Exercise Sheet 8
Algebraic Number Theory

December 8, 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
$$pO_K = I(Q_1)^{e_1} \cdots I(Q_r)^{e_r}.$$

Solution. 1. From the previous Exercise Sheet, Exercise 4, we have the ideal $I(Q)/pO_K \subset O_K/pO_K$ corresponds to $(Q)/(\bar{P}_\theta) \subset \mathbb{Z}/p\mathbb{Z}[X]/(\bar{P}_\theta)$. Hence

$$O_K/I(Q) \simeq (O_K/pO_K)/I(Q)/pO_K \simeq (\mathbb{Z}/p\mathbb{Z}[X]/(\bar{P}_\theta))/((Q)/(\bar{P}_\theta)) \simeq (\mathbb{Z}/p\mathbb{Z}[X])/(Q),$$

by the isomorphism theorems.

2. By the Chinese remainder theorem we have

$$O_K/pO_K \simeq (\mathbb{Z}/p\mathbb{Z})[X]/(\bar{P}_\theta) \simeq \prod_{i=1}^{r} (\mathbb{Z}/p\mathbb{Z}[X])/(Q_i^{e_i}) \simeq \prod_{i=1}^{r} O_K/I(Q_i^{e_i}) \simeq O_K/\prod_{i=1}^{r} I(Q_i)^{e_i}$$

And this shows the desired result. Notice that $I(Q^{e_i}) = I(Q)^{e_i}$. Assume this is false and let $k \leq e_i$ be minimal so that $I(Q^k) \neq I(Q)^k$. Then $k > 1$. Notice that $I(Q)^k \subset I(Q^k)$, in fact let F so that $\overline{Q^k}$ and let $x \in \mathfrak{p}O_K$ and $a \in O_K$, then $(x + F(\theta)a)^k = \sum_{j=0}^{k} \binom{k}{j} x^{k-j} F(\theta)^j a^j = \sum_{j=0}^{k-1} \binom{k}{j} x^{k-j} F(\theta)^j a^j + F(\theta)^k a^k \in I(Q^k)$. Hence, $I(Q^k) = I(Q)^l$ for some $l < k$. However this implies, by minimality of k, that $I(Q^k) = I(Q^l)$, which then implies $Q^k = Q^l$ and this is a contradiction.

Exercise 2. In this exercise we will prove the Dedekind recipe I. 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

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

In particular, B is free with A-basis $\mathcal{B}$ if and only if $(\mathrm{disc}\,\mathcal{B}) = \mathfrak{D}_{B/A}$.

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.

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

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

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

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

is a bijection, where P is any polynomial so that $P \,(\mathrm{mod}\, \mathfrak{p}) = \bar{P}$.

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 $\mathfrak{P} \in \mathrm{spec}_\mathfrak{p}(B)$ 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

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

and that

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

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.

Solution. We denote $d = [K : Q]$.

1. We have

$$\mathfrak{D}_{B_\mathfrak{p}/A_\mathfrak{p}} = \langle \mathrm{disc}_{K/Q}\left(\frac{z_1}{q_1}, \ldots, \frac{z_d}{q_d}\right)\ \mid z_i \in B, q_i \in A \smallsetminus \mathfrak{p}\rangle$$

and

$$\mathfrak{D}_{B/A,\mathfrak{p}} = \langle \frac{1}{q}\,\mathrm{disc}_{K/Q}(z_1, \ldots, z_d) \mid q \in A \smallsetminus \mathfrak{p}, z_1, \ldots, z_d \in B\rangle$$

Notice that $\mathrm{disc}_{K/Q}\left(\frac{z_1}{q_1}, \ldots, \frac{z_d}{q_d}\right) = \frac{1}{q_1 \cdots q_d}\,\mathrm{disc}_{K/Q}(z_1, \ldots, z_d)$. The equality of the two sets is now clear.

