Autumn Semester 2019

Introduction to Algebraic Number Theory

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

Solutions to Exercise Sheet 3

Exercise 3.1. Let $K = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt[4]{2}$, and let $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbb{Q}}$.

(a) Show that $\mathrm{Tr}(a + b\alpha + c\alpha^2 + d\alpha^3) = 4a$ for $a, b, c, d \in \mathbb{Q}$;

(b) Use part (a) to show that $\sqrt{3} \notin K$.

Solution.

(a) The complex embeddings of K are $\sigma_j(\sqrt[4]{2}) = i^j\sqrt[4]{2}$, $j = 1, \ldots, 4$, from which we find $\mathrm{Tr}(\alpha^j) = 0$, $j = 1, 2, 3$, and therefore $\mathrm{Tr}(a + b\alpha + c\alpha^2 + d\alpha^3) = 4a$, as claimed.

(b) Assume that $\sqrt{3} = a + b\alpha + c\alpha^2 + d\alpha^3$. Since $\mathrm{Tr}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(\sqrt{3}) = 0$, by transitivity of the trace we have $\mathrm{Tr}(\sqrt{3}) = 2 \cdot 0 = 0$, thus $a = 0$. Next, we compute $4b = \mathrm{Tr}(\sqrt{3}/\sqrt[4]{2}) = \mathrm{Tr}(\sqrt[4]{9/2}) = 0$, since the 4 conjugates of $\sqrt[4]{9/2}$ are $\pm\sqrt[4]{9/2}$ and $\pm i\sqrt[4]{9/2}$.

Now we have $\sqrt{3} = c\alpha^2 + d\alpha^3$, from which, after dividing by α^2, we find $\sqrt{3/2} = c + d\alpha$. Again taking the trace we get $c = 0$, so that $\sqrt{3/2} = d\sqrt[4]{2}$. However, this implies $\sqrt{2} = \frac{3}{2d^2}$, which contradicts $\sqrt{2} \notin \mathbb{Q}$ (alternatively, taking the trace of $\sqrt{3/2}/\sqrt[4]{2}$ we get $d = 0$, so that $\sqrt{3} = 0$, a contradiction).

Exercise 3.2. Let $K/\mathbb{Q}$ be an algebraic extension of degree n, and let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$.

(a) Let $\sigma_1, \ldots, \sigma_n$ be the complex embeddings of K and define

$$P = \sum_{\substack{\pi \in S_n \\ \mathrm{sgn}(\pi)=1}} \prod_{j=1}^{n} \sigma_{\pi(j)}(\alpha_j)\,,$$

$$N = \sum_{\substack{\pi \in S_n \\ \mathrm{sgn}(\pi)=-1}} \prod_{j=1}^{n} \sigma_{\pi(j)}(\alpha_j)\,.$$

Show that $P + N$ and PN are integers.

(b) Use part (a) to show that the discriminant $\mathrm{d}(\alpha_1, \ldots, \alpha_n)$ is congruent to 0 or 1 modulo 4.

(c) Let $\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \overline{\sigma}_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+r_2}$, $n = r_1 + 2r_2$ be the complex embeddings of K, where $\sigma_i(K) \subset \mathbb{R}$, $i = 1, \ldots, r_1$, and $\sigma_i(K) \not\subset \mathbb{R}$, $i = r_1 + 1, \ldots, r_1 + r_2$. Assuming that $\mathrm{d}(\alpha_1, \ldots, \alpha_n) \neq 0$ show that its sign is $(-1)^{r_2}$.

Solution. (a) Let $L/\mathbb{Q}$ be the normal closure of K. Then L is Galois over $\mathbb{Q}$ and contains $\sigma_j(K)$, $j = 1, \ldots, n$. Note that for any element $\sigma \in \mathrm{Gal}(L/K)$ and any embedding σ_j of K the composition $\sigma \circ \sigma_j$ is again an embedding, and hence composing with σ induces a permutation of $\sigma_1, \ldots, \sigma_n$. Depending on whether this permutation is even or odd, σ either fixes P and N, or interchanges them.

Therefore, $\sigma(P+N) = P+N$ and $\sigma(PN) = PN$ for all $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. This shows that $P+N$ and PN are in $\mathbb{Q}$. However, since P and N are defined as sums of products of algebraic integers, we also have that $P+N$ and PN are algebraic integers, and hence $P+N, PN \in \mathbb{Z}$.

(b) We have $\det(\sigma_i(\alpha_j)) = P - N$, and thus $\mathrm{d}(\alpha_1, \ldots, \alpha_n) = (P-N)^2 = (P+N)^2 - 4PN$. Therefore, we get the result from part (a), since squares of integers are congruent to 0 or 1 modulo 4.

