

UNIVERSITY OF MICHIGAN
DEPARTMENT OF MATHEMATICS
Solutions to September 2007 Algebra QR Exams

MORNING

1. The isomorphism class of the quotient is not affected by elementary row and column operations on the corresponding matrix, which is $\begin{pmatrix} 1 & 2 & 3 & 5 \\ 2 & 1 & 6 & 4 \\ 1 & -1 & 3 & -1 \end{pmatrix}$. Subtract twice the

first row from second and the first from the third to get $\begin{pmatrix} 1 & 2 & 3 & 5 \\ 0 & -3 & 0 & -6 \\ 0 & -3 & 0 & -6 \end{pmatrix}$. Subtract

the second row from the third, so that the third row is all zeros. Subtract multiples of the first column from the remaining columns so as to cancel the remaining entries in the first

row. This yields $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -3 & 0 & -6 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. Multiply the second row by -1 and subtract twice

the second column from the fourth to obtain $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. It is now clear that that

the quotient $F/G \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$, which has torsion-free rank 2. G itself is free of rank 2, and $G \cong \mathbb{Z} \oplus \mathbb{Z}$.

2. (a) It is possible. One may take A to be the identity and B to be zero. More generally, let k be any integer between 1 and n inclusive. Let A be the diagonal matrix such the first k diagonal entries are 1 and the other entries are 0. Let $B = \mathbf{1} - A$.

(b) $(\mathbf{1} + 2^{-1}C)^2 = \mathbf{1} + 2(2^{-1}C) + C^2 = \mathbf{1} + C$.

3. (a) The degree is $2p$, since $|D| = 2p$.

(b) The subgroups of D other than $\{e\}$ and D have order 2 or p . There are p subgroups of order 2, corresponding to p fields of degree p over \mathbb{Q} , and one subgroup of order p , corresponding one field of degree 2 over \mathbb{Q} . The total number of strictly intermediate fields is $p + 1$.

(c) The degree 2 extension is the unique normal extension among these strictly intermediate fields, since a subgroup of order p in a group of order $2p$ is normal. Since the p distinct Sylow 2-subgroups are all conjugate, none of them is normal, and, hence, none of the intermediate fields of degree p is normal.

(d) Yes, the elements can be expressed by radicals, since D is solvable: it has a normal subgroup isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and the quotient is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

4. (a) If the vectors are dependent and $h = 1$, the single vector is 0 and the result is clear. If not, one of the vectors is a linear combination of the others. Since permuting them only affects the sign of the wedge, we may assume that $v_h = a_1v_1 + \cdots + a_{h-1}v_{h-1}$ with the $a_j \in K$. Then $v_1 \wedge \cdots \wedge v_h = (v_1 \wedge \cdots \wedge v_{h-1}) \wedge (a_1v_1 + \cdots + a_{h-1}v_{h-1})$. When we distribute, v_i is repeated in the i th term, and so every term is 0. For the other direction, if v_1, \dots, v_h are independent we may complete them to a basis v_1, \dots, v_n . Introduce coordinates, i.e., choose $V \cong K^n$. There is an alternating multilinear map $V \times \cdots \times V \rightarrow K$ that sends an n -tuple of vectors to the determinant of the matrix whose columns (or rows) give the coordinates of those vectors. This map is nonzero when the matrix has rank n , which shows that $v_1 \wedge \cdots \wedge v_n$ is not 0. Alternatively, we may map V onto K^h so that v_j maps to the j th standard basis element e_j for K^h , $1 \leq j \leq h$. Then $v_1 \wedge \cdots \wedge v_h$ maps to $e_1 \wedge \cdots \wedge e_h$, which is nonzero and spans $\bigwedge^h(K^h)$ by a standard theorem.

