CHAPTER III: GROUP ALGEBRAS AND THEIR MODULES

1. Introduction

Group algebras are special in four different ways. First of all, they are symmetric algebras in the sense discussed at the end of the last chapter. Secondly, there is a character table which sums up much of the useful information about the group and its representations. Thirdly, there are operations of induction and restriction connecting the modules of a group with those of its subgroups. Finally, there is an action of the group itself by conjugation on the group algebra as a whole, which restricts to an action on each individual block. In this chapter we will be concerned mainly with the character table and with operations of restriction and induction. Since these are interesting for ordinary characters as well, we will begin with a review.

2. The ordinary character table

Theorem 2.1. *(Maschke's Theorem) If G is a finite group and R is a complete local Noetherian ring, then RG is R-semisimple if and only if the characteristic of the residue field of R does not divide $|G|$.*

Proof. (Sketch of proof in the case that R is a field K.). $\Rightarrow$: If $char(K)||G|$, then the sum of all elements in G generates a two-sided nilpotent ideal I, so KG cannot be semisimple because $\mathrm{Rad}(KG) \supset I$ and is thus not zero.

$\Leftarrow$: To show that KG is semisimple, it suffices to show that every module M is completely reducible, i.e., that every submodule is in fact a direct summand. Let U be a submodule of M. As a submodule it is surely a vector subspace, and thus a direct summand of M as vector space. Let $\pi : M \to M$ be the projection on the vector subspace V of M. Let us define a new map from M to M which will be invariant under the action of G:

$$\tilde{\pi}(m) = \sum_{g \in G} g \cdot \pi(g^{-1} \cdot m).$$

This map is invariant under the action of G. Its image is thus a KG-submodule of M. The image is clearly contained in V since V is a KG-module, so $\pi(m) \in V$ implies that $g\pi(m)$ is in V. If $m \in V$, then $g\pi(g^{-1}m) = gg^{-1}m = m$. Thus in fact the image is all of V and we

Date: Dec 1, '03.

have a projection, which demonstrates that V is a direct summand of M. $\square$

Note. The proof of the theorem in the more general ring case can be found in Thevenaz. The averaging process which formed the heart of the proof will be used many times in the sequel.

Let us assume that K is a field of characteristic which does not divide the order of the group, and which contains roots of unity for every divisor of the order $|G|$. Since, by Theorem 2.1, KG is semisimple, we set

$$\hat{A} \xrightarrow{\sim} \bigoplus_{i=1}^{t} M_{n_i}(K).$$

Let ρ_i be the projection on the i-th factor.

The center $Z(\hat{A})$ is the sum of the centers of each block, and is thus of dimension t, generated by block idempotents e_i for the blocks, inverse images of the identity matrices in each block.

An alternative basis for the center is given by the conjugacy class sums $\hat{C}_j$, where the C_j, $j = 1, 2, \ldots, t$. For each j, let G_j be a conjugacy class representative. We define as usual the irreducible character $\chi_i(g) = tr(\rho_i(g))$, which can be extended to a linear function on $\hat{A}$. Since the trace function is an invariant under matrix conjugation, χ_i is fixed on each class, the values of the χ_i are completely determined by the character table, the $t \times t$ matrix

$$X = [\chi_i(\hat{C}_j)].$$

Let $M = diag(m_1, \ldots, m_t)$ be the invertible matrix with $m_j = |C_j|$, and let $N = diag(n_1, \ldots, n_t)$ be the invertible matrix with the degrees of the irreducible characters on the diagonal. Since $\hat{C}_j$ is in the center, $\rho_i(\hat{C}_j)$ is a scalar matrix, equal to $w_{ij} I_{n_i}$ for some element w_{ij} of K. Since the representations ρ_i can be defined over R, we may assume that w_{ij} is in R. We now calculate the matrix $W = [w_{ij}]$: By the linearity of χ_i,

$$\chi_i(\hat{C}_j) = m_j \chi_i(g_j).$$

On the other hand,

$$\chi_i(\hat{C}_j) = tr(\rho_i(\hat{C}_j)) = n_i w_{ij}.$$

We conclude that

$$XM = NW,$$

or that

$$W = N^{-1} XM.$$

We also note that since W, being a basis change matrix, is invertible, we get automatically that X is invertible.

