$\mathbb{Z}$-BASIS FOR THE ORDERS GENERATED BY THE CONJUGATES OF AN ALGEBRAIC INTEGER

Stéphane Louboutin
Aix-Marseille Université (Marseille, France)

Let

$$D_\alpha$$

$:=\prod_{1\leq i<j\leq n}(\alpha_j-\alpha_i)^2$
$\in \mathbb{Z}\setminus\{0\}$
be the discriminant
of the minimal polynomial

$$\Pi_\alpha(X)=X^n-a_{n-1}X^{n-1}43;\cdots 43;(-1)^n a_0\in\mathbb{Z}[X]$$

of an algebraic integer α of degree n,
where
$\alpha_1,\cdots,\alpha_n$
are the complex conjugate of α,
i.e. are the n distinct complex roots of $\Pi_\alpha(X)$.

Set $d_\alpha=|D_\alpha|$.

We consider

$$\mathbb{M}_\alpha=\mathbb{Z}[\alpha_1,\cdots,\alpha_n],$$

and order of

$$\mathbb{L}_\alpha=\mathbb{Q}(\alpha_1,\cdots,\alpha_n)$$

be the normal closure of $\mathbb{Q}(\alpha)$.

It is a free $\mathbb{Z}$-module of rank

$$r=(\mathbb{L}_\alpha:\mathbb{Q})\geq(\mathbb{Q}(\alpha):\mathbb{Q})=n.$$

If $\mathbb{M}$ is an order of a number field,
let $D_{\mathbb{M}}\in\mathbb{Z}$ denote its discriminant.

Notice that $D_{\mathbb{Z}[\alpha]} = D_\alpha$.

The goal is to determine a $\mathbb{Z}$-basis for $\mathbb{M}_\alpha$

and the discriminant $D_{\mathbb{M}_\alpha}$

of $\mathbb{M}_\alpha$ and to give various applications of these determinations.

Let us explain how one usually constructs parametrized families of number fields

of known discriminants and regulators.

One usually starts from explicit parametrized families of monic polynomials with integral coefficients

and constant coefficient equal to ± 1,

so that their complex roots are algebraic units.

Let us for example consider the simplest cubic fields $\mathbb{Q}(\alpha)$,

where $\Pi_\alpha(X) = X^3 - aX^2 43;(a-3)X 43;1$, $a \geq 2$.

Since $D_\alpha = (a^2 - 3a 43;9)^2$ is a square,

$\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois cyclic cubic extension

and since

$\Pi_\alpha(X) = (X-\alpha)\ (X-(-\alpha^2 43;(a-1)\alpha 43;2))(X-(\alpha^2 - a\alpha 43;a-2))$,

the order $\mathbb{Z}[\alpha]$ is Galois invariant.

Moreover, the three conjugates α, α' and α'' of α are algebraic units.

Since $\mathbb{Q}(\alpha)/\mathbb{Q}$ is of prime degree,

any 2 of these conjugates are multiplicatively independent in the group of units

$\mathbb{Z}[\alpha]^\times$ of the order $\mathbb{Z}[\alpha]$.

In fact, for the simplest cubic fields we have

$\mathbb{Z}[\alpha]^\times = \langle -1, \alpha, \alpha' \rangle$.

Hence, in the cases that $\mathbb{Z}[\alpha]$ is equal to the ring of algebraic integers

$\mathbb{Z}_\mathbb{K}$ of the number field $\mathbb{K}$,

we end up with cyclic cubic fields of known discriminants and regulators.

Now, since

$D_\alpha = (\mathbb{Z}_\mathbb{K} : \mathbb{Z}[\alpha])^2 d_\mathbb{K}$

and $d_\mathbb{K} > 1$,

it follows that if $a^2 - 3a 43;9 = p$ is prime then $\mathbb{Z}_\mathbb{K} = \mathbb{Z}[\alpha]$.

Since the class number of $\mathbb{K}$ divides the class number $h_p^{43;}$

of the real cyclotomic field $\mathbb{Q}(\zeta_p)^{43;}$,

we easily end up with with examples of prime numbers $p > 3$ for which $h_p^{43;>1}$

(see [**?**]).

