Autumn Semester 2019

Introduction to Algebraic Number Theory

Lecturer: Prof. Dr. Özlem Imamoglu
Coordinator: Dr. Danylo Radchenko

Solutions to Exercise Sheet 4

Exercise 4.1. A ring R is called Noetherian if every ideal of R is finitely generated. Show that the following conditions are equivalent:

(i) R is Noetherian;

(ii) every ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ stabilizes (i.e. there exists n such that $I_n = I_{n+1} = \dots$);

(iii) Every non-empty set of ideals has a maximal element.

Solution. (i)⇒(ii): Consider the set $I = \bigcup_{k\geq 1} I_k$. If $a, b \in I$, then there exists k such that $a, b \in I_k$, hence $-a, a+b \in I_k \subseteq I$ and thus I is an additive subgroup of R. Similarly, if $a \in I$, and $r \in R$, then there exists k such that $a \in I_k$, and since I_k is an ideal, $ra \in I_k \subseteq I$. Thus I is an ideal in R. Since R is Noetherian, there exists a finite set of generators $a_1, \dots, a_l \in I$. Then for some n we have $a_1, \dots, a_l \in I_n$, and therefore $I \subseteq I_n$. Since we also have $I_n \subseteq I$, this implies $I_n = I_{n+1} = \dots = I$.

(ii)⇒(iii): Assume that some set of ideals $\mathcal{I}$ does not have a maximal element. Pick any ideal $I_1 \in \mathcal{I}$. Since I_1 is not maximal, there exists some ideal $I_2 \in \mathcal{I}$ such that $I_1 \subsetneq I_2$. Since I_2 is not maximal, there exists $I_3 \in \mathcal{I}$ such that $I_2 \subsetneq I_3$. Repeating this we obtain an ascending chain $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$ that does not stabilize, contradicting the assumption (ii).

(iii)⇒(i): Let $I \subseteq R$ be an ideal, and consider the set $\mathcal{I}$ of all finitely-generated ideals $J \subseteq I$. Let J be a maximal element of $\mathcal{I}$. If $J \subsetneq I$, then there is $a \in I \smallsetminus J$, but this contradicts the maximality of J, since the ideal $J + (a) \subseteq I$ is also finitely-generated and it strictly contains J. Thus $J = I$ is finitely generated. Since I was arbitrary, R is Noetherian.

Exercise 4.2. Let $K = \mathbb{Q}(\alpha)$, where $\alpha^3 - \alpha - 2 = 0$. (We assume that it is known that the polynomial $x^3 - x - 2$ is irreducible.)

(a) Compute the discriminant of $\{1, \alpha, \alpha^2\}$;

(b) Let $\Lambda = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 \subseteq \mathcal{O}_K$. Use the discriminant to show that $|\mathcal{O}_K/\Lambda| \leq 2$;

(c) Prove that $\frac{\alpha}{2}$, $\frac{\alpha^2}{2}$, and $\frac{\alpha^2+\alpha}{2}$ are not algebraic integers. Conclude that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Solution. (a) Let $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbb{Q}}$. We have $\mathrm{Tr}(1) = 3$, $\mathrm{Tr}(\alpha) = 0$, and, since α^2 is a solution of $x^3 - 2x^2 + x - 4 = 0$, $\mathrm{Tr}(\alpha^2) = 2$. Using this we compute

$$\mathrm{d}(1, \alpha, \alpha^2) \;=\; \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) \\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) \\ \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) & \mathrm{Tr}(\alpha^4) \end{pmatrix} \;=\; \det \begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & 6 \\ 2 & 6 & 2 \end{pmatrix} \;=\; -104\,.$$

(b) Recall that $\mathrm{disc}(\Lambda) = \mathrm{disc}(\mathcal{O}_K)|\mathcal{O}_K/\Lambda|^2$. By part (a) we have $\mathrm{disc}(\Lambda) = -104$. Since $|\mathcal{O}_K/\Lambda|^2$ must divide $104 = 2^3 \cdot 13$, we have that $|\mathcal{O}_K/\Lambda|$ is either 1 or 2, as claimed.

