# MAT4250 EXERCISE SHEET 1

## 1. Integrality, traces and norms

**Exercise 1.** Is $\frac{1+\sqrt{8}}{2}$ an algebraic integer?

**Exercise 2.** Is the ring

$$\overline{\mathbf{Z}} = \{\alpha \in \mathbf{C} : \alpha \text{ is integral over } \mathbf{Z}\}$$

of algebraic integers noetherian?

**Exercise 3.** Suppose that $d$ is a squarefree integer, and let $K = \mathbf{Q}(\sqrt{d})$. Then

$$\mathcal{O}_K = \begin{cases} \mathbf{Z}[\sqrt{d}], & d \not\equiv 1 \pmod 4, \\ \mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d \equiv 1 \pmod 4. \end{cases}$$

**Exercise 4.** Let $k$ be a field, and let $A$ be the ring $A = k[X,Y,Z,W]/(XY - ZW)$. Let $x, y, z$ and $w$ denote the cosets of $X, Y, Z$ and $W$ in $A$. Show that $x, y, z$ and $w$ are irreducible but not prime elements.

**Exercise 5.** Let $d$ be a squarefree integer, and let $K = \mathbf{Q}(\sqrt{d})$. Compute $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha)$ and $N_{K/\mathbf{Q}}(\alpha)$ of an element $\alpha = a + b\sqrt{d} \in K$.

**Exercise 6.** In this exercise we will show that the two factorizations

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{1}$$

of the element $6 \in \mathbf{Z}[\sqrt{-5}]$ are in fact distinct in the sense that no factor is a unit multiple of another. Thus $\mathbf{Z}[\sqrt{-5}]$ is not a unique factorization domain.

(a) Show that each factor in (1) is irreducible by computing their norm.
(b) Prove that no factor on one side of (1) is an associate (= unit multiple) of one from the other side.

**Exercise 7.** Recall that if $L/K$ is a separable field extension, then the form $(x, y) = \mathrm{Tr}_{L/K}(xy)$ is nondegenerate. Show that this is no longer true if $L/K$ is inseparable, for instance by considering the fields $K = \mathbf{F}_p(X)$, $L = \mathbf{F}_p(X^{1/p})$.

**Exercise 8.**

(a) Let $L/K$ be a separable field extension, and let $\alpha_1, \ldots, \alpha_n$ be a basis for $L$ over $K$. Show that

$$d(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i \alpha_j)_{i,j})^2,$$

where the $\sigma_i$'s run over all $K$-embeddings $L \to \overline{K}$.

(b) Prove *Stickelberger's discriminant relation*: The discriminant $d_K$ of a number field $K$ satisfies $d_K \equiv 0$ or $1 \pmod 4$.

(Hint: Let $\alpha_1, \ldots, \alpha_n$ be an integral basis. In the expression for $\det(\sigma_i \alpha_j)$, let $P$ denote the sum of the terms corresponding to the even permutations, and let $N$ be the sum of the odd permutations. Then $d_K = (P - N)^2 = (P + N)^2 - 4PN$. Show that the terms in the latter expression are integers.)

**Exercise 9** (A criterion for a basis to be integral)**.** Let $K$ be a number field, and let $n = [K : \mathbf{Q}]$. According to Proposition 2.12 in Neukirch, if $\mathfrak{a} \subseteq \mathfrak{a}'$ are two fractional ideals of $K$, then the index $(\mathfrak{a}' : \mathfrak{a})$ is finite and satisfies

$$d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 d(\mathfrak{a}'). \tag{2}$$

(a) Suppose that $K = \mathbf{Q}(\alpha)$ for some $\alpha \in \mathcal{O}_K$. Use (2) to show that if $d(1, \alpha, \ldots, \alpha^{n-1})$ is squarefree, then $1, \alpha, \ldots, \alpha^{n-1}$ is an integral basis, and hence $\mathcal{O}_K = \mathbf{Z}[\alpha]$.

(b) Let $\alpha$ be a root of $f(X) = X^3 + X + 1$. Compute the ring of integers $\mathcal{O}_K$ in $K = \mathbf{Q}(\alpha)$. (Remember that the discriminant of a polynomial of the form $X^3 + pX + q$ is $-4p^3 - 27q^2$.)

## 2. Dedekind rings

**Exercise 10.** Recall that any PID is also a UFD. Show that the converse holds for any Dedekind ring.

**Exercise 11.** Prove that a noetherian integral domain $\mathcal{O}$ is a Dedekind ring if and only if $\mathcal{O}_\mathfrak{p}$ is a DVR for each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$.

(This is one of several possible definitions of a Dedekind ring. In fact, for $\mathcal{O}$ a noetherian integral domain which is not a field, the following are equivalent:

(1) $\mathcal{O}$ is a Dedekind ring.
(2) $\mathcal{O}_\mathfrak{p}$ is a DVR for all nonzero prime ideals of $\mathcal{O}$.
(3) Each nonzero proper ideal of $\mathcal{O}$ admits a unique factorization into prime ideals.
(4) Every fractional ideal of $\mathcal{O}$ is invertible.)

**Exercise 12.** In this exercise we will produce infinitely many imaginary quadratic number fields with nontrivial class group. (In fact, there are only nine imaginary quadratic number fields with *trivial* class group, namely $\mathbf{Q}(\sqrt{-d})$ for $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 167\}$.)

