VIGRE Algebra QR Review, November 18, 2002

Summary of Session

The following problems are from the list for November 18 — I am including solutions for all of these problems (not all of them were discussed in full detail). In some cases I have included variants or improvements on what was said during the session, or a generalization of the original problem. The counting problem implicit in #9. is solved in a different way here, and in greater generality.

1. Let V and W be finite-dimensional vector spaces over a field k. Construct a canonical isomorphism $\mathrm{End}_k(V)\otimes_k \mathrm{End}_k(W) \cong \mathrm{End}_k(V \otimes_k W)$. You should construct the proposed isomorphism without choosing bases, but you may wish to uses bases in the course of proving that the map you have defined is in fact an isomorphism.

Solution. In this write-up we generalize slightly. Let V' and W' be two additional finite-dimensional vector spaces. We give a canonical isomorphism $\mathrm{Hom}_k(V,V')\otimes_k\mathrm{Hom}_k(W,W')$ $\to \mathrm{Hom}_k(V \otimes_k W, V' \otimes_k W')$. The original problem is the case where $V' = V$ and $W' = W$. To give the map Θ it suffices to define a bilinear map $\mathrm{Hom}_k(V,V') \times \mathrm{Hom}_k(W,W')$ $\to \mathrm{Hom}_k(V \otimes_k W, V' \otimes_k W')$. For this we use $B(f,g) = f \otimes g$: the latter is a standard construction. It is the linear map induced by the bilinear map $b : V \times W \to V' \otimes_k W'$ that sends (v,w) to $f(v) \otimes g(w)$. (One must check the bilinearity of b, which follows from the linearity of f and g and the bilinearity of $(s,t) \mapsto s \otimes t$. One must also check the bilinearity of B, which follows from the linearity of $f(v)$ in the variable f when v is held fixed, the linearity of $g(w)$ in the variable g when w is held fixed, and the bilinearity of $(s,t) \mapsto s \otimes t$.) Let $v_1, \ldots, v_m$, $v'_1 \ldots, v'_n$, $w_1, \ldots, w_r$, and $w'_1 \ldots, w'_s$ be bases for V, V', W, and W', respectively, and let h, i, j, and k be indices running from 1 to m, n, r, and s, respectively. Let S_{hi} be the linear map $V \to V'$ that sends v_h to v'_i while killing the other v_μ. The S_{hi} are a basis for $\mathrm{Hom}_k(V,V')$ (corresponding to the basis for $n \times m$ matrices consisting of matrices with a 1 in one entry and zeros in all other entries). Let T_{jk} be the linear map $W \to W'$ sending w_j to w'_k while killing the other w_ν. The T_{jk} are a basis for $\mathrm{Hom}_k(W,W')$. Thus, the $S_{ih} \otimes T_{jk}$ are a basis for $\mathrm{Hom}_k(V,V')\otimes_k \mathrm{Hom}_k(W,W')$. Now the $v_h \otimes w_j$ are a basis for $V \otimes W$, and the $v'_i \otimes w'_k$ are a basis for $V' \otimes W'$. Let U_{hijk} be the linear map $V \otimes_k W \to V' \otimes_k W'$ that sends $v_h \otimes w_j \to v'_i \otimes w'_k$ and kills the other $v_\mu \otimes w_\nu$. It is straightforward to check that $\Theta(S_{hi} \otimes T_{jk}) = U_{hijk}$. Since one basis is carried bijectively to the other, Θ is an isomorphism.

2. Let V be an n-dimensional vector space and let $\Lambda = \bigwedge V = \bigoplus_{r=0}^{n} \bigwedge^r V$ be its exterior algebra. Show that the elements of Λ of even degree form a commutative subalgebra.

Solution. It should say, "the elements all of whose components have even degree" form a commutative subalgebra. This subalgebra is actually in the center. Closure under addition and scalar multiplication is clear, and the product of two forms of even degree has even degree: closure under multiplication follows from the distributive law. Notice that this algebra is generated by the elements $v \wedge w$ where $v, w \in V$. To show that such elements are in the center, it suffices to check that they commute with generators for $\bigwedge V$, and so it suffices to check that they commute with elements $u \in V$. But $u \wedge (v \wedge w) = (u \wedge v) \wedge w = (-v \wedge u) \wedge w = -v \wedge (u \wedge w) = -v \wedge (-w \wedge u) = (v \wedge w) \wedge u$.

