

UNIVERSITY OF OSLO

Faculty of mathematics and natural sciences

Deferred exam in: MAT2200 — Groups, Rings and Fields

Day of examination: Thursday, 14 August 2025

Examination hours: 9:00–13:00

This problem set consists of 7 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 problems, each weighted equally. You may answer in English, Norwegian, Swedish or Danish.

Problem 1

For each pair of groups among the following list, determine if they are isomorphic or not. If they are isomorphic, give an isomorphism. If they are not, give a reason why.

- The subgroup of S_{16} generated by σ , where $\sigma(i) = i + 1$ for $1 \leq i < 16$ and $\sigma(16) = 1$
- The multiplicative group $\mathbb{Z}_{17}^\times = \{a \in \mathbb{Z}_{17} \mid a \neq 0\}$
- $\mathbb{Z}_4 \times \mathbb{Z}_4$

Solution

The subgroup $H = \langle \sigma \rangle \subset S_{16}$ is cyclic, and its order k is the smallest positive integer such that σ^k is the identity permutation. By definition, σ^k sends i to $i+k$, where we ignore congruence modulo 16. In particular, 16 is the smallest choice, and we obtain $H \simeq \mathbb{Z}_{16}$.

Since 17 is a prime number, $\mathbb{Z}_{17}$ is a finite field, and its multiplicative group is cyclic. This group has 16 elements, hence we again have $\mathbb{Z}_{17}^\times \simeq \mathbb{Z}_{16}$. This shows $H \simeq \mathbb{Z}_{17}^\times$.

Finally, $\mathbb{Z}_4 \times \mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_{16}$, since any element of $\mathbb{Z}_4 \times \mathbb{Z}_4$ has order 4 or less. This shows that $\mathbb{Z}_4 \times \mathbb{Z}_4$ is not isomorphic to the other ones.

Problem 2

Consider the following maps from the group $\mathbb{R}^3 = \{(x_1, x_2, x_3) \mid x_i \in \mathbb{R}\}$ to itself. Determine if they are group homomorphisms or not.

(Continued on page 2.)

- $f(x) = \sqrt{x_1^2 + x_2^2 + x_3^2}(x_1, x_2, x_3)$
- $g(x) = (x_1, 0, 0)$
- The 60° rotation around the x_3 -axis

Solution

First, f is not a group homomorphism. For example, we can take $x = (1, 0, 0)$ and compare $f(x + x)$ with $f(x) + f(x)$. On one hand, we have $f(x + x) = (\sqrt{2}, 0, 0)$, while on the other hand, we have $f(x) + f(x) = (2, 0, 0)$.

Next, g is a group homomorphism. Concretely, writing $x = (x_1, x_2, x_3)$ and $y = (y_1, y_2, y_3)$, we have

$$g(x + y) = (x_1 + y_1, 0, 0) = (x_1, 0, 0) + (y_1, 0, 0) = g(x) + g(y).$$

Similarly, we have $g(0) = 0$ and $g(-x) = -g(x)$.

Finally, the 60° rotation around the x_3 -axis is also a group homomorphism. Concretely, this can be expressed as

$$h(x) = (\cos 60^\circ x_1 - \sin 60^\circ x_2, \sin 60^\circ x_1 + \cos 60^\circ x_2, x_3),$$

and we see that the components on the right hand side are linear combinations of the components of x . In particular, we have equalities of the form

$$\begin{aligned} \cos 60^\circ(x_1 + y_1) - \sin 60^\circ(x_2 + y_2) \\ = \cos 60^\circ x_1 - \sin 60^\circ x_2 + \cos 60^\circ y_1 - \sin 60^\circ y_2, \end{aligned}$$

which shows $h(x + y) = h(x) + h(y)$. Similarly, we have $h(0) = 0$ and $h(-x) = -h(x)$.

Problem 3

Let K be the subgroup of S_5 defined as

$$K = \{\sigma \in S_5 \mid \sigma(i) = i \text{ if } i > 2\},$$

and set

$$H = \{\tau \in S_5 \mid \sigma\tau = \tau\sigma \text{ if } \sigma \in K\}.$$

Determine if H is normal or not. You should either give a proof that H is normal, or else give a concrete counterexample for the normality condition.

