Answers to the Algebra Qualifying Exam
January 1997

1. (i) Assume that $|H|$ is not a prime power. Suppose the prime p divides $|H|$, let Q be a Sylow p-subgroup of H and extend Q to a Sylow p-subgroup P of G. Then $P \cap H = Q \neq 1$, so by assumption, either $P \supseteq H$ or $H \supseteq P$. In the former case, H would be a p-group, contrary to our assumption. Thus $H \supseteq P$, and hence $|G|$ and $|H|$ have the same p-part. This clearly implies that $|H|$ and $|G : H|$ are relatively prime.

(ii) We show in fact that G/N is a p-group for some prime p, and consequently this factor group is nilpotent. Indeed, if distinct primes p and q divide $|G/N|$, then we can let $P, Q \supseteq N$ with P/N a Sylow p-subgroup of G/N and with Q/N a Sylow q-subgroup. Certainly $(P/N) \cap (Q/N) = 1$, so $P \cap Q = N \neq 1$. Also since $P, Q > N$ and $P \cap Q = N$, we conclude that P and Q are incomparable. This contradicts the given property of G.

(iii) Let $P \neq 1$ be a Sylow p-subgroup of N. By the Frattini argument, we have $G = N \cdot \mathbb{N}_G(P)$. Note that $\mathbb{N}_G(P) \cap N \supseteq P \neq 1$, and that $N \supseteq \mathbb{N}_G(P)$ and the preceding formula for G yield $G = N$, a contradiction. Thus $N \subseteq \mathbb{N}_G(P)$, so $P \triangleleft N$ and N is a nilpotent group.

2. Suppose first that $V = V_1 \dotplus V_2 \dotplus V_3 \dotplus \cdots$ is Artinian. Since any collection of submodules of V_i is a collection of submodules of V, it follows that each V_i is also Artinian. Furthermore, for each i, define the submodule $W_i = V_i \dotplus V_{i+1} \dotplus V_{i+2} \dotplus \cdots$ of V. Then $V = W_1 \supseteq W_2 \supseteq W_3 \supseteq \cdots$ is a descending chain which must stabilize at say n. In particular, if $i \geq n$, then $W_{i+1} = W_i = V_i \dotplus W_{i+1}$ (an internal direct sum), so $V_i = 0$.

Conversely, suppose only finitely many V_i are nonzero and that each is Artinian. Without loss of generality, we can assume that $V = V_1 \dotplus V_2 \dotplus \cdots \dotplus V_n$ for some finite n. We show that V is Artinian by induction on n, the case $n = 1$ being given. If $W = V_1 \dotplus V_2 \dotplus \cdots \dotplus V_{n-1}$, then W is Artinian by induction. Furthermore, since $V/W = (W \dotplus V_n)/W \cong V_n$ is Artinian by assumption, we conclude (by a known result) that V is also Artinian.

3. (i) Let us first do some group theory. According to Burnside's theorem, any group of order $p^a q^b$ is solvable. Also, any group whose order is divisible by 2 but not by 4 has a normal subgroup of index 2. Thus, if G is a nonsolvable subgroup of Sym_5, a group of order $120 = 2^3 \cdot 3 \cdot 5$, then $|G|$ must be divisible by $30 = 2 \cdot 3 \cdot 5$. Furthermore, in view of the second comment above, a group of order 30 has a normal subgroup of order 15 and hence is also solvable. Thus $|G| = 60$ or 120. If $|G| = 120$, then certainly $G = \mathrm{Sym}_5$. We claim that if $|G| = 60$, then $G = A = \mathrm{Alt}_5$. Indeed, first note that A is a nonabelian simple group and hence A has no subgroup of index 2 (which is necessarily normal). In particular, if H is a subgroup of Sym_5 of index 2, then $|A : A \cap H| \leq |\mathrm{Sym}_5 : H| = 2$ and hence $A = A \cap H$. Thus $H \supseteq A$ and, by order considerations, we have $H = A = \mathrm{Alt}_5$.

