Algebraic number theory

Marine Rougnant

Université Marie & Louis Pasteur (Besançon, France)

Algebraic Days of Gabon
École Normale Supérieure (ENS), Libreville, Gabon
10/03/25 – 14/03/25

We are interested in number fields $K = \mathbb{Q}[x]/(P) = \mathbb{Q}(\alpha)$ up to isomorphism. Given a monic irreducible polynomial $P \in \mathbb{Z}[x]$, the initialisation function `nfinit` determines invariants of K.

```
? f = x^4 - 2*x^3 + x^2 - 5;
? K = nfinit(f);
```

K contains the structure for the number field $K = Q[x]/f(x)$.
The function `polredabs` returns a canonical defining polynomial for K (this is the one given in the LMFDB for instance), `polredbest` gives a simpler defining polynomial for K (faster).

```
? #nfisisom(nfinit(P), nfinit(polredbest(P)))
% = 1
```

The `nfinit` structure contains many informations :

```
? K.pol \\ defining polynomial
% = x^4 - 2*x^3 + x^2 - 5
? K.sign \\ signature
% = [2, 1]
```

K has signature (2, 1) : it has two real embeddings and one pair of conjugate complex embeddings.

```
? K.r1 \\ number of real embeddings
% = x^4 - 2*x^3 + x^2 - 5
? K.r2 \\ number of complex embeddings
% = [2, 1]
```

```
? K.disc \\ discriminant
% = -1975
? K.p \\ primes ramified in K (div. of K.disc)
% [5, 79]
```

The field K is ramified at 5 and 79.

```
? w = K.zk[2];
? K.zk
% = [1, 1/2*x^2 - 1/2*x - 1/2, x, 1/2*x^3 - 1/2*x^2 - 1/2*x]
```

L'anneau des entiers de K est

$$\begin{aligned} \mathbb{Z}_K &= \mathbb{Z} + \frac{\alpha^2 - \alpha - 1}{2}\mathbb{Z} + \alpha\mathbb{Z} + \frac{\alpha^3 - \alpha^2 - x}{2}\mathbb{Z} \\ &= \mathbb{Z} + \mathbb{Z}\omega + \mathbb{Z}\alpha + \mathbb{Z}\omega\alpha \end{aligned}$$

Element of $K = \mathbb{Q}(\alpha)$ can be reprensented as polynomials in α. We can also use linear combinations of the integral basis. We can switch between the two representations with `nfalgtobasis` and `nfbasistoalg`.

```
? nfalgtobasis(K,x^2)
% = [1, 2, 1, 0]~
```

$$\alpha^2 = 1 \cdot 1 + 2 \cdot \omega + 1 \cdot \alpha + 0 \cdot \omega\alpha = 1 + 2\omega + \alpha.$$

```
? nfbasistoalg(K,[1,1,1,1]~)
% = Mod(1/2*x^3 + 1/2, x^4 - 2*x^3 + x^2 - 5)
```

$$1 + \omega + \alpha + \omega\alpha = \frac{\alpha^3 + 1}{2}$$

We perform operations on elements with the functions `nfeltxxxx`, which accept both representations as input.

```
? nfeltmul(K,[1,-1,0,0]~,x^2)
% = [-1, 3, 1, -1]~
```

$(1-\omega)\cdot\alpha^2 = -1 + 3\omega + \alpha - \omega\alpha.$

```
? nfeltnorm(K,x-2)
% = -1
? nfelttrace(K,[0,1,2,0]~)
% = 2
```

$N_{K/\mathbb{Q}}(\alpha - 2) = -1,\ Tr_{K/\mathbb{Q}}(\omega + 2\alpha) = 2$

We can decompose primes with `idealprimedec` :

```
? dec = idealprimedec(K,5);
? #dec
% = 2
? [pr1,pr2] = dec;
```