(c) Since $0 = \alpha^3 - \alpha - 2 = 8(\alpha/2)^3 - 2(\alpha/2) - 2$, we have that the minimal polynomial of $\alpha/2$ is $x^3 - x/4 - 1/4$.

Similarly, we have $(\alpha^2/2)^2 = (\alpha^2 + 2\alpha)/4$ and $(\alpha^2/2)^3 = (\alpha^2 + 4\alpha + 4)/8$, therefore, the minimal polynomial of $\alpha^2/2$ is $x^3 - x^2 + x/4 - 1/2$.

Finally, from $(\alpha^2 + \alpha)^2/4 = (\alpha^2 + 2\alpha + 2)/2$ and $(\alpha^2 + \alpha)^3/8 = (5\alpha^2 + 7\alpha + 6)/4$ we get that the minimal polynomial of $(\alpha^2 + \alpha)/2$ is $x^3 - x^2 - 3x/2 - 1/2$.

Therefore, $\frac{\alpha}{2}$, $\frac{\alpha^2}{2}$, and $\frac{\alpha^2+\alpha}{2}$ are not algebraic integers.

Now assume that $\omega \in \mathcal{O}_K \smallsetminus \mathbb{Z}[\alpha]$. By part (b) we must have $\omega = \frac{a+b\alpha+c\alpha^2}{2}$, where $a, b, c \in \mathbb{Z}$. Replacing ω by $\omega - \lfloor a/2 \rfloor - \lfloor b/2 \rfloor \alpha - \lfloor c/2 \rfloor \alpha^2$, we may assume that a, b, and c are in $\{0, 1\}$. Since $\mathrm{Tr}(\omega) = \frac{3}{2}a + c \in \mathbb{Z}$, we have that $2|a$, thus $a = 0$. Since $\frac{\alpha}{2}$, $\frac{\alpha^2}{2}$, and $\frac{\alpha^2+\alpha}{2}$ are not algebraic integers, the only possibility is $b = c = 0$, but this means that initially ω was in $\mathbb{Z}[\alpha]$, a contradiction.

Exercise 4.3. A cubic extension $K/\mathbb{Q}$ (i.e. $[K : \mathbb{Q}] = 3$) is called a pure cubic field if it is of the form $\mathbb{Q}(\sqrt[3]{n})$ for some integer n that is not a cube.

(a) Show that the discriminant of a pure cubic field is equal to $-3d^2$ for some $d \in \mathbb{Z}$;

(b) Show that $\mathbb{Q}(\theta)$, where $\theta^3 - 3\theta + 4 = 0$ is not a pure cubic field.

Solution. (a) Let $K = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt[3]{n}$, and let $\omega = e^{2\pi i/3}$ be the third root of unity. Since α is a root of $x^3 - n = 0$, the complex embeddings of K are given by $\alpha \mapsto \omega^j \alpha$ for $j = 0, 1, 2$. Using this we compute the discriminant of the basis $\{1, \alpha, \alpha^2\}$:

$$\mathrm{d}(1, \alpha, \alpha^2) \;=\; \det \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha\omega & \alpha^2\omega^2 \\ 1 & \alpha\omega^2 & \alpha^2\omega \end{pmatrix}^2 \;=\; \alpha^6(\omega^2 + \omega^2 + \omega^2 - \omega - \omega - \omega)^2$$

$$= \; 9n^2(\omega^4 - 2\omega^3 + \omega^2) \;=\; -27n^2.$$

Since the discriminant D_K is up to squares equal to $-27n^2 = -3(3n)^2$, we get that it is of the form $-3d^2$ for some d (and moreover $d|3n$).

(b) Let us compute the discriminant of $\{1, \theta, \theta^2\}$ using traces. Let $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbb{Q}}$. We have $\mathrm{Tr}(1) = 3$, $\mathrm{Tr}(\theta) = 0$, and since θ^2 satisfies $x^3 - 6x^2 + 9x - 16 = 0$, $\mathrm{Tr}(\theta^2) = 6$. Moreover, $\theta^3 = 3\theta - 4$ and $\theta^4 = 3\theta^2 - 4\theta$, thus $\mathrm{Tr}(\theta^3) = -12$ and $\mathrm{Tr}(\theta^4) = 18$. Therefore

$$\mathrm{d}(1, \theta, \theta^2) \;=\; \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\theta) & \mathrm{Tr}(\theta^2) \\ \mathrm{Tr}(\theta) & \mathrm{Tr}(\theta^2) & \mathrm{Tr}(\theta^3) \\ \mathrm{Tr}(\theta^2) & \mathrm{Tr}(\theta^3) & \mathrm{Tr}(\theta^4) \end{pmatrix} \;=\; \det \begin{pmatrix} 3 & 0 & 6 \\ 0 & 6 & -12 \\ 6 & -12 & 18 \end{pmatrix} \;=\; -324\,.$$

