

UNIVERSITY OF MICHIGAN
DEPARTMENT OF MATHEMATICS

Solutions to January 2007 Algebra QR Exams

MORNING

(AM1) Let $\Gamma = \{x_1, \dots, x_k\}$. Let π be any permutation of Γ . By the definition of k -fold transitive, there is an element $g \in G$ such that g sends $(x_1, \dots, x_k) \mapsto (\pi(x_1), \dots, \pi(x_k))$. Evidently, the map from H to the permutations of Γ , which is given by restriction, is surjective. For $k \geq 5$, the alternating group A_k is simple, and, hence, not solvable. Therefore Sym_k is not solvable for $k \geq 5$. Since subgroups of solvable groups are solvable, if G were solvable, H would be solvable. But then, since homomorphic images of solvable groups are solvable, Sym_k would be solvable as well.

(AM2) (a) The standard construction of \mathbf{F}_q is as the splitting field of $x^q - x$, with all elements of the field occurring as roots. Hence, the product is $x^q - x$. One may verify that the roots of this polynomial form a field with q elements as follows. Since the derivative of $x^q - x$ is -1 working mod p , the roots are mutually distinct. 0 and 1 are clearly roots. If $r^q = r$ and $s^q = s$ are roots we have $(r + s)^q = r^q + s^q = r + s$, $(rs)^q = r^q s^q = rs$, $(-r)^q = (-1)^q r^q = -r$ (this is correct even if $p = 2$, since $1 = -1$), and if $r \neq 0$, $(1/r)^q = 1/r^q = 1/r$. Thus, the q distinct roots form a field.

(b) \mathbf{F}_{q_0} is contained in \mathbf{F}_q if and only if q is a power of q_0 . Adjoining r to \mathbf{F}_p yields a field with p^d elements. Hence, the condition is that $q = p^{de}$ for some positive integer e .

(AM3) We use induction on n . If all of the matrices are invertible, the product is also invertible and cannot be 0. Hence, at least one of the matrices has rank $r < n$. Since the matrices commute, we may renumber and assume it is A_1 . If $n = 1$ we have that $A_1 = 0$ and we are done. If $n > 1$, note that since the matrices commute, $A_i A_1 V = A_1 A_i V$ for all i , and so A_2, \dots, A_n all map $W = A_1 V$ into itself. Since the dimension of W is $< n$, we may apply the induction hypothesis to the restrictions of the A_i , $i \geq 2$, to W , and conclude that we may choose $n - 1$ or fewer of these restrictions whose product is 0. Again, we may renumber and call these A_2, \dots, A_t where $t \leq n$. Then $A_2 \cdots A_t (A_1 V) = 0$, which implies that $A_2 \cdots A_t A_1 = 0$.

(AM4) Since there are 6 elements of order 4, there are three subgroups of order 4: each contains two elements of order 4, and either of these generates. (There cannot be any subgroups of order 4 in which there is no element of order 4, since there is only one element of order 2.) Each of these is normal since a subgroup of index 2 is normal. Because there is only one element of order 2, there is just one subgroup of order 2, and this is normal since its only possible conjugate is itself. Together with G , which has order 8, and the trivial subgroup, which has order 1, these constitute all of the subgroups of G . All subgroups of G are normal.

(b) By the Fundamental Theorem of Galois Theory, there is a bijective correspondence between subgroups of G and fields intermediate between K and L : the field corresponding to $H \subseteq G$ is the field fixed by H , while the subgroup corresponding to F is the Galois

group of L over F . This correspondence reverses inclusion, and the degree of the field corresponding to H is the index of H in G . Normal subgroups correspond to normal field extensions. The possible degrees are 1, 2, 4, and 8. There is one extension of degree 1, corresponding to G itself, there are three extensions of degree 2, corresponding to the three subgroups of order 4, one extension of degree 4, corresponding to the subgroup order 2, and one extension of degree 8, namely L , corresponding to the trivial subgroup of G .