$\mathbb{Z}_K$ has two prime ideals above 5, that we call $\mathfrak{p}_1$ and $\mathfrak{p}_2$.

```
? pr1.f \\ residue degree
% = 1
? pr1.e \\ ramification index
% = 2
```

$\mathfrak{p}_1$ has residue degree 1 and ramification index 2.

```
? pr1.gen
% = [5, [-1, 0, 1, 0]~]
```

$\mathfrak{p}_1$ is generated by 5 and $-1 + 0 \cdot \omega + \alpha + 0 \cdot \omega\alpha$, i.e. we have $\mathfrak{p}_1 = 5\mathbb{Z}_K + (\alpha - 1)\mathbb{Z}_K$.

```
? pr2.f
% = 1
? pr2.e
% = 2
```

$\mathfrak{p}_2$ also has residue degree 1 and ramification index 2.

An arbitrary ideal is represented by its Hermite normal form (HNF) with respect to the integral basis. We can obtain this form with `idealhnf`.

```
? idealhnf(K,pr1)
% =
[5 3 4 3]
[0 1 0 0]
[0 0 1 0]
[0 0 0 1]
```

$\mathfrak{p}_1$ can be described as $\mathfrak{p}_1 = \mathbb{Z} \cdot 5 + \mathbb{Z} \cdot (\omega + 3) + \mathbb{Z} \cdot (\alpha + 4) + \mathbb{Z} \cdot (\omega\alpha + 3)$.

```
? a = idealhnf(K,[23, 10, -5, 1]~)
% =
[260   0 228 123]
[  0 260 123 105]
[  0   0   1   0]
[  0   0   0   1]
```

We obtain the HNF of the ideal $a = (23 + 10\omega - 5\alpha + \omega\alpha)$.

```
? idealnorm(K,a)
% = 67600
```

We have $N(a) = 67600$.

We perform operations on ideals with the functions `idealxxxx`, which accept HNF forms, prime ideal structures (output of `idealprimedec`), and elements (interpreted as principal ideals).

```
? idealpow(K,pr2,3)
% =
[25 15 21 7]
[ 0  5  2 4]
[ 0  0  1 0]
[ 0  0  0 1]
? idealnorm(K,idealadd(K,a,pr2))
% = 1
```

We have $\mathfrak{a} + \mathfrak{p}_2 = \mathbb{Z}_K$: the ideals $\mathfrak{a}$ and $\mathfrak{p}_2$ are coprime

We factor an ideal into a product of prime ideals with `idealfactor`. The result is a two-column matrix : the first column contains the prime ideals, and the second one contains the exponents.

```
? fa = idealfactor(K,a);
? matsize(fa)
% = [3,2]
```

The ideal $\mathfrak{a}$ is divisible by three prime ideals.

```
? [fa[1,1].p, fa[1,1].f, fa[1,1].e, fa[1,2]]
% = [2, 2, 1, 2]
```

The first one is a prime ideal above 2, is unramified with residue degree 2, and appears with exponent 2.

```
? [fa[2,1].p, fa[2,1].f, fa[2,1].e, fa[2,2]]
% = [5, 1, 2, 2]
? fa[2,1]==pr1
% = 1
```

The second one is $\mathfrak{p}_1$, and it appears with exponent 2.

```
? [fa[3,1].p, fa[3,1].f, fa[3,1].e, fa[3,2]]
% = [13, 2, 1, 1]
```

The third one is a prime ideal above 13, is unramified with residue degree 2, and appears with exponent 1.

We can use the Chinese remainder theorem with `idealchinese` :

```
? b = idealchinese(K,[pr1,2;pr2,1],[1,-1]);
```

We are looking for an element $b \in \mathbb{Z}_K$ such that $b = 1 \mod \mathfrak{p}_1^2$ and $b = -1 \mod \mathfrak{p}_2$.

```
? nfeltval(K,b-1,pr1)
% = 2
? nfeltval(K,b+1,pr2)
% = 1
```

We check the output by computing valuations : $v_{\mathfrak{p}_1}(b-1) = 2$ and $v_{\mathfrak{p}_2}(b+1) = 1$.

