VIGRE Algebra QR Review, November 25, 2002

Summary of Session

1. Prove that an $n \times n$ matrix A over the real number numbers $\mathbb{R}$ has rank $\leq r$, where $1 \leq r \leq n$, if and only if A is the sum of r or fewer $n \times n$ matrices of rank at most 1.

Solution. The "if" direction follows from the fact, discussed in last week's summary of session, that the rank of the sum of two matrices is at most the sum of the ranks. For the other direction, it is convenient to think of the matrices as representing maps between two n-dimensional vector spaces that are not necessarily the same. Then one can change bases in both spaces so that the matrix is diagonal, with r entries equal to 1 on the diagonal, where r is the rank, and the other diagonal entries 0. It is now clear that the matrix is the sum of r diagonal matrices, each with a single 1 on the diagonal and all other entries equal to 0, and these clearly have rank one.

2. Let B_1 and B_2 be real symmetric bilinear forms on finite-dimensional real vector spaces V_1 and V_2 respectively. Show that there is a bilinear form B on $V_1 \otimes_{\mathbb{R}} V_2$ such that $B(u_1 \otimes u_2, v_1 \otimes v_2) = B_1(u_1, v_1)B_2(u_2, v_2)$. Show that B is symmetric. Express the rank of B in terms of the ranks of B_1 and B_2, and the signature (p, q, n) of B in terms of the signatures (p_1, q_1, n_1) and (p_2, q_2, n_2) of B_1 and B_2.

Solution. Each B_i gives a linear map $L_i : V_i \otimes_{\mathbb{R}} V_i \to \mathbb{R}$, by the universal property of tensor products, and we have a universal bilinear map $(V_1 \otimes_{\mathbb{R}} V_2) \times (V_1 \otimes_{\mathbb{R}} V_2) \to (V_1 \otimes_{\mathbb{R}} V_2) \otimes_{\mathbb{R}} (V_1 \otimes_{\mathbb{R}} V_2)$. From the latter space we have a map

$$(V_1 \otimes_{\mathbb{R}} V_2) \otimes_{\mathbb{R}} (V_1 \otimes_{\mathbb{R}} V_2) \cong (V_1 \otimes_{\mathbb{R}} V_1) \otimes_{\mathbb{R}} (V_2 \otimes_{\mathbb{R}} V_2),$$

by the commutativity and associativity of $\otimes$, and we have a map (constructed in the solution of #1. last week) $L_1 \otimes L_2 : (V_1 \otimes_{\mathbb{R}} V_1) \otimes_{\mathbb{R}} (V_2 \otimes_{\mathbb{R}} V_2) \to \mathbb{R} \otimes_{\mathbb{R}} \mathbb{R} \cong \mathbb{R}$. Composing gives a bilinear map $B : (V_1 \otimes_{\mathbb{R}} V_2) \times (V_1 \otimes_{\mathbb{R}} V_2) \to \mathbb{R}$, and it is straightforward to check that the definitions yield that $B(u_1 \otimes u_2, v_1 \otimes v_2) = B_1(u_1, v_1)B_2(u_2, v_2)$ for all $u_1, v_1 \in V_1$ and all $u_2, v_2 \in V_2$. It suffices to check symmetry on pairs of vectors from a spanning set for $V_1 \otimes_R V_2$. Symmetry follows from the formula just given, because $B(v_1 \otimes v_2, u_1 \otimes u_2) = B_1(v_1, u_1)B_2(v_2, u_2) = B_1(u_1, v_1)B_2(u_2, v_2)$ since both of the B_i are symmetric. Choose bases $e_1, \ldots, e_m$ and $f_1, \ldots, f_n$ for V_1 and V_2, respectively, such that the matrices of B_1 and B_2 are diagonal. Let $a_i = B_1(e_i, e_i)$ and $b_j = B_2(f_j, f_j)$. It is easy to check that the value of $B(e_i \otimes f_j, e_{i'} \otimes f_{j'})$, which is $B_1(e_i, e_{i'})B_2(f_j, f_{j'})$, is 0 unless $i = i'$ and $j = j'$, and the value in that case is $a_i b_j$. The rank of B is the number of nonzero $a_i b_j$, which is the product of the number of nonzero a_i and the number of nonzero b_j, i.e., the product of the ranks of B_1 and B_2.

The value of p is the number of positive $a_i b_j$: the value is positive precisely when a_i and b_j are both positive or both negative, and so $p = p_1 p_2 + q_1 q_2$. The value of $a_i b_j$ is negative when one is positive and the other is negative, and so $q = p_1 q_2 + q_1 p_2$. Finally, $a_i b_j$ is zero precisely when either of them is 0, and so $r = p_1 r_2 + q_1 r_2 + r_1 r_2 + r_1 p_2 + r_1 q_2$.