3. Let V be the vector space of 3×1 complex column vectors. Consider the transformation of V defined by the matrix $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 3 & -1 & 0 \end{pmatrix}$ with respect to the standard basis e_1, e_2, e_3 (these are the columns of the identity matrix).

(a) Find the matrix of the induced linear transformation on $\bigwedge^2 V$ with respect to the basis $e_1 \wedge e_2$, $e_1 \wedge e_3$, $e_1 \wedge e_2$.

(b) Let V be a complex vector space of finite dimension n, and let $T : V \to V$ be a linear transformation of V. For a natural number d, $1 \le d \le n$, consider the naturally induced transformation $\bigwedge^d T : \bigwedge^d V \to \bigwedge^d V$. Prove that if T has rank r, then $\bigwedge^d T$ has rank $\binom{r}{d}$, where this binomial coefficient is interpreted as 0 if $d > r$.

Solution. (a) Call the transformation T. Then $\bigwedge^2 T$ maps $v \wedge w$ to $T(v) \wedge T(w)$, and so the values on $e_1 \wedge e_2$, $e_1 \wedge e_3$, and $e_2 \wedge e_3$ are $(e_1 + 3e_3) \wedge (2e_2 - e_3)$, $(e_1 + 3e_3) \wedge e_1$, and $(2e_2 - e_3) \wedge e_1$. Keeping in mind that $e_j \wedge e_i = -e_i \wedge e_j$ and that $e_i \wedge e_i = 0$, these simplify to $2e_1 \wedge e_2 - e_1 \wedge e_3 - 6e_2 \wedge e_3$, $-3e_1 \wedge e_3$, and $-2e_1 \wedge e_2 + e_1 \wedge e_3$. Therefore, the matrix is

$$\begin{pmatrix} 2 & 0 & -2 \\ -1 & -3 & 1 \\ -6 & 0 & 0 \end{pmatrix}.$$

It is worth noting that when computes the wedge of k columns, the coordinates one obtains are, up to sign, the $k \times k$ minors of the matrix formed from these columns, if the basis for the kth exterior power consists of terms that are wedges of k distinct standard basis vectors $e_1, \ldots, e_n$. The length of the resulting vector, i.e., the square root of the sum of the squares of the $k \times k$ minors, is the k-dimensional volume of the parallelepiped spanned by the k column vectors in $\mathbb{R}^n$: if the vectors are $v_1, \ldots, v_k$, this parallelepiped is $\{c_1 v_1 + \cdots + c_k v_k : 0 \le c_i \le 1, 1 \le i \le k\}$.

(b) It is irrelevant that the second vector space is V, or even that it has the same dimension as V. The image of $\bigwedge^d T$ is the span of the vectors $T(v_1) \wedge \cdots \wedge T(v_d)$ as $v_1, \ldots, v_d$ vary in V. This means that if W denotes the image of T, then the image of $\bigwedge^d T$ is precisely $\bigwedge^d W$, whose dimension is $\binom{r}{d}$ (interpreted as 0 if $d < 0$ or if $d > r$). It is worth noting that, in general, if $T : V \to W$ is surjective (respectively, injective) then $\bigwedge^d T : \bigwedge^d V \to \bigwedge^d W$ is surjective (respectively, injective). (Make sure that you can prove this statement.)

4. Let V be an n-dimensional real vector space and f a nonzero element of V. If $h \in V \otimes_{\mathbb{R}} V$, prove that there exist elements $f_1 = f, f_2, \ldots, f_n, g_1, \ldots, g_n \in V$ such that $h = f_1 \otimes g_1 + \cdots + f_n \otimes g_n$.

Prove also that there exists $h \in V \otimes_{\mathbb{R}} V$ such that $h \neq f_1 \otimes g_1 + \cdots f_{n-1} \otimes g_{n-1}$ for any choice of $f_i, g_j \in V$.

For the first part, simply extend $f = f_1$ to a basis $f_1, \ldots, f_n$ for V. Then every element of $V \otimes V$ can be written as $\sum_{i,j} a_{ij} f_i \otimes f_j$, where the a_{ij} are scalars, since the $f_i \otimes f_j$ are a basis for $V \otimes_{\mathbb{R}} V$. But this is $\sum_i f_i \otimes (\sum_j a_{ij} f_j$, and so we may take $g_i = \sum_j a_{ij} f_j$ for each i.

