Algebra Exam August 2022

Show your work. Be as clear as possible. Do all problems.

(1) Let G be the quaternion group of order 8.
   (a) Determine the algebra structure of $\mathbb{R}[G]$.
   (b) Determine the algebra structure of $\mathbb{C}[G]$.

Proof. Let $G := \langle i, j, k, c \mid c^2 = 1, i^2 = j^2 = k^2 = ijk = c \rangle$. Since both $\mathbb{R}$ and $\mathbb{C}$ has characteristic 0, $\mathbb{R}[G]$ and $\mathbb{C}[G]$ are semisimple by Maschke's theorem.

(a) Note that $\langle c \rangle = Z(G)$ and $\mathbb{R}[c]/(c^2 = 1)$ is a central subalgebra of $\mathbb{R}[G]$. we have $\mathbb{R}[G] \cong \mathbb{R}[G]/(c = 1) \times \mathbb{R}[G]/(c = -1)$. On the first copy, we have

$$\mathbb{R}[G]/(c = 1) \cong \mathbb{R}[V_4] \cong \mathbb{R}^4$$

since $G/Z(G) \cong V_4 \cong (\mathbb{Z}/2)^2$ is abelian. On the second copy, we have $\mathbb{R}[G]/(c = -1) \cong \mathbb{H}$ where $\mathbb{H}$ is the quaternion algebra, which is a 4-dimensional division algebra over $\mathbb{R}$. Hence, we have $\mathbb{R}[G] \cong \mathbb{R}^4 \times \mathbb{H}$.

(b) By Artin-Wedderburn thm, we have

$$\mathbb{C}[G] \cong \mathrm{Mat}_{n_1}(\mathbb{C}) \times \cdots \times \mathrm{Mat}_{n_k}(\mathbb{C}).$$

Since G has five conjugacy classes, $k = 5$. Since $n_1^2 + \cdots + n_5^2 = 1$, we must have $n_1 = \cdots = n_4 = 1$ and $n_5 = 2$. So $\mathbb{C}[G] \cong \mathbb{C}^4 \times \mathrm{Mat}_2(\mathbb{C})$.

□

(2) Let R be a commutative ring with 1. Let $r_1, ..., r_n \in R$ which generate R as an ideal. Let $f : R^n \to R$ be defined by $f(a_1, ..., a_n) = \sum_i a_i r_i$. Show that the kernel of f is a projective module.

Proof. We have the following short exact sequence (SES)

$$0 \to \ker f \to R^n \to R \to 0.$$

Since R is a free $R-$module, it is projective; hence, the above SES splits. Therefore, $\ker f \oplus R \cong R^n$. Because $\ker f$ is a direct summand of a free R-module, $\ker f$ is projective. □

(3) Let G be a finite group with a cyclic Sylow 2-subgroup S.
   (a) Show that $N_G(S) = C_G(S)$.
   (b) Show that if $S \neq 1$, then G contains a normal subgroup of index 2 (hint: suppose that $n = [G : S]$, consider an appropriate homomorphism from G to S_n).
   (c) Show that G has a normal subgroup N of odd order such that $G = NS$.

Proof. See Spring 2017 Q3.

(a) It follows from definitions that $C_G(S) \subseteq N_G(S)$. Note that conjugation gives a homomorphism $f : N_G(S) \to \mathrm{Aut}(S)$ and $\ker f = C_G(S)$. Since S is cyclic of order 2^n for some $n \in \mathbb{Z}_{\geq 0}$, we have $|\mathrm{Aut}(S)| = 2^n - 2^{n-1}$. Hence, $[N_G(S) : C_G(S)] = 2^m$ for some $m < n$. On the other hand, S is abelian gives $S \leq C_G(S) \leq N_G(S)$, which implies

$$[N_G(S) : S] = [N_G(S) : C_G(S)] \cdot [C_G(S) : S].$$

Because S is also a Sylow 2-subgroup of $N_G(S)$, we have $[N_G(S) : S]$ is odd; hence, $m = 0$, i.e. $[N_G(S) : C_G(S)] = 1$ and $C_G(S) = N_G(S)$.

(b) Assume $S \neq 1$ and $|G| = 2^m n$ with n odd. Let $\phi : G \hookrightarrow \mathrm{Sym}(G)$ be the induced homomorphism of the left multiplication of G and $\epsilon : \mathrm{Sym}(G) \to \mathbb{Z}/2$ be the sign homomorphism. The key idea is to show that $\epsilon \circ \phi$ is surjective.
Let $s \in S$ be a generator. Then for any $g \in G$, the orbit of $\phi(s)$ is $\{g, sg, s^{2^m-1}g\}$. If we write $\phi(s)$ in cycle notation, then $\phi(s)$ is a product of n copies of 2^m-cycles. Since n is odd and the sign of an even cycle is -1, we have $\epsilon(\phi(s)) = (-1)^n = -1$. Therefore, $\epsilon \circ \phi$ is surjective.

(c) The proof is by induction on m.

□

(4) Let R be a principal ideal domain and $p \in R$ a prime element. Suppose that V is a finitely generated R-module s.t. $p^a V = 0$ and suppose $v \in V$ with the annihilator of v in R the ideal $p^a R$. Prove that $V = Ra \oplus W$ for some submodule W of V.

