

UNIVERSITY OF MICHIGAN  
DEPARTMENT OF MATHEMATICS  
Solutions to September 2006 Algebra QR exams

MORNING

(#1). Let  $V$  be an  $n$ -dimensional vector space over the complex numbers  $\mathbf{C}$ .

(a). Define what is meant by a Hermitian form  $H$  on  $V$ .

Given a Hermitian form  $H$  on  $V$ , set  $g = \operatorname{Re}(H)$  and  $\omega = \operatorname{Im}(H)$ , so that

$$H(v, w) = g(v, w) + i \cdot \omega(v, w)$$

for all  $v, w \in V$ , where  $g$  and  $\omega$  are real-valued.

(b). Show that  $g$  is a symmetric  $\mathbf{R}$ -bilinear form, and that  $\omega$  is an alternating  $\mathbf{R}$ -bilinear form on  $V$ , where now  $V$  is considered as a vector space of dimension  $2n$  over  $\mathbf{R}$ . Prove moreover that

$$g(iv, iw) = g(v, w) \quad , \quad \omega(iv, iw) = \omega(v, w)$$

for all  $v, w \in V$ .

(c). Prove conversely that if  $g$  is a symmetric  $\mathbf{R}$ -bilinear form on  $V$  satisfying  $g(iv, iw) = g(v, w)$  for all  $v, w \in V$ , then there exists a Hermitian form  $H$  on  $V$  such that  $g = \operatorname{Re}(H)$ .

SOLUTION. (b). Evidently  $g$  and  $\omega$  are  $\mathbf{R}$ -bilinear, and it follows from the relation

$$H(w, v) = \overline{H(v, w)}$$

that  $g$  is symmetric and  $\omega$  is skew. Since

$$H(iv, iw) = \overline{H(v, w)}$$

we get the stated properties of  $g$  and  $\omega$ .

(c). Given  $g$ , set

$$H(v, w) = g(v, w) + ig(v, iw).$$

Then for instance

$$H(w, v) = g(w, v) + ig(w, iv) = g(v, w) - ig(iw, v) = \overline{H(v, w)},$$

and the other required properties are similar.

(#2). Suppose  $G$  is a finite group such that its automorphism group  $\text{Aut}(G)$  is solvable. Prove that  $G$  itself is solvable.

SOLUTION.  $G$  acts on itself by conjugation. This defines a group homomorphism  $\rho : G \rightarrow \text{Aut}(G)$ . The kernel of  $\rho$  is the center  $Z(G)$  of  $G$ , so it is abelian. Now  $G/Z(G)$  is a subgroup of  $\text{Aut}(G)$ , so  $G/Z(G)$  is solvable. But then  $G$  is solvable itself.

(#3). (a). Prove that there are no  $3 \times 3$  matrices  $A$  with entries in  $\mathbf{Q}$  such that

$$A^8 = I \quad \text{but} \quad A^4 \neq I.$$

(b). What happens if we look instead for  $3 \times 3$  matrices with entries in  $\mathbf{R}$  satisfying the same conditions?

SOLUTION. (a). Assuming that such an  $A$  exists, let  $p(x)$  be its minimal polynomial. Then  $p(x)$  is a polynomial of degree  $\leq 3$  satisfying  $p(x) \mid (x^8 - 1)$ , but  $p(x) \nmid (x^4 - 1)$ . Now over  $\mathbf{Q}$  we have the irreducible factorization

$$x^8 - 1 = (x^4 + 1)(x^2 + 1)(x + 1)(x - 1),$$

and we see that no such  $p(x)$  can exist.

(b). Over  $\mathbf{R}$ , we have the factorization

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1),$$

so we can take e.g.  $A$  to be the matrix describing multiplication by  $x$  on

$$\frac{\mathbf{R}[x]}{(x^2 + \sqrt{2}x + 1)(x - 1)}$$

(#4). (a). Suppose that  $K_1, K_2$  are subfields of a field  $L$  such that  $L/(K_1 \cap K_2)$  is a finite field extension. Suppose that  $L/K_1$  and  $L/K_2$  are Galois extensions. Prove that  $L/(K_1 \cap K_2)$  is a finite Galois extension.

