Autumn Semester 2019

Introduction to Algebraic Number Theory

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

Solutions to Exercise Sheet 5

Exercise 5.1. Find the discriminant of $K = \mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p-th root of unity and p is an odd prime.

(*Hint: recall from Exercise 2.3 that* $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.)

Solution. Since $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$, we have $D_K = \mathrm{d}(1, \zeta_p, \dots, \zeta_p^{p-2})$. The discriminant $\mathrm{d}(1, \zeta_p, \dots, \zeta_p^{p-2})$ is equal to the square of the determinant of the Vandermonde matrix of $\zeta_p, \dots, \zeta_p^{p-1}$ and therefore

$$\mathrm{d}(1, \zeta_p, \dots, \zeta_p^{p-2}) \;=\; \prod_{1 \le i < j \le p-1} (\zeta_p^i - \zeta_p^j)^2 \;=\; (-1)^{\frac{(p-1)(p-2)}{2}} \prod_{1 \le i \ne j \le p-1} (\zeta_p^i - \zeta_p^j)\,.$$

For a fixed $i \in \{1, \dots, p-1\}$ we compute

$$A_i = \prod_{\substack{j=1 \\ j \ne i}}^{p-1} (\zeta_p^i - \zeta_p^j) \;=\; \zeta_p^{i(p-1)} \prod_{\substack{j=1 \\ j \ne i}}^{p-1} (1 - \zeta_p^{j-i}) \;=\; \frac{\zeta_p^{i(p-1)}}{1 - \zeta_p^{-i}} \prod_{l=1}^{p-1} (1 - \zeta_p^l) \;=\; \frac{p\zeta_p^{i(p-1)}}{1 - \zeta_p^{-i}}\,,$$

where we have used the fact that $\prod_{j=1}^{p-1}(1 - \zeta_p^j) = p$. Then we have

$$\prod_{i=1}^{p-1} A_i \;=\; p^{p-1} \prod_{i=1}^{p-1} \frac{\zeta_p^{i(p-1)}}{1 - \zeta_p^{-i}} \;=\; p^{p-2} \zeta_p^{\frac{p(p-1)^2}{2}} \;=\; p^{p-2}\,.$$

Since p is odd, $\frac{(p-1)(p-2)}{2} \equiv \frac{p-1}{2} \pmod 2$, and thus we conclude that

$$D_K \;=\; (-1)^{\frac{p-1}{2}} \prod_{i=1}^{p-1} A_i \;=\; (-1)^{\frac{p-1}{2}} p^{p-2}\,.$$

Exercise 5.2. Recall that a quadratic field $K/\mathbb{Q}$ is uniquely determined by its discriminant. In this exercise we will show that this is no longer true for (pure) cubic fields. Let $K_1 = \mathbb{Q}(\sqrt[3]{6})$ and $K_2 = \mathbb{Q}(\sqrt[3]{12})$.

(a) Show that $\mathcal{O}_{K_1}$ is spanned by $\{1, \sqrt[3]{6}, \sqrt[3]{36}\}$;

(b) Show that $\mathcal{O}_{K_2}$ is spanned by $\{1, \sqrt[3]{12}, \sqrt[3]{18}\}$;

(c) Show that $D_{K_1} = D_{K_2}$, but K_1 and K_2 are not isomorphic.

Solution. (a) We compute the discriminant of $\{1, \sqrt[3]{6}, \sqrt[3]{6}^2\}$ to be $-972 = -2^2 \cdot 3^5$. Denote the $\mathbb{Z}$-span of $\{1, \sqrt[3]{6}, \sqrt[3]{6}^2\}$ by Λ_1. By Prop. 26 we have that if $\Lambda_1 \neq \mathcal{O}_{K_1}$, then there is an integer of the form $\omega = \frac{a+b\sqrt[3]{6}+c\sqrt[3]{36}}{p}$, where $p = 2$ or $p = 3$, $0 \leq a, b, c < p$, and not all of a, b, c are divisible by p.

First, assume that $p = 2$. Since $\mathrm{Tr}(\omega) = 3a/2 \in \mathbb{Z}$, we may assume that $a = 0$. The norm of ω is then $\frac{3}{4}b^3 + \frac{9}{2}c^3$. Since $2N(\omega) = \frac{3}{2}b^3$, we get that $2|b$, but then $\frac{9}{2}c^3 = N(\omega) - \frac{3}{4}b^3 \in \mathbb{Z}$, so that $2|c$. Thus we have $2|a, b, c$, a contradiction.

Next, assume that $p = 3$. We compute

$$\mathrm{Tr}(\omega^2) \;=\; \frac{1}{9}\mathrm{Tr}(a^2 + b^2\sqrt[3]{36} + 6c^2\sqrt[3]{6} + 2ab\sqrt[3]{6} + 2ac\sqrt[3]{36} + 12bc) \;=\; \frac{a^2}{3} + 4bc\,,$$

from which we see that $3|a$, and thus $a = 0$. The norm of ω is then $N(\omega) = \frac{2}{9}b^3 + \frac{4}{3}c^3$. Since $3N(\omega) = \frac{2}{3}b^3 + 4c^3$ we have that $3|b$, and thus $N(\omega) - \frac{2b^3}{9} = \frac{4}{3}c^3$ is also an integer. Thus we see that $3|a, b, c$, a contradiction.

