VIGRE Algebra QR Review, December 2, 2002

Summary of Session

1. (a) Define the notions of nilpotent group and solvable group. Is a solvable group necessarily nilpotent? What about the converse?

(b) Let L be the splitting field of the monic polynomial $h(x)$, with rational coefficients, over the rational numbers, and let G be the Galois group of L over $\mathbb{Q}$. Describe the connection between the problem of characterizing when all roots of $h(x)$ are expressible by radicals and the group-theoretic properties of G. Without proof, what is the group G of smallest order for which it is not possible to express all roots of $h(x)$ by radicals?

(c) If G as in part (b) has a normal subgroup H of order $128 = 2^7$ and $[G : H] = 125 = 5^3$, are the roots of $h(x)$ necessarily expressible by radicals? Explain your answer.

Solution. A group G is nilpotent if it has a finite composition series in which each group is in the center of the next larger group. (Alternate: let $G_0 = G$ and, recursively, let $G_{n+1} = G_n/Z(G_n)$: G is nilpotent means that G_n is eventually trivial.) G is solvable if it has a finite composition series in which each factor is abelian. (Alternate: Let $G^{(0)} = G$, and, recursively, let $G^{(n+1)} = [G_n, G_n]$. G is solvable means G_n is eventually trivial.) Nilpotent groups are solvable but the converse is false, e.g., S_3 is solvable but not nilpotent (the center is trivial).

(b) The roots are expressible by radicals if and only if the Galois group is solvable. The smallest group that is not solvable is A_5, the alternating group on 5 elements, which has order $5!/2 = 60$, and their are equations of degree 5 with this Galois group.

(c) Groups whose orders are prime powers are solvable, in fact, nilpotent, and an extension of a solvable group by a solvable group is solvable. Since H and G/H both have prime power order, G is solvable and the roots are expressible by radicals.

2. Describe, with proof, all possible Jordan forms, over the complex numbers, for a real skew-symmetric 3×3 matrix T. Can T be a non-zero nilpotent matrix?

Solution. Call the matrix $A = \begin{pmatrix} 0 & -c & b \\ c & 0 & -a \\ -b & a & 0 \end{pmatrix}$. Assume a, b, c are not all 0. Since (a, b, c) is in the kernel, the determinant is 0, and the trace is 0. Thus, $\det(xI - A)$ has the form $x^3 + dx$, where d is easily seen to be the sum of the three minors of the diagonal elements, i.e., $a^2 + b^2 + c^2$, a positive real number. Thus, the Jordan form is either a diagonal matrix (since the eigenvalues are distinct) with diagonal entries $0, \alpha i, -\alpha i$ for some $\alpha \in \mathbb{R} - \{0\}$, or 0, and so one gets all Jordan forms by allowing any $\alpha \in \mathbb{R}$. Thus, it cannot be a non-zero nilpotent matrix.

3. Consider the eight points in $\mathbb{R}^3$ each of whose coordinates is either 1 or -1: these are the vertices of a cube. Let G be the subgroup of the real orthogonal group of $\mathbb{R}^3$ that permutes these eight points. What is the order of G? Show that the intersection of G with the diagonal matrices is the same as the intersection of the 2-Sylow subgroups of G. Is G

solvable? Describe a p-Sylow subgroup of G corresponding to each prime p dividing the order of G, and determine how many p-Sylow subgroups there are. Justify your answers.

