Answers to the Algebra Qualifying Exam
August 2006

1. (a) Let Q be a Sylow q-subgroup of N, so that $N = MQ$ and $Q \neq 1$ since N/M is a nonidentity q-group. Now G permutes the Sylow q-subgroups of $N \triangleleft G$ by conjugation, and the Sylow Theorems imply that N acts transitively. Thus, by the Frattini argument, we have $G = NH$ where $H = \mathbb{N}_G(Q)$. In particular, $G = NH = (MQ)H = M(QH) = MH$ and $1 \neq Q \triangleleft H$.

(b) Assume that M is self-centralizing. If $p = q$, then N is a p-group and hence $M = \mathbb{C}_G(M) \supseteq \mathbb{Z}(N) \neq 1$. Thus since M is minimal normal in G and since $\mathbb{Z}(N) \triangleleft G$, we have $M = \mathbb{Z}(N)$. But then $M = \mathbb{C}_G(M) = \mathbb{C}_G(\mathbb{Z}(N)) \supseteq N$ and $N/M = 1$, a contradiction.

(c) Since M is minimal normal in G and M is a p-group, it follows that $M = \mathbb{Z}(M)$. Thus M is clearly an elementary abelian p-group. Again suppose that M is self-centralizing. Now $M \cap H \triangleleft H$ since $M \triangleleft G$, and $M \cap H \triangleleft M$ since M is abelian. Thus $M \cap H \triangleleft MH = G$. In particular, the minimality of M implies that $M \cap H = M$ or 1. If $M \cap H = M$, then $G = MH = H$ has a nontrivial normal q-group Q, and $q \neq p$ by (b). Since $M \triangleleft G$ and $M \cap Q = 1$, it follows that Q centralizes M, a contradiction. Thus $M \cap H = 1$.

2. (a) Let $\bar{\ }\colon R \to R/N$ be the natural epimorphism. If e is an idempotent in R, then $e(1-e) = 0$ and hence $\overline{e}\,\overline{(1-e)} = 0$. Since R/N is a domain, that is a ring without zero divisors, it follows that either $\overline{e} = 0$ or $\overline{1-e} = 0$. Thus either $e \in N$ or $1 - e \in N$. Note that $(1-e)^2 = 1 - 2e + e^2 = 1 - e$, so $1 - e$ is also an idempotent. Furthermore, if f is an idempotent and $f \in N$, then $f^k = 0$ for some k since N is a nil ideal, and therefore $f = f^k = 0$. Thus taking $f = e$ or $f = 1 - e$, we conclude that $e = 0$ or $e = 1$.

(b) We show that every element of $R \setminus N$ is a unit and hence not a zero divisor. It will therefore follow that all zero divisors are in N and hence nilpotent. To this end, let $r \in R \setminus N$. Since R/N is a division ring, there exists an element $s \in R$ with $\overline{r}\,\overline{s} = \overline{1}$. Thus $rs = 1 - n$ for some $n \in N$. Now n is nilpotent, say $n^k = 0$, and then $1 + n + n^2 + \cdots + n^{k-1}$ is clearly an inverse for $1 - n$. Thus $s(1-n)^{-1}$ is a right inverse for r. Similarly, r has a left inverse and consequently it is invertible. Note that if R/N is merely assumed to be a domain, then it is possible for R to have non-nilpotent zero divisors.

3. (a) We may suppose in both parts that $\alpha \neq 0$. Since E is Galois over $\mathbb{Q}$, it follows from the Fundamental Theorem that E is Galois over K with Galois group, say, H. Let $h \in H$. Since $\alpha^n \in \mathbb{Q} \subseteq K$, we have $(\alpha^h)^n = (\alpha^n)^h = \alpha^n$ and hence $\alpha^h = \alpha\varepsilon_h$ for some ε_h, an nth root of unity in $\mathbb{C}$. Furthermore, ε_h is in E, so it is in K, by definition of K, and hence it is fixed by H. Now if $h, k \in H$, then $\alpha^{hk} = (\alpha^h)^k = (\alpha\varepsilon_h)^k = \alpha^k\varepsilon_h = \alpha\varepsilon_k\varepsilon_h$. Thus $\varepsilon_{hk} = \varepsilon_h\varepsilon_k$ and we see that the map $h \mapsto \varepsilon_h$ is a homomorphism from H to the cyclic group of nth roots of unity in $\mathbb{C}$. But this map is one-to-one, since if $\varepsilon_h = 1$, then h fixes α and hence it fixes $E = \mathbb{Q}[\alpha]$. Thus H is isomorphic to a subgroup of a cyclic group and is itself cyclic.

