Qualifying Review Examination: Algebra
January 8, 2005

Morning

Answer all questions. Prove your answers.

1. Let G be a group (possibly nonabelian, written multiplicatively) with subgroups H and K of finite, relatively prime indices. Prove that $G = HK$.

2. (a) Determine the elementary divisors d_1, d_2, d_3 of the matrix

$$A = \begin{pmatrix} -1 & 2 & 1 \\ -1 & 0 & 1 \\ -1 & -2 & 5 \end{pmatrix}.$$

(b) Let x_1, x_2, x_3 be indeterminates and define $y_1 = x_1^{-1}x_2^2x_3$, $y_2 = x_1^{-1}x_3$ and $y_3 = x_1^{-1}x_2^{-2}x_3^5$. (Note that the exponents are the entries of the matrix A.) Prove that the field extension $\mathbb{C}(x_1, x_2, x_3) : \mathbb{C}(y_1, y_2, y_3)$ is a Galois extension with Galois group $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \mathbb{Z}/d_3\mathbb{Z}$.

(c) How many fields are there strictly in between $\mathbb{C}(x_1, x_2, x_3)$ and $\mathbb{C}(y_1, y_2, y_3)$? (You do not have to give these fields explicitly, but you do have to motivate your answer.)

3. A 5×5 mystery matrix A with complex entries has the following properties: $\det(A) = 1$, $\operatorname{trace}(A) = 5$, $\operatorname{rank}(A - I) = 3$ and the minimum polynomial of A has degree 3. What are the possibilities for the Jordan canonical form of A?

4. Let $q = p^k$ where p is a prime number and k is a positive integer. The group $\mathrm{GL}_n(\mathbb{F}_q)$ of invertible matrices over the field $\mathbb{F}_q$ with q elements has cardinality

$$(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

(a) Let $U_n(\mathbb{F}_q)$ be the subgroup of upper triangular matrices with 1's on the diagonal. Show that $U_n(\mathbb{F}_q)$ is a p-sylow subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$.

(b) Suppose that H is a p-group of order p^r. Show that for all q, H is isomorphic to a subgroup of $U_n(\mathbb{F}_q)$ with $n = p^r$.

(c) Suppose that $\mathrm{GL}_n(\mathbb{F}_q)$ contains the cyclic group of order p^r. Prove that $n > p^{r-1}$.

5. Let V_n be the $n \times n$ symmetric matrices with real entries. Let $D \in V_n$ be a fixed diagonal matrix. Define a bilinear form $B_D(\cdot, \cdot)$ on V_n by

$$B_D(X, Y) := \operatorname{trace}(XDY).$$

(a) Prove that B_D is symmetric.

(b) Determine conditions on the diagonal entries of D that characterize when B_D is non-degenerate.

(c) Determine the rank and signature of B_D if $n = 3$ and the diagonal entries of D are $0, 1$, and -1.

Qualifying Review Examination: Algebra
January 8, 2005

Afternoon

Answer all questions. Prove your answers.

1. Consider these permutations in G, the symmetric group on $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Let H be the subgroup generated by $\alpha := (1, 2, 3)$ and $\beta := (1, 6, 2, 7, 3, 8, 9)$.
(a) Describe the orbits of H on $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
(b) Prove that $|H|$ divides $2^3 \cdot 3^2 \cdot 5 \cdot 7$.
(c) Prove that $|H|$ is divisible by $2^2 \cdot 3^2 \cdot 5 \cdot 7$.

2. Let F be a field of characteristic 0.

(a) Suppose that F contains a primitive n^{th} root of unity. Let $a \in F$ and let E be a splitting field for $x^n - a$ over F. Prove that the Galois group of E/F is an abelian group which is isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$.

(b) Let F be a field of characteristic 0. Let $a \in F$ and let E be a splitting field for $x^n - a$ over F. Prove that the Galois group of E/F is a solvable group.

3. Let V be a finite dimensional vector space over an algebraically closed field F and $T \in \mathrm{End}_F(V)$.

(a) Prove that there is a well defined linear transformation $S \in \mathrm{End}_F(\wedge^2 V)$ so that $S(v \wedge w) = Tv \wedge Tw$.

