work is about pure number fields defined by $x^{2^r \cdot 5^s} - m$, where r and s are two positive integers.



H. Ben Yakkou, A. Chillali and L. El Fadil, On Power integral bases for certain pure number fields defined by $x^{2^r \cdot 5^s} - m$, *Comm. in Algebra*, **49(7)**, (2021), 2916–2926.

- We have extended our knowledge about $N_\phi^+(F)$, the ϕ -principal Newton polygon, where ϕ is a monic irreducible factor modulo a given rational prime p of an irreducible polynomial of type $x^n - m$.
- We have used the technique of ϕ -admissible developments ([Guàrdia, Montes and Nart](#)).

Let

$$F(x) = \sum_{j=0}^n A_j(x) \phi(x)^j, \quad A_j(x) \in \mathbb{Z}_p[x],$$

be a ϕ -development of $F(x)$, not necessarily the ϕ -adic one. Take $\omega_j = \nu_p(A_j(x))$, for all $0 \leq j \leq n$. Let N be the principal polygon of the set of points $\{(j, \omega_j) \mid 0 \leq j \leq n, \omega_j \neq \infty\}$. To any $0 \leq j \leq n$, we attach a residual coefficient as follow :

$$c'_j = \begin{cases} 0, & \text{if } (j, \omega_j) \text{ lies strictly above } N, \\ \frac{A_j(x)}{p^{\omega_j}} \pmod{(p, \phi(x))}, & \text{if } (j, \omega_j) \text{ lies on } N. \end{cases}$$

Moreover, for any side S of N with slope λ , we define the residual polynomial associated to S and noted $R'_\lambda(F)(y)$ (similar to the residual polynomial $R_\lambda(F)(y)$ defined from the ϕ -adic development). We say that a ϕ -development is admissible if $c'_j \neq 0$ for each abscissa j of a vertex of N .

- $c'_j \neq 0$ if and only if $\overline{\phi(x)} \nmid \left(\frac{A_j(x)}{p^{\omega_j}} \right)$.

Lemma C : Guàrdia, Montes and Nart, 2012

If a ϕ -development of $F(x)$ is admissible, then $N_\phi^+(F) = N$ and $c'_j = c_j$. In particular, for any segment S of N we have $R'_\lambda(F)(y) = R_\lambda(F)(y)$.

We have proved the following technical lemma.

Lemma D

Let $k \geq 1$ be the highest power of a prime p dividing a positive integer $n = u \cdot p^k$ and m be an integer not divisible by p such that the monic polynomial $F(x) = x^n - m \in \mathbb{Z}[x]$ is irreducible over \mathbb{Q} . Then the following hold :

- 1 If $\nu_p(m^{p^k} - m) = 1$, then for any irreducible factor $\overline{\phi(x)}$ of $\overline{F(x)}$ in $\mathbb{F}_p[x]$, $N_{\overline{\phi}}^+(F) = S$ has a single side of height 1.
- 2 If $\overline{\phi(x)}$ is a monic irreducible factor of $\overline{F(x)}$ in $\mathbb{F}_p[x]$ of degree 1. Let $Q(x) \in \mathbb{Z}[x]$ and $a \in \mathbb{Z}$ be respectively the quotient and remainder upon the Euclidean division of $x^u - m$ by $\phi(x)$. Let

$$\omega_0 = \nu_p(m^{p^k} - m + \sum_{j=1}^{p^k} \binom{p^k}{j} m^{p^k-j} a^j). \text{ Then } N_{\overline{\phi}}^+(F) \text{ is the lower}$$

boundary convex envelope of the set of points

$\{(0, \omega_0)\} \cup \{(p^j, k - j) \mid 0 \leq j \leq k\}$ in the Euclidean plane. In particular

$$\omega_0 \geq \min\{\nu_p(m^{p^k} - m), k + 1\}.$$

Theorem 4, Ben Yakkou and El Fadil, 2021

Under the notation as in above, $\mathbb{Z}[\alpha]$ is the ring of integers of K if and only if $m \not\equiv 1 \pmod{4}$ and $m \not\equiv 1, 7, 18, 24 \pmod{25}$. In this case K is monogenic and α generates a power integral basis of \mathbb{Z}_K .

Theorem 5, Ben Yakkou and El Fadil, 2021

Under the above hypothesis. If one of the following conditions holds :

- 1 $r = 2$ and $m \equiv 1 \pmod{16}$.
- 2 $r \geq 3$ and $m \equiv 1 \pmod{32}$.
- 3 $r = 1$, $s \geq 2$ and $m \equiv \pm 1 \pmod{125}$.
- 4 $r \geq 2$ and $m \equiv 1 \pmod{25}$.

Then K is not monogenic.

