Algebra qualifying exam, January 2025

Justify all arguments completely. Every ring R is assumed to have a unit $1 \in R$. Given a field k, a k-algebra A is a ring which is equipped with a central ring homomorphism $k \to A$. Reference specific results whenever possible.

(1) Let R be a finite ring.
  (a) If $r^2 = 0$ implies $r = 0$ for any $r \in R$, show that R is commutative.
  (b) Show by example that the converse is false.

Proof. Because R is finite, R is an Artinian ring.
  (a) Suppose $0 \neq x$ is nilpotent and $x^n = 0$ with n minimal. If n is odd, then $x^{n+1} = 0$ implies $x^{\frac{n+1}{2}} = 0$, which contradicts the minimality of n. If n is even, then $x^{\frac{n}{2}} = 0$ contradicts the minimality of n. Since R is Artinian, $J(R)$ is nilpotent; hence $J(R) = 0$. By Wedderburn-Artin theorem, $R \cong \prod_{i=1}^{n} D_i$ because R has no nilpotent element. Since R is finite, each D_i is a finite division ring; hence, D_i's are fields. Therefore, R is commutative.
  (b) Note that $\mathbb{Z}/4\mathbb{Z}$ is a commutative ring, but $2^2 = 0$.

$\square$

(2) Let n be an integer which is divisible by an odd prime. Prove that the dihedral group D_n of order $2n$ is not nilpotent.

Proof. Suppose D_n has the presentation $\langle r, s \mid r^n = s^2 = 1, srs = r^{-1}\rangle$. Since $p \mid n$, we have $r^{\frac{n}{p}}$ is a nontrivial element of order p. Because $\gcd(2,p) = 1$ and $\langle s \rangle \triangleleft D_n$ and sylow subgroups of nilpotent groups are normal, we have s commutes with $r^{\frac{n}{p}}$. However, we have

$$sr^{\frac{n}{p}}s = r^{-\frac{n}{p}} \implies r^{\frac{2n}{p}} = 1.$$

This contradicts with the fact that p is odd. $\square$

(3) Let R be a commutative ring. Consider collections of prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ in R which satisfy $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ and $\mathfrak{q}_r \not\subseteq \mathfrak{q}_s$ at all pairs of distinct indices, and suppose $(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m) = (\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n)$. Prove that $m = n$ and that, after applying a permutation $\sigma \in S_n$, we have $\mathfrak{p}_i = \mathfrak{q}_{\sigma(i)}$ at all i.

Proof. The main observation is that if $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$ for some prime ideal $\mathfrak{p}$ and ideals $\mathfrak{a}, \mathfrak{b}$, then either $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$. This is because if $a \in \mathfrak{a} \setminus \mathfrak{p}$ and $b \in \mathfrak{b} \setminus \mathfrak{p}$ implies that $ab \in \mathfrak{a} \cap \mathfrak{b} \subsetneq \mathfrak{p}$ contradicts to the assumption that $\mathfrak{p}$ is prime.

From the observation, we have $\mathfrak{q}_1 \supseteq \mathfrak{p}_i$ for some i and $\mathfrak{p}_i \supseteq \mathfrak{q}_j$ for some j. Since $\mathfrak{q}_r \not\subseteq \mathfrak{q}_s$ for all $r \neq s$, we must have $j = 1$ and $\mathfrak{q}_1 = \mathfrak{p}_i$. Therefore, we have $n \leq m$ and $\mathfrak{q}_i = \mathfrak{p}_j$ for some j. Using the same argument and $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for all $i \neq j$, we have $m \leq n$. Therefore, $m = n$ and the result follows. $\square$

(4) Recall that a $\mathbb{Z}$-module M is called torsion free if, for each nonzero integer n and nonzero $m \in M$, the element $n \cdot m$ nonzero. Recall also that a $\mathbb{Z}$-module M is called projective if, for any surjective module map $\pi : N_0 \to N_1$ and arbitrary module map $f : M \to N_1$ there exists a module map $\overline{f} : M \to N_0$ which satisfies $\pi f = f$. Prove that a finitely generated $\mathbb{Z}$-module M is projective if and only if it is torsion free.

