Monogenity of number fields

Laszlo Remete
University of Debrecen

Number Theory Seminar
Prague, online
12.04.2023

Let K be an algebraic number field of degree n with ring of integers $\mathcal{O}_K$.

K is called **monogenic** if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. In this case $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ is an integral basis of K called **power integral basis**.

The index of a primitive algebraic integer α is

$$I(\alpha) = \left| \mathcal{O}_K : \mathbb{Z}[\alpha] \right|$$

K is monogenic $\Leftrightarrow I(\alpha) = 1$ for some $\alpha \in \mathcal{O}_K$.

Some advanteges of the monogenity

B. Kovács: Canonical number systems

There exists canonical number system in K if and only if K is monogenic. I.e. any $\beta \in \mathcal{O}_K$ can be uniquely represented as

$$\beta = a_0 + a_1\alpha + a_2\alpha^2 \ldots + a_r\alpha^r, \qquad a_i \in \{0, 1, 2 \ldots, |N(\alpha)| - 1\}$$

if and only if $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ is an integral basis of K.

Kummer-Dedekind theorem: Factorization of primes

Let $K = \mathbb{Q}(\alpha)$ and let $f(X)$ be the minimal polynomial of α in $\mathbb{Z}[X]$. If p does not divide the index of α, then

$$(p) = (p, \varphi_1(\alpha))^{e_1} \cdot \ldots \cdot (p, \varphi_g(\alpha))^{e_g},$$

where

$$f(X) \equiv \varphi_1(X)^{e_1} \cdot \ldots \cdot \varphi_g(X)^{e_g} \pmod p$$

is the factorization of $f(X)$ modulo p into powers of distinct monic irreducibles.

Investigation of monogenity after Dedekind

Index of the field K:

$$i(K) := \gcd\{I(\alpha) \mid K = \mathbb{Q}(\alpha), \alpha \in \mathcal{O}_K\}$$

If $p \mid i(K)$, then p divides the index of any primitive algebraic integer in K, i.e. K is not monogenic.

Dedekind

Let p be a rational prime, and let

$$(p) = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g}$$

be the factorization of (p) into prime ideals in $\mathcal{O}_K$. Then p does not divide $i(K)$ if and only if there exist distinct monic irreducible polynomials $V_1, V_2, \ldots, V_g$ over $\mathbb{F}_p$, satisfying $\deg V_i = \deg \mathfrak{p}_i$.

$i(K) > 1 \Rightarrow K$ is not monogenic. The conversion is not true, there are non-monogenic number fields K with $i(K) = 1$.

First non-monogenic example

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

$$f(X) = X^3 - X^2 - 2X - 8.$$

The factorization of $2 \cdot \mathcal{O}_K$ is

$$(2) = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3.$$

The inertia degrees of each $\mathfrak{p}_i$ is one, but there exist only two monic irreducible polynomial over $\mathbb{F}_2$ of degree one: X and $X + 1$.
The index of the field K is even, so the index of any algebraic integer is divisible by 2. The field is not monogenic.

Factorization of primes after Ore

Let $\varphi_i(X) \in \mathbb{Z}[X]$ be monic lifts of the irreducible factors of $f(X)$ modulo p:

$$f(X) \equiv \varphi_1(X)^{e_1} \cdot \ldots \cdot \varphi_g(X)^{e_g} \pmod{p}.$$

The φ_i-expansion of $f(X) \in \mathbb{Z}[X]$:

$$f(X) = a_0(X) + a_1(X) \cdot \varphi_i(X) + \ldots + a_r(X) \cdot \varphi_i(X)^r,$$

where $\deg(a_j) < \deg(\varphi_i)$.
For any polynomial $g(X) = b_n X^n + \ldots + b_1 X + b_0 \in \mathbb{Q}_p[X]$, let

$$\nu_p(g(X)) := \min\{\nu_p(b_i) \mid i = 0, \ldots, n\}$$

be the extension of the discrete valuation ν_p to $\mathbb{Q}_p[X]$.
The φ_i-Newton polygon of $f(X)$ is the lower convex hull of the points

$$\Big\{ \Big(j, \nu_p\big(a_j(X)\big) \Big) \mid j = 0, \ldots, r \Big\}$$

The sides of this polygon of negative slopes produce the principal φ_i-Newton polygon $N^{-}_{\varphi_i}(f)$.

The sides of the principal φ_i-Newton polgons provides us some factors of the principal ideal (p) in $K = \mathbb{Q}(\alpha)$, where α is a root of $f(X)$.

