LECTURE NOTES

AMRITANSHU PRASAD

1. Basic definitions

Let K be a field.

Definition 1.1. A K-algebra is a K-vector space together with an associative product $A \times A \to A$ which is K-linear, with respect to which it has a unit.

In this course we will only consider K-algebras whose underlying vector spaces are finite dimensional. The field K will be referred to as the *ground field* of A.

Example 1.2. Let M be a finite dimensional vector space over K. Then $\mathrm{End}_K M$ is a finite dimensional algebra over K.

Definition 1.3. A morphism of K-algebras $A \to B$ is a K-linear map which preserves multiplication and takes the unit in A to the unit in B.

Definition 1.4. A module for a K-algebra A is a vector space over K together with a K-algebra morphism $A \to \mathrm{End}_K M$.

In this course we will only consider modules whose underlying vector space is finite dimensional.

2. Absolutely irreducible modules and split algebras

For any extension E of K, one may consider the algebra $A \otimes_K E$, which is a finite dimensional algebra over E.

For any A-module M, one may consider the $A \otimes_K E$-module $M \otimes_K E$. Even if M is a simple A-module, $M \otimes_K E$ may not be a simple $A \otimes_K E$-module:

Example 2.1. Let $A = \mathbf{R}[t]/(t^2+1)$. Let $M = \mathbf{R}^2$, the A-module structure defined by requiring t to act by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then M is an irreducible A-module, but $M \otimes_{\mathbf{R}} \mathbf{C}$ is not an irreducible $A \otimes_{\mathbf{R}} \mathbf{C}$-module.

Date: 2006-2007.

Definition 2.2. Let A be a K-algebra. An A-module M is said to be *absolutely irreducible* if for every extension field E of K, $M \otimes_K E$ is an irreducible $A \otimes_K E$-module.

Example 2.1 gives an example of an irreducible A-module that is not absolutely irreducible. For any A-module M multiplication by a scalar in the ground field is an endomorphism of M.

Theorem 2.3. *An irreducible A-module M is absolutely irreducible if and only if every A-module endomorphism of M is multiplication by a scalar in the ground field.*

Proof. We know from Schur's lemma that $D := \mathrm{End}_A M$ is a division ring. This division ring is clearly a finite dimensional vector space over K (in fact a subspace of $\mathrm{End}_K M$). The image B of A in $\mathrm{End}_K M$ is a matrix algebra $M_n(D)$ over D. M can be realised as a minimal left ideal in $M_n(D)$. M is an absolutely irreducible A-module if and only if it is an absolutely irreducible B-module.

If $\mathrm{End}_A M = K$, then $B = M_n(K)$, and $M \cong K^n$. $B \otimes_K E = M_n(E)$, and $M \otimes_K E \cong E^n$. Thus $M \otimes_K E$ is clearly an irreducible $B \otimes_K E$-module. Therefore, M is absolutely irreducible.

Conversely, suppose M is an absolutely irreducible A-module. Let $\overline{K}$ denote an algebraic closure of K. Then $M \otimes_K \overline{K}$ is an irreducible $A \otimes_K \overline{K}$-module. Moreover, it is a faithful $B \otimes_K \overline{K}$-module. $B \otimes_K \overline{K} \cong M_m(\overline{K})$ and $M \otimes_K \overline{K} \cong \overline{K}^m$ for some m. Consequently $\dim_K B = \dim_{\overline{K}}(B \otimes_K \overline{K}) = m^2$, and similarly, $\dim_K M = m$. On the other hand, $\dim_K B = n^2 \dim_K D$ and $\dim_K M = n \dim_K D$. Therefore $\dim_K D = 1$, showing that $D = K$. □

Definition 2.4. Let A be a finite dimensional algebra over a field K. An extension field E of K is called a *splitting field* for A if every irreducible $A \otimes_K E$-module is absolutely irreducible. A is said to be *split* if K is a splitting field for A. Given a finite group G, K is said to be a splitting field for G if $K[G]$ is split.

Example 2.5. $\mathbf{Z}/4\mathbf{Z}$ is not split over $\mathbf{Q}$. It splits over $\mathbf{Q}[i]$.