Proof. The result holds for any finitely generated module over a PID. Recall that a projective module is a direct summand of a free module. Assume M is a finitely generated $\mathbb{Z}$-module. By the structure theorem for finitely generated modules over a PID, we have $M \cong \mathbb{Z}^r \oplus \mathrm{Tor}(M)$. Therefore, M is projective if and only if $\mathrm{Tor}(M) = 0$, which means M is free. $\square$

(5) Let k be a field and $A(k)$ be the group ring $k[\mathbb{Z}/p\mathbb{Z}]$ at a prime p. (This ring has basis provided by the elements g in $\mathbb{Z}/p\mathbb{Z}$ and multiplication $(\sum_g a_g \cdot g)(\sum_h a_h \cdot h) = \sum_{g,h} a_g a_h \cdot gh$.) Take for

granted that $A(k)$ is semisimple whenever k is of characteristic 0. Provide the Artin-Wedderburn decomposition for $A(k)$ when:

(a) $k = \mathbb{Q}$.
(b) $k = \mathbb{C}$.

Proof. Let $G = \mathbb{Z}/p\mathbb{Z}$. Then $k[G]$ is semisimple since p does not divides the characteristic of k. Since G is abelian, irreducible representations of G are one-dimensional. Moreover, there is a ring isomorphism $k[G] \cong k[X]/(X^p - 1)$ by sending a generator of G to the variable X.

(a) Since $X^p - 1 = (X-1)(X^{p-1} + \cdots + 1)$ over $\mathbb{Q}$, the Chinese remainder theorem says that
$$\mathbb{Q}[G] \cong \mathbb{Q}[X]/(X-1) \oplus \mathbb{Q}[X]/(X^{p-1} + X^{p-2} + \cdots + 1) \cong \mathbb{Q} \oplus \mathbb{Q}(\zeta_p)$$
where ζ_p is a primitive p-th root of unity.
In this proof, we used the trick that $x^{p-1} + \cdots + 1 = (x^p - 1)/(x-1) = f(x)$ is irreducible by checking $f(x+1)$ is irreducible using Eisentein's criterion.

(b) Since $\mathbb{C}$ is algebraically closed, $\mathbb{C}[G] \cong \mathbb{C}^p$ where each copy of $\mathbb{C}$ corresponds to a root of $X^p - 1$.

□

(6) Take $R = \mathbb{C}[x_1, ..., x_m]$ and $A \in M_{n\times n}(R)$. Write $A = [f_{ij}]$ for functions $f_{ij} \in R$. Prove that A is invertible if and only if, at each point $z \in \mathbb{C}^m$, the complex matrix $A_z = [f_{ij}(z)]$ is invertible. [Note: You may use the fact that A is invertible if and only if its determinant is a unit in R.]

Proof. Note that $f \in R$ is a unit if and only if $f(z) \in \mathbb{C}^\times$ for all $z \in \mathbb{C}^m$ and A is invertible if and only if $\det(A) \in R^\times$. Therefore, A is invertible if and only if $\det(A(z)) \in \mathbb{C}^\times$ for all $z \in \mathbb{C}^m$, i.e. $A(z)$ is invertible for all $z \in \mathbb{C}^m$.

To prove the first claim, we note that $f \in R$ is a unit implies that $fg = 1$ for some $g \in R$. Evaluate both side at $z \in \mathbb{C}^m$, we have $f(z) \neq 0$ for all $z \in \mathbb{C}^m$ if f is a unit. Conversely, if $f(z) \neq 0$ for all $z \in \mathbb{C}^m$, then $V(f) = \varnothing$ and $I(V(f)) = R$ implies that f is a unit. □