

UNIVERSITY OF MICHIGAN
DEPARTMENT OF MATHEMATICS
Solutions to May 2008 Algebra QR Exams
MORNING

Problem 1. For each point x in X , the subgroup fixing x has index 1 when x is fixed, and otherwise a positive power of p , and this index is the number of points in the orbit of x . Writing X as a disjoint union of the orbits, a) follows. For b), apply a) to the action of G on itself by conjugation.

Problem 2. Given $a \in E$, consider the map α_a . This is k -linear, and it is injective since E is a domain. Since E has finite-dimension as a k -vector space, it follows that α_a is, in fact, bijective. In particular, we can find an element a^{-1} such that $aa^{-1} = 1 = a^{-1}a$ (by commutativity). Hence E is a field.

For ii), since α_a is invertible, it follows that $\det(\alpha_a) \neq 0$. As the determinant of a k -linear map, it lies in k , hence $N(a) \in k^*$. Since we have $\alpha_a \circ \alpha_b = \alpha_{ab}$, we see by taking determinants that $N(ab) = N(a) \cdot N(b)$, that is, N is multiplicative.

Suppose now that a is purely inseparable over k , and let $f = T^{p^e} - r$ be its minimal polynomial. Note that f is also the minimal polynomial of α_a . We have $[k(a) : k] = p^e$, and let $m = [E : k]/p^e = [E : k(a)]$. Since α_a is $k(a)$ -linear, we see that $E \simeq k(a)^{\oplus m}$, such that α_a is identified with $(\alpha_a|_{k(a)}, \dots, \alpha_a|_{k(a)})$. On the other hand, the minimal polynomial of $\alpha_a|_{k(a)}$ has degree equal to $\dim_k k(a) = p^e$. This implies that if λ is a p^e -root of r in the algebraic closure of k , then the Jordan matrix of α_a consists of m Jordan blocks of size p^e , having λ on the diagonal.

Problem 3. Define first $\psi: V^p \times V \rightarrow \wedge^{p+1}V$ by $\psi_p(u_1 \dots u_p, v) = u_1 \wedge \dots \wedge u_p \wedge v$. Since ψ is multilinear and alternating in the first p variables, it induces a map $\wedge^p V \times V \rightarrow \wedge^{p+1}V$. This in turn is bilinear, hence it induces $\phi: \wedge^p V \otimes V \rightarrow \wedge^{p+1}V$, such that $\phi((u_1 \wedge \dots \wedge u_p) \otimes v) = u_1 \wedge \dots \wedge u_p \wedge v$.

This is clearly surjective, since every element in $\wedge^{p+1}V$ can be written as a sum of elements of the form $u_1 \wedge \dots \wedge u_{p+1}$, with $u_i \in V$. In particular, since $\wedge^{p+1}V \neq 0$ (recall that $p \leq n-1$), we see that ϕ is nonzero. On the other hand, the map is never injective: simply take linearly independent elements $e_1, \dots, e_p \in V$, and note that $(e_1 \wedge \dots \wedge e_p) \otimes e_1 \neq 0$, but its image by ϕ is zero.

If $\phi(u \otimes v) = 0$ for every $v \in V$, choose a basis e_1, \dots, e_n for V . We may assume $p \leq n$, and write $u = \sum_I a_I e_I$, where the sum is over the subsets $I \subseteq \{1, \dots, n\}$ with p elements, and if $i_1 < \dots < i_p$, then $e_I := e_{i_1} \wedge \dots \wedge e_{i_p}$. Note that the e_I form a basis of $\wedge^p V$. Since $\phi(u \otimes e_j) = 0$, we deduce that $a_I = 0$ whenever j is not in I (note that $e_I \wedge e_j = 0$ if $j \in I$, and $\{e_I \wedge e_j \mid j \notin I\}$ are linearly independent in $\wedge^{p+1}V$). Since this happens for every j , and since $p \leq n-1$, it follows that $a_I = 0$ for every I .

Problem 4. For a), L is the result of twice adjoining a p^{th} root of an indeterminate, and, for an indeterminate z , the polynomial $X^p - z$ is irreducible, say by Eisenstein. For any polynomial $f \in F[x, y]$, f^p is in $F[x^p, y^p]$. Therefore, for any u in L , u^p is in K , so u satisfies a polynomial equation of degree p , and $[K(u) : K]$ cannot be p^2 . Consider the fields $K(x + ay)$, as a varies over the (infinite) field K , each an extension of degree p of K . If two coincided, say $M = K(x + ay) = K(x + by)$ for $a \neq b$, the difference $(a - b)y$ is in M , so y is in M , and so therefore is $x = x + ay - ay$, so $M = L$, a contradiction.

Problem 5. Let α denote the unique real root of f . If $\beta \in \mathbb{C}$ is another root of f , then its conjugate $\bar{\beta}$ is the third root (this is a root since f has rational, hence real, coefficients; it is distinct from α , which is real, and from β , since otherwise $\beta \in \mathbb{R}$).

Let $\mathbb{Q}(\alpha) \subseteq K$ be the subfield of K generated by α . Since $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, and $\beta \notin \mathbb{R}$, it follows that $\mathbb{Q}(\alpha) \neq K$. We know that f is irreducible, and $\deg(f) = 3$, hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. On the other hand, since $\beta \notin \mathbb{Q}(\alpha)$, we see that β is the root of the irreducible polynomial $f/(x - \alpha)$ in $\mathbb{Q}(\alpha)[x]$. Hence $K = \mathbb{Q}(\alpha, \beta)$ is a degree two extension of $\mathbb{Q}(\alpha)$, and we conclude that $[K : \mathbb{Q}] = 6$.

