VIGRE Algebra QR Review, October 20, 2003

Let θ denote the positive real fourth root of $\alpha = 7 + \sqrt{33}$. It was asked whether $\mathbb{Q}[\theta]$ is Galois, and whether $\mathbb{Q}[\theta, i]$ is Galois. Since $\mathbb{Q}$ has characteristic 0, every extension is separable, and the issue is whether these extensions are normal, i.e., whether they contain all the conjugates over $\mathbb{Q}$ of their generators.

α and $\beta = 7 - \sqrt{33}$ are conjugate over the rationals. Let $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{33})$. We first note that $x^4 - \alpha$ is irreducible over K. The four roots of this equation are θ, $-\theta$, θi, and $-\theta i$ where $i = \sqrt{-1}$. If the polynomial factored it would have to have either a monic linear or monic quadratic factor, which would imply that either $\pm\theta$ or $\pm\theta^2$ is in K, since one of these would be the constant term. In either case, we would find that $\theta^2 \in K$, and so α would be a perfect square in K. This would mean that there are rational numbers a, b such that $\alpha = (a + b\sqrt{33})^2$, so that $a^2 + 33b^2 = 7$ and $2ab = 1$. But then $a^2 + 33/4a^2 = 7$, and $4a^4 - 28a^2 + 33 = 0$. Since the discriminant is $4^2(7^2) - 4(4)(33) = 4^2(49 - 33) = 16^2$, the roots for a^2 are $(28 \pm 16)/8 = (7 \pm 4)/2$, i.e., $11/2$ and $3/2$, and since neither is a perfect square, a cannot be rational. Since the equation is irreducible over K, its roots are conjugate over K and therefore over $\mathbb{Q}$. It follows that any normal field extension of $\mathbb{Q}$ that contains θ must contain all of the roots, and therefore must contain i. Therefore $\mathbb{Q}(\theta)$ is not normal and not Galois.

On the other hand, $\mathbb{Q}(\theta, i)$ *is* normal. It suffices to show that it is the splitting field of $(x^4 - 7)^2 - 33 = 0$. This equation has eight roots: the equation implies that $x^4 - 7 = \pm\sqrt{33}$, from which we see that the roots are the four fourth roots of α, described above, together with the four fourth roots of β. It is clear the four fourth roots of α generate $K(i)$. Therefore normality will follow if we can show that the four fourth roots of β are already in $K(i)$. But $\alpha\beta = 7^2 - 33 = 16 = 2^4$, and so one of the fourth roots of β is $2/\theta$, while the others are obtained by multiplying by -1, i and $-i$. These are all ready in $K(i)$. $\square$

Another problem dealt with the transformation T from V_n, the space of polynomials of degree n over the real numbers, to itself that sends $P(x)$ to $P(x - 1)$. Let's analyze the eigenvalues and eigenvectors, find the minimal and characteristic polynomials, and determine the Jordan form. The analysis is the same whether one works over the reals or over the complex numbers.

Let $N = I - T$, where I is the identity. Then $N(P) = P(x) - P(x - 1)$. The key point about N is that it kills constants and lowers degrees exactly one. To see this, note that $P(x)$ and $P(x - 1)$ have the same leading term: these cancel. If P has degree h, let $P(x) = cx^h + Q(x)$. Then $N(Q)$ has no terms in degree $h - 1$: these come entirely from cx^h, and looking at $cx^h - c(x - 1)^h$ we see that the degree $h - 1$ term is chx^{h-1}, and our claim is verified. Note that we need characteristic 0 here: in characteristic $p > 0$, we might have $p \mid h$. It follows that the only eigenvalue of N is 0, and that the only eigenvectors are the nonzero constants. Thus, the only eigenvalue of T is is 1, and, again, the only eigenvectors are the nonzero constants. Starting with x^n, we may apply N repeatedly to get one polynomial of each degree. This gives a basis for V_n. With respect to this basis the matrix is lower triangular, with 0 everywhere on the main diagonal, 1 everywhere on the diagonal just below the main diagonal, and 0 elsewhere. This is a Jordan block. T therefore has a matrix with 1 everywhere on the main diagonal, 1 everywhere on the diagonal just below the main diagonal, and 0 elsewhere, which is also a Jordan block. Thus, the characteristic and minimal polynomials of T are both $(x-1)^n$.

Let V be an n-dimensional vector space over the reals (or any field of characteristic 0). Another problem dealt with the linear transformation $T : V \otimes V \otimes V$ to itself that sends $v \otimes w \otimes z$ to $w \otimes z \otimes v$ (the analysis is exactly the same for the transformation that sends $v \otimes w \otimes z$ to $z \otimes v \otimes w$). First note that there is a unique such linear transformation because the map $V \times V \times V \to V \otimes V \otimes V$ that sends (v, w, z) to $w \otimes z \otimes v$ is 3-multilinear.

