D-MATH | Number Theory I | 31.10.2024

Prof. Dr. Emmanuel Kowalski

Exercise Sheet 4

1. Let K be a number field of degree $n = [K : \mathbb{Q}]$. For $x \in K$, the *norm* of x, denoted $N(x)$, is defined to the determinant of the $\mathbb{Q}$-linear map $m_x \colon K \to K$ defined by $m_x(y) = xy$. (Note that $N(x)$ is not necessarily ≥ 0, even when $K = \mathbb{Q}$.)

1. For $K = \mathbb{Q}(\sqrt{d})$, compute $N(a + b\sqrt{d})$ as a function of the rational numbers a and b.
2. Show that N defines a group homomorphism $K^\times \to \mathbb{Q}^\times$.
3. Let $\mathcal{E}(K)$ be the set of embeddings of K in $\mathbb{C}$. Show that
$$N(x) = \prod_{\iota \in \mathcal{E}(K)} \iota(x).$$
4. Let $x \in \mathbb{Z}_K$. Show that $N(x) \in \mathbb{Z}$. Show also that x is a unit in $\mathbb{Z}_K^\times$ if and only if $N(x) \in \{-1, 1\}$.
5. Let $x \in \mathbb{Z}_K \setminus \{0\}$. Show that there exists a $\mathbb{Z}$-basis $(e_1, \ldots, e_n)$ of $\mathbb{Z}_K$ and integers $a_1 \mid a_2 \mid \cdots \mid a_n$ such that
$$x\mathbb{Z}_K = a_1\mathbb{Z}e_1 \oplus \cdots \oplus a_n\mathbb{Z}e_n.$$
(Hint: use the classification of finitely-generated abelian groups.)
6. Deduce that for all $x \in \mathbb{Z}_K$, we have $|N(x)| = |x\mathbb{Z}_K|$, where the right-hand side is the norm of a principal ideal.

2. A number field K is said to be *euclidean* (with respect to the norm) if, for any x and y in $\mathbb{Z}_K$, with $y \neq 0$, there exists q and r in $\mathbb{Z}_K$ with $|N(r)| < |N(y)|$ such that $x = qy + r$.

1. Show that if K is euclidean, then the class group of K is trivial.
2. Show that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ are euclidean.
3. Let K be a euclidean number field. Show that there exists a non-zero element $\delta \in \mathbb{Z}_K$, which is not a unit, and has the following property: the restriction to $\mathbb{Z}_K^\times \cup \{0\}$ of the reduction map modulo δ is surjective (i.e., any element of $\mathbb{Z}_K$ is congruent modulo δ to either 0 or a unit of $\mathbb{Z}_K$.)
4. Determine all possible choices of the element δ of the previous question for $K = \mathbb{Q}$, and determine one choice for $K = \mathbb{Q}(i)$?
5. Deduce that $\mathbb{Q}(\sqrt{-19})$ and $\mathbb{Q}(\sqrt{-163})$ are not euclidean. (Hint: determine the units in the corresponding rings of integers.) Note: one can show that both of these fields have trivial class group, so the statement in Question 1 is not an equivalence.

3. Prove that any prime number p such that $p \equiv 1 \bmod 8$ or $p \equiv 7 \bmod 8$ is of the form $a^2 - 2b^2$, where a and b are integers. Show that there are infinitely many such representations. (Hint: use the field $\mathbb{Q}(\sqrt{2})$.)

4. Let d be a squarefree positive integer such that $-d \not\equiv 1 \bmod 4$. Assume that d is not a prime number. The goal of this exercise is to prove that the class group of $K = \mathbb{Q}(\sqrt{-d}) = \mathbb{Q}(i\sqrt{d})$ is not trivial.

1. Prove that there exist integers a, b with $1 < a < b$ such that $d = ab$.
2. Let u and $v \neq 0$ be integers. Show that any element of $(u + v\sqrt{-d})\mathbb{Z}_K$ has norm $\geq d$.
3. Prove that the ideal generated by a and $i\sqrt{d}$ in $\mathbb{Z}_K$ is not principal.

