Final Exam — Advanced Algebraic Structures (WBMA16000)

Wednesday January 29, 2019, 15:00h–18.00h

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 homework or 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.

Problem 1 (5+5 points) (Module Homomorphisms)

(a) Show that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$ is trivial.

[[Solution. Let $f\colon \mathbb{Q} \to \mathbb{Z}$ be a $\mathbb{Z}$-module homomorphism. Let $x \in \mathbb{Q} \setminus \{0\}$. Then, for every $a \in \mathbb{Z} \setminus \{0\}$, we have

$$a \cdot f(x/a) = f(x) \in \mathbb{Z},$$

and since $f(x/a) \in \mathbb{Z}$, we find that $f(x)$ is divisible by every integer, hence must be 0.]]

(b) Let R be a commutative ring and let $n \geq 1$ be an integer. Show that $\mathrm{Hom}_R(R^n, R) \cong R^n$.

[[Solution: One way to get started is to first define a map $\varphi_x\colon R^n \to R$ for every $x = (x_1, \ldots, x_n) \in R^n$, which sends $y = (y_1, \ldots, y_n) \in R^n$ to $\varphi_x(y) = \sum_{i=1}^n x_i y_i$.) Show that

(i) φ_x is linear

(ii) $\Psi(x) = \varphi_x$ is linear

(iii) Ψ is injective

(iv) Ψ is surjective.

One can also show that $f \in \mathrm{Hom}_R(R^n, R)$ is given by its effect on a fixed basis of R^n.]]

Problem 2 (5+4+6+5 points) (Tensor products)

(a) Find a nontrivial $\mathbb{Z}$-module M such that $M \otimes_{\mathbb{Z}} M \cong M$ and $M \not\cong \mathbb{Z}$. [[Solution: For $M = \mathbb{Z}/n\mathbb{Z}$, with $n > 1$, we have $M \otimes_{\mathbb{Z}} M \cong \mathbb{Z}/d\mathbb{Z}$, where $d = \gcd(n, n) = n$.]]

(b) Let R be a commutative ring, let I be an ideal of R and let M be an R-module. Then

$$IM = \left\{ \sum_{i=1}^{n} a_i m_i : n \geq 0, a_i \in I, m_i \in M \text{ for all } i \right\}$$

is a submodule of M (you do not need to prove this). Show that there is a unique R-module-homomorphism

$$f\colon (R/I) \otimes_R M \to M/IM$$

such that $f((r+I) \otimes m) = (rm) + IM$ for all $r + I \in R/I$ and $m \in M$.

[[Solution: This follows immediately from the universal property of the tensor product.]]

(c) Show that f in (b) is an isomorphism. (Hint: Find the inverse function.)

[[Solution: The inverse map is

$$g(m + IM) = (1 + I) \otimes m$$

. Need to show

(a) g is well-defined
(b) $f \circ g = \mathrm{id}$
(c) $g \circ f = \mathrm{id}$

]]

(d) Find an example of a commutative ring R, an ideal I of R and an R-module M such that $I \otimes_R M \ncong IM$.

[[Solution: Take $R = \mathbb{Z}, I = n\mathbb{Z}, M = \mathbb{Z}/n\mathbb{Z}$, where $n \geq 2$. Then $IM = \{0\}$, but $I \otimes_R M \cong M$.

Problem 3 (5+4+6 points) (Projective modules)

(a) Let $n > 1$ be an integer. Show that the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ is not projective.

[[Solution: First method: A $\mathbb{Z}$-module M is projective iff there is a free $\mathbb{Z}$-module F and a $\mathbb{Z}$-module Q such that $F \cong M \oplus P$. But $\mathbb{Z}/n\mathbb{Z}$ has nontrivial elements of finite order, whereas a free module does not. Second method: Let $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the canonical surjection and let $h\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the identity. If $\mathbb{Z}/n\mathbb{Z}$ were projective, there would be a homomorphism $\tilde{h}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ such that $h = \pi \circ \tilde{h}$. But all homomorphisms $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ are trivial.