Remark 2.1. We quote the following facts from character theory without proof:

(1) The entries in X can be written as sums of powers of a root of unity ζ, that is, as elements of $\mathbb{Z}[\zeta]$.
(2) Using the fact that the e_i are orthogonal idempotents,one can show that the idempotents of the i-th block can be expressed as

$$e_i = n_i/|G| \sum_{g \in G} \chi_i(g^{-1})g. \tag{1}$$

$$= n_i/|G| \sum_{j=1}^{t} \chi_i(g_j^{-1})\hat{C}_j \tag{2}$$

The character value $\chi_i(g)$ is a sum of eigenvalues which are powers of ζ, so $\chi_i(g^{-1})$ is the image $\chi_i(g)$ under the automorphism α of $\mathbb{Z}[\zeta]$ which sends ζ to ζ^{-1}. We let $\overline{X}$ be the matrix obtained from X letting α act on the entries. In the complex case this would be complex conjugation. Since W^{-1} is the base change matrix from the basis $\{\hat{C}_j\}_{j=1}^t$ to the basis $\{e_i\}_{i=1}^t$ of the center $Z(RG)$, the equation in Remark 2.1 (2) means that

$$W^{-1} = (1/|G|)\overline{X}^T N.$$

Multiplying W by the inverse we just constructed, we see that

$$I_t = WW^{-1} = (N^{-1}XM)((1/|G|)\overline{X}^T N) = (1/|G|)X(M\overline{X}^T),$$

since the identity is invariant under conjugation. Using the fact that X commutes with its inverse, we also get

$$I_t = (1/|G|)(M\overline{X}^T)X.$$

This last equation gives orthogonality relations on the columns of the character table, while the previous equation gives orthogonality relations on the rows, with the matrix M appearing in each case.

The matrix W has an additional role in the theory. If we define a linear functional w_i on $Z(KG)$ to give a dual basis to the basis of idempotents,

$$\hat{w}_i(e_k) = \delta_{ik},$$

then the value of w_i on the sum of idempotents in the block containing e_i is 1, since it is zero on every other idempotent in the block and 1 on e_i. Furthermore, the function $\hat{w}_i$ is actually a linear character of KG, that it, it is actually a homomorphism of K-algebras. The value of $\hat{w}_i$ on $\hat{C}_j$ is w_{ij}, the coefficient of e_i in the expression for $\hat{C}_j$ in that basis. Since the $w_{ij} \in R$, this means that the restriction w_i of $\hat{w}_i$ to $Z(RG)$ maps to R. It is still a linear character. Consider now the restriction of $Z(kG)$. A linear character must send the radical to zero, since the quotient is semisimple. The only linear functionals on k^t which are actually linear characters are those sending one block idempotent to 1, while the radical and all the other block idempotents to 0. Thus the number of possible linear characters equals the number of blocks. The linear character w_{ij} of $Z(RG)$ is an algebra homomorphism and must thus reduce to an algebra homomorphism mod $\mathcal{M}$. The only candidate is the character which sends the block idempotent to 1 and the other block idempotents to zero.

Thus, in order to determine which K-characters belong together in one block, it suffices to reduce the matrix W modulo the maximal ideal $\mathcal{M}$ of R, and see which rows are identical.

Example 2.1. For D_6, over a field of characteristic 3, we have

$$X = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 \\ 2 & 2 & -1 & -1 & 0 & 0 \\ 2 & -2 & -1 & 1 & 0 & 0 \end{bmatrix}, \text{and} \quad W = \begin{bmatrix} 1 & 1 & 2 & 2 & 3 & 3 \\ 1 & -1 & 2 & -2 & 3 & -3 \\ 1 & 1 & 2 & 2 & -3 & -3 \\ 1 & -1 & 2 & -2 & -3 & 3 \\ 1 & 1 & -1 & -1 & 0 & 0 \\ 1 & -1 & -1 & 1 & 0 & 0 \end{bmatrix}.$$

Reducing modulo 3, we see that the odd rows lie in one block, and the even rows in another.

Exercises:

(1) Write out explicitly the orthogonality relations between rows of the character table and between columns.
(2) Find the blocks of D_6 for characteristic 2. Calculate the idempotents of corresponding to the rows in R, and add them together to get the block idempotents.
(3) Calculate W and W^{-1} for S_3, with $K = \mathbb{C}$.