(b) The elements $v_{i_1} \wedge \cdots \wedge v_{i_k}$ for $1 \leq i_1 < \cdots < i_k \leq n$ are a basis for $\bigwedge^k(V)$ for $1 \leq k \leq n$. The cardinality of this basis is $\binom{n}{k}$. For $k > n$, $\bigwedge^k(V) = 0$ by part (a), since any k -fold wedge involves dependent vectors and so must be 0.

(c) Two vectors are independent if and only if their wedge is not zero, by part (a). Hence, $u \wedge v$ and $u' \wedge v'$ are nonzero. Moreover, $(u \wedge v) \wedge w = 0$ if and only if u, v, w are dependent, which means that w is in the plane spanned H by u, v . If $u \wedge v = c(u' \wedge v')$, we have that $(u \wedge v) \wedge u' = c(u' \wedge v') \wedge u' = 0$, and so u' is in H . Similarly v' is in H . Since u' and v' are independent, their span must be H . On the other hand if $u' = au + bv$ and $v' = cu + dv$ then $u' \wedge v'$ is nonzero and is equal to $(au + bv) \wedge (cu + dv) = adu \wedge v + bcv \wedge u = (ad - bc)(u \wedge v)$, where $ad - bc \neq 0$ because u' and v' are independent, and this is the condition required. (Note: do not confuse $\bigwedge^2(\bigwedge^2(V))$ and $\bigwedge^4(V)$. E.g., if $n = 4$, the former has dimension 15 and the latter has dimension 1. In particular $(u \wedge v) \wedge (u' \wedge v')$ may be thought of in either, but the meanings are quite different.

5. y generates a subgroup N of order 7, and x is in the normalizer, since $xyx^{-1} = y^k$. The quotient is generated by x , and must be \mathbb{Z}_3 . Let H be the the subgroup generated by x . Then $G = HN$, a semidirect product. G is determined by the action of H by conjugation on $N \cong \mathbb{Z}_7$. Since \mathbb{Z}_7 is cyclic, its automorphisms are given by multiplication by an invertible element of \mathbb{Z}_7 . These form a cyclic group of order 6, and so there are 3 elements of order dividing 3. These are given by multiplication by 1, 2, and 4 (note that $4 \equiv 2^{-1} \pmod{7}$). These are the possibilities for k . If we use $k = 1$ we obtain the unique commutative possibility, which is \mathbb{Z}_{21} . The other groups are not commutative, but are still isomorphic, since if we use y^{-1} as a generator instead of y the roles of 2 and 4 are interchanged. Thus, up to isomorphism, there are two possibilities for the group.

AFTERNOON

1. (a) The order of g is $\text{LCM}(3, 4) = 12$.

(b) The conjugates are the elements that are the product of a disjoint 3-cycle and 4-cycle. The number of choices for the elements of the 3-cycle is $\binom{7}{3} = 7 \cdot 6 \cdot 5 / 3! = 35$. Each choice of 3 elements yields $(3 - 1)! = 2$ 3-cycles. The remaining 4 elements give $(4 - 1)! = 6$ 4-cycles. Hence, the number of conjugates is $35 \cdot 2 \cdot 6 = 420$.

(c) The order of the centralizer is the order of the group divided by the number of elements in the conjugacy class, i.e., $7! / 420 = 6! / 60 = 720 / 60 = 12$.

(d) This is the number of subgroups generated by the product of a disjoint 3-cycle and 4-cycle. Such a subgroup contains $\Phi(12) = 4$ elements of this type (e.g., G contains g, g^5, g^7, g^{11}). Hence, there are $420 / 4 = 105$ groups conjugate to G .

