Introduction to modular representation theory of finite groups

Yassine El Maazouz

Abstract. The main aim of this paper is to give a short presentation of the theory of modular representations for finite groups. We will go through some fundamental results and provide some comments and a few proofs. When a proof is long or complicated we shall instead give a reference to another source.

Introduction à la théorie représentations modulaires des groupes finis

Résumé. Ces notes ont pour objectif de prśenter la théorie des représentations modulaires des groupes finis. Nous allons revisiter quelques résultats fondamentaux tout en en discutant les preuves et les conséquences. Cependant, dans le cas ou une preuve est longue ou compliquée nous dirigerons le lecteur vers d'autres sources.

1. Introduction and notation

In representation theory of a finite group (or compact group) G over $\mathbb{C}$, any space can be made invariant by averaging the action of G. For finite groups this of course involves dividing by the order $|G|$ of G whereas for compact groups one divides by the Haar measure of G. Averaging is then a very central tool in this theory.

In this paper, we are interested in representation theory of a finite group $|G|$ over a field k of positive characteristic p. When the order $|G|$ is not divisible by p, the theory is not so different from the complex case. However, when p divides $|G|$, the averaging argument no longer works since $|G| = 0$ in the field

(1) U.C. Berkeley, Department of statistics, 335 Evans Hall #3860 Berkeley, CA 94720-3860 U.S.A. — yassine.el-maazouz@berkeley.edu

k. The theory is then different from the complex case and is called modular representation theory.

This theory establishes deeper connections between the structure of the group G and its representations. The main results are due to Brauer who has manged to prove a long series of important results [Bra74a, ABG73, Bra76a, Bra76b, Bra74b, Bra79a, Bra79b]. To set things up, we start by introducing some notation.

Consider G a finite group with order $|G|$. Let K be an algebraic number field, that is a finite algebraic extension of $\mathbb{Q}$. We denote by $\mathcal{O}$ the integral closure of $\mathbb{Z}$ in K. The ring $\mathcal{O}$ is a Dedekind domain. Let P be a prime ideal of $\mathcal{O}$ and p the unique prime in $\mathbb{Z}$ such that P lies over p. We denote by k the residue field $k := \mathcal{O}/P$. The situation is summarized in the following diagram:

$$\begin{array}{ccccc} k & & P & \longrightarrow & \mathcal{O} & \longrightarrow & K \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ \mathbb{Z}/p & & p & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Q} \end{array}$$

Let v be the additive valuation map on K associated to the prime ideal P. We normalize v such that $v(p) = 1$. Let π be an element of P with minimal valuation. The element π is called a uniformizer of K and its valuation $v(\pi) = e$ is the ramification index of p in $\mathcal{O}$. Let $\mathcal{O}_P := \{x \in K, v(x) \geqslant 0\}$ be the valuation ring of v. This is a local ring with unique maximal ideal $\pi\mathcal{O}_P$.

In our discussion, we will also need the P-adic completion $\widehat{K}$ of K with respect the valuation v. Similarly, we denote $\widehat{\mathcal{O}}$ the ring of integers of $\widehat{K}$ and $\widehat{P} = \pi\widehat{\mathcal{O}}$. The residue field $k = \mathcal{O}/P = \mathcal{O}_P/\pi\mathcal{O}_P = \widehat{\mathcal{O}}/\widehat{P}$, is a finite extension of the finite field $\mathbb{F}_p := \mathbb{Z}/p$. Its degree f is the inertia degree of p in P, so $k = \mathbb{F}_{p^f}$.

We are interested in k-representation of the group G when $|G|$ is divisible by the prime p. The reason we wish to see k as a residue field of an algebraic number field K, is because we can get a collection of k-representation from each K-representation of G.

For further reading, and more details we refer the reader to the Serre's book [Ser77] as well as Curtis and Reiner's books [CR66, CR81]. These note follow the chapter on modular representations in [CR66].

2. Preliminaries on modular representations

Before we introduce the main players, let us first recall some facts on integral representations. These are representations of G with matrices that have entries in a ring. This is different from the usual theory when the entries are in a field, because many of the usual basic properties fail to hold. We will mainly consider representation with entries in a principal ideal domain. That is our main concern will be $R[G]$ modules, where R is a principal ideal domain.