3. Induction and restriction

We let G be a finite group such that p divides the order of G. If an integer n equals $p^a m$, with m relatively prime to p, we call p^a the p-part of n and denote it by n_p. Similarly the integer m is called the p'-part of n and designated by n'_p.

Hypothesis 3.1. *We assume that R is a complete discrete valuation ring, with maximal ideal $\mathcal{M}$ generated by an element π, and that $\mathcal{M}$ contains the rational prime p which is the characteristic of the residue field $k \xrightarrow{\sim} R/\mathcal{M}$. We assume that k is a splitting field for G, and in fact contains an $|G|_{p'}$-root of unity ξ. We further assume that the quotient field K of R has characteristic 0.*

Definition 3.1. A finitely-generated RG-module is called an $R-$ *lattice* if it is free as an R-module.

Let G be a finite group, and let H be a subgroup. Any RG-lattice M is an RH-lattice with the same underlying set and thus the same rank as a free module over R. This RH-lattice is call the *restriction* of M to H, and is denoted by M_H.

In the opposite direction, we can convert an RH-lattice N to an RG-lattice just by tensoring with RG, and we denote the lattice *induced* from N by N^G. Letting $g_1, g_2, \ldots, g_m$ be a transversal to H, i.e., a complete set of coset representatives, then

$$RG \otimes_{RH} N = \bigoplus g_j H \otimes_{RH} N = \bigoplus g_j \otimes_{RH} N.$$

The number m of cosets is the index $[G : H]$, and thus the rank of N^G is $[G : H]$ times the rank of N.

We collect several useful results about induction and restriction. Proofs of these facts can be found in the standard texts.

Lemma 3.1. (1) *If $K \leq H \leq G$, and N is an RK-lattice, then $(N^H)^G = N^G$.*
(2) *$(U_1 \oplus U_2)^G = U_1^G \oplus U_2^G$.*
(3) *If N is a projective RH-lattice, N^G is a projective RG-lattice.*

The most important result about induction and restriction for this book is the following:

Theorem 3.1. *(Mackey's theorem) Let G be a finite group. We assume that L and H are two subgroups of G, and that I is a set of representatives of the double cosets $H \setminus G/L$. Then if N is a L-lattice, we have the following decomposition of the induction to G followed by restriction to H:*

$$(N^G)_H = \bigoplus_{s \in I} s \otimes N^H_{sLs^{-1} \cap H}.$$

Proof. We decompose the set of cosets $H \setminus G$ into orbits under the right action of L, i.e., into double cosets. The set I consists of representatives of these orbits. If $s \in I$, then the stabilizer of Hs inside its orbit consists of all elements k of L such that $sk \in Hs$, that is, $sLs^{-1} \cap H$. The cosets of H in G induce a decomposition of RG into RH-lattices. The double cosets induce a decomposition of RG into sublattices which are RH-lattices on the left, and RL-lattices on the right. Since $RHsL$ is a right RL-lattice, we can form a tensor product with the L-lattice N, getting $RHsL \otimes_{RL} N \xrightarrow{\sim} RHsLs^{-1} \otimes_{RsLs^{-1}} (s \otimes N)$. On the other hand, we also have that

$$RHsLs^{-1} \otimes_{RsLs^{-1}} (s \otimes N) \xrightarrow{\sim} RH \otimes_{R(sLs^{-1} \cap H)} (s \otimes N)_{sLs^{-1} \cap H},$$

which gives the desired direct sum decomposition.

□

Exercises.

(1) Calculate the module induced from the top of kH for H a cyclic subgroup of order 2, to S_3.
(2) Restrict the module in the previous exercise to C_3, using the Mackey decomposition theorem.

(3) Let M be the one of the nontrivial linear representations of order 6 in C_6. Calculate M^G, where $G = D_6$.
(4) Induce and restrict a nonprojective module for two subgroups of A_4.
(5) To what does Mackey's theorem reduce if L is normal? Explain.

4. Character tables for solvable groups

The construction of character tables for a general group is rarely done by actually constructing representations and then taking traces. Instead, one uses the operations of induction and restriction to get part of the table and fills in the remaining values using the orthogonality relations for the rows and coluns of the character table.