For the second part, fix any basis $f_1, \ldots, f_n$ for V. Every element of $V \otimes_{\mathbb{R}} V$ corresponds to a unique matrix (a_{ij}) of scalars, the coefficients needed to write the element in the form $\sum_{ij} a_{ij} f_i \otimes f_j$. Next note that a decomposable tensor, i.e., one of the form $v \otimes w$, corresponds to a matrix of rank at most one: if $v = \sum b_i f_i$ and $w = \sum_j c_j f_j$, then the matrix of coefficient for $v \otimes w = \sum_{ij} b_i c_j f_i \otimes f_j$ is $(b_i c_j)$, and the span of the row $(c_1 \ \ldots \ c_n)$ contains the row space (the i th row is b_i times this vector). (Similarly the column formed from the c_j spans the column space.) Next note that the rank of the sum of two matrices is at most the sum of their ranks (the rank of $A + B$ is the dimension of its column space, which is contained in the sum of the column spaces of A and B: the largest dimension that can have is the sum of the dimensions of the column spaces of A and B). Thus, the matrix corresponding to the sum of $n - 1$ decomposable tensors has rank at most $n - 1$, and it follows that an element of $V \otimes_{\mathbb{R}} V$ whose corresponding matrix has rank n (e.g., $f_1 \otimes f_1 + \cdots + f_n \otimes f_n$, corresponding to the identity matrix,) cannot be written as the sum of $n - 1$ decomposable tensors.

5. Let V and W be real vector spaces of finite dimension m and n, respectively.

(a) What is the dimension of the vector space $V \otimes_{\mathbb{R}} W$? (No proof needed.)

(b) What is the dimension of the vector space $\bigwedge^k V$ for every integer k? (No proof needed.)

(c) Consider $Y = \bigoplus_{k=0}^{\infty} \bigwedge^k (V \otimes_{\mathbb{R}} W)$ and $Z = \left(\bigoplus_{i=0}^{\infty} \bigwedge^i (V)\right) \otimes_{\mathbb{R}} \left(\bigoplus_{j=0}^{\infty} \bigwedge^j (W)\right)$. (The direct sums are actually finite, i.e., all but finitely many terms are 0.) Find the dimensions of the vector spaces Y and Z, and determine all values of m, n such that Y and Z have the same dimension. (It may be useful that $2^N = (1 + 1)^N$.)

Solution. (a) mn.

(b) $\binom{m}{k}$, interpreted as 0 if $k < 0$ or if $k > m$.

(c) From the hint, $\sum_j \binom{N}{j} = 2^N$ (or interpret $\binom{N}{j}$ as the number of j element subsets of an N element set — the sum is then the number of all subsets). It follows that Y has dimension 2^{mn} and Z has dimension $2^m 2^n = 2^{m+n}$. Thus, that they have the same dimension iff $mn = m + n$ or $(m - 1)(n - 1) = 1$. Consequently, m, n must both be 2 or both be 0.

6. Let $f(x)$ and $g(x)$ be monic polynomials in the variable x over a field K, of degrees m and n, respectively, where m, n are positive integers. Let R be the quotient ring $K[x]/(f(x))$ and let S be the quotient ring $K[x]/(g(x))$.

(a) What is the condition on $f(x)$ for R to be a field? What is the condition on $f(x)$ for R to be an integral domain?

(b) Express the K-vector space dimensions of the following K-vector spaces in terms of m and n (and i, j in part (4)): (1) R; (2) S; (3) $R \otimes_K S$; (4) $\bigwedge^i R \otimes_K \bigwedge^j S$

Solution. (a) In both cases, by a standard theorem about principal ideal domains, the condition is that f be irreducible.

(b) (1) m (by the division algorithm); (2) n; (3) mn; (4) $\binom{m}{i}\binom{n}{j}$.

7. Let F be the splitting field of an equation of degree 6 over the rationals, thought of as a subfield of the complex numbers $\mathbb{C}$.

(a) Must the Galois group of F over $\mathbb{Q}$ be embeddable in S_6? Explain your answer.

(b) Can F have a subfield of degree 25 over $\mathbb{Q}$? Explain.

(c) Let L be the field obtained by adjoining the real root of the equation $x^7 - 2 = 0$ to $\mathbb{Q}$. Describe, with proof, all subfields of L. Can $L \cap F$ be larger than $\mathbb{Q}$? Explain.

(d) Suppose that F has a strictly smaller subfield F_0 that has dimension precisely 360 as a $\mathbb{Q}$-vector space. How many automorphisms of F over $\mathbb{Q}$ fix all elements of F_0? Explain.