Therefore, $\Lambda_1 = \mathcal{O}_{K_1}$.

(b) Note that $\sqrt[3]{18} = \frac{1}{2}\sqrt[3]{12}^2$. We compute the discriminant of $\{1, \sqrt[3]{12}, \sqrt[3]{18}\}$ to be $-972 = -2^2 \cdot 3^5$. Denote the $\mathbb{Z}$-span of $\{1, \sqrt[3]{12}, \sqrt[3]{18}\}$ by Λ_2. By Prop. 26 we have that if $\Lambda_2 \neq \mathcal{O}_{K_2}$, then there is an integer of the form $\omega = \frac{a+b\sqrt[3]{12}+c\sqrt[3]{18}}{p}$, where $p = 2$ or $p = 3$, $0 \leq a, b, c < p$, and not all of a, b, c are divisible by p.

First, assume that $p = 2$. Since $\mathrm{Tr}(\omega) = 3a/2 \in \mathbb{Z}$, we have $a = 0$. The norm of ω is then $\frac{3}{2}b^3 + \frac{9}{4}c^3$. Since $2N(\omega) = \frac{9}{2}c^3$, we get that $2|c$, and then $\frac{3}{2}b^3 = N(\omega) - \frac{9c^3}{4} \in \mathbb{Z}$, so that $2|a, b, c$, a contradiction.

Next, assume that $p = 3$. As before, we have $\mathrm{Tr}(\omega^2) = \frac{a^2}{3} + 4bc$, from which we see that $3|a$, and thus $a = 0$. The norm of ω is then $N(\omega) = \frac{4}{9}b^3 + \frac{2}{3}c^3$. Since $3N(\omega) = \frac{4}{3}b^3 + 2c^3$ we have that $3|b$, and thus $N(\omega) - \frac{4b^3}{9} = \frac{2}{3}c^3$ is also an integer. Thus we see that $3|a, b, c$, a contradiction.

Therefore, $\Lambda_2 = \mathcal{O}_{K_2}$.

(c) We have already seen that $D_{K_1} = D_{K_2} = -972$. To see that K_1 and K_2 are not isomorphic, note that if they were isomorphic, then there would exist an element $\beta \in K_1$ such that $\beta^3 = 12$. Assume that $\beta = a + b\alpha + c\alpha^2$, where $\alpha = \sqrt[3]{6}$ and $a, b, c \in \mathbb{Q}$.

Let $\zeta = e^{2\pi i/3}$ be the third root of unity. Since the complex embeddings of β are $\beta, \omega\beta, \omega^2\beta$, we have $\mathrm{Tr}(\beta) = 0$. On the other hand, we have $\mathrm{Tr}(\beta) = 3a$. Therefore, $a = 0$. Repeating this with $\beta/\alpha = b + c\alpha$ we get that $b = 0$. Finally, we get that $\beta/\alpha^2 \in \mathbb{Q}$, but $(\beta/\alpha^2)^3 = 1/3$ is not a cube, a contradiction

Exercise 5.3. Let $K = \mathbb{Q}(\sqrt{6})$.

(a) Show that $\mathfrak{p} = (2, \sqrt{6})$ is a prime ideal in $\mathcal{O}_K$;

(b) Find the generators of $\mathfrak{p}^{-1} = \{a \in \mathcal{O}_K \mid a\mathfrak{p} \subseteq \mathcal{O}_K\}$.

(c) Show that $\mathfrak{p}$ is principal and find its generator.

Solution. Since $6 \equiv 2 \pmod 4$ we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{6}]$.

(a) Note that $\mathfrak{p} = \{2a + b\sqrt{6} \mid a, b \in \mathbb{Z}\}$. Therefore, $(a + b\sqrt{6})(c + d\sqrt{6}) \in \mathfrak{p}$ if and only if $ac + 6bd$ is even, so that either a or c is even. But then either $a + b\sqrt{6}$ or $c + d\sqrt{6}$ is in $\mathfrak{p}$. Since clearly $\mathfrak{p} \neq \mathcal{O}_K$, we obtain that $\mathfrak{p}$ is a prime ideal (by definition).

(b) By definition $a+b\sqrt{6} \in \mathfrak{p}^{-1}$ if and only if $2a+2b\sqrt{6} \in \mathbb{Z}[\sqrt{6}]$ and $6b+a\sqrt{6} \in \mathbb{Z}[\sqrt{6}]$. From the second inclusion we see that $a \in \mathbb{Z}$, and from the first that $2b \in \mathbb{Z}$. Clearly, these are also sufficient, hence $\mathfrak{p}^{-1} = (1, \frac{\sqrt{6}}{2})$ (as an $\mathcal{O}_K$-submodule).

