Algebraic Number Fields in PARI/GP

PARI functions to work with number fields are located in the reference card on page 3.

Initialisation

Let $K = \mathbb{Q}(\xi)$ be an algebraic number field generated by an algebraic number $\xi \in \overline{\mathbb{Q}}$. Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of ξ. To initialise this field in PARI we use bnfinit(f(x)), e.g.

```
? K=bnfinit(x^3-2);
```

The only requirement is that $f(x)$ is irreducible and has integer coefficients. Therefore if ξ is not an algebraic integer one has to multiply its minimal polynomial by the common denominator of its coefficients. Now $K = \mathbb{Q}(\sqrt[3]{2})$, and one can ask some questions about K. K.zk is the basis over $\mathbb{Z}$ for the ring of integers $\mathcal{O}_K$. For example in our case

```
? K.zk
%1 = [1, x, x^2]
```

which means that

$$\mathcal{O}_K \ = \ \mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}\sqrt[3]{2}^2.$$

If you type K.sign, the answer will be a vector of two numbers $[r_1, r_2]$ with $r_1 + 2r_2 = \deg f$. r_1 is the number of real roots of $f(x) = 0$, and r_2 is the number of pairs of complex-conjugate roots. For example in our case

```
? K.sign
%2 = [1, 1]
```

there is one real 3rd root of 2, $\sqrt[3]{2} \approx 1.25992...$, and two complex conjugate roots $-0.62996... \pm 1.09112... * I$. You can recover the polynomial $f(x)$ and see numerical values of its roots by

```
? K.pol
%3 = x^3 - 2
? K.roots
%4 = [1.259921049894873164767210607, -0.6299605249474365823836053
036 - 1.091123635971721403560072614*I]
?
```

The latter command shows only one root in each pair of complex conjugates. To see numerical values of all $\deg f$ roots type

```
? polroots(K.pol)
%5 = [1.259921049894873164767210607 + 0.E-28*I, -0.6299605249474
365823836053036 + 1.091123635971721403560072614*I, -0.6299605249
474365823836053036 - 1.091123635971721403560072614*I]~
```

One doesn't actually need these numerical values. Just it is important to understand that for any different roots ξ_1, ξ_2 of the same irreducible polynomial $f(x)$ the fields $\mathbb{Q}(\xi_1)$ and $\mathbb{Q}(\xi_2)$ are isomorphic. Even in our case $\mathbb{Q}(\sqrt[3]{2})$, though it is a bit surprising because one of the three fields will be real (dense in $\mathbb{R}$), while the other two will be complex (dense in $\mathbb{C}$). Due to this isomorphism we do not have to specify in PARI which root do we use to define the number field. Mathematically we can express this fact by the formula $\mathbb{Q}(\xi) \cong \mathbb{Q}[x]/\langle f(x)\rangle$, i.e. the field is the quotient of the ring of polynomials by the ideal generated by $f(x)$.

Units

Dirichlet's Theorem describes the units $\mathcal{O}_K^\times$ as follows. Let $r = r_1 + r_2 - 1$ where r_1 and r_2 were defined above. Then one can choose r *fundamental units* $\varepsilon_1, \ldots, \varepsilon_r$ so that every unit $\varepsilon \in O_K^\times$ is a product of some integer powers of those $\varepsilon_1, \ldots, \varepsilon_r$ times a *torsion unit.* Torsion units are the roots of unity contained in K, i.e.

$$\mu(K) \;=\; \{\varepsilon \in \mathcal{O}_K : \exists n \text{ s.t. } \varepsilon^n = 1\}\,.$$

Then we have

$$\mathcal{O}_K^\times \;=\; \{\varepsilon_0 \varepsilon_1^{m_1} \ldots \varepsilon_r^{m_r} : \varepsilon_0 \in \mu(K), m_1, \ldots, m_r \in \mathbb{Z}\}.$$

Let us find all torsion units and some set of fundamental units in $K = \mathbb{Q}(\sqrt[3]{2})$:

```
? K.tu
%6 = [2, Mod(-1, x^3 - 2)]
```

that is there are 2 torsion units, $\mu(K) = \{1, -1\}$. The above answer means that $\mu(K)$ is generated by -1 as a multiplicative group.

```
? K.fu
%7 = [Mod(x - 1, x^3 - 2)]
```

We see that $\varepsilon = \sqrt[3]{2} - 1$ is a fundamental unit, and $\mathcal{O}_K^\times \;=\; \{\pm\varepsilon^m : m \in \mathbb{Z}\}$.

