

UNIVERSITY OF MICHIGAN
DEPARTMENT OF MATHEMATICS
Solutions to May 2007 Algebra QR Exams

MORNING

(AM1) (a) The number $kp + 1$ of Sylow p -subgroups is $\equiv 1 \pmod p$ and divides N . Since $kp + 1 > p > N$ unless $k = 0$, we must have $k = 0$, and the Sylow p -subgroup is normal.

(b) By part (a) with $N = q^b r^c$, we have that there is a normal Sylow p -subgroup H . Then H is nilpotent, and so it suffices to show that $Q = G/H$ is solvable, since an extension of one solvable group by another is solvable. By part (a) again, the Sylow q -subgroup K of Q is normal. Again, K is nilpotent, and so is Q/K , so both are solvable and so is G .

(AM2) (a) The map $(A, B) \mapsto AB - BA$ is clearly bilinear and alternating, whence it induces a map as specified.

(b) Let E_{ij} be the matrix with 1 in the i, j spot and 0 elsewhere. Then $T(E_{ii}, E_{i,j}) = E_{ij} - 0 = E_{ij}$ for $i \neq j$, while $T(E_{ij}, E_{ji}) = E_{ii} - E_{jj}$. It follows that the image of the map contains all matrices of trace 0. Since AB and BA always have the same trace, the image is precisely the matrices of trace 0.

(c) Since the dimension of the image is $9 - 1 = 8$, and the dimension of $\wedge^2(M)$ is $\binom{9}{2} = 36$, the dimension of the kernel is $36 - 8 = 28$.

(AM3) We have $A \cdot \text{adj}(A) = dI$, $d = \det(A)$. There are integer matrices P, Q , invertible over \mathbf{Z} so that $PAQ = D := \text{diag}(d_1, d_2, \dots, d_n)$. We have $(PAQ)(Q^{-1}\text{adj}(A)P^{-1}) = dI$. Therefore, $Q^{-1}\text{adj}(A)P^{-1} = D^{-1}dI = \text{diag}(d/d_1, d/d_2, \dots, d/d_n)$. Since the left side is an integer matrix, so is the right side. We have the required divisibility if we choose D to satisfy the additional condition $d_1|d_2|\dots$, and we may do so.

Alternate solution: For matrices of indeterminates U, V , over \mathbf{Z} , which are invertible over the fraction field of a polynomial ring in those indeterminates over \mathbf{Z} , we have that

$$\text{adj}(UV) = \det(UV)(UV)^{-1} = \det(U)\det(V)V^{-1}U^{-1} = \text{adj}(V)\text{adj}(U).$$

Hence, this holds in an arbitrary commutative ring. Therefore, multiplying a matrix by an invertible matrix on the left or the right will not change either its fundamental invariants, nor those of its classical adjoint. We may consequently assume that the given matrix is diagonal with entries d_1, \dots, d_n , where $d_1|d_2|\dots|d_n$. and then one sees that the adjoint is diagonal, with entries equal to the products of the d_j taken $n - 1$ at a time. Therefore, its invariants are $d/d_n, \dots, d/d_1$. Note that $(d/d_i)/(d/d_{i+1}) = d_{i+1}/d_i$, which is an integer.

(AM4) The action of the Galois group, even the action of α , on the roots is transitive, and so the polynomial must be irreducible. α and β are among the symmetries of a square whose consecutive vertices are labeled r_1, r_2, r_3, r_4 , and since the group of symmetries of a square has order 8 and β is not a power of α , which has order 4, α and β must generate the group of symmetries of a square. Since the Sylow 2-Subgroup of Sym_4 has order 8, H is a Sylow 2-subgroup. The number of such subgroups is 3, since it must divide 3 and is larger

than one (they are elements of order 2 in Sym_4 other than those specified). $d = [L^H : K]$ is the index of H in G , which is 3. Each K' of degree 3 corresponds to a Sylow 2-subgroup, and so there are 3 such fields.

(AM5) Take the basis $1, x, x^2$. Then the matrix is $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix}$. Subtract twice the first

row from the second and twice the first column from the second. Then subtract 3 times the first row from the third and 3 times the first column from the third. This gives the

equivalent matrix $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -2 \\ 0 & -2 & -4 \end{pmatrix}$. Now subtract twice the second row from the third and

twice the second column from the third to get $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. The rank is two and the

signature as a triple is $(p, q, r) = (1, 1, 1)$. [The signature $p - q$ as a single real number is 0.] The form is neither positive nor negative semi-definite.

AFTERNOON

(PM1) (a) Suppose β fixes i . The orbit of any element different from i contains all of the others, even if we only let β act. Since $\alpha(i)$ is in this orbit, the action is transitive. The orbit of (i, j) for $j \neq i$ contains all elements (i, k) for $k \neq i$, simply using the action of β . If we conjugate α by an element that maps i to j , we obtain a p -cycle that fixes j . Hence, for fixed j , all pairs (j, k) with $j \neq k$ are in the same orbit of G . But any pair (i, k) with i, k distinct can be mapped to a pair (j, k') with j, k' distinct. Hence, there is only one orbit.

(b) β is even, while α is the product of $(p+1)/2 = 2k+1$ transpositions if $p = 4k+1$. Hence the, even permutations in G form a proper non-trivial normal subgroup.