Since $-324 = -18^2$, we see that $\mathrm{disc}(K) = -m^2$ for some $m|18$. Since $-m^2$ is not of the form $-3d^2$, we conclude that $\mathbb{Q}(\theta)$ is not a pure cubic field.

Exercise 4.4. Let $K_1 = \mathbb{Q}(\gamma_1)$ and $K_2 = \mathbb{Q}(\gamma_2)$ be algebraic extensions of degrees n_1 and n_2 respectively, such that $K = \mathbb{Q}(\gamma_1, \gamma_2)$ has degree $n_1 n_2$ over $\mathbb{Q}$. Let $\{\alpha_1, \ldots, \alpha_{n_1}\}$ and $\{\beta_1, \ldots, \beta_{n_2}\}$ be integral bases of K_1 and K_2 respectively, of discriminants D_1 and D_2.

(a) Show that $\{\alpha_i\beta_j\}_{i,j}$ form a basis for K over $\mathbb{Q}$;

(b) Fix some embedding of K into $\mathbb{C}$. Show that there are exactly n_1 embeddings $\varphi_i\colon K \to \mathbb{C}$ that restrict to identity on K_2, and that there are exactly n_2 embeddings $\psi_j\colon K \to \mathbb{C}$ that restrict to identity on K_1;

(c) Let $\omega = \sum_{i=1}^{n_1}\sum_{j=1}^{n_2} u_{ij}\alpha_i\beta_j \in \mathcal{O}_K$, where $u_{ij} \in \mathbb{Q}$. Show that $D_2 u_{ij} \in \mathbb{Z}$ for all i, j;

(d) Show that if D_1 and D_2 are coprime, then $\{\alpha_i\beta_j\}_{i,j}$ forms an integral basis for K;

(e) Show that the discriminant of $\{\alpha_i\beta_j\}_{i,j}$ is $D_1^{n_2}D_2^{n_1}$ *(Hint: recall the Kronecker product of matrices)*;

(f) Using (d) and (e) write down an integral basis for the quartic field $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ and find its discriminant.

Solution. (a) The field K is generated as a vector space over $\mathbb{Q}$ by products $\gamma_1^a\gamma_2^b$, $a, b \geq 0$. Writing $\gamma_1^a = \sum_i a_i\alpha_i$, $\gamma_2^b = \sum_i b_i\beta_i$, we get that $\gamma_1^a\gamma_2^b = \sum_{i,j} a_i b_j \alpha_i\beta_j$, so that K is spanned over $\mathbb{Q}$ by n_1n_2 elements $\alpha_i\beta_j$. Since the degree of K over $\mathbb{Q}$ is n_1n_2, these elements form a basis.

(b) Since $K = \mathbb{Q}(\gamma_1, \gamma_2)$, any embedding $\sigma\colon K \to \mathbb{C}$ is uniquely determined by $\sigma(\gamma_1)$ and $\sigma(\gamma_2)$. Since the degree of K is n_1n_2, and there are n_1n_2 possibilities for $(\sigma(\gamma_1), \sigma(\gamma_2))$, all of them are realized exactly once. Thus, we get that there are exactly n_1 embeddings $\varphi_i\colon K \to \mathbb{C}$ that fix γ_2 (and hence K_2), and exactly n_2 embeddings $\psi_j\colon K \to \mathbb{C}$ that fix γ_1 (and hence K_1).