2. As $A_\mathfrak{p}$ is a PID, we know that

$$\mathfrak{D}_{B_\mathfrak{p}/A_\mathfrak{p}} = \mathrm{disc}(\mathcal{E}).A_\mathfrak{p}$$

for any $A_\mathfrak{p}$-basis $\mathcal{E}$ of $B_\mathfrak{p}$ (Proposition 2.14 in the lecture notes). In particular, if $\mathcal{B}$ is an $A_\mathfrak{p}$-basis of $B_\mathfrak{p}$, then

$$\mathrm{disc}(\mathcal{B}).A_\mathfrak{p} = \mathfrak{D}_{B_\mathfrak{p}/A_\mathfrak{p}} = \mathfrak{D}_{B/A}.A_\mathfrak{p}$$

and hence, by unique prime factorization of ideals in $A_\mathfrak{p}$ and using that $\mathfrak{p}.A_\mathfrak{p}$ is the unique non-zero prime ideal, we find that

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

So suppose now that

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

Hence,

$$\begin{aligned}\operatorname{disc}(\mathcal{B}).A_\mathfrak{p} &= (\mathfrak{p}.A_\mathfrak{p})^{v_\mathfrak{p}(\operatorname{disc}(\mathcal{B}))} = (\mathfrak{p}.A_\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{D}_{B/A})} \\ &= \mathfrak{D}_{B/A}.A_\mathfrak{p} = \mathfrak{D}_{B_\mathfrak{p}/A_\mathfrak{p}}.\end{aligned}$$

Let $\mathcal{E}$ be an $A_\mathfrak{p}$-basis of $B_\mathfrak{p}$. Let $M \in \operatorname{Mat}_n(A_\mathfrak{p})$ be the matrix that express $\mathcal{B}$ as linear combinations of $\mathcal{E}$. Then $\operatorname{disc}(\mathcal{B}) = \det(M)^2 \operatorname{disc}(\mathcal{E})$. However we have by assumption that

$$\operatorname{disc}(\mathcal{B})A_\mathfrak{p} = \mathfrak{D}_{B_\mathfrak{p}/A_\mathfrak{p}} = \operatorname{disc}(\mathcal{E}).A_\mathfrak{p}$$

and so we deduce that $\det(M) \in A_\mathfrak{p}^\times$, that is $\mathcal{B}$ is a $A_\mathfrak{p}$-basis.

We turn to the last claim. Suppose first that B is free with A-basis $\mathcal{B}$. In particular, $\mathcal{B}$ is an $A_\mathfrak{p}$-basis for every prime ideal $\mathfrak{p}$. Hence, $v_\mathfrak{p}(\mathfrak{D}_{B/A}) = v_\mathfrak{p}(\operatorname{disc}(\mathcal{B}))$ and so by the uniqueness of the factorization we deduce that $(\operatorname{disc}(\mathcal{B})) = \mathfrak{D}_{B/A}$.

For the opposite implication, suppose that $\big(\operatorname{disc}(\mathcal{B})\big) = \mathfrak{D}_{B/A}$. Then, in particular, $v_\mathfrak{p}\big(\operatorname{disc}(\mathcal{B})\big) = v_\mathfrak{p}\big(\mathfrak{D}_{B/A}\big)$ for all non-zero primes $\mathfrak{p} \in \operatorname{Spec}(A)$ and thus $\mathcal{B}$ is an $A_\mathfrak{p}$-basis of $B_\mathfrak{p}$ for every non-zero $\mathfrak{p} \in \operatorname{Spec}(A)$. By Sheet 8 Exercise 2 it follows that B is a free A-module and, as shown there in the proof, $\mathcal{B}$ is an A-basis of B.

3. Recall that $\operatorname{disc}(z) = \operatorname{disc}(1, \dots, z^{n-1})$. From the second point we have, that $(1, \dots, z^{n-1})$ is a $A_\mathfrak{p}$-basis of $B_\mathfrak{p}$. In particular, $B_\mathfrak{p} = A_\mathfrak{p}[z] \simeq A_\mathfrak{p}[X]/(P_z)$. Also, since ideals in $A_\mathfrak{p}$ are uniquely defined by their $v_\mathfrak{p}$-valutation, it is clear that $(\operatorname{disc}(z))A_\mathfrak{p} = \mathfrak{D}_{B/A}A_\mathfrak{p}$.