Regularity: To any side S of the principal φ_i-Newton polygons, we attach a polynomial called residual polynomial. If a residual polynomial is separable/square-free, then the factor of (p) corresponding to this side is a prime ideal.

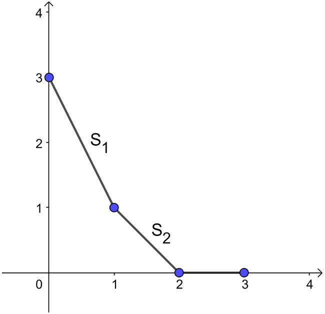
If all of the residual polynomials are separabe, then the polynomial f is called p-regular. In this case the sides of the principal Newton polgons provide the shape of the prime ideal decomposition of (p).

Ore

Any number field K can be generated by a root of a p-regular polynomial, i.e. one can always find a polynomial which completely determines the prime ideal decomposition of (p) in K.

Ore's method on Dedekind's example

$$f(X) = X^3 - X^2 - 2X - 8 \equiv X^2(X+1) = \varphi_1^2 \cdot \varphi_2 \pmod 2$$



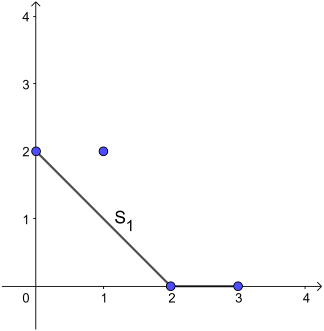
φ_1-Newton polygon of $f(X)$ $\qquad$ φ_2-Newton polygon of $f(X)$

The sides S_1, S_2 and S_3 are single sides (with no integer points on them except the endpoints), the residual polynomials attached to them are of degree one: $Y+1 \in \mathbb{F}_2[Y]$, so they are separable. We obtain:

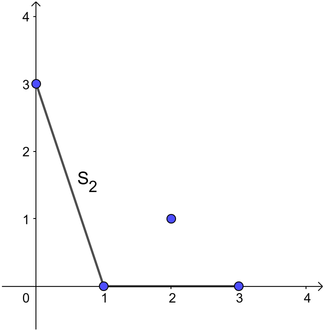
$$(2) = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3.$$

Non-regular example

$$f(X) = X^3 + X^2 - 4X + 4 \equiv X^2(X+1) = \varphi_1^2 \cdot \varphi_2 \pmod 2$$



φ_1-Newton polygon of $f(X)$



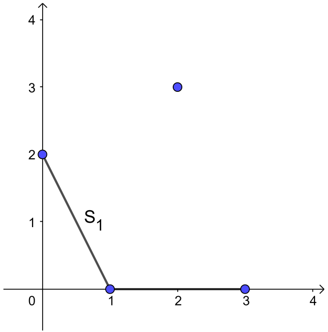
φ_2-Newton polygon of $f(X)$

$R_{S_1}(Y) = Y^2 + 1 = (Y+1)^2 \in \mathbb{F}_2[Y] \Rightarrow$ Not separable!
$R_{S_2}(Y) = Y + 1 \in \mathbb{F}_2[Y] \Rightarrow$ It is okay
We have 2 possibilities:

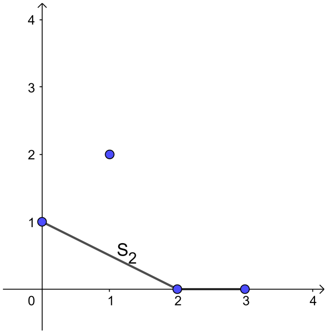
- $(2) = \mathfrak{p}_1 \cdot \mathfrak{p}_2$, where $\deg \mathfrak{p}_1 = 2$ and $\deg \mathfrak{p}_2 = 1$ or
- $(2) = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2$, where $\deg \mathfrak{p}_1 = \deg \mathfrak{p}_2 = 1$

If α is a root of $f(X) = X^3 + X^2 - 4X + 4$, then α and $(\alpha^2 + \alpha)/2$ generates the same number field, but the minimal polynomial of $(\alpha^2 + \alpha)/2$ is already regular:

$$g(X) = X^3 - 4X^2 + 5X - 4 \equiv X(X+1)^2 = \varphi_1 \cdot \varphi_2^2 \pmod 2.$$



φ_1-Newton polygon of $f(X)$



φ_2-Newton polygon of $f(X)$

All of the sides are of degree 1, so are the residual polynomials and the corresponding prime ideals:

$$(2) = \mathfrak{p}_1 \cdot \mathfrak{p}_2^2, \text{ where } \deg \mathfrak{p}_1 = \deg \mathfrak{p}_2 = 1$$

Non-monogenic number field with $i(K) = 1$

Let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(X) = X^3 - 175$.
An integral basis of K:

$$\left(1, \alpha, \frac{\alpha^2}{5}\right).$$

The index of α is $I(\alpha) = 5$.