(c) Let $v_i = (\sigma_i(\alpha_1), \ldots, \sigma_i(\alpha_n))$ for $i = 1, \ldots, r_1 + r_2$. Then $\mathrm{d}(\alpha_1, \ldots, \alpha_n)$ is the square of the determinant of a matrix with rows $v_1, \ldots, v_{r_1}, v_{r_1+1}, \overline{v_{r_1+1}}, \ldots, v_{r_1+r_2}, \overline{v_{r_1+r_2}}$.

Note that applying a row transformation $(u, v) \mapsto (\frac{1}{2}(u+v), \frac{1}{2i}(u-v))$ multiplies the determinant of the matrix by $\frac{i}{2}$. Applying this transformation to each pair of conjugate vectors $v_{r_1+j}, \overline{v_{r_1+j}}$, $j = 1, \ldots, r_2$, we obtain that $\mathrm{d}(\alpha_1, \ldots, \alpha_n)$ is equal to $(-1/4)^{r_2}$ times the square of the determinant of the matrix with rows $v_1, \ldots, v_{r_1}, \mathrm{Re}(v_{r_1+1}), \mathrm{Im}(v_{r_1+1}), \ldots, \mathrm{Re}(v_{r_1+r_2}), \mathrm{Im}(v_{r_1+r_2})$. Since this latter matrix has real entries, the square of its determinant is a nonnegative real number, and hence the sign of $\mathrm{d}(\alpha_1, \ldots, \alpha_n)$ is equal to $(-1)^{r_2}$.

Exercise 3.3. Let $K = \mathbb{Q}(\alpha)$, where $\alpha^3 - \alpha^2 - 2\alpha - 8 = 0$. Recall that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module spanned by $\{\omega_1, \omega_2, \omega_3\}$ for some $\omega_i \in \mathcal{O}_K$.

(a) Compute the discriminant $\mathrm{d}(1, \alpha, \frac{\alpha^2 - \alpha}{2})$;

(b) Show that $\mathcal{O}_K$ is the integral span of $\{1, \alpha, \frac{\alpha^2-\alpha}{2}\}$;

(c) Show that $\mathcal{O}_K$ **does not** have the form $\mathbb{Z}[\gamma]$ for any $\gamma \in \mathcal{O}_K$.

Solution. (a) Note that $\mathrm{Tr}_{K/\mathbb{Q}}(1) = 3$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 1$. Since α^2 satisfies $x^3 - 5x^2 - 12x - 64 = 0$ we also have $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^2) = 5$. Hence $\mathrm{Tr}_{K/\mathbb{Q}}(a + b\alpha + c\alpha^2) = 3a + b + 5c$. From this we compute the discriminant $\mathrm{d}(1, \alpha, \beta)$ using traces:

$$\mathrm{d}(1, \alpha, \beta) = \det \begin{pmatrix} 3 & 1 & 2 \\ 1 & 5 & 13 \\ 2 & 13 & -2 \end{pmatrix} = -503\,.$$

(b) First, we check that $\beta = \frac{\alpha^2-\alpha}{2}$ satisfies $x^3 - 2x^2 + 3x - 10$, thus $\beta \in \mathcal{O}_K$. Since $\mathcal{O}_K$ is the integral span of $\{\omega_1, \omega_2, \omega_3\}$ for some ω_i, there is an integral transition matrix A from $\{1, \alpha, \beta\}$ to $\{\omega_1, \omega_2, \omega_3\}$. Then we have $\mathrm{d}(\omega_1, \omega_2, \omega_3)\det(A)^2 = \mathrm{d}(1, \alpha, \beta) = -503$. Since 503 is squarefree, we have $\det(A) = \pm 1$, and the integral spans of $\{1, \alpha, \beta\}$ and $\{\omega_1, \omega_2, \omega_3\}$ coincide and are both equal to $\mathcal{O}_K$.

(c) Assume that $\mathcal{O}_K = \mathbb{Z}[\gamma]$ for some $\gamma \in \mathcal{O}_K$. By part (a) we may assume that $\gamma = a\alpha + b\beta + c$, where $a, b, c \in \mathbb{Z}$, and further we may assume that $c = 0$, since $\mathbb{Z}[\gamma] = \mathbb{Z}[\gamma - c]$. The transition matrix from $\{1, \gamma, \gamma^2\}$ to $\{1, \alpha, \beta\}$ is then given by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 2b(4a-b) & a^2 + 2ab + 2b^2 & 2a^2 + b^2 \end{pmatrix}.$$

Its determinant is equal to $2a^3 - a^2b - ab^2 - 2b^3$. Since $a^2b + ab^2 = ab(a+b)$ is always even, this determinant is divisible by 2 for any choice of a, b, hence $\mathcal{O}_K \neq \mathbb{Z}[\gamma]$.

