Autumn Semester 2019

Introduction to Algebraic Number Theory

Lecturer: Prof. Dr. Özlem Imamoglu
Coordinator: Dr. Danylo Radchenko

Solutions to Exercise Sheet 10

Exercise 10.1. Describe all integer solutions of $x^2 - 2y^2 = 7$.

Solution. Note that $x = 0$ and $y = 0$ do not give rise to any solutions, and that (x, y) is a solution to $x^2 - 2y^2$ if and only if $N_{K/\mathbb{Q}}(x + y\sqrt{2}) = 7$ where $K = \mathbb{Q}(\sqrt{2})$. Recall that $\varepsilon = 1 + \sqrt{2}$ is a fundamental unit in $\mathcal{O}_K$ of norm -1, and hence $3 + 2\sqrt{2} = \varepsilon^2$ is the smallest unit of norm 1. Thus, given one solution $\alpha = x_0 + y_0\sqrt{2}$, we obtain infinitely many solutions of the form $\pm(x_0 \pm y_0\sqrt{2})(3 + 2\sqrt{2})^n$, for $n \in \mathbb{Z}$.

Conversely, multiplying by an appropriate power of $(3+2\sqrt{2})$ and ± 1, we can get from any solution to a solution with $1 < x+y\sqrt{2} < 3+2\sqrt{2}$. Since $(x+y\sqrt{2})(x-y\sqrt{2}) = 7$, we also get $21-14\sqrt{2} < x-y\sqrt{2} < 7$. Adding these inequalities we get $11-7\sqrt{2} < x < 5+\sqrt{2}$, so that $2 \leq x \leq 6$. Direct check shows that only $x = 3$ and $x = 5$ work, but for $x = 5$ the solutions don't satisfy $1 < x + y\sqrt{2} < 3 + 2\sqrt{2}$. Hence the only solutions in the interval $(1, 3 + 2\sqrt{2})$ are $3 \pm \sqrt{2}$.

Thus, any integral solution (x, y) can be obtained as $x + y\sqrt{2} = \pm(3 \pm \sqrt{2})(3 + 2\sqrt{2})^n$ for some $n \in \mathbb{Z}$ (sign choices are independent).

Exercise 10.2. Let p be an odd prime, ζ_p a primitive p-th root of unity, and $K = \mathbb{Q}(\zeta_p)$.

(a) Show that the set of roots of unity in K is $\mu_K = \{\pm\zeta_p^j \mid j = 0, \ldots, p-1\}$;

(b) Show that $u_j = \frac{\zeta_p^j - 1}{\zeta_p - 1}$ is a unit in $\mathcal{O}_K$ for $j = 1, \ldots, p-1$.

Solution. (a) Since we know that μ_K is a finite cyclic group, let n be its order, and ζ_n be its generator. Since $\{\pm\zeta_p^j \mid 0 \leq j \leq p-1\}$ is a subgroup of order $2p$ in μ_K, we have $2p|n$ and $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_p)$.

Since $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ (Euler's totient function), we must have $\phi(n) = p-1 = \phi(2p)$. By multiplicativity of ϕ, we get that no other odd prime can divide n, so that $n = 2^a p^b$, $a, b \geq 1$. But then $\phi(n) = 2^{a-1}p^{b-1}(p-1) = (p-1)$ immediately implies $a = b = 1$.

(b) Since $u_j = 1 + \zeta_p + \cdots + \zeta_p^{j-1}$, we have $u_j \in \mathcal{O}_K$. Thus we need to show that $u_j^{-1} \in \mathcal{O}_K$. Recall that K is Galois with Galois group $(\mathbb{Z}/p\mathbb{Z})^\times$, where $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ acts by $\pi_a(\zeta_p) = \zeta_p^a$. Then there exists a such that $aj \equiv 1 \pmod{p}$, so that $\pi_a(u_j^{-1}) = u_a$. Since u_a is an algebraic integer, so is u_j^{-1}, and hence u_j is a unit.

