

UNIVERSITY OF MICHIGAN

DEPARTMENT OF MATHEMATICS

Solutions to January 2009 Algebra QR Exams

MORNING

1. Let  $G$  be the group of invertible  $4 \times 4$  matrices over the complex numbers, and let  $M$  be the set of all  $4 \times 4$  complex matrices.

(a) Consider the action of  $G \times G$  on  $M$  given by  $(g, h)$  acts on  $m$  by the matrix multiplication  $gmh^{-1}$ . Describe the orbits of this action.

(b) Consider the action of  $G$  on  $M$  by conjugation:  $g$  acts on  $m$  by the matrix multiplication  $gmg^{-1}$ . For what  $\lambda$  and  $\mu$  are the two matrices below in the same orbit?

$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & \mu & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \lambda & \mu \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

Solution: (a) The action of  $G$  on the left and right amounts to row and column operations. This action preserves rank, and on the other hand, a matrix of rank  $r$  can be brought to the form with  $r$  1s along the diagonal and zeros elsewhere. So there are precisely 5 orbits: the matrices of rank  $r$  for  $r = 0, 1, 2, 3, 4, 5$ .

(b) Here the orbits are given by the different Jordan forms. The first matrix has two Jordan blocks of size two, with eigenvalues 1 and 3 respectively. Since the second matrix is already in block form, we can treat the blocks separately. The upper block has the right eigenvalues, so we only need that  $\mu$  be nonzero in order to ensure that it is a size two block. In order to make the lower block be a Jordan 2-block with eigenvalue 3, we must have  $\lambda = 3$ .

2. Consider the real quadratic form  $Q(x, y, z) = x^2 + 4xy + y^2 + \lambda z^2$ , where  $\lambda$  is some fixed real number. Compute the rank and signature of  $Q$  as a function of  $\lambda$ .

Solution. The symmetric matrix corresponding to  $Q$  is  $\begin{pmatrix} 1 & 2 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & \lambda \end{pmatrix}$ .

First method. The characteristic polynomial of the  $2 \times 2$  matrix in the upper left corner is  $x^2 - 2x - 3$  which has roots 3 and  $-1$ . Hence, the matrix is orthogonally similar to a matrix with diagonal entries 3,  $-1$ ,  $\lambda$ . The rank is 3 unless  $\lambda = 0$ , in which case the rank is 2. The signature as a

triple as  $(2, 1, 0)$ ,  $(1, 1, 1)$ , or  $(1, 2, 0)$  according as  $\lambda > 0$ ,  $\lambda = 0$ , or  $\lambda < 0$ , where signature  $(p, q, r)$  indicates that the number of positive diagonal entries is  $p$ , the number of negative entries is  $q$ , and the number of zero entries is  $r$ . Alternatively the signature as a single real number  $p - q$  is 1, 0, or  $-1$ , according as  $\lambda > 0$ ,  $\lambda = 0$ , or  $\lambda < 0$ .

Second method. Subtract twice the first row from the second and twice the first column from the second: this preserves the cogredience class (although not the eigenvalues). The matrix becomes diagonal with entries 1,  $-3$ ,  $\lambda$ . The rest of the analysis is the same.

3. Let  $R$  be the ring  $\frac{\mathbf{Z}[x, y]}{(12, x^2, y^3)}$ . Find all prime ideals of  $R$ , giving explicit generators for each.

Solution:

Every prime must contain the image of  $x$  (since its square is 0) and the image of  $y$  (since its cube is 0). Also, since  $2 \cdot 2 \cdot 3 = 0$ , every prime must contain either 2 or 3. The ideal generated by the images of  $2, x, y$  is prime: the quotient is  $\mathbf{Z}/(2)$ , a field, and the ideal generated by the images of  $3, x, y$  is prime: the quotient is  $\mathbf{Z}/(3)$ . These are the only primes: they are both maximal ideals (which is unusual).

4. Fix a vector space  $V$  of dimension three over the finite field  $\mathbf{F}_q$  of  $q$  elements. Find the cardinality of the following sets (with full justification):

- (a) The set of all linear transformations  $T : V \rightarrow V$ .
- (b) The set of all invertible linear transformations  $T : V \rightarrow V$ .
- (c) The set of isomorphism classes of  $\mathbf{F}_q[X]$ -module structures on  $V$ .

Solution:

(a) We need to count the number of  $3 \times 3$  matrices over  $\mathbf{F}_q$ . This is  $q^9$ .