(b) Let G denote the Galois group of E over $\mathbb{Q}$ and note that $|\alpha|^2 = \alpha\alpha^\tau$. If $g \in G$ then, since τ is central in G, we have $(|\alpha|^2)^g = (\alpha\alpha^\tau)^g = \alpha^g\alpha^{\tau g} = \alpha^g\alpha^{g\tau} = |\alpha^g|^2$. As above, since $\alpha^n \in \mathbb{Q}$, we have $(\alpha^g)^n = (\alpha^n)^g = \alpha^n$ and hence $\alpha^g = \alpha\varepsilon_g$ for some ε_g, an nth root of unity in $\mathbb{C}$. But $|\varepsilon_g| = 1$, so $(|\alpha|^2)^g = |\alpha^g|^2 = |\alpha\varepsilon_g|^2 = |\alpha|^2$. Thus $|\alpha|^2$ is fixed by G, so $|\alpha|^2 \in E^G = \mathbb{Q}$, since E is Galois over $\mathbb{Q}$.

4. (a) Since $V \neq 0$, we have $v \neq 0$ and $\{v\}$ is linearly independent. Since V is finite dimensional, we can choose $n \geq 1$ maximal with $\{v, T(v), \ldots, T^{n-1}(v)\}$ linearly independent, and we let U be the subspace of V spanned by these n vectors. By definition of n, $T^n(v)$ is a linear combination of $\{v, T(v), \ldots, T^{n-1}(v)\}$ and, by applying T^k to this equation, for any $k \geq 0$, we see that $T^{k+n}(v)$ is a linear combination of $\{T^k(v), T^{k+1}(v), \ldots, T^{k+n-1}(v)\}$. An easy induction on k now shows that $T^{k+n}(v) \in U$ for all $k \geq 0$ and thus $U = V$. It follows that $\{v, T(v), \ldots, T^{n-1}(v)\}$ is a basis for V and hence $\dim V = n$. In particular, the characteristic polynomial $f(x)$ of T has degree n. Now let $g(x)$ be the minimal polynomial of T so that $g(x) \mid f(x)$ by the Cayley-Hamilton Theorem. If $g(x)$ has degree m, then $g(T) = 0$ yields $g(T)v = 0$ and implies that $\{v, T(v), \ldots, T^m(v)\}$ is linearly dependent. By definition of n, we have $\deg g(x) = m \geq n = \deg f(x)$. Since $g(x) \mid f(x)$ and both polynomials are monic, we conclude that $g(x) = f(x)$ and T is regular.

(b) Let $f_1(x)$ be the characteristic polynomial of T_W, and let $g_1(x)$ be its minimal polynomial. Similarly, let $f_2(x)$ be the characteristic polynomial of $T_{V/W}$, and let $g_2(x)$ be its minimal polynomial. Then we know that $g_1(x) \mid f_1(x)$ and $g_2(x) \mid f_2(x)$. Furthermore, $f_1(x)f_2(x) = f(x)$ is the characteristic polynomial of T on V since, with an appropriate choice of basis, the matrix for T is in block form

$$\begin{pmatrix} A & C \\ 0 & B \end{pmatrix},$$

where A corresponds to T_W and B to $T_{V/W}$. Finally, note that $g_2(T)$ annihilates V/W, so $g_2(T)V \subseteq W$, and then $g_1(T)g_2(T)V \subseteq g_1(T)W = 0$. Thus the minimal polynomial $g(x)$ of T on V divides $g_1(x)g_2(x)$, and we know that $g_1(x)g_2(x)$ divides $f_1(x)f_2(x) = f(x)$. But $g(x) = f(x)$, by assumption, so $g_1(x)g_2(x) = f_1(x)f_2(x)$. Since $g_1(x) \mid f_1(x)$ and $g_2(x) \mid f_2(x)$, we conclude that $g_1(x) = f_1(x)$ and $g_2(x) = f_2(x)$. Therefore both T_W and $T_{V/W}$ are regular.

5. (a) Let α be the unique eigenvalue of A in a fixed algebraic closure of F. Since $A \in \mathrm{M}_2(F)$, it follows that $2\alpha = \mathrm{trace}(A) \in F$ and $\alpha^2 = \mathrm{determinant}(A) \in F$. If the characteristic of F is not 2, then we can divide by $2 \in F$, so $2\alpha \in F$ implies that $\alpha \in F$. On the other hand, suppose the characteristic is 2. Since F is a finite field, we know that F is perfect. Thus every element of F is a square of an element of F. In particular, since $\alpha^2 \in F$, there exists $\beta \in F$ with $\alpha^2 = \beta^2$. Hence $(\alpha - \beta)^2 = 0$ and $\alpha = \beta \in F$.

(b) By Jordan canonical form, every nonzero nilpotent matrix in $\mathrm{M}_2(F)$ is conjugate to

$$N = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

In particular, the set of such matrices is the orbit of N under the conjugate action of G on the matrix ring. Now the size of this orbit is the index in G of the stabilizer G_N of N in G, and this stabilizer is just the set of matrices in G that commute with N. It is easy to see that the set of all matrices that commute with N are of the form $aI + bN$ with $a, b \in F$, and that $aI + bN$ is invertible precisely when $a \neq 0$. Thus $|G_N| = (q-1)q = q^2 - q$, so the size of the orbit of N is $|G : G_N| = |G|/|G_N| = (q^2-1)(q^2-q)/(q^2-q) = q^2 - 1$.