Qualifying Review Examination: Algebra
January 10, 2004

Solutions

Explain all of your answers. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{C}$ are the integers, rationals, and complex numbers, respectively.

Morning

1. Describe the possible Jordan forms for a matrix over $\mathbb{C}$ whose characteristic polynomial is $x^5-2x^4+x^3 = x^3(x-1)^2$. What is the trace of such a matrix? What is the determinant? Can such a matrix be nilpotent?

Solution. The possible Jordan blocks corresponding to any one eigenvalue λ of multiplicity k correspond bijectively with the various ways to write k as a sum of positive integers, with the order not mattering. The eigenvalue 1 has multiplicity 2, and 2 can be written as 2 or $1+1$, while the eigenvalue 0 has multiplicity 3, and 3 be written as 3, $2+1$, or $1+1+1$. Thus, there are $2 \cdot 3 = 6$ Jordan forms possible, shown below. The trace is the sum of the eigenvalues, which is 2, and the determinant is $(-1)^n$ times the product of the eigenvalues, with $n = 5$, which is 0. The matrix cannot be nilpotent: not all eigenvalues are 0.

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

(This is upper triangular Jordan form: some authors use lower triangular. Jordan form is unique except for the order of the blocks.)

2. For which values of the real number x is the real symmetric matrix

$$\begin{pmatrix} 1 & 4 & 5 \\ 4 & 18 & 24 \\ 5 & 24 & x \end{pmatrix}$$

positive definite? Describe the possibilities for the rank and signature of this matrix as x varies. (There are three cases.)

Solution. We do not change the equivalence class of the matrix M if we perform a row operation **and** the corresponding column operation (the new matrix has the form $A^{\mathrm{tr}}MA$, A invertible): the eigenvalues change, but the rank and signature do not. Subtract 4 times the first row from the second and five times the first row from the third and do likewise for columns. This gives first $\begin{pmatrix} 1 & 4 & 5 \\ 0 & 2 & 4 \\ 0 & 4 & x-25 \end{pmatrix}$ and then $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \\ 0 & 4 & x-25 \end{pmatrix}$. Now subtract twice the second row from the third and twice the second column from the third to get $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & x-33 \end{pmatrix}$. The matrix is positive definite iff $x > 33$. For $x > 33$ the rank is 3 and the signature is $(3, 0, 0)$ or $3 - 0 = 3$. For $x = 33$ the rank is 2, and the signature is $(2, 0, 1)$ or $2 + 0 = 2$. For $x < 33$ the rank is 3 and the signature is $(2, 1, 0)$ or $2 - 1 = 1$. (When the numbers of positive, negative and zero entries on the diagonal are p, q, and r, respectively, the rank is $p + q$, while the signature is (p, q, r) according to some authors and $p - q$ according to others.)

3. Let L be the splitting field of $x^5 - 2$ over $\mathbb{Q}$. Let G be the Galois group of L over $\mathbb{Q}$.

(a) Explain why L contains a splitting field K for $x^5 - 1$ over $\mathbb{Q}$.

(b) What are the degrees of K and L over $\mathbb{Q}$? What is the degree of L over K? What is the Galois group H of $\mathbb{Q}$?

(c) Explain why there is a natural homomorphism ϕ of G onto H whose kernel is the Galois group of L over K.

(d) Show that the restriction of ϕ to a Sylow 2-subgroup P of G maps P isomorphically onto H.

(e) How many subfields of degree 4 over $\mathbb{Q}$ does L have? How many of degree 5?

Solution. (a) Let α be the real fifth root of two, and let θ be a primitive fifth root of unity. Then $K = \mathbb{Q}[\theta]$ while $L = \mathbb{Q}[\alpha, \alpha\theta, \alpha\theta^2, \alpha\theta^3, \alpha\theta^4]$: the elements listed are the roots of $x^5 - 2$. Since $\theta = \alpha\theta/\alpha$, we have that $K \subseteq L$.

