Answers to the Algebra Qualifying Exam
August 2003

1. a. Suppose by way of contradiction that $G \subseteq \mathrm{Alt}_7 \subseteq \mathrm{Sym}_7$. If P is a Sylow 7-subgroup of G, then $|P| = 7$ and we can clearly assume that P is generated by the 7-cycle $(1\,2\,3\,4\,5\,6\,7)$. It is then easy to see that P is self-centralizing in Sym_7 and hence in G. (Alternately, one can use the fact that a transitive abelian group is regular.) In particular, if N is the normalizer of P in Sym_7, then N/P embeds in $\mathrm{Aut}(P)$, a cyclic group of order 6. But $x = (1\,7)(2\,6)(3\,5)$ is an element of order 2 in N and x, being an odd permutation, is not contained in Alt_7. Thus, the normalizer of P in Alt_7 has order dividing $7{\cdot}3$ and hence the same is true for the normalizer of P in G. It follows that n_7, the number of Sylow 7-subgroups of G is equal to $2^3{\cdot}3^2$ or $2^3{\cdot}3^2/3$, a contradiction since $n_7 \equiv 1\ (7)$.

b. Assume that G is simple and let n_3 be the number of Sylow 3-subgroups of G. Then $n_3 \neq 1$, $n_3 \mid 2^3{\cdot}7$ and $n_3 \equiv 1\ (3)$, so $n_3 = 4$, 7 or 28. If N is the normalizer of a Sylow 3-subgroup of G, then $|G : N| = n_3$ and, since G is simple, the $n!$ Theorem implies that G embeds in Sym_{n_3}. In particular, $n_3 \neq 4$ since $|G| > 4!$. Furthermore, if $n_3 = 7$, then $G \subseteq \mathrm{Sym}_7$ and, since $G \cap \mathrm{Alt}_7 \lhd G$, it follows easily that $G \subseteq \mathrm{Alt}_7$, contradicting part (a) above. Thus the only possibility is $n_3 = 28$.

2. a. Let P be a nonzero prime ideal of the integral domain R and choose $0 \neq p \in P$. Then $1/p \in K = R[1/t]$, so $1/p = r_0 + r_1/t + \cdots + r_n/t^n$ for suitable $r_i \in R$. Multiplying by p and t^n to clear denominators, we get $t^n = p(r_n + r_{n-1}t + \cdots + r_0 t^n) \in pR \subseteq P$. Thus since P is a prime ideal and $t^n \in P$, we conclude that $t \in P$.

b. Let $a_1, a_2, \ldots, a_n \in F$ and consider the evaluation map $R = F[X_1, X_2, \ldots, X_n] \to F$ given by $g(X_1, X_2, \ldots, X_n) \mapsto g(a_1, a_2, \ldots, a_n)$. This is clearly a ring homomorphism onto the field F, so the kernel is a nonzero maximal ideal of R. In particular, this kernel is a prime ideal, so by assumption, $f(X_1, X_2, \ldots, X_n)$ is contained in the kernel. In other words, $f(a_1, a_2, \ldots, a_n) = 0$.

Now let F be an infinite field. We show by induction on $n \geq 1$ that if the polynomial $f(X_1, X_2, \ldots, X_n)$ is not 0, then there exist $a_1, a_2, \ldots, a_n \in F$ with $f(a_1, a_2, \ldots, a_n) \neq 0$. First, if $n = 1$, we know that f has at most $\deg f$ roots. Thus, since F is infinite, there must exist $b \in F$ with $f(b) \neq 0$. Now let $n > 1$ and write $f(X_1, X_2, \ldots, X_n) = \sum_{i=0}^{m} g_i(X_1, \ldots, X_{n-1}) X_n^i$ as a polynomial in X_n over $F[X_1, \ldots, X_{n-1}]$. Since $f \neq 0$, we can assume that $g_m(X_1, \ldots, X_{n-1}) \neq 0$. Hence, by induction, there exist $a_1, \ldots, a_{n-1} \in F$ with $g_m(a_1, \ldots, a_{n-1}) \neq 0$ and thus $f(a_1, \ldots, a_{n-1}, X_n) = \sum_{i=0}^{m} g_i(a_1, \ldots, a_{n-1}) X_n^i$ is a nonzero polynomial in $F[X_n]$ of degree m. By the $n = 1$ case, there exists $a_n \in F$ with $f(a_1, a_2, \ldots, a_n) \neq 0$.

