Solutions to Sheet 3

Exercise 1

1. Show that $\mathcal{O}_K^\times = \{x \in \mathcal{O}_K \mid \mathrm{N}_{K/\mathbb{Q}} = \pm 1\}$.
2. Suppose that $K = \mathbb{Q}(\sqrt{m})$ for some negative squarefree integer m. Determine $\mathcal{O}_K^\times$.

Solution.

1. We know from the lecture that for any $x \in \mathcal{O}_K$, the norm $\mathrm{N}_{K/\mathbb{Q}}(x)$ lies in $\mathbb{Z}$. It is easy to check (for example by defining the norm via the determinant) that the norm induces a homomorphism of groups $\mathrm{N}_{K/\mathbb{Q}} : \mathcal{O}_K^\times \to \mathbb{Z}^\times$. This shows that units have norm ± 1.

   For the reverse inclusion, there are at least three solutions. One could argue that for $x \in \mathcal{O}_K$ with norm ± 1, $\mu_x : \mathcal{O}_K \to \mathcal{O}_K$ (given by $\mu_x(a) = ax$) has determinant ± 1, hence is invertible as a $\mathbb{Z}$-module homomorphism. Now the inverse comes from $x^{-1} \in K$, which now has to lie in $\mathcal{O}_K$ (after some argumentation). Alternatively one can use the fact that

   $$\mathrm{N}_{K/\mathbb{Q}}(x) = \prod_\sigma \sigma(x) = x \prod_{\sigma \neq \sigma_0} \sigma(x) = \pm 1,$$

   where σ runs over all inclusions of K into its algebraic closure.

   The coolest solution (of the ones I know and in my naive opinion) uses the fact that $\mathrm{N}_{K/\mathbb{Q}}(x)$ is the 0-th coefficient of the minimal polynomial of x. The minimal polynomial yields an equation

   $$x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x \pm 1 = 0,$$

   and we find

   $$x \underbrace{\left(x^{d-1} + a_{d-1}x^{d-2} + \cdots + a_2 x + a_1\right)}_{= \mp x^{-1} \in \mathcal{O}_K} = \mp 1.$$

2. Note that $K/\mathbb{Q}$ is always an imaginary extension, so there is an embedding $K \hookrightarrow \mathbb{C}$ (well-defined up to complex conjugation) and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is given by complex conjugation. Moreover, the norm is simply given by the square of the complex absolute value. Write $x = a + b\alpha \in \mathcal{O}_K$, where $a, b \in \mathbb{Z}$ and

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

   In the first case, the norm computes as

   $$\mathrm{N}_{K/\mathbb{Q}}(a + b\alpha) = (a + b\alpha)(a + b\sigma(\alpha)) = a^2 - mb^2,$$

   where $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is the non-trivial element (acting by complex conjugation after choosing a complex embedding). In the second case we find similarly

   $$\mathrm{N}_{K/\mathbb{Q}}(a + b\alpha) = (a + b\alpha)(a + b\sigma(\alpha)) = a^2 + ab + b^2\frac{(1-m)}{4}.$$

   In both cases the norm is greater than 0 and we could try to solve the exercise by solving the equations $\mathrm{N}_{K/\mathbb{Q}}(a + b\alpha) = 1$ eplicitly. But we can save a bit of work. Let's think about K as a subfield of $\mathbb{C}$. All units of $\mathcal{O}_K$ have complex norm 1, and using the triangle inequality, we find that every such $x \in \mathcal{O}_K^\times$ must have trace $\left|\mathrm{Tr}_{K/\mathbb{Q}}(x)\right| = |x + \sigma(x)| \in \{0, 1, 2\}$ (the trace of an algebraic integer is an integer!). This condition is quite restrictive! Remember that trace and norm arise as coefficients of the characteristic polynomial of x and hence every unit $x \in \mathcal{O}_K^\times$ satisfies

$$x^2 - \mathrm{Tr}_{K/\mathbb{Q}}(x)x + \mathrm{N}_{K/\mathbb{Q}}(x) = x^2 - \mathrm{Tr}_{K/\mathbb{Q}}(x)x + 1 = 0.$$

