

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

Problem 1. i). Let H be the subgroup of G consisting of transformations that fix one of the vertices v . Since G acts transitively on the set of vertices, $[G : H] = 8$. Since H maps isomorphically onto the group of permutations of the three vertices adjacent to v , $|H| = 6$. So $|G| = 8 \cdot 6 = 48$. (The transformations in G have matrices with one nonzero entry, ± 1 , in each row and column.)

ii) For $p = 3$, the subgroup of rotations in H form a subgroup of order 3. For $p = 2$, since G acts transitively on the three axes through the centers of the faces, the subgroup fixing one of these axes has order $|G|/3 = 2^4$.

Problem 2. Note that we have the following inclusions of subspaces

$$\text{Ker}(T) \subseteq \dots \subseteq \text{Ker}(T^n) \subseteq \text{Ker}(T^{n+1}) \subseteq \dots$$

$$\text{Im}(T) \supseteq \dots \supseteq \text{Im}(T^n) \supseteq \text{Im}(T^{n+1}) \supseteq \dots$$

Since V is a finite dimensional vector space, it follows that these two sequences stabilize, hence there is N such that $V_\infty = \text{Ker}(T^n)$ and $V^\infty = \text{Im}(T^n)$ for every $n \geq N$.

We first show that $V_\infty \cap V^\infty = (0)$. Indeed, suppose that $u \in V_\infty \cap V^\infty$. Since $u \in \text{Im}(T^N)$, we can write $u = T^N(w)$, for some $w \in V$. Since $u \in \text{Ker}(T^N)$, we have $T^{2N}(w) = T^N(u) = 0$, hence $w \in \text{Ker}(T^{2N}) = \text{Ker}(T^N)$. We deduce $u = 0$.

Now in order to conclude that $V = V^\infty \oplus V_\infty$ it is enough to show that $\dim(V) = \dim(V^\infty) + \dim(V_\infty)$. The assertion follows from the exact sequence

$$0 \rightarrow \text{Ker}(T^N) \rightarrow V \rightarrow \text{Im}(T^N) \rightarrow 0.$$

Problem 3. i) Take any inner product $\langle \cdot, \cdot \rangle$ on V (say by choosing a basis to identify V with \mathbf{R}^n). Then $(v, w) = \sum_{g \in G} \langle \rho(g)(v), \rho(g)(w) \rangle$ is an inner product with the required property.

ii) Let $G = \mathbf{Z}$, $V = \mathbf{R}^2$, with $\rho(n) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. The orbit of any vector $v = (a, b)$ with $b \neq 0$ is unbounded, so no such vector can be part of an orthonormal basis for V .

Problem 4. i) After changing bases, one may assume A is diagonal, with entries a_1, \dots, a_n , so $M = \bigoplus_{i=1}^n R/a_i R$, and $D = a_1 \cdot \dots \cdot a_n$, from which the result is clear. Or see ii).

ii) Yes. From Cramer's rule, for any $y = (y_1, \dots, y_n) \in R^n$, $Dy = A \cdot x$, for $x = (x_1, \dots, x_n)$, with x_i the determinant of the matrix obtained from A by replacing its

i^{th} column by y . (Cramer's rule is valid for any commutative ring, since it is a formal identity, so it suffices to prove it for a polynomial ring $\mathbf{Z}[a_{ij}]$, and such a ring is a subring of the field of complex numbers, for which Cramer's rule is standard.)

Problem 5. i) Let g and h be two irreducible factors of f in $F[x]$. Let L be a finite extension of F that is normal over E , and over which f factors into linear factors. Let $a, b \in L$ be roots of g and h , respectively. Since they are both roots of f , which is irreducible over E , it follows that there is a field isomorphism $\sigma: E(a) \rightarrow E(b)$ that is the identity on E , and such that $\sigma(a) = b$.

Since L is algebraic and normal over E , we deduce that σ admits an extension $\tilde{\sigma}: L \rightarrow L$. Since F is normal over E , and since $\tilde{\sigma}$ is the identity on E , it follows that $\tilde{\sigma}(F) = F$, hence $\tilde{\sigma}$ induces an isomorphism of $F(a)$ with $F(b)$ over E . Therefore

$$\deg(g) = [F(a): F] = \frac{[F(a): E]}{[F: E]} = \frac{[F(b): E]}{[F: E]} = \deg(h).$$

ii) If F is not normal over E , then there is an irreducible polynomial $f \in E[x]$ having a root in F , but such that not all roots of f are in F . Therefore f has an irreducible factor of degree 1 in $F[x]$, but not all its irreducible factors in $F[x]$ have degree 1.

AFTERNOON

Problem 1. i) Consider the action of G on its subgroups given by conjugation. The number of conjugates of H is the cardinality of the orbit of H , hence it is equal to $[G: N_G(H)]$, where $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$. Since H is clearly contained in $N_G(H)$, we get $[G: N_G(H)] \leq [G: H]$.

ii) Let $r = [G: H] > 1$. By i), if N is the number of conjugates of H , then $N \leq r$. Moreover, the conjugates of H have the identity in common, hence the union of these conjugates has at most $N \cdot |H| - (N - 1)$ elements. Since

$$N \cdot |H| - N + 1 \leq (|H| - 1)[G: H] + 1 = |G| - [G: H] + 1 < |G|,$$

it follows that the conjugates of H can not cover G .

iii) If $|G| = p^2$, then there is nothing to prove, since we can take the subgroup to be G . Hence we may assume $|G| < p^2$. Let n_p be the number of p -Sylow subgroups of G . By Sylow's theorems, we have $n_p \equiv 1 \pmod{p}$. Using i) we see that $n_p < p$, hence $n_p = 1$. Therefore there is only one p -Sylow subgroup of G , which has to be normal.