Solution

The subgroup H is not normal.

First, K is a copy of S_2 , since any element $\sigma \in K$ should fix the elements $i > 2$, and in particular determined by what it does to $\{1, 2\}$.

This implies that $\tau = (1, 2)$ belongs to both H and K .

(Continued on page 3.)

We now take $\sigma = (2, 3)$, and show that $\tau' = \sigma\tau\sigma^{-1}$ does not belong to K . A concrete computation gives $\tau' = (1, 3)$. Then, τ' does not commute with $\tau \in K$, by

$$\tau'\tau = (1, 2, 3), \quad \tau\tau' = (1, 3, 2).$$

Problem 4

Let G be the symmetry group of a regular tetrahedron. Determine the order of G , and determine if it is a simple group or not.

Solution

A regular tetrahedron Δ has four vertices, call them v_1, v_2, v_3, v_4 . Since a regular tetrahedron has congruent triangle faces, any permutation of these vertices induces a map from Δ to itself. Conversely, any symmetry of Δ induces a permutation of the v_i , and these correspondences are inverse to each other. Consequently, the symmetry group of Δ is isomorphic to S_4 , where $\sigma \in S_4$ corresponds to the symmetry characterized by $v_i \mapsto v_{\sigma(i)}$.

The group S_4 has a nontrivial normal subgroup A_4 , hence is not simple. Concretely, this corresponds to the symmetries represented by rotations around the axes through mid-points of opposite edges.

Problem 5

Determine if the following rings are integral domains or not.

- $\mathbb{Z}_7[X]$
- $\mathbb{Z}_{12}$

Solution

The ring $\mathbb{Z}_7[X]$ is an integral domain. Since 7 is a prime number, the coefficient ring $\mathbb{Z}_7$ is a field. In general the polynomial ring $F[X]$ is an integral domain whenever F is a field as a consequence of the Euclidean division algorithm.

The ring $\mathbb{Z}_{12}$ is not an integral domain. Since 3 and 4 are coprime, we have

$$\mathbb{Z}_3 \times \mathbb{Z}_4 \simeq \mathbb{Z}_{12}.$$

Concretely, the elements 3 and 4 in $\mathbb{Z}_{12}$ are non-zero, but their product is.

Problem 6

Determine the prime ideals of $\mathbb{Z} \times \mathbb{Z}$ which are not maximal.

(Continued on page 4.)

Solution

Suppose P is an ideal of $\mathbb{Z} \times \mathbb{Z}$. We define

$$P_1 = \{a \in \mathbb{Z} \mid (a, 0) \in P\}, \quad P_2 = \{b \in \mathbb{Z} \mid (0, b) \in P\}.$$

We first claim that

$$P = P_1 \times P_2$$

holds. On one hand, given $(a, b) \in P_1 \times P_2$, the relation $(a, b) = (a, 0) + (0, b)$ shows that $(a, b) \in P$. On the other, given $(a, b) \in P$, we have $(a, 0) = (a, b)(1, 0) \in P$, hence $a \in P_1$. Similarly we have $b \in P_2$, and get $(a, b) \in P_1 \times P_2$.

Now, suppose in addition that P is prime. Then we claim that one of P_i has to be $\mathbb{Z}$, and the other has to be a prime ideal of $\mathbb{Z}$. Indeed, if we have a, a' which are not in P_1 but satisfies $aa' \in P_1$, then we have $(a, 0)$ and $(a', 0)$ not in P but their product in P , showing that P_1 needs to be prime or equal to $\mathbb{Z}$. Same reasoning shows that P_2 has to be prime or equal to $\mathbb{Z}$. Both of the P_i cannot be both prime ideals of $\mathbb{Z}$, since $(1, 0)(0, 1) = (0, 0)$ would be a counterexample to the prime-ness.

This shows that $0 \times \mathbb{Z}$ and $\mathbb{Z} \times 0$ are the only non-maximal prime ideals of $\mathbb{Z} \times \mathbb{Z}$.