3. Let G be the set of $n \times n$ matrices over the complex numbers obtained from the $n \times n$ identity matrix by a permutation of columns.

(a) Prove that G is a subgroup of $GL(n)$ isomorphic to S_n.

Let G act on the set M_n of $n \times n$ complex matrices by left multiplication.

(b) Let $n = 3$. What is the cardinality of the orbit of the 3×3 matrix $A = (a_{ij})$ such that $a_{11} = a_{21} = a_{32} = a_{33} = 1$ and all other entries are 0? What is the cardinality of the stabilizer of A in G?

(c) Give a necessary and sufficient condition for the orbit of a matrix B under G to have cardinality $n!$. Is this condition always satisfied when B is invertible? Can it ever be satisfied if one of the rows of the matrix is 0?

Solution. (a) The set G may also be described as the set of matrices with precisely n nonzero entries, no two in the same row or column, in which the nonzero entries are all 1, and this is the same as the set of matrices whose rows are a permutation of the rows of the identity matrix. Let e_i denote the i th row of the identity matrix. Then $e_i M$ is the i th row of M. Hence, if p is a permutation of $1, \ldots, n$, and $B(p)$ denotes the matrix whose rows are $e_{p(1)}, \ldots, e_{p(n)}$, then $B(p)M$ is the matrix whose i th row is the $p(i)$ th row of M, and so $B(q)B(p)$ has as its i th row the $q(i)$ th row of $B(p)$, i.e., the $p(q(i))$ th row of the identity matrix, and so $B(q)B(p) = B(pq)$, which shows that the map sending $p \to B(p^{-1})$ is an isomorphism of S_n with this group of matrices. (These matrices are clearly orthogonal: the inverse is the transpose, and so $B(p^{-1})$ is also the matrix whose i th column is the $p(i)$ th column of the identity matrix for each i.)

(b) The orbit of a matrix B under the action of G is clearly the set of all matrices whose rows are a permutation of the rows of B. Thus, the orbit of the given matrix has cardinality 3, and so the cardinality of the stabilizer is $3!/3 = 2$.

(c) The condition is obviously that the rows of B be mutually distinct, and this is satisfied if B is invertible, since the rows must then be linearly independent. It can be satisfied if one of the rows is 0: take the others to be, say, $n - 1$ distinct rows of the identity matrix.

4. Find a primitive element (field generator) for $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. Show that this field is not a Galois extension of $\mathbb{Q}$, and find its Galois closure.

Solution. One can use $\gamma = \sqrt{2}\sqrt[3]{5}$ as the field generator, because $\gamma^3 = (2\sqrt{2})5 = 10\sqrt{2}$, so that $\sqrt{2} \in \mathbb{Q}(\gamma)$, and then $\sqrt[3]{5} = \gamma/\sqrt{2} \in \mathbb{Q}(\gamma)$ as well. The Galois closure is obtained by adjoining the other cube roots of 5 (it must contain all roots of $x^3 - 5$; it cannot contain these already, since the other two roots are not real numbers). The other cube roots of 5 may be written as $\sqrt[3]{5}\omega_j$ for $j = 1, 2$, where the ω_j are cube roots of unity other than 1. Since $x^3 - 1 = (x - 1)(x^2 + x + 1)$, the ω_j are the roots of $x^2 + x + 1$, i.e., $(-1 \pm \sqrt{-3})/2$. It follows that the Galois closure is $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}, \sqrt{-3})$.

5. Fix positive integers $r \leq n$ and a complex polynomial $f(x)$ of degree r. Prove that there are, up to similarity, only finitely many complex $n \times n$ matrices that have minimal polynomial f.

Give an example of a finite-dimensional complex vector space V with infinitely many linear transformations having the same minimal polynomial.

Solution. The similarity class of such a matrix is determined by, for each eigenvalue, how many of each size Jordan block occur, for that eigenvalue, in the Jordan form of the matrix. It follows at once that once a finite set that contains the eigenvalues is known, and the size of the matrix is known, there are only finitely many possibilities for the similarity class of the matrix. Since the eigenvalues of a matrix are identical with the roots of the minimal polynomial (although their multiplicities might be larger than their multiplicities in the minimal polynomial), there are only finitely many possibilities for the similarity class of a matrix once its minimal polynomial (or any nonzero polynomial that it satisfies) is known. Note that the sizes of the blocks for a given eigenvalue are also restricted to be at most its multiplicity in the minimal polynomial, but this is not needed to prove finiteness.

The 2×2 upper triangular matrices with 0 on the diagonal and a single nonzero entry in the upper right corner all have minimal polynomial x^2. This gives one example of an infinite family of linear transformation all with the same minimal polynomial. (It can be shown that any square matrix other than a scalar multiple of the identity has infinitely many conjugates, and this leads to many other examples.)