Solution. The axes are the lines joining the midpoints of the opposite faces, and so any symmetry of the cube must permute them. Thus each standard basis vector e_1, e_2, e_3 must be carried to $\pm e_i$ for some i, and since the values are independent every i must occur. It is easy to check that any matrix whose columns are $\pm e_{\pi(1)}$, $\pm e_{\pi(2)}$, $\pm e_{\pi(3)}$ (where the three choices of sign are independent) for some permutation π of $\{1, 2, 3\}$ does permute the eight specified points. It follows that the group consists precisely of those matrices whose columns are a permutation of those of the identity matrix, but where each column is given a sign. Since there are six permutations and eight choices of sign the group has 48 elements. The map that sends a given matrix in the group to the associated permutation $\pi \in S_3$ of the axes is a surjective homomorphism from G onto S_3 whose kernel D consists of the diagonal matrices in G: there are eight of these, each of whose diagonal entries is 1 or -1. Since $(\mathbb{Z}/2\mathbb{Z})^3$ and S_3 are both solvable, so is G. Since D is normal, it is in every 2-Sylow subgroup. The number of 2-Sylow subgroups is odd and divides 3. There are 3: the group H_i generated over D by the permutation matrix that fixes e_i and interchanges the other two standard basis vectors is a 2-Sylow subgroup for each i (these are distinct, since they have distinct images in S_3). Since D is in their intersection and D has order 8, D must be the intersection. Finally, G has eight elements of order 3. (These map to the two elements of order 3 in S_3. Corresponding to the 3-cycle (1, 2, 3) there are four preimages, depending on whether e_1 is sent to e_2 or $-e_2$ and on whether e_2 is sent to e_3 or $-e_3$, and the same holds for (1, 3, 2).) Thus, there are 4 3-Sylow groups, each consisting of the identity, one of the elements of order 3, and its inverse.

4. Consider the quotient G of the free abelian group $\mathbb{Z}^3$ by the subgroup H spanned by the elements $(4, 3, 2)$ and $(9, 7, 5)$. Express G explicitly as a direct sum of cyclic groups.

Solution. Elementary row and column operations on the matrix formed from the given vectors as columns do not affect the isomorphism class of G. Subtracting twice the first column from the second, switching the columns, subtracting the first row from the second and third rows, four times the first column from the second, multiplying the second row by -1, and subtracting 3 times the second row from the third gives:

$$\begin{pmatrix} 4 & 9 \\ 3 & 7 \\ 2 & 5 \end{pmatrix} \to \begin{pmatrix} 4 & 1 \\ 3 & 1 \\ 2 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 4 \\ 1 & 3 \\ 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 4 \\ 0 & -1 \\ 0 & -3 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & -1 \\ 0 & -3 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & -3 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix},$$

and now the quotient in question is clearly $\mathbb{Z}$, since $(1, 0, 0)$ and $(0, 1, 0)$ evidently span the kernel of the surjective map $\mathbb{Z}^3 \to \mathbb{Z}$ that sends (a, b, c) to c.

5. Let $p > 1$ be a prime integer and let G be a finite simple group whose order is divisible by p^2. Prove that every proper subgroup of G has index at least $2p$.

Solution G acts transitively on the cosets of the subgroup H, giving a map of G into S_n, where $n = [G : H]$. The kernel of this map is a normal subgroup of G that cannot be all of G, and so must be the identity, i.e., G embeds in S_n. But if $n < 2p$ then $n!$ is not divisible by p^2, and so G cannot embed in S_n.

6. Find the Galois group of the splitting field F of $x^3 - 5$ over the rational numbers $\mathbb{Q}$. Use the structure of this group to describe completely the finite partially ordered set of

subfields of F (including F and $\mathbb{Q}$). Your description should include for each subfield K a generator of K over $\mathbb{Q}$, the value of $[K:\mathbb{Q}]$, and whether K is normal over $\mathbb{Q}$, as well as indicating the containment relations among the various subfields.