Problem 7

Consider the polynomial $f(X) = X^2 + 5$ in $\mathbb{R}[X]$. Determine if

$$I_{\mathbb{R}[X], f(X)} = \{f(X)g(X) \mid g(X) \in \mathbb{R}[X]\} \subset \mathbb{R}[X]$$

is a prime ideal or not.

Solution

The (complex) roots of $f(X)$ are $\pm\sqrt{5}i$, hence not real. This shows that $f(X)$ cannot be written as a product of lower-order polynomials (which would be of order 1) with real coefficients, hence is irreducible over $\mathbb{R}$. Consequently, $I_{\mathbb{R}[X], f(x)}$ is a prime ideal.

Problem 8

Consider the same polynomial $f(X)$ as above. Find a prime number p such that the ideal

$$I_{\mathbb{Z}_p[X], f(X)} = \{f(X)g(X) \mid g(X) \in \mathbb{Z}_p[X]\} \subset \mathbb{Z}_p[X]$$

is not a prime ideal.

(Continued on page 5.)

Solution

We should look for a prime number p such that $a^2 = -5$ has a solution in $\mathbb{Z}_p$. For example, in $\mathbb{Z}_2$, this equation becomes $a^2 = 1$, and $a = 1$ is a solution. Thus, $p = 2$ makes $I_{\mathbb{Z}_p[X], f(X)}$ non-prime.

Problem 9

Consider the field $F = \mathbb{Q}(e^{\frac{\pi i}{4}})$. Find an element $\alpha \in F$ such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ holds.

Solution

We need to find an element $\alpha \in F$ whose minimal polynomial is of degree 2. For example $(e^{\frac{\pi i}{4}})^2 = e^{\frac{\pi i}{2}} = i$ has $X^2 + 1$ as its minimal polynomial, hence we can take $\alpha = i$.

Problem 10

For each of the following fields, determine if it is a splitting field for some collection of polynomials over $\mathbb{Q}$ or not.

- $\mathbb{Q}(e^{\frac{\pi i}{4}})$
- $\mathbb{Q}(\beta)$, where $\beta = 1.47577\dots$ is the real number satisfying $\beta^5 = 7$

Solution

The field $\mathbb{Q}(e^{\frac{\pi i}{4}})$ is a splitting extension of $\mathbb{Q}$. The number $e^{\frac{\pi i}{4}}$ is a root of $X^8 - 1$, and by factorization we find

$$X^8 - 1 = (X^4 + 1)(X^2 + 1)(X + 1)(X - 1).$$

We claim that the roots of $X^4 + 1$ are all conjugate over $\mathbb{Q}$. Indeed, $e^{\frac{\pi i}{4}}$ and its complex conjugate $e^{-\frac{\pi i}{4}}$ are roots of the monic polynomial

$$(X - e^{\frac{\pi i}{4}})(X - e^{-\frac{\pi i}{4}}) = X^2 - \sqrt{2}X + 1,$$

which does not belong to $\mathbb{Q}[X]$. This shows that the minimal polynomial of $e^{\frac{\pi i}{4}}$ is indeed $X^4 + 1$.

Since the roots of this polynomial, which are $e^{\frac{\pi i}{4}}$, $e^{-\frac{\pi i}{4}}$, $e^{\frac{3\pi i}{4}}$, and $e^{-\frac{3\pi i}{4}}$, all belong to $\mathbb{Q}(e^{\frac{\pi i}{4}})$, this field is a splitting extension of $\mathbb{Q}$.

The field $\mathbb{Q}(\beta)$ is not a splitting extension. The number β is a root of the polynomial $X^5 - 7$, and the other roots are of the form $e^{\frac{2\pi i k}{5}}$ for $1 \leq k \leq 4$. Since these are not real, $\mathbb{Q}(\beta)$ does not contain these roots, and is not a splitting extension of $\mathbb{Q}$.

(Continued on page 6.)