Theorem 6, Ben Yakkou and Didi, 2023

The ring $\mathbb{Z}[\alpha]$ is the ring of integers of K if and only if m is square-free, $m \not\equiv 1 \pmod{4}$, $m \not\equiv \pm 1 \pmod{9}$ and $\bar{m} \notin \{\pm 1, \pm 18, \pm 19\} \pmod{49}$. In this case, K is monogenic and α generates a power integral of \mathbb{Z}_K .

Theorem 7, Ben Yakkou and Didi, 2023

if one of the following conditions holds :

- 1 $m \equiv 1 \pmod{4}$.
- 2

lab	$m \equiv 1 \pmod{9}$.
lbb	$r \geq 2$ and $m \equiv -1 \pmod{9}$.
lcb	$r = 1$ and $m \equiv -1 \pmod{81}$.
- 3

lab	$m \equiv 1 \pmod{49}$.
lbb	$r = 1$, $s \geq 7$ and $m \equiv -1 \pmod{7^8}$.
lcb	$r \geq 2$, $s \geq 3$ and $m \equiv -1 \pmod{7^4}$,

then K is not monogenic.

Corollary, Ben Yakkou and Didi, 2023

Let K be a pure number field generated by a complex root of a monic irreducible polynomial $x^{2^r \cdot 3^k \cdot 7^s} - m^t$, with $m \neq \pm 1$ a square-free rational integer and t a positive integer which is coprime to 42. Then the following hold.

1 If $m \not\equiv 1 \pmod{4}$, $m \not\equiv \pm 1 \pmod{9}$ and $\bar{m} \notin \{\pm 1, \pm 18, \pm 19\} \pmod{49}$, then K is monogenic.

2 If $m \equiv 1 \pmod{4}$, then K is not monogenic.

3 If

lab $m \equiv 1 \pmod{9}$.

lbb $r \geq 2$ and $m \equiv -1 \pmod{9}$.

lcb $r = 1$ and $m \equiv -1 \pmod{81}$,

then K is not monogenic.

4 If

lab $m \equiv 1 \pmod{49}$.

lbb $r = 1$, $s \geq 7$ and $m \equiv -1 \pmod{7^8}$.

lcb $r \geq 2$, $s \geq 3$ and $m \equiv -1 \pmod{7^4}$,

then K is not monogenic.

- 1 Introduction, Notations
- 2 Some previous explicit works
- 3 Prime ideal factorization via Newton polygon techniques
- 4 Monogeneity of certain pure number fields
- 5 Monogeneity and indices of certain number fields defined by trinomials**
- 6 Thanks

Monogeneity of certain number fields defined by trinomials

Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a root α of a monic irreducible trinomial of type $F(x) = x^n + ax^m + b \in \mathbb{Z}[x]$ and \mathbb{Z}_K its ring of integers.

- In 2016, **Jhorar and Khanduja** studied the monogeneity of the polynomial $x^n + ax + b$.



B. Jhorar and S.K. Khanduja, On power basis of a class of algebraic number fields, *I. J. Number Theory*, **12(8)**, (2016), 2317–2321.

- In 2021, **Jones and White** identified new infinite families of monogenic trinomials with non-squarefree discriminant.



L. Jones and D. White, Monogenic trinomials with non-squarefree discriminant, *International Journal of Mathematics*, doi : 10.1142/S0129167X21500890, (2021).

- In 2022, **Ben Yakkou and El Fadil** studied the non monogeneity of number fields defined by $x^n + ax + b$.



H. Ben Yakkou and L. El Fadil, On monogeneity of certain pure number fields defined by trinomials, *Funct. et Approx. Comment. Math.*, (2022).

Theorem 8 : Ben Yakkou and El Fadil, 2022

Let $K = \mathbb{Q}(\alpha)$, $F(\alpha) = 0$, $F(x) = x^5 + ax + b$

- 1 $a \equiv 1 \pmod{4}$ and $b \equiv 2 \pmod{4}$.
- 2 $(a, b) \in \{(7, 8), (15, 0)\} \pmod{16}$.
- 3 $(a, b) \in \{(3, 20), (19, 4)\} \pmod{32}$.
- 4 $(a, b) \in \{(3, 4), (19, 20), (35, 36), (51, 52)\} \pmod{64}$.
- 5 $(a, b) \in \{(3, 12), (19, 28)\} \pmod{32}$.
- 6 $(a, b) \in \{(3, 60), (19, 44), (35, 28), (51, 12)\} \pmod{64}$.
- 7 $a \equiv 4 \pmod{8}$ and $b \equiv 0 \pmod{8}$,

then K is not monogenic.

In every case, we have proved that 2 divides $i(K)$.

