Answers to the Algebra Qualifying Exam
August 2002

1. Let $N = \mathbb{N}_G(P)$ and let $M = \mathbb{N}_G(PK)$. Since $K \triangleleft G$ we have $N \subseteq M$, and the Sylow theorems imply that $n_p(G) = |G : N|$. Let us write $\bar{}: G \to G/K$. Then $\overline{P} = PK/K$ is a Sylow p-subgroup of $\overline{G}$ with normalizer given by $\mathbb{N}_{\overline{G}}(\overline{P}) = \mathbb{N}_{\overline{G}}(PK/K) = \mathbb{N}_G(PK)/K = M/K = \overline{M}$. Hence $n_p(G/K) = n_p(\overline{G}) = |G/K : M/K| = |G : M|$.

a. Since $N \subseteq M$, we see that $n_p(G) = |G : N| = |G : M||M : N| = n_p(G/K)|M : N|$. In particular, $n_p(G/K)$ divides $n_p(G)$ with equality if and only if $M = N$.

b. If $P \triangleleft PK$, then $P \operatorname{char} PK$ since P is clearly a Sylow p-subgroup of PK. Hence $P \triangleleft M = \mathbb{N}_G(PK)$ and $N \supseteq M$. Thus $N = M$ and $n_p(\overline{G}) = n_p(G)$. Conversely if we have $n_p(\overline{G}) = n_p(G)$, then $N = M \supseteq PK$ and, since $P \triangleleft N$, we conclude that $P \triangleleft PK$.

2. a. Assume that $I \not\subseteq P$ and choose $s \in I \setminus P$. Now let p be any element of P. Then $ps \in PI = IP$ and IP is a primary ideal, so we have either $p \in IP$ or $s^n \in IP$ for some integer $n \geq 1$. But if $s^n \in IP \subseteq P$, then $s \in P$ since P is prime, and this contradicts the way s was chosen. Thus we must have $p \in IP$ for all $p \in P$ and hence $IP \supseteq P$. Since $P \supseteq IP$ is always true, we conclude that $P = IP \subseteq I$.

b. Note that M is a prime ideal and that, by (a), any prime ideal is comparable to any proper ideal. There are two possible arguments here. First, if M' is any maximal ideal, then M and M' are comparable, that is $M \supseteq M'$ or $M' \supseteq M$. In either case, we conclude that $M = M'$. Thus M is the unique maximal ideal of R and it is known that in such a situation, M must be the set of all nonunits of R. Alternately, we can observe that if $r \in M$, then r is certainly a nonunit. Conversely, suppose that r is a nonunit, so that $I = rR$ is a proper ideal of R. Then I is comparable to M, so either $I \supseteq M$ or $M \supseteq I$. But M is maximal, so $I \supseteq M$ implies that $I = M$, and consequently $M \supseteq I$ in all cases. Thus $r \in M$, as required.

c. We show by induction on $n \geq 1$ that $s^n \in J$ implies $s \in J$. This is trivial for $n = 1$. If $n \geq 2$, then $2(n-1) \geq n$ so $(s^{n-1})^2$ is a multiple of s^n and hence is contained in J. By assumption, this implies that $s^{n-1} \in J$ and, by induction, $s \in J$. Finally, we show that J is prime. To this end, let $rs \in J$. Since J is primary, we see that either $r \in J$ or $s^n \in J$ for some $n \geq 1$. But the latter implies that $s \in J$ and hence J is indeed prime.

3. a. Since $f(x)$ has n distinct roots, it is a separable polynomial. Thus E is a normal separable extension of F and the primitive element theorem implies that $E = F[\beta]$ for some $\beta \in E$. In particular, each $\alpha_i \in E = F[\beta]$ can be written as a polynomial expression $\alpha_i = p_i(\beta)$ with $p_i(x) \in F[x]$.

b. Note that $\deg g(x) = (F[\beta] : F) = (E : F)$. Since E/F is a normal extension and since $g(x) \in F[x]$ is an irreducible polynomial with one root $\beta \in E$, it follows that all roots of $g(x)$ are contained in E. Thus $\gamma \in E$ and, by degree considerations, we have $E = F[\beta] = F[\gamma]$. Furthermore, since $g(x)$ is irreducible, there exists an F-isomorphism $\sigma: F[\beta] \to F[\gamma]$ given by $\beta \mapsto \gamma$. Thus σ is an F-automorphism of E. In particular, $p_i(\gamma) = p_i(\sigma(\beta)) = \sigma(p_i(\beta)) = \sigma(\alpha_i)$. But σ permutes the roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ of $f(x)$, so $p_1(\gamma), p_2(\gamma), \ldots, p_n(\gamma)$ are clearly the elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ in some order.

c. As above, $F[\gamma] = E = F[\gamma']$ and there exists an F-field automorphism $\tau: E \to E$ with $\tau(\gamma) = \gamma'$. Since $\tau(p_i(\gamma)) = p_i(\tau(\gamma)) = p_i(\gamma')$ and since, by assumption, $p_i(\gamma) =$

$p_i(\gamma')$, we see that τ fixes all $p_i(\gamma)$ and hence all α_i. Thus τ fixes $E = F[\alpha_1, \alpha_2, \ldots, \alpha_n]$ and hence $\gamma' = \tau(\gamma) = \gamma$.