(b) Deduce that a finitely generated $\mathbb{Z}$-module is projective if and only if it's free.

[[Solution: Free $\Rightarrow$ projective was shown in the lectures. By the structure theorem for finitely generated abelian groups, such a $\mathbb{Z}$-module M is not free if and only if $M \cong N \oplus \mathbb{Z}/n\mathbb{Z}$ for some submodule N of M and $n > 1$. Since $\mathbb{Z}/n\mathbb{Z}$ is not projective, neither is M, using the characterization in the first method above.]]

(c) Let p be a prime, let $n \geq 1$ be an integer and let R be the ring $\mathbb{Z}/p^n\mathbb{Z}$. Show that the following property holds for R if and only if $n = 1$: Every submodule of a projective R-module is itself projective.

[[Solution: The R-module $M = R$ contains a submodule N isomorphic to $\mathbb{Z}/p\mathbb{Z}$ (for instance using Cauchy's theorem in group theory). Suppose that R has the mentioned property, there is some $\ell > 0$ such that $R^\ell \cong N \oplus Q$, where Q is a submodule of R^ℓ. But then n must be equal to 1, since N is not a direct summand of $\mathbb{Z}/p^n\mathbb{Z}$ for $n > 1$.

Conversely $R = \mathbb{Z}/p\mathbb{Z}$ is a field, hence all R-modules are free, so R has the desired property.]]

Problem 4 (3+6+6+6 points) (Cyclotomic and cyclic extensions)

For a positive integer n, let $\Phi_n(x) \in \mathbb{Q}[x]$ be the n-th cyclotomic polynomial over $\mathbb{Q}$ and let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$.

(a) Write down $\Phi_n(x) \in \mathbb{Q}[x]$ for $n = 7$ and $n = 17$.

(b) For each $n \in \{7, 17\}$ prove that

(i) there exists $a_n \in \mathbb{Q}$ and $b_n \in \mathbb{Q}(\zeta_n) \setminus \mathbb{Q}$ such that $b_n^2 = a_n$;

(ii) if $a'_n \in \mathbb{Q}$, $b'_n \in \mathbb{Q}(\zeta_n) \setminus \mathbb{Q}$ satisfy $b'^2_n = a'_n$, then $a'_n = \lambda^2 a_n$ for some $\lambda \in \mathbb{Q}$.

(c) Prove that there exists $f(x) \in \mathbb{Q}[x]$ such that $f(\cos(2\pi/17)) = b_{17}$, but there exists no $g(x) \in \mathbb{Q}[x]$ such that $g(\cos(2\pi/7)) = b_7$.

(d) Give an example of a cyclic extension of $\mathbb{Q}(\zeta_7)$ of degree 7 and an example of a cyclic extension of $\mathbb{Q}(\zeta_{17})$ of degree 17.

Solution:

(a) For a prime number p, we have $\Phi_p(x) = x^{p-1} + \cdots + 1$. So $\Phi_7(x) = \sum_{i=0}^{6} x^i$, $\Phi_{17}(x) = \sum_{i=0}^{16} x^i$.

(b) From lectures, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a Galois extension with Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$. When n is a prime number p, $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$, which is a cyclic group of even order $p-1$. Thus $\mathbb{Z}/(p-1)\mathbb{Z}$ has a unique subgroup of order $(p-1)/2$, giving, by the Galois correspondence, a unique subfield K of $\mathbb{Q}(\zeta_p)$ of degree $2 = (p-1)/((p-1)/2)$ over $\mathbb{Q}$. From lectures, any quadratic extension of $\mathbb{Q}$ of degree 2 is of the form $\mathbb{Q}(\sqrt{a})$ for some $a \in \mathbb{Q} \setminus \mathbb{Q}^2$. Suppose $\sqrt{a'} \in \mathbb{Q}(\sqrt{a}) = K$ ($a' \in \mathbb{Q}$, not a square) and let σ be the non trivial element of $\mathrm{Gal}(K/\mathbb{Q})$, so $\sigma(\sqrt{a}) = -\sqrt{a}$. Then $\sigma(\sqrt{a'})^2 = a'$ and thus, since $\sqrt{a'} \notin \mathbb{Q}$, $\sigma(\sqrt{a'}) = -\sqrt{a'}$. Thus $\sqrt{a/a'} \in \mathbb{Q}$.

