Model answers to Week 02 review worksheet — exercises for §2

The general form of a presentation of an associative unital algebra is $\mathbb{C}\langle X \mid \mathcal{R}\rangle$ where X is a set and $\mathcal{R}$ is a subset of the free tensor algebra $\mathbb{C}\langle X\rangle$. There are several notational conventions:

- inside $\langle \quad \rangle$, sets can be written without $\{\ \}$;
- relations (elements of $\mathcal{R}$) can be written in the form "$P = Q$" where $P, Q \in \mathbb{C}\langle X\rangle$; this is interpreted to mean that $P - Q$ is an element of $\mathcal{R}$.

Part A. Exercises for interactive discussion

E2.1 (a group algebra of a finite cyclic group) Let $\Gamma = \{e, g, g^2\}$ denote the cyclic group of orger 3, where $g^3 = e$. Let $\mathbb{C}\Gamma$ be the group algebra of Γ. Which statements about $\mathbb{C}\Gamma$, given below, are true? Explain your answers.

(A) The subspace of $\mathbb{C}\Gamma$ spanned by e is a subalgebra of $\mathbb{C}\Gamma$.
(B) $\mathbb{C}\langle x \mid x^3 = 1\rangle$ is a presentation of $\mathbb{C}\Gamma$.
(C) The map $\epsilon\colon \mathbb{C}\Gamma \to \mathbb{C}$ given by $\epsilon(\alpha e + \beta g + \gamma g^2) = \alpha + \beta + \gamma$ is a homomorphism of algebras.
(D) The subspace $Z = \{\alpha e + \beta g + \gamma g^2 : \alpha + \beta + \gamma = 0\}$ is a subalgebra of $\mathbb{C}\Gamma$.
(E) The subspace $Z = \{\alpha e + \beta g + \gamma g^2 : \alpha + \beta + \gamma = 0\}$ is an ideal of $\mathbb{C}\Gamma$;
(F) If $x, y \in \mathbb{C}\Gamma$, $x \neq 0$, $y \neq 0$, then $xy \neq 0$.

Answer to E2.1. (A) True: in fact, for any associative algebra A the one-dimensional subspace $\mathbb{C}1_A$ spanned by 1_A is a subalgebra. Indeed, it is closed under multiplication: $(\lambda 1_A)(\mu 1_A) = (\lambda\mu)(1_A 1_A) = (\lambda\mu)1_A \in \mathbb{C}1_A$, and contains 1_A.

(B) True: let us construct an isomorphism between $\mathbb{C}\langle x \mid x^3 = 1\rangle$ and $\mathbb{C}\Gamma$. First, by the universal mapping property of the free algebra, there exists a homomorphism $f\colon \mathbb{C}\langle x\rangle \to \mathbb{C}\Gamma$ such that $f(x) = g$.

We observe that $f(x^3) = f(x)^3 = g^3 = 1_{\mathbb{C}\Gamma}$ and so $f(x^3 - 1) = 0$ and $x^3 - 1 \in \ker f$. Since $\ker f$ is an ideal, the ideal of $\mathbb{C}\langle x\rangle$ generated by $x^3 - 1$ is contained in $\ker f$. Hence by the universal mapping property of the quotient space, f factors as $\mathbb{C}\langle x\rangle \twoheadrightarrow \mathbb{C}\langle x \mid x^3 - 1\rangle \xrightarrow{\overline{f}} \mathbb{C}\Gamma$; the linear map $\overline{f}$ is seen to be an algebra homomorphism because f is.

Note that $\overline{f}$ is surjective because the image of $\overline{f}$ contains g; the image of an algebra homomorphism is a subalgebra, so $im\,\overline{f}$ contains g, g^2 and $1_{\mathbb{C}\Gamma}$; these form a spanning set.