(b) Since $\Phi(5) = 4$ (Euler phi function), K, which is the splitting field of $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$ has degree 4 over the over $\mathbb{Q}$, by a standard theorem. Its Galois group is the multiplicative group of $\mathbb{Z}/5Z$, which is cyclic of order 4. By Eisenstein's criterion, $x^5 - 2$ is irreducible over $\mathbb{Q}$, and so α has degree 5 over $\mathbb{Q}$. The degree of L over $\mathbb{Q}$ is therefore divisible by both 5 and 4, and so is a multiple of 20. On the other hand, since $L = \mathbb{Q}[\theta][\alpha]$ it cannot be more than $4 \cdot 5 = 20$. Thus, $[L : \mathbb{Q}] = 20$. Then $[L : K] = [L : \mathbb{Q}]/[K : \mathbb{Q}] = 20/4 = 5$.

(c) Since K is normal over $\mathbb{Q}$, any automorphism of L maps K into itself. This gives the homomorphism of Galois groups. It is onto because an automorphism of a normal extension field extends to any larger normal extension. Clearly, a $\mathbb{Q}$-automorphism of L is in the kernel if and only if it is the identity on K, which means that the kernel is precisely the set of K-automorphisms of L.

(d) Since G has order 20 and H has order 4, the kernel has order 5, and must be the unique Sylow 5-subgroup. A Sylow 2-subgroup P has order 4, and is disjoint from the kernel, so that its image in H also has order 4, and must be all of H.

(e) Subfields of degree 4 correspond to subgroups of G of index 4: any such is a Sylow 5-subgroup, and there is only one (namely, K), since the number $|4$ and is $\equiv 1 \bmod 5$. Subfields of degree 5 correspond to subgroups of index 5, and these are Sylow 2-subgroups. The number of these must divide 5 and be congruent to 1 mod 2. Thus, the number is either 1 or 5. But $\mathbb{Q}[\alpha\theta^i]$ has degree 5, since $x^5 - 2$ is irreducible, and these are not all the same (e.g., α is real, while $\alpha\theta$ is not). This, there are 5 subfields of degree 5.

4. A group G of order $81 = 3^4$ acts on a set S. Prove the following statements or give counter-examples:

(a) If $|S| = 10$, some element of S must be fixed by the entire group.

(b) If $|S| = 9$ and G acts faithfully, then G acts transitively.

Solution. (a) This is true. The length of an orbit of the action is the index of the stabilizer of an element in the orbit, and so must divide 81. Thus, there must be fixed points, or else 10 would be a sum of multiples of 3.

(b) This is also true. The faithful action of G on the set of 9 elements embeds G into S_9. The only multiples of 3 that are factors in $9! = 9\cdot8\cdot7\cdot6\cdot5\cdot4\cdot3\cdot2\cdot1$ are 3, 6, and 9, which means that a Sylow 3-subgroup has order $3 \cdot 3 \cdot 9 = 81$, so $G \cong$ a Sylow 3-subgroup of S_9. Since every element of order p^k, p prime, is in some Sylow p-subgroup, and these are all conjugate, we have that the image of G contains a 9-cycle, which implies transitivity. Alternate: if the action is not transitive, the orbit lengths are integers $a_i > 0$ whose sum is 9, and none of which is 9. At most 3 of these integers can be multiples of 3 (or else the sum will be too large), and none can be divisible by 3^k, $k > 1$. Thus, no 3-group of order $> 3^3$ can be embedded in the product of the S_{a_i}.

5. Let S be the polynomial ring $\mathbb{Q}[x]$ in one variable over $\mathbb{Q}$. Let $F = S^3$ be the free S-module on three generators. Let M be the submodule of F spanned by the elements $(1, x, x^2)$ and $(x, x^2 + x, x^3 + 1)$. The quotient module F/M is isomorphic with a direct sum $S/f_1S \oplus \cdots \oplus S/f_nS$: determine explicitly a valid choice of $f_1, \ldots, f_n$.