Solution. Let r denote the real cube root of 5 and let ω and ω^2 be the primitive cube roots of 1, i.e., the roots of $x^2+x+1=0$. Then the roots of $x^3-5=0$ are r, ωr and $\omega^2 r$, and the spitting field $F=\mathbb{Q}(r,\omega)$. Since r has degree 3 over $\mathbb{Q}$ and ω has degree 2 over $\mathbb{Q}(r)$ (it is complex), we have that $[F:\mathbb{Q}]=6$. Since the Galois group of a splitting field of a polynomial is isomorphic to a subgroup of the permutations of the roots, the Galois group must be S_3. Thus, the intermediate fields correspond to the subgroups of S_3 (given the subgroup, the field is the fixed field of that subgroup). The subgroups of S_3 other than $\{e\}$ and the whole group have order properly dividing six, and so must be of order two or three. There are no proper containments among these subgroups: the only proper containments are that all the fields contain $\mathbb{Q}$ and are contained in F. There is one subgroup H of order 3, containing both elements of order 3, and the fixed field has index 3 and in F and must be $\mathbb{Q}(\omega)$. H is normal and this is a normal extension of $\mathbb{Q}$. The only other subgroups have order two, one generated by each element of order 2. There are 3 of these, each corresponding to a subfield of index 2, and, hence, of degree 3 over $\mathbb{Q}$. These three subfields must be $\mathbb{Q}(r)$, $\mathbb{Q}(r\omega)$, and $\mathbb{Q}(r\omega^2)$.

7. Let k be an algebraically closed field and let $G=GL(n,k)$ act on the set M of $n\times n$ matrices by conjugation. Let S be a finite subset of k, and let X be the subset of M consisting of those $n\times n$ matrices all of whose whose eigenvalues are in S.

(a) Prove that the action of G on M restricts to an action of G on X.

(b) Prove that the action of G on X has only finitely many orbits.

(c) Now let $n=3$. Find a formula for the number of orbits of G on X in terms of the cardinality of S.

(a) Conjugation does not change eigenvalues (it preserves the characteristic polynomial) so G takes elements of X back to X.

(b) The orbits of the action of G on M are represented by the Jordan canonical forms. Since Jordan forms are determined by the number of Jordan blocks and the eigenvalues for each block, there are only finitely many Jordan forms whose eigenvalues are in S, and so finitely many orbits in X.

(c) Let $n=|S|$. There are $\binom{n}{3}$ forms with distinct eigenvalues, $2n(n-1)$ with one repeated eigenvalue (there can be one block or two for that eignevalue) and $3n$ with a single eigenvalue (depending on whether the block sizes are 3, 2 and 1, or three of size 1). So there are $\binom{n}{3}+2n(n-1)+3n$ orbits.

8. Let A be an $n\times n$ real orthogonal matrix, thought of as an $\mathbb{R}$-linear map $\mathbb{R}^n\to\mathbb{R}^n$.

(a) Consider the matrix of $\bigwedge^t A$ with respect to the basis for A consisting of vectors $e_{i_1}\wedge\cdots\wedge e_{i_t}$, where $i_1<\cdots<i_t$. Describe the entry in the spot corresponding to the pair of vectors $e_{i_1}\wedge\cdots\wedge e_{i_t}$, $e_{j_1}\wedge\cdots\wedge e_{j_t}$. Here $i_1<\cdots<i_t$, $j_1<\cdots<j_t$, the first vector should be thought of as determining a row of the matrix, and the second a column. (Technically, to get an actual matrix, one needs to order the basis. But the ordering does not affect the answer to this question or the next.)

(b) Is it true that if A is orthogonal then the matrix constructed in part (a) for $\bigwedge^t A$ is orthogonal? Prove your answer.