4. We have $B_\mathfrak{p} = A_\mathfrak{p}[z]$. Hence we can use Exercise Sheet 7, Exercise 4 (in the notation of the exercise, $B = B_\mathfrak{p}$ and $A = A_\mathfrak{p}$) we have

$$B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} \simeq (A_\mathfrak{p}/pA_\mathfrak{p})[X]/(P_z \,(\operatorname{mod} \mathfrak{p}A_\mathfrak{p})),$$

where we momentarily denote $P_z \,(\operatorname{mod} A_\mathfrak{p})$ the image of $A_\mathfrak{p}[X] \ni P_z \mapsto P_z \,(\operatorname{mod} \mathfrak{p}A_\mathfrak{p}) \in A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}[X]$. From the class we canonically have $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \simeq A/\mathfrak{p}$ induced by the map $A \hookrightarrow A_\mathfrak{p} \to A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ and under this map $P_z \,(\operatorname{mod} \mathfrak{p}A_\mathfrak{p})$ to $\bar{P}_z$. Hence we get the desired isomorphism

$$B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} \simeq k_\mathfrak{p}[X]/(\bar{P}_z),$$

which concretely takes a polynomial $\bar{P} \in k_\mathfrak{p}[X]$, take a $P \in A[X]$ that maps onto $\bar{P}$, and maps $[\bar{P}] \in k_\mathfrak{p}[X]/(\bar{P}_z)$ to $P(\alpha) + \mathfrak{p}B_\mathfrak{p} \in B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$.

In particular, we have restricting to prime ideals, that

$$\{ \text{ irreducible factors of } \bar{P}_z\} \to \operatorname{spec}(B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p});\ \bar{P} \mapsto (P(\alpha)B_\mathfrak{p} + \mathfrak{p}B_\mathfrak{p})/\mathfrak{p}B_\mathfrak{p}.$$

Also, the set $\operatorname{spec}(B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p})$ is in natural bijection with the set of prime ideals $\mathfrak{P}$ of $B_\mathfrak{p}$ so that $\mathfrak{p}B_\mathfrak{p} \subset \mathfrak{P}$ and the latter is in bijection with the set $\operatorname{spec}_\mathfrak{p}(B)$, more concretely

$$\begin{aligned}\operatorname{spec}(B_\mathfrak{p}/\ \mathfrak{p}B_\mathfrak{p}) &\longrightarrow \operatorname{spec}_{\mathfrak{p}B_\mathfrak{p}}(B_\mathfrak{p}) \longrightarrow \operatorname{spec}_{\mathfrak{p}B}(B) \\ \bar{I} &\longmapsto I + \mathfrak{p}B_\mathfrak{p} \longmapsto (I + \mathfrak{p}B_\mathfrak{p}) \cap B,\end{aligned}$$

where I is any ideal so that its image under $B_\mathfrak{p} \to B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$ is $\bar{I}$. In particular, we get the desired bijection.

5. The first assertion is classical from Isomorphism theorems and we actually used it already repeatedly. The inertia degree $f_{\mathfrak{P}/\mathfrak{p}}$ is the degree of the extension $B/\mathfrak{P}B$ over $A/\mathfrak{p}A$. Let $P \in A[X]$ that maps to $\bar{P} \in k_\mathfrak{p}[X]$, then

$$B/\mathfrak{P}B = B/(\mathfrak{p}B + P(z)B) \simeq (B/\mathfrak{p}B)/(\mathfrak{p}B + P(z)B)/\mathfrak{p}B \simeq (k_\mathfrak{p}[X]/(\bar{P}_z))/(\bar{P}) \simeq k_\mathfrak{p}[X]/(\bar{P}).$$

By classical field theory, the right hand side is a field extension of degree $\deg(\bar{P})$ of $k_\mathfrak{p}$ and so the claim.