(b) If the characteristic of F is not 2, find a formula for the trace of S in terms of $\mathrm{tr}(T)$ and $\mathrm{tr}(T^2)$, where tr means trace on V.

4. Let F be a field and p a prime number. Let M be the permutation matrix for a p-cycle,

$$\text{e.g., } M = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ \vdots & & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

(a) Find the rational canonical form for M.

(b) Assume that the characteristic polynomial for M factorizes completely into linear factors in $F[x]$. Find the Jordan canonical form.

(c) Suppose that $F = \mathbb{F}_2$, the field of integers modulo 2 and S is an $n \times n$ matrix whose minimal polynomial is $m(x) = (x^2 + x + 1)(x^3 + x^2 + 1)$. For the action of S on $V := \mathbb{F}_2^n$, there is a decomposition of V into summands V_i corresponding to the irreducible factors of $m(x)$ in $F[x]$. Show how to compute the projections to the V_i, as particular polynomial expressions in S.

5. A group G is called nilpotent if there is a series $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ so that $G_i/G_{i-1} \leq Z(G/G_{i-1})$.

When G is finite, prove that this is equivalent to G being the direct product of its Sylow p-groups, for the primes p which divide $|G|$.

Qualifying Review Examination: Algebra
January 8, 2005

Solutions

Morning

1. Let the indices of H and K be r and s, respectively. G acts on the left cosets of K by left multiplication, and is their union. Restrict the action to H, and consider the orbit of K. Note that $h_1K = h_2K$ iff $h_2^{-1}h_1 \in K$ iff $h_2^{-1}h_1 \in H \cap K$ iff $h_2(H \cap K) = h_1(H \cap K)$. Thus, the number of elements in the orbit is the same as $[H : H \cap K]$, and it suffices to show that $[H : H \cap K] = [G : K] = s$. Now $[H : H \cap K] = [G : H \cap K]/[G : H]$ which shows that $[G : H \cap K]$ is divisible by r. Similarly, $[G : H \cap K]$ is divisible by s. Thus, $[G : H \cap K]$ is divisible by rs. Consider the map $f : G \to G/H \times G/K$ that sends $g \mapsto (gH, gK)$. Then $f(g_1) = f(g_2)$ iff $g_1H = g_2H$ and $g_1K = g_2K$ iff $g_2g_1^{-1}$ is in both H and K iff $g_1(H \cap K) = g_2(H \cap K)$. Hence, f induces an injection of $G/(H \cap K)$ into $G/H \times G/K$, and this shows that $[G : H \cap K] \leq rs$. It follows that $[G : H \cap K] = rs$, and $[H : H \cap K] = [G : H \cap K]/[G : H] = rs/r = s$, as required. $\square$

2. (a) Subtract the first row from the second and third rows, multiply the first column by -1, and then subtract multiples of the first column from the other two to get $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & -4 & 4 \end{pmatrix}$. Reverse the sign of the second row and subtract twice the second row from the third to get a diagonal matrix with diagonal entries 1, 2, 4. Since $1|2|4$, these are the elementary divisors.

(b) These elementary operations correspond to taking new sets of generators for the two fields. Using the new generators, we find that we have the inclusion of $\mathbb{C}(v_1, v_2, v_3)$ in $\mathbb{C}(u_1, u_2, u_3)$ where $v_1 = u_1$, $v_2 = u_2^2$, and $v_3 = u_3^4$. The Galois group when one adjoins a dth root of a variable is $\mathbb{Z}/d\mathbb{Z}$, since all the roots of unity are in $\mathbb{C}$. Note that automorphisms that permute the d_j th roots of v_j while fixing the other v_i mutually commute. Thus, the Galois group is the product of the $\mathbb{Z}/d_i\mathbb{Z}$, which is $\mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_2 \times \mathbb{Z}_4$. $\square$
(c) Let a, b be the respective generators. Then $(0, \pm b)$ and $(a, \pm b)$ have order 4 while $(a, 2b), (a, 0)$ and $(0, 2b)$ have order 2. These three and 0 give a subgroup of order 4, and $(0, b)$, (a, b) give cyclic subgroups or order 4. Thus, the proper non-trivial subgroups consist of three subgroups of order 4 and three subgroups of order 2, six in all. By the fundamental theorem of Galois theory that there are six strictly intermediate fields.