(b). Let  $x$  be a transcendental element over  $\mathbf{Q}$ . Suppose that  $M$  is a subfield of  $\mathbf{Q}(x)$  containing  $\mathbf{Q}$ , but not equal to  $\mathbf{Q}$ . Prove that  $\mathbf{Q}(x)/M$  is a finite field extension.

(c). Prove that  $L/K_1 \cap K_2$  is not a finite field extension, where  $L = \mathbf{Q}(x)$ ,  $K_1 = \mathbf{Q}(x^2)$  and  $K_2 = \mathbf{Q}((x - 1)^2)$ . (Hence  $K_1 \cap K_2 = \mathbf{Q}$  by (b)).

SOLUTION. (a). Let  $H_1 = \text{Gal}(L/K_1)$  and  $H_2 = \text{Gal}(L/K_2)$ . Let  $H$  be the group generated by  $H_1$  and  $H_2$ . Clearly, an element of  $L$  is fixed by  $H$  if and only if it is fixed by  $H_1$  and  $H_2$ . Therefore,

$$L^H = L^{H_1} \cap L^{H_2} = K_1 \cap K_2.$$

Every element of  $H$  fixes all elements of  $K_1 \cap K_2$ . So we may view  $H$  as a subgroup of the group of automorphisms of  $L$  over  $K_1 \cap K_2$ . The order  $|H|$  is at most the degree of the

extension  $L/(K_1 \cap K_2)$ . Because  $H$  is finite,  $L/(K_1 \cap K_2) = L/L^H$  is a Galois extension with Galois group  $H$ .

(b). Suppose that  $a(x)/b(x) \in M$  where  $a(x)$  and  $b(x)$  are nonzero polynomials such that  $a(x)/b(x)$  is not a constant. Then  $x$  is a root of the polynomial

$$b(Y) - a(Y) \frac{a(x)}{b(x)} \in M[Y].$$

This shows that  $x$  is algebraic over  $M$ , so  $L/M$  is a finite field extension.

(c). We can define automorphisms  $\sigma$  and  $\tau$  of  $\mathbf{Q}(x)$  by  $\sigma(x) = -x$  and  $\tau(x) = -1 - x$ . Then  $\gamma = \sigma\tau$  is an automorphism of  $L$  such that  $\gamma(x) = x + 1$ . Then  $\gamma^r(x) = x + r$  for all positive integers  $r$ , so  $\gamma$  has infinite order. This shows that  $L/(K_1 \cap K_2)$  is an infinite field extension.

(#5). Suppose that  $G$  a group of order  $4n$  with  $n$  odd, containing an element of order 4.

(a). Prove that the elements of order 4 in  $G$  fall into in at most 2 conjugacy classes.

(b). Prove that the elements of order 4 cannot form a single conjugacy class.

SOLUTION. (a). Let  $H$  be the group generated by the element  $h$  of order 4. Then  $H$  is a 2-Sylow group. Suppose that  $g \in G$  has order 4. Then  $g$  is conjugate to an element of the 2-Sylow group  $H$ .  $SH$  has two elements of order 4, namely  $h$  and  $h^3$ . So  $g$  is conjugate to  $h$  or to  $h^3$  (and perhaps both). So there are at most 2 conjugacy classes of elements of order 4.

(b). We have to show that  $h$  and  $h^3$  are not conjugate. Suppose that  $ghg^{-1} = h^3$ . Let  $U$  be the group generated by  $g$  and  $h$ . Then  $H$  is normal in  $U$  and  $|U/H| = |U|/|H|$  is odd (because  $H$  is a 2-Sylow subgroup of  $G$  and also of  $U$ ). The order of  $gH$  in  $U/H$  is odd, so  $g^r \in H$  for some odd integer  $r$ . Now  $g^2$  and  $g^r$  commute with  $h$ , hence  $g$  commutes with  $h$ . Contradiction.

## AFTERNOON

(#1). Let  $R$  be a commutative ring with 1, and let  $I \subseteq R$  be an ideal.

(a). The *radical*  $\sqrt{I}$  of  $I$  is defined to be the set

$$\sqrt{I} = \{a \in R \mid a^n \in I \text{ for some } n > 0 \text{ depending on } a \}.$$

Prove that  $\sqrt{I}$  is an ideal, and that  $R/\sqrt{I}$  has no non-zero nilpotents.