Let $\gamma = \frac{\alpha^2}{5}$. It is a root of $X^3 - 245$, and $\mathbb{Q}(\alpha) = K = \mathbb{Q}(\gamma)$.
An integral basis of K:

$$\left(1, \gamma, \frac{\gamma^2}{7}\right).$$

The index of γ is $I(\gamma) = 7$.

The gcd of the indices is $i(K) = 1$. But it can be shown, that the field is not monogenic.

Cubic fields

Let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(X) = X^3 + a_1 X^2 + a_2 X + a_3$. Let $I(\alpha)$ be the index of α. Then the discriminant of K is

$$D_K = \frac{D(\alpha)}{I(\alpha)^2}.$$

Assume that

$$\beta = \frac{a + x \cdot \alpha + y \cdot \alpha^2}{d} \in \mathcal{O}_K$$

generates a power integral basis in K. Equivalently, the discriminant of the basis $(1, \beta, \beta^2)$ is equal to the discriminant of K.
Let $\beta = \beta^{(1)}, \beta^{(2)}, \beta^{(3)}$ be the conjugates of β. Discriminant of $(1, \beta, \beta^2)$ is

$$D(\beta) = \left(\beta^{(1)} - \beta^{(2)}\right)^2 \cdot \left(\beta^{(1)} - \beta^{(3)}\right)^2 \cdot \left(\beta^{(2)} - \beta^{(3)}\right)^2$$

$$D(\beta) = \frac{1}{d^6} \cdot \left(x\left(\alpha^{(1)} - \alpha^{(2)}\right) + y\left(\alpha^{(1)^2} - \alpha^{(2)^2}\right)\right)^2 \cdot$$
$$\left(x\left(\alpha^{(1)} - \alpha^{(3)}\right) + y\left(\alpha^{(1)^2} - \alpha^{(3)^2}\right)\right)^2 \cdot$$
$$\left(x\left(\alpha^{(2)} - \alpha^{(3)}\right) + y\left(\alpha^{(2)^2} - \alpha^{(3)^2}\right)\right)^2 =$$
$$= \frac{1}{d^6} \cdot \left(\alpha^{(1)} - \alpha^{(2)}\right)^2 \cdot \left(x + y\left(\alpha^{(1)} + \alpha^{(2)}\right)\right)^2 \cdot$$
$$\left(\alpha^{(1)} - \alpha^{(3)}\right)^2 \cdot \left(x + y\left(\alpha^{(1)} + \alpha^{(3)}\right)\right)^2 \cdot$$
$$\left(\alpha^{(2)} - \alpha^{(3)}\right)^2 \cdot \left(x + y\left(\alpha^{(2)} + \alpha^{(3)}\right)\right)^2 =$$
$$= \frac{D(\alpha)}{d^6} \cdot \left(x^3 - 2a_1x^2y + (a_1^2 + a_2)xy^2 - (a_1a_2 - a_3)y^3\right)^2$$

Thus $D(\beta) = \dfrac{D(\alpha)}{I(\alpha)^2}$, iff (x, y) is a solution of the index form equation

$$I(x, y) = x^3 - 2a_1x^2y + (a_1^2 + a_2)xy^2 - (a_1a_2 - a_3)y^3 = \pm\frac{d^3}{I(\alpha)}.$$

Index form in the previous example

Let again $K = \mathbb{Q}(\alpha)$, where α is a root of $f(X) = X^3 - 175$.

An integral basis of K: $\left(1, \alpha, \frac{\alpha^2}{5}\right)$. The index of α is $I(\alpha) = 5$.

Any algebraic integer can be written in the form

$$\beta = \frac{a + x\alpha + y\alpha^2}{5},$$

where $a, x, y \in \mathbb{Z}$, and a and x are multiples of 5.

