Resit Exam of Advanced Algebraic Structures
Block 1B, 2024–2025
April 9, 2025, 11:45 – 13:45

By Steffen Müller, Ekin Özman and Manoy Trip

Att	Q1	Q2	Q3	Q4	TOTAL
4					
4 pts	14 pts	4 pts	4 pts	14 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. Let E be the splitting field of $x^{19}-2$ over $\mathbb{Q}$.
   (a) (3 Points) Show that $E = \mathbb{Q}(\omega, \sqrt[19]{2})$ where $\omega = e^{2\pi i/19}$.
   Solution: $\mathbb{Q}(\omega, \sqrt[19]{2})$ clearly contains all roots of $x^{19}-2$. Conversely any field that contains all roots of $x^{19}-2$ must contain $\sqrt[19]{2}$ and $\omega\sqrt[19]{2}$ hence, must contain $\sqrt[19]{2}$ and ω therefore $E = \mathbb{Q}(\omega, \sqrt[19]{2})$.
   (b) (4 Points) Show that the size of the Galois group G of E over $\mathbb{Q}$ is $19 \cdot 18$.
   Solution: The degree of $A = \mathbb{Q}(\sqrt[19]{2})$ over $\mathbb{Q}$ is 19 since $x^{19}-2$ is irreducible over $\mathbb{Q}$ by Eisenstein. The degree of $B = \mathbb{Q}(\omega)$ over $\mathbb{Q}$ is 18 since 19 is prime hence minimal polynomial of ω over $\mathbb{Q}$ is $x^{18}+x^{17}+\ldots+x+1$. Note that E is composite field of A and B and since $(|A:\mathbb{Q}|, |B:\mathbb{Q}|) = 1$, $|E:\mathbb{Q}| = 19 \cdot 18$.
   (c) (3 Points) Show that there is an intermediate field L such that $\mathbb{Q} \subset L \subset E$ and L corresponds to a normal subgroup H of G of size 19.
   Solution: Let $L = \mathbb{Q}(\omega)$, since L is the splitting field of $x^{18}+x^{17}+\ldots+x+1$, it is Galois over $\mathbb{Q}$. By main theorem of Galois theory $L = E^H$ for a normal subgroup H of the Galois group of E over $\mathbb{Q}$ where H is of size 19.
   (d) (4 Points) Prove or disprove: The Galois group G of E over $\mathbb{Q}$ is abelian.
   Solution: It is not abelian since if it was abelian all subgroups would be normal hence all intermediate fields M such that $\mathbb{Q} \subset M \subset E$ would be Galois. However this does not hold for $M = \mathbb{Q}(\sqrt[19]{2})$.

2. (4 Points) Let p be a prime integer and consider $f(x) = x^p - x - 1$ over $\mathbb{F}_p[x]$. Let α be a root of $f(x)$ in the algebraic closure of $\mathbb{F}_p$. Show that $\mathbb{F}_p(\alpha)$ is a Galois extension of $\mathbb{F}_p$. (Hint: if α is a root of $f(x)$ then what about $\alpha + i$ for $1 \le i \le p-1$?)
   Solution: $f(x) = x^p - x - 1$ is separable over $\mathbb{F}_p[x]$ since $f'(x) = -1$. Let α be a root of $f(x)$ then for all $i \in \mathbb{F}_p$, $f(\alpha+i) = (\alpha+i)^p - (\alpha+i) - 1 = \alpha^p + i - \alpha - i - 1 = 0$ since $f(\alpha) = 0$ and $i \in \mathbb{F}_p$. Hence $\mathbb{F}_p(\alpha)$ is splitting field of $f(x)$ therefore Galois.

3. Let $K := \mathbb{Q}(t)$ be the field of rational functions in one variable t over $\mathbb{Q}$. This is the field of fractions of the polynomial ring $R := \mathbb{Q}[t]$ (so every element $q(t) \in K$ can be written as $q(t) = g(t)/h(t)$ with $g, h \in R$). Then K has the structure of an R-module via

$$R \times K \to K\,, \quad (f(t), q(t)) \mapsto f(t)q(t)$$

(you do not have to show that this gives K the structure of an R-module).

(a) (3 points) Let $\varphi \in \mathrm{Hom}_R(K, R)$. By considering $\varphi(t^{-n})$ for positive integers n, show that $\varphi(1) = 0$.

Solution: $\varphi(t^{-n}) = t^{-n}\varphi(1) \in R$, so $\varphi(1)$ is divisible by t^n for all n, hence it's 0.

(b) (1 point) Deduce that $\#\mathrm{Hom}_R(K, R) = 1$.

Solution: For $\varphi \in \mathrm{Hom}_R(K, R)$ and for all $a \in K$, we have $\varphi(a) = a\varphi(1) = 0$.

4. Let $R := \mathbb{Q}[t]$ be the polynomial ring over the rational numbers $\mathbb{Q}$ in one variable t. Then $\mathbb{Q}$ has the structure of an R-module via

$$R \times \mathbb{Q} \to \mathbb{Q}\,, \quad (f(t), a) \mapsto f(0) \cdot a$$

(you do not have to prove this).

(a) (1 point) Find the torsion submodule $\mathrm{Tor}_R(\mathbb{Q})$ $= \{r \in \mathbb{Q} \mid \exists\, p(t) \in \mathbb{Q}[t] \text{ s.t. } p(0)\cdot r = 0\}$ let $p(t) = t$ so $p(0) = 0$ and for any $r \in \mathbb{Q}$, $p(0)r = 0$ hence $\mathrm{Tor}_R(\mathbb{Q}) = \mathbb{Q}$.

Solution. ~~$a \in \mathrm{Tor}_R(\mathbb{Q})$ implies $f(0) \cdot a = 0$ for all $f \in R$, so taking $f = 1$ shows $\mathrm{Tor}_R(\mathbb{Q}) = 0$.~~

(b) (5 points) Show that there is an exact sequence of R-modules

$$0 \to tR \to R \to \mathbb{Q} \to 0\,.$$

Solution. Let $\varphi = \mathrm{id} : tR \to R$ and $\psi : R \to \mathbb{Q}$ be given by $f(t) \mapsto f(0)$. Then

- φ is clearly an injective hom;
- ψ is a hom: clearly additive and $\psi(g(t)f(t)) = g(0)f(0) = g(0)\psi(f(t)) = g(t) \cdot \psi(f(t))$; it's surjective using constant polynomials.
- Both $\ker(\psi)$ and $\mathrm{im}(\varphi)$ consist of exactly the constant polynomials.

(c) (4 points) Show that no R-submodule of R is isomorphic to $\mathbb{Q}$.

Solution. Suppose $M \subset R$ is an R-submodule of R and $\varphi : \mathbb{Q} \to M$ is an R-mod-isom. Since φ is an isom, there is $0 \neq b \in \mathbb{Q}$ such that $\varphi(b) = t$ and $1/t \in M \subset R$ since $1/b \in \mathbb{Q}$; contradiction.

(d) (2 points) Show that the exact sequence in (b) is not split.

Solution. Being split would imply $R \cong tR \oplus \mathbb{Q}$, so that $\mathbb{Q}$ would be isomorphic to an R-submodule of R. Now use (c).

(e) (2 points) Is $\mathbb{Q}$ a projective R-module?

Solution. For a projective R-module M, every short exact sequence ending in M is split, so the answer is 'no' by (d).