MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Examinator: Sofia Tirabassi

Make up assignment
MM5020 Abstract Algebra
7.5 hp
August 6, 2025

Please read carefully the general instructions:

- During the exam any textbook, class notes, or any other supporting material is forbidden.
- In particular, calculators are not allowed during the exam.
- In all your solutions show your reasoning, explaining carefully what you are doing. Justify your answers. A correct answer without proper justification will not award full points.
- Use natural language, not just mathematical symbols.
- Use clear and legible writing. Write preferably with a ball-pen or a pen (black or dark blue ink).
- A maximum score of 24 points can be achieved.

GOOD LUCK!

Throughout this exam, for a positive integer n, S_n denotes the symmetric group on n letters, A_n is the alternating group on n letters, and $\mathbb{Z}/n$ is the cyclic group of order n. If n is prime and we want to emphasize the field structure of $\mathbb{Z}/n$, we denote it by $\mathbb{F}_n$.

1. Let G be a group and consider H a subgroup of index 2.

   (a) (2 pts) Write an argument that shows that H is normal in G (To get full points it is not enough to cite the textbook, lectures and homework: you have to provide an argument).

   For an element $h \in H$, denote by $[h]_G$ its conjugacy class in G.

   (b) (2 pts) Show that $[h]_G \subseteq H$.

   (c) (2 pts) Prove the following: If $\mathrm{C}_G(h) \leq H$, then $[h]_G$ splits as the union of two conjugacy classes of H.

2. This exercise aims to show that A_5 is the only simple group of order 60.

   (a) (2 pts) Let G be a simple subgroup of S_n, show that either $G < A_n$ or $|G| \leq 2$.

   (b) (2 pts) Suppose now that G is a simple group of order 60, show that $n_5 = 6$.

   (c) (2 pts) Deduce from (a) and (b) that a simple group of order 60, G, is isomorphic to a subgroup of A_6. Show that $[A_6 : G] = 6$ (You can use without proof that $|A_6| = 360$.)

   (d) (2 pts) In the notation of (c), let S be the set of left cosets of G in A_6. Then G acts on S by left multiplication. Show that the action is nontrivial and admits one fixed point - that is that there is $s \in S$ such that $g \cdot s = s$ for all $g \in G$. Deduce that $G < S_5$ and conclude the proof. (You can use without proof that A_6 is simple)

3. (2 pts) List all the abelian groups of order 24 up to isomorphism (to get full points you should provide ONE group for every isomorphism class).

4. (2 pts) Let R be a unitary commutative ring and consider $I \subseteq R$ an ideal. Given $\varphi : R \to S$ a SURJECTIVE homomorphism of unitary commutative rings, show that $\varphi(I)$ is an ideal of S.

5. Let $\alpha = \sqrt[2]{2 + \sqrt{2}} \in \mathbb{C}$.

   (a) (2 pts) Find the minimal polynomial of α over $\mathbb{Q}$ (to get full points you also have to show that this is indeed the minimal polynomial).

   (b) (2 pts) Compute $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ and find a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

   (c) (2 pts) Express α^{-2} as a $\mathbb{Q}-$linear combination of the elements of the basis provided in (b).

Abstract algebra - Exam 2025.

1) G a gp and H a subgroup of index 2.

a) H has two left, respectively right cosets in G

To show H is normal in G one needs to show that these two left and right cosets coincide.

- If $g \in H$, $gH = H = Hg$
- If $g \notin H$ then $gH = G \setminus H$ because $gH \neq H$, there are only two left cosets (one being H) and the cosets give a set partition of G. On the same way one can show that if $g \notin H$ $Hg = G \setminus H$.

So for any $g \in H$ one has $gH = Hg$, namely H is a normal subgp.

b) Let $h \in H$ and $[h]_G$ its conjugacy class in G

Then $[h]_G = \{ghg^{-1} : g \in G\} \subset gHg^{-1} = H$ as H is normal in G.

c) Assume $C_G(h) = \{g \in G \mid ghg^{-1}\} \leq H$ $(\Leftrightarrow C_G(h) = C_H(h))$

Now let $[h]_H = \{ghg^{-1} : g \in G\}$. We have to show that

$\#[h]_H = \frac{1}{2} \#[h]_G$.