To obtain the class group and unit group of a number field, we need a more expensive computation than `nfinit`. The relevant information is contained in the structure computed with `bnfinit`.

```
? K2 = bnfinit(K);
? K2.nf == K \\ the underlying nf structure
% = 1
? K2.no \\ class number
% = 1
```

K has a trivial class group.

```
? lift(K2.tu) \\torsion units
% = [2, -1]
? K2.tu[1]==nfrootsof1(K)[1]
% = 1
```

K has two roots of unity, ± 1. We can also compute them with `nfrootsof1`.

```
? lift(K2.fu) \\ fundamental units
% = [1/2*x^2-1/2*x-1/2, 1/2*x^3-3/2*x^2+3/2*x-1]
```

The free part of $\mathbb{Z}_K^\times$ is generated by $\frac{\alpha^2 - x - 1}{2}$ and $\frac{\alpha^3 - 3x^2 + 3x - 2}{2}$

```
? L = bnfinit(x^3 - x^2 - 54*x + 169);
? L.cyc
% = [2, 2]
? L.gen
% = [[5,3,2;0,1,0;0,0,1], [5,4,3;0,1,0;0,0,1]]
```

$\mathcal{C}\ell = \mathbb{Z}/2\mathbb{Z} \cdot g_1 \oplus \mathbb{Z}/2\mathbb{Z} \cdot g_1 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
The two generators, g_1 and g_2 are given as ideals in HNF form.

`bnfisprincipal` expresses the class of the ideal in terms of the generators of the class group (discrete logarithm)

```
? pr = idealprimedec(L,13)[1]
? [dl,g] = bnfisprincipal(L,pr);
? dl
% = [1, 0]~
```

$\mathfrak{p} = (g)g_1^1 g_2^0$ for some $g \in L$. In particular, the ideal is not principal, but its square is (pr is a 2-torsion element).

```
? g
% = [0, 1/5, 2/5]~
? {idealhnf(L,pr) == idealmul(L,g,idealfactorback(L,L.gen,dl))}
% = 1
```

The second component of the output of `bnfisprincipal` is an element $g \in L$ that generates the remaining principal ideal. (`idealfactorback` = inverse of `idealfactor` $= \prod_i \mathsf{L.gen[i]}^{\mathsf{dl[i]}}$)

We know that pr is a 2-torsion element ; let's compute a generator of its square :

```
? [dl2,g2] = bnfisprincipal(L,idealpow(L,pr,2));
? dl2
% = [0, 0]~
```

The ideal is indeed principal (trivial in the class group).

```
? g2
% = [1, -1, -1]~
? idealhnf(L,g2) == idealpow(L,pr,2)
% = 1
```

g2 is a generator of $\mathfrak{p}_2$.

We can use these functionalities to find solutions in $\mathbb{Z}_K$ of norm equations with bnfisintnorm :

```
? bnfisintnorm(L,5)
% = []
? bnfisintnorm(L,65)
% = [x^2 + 4*x - 36, -x^2 - 3*x + 39, -x + 2]
```

There is no element of norm 5 in $\mathbb{Z}_L$.
There are three elements of $\mathbb{Z}_L$ of norm 65, up to multiplication by elements of $\mathbb{Z}_L^\times$ with positive norm.

```
? u = [0,2,1]~;
? nfeltnorm(L,u)
% = 1
```

We have found a unit $u \in Z_L^\times$.

```
? bnfisunit(L,u)
% = [1, 2, Mod(0, 2)]~
? lift(L.fu)
% = [x^2 + 4*x - 34, x - 4]
? lift(L.tu)
% = [2, -1]
```

We express it in terms of the generators withbnfisunit :
$u = (\alpha^2 + 4\alpha - 34) \cdot (\alpha - 4)^2 \cdot (-1)^0$.