Example 2.6. Consider Hamilton's quaternions: $\mathbf{H}$ is the $\mathbf{R}$ span in $M_2(\mathbf{C})$ the matrices

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

$\mathbf{H}$ is a four-dimensional simple $\mathbf{R}$ algebra (since it is a division ring), which is not isomorphic to a matrix algebra for any extension of $\mathbf{R}$. $\mathbf{H}$ is an irreducible $\mathbf{H}$-module over $\mathbf{R}$, but $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{C}$ is isomorphic to $M_2(\mathbf{C})$

and the $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{C}$-module $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{C}$ is no longer irreducible. Therefore $\mathbf{H}$ does not split over $\mathbf{R}$.

Theorem 2.7 (Schur's lemma for split finite dimensional algebras)**.** *Let A be a split finite dimensional algebra over a field K. Let M be an irreducible A-module. Then* $\mathrm{End}_A M = K$.

Proof. Let $T : M \to M$ be an A-module homomorphism. T is a K-linear map. Fix an algebraic closure L of K. Let λ be any eigenvalue of $T \otimes 1 \in \mathrm{End}_{A \otimes_K L} M \otimes L$. Then $T \otimes 1 - \lambda I$, where I denotes the identity map of $M \otimes_K L$ is also an $A \otimes_K L$-module homomorphism. However, $T \otimes 1 - \lambda I$ is singular. Since M is irreducible, this means that $\ker(T \otimes 1 - \lambda I) = M$, or in other words, $T \otimes 1 = \lambda I$. It follows that $\lambda \in K$ and that $T = \lambda I$ (now I denotes the identity map of M). □

Corollary 2.8 (Artin-Wedderburn theorem for split finite dimensional algebras)**.** *If A is a split semisimple finite dimensional algebra over a field K if and only if*

$$A = M_{n_1}(K) \oplus \cdots \oplus M_{n_c}(K)$$

for some positive integers $n_1, \ldots, n_k$.

Proof. A priori, by the Artin-Wedderburn theorem, A is a direct sum of matrix rings over division algebras containing K in the centre. However, each such summand gives rise to an irreducible A-module whose endomorphism ring is the opposite ring of the division algebra. From Theorem 2.7 it follows therefore that the division algebra must be equal to K. □

Proposition 2.9. *A finite dimensional algebra A is split over a field K if and only if $\frac{A}{\mathrm{Rad} A}$ is a sum of matrix rings over K.*

Proof. The simple modules for A and $\frac{A}{\mathrm{Rad} A}$ are the same. □

Theorem 2.10. *Every finite group splits over some number field.*

Proof. Let $\overline{\mathbf{Q}}$ be an algebraic closure of $\mathbf{Q}$. Then by Corollary 2.8,

$$\overline{\mathbf{Q}}[G] = M_{n_1}(\overline{\mathbf{Q}}) \oplus \cdots \oplus M_{n_c}(\overline{\mathbf{Q}})$$

Let e^k_{ij} denote the element of $\overline{\mathbf{Q}}[G]$ corresponding to the (i, j)th entry of the kth matrix in the above direct sum decomposition. The e^k_{ij}'s for $1 \leq k \leq c$, and $1 \leq i, j \leq n_k$ form a basis of A. Each element $g \in G$ can be written in the form

$$g = \sum_{i,j,k} \alpha^k_{ij}(g) e^k_{ij}$$

for a unique collection of constants $\alpha_{ij}^k(g) \in \overline{\mathbf{Q}}$. Similarly, define constants $\beta_{ij}^k(g)$ by the identities

$$e_{ij}^k = \sum_{g \in G} \beta_{ij}^k(g) g.$$

Let K be the number field generated over $\mathbf{Q}$ by

$$\{\alpha_{ij}^k(g), \beta_{ij}^k(g) | 1 \leq k \leq c,\ 1 \leq i, j \leq n_k\ g \in G\}.$$

Set $\tilde{A} = \bigoplus_{i,j,k} K e_{ij}^k$. Then $\tilde{A}$ is a subalgebra of $\overline{\mathbf{Q}}[G]$ that is isomorphic to $K[G]$. Moreover,

$$\tilde{A} = M_{n_1}(K) \oplus \cdots \oplus M_{n_c}(K).$$

It follows that every irreducible $\tilde{A}$-module is absolutely irreducible. Therefore, $\tilde{A}$, and hence $K[G]$ is split. □

