Final Exam — Advanced Algebraic Structures (WBMA011-05)

Wednesday January 25, 2022, 8:30h–10:30h

University of Groningen

Instructions

1. Write your name and student number on every page you hand in.
2. All answers need to be accompanied with an explanation or a calculation.
3. You may use results obtained in tutorial problems.
4. In total you can obtain at most 90 points on this exam. Your final grade is $(P+10)/10$, where $P \leq 90$ is the number of points you obtain on the exam.
5. We wish you success!

Problem 1 (4+6+6+6+8 = 30 points)

Let $\zeta = e^{2\pi i/5}$ be a primitive fifth root of unity.

(a) Find the minimal polynomial of ζ over $\mathbb{Q}$.

(b) Show that there exists a cyclic extension of degree 5 over $\mathbb{Q}(\zeta)$.

(c) Let $\alpha = \zeta + \zeta^{-1}$. Show that $\mathbb{Q}(\alpha)$ is a subextension of $\mathbb{Q}(\zeta)$ of degree 2 over $\mathbb{Q}$.

(d) Show that there are no other subextensions of $\mathbb{Q}(\zeta)$ of degree 2 over $\mathbb{Q}$.

(e) Let τ be the nontrivial element of $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$. Show that $\tau(\alpha) = \zeta^2 + \zeta^{-2}$.

[[Solution:

(a) The minimal polynomial of ζ is the fifth cyclotomic polynomial

$$\Phi_5(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1.$$

(b) Let $L = \mathbb{Q}(\zeta, \sqrt[5]{2})$. We have $\sqrt[5]{2} \notin \mathbb{Q}(\zeta)$ since the degree $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ is not divisible by 5. Since $\mathbb{Q}(\zeta)$ contains a primitive fifth root of unity, the extension $L/\mathbb{Q}(\zeta)$ is cyclic of degree 5 by what we proved in the lecture.

(c) The element ζ is a root of

$$(x - \zeta)(x + \zeta) = x^2 - \alpha x + 1,$$

so ζ has degree at most 2 over $\mathbb{Q}(\alpha)$. On the other hand $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ since $\alpha = \zeta + \overline{\zeta}$ is real, whereas ζ is complex. So $[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)] = 2$. Since $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(5) = 4$, this implies that $\mathbb{Q}(\alpha)$ has degree 2 over $\mathbb{Q}$.

(d) We showed in the lecture that the map

$$\theta\colon \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \to (\mathbb{Z}/5\mathbb{Z})^\times, \quad \sigma \mapsto a \bmod 5, \text{ where } \sigma(\zeta) = \zeta^a,$$

is an isomorphism. The group $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$ is cyclic, so there exists exactly one subgroup of index 2. By the Galois correspondence, there is only one subextension of $\mathbb{Q}(\zeta)/\mathbb{Q}$ of degree 2 over $\mathbb{Q}$.

(e) The element 2 has multiplicative order 4 modulo 5, hence is a generator of $(\mathbb{Z}/5\mathbb{Z})^\times$. This means the Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ is generated by σ with $\sigma(\zeta) = \zeta^2$. Since the restriction map $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ is surjective, the image of σ in the latter group is the nontrivial element τ. Therefore,

$$\tau(\alpha) = \sigma(\alpha) = \sigma(\zeta + \zeta^{-1}) = \zeta^2 + \zeta^{-2}.$$

]]

Problem 2 (6+4+10 = 20 points)

Let K be a field with $\mathrm{char}(K) = 0$, and let $f \in K[x]$ be an irreducible polynomial of the form

$$f(x) = x^4 + bx^2 + 1$$

with $b \in K$. Let $L = K(\alpha)$ where α is a root of f.

(a) Show that $\pm\alpha, \pm 1/\alpha$ are the pairwise distinct roots of f.

(b) Show that L/K is a Galois extension.

(c) Determine the Galois group $\mathrm{Gal}(L/K)$.

[[Solution:

(a) If γ is a root of f, so are $-\gamma$ and $1/\gamma$:

$$f(-\gamma) = (-\gamma)^4 + b(-\gamma)^2 + 1 = \gamma^4 + b\gamma^2 + 1 = f(\gamma) = 0,$$
$$f(1/\gamma) = (1/\gamma)^4 + b(1/\gamma)^2 + 1 = f(\gamma)/\gamma^4 = 0.$$

So $\pm\alpha, \pm 1/\alpha$ are roots of f. These are distinct: if $\gamma = -\gamma$ for a root γ of f, then $\gamma = 0$ (using $\mathrm{char}(K) = 0$). If $\gamma = 1/\gamma$, then $\gamma = \pm 1$. If $\gamma = -1/\gamma$, then $\gamma = \pm i$. But neither of these can have $f(x)$ as its minimal polynomial, since their minimal polynomials have degrees 1 or 2, whereas f has degree 4.

(b) The extension is normal by (a). It is automatically separable since $\mathrm{char}(K) = 0$. Hence it is normal.

