Exercise sheet #1

Exercises marked with a ✎ are to be handed in before **Monday September 30** 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 (Finite fields exist!) {✎ : 3 points} – Let q be the power of a prime number p. Show that there exists a unique field with q elements, denoted by $\mathbb{F}_q$, up to isomorphism.
Hint: Start by proving the statement when $q = p$. Given the existence of $\mathbb{F}_p$, fix an algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$ and consider the set $\mathrm{F}_q := \{x \in \overline{\mathbb{F}_p} : x^q - x = 0\}$. Prove that F_q is a field with q elements.

Exercise 2 (Sums of two squares in $\mathbb{F}_q$) {✎ : 3 points} – Let $\mathbb{F}_q$ be the finite field with q elements. We let p denote the characteristic of $\mathbb{F}_q$. The goal of the exercise if to prove that, for any $x \in \mathbb{F}_q$, there exist $a, b \in \mathbb{F}_q$ such that $x = a^2 + b^2$. *I.e.*, that any element of $\mathbb{F}_q$ is the sum of two squares.

2.1. Treat the case where q is a power of 2 (*i.e.*, $p = 2$).

We now assume that $p \geqslant 3$ is odd.

2.2. Consider the map $f : \mathbb{F}_q^\times \to \mathbb{F}_q^\times$ given by $a \mapsto a^2$. Prove that f is a group morphism. Compute $\#\operatorname{Ker}(f)$ and $\#\operatorname{Im}(f)$.

2.3. Compute $\#\{a^2,\ a \in \mathbb{F}_q\}$. Given $x \in \mathbb{F}_q$, compute the number of values taken by $b \mapsto x - b^2$.
In particular, some elements of $\mathbb{F}_q$ are not squares.

2.4. Deduce that, for any $x \in \mathbb{F}_q$, the sets $\{a^2,\ a \in \mathbb{F}_q\}$ and $\{x - b^2,\ b \in \mathbb{F}_q\}$ cannot be disjoint. Conclude that x is the sum of two squares.

Exercise 3 {✎ : 3 points} –

3.1. Let p be a prime. Show that $(p-1)! \equiv -1 \bmod p$.
Hint: factor $x^{p-1} - 1 \in \mathbb{F}_p[x]$ and evaluate at a well-chosen point.

3.2. (Wilson's theorem) Let $n \geqslant 1$ be an integer. Show that

$$n \text{ is prime} \quad \Leftrightarrow \quad n \text{ divides } (n-1)! + 1.$$

3.3. Let p be an odd prime number. Prove that

$$(p-1)! \equiv (-1)^{(p-1)/2} \cdot \left(\left(\tfrac{p-1}{2}\right)!\right)^2 \bmod p.$$

Deduce that -1 is a square modulo p if and only if $p \equiv 1 \bmod 4$.

Exercise 4 (Euclidean ⇒ PID ⇒ UFD) – In this exercise, rings are assumed to be commutative, to admit a unit element, and to have at least two elements.

Recall the following definitions. A ring A is called a Euclidean domain if it is an integral domain, and if there is a map $\mathrm{N} : \mathrm{A} \smallsetminus \{0\} \to \mathbb{Z}_{\geqslant 0}$ satisfying the following property: *for all $a, b \in \mathrm{A}$ with $b \neq 0$, there exists a unique pair $(q, r) \in \mathrm{A}^2$ such that $a = bq + r$ and either $r = 0$ or $\mathrm{N}(r) < \mathrm{N}(b)$.* A ring A is called a principal ideal domain (PID) if it is an integral domain, and if any ideal I of A is principal. A ring A is called a unique factorisation domain (UFD) if it is an integral domain, and if the following property holds: *for any given $a \in \mathrm{A}$, one can decompose $a = u \cdot p_1 \dots p_r$ where $u \in \mathrm{A}^\times$ is a unit and $p_1, \dots, p_r \in \mathrm{A}$ are prime elements. Moreover, up to multiplication by a unit or changing the order of the factors, this decomposition is unique.*

4.1. Show that a Euclidean domain is a principal ideal domain.

4.2. Show that a principal ideal domain is a unique factorisation domain.

4.3. ($\star$) Is a UFD necessarily a PID? Prove or give a counterexample.

