Solutions to Sheet 4

Exercise 1

Let $m \in \mathbb{Z} \setminus 0, 1$ be a square-free integer and set $K = \mathbb{Q}(\sqrt{m})$. Show that

$$\Delta_K = \begin{cases} m, & \text{if } m \equiv 1 \pmod 4 \\ 4m, & \text{if } m \equiv 2, 3 \pmod 4. \end{cases}$$

Solution. Recall the definition of Δ_K. In the case where K is an arbitrary number field with degree d over $\mathbb{Q}$, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of degree d. For a choice of generators $x_1, \ldots, x_n$ of $\mathcal{O}_K$ as a $\mathbb{Z}$-module, we defined

$$\Delta_K := \Delta_{K/\mathbb{Q}}(x_1, \ldots, x_n)$$

and as every choice of basis only differes by multiplication with a matrix with determinant ± 1, this does not depend on the choice of generators by Lemma 1.3.2. Hence, in order to determine Δ_K, we need to find such generators. In the situation at hand, we already know (Example 1.39) that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \frac{1+\sqrt{m}}{2}\mathbb{Z}, & \text{if } m \equiv 1 \pmod 4 \\ \mathbb{Z} + \sqrt{m}\mathbb{Z}, & \text{if } m \equiv 2, 3 \pmod 4. \end{cases}$$

This gives the desired generators. In the first case we calculate

$$\Delta_K = \Delta_{K/\mathbb{Q}}(1, \tfrac{1+\sqrt{m}}{2}) = \det \begin{pmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{pmatrix}^2 = (\sqrt{m})^2 = m.$$

In the second case we find

$$\Delta_K = \Delta_{K/\mathbb{Q}}(1, \sqrt{m}) = \det \begin{pmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{pmatrix}^2 = (-2\sqrt{m})^2 = 4m.$$

Exercise 2

Let $m \in \mathbb{Z} \setminus \{0, \pm 1\}$ be a squarefree integer. Using Eisenstein's criterion, one shows that $X^3 - m \in \mathbb{Q}[X]$ is irreducible. Let $K = \mathbb{Q}[X]/(X^3 - m)$ and write x for the image of X in K, so that $x^3 = m$. Let $z = a + bx + cx^2$. We know that $\mathrm{N}_{K/\mathbb{Q}}(z) = a^3 + mb^3 + m^2c^3 + 3mabc$.

(iii) Show that $3a, 3mb, 3mc \in \mathbb{Z}$ if $z \in \mathcal{O}_K$.

(iv) Using (*ii*) and (*iii*), show that $3z \in \mathbb{Z}[x]$ if $3 \nmid m$ and $z \in \mathcal{O}_K$.

Solution.

(iii) From the matrix we wrote down for (*ii*) we find that $\mathrm{Tr}_{K/\mathbb{Q}}(z) = 3a$. This is an integer if $z \in \mathcal{O}_K$. As $zx = mc + ax + bx^2$, we find $\mathrm{Tr}_{K/\mathbb{Q}}(zx) = 3mc$ and as $zx^2 = mb + mcx + ax^2$ we find $\mathrm{Tr}_{K/\mathbb{Q}}(zx^2) = 3mb$. We know that x lies in $\mathcal{O}_K$ because $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K, and $x \in K$ is a root of the monic polynomial $T^3 - m \in \mathbb{Z}[T]$. Hence also $zx, zx^2 \in \mathcal{O}_K$, which implies that all the traces above lie in $\mathbb{Z}$.

(iv) We basically want to show that $3\mathcal{O}_K \subset \mathbb{Z}[x]$. We encountered a similar problem on exercise 4 of the last sheet. There we used Lemma 1.3.5 from the lecture notes, which in the situation at hand tells us that

$$\Delta_{K/\mathbb{Q}}(1, x, x^2)\mathcal{O}_K = -3^3 m^2 \mathcal{O}_K \subset \mathbb{Z}[x].$$

This is not enough! From (iii) we find directly that with $z = a + bx + cx^2 \in \mathcal{O}_K$, the element $3mz = 3ma + 3mbx + 3mcx^2$ lies in $\mathbb{Z}[x]$, so we already know that $3m\mathcal{O}_K \subset \mathbb{Z}[x]$. This is better than the first inclusion, but still not enough. But we have $3a \in \mathbb{Z}$, and the only thing that could go wrong for $3b, 3c \in \mathbb{Z}$ to hold is that there may be (prime) divisors of m in the denominator of b or c, at most with multiplicity 1. Here we might try using (ii), which gives that

$$\mathbb{Z} \ni \mathrm{N}_{K/\mathbb{Q}}(3z - 3a) = \mathrm{N}_{K/\mathbb{Q}}(3bx + 3cx^2) = m(3b)^3 + m^2(3c)^3.$$

Multiplying this with m, we find

$$m^2(3b)^3 + \underbrace{(3mc)}_{\in\mathbb{Z}}{}^3 \in \mathbb{Z},$$

so that $m^2(3b)^3 \in \mathbb{Z}$, directly implying $3b \in \mathbb{Z}$ (look at the prime factorization and remember that m is square-free). Coming back to the old statement

$$\mathrm{N}_{K/\mathbb{Q}}(3bx + 3cx^2) = \underbrace{m(3b)^3}_{\in\mathbb{Z}} + m^2(3c)^3 \in \mathbb{Z},$$

we find similarly that $3c \in \mathbb{Z}$. This is what we wanted to show.

Exercise 3

Let R be a principal ideal domain. Show that R is a Dedekind domain.

Solution. This is just a matter of repeating the definition. Remember that a domain R is a Dedekind domain if it is

- noetherian,
- normal (that is, integrally closed in its field of fractions),
- and of Krull-dimension 1 (that is, every non-zero prime ideal is maximal).

The first two statements are directly verified for PIDs. Indeed, R is noetherian if and only if all of its ideals are finitely generated, and this is clear for PIDs. The second statement is true for all UFDs, in particular for PIDs. The last statement is also verified quickly: If (p) is a prime ideal which is contained by another ideal $(q) \supseteq (p)$, then there is some $r \in R$ with $rq = p$. By primality of (p), this implies $q \in (p)$ or $r \in (p)$. Now $(q) \subseteq (p)$ implies $(q) = (p)$, so let's assume $r \in (p)$. In this case we may write $r = r_0 p$, so that $pr_0 q = p$. As R is a domain we can cancel p's on both sides to find that $q \in R^\times$, i.e., $(q) = (1)$. Hence, (p) is maximal.

Max von Consbruch, email: mvconsbruch@uni-bonn.de. Date: November 6, 2023