(c) Since $\cos(2\pi/n) = \frac{\zeta_n + \zeta_n^{-1}}{2}$, we have $\mathbb{Q}(\cos(2\pi/n)) \subset \mathbb{Q}(\zeta_n)$. In particular $\cos(2\pi/n)$ is algebraic, so $\mathbb{Q}(\cos(2\pi/n)) = \mathbb{Q}[\cos(2\pi/n)]$. The problem is then equivalent to showing that $\mathbb{Q}(b_7) \not\subset \mathbb{Q}(\cos(2\pi/7))$ and $\mathbb{Q}(b_{17}) \subset \mathbb{Q}(\cos(2\pi/17))$. For this we use the Galois correspondence. For any $n \geq 3$, we have $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\cos(2\pi/n))] \leq 2$ since ζ_n is a root of $(x - \zeta_n)(x - \zeta_n^{-1}) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1 \in \mathbb{Q}(\cos(2\pi/n))$. But also $\cos(2\pi n)$ is fixed by the non-trivial $-1 \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, so the degree is 2.

Thus when $n = 7$, by the tower law, we have $[\mathbb{Q}(\cos(2\pi/n) : \mathbb{Q}] = 3$ and hence (again by the tower law) the degree two $\mathbb{Q}(b_7)$ cannot be contained in $\mathbb{Q}(\cos(2\pi/n))$.

When $n = 17$, $(\mathbb{Z}/n\mathbb{Z})^* \cong \mathbb{Z}/2^4\mathbb{Z}$ and, with this identification, the subgroup fixing $\mathbb{Q}(\cos(2\pi/n))$ is thus generated by $8 \bmod 2^4$, which is contained in every non-trivial subgroup and in particular in the subgroup corresponding to $\mathbb{Q}(b_7)$.

(d) Let K be a field of characteristic coprime with n and containing a primitive n-th root of 1. From lectures, for every $a \in K$ which is not a d-th power in K for any $d > 1$, $d \mid n$, the splitting field of $x^n - a$ is a cyclic extension of K of degree n.

The polynomials $x^7 - 2 \in \mathbb{Q}[x]$ and $x^{17} - 2 \in \mathbb{Q}[x]$ are irreducible by Eisenstein's criterion with 2. Let $n \in \{7, 17\}$. Thus, by the tower law, if $\mathbb{Q}(\zeta_n)$ contains an n-th root of 2, we have $n \mid [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = n - 1$. So: splitting field of $x^n - 2$ over $\mathbb{Q}(\zeta_n)$ works.

Problem 5 (6+6+6+6 points) (Galois group of the splitting field of a cubic)

Let K be a field of characteristic different from 2 and 3 and consider a separable polynomial

$$f(x) = x^3 + ax^2 + bx + c \in K[x].$$

Let L be the splitting field of f over K and let $G = \mathrm{Gal}(L/K)$.

(a) Show that G is isomorphic to a subgroup of S_3.

(b) Assume now that $f(x)$ is irreducible in $K[x]$; deduce that $G \cong A_3$ or $G \cong S_3$. Let $\alpha_1, \alpha_2, \alpha_3 \in L$ be the roots of $f(x)$. Define

$$\Delta = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2.$$

   (i) Prove that $\Delta \in K$.

   (ii) Prove that Δ is a square in K if and only if $G \cong A_3$.

(c) Let $K = \mathbb{F}_5$. Show that for every irreducible $f(x) \in K[x]$ as above, Δ is a square.