Exercise 10.3. Let $K = \mathbb{Q}(\sqrt{5}, \sqrt{-2})$.

(a) Show that $\mathcal{O}_K = \mathbb{Z}[\frac{\sqrt{5}+1}{2}, \sqrt{-2}]$;

(b) Show that the only roots of unity in $\mathcal{O}_K$ are ± 1;

(c) Show that $\frac{\sqrt{5}+1}{2}$ is a fundamental unit in K, i.e., $\mathcal{O}_K^\times = \{\pm(\frac{\sqrt{5}+1}{2})^n \mid n \in \mathbb{Z}\}$.

(*Hint: in (a) use Exercise 4.4; in (b) and (c) use the norm maps $N_{K/F}$ for quadratic subfields F.*)

Solution. (a) We get this immediately by the result of Exercise 4.4, since the discriminants of $K_1 = \mathbb{Q}(\sqrt{5})$ and $K_2 = \mathbb{Q}(\sqrt{-2})$ are coprime. Moreover, the discriminant of K is 1600.

(b) We have $[K : \mathbb{Q}] = 4$, K is Galois with Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and the only quadratic subfields in K are $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{5})$, and $\mathbb{Q}(\sqrt{-10})$. Note that K is not itself a cyclotomic field, since the only cyclotomic fields of degree 4 are $\mathbb{Q}(\zeta_5)$, $\mathbb{Q}(\zeta_8)$, and $\mathbb{Q}(\zeta_{12})$, but their discriminants divide 125, 256, and 144 respectively (these are the discriminants of the minimal polynomials), and hence $\neq 1600 = D_K$.

Therefore, any root of unity ζ in K is contained in a quadratic subfield: in $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{5})$ or in $\mathbb{Q}(\sqrt{-10})$. Since the only roots of unity in these quadratic fields are ± 1, the only roots of unity in K are also ± 1.

(c) Denote $\phi = \frac{1+\sqrt{5}}{2}$, and let $\alpha = (a+b\phi)+(c+d\phi)\sqrt{-2}$ be a unit. Then $N_{K/\mathbb{Q}(\sqrt{d})}(\alpha)$ is a unit in $\mathbb{Q}(\sqrt{d})$ for $d = -2, 5, -10$. For $d = -2$ we get

$$N_{K/\mathbb{Q}(\sqrt{-2})}(\alpha) = ((a^2 + ab - b^2) - 2(c^2 + cd - d^2)) + (a(2c + d) + b(c - 2d))\sqrt{-2}\,.$$

Similarly, for $d = -10$ we write $\sqrt{-2} = \frac{\sqrt{-10}}{\sqrt{5}}$ and calculate:

$$N_{K/\mathbb{Q}(\sqrt{-10})}(\alpha) = ((a^2 + ab - b^2) + 2(c^2 + cd - d^2)) + (ad - bc)\sqrt{-10}\,.$$

Since the only units in $\mathbb{Q}(\sqrt{-2})$ and in $\mathbb{Q}(\sqrt{-10})$ are ± 1 this implies that

$$(a^2 + ab - b^2) \pm 2(c^2 + cd - d^2) \;=\; \pm 1\,.$$

By taking the absolute value of the difference of these two equations we obtain that $4|c^2 + cd - d^2| \leq 2$, so that $c^2 + cd - d^2 = 0$. If $d \neq 0$, then $c^2 + cd - d^2 = d^2((c/d)^2 + (c/d) - 1) \neq 0$, since $x^2 + x - 1$ is irreducible. Therefore, $c = d = 0$.

This implies that $\alpha = a + b\phi \in \mathbb{Q}(\sqrt{5})$. Since $\alpha \in \mathcal{O}_K^\times$, $a + b\phi$ is a unit in $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, and since the fundamental unit in this quadratic field is ϕ, we get $\alpha = \pm\phi^n$ for some $n \in \mathbb{Z}$ as claimed.

