Algebraic number theory
Exercise sheet for chapter 5

Nicolas Mascot (n.a.v.mascot@warwick.ac.uk),
Aurel Page (a.r.page@warwick.ac.uk)

TAs: Chris Birkbeck (c.d.birkbeck@warwick.ac.uk),
George Turcas (g.c.turcas@warwick.ac.uk)

Version: March 17, 2017

Answers must be submitted by Monday April 24, 14:00

Exercise 1 (65 points)**.** Let $K = \mathbb{Q}(\sqrt{229}) \subset \mathbb{R}$. (Note: 229 is prime)

1. (3 points) Write down without proof the ring of integers, the discriminant and the signature of K.
2. (5 points) Determine the fundamental unit $u \in \mathbb{Z}_K^\times$ such that $u > 1$, and compute $N_{\mathbb{Q}}^K(u)$.
3. (10 points) Determine a set of prime ideals of $\mathbb{Z}_K$ whose classes generate $\mathrm{Cl}(K)$ and give their residue degree.
4. (6 points) Let $\alpha = \frac{7+\sqrt{229}}{2}$ and $\beta = \frac{11+\sqrt{229}}{2}$. Determine the prime factorisations of the ideals (α) and (β).
5. (5 points) Let $z = x + y\sqrt{229} \in K$ ($x, y \in \mathbb{Q}$) be such that $N_{\mathbb{Q}}^K(z) = \pm 3$. Prove that, after possibly multiplying z by a unit in $\mathbb{Z}_K^\times$, we may assume that
$$u^{-1/2} \leq z \leq u^{1/2}. \tag{1}$$
6. (5 points) Let $z = x + y\sqrt{229} \in K$ ($x, y \in \mathbb{Q}$) satisfying (1). Prove that if $N_{\mathbb{Q}}^K(z) = 3$, then
$$\frac{1-3u}{2\sqrt{229u}} \leq y \leq \frac{u-3}{2\sqrt{229u}}.$$
Hint: Relate $y\sqrt{229} - x$ *to* z*, and sum the inequalities obtained for* z *and for* $y\sqrt{229} - x$.

7. (5 points) Let $z = x + y\sqrt{229} \in K$ ($x, y \in \mathbb{Q}$) satisfying (1). Prove that if $N^K_{\mathbb{Q}}(z) = -3$, then
$$\frac{2}{\sqrt{229u}} \leq y \leq 2\sqrt{\frac{u}{229}}.$$
8. (5 points) Prove that no integral ideal of $\mathbb{Z}_K$ of norm 3 is principal.
9. (6 points) Prove that $\mathrm{Cl}(K) \cong \mathbb{Z}/3\mathbb{Z}$.
10. (5 points) Describe the integral ideals of $\mathbb{Z}_K$ of norm 27, and determine which ones are principal.
11. (10 points) Describe the set of elements in $\mathbb{Z}_K$ of norm 27 in terms of u and β, and deduce the set of $(x, y) \in \mathbb{Z}^2$ such that $x^2 + xy - 57y^2 = 27$.

Exercise 2 (35 points)**.** Let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x) = x^3 - 6x - 3$.

1. (3 points) Prove that f is irreducible over $\mathbb{Q}$.
2. (5 points) Determine the ring of integers and the discriminant of K.
3. (5 points) Determine the decomposition of 3 in K.
4. (5 points) Compute the prime factorisation of the fractional ideal (u_1) generated by $u_1 = \alpha^3/3$. What can you deduce about u_1? Express u_1 in terms of the basis $1, \alpha, \alpha^2$.
5. (3 points) Determine a unit u_2 in $\mathbb{Z}_K^\times$ of the form $\alpha + n$ for $n \in \mathbb{Z}$. *Hint: you may use without proof the fact that* $N^K_{\mathbb{Q}}(\alpha - n) = f(n)$ *for all* $n \in \mathbb{Z}$.
6. (4 points) Let $\mathcal{L}$ be the logarithmic embedding of K. Compute approximate values of $\mathcal{L}(u_1)$ and $\mathcal{L}(u_2)$ up to 10^{-3}. *You may use without proof the fact that* $f(x)$ *has three real roots, with approximate values* $-2.14510, -0.52397, 2.66907$.
7. (10 points) Prove that $\{u_1, u_2\}$ generate a subgroup of $\mathbb{Z}_K^\times$ of rank 2. *Hint: you can prove that a matrix has nonzero determinant by computing an approximate value of the determinant.*

UNASSESSED QUESTIONS

The next questions are not worth any points. I still recommend you to try to solve them, for practice. Corrections will be available online, just like for the marked questions.

Exercise 3.

1. Prove that there is no number field K such that the unit group $\mathbb{Z}_K^\times$ is isomorphic to $\mathbb{Z}/50\mathbb{Z} \times \mathbb{Z}^{10}$.
2. Find a number field K such that $\mathbb{Z}_K \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$.

Exercise 4. Let $K = \mathbb{Q}(\alpha)$ where α is a root of $f(x) = x^4 - x^3 - x^2 + x + 1$. We will assume without proof that f is irreducible and that $\operatorname{disc} f = 117 = 3^2 \cdot 13$.

1. Let $\zeta = \alpha^3 - \alpha^2$. Prove that $\zeta^3 = 1$.
2. Exhibit a primitive 6-th root of unity in K.
3. Prove that $\#W_K = 6$.
4. Prove that K is totally complex. What is $\mathbb{Z}_K^\times$ isomorphic to as an abelian group?
5. Prove that $\alpha \in \mathbb{Z}_K^\times$ but $\alpha \notin W_K$.

Exercise 5.

1. Log in to a university computer that has the computer algebra software `gp` installed (Linux computers should have it).
2. Type `gp` in a terminal to start the software.
3. Pick $d > 0$ squarefree.
4. Type `bnfinit(x^2-d).fu[1]` and hit `Enter`. This will compute a fundamental unit of $K = \mathbb{Q}(\sqrt{d})$ and display it in the form `Mod(a*x+b,x^2-d)`, meaning $a\sqrt{d} + b$.
5. Compute a fundamental unit of K by hand. Note that it might not be the same that `gp` computed: check that the two answers are compatible!
6. Type `bnfinit(x^2-d).clgp[2]` and hit `Enter`. This will compute the class group of K and display its structure in the form of a list $[a_1, \ldots, a_n]$ representing the group $\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$.
7. Compute the class group $\operatorname{Cl}(K)$ by hand.