UNIVERSITY OF OSLO

Faculty of Mathematics and Natural Sciences

Examination in:	MAT2200 — Groups, Rings and Fields
Day of examination:	Wednesday June 5, 2024
Examination hours:	15.00 – 19.00

This problem set consists of 4 pages.

Appendices:	None
Permitted aids:	None

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

All subproblems have the same weight.
Note: You must give full reasons for all your answers!

Exercise 1

a) Let H be a subgroup of G. Explain what it means that H is a **normal** subgroup of G.

b) Let G be a finite group, and let H be a subgroup of index 2. Show that H is normal in G.

c) If G is a group we define $Z(G)$ to be the **center** of G, i.e.

$$Z(G) = \{x \in G \,|\, xy = yx \ \ \forall y \in G\}$$

Show that if G has only one element of order 2, then this element is in the center of G.

Løsning.
a) H is a normal subgroup of G if the conjugate $g^{-1}Hg = H$ for any element $g \in G$.

b) Let $g \in G$, but $g \neq H$ we have $gH \neq H \neq Hg$. Since the index of H in G is 2, it follows that $gH = Hg$, ie. $g^{-1}Hg = H$.

c) Let $x \in G$ be the only element of order 2, and let $y \in G$. Then the conjugate $y^{-1}xy$ satisfies

$$(y^{-1}xy)(y^{-1}xy) = y^{-1}x^2y = y^{-1}y = e$$

It is impossible that $y^{-1}xy = e$, since then $x = e$ which has order 1. Thus $y^{-1}xy$ must have order 2 and $y^{-1}xy = x$. It follows that $xy = yx$ and $x \in Z(G)$.

(Continued on page 2.)

EXERCISE 2

a) Classify all abelian groups of order 56 up to isomorphisms.

b) Show that any group of order 56 has a normal subgroup.

Løsning.
a) The abelian groups of order 56 are

$$\mathbb{Z}_{56}, \quad \mathbb{Z}_2 \times \mathbb{Z}_{28}, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{14}$$

b) **Notice:** As the problem is stated possible solutions are the whole group or the trivial group. The text should be: *... has a non-trivial proper normal subgroup.*
According to Sylow´s third theorem there are possibly $1, 8, 15, \ldots$ Sylow-7-subgroups and $1, 3, 5, 7, 9, 11, \ldots$ Sylow-2-subgroups. The number of Sylow-p-subgroups divides the order of the group, thus the possibilities are 1 or 8 Sylow-7-subgroups and 1 ore 7 Sylow-2-subgroups. If we have 8 Sylow-7 and 7 Sylow-2 there are 48 elements of order 7 and more than 8 elements of order dividing 8. Together this exceeds the order of the group and is therefore not possible. Thus at least one of the Sylow-p-subgroups must be normal.

EXERCISE 3

a) Let F be a field and E an algebraic extension of F of degree p. Let further K be an algebraic extension of E of degree q. What is the degree of K over F?

b) Let α be an element of an algebraic extension of F such that $[F(\alpha) : F]$ is an odd number. Show that this implies that $F(\alpha^2) = F(\alpha)$.

Løsning.
a) We have $[K : F] = [K : E] \cdot [E : F] = pq$.
b) We have $F \leq F(\alpha^2) \leq F(\alpha)$ and consequently $[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)] \cdot [F(\alpha^2) : F]$. If $\alpha \notin F(\alpha^2)$ it follows that the irreducible polynomial of α over $F(\alpha^2)$ is

$$\operatorname{irr}(\alpha, F(\alpha^2)) = x^2 - \alpha^2$$

But $[F(\alpha) : F]$ is odd, and not divisible by 2, thus $\alpha \in F(\alpha^2)$ and $F(\alpha^2) = F(\alpha)$.

EXERCISE 4 Let $f(x) \in F[x]$ be a nonzero polynomial over the field F and let $\alpha \in \overline{F}$ be a root of f, i.e. $f(\alpha) = 0$. Show that the two statements below are equivalent.

i) For any $g(x) \in F[x]$ with $g(\alpha) = 0$ we have $\deg(f) \leq \deg(g)$.