2.1. Some preliminaries on integral representations

Let $L \coloneqq \mathrm{Frac}(R)$ be the fraction field of R and M be a finitely generated torsion-free module over $R[G]$. Since R is a principal ideal domain, this just means that M has a finite R-basis. Such a module is called an R-representation of G. Fixing an R-basis of M, this representation can be thought of as a group isomorphism $\rho : G \to \mathrm{GL}_n(R)$. Two R-representations $\rho, \sigma : G \to \mathrm{GL}_n(R)$ are R-equivalent if they are intertwined by a R-isomorphism of modules. That is if there exists a matrix $A \in \mathrm{GL}_n(R)$ such that

$$\rho(g) = A\sigma(g)A^{-1} \text{ for all } g \in G.$$

To an R-representation M of G we can associate an L-representation by scalar extension, i.e, by considering the $L[G]$ module $L \otimes M$ where $g \in G$ acts as

$$g.\left(\sum_i \alpha_i \otimes m_i\right) = \sum_i \alpha_i \otimes g.m_i.$$

So if $e_1, \ldots, e_n$ is an R-basis of M, we get a basis $1 \otimes e_1, \ldots, 1 \otimes e_n$ of the vector space $L \otimes M$. Thus we can think of R-representations as representations over the field L. We can also think of M as a submodule of $L \otimes M$ by identifying $m \in M$ with $1 \otimes m$. So each representations of G over R is contained in an L-representation.

Conversely, each L-representation of G contains a representation over R. To see why, let V be a representation over L with basis $e_1, \ldots, e_n$ and define the $R[G]$-module M as follows:

$$M = \sum_{g \in G} \sum_{i=1}^{n} Rg.e_i.$$

This is a torsion free, finitely generated module over R. So it is a representation of G over R. Moreover, since $V = L \otimes M$, the module M has rank $\dim_L(V)$ over R.

In our case, we take the ring R to be $\mathcal{O}_P$ which is a local ring, and hence in particular a principal ideal domain. And from representations of G over the number field K, we can get representations of G over the ring $\mathcal{O}_P$. Modulo the prime ideal $\pi\mathcal{O}_P$, these integral representations become representations over the finite residue field k. As we shall explain next, we get a collection of k-representations from a single representation over K.

2.2. First results on modular representations

Let $\rho : G \to \mathrm{GL}(V)$ a representation of G, where V is a vector space of dimension n. This is a $K[G]$-module and as explained in the previous subsection, it contains $\mathcal{O}_P[G]$-modules of rank n. So, by choosing different basis of V, the representation ρ gives a collection of $\mathcal{O}_P$-representations $(\sigma_i)_{i\in I}$. While these representations are clearly K-equivalent, they are not necessarily $\mathcal{O}_P$-equivalent.

EXAMPLE 2.2.1. — *Let $G = \mathbb{Z}/2\mathbb{Z} = \langle x\rangle$ a group of order 2 and two matrices*

$$g_1(x) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad g_2(x) = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}.$$

The polynomial X^2-1 is the characteristic polynomial of both these matrices and since it has simple roots they are equivalent. More explicitly, if $A = \begin{pmatrix} 1 & 1 \\ 0 & -2 \end{pmatrix}$, we have

$$g_2(x) = Ag_1(x)A^{-1},$$

with $A^{-1} = \frac{1}{2}\begin{pmatrix} 2 & 1 \\ 0 & -1 \end{pmatrix}$. So these two representation or equivalent over $\mathbb{Q}$. However, they are not equivalent over the local ring $\mathbb{Z}_{(2)}$. This is because the two matrices $g_1(x), g_2(x)$ are not equivalent over the residue field $\mathbb{Z}/2$.

Notice however that the two $\mathbb{Z}_{(2)}[G]$-modules given by these representations have the same composition factors. This is actually a general result due to Brauer and Nesbitt [BN41].