The corresponding index form:

$$x^3 - 175y^3 = \pm\frac{5^3}{5}$$

Let $x = 5z$, then β generates a power integral basis, if and only if

$$5z^3 - 7y^3 = \pm 1.$$

This is not solvable modulo 7, so the field K is not monogenic.

Index form equations in general

We can do the same in number fields of any degree.
Let K be an algebraic number field of degree n with integral basis $(1, \omega_2, \ldots, \omega_n)$ and set

$$L^{(i)}(X_1, \ldots, X_n) = X_1 + X_2\omega_2^{(i)} + \ldots + X_n\omega_n^{(i)},$$

where $\gamma^{(i)}$ $(1 \le i \le n)$ are the conjugates of any $\gamma \in K$. Let D_K be the discriminant of K, and $D(L)$ be the discriminant of L:

$$D(L) = \begin{vmatrix} 1 & L^{(1)} & (L^{(1)})^2 & \ldots & (L^{(1)})^{n-1} \\ 1 & L^{(2)} & (L^{(2)})^2 & \ldots & (L^{(2)})^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & L^{(n)} & (L^{(n)})^2 & \ldots & (L^{(n)})^{n-1} \end{vmatrix}^2$$

Then there is a homogeneous polynomial $I(X_2, X_3, \ldots, X_n) \in \mathbb{Z}[X_2, \ldots, X_n]$, for which

$$D(L) = I(X_2, X_3, \ldots, X_n)^2 \cdot D_K.$$

Index and the index form

$$D(L) = I(X_2, X_3, \ldots, X_n)^2 \cdot D_K$$

Let $(x_1, x_2, x_3, \ldots, x_n) \in \mathbb{Z}^n$ and

$$\beta = x_1 + x_2\omega_2 + \ldots + x_n\omega_n \in \mathcal{O}_K.$$

The discriminant of β is equal to $D(L(x_2, x_3, \ldots, x_n))$ by definiton, and we also have

$$D(\beta) = I(\beta)^2 \cdot D_K$$

So the index of β is

$$I(\beta) = |I(x_2, x_3, \ldots, x_n)|.$$

Index form equation

β generates a power integral basis in K, if and only if the $n-1$-tuple $(x_2, x_3, \ldots, x_n)$ is a solution of the index form equation

$$I(X_2, X_3, \ldots, X_n) = \pm 1.$$

Solutions of the index form equations

The index form is a homogeneous polynomial of degree $n(n-1)/2$ and with $n-1$ variables.
Large $n \Rightarrow$ extremely complicated.

Győry

Effective upper bound for the solutions of the index form equations $\Rightarrow$ there are finitely many solutions.

Equivalence: $I(\beta) = I(x_1 \pm \beta)$, where $x_1 \in \mathbb{Z}$. Up to this equivalence, there are only finitely many $\beta \in \mathcal{O}_K$ with index 1.

- Method uses Baker's results on the linear forms in the logarithms of algebraic numbers, i.e. the bounds are huge.
- Not applicable in case of infinite parametric families of number fields.

Bilu, Gaál, Győry, Pethő, Pohst, etc.: Fast algoritmic solution in cases of degrees 3,4,5 and 6, also in some relative extensions.
See I.Gaál, *Diophantine Equations and Power Integral Bases* (2019).

Change of basis

Let $(1, \omega_2, \dots, \omega_n)$ be an integral basis of $K = \mathbb{Q}(\alpha)$, $\alpha \in \mathcal{O}_K$. Assume that M is the trasition matrix $(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) \mapsto (1, \omega_2, \dots, \omega_n)$, i.e

$$I(\alpha) = \det(M^{-1}) \text{ and } \det(M)^2 \cdot D(\alpha) = D_K.$$

Then

$$\begin{aligned} L^{(i)}(X_1, X_2, \dots, X_n) = & \quad (X_1, X_2, \dots, X_n) \cdot (1, \omega_2^{(i)}, \dots, \omega_n^{(i)})^T = \\ = & \quad (X_1, X_2, \dots, X_n) \cdot M \cdot (1, \alpha^{(i)}, \dots, {\alpha^{(i)}}^{n-1})^T \end{aligned}$$