(c) We claim that $\mathfrak{p} = (2+\sqrt{6})$. Indeed, clearly $(2+\sqrt{6}) \subseteq (2, \sqrt{6})$. On the other hand, we have $2 = (\sqrt{6}+2)(\sqrt{6}-2) \in (2+\sqrt{6})$, and hence also $\sqrt{6} = (2+\sqrt{6}) - 2 \in (2+\sqrt{6})$. Thus $(2+\sqrt{6}) \supseteq (2, \sqrt{6})$, and we get $\mathfrak{p} = (2+\sqrt{6})$ is principal.

Exercise 5.4. Let $D \equiv 1 \pmod 4$ be a squarefree number, $D > 1$, and let $K = \mathbb{Q}(\sqrt{-D})$. Show that $\mathfrak{p} = (2, 1+\sqrt{-D})$ is not a principal ideal of $\mathcal{O}_K$.

Solution. Recall that in this case $\mathcal{O}_K = \mathbb{Z}[\sqrt{-D}]$. First, note that $\mathfrak{p} \neq \mathcal{O}_K$. Indeed, if we had $1 = 2(a+b\sqrt{-D}) + (1+\sqrt{-D})(c+d\sqrt{-D}) = (2a+c-Dd) + (2b+c+d)\sqrt{-D}$, then we would have $c - Dd \not\equiv c + d \pmod 2$, which is clearly false.

Assume that $\mathfrak{p}$ is generated by $a + b\sqrt{-D}$. Since $2 \in \mathfrak{p}$, we get that 2 is divisible by $a + b\sqrt{-D}$, so that taking the norms we get $(a^2 + Db^2)|4$. Since $D \geq 5$, we get $b = 0$, and thus $a \in \{-2, -1, 1, 2\}$.

If $a = \pm 1$, then we would have $\mathfrak{p} = \mathcal{O}_K$, but we have already checked that this is not the case. If $a = \pm 2$, then we would have $1 + \sqrt{-D} \in 2\mathbb{Z}[\sqrt{-D}]$, which is clearly impossible. Therefore, $\mathfrak{p}$ is not a principal ideal.

Exercise 5.5. Show that the ring of integers $\mathcal{O}_K$ is a unique factorization domain if and only if it is a principal ideal domain.

(*Hint: Use unique factorization of ideals in $\mathcal{O}_K$.*)

Solution. ($\Leftarrow$) First, we show that any irreducible element π is prime. Indeed, if π is not prime, then there is a nontrivial factorization $(\pi) = \mathfrak{p}_1 \dots \mathfrak{p}_k$ for some prime ideals $\mathfrak{p}_i$, and by PID property we have $\mathfrak{p}_i = (\pi_i)$ for some prime π_i. But then $\pi = u\pi_1 \dots \pi_k$ for some unit $u \in \mathcal{O}_K^\times$, contradicting the irreducibility of π.

Let a be a nonzero integer in $\mathcal{O}_K$. By unique factorization of ideals we have $(a) = \mathfrak{p}_1 \dots \mathfrak{p}_k$, and since all ideals are principal we have $(a) = (\pi_1) \dots (\pi_k)$, which gives a factorization into irreducibles. Conversely, if $a = u\pi_1' \dots \pi_l'$, then $(a) = (\pi_1') \dots (\pi_l')$ is a prime factorization of ideal (a), and by unique factorization of ideals, we get that $\{(\pi_1'), \dots, (\pi_l')\}$ is a permutation of $\{(\pi_1), \dots, (\pi_k)\}$.

($\Rightarrow$) Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$, and assume that $\mathfrak{a}$ is not principal. Recall from the lectures that $\mathfrak{a}$ can be uniquely factorized into prime ideals: $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_k$. Then one of $\mathfrak{p}_i$ is also not principal, since otherwise $\mathfrak{a}$ would be principal as a product of principal ideals. Therefore, we may assume that $\mathfrak{a} = \mathfrak{p}$ is a prime ideal.

Since $\mathfrak{p}$ is prime, for any element $a \in \mathfrak{p}$ if we write $a = u\pi_1 \dots \pi_l$ as a product of irreducibles, then one of π_i, call it π, lies in $\mathfrak{p}$. Since $\mathfrak{p}$ is not principal, $\mathfrak{p} \supsetneq (\pi)$, and therefore (π) is not a maximal ideal. We know that in $\mathcal{O}_K$ prime ideals are maximal (since it is a Dedekind domain), so (π) cannot be a prime ideal. Hence there exist elements $b, c \in \mathcal{O}_K$ such that $\pi | bc$, but π does not divide b or c. But this contradicts unique factorization, since bc has two different factorizations into irreducibles, corresponding to $bc = \pi \cdot \frac{bc}{\pi}$ and $bc = b \cdot c$, one with π (up to units), and the other without.