THEOREM 2.2.2. — *Two k-representations σ_1, σ_2 obtained from the same K-representation ρ have the same composition series.*

Proof. — Let $n := \dim(\rho)$ and π_1, π_2 a pair of $\mathcal{O}_P$-representations from ρ with $\overline{\pi_i} = \sigma_i$ for $i = 1, 2$. The two representations π_1, π_2 are K-equivalent. So there exists a matrix $A \in \mathrm{GL}_n(K)$ such that for any $g \in G$ such that $\pi_1(g)A = A\pi_2(g)$. Since $\mathcal{O}_P$ is a discrete valuation ring with fraction field K, we can assume that A has entries in $\mathcal{O}_P$ with at least one entry in $\mathcal{O}_P^\times$ (if not we can simply multiply by a large enough power of π). Let's denote by $\overline{A}$ the image

modulo $\pi\mathcal{O}_P$ of A. If $\overline{A}$ is invertible, then we simply have $\overline{\pi_1(g)}\overline{A} = \overline{A}\overline{\pi_2(g)}$ hence $\sigma_1(g)A = A\sigma_2(g)$. So we deduce that σ_1, σ_2 are k-equivalent and hence have the same composition factors. Now, if $\overline{A}$ is not invertible let's pick two matrices $U, V \in \mathrm{GL}_n(\mathcal{O}_P)$ such that

$$k[UAV = \begin{pmatrix} C & 0 \\ 0 & \pi D \end{pmatrix},$$

where $C \in \mathrm{GL}_r(\mathcal{O}_P)$ for $r \leqslant n$ and $D \in \mathrm{GL}_{n-r}(K)$ with entries in $\mathcal{O}_P$. If we set

$$\pi_1'(g) = U\pi_1(g)U^{-1} \text{ and } \pi_2'(g) = V^{-1}\pi_2(g)V,$$

then π_1' and π_2' are K-equivalent because we have $\pi_1'(g)UAV = UAV\pi_2'(g)$. Since U, V are in $\mathrm{GL}_n(\mathcal{O}_P)$, to show that σ_1, σ_2 have the same composition factors, it suffices to show that $\sigma_1' \coloneqq \overline{\pi_1'}$ and $\sigma_2 \coloneqq \overline{\pi_2'}$. Let us write the representations π_1' and π_2' in matrix form as

$$\pi_1'(g) = \begin{pmatrix} X_1 & Y_1 \\ Z_1 & T_1 \end{pmatrix} \text{ and } \pi_2'(g) = \begin{pmatrix} X_2 & Y_2 \\ Z_2 & T_2 \end{pmatrix}.$$

The block matrices of course depend on g, but we omit it for simplicity. Then, since π_1' and π_2' are intertwined by UAV then

$$\begin{pmatrix} X_1 & Y_1 \\ Z_1 & T_1 \end{pmatrix}\begin{pmatrix} C & 0 \\ 0 & \pi D \end{pmatrix} = \begin{pmatrix} C & 0 \\ 0 & \pi D \end{pmatrix}\begin{pmatrix} X_2 & Y_2 \\ Z_2 & T_2 \end{pmatrix}.$$

and so we deduce $Z_1C = \pi DZ_2$ and $\pi Y_1 D = CY_2$. Now, since $C \in \mathrm{GL}_r(\mathcal{O}_P)$, taking the two previous equation modulo π we get

$$\overline{Y_2} = 0 \text{ and } \overline{Z_1} = 0.$$

So the modular representations σ_1' and σ_2' are given by

$$\sigma_1'(g) = \begin{pmatrix} \overline{X_1} & \overline{Y_1} \\ 0 & \overline{T_1} \end{pmatrix} \text{ and } \sigma_2'(g) = \begin{pmatrix} \overline{X_2} & 0 \\ \overline{Z_2} & \overline{T_2} \end{pmatrix}.$$

Since these to distributions are the triangular, the composition factors of σ_1' are those of $\overline{X_1}$ together with those $\overline{T_1}$ while the composition factors are those of $\overline{X_2}$ with those of $\overline{T_2}$. But we have the following:

$$\overline{X_1}\,\overline{C} = \overline{C}\,\overline{X_2} \quad \text{and} \quad T_1\, D = D\, T_2.$$

The first equation means that the composition factors of $\overline{X_1}$ and $\overline{X_2}$ are the same. The second equation means that T_1, T_2 are once more two representations over $\mathcal{O}_P$ that are K-equivalent. So we deduce the result by induction. □

Representations over k are called *modular*. As we just saw, from a representation of G over K, we can obtain a collection of modular presentations that may not be equivalent, but all have the same composition factors (as modules of finite length). When p does not divide g, the module $k[G]$ is semi-simple.

