Final Exam of Advanced Algebraic Structures
Block 1B, 2024–2025
January 22, 2025, 8:30-10:30
By Steffen Müller, Ekin Özman and Manoy Trip

university of groningen

Att	Q1	Q2	Q3	Q4	TOTAL
4					
4 pts	14 pts	4 pts	9 pts	9 pts	40 pts

Full Name: ..... **Student Number:** .....

INSTRUCTIONS

- You have 2 hours to complete the exam.
- Write your name and student number on every page you hand in.
- You have to give complete arguments for all your answers.
- No electronic devices are allowed.
- You may use results obtained in the lecture, tutorial and homework problems unless it is explicitly asked to prove such a result.
- In total you can obtain at most 36 points on this exam. Your grade for the exam is $(P+4)/4$, where P is the number of points you obtain on the exam.
- Good luck!

1. (4 Points) Let $\mathbb{F}_{p^n}$ denote the finite field of size p^n where p is a prime and $n > 2$ is an integer.

   Prove or disprove by giving a counterexample: For every integer d such that $1 \leq d \leq n$, there is a subfield of $\mathbb{F}_{p^n}$ with p^d elements.

2. Let p be a prime integer. Let K be the splitting field of $x^p - 1$ over $\mathbb{Q}$.

   (a) (3 Points) Show that the Galois group of K over $\mathbb{Q}$ is cyclic of size $p-1$.

   (b) Let $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$. Then $f(x)$ is irreducible and its discriminant is 81 (you do not need to prove this). Let α be a root of $f(x)$.

      i. (2 Points) Prove or disprove: $\mathbb{Q}(\alpha)$ is a Galois extension of $\mathbb{Q}$.

      ii. (2 Points) Let E be the compositum of the fields $\mathbb{Q}(\alpha)$ and K, namely E is the smallest field that contains both K and $\mathbb{Q}(\alpha)$ as a subfield. Show that E is Galois over $\mathbb{Q}$.

      iii. (2 Points) Let G be the Galois group of E over $\mathbb{Q}$. Does G have a normal subgroup of index $p-1$? Why, why not? (Recall that the index of a subgroup H of G is $|G|/|H|$.)

      iv. (5 Points) Let $p \equiv 2 \pmod 3$. Show that G is a cyclic group of size $3p-3$.

3. Let R be a commutative ring and let I be an ideal in R. By $\pi\colon R \to R/I$ we denote the canonical R-module homomorphism $r \mapsto r + I$. Let M be any R-module.

   (a) (2 Points) Let $\alpha\colon \mathrm{Hom}_R(R/I, M) \to \mathrm{Hom}_R(R, M)$ be defined by $\alpha(f) := f \circ \pi$ for $f \in \mathrm{Hom}_R(R/I, M)$. Show that α is an injective R-module homomorphism.

(b) (4 points) Show that the sequence

$$0 \longrightarrow \mathrm{Hom}_R(R/I, M) \xrightarrow{\alpha} \mathrm{Hom}_R(R, M) \xrightarrow{\gamma} \mathrm{Hom}_R(I, M)$$

(where γ is defined by restricting maps $R \to M$ to maps $I \to M$) is an exact sequence of R-modules.

(c) (3 points) Show that γ is not always surjective, for instance using the example $R = \mathbb{Z}$, $I = 2\mathbb{Z}$ and $M = \mathbb{Z}/2\mathbb{Z}$.

4. Let R be a commutative ring. We say that an R-module $M \neq \{0\}$ is *simple* if its only R-submodules are M and $\{0\}$.

(a) (3 points) Let $I \subsetneq R$ be an ideal of R. Show that the R-module R/I is simple if and only if I is maximal.

(b) (3 points) Show that an R-module $M \neq \{0\}$ is simple if and only if there exists a maximal ideal I of R such that $M \cong R/I$. (Hint: Consider, for $x \in M$, the submodule Rx of M. You may use without proof that $a \mapsto ax$ defines an R-module homomorphism $R \to M$.)

(c) (3 points) Using (b), find an example of a $\mathbb{Z}$-module $M \neq \{0\}$ such that M has no simple $\mathbb{Z}$-submodules $N \neq \{0\}$.