Solutions to Sheet 7

Exercise 1

1. Let K be a number field and let $n \in \mathbb{N}$. Show that

$$a_n(K) = \#\{I \subset \mathcal{O}_K \mid I \text{ is an ideal such that } \mathrm{N}(I) = n\}$$

is finite.

2. Let $K = \mathbb{Q}(\sqrt{-3})$. Use Theorem 3.11 to determine $a_n(K)$ for all $n \in \{1, \dots, 7\}$, where we use the notation from 1.

Solution.

1. Let $I \subset \mathcal{O}_K$ be any ideal. We can write $I = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_s^{e_s}$ and obtain

$$\mathrm{N}(I) = \mathrm{N}(\mathfrak{P}_1)^{e_1} \cdots \mathrm{N}(\mathfrak{P}_s)^{e_s}.$$

Note that $p \mid \mathrm{N}(\mathfrak{P})$ if and only if $\mathfrak{P} \mid p\mathcal{O}_K$. Indeed, if $p \mid \mathrm{N}(\mathfrak{P}) = [\mathcal{O}_K : \mathfrak{P}]$, then multiplication with p^k induces the zero-endomorphism on $\mathcal{O}_K/\mathfrak{P}$, hence $p^k \in \mathfrak{P}$, implying $p \in \mathfrak{P}$, i.e., $\mathfrak{P} \mid p\mathcal{O}_K$. On the other hand, if $\mathfrak{P}$ divides $p\mathcal{O}_K$, then $\mathrm{N}(\mathfrak{P})$ divides $\mathrm{N}(p\mathcal{O}_K) = p^{[K:\mathbb{Q}]}$, and as $\mathrm{N}(\mathfrak{P}) \neq 1$ we find $p \mid \mathrm{N}(\mathfrak{P})$. But in $\mathcal{O}_K$ we have a finite decomposition $p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_n^{e_n}$. This implies that there are only finitely many prime ideals in $\mathcal{O}_K$ with norm divisible by p. But a fortiori there now are only finitely many ideals I with norm n.

2. Note that $\mathcal{O}_K = \mathbb{Z}[\beta]$ with $\beta = \frac{-1+\sqrt{-3}}{2}$, which has minimal polynomial $A(T) = T^2 + T + 1$. This implies that $[\mathcal{O}_K : \mathbb{Z}[\beta]] = 1 \notin (p)$ for any prime ideal (p) of $\mathbb{Z}$, so we can apply 3.11 without hesitation. The unit ideal is the only one with norm 1. To determine the other $a_n(K)$, we first determine the number of prime ideals that have a chance of dividing (n). Here we use 3.11. We need factorizations into irreducible factors of $T^2 + T + 1$ modulo $2, 3, 5, 7$. These are given by

- $T^2 + T + 1 \equiv T^2 + T + 1 \pmod 2$
- $T^2 + T + 1 \equiv (T-1)^2 \pmod 3$
- $T^2 + T + 1 \equiv T^2 + T + 1 \pmod 5$
- $T^2 + T + 1 \equiv (T-2)(T-5) \pmod 7$.

Theorem 3.11 now states that the we have the following prime ideals above each p:

- $\mathfrak{P}_2 = 2\mathcal{O}_K + f(\beta)\mathcal{O}_K$ above (2), its norm is $\mathrm{N}(\mathfrak{P}_2) = 2^2$.
- $\mathfrak{P}_3 = 3\mathcal{O}_K + (\beta - 1)\mathcal{O}_K$ above (3), its norm is $\mathrm{N}(\mathfrak{P}_2) = 3$.
- $\mathfrak{P}_5 = 5\mathcal{O}_K + f(\beta)\mathcal{O}_K$ above (5), its norm is $\mathrm{N}(\mathfrak{P}_2) = 5^2$.
- $\mathfrak{P}_2 = 7\mathcal{O}_K + (\beta - 2)\mathcal{O}_K$, $\mathfrak{P}_2' = 7\mathcal{O}_K + (\beta - 5)$ above (7). These ideals both have norm 7.

