Exercise Sheet 2

Reminder about the theory:

Let K be a number field, $\mathcal{O}_K$ the ring of integers in K, and let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p} \cap \mathbb{Z} = (p)$ for a unique prime number p. The localization $\mathcal{O}_{K,\mathfrak{p}}$ is a discrete valuation ring, with maximal ideal $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} = \{\frac{a}{s} \in \mathcal{O}_{K,\mathfrak{p}};\ a \in \mathfrak{p},\ s \in \mathcal{O}_K \setminus \mathfrak{p}\}$. Let $\pi \in \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} \setminus \mathfrak{p}^2\mathcal{O}_{K,\mathfrak{p}}$, this is called a uniformizing element of $\mathcal{O}_{K,\mathfrak{p}}$, because it generates the maximal ideal $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$. The valuation $v_\mathfrak{p}\colon K \to \mathbb{Z} \cup \{\infty\}$ is defined by $v_\mathfrak{p}(0) = \infty$ and $v_\mathfrak{p}(\varepsilon\pi^m) = m$ for every $\varepsilon \in (\mathcal{O}_{K,\mathfrak{p}})^\times$ and $m \in \mathbb{Z}$.

The ramification index of $\mathfrak{p}$ over p is $e_\mathfrak{p} = e_{\mathfrak{p}/p} := v_\mathfrak{p}(p)$.

The homomorphism $\mathbb{Z} \to \mathcal{O}_K$ induces a field homomorphism $\mathbb{F}_p = \mathbb{Z}/(p) \to \mathcal{O}_K/\mathfrak{p}$. The degree $f_\mathfrak{p} = f_{\mathfrak{p}/p} := [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$ of this extension is called the residue class degree.

The ring $\mathcal{O}_K$ is a Dedekind domain, hence the ideal (p) can be uniquely decomposed into a product of nonzero prime ideals: $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. For a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, we have $p \in \mathfrak{p} \Leftrightarrow \mathfrak{p} = \mathfrak{p}_i$ for some i. Moreover $(p) \subseteq \mathfrak{p}_i^{e_i}$ but $(p) \not\subseteq \mathfrak{p}_i^{e_i+1}$ for every $i \in \{1, \ldots, r\}$.

Suppose $K = \mathbb{Q}(\alpha)$, and let $f(X) \in \mathbb{Q}[X]$ be the minimal polynomial of α over $\mathbb{Q}$. Let p be a prime number. Then $f(X)$ in $\mathbb{Q}_p[X]$ decomposes as a product of irreducible polynomials: $f(X) = \prod_{j=1}^{r_p} f_{p,j}(X)$. Here $f_{p,j} \neq f_{p,k}$ for $j \neq k$, because f is separable. The primes $\mathfrak{p}$ of $\mathcal{O}_K$ lying over p are in bijection with the factors $f_{p,j}$, because $\mathbb{Q}_p(\alpha) \cong \prod_{j=1}^{r_p} \mathbb{Q}_p(\alpha_{p,j})$, where $\alpha_{p,j}$ is a zero of the irreducible polynomial $f_{p,j}(X)$. The absolute value $|\cdot|_p$ on $\mathbb{Q}_p$ has a unique extension to $\mathbb{Q}_p(\alpha_{p,j})$. Since $K = \mathbb{Q}(\alpha) \hookrightarrow \mathbb{Q}_p(\alpha_j)$, $\alpha \mapsto \alpha_j$ is a field extension, we can pull back this absolute value to K, and we will get $|\cdot|_{\mathfrak{p}_j}$ for some prime ideal $\mathfrak{p}_j$ lying over p. Here the completion $K_{\mathfrak{p}_j}$ is in fact $\mathbb{Q}_p(\alpha_{p,j})$. So $n_{\mathfrak{p}_j} = n_{\mathfrak{p}_j/p} := [K_{\mathfrak{p}_j} : \mathbb{Q}_p] = \deg(f_{p,j})$, and clearly $\sum_{j=1}^{r_p} n_{\mathfrak{p}_j} = \sum_{j=1}^{r_p} \deg(f_{p,j}) = \deg(f) = [K : \mathbb{Q}]$.

We have $n_\mathfrak{p} = e_\mathfrak{p} f_\mathfrak{p}$, therefore $\sum_{i=1}^{r} e_{\mathfrak{p}_i/p} f_{\mathfrak{p}_i/p} = [K : \mathbb{Q}]$.