In the case of solvable groups, the character table is almost completely determined by induction from a maximal normal subgroup. This is an application of the more general *Clifford theory* for induction from a normal subgroup, but for this book we will restrict ourselves to the relatively uncomplicated case of a subgroup of prime index p, where p is not the characteristic of the field K. In fact, we will assume that the characteristic of the field is either 0 or is relatively prime to the order of the group. Let G be the group, H the normal subgroup of index p, and a an element of a p-Sylow subgroup P of G which is not in $P \cap H$, so that a is an element of p-power order which generates the quotient group.

Conjugation by a induces an automophism of H and thus permutes the characters of H. Since a^p, as an element of H, induces the trivial permutation of the characters, all orbits are of length 1 or p. Assume that the orginal character, ϕ, was of degree d.

Case 1: If the orbit is of length one, then the block idempotent of the character will still be central in KG. It cannot, however, be primitive, since the dimension of the block corresponding to the original character $\phi$was a perfect square, d^2, and the projective module generated by this idempotent is of dimension pd^2, which surely is not a perfect square. One can show that in this case, the block of H of degree d splits into p blocks of degree d, which are identical to the original ϕ when restricted to H, and differ only on the values for the other cosets of H.

Case 2: If the orbit is of length p, then the original block idempotents are no longer central, but their sum is. This is a new idempotent generating a projective module of dimension d^2p^2. This corresponds to a new irreducible character *chi* of degree dp, which is the sum of the original characters on H, and is zero on all other cosets of H. Of course, some of the conjugacy classes in H coallesce into a single class in G, because the action of a permutes the conjugacy classes of H. This permutation of conjugacy classes, in fact, is enough to determine the permutation of the characters.

Example 4.1. Let D_n be a dihedral group, with normal cyclic subgroup C_n of index 2, generated by b. Let a be an element of order 2 such the $ba = ab^{-1}$. Since C_n is abelian, every element is a separate conjugacy class, so action by a interchanges the class of b^j and the class of b^{-j} for all j. Let ζ be an nth root of unity. The rows of the character table of C_n are the characters ϕ_i defined by $\phi_i(b^j) = \zeta^{ij}$, for $i = 0, \ldots, n-1$. The action of conjugation by a then interchanges the values ζ^{ij} with ζ^{-ij}. on the rows this corresponds to switching ϕ_i with ϕ_{n-i}, and leaving ϕ_0 fixed. If n is even, then the row $\phi_{n/2}$ is also fixed, as is the conjugacy class of $b^{n/2}$. Since $bab^{-1} = ab^{-2}$, the conjugacy class of a consists of all the elements ab^{2j}. If n is odd, this is has n elements and contains all the elements of aH. If n is even, this has $n/2$ elements, and there is a second conjugacy class in aH containing all the elements $ab^{2j+(n/2)}$.

In the character table of D_n, the fixed characters each split into two, identical on H, and differing as to whether a has the value 1 or -1. If n is even, the value on the conjugacy class of $ab^{n/2}$ is the product of the value on a and the value on $b^{n/2}$. The rows which are permuted are added together. They will now have the same values $\zeta^{ij} + \zeta^{-ij}$ on b^j and b^{-j}, so these give a single column in the character table of G. See Example 2.1.

Example 4.2. More generally, when ever H is an abelian normal subgroup of G with prime index p, the irreducible characters all have degrees 1 or p. Furthermore, since an abelian group is a direct product of cyclics, and the characters in a direct product are the products of the character of the components, we can easily comppute the entire character table for G, since the characters which split are all linear characters splitting to linear characters, and thus the characters are actually homomorphisms of groups, so that the character values are all determined b the value at a. As an example, we give the character tables of $H = C_2 \times C_2$ and $G = A_4$, where ω is a third root of unity.

$$X_H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, X_G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega^2 \\ 1 & 1 & \omega^2 & \omega \\ 3 & -1 & 0 & 0 \end{bmatrix}$$

/endexamp

Exercises:

(1) Calculate the character table for D_7.
(2) Prove Cases 1 and 2 above as special cases of the following general theorem from Clifford theory:

If G is a finite group, N is a normal subgroup, and χ is an irreducible character of KG, then there are characters ϕ_i of N, conjugate with respect to G, and an integer e, such that

$$\chi = e(\sum_i \phi_i).$$

(3) The character table of the quaternion group Q_8 is identical to the character table of D_8. The group Q_8 has an automophism which cyclically permutes i,j, and k. Show that the character table of $SL(2,3) \tilde{\to} Q_8 \ltimes C_3$ contains three characters of degree 1, one character of degree 3, and three characters of degree 2.

