Solutions to Exercise Sheet 9
Algebraic Number Theory

December 9, 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 $(1 + 2\sqrt{-5})O_K$?

Solution. 1. Since $-30 \equiv 2 \bmod 4$, the ring of integers is given by $O_K = \mathbb{Z}[\sqrt{-30}]$. The minimal polynomial of $\sqrt{-30}$ is given by

$$P(X) = X^2 + 30.$$

We now look one by one at the different ideals and apply the Dedekind recipe.

<u>$2O_K$:</u> We have that the reduction mod 2 of P is simply given by

$$\overline{P}(X) = X^2.$$

Thus

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

<u>$7O_K$:</u> Here the reduction mod 7 of P is

$$\overline{P}(X) = X^2 + 2.$$

Since 2 is not a square mod 7 this polynomial must be irreducible and we see that $7O_K$ is already prime.

<u>$11O_K$:</u> This time the reduction mod 11 of P is

$$\overline{P}(X) = X^2 + 8 = (X + 5)(X + 6),$$

so that

$$11O_K = \mathfrak{p}_1\mathfrak{p}_2$$

with

$$\mathfrak{p}_1 = 11O_K + (\sqrt{-30} + 5)O_K \quad \text{and} \quad \mathfrak{p}_2 = 11O_K + (\sqrt{-30} + 6)O_K.$$

2. Since $17 \equiv 1 \bmod 4$, we have that the ring of integers is given by $O_K = \mathbb{Z}[\theta]$ with $\theta = (1+\sqrt{17})/2$. The minimal polynomial of θ over $\mathbb{Q}$ is given by

$$P(X) = X^2 - X - 4.$$

Since $K = \mathbb{Q}(\theta)$ we can again directly applying Dedekind recipe.

<u>$2O_K$:</u> The reduction mod 2 of P is

$$\overline{P}(X) = X^2 - X = X(X - 1),$$

and hence

$$2O_K = \mathfrak{p}_1\mathfrak{p}_2$$

with

$$\mathfrak{p}_1 = 2O_K + \frac{\sqrt{17}+1}{2}O_K \quad \text{and} \quad \mathfrak{p}_2 = 2O_K + \frac{\sqrt{17}-1}{2}O_K.$$

$\underline{3O_K}$: Here the reduction mod 3 of P is given by

$$\overline{P}(X) = X^2 - X - 1,$$

which is irreducible in $(\mathbb{Z}/3\mathbb{Z})[X]$. Thus $3O_K$ is prime.

3. The idea is to use the identity

$$(1+2\sqrt{-5})(1-2\sqrt{-5}) = (21) = (3)(7).$$

Let us first determine the prime factorizations of the ideals (3) and (7), again by applying Dedekind recipe. Since $-5 \equiv 3 \bmod 4$, we have $O_K = \mathbb{Z}[\sqrt{-5}]$. The minimal polynomial of $\sqrt{-5}$ is obviously given by $P(X) = X^2 + 5$.

$\underline{3O_K}$: The reduction of $P(X)$ mod 3 is

$$\overline{P}(X) = X^2 - 1 = (X+1)(X-1),$$

and hence

$$3O_K = \mathfrak{p}_1\mathfrak{p}_2$$

with

$$\mathfrak{p}_1 = 3O_K + (\sqrt{-5}+1)O_K \quad \text{and} \quad \mathfrak{p}_2 = 3O_K + (\sqrt{-5}-1)O_K.$$

$\underline{7O_K}$: The reduction of $P(X)$ mod 7 is

$$\overline{P}(X) = X^2 - 9 = (X+3)(X-3),$$

and hence

$$7O_K = \mathfrak{p}_3\mathfrak{p}_4$$

with

$$\mathfrak{p}_3 = 7O_K + (\sqrt{-5}+3)O_K \quad \text{and} \quad \mathfrak{p}_4 = 7O_K + (\sqrt{-5}-3)O_K.$$

From this we see that the prime factorization of $21O_K$ is given by

$$21O_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4.$$

Furthermore, we obviously have

$$1+2\sqrt{-5} = 3\cdot(-3) + (\sqrt{-5}-1)\cdot(-2\sqrt{-5}) \in \mathfrak{p}_2,$$

and

$$1-2\sqrt{-5} = 3\cdot(-3) + (\sqrt{-5}+1)\cdot(-2\sqrt{-5}) \in \mathfrak{p}_1,$$

and hence

$$\mathfrak{p}_2 \mid (1+2\sqrt{-5})O_K \qquad \text{and} \qquad \mathfrak{p}_1 \mid (1-2\sqrt{-5})O_K. \tag{1}$$