(Continued on page 3.)

ii) $f(x)$ is irreducible over F.

(It might be useful to use long division of polynomials, i.e. the fact that we can write $f(x) = q(x)g(x) + r(x)$ where $\deg(r) < \deg(g)$.)

Løsning.
Suppose $f(x)$ is reducible, i.e. $f(x) = p(x)q(x)$ for some polynomials $p(x)$ and $q(x)$ of order strict less than the order of $f(x)$. Then $f(\alpha) = p(\alpha)q(\alpha) = 0$ implies that $p(\alpha) = 0$ or $q(\alpha) = 0$ (F is a field and has no zero-divisors), contradicting the conclusion of i). Thus i) implies ii).

Now, assume i) is false, and let $g(x)$ be a polynomial with $g(\alpha) = 0$ and $\deg(g) < \deg(f)$ and of minimal degree with those properties. By the division algorithm we have

$$f(x) = q(x)g(x) + r(x)$$

with $\deg(r) < \deg(g)$. But $r(\alpha) = f(\alpha) - q(\alpha)g(\alpha) = 0$, contradicting the minimality of $g(x)$.

EXERCISE 5 Let $\alpha = \sqrt{2+\sqrt{2}}$. The minimal polynomial of α over $\mathbb{Q}$ is given by $f(x) = x^4 - 4x^2 + 2$ with roots

$$\sqrt{2+\sqrt{2}}, \quad -\sqrt{2+\sqrt{2}}, \quad \sqrt{2-\sqrt{2}}, \quad -\sqrt{2-\sqrt{2}}$$

a) Show that $\mathbb{Q}(\alpha)$ is a normal extension of $\mathbb{Q}$. (Hint: Consider $\alpha(\sqrt{2-\sqrt{2}})$.)

b) Show that $G(K/\mathbb{Q})$ is a cyclic group where $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$.

(Continued on page 4.)

Løsning.
a) We have

$$\begin{aligned}\alpha(\sqrt{2-\sqrt{2}}) &= \sqrt{2+\sqrt{2}}\cdot\sqrt{2-\sqrt{2}} \\ &= \sqrt{(2+\sqrt{2})(2-\sqrt{2})} \\ &= \sqrt{2} = \alpha^2 - 2\end{aligned}$$

Thus $\sqrt{2-\sqrt{2}} = \frac{\alpha^2-2}{\alpha} \in \mathbb{Q}(\alpha)$, and all four roots are elements of $\mathbb{Q}(\alpha)$ showing that this is the splitting field of $f(x)$.
b) Define $\psi : K \to K$ by $\psi(\alpha) = \frac{\alpha^2-2}{\alpha}$. Then $\psi(-\alpha) = -\frac{\alpha^2-2}{\alpha}$, and

$$\begin{aligned}\psi(\frac{\alpha^2-2}{\alpha}) &= \frac{(\frac{\alpha^2-2}{\alpha})^2 - 2}{(\frac{\alpha^2-2}{\alpha})} \\ &= \frac{\alpha^4 - 6\alpha^2 + 4}{\alpha(\alpha^2-2)} \\ &= \alpha\frac{\alpha^4 - 6\alpha^2 + 4}{\alpha^4 - 2\alpha^2}\end{aligned}$$

We have $\alpha^4 = 4\alpha^2 - 2$ and therefore $\alpha^4 - 6\alpha^2 + 4 = -2\alpha^2 + 2$, $\alpha^4 - 2\alpha^2 = 2\alpha^2 - 2$. It follows that

$$\psi(\frac{\alpha^2-2}{\alpha}) = \alpha\frac{\alpha^4 - 6\alpha^2 + 4}{\alpha^4 - 2\alpha^2} = \alpha\frac{-2\alpha^2+2}{2\alpha^2-2} = -\alpha$$

Thus ψ has order 4 and generates $G(K/\mathbb{Q})$.