Homework 3 - Number Theory

Exercise 1. Let F be a number field and $\alpha \in F$ a nonzero algebraic integer of degree $n = [F : \mathbb{Q}]$. Suppose the minimal polynomial $p_{\alpha,\mathbb{Q}}(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ is Eisenstein with respect to the rational prime p ($p | a_i$ for $0 \leq i \leq n-1$ and $p^2 \nmid a_0$).

a) Show that $p | [\mathcal{O}_F : \mathbb{Z}[\alpha]]$ implies there exists an element $\xi \in \mathcal{O}_F$ such that $p\xi \in \mathbb{Z}[\alpha]$ and $\xi \notin \mathbb{Z}[\alpha]$.

b) Write $p\xi = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$ where $b_i \in \mathbb{Z}$ and let j be the smallest index $0 \leq j \leq n-1$ for which $p \nmid b_j$. Show that

$$\frac{b_j}{p}\alpha^j + \cdots + \frac{b_{n-1}}{p}\alpha^{n-1} \in \mathcal{O}_F.$$

Deduce that $N_{F/\mathbb{Q}}(\frac{b_j}{p}\alpha^{n-1}) \in \mathbb{Z}$.

c) Prove that $p \nmid [\mathcal{O}_F : \mathbb{Z}[\alpha]]$.

d) Show that (p) is totally ramified in $\mathcal{O}_F$ (only one prime lies above (p) in $\mathcal{O}_F$ and it has ramification index n).

e) Show that $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} = \mathbb{Z}[\sqrt[3]{2}]$.

f) Find the prime factorizations of (5), (7), (29) and (31) in $\mathbb{Z}[\sqrt[3]{2}]$. Compare the residue class degrees of the prime ideals lying above (5).

Exercise 2. Let α be a zero of $f(X) = X^3 + 10X + 1$ and β a zero of $g(X) = X^3 - 8X + 15$. Set $F = \mathbb{Q}(\alpha)$ and $E = \mathbb{Q}(\beta)$.

a) Show that $\mathcal{O}_F = \mathbb{Z}[\alpha]$ and $\mathcal{O}_E = \mathbb{Z}[\beta]$.

b) Find the prime factorizations of (17) in $\mathcal{O}_F$ and $\mathcal{O}_E$.

c) Conclude there exist non-isomorphic cubic number fields with the same discriminant.

d) Examples of non-isomorphic quadratic number fields with the same discriminant?

Exercise 3. **a**) Verify that $\mathbb{Z}[\sqrt{-13}]$ is not a unique factorization domain by finding two distinct factorizations of the same element.

b) In $\mathbb{Z}[\sqrt{-5}]$ let $\mathfrak{p}_1 = (2, 1+\sqrt{-5})$, $\mathfrak{p}_2 = (2, 1-\sqrt{-5})$, $\mathfrak{p}_3 = (3, 1+\sqrt{-5})$, $\mathfrak{p}_4 = (3, 1-\sqrt{-5})$. Show that $\mathfrak{p}_i$ is a maximal ideal and identify its residue field (for $1 \leq i \leq 4$). Verify the factorizations $(2) = \mathfrak{p}_1\mathfrak{p}_2$, $(3) = \mathfrak{p}_3\mathfrak{p}_4$, $(1+\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3$, $(1-\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_4$.

c) In $\mathbb{Z}[\sqrt{-3}]$ let $\mathfrak{p} = (2, 1+\sqrt{-3})$. Show that $\mathfrak{p}^2 = (2)\mathfrak{p}$, $\mathfrak{p} \neq (2)$. Does this contradict the result that in Dedekind rings every ideal admits a unique factorization into prime ideals?

Exercise 4. **a**) Suppose $\mathfrak{a} \neq 0$ is an ideal in a Dedekind ring R. Then $R/\mathfrak{a}$ has only finitely many prime ideals $\overline{\mathfrak{p}}_i$ (say $1 \leq i \leq n$) and there exist uniquely determined natural numbers e_i with the following property: For all natural numbers $e_1', \ldots, e_n'$, $\overline{\mathfrak{p}}_1^{e_1'} \cdots \overline{\mathfrak{p}}_n^{e_n'} = 0$ if and only if $e_i' \geq e_i$ for all i. Moreover, for the prime ideals $\mathfrak{p}_i \in \operatorname{Spec}(R)$ (here $\mathfrak{p}_i$ is the inverse image of $\overline{\mathfrak{p}}_i$ under the natural surjection $R \to R/\mathfrak{a}$), $\mathfrak{a} = \prod \mathfrak{p}_i^{e_i}$.

b) Learn the main ideas in the proofs of Propositions 8.2, 8.3, and Theorem 8.6.