6. Write $\mathfrak{p}B = \prod_{\mathfrak{P}' \neq \mathfrak{P} \in \mathrm{spec}_{\mathfrak{p}}(B)} \mathfrak{P}'^{e_{\mathfrak{P}'/\mathfrak{p}}} \mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}}$, then

$$\mathfrak{p}B_{\mathfrak{P}} = \prod_{\mathfrak{P}' \neq \mathfrak{P} \in \mathrm{spec}_{\mathfrak{p}}(B)} \mathfrak{P}'^{e_{\mathfrak{P}'/\mathfrak{p}}} B_{\mathfrak{P}} \mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}} B_{\mathfrak{P}} = \mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}} B_{\mathfrak{P}} = (\pi^{e_{\mathfrak{P}/\mathfrak{p}}}),$$

where the secon equality comes from the fact that for $\mathfrak{P}' \neq \mathfrak{P}$, then $\mathfrak{P}' B_{\mathfrak{P}} = B_{\mathfrak{P}}$ (since it contains invertible elements).

Let $n < e_{\mathfrak{P}/\mathfrak{p}}$, π is not a unit in $B_{\mathfrak{P}}/\mathfrak{p}B_{\mathfrak{P}}$, since $\pi^{e_{\mathfrak{P}/\mathfrak{p}}} = 0$ and $\pi^n \notin \mathfrak{p}B_{\mathfrak{P}}$ and so $e_{\mathfrak{P}/\mathfrak{p}} \leq \min\{n \in \mathbb{N} \mid \forall x \in (B_{\mathfrak{P}}/\mathfrak{p}B_{\mathfrak{P}}) \text{ not a unit} : x^n = 0\}$. The other inequality is easy verified as well.

7. We conclude by showing that

$$e = e_{\mathfrak{P}/\mathfrak{p}}$$

using the above characterization. We have that

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

Note that localization commutes with taking quotients i.e.

$$B_{\mathfrak{P}}/\mathfrak{p}B_{\mathfrak{P}} \simeq (B/\mathfrak{p}B)_{\mathfrak{P}}$$

and you have seen that

$$B/\mathfrak{p}B \simeq B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}.$$

We have then that

$$B_{\mathfrak{P}}/\mathfrak{p}B_{\mathfrak{P}} \simeq (B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}})_{\mathfrak{P}} \simeq \left(k_{\mathfrak{p}}[X]/(\overline{P_z})\right)_{\mathfrak{P}} = (k_{\mathfrak{p}}[X]/(\overline{P}_z))_{(\overline{P})}$$

Applying the Chinese Remainder Theorem finally shows that

$$B_{\mathfrak{P}}/\mathfrak{p}B_{\mathfrak{P}} \simeq \left(\prod_{\bar{Q}} k_{\mathfrak{p}}[X]/(\bar{Q}^{e_Q})\right)_{(\overline{P})} \simeq \prod_{\bar{Q}} (k_{\mathfrak{p}}[X]/\bar{Q}^{e_Q})_{(\overline{P})},$$

where the product is taken over all irreducible factors $\bar{Q}|\bar{P}_z$. Notice that for $\bar{Q} \neq \bar{P}$ we have $(k_{\mathfrak{p}}[X]/\overline{Q}^{e_q})_{(\bar{P})}$ is 0, in fact $\bar{Q}^{e_i} \notin (\bar{P})$ and $1 \cdot \bar{Q}^{e_Q} = 0 \in k_{\mathfrak{p}}[X]/(\bar{Q}^{e_Q})$ so $1 \equiv 0 \in (k_{\mathfrak{p}}[X]/(\bar{Q}^{e_Q}))_{\bar{P}}$. Hence

$$B_{\mathfrak{P}}/\mathfrak{p}B_{\mathfrak{P}} \simeq (k_{\mathfrak{p}}[X]/\bar{P}^e)_{(\bar{P})} \simeq k_{\mathfrak{p}}[X]/(\bar{P}^e).$$

We can conclude using 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

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

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.