The extension K/\mathbb{Q} is clearly normal, and separable (since we are in characteristic zero), hence $G = G(K/\mathbb{Q})$ has order six. Therefore we either have $G \simeq \mathbb{Z}/6\mathbb{Z}$, or $G \simeq S_3$. In order to show that $G \simeq S_3$, it is enough to show that G has at least two subgroups of order two (which rules out $G \simeq \mathbb{Z}/6\mathbb{Z}$).

We have already found one such subgroup, namely $G(K/\mathbb{Q}(\alpha))$. On the other hand, since β is a root of f , we also have $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$. Since $\beta \notin \mathbb{Q}(\alpha)$, the two subextensions $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are distinct, which proves our assertion.

AFTERNOON

Problem 1. Note that $A = \mathbb{C}[x]/((x - \sqrt{2})^3) \oplus \mathbb{C}[x]/((x + \sqrt{2})^3)$. Since $x^3 - 2\sqrt{2} = (x - \sqrt{2})(x^2 + \sqrt{2}x + 2)$, it follows that $(x^3 - 2\sqrt{2})^3 = 0$ in the first factor, but $(x^3 - 2\sqrt{2})^2 \neq 0$. Similarly for powers of $x^3 + 2\sqrt{2}$ in the second factor. The minimal polynomial is therefore $(X - 2\sqrt{2})^3(X + 2\sqrt{2})^3 = (X^2 - 8)^3$. The Jordan canonical form has two 3 by 3 blocks, one with $2\sqrt{2}$'s down the diagonal, the other with $-2\sqrt{2}$'s down the diagonal, both with 1's just above (or below) the diagonal, 0's elsewhere.

Problem 2. Consider the group homomorphism $f: G \rightarrow \text{Aut}(G)$, where $f(x)$ is conjugation by x , that is $y \rightarrow xyx^{-1}$. The kernel of f is the center $Z(G)$ of G . Therefore $G/Z(G)$ is a subgroup of a cyclic group, hence it is cyclic itself. This implies that there is $u \in G$ such that every element in G can be written as gu^m for some $g \in Z(G)$ and $m \in \mathbb{Z}$. Given $x = gu^m$ and $y = hu^n$, with $g, h \in Z(G)$, we have

$$xy = gu^m hu^n = gh u^{m+n} = u^{m+n} hg = yx.$$

Therefore G is commutative.

Problem 3. The characteristic polynomial of A has the form $X^3 - bX^2 + dX - a = \prod_{i=1}^3 (X - \lambda_i)$, from which it follows that $b = \sum_{i=1}^3 \lambda_i$, $c = \sum_{i=1}^3 \lambda_i^2$, $d = \sum_{i < j} \lambda_i \lambda_j$, so $c = b^2 - 2d$. The companion matrix

$$\begin{pmatrix} 0 & 0 & a \\ 1 & 0 & -d \\ 0 & 1 & b \end{pmatrix}$$

will produce any a, b, c , if the characteristic is not 2, with $d = (b^2 - c)/2$. If the characteristic is 2, a triple can be achieved exactly when $c = b^2$, for example by this matrix, with any d .

Problem 4. Since ζ is a primitive 12th root of 1, it is a 6th (but not square) root of -1 , so it satisfies the polynomial $(X^6 + 1)/(X^2 + 1) = X^4 - X^2 + 1$. The other roots of this polynomial are ζ^5, ζ^7 , and ζ^{11} , which shows that it cannot satisfy a polynomial of lower degree, and that the field extension it generates is Galois. The four automorphisms of this field take ζ to ζ^i , for $i = 1, 5, 7, 11$, which identifies the Galois group with $(\mathbb{Z}/12\mathbb{Z})^*$. Each element of this group has square the identity, so it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. The fixed fields of its nontrivial elements are $\mathbb{Q}(\zeta + \zeta^5) = \mathbb{Q}(i)$, $\mathbb{Q}(\zeta + \zeta^{11}) = \mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\zeta^2 + \zeta^4) = \mathbb{Q}(\sqrt{-3})$.

Problem 5. For i) consider the ring homomorphism $\phi: C([0, 1]) \rightarrow \mathbb{R}$ given by $\phi(f) = f(p)$. This is clearly surjective (every $a \in \mathbb{R}$ is the image of the constant function a), and its kernel is \mathfrak{m}_p . Since $C([0, 1])/\mathfrak{m}_p \simeq \mathbb{R}$ is a field, it follows that \mathfrak{m}_p is a maximal ideal.

For ii), it is enough to show that given any proper ideal I of $C([0, 1])$, there is $p \in [0, 1]$ such that $I \subseteq \mathfrak{m}_p$, that is, every function in I vanishes at p . For every $f \in I$, let $Z(f)$ denote the set $\{q \in [0, 1] \mid f(q) = 0\}$. We need to show that $\bigcap_{f \in I} Z(f) \neq \emptyset$.

Suppose that this is not the case: since $[0, 1]$ is a compact topological space, we deduce that there are $f_1, \dots, f_m \in I$ such that $Z(f_1) \cap \dots \cap Z(f_m) = \emptyset$. We claim that in this case $I = C([0, 1])$. Indeed, since the f_i have no common zero, we can define

$$h_i = \frac{f_i}{\sum_{i=1}^m f_i^2}.$$

Therefore $h_i \in C([0, 1])$ for every i , and since $\sum_i h_i f_i = 1 \in I$, this proves our claim. We get a contradiction, showing that in fact there is $p \in [0, 1]$ such that $I \subseteq \mathfrak{m}_p$.