

UNIVERSITY OF MICHIGAN  
DEPARTMENT OF MATHEMATICS  
Solutions to January 2005 Algebra QR exams

Morning

- (1) Let  $v$  be a nonzero integer  $n \times 1$  column vector, and define the matrix  $B := vv^T$ . Determine the elementary divisors (Smith invariants) of  $B$ .

*Solution.* Since  $B$  has rank 1, the last  $n - 1$  elementary divisors are 0. The first nonzero elementary divisor is just the gcd of the entries of  $B$ , which is the square of the gcd of the entries of  $v$ .

- (2) Consider the polynomial

$$f(X) = X^4 + rX^2 + s \in \mathbb{Q}[X]$$

and let  $K$  be its splitting field over  $\mathbb{Q}$ .

- (a) Show that the degree of the extension  $K : \mathbb{Q}$  is either 1, 2, 4 or 8.  
 (b) Show that  $f(X)$  is irreducible if and only if  $r^2 - 4s$  is not a square (of an element in  $\mathbb{Q}$ ), and either  $s$  is not a square or  $s$  is a square and both  $2\sqrt{s} - r$  and  $-2\sqrt{s} - r$  are not squares.  
 (c) Compute  $\text{Gal}(K : \mathbb{Q})$  if  $r = s = -1$ .

*Solution.* Let  $\alpha_1, \alpha_2$  be the roots of  $g(X) = X^2 + rX + s$ . Choose  $\beta_1, \beta_2$  such that  $\beta_1^2 = \alpha_1$  and  $\beta_2^2 = \alpha_2$ . The roots of  $f(X)$  are  $\beta_1, -\beta_1, \beta_2, -\beta_2$ .

(a) Let us write  $[M : L]$  for the degree of a field extension  $M : L$ . We have

$$[K : \mathbb{Q}] = [\mathbb{Q}(\beta_1, \beta_2) : \mathbb{Q}] = [\mathbb{Q}(\beta_1, \beta_2) : \mathbb{Q}(\beta_1)] \cdot [\mathbb{Q}(\beta_1, \alpha_1) : \mathbb{Q}(\alpha_1)] \cdot [\mathbb{Q}(\alpha_1) : \mathbb{Q}]$$

and each of  $[\mathbb{Q}(\beta_1, \beta_2) : \mathbb{Q}(\beta_1)]$ ,  $[\mathbb{Q}(\beta_1, \alpha_1) : \mathbb{Q}(\alpha_1)]$ ,  $[\mathbb{Q}(\alpha_1) : \mathbb{Q}]$  is equal to 1 or 2. (Note that  $\beta_2^2 = \alpha_2 \in \mathbb{Q}(\alpha_1) \subseteq \mathbb{Q}(\beta_1)$ .)

(b) If  $s^2 - 4r$  is a square then  $g(X) = X^2 + rX + s$  factors, so  $f(X) = g(X^2)$  factors nontrivially as well. Suppose that  $b$  is a square and  $2d - r$  is a square where  $d^2 = s$ , say  $2d - r = u^2$ . Then we can write

$$f(X) = X^4 + rX^2 + s = (X^2 + d)^2 - (cX)^2 = (X^2 + cX + d)(X^2 - cX + d).$$

Conversely, assume that  $f(X)$  factors. If  $f(X)$  factors into a linear and a degree 3 polynomial, then  $f(X)$  has a rational root. But then  $\beta_1$  or  $\beta_2$  is rational and  $f(X)$  has at least 2 rational roots (namely  $\pm\beta_1$  or  $\pm\beta_2$ ). Therefore, if  $f(X)$  is not irreducible, it factors into 2 quadratic polynomials, say  $f(X) = f_1(X)f_2(X)$ . Without loss of generality we assume  $f_1(\beta_1) = 0$ .

If the other root of  $f_1(X)$  is  $-\beta_1$ , then  $(\beta_1)(-\beta_1) = -\alpha_1 \in \mathbb{Q}$ . This implies that  $s^2 - 4r$  is a square.

Suppose that the other root of  $f_1(X)$  is  $\beta_2$ . Then  $d := \beta_1\beta_2 \in \mathbb{Q}$  and  $d^2 = (\beta_1\beta_2)^2 = \alpha_1\alpha_2 = s$ . Let  $c = \beta_1 + \beta_2 \in \mathbb{Q}$ . Then  $f_1(X) = X^2 - cX + d$ . Now  $f_2(X)$  has roots  $-\beta_1, -\beta_2$  and hence it is equal to  $X^2 + cX + d$ . We have

$$f(X) = X^4 + rX^2 + s = (X^2 + cX + d)(X^2 - cX + d).$$

From this follows that  $r = 2d - c^2$ , so  $2d - r = c^2$  is a square. (The case where the other root of  $f_1(X)$  is  $-\beta_2$  reduces to this case after relabeling the roots.)