Solution. (a) Yes, since the Galois group embeds into the permutation group of the roots.

(b) No, since 25 does not divide $6! = 720$, the order of S_6.

(c) The equation is irreducible (e.g., by Eisenstein's criterion), and so adjoining one root gives an extension of degree 7. This can have no proper subfield strictly larger than $\mathbb{Q}$, since the degree of the subfield over $\mathbb{Q}$ would have to divide 7, which is prime. The subfields of L are $\mathbb{Q}$ and L. Now, $L \subseteq F$ is impossible, for then the degree of L over $\mathbb{Q}$ would divide 720, and 7 does not divide 6!. Thus, $L \cap F = \mathbb{Q}$.
(d) $[F : F_0] = 720/360 = 2$, so the order of the Galois group of F over F_0 is 2, and there are two such automorphisms.

8. (a) Let $(V, +)$ and $(W, +)$ be $\mathbb{Q}$-vector spaces and suppose that f is an isomorphism of V with W *as abelian groups*. Prove that f must be an isomorphism of $\mathbb{Q}$-vector spaces.

(b) An abelian group $(G, +)$ is called *divisible* if for every positive integer n, every element of G has the form ng for some $g \in G$. Prove that a finite divisible group must be zero.

Solution. (a) We must show that $f(\frac{a}{b})v = \frac{a}{b}f(v)$ when $a, b \neq 0$ are integers. But $bf(\frac{a}{b}v) = f(b\frac{a}{b}v) = f(av) = af(v) = b(\frac{a}{b})f(v)$, and we may multiply by $\frac{1}{b}$ to get the desired conclusion.

(b) If the group is not trivial choose an element g of largest order, and call the order $n = pm$, where p is simply any prime factor of n, and $m > 0$ is an integer. Then we can write $g = ph$ for some h, since the group is divisible. The order of h must be divisible by n, since $g \in \langle h \rangle$, but it cannot be n, since $nh = mpg = mg$ and m is smaller than the order of g, which is n. Thus, h has order larger than n, contradicting the fact that g was chosen of maximum order. It follows that the group is trivial.

9. What are all the possible Jordan forms for a complex 4×4 matrix A satisfying $A^3 = A$? Explain your answer.

Solution. A satisfies $x^3 - x = 0$, so its minimal polynomial must divide $x^3 - x$. Since this has distinct roots, A must be diagonalizable, and its eigenvalues must be in the set $\{-1, 0, 1\}$. Conversely, any diagonalizable matrix with eigenvalues in this set will satisfy $A^3 = A$. The Jordan form is simply a diagonal matrix whose diagonal entries are all -1, 0, or 1. It becomes unique if we require that all occurrences of -1 precede all occurrences of 0, which, in turn, should precede all occurrences of 1. The number of possibilities for the Jordan form is the number of ways to choose integers $n_1, n_2, n_3 \geq 0$ (the numbers of occurrences of -1, 0 and 1, respectively), such that $n_1 + n_2 + n_3 = 4$. This is the same as the number of monomials of degree 4 in 3 variables. The counting can be done in many ways, but most efficient is to note that this is the number of sequences involving 4 dots and two slashes (write down n_1 dots, a slash, n_2 dots, a slash, and then n_3 dots). Thus, the number of similarity classes is $\binom{6}{2} = 15$. More generally, if a size n matrix is given to satisfy a degree k equation with distinct roots, the number of similarity classes is the number of ways to choose a k-tuple of non-negative integers that add up to n: the Jordan form can be any diagonal matrix whose diagonal entries are a subset, with repetitions, of the roots of the given polynomial. The number of possibilities is $\binom{n+k-1}{k-1}$.

10. Consider a polynomial $f(x)$ with rational coefficients. Let G be the Galois group of the splitting field of f over $\mathbb{Q}$. In each case below, discuss whether or not f is solvable by radicals.

(a) G is a simple non-abelian group.

(b) G is abelian.

(c) G is isomorphic to a semi-direct product of two nilpotent groups.

(d) G contains A_5.

Solution. f is solvable by radicals if and only if G is a solvable group.

(a) Not solvable, since there are no non-trivial normal subgroups. Solvable groups have a subnormal series with abelian factors.

(b) Solvable, clearly: it is immediate from the definition that all abelian groups are solvable.

(c) Since nilpotent groups are solvable, and an extension of a solvable group by a solvable group is solvable, G is solvable.

(d) A_5 is a non-abelian simple group, and so is not solvable.