$C_H(h)$ by assumption.

$$\#[h]_G \Big/ \#[h]_H = \frac{\#G \Big/ \overset{=}{\boxed{\#C_G(h)}}}{\#H \Big/ \#C_H(h)} = \frac{1}{2}$$

2) a) G simple gp of S_n. Then either $G \leq A_n$ or $G \nleq A_n$

In the latter case

$G \cap A_n$ is a subgp of A_n which is normal in G because A_n is normal in S_n so $\forall h \in G \cap A_n$ and any $g \in G$ $ghg^{-1} \in A_n$ (and $ghg^{-1} \in G$ because $h \in G$).

But G is simple so $A_n \cap G = \{id\}$ ⟵ the identity permutation

Assume that $\# G \neq \{id\}$

and let $g \in G$ s t $g \neq \{id\}$

and $g \circ g \in G$. As $A_n \cap G = \{id\}$, necessarily

composition of the permutations, which is the gp law on S_n.

g is of even signature,

so $g \circ g$ is of odd signature,

therefore $g \circ g \in A_n \cap G$, so

$$g \circ g = id \Rightarrow g = g^{-1}.$$

Hence $\# G \leq 2$

b) G is a simple gp of order $60 = 2^2 \times 3 \times 5$

It therefore has n_2: 2-Sylow (of order 4)
n_3: 3-Sylow (of order 3)
n_5: 5-Sylow (of order 5)

Note that $n_i \neq 1$ $\forall i \in \{2, 3, 5\}$ since G is simple.

$n_5 \mid 60$ and $n_5 \equiv 1$ [5] so $n_5 = 1$ or 6 hence $n_5 = 6$

c) G acts on the set of its 5-Sylow by permuting them. (remember that 5-Sylow are conjugate under G). This set has 6 elements (by b)) so G is isomorphic to a subgp of S_6. By a) it is therefore iso to a subgroup of A_6 -

(d) S: left cosets of G in A_6

$$G \times S \longrightarrow S$$
$$(g, s) \longmapsto g \cdot s$$

$s \in S$ is fixed iff $\forall g \in G$ $gs = s$. As $s \in S$ it is of shape σG for some $\sigma \in A_6$.

Cl'de that the action of G on S induces a group homomorphism $\varphi: \underset{g}{G} \underset{\longmapsto}{\longrightarrow} \underset{m_g}{\mathrm{Sym}(S)} \cong S_6$ whose kernel (as any kernel) is normal in G, which is simple. Hence

$\ker \varphi = G$ or $\{1\}$

- If $\ker \varphi = G$, then $\forall g \in G$, $m_g: \underset{s}{S} \underset{\longmapsto}{\longrightarrow} \underset{gs}{S}$ is the identity map.

This means that $\forall g \in G, \forall \sigma \in A_6, \; g\sigma G = \sigma G \iff \sigma^{-1} g \sigma \in G$ $\forall \sigma \in A_6$ $\forall g \in G$

Namely $\ker \varphi = G \iff G$ is a normal subgp of A_6 which is impossible because A_6 is simple.

- So $\ker \varphi = 1$ and the action is not trivial.

Cl'de that the coset of the identity is a fixed point (as $\forall g \in G$, one has $g\,\mathrm{id}\,G = gG = G = \mathrm{id}\,G$.)
Hence the action has at least one fixed point.
Cl'de that the action of G on S splits into two actions: one, which is trivial, on the set of fixed points and the other one on the non trivial orbits of the action, let's call this set $\mathcal{O}$.
Assume $\#\mathcal{O} \geq 2$, then the latter reduced action induces a gp

homomorphism

$$\varphi : G \longrightarrow \mathrm{Sym}(\mathcal{S})$$

As G is simple and the action is not trivial (as it is the action on G on non fixed points of S), $\ker \tilde{\varphi} = \{1\}$

Hence G identifies as a subgp of $\mathrm{Sym}(\mathcal{S}) \cong S_{\#\mathcal{S}}$

where $\#\mathcal{S}$: number of non fixed points Since $\# G > 2$, G identifies as a subgroup of $A_{\#\mathcal{S}}$. And $\# G = 60 \Rightarrow \#\mathcal{S} \geq 5$, whence the action of G on S has a unique non fixed point and G is isomorphic to a subgroup of A_5 which is of order 60 so $G \cong A_5$.