However, still assuming that α is an algebraic unit

such that $\mathbb{Q}(\alpha)/\mathbb{Q}$ Galois cyclic of prime degree $p \geq 3$,

the order $\mathbb{Z}[\alpha]$ is not generally Galois invariant.

For example, for given bound B we computed the number $N(B)$ of $\mathbb{Q}$-irreducible

cubic polynomials $\Pi(X) = X^3 - aX^243; bX - c \in \mathbb{Z}[X]$

with $0 \leq a, |b|, |c| \leq B$ and whose discriminants are squares in $\mathbb{Z}$.

Let α denote any root of $\Pi(X)$ and $\alpha_1, \alpha_2, \alpha_3$ denote its three real roots.

We computed the number $N(\alpha)$ of these polynomials for which

$\mathbb{Z}[\alpha] = \mathbb{Z}_{\mathbb{Q}(\alpha)}$,

i.e. for which $D_\alpha = D_\mathbb{K}$,

the number $N_{inv}(\alpha)$ of these polynomials for which the order $\mathbb{Z}[\alpha]$ is Galois invariant, i.e. for which D divides $3b-a^2$ and $3ac-b^2$ (Corollary **??**),

and the number $N(\alpha_1, \alpha_2, \alpha_3)$ of these polynomials for which

$\mathbb{Z}[\alpha_1, \alpha_2, \alpha_3] = \mathbb{Z}_{\mathbb{Q}(\alpha)}$,

i.e. for which $\Delta^2 = D_\mathbb{K}$ (Theorem **??**).

Table

B	$N(B)$	$N(\alpha)$	$N_{inv}(\alpha)$	$N(\alpha_1, \alpha_2, \alpha_3)$
10	62	30 (48.4%)	36 (58.1%)	44 (71.0%)
20	190	64 (33.7%)	77 (40.5%)	137 (72.1%)
30	387	97 (25.1%)	116 (30.0%)	280 (72.4%)
40	613	136 (22.2%)	161 (26.3%)	431 (70.3%)
50	853	168 (19.7%)	202 (23.7%)	592 (69.4%)
100	2506	351 (14.0%)	414 (16.5%)	1686 (67.3%)
200	7125	713 (10.0%)	840 (11.8%)	4663 (65.4%)
300	12762	1071 (8.4%)	1261 (9.9%)	8263 (64.7%)
500	26349	1794 (6.8%)	2117 (8.0%)	16991 (64.5%)
1000	69696	3603 (5.2%)	4266 (6.1%)	44005 (63.1%)

(1)

However, the order $\mathbb{M}_\alpha$ is always Galois invariant.

Hence it would be much more satisfactory to have families of parametrized polynomials

for which $D_{\mathbb{M}_\alpha}$ would be known

and for which any $p-1$ of the p conjugates of α

would form a system of fundamental units of the order $\mathbb{M}_\alpha$.

In this respect we proved:

theorem

(See [**?**, Theorem 1.2]).

Let ε, ε' and ε'' be the three real roots

of any one of the following parametrized families of $\mathbb{Q}$-irreducible cubic polynomials

of discriminants a square:

$$X^3-n(n^2 43;n43;3)(n^2 43;2)X^2-(n^3 43;2n^2 43;3n43;3)X-1 \quad (n\in\mathbb{Z}),$$

$$X^3$$

-(n$^3-2n^2 43;3n-3)X^2$

-n^2X

-1 (1, $2\neq n\in\mathbb{Z}$),

$$X^3$$

$43;$(n$^8 43;2n^6-3n^5 43;3n^4-4n^3 43;5n^2-3n43;3)X^2$

-(n$^3-2)n^2X$

-1 (n$\in\mathbb{Z}$).

Then, $\{1,\varepsilon,\varepsilon^2\varepsilon'\}$ is a $\mathbb{Z}$-basis

of the totally real cubic order $\mathbb{Z}[\varepsilon,\varepsilon']$

and $\{\varepsilon,\varepsilon'\}$ is a system of fundamental units

of this cubic order $\mathbb{Z}[\varepsilon,\varepsilon']$.

Indeed, in these three cases $3ac-b^2$ divides D_α and $3b-a^2$.

Hence the results on the $\mathbb{Z}$-basis follow from Theorem **??**.