Solution. 1. By Cauchy's theorem there must exist $\xi \in O_K$ such that its equivalence class $\xi + \mathbb{Z}[\theta]$ is of order p in $O_K/\mathbb{Z}[\theta]$. In other words, we have $\xi \notin \mathbb{Z}[\theta]$ but $p\xi \in \mathbb{Z}[\theta]$.

2. Since $p\xi \in \mathbb{Z}[\theta]$, we can write it in the form

$$p\xi = b_0 + b_1\theta + \ldots + b_{d-1}\theta^{d-1}$$

for some $b_0, \ldots, b_{d-1} \in \mathbb{Z}$. Furthermore note that not all b_i are divisible by p, since otherwise we would have $\xi \in \mathbb{Z}[\theta]$. So there is a smallest index j such that $p \nmid b_j$. Then we can write $b_j\theta^{d-1}$ in the following way,

$$b_j\theta^{d-1} = \left(p\xi - b_0 - \ldots - b_{j-1}\theta^{j-1}\right)\theta^{d-j-1} - \left(b_{j+1} + \ldots + b_{d-1}\theta^{j-d-2}\right)\theta^d.$$

By definition of b_j we have

$$p\xi - b_0 - b_1\theta - \ldots - b_{j-1}\theta^{j-1} \in pO_K,$$

and since P is Eisenstein at p we also have

$$\theta^d = -a_{d-1}\theta^{d-1} - \ldots - a_1\theta - a_0 \in pO_K.$$

Thus

$$b_j\theta^{d-1} \in pO_K,$$

as we wanted to show.

3. We have

$$N_{K/\mathbb{Q}}\left(\frac{b_j\theta^{d-1}}{p}\right) = \frac{{b_j}^d}{p^d}N_{K/\mathbb{Q}}(\theta)^{d-1} = \frac{{b_j}^d{a_0}^{d-1}}{p^d} \notin \mathbb{Z},$$

since $p \nmid b_j$ and $p^2 \nmid a_0$.

4. As we have shown in 2, $b_j\theta^{d-1}/p \in O_K$ and thus

$$N_{K/\mathbb{Q}}\left(\frac{b_j\theta^{d-1}}{p}\right) \in \mathbb{Z}.$$

This obviously contradicts the result we have shown in 3. Hence we can conclude that p does not divide $|O_K/\mathbb{Z}[\theta]|$.

Exercise 4. Let p be a prime, let $\ell \geq 1$, 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 $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta - 1]]$

Solution. 1. First of all note that

$$\Phi(X) = 1 + X^{p^{\ell-1}} + X^{2p^{\ell-1}} + X^{3p^{\ell-1}} + \ldots + X^{(p-1)p^{\ell-1}},$$

so $\Phi(X)$ is indeed a polynomial in $\mathbb{Z}[X]$ of degree $\phi(p^\ell) = p^{\ell-1}(p-1)$. Now, since ζ is a primitive p^ℓ-th root of unity, we have that

$$\zeta^{p^\ell} = 1 \qquad \text{and} \qquad \zeta^{p^{\ell-1}} \neq 1,$$

and thus

$$\Phi(\zeta) = \frac{\zeta^{p^\ell} - 1}{\zeta^{p^{\ell-1}} - 1},$$

which shows that ζ is indeed a root of $\Phi(X)$.

In order to show irreducibility, we will apply Eisenstein's criterion on the polynomial $\Phi(X+1)$. Let $\overline{\Phi}(X) \in \mathbb{F}_p[X]$ be the reduction of $\Phi(X)$ mod p. Because of

$$X^{p^j} = (X+1)^{p^j} - 1 \quad \text{for} \quad j \geq 0$$

in $\mathbb{F}_p[X]$, it follows that

$$\overline{\Phi}(X+1)X^{p^{\ell-1}} = \overline{\Phi}(X+1)((X+1)^{p^{\ell-1}} - 1) = (X+1)^{p^\ell} - 1 = X^{p^\ell},$$

and thus

$$\overline{\Phi}(X+1) = X^{(p-1)p^{\ell-1}}.$$

This shows that all but the leading coefficients of the polynomial $\Phi(X+1)$ are divisible by p. Furthermore, a direct calculation shows that the constant coefficient of $\Phi(X+1)$ is equal to p. Hence we can apply the Eisenstein criterion and we see that $\Phi(X+1)$ is indeed irreducible. By consequence, so is $\Phi(X)$.

