Diskrete Mathematik HS2025 — Prof. Dennis HOFHEINZ

Marian DIETZ — Milan GONZALEZ-THAUVIN — Zoé REINKE

Exercise sheet 10

This is the exercise sheet number 10. The difficulty of the questions and exercises are rated from very easy ($\star$) to hard ($\star\star\star\star$) . The graded exercise is Exercise 10.3 and your solution has to be uploaded on the Moodle page of the course **by 27/11/2025, 23:59**. The solution to this exercise must be your own work, you may not share your solutions with anyone else. See also the note on dishonest behavior on the Moodle page.

Exercise 10.1 Warm-Up ($\star$)

1. What is the definition of a field?
2. What is the definition of a root of a polynomial $a(x) \in R[x]$?
3. Is the polynomial $b(x) = x^2 + 2 \in \mathrm{GF}(3)[x]$ irreducible? If not, give its factorization.

Exercise 10.2 Integral Domains and Fields

1. ($\star$) Recall an example of an integral domain that is not a field.
2. ($\star\star\star$) Prove that every finite integral domain D is a field.
   Hint: For an $a \in D \setminus \{0\}$, consider the function $f_a(x) = a \cdot x$.

Exercise 10.3 Characteristic of a Field ($\star\star$) — GRADED *(8 points)*

Please upload your solution by 27/11/2025

Let $\langle F; +, -, 0_F, \star, 1_F \rangle$ be a field. We say that F has finite characteristic if there exists a positive integer q such that

$$\underbrace{1_F + 1_F + \cdots + 1_F}_{q \text{ times}} = 0_F.$$

The smallest q such that the above equation holds is then called the *characteristic* of F.
To simplify notations in the field F, we will write $n \times a$ to denote $\underbrace{a + a + \cdots + a}_{n \text{ times}}$, and we will write a^n to denote $\underbrace{a \star a \star \cdots \star a}_{n \text{ times}}$ (where $a \in F$ and $n \in \mathbb{N}$). By convention, $0 \times a = 0_F$, $a^0 = 1_F$ and an empty product of integers is equal to 1.

1. Let $\langle F; +, -, 0_F, \star, 1_F \rangle$ be a field with finite characteristic q. Prove that for all $a \in F$, it holds that $q \times a = 0_F$.

2. Let $\langle F; +, -, 0_F, \star, 1_F \rangle$ be a field with finite characteristic q, where *q is a prime*. Let $a, b \in F$. Show that $(a+b)^q = a^q + b^q$.
   Hint: you may use without proof the binomial theorem, stated as follows. For every $a \in F$ and $b \in F$, and for every natural number $n \in \mathbb{N}$, the following holds:

$$(a+b)^n = \sum_{k=0}^{n} \left[\binom{n}{k} \times (a^k \star b^{n-k}) \right] \qquad \text{with } \binom{n}{k} \stackrel{\text{def}}{=} \frac{n \cdot (n-1) \cdots (n-k+1)}{k \cdot (k-1) \cdots 2 \cdot 1} \in \mathbb{N}$$

   You can assume that $\binom{n}{k}$ defined above is indeed a natural number. For which values of k does q divide $\binom{q}{k}$ when $0 \le k \le q$?

3. Let $\langle F; +, -, 0_F, \star, 1_F \rangle$ be a field with finite characteristic q, where *q is a prime*. Show using a proof by induction that for all $k \ge 1$ and for all $a_1, \cdots, a_k \in F$:

$$\left(\sum_{i=1}^{k} a_i \right)^q = \sum_{i=1}^{k} a_i^q$$

   Hint: use the result of question 2 wisely to avoid doing a similar proof again.
   Expectation: Your proof by induction (Section 2.6.10) should be clear and formal. In particular, you must explicitly define a statement P, then prove the basis step and the induction step, and finally conclude the above.