(c) Rewrite $\omega = \sum_{j=1}^{n_2} v_j\beta_j$, where $v_j = \sum_{i=1}^{n_1} u_{ij}\alpha_i \in K_1$. Multiplying ω by β_k and applying ψ_l, where $k, l \in \{1, \ldots, n_2\}$ we get (since ψ_l fixes K_1)

$$\psi_l(\beta_k\omega) = \sum_{j=1}^{n_2} v_j\psi_l(\beta_j\beta_k)\,.$$

Summing the last identity over $l = 1, \ldots, n_2$, we get

$$\sum_{j=1}^{n_2} \mathrm{Tr}_{K_2/\mathbb{Q}}(\beta_j\beta_k)v_j = \sum_{l=1}^{n_2} \psi_l(\beta_k\omega)\,, \qquad k = 1, \ldots, n_2\,.$$

Note that the left-hand side is in K_1 (since all the traces are rational numbers), while the right-hand-side is an algebraic integer, since it is given as a sum of algebraic integers. Therefore,

$$\sum_{j=1}^{n_2} \mathrm{Tr}_{K_2/\mathbb{Q}}(\beta_j\beta_k)v_j \in \mathcal{O}_{K_1}\,, \qquad k = 1, \ldots, n_2\,.$$

From this, by Cramer's rule for the matrix $A = (\mathrm{Tr}_{K_2/\mathbb{Q}}(\beta_j\beta_k))_{j,k}$, we get $\det(A)v_j \in \mathcal{O}_{K_1}$ for $j = 1, \ldots, n_2$. Since $D_2 = \det(A)$ and $\{\alpha_i\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_{K_1}$, this implies that $D_2u_{ij} \in \mathbb{Z}$ for all i, j.

(d) Let $\omega = \sum_{i=1}^{n_1}\sum_{j=1}^{n_2} u_{ij}\alpha_i\beta_j \in \mathcal{O}_K$. By (c) we have $D_1u_{ij} \in \mathbb{Z}$ and $D_2u_{ij} \in \mathbb{Z}$. Since D_1 and D_2 are coprime we get $u_{ij} \in \mathbb{Z}$, so that $\{\alpha_i\beta_j\}_{i,j}$ is an integral basis for $\mathcal{O}_K$.

(e) As in (b) any embedding $\sigma\colon K \to \mathbb{C}$ is uniquely determined by the images of γ_1 and γ_2, and thus $\sigma(\alpha\beta)$, $\alpha \in K_1$, $\beta \in K_2$ is equal to $\varphi_i(\alpha)\psi_j(\beta)$ for some uniquely determined pair of indices (i, j).

Therefore, the matrix of embeddings for the basis $\{\alpha_{i_2}\beta_{j_2}\}_{i_2,j_2}$ is equal to $C = (\varphi_{i_1}(\alpha_{i_2})\psi_{j_1}(\beta_{j_2}))_{(i_1,j_1),(i_2,j_2)}$. The matrix C is evidently the Kronecker product of the

matrices $A = (\varphi_i(\alpha_j))_{i,j=1}^{n_1}$ and $B = (\psi_i(\beta_j))_{i,j=1}^{n_2}$. Therefore, by a formula for the determinant of a Kronecker product of matrices we have $\det(C) = \det(A)^{n_2} \det(B)^{n_1}$, and since $\det(A)^2 = D_1$, $\det(B)^2 = D_2$ by definition, we get the desired identity for $\det(C)^2$.

(f) Consider $\gamma_1 = \sqrt{2}$, $\gamma_2 = \sqrt{5}$, $n_1 = n_2 = 2$. Recall that the integral basis for $\mathbb{Q}(\sqrt{2})$ is $\{1, \sqrt{2}\}$, and the integral basis for $\mathbb{Q}(\sqrt{5})$ is $\{1, \frac{1+\sqrt{5}}{2}\}$. We compute $D_1 = \mathrm{d}(1, \sqrt{2}) = 8$ and $D_2 = \mathrm{d}(1, \frac{1+\sqrt{5}}{2}) = 5$. Since D_1 and D_2 are coprime, by (b) we have that $\mathcal{O}_K$ is generated by $\{1, \sqrt{2}, \frac{1+\sqrt{5}}{2}, \frac{\sqrt{2}+\sqrt{10}}{2}\}$, and by (c) we have that the discriminant is $(D_1 D_2)^2 = 1600$.