Lecture 1-27: The Normal Basis Theorem

January 27, 2025

There is a beautiful connection between a Galois extension L of a field K and the group algebra KG of its Galois group G. This is established by

Normal Basis Theorem

If L is finite Galois over K with Galois group G and if $g_1, \ldots, g_n$ are the elements of G then there is $x \in L$ such that $g_1x, \ldots, g_nx$ is a basis of L over K.

Such a basis is called a normal basis. Its existence shows that $L \cong KG$ as representaitons of G over K (but not as algebras).

To prove this result I need another one of interest in its own right.

Theorem: algebraic independence of automorphisms

With notation as above, if K is infinite, then the automorphisms g_i are algebraically independent; that is, the only polynomial $f \in K[x_1, \ldots, x_n]$ with $p(g_1, \ldots, g_n) = 0$ as a map from L to itself is the zero polynomial.

Proof.

Let f satisfy $f(g_1, \ldots, g_n) = 0$ and let $u_1, \ldots, u_n$ be a basis of L over K. For any $a_i \in K$ we have
$f(g_1(\sum a_i u_i,) \ldots, g_n(\sum a_i u_i)) = f(\sum a_i g_1(u_i), \ldots \sum a_i g_n(u_i)) = 0$. Setting $g(x_1, \ldots x_n) = f(\sum g_1(u_i)x_i, \ldots \sum g_n(u_i)x_i) = 0$, we get $g(a_1, \ldots, a_n) = 0$ for all $a_i \in K$. Since K is infinite it follows that g is identically 0 when regarded as a polynomial in the x_i over K. Define an $n \times n$ matrix $M = (m_{ij})$ over L via $m_{ij} = g_j(u_i)$. Linear independence of homomorphisms into a field (proved last time) implies that the columns of M are linearly independent over L, whence M has an inverse $R = (r_{ij})$. Then
$g(\sum_{j,k} r_{1j} g_j(u_k)x_k, \ldots, \sum_{j,k} r_{nj} g_n(u_k)) = f(x_1, \ldots, x_n) = 0$ identically, as claimed. $\square$

Now we can prove the Normal Basis Theorem. Suppose first that K is infinite. Regarding the g_i as independent variables over K and defining a matrix $N = (n_{ij})$ over $K[g_1, \ldots, g_n]$ via $n_{ij} = g_i g_j$, we find that the coefficient of g_1^n in $\det N$ is $\pm 1 \neq 0$, so $\det N$ is not identically 0. By the algebraic independence result, there is $x \in L$ such that $\det N(x) \neq 0$. But then a dependence relation among $g_1 g_1 x, \ldots, g_1 g_n x$ over K would also hold with the same coefficients among $g_i g_1 x, \ldots, g_i g_n x$ for all i, since the g_i commute with left multiplication by K, and the columns of $N(x)$ would be dependent over K, forcing $\det N(x) = 0$. This is a contradiction.

Finally, suppose that K is finite. In this case G must be cyclic, say generated by g. The minimal polynomial of g, regarded as K-linear transformation from L to itself, must be $x^n - 1$, since the powers $1, g, \ldots, g^{n-1}$ are linearly independent automorphisms. Using the *elementary divisor* version of the rational canonical form, we find that the rational canonical form of g is the companion matrix of $x^n - 1$, so that there is $x \in L$ such that $x, gx, \ldots, g^{n-1}x$ form a basis of L over K. This is exactly what we want.

In particular, the Normal Basis Theorem applies to any field L admitting a finite group G of automorphisms; it says that there is always $x \in L$ such that the G-conjugates gx of x are distinct and form a basis of L over the fixed field L^G. You have already seen one of the most interesting and important special cases, namely that of the symmetric group S_n acting on the rational function field $L = K(x_1, \ldots, x_n)$ in n variables x_i over a field K, by permuting the variables. Recall the elementary symmetric functions $s_i = \sum_{j_1,\ldots,j_i} x_{j_1} \cdots x_{j_i}$; here the indices j_k range over all distinct sets of i indices among $\{1, \ldots, n\}$ and $1 \leq i \leq n$. I showed previously that the s_i generate the fixed field L^{S_n} over K; now I can sharpen this result. To do this observe first that $G = S_n$ also acts on the *polynomial* ring $S = K[x_1, \ldots, x_n]$. Polynomials fixed by S_n are called symmetric.

Fundamental Theorem on Symmetric Functions

The ring S^G of symmetric polynomials is freely generated by the s_i, so that every symmetric polynomial is uniquely a polynomial in the s_i. In particular, S^G is also a polynomial ring in n generators over K.

Proof.

First note that $p \in S$ lies in S^G if and only if whenever a monomial term $cx_1^{a_1} \cdots x_n^{a_n}$ occurs in the p, then so does $cx_1^{a_{\pi(1)}} \cdots x_n^{a_{\pi(n)}}$, for all permutations $\pi \in S_n$. Since p lies in S if and only if the sum of the monomials of p of each fixed degree d does, we may assume that p is homogeneous of degree d. As we did last quarter, order all monomials in the x_i of degree d lexicographically, so that $cx_1^{b_1} \cdots x_n^{b_n} < dx_1^{c_1} \cdots x_n^{c_n}$ if and only if the smallest index i with $b_i \neq c_i$ has $b_i > c_i$. Now, given a homogeneous symmetric polynomial s, let $x_1^{a_1} \cdots x_n^{a_n}$ be the lexicographically first monomial m occurring in s. Then $a_1 \geq \cdots \geq a_n$, lest some S_n-conjugate of this monomial be a lexicographically earlier term in s. $\square$

Proof.

Then one checks immediately that $s - cs_n^{a_n} s_{n-1}^{a_{n-1}-a_n} \cdots s_1^{a_1-a_2}$ is symmetric and a combination of monomials of degree d lexicographically later than m, so by iterating this process we write s as a combination of monomials in the s_i, as claimed. A similar argument shows that the monomials in the s_i are linearly independent: the lexicographically earliest monomial occurring in any combination C of such monomials comes from just one of them and is not cancelled out by any other one, so that $C \neq 0$. $\square$

I can form the quotient $C = S/S^+$, where S^+ is the ideal of S generated by the homogeneous elements of S^G of positive degree. This quotient C is called the coinvariant algebra. Then G acts naturally on C; it turns out that if homogeneous polynomials $p_1, \ldots, p_m$ are chosen so that their images in C form a basis of it over K, then the p_i provide both a free basis of S as an S^G module and a basis of L over L^G.

The Normal Basis Theorem then implies that C is isomorphic as a KG-module (but not as a ring) to KG itself. This alternative model of the regular representation of G is more revealing in a number of ways than KG itself, since it has a graded structure not present in KG.

For example, the 1-graded piece C_1 of C may be identified with the span over K of the variables x_i, modulo the line spanned by the sum $s_1 = x_1 + \ldots + x_n$. G acts irreducibly on C_1 via the representation corresponding to the partition $(n-1, 1)$ (using the parametrization of G-modules given last quarter). This is called the reflection representation.

The 0-graded piece C_0 is just the basefield K, carrying the trivial representation of G. It turns out that the $\binom{n}{2}$-graded piece $C_{\binom{n}{2}}$ of C is also one-dimensional, carrying the sign representation. In general, there is a beautiful way to read off in which degrees of C the $\dim \pi$ copies of every irreducible representation π of G live, using the standard tableaux from last quarter that parametrize a basis of π.