Now, let S denote the splitting field of $f(x) \in \mathbb{Q}[x]$. Then we know that $S/\mathbb{Q}$ is Galois with Galois group G and that G is a subgroup of Sym_5 since $f(x)$ has degree 5. Furthermore, by assumption, the field extension is not solvable and therefore the group G is not solvable. By the above considerations, we know that $G = \mathrm{Sym}_5$ or Alt_5. Finally, if

E is an intermediate field with $|E:\mathbb{Q}|=2$, then $E=S^H$ is the subfield of S elementwise fixed by a subgroup H of G of index 2. But as we have seen, Alt_5 has no subgroup of index 2 and Sym_5 has a unique subgroup of index 2. Thus, if E exists, it must be unique.

(ii) Let α and β be given with $\alpha^2, \beta^2 \in \mathbb{Q}$ and $\alpha, \beta \in S \setminus \mathbb{Q}$. Then $\mathbb{Q}[\alpha]$ and $\mathbb{Q}[\beta]$ are both quadratic extensions of $\mathbb{Q}$ contained in S. By the result of (i), these two subfields must be the same. In particular, $\beta \in \mathbb{Q}[\alpha]$, so $\beta = a\alpha + b$ with $a, b \in \mathbb{Q}$. Since $\beta^2 = a^2\alpha^2 + 2ab\alpha + b^2$, it follows that $2ab\alpha \in \mathbb{Q}$ and hence $ab = 0$. If $a = 0$, then $\beta \in \mathbb{Q}$, contradiction. Thus $b = 0$, so $\beta = a\alpha$ and $\alpha\beta = a\alpha^2 \in \mathbb{Q}$, as required.

4. Note that elements of $G = \mathrm{GL}_n(K)$ are conjugate if and only if these matrices are similar. Thus, we are asking for the number of similarity classes of involutions (elements of order 2).

(i) If $\operatorname{char} K \neq 2$, then each involution satisfies the separable polynomial $\zeta^2 - 1 = (\zeta-1)(\zeta+1)$ and hence is diagonalizable with diagonal entries ± 1. Indeed, there must be at least one -1 present here since otherwise we obtain the identity matrix, an element of order 1. Up to conjugation, we can put the $r \geq 1$ minus ones on top, so X is conjugate to $D_r = \mathrm{diag}(-1, \ldots, -1, 1, \ldots, 1)$. Furthermore, since $r = \mathrm{rank}(I - D_r)$, we see that the various D_r's are not conjugate. Thus, since $r = 1, 2, \ldots, n$, there are precisely n conjugacy classes in this case.

(ii) If $\operatorname{char} K = 2$, then the polynomial $\zeta^2 - 1 = (\zeta - 1)^2$ is not separable. However all eigenvalues are equal to 1 and we can use the Jordan canonical form to conclude that each such X is similar to a block diagonal matrix of the form $D_r = \mathrm{diag}(J, \ldots, J, 1, \ldots, 1)$ where there are r Jordan block matrices $J = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Again $r \geq 1$ and $2r \leq n$, so $r = 1, 2, \ldots, [n/2]$. Also $r = \mathrm{rank}(I - D_r)$ (check this) so the various D_r's are not similar. Thus, there are $[n/2]$ classes in this case.

5. Since S is a commutative ring which is a finite module over R, we know that S is integral over R. In the following, the elements r_i belong to R.

Suppose first that R is a field and let $\sum_{i=m}^{n} r_i s^i = 0$ be a polynomial equation of smallest degree n satisfied by s over R. Here $0 \leq m \leq n$, $r_n \neq 0$ and $r_m \neq 0$. If $m > 0$, then we can factor s^m out of this polynomial expression, since S is a domain and $s \neq 0$, to obtain a polynomial of smaller degree $n - m$, contradiction. Thus, $m = 0$ and $s(\sum_{i=0}^{n-1} r_{i+1} s^i) = -r_0 \neq 0$. But $-r_0$ is a nonzero element of the field R, so $-r_0$ is invertible and hence so is s. Indeed, $s^{-1} = -r_0^{-1}(\sum_{i=0}^{n-1} r_{i+1} s^i)$. Alternately, this direction follows easily from the Wedderburn theorem since S, being finite dimensional over the field R, is an Artinian integral domain and hence a field.

Conversely, suppose S is a field and let $0 \neq r \in R$. Then $r^{-1} \in S$, so r^{-1} is integral over R. Say $(r^{-1})^n = \sum_{i=0}^{n-1} r_i (r^{-1})^i$. Multiplying by r^{n-1}, we get $r^{-1} = \sum_{i=0}^{n-1} r_i r^{n-1-i} \in R$ and hence R is a field.