3. a. Assume that $\alpha^m \in F$ and write $m = nq + r$ with integers q and r satisfying $0 \leq r < n$. Then $\alpha^r = \alpha^m/(\alpha^n)^q \in F$ and the minimality of n yields $r = 0$. Thus $n \mid m$.

b. Suppose $\mathrm{char}\, F = p > 0$ and that $p \mid n$. If $m = n/p$, then $\beta = \alpha^m \in E$ and $\beta^p = \alpha^n = b \in F$. In particular, β is a root of $f(X) = X^p - b \in F[X]$ and hence $g(X)$, the minimal monic polynomial of β over F, divides $f(X)$. Furthermore, $g(X)$ has

distinct roots since E/F is separable, and in $E[X]$ we have $g(X) \mid f(X) = (X-\beta)^p$. Thus $g(X) = X - \beta$, so $\alpha^m = \beta \in F$ and this contradicts the minimality of n.

c. Let $\alpha^n = a \in F$ so that α is a root of $f(X) = X^n - a \in F[X]$. We show that $f(X)$ is irreducible. Indeed, let $g(X)$ be any monic factor of $f(X)$ in $F[X]$ with $\deg g(X) = m \geq 1$. Then the roots of $g(X)$ are roots of $f(X)$, so they are all of the form $\alpha\varepsilon$ with $\varepsilon^n = 1$. Thus the product of the roots of $g(X)$ is equal to $\alpha^m\delta$ with $\delta^n = 1$. But this product is $\pm$ a coefficient of $g(X)$ and hence is contained in F. In particular, since $0 \neq \alpha^m \in E$, we see that δ is a root of unity in E and hence in F, by assumption. It now follows that $\alpha^m \in F$ and the minimality of n implies that $m = n$, as required. Since $f(X)$ is irreducible in $F[X]$, $f(\alpha) = 0$ and $E = F[\alpha]$, we conclude that $|E : F| = \deg f(X) = n$.

4. a. Let a be a real number. If $a \geq 0$, we can write $a = b^2 - c^2$ with $c = 0$ and if $a < 0$, we can write $a = b^2 - c^2$ with $b = 0$. Thus, in general, $a = b^2 - c^2$ with b and c real and $bc = 0$. Now if $A = \operatorname{diag}(a_1, a_2, \ldots, a_n)$ is a real diagonal matrix, write each $a_i = b_i^2 - c_i^2$ as above, with $b_i c_i = 0$, and define $B = \operatorname{diag}(b_1, b_2, \ldots, b_n)$ and $C = \operatorname{diag}(c_1, c_2, \ldots, c_n)$. Then, by the way diagonal matrices multiply, we conclude that $A = B^2 - C^2$ and also that $BC = CB = 0$.

b. If A is a real symmetric matrix, then we know that A is diagonalizable. Thus there exists an invertible matrix U and a diagonal matrix A_0 with $A = U^{-1}A_0U$. By part (a), we have $A_0 = B_0^2 - C_0^2$ with $B_0C_0 = C_0B_0 = 0$. In particular, if we set $B = U^{-1}B_0U$ and $C = U^{-1}C_0U$, then since conjugation is an algebra automorphism, it follows that $A = B^2 - C^2$ and $BC = CB = 0$. Since A is symmetric, we can actually assume that U is an orthogonal matrix so that $U^{-1} = U^T$. Furthermore, since we can take B_0 and C_0 to be diagonal, it follows that we can find suitable B and C which are both symmetric.

c. Suppose B has a nonzero real eigenvalue λ and choose v to be a nonzero column vector with $Bv = \lambda v$. Then $B^2v = B(\lambda v) = \lambda^2 v$, and $\lambda(Cv) = C(Bv) = 0$ since $CB = 0$. Thus, since $\lambda \neq 0$, we have $Cv = 0$ and hence $C^2v = 0$. It follows that $Av = (B^2 - C^2)v = \lambda^2 v$, so v is an eigenvector for A with eigenvalue $\lambda^2 > 0$.

5. a. Note that $DM(x^n) = D(x^{n+1}) = (n+1)x^n$ and that $MD(x^n) = M(nx^{n-1}) = nx^n$. Thus $(DM - MD)(x^n) = x^n = I(x^n)$ and, since this is true for all $n \geq 0$, it follows that $DM - MD = I$.

b. Suppose, by way of contradiction, that there exist field elements $k_{i,j} \in K$, not all zero, with $\sum_{i,j} k_{i,j} M^i D^j = 0$, and let n be the smallest j-subscript with some $k_{i,j} \neq 0$. Using $D^j(x^n) = 0$ for $j > n$, $D^n(x^n) = n!$, and $k_{i,j} = 0$ for $j < n$, we obtain $0 = \sum_{i,j} k_{i,j} M^i D^j(x^n) = \sum_i k_{i,n} M^i(n!) = n! \sum_i k_{i,n} x^i$. Since $\operatorname{char} K = 0$, we can cancel the $n!$ factor and conclude that the polynomial $\sum_i k_{i,n} x^i$ is 0. Thus $k_{i,n} = 0$ for all i, contradicting the fact that some $k_{i,n}$ is supposed to be nonzero.

c. We show by induction on $t \geq 0$ that DM^t is in KL, the K-linear span of the elements of L. This is clear for $t = 0$ since $DM^0 = M^0D \in L$. Suppose now that the result holds for t and observe that $DM^{t+1} = DM \cdot M^t = (I + MD) \cdot M^t = M^t + M \cdot DM^t$. Now $M^t = M^t D^0 \in L$ and $DM^t \in KL$. Thus, since L is closed under left multiplication by M, it follows that $M \cdot DM^t \in M \cdot KL \subseteq KL$. Hence $DM^{t+1} = M^t + M \cdot DM^t \in KL$, and the result follows by induction.