2. Since $30 = 2 \cdot 3 \cdot 5 \in m$, we must have either $2 \in m$ or $3 \in m$ or $5 \in m$. The maximal ideals of $\mathbb{Z}[x]$ containing the prime integer p and $x^2 + 1$ correspond bijectively to the maximal ideals of $\mathbb{Z}_p[x]$ containing $x^2 + 1$, and these in turn correspond bijectively to the distinct irreducible factors of $x^2 + 1$. If $p = 2$, $x^2 + 1 = (x + 1)^2$, and there is only one choice of m , $(2, x + 1)$. If $p = 3$ then $x^2 + 1$ is irreducible over \mathbb{Z}_3 , and there is again only one choice of m , $(3, x^2 + 1)$. If $p = 5$, $x^2 + 1 = (x - 2)(x - 3)$, and there are two choices of m , $(5, x - 2)$ and $(5, x - 3)$. (The generators can be written in many different ways, since, for example, the coefficients of the polynomial can be changed to other integers that are congruent mod p .)

3. The issues are unaffected if we perform elementary row and column operations in such a way that each time we perform a row operation we perform the corresponding column operation as well. This changes the matrix M to one of the form AMA^{tr} , where A is a 4×4 invertible matrix and A^{tr} is its transpose. Subtract twice the first row from the second and twice the first column from the second. Subtract 3 times the first row from the third and three times the first column from the third. Subtract 4 times the first row from the fourth and 4 times the first column from the fourth. This gives

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 1 & 1 & a - 16 \end{pmatrix}.$$

Now subtract the second row from the third and the second column from the third. Then subtract the second row from the fourth and the second column from the fourth. This yields

$D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & a - 17 \end{pmatrix}$. Thus, the signature given as a triple is $(4, 0, 0)$ if $a > 17$, and

then the matrix is positive definite, $(3, 0, 1)$ if $a = 17$, and then the form is degenerate, and $(3, 1, 0)$ if $a < 17$. Here, the first entry of the triple (p, q, r) is the number of positive entries on the diagonal of a cogredient diagonal matrix, the second entry is the number of negative entries on the diagonal, and the third is the number of zeros on the diagonal. The other definition of signature is $p - q$, and is 4 if $a > 17$, 3 if $a = 17$, and 2 if $a < 17$. The form is positive definite precisely if $a > 17$ and nondegenerate precisely if $a \neq 17$. The rank is 4 if $a \neq 17$ and 3 if $a = 17$. (Note: the eigenvalues of the cogredient diagonal

matrix D are not necessarily the same as those of the original matrix, but they have the same *signs* as the eigenvalues of the original matrix.)

4. Then $A^{rs} = B^s = A$, so that the minimal polynomial of A divides $x^{rs} - x = 0$. The roots of this polynomial are simple: 0 is a simple root, and the remaining roots are those of $x^{rs-1} - 1 = 0$, which are distinct since the derivative is $(rs - 1)x^{rs-2}$ with $rs \geq 4$. Hence, the minimal polynomial of A has no multiple roots, and A is diagonalizable. The same reasoning shows that B is as well.

5. (a) r must be a positive integer power of q , so that $r = q^n$, since R is a finite dimensional vector space over K , and so isomorphic with K^n .

(b) $GF(q)$ is the splitting field of $x^q - x = 0$, which is one way of constructing it. It is immediate that the set roots of this equation is closed under addition, subtraction, and multiplication, that the inverse of a nonzero root is a root, and that 0 and 1 are roots. The derivative is -1 , so there are no multiple roots, and the set of roots therefore has q elements.

(c) We have $r = q^n$ and $q = p^k$. Let F denote the Frobenius automorphism of the field $GF(q^n)$: $F(a) = a^p$ for all a in the field. The Galois group, by a standard theorem, is \mathbb{Z}_n , and is generated by F^k , where the exponent indicates k -fold composition. Note that $(F^k)^n$ is the identity on $GF(q^n)$.

(d) The subfields are precisely the fields $GF(p^k)$ such that p^n is a power of p^k , i.e., such that k divides n . Alternatively, the subfields correspond to the subgroups of \mathbb{Z}_n , and these are in bijective correspondence with the divisors of n , where $d|n$ corresponds to the subgroup generated by $[d]$.