Here we used that if $\mathfrak{P}$ is a prime above $p \in \mathbb{Z}$, we have $\mathrm{N}(\mathfrak{P}_p) = p^{f(\mathfrak{P}|p)}$. By multiplicativity of the norm, we arrive at

$$a_2(K) = 0, \quad a_3(K) = 1, \quad a_4(K) = 1, \quad a_5(K) = 0, \quad a_6(K) = 0, \quad a_7(K) = 2.$$

Exercise 2

Let $K = \mathbb{Q}(2^{1/3})$. We know from previous exercise sheets that $[K : \mathbb{Q}] = 3$ and that $\mathcal{O}_K = \mathbb{Z}[2^{1/3}]$. Use theorem 3.11 to determine the prime ideal factorization of $2\mathcal{O}_K, 5\mathcal{O}_K$ and $7\mathcal{O}_K$.

Solution. We have seen in previous exercises that $\mathcal{O}_K = \mathbb{Z}[2^{1/3}]$. Hence we don't have do worry about divisibility constraints when using 3.11. The minimal polynomial of $2^{1/3}$ is $A(T) = T^3 - 2$. Again we need to find its factors modulo $2, 5, 7$.

- Mod 2: $\overline{A}(T) = T^3 = \overline{A}_1(T)^3$
- Mod 5: $\overline{A}(T) = (T-3)(T^2+3T+4) = \overline{A}_1(T)\overline{A}_2(T)$
- Mod 7: $\overline{A}(T) = T^3 - 2 = \overline{A}_1(T)$.

Theorem 3.11 now provides us with explicit formulas for the divisors of $p\mathcal{O}_K$:

- $2\mathcal{O}_K = \overline{A}_1(2^{1/3})\mathcal{O}_K = (2^{1/3}\mathcal{O}_K)^3$
- $5\mathcal{O}_K = (5\mathcal{O}_K + \overline{A}_1(2^{1/3})\mathcal{O}_K)(5\mathcal{O}_K + \overline{A}_2(2^{1/3})\mathcal{O}_K)$
- $7\mathcal{O}_K = 7\mathcal{O}_K + \overline{A}_1(2^{1/3})\mathcal{O}_K = 7\mathcal{O}_K$

Exercise 3

Let $P = T^3 - T^2 - 2T - 8 \in \mathbb{Z}[X]$, set $K = \mathbb{Q}[T]/P\mathbb{Q}[T]$, and let α denote the image of T in K. The reduction of P modulo 3 has no zero in $\mathbb{F}_3 = \mathbb{Z}/3$ and so is irreducible in $\mathbb{F}_3[T]$. This implies that P is irreducible in $\mathbb{Q}[T]$ (it has no roots, and every factorization contains at least one linear term, implying a root). Hence, K is a number field of degree 3. One computes that $\Delta_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = -2^2 \cdot 503$.

1. Prove that $4\alpha^{-1} \in \mathcal{O}_K$ and $\mathbb{Z} + \alpha\mathbb{Z} + 4\alpha^{-1}\mathbb{Z} \supsetneq \mathbb{Z}[\alpha]$.
2. Deduce that $(1, \alpha, 4\alpha^{-1})$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$.
3. Let $\beta \in \mathcal{O}_K$ be a primitive element of $K/\mathbb{Q}$, i.e., $K = \mathbb{Q}(\beta)$, and let $A = (a_{ij})_{1 \le i,j \le 3}$ such that
$$\beta^{i-1} = a_{i,1} + a_{i,2}\alpha + a_{i,3}\frac{4}{\alpha} \quad \text{for all } i \in \{1, 2, 3\}.$$
Show that $2 \mid \det A$ and deduce that $2 \mid [\mathcal{O}_K : \mathbb{Z}[\beta]]$.

Solution.

1. We have $4\alpha^{-1} \in K$, so it suffices to find algebraic relations for $4\alpha^{-1}$. Note that $P(\alpha) = 0$, so that
$$(4\alpha^{-1})^2 = 16\alpha^{-2} = 2(\alpha^3 - \alpha^2 - 2\alpha)\alpha^{-2} = 2\alpha - 2 - 4\alpha^{-1}.$$
In particular, $(4\alpha^{-1})^2 + 4\alpha^{-1} - 2\alpha + 2 = 0$, which is the algebraic relation we are looking for (now $4\alpha^{-1}$ is a root of the monic polynomial $T^2 + T - 2(\alpha - 1) \in \mathcal{O}_K[T]$).