(d) Let K be the splitting field of $x^3 - 5 \in \mathbb{Q}[x]$ and let L be the splitting field of $f(x) = x^3 - 7 \in K[x]$ over K. Prove that $G \cong A_3$.

Solution:

(a) If $\sigma \in G$ and $\alpha \in L$ is a root of $f(x)$ then $0 = \sigma(f(\alpha)) = f(\sigma(\alpha))$ so $\sigma(\alpha)$ is a root of $f(x)$. Since σ is bijective, we conclude that it permutes the roots of $f(x)$. Label the roots of $f(x)$ by $\alpha_1, \alpha_2, \alpha_3$. Consider then the map $G \to S_3$, mapping σ to $\left(\begin{smallmatrix} 1 & 2 & 3 \\ k_1 & k_2 & k_3 \end{smallmatrix}\right)$ if $\sigma(\alpha_i) = \alpha_{k_i}$. This is a group homomorphism (check) and injective, since $L = K(\alpha_1, \alpha_2, \alpha_3)$.

(b) If α is a root of $f(x)$ and $f(x)$ is irreducible, then $[K(\alpha) : K] = 3$. Since $\#G = [L : K]$, by the tower law we conclude that $3 \mid \#G$ and thus follows from (a).

   (i) Δ is fixed by (12), (123), which generate S_3.

   (ii) Let $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$. It is fixed by (123), so if $G \cong A_3$, then $\delta \in K$ and hence Δ is a square. Conversely, if $G \cong S_3$, $\delta \notin K$ since not fixed by (12).

(c) The Galois group of a finite extension of finite fields is cyclic (was proved in HW). Since S_3 is not cyclic, in (b) must have A_3.

(d) The polynomial $g(x) = x^3 - 5 \in \mathbb{Q}[x]$ is irreducible by Eisenstein's criterion with 5. So $\mathrm{Gal}(K/\mathbb{Q})$ is either S_3 or A_3. Now, the roots of $g(x)$ are $\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$ where ζ is a primitive 3-rd root of unity. Thus $\zeta \in K$ and so $2 = \#\,\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \mid \#\,\mathrm{Gal}(K/\mathbb{Q})$ and hence $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$. Thus for $f(x)$ we have

$$\delta = 7(1 - \zeta)(1 - \zeta^2)(\zeta - \zeta^2) \in K$$

and hence $G \cong A_3$, provided that we show that $f(x)$ is irreducible over K. Suppose $f(x)$ is reducible over $K[x]$. Since $\deg f = 3$, then $f(x)$ has a root in K.

Now consider $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\sqrt[3]{5}) = \zeta\sqrt[3]{5}$, $\sigma(\zeta\sqrt[3]{5}) = \zeta^2\sqrt[3]{5}$. So $\zeta = (\zeta\sqrt[3]{5})/\sqrt[3]{5}$ is fixed by σ and since σ has order 3 and $\mathbb{Q}(\zeta)/\mathbb{Q}$ degree 2, $L = \mathbb{Q}(\zeta)^{\langle\sigma\rangle}$. If $\sqrt[3]{7} \in K$, then $\sigma(\sqrt[3]{7})^3 = 7$. So we have one of the following

- $\sigma(\sqrt[3]{7}) = \sqrt[3]{7}$. Then $\sqrt[3]{7} \in \mathbb{Q}(\zeta)$, so $3 \mid 2$, contradiction
- $\sigma(\sqrt[3]{7}) = \zeta\sqrt[3]{7}$. Then $\sqrt[3]{7/5} \in \mathbb{Q}(\zeta)$, so $3 \mid 2$, contradiction
- $\sigma(\sqrt[3]{7}) = \zeta^2\sqrt[3]{7}$. Then $\sqrt[3]{7/25} \in \mathbb{Q}(\zeta)$, so $3 \mid 2$, contradiction

End of test (90 points)