(b) We need to count the number of *invertible*  $3 \times 3$  matrices over  $\mathbf{F}_q$ . There are  $q^3 - 1$  choices for the first column. The second column can be any vector from  $V$  not in the span of the first column: there are  $q^3 - q$  such choices. The third column can be any vector not in the span of the first two: there are  $q^3 - q^2$  such choices. The grand total is:  $(q^3 - 1)(q^3 - q)(q^3 - q^2)$ .

(c) This amounts to counting the number of different rational canonical forms for  $3 \times 3$  matrices  $T$  over  $\mathbf{F}_q$ . If the module is cyclic, it is completely determined by the characteristic polynomial of  $T$ : there are  $q^3$  such choices of different characteristic polynomials. If it has two cyclic summands, the monic annihilators  $f, g$  must have degrees one and two, respectively, and  $f$  must divide  $g$ , so that we must have  $f = x - a$  and  $g = (x - a)(x - b)$ . Both  $a$  and  $b$  are uniquely determined and determine the module, and the number of classes is therefore  $q^2$ . If there are three summands the

three monic annihilators all have the form  $x - a$ , and there are  $q$  possibilities. Hence, the total number of isomorphism classes is  $q^3 + q^2 + q$ .

5. Consider the polynomial  $F(x) = (x^2 - 2)(x^2 - 3)$  over  $\mathbf{Q}$ , and let  $E$  be its splitting field.

(a) Compute the degree of  $E/\mathbf{Q}$  and find an element  $\alpha \in E$  such that  $E = \mathbf{Q}(\alpha)$ .

(b) Describe the Galois group  $G$  of  $E/\mathbf{Q}$ , giving explicit generators and relations.

(c) Describe the lattice of subgroups of  $G$ , giving explicit generators and relations for each.

(d) Describe the lattice of intermediate fields  $K$  between  $\mathbf{Q}$  and  $E$ , and explain the relation with part (c). Which of these field extensions are Galois?

Solution:

(a) The degree is four: adjoining  $\sqrt{2}$  yields a degree 2 extension  $E_0$ , and further adjoining  $\sqrt{3}$  gives an extension that evidently has degree 1 or 2 over  $E_0$ , depending on whether or not  $\sqrt{3} \in E_0$ . But if  $\sqrt{3} = a + b\sqrt{2}$  with  $a$  and  $b$  rational, the automorphism of  $E_0$  that sends  $\sqrt{2} \mapsto -\sqrt{2}$  must also produce a square root of 3, so that  $a - b\sqrt{2}$  is also a square root of 3. It cannot be the same one, since we must have  $b \neq 0$ , but this would mean that  $a + b\sqrt{2} = -(a - b\sqrt{2})$ , which implies that  $a = 0$ , i.e.,  $\sqrt{3} = b\sqrt{2}$  and so  $b^2 = 3/2$ , which is clearly impossible (write  $b$  in lowest terms). Thus, the second field extension is also degree 2, and the degree is four. One may choose  $\alpha = \sqrt{3} + \sqrt{2}$ . Then  $1/\alpha = \sqrt{3} - \sqrt{2}$ . Hence, adjoining  $\alpha$  gives a field extension that contains  $\sqrt{3} = (\alpha + 1/\alpha)/2$  and  $\sqrt{2} = (\alpha - 1/\alpha)/2$ .

(b) Since  $[E : \mathbf{Q}] = 4$ ,  $|G| = 4$ . Since  $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$  generate  $E$  and evidently are closed under the action of  $G$ ,  $G$  may be viewed as a group of permutations of these four elements. Since we may think of  $E$  as the degree 2 extension of  $\mathbf{Q}[\sqrt{2}]$  obtained by adjoining  $\sqrt{3}$ ,  $E$  has an automorphism  $g$  that fixes  $\sqrt{2}, -\sqrt{2}$  and interchanges  $\sqrt{3}$  and  $-\sqrt{3}$ . Similarly, it has an automorphism  $h$  that fixes  $\sqrt{3}, -\sqrt{3}$  and interchanges  $\sqrt{2}, -\sqrt{2}$ . Since these two permutations generate a group of order four isomorphic with  $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ , we must have that  $G$  is this group. Generating relations on  $g, h$  are  $g^2 = e = h^2$  and  $gh = hg$ .

(c)  $G$  has three proper nontrivial subgroups, all of order two, each generated by one of the three elements of order 2,  $g, h$ , and  $gh$ .

(d) Since  $G$  is abelian, these are normal subgroups and all the three strictly intermediate fields are Galois quadratic extensions. Since these fields have characteristic 0, separability is not an issue, only normality. The fixed field of  $g$  is  $\mathbf{Q}[\sqrt{2}]$ , the fixed field of  $h$  is  $\mathbf{Q}[\sqrt{3}]$ , and the fixed field of  $gh$  is  $\mathbf{Q}[\sqrt{2}\sqrt{3}] = \mathbf{Q}[\sqrt{6}]$ .