6. Find the Galois group of the splitting field of the polynomial $x^5 - 7x^4 + 3$ over the rational numbers $\mathbb{Q}$.

Solution. The Galois group $G \cong S_5$: this is similar to an earlier problem, but it is harder to show that the polynomial is irreducible in this case. The idea is to show first that the polynomial has exactly three real roots, and, hence, two conjugate complex roots. Therefore complex conjugation provides a 2-cycle when the Galois group is viewed as a subgroup of S_5 (the permutations of the roots). Second, one wants to show that the polynomial is irreducible. This implies that adjoining one root gives a field extension of degree 5, and this shows that the Galois group has order divisible by 5, and so contains an element of order 5. Thus, thought of as a subgroup of S_5, it contains a 5-cycle as well as a 2-cycle. It was shown earlier that any 5-cycle and any 2-cycle generate S_5, and so $G \cong S_5$.

For the first part note that the derivative is $5x^4 - 28x^3 = x^3(5x - 28)$, which vanishes only for $x = 0$ and $x = 28/5$. The derivative is positive for $x < 0$, negative between 0 and $28/5$, and positive again for $x > 28/5$. Thus, the function is increasing for $x > 0$, decreasing on $(0, 28/5)$, and increasing for $x > 28/5$. Since the value at 0 is $3 > 0$, the function has exactly one root in the interval $(-\infty, 0]$. Since the value at 1 is -3, the function has exactly one root in the interval $(0, 28/5]$, which is actually in the interval $(0, 1)$. Since the function is negative at $28/5$ (the value must be smaller than the value at 1) and is eventually positive, the function has exactly one root in the interval $(28/5, +\infty)$. This shows that there are exactly three real roots.

It remains to show that the polynomial is irreducible. It is easy to check that ± 1 and ± 3 are not roots, so that if it factors it must factor into the product of two monic polynomials, one of degree 2 and the other of degree 3. If this happens, it will happen mod p for every prime integer p. Therefore, it suffices to show that there is no such factorization mod 7. Mod 7, the polynomial becomes $x^5 + 3 = x^5 - 4$. Now $2^5 = 4$ mod 7, so that there is a root, and $x^5 - 4 = (x-2)(\sum_{k=0}^{4}(2x)^k)$. To complete the proof, it suffices to show that $\sum_{k=0}^{4}(2x)^k$ is irreducible mod 7. Let $z = 2x$. It is equivalent to show that $\sum_{k=0}^{4} z^k = z^4 + z^3 + z^2 + z + 1$ is irreducible mod 7. (This is the equation satisfied by the fifth roots of unity, other than one.) Since the multiplicative group of $\mathbb{Z}_7$ has order 6, there are no fifth roots of unity except 1 in the field. If the polynomial factored into two quadratics we could introduce a non-trivial fifth root of unity in a field which is a quadratic extension of $\mathbb{Z}_7$, which means that it would have 49 elements. But then the order of the multiplicative group is $49 - 1$, which is not divisible by 5, a contradiction. Thus, $z^4 + z^3 + z^2 + z + 1$ is irreducible over $\mathbb{Z}_7$, as required.

7. (a) Prove that every group of order $77 = 7 \cdot 11$ is abelian.

(b) Let G be a group of order $231 = 3 \cdot 7 \cdot 11$. Prove that any subgroup H of G of order 11 is contained in the center of G.

Solution. (a) The number of 11-Sylow subgroups divides 7 and is $\equiv 1 \mod 11$: hence, there is only one. Given an element of order 7 acting on this group by conjugation, the action must be trivial, since the automorphism group of Z_{11} has order $11 - 1$ and is not divisible by 7. Thus, a group of order 77 is abelian.

(b) Similarly, the number of 11-Sylow subgroups of a group of order $11 \cdot 21$ must divide $3 \cdot 7$ and be $\equiv 1 \mod 11$. It follows that there is only one. Since neither 7 nor 3 divides $11-1$, elements of order 3 and 7 centralize any element of order 11 as above, and the order of the centralizer must be divisible by $3 \cdot 7 \cdot 11$, which $\Rightarrow$ the 11-Sylow subgroup is in the center of the group.

8. Let $R = k[x]$ be the polynomial ring in one variable over a field k. Recall that a proper ideal I of R is *prime* if whenever $f,\, g \in R$ and $fg \in I$, either $f \in I$ or $g \in I$.

(a) Show that the set of nonzero prime ideals of R is in bijective correspondence with the set of irreducible monic polynomials in R.

(b) Find the prime ideals that contain both $x^5 - x^3$ and $x^4 - 1$. Describe these prime ideals by giving generators for each.