Problem 11

Let $E \supset \mathbb{Q}$ be the splitting field of the polynomial $f(X) = X^3 + 5X^2 + 5$ over $\mathbb{Q}$. Determine the degree $[E : \mathbb{Q}]$. You may assume that $f(X)$ is irreducible over $\mathbb{Q}$.

Solution

There is exactly one real solution to $f(t) = 0$. To see this, we take the derivative $f'(t) = 3t^2 + 10t$, which vanishes at $t = 0$ and $t = -\frac{10}{3}$. This means that $f(t)$ takes local minima at $t = 0$, and the corresponding value is $f(0) = 5 > 0$.

Thus, there are two complex roots α and $\bar{\alpha}$, and one real root β for $f(X)$. In particular, the field $\mathbb{Q}(\beta)$, which should have degree $3 = \deg f(X)$, is not a splitting field for $f(X)$.

Since α and $\bar{\alpha}$ are conjugate complex numbers, they have the same minimal polynomial over $\mathbb{R}$ of degree 2, which should agree with the one over $\mathbb{Q}(\beta)$. We thus have $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \bar{\alpha}, \beta) = E$, which has degree 2 over $\mathbb{Q}(\beta)$.

Overall, we have

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

Problem 12

For the field E above, give a complete list of the intermediate extensions $E \supset F \supset \mathbb{Q}$. For each F , determine if $F \supset \mathbb{Q}$ is a normal extension or not. To describe F , it is enough to give a generator $\gamma \in F$ together with its minimal polynomial over $\mathbb{Q}$.

Solution

The Galois group $\text{Gal}(E/\mathbb{Q})$ of the splitting extension $E \supset \mathbb{Q}$ has order 6, and is a subgroup of S_3 , since it induces permutation of the roots $\alpha, \bar{\alpha}, \beta$. Since the order of S_3 is also 6, we have $\text{Gal}(E/\mathbb{Q}) \simeq S_3$.

The intermediate extensions of $E \supset \mathbb{Q}$ correspond to the subgroups of S_3 . The subgroups are:

- the trivial subgroup $\{e\}$, of index 6;
- the subgroups $\langle(1, 2)\rangle$, $\langle(2, 3)\rangle$, and $\langle(1, 3)\rangle$ generated by transpositions, each of index 3;
- the subgroup $A_3 = \langle(1, 2, 3)\rangle$, of index 2; and
- the entire group S_3 itself.

The corresponding intermediate extensions are:

- E itself, of degree 6 over $\mathbb{Q}$ (normal);
- $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\bar{\alpha})$, and $\mathbb{Q}(\beta)$, each of degree 3 over $\mathbb{Q}$ (not normal);

(Continued on page 7.)

- an extension $\mathbb{Q}(\gamma)$ of degree 2 over $\mathbb{Q}$ (normal); and
- $\mathbb{Q}$ itself (normal).

For a concrete choice of γ , we can take

$$\gamma = \frac{\alpha}{\bar{\alpha}} + \frac{\bar{\alpha}}{\beta} + \frac{\beta}{\alpha},$$

which is invariant under the cyclic permutation of roots $\alpha \mapsto \bar{\alpha} \mapsto \beta \mapsto \alpha$ but not under the complex conjugation. To get the minimal polynomial of γ , we use

$$\alpha + \bar{\alpha} + \beta = -5, \quad \alpha\bar{\alpha} + \bar{\alpha}\beta + \beta\alpha = 0, \quad \alpha\bar{\alpha}\beta = -5,$$

which follow from the relation between elementary symmetric polynomials and the coefficients of minimal polynomial $f(X)$. We have

$$\gamma + \bar{\gamma} = \frac{\bar{\alpha} + \beta}{\alpha} + \frac{\alpha + \beta}{\bar{\alpha}} + \frac{\alpha + \bar{\alpha}}{\beta} = -3,$$

and

$$\gamma\bar{\gamma} = 3 + \left(\frac{\bar{\alpha}\beta}{\alpha^2} + \dots \right) = 3 - 5 \left(\frac{1}{\alpha^3} + \dots \right) + \frac{-125}{-5} = -48.$$

This shows that γ is a root of $g(X) = X^2 + 3X - 48$.

END