Lecture 4-3: Structure of the group algebra

April 3, 2024

In this lecture we analyze the structure of the group algebra kG completely, both as a ring and as a G-module, for every algebraically closed field k whose characteristic does not divide the order of G. We will see that G has only finitely many inequivalent irreducible representations and that they all occur in kG.

For any positive integer r, denote by $M_r(k)$ the ring of $r \times r$ matrices over k.

Theorem

For every algebraically closed basefield k whose characteristic does not divide the order of the finite group G, the group algebra kG is isomorphic to the direct sum $\bigoplus_{i=1}^{m}$ of finitely many rings $M_{n_i}(k)$. Irreducible kG-modules (up to equivalence) are in bijection to summands $S_i = M_{n_i}(k)$ of kG, with the module $M_i = k^{n_i}$ corresponding to the summand S_i, such that S_i acts on M_i by matrix multiplication by column vectors while the other summands (even those isomorphic to S_i) act by 0. In particular, kG is isomorphic as a G-module to the direct sum of n_i copies of k^{n_i} for $1 \leq i \leq m$. The sum $\sum_{i=1}^{m} n_i^2$ of the squares of the n_i equals the order of G.

Proof.

Let M be an irreducible G-module of degree d. Let $m_1, \ldots, m_e$ be linearly independent vectors in M. I claim that $kG(m_1, \ldots, m_e) \subset M^e$ is all of M^e. I prove this by induction on e, the base case $e = 0$ being trivial. If the assertion holds for $e < d$ and $v_1, \ldots, v_{e+1}$ are independent in M, then the projection of $S = kG(v_1, \ldots, v_{e+1})$ to the first e coordinates is all of M^e. Then $N = \{m \in M : (0, \ldots, 0, m) \in S\}$ is a submodule of M; if it is not 0, then it must be all of M by irreducibility, implying the desired result. But if $N = 0$, then for all $(m_1, \ldots, m_e) \in M^e$ there is a *unique* $m_{e+1} \in M$ with $(m_1, \ldots, m_{e+1}) \in S$ and the map sending $(m_1, \ldots, m_e)$ to m_{e+1} is a G-module map. □

Proof.

Its restriction to each copy of M in M^e must then be a scalar, by Schur's Lemma, whence there are $c_1, \ldots, c_e \in k$ with $m_{e+1} = \sum_{i=1}^{e} c_i m_i$. This is a contradiction, since $(v_1, \ldots, v_{e+1}) \in S$ and the v_i are independent. Hence in particular we have $kG(v_1, \ldots, v_d) = M^d$ for any basis $v_1, \ldots, v_d$ of M. In a similar way, if $M_1, \ldots, M_r$ are r inequivalent irreducible G-modules, of degrees $n_1, \ldots, n_r$, and for each i we choose a basis $v_{i1}, \ldots, v_{in_i}$ of M_i, then the tuple v whose coordinates are the v_{ij} is such that $kG(v)$ is all of $M_1^{n_1} \oplus \ldots \oplus M_r^{n_r}$. □

Proof.

This says exactly that kG acts on the direct sum $M' = \oplus_i M_i$ as the sum of matrix rings in the theorem, with $M_i \cong k^{n_i}$. Since the dimension of kG over k equals the order n of G, we see that there are only finitely many inequivalent irreducible G-modules and the sum of the squares of their degrees is at most n. But now if any $x \in kG$ acts by 0 on all irreducible G-modules, then it would have to do so on kG itself, since kG is the sum of its irreducible submodules, forcing $x = 0$. Hence the sum of the squares of the n_i is exactly n, as claimed. □

If we had an explicit isomorphism from kG to the sum of matrix rings, then we could read off the degrees n_i of the irreducible representations from G. We cannot quite do this, but we will now see that we can at least compute the number m of irreducible modules from G.

Theorem: DF, p. 861

The number m of inequivalent irreducible representations of G equals the number of conjugacy classes in G.

Proof.

We compute the dimension of the center Z of kG in two different ways. First, an element of kG is central if and only if it acts on every irreducible representation of G by a scalar, so that as a vector space (and as a ring) Z is isomorphic to k^m. On the other hand, a combination $x = \sum_{g \in G} c_g g$ is central if and only if $hxh^{-1} = x$ for all $h \in G$; but $hxh^{-1} = \sum_{g \in G} c_g hgh^{-1}$, so that x is central if and only if $c_g = c_{hgh^{-1}}$ for all g, h in G. Thus a basis for Z is given by the sums $s_C = \sum_{g \in C} g$ of the elements in C as C ranges over the conjugacy classes in G and m is the number of such classes. □

The elements s_C occurring the preceding proof will soon reappear in the course; we will use them to say more about the scalars arising in applications of Schur's Lemma. For now we will consider some examples. First, if G is abelian, then all of its conjugacy classes have just one element, so the number of its irreducible representations equals the order of G, in accordance with a previous result. Next, if G is the simplest nonabelian group, namely the symmetric group S_3 on three letters, then it has two irreducible representations of degree one. One is the trivial representation on k, where every $g \in G$ fixes all elements of k; the other is the sign representation, also on k, where $g \in G$ acts by 1 if g is even as a permutation and by -1 if g is odd.

Since G has just three conjugacy classes, it has just one more irreducible representation. This must have degree 2, since $|G| = 6 = 2^2 + 1^2 + 1^2$. It is easy to identify this representation. Since G is isomorphic to the symmetry group of an equilateral triangle, whence its elements may be naturally regarded as real or complex orthogonal matrices. Working out the entries of these matrices explicitly, by writing down vertices for the triangle, we see that they make sense over any algebraically closed field k of characteristic different from 2 or 3, so that indeed G has an irreducible representation of degree 2 over k.

In a similar way, the dihedral group D of order 8 has a natural irreducible two-dimensional representation over any field (algebraically closed or not) of characteristic different from 2, arising from its realization as the symmetries of a square in k^2. D has five conjugacy classes, and accordingly four more irreducible representations, necessarily of degree 1. Writing x, y for the generators of D, with x a 90° rotation and y any reflection, we recall that $x^4 = y^2 = 1, yxy = x^{-1}$. If we decree that the 180° rotation x^2 act trivially on k, then, moding out by the central subgroup generated by this element, we get the Klein four-group. Letting the generators of this last group act by ± 1, we obtain the four remaining representations of G.

So far we have studiously avoided working with the matrices arising from a homomorphism π from G to some $GL(V)$; but now the time has come to consider them more carefully. It is too much, however, to understand such matrices all at once. We would like to replace a matrix $\pi(g)$ by a single number $\chi(g)$ that would somehow capture enough information that one could recover $\pi(g)$ from it. At first this would seem like a miracle, but it turns out that we have enough structure in place to perform it.

Definition: DF, p. 866

Given a representation $\pi : G \to GL_n(k)$, its *character* χ is the k-valued function defined by $\chi(g) = \text{tr}\, \pi(g)$, where tr denotes the trace.

Clearly $\chi(g)$ is a class function, meaning that $\chi(g) = \chi(h)$ whenever g, h lie in the same conjugacy class in G. Recall that the trace of any (square) matrix equals the sum of its eigenvalues and that the eigenvalues of $\pi(g)$ are all roots of unity in k. We will continue with character theory next time.