(c) From part (b) we know that  $f(X)$  is irreducible and  $\alpha_1 \notin \mathbb{Q}$ . The polynomial  $g(X) = X^2 - X - 1$  has a positive and a negative root, hence  $f(X) = g(X^2)$  has two real roots and two complex (non-real) roots. Assume that  $\beta_1, -\beta_1$  are the real roots. If  $\beta_1 \in \mathbb{Q}(\alpha_1) = \mathbb{Q}(\beta_1^2)$  then by the transitive Galois group action  $\beta_2 \in \mathbb{Q}(\beta_2^2) = \mathbb{Q}(\alpha_1)$  and  $K = \mathbb{Q}(\alpha_1)$ . This is a contradiction because  $f(X)$  is irreducible and  $\mathbb{Q}(\alpha_1) : \mathbb{Q}$  is only a quadratic extension. Therefore  $\mathbb{Q}(\beta_1) \neq \mathbb{Q}(\alpha_1)$  and  $[\mathbb{Q}(\beta_1) : \mathbb{Q}] = 4$ . Since  $\beta_2$  is complex we have  $[K : \mathbb{Q}] = [\mathbb{Q}(\beta_1, \beta_2) : \mathbb{Q}] = 8$ . The Galois group has 8 elements and must be isomorphic to a (and therefore every) 2-Sylow subgroup of the symmetric group  $S_4$ . (For example take  $\{e, (12)(34), (13)(24), (14)(23), (12), (34), (1324), (1423)\}$ .)  $\square$

- (3) Let  $G$  be a finite solvable group. (a) Suppose that  $K$  is a minimal normal subgroup of  $G$ . Prove that  $K$  is an elementary abelian  $p$ -group, for some prime,  $p$ , i.e. a direct product of cyclic groups of order  $p$ . (b) Suppose that  $M$  is a maximal subgroup of  $G$ . Prove that  $|G : M|$  is a power of a prime.

*Solution.*

(a) Since  $K$  is not the identity and is solvable, the commutator subgroup  $K'$  is proper in  $K$ . The commutator subgroup of  $K$  is characteristic, hence is normal in  $G$ . Since  $K$  is minimal normal,  $K'$  is the identity. Therefore,  $K$  is abelian. Each of its Sylow groups is characteristic. Therefore  $K$  is an abelian  $p$ -group, for some prime  $p$ . The subgroup generated by  $p$ -th powers is proper and is characteristic, so is 1.

(b) Let  $K$  be a minimal normal subgroup.

Suppose  $K$  is not contained in  $M$ . Then  $G = KM$  and so  $|G| = |M||K : K \cap M|$ . Since  $|G| = |M||G : M|$ , we get  $|G : M| = |K : K \cap M|$ . Since  $|K : K \cap M|$  divides  $|K|$ , it is a power of  $p$ . The result follows.

Suppose that  $K$  is contained in  $M$ . Then we apply induction to the maximal subgroup  $M/K$  of  $G/K$ .

- (4) Let  $K$  be a field. Suppose that  $V$  is a finite dimensional  $K$ -vector and  $A : V \rightarrow V$  is an endomorphism. A vector  $v \in V$  is called cyclic (for  $A$ ) if  $V$  is spanned by  $v, Av, A^2v, \dots$ .
- (a) Show that if there exists a cyclic vector for  $A$ , then the minimum polynomial and the characteristic polynomial of  $A$  are the same.
- (b) Suppose there exists a cyclic vector and  $B : V \rightarrow V$  is an endomorphism which commutes with  $A$  (i.e.,  $AB = BA$ ). Show that there exists a polynomial  $p \in K[X]$  such that  $B = p(A)$ .

*Solution.* Let  $n = \dim V$  and  $v \in V$  be a cyclic vector. Then  $v, Av, A^2v, \dots, A^{n-1}v$  is a basis of  $V$ .

(a) Suppose that  $p(X)$  is the minimum polynomial and  $q(X)$  is the characteristic polynomial of  $A$ . If the degree of  $p(X)$  is smaller than  $n$ , then  $p(A)v \neq 0$  because  $v, Av, \dots, A^{n-1}v$  are independent. So  $\deg(p(X)) \geq n = \deg(q(X))$ . It follows that  $p(x) = q(x)$ .