Now there are three tracases:

- $\mathrm{Tr}(x) = \pm 2$. In this case $x^2 \mp 2x + 1 = (x \mp 1)^2$ and $x = \pm 1$.
- $\mathrm{Tr}(x) = 0$. In this case x satisfies $x^2 = -1$, hence $x = \pm \mathrm{i}$. It is easy to check that $\mathrm{i} \in \mathcal{O}_K$ iff $m = -1$.
- $\mathrm{Tr}(x) = \pm 1$. In this case x is a third or a sixth root of unity. Indeed, if $\mathrm{Tr}(x) = -1$ we find $0 = (x-1)(x^2+x+1) = x^3 - 1$, so x is a third root of unity. If $\mathrm{Tr}(x) = 1$ we find $0 = (x+1)(x^2 - x + 1) = x^3 + 1$, so x is a sixth root of unity. Note that we have already seen that $\zeta_3 \in \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$, and $\zeta_6 = \frac{1}{2} + \frac{\sqrt{-3}}{2}$ also lies in this ring of integers.[1]

Finally, it is not hard to see that two non-isomorphic quadratic number fields have trivial intersection after choosing embeddings into $\mathbb{C}$, this follows from the fact that degree-2 extensions don't have intermediate extensions. This finishes the characterization of the units the ring of integers of $\mathbb{Q}(\sqrt{m})$ for negative square-free integers m. It is given by the following subgroup of the multiplicative group of complex numbers:

$$\mathcal{O}_{\mathbb{Q}(\sqrt{m})}^\times = \begin{cases} \mathrm{i}^{\mathbb{Z}}, & \text{if } m = -1 \\ \zeta_6^{\mathbb{Z}}, & \text{if } m = -3 \\ (-1)^{\mathbb{Z}}, & \text{otherwise.} \end{cases}$$

Exercise 2

Let K and L be number fields and let $\varphi : K \to L$ be a ring homomorphism. Show that $\varphi(\mathcal{O}_K) \subset \mathcal{O}_L$.

Solution. We know that $\mathcal{O}_L$ is the integral closure of $\mathbb{Z}$ in L. This means $\mathcal{O}_L$ is the subring of elements in L that arise as roots of polynomials in $\mathbb{Z}$. The same is true for $\mathcal{O}_K$ in K. If any $x \in \mathcal{O}_K$ is a root of a monic polynomial $f_x(T) \in \mathbb{Z}[T]$. Then $\varphi(x) \in L$ is a root of f as well, as $f(\varphi(x)) = \varphi(f(x)) = 0$ (remember that any ring morphism is a homomorphism of abelian groups. In particular, φ is the identity on $\mathbb{Z}$ and thereby does not change the coefficients of f).

Exercise 3

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 (you do not need to check this). Set $K = \mathbb{Q}[X]/(X^3 - m\mathbb{Q}[X])$, we write x for the image of X in K so that $x^3 = m$.

1. Show that $\Delta_{K/\mathbb{Q}}(1, x, x^2) = -3^3 m^2$.

[1] All of this could have been done purely geometrically with points in $\mathbb{C}$, arguing purely with the conditions on trace and absolute value, without referring to the minimal polynomial.

2. Let $a, b, c \in \mathbb{Q}$. Compute $\mathrm{N}_{K/\mathbb{Q}}(a + bx + cx^2)$.

Solution.

1. The Galois group of K over $\mathbb{Q}$ is of degree 3 and generated by the morphism sending x (a primitive element of K) to $\zeta_3 x$, at least after embedding K into $\mathbb{C}$ (say). By Lemma 1.32 in the script we obtain
$$\Delta_{K/\mathbb{Q}}(1, x, x^2) = \det \begin{pmatrix} 1 & x & x^2 \\ 1 & \zeta_3 x & \zeta_3^2 x \\ 1 & \zeta_3^2 x & \zeta_3 x^2 \end{pmatrix}^2.$$
The determinant of the matrix is readily computed to $3x^3(\zeta_3^2 - \zeta_3)$, which has square $9x^6(-3) = -3^3 m^2$, as desired.

