Answers to the Algebra Qualifying Exam
January 1998

1. (i) Since $N \triangleleft G$, $P \cap N \in \mathrm{Syl}_p(N)$ and $Q \cap N \in \mathrm{Syl}_p(N)$. Thus, by the second Sylow theorem applied to N, we have $Q \cap N = (P \cap N)^n$ for some $n \in N$. Note that $Q \supseteq Q \cap N$ and $P^n \supseteq (P \cap N)^n = Q \cap N$. Thus, since $P^n \in \mathrm{Syl}_p(G)$ and $Q \cap N \neq 1$ (remember that $|N|$ is divisible by p), we conclude that $Q = P^n$.

(ii) Let $^{-}\colon G \to G/N$ be the natural epimorphism. If $P_1, Q_1 \in \mathrm{Syl}_p(G/N)$, then there exist $P, Q \in \mathrm{Syl}_p(G)$ with $\bar{P} = P_1$, $\bar{Q} = Q_1$. By (i) above, $Q = P^n$ for some $n \in N$. Thus since $\bar{n} = 1$, we have $Q_1 = \bar{Q} = \overline{P^n} = \bar{P}^{\bar{n}} = \bar{P} = P_1$ and G/N has a unique Sylow p-subgroup.

2. (i) We have $(a) \subseteq (b)$ if and only if $a \in (b)$ and hence if and only if $b|a$. Thus $(a) = (b)$ if and only if $b|a$ and $a|b$. In the latter case, we have $b = au$ and $a = bv$, so $b = au = bvu$. Since $b \neq 0$ and R is a domain, this yields $1 = vu$ and u is a unit. Conversely, if $b = au$ for some unit u, then $a = bu^{-1}$, so $a|b$ and $b|a$.

(ii) If $0 \neq a \in R$, then we can write $a = up_1 \cdots p_n$ where u is a unit and the p_i are prime. By uniqueness, $a^{\#} = n$ is well defined. For convenience, set $0^{\#} = \infty$. Let $\mathcal{P}$ be a nonempty set of principal ideals of R. We can assume that $\mathcal{P}$ does not just consist of the 0 ideal. Choose $0 \neq a \in R$ with $(a) \in \mathcal{P}$ and with $a^{\#}$ minimal. We claim that (a) is a maximal member of $\mathcal{P}$. Indeed, if $(b) \in P$ and $(b) \supseteq (a)$, then $b|a$ by (i). If $a = bc$, then the UFD property implies that $a^{\#} = b^{\#} + c^{\#}$. Thus the minimal nature of $a^{\#}$ implies that $a^{\#} = b^{\#}$ and hence $c^{\#} = 0$. The latter says that $c = u$ is a unit of R, so $a = bu$ and $(a) = (b)$, as required.

(iii) Let $\mathcal{C}$ be the set of all principal ideals (a) such that $a \neq 0$, a is not a unit, and a cannot be written as a finite product of irreducibles. If $\mathcal{C}$ is not empty, the maximal conditions implies that it contains a maximal member, say (a). Certainly, (a) is not irreducible, so say $a = bc$ where neither b nor c is a unit of R. Thus $b, c|a$ so $(b) \supseteq (a)$ and $(c) \supseteq (a)$. Note that $(b) = (a)$ implies that c is a unit, by (i) and the fact that R is a domain, and $(c) = (a)$ implies that b is a unit. Since neither of these occur, (b) and (c) are properly larger than (a), and hence they are not contained in $\mathcal{C}$. By definition, b and c can each be written as a finite product of irreducibles, and hence the same is true of a, contradiction. Thus $\mathcal{C} = \emptyset$ and the result is proved.

3. To avoid ambiguity, we work in a fixed algebraic closure $\tilde{K}$ of K.

(i) Let $f(x) = x^p - a \in K[x]$ and let $E = K[f]$ be the splitting field of f over K. Write $f(x) = g_1(x)g_2(x) \cdots g_r(x)$ as a product of irreducible polynomials in $K[x]$. If α_i is a root of $g_i(x)$, then α_i is a root of $f(x)$ and $|K[\alpha_i] : K| = \deg g_i(x)$. But $F \subseteq K$ contains a primitive pth root of 1, so $K[\alpha_i]$ contains all the roots of $f(x)$ and hence $K[\alpha_i] = E$. In other words, $|E : K| = \deg g_i(x)$, so all $g_i(x)$ have the same degree and $|E : K|r = \deg f(x) = p$. It follows that $|E : K| = 1$ or p. Of course, E contains a pth root of a.