If $a \in \mathcal{O}_K$, then $(a) = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(a)}$, and $|x|_\mathfrak{p} = p^{-v_\mathfrak{p}(x)/e_\mathfrak{p}}$ for every $x \in K^\times$, where $\mathfrak{p} \cap \mathbb{Z} = (p)$. (So $|p|_\mathfrak{p} = 1/p = |p|_p$.) Since $|\mathcal{O}_K/\mathfrak{p}| = p^{f_\mathfrak{p}}$, we have $|x|_\mathfrak{p} = |\mathcal{O}_K/\mathfrak{p}|^{-v_\mathfrak{p}(x)/n_\mathfrak{p}}$.

Bitte wenden!

1. **a)** Check the formula $\sum_{i=1}^{r} e_{\mathfrak{p}_i/p} f_{\mathfrak{p}_i/p} = [K : \mathbb{Q}]$ for $K = \mathbb{Q}(\sqrt{-5})$ and $p = 2, 3, 5, 7$.

b) Check the product formula for $K = \mathbb{Q}(\sqrt{-5})$ and $x = 2, 3, 5, 7$.

2. **a)** Check the formula $\sum_{i=1}^{r} e_{\mathfrak{p}_i/p} f_{\mathfrak{p}_i/p} = [K : \mathbb{Q}]$ for $K = \mathbb{Q}(\sqrt[3]{2})$ and $p = 2, 3, 5, 7$.

b) Check the product formula for $K = \mathbb{Q}(\sqrt[3]{2})$ and $x = 2, 3, 5, 7$.

3. The aim of this exercise is to prove Stickelberger's theorem, which states that $\Delta_K \equiv 0$ or $1 \bmod 4$ for every number field K.

The determinant and permanent of a square matrix $M = (a_{i,j})_{1 \le i,j \le n}$ are defined by

$$\det(M) := \sum_{\pi \in \mathfrak{S}_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} a_{i,\pi(i)}, \qquad \operatorname{perm}(M) := \sum_{\pi \in \mathfrak{S}_n} \prod_{i=1}^{n} a_{i,\pi(i)},$$

where $\mathfrak{S}_n$ denotes the group of permutations of $\{1, \ldots, n\}$, and $\operatorname{sgn}(\pi) \in \{-1, 1\}$ is the sign of π. So the permanent's definition is similar to the determinant's, except that in the case of the permanent we omit the signs $\operatorname{sgn}(\pi)$.

Let $n = [K : \mathbb{Q}]$ and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K into $\mathbb{C}$. Let $d = \det(\sigma_i(\omega_j))$ and $d' = \operatorname{perm}(\sigma_i(\omega_j))$, where $\{\omega_1, \ldots, \omega_n\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$ (i.e. $\mathcal{O}_K = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n$).

a) Show that $d, d', \frac{d-d'}{2} \in \mathbb{C}$ are algebraic integers.

b) Show that $d' \in \mathbb{Q}$. Conclude using a) that $d' \in \mathbb{Z}$.

c) Prove that $\Delta_K = d^2 \equiv 0$ or $1 \bmod 4$, using a), b) and the fact that $\Delta_K \in \mathbb{Z}$.

4. **a)** Prove that $\mathbb{Z}[i]$ is a UFD. (Hint: Prove that it is an Euclidean domain.)

b) Prove that $\mathbb{Z}[\sqrt{2}]$ is a UFD. (Hint: Prove that it is an Euclidean domain.)

c) Let p be a prime in $\mathbb{Z}$. Show that p is irreducible in $\mathbb{Z}[i]$ if and only if $p > 2$ and $\left(\frac{-1}{p}\right) = 1$. Describe the factorization of p in $\mathbb{Z}[i]$ if $p = 2$ or $\left(\frac{-1}{p}\right) = -1$. Check that the product formula holds for $x = p$.

Siehe nächstes Blatt!

Remark: Here $\left(\frac{a}{p}\right)$ is the Legendre symbol: it is zero if $p \mid a$, otherwise if $\exists\, x \in \mathbb{Z}$ such that $x^2 \equiv a \pmod{p}$, then $\left(\frac{a}{p}\right) = 1$, while if there is no such x, then $\left(\frac{a}{p}\right) = -1$. It is known for $p > 2$ that

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Hint: If $\left(\frac{a}{p}\right) = 1$, then show that $p \mid uv$ for some $u, v \in \mathbb{Z}[i]$ such that $p \nmid u, v$. Conclude that p can not be irreducible (since $\mathbb{Z}[i]$ is a UFD).

d) Similarly to c), describe the factorization in $\mathbb{Z}[\sqrt{2}]$ of primes $p \in \mathbb{Z}$, and check that the product formula holds for $x = p$.