

UNIVERSITY OF MICHIGAN  
DEPARTMENT OF MATHEMATICS  
Solutions to September 2009 Algebra QR Exams  
MORNING

1. Let  $K$  be a finite normal separable extension of a field  $F$ , with Galois group  $G$ . For each case below, find the number of distinct intermediate fields  $E$  such that  $F \subset E \subset K$ , with  $E \neq K$  and  $E \neq F$

- Case 1:  $G$  is cyclic of order  $d$  with  $d > 1$ .
- Case 2:  $G$  has order 8 and  $g^2 = \text{id}$  for every element of  $G$ .
- Case 3:  $G \cong D_7$ , the symmetry group of a regular 7-gon.

*Solution:* Case 1: If  $G = \langle g \rangle$  then the subgroups of  $G$  are of the form  $\langle g^e \rangle$  where  $e$  is a positive divisor of  $d$ . Let  $m$  be the number of divisors of  $d$ . Then  $G$  has  $m$  distinct subgroups, and  $m - 2$  distinct subgroups that are not equal to  $\{\text{id}\}$  or  $G$ . By the Galois correspondence there are  $m - 2$  proper intermediate fields. Case 2: If  $g^2 = \text{id}$  for all  $g \in G$ , then  $G$  is abelian. So  $G$  is isomorphic to  $(\mathbb{Z}/2\mathbb{Z})^3 = \mathbb{F}_2^3$ , where  $\mathbb{F}_2$  is the field with 2 elements. A subgroup of  $\mathbb{F}_2^3$  is a subspace (as a vector space over  $\mathbb{F}_2$ ). A one dimensional vector space is spanned by a uniquely determined nonzero vector, so there are  $2^3 - 1 = 7$  1-dimensional subspaces. By duality, there are also 7 2-dimensional subspaces. The 0-dimensional and the 3-dimensional subspace correspond to the fields  $F$  and  $K$  respectively. So there are  $7 + 7 = 14$  intermediate fields. Case 3: The group  $D_7$  has order  $2 \cdot 7 = 14$ . A proper subgroup has order 2 or 7. There is a unique subgroup of order 7, and there are 7 subgroups of order 2 (corresponding to the 7 symmetry lines of the heptagon). So there are  $1 + 7 = 8$  intermediate fields.

2. How many elements of order seven are there in a simple group of order 168?

*Solution:* First  $168 = 2^3 \cdot 3 \cdot 7$ , so the number of Sylow 7-subgroups is divisor of 24 and also congruent to 1 mod 7. So there can be either one or eight such groups. However, if there is only one, then it is normal, contrary to the assumption that the group is simple. The eight sylow 7-groups can share only the identity element, so that there are exactly  $8 \cdot 6$ , or 48, elements of order 7.

3. Find the Jordan canonical form of a  $7 \times 7$  matrix  $A$  whose characteristic polynomial is  $(x - 2)^4(x - 5)^3$ , whose minimal polynomial is  $(x - 2)^2(x - 5)^2$ , and such that the dimension of the kernel of the matrix  $2I - A$  is three (here  $I$  is the  $7 \times 7$  identify matrix).

*Solution:* The eigenvalue 2 has multiplicity 4 and the eigenvalue 5 has multiplicity 3. From the minimum polynomial we see that there is a Jordan block of size 2 with eigenvalue 2 and a block of size 2 with eigenvalue 5. There can only be one other Jordan block with eigenvalue 5, and this block must have size 1. For eigenvalue 2, here are either 2 blocks of size 2, or one block of size 2 and two blocks of size 1. Since the dimension of the kernel of  $2I - A$  is three, there are 3 blocks for eigenvalue 2, so the blocks are of size 2,1,1. The Jordan normal

form is

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 5 \end{pmatrix}.$$

4. Count the number of prime ideals in the ring

$$\frac{\mathbf{Z}[x, y]}{(6, (x - 2)^2, y^6)},$$

giving an explicit set of generators for each. Which of these contain the class of  $x$ ?

*Solution.* Prime ideals in  $R := \mathbf{Z}[x, y]/(6, (x - 2)^2, y^6)$  correspond to prime ideals in  $\mathbf{Z}[x, y]$  containing  $(6, (x - 2)^2, y^6)$ . Let  $I$  be a prime ideal containing  $6, (x - 2)^2, y^6$ . From the prime property follows that  $x - 2, y \in I$ . Since  $6 \in I$  we have  $2 \in I$  or  $3 \in I$ . So we have  $(2, x - 2, y) \subseteq I$  or  $(3, x - 2, y) \subseteq I$ . We have  $\mathbf{Z}[x, y]/(2, x - 2, y) \cong \mathbb{F}_2$  and  $\mathbf{Z}[x, y]/(3, x - 2, y) \cong \mathbb{F}_3$  where  $\mathbb{F}_p$  is the field with  $p$  elements. So  $(2, x - 2, y)$  and  $(3, x - 2, y)$  are maximal ideals. So, either  $I = R$ ,  $I = (2, x - 2, y) = (2, x, y)$  or  $I = (3, x - 2, y)$ . The ideals  $R$  and  $(2, x, y)$  contain  $x$ . The ideal  $(3, x - 2, y)$  does not contain  $x$ , because otherwise it would contain  $3 - x + (x - 2) = 1$ .