2. Let $\alpha = a + bx + cx^2$. Let B be the basis $(1, x, x^2)$ of K as a $\mathbb{Q}$ vector space. Then α sends 1 to the vectors (a, b, c), x to the vector (mc, a, b) and x^2 to the vector (mb, mc, a). We find that as a matrix with respect to B, multiplication by α is given by
$$\begin{pmatrix} a & mc & mb \\ b & a & mc \\ c & b & a \end{pmatrix},$$
and the determinant of this matrix is (hopefully)
$$a^3 + mb^3 + m^2c^3 - 3mabc.$$
This is $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$.

Exercise 4

To the right, you do not see the flag of Nepal. The ration of its height to its width is equal to a number $\alpha \in \mathbb{R}$ such that $K := \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{59 - 24\sqrt{2}})$.

1. Show that $[K : \mathbb{Q}] = 4$ and that
$$\left(1, \sqrt{59 - 24\sqrt{2}}, \sqrt{2}, \sqrt{2}\sqrt{59 - 24\sqrt{2}}\right)$$
is a $\mathbb{Q}$-basis of K.

2. Show that $\beta := (-1 + \sqrt{59 - 24\sqrt{2}}/\sqrt{2} \in \mathcal{O}_K$.

3. Set $F = \mathbb{Q}(\sqrt{2})$. Show that $2(59 - 24\sqrt{2})\mathcal{O}_K \subset \mathcal{O}_F[\beta]$.

Solution.

1. First, after squaring twice we find that α is a root of the polynomial
$$f(X) = X^4 - 118X^2 + 2329.$$
We find that f is irreducibe by seeing that there are no rational roots to f (we only have to check divisors of 2329), and the approach
$$f(X) = (aX^2 + bX + c)(dX^2 + eX + f)$$
reveals that there is no factorization.[2] This shows that $(1, \alpha, \alpha^2, \alpha^3)$ is a basis for $L/\mathbb{Q}$.

[2] Alternatively, ask Wolframalpha or smth idk.

Note that $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2})$. This shows that $(1, \alpha, \sqrt{2}, \sqrt{2}\alpha)$ is a basis too.

2. Note that $\beta^2 = 30 - 12\sqrt{2} \in \mathcal{O}_K$ and that $\beta = \sqrt{2}^{-1}(-1+\alpha) \in K$. As $\mathcal{O}_K$ in integrally closed in K, this implies that $\beta \in \mathcal{O}_K$. Indeed, $\beta \in K = \mathrm{Frac}(\mathcal{O}_K)$ is a root of the monic polynomial $T^2 - \beta^2 \in \mathcal{O}_K[T]$.

3. As $(1, \beta)$ is an F-basis for K, the lecture notes reveal the fact that

$$\Delta_{K/F}(1,\beta)\mathcal{O}_K \subseteq \mathcal{O}_F + \beta\mathcal{O}_F \subseteq \mathcal{O}_F[\beta].$$

So perhaps calculating the discriminant solves the exercise in an instant. The minimal polynomial of α over F is given by $T^2 - (59 - 24\sqrt{2}) = 0$, which shows that $\mathrm{Gal}(K/F)$ is the group of order 2 generated by the F-linear K-automorphism σ that sends α to $-\alpha$ (i.e., $\sigma(x + \alpha y) = x - \alpha y$). Writing $\beta = \frac{1-\alpha}{\sqrt{2}}$, we find that

$$\Delta_{K/F}(1,\beta) = \det\begin{pmatrix} 1 & \beta \\ 1 & \sigma(\beta) \end{pmatrix}^2 = (\sigma(\beta) - \beta)^2 = 2\alpha^2.$$

This is exactly what we needed. The result from the lecture now implies

$$\mathcal{O}_F[\beta] \supseteq \Delta_{K/F}(1,\beta)\mathcal{O}_K = 2\alpha^2\mathcal{O}_K = 2(59 - 24\sqrt{2})\mathcal{O}_K.$$