So the modular representations coming from a representation over K are all equivalent over k.

Unfortunately, there exist modular representations that can't be produced this way, as explained in this example.

EXAMPLE 2.2.3. — *Let $p > 3$ a prime number and G a group of order p with generator g and consider the representation σ of G over $\mathbb{F}_p$ determined by the matrix $\sigma(g) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. There exists no representation π of G over $\mathbb{Q}$ with matrix entries in $\mathbb{Z}_{(p)}$ such that $\overline{\pi} = \sigma$.*

It is known that, if two modular representations have the same characteristic polynomials at every element $g \in G$, then they have the same composition factors. This is because in particular they have the same character (when in characteristic 0 this even means that they are isomorphic). An element $g \in G$ is called *p-regular* if its order is not divisible by p otherwise we say that g is *p-singular*. It turns out that the fact that two k-representations have the composition factors actually depends only on their characteristic roots on *p-regular* elements of G.

PROPOSITION 2.2.4. — *Two k-representations ρ and π have the same composition factors if and only if for any p-regular element $g \in G$ the matrices $\rho(g)$ and $\pi(g)$ have the same characteristic roots.*

Proof. — We only need to prove the if direction. So suppose that $\rho(g)$ and $\pi(g)$ have the same characteristic roots whenever g is p-regular. If $g \in G$ is p-singular then $g^{pm} = 1$ for some m. Hence the eigenvalues of $\rho(g)$ and $\pi(g)$ are all equal to 1 since $\mathrm{char}(k) = p$. Now for any element $g \in G$ we can write $g = g_1 g_2$ where $g_1, g_2 \in G$ commute and g_1 is p-regular and g_2 is p-singular. So, since $\rho(g) = \rho(g_1)\rho(g_2)$ and $\rho(g_1), \rho(g_2)$ commute, we deduce that the eigenvalues of $\rho(g)$ are the same as those of $\rho(g_1)$. The eigenvalues of $\rho(g_1)$ are the same as those of $\pi(g_1)$ by assumption since g_1 is p-regular. So using the same argument on π we deduce that $\pi(g)$ and $\rho(g)$ have the same characteristic roots for any $g \in G$ which finishes the proof. □

THEOREM 2.1. — *Let ρ and π two k-representations of G. Then their characters χ_π and χ_ρ are equal if and only if they are equal on p-regular element of G*

Proof. — Follows easily from the proof of the previous theorem. □

COROLLARY 2.2.5. — *If ρ and π are two absolutely irreducible k-representations of G. Then ρ and π are isomorphic over k if and only if the their characters are equal on p-regular elements of G.*

COROLLARY 2.2.6. — *The number of non-isomorphic absolutely irreducible k-representations of G is less or equal than the number of p-regular conjugacy classes in G.*

Proof. — Let $\chi_1, \ldots, \chi_r$ the characters of the absolutely irreducible k-representations of G. These characters are linearly independent, and if $g_1, \ldots, g_t$ are representative of the t p-regular conjugacy classes in G, then each character is totally determined by its values on the g_i's, i.e,

$$\chi_j \equiv (\chi_i(g_1), \ldots, \chi_i(g_t)).$$

Then, since these vectors are linearly independent over k, we deduce that $r \leqslant t$. □

2.3. Brauer characters

Let V be a K-representation of G and M an $\mathcal{O}_P[G]$-module in V. The character μ of the representation V is the same as the character of the $\mathcal{O}_P$-representation M. Now we taking μ modulo P, we get the character of the k-representation M/PM. This is the character

$$\overline{\mu} : g \mapsto \overline{\mu(g)},$$

Now, let m be the lowest common multiple of orders of p-regular elements of G. Notice that p does not divide m and let ζ_m a primitive m-th roots of the unit. Define the following field extensio $\tilde{K} = K[\zeta_m]$ and $\tilde{\mathcal{O}}$ its ring of integers. Let $\tilde{P}$ a prime ideal in $\tilde{\mathcal{O}}$ above P. Since ζ_m is a primitive root of the unit, its image modulo $\tilde{P}$ is a primitive m-th root of the unit in the field $\tilde{k} \coloneqq \tilde{\mathcal{O}}/\tilde{P}$. So we deduce that $\tilde{k} = k[\overline{\zeta}_m]$.