Solution. (a) The polynomial ring is a principal ideal domain, and every nonzero ideal is generated by the monic polynomial h of smallest degree that it contains (which is unique): given any nonzero element of the ideal, it must be divisible by that monic polynomial (or else the remainder would be monic of smaller degree). If it has the same degree as h, it must be a scalar times h, by a degree argument, which shows that the monic generator is unique. Thus, there is a bijection between nonzero ideals and monic polynomials. There is a bijection between proper nonzero ideals and monic polynomials of positive degree.

It remains to show that h of positive degree is irreducible if and only if hR is prime. If $h = fg$ is a factorization into polynomials of smaller degree then $fg \in hR$ but neither f nor g is in hR. Thus, if h is reducible I is not prime, i.e., if hR is prime then h is irreducible. It remains only to show that if h is irreducible, then hR is prime. This is quite standard: it follows from the fact that R is a UFD. Without assuming this, note that if $h|(fg)$ but h does not divide f, then the ideal generated by h and f must be the whole ring: otherwise, its unique monic generator must divide h and would be different from h and 1, contradicting the irreducibility. Thus, there are polynomials $u,\, v$ such that $uf + vh = 1$. The $g = g(uf + vh) = u(fg) + gvh$. Since $h|(fg)$, it divides both terms, which implies that it divides g, as required. (One can say a lot less for this problem, quoting standard theorems — it was not clear to me from the wording what the examiners wanted. In that situation it is safest to respond maximally rather than minimally.)

(b) Since $x^5 - x^3 = x^3(x^2-1) = x^3(x-1)(x+1)$, the primes that contain this polynomial are xR, $(x-1)R$, and $(x+1)R$. The first of these does not contain $x^4 - 1$, but the latter two, $(x-1)R$, and $(x+1)R$ both do. If the characteristic of the field is not 2, this appears to be all that one needs to say. If the characteristic is 2, it may be worth remarking that $x - 1 = x + 1$, so that there is only one prime that contains the given polynomials.

9. Let G and H be non-abelian simple groups. Prove that every non-trivial normal subgroup N of $G \times H$ must contain G or contain H.

Solution. Suppose N is normal in $G \times H$ but contains neither. Its projection on H is easily seen to be a normal subgroup of H, and if the projection is the trivial group we see that N is contained in $G \times \{1\}$, which means that N is trivial, since it cannot contain G. Thus, N must project onto H. Since H is not abelian, we can pick $u, h \in H$, $g \in G$ such that $h' = uhu^{-1} \neq h$, while $(g, h) \in N$. Conjugating $(g, h) \in N$ by $(1, u)$ gives $(g, h') \in N$, with $h' \neq h$. Then $(1, h(h')^{-1}) \in N$, and so $N \cap H$ is a non-trivial normal subgroup of H and must be all of H. [Alternate solution. Deny the conclusion. Then $N \cap G = \{1\} = N \cap H$. Since all these are normal, $[N, G] = \{1\} = [N, H]$. This means N is in the center. But $Z(G \times H) = Z(G) \times Z(H) = \{1\} \times \{1\}$, so $N = \{1\}$.]

10. Let k be a field and let $k[x]$ be the polynomial algebra in one variable over k. Let D be the k-subalgebra of the k-algebra $\mathrm{End}_k k[x]$ of all k-vector space endomorphisms of $k[x]$ generated by the "derivative operator" d (the k-linear map defined by $d(x^n) = nx^{n-1}$ for all non-negative integers n) and the operator $\mathbf{x}$ (the linear operator defined by $\mathbf{x}(f) = xf$ for all polynomials f). Note that there is a natural D-module structure on $k[x]$. (Recall that a module is *simple* if it has no proper non-trivial submodules.)

(a) Is D a commutative ring? Prove it or give a counterexample.

(b) Prove that if k has characteristic zero, then $k[x]$ is a simple D-module.

(c) Is $k[x]$ a simple D-module if the characteristic of k is non-zero? Prove it or give a counterexample.

Solution. (a) No. The operators $\mathbf{x} \circ d$ and $d \circ \mathbf{x}$, for example, take the values 0 and 1, respectively, on the vector 1. (If one uses the vector x^n one gets nx^n and $(n+1)x^n$, respectively.)

(b) Note that D contains $k[x]$ (interpreted as linear endomorphisms of $k[x]$ by multiplication) since this is the k-algebra generated by $\mathbf{x}$. Let $f(x) = ax^n + \cdots$ be a polynomial of degree n. Repeated application of the action of d to f produces, after n steps, the scalar $an!$. Since k is in D, we can multiply by $\frac{1}{an!}$ to see that the D submodule generated by f contains 1. Thus the submodule generated by f is all of $k[x]$. As f was arbitrary, the module is simple.

(c) No. Consider the ideal of $k[x]$ generated by x^p. This is a non-trivial proper D-submodule of $k[x]$. Since $d(x^p) = 0$, it is easy to see that D sends every element x^n where $n \geq p$ (hence any k-linear combination of these) back into (x^p).