3. Since the minimal polynomial has degree 3, it has at most three distinct roots. Since $\text{rank}(A - I) = 3$, 1 is at least a double eigenvalue. If 1 is a triple eigenvalue then the remaining eigenvalues b, c satisfy $bc = 1$ ad $b + c = 2$ from the determinant and trace conditions, which forces $b = c = 1$. If not, the remaining eigenvalues must have a repetition: call them b, b, c (where $b = c$ is possible). Then $b^2c = 1$ and $2b+c = 3$ whence $c = 1/b^2$ and $2b + 1/b^2 = 3$ yielding $2b^3 - 3b^2 + 1 = 0$ or $(b - 1)^2(2b + 1) = 0$. We must have $b = -1/2$ and $c = 4$. We get two possible Jordan forms:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1/2 & 0 & 0 \\ 0 & 0 & 0 & -1/2 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{pmatrix}$$

from the two cases: no other possibilites have $\mathrm{rank}(A - I) = 3$.

4. (a) Each matrix in $U = U_n(\mathbb{F}_q)$ has $(n-1)+\cdots+1 = n(n-1)/2$ entries above the main diagonal, with q possibilities for each, so that $|U| = q^{n(n-1)/2}$. But the highest power of p dividing $q^n - q^i$ is q^i, $0 \le i \le n-1$, and so the highest power of p dividing the order of $\mathrm{GL}_n(\mathbb{F}_q)$ is $q^{0+1+2+\cdots+(n-1)} = q^{n(n-1)/2}$, and it follows that U is a Sylow p-subgroup. $\square$

(b) H acts faithfully on itself by left multiplication. We may take H as the basis of a vector space of dimension $|H| = p^r$ over $\mathbb{F}_q$. The permutations of the basis extend to linear transformations, and this gives an embedding of H into $\mathrm{GL}_n(\mathbb{F}_q)$ with $n = p^r$. But the image of H is contained in some Sylow p-subgroup, which will be conjugate to and, hence, isomorphic to $U_n(\mathbb{F}_q)$. $\square$

(c) It follows that $U_n(\mathbb{F}_q)$ contains a matrix A of order exactly p^r. The characteristic polynomial of A is $(x-1)^n = 0$, and $(x-1)^{p^{r-1}} = x^{p^{r-1}} - 1 \ne 0$, so that $n > p^{r-1}$. $\square$

5. (a) Let $'$ indicate transpose. We then have $B_D(Y, X) = \mathrm{trace}(YDX) = \mathrm{trace}\big((YDX)'\big)$ $= \mathrm{trace}(X'D'Y') = \mathrm{trace}(XDY) = B_D(X, Y)$. $\square$ Alternatively, the basis calculation for part (b) shows the symmetry as well.

(b) Let E_{ij} be the $n \times n$ matrix with a 1 in the ij spot and 0 elsewhere. $E_{hi}E_{jk} = 0$ unless $i = j$, in which case it is E_{ik}. B_D is defined for any pair of matrices, and $B_D(E_{hi}, E_{jk}) = \mathrm{trace}(E_{hi} \sum_t d_t E_{tt} E_{jk})$. All terms are 0 unless $i = j$, in which case the value is $d_i \mathrm{trace}(E_{hk})$. Thus, $B_D(E_{hi}, E_{jk}) = 0$ unless $h = k$ and $i = j$, in which case its value is d_i. As a basis for V_n we take the E_{ii} (n elements) and the $E_{ij} + E_{ji}$ for $i \ne j$ ($n(n-1)/2$ elements). It is easy to check that the matrix of B_D with respect to this basis is diagonal: the value on (E_{ii}, E_{ii}) is d_i, and the value on $E_{ij} + E_{ji}$ for $i \ne j$ is $d_i + d_j$. (This again shows symmetry.) The condition for non-degeneracy is that all the b_i are non-zero, and none is the negative of another.

