Answers to the Algebra Qualifying Exam
January 1999

1. Since A contains no nonidentity normal subgroup, it contains no nonidentity central element. In particular, if $1 \neq a \in A$, then $\mathbb{C}_G(A) \neq G$. But A is abelian, so $\mathbb{C}_G(a) \supseteq A$. Hence, since A is maximal, we have $\mathbb{C}_G(a) = A$ for all $1 \neq a \in A$.

(i) Suppose $|A|$ is divisible by p and let $x \in A$ have order p. Choose a Sylow p-subgroup P of G with $x \in P$. Then $A = \mathbb{C}_G(x) \supseteq \mathbb{Z}(P)$. But $\mathbb{Z}(P) \neq 1$ since $P \neq 1$, so we can choose $1 \neq z \in \mathbb{Z}(P) \subseteq A$. Then $A = \mathbb{C}_G(z) \supseteq P$ and consequently $|G : A|$ must be prime to p, a contradiction since $|G : A| = p^n \neq 1$.

(ii) Since $1 \neq A \subseteq \mathbb{N}_G(A) \subseteq G$ and since A is not normal in G, it follows from the maximality of A that $A = \mathbb{N}_G(A)$. Furthermore, if A^x and A^y are conjugates of A having a nonidentity element b in common, then $\mathbb{C}_G(b) \supseteq \langle A^x, A^y \rangle$. But A^x and A^y are maximal and b is not central, so $A^x = \mathbb{C}_G(b) = A^y$. In other words, the $p^n = |G : A| = |G : \mathbb{N}_G(A)|$ distinct conjugates of A are disjoint. It follows that $|S| = |\bigcup_x A^x \setminus 1| = p^n(|A| - 1) = |G| - p^n$, so $|G \setminus S| = p^n$.

(iii) Let P be a Sylow p-subgroup of G. Since p does not divide $|A|$ and $p^n = |G : A|$, we see that $|P| = p^n$. Furthermore, P is disjoint from the set S. Thus $P \subseteq G \setminus S$ and, since both of these sets have the same size, we conclude that $P = G \setminus S$. But $G \setminus S$ is clearly a normal subset of G, and hence P is a normal subgroup of G.

2. (i) Note that the R-submodules of R_R are precisely the right ideals of R. If R is a division ring and if I is a nonzero submodule of R_R, then I is a right ideal containing a unit and hence $I = R$. Thus R_R is simple. Conversely, suppose R_R is simple and let $0 \neq x \in R$. Then xR is a nonzero submodule of R_R, so $xR = R$ and there exists $y \in R$ with $xy = 1$. Similarly, since $y \neq 0$, there exists $z \in R$ with $yz = 1$. Thus $x = x(yz) = (xy)z = z$, so $yx = yz = 1$ and $y = x^{-1}$. Therefore R is a division ring.

(ii) If R is a division ring and if V is a nonzero right R-module, choose $0 \neq v \in V$. Then the map $\theta\colon R \to V$ given by $\theta(r) = vr$ is an R-module homomorphism and its kernel is a proper right ideal of R. In particular, $\ker\theta = 0$, so θ is one-to-one and $V \supseteq \theta(R) \cong R_R$. Conversely, suppose every nonzero R-module contains an isomorphic copy of R_R and let M be a maximal right ideal of R. Then $V = R/M$ is an irreducible R-module which, by assumption, contains R_R. Thus $V = R_R$, so R_R is irreducible and consequently R is a division ring by part (i).

3. We use the fact that if $E \subseteq \mathbb{C}$ is a finite Galois extension of $\mathbb{Q}$ and if $\theta\colon E \to \mathbb{C}$ is a field homomorphism, then $\theta(E) = E$ and θ restricts to a field automorphism of E.

(i) Let $F \subseteq \mathbb{C}$ be a finite Galois extension of $\mathbb{Q}$ with $\alpha, \beta \in F$ and $E \subseteq F$. Say F is the splitting field of the polynomial $g(x) \in \mathbb{Q}[x]$. Since α and β are roots of the same irreducible polynomial $f(x) \in \mathbb{Q}[x]$, there exists a field isomorphism $\sigma\colon \mathbb{Q}[\alpha] \to \mathbb{Q}[\beta]$ with $\sigma(\alpha) = \beta$. Note that F is the splitting field of $g(x)$ over $\mathbb{Q}[\alpha]$ and it is the splitting field of $g(x)$ over $\mathbb{Q}[\beta]$. Thus, since σ fixes $g(x) \in \mathbb{Q}[x]$, we see that σ extends to a field isomorphism $\tau\colon F \to F$. Indeed, since $E \subseteq F$ and E is Galois over $\mathbb{Q}$, we see that τ restricts to an automorphism of E. In particular, $\tau\colon \mathbb{Q}[\alpha] \cap E \to \mathbb{Q}[\beta] \cap E$. Since τ^{-1} maps E to E