Theorem 9 : Ben Yakkou and El Fadil, 2022

Let $K = \mathbb{Q}(\alpha)$, $F(\alpha) = 0$, $F(x) = x^6 + ax + b$

- 1 $a \equiv 0 \pmod{8}$ and $b \equiv 7 \pmod{8}$.
- 2 $a \equiv 2 \pmod{4}$, $b \equiv 1 \pmod{4}$ and $\nu_2(1 + a + b) = 2\nu_2(a + 6)$. In particular if $(a, b) \in \{(6, 9), (14, 1), (22, 25), (30, 17)\} \pmod{64}$.
- 3 $a \equiv 0 \pmod{8}$ and $b \equiv 3 \pmod{8}$.
- 4 $a \equiv 0 \pmod{9}$ and $b \equiv -1 \pmod{9}$,

then K is not monogenic.

• In (1)(2)(3), we have 2 divides $i(K)$. But in (4), we have 3 divides $i(K)$.

Remark : Independently, in 2022, **Jakhar and Kumar** proved that if one of the conditions (1) or (4) holds, then K is monogenic.

Some fundamental results about the index of a number field

Recall that

$$i(K) = \gcd \{ (\mathbb{Z}_K : \mathbb{Z}[\theta]) \mid K = \mathbb{Q}(\theta) \text{ and } \theta \in \mathbb{Z}_K \}.$$

- 1878, **Dedekind** : $p \mid i(K) \Leftrightarrow L_p(f) > N_p(f)$ for some positive integer f (Lemma A).
- 1913, **Żyliński** : $p \mid i(K) \implies p < n$.
- 1926, **Ore** : $\nu_p(i(K))$ is not in general determined by the form of the factorization of $p\mathbb{Z}_K$.
- 1930, **Engstrom** : Confirmed Ore's conjecture (example $n = 8$) + Explicit formulas for $\nu_p(i(K))$ in certain general cases.
 \implies For $n \leq 7$, in the majority of cases, $\nu_p(i(K))$ is determined by the form of the factorization of $p\mathbb{Z}_K$ (tables).
- 1982, **Śliwa** : $\nu_p(i(K))$ when p is unramified in K .
- 1984, **Nart** : gave $\nu_p(i(K))$ in totally case (arithmetic invariants) + Extend some of Engstrom's formulas + Confirmed Ore's conjecture in a more general case.

One of the unsolved problems in Algebraic Number Theory is determining the indices (highest powers of primes dividing indices) in infinite families of number fields. This problem is referred to as Problem 22 in Narkwicz's book.

- 1983, Llorente and Nart for $F(x) = x^3 + ax + b$.
- 2017, Davis and Spearman for $F(x) = x^4 + ax + b$.
- 2022, Gaál and El Fadil for $F(x) = x^4 + ax^2 + b$.
- 2022, Ben Yakkou for $F(x) = x^5 + ax^3 + b$ (independently, El Fadil).
- 2022, Jakhar, Kaur and Kumar for $F(x) = x^5 + ax + b$.
- 2022, El Fadil, Kchit for $F(x) = x^7 + ax^3 + b$.

The index of the septic number field defined by $x^7 + ax^5 + b$

In 2023, **Ben Yakkou** completely characterized indices in number fields defined by trinomials of type $x^7 + ax^5 + b$. More precisely, he proved the following result.

Theorem 10 : (Ben Yakkou, 2023)

Let $K = \mathbb{Q}(\theta)$ be a number field with θ a root of a monic irreducible polynomial $F(x) = x^7 + ax^5 + b \in \mathbb{Z}[x]$. Then $i(K) \in \{1, 2, 4\}$.

To prove the above result :

- For any odd rational p , p is not a common index divisor of K ; p does not divide $i(K)$.
 - For $p = 2$, in every case, $\nu_2(i(K))$ is given.
- ▷ Żyliński's condition + $\deg(K) = 7 \implies$ If $p \mid i(K)$, then $p < 7 \implies p = 2, 3, 5$
▷ the index-discriminant relation :

$$\nu_p(D(\eta)) = 2\nu_p((\mathbb{Z}_K : \mathbb{Z}[\eta])) + \nu_p(D_K),$$

and the discriminant formula

$$\Delta(F) = -b^4(7^7 b^2 + 2^2 \times 5^5 a^7).$$

\implies For $p = 3$, if 3 divides $i(K)$, then

$$(a, b) \in \{(1, 0), (-1, 0), (1, 1), (-1, 1), (0, 0)\} \pmod{3}.$$

▷ if p divides both a and b , then $\nu_p(a) < 2$ or $\nu_p(b) < 7$.

