Algebraic number theory

A GP tutorial

A. Page

IMB
Inria/Université de Bordeaux

09/01/2024

Documentation

- refcard-nf.pdf: list of functions with a short description.
- users.pdf Section 3.13: introduction and detailed descriptions of the functions.
- in gp, `?10`: list of functions.
- in gp, `?functionname`: short description of the function.
- in gp, `??functionname`: long description of the function.

To record the commands we will type during the tutorial:

```
? \l TAN.log
```

Plan

Number Fields

Irreducibility

In GP, we describe a number field K as

$$K = \mathbb{Q}[x]/f(x)$$

where $f \in \mathbb{Z}[x]$ is a monic irreducible polynomial.

```
? f = x^4 - 2*x^3 + x^2 - 5;
? polisirreducible(f)
% = 1
```

GP knows cyclotomic polynomials:

```
? g = polcyclo(30)
% = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1
```

Algebraic numbers

To perform simple operations in $K = \mathbb{Q}[x]/f(x) = \mathbb{Q}(\alpha)$ where $f(\alpha) = 0$, we can use `Mod`:

```
? Mod(x,f)^5
% = Mod(3*x^3-2*x^2+5*x+10, x^4-2*x^3+x^2-5)
```

Interpretation: $\alpha^5 = 3\alpha^3 - 2\alpha^2 + 5\alpha + 10$.

We check that the roots of g are 30th roots of unity:

```
? lift(Mod(x,g)^15)
% = -1
```

We used `lift` to make the output more readable.

polredbest

Sometimes we can find a simpler defining polynomial for the same number field by using `polredbest`:

```
? {h = x^5 + 7*x^4 + 22550*x^3 - 281686*x^2
  - 85911*x + 3821551};
? polredbest(h)
% = x^5 - x^3 - 2*x^2 + 1
```

Interpretation: $\mathbb{Q}[x]/h(x) \cong \mathbb{Q}[x]/(x^5 - x^3 - 2x^2 + 1)$.

nfinit

Most operations on number fields use a structure representing the field and its ring of integers, which is computed by `nfinit`.

```
? K = nfinit(f);
```

`K` contains the structure for the number field $K = \mathbb{Q}[x]/f(x)$.

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

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

Computed information

```
? K.disc
% = -1975
? K.zk
% = [1,1/2*x^2-1/2*x-1/2,x,1/2*x^3-1/2*x^2-1/2*x]
? w = K.zk[2];
```

K has discriminant -1975, and its ring of integers is

$$\mathbb{Z}_K = \mathbb{Z}+\mathbb{Z}\frac{\alpha^2-\alpha-1}{2}+\mathbb{Z}\alpha+\mathbb{Z}\frac{\alpha^3-\alpha^2-\alpha}{2} = \mathbb{Z}+\mathbb{Z}w+\mathbb{Z}\alpha+\mathbb{Z}w\alpha.$$

Elements of a number field

We saw that we could represent elements of a number field 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]~
```

Interpretation: $\alpha^2 = 1 \cdot 1 + 2 \cdot w + 1 \cdot \alpha + 0 \cdot w\alpha = 1 + 2w + \alpha$.

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

Interpretation: $1 + w + \alpha + w\alpha = \frac{\alpha^3+1}{2}$.

Elements of a number field: operations

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]~
```

Interpretation: $(1-w)\cdot\alpha^2 = -1+3w+\alpha-w\alpha$.

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

Interpretation: $N_{K/\mathbb{Q}}(\alpha-2) = -1$, $\mathrm{Tr}_{K/\mathbb{Q}}(w+2\alpha) = 2$.

Ideals

Reminder

In $\mathbb{Z}_K$, ideals factor uniquely into products of prime ideals:

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{a_i}.$$

In particular, prime numbers admit a decomposition:

$$p\mathbb{Z}_K = \prod_i \mathfrak{p}_i^{e_i} \text{ with } \mathbb{Z}_K/\mathfrak{p}_i \cong \mathbb{F}_{p^{f_i}}.$$

- e_i = ramification index of $\mathfrak{p}_i$.
- f_i = residue degree of $\mathfrak{p}_i$.

Decomposition of primes

We can decompose primes with `idealprimedec`:

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

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

```
? pr1.f
% = 1
? pr1.e
% = 2
```

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

Decomposition of primes

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

$\mathfrak{p}_1$ is generated by 5 and $-1 + 0 \cdot w + \alpha + 0 \cdot w\alpha$, 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.

