Exercise Sheet 7
Algebraic Number Theory

November 5, 2025

Exercise 1. Let A be a Dedekind ring with field of fractions K. Let $L = K(\theta)$ with $[L : K] = d$ and let $a \in A$. Prove that

$$\mathrm{disc}_{L/K}(1, \theta, ..., \theta^{d-1}) = \mathrm{disc}_{L/K}(1, (\theta - a), ..., (\theta - a)^{d-1}).$$

Exercise 2. The goal of this exercise is to show that the ring of integers of $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$ is not monogeneous, i.e. $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for all $\alpha \in \mathcal{O}_K$. Let $\alpha \in O_K$ and Let $f \in \mathbb{Z}[X]$ be its minimal polynomial. For any $g \in \mathbb{Z}[X]$ we denote by $\overline{g}$ the image of g under the unique ring morphism $\mathbb{Z}[X] \to \mathbb{F}_3[X]$ which maps $X \mapsto X$ and $\mathbb{Z} \ni a \mapsto a \,(\mathrm{mod}\, 3)$.

1. Let $g \in \mathbb{Z}[X]$. Show that 3 divides $g(\alpha)$ in $\mathbb{Z}[\alpha]$ if and only if $\overline{f}$ divides $\overline{g}$ in $\mathbb{F}_3[X]$.
2. We now assume that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Consider the following four elements of $\mathcal{O}_K$

$$\alpha_1 = (1 + \sqrt{7})(1 + \sqrt{10})$$
$$\alpha_2 = (1 + \sqrt{7})(1 - \sqrt{10})$$
$$\alpha_3 = (1 - \sqrt{7})(1 + \sqrt{10})$$
$$\alpha_4 = (1 - \sqrt{7})(1 - \sqrt{10}).$$

   Show that all products $\alpha_i \alpha_j$ $(i \neq j)$ are divisible by 3 in $\mathbb{Z}[\alpha]$, but 3 does not divide any power of α_i.

   Hint: Show that $\alpha_i^n/3$ is not in $\mathcal{O}_K$ by considering its trace: Show that

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i^n) = \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n$$

   and show that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i^n)$ is congruent modulo 3 (in $\mathbb{Z}[\alpha]$) to

$$(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^n = 4^n.$$

3. Let $\alpha_i = f_i(\alpha)$, $f_i \in \mathbb{Z}[X]$ for all $i = 1, 2, 3, 4$. Show that $\overline{f} \mid \overline{f_i f_j}$ $(i \neq j)$ in $\mathbb{F}_3[X]$ but $\overline{f} \nmid \overline{f_i}^n$. Conclude that for all i it exists an irreducible factor of $\overline{f}$ (in $\mathbb{F}_3$) that does not divide $\overline{f_i}$ but divides all $\overline{f_j}$, $i \neq j$.
4. Part c) shows that $\overline{f}$ has at least four irreducible factors in $\mathbb{F}_3$. Argue why this contradicts the fact that f is of degree at most 4.
5. Conclude that O_K is not monogeneous.

Exercise 3. Let A be a Dedekind ring with field of fractions K. Let L/K be a finite, separable field extension, and let B be the integral closure of A in L. Let $\mathcal{B}$ be a K-basis of L contained in B. Finally, let M be the free A-module generated by $\mathcal{B}$, and let $\iota : M \to B$ be the canonical injection into B.

1. Prove that $\mathcal{B}$ is an A-basis of B if and only if it is an $A_\mathfrak{p}$-basis of $B_\mathfrak{p}$ for every $\mathfrak{p} \in \mathrm{spec}(A)$.

2. Prove that if A is a principal ideal domain, then

$$\det(\iota)^2 \mathfrak{D}_{B/A} = (\mathrm{disc}_{L/K}(\mathcal{B})).$$

Hint: you can assume the existence of aligned bases for free finitely generated modules over PID. That is, there exist $(b_j)_{1\leq j\leq d}$ a basis of B as A-module and $(a_j)_{1\leq j\leq d} \in A$ so that $(a_j b_j)_{1\leq j\leq d}$ is a basis of M.

3. Show that if A is a principal ideal domain and $\mathfrak{p} \in \mathrm{spec}(A)$, then $\mathcal{B}$ is an $A_\mathfrak{p}$-basis of $B_\mathfrak{p}$ if and only if $\mathfrak{p} \nmid (\det(\iota))$.

4. We do not assume that A is a PID anymore. Show that if $(\mathrm{disc}_{L/K}(\mathcal{B}))$ is a squarefree ideal, then $\mathcal{B}$ is an A-basis of B.

Exercise 4. Let A be a Dedekind ring, K its field of fractions, and $\overline{K}$ be an algebraic closure of K. Let $\alpha \in \overline{K}$ be integral over A, $P_\alpha \in A[X]$ be its minimal polynomial, and set $B := A[\alpha]$. Moreover, let $\mathfrak{p}$ be a prime ideal of A, and denote by $\overline{P_\alpha} \in (A/\mathfrak{p})[X]$ the image of P_α under the natural projection $A[X] \to (A/\mathfrak{p})[X]$.

The aim of this exercise is to show that there is bijective correspondence between the ideals of B containing $\mathfrak{p}$ and the monic factors of $\overline{P_\alpha}$.

1. Let $Q \in (A/\mathfrak{p})[X]$ be a divisor of $\overline{P_\alpha}$. Choose $F \in A[X]$ such that $\overline{F} = Q$, and define

$$I(Q) := \mathfrak{p}B + F(\alpha)B \subset B.$$

Prove that $I(Q)$ is well-defined, i.e. that it does not depend on the specific choice of F.

2. Show that the evaluation map $e_\alpha : A[X] \to B$, $f \mapsto f(\alpha)$ induces an isomorphism

$$B \cong A[X]/(P_\alpha),$$

that is, show that if $f \in A[X]$ is so that $f(\alpha) = 0$, then $P_\alpha | f$ already in $A[X]$.

Hint: Write $f = P_\alpha \cdot h$ for some $h \in K[X]$. To show that $h \in A[X]$ first show that $h \in A_\mathfrak{q}[X]$ for any prime ideal $\mathfrak{q} \in \mathrm{spec}(A)$. Then try to show $A = \bigcap_{\mathfrak{q}\in\mathrm{spec}(A)} A_\mathfrak{q}$.

3. Consider the following surjective maps

$$B/\mathfrak{p}B \leftarrow B \overset{e_\alpha}{\leftarrow} A[X] \to (A/\mathfrak{p})[X] \to (A/\mathfrak{p})[X]/(\overline{P_\alpha}),$$

and prove that we have a ring isomorphism

$$B/\mathfrak{p}B \cong (A/\mathfrak{p})[X]/(\overline{P_\alpha}).$$

Furthermore, verify that if $Q \in (A/\mathfrak{p})[X]$ is a divisor of $\overline{P_\alpha}$, the ideal $(Q)/(\overline{P_\alpha})$ corresponds to the ideal $I(Q)/\mathfrak{p}B$ under this isomorphism.

4. Conclude that the map $Q \mapsto I(Q)$ gives a bijection between the monic factors of $\overline{P_\alpha}$ and the ideals in B containing $\mathfrak{p}$ in such a way that $Q' \mid Q$ if and only if $I(Q) \subset I(Q')$.