The index of the septic number field defined by $x^7 + ax^5 + b$

Case	Conditions	Factorization of $3A_K$
A1	$a \equiv 1 \pmod{3}, b \equiv 0 \pmod{3}$ and $5 \nmid \nu_3(b)$	$[1^5, 2]$
A2	$a \equiv 1 \pmod{3}$ and $5 \mid \nu_3(b)$	$[1, 2, 4]$
A3	$a \equiv -1 \pmod{3}, b \equiv 0 \pmod{3}$ and $5 \nmid \nu_3(b)$	$[1, 1, 1^5]$
A4	$a \equiv -1 \pmod{3}$ and $5 \mid \nu_3(b)$	$[1, 1, 1, 4]$
A5	$a \equiv 1 \pmod{3}, b \equiv 1 \pmod{3}$	$[1, 1, 2, 3], [1^2, 2, 3]$ or $[2, 2, 3]$
A6	$a \equiv -1 \pmod{3}, b \equiv 1 \pmod{3}$	$[7]$
A7	$7\nu_3(a) > 2\nu_3(b)$ and $\nu_3(b) \in \{1, 2, 3, 4, 5, 6\}$	$[1^7]$
A8	$\nu_3(a) = 1, \nu_3(b) \geq 4$ and $5 \nmid \nu_3(b)$	$[1^2, 1^5]$
A9	$\nu_3(a) = 1$ and $5 \mid \nu_3(b)$	$[1, 1^2, 4]$

Table – The factorization of $3A_K$

\Rightarrow Lemma A+ the above table, 3 does not divide $i(K)$.

+ similarly, we show that 5 does not divide $i(K)$.

\Rightarrow The unique rational prime which can divide $i(K)$ is 2.

$\Rightarrow i(K) = 2^{\nu_2(i(K))}$.

The index of the septic number field defined by $x^7 + ax^5 + b$

Case	Conditions	$2A_K$	$i(K)$
C1	$a \equiv 1 \pmod{2}$ and $b \equiv 1 \pmod{2}$	$[2^1, 5^1]$	1
C2	$a \equiv 0 \pmod{2}$ and $b \equiv 1 \pmod{2}$	$[1, 3, 3]$	1
C3	$7\nu_2(a) > 2\nu_2(b)$ and $\nu_2(b) \in \{1, 2, 3, 4, 5, 6\}$	$[1^7]$	1
C4	$\nu_2(a) = 1, \nu_2(b) \geq 4$ and $5 \nmid \nu_2(b)$	$[1^2, 1^5]$	1
C5	$\nu_2(a) = 1$ and $5 \mid \nu_2(b)$	$[1, 1^2, 4]$	1
C6	$a \equiv 3 \pmod{8}, b \equiv 0 \pmod{8}$, and $5 \nmid \nu_2(b)$	$[1^5, 2]$	1
C7	$a \equiv 3 \pmod{8}, b \equiv 0 \pmod{8}$, and $5 \mid \nu_2(b)$	$[1, 2, 4]$	1
C8	$a \equiv 7 \pmod{8}, b \equiv 4 \pmod{8}$	$[2, 1^5]$	1
C9	$a \equiv 3 \pmod{8}, b \equiv 4 \pmod{8}$	$[1, 1, 1^5]$	2
C10	$a \equiv 7 \pmod{8}, b \equiv 0 \pmod{8}$, and $5 \nmid \nu_2(b)$	$[1, 1, 1^5]$	2
C11	$a \equiv 7 \pmod{8}, b \equiv 0 \pmod{8}$, and $5 \mid \nu_2(b)$	$[1, 1, 1, 4]$	2
C12	$a \equiv 3 \pmod{4}$ and $b \equiv 2 \pmod{4}$	$[1^2, 1^5]$	1
C13	$a \equiv 1 \pmod{4}, b \equiv 0 \pmod{4}$ and $5 \nmid \nu_2(b)$	$[1^2, 1^5]$	1
C14	$a \equiv 1 \pmod{4}, b \equiv 0 \pmod{4}$ and $5 \mid \nu_2(b)$	$[1, 1^2, 4]$	1
C15	$(a, b) \in \{(1, 10), (9, 2), (1, 6), (9, 14)\} \pmod{16}$	$[1^2, 1^5]$	1
C16	$(a, b) \in \{(1, 18), (17, 2), (1, 14), (17, 30)\} \pmod{32}$	$[2, 1^5]$	1
C17	$(a, b) \in \{(1, 2), (17, 18), (1, 30), (17, 14)\} \pmod{32}$	$[1, 1, 1^5]$	2 or 4
C18	$(a, b) \in \{(5, 2), (5, 14), (13, 6), (13, 10)\} \pmod{16}$	$[1^5, 1^5]$	1

Table – The factorization of $2A_K$ and the value of $i(K)$

The index of the octic number field defined by $x^8 + ax + b$

Theorem 11 : Ben Yakkou and Boudine, 2023 (to appear in Acta. Math. Hungar)

Let $K = \mathbb{Q}(\alpha)$, $F(\alpha) = 0$, $F(x) = x^8 + ax + b$. Then $i(K) = 2^m$ for some natural integer m .

The index of the octic number field defined by $x^8 + ax + b$

For $t \in \mathbb{Z}$, $t_p = \frac{t}{p^{\nu_p(t)}}$.