5. Let  $E, F$  and  $G$  be finite dimensional real vector spaces, and suppose that  $B : E \times F \rightarrow G$  is a bilinear form.

a) Is the image of  $B$  necessarily a vector space? Prove or give a counterexample.

b) For  $v \in F$ , define  $\phi_v : E \rightarrow G$  by  $\phi_v(w) = B(w, v)$ . Does there exist a bilinear form  $B$  and nonzero vectors  $v, w \in F$  such that  $\phi_v$  and  $\phi_w$  do not have the same rank? Prove or disprove.

*Solution:*

(a) No, take for  $E = \text{Mat}_{2,1}$ ,  $F = \text{Mat}_{1,2}$  and  $G = \text{Mat}_{2,2}$  where  $\text{Mat}_{p,q}$  is the space of  $p \times q$  matrices, and let  $B : E \times F \rightarrow G$  defined by  $B(w, v) = wv$ . The image contains all rank 1 matrices, but no rank 2 matrices. However, a rank 2 matrix is the sum of two rank 1 matrices, so the image cannot be a subspace.

(b) Yes, Take  $E = F = G = \text{Mat}_{2,2}$  and let  $B$  be matrix multiplication. Then  $\phi_v$  is onto if and only if  $v \in F$  is an invertible matrix.

AFTERNOON

1. Let  $G$  be a finite abelian group that contains 8 elements of order three, 18 elements of order nine, and no other elements besides the identity. Describe all possibilities for  $G$ , by giving explicit decompositions into cyclic groups, up to isomorphism.

*Solution:* The order of  $G$  is  $1 + 8 + 18 = 27$ , so  $G$  is an abelian 3-group. The only possibilities are  $\mathbb{Z}/27\mathbb{Z}$ ,  $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  or  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ . Since  $G$  has elements of order nine, but no elements of order 27, it has to be equal isomorphic to  $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ .

2. The characteristic polynomial and the minimum polynomial of a linear transformation  $T : V \rightarrow V$  of complex vector spaces are both equal to  $(x - 1)^2(x - b)^2$ , where  $b$  is a complex number.

a) Find the characteristic polynomial of the induced map  $\wedge^2 T : \wedge^2 V \rightarrow \wedge^2 V$ .

b) Describe the rank of  $\wedge^2 T$  as a function of  $b$ .

*Solution:* Choose a basis  $(e_1, e_2, e_3, e_4)$  of  $V$  such that  $T$  has the (lower triangular) Jordan normal form. Then  $(e_1 \wedge e_2, e_1 \wedge e_3, e_1 \wedge e_4, e_2 \wedge e_3, e_2 \wedge e_4, e_3 \wedge e_4)$  is a basis of  $\wedge^2 V$  and the matrix of  $\wedge^2 T$  with respect to this basis is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & b & 0 & 0 & 0 & 0 \\ 0 & 1 & b & 0 & 0 & 0 \\ 0 & 1 & 0 & b & 0 & 0 \\ 0 & 1 & 1 & 1 & b & 0 \\ 0 & 0 & 0 & 0 & 0 & b^2 \end{pmatrix}$$

if  $b \neq 1$  and

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

if  $b = 0$ . So the characteristic polynomial is  $(x - 1)(x - b)^4(x - b^2)$ .

(b) if  $b \neq 0$  then the rank is 6. If  $b = 0$ , then the rank is 3.

3.

a) Show that the polynomial  $x^6 + 3$  is irreducible over  $\mathbb{Q}$ .

b) Suppose that  $\alpha$  is a root of  $x^6 + 3$ . Show that  $\beta := (\alpha^3 + 1)/2$  is a primitive 6th root of unity.

c) Show that  $\mathbb{Q}(\alpha)/\mathbb{Q}$  is a Galois extension.

d) Determine the Galois group of this extension.