Now observe that $\dim \mathbb{C}\langle x \mid x^3 - 1\rangle \leq 3$: modulo the ideal I_{x^3-1}, x^n is congruent to $x^n - 3$ if $n \geq 3$, so every power of x is congruent to 1, x or x^2; these three elements form a spanning set of $\mathbb{C}\langle x \mid x^3 - 1\rangle$, and so $\dim \mathbb{C}\langle x \mid x^3 - 1\rangle \leq 3$. A surjective linear map from a space of dimension ≤ 3 to a space of dimension 3 must be bijective, so $\overline{f}$ is the required isomorphism of algebras.

(C) True: consider the group homomorphism $\Gamma \to \{1\}$ to the trivial group, i.e., the map which sends all elements of Γ to 1. Extending this map linearly from the basis Γ of $\mathbb{C}\Gamma$ gives ϵ. But the extension is an algebra homomorphism: ϵ is multiplicative on the basis of $\mathbb{C}\Gamma$ hence is multiplicative everywhere, and $\epsilon(1_{\mathbb{C}\Gamma}) = 1$.

(D) False: $1_{\mathbb{C}\Gamma} \notin Z$. Note that our definition of a subalgebra of a unital associative algebra requires the subalgebra to contain the identity element of the whole algebra.

(E) True: $Z = \ker \epsilon$, and the kernel of an algebra homomorphism is always an ideal.

(F) False. In the algebra $\mathbb{C}\langle x \mid x^3 - 1\rangle$, the product of non-zero elements $x - 1$ and $x^2 + x + 1$ is $x^3 - 1$ which is zero. This leads to a simple counterexample, $(e - g)(e + g + g^2) = 0$ in $\mathbb{C}\Gamma$.

E2.2 (algebra characters are lin. independent) If A is an algebra over $\mathbb{C}$, let $\mathrm{Alg}(A, \mathbb{C})$ be the subset of A^* formed by **algebra homomorphisms** from A to $\mathbb{C}$. Show: $\mathrm{Alg}(A, \mathbb{C})$ is a linearly independent set in A^*.

Answer to E2.2. Follows directly from E1.2(c) as algebra homomorphisms to $\mathbb{C}$ are multiplicative characters.

E2.3 (multiplicative characters in $(\mathbb{C}\Gamma)^*$**)** Let $\mathbb{C}\Gamma$ be the group algebra of $\Gamma = \{e, g, g^2\}$ from E2.1.

(a) Calculate $\mathrm{Alg}(\mathbb{C}\Gamma, \mathbb{C})$ and show that this set is a basis of $(\mathbb{C}\Gamma)^*$.

(b) Will the result obtained in (a) still hold if:

- the group Γ is replaced by another finite cyclic group?
- the group Γ is replaced by another finite abelian group?
- the group Γ is replaced by a finite non-abelian group?
- the field $\mathbb{C}$ is replaced by a smaller field of characteristic 0, say, $\mathbb{R}$ or $\mathbb{Q}$?

Answer to E2.3. (a) A linear map $\phi\colon \mathbb{C}\Gamma \to \mathbb{C}$ is uniquely defined by its values on the basis, Γ, of $\mathbb{C}\Gamma$. If, in addition, ϕ is an algebra homomorphism, $\phi(g^2) = \phi(g)^2$ and $1 = \phi(e) = \phi(g^3) = \phi(g)^3$ so ϕ is determined by its value $\phi(g) \in \mathbb{C}$ which must be a cube root of unity.

Accordingly, we can construct three algebra homomorphisms $\chi_1, \chi_\omega, \chi_{\bar\omega}\colon \mathbb{C}\Gamma \to \mathbb{C}$ where

$$\chi_1(g) = 1, \quad \chi_\omega(g) = \omega, \quad \chi_{\bar\omega}(g) = \bar\omega,$$

with $\omega = e^{i\pi/3} = \frac{-1+i\sqrt{3}}{2}$ and $\bar\omega = \omega^2 = \frac{-1-i\sqrt{3}}{2}$. Note that $\{1, \omega, \omega^2\}$ is the group of the cube roots of unity in $\mathbb{C}$. Algebra homomorphisms from $\mathbb{C}\Gamma$ to $\mathbb{C}$ are linearly independent by exercise E2.2. Hence $\chi_1, \chi_\omega, \chi_{\bar\omega}$ form a basis of the 3-dimensional space $(\mathbb{C}\Gamma)^*$.

