Math 504, 10/17

We now describe an interesting application of the rational canonical form to a mathematical card trick (!) Begin by noting that the companion matrix $C(p^i)$ of a power of an irreducible polynomial p over a field K is the only matrix up to similarity of its size with minimal polynomial p^i, since in general, as noted in the last lecture, the minimal polynomial of any rational canonical form is the least common multiple of the polynomials of which its blocks are the companion matrices. In particular, the transpose $C(p^i)^t$ of $C(p^i)$ has the same minimal polynomial p^i, so is similar to $C(p^i)$; in later homework you will show that any square matrix over any field is similar to its transpose. Now let $K = \mathbf{Z}_2$, the field with two elements, and let $L = \mathbf{Z}_2[x]/(x^5 + x^2 + 1)$. As it is easy to check that $x^5 + x^2 + 1$ is irreducible in $\mathbf{Z}_2[x]$, it follows that L is a field that is 5-dimensional as a vector space over K, so L has exactly 32 elements. A basis of L over K is given by the powers $1, x, \ldots, x^4$; the matrix M of multiplication by x as a K-linear transformation of L with respect to this basis is just the companion matrix of $x^5 + x^2 + 1$. Its 31st power is the identity, since we must have $x^3 1 = 1$ in L, but no lower power x^i of x has $x^i v = v$ for any nonzero v in L. By the remark made at the beginning, the transpose $N = M^t$ of M also has $N^{31} = I$ but $N^i v \neq v$ for any positive $i < 31$ and nonzero v. Multiplying M^t by a column vector $(a_1, \ldots, a_5)$, we get $(a_2, \ldots, a_5, a_1 + a_3)$. It follows that if we define a 31-element sequence $b_1, \ldots, b_{31}$ of elements of K recursively via $b_1 = b_2 = b_3 = b_4 = 0, b_5 = 1, b_n = b_{n-3} + b_{n-5}$ for $n \geq 6$, then the *consecutive* 5-bit subsequences $b_i, \ldots, b_{i+5}$ run through all the nonzero 5-bit sequences of elements of K, each occurring once and only once; here $1 \leq i \leq 31$ and the addition in the subscripts takes place modulo 31. If we continued the sequence $b_1, b_2, \ldots$ by the same recursive rule inductively, we would get its first block $b_1, \ldots, b_{31}$ repeated indefinitely. Instead we continue for just one more term, setting $b_{32} = 0$. Now the consecutive 5-bit subsequences $b_i, \ldots, b_{i+5}$ of this sequence $b_1, \ldots, b_{32}$ run through *all* the 5-bit sequences of elements in K, each occurring exactly once, where the addition of subscripts now takes place modulo 32. Such a 32-bit sequence is called a *deBruijn sequence* (of length 32) and is of interest in combinatorics; it can be constructed in several ways quite different from the above. We use this sequence to perform a card trick, as follows. Discard the nines through the kings from an ordinary 52-card deck of cards, leaving just 32 cards. Encode each card in the deck by a 5-bit sequence, using the first three bits to encode the rank (ace=000,...,eight=(111)), while the last two bits encode the suit (spades=00, hearts=(01), diamonds=(10), clubs=(11). Now arrange the 32-card deck so that the ith card from the top is the one encoded by the ith 5-bit subsequence. Thus the first card, encoded by 00001, is the ace of hearts; the next one, encoded by 00010, is the ace of diamonds, and so on. The resulting order of cards will seem completely random to anyone who examines the deck, but you can essentially memorize it, working out in your head what the card following any given one is, by applying the recurrence $b_n = b_{n-3} + b_{n-5}$. Thus you can use this deck to "prove" that you have ESP, announcing in advance what the order of the cards in it will be. This trick can

be adapted to any deck (not necessarily one of ordinary playing cards) whose size is any power 2^k of 2, provided only that one can encode the cards by k-bit sequences; one uses the existence of a field of order 2^k (which we will prove later) to construct the required deBruijn sequence.

We now consider more general modules over any commutative ring R. Let M, N be two R-modules. A *bilinear* map from $M \times N$ to another R-module P is a map f such that $f(m_1+m_2, n) = f(m_1, n)+f(m_2, n), f(m, n_1+n_2) = f(m, n_1)+f(m, n_2), f(rm, n) = f(m, rn) = rf(m, n)$ for all $m, m_1, m_2 \in M, n, n_1, n_2 \in N, r \in R$. We construct a new module $M \otimes N$ or $M \otimes_R N$ called their *tensor product* such that bilinear maps from $M \times N$ to P are in natural bijection to R-linear maps from $M \otimes N$ to P, as follows. Start with the free R-module on the Cartesian product $M \times N$ and mod out by the submodule S generated by $(m, n) + (m', n) - (m + m', n), (m, n) + (m, n') - (m, n + n'), (rm, n) - (m, rn), (m, rn) - r(m, n)$ for all $r \in R, m, m' \in M, n, n' \in N$; note that any bilinear map would have to send any generator of S to 0. The individual elements $m \otimes n$ of $M \otimes N$ are called *tensors*; note that a general element of $M \otimes N$ is a sum of tensors rather than a single tensor. As a first example, suppose that M and N are both free over R, say ranks m, n, respectively, with respective bases $x_1, \ldots, x_m$ and $y_1, \ldots, y_n$. Then it is not difficult to show that a bilinear map f from $M \times N$ to P is completely determined by the images $v_{ij} = f(x_i, y_j)$ of ordered pairs of basis vectors, which can be any elements of P. It follows that $M \otimes N$ is also free over R, with basis $\{x_i \otimes y_j\}$. In general, however, tensor products can behave in quite unexpected ways; we will explore some of these in the next few lectures.