(4) * Fill in the missing values in the character table of $SL(2,3)$, either by using orthgonality relations, or by using the fact that in a degree two representation of an element of order 3, the eigenvalues must be either 1 or one of the two cubed roots of unity, and the eigenvalues for the inverse must be inverses to these.

5. Brauer characters

We assume as before that R is a complete discrete valuation ring, and in addition we assume that the residue field k is sufficiently large be a splitting field for G, and to contain a root of unity ξ for the p'-part of the order $|G|$ of G As stated in the introduction, we want the ring R to serve as a bridge between the residue field k of characteristic p and the quotient field K of characteristic 0.

We have already proven in Chapter II that every unit in k lifts to a unit in R. Thus $R^* \to k^*$ is surjective. Since the ring is local and thus the unique maximal ideal is the radical, every element in $1+\mathcal{M}$ is invertible, so this is the kernal of the surjection. Thus we have a short exact sequence

$$1 \to 1+\mathcal{M} \to R^* \to k^* \to 1.$$

If k is algebraically closed this sequence splits uniquely, so that k^* can be regarded as a subgroup of R^*.

Hypothesis 5.1. *We assume henceforward that k is sufficiently large that k^* embeds uniquely in R^*.*

In particular, the root of unity ξ for the p'-part $|G|_{p'}$ of $|G|$ has a unique lifting to R^*. This is in contrast to the p-th root of unity, 1, which splits into p distinct roots in R.

Since characters are so useful in studying ordinary respresentations, we wish to introduce characters to the study of modular representations as well. Unfortunately, the technique of representing a simple module and taking traces is not adequate, because if any eigenvalue appears p times on the diagonal, it is lost modulo p.

The solution which Brauer found was to concentrate on those character values for which there is a unique lifting to R, namely the character values for the elements of order prime to p, all of which are sums of powers of the root of unity ξ.

Definition 5.1. An element h of G is called p-regular if p does not divide $|h|$.

Lemma 5.1. *If H is a p'-group, then every simple kH-module M lifts uniquely to an RH-lattice N, such that*

$$M \xrightarrow{\sim} N/\mathcal{M}N.$$

Proof. In kH, every simple module is projective, isomorphic to $kH\overline{e}_i$ for some primitive idempotent $\overline{e}_i$. We lift to an idempotent e_i of RH. This generates a projective module N of RG. Any other lifting of the idempotent is conjugate, so all possible choices of N are isomorphic. Since kH is semisimple, and $\mathrm{Rad}(RH) \supset \mathcal{M}$, we have that $\mathrm{Rad}(RH) = \mathcal{M}RH$. Thus $N/\mathcal{M}N$ is the simple module generated by $\overline{e}_i$. By Maschke's theorem, every RH-lattice is projective. If it is not indecomposable, then its image modulo its radical is not indecomposable and in particular is not simple. Any indecomposable module whose top lies in the designated simple of kH is generated by an idempotent which is conjugate to e_i, and thus is isomorphic to N. □

Definition 5.2. If M is a simple kG-module, and h is a p-regular elements of G, then we define the value $\phi_M(h)$ of the *irreducible Brauer character ϕ_M* at h by restricting M to the cyclic subgroup $H =< h >$, lifting the corresponding H-module uniquely to an RH-module, and then taking the character value of the lifted module in R at h.

The irreducible Brauer character is fixed on conjugacy classes, since conjugate elements induce conjugate cyclic subgroups, and conjugate liftings of modules. One can define a Brauer character for any kG-module V, also denoted by ϕ_V, by taking the sum of the indecomposable Brauer characters of its composition factors, with appropriate multiplicities.

