# Solutions to Sheet 6

### Exercise 1

Let $K$ be a number field. Show that $\mathcal{O}_K$ has infinitely many prime ideals.

**Solution.** There are many ideas one could use. For example, the statement is a direct consequence of the lying over theorem for integral extensions. But we proof this mimicking Euclid's proof. Assume there is only a finite number of primes $\mathfrak{p}_1, \dots, \mathfrak{p}_n$. Let $n \in \mathbb{Z}$ be an integer such that $n\mathbb{Z} = \mathfrak{p}_1 \cdots \mathfrak{p}_n \cap \mathbb{Z}$. Now $(n+1)\mathcal{O}_K$ is a proper ideal not contained in any of the ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$. In particular, the decomposition statement of Ideals into prime ideals cannot hold. This is a contradiction, as $\mathcal{O}_K$ is a Dedekind domain.

### Exercise 2

Let $m \in \mathbb{Z}$ be negative and squarefree with $m \equiv 1 \bmod 4$ and set $K = \mathbb{Q}(\sqrt{m})$. We assume that $\mathcal{O}_K$ is a UFD (this is used in parts (ii) and (iv)).

1. Let $p$ be a prime number and $k \in \mathbb{Z}$ such that $p \mid k^2 - k + \frac{1-m}{4}$. Show that $p$ is not a prime element in $\mathcal{O}_K$.
2. Let $p$ be as in $(i)$. Show that there exists $u, v$ in $\mathcal{O}_K$ such that $p \equiv uv$ and $\mathrm{N}_{K/\mathbb{Q}}(u) = p$.
3. Let $p$ be a prime number of the form $\mathrm{N}_{K/\mathbb{Q}}(u)$ for some $u \in \mathcal{O}_K$. Show that $p \geq (1-m)/4$.
4. Suppose that $m < -3$. Deduce that every number of the form $k^2 - k + \frac{1-m}{4}$ with $0 \leq k \leq \frac{-3-m}{4}$ is prime.

**Solution.**

1. Let $\alpha = \left(\frac{1+\sqrt{m}}{2}\right)$. Then we can factor $k^2 - k + \frac{1-m}{4} = (k-\alpha)(k-\sigma(\alpha))$, where $\sigma$ is complex conjugation (in particular, $k^2 - k + \frac{1-m}{4} = \mathrm{N}_{K/\mathbb{Q}}(k-\alpha)$). We know that $(1, \alpha)$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$, and wee see that $k - \alpha, k - \sigma(\alpha) \notin p\mathcal{O}_K$. Hence $p\mathcal{O}_K$ is not a prime ideal, and $p$ is not prime.

2. We make use of the fact that $\mathcal{O}_K$ is a UFD. Let $p = q_1 \dots q_r$ be a decomposition of $p$ into (possibly repeating) irreducible factors (without units). Then $p^2 = \mathrm{N}_{K/\mathbb{Q}}(p) = \mathrm{N}_{K/\mathbb{Q}}(q_1) \cdots \mathrm{N}_{K/\mathbb{Q}}(q_r)$, and we find that $r \leq 2$. As $\mathcal{O}_K$ is a UFD, $p$ is not irreducible (prime = irreducible in UFDs). This shows that $r \geq 2$, so we have equality, and we get two elements $q_1, q_2$ with $\mathrm{N}_{K/\mathbb{Q}}(q_1) = \mathrm{N}_{K/\mathbb{Q}}(q_2) = p$.

3. Write $u = a + b\alpha$. Then

$$\mathrm{N}_{K/\mathbb{Q}}(u) = \left(a + \frac{b}{2}\right)^2 - \frac{b^2}{4}m \geq \frac{1-m}{4}.$$

Here we used that necessarily $b \neq 0$ if this is suppsed to be prime. Also, note that both terms are non-negative.

4. Suppose $p_1$ and $p_2$ are prime numbers that divide $k^2 - k + \frac{1-m}{4}$. By 2. there are $u_1, u_2$ in $\mathcal{O}_K$ such that $\mathrm{N}_{K/\mathbb{Q}}(u_i) = p_i$. In particular we find by 3. that $p \geq \frac{1-m}{4}$. Now as $m < -3$, we find that

$$p_1 p_2 \geq \left(\frac{1-m}{4}\right)^2 \leq k^2 - k + \frac{1-m}{4}.$$

The last inequality rewrites as

$$\left(\frac{1-m}{4}\right)\left(\frac{1-m}{4} - 1\right) \leq k(k-1),$$

which is only possible if $k \geq \frac{1-m}{4}$ or $k < 0$.