Similarly, we see that

$$1+2\sqrt{-5} = 7\cdot 1 + (\sqrt{-5}-3)\cdot 2 \in \mathfrak{p}_4,$$

and

$$1-2\sqrt{-5} = 7\cdot 1 + (\sqrt{-5}+3)\cdot(-2) \in \mathfrak{p}_3,$$

which means that

$$\mathfrak{p}_4 \mid (1+2\sqrt{-5})O_K \qquad \text{and} \qquad \mathfrak{p}_3 \mid (1-2\sqrt{-5})O_K. \tag{2}$$

In view (1) and (2), it follows that the factorization of $(1+2\sqrt{-5})O_K$ into prime ideals must be given by

$$(1+2\sqrt{-5})O_K = \mathfrak{p}_2\mathfrak{p}_4 = \big(3O_K + (\sqrt{-5}-1)O_K\big)\cdot\big(7O_K + (\sqrt{-5}-3)O_K\big).$$

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

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

Solution. Let $\mathcal{E}$ be an $A_{\mathfrak{p}}$-basis of $B_{\mathfrak{p}}$ (recall that $A_{\mathfrak{p}}$ is a PID). Let $M \in \mathrm{Mat}_d(A_{\mathfrak{p}})$ the matrix that express $(1, \dots, z^{d-1})$ with respect to the basis $\mathcal{E}$. Then

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

and $\operatorname{disc}(z) = \det(M)^2 \operatorname{disc}(\mathcal{E})$. However since $\mathfrak{p}^2 \nmid (\operatorname{disc}(z))$ we deduce that $\det(M)$ is a $A_{\mathfrak{p}}$-unit, and so $\operatorname{disc}(z) A_{\mathfrak{p}} = \mathfrak{D}_{B/A} A_{\mathfrak{p}}$, that is, the evaluation of the two ideals at $\mathfrak{p}$ is equal.

Exercise 3.

Let A be a Dedekind 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 suppose that

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

are 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
$$\beta_1 z_1^{(2)} + \ldots + \beta_{n_2} z_{n_2}^{(2)} \in L_1 L_2$$
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
$$\mathcal{B} := \{z_{j_1}^{(1)} z_{j_2}^{(2)} : 1 \leq j_i \leq n_i\}$$
forms an A-basis for the integral closure of A in $L_1 L_2$.

3. Prove that
$$\operatorname{disc}_{L_1 L_2/K}(\mathcal{B}) = {d_1}^{n_2} {d_2}^{n_1}.$$

Solution.

1. Write $\mathrm{Gal}(L_1L_2/L_1) = \{\sigma_1^{(2)}, \dots, \sigma_{n_2}^{(2)}\}$ (notice the cardinality is n_2 since $\mathrm{Gal}(L_1L_2/L_1) \simeq \mathrm{Gal}(L_2/K)$, where the map goes by restriction). Consider the matrix $D = (\sigma_i^{(2)}(z_j^{(2)}))_{1 \leq i,j \leq n_2}$, then
$$D \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_{n_2} \end{pmatrix}$$
is a vector whose coordinate $\sum_{j=1}^{n_2} \sigma_i^{(2)}(z_j^{(2)})\beta_j = \sigma_i(\sum_{j=1}^{n_2} \beta_j z_j^{(2)})$ are all integral over A. Also, D is invertible and its inverse is given by $\frac{1}{\det(D)} \operatorname{coadj}(D)$ and also $d_2 = \det(D)^2$. Therefore
$$\begin{pmatrix} d_2\beta_1 \\ \vdots \\ d_2\beta_{n_2} \end{pmatrix} = \det(D) \operatorname{coadj}(D) \begin{pmatrix} \sigma_1(\sum_{j=1}^{n_2} \beta_j z_j^{(2)} \\ \vdots \\ \sigma_{n_2}(\sum_{j=1}^{n_2} \beta_j z_j^{(2)})). \end{pmatrix}$$
The entries of $\operatorname{coadj}(D)$ are polynomial in the entries of D, which are integral over A (since $z_i^{(2)}$ are). Hence we deduce that $d_2\beta_i$ are all integral over A

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

2. $\mathcal{B}$ is a K-basis of L_1L_2. Let $z \in O_{L_1L_2/K}$ be an integral element. Then we can write

$$z = \sum_{\substack{1\le j_1\le n_1\\1\le j_2\le n_2}} a_{j_1,j_2} z_{j_1}^{(1)} z_{j_2}^{(2)}$$

with $a_{j_1,j_2} \in K$. We want to show that each $a_{j_1,j_2} \in A$. Let $\beta_{j_2} = \sum_{1\le j_1\le n_1} a_{j_1,j_2} z_{j_1}^{(1)} \in L_1$, then $d_2\beta_{j_2}$ is integral over A. In particular, since $(z_1^{(1)}, \dots, z_{n_1}^{(1)})$ is an integral basis of B_1 over A we deduce that $d_2 a_{j_1,j_2} \in B_1$ for every j_1, j_2.