2. By what we have shown in 1, the minimal polynomial of ξ (which is a p-th root of unity) over $\mathbb{Q}$ is given by

$$1 + X + X^2 + \ldots + X^{p-1}.$$

Thus the minimal polynomial of $\xi - 1$ is

$$1 + (X+1) + (X+1)^2 + \ldots + (X+1)^{p-1},$$

and since the constant coefficient of this polynomial is equal to p, we get

$$N_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi - 1) = p.$$

Using this result we can also deduce

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\xi - 1) = N_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi - 1)^{[\mathbb{Q}(\zeta):\mathbb{Q}(\xi)]} = p^{p^{\ell-1}},$$

where we have made use of the fact that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\xi)] = p^{\ell-1}$.

3. We have

$$(X^{p^{\ell-1}} - 1)\Phi(X) = X^{p^\ell} - 1$$

which by taking the derivative with respect to X gives

$$p^{\ell-1}X^{p^{\ell-1}-1}\Phi(X) + (X^{p^{\ell-1}} - 1)\Phi'(X) = p^\ell X^{p^\ell - 1}.$$

The identity in question follows immediately by evaluating both sides at ζ.

4. By Sheet 6 Exercise 1 we have

$$\left|\operatorname{disc}_{K/\mathbb{Q}}\left(1,\zeta,\zeta^2,\ldots,\zeta^{\phi(p^\ell)-1}\right)\right| = N_{K/\mathbb{Q}}(\Phi'(\zeta)).$$

so that by the identity proven in 3,

$$\left|\operatorname{disc}_{K/\mathbb{Q}}\left(1,\zeta,\zeta^2,\ldots,\zeta^{\phi(p^\ell)-1}\right)\right| = N_{K/\mathbb{Q}}\left(\frac{p^\ell}{\zeta(\xi-1)}\right) = \frac{N_{K/\mathbb{Q}}(p^\ell)}{N_{K/\mathbb{Q}}(\zeta)N_{K/\mathbb{Q}}(\xi-1)}.$$

Noting that

$$N_{K/\mathbb{Q}}(p^\ell) = p^{\ell\phi(p^\ell)}, \qquad N_{K/\mathbb{Q}}(\zeta) = 1 \qquad \text{and} \qquad N_{K/\mathbb{Q}}(\xi-1) = p^{p^{\ell-1}}$$

the identity in question follows.

5. Let B be a basis of O_K, and let M be the matrix representing the tuple

$$1,\zeta,\zeta^2,\ldots,\zeta^{\phi(p^\ell)-1}$$

in this basis. Then we have the relation

$$\operatorname{disc}_{K/\mathbb{Q}}\left(1,\zeta,\zeta^2,\ldots,\zeta^{\phi(p^\ell)-1}\right) = (\det M)^2 \operatorname{disc}_{K/\mathbb{Q}}(B).$$

We have

$$|\det(M)| = |O_K/\mathbb{Z}[\zeta]|,$$

and by 4,

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

for some positive integer s. Together this shows that the only prime divisor of $|O_K/\mathbb{Z}[\zeta]|$ is p.

On the other hand, as shown in 1, the polynomial $\Phi(X+1)$ satisfies the Eisenstein condition at p. It follows that p does not divide

$$\left|O_{\mathbb{Q}(\zeta-1)}/\mathbb{Z}[\zeta-1]\right|,$$

and since obviously $\mathbb{Q}(\zeta-1) = \mathbb{Q}(\zeta)$ and $\mathbb{Z}[\zeta-1] = \mathbb{Z}[\zeta]$, we see that p does also not divide $|O_K/\mathbb{Z}[\zeta]|$. So, we must have

$$|O_K/\mathbb{Z}[\zeta]| = 1,$$

or, in other words, $O_K = \mathbb{Z}[\zeta]$.