Algebraic number theory, class field theory

Marine Rougnant

19/02/2024 - 23/02/2024

1 Number field

Exercise 1. Let $Q = x^3 - 111x^2 + 6064x - 189804$.

1. Check that Q is irreducible.
2. Compute a nicer defining polynomial P for the same field
3. Check that they really define the same number field.
4. Initialise the number field $F = \mathbb{Q}(\alpha)$ defined by P (`nfinit`).
5. What are
   - the signature of F?
   - the discriminant of F?
   - a $\mathbb{Z}$-basis of $\mathbb{Z}_F$?
6. You can represent elements in polynomial form (`Mod(...,P)`) or as column vectors of coefficients on the basis of $\mathbb{Z}_F$. What are the coefficients of $-\frac{5}{2}\alpha^2 + \frac{19}{2}\alpha - 3$ on the basis? Is it an algebraic integer? What are its trace and norm ?
7. Compute the prime decomposition of $2, 3, 19$. How many primes ideals are there above them? What are their ramification indices? Residue degree? Compute a basis of these prime ideals. Compute the image of some elements in the residue field (`nfmodpr`).
8. Compute a product of some ideals in F (`idealmul`, `idealpow`, `idealfactorback`). Factor it as a product of prime ideals (`idealfactor`). Check the valuations separately (`idealval`).
9. Is F Galois (`galoisinit`)? Does it have automorphisms (`nfgaloisconj`)? What is the Galois group of its Galois closure (`polgalois`)? Compute a defining polynomial of its Galois closure (`nfsplitting`).

2 Class group and units

Exercise 2.
To compute the class group and unit group, use `bnfinit`. Let's denote by L the number field defined by $P = x^3 - x^2 - 92x - 236$

1. What is L[7] ? Find a way to recover it using `L.xxx`.
2. What is the structure of the class group?
3. What are the corresponding generators of the class group?
4. What is the rank of the unit group? What are generators of the unit group ?
5. Explore and experiment with `bnfisprincipal` :

(a) Compute the prime decomposition of 13. Let pr_i be the i-th component of the output.

(b) Express the class of each ideal pr_i in terms of the generators of the class group. Are they principal ideals?

(c) Use `idealfactorback` and `bnfisprincipal(L,pr)` to compute the Hermite normal form of the ideal $pr1$. Compare with `idealhnf(L,pr1)`.

(d) Show that the square of the ideal $pr1$ is a principal ideal.

Exercise 3.

Consider the quartic field $K = \mathbb{Q}(\sqrt[4]{65})$.

1. Initialize K.
2. Determine a $\mathbb{Z}$-basis of $\mathcal{O}_K$ (see `nfbasis`).
3. Find a polynomial over $\mathbb{Q}$ for the fourth term in the $\mathbb{Z}$-basis (see `real` and `polroots`).
4. Compute the discriminant ok K. Deduce the list of the ramified primes in K.
5. What is $[\mathcal{O}_K : \mathbb{Z}(\sqrt[4]{65})]$?
6. Determine the prime ideal factorizations of 2, 3, 5, and 7 in K.
7. What is the class group of K? *(you need a bnf structure of K).*
8. Give a system of fundamental units of K.
9. What is the regulator of K? (see `bnfreg`)

3 Ramification groups

Exercise 4.

Consider $P = x^4 - x^3 - 3x^2 + x - 1$ and denote by K its splitting field.

1. Compute the polynomial Q defing K (use `polredbest`).
2. Initialize the number field K.
3. Which primes ramify in $K/\mathbb{Q}$?
4. Compute the decomposition of 3 in prime ideals. How many prime ideals are above 3 ? With which residue degree and ramification index ? Denote by pr the first one.
5. Use `idealramgroups`to compute the decomposition group of pr and its inertia group.

4 Subfields

Exercise 5.

Let $K = \mathbb{Q}[X]/P(X) = \mathbb{Q}(\alpha)$ be the number fields defined by $P = y^8 - y^6 + 2y^2 + 1$. Explore and experiment with `nfsubfields` :

1. Give the number of subfields of K (up to isomorphisms).
2. How many of them have degree 4 over $\mathbb{Q}$?
3. For each of these (degree 4) subfields L_i :

   (a) give the absolute equation (ie the polynomial P_i definig $L_i/\mathbb{Q}$),

   (b) the embedding $L_i \subset K$ (ie a root of P_i as a polynomial in α),

   (c) the image in K of the element $a = y^2 + y \in L_i$ (see `minpoly`).

Exercise 6. Abelian extensions of $\mathbb{Q}$

Recall that every Abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field (Kronecker–Weber).

1. Compute every subfield of $\mathbb{Q}(\zeta_{60})$ of degree 8 (see `polsubcyclo`).
2. Computes the subfield fixed by the subgroup of $(\mathbb{Z}/60\mathbb{Z})^\times$ generated by `-1` (see `galoissubcyclo`)

Exercise 7.

1. Let $K = \mathbb{Q}[\alpha]$ the field defined by $P = x^4 - x^3 - 3x + 4$. Use `nfinit` to compute K.
2. We consider
$$Q = y^3 + (-\alpha - 1)y^2 + (\alpha^3 + \alpha - 2)y + (-\alpha^3 + 3) \in \mathbb{Q}[\alpha][y].$$
Check that Q is irreducible over K using `nffactor`.
Remark : by default, $\mathbb{Q}[x, y] = \mathbb{Q}[y][x]$. To force $\mathbb{Q}[x, y] = \mathbb{Q}[x][y]$, you have to specify `y=varhigher("y")`.
3. Consider the extension $L = K[\beta]$ where β is a root of Q. What is the degree of the extension $L/\mathbb{Q}$?
4. Compute a polynomial which defines $L/\mathbb{Q}$ using `rnfequation`.
5. With `nfsubfields`, find the number of subfields of L. Do some of them are isomorphic ?

5 Hilbert class field

Exercise 8.

Consider the number field K defined by $P = y^2 - y + 1007$.

1. Initialize K and check that the class group is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
2. Using `bnrclassfield`, compute the Hilbert class field H of K. The output is a couple of polynomial of degree 3, why ?
3. With `nfcompositum` , compute a single defining polynomial of H/K. Find a way to get this polynomial without using the function `nfcompositum` (see the documentation of `bnrclassfield`).
4. Give a single absolute defining polynomial of $H/\mathbb{Q}$.

6 Ray class field

Exercise 9.

Consider the number field K defined by $P = y^2 - y + 1007$ and le prime ideal $\mathfrak{p}$ above 13 given by `pr = idealprimedec(bnf,13)[1]`.

1. Use `bnrinit` to initialize the ray class group structure corresponding to $\mathfrak{p}$.
2. Find its structure (`bnr.cyc`).
3. Using `bnrclassfield`, compute the ray class field L of K. Give :
   (a) its degree (see `bnrdisc`),
   (b) its definition as a compositum of several extensions of K (use `polredbest` and `lift` to simplify the relative defining polynomials),
   (c) an absolute defining polynomial.