Theorem 12 : Ben Yakkou and Boudine, 2023 (to appear in Acta. Math. Hungar)

Let $K = \mathbb{Q}(\alpha)$, $F(\alpha) = 0$, $F(x) = x^8 + ax + b$ such that $(a, b) \not\equiv (32, 16) \pmod{64}$ and $(a, b) \notin \{(0, 112), (64, 112)\} \pmod{128}$. When

$a \equiv 8 \pmod{16}$ and $b \equiv 7 \pmod{16}$, let

$$\omega = \nu_2(b^7 - 7^7 a_2^8), A_{a,b}^1 = b(b^7 - 7^7 a_2^8)_2 + 7a_2(7^7 a_2^8 - b^7 + b^6 a_2),$$

$$A_{a,b}^2 = (b(b^7 - 7^7 a_2^8)_2 + 7a_2(7^7 a_2^8 - b^7 + b^6 a_2))_2 + b^4(245a_2 - 14b),$$

$$B_{a,b} = (b^7 - 7^7 a_2^8)_2 + 7^3 \cdot a_2^2 \cdot b^6.$$

Then 2 divides $i(K)$ if and only if one of the following conditions hold :

- 1 $a \equiv 4 \pmod{8}$ and $b \equiv 3 \pmod{8}$.
- 2 $(a, b) \in \{(0, 31), (16, 15)\} \pmod{32}$.
- 3 $a \equiv 8 \pmod{16}$, $b \equiv 7 \pmod{32}$ and ω is odd.
- 4 $a \equiv 8 \pmod{16}$, $b \equiv -9 \pmod{32}$ and $A_{a,b}^1 \equiv 0 \pmod{4}$.
- 5 $a \equiv 8 \pmod{16}$, $b \equiv -9 \pmod{32}$, $A_{a,b}^1 \equiv 2 \pmod{4}$ and $A_{a,b}^2 \equiv 0 \pmod{4}$.
- 6 $\omega \geq 6$ is even and $B_{a,b} \equiv 2 \pmod{4}$.
- 7 $\omega \geq 6$ is even and $B_{a,b} \equiv 0 \pmod{8}$.

When the polynomial $F(x)$ is not p -regular; certain factors of $F(x)$ provided by Hensel's factorization and refined by Residual Polynomial Theorem of first order; some residual polynomial $R_{\lambda_{ij}}(F)(y)$ is not irreducible in $\mathbb{Q}_p(x)$, then **Guàrdia, Montes, and Nart**, introduced in 2012 an efficient algorithm to factorize completely the principal ideal $p\mathbb{Z}_K$. They defined the Newton polygon of order r and they proved an extension of the theorem of the product, theorem of the polygon, theorem of the residual polynomial and theorem of index in order r .



J. Guàrdia, J. Montes and E. Nart, Newton polygons of higher order in algebraic number theory, *Tran. Math. Soc. American* **364(1)**, (2012), 361–416.

- To investigate some cases, we have analyzed Newton polygons of second order and we have used a key polynomial of a general form

$$x^2 - \rho x - \sigma \in \mathbb{Z}_p[x].$$

- To make ourselves in the regular case in **C3-C7**, we have replaced the factor $x - 1$ of $F(x)$ modulo 2 by $x - s$ where $s \in \mathbb{Z}_2$ has the form $s = 2^r - E(a, b)$ for an adequate r and $E(a, b) \in \mathbb{Z}_2$ with $\nu_2(s) = 0$. **This method (called refinement) was used previously by Guàrdia, Khanduja, Llorente, Montes, Nart, Vila, and others in different contexts...**

An upper bound of the index $i(K)$

Remark that $\nu_2(\mathbb{Z}_K : \mathbb{Z}[\alpha]) \leq \nu_2(i(K))$.

Case	Conditions	$\nu_2(\mathbb{Z}_K : \mathbb{Z}[\theta])$	$\nu_2(i(K))$
C1	$a \equiv 4 \pmod{8}$ and $b \equiv 3 \pmod{8}$	5	≤ 5
C2	$(a, b) \in \{(0, 31), (16, 15)\} \pmod{32}$	7	≤ 7
C3	$a \equiv 8 \pmod{16}$, $b \equiv 7 \pmod{32}$ and ω is odd	$\frac{\omega+9}{2}$	$\leq \frac{\omega+9}{2}$
C4	$a \equiv 8 \pmod{16}$, $b \equiv -9 \pmod{32}$, and $A_{a,b}^1 \equiv 0 \pmod{4}$	7	≤ 7
C5	$a \equiv 8 \pmod{16}$, $b \equiv -9 \pmod{32}$, $A_{a,b}^1 \equiv 2 \pmod{4}$ and $A_{a,b}^2 \equiv 0 \pmod{4}$	8	≤ 8
C6	$\omega = 2 + 2k$, $k \geq 2$ and $B_{a,b} \equiv 2 \pmod{4}$	$k + 6$	$\leq k + 6$
C7	$\omega = 2 + 2k$, $k \geq 2$ and $B_{a,b} \equiv 0 \pmod{8}$	$k + 7$	$\leq k + 7$

Table –

Remark :

- when $(a, b) \equiv (32, 16) \pmod{64}$ or $(a, b) \in \{(0, 112), (64, 112)\} \pmod{128}$, the problem is still open.
- All the sufficient and necessary conditions under which 2 will be a prime common index divisor of K depending only on a and b .