and $\mathbb{Q}[\beta]$ to $Q[\alpha]$, we have $\tau^{-1}: \mathbb{Q}[\beta] \cap E \to \mathbb{Q}[\alpha] \cap E$. Thus $\tau: \mathbb{Q}[\alpha] \cap E \to \mathbb{Q}[\beta] \cap E$ is the required field isomorphism.

(ii) If $E = \mathbb{Q}[\varepsilon]$, where ε is a root of unity, then we know that $G = \mathrm{Gal}(E/\mathbb{Q})$ is abelian. Thus every subgroup of G is normal and hence every intermediate field is Galois over $\mathbb{Q}$. In particular, $\mathbb{Q}[\alpha] \cap E$ is Galois over $\mathbb{Q}$ and since $\tau: \mathbb{Q}[\alpha] \cap E \to \mathbb{Q}[\beta] \cap E$ is an isomorphism, we must have $\tau(\mathbb{Q}[\alpha] \cap E) = \mathbb{Q}[\alpha] \cap E$ and hence $\mathbb{Q}[\alpha] \cap E = \mathbb{Q}[\beta] \cap E$.

4. (i) Say $\dim_F V = n$ and let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the n distinct roots of the characteristic polynomial of S. Then these are the n eigenvalues of S with correponding eigenvectors $v_1, v_2, \ldots, v_n$. We know that $v_1, v_2, \ldots, v_n$ form a basis for V and that the only eigenvectors for S are contained in the n lines $Fv_1, Fv_2, \ldots, Fv_n$. Since S and T commute, we have $(v_iT)S = (v_iS)T = (\alpha_i v_i)T = \alpha_i(v_iT)$. Thus v_iT is either 0 or an α_i-eigenvector for S. But α_i occurs with multiplicity 1 as a root of the characteristic polynomial for S, so the α_i-eigenspace has dimension 1 and hence $v_iT \in Fv_i$. In other words, $v_iT = \beta_i v_i$ for some $\beta_i \in F$ and hence each v_i is an eigenvector for T.

(ii) If T is nilpotent, then each β_i must be 0, so $v_iT = 0$. But V is spanned by $v_1, v_2, \ldots, v_n$, so $VT = 0$ and hence $T = 0$.

5. (i) Let $\theta_i: V \to V/M_i$ be the natural epimorphism with $\ker \theta_i = M_i$ and let $\theta: V \to W$ be given by $\theta(v) = (\theta_1(v), \theta_2(v), \ldots, \theta_n(v))$. Then $\theta(v) = 0$ if and only if $\theta_i(v) = 0$ for all i. Thus $\ker \theta = \bigcap_i \ker \theta_i = \bigcap_i M_i = 0$, by assumption. In other words, θ is one-to-one and hence $V \cong \theta(V) \subseteq W$.

(ii) Write $W_i = V/M_i$ so that $W = W_1 \oplus W_2 \oplus \cdots \oplus W_n$, and note that

$$(*) \qquad 0 \subseteq W_1 \subseteq W_1 \oplus W_2 \subseteq \cdots \subseteq W_1 \oplus W_2 \oplus \cdots \oplus W_n = W$$

is an ascending series of submodules of W. Since $(W_1 \oplus \cdots \oplus W_i)/(W_1 \oplus \cdots \oplus W_{i-1}) \cong W_i$ is a simple R-module, we see that $(*)$ is a composition series for W of length n. Furthermore, V is isomorphic to a submodule of W, so V and all its submodules have composition series of length $\leq n$. We consider the composition factors for V. Since the series $0 \subseteq M_i \subseteq V$ can be refined to a composition series, we see that V has a composition factor isomorphic to V/M_i for each i. But these irreducible modules V/M_i are given to be all nonisomorphic. Hence V must have at least n distinct composition factors and the composition length of V is $\geq n$. As we saw, W has composition length precisely n and W contains an isomorphic copy $\theta(V)$ of V. In particular, $W/\theta(V)$ must have composition length 0, so $W = \theta(V) \cong V$, as required.