Lemma 5.2. *The set of all irreducible Brauer characters forms an R basis for the space of class functions from the p-regular conjugacy classes of G to R, and the number of simple kG-modules equals the number of p-regular conjugacy classes.*

Lemma 5.3. *If P is a projective RG-lattice, then, χ_P, the ordinary character of P, satisfies $\chi_P(g) = 0$ for every g which is not p-regular. The set of characters χ_P for a set of indecomposable P is a K-basis of the set of class functions on the p-regular classes of G.*

Example 5.1. The case when the p-Sylow subgroup P is normal is of particular importance. In this case, by the Zassenhaus lemma, G has a complementary subgroup H of p'-order, and

$$G/P \xrightarrow{\sim} H.$$

For any normal subgroup N of G, here is a one-to-one correspondence between characters of G/N and characters of G with kernal N, i.e., such that the value of the character on every element of N is the same as the value of the character on the identity of the group. Thus in the case where the normal subgroup is the p-Sylow subgroup P with complement H, the characters of H are in one-to-one correspondence with characters of G with kernal P. Furthermore, the conjugacy classes of H remain distinct in G, since if $k \in P$ and $h \in H$, then $k^{-1}hk = hk'$ for some $k' \in P$. Since the restriction of the characters of H are linearly independent on the conjugacy classes from H, they form a basis for the set of Brauer characters of G.

Exercises.

(1) * Let G be D_6, the character table of which was given in an earlier exercise. Let $p = 3$. Show that the characters which have P in their kernal form a complete set of irreducible Brauer characters when restricted to p-regular classes.
(2) Let R be $\mathbb{Z}_2$. Let G be S_3. Find the liftings of the projective modules to RG and show that the characters vanish on elements of order divisible by 2.
(3) Show that if G is a group with normal p-Sylow subgroup P, then the characters with kernal containing P form a complete set of Brauer characters for the group, with all details.
(4) If G is a group with a normal abelian p-Hall subgroup H, i.e., $|H|$=$|G|_{p'}$, show that the Brauer characters are in one-to-one correspondence with conjugacy classes of characters of H.

6. Decomposition numbers

In the previous section we started with a simple kG-module and produced a function from the p-regular conjugacy classes into R. Now we are going to start with a simple KG-module, and try to express its character as a linear combination of irreducible Brauer characters, with positive integral coefficients.

Let $\hat{W}$ be a simple KG-module. Take a K-basis, and consider the RG-module W with this basis. Then $\hat{W} \xrightarrow{\sim} W \otimes K$. The RG-lattice W is not uniquely determined.

Example 6.1. In S_3 there is a unique simple module of dimension 3. Let R be the local ring $\mathbb{Z}_{(p)}$, obtained from $\mathbb{Z}$ by inverting every element not divisible by p. The quotient field is $\mathbb{Q}$. The following is a representation of S_3 via this module:

$$a \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, b \mapsto \begin{bmatrix} -1/2 & 3/2 \\ -1/2 & -1/2 \end{bmatrix}.$$

Since the entries of the matrix are elements of R, this is actually an R module, L. The transposes of this representation give a second representation, L'. In both cases, tensoring with K produces a faithful representation, and since the only two-dimensional representation of S_3 which is faithful is the unique simple, we must have

$$K \otimes L \xrightarrow{\sim} K \otimes L'.$$

However, the two modules are not, in fact, isomorphic as R-modules. Any matrix D which leaves the image of a fixed under conjugation must in fact be diagonal, and no such matrix will act on b as a transpose, so in fact the two RG-modules are not isomorphic. This shows that the lifting L of a simple K-module is not unique.

In terms of kG-modules, let e_1 and e_2 be the two primitive idempotents of kG. One of L and L' corresponds in kG to the quotient of kGe_1 by its socle, and the other to the quotient of kGe_2 by its socle. Although they are not isomorphic, they do have the same composition factors, one copy of each of the two simples in kG.

We are now prepared to define the decomposition numbers:

Definition 6.1. Let $\chi_1, \ldots, \chi_t$ be the characters of the simple KG-modules, and let $\phi_1, \ldots, \phi_r$ be the irreducible Brauer characters. Then the *decomposition number* d_{ij} is the multiplicity of the simple module corresponding to ϕ_j as a composition factor in the kG-module $\overline{L}$ obtained by lifting the simple KG-module to a RG-lattice L and then taking the residue modulo $\mathcal{M}$ to obtain a kG-module. The matrix $[d_{ij}]$ is called the *decomposition matrix.*

In order for the decomposition numbers to be well-defined, we must show that, as happened in Example 6.1, the composition factors for two different liftings will be the same.

