Exercises for Algebraic Number Theory
List 4 to hand in at 30.1.2017 in the exercise class

Exercise 1 (Fundamental units)**.**
Let $D \geq 2$ be a squarefree integer and let $\mathcal{O}_K$ be the ring of integers of $K = \mathbb{Q}[\sqrt{D}]$. A *fundamental unit of* K is an element ϵ of $\mathcal{O}_K^\times$ such that $\mathcal{O}_K^\times = \{\pm\epsilon^i\}_{i\in\mathbb{Z}}$.

1. Fix an embedding $K \hookrightarrow \mathbb{R}$. Show that each of the intervals $(-\infty, -1)$, $(-1, 0)$, $(0, 1)$ and $(1, \infty)$ contains precisely one fundamental unit of K.
2. Conclude that for a unit $u = a + b\sqrt{D} \in \mathcal{O}_K^\times$, we have $u > 1$ if and only if $a, b > 0$.
3. Let $u = a + b\sqrt{D} \in \mathcal{O}_K^\times$ be a unit larger than 1 and $u^n = c + d\sqrt{D}$ with $n \geq 1$. Show that $a \leq c$ and $b \leq d$.
4. Use this to determine fundamental units for $D \in \{2, 3, 5, 6, 7, 10\}$.

Exercise 2 (Pell equation)**.**
Find all solutions $(a, b) \in \mathbb{Z}$ with $|a|, |b| \leq 200$ to the Pell equations $X^2 - 3Y^2 = 1$ and $X^2 - 5Y^2 = 1$.

Extra exercise: Show that the Pell equation $X^2 + DY^2 = 1$ has an integer solution (a, b) with $b > 0$ for every squarefree $D \geq 2$.

Exercise 3.
Let p be a prime number. Show that

- p ramifies in $\mathbb{Z}[i]$ if and only if $p = 2$;
- p splits in $\mathbb{Z}[i]$ if and only if $p \equiv 1 \pmod 4$;
- p is inert in $\mathbb{Z}[i]$ if and only if $p \equiv 3 \pmod 4$;

Hint: Use that $p = a^2 + b^2 = (a + bi)(a - bi)$ if and only if $p \equiv 1$ or $2 \pmod 4$.

Exercise 4.

1. Show that $\mathbb{Z}[\sqrt[3]{2}]$ is the ring of algebraic integers of $\mathbb{Q}(\sqrt[3]{2})$.
2. What is the conductor of $\mathbb{Z}[\sqrt[3]{2}]$ (w.r.t. $\mathbb{Z}$)?
3. Determine the prime decompositions of the ideals $2B$, $3B$, $5B$ and $7B$ in $B = \mathbb{Z}[\sqrt[3]{2}]$.

Hint: Part 1 can be solved as follows. Let $\delta = \sqrt[3]{2}$. If $f = T^3 + c_2T^2 + c_1T + c_0$ is the minimal polynomial of an element $z = a + b\delta + c\delta^2 \in \mathbb{Q}(\delta)$ with $a, b, c \in \mathbb{Q}$, then $c_2 = 3a$, $c_1 = 3a^2 - 6bc$ and $c_0 = a^3 + 2b^3 + 4c^3 - 6abc$. Consider c_2, c_1, c_0 for z, δz and $\delta^2 z$ to show that $c_2, c_1, c_0 \in \mathbb{Z}$ only if $a, b, c \in \mathbb{Z}$.

Exercise 5.
Let A be a Dedekind domain.

1. Show that given pairwise coprime ideals $I_1, \dots, I_n$ and elements $a_1, \dots, a_n \in A$, then there is an element $b \in A$ such that $b \equiv a_i \pmod{I_i}$ for $i = 1, \dots, n$. (*Hint:* Use the Chinese remainder theorem.)

2. Show that any powers of different nonzero prime ideals of I are coprime.

3. Conclude that given an ideal $I = \prod \mathfrak{p}_i^{e_i}$ of A and a nonzero $a \in I$ with $(a) = \prod \mathfrak{p}_i^{e_i'} \cdot \prod \mathfrak{q}_j^{f_j}$, there exists a $b \in I$ such that $I = (a, b)$.

***Exercise 6.**
Recall the proof of the main theorem of Galois theory.

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

***Exercise 8.**
Let A be a Dedekind domain, K its fraction field, L/K a finite separable field extension of degree n and B the integral closure of A in L. Show that B is a Dedekind domain.

***Exercise 9** (Classification of finitely generated modules over a Dedekind domain)**.** Let A be a Dedekind domain and M a finitely generated torsionfree A-module.

1. Show that there are ideal $I_1, \dots, I_n$ of A such that $M \simeq I_1 \oplus \cdots \oplus I_n$.

2. Show that $I_1 \oplus \cdots \oplus I_n \simeq J_1 \oplus \cdots \oplus J_m$ for ideals $I_1, \dots, I_n, J_1, \dots, J_m$ of A if and only if $n = m$ and if the products $I_1 \cdots I_n$ and $J_1 \cdots J_n$ represent the same class in the class group $\mathrm{Cl}(A)$ of A.

3. Conclude that the isomorphism classes of nonzero finitely generated torsionfree A-modules M correspond bijectively to pairs of a natural number $n \in \mathbb{N}$ and a class $[I] \in \mathrm{Cl}(A)$ via $M \simeq A^n \oplus I$.

4. Show more generally that every finitely generated A-module M is isomorphic to a direct sum of the form

$$A^n \oplus I \oplus A/\mathfrak{p}_1^{e_1} \oplus \cdots \oplus A/\mathfrak{p}_r^{e_r}$$

for some $n, r, e_1, \dots, e_r \geq 0$, some ideal $I \subset A$ and some non-zero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r \subset A$.

Hint: A proof can be found in [Jacobson, Basic Algebra 2, 10.6]. If A is a PID, then this is an easy consquence of the elementary divisor theorem (what are the classes of $\mathrm{Cl}(A)$ in this case?).

The starred exercises are not to hand in.