Exercise 3.4*. Let $K = \mathbb{Q}(\sqrt{-2}, \sqrt{-5})$.

(a) Show that $\mathcal{O}_K$ is the integral span of $\{1, \sqrt{-2}, \sqrt{-5}, \frac{\sqrt{-2}+\sqrt{10}}{2}\}$;

(b) Show that $\mathcal{O}_K$ **does not** have the form $\mathbb{Z}[\gamma]$ for any $\gamma \in \mathcal{O}_K$.

Solution. (a) Let $\alpha = a + b\sqrt{-2} + c\sqrt{-5} + d\sqrt{10} \in \mathcal{O}_K$. Then all of its conjugates are also algebraic integers:

$$\begin{aligned} \alpha_2 &= a - b\sqrt{-2} + c\sqrt{-5} - d\sqrt{10}\,, \\ \alpha_3 &= a + b\sqrt{-2} - c\sqrt{-5} - d\sqrt{10}\,, \\ \alpha_4 &= a - b\sqrt{-2} - c\sqrt{-5} + d\sqrt{10}\,. \end{aligned}$$

Since $\alpha + \alpha_2 = 2a + 2c\sqrt{-5}$ is an algebraic integer in $\mathbb{Q}(\sqrt{-5})$, we get $2a, 2c \in \mathbb{Z}$ (since $-5 \equiv 3 \pmod 4$). Similarly, from $\alpha + \alpha_3$ we get $2b \in \mathbb{Z}$, and from $\alpha + \alpha_4$ we get $2d \in \mathbb{Z}$. We write $\alpha = \frac{A+B\sqrt{-2}+C\sqrt{-5}+D\sqrt{10}}{2}$, where $A, B, C, D \in \mathbb{Z}$. Then $\alpha\alpha_2$ is an algebraic integer, thus

$$(a + c\sqrt{-5})^2 + 2(b + d\sqrt{-5})^2 = \frac{A^2 - 5C^2 + 2B^2 - 10D^2}{4} + \frac{AC + 2BD}{2}\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]\,.$$

From this we see that $2|AC$ and $4|A^2 - 5C^2 + 2B^2 - 10D^2$. From the first divisibility we have that at least one of A or C is even, and from the second we get $2|A^2 - C^2$, hence A and C have the same parity. Thus $2|A, C$. Then we get $2|(B^2 - D^2)$, so that B and D have the same parity. This implies that $\{1, \sqrt{-2}, \sqrt{-5}, \frac{\sqrt{-2}+\sqrt{10}}{2}\}$ is an integral basis.

(b) Consider the elements $\alpha_i = (1 \pm \sqrt{-2})(1 \pm \sqrt{-5})$, $i = 1, \ldots, 4$. Then one can check that $3|\alpha_i\alpha_j$ for all $i \neq j$. Also note that $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 4$. This implies that

$$1 \equiv (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^n \equiv \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n \pmod 3\,.$$

From this we get that $3 \nmid \alpha_1^n$, since otherwise we would have $3|\alpha_i^n$, $i = 1, 2, 3, 4$, and then 3 would also divide $\alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n$. Assume that $\mathcal{O}_K = \mathbb{Z}[\gamma]$ for some $\gamma \in \mathcal{O}_K$, let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of γ, and let $\alpha_i = f_i(\gamma)$, $f_i \in \mathbb{Z}[x]$.

For any g in $\mathbb{Z}[x]$ we consider $\overline{g} \in (\mathbb{Z}/3\mathbb{Z})[x]$, obtained by reduction mod 3. Note that $3|g(\gamma)$ in $\mathbb{Z}[\gamma]$ if and only if $\overline{f}|\overline{g}$ in $(\mathbb{Z}/3\mathbb{Z})[x]$ (indeed, both statements are equivalent to the existence of $h, r \in \mathbb{Z}[x]$ such that $g(x) = 3h(x) + f(x)r(x)$).

From the above divisibility properties for α_i we get $\overline{f}|\overline{f_i f_j}$ for all $i \neq j$, but $\overline{f} \nmid \overline{f_i}^n$ for any i, n. This implies that for each $i = 1, 2, 3, 4$, $\overline{f}$ has an irreducible factor that divides $\overline{f_i}$, but not any $\overline{f_j}$ for $j \neq i$.

Thus $\overline{f}$ has at least 4 different irreducible factors. On the other hand, $\deg(\overline{f}) = 4$, so this means that $\overline{f}$ has 4 different linear factors, but in $(\mathbb{Z}/3\mathbb{Z})[x]$ there are only 3 different monic linear polynomials: $x, x-1, x-2$. This contradiction shows that $\mathcal{O}_K \neq \mathbb{Z}[\gamma]$.