(b) A finite cyclic group Γ_n of order n has n multiplicative characters, the same as the number of nth roots of unity in $\mathbb{C}$. Hence $\mathrm{Alg}(\mathbb{C}\Gamma_n, \mathbb{C})$ is still a basis of $\mathbb{C}\Gamma$. The same is true for any abelian group of order n: by the structure theorem for finitely-generated abelian groups, a finite abelian group G is a direct product of finite cyclic groups, which can be seen to have $n = |G|$ multiplicative characters.

Note that every element of the form $xyx^{-1}y^{-1}$ of Γ is sent by all characters $\mathbb{C}\Gamma \to \mathbb{C}$ to 1. Hence the algebra characters of $\mathbb{C}\Gamma$ are in fact multiplicative characters of the abelian group Γ/Γ' where Γ' is the subgroup of Γ generated by all elements of the form $xyx^{-1}y^{-1}$, called the commutator subgroup. Accordingly, the cardinality of $\mathrm{Alg}(\mathbb{C}\Gamma, \mathbb{C})$ is equal to the number of elements of Γ/Γ'. If Γ is not abelian, $|\Gamma/\Gamma'| < |\Gamma| = \dim(\mathbb{C}\Gamma)^*$ and so the linearly independent set $\mathrm{Alg}(\mathbb{C}\Gamma, \mathbb{C})$ is not a basis.

If $\mathbb{C}$ is replaced with another field, the field may contain fewer than n roots of unity, and so Γ_n will have fewer multiplicative characters. For example, $\mathbb{Q}$ and $\mathbb{R}$ contain only one cube root of 1, so $\mathrm{Alg}(\mathbb{Q}\Gamma, \mathbb{Q})$ and $\mathrm{Alg}(\mathbb{R}\Gamma, \mathbb{R})$ both consist of one element.

E2.4 (a presentation for the polynomial algebra) The algebra $\mathbb{C}[x, y]$ of polynomials in two variables has, by definition, a basis of **standard monomials:** monomials of the form $x^m y^n$ where $m, n \geq 0$, i.e., where all instances of x precede all instances of y. Note that the monoid $\mathrm{StMon}(x, y)$ of standard monomials is **not** a submonoid of $\mathrm{Mon}(x, y)$: it has different multiplication, $x^m y^n \cdot x^p y^q = x^{m+p} y^{n+q}$. The algebra $\mathbb{C}[x, y]$ can be viewed as the algebra of the monoid $\mathrm{StMon}(x, y)$.

Suggest a presentation for the algebra $\mathbb{C}[x, y]$. Prove that what you suggest is indeed a presentation.

Answer to E2.4. We claim that

$$\mathbb{C}\langle x, y \mid xy = yx \rangle$$

is a presentation of the polynomial algebra $\mathbb{C}[x, y]$.

To show this, denote by I_{xy-yx} the ideal of the free tensor algebra $\mathbb{C}\langle x, y\rangle$ generated by $xy - yx$. By the universal mapping property of the free algebra, there exists a homomorphism $F\colon \mathbb{C}\langle x, y\rangle \to \mathbb{C}[x, y]$, sending x to x and y to y. The element $xy - yx$ of $\mathbb{C}\langle x, y\rangle$, and therefore also the whole ideal I_{xy-yx}, is in $\ker F$.

By the universal mapping property of the quotient, we have the homomorphism

$$f = \overline{F}\colon \mathbb{C}\langle x, y\rangle / I_{xy-yx} \overset{\text{def}}{=} \mathbb{C}\langle x, y \mid xy = yx\rangle \ \to\ \mathbb{C}[x, y]$$

which again sends x to x and y to y. Clearly, f is surjective because $\mathbb{C}[x, y]$ is spanned by monomials $x^m y^n$ which are in the image of f.