Suppose that π is a modular representation of G over the field k with $n \coloneqq \dim(\pi)$. Let $\overline{\chi}_\pi$ be its character and g a p-regular element in G. Since $g^m = 1$, the characteristic roots of $\pi(g)$ are powers of $\overline{\zeta}_m$ and thus we can write

$$\overline{\chi}_\pi(g) = \overline{\zeta}_m^{\alpha_1} + \cdots + \overline{\zeta}_m^{\alpha_n}$$

From this we can define a map χ_π on p-regular elements of G as

$$\chi_\pi(g) = \zeta_m^{\alpha_1} + \cdots + \zeta_m^{\alpha_n} \in \tilde{\mathcal{O}}.$$

The map χ_π is called the Brauer character of π and $\overline{\chi}_\pi$ is called the modular character of π. By definition we have $\overline{\chi}_\pi(g) = \overline{\chi_\pi(g)}$ for p-regular $g \in G$.

Clearly, equivalent modular representations have the same Brauer character. Also, if ρ is a representation of G over $\tilde{\mathcal{O}}$ with character μ, and $\overline{\rho}$ is its corresponding k-representation, then μ coincides with the Brauer character $\chi_{\overline{\rho}}$ of $\overline{\rho}$ on p-regular elements g of G.

THEOREM 2.3.1. — *Let ρ and π be two modular representations of G with Brauer characters χ_ρ, χ_π. Then ρ and π have the same composition factors if and only if $\chi_\pi = \chi_\rho$.*

Proof. — The only if direction is trivial. Suppose that we have $\chi_\pi = \chi_\rho$. Let g a p-regular element in G, then so is g^k for $k = 0, 1 \dots$ and we have

$$\chi_\pi(g^k) = \chi_\rho(g^k).$$

Let us write $\chi_\pi(g) = \zeta_m^{\alpha_1} + \cdots + \zeta_m^{\alpha_n} = \zeta_m^{\beta_1} + \cdots + \zeta_m^{\beta_n} = \chi_\rho(g)$. So, since $\chi_\pi(g^k) = \chi_\rho(g^k)$ for any $k \geqslant 0$, we have

$$\zeta_m^{k\alpha_1} + \cdots + \zeta_m^{k\alpha_n} = \zeta_m^{k\beta_1} + \cdots + \zeta_m^{k\beta_n}.$$

This implies that $\{\zeta_m^{\alpha_1}, \dots, \zeta_m^{\alpha_n}\} = \{\zeta_m^{\beta_1}, \dots, \zeta_m^{\beta_n}\}$ as sets. So, for any p-regular g the matrices $\rho(g)$ and $\pi(g)$ have the same characteristic roots. Then the result follows by Proposition 2.2.4. □

3. Cartan invariants and decomposition numbers

Assume that K is a splitting field of G. We denote by $(\rho_1, V_1), \dots, (\rho_s, V_s)$ the set of all irreducible K-presentations of G up-to isomorphism. As we have seen, we may choose basis of the V_i's such that the matrices $\rho_i(g)$ have entries in $\mathcal{O}_P$ for any $i = 1, \dots, s$ and any $g \in G$. So we can think of each V_i as an $\mathcal{O}_P[G]$-module. Since K is a splitting field of G, all the representations (ρ_i, V_i) are absolutely irreducible over K and also their number s is the number of conjugacy classes of G.

Let's denote by $(\pi_1, W_1), \dots, (\pi_r, W_r)$ the full set of non-isomorphic irreducible k-representation and $M_1, \dots, M_r$ the set of non-isomorphic principal indecomposable submodules of $k[G]$. It is known from the group algebra theory that we have

$$k[G] = \bigoplus_{i=1}^{m} k[G]e_i$$

where the summands $k[G]e_i$ are the principal indecomposable submodules of $k[G]$, and the e_i's are orthogonal idempotent elements of $k[G]$ with $1 = e_1 + \cdots + e_m$. So if we denote by $\mathrm{rad}(k[G])$ the Jacobson radial of the ring $k[G]$, we have

$$M_i = k[G]e_i \text{ and } W_i = k[G]e_i/\,\mathrm{rad}(k[G])e_i.$$

Let α_j be the degree of M_j, and β_k the degree of W_k and finally n_i the degree of the representation V_i. We recall the following result.