Proposition 2.11. *Let K be a splitting field for G. Then every irreducible $\mathbf{C}[G]$-module is of the form $M \otimes_K \mathbf{C}$ for some irreducible $K[G]$-module.*

Proof. This follows from the fact that $\mathbf{C}[G] \cong K[G] \otimes_K \mathbf{C}$, and that

$$K[G] = M_{n_1}(K) \oplus \cdots \oplus M_{n_c}(K).$$

□

Theorem 2.12. *Suppose that A is split over K. Then an irreducible A-module $Ae/\mathrm{Rad}Ae$ (where e is a primitive idempotent) occurs* $\dim_K eM$ *times as a composition factor in a finite dimensional A-module M.*

Proof. Let

$$0 = M_0 \subset \cdots M_m = M$$

be a composition series for M. Suppose that k of the factors M_{i_j}/M_{i_j-1}, $1 \leq i_1 < \cdots < i_k$ are isomorphic to $Ae/\mathrm{Rad}Ae$. Recall that $M_i/M_{i-1} \cong Ae/\mathrm{Rad}Ae$ if and only if eM_i is not contained in M_{i-1}. Therefore, can find $m_{i_1}, \ldots, m_{i_k}$ in $M_{i_1}, \ldots, M_{iK}$ respectively such that $em_{i_j} \notin M_{i_j-1}$. Replacing m_{i_j} by em_{i_j} may assume that $m_{i_j} \in eM$. Since M_{i_j}/M_{i_j-1} is irreducible,

$$Am_{i_j} + M_{i_j-1} = M_{i_j},$$

and hence

$$eM_{i_j} = eAem_{i_j} + eM_{i_j-1}.$$

On the other hand if $i \notin \{i_1, \ldots, i_k\}$ then

$$eM_i \subset M_{i-1}.$$

Let $a \mapsto \overline{a}$ be the mapping of A onto the semisimple algebra $\overline{A} = A/RadA$. Then $\mathrm{End}_{\overline{A}} \overline{A}\overline{e} = \overline{e}\overline{A}\overline{e}$. Since K is a splitting field for A,

$\overline{e}\overline{A}\overline{e} = K$. Therefore $eAe = Ke + e\text{Rad}Ae$. Moreover, $e\text{Rad}AeM_i \subset M_{i-1}$ for all i, and we have that

$$eM_{i_j} = Km_{i_j} + eM_{i_j-1}.$$

We prove that $\{m_{i_1}, \ldots, m_{i_k}\}$ is a basis of eM. It is clear that it is a linearly independent set. If $m \in eM$, then $em = m$. Therefore, $m \in M_{i_k}$. There exists $\xi_k \in K$ such that $m - \xi_k m_k \in eM_{i-1}$. Now $m - \xi_k m_k \in M_{i_{k-1}}$. Continuing in this way, we see that $m - \xi_1 m_1 - \cdots - \xi_k m_k \in M_0 = 0$. □

3. Associated modular representations

Let K be a number field with ring of integers R. Let $P \subset R$ be a prime ideal in R. Denote by $\mathbf{k}$ the finite field R/P. Consider

$$R_P := \{x \in K | x = a/b \text{ where } a \in R,\ b \notin P\}.$$

R_P is called the *localisation of R at P*.

Lemma 3.1. *The natural inclusion $R \hookrightarrow R_P$ induces an isomorphism $\mathbf{k} = R/P \tilde{\rightarrow} R_P/PR_P$.*

Proof. The main thing is to show surjectivity, which is equivalent to the fact that $R_P = R + PR_P$. Given a/b, with $a \in R$ and $b \notin P$, by the maximality of P, we know that $R = bR + P$. Therefore a can be written in the form $a = bx + c$, with $x \in R$ and $c \in P$. We then have that $a/b = x + c/b \in R + PR_P$. □

It is easy to see that R_P is a local ring and that PR_P is its unique maximal ideal.

Proposition 3.2. *Let π be any element of $P \setminus P^2$. Then PR_P is a principal ideal generated by π. Every element x of K can be written as $x = u\pi^n$ for a unique unit $u \in R_P$ and a unique integer n. The element $x \in R_P$ if and only if $n \geq 0$.*

For a proof, we refer the reader to [Ser68, Chapitre I]. The integer n is called the *valuation* of x with respect to P (usually denoted $v_p(x)$) and does not depend on the choice of π. The ring R_P is an example of a *discrete valuation ring.*

The following proposition follows from the fact that R_P is a principal ideal domain. We also give a self-contained proof below.