On the other hand, observe that standard monomials $x^m y^n$ span $\mathbb{C}\langle x, y \mid xy = yx\rangle$. This is because every noncommutative monomial in $\mathbb{C}\langle x, y\rangle$ is congruent, modulo I_{xy-yx}, to a standard monomial.

To justify this, assume that $MyxN$ is a noncommutative monomial where y precedes x (here M, N are some monomials). We have

$$MyxN = MxyN + M(yx - xy)N.$$

The second summand, $M(yx - xy)N$, belongs to the ideal I_{xy-yx}, therefore $MyxN$ and $MxyN$ are in the same coset modulo I_{xy-yx}. If $MxyN$ is not yet a standard monomial, we can continue applying this "straightening step" to $MxyN$, staying in the same coset, until we obtain a standard monomial in this coset.

Thus, $\{x^m y^n\}_{m,n\geq 0}$ is a spanning set of $\mathbb{C}\langle x, y \mid xy = yx\rangle$. Since f carries this spanning set to a basis of $\mathbb{C}[x, y]$, it follows that $\{x^m y^n\}_{m,n\geq 0}$ is in fact a basis of $\mathbb{C}\langle x, y \mid xy = yx\rangle$ and that f is a linear isomorphism (because it carries a basis to a basis). We have proved that $\mathbb{C}\langle x, y \mid xy = yx\rangle \cong \mathbb{C}[x, y]$.

Part B. Extra exercises

E2.5 (actions are homomorphisms to $\mathrm{End}(V)$**)** Let A be an algebra and V be a vector space over the field $\mathbb{C}$. Prove that there is a 1-to-1 correspondence between actions $\triangleright\colon A \otimes V \to V$ of A on V and algebra homomorphisms $\rho\colon A \to \mathrm{End}(V)$, where an action $\triangleright$ corresponds to the homomorphism

$$\rho_\triangleright\colon A \to \mathrm{End}(V), \qquad \rho_\triangleright(a) \text{ is the element of } \mathrm{End}(V) \text{ defined by } (\rho_\triangleright(a))(v) = a \triangleright v.$$

Answer to E2.5. Let $\triangleright\colon A \otimes V \to V$ be an action. We check that $\rho_\triangleright$ is an algebra homomorphism:

- $\rho_\triangleright(a)$ is linear in a, because, by definition of an action, $a \triangleright v$ is linear in a;
- let $a, b \in A$. By definition, $\rho_\triangleright(ab)v = (ab) \triangleright v$ and $\rho_\triangleright(a)(\rho_\triangleright(b)v) = a \triangleright (b \triangleright v)$. By the first axiom of action, these two expressions are equal, which shows that $\rho_\triangleright(ab) = \rho_\triangleright(a)\rho_\triangleright(b)$;
- $\rho_\triangleright(1_A)v = 1_A \triangleright v = v$ (by the second axiom of action), which shows that $\rho_\triangleright(1_A)$ is the identity map on V, i.e., the identity element in the algebra $\mathrm{End}(V)$.

Thus, $\rho_\triangleright$ satisfies the definition of an algebra homomorphism.

Now, if $\sigma\colon A \to \mathrm{End}(V)$ is a homomorphism, define $\triangleright_\sigma\colon A \otimes V \to V$ by the formula $a \triangleright_\sigma v = \sigma(a)v$. Similarly to the above, it is easy to check that $\triangleright_\sigma$ is an action of A on V. Moreover, $\triangleright_{\rho_\triangleright} = \triangleright$ and $\rho_{\triangleright_\sigma} = \sigma$, which shows that $\sigma \mapsto \triangleright_\sigma$ is the inverse map to $\triangleright \mapsto \rho_\triangleright$, proving that $\triangleright \mapsto \rho_\triangleright$ is a bijection.