Exercise Sheet 8
Algebraic Number Theory

November 19, 2025

Exercise 1. 1. Let $K = \mathbb{Q}(\sqrt{-30})$. Show that the factorization into prime ideals of $2O_K$ is given by

$$2O_K = \mathfrak{p}^2 \qquad \text{with} \qquad \mathfrak{p} = 2O_K + \sqrt{-30}O_K,$$

and determine likewise the prime factorization of the ideals $7O_K$ and $11O_K$.

2. Let $K = \mathbb{Q}(\sqrt{17})$. Find the prime factorization of the ideals $2O_K$ and $3O_K$.

3. Let $K = \mathbb{Q}(\sqrt{-5})$. What is the factorization into prime ideals of $(1+2\sqrt{-5})O_K$?

Exercise 2. Let A be a Dedekind ring, $Q = \mathrm{Frac}(A)$, K/Q a separable extension of degree d, B algebraic closure of A in K and $z \in B$ so that $K = Q(z)$. Let $\mathfrak{p} \subset A$ be a prime ideal so that $\mathfrak{p} | \operatorname{disc}(z)$[1] but $\mathfrak{p}^2 \nmid \operatorname{disc}(z)$. Show that

$$v_{\mathfrak{p}}(\operatorname{disc}(z)) = v_{\mathfrak{p}}(\mathfrak{D}_{B/A}).$$

Exercise 3.

Let A be a Dedekind ring with field of fractions K. Let $L_1, L_2 \subset \overline{K}$ be two finite Galois extensions of K with the property that $L_1 \cap L_2 = K$, and let $n_1 := [L_1 : K]$ and $n_2 := [L_2 : K]$. Furthermore, for $i = 1, 2$, let B_i be the integral closure of A in L_i and let

$$(z_1^{(i)}, \dots, z_{n_i}^{(i)}) \subset B_i$$

be an A-basis of B_i. Finally, set

$$d_i := \operatorname{disc}_{L_i/K}\left(z_1^{(i)}, \dots, z_{n_i}^{(i)}\right) \in A,$$

and assume that d_1 and d_2 are relatively prime (i.e. $(d_1, d_2) = (1)$ as ideals in A).

1. Let $\beta_1, \dots, \beta_{n_2} \in L_1$ be such that

$$\beta_1 z_1^{(2)} + \dots + \beta_{n_2} z_{n_2}^{(2)} \in L_1 L_2$$

is integral over A. Prove that the elements $d_2\beta_1, \dots, d_2\beta_{n_2}$ are then integral over A.

2. Deduce that the set

$$\mathcal{B} := \{z_{j_1}^{(1)} z_{j_2}^{(2)} : 1 \le j_i \le n_i\}$$

forms an A-basis for the integral closure of A in L_1L_2.

3. Prove that

$$\operatorname{disc}_{L_1L_2/K}(\mathcal{B}) = {d_1}^{n_2} {d_2}^{n_1}.$$

[1] Recall that $\operatorname{disc}(z) = \operatorname{disc}(1, z, \dots, z^{d-1})$

Exercise 4. For each positive integer $n \geq 1$, let ζ_n be a primitive n-th root of unity. The aim of this exercise is to show that the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta_n)$ is given by

$$O_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n].$$

1. Prove that $\mathbb{Q}(\zeta_{n_1}, \zeta_{n_2}) = \mathbb{Q}(\zeta_{[n_1,n_2]})$ and that $\mathbb{Z}[\zeta_{n_1}, \zeta_{n_2}] = \mathbb{Z}[\zeta_{[n_1,n_2]}]$, where $[n_1, n_2]$ denotes the least common multiple of n_1 and n_2.

2. Prove that $\mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2}) = \mathbb{Q}(\zeta_{(n_1,n_2)})$.

3. Conclude that $O_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.

   Hint: Set up an induction proof using Exercise 4, Sheet 8 and Exercise 3 of this sheet.

Exercise 5 (Complement on the cyclotomic extension)**.** Let $n \geq 1$ and let ζ_n be a primitive n-th root of unity over $\mathbb{Q}$. In this exercise, we want to show that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is an abelian Galois extension of degree $\phi(n)$.

1. Prove that there is an injective homomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^{\times}$.

2. Let $\Phi_n \in \mathbb{Q}[X]$ be the minimal polynomial of ζ_n. Show that $\Phi_n \in \mathbb{Z}[X]$, and that $\Phi_n({\zeta_n}^p) = 0$ for any prime $p \nmid n$.

3. Prove that
$$\Phi_n(X) = \prod_{\substack{a \pmod n \\ (a,n)=1}} (X - {\zeta_n}^a)\,.$$

4. Conclude that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ and that its Galois group is abelian.