(ii) Since K/F is Galois, we know that $K = F[g]$ is the splitting field of $g(x) \in F[x]$. Also let $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ be the Galois group of K/F. For each $1 \le j \le n$, let $f_j(x) = \prod_{i=1}^{j}(x^p - \sigma_i(a))$ and, for convenience, set $f_0(x) = 1$. Note that $f_n(x) \in F[x]$, since we are multiplying over the full Galois group, and we let $E = K[f] = F[gf]$ be the appropriate splitting field. Since K has characteristic 0, E/F is Galois. It remains to compute $|E : K|$. To this end, let $E_j = K[f_j]$, so that $K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = E$. Then $E_j = E_{j-1}[x^p - \sigma_j(a)]$ and, since F contains a primitive pth root of 1, we conclude from part (i) that $|E_j : E_{j-1}| = 1$ or p. But $|E : K| = \prod_{i=1}^{n} |E_i : E_{i-1}|$, so $|E : K|$ is a power of p, as required. Of course, E contains a pth root of a.

4. (i) Let $\dim V = n$ and let $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ denote the characteristic polynomial of T. Then $0 = f(T) = T^n + a_1T^{n-1} + \cdots + a_{n-1}T + a_nI$, by the Cayley-Hamilton theorem, where I is the identity operator. Since the trace is a linear map, and $\operatorname{tr}(T^k) = 0$ for $k \ge 1$, we conclude by taking traces of $0 = f(T)$ that $0 = a_n\operatorname{tr}(I) = na_n$. But the field has characteristic 0, so this yields $a_n = 0$. Moreover $\det T = \pm a_n = 0$, so T is singular and consequently $T(V) \ne V$.

(ii) Note that $T(T(V)) \subseteq T(V)$ so the restriction S makes sense. Now take a basis $\mathcal{A}$ of $T(V)$ and extend it to a basis $\mathcal{B}$ of V. If A denotes the matrix of S with respect to $\mathcal{A}$ and B denotes the matrix of T with respect to $\mathcal{B}$, then surely $B = \begin{bmatrix} A & * \\ 0 & 0 \end{bmatrix}$ since $T\colon V \to T(V)$. Moreover, $B^k = \begin{bmatrix} A^k & * \\ 0 & 0 \end{bmatrix}$, so we see that $\operatorname{tr}(S^k) = \operatorname{tr}(A^k) = \operatorname{tr}(B^k) = \operatorname{tr}(T^k) = 0$ for all integers $k \ge 1$.

(iii) We proceed by induction on $\dim V$, then case of dimension 1 being trivial. Since $\dim T(V) < \dim V$, part (ii) implies that S is nilpotent on $T(V)$. But $S = T$ on $T(V)$, so if $S^j = 0$, then $0 = S^j(T(V)) = T^j(T(V)) = T^{j+1}(V)$, and T is nilpotent.

5. (i) If $H = \ker\theta^2$, then $\theta^2(H) = 0$, so $\theta(H) \subseteq \ker\theta$. Since the image of $\theta\colon H \to \ker\theta$ is finite, and the kernel is $H \cap \ker\theta$, also finite, we conclude that H is finite. We show that G is finite by induction on n, the cases $n = 0$ and 1 being trivial. Consider the composite map $G \xrightarrow{\theta} G \to G/\ker\theta$. Since $\ker\theta$ maps to 0, this gives rise to a map $\phi\colon G/\ker\theta \to G/\ker\theta$. Indeed, since $\theta^{n-1}(G) \subseteq \ker\theta$, it follows that $\phi^{n-1}(G/\ker\theta) = 0$. Also $\ker\phi = \ker\theta^2/\ker\theta$ is finite, so induction implies that $G/\ker\theta$ is finite, and hence G is finite.

(ii) Since $|G : \theta(G)| < \infty$, it follows by applying θ that $|\theta(G) : \theta^2(G)| < \infty$. Thus $|G : \theta^2(G)| = |G : \theta(G)|\,|\theta(G) : \theta^2(G)| < \infty$. We show by induction on n that G is finite, the cases $n = 0$ and 1 being trivial. Note that $\theta(\theta(G)) \subseteq \theta(G)$, so we can let $\phi\colon \theta(G) \to \theta(G)$ be the restriction of θ. Since $\phi^{n-1}(\theta(G)) = \theta^{n-1}(\theta(G)) = 1$, and since $|\theta(G) : \phi(\theta(G))| = |\theta(G) : \theta(\theta(G))| < \infty$, it follows by induction that $\theta(G)$ is finite. But $|G : \theta(G)| < \infty$, so we conclude that G is finite.