Exercises for Algebraic Number Theory
List 5 to hand in at 6.2.2017 in the exercise class

Exercise 1.
Let D be a squarefree integer different from 0 and 1 and let p be an odd prime number. Let $L = \mathbb{Q}(\sqrt{D})$ and B the integral closure of $\mathbb{Z}$ in L.

1. Calculate the conductor $\mathfrak{f}$ of $\mathbb{Z}[\sqrt{D}]$ and show that $\gcd((p), \mathfrak{f}) = (1)$.
2. Show that
   - p ramifies in $\mathbb{Q}(\sqrt{D})$ if and only if $p|D$;
   - p splits in $\mathbb{Q}(\sqrt{D})$ if and only if $p \nmid D$ and $\left(\frac{D}{p}\right) = 1$;
   - p is inert in $\mathbb{Q}(\sqrt{D})$ if and only if $p \nmid D$ and $\left(\frac{D}{p}\right) = -1$.

   See Exercise 6 for the definition of the Legendre symbol $\left(\frac{D}{p}\right)$.

Compare this result with Exercise 3 of List 4.

Exercise 2.
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 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 (cf. Exercise 1).
3. Determine the ramification indices and the inertia degrees of 2, 3, 5 and 7 in L (cf. Exercise 10).

Exercise 4 (Class group calculation 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 prime ideals above (2). This can be done by similar techniques as explained in Exercise 5.

Exercise 5 (Class group calculation 3)**.**
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** (Legendre symbols)**.**
For an odd prime number p and $a \in \mathbb{Z}$, we define the *Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } \overline{a} \text{ is a square in } \mathbb{F}_p^\times, \\ -1 & \text{if } \overline{a} \text{ is in } \mathbb{F}_p^\times, \text{ but not a square,} \\ 0 & \text{if } \overline{a} = 0 \text{ in } \mathbb{F}_p. \end{cases}$$

1. Show that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for $a, b \in \mathbb{Z}$.
2. Show that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

***Exercise 7** (Gaussian reciprocity law)**.** Find as many different proofs as possible (in the literature) for the Gaussian reciprocity law:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

for two different odd prime numbers p and q.

***Exercise 8.** Let K be a field and B a finite dimensional K-algebra.

1. Show that B is the direct sum of K-algebras of the form $K[T]/(f)^e$ for an irreducible polynomial $f \in K[T]$ and $e \geq 1$.
2. Show that the trace $\mathrm{Tr}_{B/K} : B \to K$ is constant 0 if f is not separable or if $e > 1$.

*__Exercise 9.__ Let A be an integral domain and $S \subset A$ a multiplicative set.

1. Show that $A = \bigcap_{\mathfrak{m} \subset A} A_{\mathfrak{m}}$ where $\mathfrak{m}$ varies through all maximal ideals of A.

2. Show that the associations $\Phi(I) = \langle I \rangle_{S^{-1}A}$ and $\Psi(J) = J \cap A$ define mutually inverse bijections

$$\left\{ \text{prime ideals } I \subset A \text{ such that } I \cap S = \emptyset \right\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \left\{ \text{prime ideals } J \subset S^{-1}A \right\}.$$

3. Show that the natural homomorphism $A/I \to S^{-1}A/\langle I \rangle_{S^{-1}A}$ of rings is an isomorphism if S has empty intersection with every ideal J of A that contains I.

*__Exercise 10.__

Let A be a Dedekind domain and $K = \text{Frac}A$. 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 $G = \text{Gal}(N/K)$ be the Galois group of N over K and H the subgroup $H = \text{Gal}(N/L)$ 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 $\mathfrak{q} \in \{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$ in N over K.

1. Show that

$$\begin{array}{ccc} H \backslash G / G_{\mathfrak{p}} & \longrightarrow & \{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\} \\ [\tau] & \longmapsto & \tau(\mathfrak{q}) \end{array}$$

   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.

The starred exercises are not to hand in.