So with $(Y_1, Y_2, \dots, Y_n) = (X_1, X_2, \dots, X_n) \cdot M$, we can write

$$D(L) = I(X_2, X_3, \dots, X_n)^2 \cdot D_K = I(Y_2, Y_3, \dots, Y_n)^2 \cdot D(\alpha),$$

where $I(Y_2, Y_3, \dots, Y_n)$ is a homogeneous polynomial with rational coefficients:

$$I(X_2, X_3, \dots, X_n)^2 \cdot \det(M)^2 = I(Y_2, Y_3, \dots, Y_n)^2$$

Non 2-transitive case

$$D(L) = I(X_2, X_3, \ldots, X_n)^2 \cdot D_K = I(Y_2, Y_3, \ldots, Y_n)^2 \cdot D(\alpha)$$

$$\prod_{1 \le i < j \le n} \left(L^{(i)} - L^{(j)}\right)^2 = I(Y_2, Y_3, \ldots, Y_n)^2 \cdot \prod_{1 \le i < j \le n} \left(\alpha^{(i)} - \alpha^{(j)}\right)^2$$

If the galois group of the normal closure of K is not 2-transitive, then the index form

$$I(X_2, X_3, \ldots, X_n) = \pm \frac{I(Y_2, Y_3, \ldots, Y_n)}{I(\alpha)} = \pm \frac{1}{I(\alpha)} \cdot \prod_{1 \le i < j \le n} \left(\frac{L^{(i)} - L^{(j)}}{\alpha^{(i)} - \alpha^{(j)}} \right)$$

is reducible over $\mathbb{Q}$. But $I(\underline{X}) \in \mathbb{Z}[\underline{X}]$, so it is reducible over $\mathbb{Z}$ too:

$$I(\underline{X}) = F_1(\underline{X}) \cdot F_2(\underline{X}) \cdot \ldots \cdot F_k(\underline{X}) \in \mathbb{Z}[\underline{X}]$$

Then $I(\underline{X}) = \pm 1$ if and only if $F_i(\underline{X}) = \pm 1$, $(1 \le i \le k)$.

Application of the factorization of the index form

Let $K_t = \mathbb{Q}(\alpha_t)$, where α_t is a root of $X^6 - 36t - 26$, with $t \in \mathbb{Z}$ such that $36t + 26$ is square-free. It can be shown that

$$\left(1, \alpha_t, \alpha_t^2, \alpha_t^3, \frac{1 + 2\alpha_t^2 + \alpha_t^4}{3}, \frac{\alpha_t + 2\alpha_t^3 + \alpha_t^5}{3}\right),$$

is an integral basis of K_t and $i(K_t) = 1$. The galois group of $X^6 - 36t - 26$ is isomorphic to the dihedral group D_6, which is not 2-transitive. Its natural action on the set of pairs of integers

$$\{(i,j) \mid i < j;\ i,j \in \{1,2,3,4,5,6\}\}$$

has 3 orbits. For example, if $\alpha_t = \sqrt[6]{36t+26}$, ε_6 is a primitive sixth root of unity and $\alpha_t^{(i)} = \varepsilon_6^{i-1} \cdot \alpha_t$, then the 3 orbits:

$$\{(1,4),(2,5),(3,6)\},$$

$$\{(1,3),(2,4),(3,5),(4,6),(1,5),(2,6)\},$$

$$\{(1,2),(2,3),(3,4),(4,5),(5,6),(1,6)\},$$

thus the index form has 3 factors of degrees $3, 6, 6$ respectively:

$$I(\underline{X}) = F_1(\underline{X}) \cdot F_2(\underline{X}) \cdot F_3(\underline{X}).$$

Non-monogenity of an infinite family with field index 1

Explicit calculations show that

$$\frac{9F_3(\underline{X}) - F_2(\underline{X})}{4(36t+26)}$$

is an integer polynomial. If K_t is monogenic, then there is a quintuple $\underline{x} = (x_2, x_3, x_4, x_5, x_6) \in \mathbb{Z}^5$, for which

$$F_2(x_2, x_3, x_4, x_5, x_6) = \pm 1, \qquad F_3(x_2, x_3, x_4, x_5, x_6) = \pm 1,$$

so if K_t is monogenic, then

$$4(36t+26) \mid 9F_3(\underline{x}) - F_2(\underline{x}) = \pm 8, \pm 10$$

There is no $t \in \mathbb{Z}$ for which this can be true, so K_t is not monogenic.

Monogenity of pure sextic fields

Let $K_m = \mathbb{Q}(\alpha_m)$, where $m \in \mathbb{Z}$ is square-free and α_m is a root of $x^6 - m$. Then K_m is monogenic if and only if

$$m \pmod 4 \in \{2,3\} \text{ and } m \pmod 9 \in \{2,3,4,5,6,7\}.$$