(b) We can write

$$Bv = \sum_{i=0}^{n-1} \alpha_i A^i v$$

with  $\alpha_0, \dots, \alpha_{n-1} \in K$ . We claim that  $B = \sum_{i=0}^{n-1} \alpha_i A^i$ . It suffices to verify this on the basis elements:

$$B(A^j v) = A^j Bv = A^j \sum_{i=0}^{n-1} \alpha_i A^i v = \left( \sum_{i=0}^{n-1} \alpha_i A^i \right) (A^j v)$$

for  $j = 0, 1, \dots, n-1$ . □

- (5) Let  $G$  be a nonabelian simple group and let  $G_1, G_2, G_3$  be isomorphic copies of  $G$ .

(a) Prove that the complete set of normal subgroups of  $G_1 \times G_2$  is

$$\{1, G_1, G_2, G_1 \times G_2\}.$$

(We identify  $G_1$  with  $\{(x, 1) \in G_1 \times G_2 \mid x \in G_1\}$ , etc. )

(b) Now assume that  $G$  is finite. Let  $\varphi$  be a monomorphism of groups,

$$\varphi : G_1 \times G_2 \rightarrow G_1 \times G_2 \times G_3.$$

Prove that there exist indices  $i$  and  $j$ , not necessarily distinct, so that  $\varphi(G_i) = G_j$ .

*Solution.* (a) Let  $K$  be a normal subgroup. Suppose that  $K$  contains an element of the form  $(x, y)$ , where  $x \neq 1$ . Then, by conjugating with elements of the first factor, we see that  $K$  contains every element of the form  $(x', y)$ , where  $x'$  is conjugate in  $G_1$  to  $x$ . Taking ratios, we see that  $K$  contains every commutator  $x^{-1}x'$  in  $G_1$ . Such

commutators generate  $G_1$  (nonabelian simple, so has only trivial abelian quotients) and so  $K$  contains  $G_1$ . If  $K$  contains an element of the form  $(x, y)$ , where  $y \neq 1$ , then  $K$  contains  $G_2$  by a symmetric argument. It follows that if  $K$  is not the identity, it contains  $G_i$  for some  $i$ . If  $K > G_i$ ,  $K$  maps to a nonidentity normal subgroup of  $(G_1 \times G_2)/G_i$ , which is simple, whence  $K = G_1 \times G_2$ . The conclusion follows.

(b) Suppose that  $G_1$  maps into some  $G_k$ . By finiteness, the image of  $G_1$  is  $G_k$  and we may take  $i = 1, j = k$ .

Suppose that  $G_1$  maps into no  $G_k$ . Then, there is a pair of distinct indices  $p, q$  so that  $\varphi(G_1)$  projects nontrivially to  $G_p$  and  $G_q$ . By finiteness and simplicity, each projection is onto.

We quote a fact, that two elements of a direct product  $H_1 \times \cdots \times H_m$  commute if and only if their respective projections to each  $H_i$  commute.

Using the fact, we see that  $\varphi(G_2)$  maps into the centralizer in  $G_1 \times G_2 \times G_3$  of  $G_p \times G_q$ , which is just the third factor  $G_r$ . We take  $i = 2, j = r$ .

## Afternoon

- (1) Suppose that  $K : \mathbb{Q}$  is a Galois extension. Prove that for any subfield  $L$  of  $K$  there exist subfields  $L_1, L_2, \dots, L_r \subseteq K$  such that  $L = L_1 \cap \dots \cap L_r$  and the degree of the field extension  $K : L_i$  is a prime power for all  $i$ .

*Solution.* Since the extension is Galois, there is a subgroup  $F$  of  $G = \text{Gal}(K : \mathbb{Q})$  corresponding to  $L$ . The degree of  $K : L$  is  $|F|$ . Let  $P_1, \dots, P_r$  be Sylow groups of  $F$ , one for each prime divisor of  $|F|$ . Take  $L_i$  to be the fixed field of  $P_i$ . The fundamental theorem says that  $K : L_i$  is the prime power  $|P_i|$ . Also  $L_1 \cap \dots \cap L_r$  is the subfield fixed by the group generated by the  $P_i$ , which is  $F$ .

- (2) Let  $H$  be a group of order  $5^p \cdot 7^q$ , for integers  $p \geq 0, q \geq 0$ .
- Show that an action of  $H$  on a set with 23 elements has a fixed point.
  - Suppose that  $H$ , as above, is a subgroup of index 24 in the larger group  $G$ . Prove that the normalizer  $N_G(H)$

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

is strictly larger than  $H$ .

*Solution.*

(a) Suppose that  $H$  acts on a set  $S$  with 23 elements. The length of an  $H$ -orbit always divides the order of  $H$ . Hence, the length of an  $H$ -orbit is either 1 (a fixed point) or a multiple of 5 or 7. If  $S$  does not have any fixed points, then  $23 = 5a + 7b$  for some nonnegative integers  $a, b$ . It is easy to verify that this equation does not have any solution, so  $H$  must have a fixed point.