3) $24 = 2^3 \times 3$

The theorem of classification of finite ab. gp tells us that any G of order 24 decomposes as a product of

$$\mathbb{Z}/_{d_i \mathbb{Z}} \quad \text{where } d_i \mid \# G \text{ and } d_i \mid d_{i+1}$$

Hence we have the following possibilities:

$$\mathbb{Z}/_{24\mathbb{Z}} \qquad \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{12\mathbb{Z}} \qquad \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{6\mathbb{Z}}$$

Indeed, write $G = \mathbb{Z}/_{d_1\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{d_r\mathbb{Z}}$

If $r = 1$ G is cyclic of order 24

If $r \geq 2$ assume $3 \mid d_i$, then as $d_i \mid d_{i+1}$ necessarily $3 \mid d_{i+1}$ so $3 \mid d_r$. For the same reason $2 \mid d_r$. As $d_r \mid 24$ we are left with two possibilities: either $d_r = 12$ or $d_r = 6$

If $d_r = 12$ necessarily $d_{r-1} = 2$ as $\prod_{i=1}^{r} d_i = 24$, so $G = \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{12\mathbb{Z}}$

If $d_r = 6$ then $d_{r-1} | 6$ and $3 \nmid d_{r-1}$ so $d_{r-1} = 2$ and because $\prod_{i=1}^{r} d_i = 24$ we deduce that $r = 3$ and $d_{r-2} = d_1 = 2$

So $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

4) R : unitary commutative ring
$\cup|$
I ideal

$\varphi : R \twoheadrightarrow S$ surjective homomorphism of unitary commutative rings

So φ is in particular an homomorphism of additive gps, hence $\varphi(I)$ is a subgroup of S.
Moreover, let $x \in \varphi(I)$, so $\exists r \in R$ s.t $\varphi(r) = x$. Let $s \in S$ as φ is surjective $\exists r_s \in R$ s.t $\varphi(r_s) = s$, whence $xs = \varphi(r)s = \varphi(r)\varphi(r_s) = \varphi(r r_s) \in \varphi(I)$ as $r r_s \in I$ because I is an ideal of R.

5) Let $\alpha = \sqrt{2+\sqrt{2}} \in \mathbb{C}$

a) $(\sqrt{2+\sqrt{2}})^2 = 2+\sqrt{2}$

$(2+\sqrt{2})^2 = 4 + 2 + 4\sqrt{2}$
$= 6 + 4\sqrt{2}$

$P(X) = X^4 - 4X^2 + 2$ is a candidate clearly α is a root.
It remains to show it is irreducible in $\mathbb{Q}(x)$

By Gauss lemma if P is irr in $\mathbb{Z}[X]$, so it is in $\mathbb{Q}[X]$.
Now you are given 3 options:
1) You use directly Eisenstein criterion (Proposition 13 on page 309 of Dummit & Foote)
2) You actually go through the proof of Eisenstein criterion

and you adapt it to this specific case.

3) a) Assume P has a root $\frac{a}{b} \in \mathbb{Q}$, wlog $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$ and $\gcd(a,b) = 1$ write

$$P(a/b) = \left(\frac{a}{b}\right)^4 - 4\left(\frac{a}{b}\right)^2 + 2$$

$$= a^4/b^4 - 4a^2/b^2 + 2 = 0$$

$\Rightarrow a^4 - 4a^2b^2 + 2b^4 = 0$

$\Rightarrow b \mid a^4$ as b divides the other terms. But a and b are relatively primes so $b = 1$

Hence $a^4 - 4a^2 + 2 = 0$ so $a \mid 2$ and $a = \pm 1$ or ± 2

none of these are roots of P, hence P is irreducible.
As it is a monic, it is the min polynomial.

b) $[\mathbb{Q}(\alpha) : \mathbb{Q}] =$ deg of a min polynomial
$= 4$

$\mathbb{Q}[\alpha]$ is generated by $\{1, \alpha, \alpha^2, \alpha^3\}$

Indeed • $\alpha \notin \mathbb{Q}$ as its min polynomial is irr over $\mathbb{Q}$
• $\{1, \alpha, \alpha^2, \alpha^3\}$ is a free family of $\# 4 = \dim(\mathbb{Q}[\alpha])$ as $\mathbb{Q}$-vector space of dim^T of $\mathbb{Q}(\alpha)$

c) $\alpha^{-2} = ?$

$\alpha^4 - 4\alpha^2 + 2 = 0 \Leftrightarrow \alpha^4 - 4\alpha^2 = -2$

$\Rightarrow \alpha^2 - 4 = -2\alpha^{-2}$

$\Rightarrow \boxed{2 - \frac{1}{2}\alpha^2 = \alpha^{-2}}$