Lemma 6.1. *Suppose that M is a simple KG-module with character χ_i. Let L be a lifting to RG, and let $\overline{L}$ be the restriction to kG. The multiplicities of the composition factors of $\overline{L}$ are independent of the choice of L.*

Proof. The restriction of χ_i to the p-regular classes is a class function on these classes, and since the character values lie in R, we have that χ_i can be expressed in a unique way as an R-linear combination of the ϕ_j, since, as quoted in Lemma 5.2, these are linearly independent. If L and L' are two liftings of M, then each has character equal to χ_i on the p-regular classes, and each induces a $\mathbb{Z}$ linear combination of the ϕ_j with coefficients determined by the multiplicities of the composition factors. Since $\mathbb{Z}$ is a subring of R, these two decompositions have coefficients in R, so by the uniqueness, the multiplicities of the composition factors of the two modules must coincide. $\square$

There is another, equivalent way of calculating the decomposition numbers. Choose a complete orthogonal set of idempotents $\overline{f}$ of simple modules for kG and lift them, by straightening out, to a set of idempotents for RG, which will, in fact, be idempotents in KG. Now multiply these idempotents by block idempotents e_i of KG. The decomposition number d_{ij} will be the number of primitive idempotents in $f_j e_j$, divided by the degree of f_j.

Example 6.2. Let G be $P \triangleright H$, where H is a p'-groups, and k is a field of characteristic p. The Brauer characters correspond to the ordinary characters of H. Thus the decomposition matrix contains an identity matrix for these characters.

Example 6.3. In A_5, the character table, with elements of order 1,2,3,5, and 5, is

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 3 & -1 & 0 & A & B \\ 3 & -1 & 0 & B & A \\ 4 & 0 & 1 & -1 & -1 \\ 5 & -1 & -1 & 0 & 0 \end{bmatrix}$$

In this case the Brauer characters when $p = 2$ are not all restrictions of any ordinary characters, but rather chi_1, $\chi_2 - \chi_1$, and $\chi_3 - \chi_1$.

The row of degree 4 is a block by itself, of dimension 16. The decomposition matrix is for the other block, of dimension 44, is:

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

The Cartan matrix, described in Chapter II, is closely related to the decomposition matrix. Let us recall that column j of the Cartan matrix consists of the multiplicities of the various simples of kG in a composition series for the projective module $\overline{P}_j$, whose top is the simple module $\overline{S}_j$. The projective module $\overline{P}_j$ lifts to an RG-module P_j, and thence it induces a KG-module $\hat{P}_j$. Let a_{sj} be the multiplicity of the simple KG-module W_s in $\hat{P}_j$, so

$$\hat{P}_j = \sum a_{sj} W_s.$$

Taking the Hom into W_s and noting that there are no ontrivial homomorphismas between nonisomorphic simples, we get

$$a_{sj} = dim_K(\mathrm{Hom}_{KG}(\hat{P}_j, W_s)).$$

(We have essentially used duality at the point, for this works because KG is a symmetric algebra.) However, these homomorphisms correspond to RG-homomorphisms. Recall that W_s lifts non-uniquely to an RG-module L_s, in such a way that

$$a_{sj} = dim_k(\mathrm{Hom}_{kG}(\overline{P}_j, \overline{L}_s) = d_{sj},$$

since the number of homomorphisms of a projective module into another module is the number of times its top occurs as a composition factor.

Thus, altogether, the number c_{ij} of times that $\overline{S}_i$ occurs as a composition factor in the projective $\overline{P}_j$ is the sum of the number of times S_i occurs in each L_s, times the numer of times W_s occurs in a decomposition of P_j. In short,

$$c_{ij} = \sum_s d_{si} d_{sj}.$$

Thus $C = D^T D$, and is thus symmetric. No such result holds for nonsymmetric algebras.

The decomposition matrix actually decomposes into a diagonal series of rectangular matrices corresponding to the different blocks of kG. For a given block B, the decomposition matrix of the blocks, D_B is a matrix with $k(B)$ rows, where $k(B)$ is the number of irreducible character of G associated with the block. The number of columns $\ell(B)$ is the number of simple modules in the block. Unless B is a matrix block, in which case $k(B) = \ell(B) = 1$, we always have $k(B) > \ell(B)$. The sum of the $k(B)$ for the various blocks is t, the number of irreducible characters. The sum of the $\ell(B)$ is the number of p-regular classes. The Cartan matrix of a block cannot be decomposed any further, for if it could, the projectives could be separated into two sets with no homomorphisms between them, and since the quiver of a block is connected, this is impossible. The decomposition matrix of a block is also indecomposable, for otherwise there would be a decomposition of the Cartan matrix.

