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

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

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

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.

   Disprove: Let d be any integer such that $1 \leq d \leq n$ and $d \nmid n$. For instance let $d = n - 1$.

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 $p - 1$.
   Since any root of $x^p - 1$ is a power of ζ_p, we have $\mathbb{Q}(\zeta_p) = K$ by definition of the splitting field. Let f be the map between the group of units in $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$ to the Galois group of K over $\mathbb{Q}$ given by $a \mapsto \sigma_a : \zeta_p \mapsto \zeta_p^a$. For $a, b \in (\mathbb{Z}/p\mathbb{Z})^*$ we get $f(ab) = \sigma_{ab}$ where $\sigma_{ab} : \zeta_p \mapsto \zeta_p^{ab} = (\zeta_p^a)^b = \sigma_b \circ \sigma_a(\zeta_p)$ hence $f(ab) = f(a) \circ f(b)$ i.e. f is a group homomorphism. Let a be in the kernel of f then σ_a is the identity homomorphism i.e. $\zeta_p = \zeta_p^a$ for $a \in (\mathbb{Z}/p\mathbb{Z})^*$ which means that $a = 1$ and f is injective. The degree $|K : \mathbb{Q}|$ is the degree of the minimal polynomial of ζ_p. We proved in class that this minimal polynomial is $x^{p-1} + \ldots + x + 1$ hence the degree of K over $\mathbb{Q}$ is $p - 1$. This implies that the size of the Galois group of K over the rationals is $p - 1$ which is equal to the size of $(\mathbb{Z}/p\mathbb{Z})^*$, hence f is an isomorphism.

   (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 $\mathbb{Q}$.
   Since the discriminant of f is a square in $\mathbb{Q}$, by a result proved in class, the splitting field of f over the rationals is of degree 3. Since the splitting field of f over $\mathbb{Q}$ contains $\mathbb{Q}(\alpha)$ and the degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is 3 we can conclude that $\mathbb{Q}(\alpha)$ is the splitting field of f over $\mathbb{Q}$ hence Galois.

   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 $\mathbb{Q}$.
   Soln: We know that $\mathbb{Q}(\alpha)$ is Galois over $\mathbb{Q}$ by previous part and K is Galois over $\mathbb{Q}$ by definition. Then their compositum $E = \mathbb{Q}(\alpha, \beta)$ is also Galois over $\mathbb{Q}$ by a result we proved in the lecture.

   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 $|G|/|H|$.)
   Soln: We know that $E/\mathbb{Q}$ is Galois by previous part. By definition of E, K is a subfield of E and K is Galois over $\mathbb{Q}$ with Galois group of size $p - 1$. By Galois theory, $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to G/H where $H = \mathrm{Gal}(E/K)$. By Part (b) we know that the size of G/H is $p - 1$ hence H is the normal subgroup of G of index $p - 1$, moreover H is the fixing subgroup of K.

   iv. (5 Points) Let $p \equiv 2 \pmod 3$. Show that G is a cyclic group of size $3p - 3$.
   Soln: By assumption $(3, p - 1) = 1$ hence by a result from class, the degree of $E/\mathbb{Q}$ is the product of degrees of K over $\mathbb{Q}$ and $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ which is $3(p - 1)$. We know by part (ii) that E is Galois over $\mathbb{Q}$ and the Galois group is isomorphic to a subgroup of the direct product of the Galois groups

of $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ and $\mathrm{Gal}(K/\mathbb{Q})$ which is $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^*$. But this direct product has size precisely $3 * (p-1)$ hence G is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^*$ and has size $3p-3$. In other words, G is cyclic of order $3p-3$.

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.

   Soln: To show α is an R-mod-hom, verify the two axioms directly from the definition. If $f \in \ker(\alpha)$, then $f(a+I) = 0$ for all $a \in R$, so f is the zero map (since π is surjective).

   (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.

   Soln: By (a), we only need to show $\mathrm{im}\alpha = \ker\gamma$.

   $\subset$: Let $f \circ \pi \in \mathrm{im}\alpha$, then $f(\pi(i)) = f(0) = 0$ for all $i \in I$, so $f \circ \pi \in \ker\gamma$.

   $\supset$: Let $g \in \ker\gamma$, so $g(i) = 0$ for all $i \in I$. Define $f : R/I \to M$ by $f(r+I) := g(i)$. This is well-defined, since if $r + I = r' + I$, then $g(r) - g(r') = 0$, since $r - r' \in I$. To show g is an R-mod-hom, verify the two axioms directly from the definition.

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

   Soln: If $f \in \mathrm{Hom}(\mathbb{Z}, M) = \{0, \pi\}$, then $\gamma(f) = 0$ by definition. Let $\psi : 2\mathbb{Z} \to M$ be defined by $\psi(2x) := x \bmod 2$. Then ψ is a $\mathbb{Z}$-mod-hom (show directly), but is nontrivial, hence not in the image of γ.

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.

   Soln: First show that the submodules N of R/I are of the form R/J, where J is an ideal of R and $J \supset I$. E.g. one can prove this by looking at the preimage of N under $\pi : R \to R/I$. So R/I is simple iff there is no ideal J of R that contains I iff 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 $R \to M$.)

   Soln: One direction is clear by (a). So suppose M is simple, then the submodule Rx of M is either M (if $x \neq 0$, since $x \in Rx$) or $\{0\}$. Let $\phi : R \to M$ defined by $a \mapsto ax$. Then $R/\ker\phi \cong \mathrm{im}\phi = Rx = M$, and $\ker\phi$ is maximal by (a).

   (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 $N \neq \{0\}$.

   Soln: Take $M = \mathbb{Z}$. By (b) a submodule N of M is simple iff it's isomorphic to $\mathbb{Z}/I$ for some maximal ideal I of $\mathbb{Z}$. But all nonzero ideals of $\mathbb{Z}$ are of the form $I = n\mathbb{Z}$, hence $\mathbb{Z}/I$ is finite. And the nonzero submodules of $\mathbb{Z}$ are also of the form $N = n\mathbb{Z}$, hence infinite.