(c) In the specified case the diagonal entries of the matrix for B_D are $-1, 0, 1$ together with their sums two at a time, which turn out to be $-1, 0, 1$ again. The rank is 4, and the signature is (2,2,2) as a triple, or $2 - 2 = 0$ as a single integer.

Afternoon

1. (a) The elements S occurring in β, namely $\{1,2,3,6,7,8,9\}$, give one orbit, since these also contain the elements occurring in α, and $\{4\}$, $\{5\}$ are the remaining orbits.

(b) Evidently, the group embeds in the permutations of the seven elements in S, and since both permutations are odd, the group is a subgroup of A_7, and so its order divides $|A_7| = 7!/2 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$.

(c) It is clear that the order is divisible by 7. The action of β on α by conjugation successively produces the 3-cycles $(6,7,8)$, $(2,3,9)$ $(7,8,1)$. Since $(1,2,3)$ and $(6,7,8)$ generate a subgroup of order 9, we see that 9 divides the order. Since $(7,8,1)(1,2,3) = (1,2,3,7,8)$ we see that 5 divides the order. Since $(1,2,3)$ and $(1,2,3,7,8)$ generate a subgroup of A_5 of order a multiple of 15, and the simple group A_5 has no proper subgroup of index dividing 4 (or it would embed via the action on left cosets into S_k for $k \leq 4$), $(1,2,3)$ and $(1,2,3,7,8)$ generate all odd permutations of $\{1,2,3,7,8\}$, a group of order 60, and so 2^2 divides the order as well (one may also prove this computationally by producing explicitly the elements of a subgroup of order 4).

Note: the group generated is actually all permutations of $\{1,2,3,6,7,8,9\}$, since the simple group A_7 has no subgroup of index 2 (such a subgroup would be normal).

2. (a) If $a = 0$, the result is obvious. Suppose that $a \neq 0$. Let θ be a primitive nth root of 1. Let b denote one bth root of a. The others are the elements $b\theta^i$, $0 \leq i < n$. Each automorphism must map a to $a\theta^j$ for some choice of j, $0 \leq j < n$, and then $a\theta^i$ maps to $a\theta^{i+j}$, where the exponent may be interpreted in $\mathbb{Z}/n\mathbb{Z}$. The composition of the automorphisms corresponding to j and j' is the one corresponding to $j + j'$. This gives an embedding of the automorphism group into $\mathbb{Z}/n\mathbb{Z}$. $\square$

(b) The result is clear if $a = 0$. If $a \neq 0$ the Galois group must contain the nth roots of unity, as these are ratios of nth roots of a. Any automorphism α of $F[\theta]$ must send θ to θ^j for some j, where j is invertible mod n (since θ^j must als be a primitive nth root of 1), which determines α, and the composition of the automorphisms corresponding to $\theta \mapsto \theta^j$ and $\theta \mapsto \theta^{j'}$ corresponds to $\theta \mapsto \theta^{jj'}$. This embeds the automorphism group in the multiplicative group of $\mathbb{Z}/n\mathbb{Z}$, which shows that it is abelian. The splitting field is obtained by first adjoining all the nth roots of unity (in characteristic 0 these are distinct, and so the extension is Galois), and then one root of $x^n - a$. The Galois group therefore has a normal abelian subgroup H such that G/H embeds in $\mathbb{Z}/n\mathbb{Z}$, and so is solvable. $\square$

3. (a) The map $V \times V \to \wedge^2 V$ that sends (v, w) to $T(v) \wedge T(w)$ is bilinear and alternating, and so the map exists by the universal property of $\wedge^2 V$.

(b) Choose a basis $v_1, \dots, v_n$ for V with respect to which the matrix of T is upper triangular: call the diagonal entries $\lambda_1, \dots, \lambda_n$. Then $\mathrm{tr}(T) = \sum_j \lambda_j$, and $\mathrm{tr}(T^2) = \sum_j \lambda_j^2$, since the λ_j^2 are the diagonal entries of T^2. A matrix for $\wedge^2(T)$ with respect to the basis $v_i \wedge v_j$, $i \leq j$ is upper triangular with diagonal entries that are the products $\lambda_i \lambda_j$. Their sum is therefore $(1/2)\big(\mathrm{tr}(T)^2 - \mathrm{tr}(T^2)\big)$.