4. a. Since K is algebraically closed, A is similar to a matrix with Jordan blocks down the diagonal. In other words, there exists a nonsingular matrix P with $P^{-1}AP = \operatorname{diag}(J_1, J_2, \ldots, J_k)$. Here each J_i is a $k_i \times k_i$ matrix of the form

$$J_i = \begin{pmatrix} \lambda_i & 1 & & & \\ & \lambda_i & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda_i & 1 \\ & & & & \lambda_i \end{pmatrix} = \lambda_i I_i + N_i$$

where N_i is a nilpotent matrix with $N_i^{k_i} = 0$. Consequently, $P^{-1}AP = D + E$ where $D = \operatorname{diag}(\lambda_1 I_1, \lambda_2 I_2, \ldots, \lambda_k I_k)$ and $E = \operatorname{diag}(N_1, N_2, \ldots, N_k)$. Certainly D and E commute, D is a diagonal matrix and E is nilpotent with $E^n = 0$. Since $A = PDP^{-1} + PEP^{-1}$, the result follows with $B = PDP^{-1}$ and $C = PEP^{-1}$.

b. If $\operatorname{char} K = p > 0$ and if we choose p^t to be larger than n, then since B and C commute and $C^{p^t} = 0$, we have $A^{p^t} = (B + C)^{p^t} = B^{p^t} + C^{p^t} = B^{p^t}$. Since B is similar to a diagonal matrix, so is B^{p^t}, and hence A^{p^t} is a diagonalizable matrix.

c. There are two possible arguments. First for any $n \times n$ matrix X, let $\|X\|$ denote the maximum absolute value of its n^2 entries. Then the definition of multiplication implies that $\|XY\| \leq n\|X\|\|Y\|$ and this easily yields $\|A^k\| \leq (n\|A\|)^k$ for all integers $k \geq 0$. Since $\sum_{k=0}^{\infty}(n\|A\|)^k/k! = \exp(n\|A\|)$ exists, it follows that $\sum_{k=0}^{\infty}\|A^k\|/k!$ converges and hence $\sum_{k=0}^{\infty} A^k/k!$ converges at each entry. For a second argument, write $A = B + C$ as in part (a). Then there exists a nonsingular matrix P with $B = P^{-1}DP$ where $D = \operatorname{diag}(\mu_1, \mu_2, \ldots, \mu_n)$ is diagonal. Since $B^k = P^{-1}D^kP$, we see that $\exp(B) = P^{-1}\operatorname{diag}(e^{\mu_1}, e^{\mu_2}, \ldots, e^{\mu_n})P$ exists. Finally, since $BC = CB$ and $C^n = 0$, we have $A^k/k! = \sum_{i=0}^{n-1}\binom{k}{i}B^{k-i}C^i/k! = \sum_{i=0}^{n-1} B^{k-i}/(k-i)!\cdot C^i/i!$ and hence $\exp(A) = \sum_{k=0}^{\infty} A^k/k! = \sum_{k=0}^{\infty}\sum_{i=0}^{n-1} B^{k-i}/(k-i)!\cdot C^i/i! = \exp(B)\sum_{i=0}^{n-1} C^i/i!$ exists.

5. a. Set $V^i = V_1 \dot{+} V_2 \dot{+} \cdots \dot{+} V_i$. Then $0 = V^0 \subseteq V^1 \subseteq \cdots \subseteq V^n = V$ is a series for V with $V^i/V^{i-1} \cong V_i$ irreducible. Thus V has a composition series of length n. It follows that the submodules of V satisfy both the maximal and the minimal conditions. Now assume $V \supseteq W \neq 0$. Since $W \neq 0$, it contains a minimal nonzero submodule X, and X is clearly a minimal submodule of V. Similarly, W has a maximal proper submodule Y.

b. Since W is properly smaller than V and since V is generated by $V_1, V_2, \ldots, V_n$, there exists a subscript k with $W \not\supseteq V_k$. Thus $W \cap V_k$ is properly smaller than the irreducible module V_k, so $W \cap V_k = 0$. Since $W \dot{+} V_k$ is a submodule of V properly larger than the maximal proper submodule W, we conclude that $V = W \dot{+} V_k$ and hence $V/W \cong V_k$.

c. Let $\pi_k \colon V \to V_k$ denote the natural projection to the direct summand V_k in $V = V_1 \dot{+} V_2 \dot{+} \cdots \dot{+} V_n$. Then $\ker \pi_k = V_k'$ and clearly $\bigcap_{k=1}^n V_k' = \bigcap_{k=1}^n \ker \pi_k = 0$. Since $W \neq 0$, there exists a subscript j with W not contained in V_j'. Thus $W \cap V_j'$ is a submodule of W properly smaller than W and since W is simple, we must have $W \cap V_j' = 0$. Thus $W \dot{+} V_j'$ is a submodule of V properly larger than V_j'. Since $V/V_j' \cong V_j$ is simple, we see that V_j' is maximal in V and hence $V = W \dot{+} V_j'$. In particular, $W \cong V/V_j' \cong V_j$.