Exercises for Algebraic Number Theory Oliver Lorscheid
Series 5 Instituto Nacional de Matemática Pura e Aplicada
To hand in until 12.2.2015 with Emilio Peixoto Assemany or Roberto Alvarenga Jr.

Exercise 1.
Let ζ_n be a primitive n-root of unity. Show that the discriminant of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is

$$d(1,\dots,\zeta_n^{\varphi(n)-1}) \;=\; (-1)^{\varphi(n)/2}\cdot n^{\varphi(n)}\cdot \prod_{p|n} p^{-\varphi(n)/(p-1)}$$

where the product ranges over all prime numbers p dividing n.

Exercise 2.
Let A be a Dedekind domain and $K = \mathrm{Frac}A$. Let L/K be a separable field extension with normal closure N. Let B and C be the integral closures of A in L and N, respectively. Let $G = \mathrm{Gal}(N/K)$ be the Galois group of N over K and H the subgroup $H = \mathrm{Gal}(N/L)$ that fixes $L = N^H$. Let $\mathfrak{p}$ be a prime ideal of A and $\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{q}^{e_i}$ be the prime decomposition in B. Let $G_\mathfrak{q}$ be the decomposition group of $\mathfrak{q} \in \{\mathfrak{q}_1,\dots,\mathfrak{q}_r\}$ in N over K.

1. Show that
$$\begin{array}{ccc} H\setminus G\,/\,G_\mathfrak{p} & \longrightarrow & \{\mathfrak{q}_1,\dots,\mathfrak{q}_r\} \\ [\tau] & \longmapsto & \tau(\mathfrak{q}) \end{array}$$
is a well-defined bijection.

2. Let $\mathfrak{p}C = \prod \tilde{\mathfrak{q}}^{\tilde{e}}$ the prime decomposition in C, f_i be the inertia degree of $\mathfrak{q}_i$ over $\mathfrak{p}$ and $\tilde{f}$ the inertia degree of $\tilde{\mathfrak{q}}_i$ over $\mathfrak{p}$. Show that $e_i|\tilde{e}$ and $f_i|\tilde{f}$ for all i.

Exercise 3.
Let L be the normal closure of $K_3 = \mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ and $G = \mathrm{Gal}(L/\mathbb{Q})$ the Galois group of L over $\mathbb{Q}$.

1. Determine all subgroups of G and the corresponding subfields of L. What is the unique quadratic number field K_2 that is contained in L?

2. Calculate the prime decompositions of 2, 3, 5 and 7 in K_2 and recall Exercise 4.6.

3. Determine the ramification indices and the inertia degrees of 2, 3, 5 and 7 in L.

Exercise 4 (Class group calculation 1)**.**

1. Show that for $D \in \{-7,-3,-2,-1,2,3,5,13\}$, the class group of $\mathbb{Q}(\sqrt{D})$ is trivial. *Hint:* Calculate the Minkowski bound of $\mathbb{Q}(\sqrt{D})$ and use Exercise 6.

2. Show that $\mathbb{Q}(\sqrt{-5})$ has class group $\mathbb{Z}/2\mathbb{Z}$ and that $\mathbb{Q}(\sqrt[3]{2})$ has trivial class group. *Hint:* The Minkowski bound shows that it is enough to inspect in both cases the primes ideals above (2). This can be done by the same techniques as explained in Exercise 5.

Exercise 5 (Class group calculation 2)**.**
Show that the class group of $K = Q(\sqrt{-14})$ is cyclic of order 4. You can do this along the following steps:

1. Calculate the Minkowski bound M_K and conclude that the class group is generated by the prime ideals above 2 and 3.
2. Show that 2 ramifies in K, i.e. $2\mathcal{O}_K = \mathfrak{q}^2$ for a prime ideal $\mathfrak{q}_2$ of the integers $\mathcal{O}_K$ of K. Thus the class of $\mathfrak{q}_2$ has order 2 in the class group of K. Show that $a^2+14b^2 = 2$ has no integral solutions. Why does it follow that $\mathfrak{q}_2$ is not a principal ideal?
3. Show that 3 splits into two prime ideals $\mathfrak{q}_3$ and $\mathfrak{q}_3'$ in $\mathcal{O}_K$, thus $[\mathfrak{q}_3'] = [\mathfrak{q}_3]^{-1}$ in $\mathrm{Cl}(\mathcal{O}_K)$. Show that $\mathfrak{q}_3$ is not principal, using the same strategy as for $\mathfrak{q}_2$.
4. Calculate the norm of $2+\sqrt{-14}$ and show that $(2+\sqrt{-14})\mathcal{O}_K$ decomposes as $\mathfrak{q}_2\mathfrak{q}_3^2$ or $\mathfrak{q}_2(\mathfrak{q}_3')^2$. Conclude that $[\mathfrak{q}_2] = [\mathfrak{q}_3]^{\pm 2}$, that $[\mathfrak{q}_3]$ generates $\mathrm{Cl}(\mathcal{O}_K)$ and that its order is 4.

***Exercise 6** (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 7.**
Recall the proofs of all basic facts about localizations of rings and modules.

The starred exercises are not to hand in.