The index of the octic number field defined by $x^9 + ax + b$

Let $K = \mathbb{Q}(\alpha)$, $F(\alpha) = 0$ and $F(x) = x^9 + ax + b$.

Theorem 13 : Ben Yakkou and Teibekabe, 2023

p divides $i(K) \implies p \in \{2, 3\}$.

Theorem 14 : Ben Yakkou and Teibekabe, 2023

2 divides $i(K)$ if and only if one of the following conditions hold :

- 1 $a \equiv 1 \pmod{4}$ and $b \equiv 2 \pmod{4}$.
- 2 $a \equiv 3 \pmod{8}$ and $b \equiv 4 \pmod{8}$.
- 3 $(a, b) \in \{(15, 0), (31, 16)\} \pmod{32}$.
- 4 $(a, b) \in \{(15, 16), (31, 0)\} \pmod{32}$.
- 5 $a \equiv 7 \pmod{16}$ and $b \equiv 8 \pmod{16}$.

Example : Let $F(x) = x^9 + 289x + 34$. The polynomial $F(x)$ irreducible over \mathbb{Q} as it is a 3-Eisenstein polynomial. By Case Theorem 14 (Ben Yakkou and Teibekabe), 2 divides $i(K)$. So, K is not monogenic.

The index of the octic number field defined by $x^9 + ax + b$

Theorem 15 : Ben Yakkou and Teibekabe, 2023

Let $\nu = \nu_3(1 + a + b)$, $\mu = \nu_3(9 + a)$ and $\omega = \nu_3(-1 - a + b)$. Then **3 divides $i(K)$** if and only if one of the following conditions hold :

- 1 $(a, b) \in \{(72, 170), (234, 8), (234, 73)\} \pmod{243}$.
- 2 $a \equiv 153 \pmod{143}$, $b \equiv 89 \pmod{243}$ $2\mu < \nu + 2$.
- 3 $a \equiv 153 \pmod{243}$, $b \equiv 89 \pmod{243}$, $2\mu > \nu + 2$, ν is even, and $(1 + a + b)_3 \equiv -1 \pmod{3}$.
- 4 $a \equiv 234 \pmod{243}$, $b \equiv 235 \pmod{243}$ and $2\mu < \omega + 2$.
- 5 $a \equiv 234 \pmod{243}$, $b \equiv 235 \pmod{243}$, $2\mu > \omega + 2$, ω is even, and $(-1 - a + b)_3 \equiv 1 \pmod{3}$.

Example : Let $p \geq 5$ be a rational prime and $F(x) = x^9 + p^k x + p$, where k is a positive integer. Since $F(x)$ is an Eisenstein polynomial with respect p , it is irreducible over the field of rationals. By Theorems 13, 15, and 15 (Ben Yakkou and Teibekabe), the index of K is trivial ; $i(K) = 1$.

Non-monogenic number fields defined by $x^n + ax^m + b$

Let $K = \mathbb{Q}(\alpha)$, $F(\alpha)$, with $F(x) = x^n + ax^m + b$.

For two positive rational integers d and s , we shall denote by $N_p(d, s, t)$ the number of monic irreducible factors of degree d of the polynomial $x^s + \bar{t}$ in $\mathbb{F}_p[x]$, and $N_p(d, s, t)[m, c]$ the number of monic irreducible factors of degree d of $x^s + \bar{t}$ in $\mathbb{F}_p[x]$ which do not divide $x^m + \bar{c}$.

Theorem 16 : Ben Yakkou, 2023 (to appear in Rocky. J. Math)

Let p be an odd rational prime such that $p \mid a$, $p \nmid b$, and $p \mid n$. Set $n = s \cdot p^f$ with $p \nmid s$. Let $\mu = \nu_p(a)$ and $\nu = \nu_p(b^{p-1} - 1)$. If for some positive integer d , one of the following conditions holds :

- 1 $\mu < \min\{\nu, r + 1\}$ and $N_p(d) < \mu N_p(d, s, b)$,
- 2 $\nu < \min\{\mu, r + 1\}$ and $N_p(d) < \nu N_p(d, s, b)$,
- 3 $\mu = \nu \leq r$ and $N_p(d) < \mu N_p(d, s, b)[m, \frac{b+(-b)^{p^f}}{a}]$,
- 4 $r + 1 \leq \min\{\nu, \mu\}$ and $N_p(d) < (r + 1)N_p(d, s, b)$,

then p is a common index divisor of K . In particular, if one of these conditions holds, then K is not monogenic.