Similarly if we set $\beta'_{j_1} = \sum_{1\le j_2\le n_2} a_{j_1,j_2} z_{j_2}^{(2)}$ we see that $d_1\beta'_{j_1} \in L_2$ is integral over A and again as before $d_1 a_{j_1,j_2} \in B_2$ is integral over A. Since $(d_1, d_2) = 1$, then $1 \in (d_1) + (d_2)$ and so $1 = md_1 + nd_2$ for some $m, n \in A$. Then $a_{j_1,j_2} = (md_1 + nd_2)a_{j_1,j_2}$ is integral over A and since A is integrally closed in K we see that $a_{j_1,j_2} \in A$.

3. This is a general fact about tensor product of linear maps: suppose V and W are finite dimensional K-vector spaces and T_V and T_W endomorphisms of V and W respectively. Then $\det(T_V \otimes T_W) = \det(T_V)^{\dim W} \det(T_W)^{\dim V}$. In fact, notice that $T_V \otimes T_W = (T_V \otimes I_{\dim W}) \circ (I_{\dim V} \otimes T_W)$ and $(T_V \otimes I_{\dim W})$ can be represented by a block diagonal matrix with $\dim W$-many blocks and each block is (a representation of) T_V.

I will let you figure out why this solves the problem.

Exercise 4. For each positive integer $n \ge 1$, 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.

Solution. 1. We can choose explicit primitive roots $\zeta_{n_i} = e^{\frac{2\pi i}{n_i}}$. We have $(n_1, n_2)[n_1, n_2] = n_1 n_2$ Then $\zeta_{[n_1,n_2]}^{\frac{n_1}{(n_1,n_2)}} = \zeta_{n_2}$. Hence, we deduce that $\mathbb{Z}[\zeta_{n_2}] \subset \mathbb{Z}[\zeta_{[n_1,n_2]}]$ and by symmetry $\mathbb{Z}[\zeta_{n_1}] \subset \mathbb{Z}[\zeta_{[n_1,n_2]}]$. For the other inclusion, let $m_1, m_2 \in \mathbb{Z}$ so that $m_1n_1 + m_2n_2 = (n_1, n_2)$. Then $\zeta_{[n_1,n_2]} = \zeta_{n_1}^{m_2}\zeta_{n_2}^{m_1}$. This shows that $\mathbb{Z}[\zeta_{[n_1,n_2]}] \subset \mathbb{Z}[\zeta_{n_1}, \zeta_{n_2}]$. The same prove show also the equality of the fields.

2. The extension $\mathbb{Q}_{\zeta_{(n_1,n_2)}}$ is of degree $\varphi((n_1, n_2))$ (see next exercise) over $\mathbb{Q}$ and it is contained in $\mathbb{Q}(\zeta_{n_1})$ and $\mathbb{Q}(\zeta_{n_2})$. Indeed we have for $\zeta_{n_1}^{\frac{n_1}{(n_1,n_2)}} = \zeta_{(n_1,n_2)}$. We try to compute the degree extension $\mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2})/\mathbb{Q}$. First notice that we have,

$$[\mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2}) : \mathbb{Q}(\zeta_{n_1})] = [\mathbb{Q}(\zeta_{n_2}) : \mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2})].$$

This is seen by the fact that the map

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2})/\mathbb{Q}(\zeta_{n_1})) \to \mathrm{Gal}(\mathbb{Q}(\zeta_{n_2})/\mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2}));\ \sigma \mapsto \sigma|_{\mathbb{Q}(\zeta_{n_2})}$$

is an isomorphism.[2] In particular, we get

$$\begin{aligned}
[\mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2}) : \mathbb{Q}] &= \frac{[\mathbb{Q}(\zeta_{n_1}) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_{n_1}) : \mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2})]} \\
&= \frac{\varphi(n_1)}{[\mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2}) : \mathbb{Q}(\zeta_{n_2})]} \\
&= \frac{\varphi(n_1)[\mathbb{Q}(\zeta_{n_2}) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_{n_1}\zeta_{n_2}) : \mathbb{Q}]} = \frac{\varphi(n_1)\varphi(n_2)}{\varphi([n_1, n_2])}.
\end{aligned}$$

[2] Ask on the forum if you don't see why.

