Exercise Sheet 8
Algebraic Number Theory

November 12, 2025

Exercise 1. Let $K := \mathbb{Q}(\theta)$ be a number field for some algebraic integer $\theta \in \mathbb{C}$, and assume that its ring of integers is given by $O_K = \mathbb{Z}[\theta]$. Let p be a prime number. We denote by $P_\theta \in \mathbb{Z}[X]$ the minimal polynomial of θ, and by $\bar{P}_\theta \in (\mathbb{Z}/p\mathbb{Z})[X]$ its reduction mod p. Given a divisor $Q \mid \bar{P}_\theta$, we furthermore define the ideal $I(Q) \subset O_K$ to be

$$I(Q) := pO_K + F(\theta)O_K,$$

where $F \in \mathbb{Z}[X]$ is any polynomial such that $F \equiv Q \bmod p$.

1. Show that
$$O_K/I(Q) \cong (\mathbb{Z}/p\mathbb{Z})[X]/(Q),$$
and deduce that $I(Q)$ is prime if and only if Q is irreducible.

2. Write $\bar{P}_\theta$ as
$$\bar{P}_\theta = {Q_1}^{e_1} \cdots {Q_r}^{e_r},$$
where the $Q_i \in (\mathbb{Z}/p\mathbb{Z})[X]$ are pairwise distinct, irreducible, monic polynomials. Show that the prime factorization of the ideal pO_K is then given by
$$pO_K = I(Q_1)^{e_1} \cdots I(Q_r)^{e_r}.$$

Exercise 2. In this exercise we will start the proof of the Dedekind recipe I. The missing part of the proof will be given in the solutions. As in the statement let $A \subset Q$ be a Dedekind domain. Let B be the integral closure of A in a finite separable extension K of Q. We may assume $K = Q[z]$ for $z \in B$. Let $n = [K : Q]$. First we prove some preliminaries

1. Prove that for every $\mathfrak{p} \in \operatorname{spec}(A)$
$$\mathfrak{D}_{B_\mathfrak{p}/A_\mathfrak{p}} = \mathfrak{D}_{B/A,\mathfrak{p}}.$$
Hint: By $\mathfrak{D}_{B/A,\mathfrak{p}}$ we mean the localization of $\mathfrak{D}_{B/A}$ at $\mathfrak{p}$, that is $\mathfrak{D}_{B/A}A_\mathfrak{p}$. Also note recall that $A_\mathfrak{p}$ is a PID, and we have a result for the Discriminant ideal in this case.

2. Let $\mathcal{B} \subset B$. Prove that $\mathcal{B}$ is an $A_\mathfrak{p}$-basis of $B_\mathfrak{p}$ if and only if
$$v_\mathfrak{p}(\operatorname{disc}(\mathcal{B})) = v_\mathfrak{p}(\mathfrak{D}_{B/A}).$$
In particular, B is free with A-basis $\mathcal{B}$ if and only if $(\operatorname{disc}\mathcal{B}) = \mathfrak{D}_{B/A}$.
Hint: Use Exercise 3 from Sheet 7.

Next, we start the actual proof of Dedekind recipe 1, so let $P_z(X) \in A[X]$ be the minimal polynomial of z. Consider a prime $\mathfrak{p} \subseteq A$ s.t.
$$v_\mathfrak{p}(\operatorname{disc}(z)) = v_\mathfrak{p}(\mathfrak{D}_{B/A}).$$

3. Prove that $B_\mathfrak{p} \simeq A_\mathfrak{p}[X]/(P_z)$ and $\mathfrak{D}_{B/A}A_\mathfrak{p} = (\operatorname{disc}(z))A_\mathfrak{p}$.

4. Prove that the stated bijection between the ideals, that is prove that

$$\{\text{irreducible factors of } \bar{P}_z\} \to \operatorname{spec}_{\mathfrak{p}} B;\ \overline{P} \mapsto (\mathfrak{p}B_{\mathfrak{p}} \cap P(z)B_{\mathfrak{p}}) \cap B$$

is a bijection, where P is any polynomial so that $P \pmod{\mathfrak{p}} = \bar{P}$.

Hint: Show first that $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} \simeq k_{\mathfrak{p}}[X]/(\bar{P}_z)$, where $k_{\mathfrak{p}} = A/\mathfrak{p}$.