THEOREM 3.0.1. — *Assume that k is a also splitting field of G. For each $j = 1, \dots, r$, exactly α_j of the composition factors of the module $k[G]$ are isomorphic to W_j, and exactly β_j of the the principal modules $k[G]e_\ell$ are isomorphic to U_j. Moreover, for any $k[G]$-module N, the number of composition factors of N which are isomorphic to W_i is $\dim_k(e_j N)$.*

For $i = 1, \dots, s$, thinking of V_i as a $\mathcal{O}_P$-module, let $\overline{V_i} \coloneqq V_i/PV_i$ which is a $k[G]$-module. We can then write

$$\overline{V_i} \simeq \bigoplus_{j=1}^{r} d_{i,j} W_j,$$

these are the decomposition factors of each of the V_i's. The $d_{i,j}$'s are non-negative integers called the *decomposition numbers* of $K[G]$ with respect to the prime P. This defines the *decomposition matrix* $D = (d_{i,j}) \in \mathbb{Z}^{s\times r}$. We call the p-rank of a matrix in $\mathbb{Z}^{s\times r}$ the rank of its image modulo p in the field $\mathbb{F}_p \coloneqq \mathbb{Z}/p$.

THEOREM 3.1. — *If both K and k are splitting fields of G, then r is exactly the number of p-regular classes in G and is also the p-rank of D.*

Proof. — Let n be the exponent of G (the l.c.m of the order of all elements of G). replacing K by the extension $K(\sqrt[n]{1})$ does not change the matrix D. Also, this does not affect the assumption that K and k are splitting fields. So we may assume that $\sqrt[n]{1} \in K$.

Denote by $C_1, \dots, C_t$ the p-regular classes of G. We have already seen in Corollary (2.2.6), that $r \leqslant t$. Let $\xi_1, \dots, \xi_t$ generalized characters such that

(i) $\xi_i(g) \in \mathbb{Z}$ for each $g \in G$.
(ii) $\xi_i(g) = 1 \mod p$ for each $g \in C_i$
(iii) $\xi_i(g) = 0$ for $g \in C_j$ when $i \neq j$.

Each of the ξ_i's is an $\mathcal{O}$ linear combination of the s characters $\chi_1, \dots, \chi_s$ of irreducible K-representations of G. So each $\overline{\xi_i}$ is a k-linear combination of the characters $\overline{\chi_j}$ where $j = 1, \dots, r$. But, $\overline{\xi_1}, \dots, \overline{\xi_t}$ are clearly linearly independent over k (from the three conditions above). So we deduce that $t \leqslant r$. Hence we deduce that $r = t$.

Now, if $D \in \mathbb{Z}^{s\times r}$ has rank less than r, then at most $r-1$ of the characters $\overline{\chi_1}, \dots \overline{\chi_s}$ are linearly independent over k. The same then holds for the ξ_i's. But this is not true, so D has rank r. □

COROLLARY 3.1. — *If K is a splitting field of G, then so is k.*

Proof. — The proof is omitted. We refer the reader to [CR66, Corollary 83.7] □

Next, let's write the each $i = 1, \dots, r$ the following:

$$M_i \simeq \bigoplus_{i=1}^{r} c_{i,j} W_j,$$

where the $C = (c_{i,j}) \in \mathbb{Z}^{r \times r}$ is a matrix of non-negative integers entries. We call C the *Cartan matrix* and its entries the *Cartan invariants* of $k[G]$. It is at this moment that the P-adic completion $\widehat{K}$ comes into play, to establish a relation between the two matrices C and D.

Let's define $\widehat{V_i}$ to be the $\widehat{\mathcal{O}}$-module $\widehat{V_i} := \widehat{\mathcal{O}} V_i$. So the $\widehat{V_i}$ are the non-isomorphic irreducible $\widehat{\mathcal{O}}[G]$-modules and the representations $\widehat{K}\widehat{V_i}$ are absolutely irreducible over $\widehat{K}$. We also have

$$\widehat{V_i}/\widehat{P}\widehat{V_i} \simeq V_i/PV_i = \overline{V_i}.$$

So, working with $\widehat{K}$ does not change the matrices D and C.