Solution. F/M is the quotient of S^3 by the row space of the matrix $\begin{pmatrix} 1 & x & x^2 \\ x & x^2+x & x^3+1 \end{pmatrix}$ (One may also work with the column space of the transpose of this matrix.) The quotient is unaffected by row and column operations on the matrix. Subtract x times the first column from the second and x^2 times the first column from the third to get $\begin{pmatrix} 1 & 0 & 0 \\ 1 & x & 1 \end{pmatrix}$ and subtract the the first row from the second and x times the third column from the second to get $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. (One may also switch the second and third columns.) The quotient module is therefore obtained from S^3 by killing two of the three standard free basis elements, and so the quotient is simply $\cong S$. One may take $n = 1$ and $f_1 = 0$.

Afternoon

1. Determine up to isomorphism all groups G with identity 1 such that G is generated by x and y satisfying $x^5 = y^{11} = 1$, $xy = y^4x$, while $x \neq 1$ and $y \neq 1$. Does y generate a normal subgroup in G? Does x? What is $|G|$? Show that G is a non-trivial semi-direct product.

Solution. The order d of y is 11, since $d\,|\,!!$ and 11 $d \neq 1$, and, similarly that x has order 5. Since $xy = y^4x$, we have $xyx^{-1} = y^4$. Thus, y generates a normal subgroup N of order 11, and x generates a subgroup H of order 5. Since these generate G, $G = HN$ is the semidirect product of these two. If we think of N as $\mathbb{Z}/11Z$ and H as $\mathbb{Z}/5Z$, the action of H on N by conjugation corresponds to multiplication by 4 on $Z/11Z$: for there to exist such a semidirect product, we need that $4^5 \equiv 1 \bmod 11$, which is true by Fermat's little theorem since $4^5 = 2^{10}$. Then y generates a normal subgroup, as already indicated, but x does not (or the product would be direct). $|G| = 55$.

2. Let A and B be abelian groups written additively. Let $\mathrm{Hom}\,(A,\,B)$ denote the set of group homomorphisms from A to B, regarded as an additive abelian group under the usual operation defined by the rule $(f+g)(a) = f(a) + g(a)$ for all $a \in A$.
(a) Let $m,\, n \in \mathbb{Z} - \{0\}$ have greatest common divisor d. Prove that $\mathrm{Hom}\,(\mathbb{Z}/m\mathbb{Z},\, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$.

(b) Show that $\mathrm{Hom}\,(A \oplus A',\, B) \cong \mathrm{Hom}\,(A,\, B) \oplus \mathrm{Hom}\,(A',\, B)$ and $\mathrm{Hom}\,(A, B \oplus B') \cong \mathrm{Hom}\,(A, B) \oplus \mathrm{Hom}\,(A,\, B')$ for all abelian groups $A,\, A',\, B,\, B'$.

(c) Let A and B be finite abelian groups. Prove that $\mathrm{Hom}\,(A,\, B) \cong \mathrm{Hom}\,(B,\, A)$.

(d) Is the conclusion of 2(c) true if A and B are finitely generated but not necessarily finite? Either prove that it is true, or give a counter-example.

Solution. (a) Each element of $H = \mathrm{Hom}\,(\mathbb{Z}/mZ,\, \mathbb{Z}/nZ)$ is uniquely determined by where the image of $[1]_m$, the generator maps, and it must map to an element $[a]_n \in \mathbb{Z}/nZ$ that is killed by m. Thus, there is one such homomorphism for all a, $0 \leq a < n$ such that $n|(ma)$. Let $m = m'd$ and $n = n'd$ where $\mathrm{GCD}(m', n') = 1$. Then $(n'd)|(m'da)$ iff $n'|(m'a)$ iff $n'|a$, so that the elements of H correspond bijectively with the multiples of n' mod dn', which is a cyclic group of order d.

(b) Given an element of $h \in \mathrm{Hom}\,(A \oplus A',\, B)$ we obtain elements $f_h \in \mathrm{Hom}\,(A, B)$ and $g_h \in \mathrm{Hom}\,(A',\, B)$ by restriction, and we map h to $f_h \oplus g_h$. In the other direction, given an element $k \in \mathrm{Hom}\,(A,\, B) \oplus \mathrm{Hom}\,(A', B)$, it has the form $f \oplus g$, and we define $h \in \mathrm{Hom}\,(A \oplus A', B)$ by the rule $h(a \oplus a') = f(a) + g(a')$. It is straightforward to check that these maps are group homomorphisms and mutually inverse.