**Remark.** The last statement implies the funny result that $k^2 - k + 41$ is a prime for all integers $0 \leq k < 41$, as $\mathcal{O}_{\mathbb{Q}(\sqrt{-163})}$ is known to be a UFD.

## Exercise 3

Let $K$ be a number field. Let $I$ and $J$ be ideals of $\mathcal{O}_K$ and let $\sigma : K \to K$ be a field automorphism. Recall that $\sigma(\mathcal{O}_K) \subset \mathcal{O}_K$.

1. Show that $\sigma(I)$ is an ideal of $\mathcal{O}_K$.
2. Show that $\sigma(I)$ is prime if $I$ is prime.
3. Show that $\sigma(IJ) = \sigma(I)\sigma(J)$.

**Solution.**

1. For $x \in I$, $r \in \mathcal{O}_K$ we have

$$r\sigma(x) = \sigma(\sigma^{-1}(r)x) \in \sigma(I).$$

Hence $\sigma(I)$ is an ideal.

2. Same trick: If $I$ is prime and $xy \in \sigma(I)$, then $\sigma^{-1}(x)\sigma^{-1}(y) \in I$, so by primality of $I$ and without loss of generality $\sigma^{-1}(x) \in I$. But now $x \in \sigma(I)$, so $\sigma(I)$ is prime.

3. $\sigma(IJ) = \{\sigma(x)\sigma(y) \mid x \in I, y \in J\} = \sigma(I)\sigma(J)$.

## Exercise 4

Let $R$ be a Dedekind domain.

1. Let $I$ and $I_1, \ldots, I_n$ be ideals such that $I_j \nmid I$ for all $j = 1, \ldots, n$. Show that

$$I \setminus (I_1 \cup \cdots \cup I_n) \neq \emptyset.$$

2. Suppose that $R$ has at most finitely many prime ideals. Show that $R$ is a principal ideal domain.

**Solution.** The following lemma will prove useful (and is really just a weak form of 4.1):

**Lemma 1.** *Let $R$ be a Dedekind domain and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ prime ideals of $R$. Let $e_1 \ldots, e_n \in \mathbb{Z}$ be arbitrary integers. Then there is some $r \in R$ with $r \in \mathfrak{p}_j^{e_j} \setminus \mathfrak{p}_j^{e_j+1}$ for all $j$.*

*Proof.* We'll make use of the Chinese remainder theorem. We have the map

$$R \to R/(\mathfrak{p}_1^{e_1+1} \cap \ldots \mathfrak{p}_n^{e_n+1}) \cong \prod_j R/\mathfrak{p}_j^{e_j+1}.$$

Now choose non-zero elements $s_j \in \mathfrak{p}_j^{e_j}/\mathfrak{p}_j^{e_j+1} \subset R/\mathfrak{p}_j^{e_j+1}$. Any element $r$ in the preimage of

$$(s_1, \ldots, s_n) \in \prod_j R/\mathfrak{p}_j^{e_j+1}$$

works. □

1. We are in the Dedekind situation, so of course we look at the prime factorization of the Ideals at hand. Let $I = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_m^{e_m}$. Also, by the divisibility assumption, for any $j$ there is some prime ideal $\mathfrak{q}_j$ and some integer $f_j$ such that $\mathfrak{q}_j^{f_j} \mid I$, $\mathfrak{q}_j^{f_j+1} \nmid I$ and $\mathfrak{q}_j^{f_j+1} \mid I_j$. Now, there is some element $r \in R$ with $r \in \mathfrak{p}_i^{e_i}$ for all $i$ (i.e., $r \in I$) and $r \in \mathfrak{q}_j^{e_j} \setminus \mathfrak{q}_j^{e_j+1}$ (i.e., $r \notin I_j$).
2. As $R$ is a Dedekind domain, it suffices to show that all prime ideals are principal. By assumption there are only finitely many, let's call them $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. We now use lemma 1 to find an element $x \in R$ with $x \notin \mathfrak{p}_j$ for $j \neq 1$ and $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$. This forces $(x) = \mathfrak{p}_1$.