Let $d > 1$ be an odd squarefree integer such that $-d \not\equiv 1 \pmod 4$, and let $K = \mathbf{Q}(\sqrt{-d})$. Hence $\mathcal{O}_K = \mathbf{Z}[\sqrt{-d}]$.

(a) Show that in $\mathcal{O}_K$ we have $(2) = (2, 1 + \sqrt{-d})^2$.

(b) Show that $(2, 1 + \sqrt{-d})$ is not a principal ideal.

**Exercise 13** (Orders of ideals at primes)**.** Let $\mathfrak{a}$ be a fractional ideal of a Dedekind ring $\mathcal{O}$, and let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$. We define the *order of* $\mathfrak{a}$ *at* $\mathfrak{p}$ as

$$\operatorname{ord}_\mathfrak{p}(\mathfrak{a}) := \nu_\mathfrak{p},$$

where $\nu_\mathfrak{p}$ is the uniquely determined exponent of $\mathfrak{p}$ occuring in the prime factorization $\mathfrak{a} = \prod_\mathfrak{q} \mathfrak{q}^{\nu_\mathfrak{q}}$ of $\mathfrak{a}$. We say that $\mathfrak{a}$ has a *zero at* $\mathfrak{p}$ (written $\mathfrak{p}|\mathfrak{a}$) if $\operatorname{ord}_\mathfrak{p}(\mathfrak{a}) > 0$, or a *pole at* $\mathfrak{p}$ if $\operatorname{ord}_\mathfrak{p}(\mathfrak{a}) < 0$.

(a) Show that $\operatorname{ord}_\mathfrak{p}$ defines a discrete valuation $K^\times \to \mathbf{Z}$, $x \mapsto \operatorname{ord}_\mathfrak{p}(x)$ (where $K$ is the fraction field of $\mathcal{O}$). This means that
  (1) $\operatorname{ord}_\mathfrak{p}(xy) = \operatorname{ord}_\mathfrak{p}(x) + \operatorname{ord}_\mathfrak{p}(y)$, and
  (2) $\operatorname{ord}_\mathfrak{p}(x + y) \geq \min\{\operatorname{ord}_\mathfrak{p}(x), \operatorname{ord}_\mathfrak{p}(y)\}$.

(b) Show that $\mathfrak{a} = \mathfrak{b}$ if and only if $\operatorname{ord}_\mathfrak{p}(\mathfrak{a}) = \operatorname{ord}_\mathfrak{p}(\mathfrak{b})$ for all prime ideals $\mathfrak{p}$.

**Exercise 14.** In this exercise we aim to show that any ideal in a Dedekind ring $\mathcal{O}$ can be generated by two elements.

(a) Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be a sequence of prime ideals in the Dedekind ring $\mathcal{O}$, and let $\nu_1, \ldots, \nu_r$ be a sequence of nonnegative integers. Show that there is an element $a \in \mathcal{O}$ such that $\operatorname{ord}_{\mathfrak{p}_i}(a) = \nu_i$ for all $i = 1, \ldots, r$.

(Hint: Use that, by the Chinese remainder theorem, the natural map

$$\mathcal{O} \to \prod_i \mathcal{O}/\mathfrak{p}_i^{\nu_i + 1}$$

is surjective.)

(b) Let $\mathfrak{a}$ be a proper ideal of $\mathcal{O}$. Show that $\mathfrak{a}$ can be generated by two elements.

(Hint: By (a), there is an element $a \in \mathcal{O}$ such that $\mathrm{ord}_{\mathfrak{p}}(a) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ for all $\mathfrak{p}|\mathfrak{a}$. However, $(a)$ might have zeros at other primes. Find an appropriate element $b \in \mathcal{O}$ to remedy this.)

## 3. Lattices

**Exercise 15.**

(a) Let $K = \mathbf{Q}(\sqrt{-3})$. Draw a picture of the lattice $\Gamma$ of integers from $\mathcal{O}_K = \mathbf{Z}[\frac{1}{2}(1+\sqrt{-3})]$ in the complex plane. Mark the fundamental mesh of $\Gamma$. What is $\mathrm{vol}(\Gamma)$?

Now let $K = \mathbf{Q}(\sqrt{3})$. We can realize $\mathcal{O}_K = \mathbf{Z}[\sqrt{3}]$ as a lattice in $\mathbf{R}^2$ via the map

$$\Sigma\colon K \to \mathbf{R}^2$$

given by $\Sigma(x+\sqrt{3}y) = (x+\sqrt{3}y, x-\sqrt{3}y)$. So $\mathcal{O}_K$ is naturally a 2-dimensional object, which suggests that we should obtain accumulation points when considering it as a subset of the 1-dimensional space $\mathbf{R}$. We will show that this is indeed the case:

(b) Verify that $u = 2-\sqrt{3}$ is a unit in $\mathcal{O}_K$. Use $u$ to define a sequence of elements from $\mathcal{O}_K$ converging to $0 \in \mathbf{R}$.

(c) Show that $\mathbf{Z}[\sqrt{3}]$ is dense in $\mathbf{R}$.

**Exercise 16.** Read §5 in Neukirch.