1. Let  $G$  be a group.

(a) Characterize what it means for  $G$  to be solvable, and what it means for  $G$  to be nilpotent.

(b) Given an example of a finite group that is solvable but not nilpotent.

(c) For each group given below, if  $G$  is the Galois group of the splitting field of a polynomial  $f$  over the rational numbers, can  $f$  be solved by radicals? Explain your answer.

1.  $G = S_4 \times S_4 \times S_4$

2.  $G = S_5$

3.  $G$  is the group of symmetries of a regular  $n$ -sided polygon,  $n \geq 3$ .

Solution:

(a)  $G$  is solvable (respectively, nilpotent) precisely if it has a finite ascending sequence of normal subgroups  $e = G_0 \subseteq \cdots \subseteq G_i \subseteq \cdots \subseteq G_n = G$  such that each quotient  $G_{i+1}/G_i$  is abelian (respectively, each  $G_{i+1}/G_i$  is the center of  $G/G_i$ ).

(b)  $S_3$  is solvable, since it has a normal cyclic subgroup  $A_3$  of order 3 such that the quotient is cyclic of order 2, but is not nilpotent, since its center is trivial.

(c) The equation can be solved by radicals if and only if its Galois group is solvable.  $S_n$  (and  $A_n$ , the alternating group) are solvable if and only if  $n \leq 4$ , and an extension of a solvable group by a solvable group is solvable. Hence,  $S_4 \times S_4 \times S_4$  is solvable and  $S_5$  is not. The group of symmetries of a regular  $n$ -sided polygon has a cyclic subgroup of order  $n$  generated by rotation through an angle of  $2\pi/n$ : the quotient by this subgroup is  $\mathbf{Z}_2$  (the elements not in the rotation subgroup correspond to reflections around various axes of symmetry). So the third group is solvable.

2. Let  $K$  be a field of 27 elements. Find the number of solutions of the equation  $x^{13} = 1$  in  $K$ , and the number of solutions of the equation  $x^{13} = -1$  in  $K$ .

First solution.  $K$  is the splitting field of  $x^{27} - x = 0$  or of  $x^{26} - 1 = 0$ . This second equation has 26 distinct solutions (all nonzero elements of  $K$ ), and factors as  $(x^{13} - 1)(x^{13} + 1) = 0$ . Hence, each factor must have exactly 13 roots in  $K$ .

Second solution. The multiplicative group of nonzero elements of  $K$  is abelian of order 26, and so must be the direct sum of a cyclic group  $C$  of order 13 and a cyclic group of order 2. The unique

element of order 2 in the group is  $-1$ . It follows that there are exactly 13 elements of order dividing 13, the elements of the cyclic group of order 13, while the thirteenth power of any element not in that cyclic group is  $(c(-1))^{13}$  where  $c \in C$ , and this is  $c^{13}(-1)^{13} = -1$ . Hence, each equation has 13 solutions.

**3.** Let  $G$  be a finite group of order  $p^e m$ , where  $p$ ,  $e$  and  $m$  are positive integers, with  $p$  prime and not a divisor of  $m$ . Suppose that the Sylow  $p$ -subgroups of  $G$  are not normal. Show that there is a homomorphism  $\theta$  of  $G$  to the symmetric group  $S_h$  on  $h$  elements, where  $h > 1$  is a divisor of  $m$  that is congruent to 1 modulo  $p$ , such that  $\text{Ker}(\theta)$  is the intersection of the normalizers of the Sylow  $p$ -subgroups and for any choice of  $a, b$  in the set of  $h$  elements, there is an element  $g \in G$  such that  $\theta(g)$  maps  $a$  to  $b$ .

Solution: Let  $h$  be the number of Sylow  $p$ -subgroups of  $G$ . By the Sylow theorems,  $h$  divides  $m$ ,  $h \equiv 1 \pmod{p}$ , and  $G$  acts transitively on these  $h$  elements by conjugation, which gives a homomorphism  $\theta$  from  $G \rightarrow S_h$  satisfying the last condition. An element  $g \in G$  fixes a given Sylow  $p$ -subgroup if and only if it is in the normalizer of that subgroup, from which it follows that an element acts trivially on all of the Sylow  $p$ -subgroups iff it is in the intersection of their normalizers, and this is the kernel of  $\theta$ .

**4.** Let  $M$  be a finitely generated module over the principal ideal domain  $D$ . Suppose that  $d \in D - \{0\}$  is such that  $dM = 0$ . Prove that the  $D$ -module  $\text{Hom}_D(M, D/dD)$  of  $D$ -linear maps from  $M$  to  $D/dD$  is isomorphic to  $M$  as a  $D$ -module.

