# UNIVERSITY OF OSLO

## Faculty of mathematics and natural sciences

| | |
|---|---|
| Exam in: | MAT2200 — Groups, Rings and Fields |
| Day of examination: | Wednesday, 31 May 2023 |
| Examination hours: | 15.00 – 19.00 |
| This problem set consists of 2 pages. | |
| Appendices: | None |
| Permitted aids: | None |

Please make sure that your copy of the problem set is complete before you attempt to answer anything.

There are 12 subproblems, each weighted equally. You may answer in English, Norwegian, Swedish or Danish.

## Problem 1 Group theory

### 1a

Prove that the set

$$S = \{2^n \mid n \in \mathbb{Z}\},$$

equipped with the usual operation of multiplication, is a group.

### 1b

List all finite abelian groups of order 20, up to isomorphism.

### 1c

Let $A_4$ be the alternating group on 4 letters, that is the subgroup of $S_4$ consisting of even permutations. Find elements $\sigma_1, \sigma_2, \sigma_3 \in A_4$ such that $\sigma_1$ has order 1, $\sigma_2$ has order 2, and $\sigma_3$ has order 3.

### 1d

Prove that $A_4$ is not abelian.

## Problem 2 Rings

### 2a

Determine the 0-divisors in the ring $\mathbb{Z}_{10}$.

*(Continued on page 2.)*

### 2b

Let $R$ be the ring $\mathbb{Z} \times \mathbb{Z}$, where addition and multiplication is given by, for $(a, b), (c, d) \in R$, setting

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b)(c, d) = (ac, bd).$$

Let

$$I = \{(a, 0) \mid a \in \mathbb{Z}\} \subset R.$$

Prove that $I$ is an ideal of $R$.

### 2c

Prove that $I$ is a prime ideal and that $I$ is not a maximal ideal.

## Problem 3 Finite fields

### 3a

Let $p$ be a prime number, and let $f(x) = x^p - x \in \mathbb{Z}_p[x]$. Determine (with justification) the zeros of $f(x)$ in $\mathbb{Z}_p$.

### 3b

Consider $x^2 + 1 \in \mathbb{Z}_3[x]$. Prove that the ring $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$ is a field, and determine its number of elements.

## Problem 4 Field theory

Let $f(x) = x^5 - 8x^4 + 2x + 2 \in \mathbb{Q}[x]$. You may use without proof that this polynomial is irreducible.

### 4a

Let $\alpha \in \overline{\mathbb{Q}}$ be a zero of $f(x)$. Compute $[\mathbb{Q}(\alpha) : \mathbb{Q}]$, and give a basis for $\mathbb{Q}(\alpha)$ as a vector space over $\mathbb{Q}$.

### 4b

Let $\beta \in \mathbb{Q}(\alpha) \setminus \mathbb{Q}$. Prove that $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$.

### 4c

Let $E \leq \overline{\mathbb{Q}}$ be the splitting field of $f(x)$ over $\mathbb{Q}$. It can be shown that $G(E/\mathbb{Q}) \simeq S_5$. Using this, show that there exists a field $K$ with $\mathbb{Q} \leq K \leq E$ such that $[K : \mathbb{Q}] = 24$.