Solutions to Sheet 2

Exercise 1

Let $K = \mathbb{Q}(2^{1/3})$. Compute $\mathrm{N}_{K/\mathbb{Q}}(x)$ and $\mathrm{Tr}_{K/\mathbb{Q}}(x)$ for

$$x \in \{2023, 2^{1/3}, 2^{1/3} - 1, (2^{1/3} + 1)^2\}.$$

Solution. Note that $[K : \mathbb{Q}] = 3$, as K is generated as a $\mathbb{Q}$-vector space via $(1, 2^{1/3}, 2^{2/3})$. For any $x \in K$, let $\mu_x : K \to K$ denote the $\mathbb{Q}$-linear vector space endomorphism of K given by $\mu_x(\alpha) = x\alpha$. Now we have $\mathrm{N}_{K/\mathbb{Q}}(x) = \det(\mu_x)$ and $\mathrm{Tr}_{K/\mathbb{Q}}(x) = \mathrm{Tr}(\mu_x)$. We will think of K as $\mathbb{Q}^3$, by the basis given above. To calculate trace and norm, simply express μ_x with respect to this basis as a matrix, then calculate determinant and trace of the matrix obtained this way. I will not do this here.

Exercise 2

Let K/F be a finite field extension.

- Show that $\mathrm{Tr}_{K/F}(\lambda x + \mu y) = \lambda \,\mathrm{Tr}_{K/F}(x) + \mu \,\mathrm{Tr}_{K/F}(y)$ for all $x, y \in K$ and $\lambda, \mu \in F$.
- Show that $\mathrm{N}_{K/F}(xy) = \mathrm{N}_{K/F}(x)\,\mathrm{N}_{K/F}(y)$.

Solution. This also follows directly from the description of norm and trace as determinant and trace of the associated F-linear endomorphism on K. Let for any $x \in K$ $\mu_x : K \to K$ denote the corresponding F-linear maps, similar to the notation in the solution of exercise 1. Note that $\mu_{(l\mu_x + m\mu_y)} = l\mu_x + m\mu_y$ for all $x, y \in K$ and $m, l \in F$. Knowing this, the first statement becomes $\mathrm{Tr}(l\mu_x + m\mu_y) = l\,\mathrm{Tr}(\mu_x) + m\,\mathrm{Tr}(\mu_y)$, which is known from linear algebra. Similarly we find that $\mu_{xy} = \mu_x\mu_y$, so that the second statement becomes $\det(\mu_{xy}) = \det(\mu_x\mu_y) = \det(\mu_x)\det(\mu_y)$. This is also known from linear algebra.

Exercise 3

Show that $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$[1] contains infinitely many units.

Solution. If we knew Dirichlet's unit theorem, we'd directly find that $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$, where r is the number of real embeddings of $K = \mathbb{Q}(\sqrt{2})$ (which is 2), s is the number of conjugate complex embeddings (which is 0), and $\mu(K)$ is the group of roots of unity of K, which is $\mathbb{Z}/2\mathbb{Z}$. Hence we'd obtain $\mathcal{O}_K^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

In our case, a simple calculation shows that $\mathcal{O}_K^\times = \{x \in \mathbb{Z}[\sqrt{2}] \mid \mathrm{N}(x) = \pm 1\}$. Writing $x = a + \sqrt{2}b \in \mathcal{O}_K$, we have $\mathrm{N}(x) = a^2 - 2b^2$. Hence the units are in bijection with the solutions of the Pell equation $a^2 - 2b^2 = \pm 1$, and it suffices to find infinitely many solutions to $a^2 - 2b^2 = 1$. We have trivial solutions $(a, b) = (\pm 1, 0)$. But there is also the non-trivial solution

[1] I write $\mathcal{O}_K$ instead of $\mathbb{Z}[\sqrt{2}]$ because $\mathbb{Z}[\sqrt{2}]$ is the ring of integers of the Galois extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, and this notation requires less typing.

$(a,b) = (3,2)$, corresponding to $3+2\sqrt{2} \in \mathcal{O}_K^\times$. Now all powers of this element are units as well, and it is easy to see that $(3+2\sqrt{2})^k \neq 1$ for all $k \neq 0$ by taking real absolute value. Hence the set $\{(3+2\sqrt{2})^k \mid k \in \mathbb{Z}\} \subset \mathcal{O}_K^\times$ is infinite.

Exercise 4

Let A be an integral domain and let M be a finitely generated torsion-free A-module, i.e., $am = 0$ implies $a = 0$ or $m = 0$. Show that there exist $r \in \mathbb{Z}_{\geq 0}, a \in A \setminus \{0\}$ and a submodule N of M such that N is free of rank r and $aM \subseteq N$. Deduce that M is free if A is a PID.

Solution. Let $(m_1, \ldots, m_n)$ be a generating tuple for M. We begin with $i = 1$, $a_1 = 1$ and $N_1 = (m_1)$. If $N_1 = M$ we are done. Otherwise, either $m_2 \in (m_1)$, in which case $a_2(m_1, m_2) \subseteq (m_1) =: N_2$ for some $a_2 \in A$, or $m_2 \notin (m_1)$, in which case we set $N_2 \coloneqq N_1 + (m_2) = (m_1, m_2)$, which is free, and $a_2 = 1$. We continue this procedure to obtain for every $1 \leq r \leq n$ a free submodule $N_r \subseteq M$ and an integer a_r with $a_1 a_2 \cdots a_r(m_1, \ldots, m_r) \subseteq N_r$. After terminating, we set $a = a_1 \cdots a_n$ and $N = N_n$ (that's cursed) to find $a(m_1, \ldots, m_n) = aM \subseteq N$. As N is a free module, the first part of the exercise is done.

If A is additionally assumed to be a PID, the statement $aM \subseteq N$ implies that aM is free, as submodules of free modules are free. As $M \cong aM$ (multiplication by $a \in A$ is injective because M is torsion-free and surjective by construction) this implies that M is free as well.

Max von Consbruch, email: mvconsbruch@uni-bonn.de. Date: October 24, 2023