(AM5) After a change of basis in each vector space, we may assume that each matrix is in Jordan canonical form or at least, say, upper triangular. Let s_1, \dots, s_p be the eigenvalues of S and t_1, \dots, t_q be the eigenvalues of T . Then there is a matrix for $S \otimes T$ in block form, which is a $p \times p$ matrix of $q \times q$ blocks in which a typical block is $a_{ij}T$, where $S = (a_{ij})$. This matrix is upper triangular with diagonal entries $s_i t_j$, from which it follows that $\text{Trace}(S \otimes T) = \sum_{i,j} s_i t_j = (\sum_i s_i)(\sum_j t_j) = \text{Trace}(S)\text{Trace}(T)$, as required. Moreover, $\det(ST) = \prod_{i,j} (s_i t_j) = (\prod_i s_i)^q (\prod_j t_j)^p$, since every s_i occurs in q terms and every t_j occurs in p terms. But this is $\det(S)^q \det(T)^p$.

AFTERNOON

(PM1) Each eigenvalue x must satisfy $x^4 - x^2 = 0$, and so the only possible eigenvalues are 0, 1, and -1 . Since 1 and -1 have multiplicity 1 and each Jordan block of the matrix must satisfy the equation, 1 and -1 can only occur in 1×1 blocks, while 0 can occur either in a 1×1 block or in a 2×2 block, namely, $J_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. We may then have:

- (1) The matrix is the direct sum of two copies of J_2 . This yields one similarity class.
- (2) The matrix is the direct sum of J_2 and two 1×1 blocks. The 2 eigenvalues of the size 1 blocks may be equal (3 cases) or distinct (3 cases). This yields 6 similarity classes.
- (3) The matrix is diagonal. All 4 entries may be equal (3 cases), three equal and one distinct (6 cases), or 2 equal and 2 distinct (3 cases). This yields 12 similarity classes.

Hence, there are $1 + 6 + 12 = 19$ similarity classes of such matrices.

(PM2) (a) If G is a group, we may define $Z(G)$ to be the center of G . We may then define the *upper central series* of G by letting $U^0(G) = \{e\}$, the trivial subgroup of G , and by letting $U^{i+1}(G)$ be the inverse image in G of $Z(G/U^i(G))$. G is *nilpotent* if there exists an integer n such that $U^n(G) = G$.

[Alternate. Define the *lower central series* L_n of G by letting $L_0(G) = G$ and $L_{i+1}(G) = (G, L_i(G))$, the commutator subgroup of G with $L_i(G)$, $i \geq 0$. Then G is *nilpotent* if there exists an integer n such that $L_n(G) = \{e\}$, the trivial subgroup of G .]

[Alternate: a group G is *nilpotent* if it has a finite central series, that is, a sequence of normal subgroups $\{e\} = Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq \cdots \subseteq Z_n = G$ such that Z_{i+1}/Z_i is in the center of G/Z_i , $0 \leq i \leq n-1$.]

(b) Call the two subgroups N and N' . Since the quotient by either N or N' is a homomorphic image of an abelian group and so abelian, $(G, G) \subseteq N \cap N'$, and since every element of $N \cap N'$ commutes with every element of N , and also with every element of N' , and N, N' generate G , $N \cap N' \subseteq Z(G)$. Hence (G, G) is a subgroup of the center, and $G/(G, G)$ is abelian.

(PM3) Elementary row and column operations on the matrix do not affect the isomorphism class of the module E/D . We may subtract multiples of the first row from the second and third rows and of the fourth row from the second third rows to produce the first matrix shown. We then move the third row first, subtract $x^2 + 1$ times the first column from the third, and subtract x times the first row from the second to obtain the second matrix shown. Finally, we can subtract the second row from the third and switch them to obtain the third matrix shown, which is diagonal.

$$\begin{pmatrix} x & 0 & 0 & 0 \\ 0 & x+1 & x^3+x & 0 \\ 1 & 0 & x^2+1 & 0 \\ 0 & 0 & 0 & x \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & x^3+x & 0 \\ 0 & x+1 & x^3+x & 0 \\ 0 & 0 & 0 & x \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x+1 & 0 & 0 \\ 0 & 0 & x^3+x & 0 \\ 0 & 0 & 0 & x \end{pmatrix}.$$

Noting that $x^3 + x = x(x^2 + 1) = x(x + 1)^2$, we see that the quotient E/D is clearly $R/(x + 1)R \oplus R/x(x + 1)^2R \oplus R/xR$. When f and g are relatively prime in a PID, (#) $R/fgR \cong R/fR \oplus R/gR$, so that we can combine the first and third summands. Thus,

$E/D \cong R/x(x+1)R \oplus R/x(x+1)^2R$, which has the required form for part (a). For part (b) we may use (#) repeatedly to rewrite this as $R/xR \oplus R/xR \oplus R/(x+1)R \oplus R/(x+1)^2R$, which has the required form.

