Exercise sheet #3

Exercises marked with a ✎ are to be handed in before **Monday October 14** at noon, in the mailbox at Spiegelgasse 1. Each of these is worth a number of points, as indicated.
Questions marked with a $\star$ are more difficult.

Exercise 1 (Dedekind's lemma and non-degeneracy of the trace) – Let G be a group, and C be a field. Let $\sigma_1, \ldots, \sigma_n$ be distinct group homomorphism $\mathrm{G} \to \mathrm{C}^\times$. We will say that $\sigma_1, \ldots, \sigma_n$ are linearly independent over C if the following holds: the only n-tuple $(\lambda_1, \ldots, \lambda_n) \in \mathrm{C}^n$ such that $\sum_{i=1}^n \lambda_i \cdot \sigma_i(g) = 0$ for all $g \in \mathrm{G}$, is the trivial one $(\lambda_1, \ldots, \lambda_n) = (0, \ldots, 0)$.

1.1. Prove that $\sigma_1, \ldots, \sigma_n$ are linearly independent over C.

Now, let K be field of characteristic 0 or a finite field, and C be an algebraic closure of K. Let L/K be a finite extension of degree n. As we've seen in an earlier exercise, there are n distinct K-embeddings $\sigma_i : \mathrm{L} \to \mathrm{C}$. Let $x_1, \ldots, x_n$ be a base for L over K.

1.2. Prove that $\mathrm{D}(x_1, \ldots, x_n) = \left(\det\left[\sigma_i(x_j)\right]_{1 \leqslant i,j \leqslant n}\right)^2$.

1.3. Prove that $\mathrm{D}(x_1, \ldots, x_n)$ is non-zero. *Hint: assume for a contradiction that* $\mathrm{D}(x_1, \ldots, x_n) = 0$, *and show that there would then exist* $(\lambda_1, \ldots, \lambda_n) \in \mathrm{C}^n$ *such that* $\sum_{i=1}^n \lambda_i \sigma_i(x_j) = 0$ *for all* j.

Exercise 2 (Explicit computation of the discriminant) – Let K be a field of characteristic 0, and C be an algebraic closure of K. Let $\alpha \in \mathrm{C}$ be an algebraic element: we let $\mathrm{L} = \mathrm{K}[\alpha]$, n be the degree of α over K, and let $f(x) \in \mathrm{K}[x]$ denote the minimal polynomial of α over K.

Let $\sigma_1, \ldots, \sigma_n$ denote the n distinct K-embeddings $\mathrm{L} \to \mathrm{C}$. Let $\alpha_1, \ldots, \alpha_n$ denote the (distinct) roots of f in C.

2.1. Consider the matrix $\mathrm{A} := [\alpha_i^j]_{1 \leqslant i,j \leqslant n}$. Prove that $\det \mathrm{A} = \prod_{i<j}(\alpha_i - \alpha_j)$.

2.2. Show that, up to renumbering the α_i's, we have $\sigma_i(\alpha) = \alpha_i$ for all $i \in \{1, \ldots, n\}$.

2.3. Deduce that $\mathrm{D}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2} \cdot \mathrm{N}_{\mathrm{L}/\mathrm{K}}(f'(\alpha))$.

We now assume that $f(x) \in \mathrm{K}[x]$ is of the following form: $f(x) = x^n + ax + b$ for some $a, b \in \mathrm{K}$.

2.4. Deduce from the previous question that

$$\mathrm{D}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2} \cdot (n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n).$$

2.5. Specialise the above formula in the case where $n = 2$. What do you notice?

2.6. In the case where $n = 3$, give a general formula for $\mathrm{D}(1, \alpha, \alpha^2)$ in terms of the coefficients of f.