Corollary

For $F(x) = x^{2^k \cdot 3^r} + ax^m + b$. If one of the following conditions holds :

- 1 $k \geq 1, r \geq 2, a \equiv 9, 18 \pmod{27}$, and $b \equiv -1 \pmod{27}$,
- 2 $k \geq 1, r \geq 3, a \equiv 27, 54 \pmod{81}$, and $b \equiv -1 \pmod{81}$,
- 3 $k \geq 1, r \geq 2, a \equiv 0 \pmod{27}$, and $b \equiv 8, 17 \pmod{27}$,
- 4 $k \geq 1, r \geq 3, a \equiv 0 \pmod{81}$, and $b \equiv 26, 53 \pmod{81}$,
- 5 $k \geq 1, r = 1, a \equiv 0 \pmod{9}$, and $b \equiv -1 \pmod{9}$,
- 6 $k \geq 1, r = 2, a \equiv 0 \pmod{27}$, and $b \equiv -1 \pmod{27}$,
- 7 $k = 1, r \geq 7, a \equiv 3^7, 2 \cdot 3^7 \pmod{3^8}$, and $b \equiv 1 \pmod{3^8}$,
- 8 $k = 1, r \geq 7, a \equiv 0 \pmod{3^8}$, and $b \equiv 1 + 3^7, 1 + 2 \cdot 3^7 \pmod{3^8}$,
- 9 $k = 1, r = 6, a \equiv 0 \pmod{3^7}$, and $b \equiv 1 \pmod{3^7}$,
- 10 $k = 2, r \geq 4, a \equiv 81, 162 \pmod{243}$, and $b \equiv 1 \pmod{243}$,
- 11 $k = 2, r \geq 4, a \equiv 0 \pmod{243}$, and $b \equiv 82, 163 \pmod{3^5}$,
- 12 $k = 2, r = 3, a \equiv 0 \pmod{81}$, and $b \equiv 1 \pmod{81}$,

then 3 is a common index divisor of K . In particular, if one of these conditions holds, then K is not monogenic.

Theorem 17 : Ben Yakkou, 2023 (to appear in Rocky. J. Math)

Let p be an odd rational prime such that $p \nmid a$, $p \mid b$, and $p \mid n - m$. Set $n - m = u \cdot p^k$ with $p \nmid u$. Let $\delta = \nu_p(b)$ and $\kappa = \nu_p(a^{p-1} - 1)$. If for some positive integer d , one of the following conditions holds :

- 1 $\delta < \min\{\kappa, k + 1\}$ and $N_p(d) < \delta N_p(d, u, a)$,
- 2 $\kappa < \min\{\delta, k + 1\}$ and $N_p(d) < \kappa N_p(d, u, a)$,
- 3 $\kappa = \delta \leq k$ and $N_p(d) < \kappa N_p(d, s, b)[m, \frac{b}{a+(-a)^{p^k}}]$,
- 4 $k + 1 \leq \min\{\kappa, \delta\}$ and $N_p(d) < (k + 1)N_p(d, u, a)$,

then p is a common index divisor of K . In particular, if one of these conditions holds, then K is not monogenic.

Corollary

For $F(x) = x^{(s+1)\cdot 2^r\cdot 3^k} + ax^{s\cdot 2^r\cdot 3^k} + b$ with s is a positive rational integer. If one of the following conditions holds :

- 1 $r = 0, k \geq 5, a \equiv \pm 1 \pmod{243},$ and $b \equiv 81, 162 \pmod{243},$
- 2 $r = 0, k \geq 5, a \equiv 80, 82, 161, 163 \pmod{243},$ and $b \equiv 0 \pmod{243},$
- 3 $r = 0, k = 3, a \equiv \pm 1 \pmod{81},$ and $b \equiv 0 \pmod{81},$
- 4 $r \geq 1, k \geq 2, a \equiv -1 \pmod{27},$ and $b \equiv 9, 18 \pmod{27},$
- 5 $r \geq 1, k \geq 2, a \equiv 8, 17 \pmod{27},$ and $b \equiv 0 \pmod{27},$
- 6 $r \geq 1, k = 1, a \equiv -1 \pmod{9},$ and $b \equiv 0 \pmod{9},$
- 7 $r = 1, k \geq 7, a \equiv 1 \pmod{3^8},$ and $b \equiv 3^7, 2 \cdot 3^7 \pmod{3^8},$
- 8 $r = 1, k \geq 7, a \equiv 1 + 3^7, 1 + 2 \cdot 3^7 \pmod{3^8},$ and $b \equiv 0 \pmod{3^8},$
- 9 $r = 1, k = 6, a \equiv 1 \pmod{3^7},$ and $b \equiv 0 \pmod{3^7},$
- 10 $r = 2, k \geq 5, a \equiv 1 \pmod{243},$ and $b \equiv 81, 162 \pmod{243},$
- 11 $r = 2, k \geq 5, a \equiv 82, 163 \pmod{243},$ and $b \equiv 0 \pmod{243},$
- 12 $r = 2, k = 3, a \equiv 1 \pmod{243},$ and $b \equiv 0 \pmod{243},$

then 3 is a common index divisor of K . In particular, if one of these conditions holds, then K is not monogenic.