(c) The elements of $\mathrm{Gal}(K(\alpha)/K)$ are in bijection with the roots of the minimal polynomial $f(x)$ of α. Let σ be the Galois automorphism with $\sigma(\alpha) = -\alpha$, let τ be the one with $\tau(\alpha) = 1/\alpha$, and ρ the one with $\rho(\alpha) = -1/\alpha$. Then the Galois group is

$$\mathrm{Gal}(L/K) = \{\mathrm{id}, \sigma, \tau, \sigma\tau\}.$$

All three nontrivial elements have order 2:

$$\begin{aligned}
\sigma^2(\alpha) &= \sigma(-\alpha) = -\sigma(\alpha) = -(-\alpha) = \alpha, \\
\tau^2(\alpha) &= \tau(1/\alpha) = 1/\tau(\alpha) = 1/(1/\alpha) = \alpha, \\
\rho^2(\alpha) &= \rho(-1/\alpha) = -1/\rho(\alpha) = -1/(-1/\alpha) = \alpha.
\end{aligned}$$

So the Galois group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

]]

Problem 3 (7+6+6+7+8+6 = 40 points)

Let $R = \mathbb{Z}[w]$, where $w^2 = -2$. Let M be the R-module $\mathbb{Z}/3\mathbb{Z}$, with scalar multiplication

$$R \times M \to M\,; \quad (a + bw)m = \bar{a}m + \bar{b}m$$

and let N be the R-module $\mathbb{Z} \times \mathbb{Z}$, with scalar multiplication

$$R \times N \to N\,; \quad (a + bw)(x, y) = (ax - 2by, ay + bx)$$

(you do not need to prove that M and N are R-modules).

(a) Show that N is free of rank 1.

(b) Use (a) to show that $\mathrm{Tor}_R(M \oplus N) \cong M$ (here and below, "$\cong$" means "R-module-isomorphism").

(c) Is the R-module $M \oplus N$ projective?

(d) Let I be the ideal $I = (1 - w)R$ of R. Show that $R/I \cong M$. (Hint: One way to approach this problem is to first find $\mathrm{Ann}_R(M)$. Also note that $3 = (1 - w)(1 + w)$.)

(e) Show that $\mathrm{Hom}_R(M \oplus N, M) \cong M \oplus M$.

(f) Show that $M \otimes_R M \cong M$.

[[Solution:

(a) The map $\varphi\colon N \to R$ sending (x, y) to $x + yw$ is clearly a group homomorphism. By explicit computation, φ is an R-module homomorphism. It is bijective, since $w \notin \mathbb{Q}$, so $x, y \in \mathbb{Z}$ implies $x + wy \neq 0$.

(b) An element $a = (m, x, y) \in M \oplus N$ is torsion if and only if there is a nonzero $r \in R$ such that $rm = 0$ and $r(x, y) = 0$. Since R is a domain and N is free, this implies $(x, y) = 0$. But $r = 3 \in R \setminus \{0\}$ satisfies $rm = 0$ for all $m \in M$. Hence $\mathrm{Tor}_R(M \oplus N) = M \oplus \{0\}$, which is isomorphic to M via the R-module-isomorphism $(m, 0) \mapsto m$.

(c) Suppose that $M \oplus N$ is projective. Then $M \oplus N \oplus Q =: F$ is a free R-module for some R-module Q. Suppose $F \cong \oplus_{i \in I} R$, then, since R is a domain, any $f = \sum_i \lambda_i a_i \in F$ satisfies $rf = 0$ for some $r \in R$ only if either $r = 0$ or all $a_i = 0$, so $f = 0$. Hence F is torsion-free. But by (b), $(m, 0, 0, 0) \in \mathrm{Tor}_R(F)$ for every $m \in M$, a contradiction.

(d) Let $r = a + bw \in \mathrm{Ann}_R(M)$, so $a + b \equiv 0 \pmod 3$. This implies $r = a(1-w) + 3k$ for some $k \in \mathbb{Z}$ and every such r is in $\mathrm{Ann}_R(M)$. Hence $\mathrm{Ann}_R(M)$ is the ideal generated by $1 - w$ and 3, and by the hint, this is just I. Now $M = \{r\bar{1} : r \in R\}$ is cyclic, so by tutorials, $R/I \cong M$.

(e) By tutorials, $\mathrm{Hom}_R(M \oplus N, M) \cong \mathrm{Hom}_R(M, M) \oplus \mathrm{Hom}_R(N, M)$. By (a), $\mathrm{Hom}_R(N, M) \cong \mathrm{Hom}_R(R, M)$ and the latter is $\cong M$ for any R-module M, as shown in the lectures. Since M is cyclic, any $f \in \mathrm{Hom}_R(M, M)$ is determined by $f(\bar{1})$. To conclude, show that $f_i(\bar{m}) = \overline{im}$ is indeed in $\mathrm{Hom}_R(M, M)$ for $i = 0, 1, 2$, and that $f_i \mapsto \bar{i}$ defines an R-module-homomorphism.

(f) Using (d), $M \otimes_R M \cong R/I \otimes_R R/I$. By tutorials, $R/I \otimes_R R/I \cong (R/I)/(I(R/I))$, but $I(R/I) = 0$.

End of test (90 points)