(PM4) (a) Both G and H permute the roots of f and each element is determined by its action on the roots. Therefore, each may be thought of as a subgroup of the permutations Σ of the roots of f . The image of H is a subgroup of G . By the Fundamental Theorem of Galois Theory, every subgroup H occurs, simply by taking L to be the fixed field of H within the splitting field of f over \mathbf{Q} .

(b) By Eisenstein's criterion, $x^p - 2$ is irreducible over \mathbf{Q} , and so if r denotes a root we have that $[\mathbf{Q}[r] : \mathbf{Q}] = p$. Let θ be a primitive p th root of unity. Then the roots of $x^p - 2$ are the elements $\theta^k r$, $0 \leq k \leq p-1$, and the splitting field K is $\mathbf{Q}[r, \theta]$. Since $[\mathbf{Q}[\theta] : \mathbf{Q}] = p-1$, the Galois group G must have order $(p-1)p$: we must have that $x^p - 2$ is irreducible over $\mathbf{Q}[\theta]$, or else $|G|$ will fail to be divisible by p . There will be an automorphism α that sends r to θr , and that fixes θ (if it maps $\theta \mapsto \theta^k$ where k has inverse k' mod p , we may compose with an automorphism that fixes r and sends $\theta \mapsto \theta^{k'}$). Then α corresponds to the p -cycle that sends $\theta^j r \mapsto \theta^{j+1} r$, $0 \leq j \leq p-1$. G is the product of $\langle \alpha \rangle$ and the cyclic group H of order $p-1$ consisting of automorphisms that fix r and permute $\{\theta^j : 1 \leq j \leq p-1\}$: H is isomorphic to the multiplicative group of $\mathbf{Z}/p\mathbf{Z}$. Note that H is the group corresponding to the intermediate field $\mathbf{Q}[r]$ and is not normal: $\alpha H \alpha^{-1}$ is the group corresponding to $\mathbf{Q}[\alpha(r)]$, which is different from $\mathbf{Q}[r]$. $\langle \alpha \rangle$ is normal, and corresponds to the intermediate field $\mathbf{Q}[\theta]$.

(PM5) (a) Any symmetric form is equivalent by change of basis to a diagonal matrix whose only diagonal entries are 1, -1 , and 0, and if p , q , and r denote the number of each, the equivalence class of the matrix is uniquely determined by the triple (p, q, r) , where $p + q + r = n$. The term "signature" is used either for the triple (p, q, r) or for the trace, which is $p - q$. The equivalence relation on symmetric matrices is given by $S \sim T$ if there exists A real invertible such that $S = A T A^{tr}$ where A^{tr} is the transpose of A . The equivalence relation on matrices is called congruence by some authors and cogredience by others.

(b) Choose a basis so that the matrix has a standard form as above. With notation as above, the form is nondegenerate if and only if $r = 0$, so that $p + q = n$. Let d be the smaller of p , q . Suppose $p \geq q$ (respectively, $p \leq q$). On the subspace U spanned by the last $2d$ (respectively, first $2d$) standard basis vectors, the matrix is equivalent to $\begin{pmatrix} I_d & 0 \\ 0 & -I_d \end{pmatrix}$.

This matrix is equivalent to $\begin{pmatrix} 0 & I_d \\ I_d & 0 \end{pmatrix}$: after permuting the basis, one may think of the original matrix as the direct sum of d 2×2 matrices each of which is $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and each of these is equivalent to $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ by 45 degree rotation and dilation. On U^\perp , the form is positive definite or negative definite. In either case, there is no $v \in U^\perp - \{0\}$ such that $B(v, v) = 0$. If we use the version of signature where the value is $p - q$, $d = (n - |p - q|)/2$.