4.4. ($\star\star$) Is a PID necessarily Euclidean? Prove or give a counterexample.

Exercise 5 (Chevalley–Warning theorem) – Let $q > 1$ be a power of a prime p, and let $\mathbb{F}_q$ denote the finite field with q elements. Fix integers $s, n \geqslant 1$. Consider a set of s homogeneous polynomials $f_i(\mathrm{X}_1, \dots, \mathrm{X}_n) \in \mathbb{F}_q[\mathrm{X}_1, \dots, \mathrm{X}_n]$ in n variables with coefficients in $\mathbb{F}_q$. For any $i \in \{1, \dots, s\}$, write $d_i := \deg f_i$. Let $\mathrm{V} := \{(x_1, \dots, x_n) \in (\mathbb{F}_q)^n \mid f_i(x_1, \dots, x_n) = 0 \ \forall i \in \{1, \dots, s\}\} \subset (\mathbb{F}_q)^n$ denote the set of common zeros of the f_i's. For any polynomial $f \in \mathbb{F}_q[\mathrm{X}_1, \dots, \mathrm{X}_n]$, let

$$\sigma(f) := \sum_{(x_1, \dots, x_n) \in (\mathbb{F}_q)^n} f(x_1, \dots, x_n) \in \mathbb{F}_q.$$

5.1. Prove that $y^{q-1} = 1$ for all $y \in \mathbb{F}_q^\times$. For any integer $k \geqslant 1$, deduce that $\displaystyle\sum_{x \in \mathbb{F}_q} x^k = \begin{cases} -1 & \text{if } q-1 \mid k, \\ 0 & \text{otherwise.} \end{cases}$
For non-negative integers $a_1, \dots, a_n$, compute $\sigma(\mathrm{X}_1^{a_1} \cdots \mathrm{X}_n^{a_n})$ when $\sum_{j=1}^n a_j < n(q-1)$.

5.2. Let $\mathrm{P}(\mathrm{X}_1, \dots, \mathrm{X}_n) = \prod_{i=1}^s \left(1 - f_i(\mathrm{X}_1, \dots, \mathrm{X}_n)^{q-1}\right) \in \mathbb{F}_q[\mathrm{X}_1, \dots, \mathrm{X}_n]$. Check that P is a linear combination of monomials $\mathrm{X}_1^{a_1} \cdots \mathrm{X}_n^{a_n}$ with $\sum_{j=1}^n a_j \leqslant (q-1) \sum_{i=1}^s d_i$. Secondly, given $(x_1, \dots, x_n) \in (\mathbb{F}_q)^n$, show that $\mathrm{P}(x_1, \dots, x_n) = \begin{cases} 1 & \text{if } x \notin \mathrm{V}, \\ 0 & \text{if } x \in \mathrm{V}. \end{cases}$

5.3. Deduce that $\sigma(\mathrm{P}) \equiv \#\mathrm{V} \bmod p$.

5.4. Assume that $\sum_{i=1}^n d_i < n$. Show that $\sigma(\mathrm{P}) = 0$.

5.5. Conclude that, if $\sum_{i=1}^n d_i < n$, then $\#\mathrm{V} \geqslant p$. In particular, under the same assumption, there exists at least one element $(x_1, \dots, x_n) \in \mathrm{V}$ with $(x_1, \dots, x_n) \neq (0, \dots, 0)$.

5.6. Application: a homogeneous polynomial of degree 2 (*i.e.*, a conic) in $n \geqslant 3$ variables has at least one non trivial zero in $(\mathbb{F}_q)^n$.