Exercise 3 – Let A be a ring, and M be an A-module. Given a sub-A-module M′ of M, prove that

$$\mathrm{M} \text{ is noetherian} \iff \mathrm{M}' \text{ and } \mathrm{M}/\mathrm{M}' \text{ are noetherian.}$$

Exercise 4 (A PID which is not Euclidean) {✎ : 5 points} – Let $\alpha := \frac{1+i\sqrt{19}}{2} \in \mathbb{C}$, and consider the subring $\mathrm{R} := \mathbb{Z}[\alpha]$ of $\mathbb{C}$. We've proved in the second exercise class that R is not a Euclidean domain. The goal of this exercise is to prove that R is a PID. Since R is a subring of $\mathbb{C}$, it is clear that R is an integral domain: it remains to prove that all ideals in R are principal.

We say that a pair $(a, b) \in \mathrm{R} \times \mathrm{R} \smallsetminus \{0\}$ has division with remainder in R (DWR) if there exists a pair $q, r \in \mathrm{R}$ with $a = bq + r$ and $|r| < |b|$ (here $|.|$ denotes the usual absolute value on $\mathbb{C}$, restricted to $\mathrm{R} \subset \mathbb{C}$). We let

$$\mathrm{U} := \{r + z,\ r \in \mathrm{R},\ z \in \mathbb{C} \text{ s.t. } |z| < 1\} \subset \mathbb{C}$$

denote the union of the open disks of radius 1 centred at elements of R.

4.1. Let $z \in \mathbb{C} \smallsetminus \mathrm{U}$. Prove that $\left|\mathrm{Im}(z) - \frac{\sqrt{19}}{2}n\right| \geqslant \frac{\sqrt{3}}{2}$, for all integers n.

4.2. Show that the sum of two elements in $\mathbb{C} \smallsetminus \mathrm{U}$ lies in U.

4.3. Prove the following assertions:

- (a, b) has DWR in R if and only if $a/b \in \mathbb{C}$ lies in U.
- If (a, b) does not have DWR in R, then $(2a, b)$ has DWR in R.
- If (a, b) does not have DWR in R then one of $(\alpha a, b)$ or $((1-\alpha)a, b)$ has DWR in R.

4.4. Show that 2 is coprime to α in R. Show that 2 is also coprime to $1 - \alpha$ in R.

4.5. Conclude that R is a PID. *Hint: If* $\mathrm{I} \subset \mathrm{R}$ *is a proper ideal, consider* $g \in \mathrm{I} \smallsetminus \{0\}$ *such that* $|g|$ *is minimal. Prove that* g *generates* I.

Exercise 5 (A Diophantine equation) {✎ : 5 points} – In this exercise, we determine the solutions $(x, y) \in \mathbb{Z}^2$ to

$$x^2 + 1 = y^3.$$

5.1. Let A be a principal ideal domain, and $n \geqslant 2$ be an integer. Let $u, v \in \mathrm{A}$ be two coprime elements whose product is an n-th power in A. Show that, up to multiplication by units, both u and v are n-th powers in A.

Let $\mathrm{R} = \mathbb{Z}[i]$ denote the ring of Gaussian integers. Recall that R is a PID, and that $\mathrm{R}^\times = \{\pm 1, \pm i\}$.

5.2. Prove that, up to multiplication by units, the only prime divisors of 2 in R are $1 + i$ and $1 - i$.

5.3. Let $x \in \mathbb{Z}$ be an odd integer. Can $x^2 + 1$ be a cube in $\mathbb{Z}$? *Hint : what are the cubes modulo 4?*

Now let $(x, y) \in \mathbb{Z}^2$ be a solution to the equation $x^2 + 1 = y^3$. In R, we have $y^3 = (x + i)(x - i)$.

5.4. Prove that $x + i$ and $x - i$ are coprime in R. *Hint : let* $q \in \mathrm{R}$ *be a prime element dividing them both, then* q *divides their sum and difference.*

5.5. Deduce from question **5.1** that there exist integers $a, b \in \mathbb{Z}$ such that $x + i = (a + ib)^3$. Deduce that

$$x = a(a^2 - 3b^2) \qquad \text{and} \qquad 1 = (3a^2 - b^2)b.$$

5.6. Conclude that the only solution $(x, y) \in \mathbb{Z}^2$ to the equation $x^2 + 1 = y^3$ is $(x, y) = (0, 1)$.

Hence, a non-zero square in $\mathbb{Z}$ is never followed by a cube.