Given $u \in \mathrm{Hom}\,(A, B \oplus B')$ we define maps $v_u : A \to B$ and $w_u : A \to B'$ be composing with the surjections $B \oplus B' \to B$ and $B \oplus B' \to B'$, respectively, where the first sends $b \oplus b'$ to b and the second sends $b \oplus b'$ to b'. We map w to $w_u \oplus w_v$. Given $v : A \to B'$ and

$w : A \to B'$, we map $u \oplus v$ to w, where $w(a) = u(a) \oplus v(a)$. It is straightforward to check that the these maps are group homomorphisms and mutually inverse.

(c) Since Hom commutes with finite direct sum in either variable, by part (b) and a completely straightforward induction, and since each of A and B is a finite direct sum of finite cyclic groups, we may reduce to the case where $A = \mathbb{Z}/m\mathbb{Z}$ and $B = \mathbb{Z}/n\mathbb{Z}$. The result now follows from part (a) and the fact the GCD of two integers does not depend on their order.

(d) This is false if $A = \mathbb{Z}$ and $B = \mathbb{Z}/n\mathbb{Z}$ for some integer $n > 1$, for then Hom $(A, B) \cong \mathbb{Z}/n\mathbb{Z}$ while Hom $(B, A) = 0$.

3. (a) Let V and W be finite-dimensional vector spaces over a field K. Let $v, v' \in V$ be nonzero and $w, w' \in W$ be nonzero. Show that $v \otimes w = v' \otimes w'$ in $V \otimes_K W$ if and only if there are scalars $a, b \in K$ such that $v' = av$, $w' = bw$ and $ab = 1$.

(b) Let K be a finite field with q elements. Give an explicit formula for the number nonzero of vectors in $K^2 \otimes_K K^3$ that have the form $v \otimes w$ for some $v \in K^2$ and $w \in K^3$.

Solution. (a) The condition is sufficient, since $v' \otimes w' = av \otimes bw = (ab)v \otimes w = v \otimes w$. Now suppose that v and v' are independent. We give two proofs that this leads to a contradiction.

First proof. Choose a linear functional on V, say h, so that $h(v) = 0$, $h(v') \neq 0$. Then we have a bilinear map $f : V \times W \to W$ by $(x, y) \mapsto h(x)w$. The corresponding linear map $V \otimes W \to W$ takes $v \otimes w$ to 0 but is nonzero on $v' \otimes w'$, a contradiction. $\square$

Second proof. If v and v' are independent, extend them to a basis for $v_1, \ldots, v_n$ for V with $v_1 = v$, $v_2 = v'$. Extend $w = w_1$ to a basis $w_1, \ldots, w_m$ for W with $w_2 = w'$ if it is independent of V: if not, $w' = c'w_1$, $c' \neq 0$. Then $v \otimes w = v_1 \otimes w_1$ and $v' \otimes w'$, which is either $v_2 \otimes w_2$ or $c'(v_2 \otimes w_1)$, are not equal, since, by a standard theorem, the $v_i \otimes w_j$ are a basis for $V \otimes W$. $\square$

We now finish the argument. We must have that w and w' are dependent similarly, and so we have $v' = av$ and $w' = bw$ for suitable $a, b \in K - \{0\}$. Then $v \otimes w = (av) \otimes (bw) = ab(v \otimes w)$, and so $(ab - 1)(v \otimes w) = 0$. Since v and w are nonzero, $ab - 1 = 0$ and the result follows. $\square$

(b) These come from choosing $v \in K^2 - \{0\}$ and $w \in K^3 - \{0\}$. This gives $(p^2 - 1)(p^3 - 1)$ choices for the pair (v, w), but some of these give the same result for $v \otimes w$: by part (a), each nonzero $v \otimes w$ occurs $p - 1$ times, from the pairs $(cv, c^{-1}w)$ as c varies in $K - \{0\}$. Thus, there are $\big((p^2 - 1)(p^3 - 1)\big)/(p - 1)$ such vectors, or $(p + 1)(p^3 - 1) = p^4 + p^3 - p - 1$.