Problem 2. The coefficients of this polynomial are the elementary symmetric polynomials in x_1, \dots, x_n , so are invariant by G , so the polynomial is in $F[X]$. If P is the (irreducible) minimal polynomial of x , the G -conjugates of x must be roots of P since $P(g \cdot x) = g \cdot P(x) = 0$; hence $\prod_{i=1}^n (X - x_i)$ divides P , so $\prod (X - x_i) = P$ is irreducible.

Problem 3. One can make a field extension without changing the conclusion, so one can assume (say by the Jordan canonical form) that V has a basis for which L is represented by an upper triangular matrix A . Using the corresponding standard basis of exterior products, $\wedge^k(L)$ is also represented by an upper triangular matrix, whose diagonal entries are products of k of the diagonal entries of A . Its trace is therefore the k^{th} elementary polynomial in the diagonal entries of A , which is a_k .

Problem 4. Let $u = \sqrt{4 + \sqrt{7}}$, and let $w = u^2 = 4 + \sqrt{7}$. If $w' = 4 - \sqrt{7}$, then $w + w' = 8$ and $ww' = 9$, hence u is a root of f , where $f = x^4 - 8x^2 + 9 \in \mathbf{Q}[x]$. In order to show that f is the minimal polynomial of u , it is enough to show that f is irreducible over \mathbf{Q} . It follows from the above computation that the roots of f are $\pm\sqrt{4 + \sqrt{7}}$ and $\pm\sqrt{4 - \sqrt{7}}$. Since none of these is a rational number, in order to show that f is irreducible it is enough to show that it does not factor as a product $f = gh$, with both g and h of degree two. Hence it is enough to show that if u' is one of $-\sqrt{4 + \sqrt{7}}$, $\sqrt{4 - \sqrt{7}}$, $-\sqrt{4 - \sqrt{7}}$, then either $u + u' \notin \mathbf{Q}$, or $uu' \notin \mathbf{Q}$.

In the first case, it is clear that $uu' = -(4 + \sqrt{7}) \notin \mathbf{Q}$. In the other two cases we have $u + u' \notin \mathbf{Q}$, by computing $\sqrt{4 + \sqrt{7}} + \sqrt{4 - \sqrt{7}} = \sqrt{14}$ and $\sqrt{4 + \sqrt{7}} - \sqrt{4 - \sqrt{7}} = \sqrt{2}$. Hence f is irreducible. This computation also gives $u = \frac{\sqrt{2} + \sqrt{14}}{2}$.

It follows from the above description of the roots of f , and from the formula for u , that the splitting field of f is $K = \mathbf{Q}(\sqrt{2}, \sqrt{14}) = \mathbf{Q}(\sqrt{2}, \sqrt{7})$. It is clear that every

automorphism σ of K takes $\sqrt{2}$ to $\pm\sqrt{2}$, and $\sqrt{7}$ to $\pm\sqrt{7}$, and moreover, it is determined by these two values. Hence we get an injective group homomorphism $\phi: G(K/\mathbf{Q}) \rightarrow \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Since the extension K/\mathbf{Q} is Galois (it is normal, K being a splitting field over \mathbf{Q} , and it is separable, since we are in characteristic zero), $|G(K/\mathbf{Q})| = [K : \mathbf{Q}] \geq \deg(f) = 4$. Therefore ϕ is an isomorphism.

Problem 5. i) Suppose that we have another basis $(f_\lambda)_{\lambda \in \Gamma}$ of F , with respect to which $a = \sum_\lambda b_\lambda f_\lambda$. If we write $e_\lambda = \sum_{\mu \in \Gamma} c_{\lambda\mu} f_\mu$, then $a = \sum_{\lambda, \mu \in \Gamma} a_\lambda c_{\lambda\mu} f_\mu$, hence $b_\mu = \sum_\lambda c_{\lambda\mu} a_\lambda$. It follows that each b_μ lies in $\sum_\lambda a_\lambda R$, hence $\sum_{\lambda \in \Gamma} b_\lambda R \subseteq \sum_{\lambda \in \Gamma} a_\lambda R$. The reverse inclusion follows by symmetry.

A more conceptual way of showing i) is by showing that if we consider the R -linear map $\phi: R \rightarrow F$ that takes 1 to a , then $\sum_{\lambda \in \Gamma} a_\lambda R$ is the image of the induced map $\text{Hom}(\phi, R): \text{Hom}_R(F, R) \rightarrow \text{Hom}_R(R, R) \simeq R$.

ii) Suppose first that a appears in some basis (g_λ) of F . By i), we can use this basis to compute $\sum_{\lambda \in \Gamma} a_\lambda R$, and writing a in this basis we see that 1 lies in this ideal. Conversely, suppose that a is primitive. In order to show that a can be completed to a basis of F , it is enough to show that $F/R \cdot a$ is torsion-free, hence free (if $\{b_i\}_i$ with $b_i \in F$ are such that their classes in $F/R \cdot a$ give a basis of this quotient module, then a together with the b_i give a basis of F).

Suppose now that a' in F is such that $ca' \in R \cdot a$ for some nonzero $c \in R$. If we write $a' = \sum_{\lambda \in \Gamma} a'_\lambda e_\lambda$, and $ca' = ta$, for some $t \in R$, we see that $ca'_\lambda = ta_\lambda$. Since each $ta_\lambda \in cR$, it follows that

$$tR = \sum_{\lambda} ta_\lambda R \subseteq cR,$$

hence c divides t , and we deduce $a' \in R \cdot a$.