Exercise 1: Construct fundamental units in several real quadratic fields $\mathbb{Q}(\sqrt{m})$ for small $m > 0$.

Exercise 2: In the expression $(1 + \sqrt{2})^n = a_n + b_n\sqrt{2}$ write formulas for $a_n, b_n \in \mathbb{Z}$. It follows from the multiplicativity of norm that the pairs (a_n, b_n) are solutions to Pells' equations $a_n^2 - 2b_n^2 = (-1)^n$. Can you prove it explicitly using your formulas for a_n, b_n? Notice that this way you are getting all solutions to Pell's equation as we proved in class.

Class numbers

For any two ideals $I_1, I_2 \subseteq O_K$ one can define their *product ideal* as the set of all possible finite sums of products of elements of I_1 and I_2, i.e.

$$I_1 \cdot I_2 \;=\; \{x_1 y_1 + \cdots + x_m y_m : m \in \mathbb{N}, x_i \in I_1, y_i \in I_2\}$$

It is easy to check that this is again an ideal. Let us consider the set of ideals modulo principal ideals, i.e.

$$\mathrm{Cl(K)} \;=\; \{0 \neq \mathrm{I} \subseteq \mathcal{O}_\mathrm{K}\}/\sim$$

where $I_1 \sim I_2$ when $\langle\alpha_1\rangle I_1 = \langle\alpha_2\rangle I_2$ for some $\alpha_1, \alpha_2 \in \mathcal{O}_K$.

Theorem. With the above operation of multiplication, Cl(K) is a finite abelian group, called the class group of K. The following conditions are equivalent:

(i) O_K is a UFD

(ii) O_K is a PID

(iii) the group Cl(K) is trivial

Finiteness of the class group is an important result, and its size $h(K) = \#\mathrm{Cl(K)}$ is an important numerical characteristics of the number field K, called *the class number* of K. According to the above theorem, factorisation into primes is unique in $\mathcal{O}_K$ if and only if the class number is 1, i.e. $h(K) = 1$.

To see the class group in PARI one has to type

```
? K.clgp
%8 = [1, [], []]
```

Here the class number goes first, and then some description of the structure of Cl(K). We see that Cl(K) is trivial for $K = \mathbb{Q}(\sqrt[3]{2})$.

Exercise 3: Make a table of class numbers of some quadratic fields. Here is one example:

```
? m=[-10,-7,-6,2,3,15];
? for(i=1,#m,F=bnfinit(x^2-m[i]);print(m[i]," ",F.clgp[1]))
-10 2
-7 1
-6 2
2 1
3 1
15 2
```

Do separate tables for $m < 0$ and $m > 0$. The phenomenon you should observe is that $h(\mathbb{Q}(\sqrt{m})) \to +\infty$ when $m \to -\infty$, and there are finitely many imaginary quadratic fields K with a given value of the class number $h(K)$. Draw the graph of $m \mapsto h(\mathbb{Q}(\sqrt{m}))$ and find the list of all $m < 0$ with class number 1. Make a table of the corresponding m for each value of $h(K) = 1, 2, \ldots$ in some range. What is the largest class number you've found?

In the case of real quadratic fields, choose some large $M > 0$ and compute frequencies with which various class numbers occur for square-free $m \in [2, M]$. Draw the graph if possible. Make a table of frequencies. What is the largest class number you've found?

Exercise 4: For all $K = \mathbb{Q}(\sqrt{m})$ with small m and $h(K) > 1$ give explicit examples of non-unique factorisation into primes in $\mathcal{O}_K$. E.g. $m = -6$ and

$$10 \;=\; 2 \cdot 5 \;=\; (2 - \sqrt{-6})(2 + \sqrt{-6}).$$