(b) Consider the action of  $H$  on  $G/H$ . The coset  $eH$  is clearly a fixed point. So  $H$  also acts on  $S := G/H \setminus \{eH\}$ . Since  $S$  has 23 elements, there must be a fixed point in  $S$  by part (a). So there exists  $gH \in G$  such that  $gH \neq eH$  (i.e.,  $g \notin H$ ) and  $HgH = gH$  which implies that  $g^{-1}Hg = H$ . It follows that  $g \in N_G(H) \setminus H$ .  $\square$

- (3) Given a pair of linear transformations  $T_i : V_i \rightarrow W_i, i = 1, 2$ , of vector spaces, there is a unique linear transformation  $V_1 \otimes V_2 \rightarrow W_1 \otimes W_2$  which takes  $x_1 \otimes x_2$  to  $T_1x_1 \otimes T_2x_2$ , for all  $x_i \in V_i, i = 1, 2$ .

Now suppose that the 3-dimensional complex vector space  $V$  has an endomorphism  $T$  with matrix

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Determine the Jordan canonical form of the transformation  $T \otimes T$ .

*Solution.* Let  $e_1, e_2, e_3$  be the standard basis of column vectors. Define  $e_{ij}$  to be  $e_i \otimes e_j$ . The action of  $S := T \otimes T$  on the  $e_{ij}$  is easy to calculate. In fact,  $Se_{ij} = e_{i-1, j-1}$ , where the right side is 0 if either subscript is negative. The subspaces  $\text{span}\{e_{11}, e_{22}, e_{33}\}$ ,  $\text{span}\{e_{12}, e_{23}\}$ ,  $\text{span}\{e_{21}, e_{32}\}$ ,  $\text{span}\{e_{13}\}$ ,  $\text{span}\{e_{31}\}$  give an  $S$ -invariant direct sum decomposition of  $V \otimes V$  and exhibit the Jordan decomposition with blocks of size 3, 2, 2, 1, 1, all for eigenvalue 0.

- (4) (a) Suppose that  $R$  is a ring and  $I, J \subseteq R$  are ideals. Prove that

$$(I \cap J)(I + J) \subseteq IJ.$$

- (b) Suppose that  $R$  is a principal ideal domain (PID) and  $I, J \subseteq R$  are ideals. Prove that

$$(I \cap J)(I + J) = IJ.$$

- (c) Suppose that  $R$  is a unique factorization domain (UFD) and let  $a, b \in R$ . Prove that  $(a) \cap (b)$  is a principal ideal.  
 (d) Suppose that the UFD  $R$  is Noetherian (i.e., every ideal of  $R$  is finitely generated) and that  $(I \cap J)(I + J) = IJ$  for all ideals  $I, J \subseteq R$ . Prove that  $R$  is a PID.

*Solution.*

(a) Clearly  $(I \cap J)I \subseteq JI = IJ$  and  $(I \cap J)J \subseteq IJ$ , hence  $(I \cap J)(I + J) = (I \cap J)I + (I \cap J)J \subseteq IJ$ .

(b) Let  $I = (a)$ ,  $J = (b)$  and  $I + J = (c)$ . Let  $d = ab/c$ . Then clearly  $d = a(b/c) \in I$  and  $d = b(a/c) \in J$  because  $b/c, a/c \in R$ . Hence  $d \in I \cap J$ . It follows that  $(I \cap J)(I + J) \supseteq (d)(c) = (ab) = IJ$ .

(c) We can write  $a = a'c$ ,  $b = b'c$  for some  $c \in R$  where  $a'$  and  $b'$  do not have a common irreducible factor. Let  $d = ab/c = a'b'c$ . Clearly  $d \in (a) \cap (b)$ . Looking at the factorization of  $e$  shows that  $e$  is divisible by  $a'b'c$ , hence  $e \in (d)$ .

(d) Let  $a, b \in R$  both nonzero. Let  $I = (a)$ ,  $J = (b)$ . Then  $(a) \cap (b) = (d)$  is principal. Let  $c = ab/d$ . From  $(d)(I + J) = (ab)$  follows  $I + J = (c)$ . This shows that  $(a, b)$  is principal. By induction and the Noetherian property, any ideal is generated by 1 element.  $\square$

- (5) Determine the Sylvester signature of the real matrix

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix}.$$

*Solution.* Since the matrix is symmetric and real, all eigenvalues are real. The determinant is  $-1$ , so the number of negative eigenvalues is odd. If that number were 3, the form would be negative definite. This would imply that all diagonal terms are negative, which is false. Therefore, the signature is 2, 1, 0.