

## Math 505, 1/23

We conclude our treatment of Galois theory with the Normal Basis Theorem, which generalizes the result of an earlier homework problem to arbitrary finite Galois extensions. More precisely, let  $L$  be finite and Galois over a field  $K$ , with Galois group  $G$ . Then *there is  $x \in L$  such that the  $G$ -conjugates of  $x$  form a basis of  $L$  over  $K$* . To prove this, we begin by assuming that  $K$  is infinite, as we may since if  $K$  is finite, then  $G$  is cyclic and the result follows from the homework problem mentioned above. We first derive a criterion for determining when a subset  $x_1, \dots, x_n$  of  $L$  is a basis of it over  $K$ , where  $n$  is the degree of  $L$  over  $K$ . Enumerate the elements of  $G$  as  $g_1, \dots, g_n$ . Given  $x_1, \dots, x_n \in L$ , form a matrix  $M = M(x_1, \dots, x_n)$  whose  $ij$ th entry is the image  $g_i(x_j)$  of  $x_j$  under  $g_i$ . Then the  $x_i$  are a basis if and only if the determinant of  $M$  is nonzero. Indeed, if there is a nontrivial dependence relation  $\sum_i k_i x_i = 0$  among the  $x_i$  with  $k_i \in K$ , then  $\sum_i k_i g_j(x_i) = 0$  for all  $j$ , so that the columns of  $M$  are dependent and its determinant is 0. Conversely, given a nontrivial dependence relation  $\sum_j y_j g_j(x_i) = 0$  among the columns of  $M$  with the  $y_j$  in  $L$ , then the  $x_i$  cannot span  $L$  over  $K$ , lest this relation amount to a dependence relation  $y_j g_j = 0$  among the  $g_j$  themselves as  $K$ -linear transformations of  $L$ , which we ruled out last quarter (toward the end we showed the elements of  $G$  are an  $L$ -basis for the set of all  $K$ -linear transformations of  $L$ ). In particular, the columns (or rows) of our matrix  $M$  are dependent over  $K$  if and only if they are dependent over  $L$ . Next, I claim that *the  $g_i$  are algebraically independent over  $L$  as  $K$  linear transformations of  $L$ , where we interpret products of the  $g_i$  as products, not compositions, of the corresponding functions from  $L$  to itself* (we do not take the products in  $G$ ). Indeed, the independence of the  $g - i$  over  $L$  guarantees that the  $n$ -tuple  $(g_1(x), \dots, g_n(x))$  runs over an  $n$ -dimensional  $K$ -subspace  $S$  of  $L^n$  whose  $L$ -span is all of  $L^n$ , as  $x$  runs over  $L$ ; an easy induction using the infiniteness of  $L$  shows that such any polynomial vanishing identically on a such a subspace must be 0. Now we can complete the proof of the Normal Basis Theorem: set up a matrix  $M'$  whose  $i$ th row is the permutation  $g_i g_1, \dots, g_i g_n$  of  $g_1, \dots, g_n$  (this time we do take products in  $G$ ). Regarding the  $g_i$  as independent variables, we find that the determinant of  $M'$  is a nonzero polynomial in the  $g_i$  (the coefficient of  $g_1^n$  in it is  $\pm 1$ ). By the algebraic independence of the  $g_i$  there is  $x \in L$  such that the matrix  $M$  obtained from  $M'$  by evaluating each of its entries at  $x$  is nonzero. But this matrix  $M$  is exactly the one whose nonzero determinant forces  $\{g_1(x), \dots, g_n(x)\}$  to be a  $K$ -basis of  $L$ , as desired.

A beautiful representation-theoretic consequence of this result is that *the field  $L$ , regarded as module over the group algebra  $KG$ , is isomorphic to  $KG$  itself, the regular representation of  $G$  over  $K$* . As a cautionary note, we remark that this does *not* mean that all the structural results that we proved last term about the complex group algebra  $\mathbf{C}G$  carry over to  $KG$ , as the field  $K$  is never algebraically closed in this situation. For example, suppose  $G$  is the cyclic group  $\mathbf{Z}_3$  and  $K$  has a primitive cube root of 1. Then  $G$  has exactly three irreducible representations over  $K$  up to equivalence, each of dimension 1 (as it does over  $\mathbf{C}$ ) and  $L$  is isomorphic as a representation of  $G$  to the sum of these representations.

On the other hand, if  $K$  does not have a primitive cube root of 1, then  $G$  has only two irreducible representations over  $K$ , one of dimension 1, the other of dimension 2, and again  $L$  is isomorphic to the sum of these as a representation of  $G$ .

We will spend the rest of the course on commutative algebra, starting with a beautiful class of rings that are closely related to the Galois extensions of fields that we have been studying. We need to recall and generalize a definition that we made last quarter. Let  $L$  be a finite separable but not necessarily Galois extension of a field  $K$  and let  $L'$  be its normal closure (the splitting field of the product of the minimal polynomials for the elements of say a basis of  $L$  over  $K$ ). If  $n$  is the degree of  $L$  over  $K$ , then we know that there are exactly  $n$  distinct  $K$ -homomorphisms  $f_1, \dots, f_n$  from  $L$  into  $L'$ . Given  $x \in L$ , the sum  $\sum_i f_i(x)$  of the images of  $x$  under these homomorphisms is fixed by the Galois group of  $L'$ , so must lie in  $K$ ; we call it the *trace*  $\text{Tr}(x)$  of  $x$ . If in addition  $K = \mathbf{Q}$  and  $x$  happens to be an algebraic integer in  $L$ , then its trace  $\text{Tr}(x)$  is a sum of algebraic integers in  $\mathbf{Q}$ , so is an integer (as we saw in our treatment of the representation theory of finite groups last quarter). The other fact we need about the trace in the special case  $K = \mathbf{Q}$  is that *the map sending the ordered pair  $(x, y) \in L^2$  to  $\text{Tr}(xy)$  is a nondegenerate bilinear form*, that is, that it is bilinear (which is clear) and for all  $x \in L, x \neq 0$  there is  $y \in L$  with  $\text{Tr}(xy) \neq 0$ ; indeed, we need only take  $y = x^{-1}$ . In a similar manner, we define the *norm* of any  $x \in L$  to be the product of the images  $x_i$  of  $x$  under the  $f_i$ ; this too lies in the basefield  $K$ .