Example 6.4. Let G be D_5, $p = 5$. We wish to calculate the decomposition matrix. In RG there are two indecomposable projective modules, $P_1 = Ae_1$ and $P_2 = Ae_2$, each of rank 5 as R-modules. In the reduction of P_1 modulo 5, the simple S_1 has multiplicity 3 and the simple S_2 has multiplicity 2. In $\overline{P}_2$, the multiplicities are reversed. In KG, there are four isomorphism classes of simple modules, W_1 and W_2 of dimension 1, and W_3 and W_4 of dimension 2, as shown by the degrees of the character table. Take as bases of W_1 and W_2 the block idempotents g_1 and g_2, as basis of W_3 the matrix units E^3_{11}, E^3_{21} and as basis of W_4 the matrix units E^4_{22}, E^4_{12}. Let b be a generator of the normal subgroup C_5. Over K, abelian group algebra KC_5 has five idempotents f_i, with

$$f_i = \sum_{j=0}^{4} \xi^{-ij} b^j.$$

The block idempotent of W_3 is $g_3 = f_1 + f_4$, and the block idempotent of W_4 is $G_4 = f_2 + f_3$. Since we are in the situation of a normal p-Sylow subgroup,we may choose $e_1 = (1/2)(e + a)$ and $e_2 = (1/2)$(e-a) be idempotents of a 2-sylow subgroup. Then we may choose $E_{11}^3 = e_1 g_3$ and $E_2 2^4 = e_2 g_4$. Let $x = b - b^{-1}$. Then it can be checked that e_1, $xe_1, \ldots,$ $x^4 e_1$ is a basis for P_1, and that e_2, $xe_2, \ldots$ $x^4 e_2$ is a basis for P_2. Either W_3 or W_4 can be lifted to the quotient of either P_1 or P_2 by its radical squared. In all posible liftings, the composition factors are two distinct simples. The decomposition matrix is and Cartan matrix are

$$D = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}, C = \begin{bmatrix} 3 & 2 \\ 2 & 3 \end{bmatrix}.$$

The orthogonality relation for columns,

$$M\overline{X}^T \cdot X = |G| I_t,$$

induces a form of blockwise orthogonality relations between p-regular columns and p-singular columns for any fixed block. (Curtis and Reiner, p.690)

Lemma 6.2. *For the rows in any fixed block, the product of a column corresponding to a p-regular class and a p-singular class is zero.*

Proof. Let F be the invertible square $s \times s$ matrix of Brauer characters on the p-regular classes, let D be the $t \times s$ decomposition matrix, and let Y be the $(t-s) \times s$ submatrix of $\overline{X}^T$ consisting of rows corresponding to p-singular classes, and let X_{reg} be the $s \times t$ matrix of p-regular columns, so the $X_{reg} = D \cdot F$. Then

$$0^{(t-s)\times s} = Y \cdot X = Y \cdot D \cdot F.$$

Since F in nonsingular,

$$Y \cdot D = 0.$$

If we have numbered the rows of F to separate Brauer characters into different blocks, then there is actually a separate equation for each block, involving only the rows of that block. Multiplying by the corresponding rows of F gives the desired orthogonality relation. □

In addition to the ordinary decomposition numbers, which are positive integers, we can also consider *generalized decomposition numbers*, which make use of information in the columns of the character table corresponding to elements which are not p-regular. The combination of all the decomposition numbers is a square $t \times t$ matrix. We will put off a detailed discussion of the generalized decomposition matrix until the next chapter.

Exercises:

(1) Construct decomposition matrices for D_6, for p=2,3.

(2) From the fact that the decomposition matrix decomposes into rectangular blocks, and that the Cartan matrix $C = D^t D$, conclude that the Cartan matrix decomposes into a diagonal series of square matrices.
(3) Check that the Brauer characters given in Example 6.3 do generate all the characters in the block.
(4) Find the decomposition matrix for A_4, for p=2, using the fact that the p-Sylow is normal.