Exercise 10.4. Let $K = \mathbb{Q}(\sqrt[3]{2})$. Show that $\mathcal{O}_K^\times = \{\pm(\sqrt[3]{2} - 1)^n \mid n \in \mathbb{Z}\}$.

(*Hint: Use the embedding $i\colon \mathcal{O}_K \to \mathbb{R} \times \mathbb{C}$ and find a bounded region $B \subseteq \mathbb{R} \times \mathbb{C}$ such that for any unit $\alpha \in \mathcal{O}_K^\times$, $i(\pm\alpha(\sqrt[3]{2} - 1)^n) \in B$ for some n.*)

Solution. As it was shown during the Übungsstunde, $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$. We also have $r_1 = r_2 = 1$, and the standard embedding $i\colon \mathcal{O}_K \to \mathbb{R} \times \mathbb{C}$ is given by

$$i(a + b\sqrt[3]{2} + c\sqrt[3]{4}) \;=\; (a + b\sqrt[3]{2} + c\sqrt[3]{4}, (a - c\sqrt[3]{4}) + \omega(b\sqrt[3]{2} - c\sqrt[3]{4}))\,,$$

where ω is the cubic root of unity $e^{2\pi i/3}$. Note that $\sqrt[3]{2} - 1$ is indeed a unit, since $(\sqrt[3]{2} - 1)^{-1} = 1 + \sqrt[3]{2} + \sqrt[3]{4}$.

Let $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ be a unit, and let $i(\alpha) = (x, z)$. Since $1 < 1 + \sqrt[3]{2} + \sqrt[3]{4} < 4$, by replacing α by $\pm\alpha(\sqrt[3]{2} - 1)^n$ for some $n \in \mathbb{Z}$, we may assume that $1 < x < 4$. Since we must have $x|z|^2 = 1$, we also have $1/2 < |z| < 1$.

If we denote $A = a$, $B = b\sqrt[3]{2}$, and $C = c\sqrt[3]{4}$, then these inequalities are equivalent to

$$1 < A + B + C < 4\,,$$
$$1/4 < A^2 + B^2 + C^2 - AB - BC - CA < 1\,.$$

Rewriting

$$A^2 + B^2 + C^2 - AB - BC - CA \;=\; \frac{1}{4}(A + B - 2C)^2 + \frac{3}{4}(A - B)^2\,,$$

we get $|A - B| < 2/\sqrt{3}$, and by symmetry $|B - C| < 2/\sqrt{3}$ and $|C - A| < 2/\sqrt{3}$. Then from $3A = (A + B + C) + (A - B) + (A - C)$ we get $1 - 4/\sqrt{3} < 3A < 4 + 4/\sqrt{3}$. By symmetry we get the same estimates for B and C. Recalling that $A = a$, $B = b\sqrt[3]{2}$, $C = c\sqrt[3]{4}$, where $a, b, c \in \mathbb{Z}$, we obtain that $a \in \{0, 1, 2\}$, $b \in \{0, 1\}$, $c \in \{0, 1\}$.

To finish the proof one can directly go through all 12 possibilities. Alternatively, if we use the norm

$$N_{K/\mathbb{Q}}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) \;=\; a^3 + 2b^3 + 4c^3 - 6abc\,,$$

then we see that if $2|a$, then the norm is even, hence $\neq \pm 1$. Therefore, we must have $a = 1$, and checking the norms in the remaining four cases we see that $N(1) = 1$, $N(1+\sqrt[3]{2}) = 3$, $N(1 + \sqrt[3]{4}) = 5$, and $N(1 + \sqrt[3]{2} + \sqrt[3]{4}) = 1$. Since $1 + \sqrt[3]{2} + \sqrt[3]{4} = (\sqrt[3]{2} - 1)^{-1}$, this implies that all units are of the form $\pm(\sqrt[3]{2} - 1)^n$ for some integer n.