Theorem 18 : Ben Yakkou, 2023 (to appear in Rocky. J. Math)

Under the hypotheses of Theorem 17, if $\gcd\{\delta, m\} = 1$, and one of the following conditions holds :

- 1 $\delta < \min\{\kappa, k + 1\}$ and $p < 1 + \delta N_p(1, u, a)$,
- 2 $\kappa < \min\{\delta, k + 1\}$ and $p < 1 + \kappa N_p(1, u, a)$,
- 3 $\kappa = \delta \leq k$ and $p < 1 + \kappa N_p(1, s, b)[m, \frac{b}{a+(-a)^{p^k}}]$,
- 4 $k + 1 \leq \min\{\kappa, \delta\}$ and $p < 1 + (k + 1)N_p(1, u, a)$,

then p is a common index divisor of K . In particular, if one of these conditions holds, then K is not monogenic.

Theorem 19 : Ben Yakkou, 2022

Let $F(x) = x^{2^r} + ax^m + b$ be a monic irreducible trinomial and $K = \mathbb{Q}(\alpha)$ a number field generated by α , a root of $F(x)$. If $r \geq 3$ and a and $b + 1$ are both divisible by 32, then **2 is a prime common index divisor** of K . In particular, K is not monogenic.

Theorem 20 : Ben Yakkou, 2022

Let $K = \mathbb{Q}(\theta)$ be a number field with θ root of a monic irreducible trinomial $F(x) = x^{2^r} + ax + b \in \mathbb{Z}[x]$. If one of the following conditions holds

- 1 $r \geq 3$, $a \equiv 4 \pmod{8}$ and $b \equiv 3 \pmod{8}$.
- 2 $r \geq 4$, $a \equiv 8 \pmod{16}$ and $b \equiv 7 \pmod{16}$.
- 3 $r \geq 3$ and $(a, b) \in \{(0, 31), (16, 15)\} \pmod{32}$,

then **2 is a prime common index divisor** of K . In particular, if one of these conditions holds, then K is not monogenic.

Theorem 21 : Ben Yakkou, 2022

Let $F(x) = x^n + ax^m + b \in \mathbb{Z}[x]$ be a monic polynomial with discriminant D . Suppose that there exist a rational prime p dividing both a and b such that $\nu_p(b) \geq 2$, $\gcd(n, \nu_p(b)) = 1$, $n\nu_p(a) > (n - m)\nu_p(b)$, and D_p is square free. Then $F(x)$ is irreducible over \mathbb{Q} . Let $K = \mathbb{Q}(\alpha)$ be a number field with α a root of $F(x)$. Then $F(x)$ is not monogenic ($\mathbb{Z}_K \neq \mathbb{Z}[\alpha]$), but K is monogenic. Moreover, in this case, $\mathbb{Z}_K = \mathbb{Z}[\theta]$, with $\theta = \frac{\alpha^s}{p^t}$, where $(s, t) \in \mathbb{N}^2$ is the unique positive solution of the Diophantine equation $\nu_p(b)s - nt = 1$ with $0 \leq s < n$.

Example : The polynomial $F(x) = x^8 + 8x + 8 \in \mathbb{Z}[x]$ has discriminant $D = 2^{24} \times 1273609$. Then $F(x)$ satisfies the conditions of Theorem 21 for $p = 2$. Hence, it is irreducible over \mathbb{Q} . Let $K = \mathbb{Q}(\alpha)$ with α is a root of $F(x)$. Then $\mathbb{Z}_K \neq \mathbb{Z}[\alpha]$. But, K is monogenic and $\theta = \frac{\alpha^3}{2}$ generates a power integral basis of \mathbb{Z}_K .

- 1 Introduction, Notations
- 2 Some previous explicit works
- 3 Prime ideal factorization via Newton polygon techniques
- 4 Monogeneity of certain pure number fields
- 5 Monogeneity and indices of certain number fields defined by trinomials
- 6 Thanks**

- Thanks to the organizers of Number Theory Seminar of University of Debrecen for inviting me to talk on the monogeneity of number fields. I Thank them for the nice welcome.
- I am deeply grateful to Professor Kálmán Győry for his wise guidance, precious remarks, valuable comments, suggestions, and helpful discussions. I thank him for his continuous encouragements.

THANK YOU FOR YOUR
ATTENTION