For the second part, use that $4\alpha^{-1}$ lies in the left hand side, but not the right hand side (express it with $(1, \alpha, \alpha^2)$ as a $\mathbb{Q}$-linear combination to see this).

2. We calculate the discriminant of $(1, \alpha, 4\alpha^{-1})$ and compare it with $\Delta_{K/\mathbb{Q}} = -2^2 \cdot 503$. Denote by M the module given by $\mathbb{Z} + \alpha\mathbb{Z} + 4\alpha^{-1}\mathbb{Z} \subset \mathcal{O}_K$. We have that

$$\Delta_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = [M : \mathbb{Z}[\alpha]]^2 \Delta_{K/\mathbb{Q}}(1, \alpha, 4\alpha^{-1}).$$

Using the given fact that $\Delta_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = -2^2 \cdot 503$, we find that $[M : \mathbb{Z}[\alpha]] \mid 2$. Part 1 shows that $[M : \mathbb{Z}[\alpha]] \neq 1$, so we have $[M : \mathbb{Z}[\alpha]] = 2$ and $\Delta_{K/\mathbb{Q}}(1, \alpha, 4\alpha^{-1}) = -503$. The same idea reveals that

$$\Delta_{K/\mathbb{Q}}(1, \alpha, 4\alpha^{-1}) = [\mathcal{O}_K : M]^2 \Delta_{K/\mathbb{Q}},$$

but as $\Delta_{K/\mathbb{Q}} \neq 1$ this is only possible if $[\mathcal{O}_K : M] = 1$, i.e., $\mathcal{O}_K = M$. This is what we had to show.

3. We are only interested in residues mod 2, so it suffices to work out the entries of A mod 2. But to figure out the coefficients of A mod 2 is the same as working out the coordinates of the residue class of β in $\mathcal{O}_K/2\mathcal{O}_K$ (which is a 3-dimensional $\mathbb{F}_2$-vector space) with respect to the basis given by the residue classes of $(1, \alpha, 4\alpha^{-1})$. Suppose that we have

$$\beta = a + b\alpha + c(4\alpha^{-1}).$$

Then

$$\beta^2 = (a + b\alpha + c(4\alpha^{-1}))^2 \equiv a^2 + b^2\alpha^2 + c^2(4\alpha^{-1})^2 \pmod 2.$$

Note that we have

$$\alpha^2 = \frac{\alpha^3}{\alpha} = \frac{\alpha^2 + 2\alpha + 8}{\alpha} = 2 + \alpha + 2(4\alpha^{-1}) \equiv \alpha \pmod 2$$

and

$$(4\alpha^{-1})^2 = -2 + 2\alpha - 4\alpha^{-1} \equiv 4\alpha^{-1} \pmod 2.$$

Hence we find that

$$\beta^2 \equiv a^2 + b^2\alpha + c^2(4\alpha^{-1}) \pmod 2,$$

and this yields that mod 2, A is given by the matrix $\begin{pmatrix} 1 & 0 & 0 \\ a & b & c \\ a^2 & b^2 & c^2 \end{pmatrix}$, which has determinant

$$\det \begin{pmatrix} b & c \\ b^2 & c^2 \end{pmatrix} = bc^2 - cb^2 \equiv 0 \pmod 2.$$

Now we can use that

$$[\mathcal{O}_K : \mathbb{Z}[\beta]] = |\det(A)|$$

implying that $2 \mid [\mathcal{O}_K : \mathbb{Z}[\beta]]$.

Remark. In particular, part 3 shows that there is no such thing as an *integral* theorem of the primitive element: There is no primitive element $\beta \in K$ such that $\mathbb{Z}[\beta] = \mathcal{O}_K$. Number fields that satisfy this condition are called *monogenic*. According to Wikipedia, the example covered in this exercise was the first known example of a non-monogenic number field, discovered by Richard Dedekind.

Max von Consbruch, email: mvconsbruch@uni-bonn.de. Date: December 4, 2023