*Solution:* (a) Use the Eisenstein criterion for the prime  $p = 3$ . (b)

$$\beta^3 = \frac{1}{8}(1 + 3\alpha^3 + 3\alpha^6 + \alpha^9) = \frac{1}{8}(1 + 3\alpha^3 - 3 \cdot 3 - 3\alpha^3) = -1.$$

So  $\beta^6 = 1$  and  $\beta$  is a 6th root of unity.  $\beta^3 = -1 \neq 1$ , and  $\beta \neq 1, -1$ , so  $\beta$  is not a third or a second root of unity. (c) The roots of  $x^6 + 3$  are  $\beta^i \alpha$ ,  $0 \leq i \leq 5$ . The field contains all these roots, so  $\mathbb{Q}(\alpha)/\mathbb{Q}$  is a normal, separable extension, so it is Galois. (d) The Galois group has 6 elements, so it must be  $\mathbb{Z}/6\mathbb{Z}$  or  $S_3$ . There exists a unique automorphism  $\sigma$  of  $\mathbb{Q}(\alpha)$  with

$\sigma(\alpha) = \beta\alpha$ . We have  $\sigma(\beta) = (1 - \alpha^3)/8 = \beta^{-1}$ . One easily verifies  $\sigma(\beta^i\alpha) = \beta^{1-i}\alpha$ . There also exists an automorphism  $\tau$  with  $\tau(\alpha) = \beta^2\alpha$ . One has  $\tau(\beta) = \beta$  and  $\tau(\beta^i\alpha) = \beta^{i+2}\alpha^i$ . Now  $\tau$  and  $\sigma$  do not commute:  $\tau\sigma(\alpha) = \beta^3\alpha$  and  $\sigma\tau(\alpha) = \beta^{-1}\alpha$ . So the Galois group is  $S_3$ .

4. Let  $R$  be a UFD, and let  $f$  be any non-zero, non-unit irreducible element of  $R$ . Is  $R/(f)$  also a UFD? Prove or give a counterexample. What happens if  $R$  happens to also be a PID?

*Solution:* No. Let  $R$  be a polynomial ring over a field in three variables,  $x, y$ , and  $z$ . Then  $f = z^2 - xy$  is irreducible (using, for instance, Eisenstein with the prime ideal  $(x)$ ). But  $R/(f)$  is not a UFD since the class of  $z^2$  factors as also  $xy$ . In the case where  $R$  is a PID, any irreducible element generates a maximal ideal, so  $R/(f)$  is actually a field.

5. Let  $p$  be a prime.

a) Suppose that  $G$  is a finite group and  $H$  is a normal subgroup. Let

$$Z_G(H) = \{g \in G \mid \forall h \in H \ gh = hg\}$$

be the centralizer of  $H$  in  $G$ . Show that  $Z_G(H)$  is a normal subgroup of  $G$  and that  $G/Z_G(H)$  is isomorphic to a subgroup of  $\text{Aut}(H)$ , the group of automorphisms of  $H$ .

b) Show that every group of order  $p^4$  has an abelian normal subgroup of order  $p^2$ .

c) Show that every group of order  $p^4$  has an abelian normal subgroup of order  $p^3$ .

*Solution:*

(a) There is a natural homomorphism  $\varphi : G \rightarrow \text{Aut}(H)$  defined by  $\varphi(g) = \psi_g$ , where  $\psi_g : H \rightarrow H$  is conjugation by  $g$ . The kernel of  $\varphi$  is exactly  $Z_G(H)$ , so  $G/Z_G(H)$  is isomorphic to the image of  $\varphi$ .

(b) Let  $G$  be a group of order  $p^4$ . Since  $G$  is a  $p$ -group it is nilpotent and the center  $Z(G)$  is nontrivial. If  $Z(G)$  has  $\geq p^2$  elements then we can take any subgroup of  $Z(G)$  with  $p^2$  elements. Otherwise  $Z(G)$  is cyclic of order  $p$ . Choose a subgroup  $\text{Aut}(H)$  of  $G$  containing  $Z(G)$  such that  $H/Z(G)$  is a normal subgroup of  $G/Z(G)$  of order  $p$ . Then  $H$  is abelian and normal of order  $p^2$ .

(c) Let  $H$  be an abelian normal subgroup of order  $p^2$ . We have that  $G/Z_G(H)$  is isomorphic to a subgroup of  $H$ . The automorphism group of  $H$  has  $p(p^2 - 1)(p - 1)$  (if  $H \cong (\mathbb{Z}/p\mathbb{Z})^2$ ) or  $p(p - 1)$  elements (if  $H \cong \mathbb{Z}/p^2\mathbb{Z}$ ). It follows that  $G/Z_G(H)$  has at most  $p$  elements because it is a  $p$ -group. In particular  $Z_G(H) \neq H$ . Choose a subgroup  $H'$  of  $Z_G(H)$  containing  $H$  such that  $H'/H$  is a normal subgroup of  $G/H$  of order  $p$ . Then  $H'$  is abelian normal subgroup of  $G$  of order  $p^3$ .