THEOREM 3.2. — *The Cartan matrix C and the decomposition matrix D are related by the equation $C = D^T D$, where D^T is the transpose of D.*

Proof. — It is known that there exists $\epsilon_1, \dots, \epsilon_m$ orthogonal idempotent elements of $\widehat{\mathcal{O}}[G]$ such that $1 = \epsilon_1 + \dots \epsilon_m$ and $\overline{\epsilon_i} = e_i$. Then we get

$$\widehat{K} = \widehat{K}[G]\epsilon_1 \oplus \cdots \oplus \widehat{K}[G]\epsilon_m.$$

Thanks to Theorem 3.0.1, the multiplicity $a_{i,j}$ of $\widehat{K}\widehat{V_i}\epsilon_j$ as a composition factor of $\widehat{K}[G]\epsilon_j$ is $\dim_{\widehat{K}} \widehat{K}\widehat{V_i}\epsilon_j$. So $a_{i,j}$ is also the number of elements in an $\widehat{\mathcal{O}}$-basis of $\epsilon_j \widehat{V_i}$. Now, since $\overline{e_j \widehat{V_i}} = e_j \overline{Z_i}$, we get

$$a_{i,j} = \dim_k(e_j \overline{V_i}).$$

Again Theorem 3.0.1 allows to conclude that $a_{i,j} = d_{i,j}$, so we have

$$\widehat{K}[G]\epsilon_j \simeq \bigoplus_{i=1}^{s} d_{i,j} \widehat{K}\widehat{V_i}$$

. Passing to the associated $k[G]$-modules, we get by Theorem 2.2.2

$$M_j \simeq \bigoplus_{i=1}^{s} d_{i,j} \overline{Z_i} = \bigoplus_{i=1}^{s} \bigoplus_{k=1}^{r} d_{i,j} d_{i,k} W_k.$$

Therefore, by definition of the matrix C, we deduce the desired result. □

This of course means that C is a symmetric definite-positive matrix. To conclude this section we give an example.

EXAMPLE 3.2. — *Let G be a p-group and $V_1, \dots, V_s$ the irreducible K-representations of G. It is known for p-groups, the only irreducible representation is the trivial one W_1. Also we have one principal indecomposable module M_1. So $d_{i,1} = n_i$ is the degree of V_i and we have the relation*

$$D^T D = \sum_{i=1}^{s} n_i^2 = |G| = c_{1,1}.$$

Bibliography

[ABG73] J. L. Alperin, Richard Brauer, and Daniel Gorenstein. The extended ZJ-theorem. In *Finite groups '72 (Proc. Gainesville Conf., Univ. Florida, Gainesville, Fla., 1972)*, pages 6–7. North–Holland Math. Studies, Vol. 7, 1973.

[BN41] R. Brauer and C. Nesbitt. On the modular characters of groups. *Ann. of Math. (2)*, 42:556–590, 1941.

[Bra74a] Richard Brauer. On the structure of blocks of characters of finite groups. In *Proceedings of the Second International Conference on the Theory of Groups (Australian Nat. Univ., Canberra, 1973)*, pages 103–130. Lecture Notes in Math., Vol. 372, 1974.

[Bra74b] Richard Brauer. Some applications of the theory of blocks of characters of finite groups. V. *J. Algebra*, 28:433–460, 1974.

[Bra76a] Richard Brauer. Notes on representations of finite groups. I. *J. London Math. Soc. (2)*, 13(1):162–166, 1976.

[Bra76b] Richard Brauer. On finite groups with cyclic Sylow subgroups. I. *J. Algebra*, 40(2):556–584, 1976.

[Bra79a] Richard Brauer. Blocks of characters and structure of finite groups. *Bull. Amer. Math. Soc. (N.S.)*, 1(1):21–38, 1979.

[Bra79b] Richard Brauer. On finite groups with cyclic Sylow subgroups. II. *J. Algebra*, 58(2):291–318, 1979.

[CR66] Charles W Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*, volume 356. American Mathematical Soc., 1966.

[CR81] Charles W Curtis and Irving Reiner. *Methods of representation theory–with applications to finite groups and orders*, volume 2. Wiley-Interscience, 1981.

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups*, volume 42. Springer, 1977.