(c) By part (a), the stabilizer of any one pair, say $(0,1)$, has index $p(p+1)$. Alternatively, since the group contains an element of order p , its order is divisible by p . Since the action is transitive, the stabilizer of one element has index $p+1$, and so $p+1$ divides the order. Since p and $p+1$ are relatively prime, we have that $p(p+1)$ divides $|G|$.

(PM2) (a) Let h be N restricted to the multiplicative group of \mathbf{F}_{q^n} . Then $h : \mathbf{F}_{q^n}^\times \rightarrow \mathbf{F}_q^\times$ is a homomorphism from a cyclic group of order $q^n - 1$ to its subgroup of order $q - 1$, $h(x) = x^s$, where $s = 1 + q + \cdots + q^{n-1}$. Since s divides $q^n - 1$, $s = |Ker(h)|$. Since $|Im(h)| = (q^n - 1)/s = q - 1$, h is onto.

Alternate: Let $s = 1 + q + \cdots + q^{n-1}$. Evidently, 0 is in the image of N . Suppose $a \in \mathbf{F}_q - \{0\}$. There exists an element of the algebraic closure of \mathbf{F}_q , call it b , such that $b^s = a$. Then $b^{s(q-1)} = a^{q-1} = 1$, and $s(q-1) = q^n - 1$, so that $b^{q^n-1} = 1$. Hence, $b \in \mathbf{F}_{q^n}$, as needed.

(b) The product of norm 1 elements has norm 1, so $\text{span}(S)$ (meaning, span over \mathbf{F}_q) is a subring of \mathbf{F}_{q^n} . In general, a subring of an integral domain is an integral domain, and a finite integral domain is a field. Therefore, $\text{span}(S)$ is a subfield of \mathbf{F}_{q^n} . Since $\text{span}(S)$ contains \mathbf{F}_q as a subfield, the theory of finite fields tells us that $|\text{span}(S)| = q^r$, for some $r, 1 \leq r \leq n$. Since the set of norm 1 elements has cardinality $1 + q + \cdots + q^{n-1} > q^{n-1}$, $r = n$, i.e., $\text{span}(S) = \mathbf{F}_{q^n}$.

Alternate proof: The multiplicative group of \mathbf{F}_{q^n} is cyclic of order $q^n - 1 = (q-1)s$. Let u be a generator. Then the roots of $x^s = 1$ are the powers of $y = u^{q-1}$, which has order s . The smallest Galois field containing y and \mathbf{F}_q must be \mathbf{F}_{q^m} where $s|(q^m - 1)$, and so $q^n - 1 = (q-1)s$ divides $(q-1)(q^m - 1)$ properly. If this field is strictly contained in \mathbf{F}_{q^n} , we must have that $m|n$ properly. But then $q^n - 1 > (q-1)(q^m - 1)$, a contradiction.

(PM3) If two matrices commute, each stabilizes the eigenspace of a given eigenvalue of the other. The result follows by induction on the number of elements in a set of generators for R , since the restriction of a diagonalizable transformation to a subspace it stabilizes is still diagonalizable (the minimal polynomial of the restriction is obviously square-free).

(PM4) (a) Let $f : R/(a) \rightarrow R/(b)$ be an R -homomorphism. For all $x \in R$, $af(x + (a)) = f(0 + (a)) = 0$. So $f(x) \in R/(b)$ is annihilated by a . If $b = 0$, $a = 0$.

Suppose $b \neq 0$. Then both a and b annihilate $f(x)$, whence so does (a, b) . The image of f is determined by the single element $f(1)$, which is annihilated by (a, b) . Therefore,

$H := \text{Hom}_R(R/(a), R/(b)) \cong R/(c)$ for some $c \in R$ so that (c) contains (a, b) . We show that $(c) = (a, b)$ by producing a member of H whose annihilator is exactly (a, b) . Let d be a g.c.d. of a and b . Define $u := a/d, v := b/d$. Define $f \in R$ to be the homomorphism which satisfies $f(x + (a)) = xv + (b)$, for all $x \in R$. One must check that this is well-defined and that the annihilator of $f(1)$ is just (d) .

(b) Since Hom preserves direct sums, H is isomorphic to a direct sum of R -modules as in (a). We get a torsion module only in one of these cases: $\text{Hom}(R, R/(b))$ for $b \neq 0$ and $\text{Hom}(R/(a), R/(b))$ when $a \neq 0, b \neq 0, (a, b) \neq (1)$. For the given example ($R = K[x]$), this means the cases $\text{Hom}(R, R/((x-1)^3)) \cong R/((x-1)^3)$ (two times) and $\text{Hom}(R/(x^2-1), R/((x-1)^3))$ (one time). The torsion submodule T of H therefore satisfies $T \cong R/((x-1)^3) \oplus R/((x-1)^3) \oplus R/(x-1)$. The torsion-free part is the same as $\text{Hom}_R(R^2, R^3)$, or the direct sum of six copies of $\text{Hom}_R(R, R)$, i.e., R^6 .

(PM5) Since $x^6 - x^4$ factors $x^4(x-1)(x+1)$ and $x^4 - 2x^3 + x^2$ factors $x^2(x-1)^2$, the conditions hold if and only if A satisfies the GCD, namely $x^2(x-1)$. Each Jordan block for the eigenvalue 0 is either 1×1 or 2×2 , while the Jordan blocks for the eigenvalue 1 are all size one. Thus, there are either two size 2 blocks for 0 (one possibility), one size two block for 0 and two blocks of size 1 (3 possibilities), or else the Jordan form is diagonal with eigenvalues 0 and or 1 (5 possibilities, governed by the number of 1s which occur).