4. (a), (b) The minimal polynomial of M is $x^p - 1$, which is also the characteristic polynomial. The matrix is cyclic, and so it is already in rational canonical form. If the

characteristic is not p, the roots of $x^p - 1$ are distinct, and the Jordan form will be diagonal with each root occurring once on the diagonal. If the characteristic is p, the Jordan form will have a single block, with all entries one on the main diagonal, and all entries one on the diagonal just below (or just above, depending on whether one uses lower triangular or upper triangular Jordan form) the main diagonal.

(c) Each of $f = x^2 + x + 1$ and $g = x^3 + x^2 + 1$ is irreducible, since otherwise there would be a linear factor and 0 or 1 would be a root. The corresponding $F[x]$-module will have the form $\left(F[x]/(x^2 + x + 1)\right)^{\oplus r} \oplus \left(F[x]/(x^3 + x^2 + 1)\right)^{\oplus s}$ where we may take V_1 to be $\left(F[x]/(x^2 + x + 1)\right)^{\oplus r}$, the kernel of $S^2 + S + 1$ (or the annihilator of $x^2 + x + 1$) and V_2 to be $\left(F[x]/(x^3 + x^2 + 1)\right)^{\oplus s}$, the annihilator of $S^3 + S^2 + 1$. If one writes $1 = a(S)(S^2 + S + 1) + b(S)(S^3 + S^2 + 1)$ for polynomials a and b (which one can do using the Euclidean algorithm) then the linear transformation that is the identity on V_1 and 0 on V_2 can be obtained as $b(S)(S^3 + S^2 + 1)$, while the linear transformation that is 0 on V_1 and the identity on V_2 can be obtained as $a(S)(S^2 + S + 1)$. The component matrices of S can then be obtained by multiplying these respective maps by S.

The Euclidean algorithm goes as follows:

$x^3 + x^2 + 1 = x(x^2 + x + 1) + (x + 1)$

$x^2 + x + 1 = x(x + 1) + 1.$

Working backwards, $1 = f + x(x + 1) = f + x(g - xf) = (x^2 + 1)f + xg$. Thus, we may take $a(S) = S^2 + 1$ and $b(S) = S$.

5. A finite p-group G is nilpotent since, if G is non-trivial, its center is non-trivial (if G is non-trivial, every conjugacy class has order a power of p, and hence there must be a class, besides that of the identity with just one element). The center of a product G of finite p-groups, if G is non-trivial, is therefore non-trivial, and it follows by induction on the order that such a group is nilpotent. $\square$

For the converse, we give two arguments. Assume the finite group is nilpotent. It suffices to show that there is just one Sylow p-subgroup for each prime p dividing the order: these are then normal, say $N_1, \cdots, N_h$. Given disjoint normal subgroups N, N', NN' is normal and isomorphic with $N \times N'$. Thus, if all Sylow subgroups are normal, $N_1 \cdots N_h \cong N_1 \times \cdots \times N_h$ is a normal subgroup, and has the same order as the original group. To see that there is just one Sylow p-subgroup, choose an element z of prime order q in the center, and let H be the subgroup generated by z. Then G/H is nilpotent. By induction on the order it has only one Sylow q-subgroup. Since z must be in every Sylow q-subgroup, there is also only one in G. Finally, suppose that G/H has only one Sylow p-subgroup for some $q \neq p$, but that G has two such subgroups, P and P'. Then both have the same image in G/H, so we can find an element $u \in P$ and an element $u' \in P'$ such that $u \neq u'$ but such that u and u' have the same image mod H. Then $u' = uz^j$ for $j < p$. Since u has order p^k, $k \geq 1$, z^j has order q, and they commute, this is a contradiction: u' will have order $p^j q$. $\square$ Alternatively, the normalizer of a Sylow p-subgroup of a finite group is self-normalizing, by a standard theorem, and therefore must be the whole group, since every proper subgroup H of a nilpotent group is a proper subgroup of its normalizer, again by a standard theorem. $\square$