The problem was to show that there is a basis for $V \otimes V \otimes V$ with respect to which the matrix of T consists of the direct sum of n blocks that are 1×1 and $(n^3 - n)/3$ blocks that are 3×3, and to find the characteristic and minimal polynomials of T.

Now, if v_i is a basis for V and w_j is a basis for W, then the vectors $v_i \otimes w_j$ form a basis for $V \otimes W$. It follows that $V \otimes V \otimes V$ has as a basis the n^3 vectors $v_i \otimes v_j \otimes v_k$ where $v_1, \ldots, v_n$ is any basis for V. Note that T permutes these vectors. There are n basis elements that are fixed by T, those of the form $v_i \otimes v_i \otimes v_i$. These give the n blocks that are 1×1, with the single entry 1, each of which has characteristic and minimal polynomial equal to $x - 1$. All other basis vectors break up into orbits of length 3 cyclically permuted by T. There must be $(n^3 - n)/3$ of these orbits, and each gives rise to a 3×3 block of the form $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ whose characteristic and minimal polynomials are both $x^3 - 1$. The minimal polynomial of the transformation is the least common multiple of these minimal polynomials and is therefore $x^3 - 1$. The characteristic polynomial is the product of the characteristic polynomials, and is $(x-1)^n(x^3-1)^{(n^3-n)/3}$.

Every matrix over a PID can be made diagonal by multiplying on the left and right by square invertible matrices, and in such a way that each diagonal entry divides the ones that come after it. Over a polynomial ring, this can be done by row and column operations. These operations are permuting the rows and columns, multiplying a row or column by a unit, and adding or subtracting a multiple of one row (resp., column) from another row (resp., column). This form for the matrix is unique, except that one may multiply the entries on the diagonal by units. This is essentially equivalent to the fact that every finitely generated module over a PID R is a finite direct sum of cyclic modules $R/(f_i)$ in such a way that every f_i divides the next, with the same uniqueness condition on the f_i. Over a polynomial ring $K[x]$ we achieve complete uniqueness by requiring the nonzero f_i to be monic.

One has the following connection with putting an $n \times n$ matrix A over the field K into rational canonical form. Consider the matrix $xI - A$, and put it in the diagonal form described above (Smith form). The $K[x]$-module associated with A (K^n, on which the action of $f(x)$ is the same as the action of $f(A)$) has the following connection with the matrix A: the modules defined by matrices A and B are isomorphic if and only if the matrices are similar. The module is obtained from the matrix $xI - A$ by killing the $K[x]$-span of the columns in $K[x]^{\oplus n}$, and the isomorphism class of the module obtained from a matrix over $K[x]$ (by killing the $K[x]$-span of the columns in $K[x]^{\oplus n}$) does not change when one performs elementary row and column operations. If one gets to a diagonal matrix with diagonal entries f_i, the module is the direct sum of the cyclic modules $K[x]/(f_i)$. When we start with $xI - A$, the determinant is a non-zero polynomial, which implies that a diagonal matrix that is equivalent cannot have any zeros on the diagonal.

If one gets a diagonal form with monic diagonal entries each of which divides the next, then the f_i that occur, other than 1, are the same polynomials to be used to give the rational form of the original matrix. This rational form will be the direct sum of the companion matrices for the f_i.

Suppose that we want to find the rational canonical form of the matrix

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 3 & 0 \\ -1 & 0 & -1 \end{pmatrix}$$

over the rationals $\mathbb{Q}$. First form $xI - A = \begin{pmatrix} x-1 & 0 & -1 \\ 0 & x-3 & 0 \\ 1 & 0 & x+1 \end{pmatrix}$. Subtract $x-1$ times the third row from the first to get $\begin{pmatrix} 0 & 0 & -x^2 \\ 0 & x-3 & 0 \\ 1 & 0 & x+1 \end{pmatrix}$. Subtract $x+1$ times the first column from the third to get: $\begin{pmatrix} 0 & 0 & -x^2 \\ 0 & x-3 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. Multiply the first row by -1 and interchange the first and third row to get $\begin{pmatrix} 1 & 0 & 0 \\ 0 & x-3 & 0 \\ 0 & 0 & x^2 \end{pmatrix}$. At this point it is easier to work with modules than to continue with row and column operations. Since this matrix is diagonal, the corresponding module is $\mathbb{Q}[x]/(x-3) \oplus \mathbb{Q}[x]/(x^2)$, and since $x-3$ and x^2 are relatively prime, this is isomorphic with $\mathbb{Q}[x]/\big((x-3)x^2\big)$. The rational form is the companion matrix of $(x-3)x^2 = x^3 - 3x^2$. (This is the same as a matrix for multiplication by x acting on a suitable basis for the cyclic module: one uses the basis $1, x, x^2$ for a lower triangular companion matrix: $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 3 \end{pmatrix}$.)