Ideals

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]
```

Interpretation: $\mathfrak{p}_1$ can be described as

$$\mathfrak{p}_1 = \mathbb{Z} \cdot 5 + \mathbb{Z} \cdot (w+3) + \mathbb{Z} \cdot (\alpha+4) + \mathbb{Z} \cdot (w\alpha+3).$$

Ideals

```
? 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 $\mathfrak{a} = (23 + 10w - 5\alpha + w\alpha)$.

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

We have $N(\mathfrak{a}) = 67600$.

Ideals: operations

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.

Ideals: factorisation

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.

Ideals: factorisation

```
? [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.

Class groups and units

Reminder

The class group

$$\mathrm{Cl}(K) = \frac{(\text{nonzero ideals of } K)}{(\text{principal ideals } \beta\mathbb{Z}_K)}.$$

is a finite abelian group.

The unit group

$$\mathbb{Z}_K^\times \cong \mathbb{Z}/w\mathbb{Z} \times \mathbb{Z}^{r_1+r_2-1}$$

is a lattice under the logarithmic embedding, whose covolume is called the regulator Reg_K.

bnfinit

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` (b = Buchmann).

```
? K2 = bnfinit(K);
? K2.nf == K
% = 1
? K2.no
% = 1
```

K has a trivial class group (no = class number).

```
? K2.reg
% = 1.7763300299706546701307646106399605586
```

We obtain an approximation of the regulator of K.

bnfcertify

The output of `bnfinit` is a priori only correct under GRH (Generalised Riemann Hypothesis). We can unconditionally certify it with `bnfcertify`.

```
? bnfcertify(K2)
% = 1
```

The computation is now certified! If `bnfcertify` outputs `0`, it means we have found a counter-example to GRH (or more likely a bug in PARI/GP)!

bnfinit: units

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

K has two roots of unity (tu = torsion units), ± 1. We can also compute them with `nfrootsof1`.

```
? lift(K2.fu)
% = [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 $\frac{\alpha^2-\alpha-1}{2}$ and $\frac{\alpha^3-3\alpha^2+3\alpha-2}{2}$ (fu = fundamental units).

Class group

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

$\mathrm{Cl}(L) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

```
? L.gen
% = [[5,0,0;0,5,3;0,0,1], [5,0,3;0,5,2;0,0,1]]
```

Generators of the class group, given as ideals in HNF form.

Testing whether an ideal is principal

We test whether an ideal is principal with `bnfisprincipal`:

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

`bnfisprincipal` expresses the class of the ideal in terms of the generators of the class group (discrete logarithm). Here, the ideal `pr` is in the same class as the first generator. In particular, the ideal is not principal, but its square is.

Testing whether an ideal is principal

```
? g
% = [-2/5, 1/5, 0]~
? {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 = $\prod_i \texttt{L.gen[i]}^{\texttt{dl[i]}}$)

Computing a generator of principal ideal

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 $\mathtt{pr}^2$.

Class field theory

Reminder

A modulus $\mathfrak{m}$ of a number field K is a pair $(\mathfrak{m}_f, \mathfrak{m}_\infty)$ of a nonzero ideal $\mathfrak{m}_f$ and a set $\mathfrak{m}_\infty$ of real embeddings of K.

Define $U_K(\mathfrak{m}) \subset K^\times$: we have $\beta \in U_K(\mathfrak{m})$ iff

- $v_\mathfrak{p}(\beta - 1) \geq v_\mathfrak{p}(\mathfrak{m}_f)$ for all $\mathfrak{p} \mid \mathfrak{m}_f$, and
- $\sigma(\beta) > 0$ for all $\sigma \in \mathfrak{m}_\infty$.

The ray class group

$$\mathrm{Cl}_\mathfrak{m}(K) = \frac{(\text{nonzero ideals of } K \text{ coprime to } \mathfrak{m}_f)}{(\text{principal ideals } \beta\mathbb{Z}_K \text{ with } \beta \in U_K(\mathfrak{m}))}.$$

is a finite abelian group.

Reminder

For every modulus $\mathfrak{m}$, there exists a unique Abelian extension of K, the ray class field $K(\mathfrak{m})$, such that

- $\mathrm{Gal}(K(\mathfrak{m})/K) \cong \mathrm{Cl}_{\mathfrak{m}}(K)$, and
- a prime ideal $\mathfrak{p}$ coprime to $\mathfrak{m}_f$ splits in $K(\mathfrak{m})$ if and only if the class of $\mathfrak{p}$ in $\mathrm{Cl}_{\mathfrak{m}}(K)$ is trivial.

The special case $K(1)$ is called the Hilbert class field.

Every Abelian extension of K is contained in some $K(\mathfrak{m})$, and can therefore be described by a pair $(\mathfrak{m}, H)$ where $H \subset \mathrm{Cl}_{\mathfrak{m}}(K)$.

Hilbert class field

To compute a Hilbert class field, we first need to compute the class group.

