Exercises for Algebraic Number Theory
List 3 to hand in at 23.1.2017 in the exercise class

Exercise 1.
Let K be a quadratic number field and $\mathcal{O}_K$ its integers. Let $j : K \to K_\mathbb{R}$ be the embedding into the Minkowski space of K, and vol the canonical measure and vol_M the Minkowski measure. Calculate $\mathrm{vol}(\Gamma)$ and $\mathrm{vol}_M(\Gamma)$ for the lattice $\Gamma = j(\mathcal{O}_K)$.

Exercise 2.
Let V be a real vector space and Γ a subgroup of V.

1. Show that Γ is a discrete subgroup if and only if $\Gamma = \langle v_1, \dots, v_m \rangle$ for vectors $v_1, \dots, v_m \in V$ that are linearly independent over $\mathbb{R}$.
2. Show that Γ spans V over $\mathbb{R}$ if and only if there is a bounded subset $M \subset V$ such that $V = \bigcup_{\gamma\in\Gamma} \gamma + M$. Show that if Γ is a lattice in V, then any fundamental mesh Φ satisfies $V = \coprod_{\gamma\in\Gamma} \gamma + \Phi$.

Exercise 3.
Let K be an algebraic number field of degree n with integers $\mathcal{O}_K$ and discriminant d_K.

1. Show that there exists a primitive element $a \in \mathcal{O}_K$, i.e. $K = \mathbb{Q}[a]$.
2. Show that
$$d(1, a, \dots, a^{n-1}) \;=\; (\mathcal{O}_K : \mathbb{Z}[a])^2 \cdot d_K.$$
3. Conclude that $\mathcal{O}_K = \mathbb{Z}[a]$ if $d(1, a, \dots, a^{n-1})$ is squarefree.

Exercise 4.
Let K be a number field. Show that there is a unique $\mathbb{C}$-linear map $\varphi : K \otimes_\mathbb{Q} \mathbb{C} \to \prod_\tau \mathbb{C}$ with $\varphi(a \otimes 1) = (\tau(a))_\tau$ where $\tau : K \to \mathbb{C}$ ranges through all field embeddings, and that this map is an isomorphism of $\mathbb{C}$-vector spaces.

Hint: The linear independence of characters is a general fact (e.g. see [Lang: Algebra, VIII.4 Thm. 7]), which implies that the embeddings $\tau : K \to \mathbb{C}$ are linearly independent over $\mathbb{C}$.

Exercise 5.
Show that the class group of $\mathbb{Q}[\sqrt{D}]$ is trivial for $D \in \{-7, -3, -2, -1, 2, 3, 5, 13\}$.
Hint: Use the Minkowski bound, cf. Exercise 8.

Extra exercises: Calculate the class group for some other quadratic number field. Find a cubic number field with trivial class group.

*__Exercise 6.__ What is the canonical volume of the ideal $(1+i)$ of $\mathbb{Z}[i]$ inside the Minkowski space of $\mathbb{Q}[i]$? Is it equal to the Minkowski volume?

*__Exercise 7.__
Let V be an n-dimensional Euclidean space with scalar product $\langle -,-\rangle$. Let $\Phi \subset V$ be the parallelepiped spanned by the vectors $v_1,\ldots,v_n \in V$. Show that

$$\mathrm{vol}(\Phi)^2 \;=\; \big|\det\big((\langle v_i, v_j\rangle)_{i,j}\big)\big|.$$

This number is also called the *Gram determinant of* $v_1,\ldots,v_n$.

*__Exercise 8__ (Minkowski bound)__.__
Let K be a number field of degree n with r real embeddings and s pairs of complex embeddings. Let $\mathcal{O}_K$ be its integers, d_K its discriminant and $K_{\mathbb{R}}$ its Minkowski space.

1. Show that
$$X \;=\; \Big\{ (z_\tau) \in K_{\mathbb{R}} \;\Big|\; \sum_\tau |z_\tau| < t \Big\}$$
is a convex symmetric set of (canonical) volume $2^r\pi^s t^n/n!$.

2. Show that every nonzero ideal I of $\mathcal{O}_K$ contains a nonzero element a with
$$\big|N_{K/\mathbb{Q}}(a)\big| \;\leq\; M_K \cdot (\mathcal{O}_K : I)$$
where $M_K = n!/n^n(4/\pi)^s\sqrt{|d_K|}$ is the so-called *Minkowski bound for* K.
Hint: Make use of the inequality $1/n\sum|z_\tau| \geq (\prod|z_\tau|)^{1/n}$.

3. Show that every ideal class $[I] \in \mathrm{Cl}(\mathcal{O}_K)$ contains an integral ideal I_0 of norm $N(I) \leq M_K$.

4. Show that $M_K \leq (2/\pi)^s\sqrt{|d_K|}$, i.e. the Minkowski bound is better than the bound from the lecture.

*__Exercise 9__ (Elementary divisor theorem)__.__ Let A be a PID, M be a free module over A and $M' \subset M$ a finitely generated submodule. Then there exists a basis $\mathcal{B}$ of M, $b_1,\ldots,b_n \in \mathcal{B}$ and non-zero elements $a_1,\ldots,a_n \in A$ such that

1. $(a_1b_1,\ldots,a_nb_n)$ is a basis for M', and
2. $a_i | a_{i+1}$ for $i = 1,\ldots,n-1$.

The sequence of ideals $(a_n) \subset \ldots \subset (a_1)$ is uniquely determined by the previous conditions.

Hint: A proof can be found in [Lang, Algebra, III.7].

The starred exercises are not to hand in.