(b). Let  $R = \mathbf{Z}$  and fix an integer  $m \geq 2$ . What is the radical  $\sqrt{(m)}$  of the principal ideal generated by  $m$ ?

(c). Let  $R = \mathbf{Q}[x, y]$  be the ring of polynomials in two variables with rational coefficients, and let  $I = (x^2, y^5)$  be the ideal generated by  $x^2$  and  $y^5$ . Find  $\sqrt{I}$ .

SOLUTION (a). To prove that  $\sqrt{I}$  is an ideal, the essential point is to show that it is closed under addition. Given  $a, b \in \sqrt{I}$ , choose  $n \gg 0$  so that  $a^n, b^n \in I$ . Then

$$(a + b)^{2n} = \sum \binom{2n}{k} a^k b^{2n-k}$$

is a sum of elements of  $\sqrt{I}$ , hence is itself in  $\sqrt{I}$ . By definition, a nilpotent in  $R/\sqrt{I}$  corresponds to an element  $a \in R$  such that  $a^k \in \sqrt{I}$ , which in turn means that  $a^{nk} \in I$  and hence  $a \in \sqrt{I}$ .

(b). Let  $m = p_1^{e_1} \cdots p_r^{e_r}$  be the prime factorization of  $m$ , with  $e_i > 0$ . Then  $\sqrt{I}$  is the principal ideal generated by  $m_{red} = p_1 \cdots p_r$ . In fact, clearly  $m_{red} \in \sqrt{(m)}$ . On the other hand, if  $m \mid a^n$  for some  $n > 0$ , then each  $p_i$  must divide. Therefore  $m_{red}$  divides  $a$ .

(c). Here  $\sqrt{I} = (x, y)$ . Both inclusions are clear.

(#2). (a). Suppose that  $G$  is a finite group acting on a finite set  $X$ . Prove that

$$\sum_{x \in X} |G_x|$$

is divisible by the group order  $|G|$ , where  $G_x$  is the stabilizer group of  $x \in X$ .

(b). For a finite group  $G$ , prove that the number of pairs  $(a, b)$  with  $a, b \in G$  and  $ab = ba$  is divisible by  $|G|$ .

SOLUTION. Let  $\mathcal{O}$  be an orbit. If  $x \in \mathcal{O}$ , then  $|\mathcal{O}| = |G|/|G_x|$ . We get

$$\sum_{x \in \mathcal{O}} |G_x| = \sum_{x \in \mathcal{O}} \frac{|G|}{|\mathcal{O}|} = |G|.$$

If we write  $X = \mathcal{O}_1 \cup \mathcal{O}_2 \cdots \cup \mathcal{O}_r$  as a disjoint union of orbits, then

$$\sum_{x \in X} |G_x| = \sum_{i=1}^r \sum_{x \in \mathcal{O}_i} |G_x| = \sum_{i=1}^r |G| = r|G|.$$

For (b), set  $X = G$  where  $G$  acts on  $X$  by conjugation. Then we have

$$G_x = \{g \in G \mid gx = xg\}$$

and

$$\sum_{x \in X} |G_x| = |\{(g, x) \in G^2 \mid gx = xg\}|$$

is divisible by  $|G|$  by part (a).

(#3). Suppose that  $A$  is a  $3 \times 3$  matrix with complex entries such that  $A$  is conjugate to  $-A$ . What are the possible Jordan normal forms of  $A$ .

SOLUTION. If  $A$  has an eigenvalue  $\lambda \neq 0$ , then  $-A$  has an eigenvalue  $-\lambda$ , so  $A$  has also the eigenvalue  $-\lambda$  because  $A$  is conjugate to  $-A$ . The third eigenvalue has to be 0 because  $\text{trace}(A) = \text{trace}(-A)$ , hence the sum of the eigenvalues is  $\text{trace}(A) = 0$ . In this case, the Jordan normal form of  $A$  is

$$B_\lambda := \begin{pmatrix} \lambda & 0 & 0 \\ 0 & -\lambda & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Also note that the matrix  $B_\lambda$  is conjugate to  $-B_\lambda$  because both have the same Jordan blocks.