4. Let q be a prime. Show (using the previous questions) that in the field $\langle \mathbb{Z}_q; \oplus_q, \ominus_q, 0_q, \odot_q, 1_q \rangle$, for every $a \in \mathbb{Z}_q$, it holds that $a^q = a$.
   Expectation: You are *not* allowed to use any results from Section 5.3 since the goal of the bonus exercise is to come up with a new proof for Fermat's (little) theorem.

Exercise 10.4 Polynomials over a Field ($\star$)

1. Divide $x^5 + 6x^2 + 5$ by $5x^2 + 2x + 1$ over $\mathbb{Z}_7$ with remainders.
2. Determine all irreducible polynomials of degree 4 over $\mathrm{GF}(2)$.

Exercise 10.5 The Ring $F[x]_{m(x)}$ ($\star\star$)

1. Find all zero-divisors in the ring $\mathrm{GF}(3)[x]_{x^2+2x}$.
2. Determine all elements of $\mathrm{GF}(3)[x]_{x^2+2}$ and of the multiplicative group $\mathrm{GF}(3)[x]^*_{x^2+2}$.
3. Compute the inverse of the polynomial x in $\mathrm{GF}(3)[x]^*_{x^2+2}$.

Exercise 10.6 Secret Sharing ($\star\star$)

We find ourselves on a lonely island, where the ballistic missile system can be activated with a secret key $s \in \mathrm{GF}(q)$ (where q is a prime). This key is distributed among $n < q$ generals $G_1, \ldots, G_n$ as follows: random coefficients $a_1, \ldots, a_{t-1} \in \mathrm{GF}(q)$ are chosen, such that

$$a(x) \stackrel{\text{def}}{=} a_{t-1}x^{t-1} + \ldots + a_1 x + s.$$

Each general G_i receives a **share** $s_i = a(\alpha_i)$, where $\alpha_1, \ldots, \alpha_n$ are publicly known and pairwise distinct values from $\mathrm{GF}(q) \setminus \{0\}$.

1. All except t generals die on a fishing trip. Show that the key is not lost, because it can be determined uniquely from t shares.

2. Mario (one of the generals) wants to resolve a dispute with his neighbor by using a ballistic missile. In order to determine the key s, he has collected a total of $t-1$ shares (including her own share). How many values from $\mathrm{GF}(q)$ are still possible for the key, given $t-1$ shares? Prove your answer.

Exercise 10.7 Structure of Multiplicative Groups of Finite Fields ($\star\star\star$)

In this exercise we break down the proof of Theorem 5.40 from the lecture notes in smaller steps. Let F be a finite field and let $n = |F^*|$.

1. Let $a, b \in \mathbb{Z}$. Prove that $\gcd(a, b) = d \iff d \mid a$ and $d \mid b$ and $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

2. For $d \mid n$ define $A(d) = \{k \in \{1, \ldots, n\} \mid \gcd(k, n) = d\}$. Prove that $|A(d)| = \varphi\left(\frac{n}{d}\right)$.

3. Prove that $\sum_{d|n} \varphi\left(\frac{n}{d}\right) = n$.

4. Prove that $n = \sum_{d|n} \varphi(d)$.

5. Let $B(d) = \{k \in F^* \mid \mathrm{ord}(k) = d\}$. Show that $|B(d)| \in \{0, \varphi(d)\}$.
   Hint: consider the polynomial $x^d - 1 \in F[x]$.

6. Show that if $d \mid n$ then $|B(d)| = \varphi(d)$.

7. Conclude that F^* is cyclic.

Exercise 10.8 Common root and GCD ($\star\star$)

This exercise is taken from the spring exam of 2024.
Let F be a field. **Prove** that the following two statements are equivalent.

1. Every polynomial $a(x) \in F[x]$ with $\deg(a(x)) \geq 1$ has a root in F.
2. For all $a(x), b(x) \in F[x]$, if $a(x)$ and $b(x)$ have no common root, then $\gcd(a(x), b(x)) = 1$.

Due by 27/11/2025, 23:59.
Exercise 10.3 will be graded.