Proof. By structure theorem of finite module over PID, we have

$$V \cong R/(p^{a_1}) \oplus \cdots \oplus R/(p^{a_k}) \oplus R/(p^a)$$

where $a_i \leq a$ for $i \in [k]$. Let $\{e_1, \cdots, e_{k+1}\}$ be a basis of V where e_i corresponds to the i-th summand and e_{k+1} corresponds to $R/(p^a)$. Since $\mathrm{Ann}_R(v) = (p^a)$, we have $v = r_1 e_1 + \cdots + r_k e_k + q e_{k+1}$ for some $r_i \in R, 0 \neq q \in R$ with $\gcd(p, q) = 1$. If we can choose $W = \langle e_1, \cdots, e_k \rangle$, then we have $V = Rv \oplus W$. □

(5) Let $f(x) = x^7 - 3 \in \mathbb{Q}[x]$.
  (a) Show that f is irreducible in $\mathbb{Q}[x]$.
  (b) Let K be the splitting field of f over $\mathbb{Q}$. What is the Galois group of $K/\mathbb{Q}$.
  (c) How many subfields L of K are there such that $[K : L] = 7$?

Proof. (a) By applying Eisenstein's criterion with $p = 3$, f is irreducible in $\mathbb{Q}[x]$.

(b) Note that f has 7 distinct roots in $\mathbb{C}$, which are the 7th roots of 3. Therefore, the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is a transitive subgroup of S_7 with order 7!. Since f is irreducible, we have $\mathrm{Gal}(K/\mathbb{Q}) \cong S_7$.

(c) We can prove a more general case where $f = x^p - a$ for some prime p and $a \in \mathbb{Q}$. Note that the splitting field of $f(x) := x^p - a$ is $\mathbb{Q}(\sqrt[p]{a}, \zeta) =: E$ where ζ is a primitive p-th root of unity. First, we know that the Cyclotomic extension $\mathbb{Q}(\zeta)$ is Galois with Galois group $\mathrm{Aut}(\mathbb{Z}/p) \cong \mathbb{Z}/(p-1)$. Also, $E/\mathbb{Q}$ is galois since f is a separable polynomial and E is the splitting field of f.
If $a = 1$ then we are done. If not, then $p = [\mathbb{Q}(\sqrt[p]{a}) : \mathbb{Q}] \mid [E : \mathbb{Q}]$ since f is the minimal polynomial of $\sqrt[p]{a}$ over $\mathbb{Q}$. Because $p \nmid p - 1$, the degree $[E : \mathbb{Q}(\zeta)] = p$ and the Galois group $\mathrm{Gal}(E/\mathbb{Q}(\zeta)) \cong \mathbb{Z}/p$. By the Fundamental theorem of Galois theory, $\mathbb{Z}/p$ is normal in $\mathrm{Gal}(E/\mathbb{Q})$. Thus, $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/(p-1) \ltimes \mathbb{Z}/p$. We define the generator of $\mathbb{Z}/(p-1)$ and $\mathbb{Z}/p$ as follows:

$$\phi : E \longrightarrow E \qquad \psi : E \longrightarrow E$$

$$\zeta \longmapsto \zeta^3 \qquad \sqrt[p]{a} \longmapsto \zeta \sqrt[p]{a}$$

A direct computation shows that

$$\mathrm{Gal}(E/\mathbb{Q}) = \langle \phi, \psi \mid \phi^6 = \psi^7 = 1, \phi\psi = \psi^3 \phi \rangle.$$

(d) By the Galois correspondence, the subfields L of K with $[K : L] = 7$ are in one-to-one correspondence with the normal subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ of order 7. By Sylow's theorem, there is exactly one subfield L such that $[K : L] = 7$.

□

(6) Let M be a maximal ideal of $\mathbb{Q}[x_1, ..., x_t]$.
  (a) Show for each i, there exists a nonzero polynomial f_i with coefficients in $\mathbb{Q}$ such that $f_i(x_i) \in M$.
  (b) Show that there are only finitely many maximal ideals of $\mathbb{C}[x_1, ..., x_t]$ which contain M.

Proof. (a) The problem uses Zariski's Lemma: If $k \subset K$ is a field extension and K is finitely generated as k-algebra, then $[K : k] < \infty$.

Let $L = \mathbb{Q}[x_1, \cdots, x_t]/M$. Since M is a maximal ideal, L is a field. Since L is finitely generated as $\mathbb{Q}$-algebra, we have $[L : \mathbb{Q}] < \infty$ by Zariski's Lemma. Let $\{a_1, \cdots, a_t\}$ be the images of $\{x_1, \cdots, x_t\}$ in L. Since α_i is algebraic, it satisfies a minimal polynomial with coefficients in $\mathbb{Q}$ and the minimal polynomial is contained in M.

(b) Consider the following SES

$$M \to \mathbb{Q}[x_1, \cdots, x_t] \to L \to 0.$$

Since tensor product is right-exact, we have another SES

$$M \otimes_{\mathbb{Q}} \mathbb{C} \to \mathbb{C}[x_1, \cdots, x_t] \to L \otimes_{\mathbb{Q}} \mathbb{C} \to 0.$$

It suffices to show that $L \otimes_{\mathbb{Q}} \mathbb{C}$ has finitely many maximal ideals since preimage of a maximal ideal in $L \otimes_{\mathbb{Q}} \mathbb{C}$ is a maximal ideal in $\mathbb{C}[x_1, \cdots, x_t]$ containing M. By part (a), L is finite-dimensional over $\mathbb{Q}$. Therefore, $\dim_{\mathbb{C}} L \otimes_{\mathbb{Q}} \mathbb{C} = \dim_{\mathbb{Q}} L < \infty$. Hence, $L \otimes_{\mathbb{Q}} \mathbb{C}$ is a finite dimensional $\mathbb{C}$-algebra, which is Artinian. The result follows from the fact that an Artinian ring has finitely many maximal ideals.

□