The other case is where  $A$  has only zero eigenvalues. So  $A$  is nilpotent. Then the Jordan normal form of  $A$  is one of the following matrices.

$$N_{1,1,1} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, N_{2,1} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, N_3 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

The ranks of  $N_{1,1,1}, N_{2,1}, N_3$  are distinct, namely 0,1,2 respectively. Since  $-N_3$  has rank 2, it must be conjugate to  $N_3$ . Similarly  $N_{2,1}$  is conjugate to  $-N_{2,1}$ .

(#4). Let  $n$  be a positive integer.

(a). Prove that  $\cos(\frac{2\pi}{n})$  is an algebraic number, and compute its degree over  $\mathbf{Q}$  in terms of the Euler  $\phi$ -function.

(b). Find with proof all values of  $n$  for which  $\cos(\frac{2\pi}{n})$  is rational.

SOLUTION. (a). Let  $\zeta = e^{2\pi i/n}$  be a primitive  $n^{\text{th}}$  root of unity, so that

$$\cos(\frac{2\pi}{n}) = \frac{1}{2}(\zeta + \bar{\zeta}) = \frac{1}{2}(\zeta + \zeta^{n-1}).$$

Therefore  $\cos(\frac{2\pi}{n}) \in \mathbf{Q}(\zeta)$ , and in particular this cosine is algebraic. I claim that  $\cos(\frac{2\pi}{n})$  has degree  $\frac{\phi(n)}{2}$  over  $\mathbf{Q}$ . In fact, since  $\mathbf{Q}(\zeta)$  has degree  $\phi(n)$  over  $\mathbf{Q}$ , it is enough to show that  $\mathbf{Q}(\zeta)$  has degree two over  $\mathbf{Q}(\zeta + \bar{\zeta})$ . The degree is at most two since  $\zeta$  satisfies the equation

$$x^2 - (\zeta + \bar{\zeta})x + 1,$$

and the degree is  $\geq 2$  since the two fields in question are evidently different (e.g. the one generated by the cosine is real).

(b).  $\cos(\frac{2\pi}{n})$  is rational if and only if  $n = 1, 2, 3, 4, 6$ . Clearly it is rational in these cases. Conversely, we need to show that these are the only instances when  $\phi(n) = 1, 2$ . So suppose that  $\phi(n) = 1$  or  $2$ . Using that  $\phi(\ell m) = \phi(\ell)\phi(m)$  if  $\ell, m$  are relatively prime, we find that the only prime factors of  $n$  are 2 and/or 3, and since  $\phi(2^a) \geq 4$  if  $a \geq 4$  and  $\phi(3^b) \geq 4$  if  $b \geq 2$  we get the stated fact.

(#5). Let  $V$  be vector space over a field  $k$  of characteristic  $\neq 2$ , with  $n = \dim V \geq 3$ .

(a). Prove that there is a non-zero canonical map

$$V \otimes \Lambda^2 V \longrightarrow \Lambda^3 V.$$

(“Canonical” means that the map you construct should be independent of any choice of bases.)

(b). Show that the map in (a) is surjective, but not an isomorphism.

SOLUTION: (a). Consider first the mapping

$$V \times (V \times V) \longrightarrow \Lambda^3 V \quad , \quad (u, (v, w)) \mapsto u \wedge v \wedge w.$$

For fixed  $u$ , the map  $T(u)$  sending  $(u, v, w)$  to  $u \wedge v \wedge w$  is alternating in  $v, w$ . So it induces a linear map  $L(u)$  from the second exterior power of  $V$ . Then the map sending  $(u, z)$  to  $L(u)(z)$  is easily checked to be bilinear in  $u$  and  $z$ . So it induces

$$V \otimes (V \times V) \longrightarrow \Lambda^3 V \quad , \quad u \otimes (v \times w) \mapsto u \wedge v \wedge w.$$

This in turn is alternating in  $(v, w)$  so we get finally the required map. It is evidently independent of choices of bases, and non-zero.

(b). It is clearly surjective since every pure tensor  $u \wedge v \wedge w$  is in the image, and these span  $\Lambda^3 V$ . That it fails to be injective follows from a dimension count: one has

$$\dim V \otimes \Lambda^2 V = n \cdot \binom{n}{2} \quad , \quad \dim \Lambda^3 V = \binom{n}{3},$$

and the first is strictly bigger than the second.