Solution. (a) Let $A = (a_{ij})$. The value of T on $e_{j_1} \wedge \cdots \wedge e_{j_t}$ is $T(e_{j_1}) \wedge \cdots \wedge T(e_{j_t})$. Note that $T(e_j) = a_{1j}e_1 + \cdots + a_{nj}e_n$. Put in these expressions for the $T(e_{j_\mu})$ and expand by the generalized distributive law. We then want to collect the terms that involve $e_{i_1} \wedge \cdots \wedge e_{i_t}$. There are $t!$ such terms. Let σ be a permutation of $1, \ldots, t$. The $t!$ terms one needs to take account of are those of the form $a_{i_{\sigma(1)},j_1} \cdots a_{i_{\sigma(t)},j_t} e_{i_{\sigma(1)}} \wedge \cdots \wedge e_{i_{\sigma(t)}}$. The wedge can be rewritten as $(\operatorname{sgn}\sigma)e_{i_1} \wedge \cdots \wedge e_{i_t}$. Therefore, the coefficient of $e_{i_1} \wedge \cdots \wedge e_{i_t}$ is $\sum_\sigma (\operatorname{sgn}\sigma) a_{i_{\sigma(1)},j_1} \cdots a_{i_{\sigma(t)},j_t}$, which is precisely the determinant of the $t \times t$ submatrix of A formed from the intersection of the given rows and the given columns. Thus, the matrix of $\bigwedge^t(A)$ is $\binom{n}{t} \times \binom{n}{t}$: its entries are the $t \times t$ subdeterminants (or *minors*) of A.

(b) Yes. Since $AA^{-1} = I$, $\bigwedge^t A \bigwedge^t(A^{-1}) = \bigwedge^t I$, and this last is the identity map on $\bigwedge^t \mathbb{R}^n$. It follows that $(\bigwedge^t A)^{-1} = \bigwedge^t(A^{-1}) = \bigwedge^t(A^{\mathrm{tr}})$, and this is easily seen to be $\left(\bigwedge^t(A)\right)^{\mathrm{tr}}$.

9. Let $\mathbb{Q}[x]$ be the polynomial ring in one variable over the rational numbers $\mathbb{Q}$ and let M be the $\mathbb{Q}[x]$-module whose underlying $\mathbb{Q}$-vector space is $\mathbb{Q}^3$, and such that the action of x on an element of M is given by the $\mathbb{Q}$-linear transformation A with matrix $\begin{pmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \\ -1 & 0 & -2 \end{pmatrix}$.

Express M as a direct sum of cyclic modules over $\mathbb{Q}[x]$.

Solution. The module is the cokernel (quotient of $Q[x]^{\oplus 3}$ by the column space) of $xI - A$, and so we may solve the problem by performing elementary row and column operations over $\mathbb{Q}[x]$ on that matrix. Switch the first and second rows and also the first and second columns. Subtract $x-2$ times the third row from the second and $x+2$ times the second column from the third. Interchange the second third rows, and multiply the third row by -1. We get:

$$\begin{pmatrix} x-3 & 0 & 0 \\ 0 & x-2 & -4 \\ 0 & 1 & x+2 \end{pmatrix} \to \begin{pmatrix} x-3 & 0 & 0 \\ 0 & 0 & -x^2 \\ 0 & 1 & x+2 \end{pmatrix} \to \begin{pmatrix} x-3 & 0 & 0 \\ 0 & 0 & -x^2 \\ 0 & 1 & 0 \end{pmatrix} \to \begin{pmatrix} x-3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^2 \end{pmatrix}$$

which yields the direct sum $\mathbb{Q}[x]/(x-3) \oplus \mathbb{Q}[x]/(1) \oplus \mathbb{Q}[x]/(x^2)$. The middle term is 0, and so we may write this as $\mathbb{Q}[x]/(x-3) \oplus \mathbb{Q}[x]/(x^2) \cong \mathbb{Q}[x]/\big((x-3)x^2\big)$.

10. Let A and B be $n \times n$ matrices over the real numbers such that $AB = 0$.

(a) Prove that the sum of the ranks of A and B is at most n.

(b) Show by example that BA can be nonzero.

(c) Must BA be nilpotent? Prove your answer.

Solution. (a) The column space of B is in the kernel of A, and so the rank of B is at most the nullity of A. But the rank and nullity of A have sum n.

(b) Let $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ and let $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Then $AB = 0$ while $BA = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

(c) $(BA)^2 = (BA)(BA) = B(AB)A = B(0)A = 0$. [Alternate: As in a previous problem, BA and AB have the same characteristic polynomial. Since $AB = 0$, the characteristic polynomial is x^n, and so $(BA)^n = 0$. Thus, BA is nilpotent.]