5. The goal of this exercise is to prove that the Fermat equation $x^3 + y^3 = z^3$ has no integral solution with $xyz \neq 0$, which was first proved by Euler. This is a fairly long exercise – the more interesting part start at Question 3, and the first two questions may be assumed without proof.

We denote $\omega = e^{2i\pi/3} = (-1 + i\sqrt{3})/2$ and $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$. We have $\mathbb{Z}_K = \mathbb{Z}[\omega]$.

We consider the equation

$$x^3 + y^3 = uz^3 \tag{1}$$

where $u \in \mathbb{Z}_K^\times$ is a parameter and the unknowns (x, y, z) are in $\mathbb{Z}_K$.

1. Show that $\mathbb{Z}_K$ is a euclidean domain and that $\mathbb{Z}_K^\times = \{-1, 1, \omega, \omega^2, -\omega, -\omega^2\}$.
2. Let $\lambda = 1 - \omega$. Show that $\lambda\mathbb{Z}_K$ is a prime ideal with norm 3. In particular, the field $\mathbb{Z}_K/\lambda\mathbb{Z}_K$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. We denote by v the λ-adic valuation on (non-zero) ideals.
3. Show that if $x \in \mathbb{Z}_K$ satisfies $x \equiv 1 \bmod \lambda$, then $x^3 \equiv 1 \bmod \lambda^4$. (Hint: write $x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$ and use the fact that $\omega^2 \equiv 1 \bmod \lambda$.)
4. Show that (1) has no solution with λ not dividing xyz. (Hint: reduce modulo λ and check cases.)
5. Let (x, y, z) be a solution of (1) for a given $u \in \mathbb{Z}_K^\times$ with $v(xy) = 0$. Show that $v(z) \geq 2$. (Hint: use the previous question and reduce modulo λ^2.)
6. We fix from now on a solution (x, y, z) of (1) for a given $u \in \mathbb{Z}_K^\times$ with $v(xy) = 0$ and x coprime to y. Show that one of $x + y$, $x + \omega y$ or $x + \omega^2 y$ has λ-valuation ≥ 2, and that one may assume that $x + y$ has this property, which we consider to be the case from now on.
7. Show then that $v(x + \omega y) = v(x + \omega^2 y) = 1$ and that $v(x + y) = 3v(z) - 2$.
8. Show that $\gcd(x + y, x + \omega y) = \gcd(x + y, x + \omega^2 y) = \gcd(x + \omega y, x + \omega^2 y) = \lambda\mathbb{Z}_K$ (where the gcds are in the sense of ideals).

9. Deduce that there exist units (ξ, η, ϑ) and elements (a, b, c) of $\mathbb{Z}_K$, each coprime to λ, such that
$$\xi a^3 \lambda^{v(x+y)} + \omega\eta b^3 \lambda + \omega^2 \vartheta c^3 \lambda = 0.$$
(Hint: use unique factorization in $\mathbb{Z}_K$ and combine the resulting expressions for $x + y$, $x + \omega y$, $x + \omega^2 y$.)
10. Deduce that there exist units ϵ and ϵ' and elements r, s and $t \in \mathbb{Z}_K$ such that
$$r^3 + \epsilon s^3 = \epsilon' t^3$$
and $v(t) = v(z) - 1$.
11. Show that $\epsilon \in \{-1, 1\}$ and deduce that there is a solution (x', y', z') of (1), possibly for a different unit than u, with $v(z') = v(z) - 1$.
12. Conclude that (1), and the Fermat equation with exponent 3, have no solutions with $xyz \neq 0$. (This method of proof is known as *infinite descent*, and has its origin in the proof by Fermat himself that the equation for exponent 4 has no solution, which is easier as it does not require any algebraic number theory.)

Due date: 11.11.2024