VIGRE Algebra QR Review, November 10, 2003

A problem asking for the calculation of the Galois group of $f(x) = x^5 - 6x + 3$ over the rationals was raised. First note that the equation is irreducible by Eisenstein's criterion, since every coefficient but the highest is divisible by the prime number 3, but the constant term is not divisible by 9. This shows that if we adjoin any one root of the equation to $\mathbb{Q}$, we get a field extension of degree 5. Therefore, the order of the splitting field is divisible by 5, and this is the same as the order of the Galois group. The Galois group G may be viewed as a group of permutations of the roots of the equation: each automorphism is uniquely determined by what it does to the roots, since they generate the splitting field. Thus, G is a subgroup of S_5 whose order is divisible by 5. This implies that G contains a 5-cycle, since every element of S_5 of order 5 is a 5-cycle.

We next show that f has precisely three real roots, and therefore two complex roots, which must be conjugate. It follows that $G \in S_5$ contains a two-cycle, corresponding to the action of complex conjugation on the splitting field. From this we will be able to deduce that G is S_5. To determine that there are precisely three real roots, note that the derivative is $5x^4 - 6$, which vanishes only at $x = (6/5)^{1/4} = r$ and at $-r$. Note that $6/5 = 1.2$, and so r is between 1 and 1.2 (we could make a finer estimate, but don't need one). The derivative is positive for $x < -r$, negative for $-r < x < r$, and positive for $x > r$. Therefore the function is increasing for $x < -r$, with $f(-r) = (-r)^5 - 6(-r) + 3 = -r^4 r + 6r + 3 > -(6/5)r + 6(1) + 3 > 9 - (6/5)(6/5) > 0$, decreasing from $-r$ to r, with $f(r) = r^5 - 6r + 3 < (6/5)(6/5) - 6 + 3 < 0$, and then increasing for $x > r$. It follows that there is precisely one real root of f in each of the intervals $(-\infty, -r)$, $(-r, r)$, and $(r, +\infty)$, and so there are precisely three real roots, and two complex roots.

As observed above, this means that G contains a 2-cycle. Suppose by renumbering that the 2-cycle is $g = (1\ 2)$. Some power of the 5-cycle will take 1 to 2. After renumbering we may assume that the 5-cycle is $h = (1\ 2\ 3\ 4\ 5)$. The conjugates of g by powers of h (which may be calculated by letting the powers of h act on the entries of g written in cycle notation) include $(2\ 3)$, $(3\ 4)$, and $(4\ 5)$. The transpositions of consecutive elements are sufficient to generate S_5, and so $G \cong S_5$.

A question was asked about an old QR problem (which was also discussed at the first session this year): V is a real vector space of dimension n. One part of the problem is to show that if $f = f_1$ is not 0 in V then every element of $V \otimes_{\mathbb{R}} V$ can be expressed in the form $f_1 \otimes g_1 + \cdots + f_n \otimes g_n$ for suitable elements f_i, g_i in V. To do this, extend f to a basis $f = f_1, \ldots, f_n$ for V, and let $v_1, \ldots, v_n$ be another basis. The then every element of $V \otimes V$ can be written as a linear combination of elements $f_i \otimes v_j$, say as $\sum_{ij} c_{ij} f_i \otimes v_j$. But this can be rewritten as $\sum_i f_i \otimes (\sum_j c_{ij} v_j)$ which has the required form.

Another part of the problem required showing that there is some element of $V \otimes V$ that cannot be written as the sum of $n - 1$ terms of the form $f_i \otimes g_j$. Here is one way to do this. Pick a basis $v_1, \ldots, v_n$ for V, and a possibly different basis $w_1, \ldots, w_n$ as well.

Then every element of $V \otimes V$ can be written uniquely in the form $\sum_{ij} c_{ij} v_i \otimes v_j$. This give a vector space isomorphism between $V \otimes V$ and $n \times n$ matrices (c_{ij}). An element of the form $f \otimes g$ can be written as $(\sum_i a_i v_i) \otimes \sum_j b_j w_j) = \sum_{i,j} (a_i b_j) v_i \otimes w_j$ so that the corresponding matrix $(a_i b_j)$ is the product of the $n \times 1$ column with entries a_i and the $1 \times n$ row with entries b_j. This implies that the matrix corresponding to $f \otimes g$ has rank at most one. The rank of the sum of two matrices is at most the sum of their ranks, since the column space of the sum is contained in the sum of the column spaces of the two matrices. Thus, the matrix corresponding to the sum of $n-1$ elements $f_i \otimes g_i$ has rank at most $n-1$. It follows that a element of $V \otimes V$ whose corresponding matrix has rank n, such as $v_1 \otimes w_1 + \cdots + v_n \otimes w_n$, which corresponds to the identity matrix, cannot be a sum of $n-1$ elements of the form $f_i \otimes g_i$.