We still need to show the statement about the inertia and the ramification degrees. So let $\bar{P}$ an irreducible factor of $\bar{P}_z$ and let $\mathfrak{P} \in \operatorname{spec}_{\mathfrak{p}}(B)$ the corresponding prime ideal. Also let e be the biggest power of $\bar{P}$ that divides $\bar{P}_z$.

5. Show that for any commutative ring A and any two ideals I, J one has

$$A/(I+J) \simeq (A/I)/((I+J)/I)$$

and use it to deduce that $\deg(\bar{P}) = f_{\mathfrak{P}/\mathfrak{p}}$.

6. Recall that $B_{\mathfrak{P}}$ is principal, so write $\mathfrak{P}B_{\mathfrak{P}} = (\pi)$. Show that

$$\mathfrak{p}B_{\mathfrak{P}} = (\pi^{e^{\mathfrak{P}/\mathfrak{p}}})$$

$$e_{\mathfrak{P}/\mathfrak{p}} = \min\ \{n \in \mathbb{N} \mid \forall x \in (B_{\mathfrak{P}}/\mathfrak{p}B_{\mathfrak{P}}) \text{ not a unit} : x^n = 0\}$$

7. Show that $e = e_{\mathfrak{P}/\mathfrak{p}}$.

Hint: Write $\bar{P}_z = \prod_i \bar{P}_i^{e_i}$ Use that $B_{\mathfrak{P}}/\mathfrak{p}B_{\mathfrak{P}} \simeq \left(k_{\mathfrak{p}}[X]/(\bar{P}_z))\right)_{\mathfrak{P}}$ to find the minimal n as in the previous subexercise.

Exercise 3. Let $K/\mathbb{Q}$ be a number field of degree d, let θ be an algebraic integer of degree d, and let

$$P(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_1 X + a_0$$

be its minimal polynomial. Furthermore, suppose that P is Eisenstein with respect to the prime p, that is

$$p \mid a_j \quad \text{for} \quad 0 \le j \le n-1 \qquad \text{and} \qquad p^2 \nmid a_0.$$

The goal of this exercise is to show that then $p \nmid |O_K/\mathbb{Z}[\theta]|$.

1. Assume to the contrary that p divides $|O_K/\mathbb{Z}[\theta]|$. Show that in this case we can find $\xi \in O_K$, such that $p\xi \in \mathbb{Z}[\theta]$ and $\xi \notin \mathbb{Z}[\theta]$.

2. Write

$$p\xi = b_0 + b_1\theta + \ldots + b_{d-1}\theta^{d-1} \quad \text{with} \quad b_i \in \mathbb{Z},$$

and let j be the smallest index such that $p \nmid b_j$. Prove that $b_j\theta^{d-1} \in pO_K$.

3. Show that $N_{K/\mathbb{Q}}\left(b_j\theta^{d-1}/p\right) \notin \mathbb{Z}$.

4. Conclude by finding a contradiction.

Exercise 4. Let p be a prime, let $\ell \ge 1$, let ζ be a primitive p^ℓ-th root of unity, and let K be the cyclotomic field $K := \mathbb{Q}(\zeta)$. In this exercise we want to determine the ring of integers of K.

1. Show that

$$\Phi(X) := \frac{X^{p^\ell} - 1}{X^{p^{\ell-1}} - 1} \in \mathbb{Z}[X]$$

is the minimal polynomial of ζ.

Hint: Show that $\Phi(X+1)$.

2. Let $\xi := \zeta^{p^{\ell-1}}$. Prove that

$$\left|N_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi-1)\right| = p \quad \text{and} \quad \left|N_{K/\mathbb{Q}}(\xi-1)\right| = p^{p^{\ell-1}}.$$

3. Verify that

$$(\xi-1)\Phi'(\zeta) = p^{\ell}\zeta^{-1}.$$

4. Prove that

$$\left|\operatorname{disc}_{K/\mathbb{Q}}\left(1,\zeta,\zeta^2,\ldots,\zeta^{\phi(p^{\ell})-1}\right)\right| = p^s \quad \text{with} \quad s := p^{\ell-1}(\ell p-\ell-1).$$

5. Conclude that $O_K = \mathbb{Z}[\zeta]$.

   Hint: For prime p, you may like to consider $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta-1]]$