```
bnf = bnfinit(y^2-y+50);
bnf.cyc
% = [9]
```

The class group is isomorphic to $\mathbb{Z}/9\mathbb{Z}$. We compute a relative defining polynomial for the Hilbert class field with the function `bnrclassfield`.

```
R = bnrclassfield(bnf)[1]
% = x^9 - 24*x^7 + (2*y - 1)*x^6 + 495*x^5
 + (-12*y + 6)*x^4 - 30*x^3 + (18*y - 9)*x^2
 + 18*x + (-2*y + 1)
```

Hilbert class field

Conversely, from an abelian extension, we can recover its corresponding class group with `rnfconductor`.

```
[cond,bnr,subg] = rnfconductor(bnf,R);
cond
% = [[1, 0; 0, 1], []]
subg
% = [9]
```

Here the conductor is trivial, and its norm group is trivial in the class group.

Hilbert class field

We can also ask for an absolute defining polynomial for the Hilbert class field with the optional `flag=2`.

```
R2 = bnrclassfield(bnf,,2)
% = x^18 - 48*x^16 + 1566*x^14 - 23621*x^12
  + 244113*x^10 - 19818*x^8 - 3170*x^6
  + 17427*x^4 - 3258*x^2 + 199
```

Ray class fields

We can also consider class fields with nontrivial conductor. The function `bnrinit` computes $\mathrm{Cl}_{\mathfrak{m}}(K)$.

```
bnr = bnrinit(bnf,12);
bnr.cyc
% = [72,2]
```

We can compute in advance the absolute degree, signature and discriminant of the corresponding class field with `bnrdisc`.

```
[deg,r1,D] = bnrdisc(bnr);
[deg,r1]
% = [288,0]
D
% = 92477896[...538 digits...]84942237696
```

This field is huge!

Ray class fields

For efficiency, we compute the class field as a compositum of several smaller fields.

```
bnrclassfield(bnr)
% = [x^2 - 3, x^8 + (-27*y+24)*x^6
 + (-294*y-3273)*x^4 + (-3*y-3852)*x^2 - 3,
 x^9 - 24*x^7 + (2*y-1)*x^6 + 495*x^5
 + (-12*y+6)*x^4 - 30*x^3 + (18*y-9)*x^2
 + 18*x + (-2*y+1)]
```

We can force the computation of a single polynomial with `flag=1`.

```
bnrclassfield(bnr,,1)
% = [... big polynomial ...]
```

Ray class fields

We can also compute a subfield of the ray class field by specifying a subgroup.

```
bnr = bnrinit(bnf,7)
bnr.cyc
% = [54,3]
bnrclassfield(bnr,3) \\elementary 3-subextension
% = [x^3 + 3*x + (14*y - 7),
 x^3 + (-1008*y - 651)*x + (-1103067*y - 8072813)]
```

Without the explicit field

Computing a defining polynomial with `bnrclassfield` can be time-consuming, so it is better to compute the relevant information without constructing the field, if possible.

We already saw the use of `bnrdisc`; we can also compute splitting information without the explicit field.

```
pr41 = idealprimedec(bnf,41)[1];
bnrisprincipal(bnr,pr41,0)
% = [0,0]~
```

The Frobenius at $\mathfrak{p}_{41}$ is trivial: this prime splits completely in the degree 162 extension (which we did not compute).

Ray class fields

Let’s do a full example with an HNF ideal and a subgroup given by a matrix.

```
bnr = bnrinit(bnf,[102709,43512;0,1]);
bnr.cyc
% = [17010, 27]
bnrclassfield(bnr,[9,3;0,1]) \\subgroup of index 9
% = [x^9 + (-297*y - 4470)*x^7 + ... ]
```

Modulus with infinite places

If the base field has real places, we can specify the modulus at infinity by providing a list of 0 or 1 of length the number of real embeddings.

```
bnf=bnfinit(a^2-217);
bnf.cyc
% = []
bnrinit(bnf,1).cyc
% = []
bnrinit(bnf,[1,[1,1]]).cyc
% = [2]
```

The field $\mathbb{Q}(\sqrt{217})$ has narrow class number 2.

Questions ?

Have fun with GP !