Since φ is a multiplicative function we have

$$\frac{\varphi(n_1)\varphi(n_2)}{\varphi([n_1, n_2])} = \varphi(n_1, n_2)$$

and so we deduce that $\mathbb{Q}(\zeta_{(n_1,n_2)}) = \mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2})$.

3. Write $n = \prod_{k=1}^{m} p^{j_k}$. We proceed by induction on the number of prime divisors m. In particular, we claim that for every $n \geq 1$ we have $O_{\mathbb{Q}_{\zeta_n}} = \mathbb{Z}[\zeta_n]$ and if $p|\operatorname{disc}(\zeta_n) \Leftrightarrow p|n$. The induction hypothesis $n = 1$, that is $m = 0$, is trivially true. Suppose now $m \geq 1$. We have $\mathbb{Q}(\zeta_{n/p_m^{j_m}}) \cap \mathbb{Q}(\zeta_{p_m^{j_m}}) = \mathbb{Q}$ and $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n/p_m^{j_m}})\mathbb{Q}(\zeta_{p_m^{j_m}})$. Also, by induction hypothesis $\operatorname{disc}(\mathbb{Q}(\zeta_{n/p_m^{j_m}}))$ and $\operatorname{disc}(\mathbb{Q}(\zeta_{p_m^{j_m}}))$ are coprime and so by the previous exercise and the induction hypothesis again $O_{\mathbb{Q}(\zeta_n)} = O_{\mathbb{Q}(\zeta_{n/p_m^{j_m}})} O_{\mathbb{Q}(\zeta_{p_m^{j_m}})} = \mathbb{Z}[\zeta_{n/p_m^{j_m}}]\mathbb{Z}[\zeta_{p_m^{j_m}}] = \mathbb{Z}[\zeta_n]$.

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 $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$.
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
$$\Phi_n(X) = \prod_{\substack{a \,(\mathrm{mod}\, n)\\ (a,n)=1}} (X - {\zeta_n}^a)\,.$$
4. Conclude that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ and that its Galois group is abelian.

Solution. 1. Let $\sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Then $\sigma(\zeta_n)$ is again a primitive n'th root of unity. Hence $\sigma(\zeta_n) = \zeta_n^k$ for some $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. Since ζ_n generates the group of n'th roots of unity, σ is uniquely determined by k. The map sending σ to k is evidently a morphism.

2. By definition $\Phi_n|(X^n - 1)$. Both polynomials are monic and so $\Phi_n \in \mathbb{Z}[X]$ by Gauss Lemma. Write $\Phi_n Q = X^n - 1$. Let $p \nmid n$ and suppose $\Phi(\zeta_n^p) \neq 0$. Then $Q(\zeta_n^p) = 0$. Consider the polynomial $Q_p(X) = Q(X^p)$. Then ζ_n is a root of Q_p and so $Q_p = \Phi_n Q'$. Taking the projection modulo p we have then
$$\overline{\Phi_n Q'} = \overline{Q_p} = \overline{Q}^p.$$
Let $x \in \overline{\mathbb{F}_p}$ be a root of $\overline{\Phi_n}$, then $(X - x)|\overline{Q}$ and so $(X - x)^2|\overline{X^n - 1}$. However since $(p, n) = 1$, the polynomial $X^n - 1$ has only simple roots, contradiction. Hence we deduce that ζ_n^p is a root of Φ_n.

3. Let a be an integer so that $(a, n) = 1$. We prove that ζ_n^a is a root of Φ_n. Notice that is it sufficient to prove it for positive integers a, so suppose $a \geq 1$ and write $a = p_1^{j_1} \cdots p_m^{j_m}$. We proceed by induction on $M = \sum_{i=1}^{m} j_i$. If $M = 0$, then $a = 1$ and the claim is true trivially. Suppose $M > 0$ and let $b = \frac{a}{p_m}$, then by induction hypothesis $\Phi_n(\zeta^b) = 0$. By literally the same proof as in the previous point we deduce that $\Phi_n(\zeta^a) = \Phi_n((\zeta^b)^p) = 0$. This proves the claim.

We have then
$$\prod_{\substack{a \,(\mathrm{mod}\, n)\\ (a,n)=1}} (X - \zeta_n^a)|\Phi_n(X) \in \mathbb{Q}(\zeta_n)[X].$$

On the other hand, by the first point, we see that $\deg(\Phi_n) \leq \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ and so we deduce the desired equality.

4. We see that $\deg(\Phi_n) = \varphi(n)$ and so we deduce the desired degree of the Extension. Also, we see that the map in the first point is surjective and so the Galois group $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.