4. (a) Show that for every prime integer $p \geq 2$, the polynomial $f(x) = x^5 - 2px + p$ is irreducible over $\mathbb{Q}$.

(b) Let $r = (2p/5)^{1/4} > 0$. Show using basic calculus that $f(x)$ is increasing on $(-\infty, -r)$, decreasing on $(-r, r)$, and increasing on $(r, +\infty)$. Since $f(-1) > 0$ and $f(1) < 0$, conclude that f has precisely 3 real roots.

(c) Prove that the Galois group of f over $\mathbb{Q}$ is isomorphic with S_5.

(d) What does this imply about whether f can be solved by radicals? Explain your answer.

Solution. (a) The polynomial is irreducible by Eisenstein's criterion: all coefficients except the first are divisible by p, while the constant term is not divisible by p^2.

(b) $f'(x) = 5x^4 - 2p$ whose roots are $-r$ and r. The derivative can only change sign at $-r$ and r. The derivative is positive for $|x| \gg 0$, and so must be positive if $x < r$ and if $x > r$. It is negative at $x = 0$, and so is negative on $(-r, r)$. It follows that $f(x)$ is increasing for $x < -r$, decreasing for $-r < x < r$, and increasing for $x > r$. That f has exactly three real roots is now clear.

(c) The Galois group G embeds in the permutations of the 5 roots of f, i.e., $G \hookrightarrow S_5$. Since f is irreducible, adjoining one root gives a degree 5 extension, and so $5 \mid |G|$. Thus, G contains a 5-cycle (elements of S_5 of order 5 are all 5-cycles). Since there are precisely 3 real roots there are 2 conjugate complex roots, and complex conjugation gives an automorphism that interchanges them. But a subgroup of S_5 that contains a 5-cycle and a transposition must be all of S_5. (More generally, any p-cycle and any 2-cycle generate S_p, p prime.)

(d) Since S_5, which contains the noncommutative simple group A_5, is not solvable, f cannot be solved by radicals.

5. Let p be a prime number and G a finite p-group. Let $Z(G)$ denote its center (the set of elements of G that commute with every element of G).

(a) Show that if $K \neq \{1\}$ is a normal subgroup of G, then $K \cap Z(G) \neq \{1\}$. (Partial credit will be given for doing the standard case where $K = G$.)

(b) Let M be a maximal subgroup of G (that is, M is a proper subgroup with no subgroup strictly between M and G). Show that M is normal in G of index p. (Hint: condition on whether or not $M \cap Z(G) = \{1\}$.)

Solution. (a) Since K is normal, it is a union of conjugacy classes C_i under conjugation by elements of G. Each $|C_i| \mid |G|$, and so $|C_i|$ is a power of p. The class of 1 contains just 1 element. Since $|K| = p^k$ is a power of p, $k > 0$, we have $p^k = \sum_i |C_i|$, and so there must be other classes with just one element: otherwise, $p^k \equiv 1 \bmod p$. $\square$

(b) We use induction on $|G|$ (the case $|G| = p$ is obvious). If $M \cap Z(G) = \{1\}$, then since $Z(G)$ is normal and non-trivial, these two generate G, for M is maximal, and so G is the semidirect product of these. But $Z(G)$ acts trivially on M, which then implies that $G \cong M \times Z(G)$. Then M is normal, and cannot be maximal unless $|Z(G)| = p$, or else we can enlarge by adjoining an element of $Z(G)$ which has order p. We may therefore assume that $Z(G) \cap M = N$ is non-trivial. But then N is normal in G, and we may apply the induction hypothesis to M/N, which will be maximal in G/N, to conclude that it is normal of index p. $\square$