Solution:

$M$  is isomorphic to a finite direct sum of cyclic modules, each of which is annihilated by  $d$ , and so has the form  $D/cD$  where  $c|d$ , say  $d = bc$ . Since  $\text{Hom}_D(\ , D/dD)$  commutes with direct sum, it suffices to prove the result when  $M = D/cD$  is cyclic of this form. To give an element of  $\text{Hom}_D(D/cD, D/bcD)$  is the same as to specify where the coset of 1 maps, and it must map to an element annihilated by  $c$ . Thus,  $\text{Hom}_D(D/cD, D/bcD)$  is isomorphic with the set of elements of  $D/bcD$  annihilated by  $c$ , and this may be identified with  $bD/bcD$ . There is an isomorphism  $D/cD \cong bD/bcD$  that sends the coset of  $u$  to the coset of  $bu$ , which proves the result in this case, as required.

**5.** Let  $V$  be an  $n$ -dimensional vector space over a field  $K$ , and let  $T : V \rightarrow V$  be  $K$ -linear.

(a) Suppose that the matrix of  $T$  with respect to the basis  $v_1, \dots, v_n$  for  $V$  is upper triangular. For  $i \leq 1 \leq n$ , describe an ordered basis for  $\bigwedge^i V$  in terms of  $v_1, \dots, v_n$  such that the matrix of  $\bigwedge^i T : \bigwedge^i V \rightarrow \bigwedge^i V$  with respect to this ordered basis is upper triangular.

(b) Describe the diagonal entries of the matrix for  $\bigwedge^i T$  in terms of the diagonal entries of the matrix for  $T$ .

(c) Let  $c_i$  denote the trace of the matrix  $\bigwedge^i T : \bigwedge^i V \rightarrow \bigwedge^i V$ ,  $1 \leq i \leq n$ . Describe the relation of the coefficients of the characteristic polynomial  $\det(xI - T)$  to the  $c_i$ .

Solution:

(a) One may take the basis to consist of all elements  $v_{t_1} \wedge \cdots \wedge v_{t_i}$  such that  $t_1 < \cdots < t_i$ . These can be totally ordered so that (\*) if  $s_j \leq t_j$  for  $1 \leq j \leq i$ , and the  $s_j$  are mutually distinct, then  $\pm v_{s_1} \wedge \cdots \wedge v_{s_i} \leq v_{t_1} \wedge \cdots \wedge v_{t_i}$ . (The sign may need to be adjusted when the  $s_i$  are rearranged to be increasing.) For example, one can require that  $v_{s_1} \wedge \cdots \wedge v_{s_i} < v_{t_1} \wedge \cdots \wedge v_{t_i}$  whenever  $s_1 + \cdots + s_i < t_1 + \cdots + t_i$ : it does not matter how one orders those terms for which the sum of the subscripts is a given fixed integer. (There are many other possibilities that work.) Under condition (\*), when one applies  $T$  to  $w = v_{t_1} \wedge \cdots \wedge v_{t_i}$ , each  $v_{t_j}$  is replaced by a  $K$ -linear combination of the  $v_s$  for  $s \leq t_j$ . When one expands by the generalized distributive law, all the terms that survive are either scalar multiples of  $w$  or of terms that are scalar multiples of some  $v_{s_1} \wedge \cdots \wedge v_{s_i}$  satisfying the hypothesis of (\*), and so precede  $w$  in the ordering.

(b) Let  $\lambda_1, \dots, \lambda_n$  be the diagonal entries of the matrix of  $T$ . Then  $w = v_{t_1} \wedge \cdots \wedge v_{t_i}$  maps to  $(\lambda_{t_1} v_{t_1} + L_{t_1}) \wedge \cdots \wedge (\lambda_{t_i} v_{t_i} + L_{t_i})$ , where  $L_{t_j}$  involves only vectors that preceded  $v_{t_j}$  in the basis. The expansion contains  $(\lambda_{t_1} \cdots \lambda_{t_i})w + L$  where  $L$  involves only elements of the basis that precede  $w$ . It follows that the diagonal entry corresponding to  $w$  is  $\lambda_{t_1} \cdots \lambda_{t_i}$ . Thus, the diagonal entries are the products of the original diagonal entries taken  $i$  at a time.

(c) It follows that  $c_i$  is the  $i$ th elementary symmetric function of the eigenvalues of  $T$ , which means that  $(-1)^i c_i$  is the coefficient of  $x^{n-i}$  in the characteristic polynomial.