Proposition 3.3. *Every finitely generated torsion-free module over R_P is free.*

Proof. Suppose that M is a finitely generated torsion free module over R_P. Then $\overline{M} := M/PR_PM$ is a finite dimensional vector space over $\mathbf{k}$. Let $\{\overline{m}_1, \dots, \overline{m}_r\}$ be a basis of $\overline{M}$ over $\mathbf{k}$. For each $1 \leq i \leq r$ pick an arbitrary element $m_i \in M$ whose image in $\overline{M}$ is $\overline{m}_i$. Let M' be the R_P-module generated by $m_1, \dots, m_r$. Then $M = M' + PR_PM$. In other words, $M/M' = PR_P(M/M')$.

Denote by N the R_P-module M/M'. Now take a set $\{n_1, \dots, n_r\}$ of generators of N. The hypothesis that $PR_PN = N$ implies that for each i, $n_i = \sum a_{ij} n_j$ where $a_{ij} \in PR_P$ for each j. Now regard N as an $R_P[x]$-module where x acts as the identity. Let A denote the $r \times r$-matrix whose (i,j)th entry is a_{ij}. Let $\mathbf{n}$ denote the column vector whose entries are $n_1, \dots, n_r$. We have

$$(xI - A)\mathbf{n} = 0.$$

By Cramer's rule,

$$\det(xI - A)\mathbf{m} = 0.$$

All the coefficients of $\det(xI - A)$ lie in PR_P. Therefore, we see that $(1 + c)\mathbf{m} = 0$ for some $c \in PR_P$. Since PR_P is the unique maximal ideal of R_P, it is also the Jacobson radical, which means that $(1 + c)$ is a unit. It follows that $N = 0$.[1]

Consequently M is also generated by $\{m_1, \dots, m_r\}$. Consider a linear relation

$$\alpha_1 m_1 + \cdots + \alpha_r m_r = 0$$

between that m_i's and assume that $v := \min\{v_P(\alpha_1), \dots, v_P(\alpha_r)\}$ is minimal among all such relations. The fact that the $\overline{m}_i$'s are linearly independent over $\mathbf{k}$ implies that $v > 0$. Therefore each α_i is of the form $\pi\alpha_i'$, for some $\alpha_i' \in R_P$. Replacing the α_i's by the α_i''s gives rise to a linear relation between the m_i's where the minimum valuation is $v - 1$, contradicting our assumption that v is minimal.

Therefore M is a free R_P-module generated by $\{m_1, \dots, m_r\}$. □

Let G be a finite group. Let M be a finitely generated $K[G]$-module.

Proposition 3.4. *There exists a $R_P[G]$-module M_P in M such that $M = KM_P$. M_P is a free over R_P of rank $\dim_K M$.*

Proof. Let $\{m_1, \dots, m_r\}$ be a K-basis of M. Set

$$M_P = \sum_{g \in G} \sum_{j=1}^{r} R_P e_g m_j.$$

Then M_P is a finitely generated torsion-free module over R_P. By Proposition 3.3 it is free. Since each $m_i \in M_P$, $M = KM_P$. An

[1] This is a special case of *Nakayama's lemma.*

R_P-basis of M_P will also be a K-basis of M. Therefore the rank of M_P as an R_P-module will be the same as the dimension of M as a K-vector space. □

Start with a finite dimensional $K[G]$-module M. Fix a prime ideal P in R. By Proposition 3.4 there exists an $R[G]$-module M_P in M such that M_R such that $KM_R = M$. $\overline{M} := M_P/PR_PM_P$ is a finite dimensional $\mathbf{k}[G]$-module. We will refer to any module obtained by such a construction as *a* $\mathbf{k}[G]$*-module associated to* M. However, the module M_P is not uniquely determined. Different choices of M_P could give rise to non-isomorphic $\mathbf{k}[G]$-modules, as is seen in the following

Example 3.5. Let $G = \mathbf{Z}/2\mathbf{Z} = \{0, 1\}$. Consider the two dimensional $\mathbf{Q}[G]$ modules M_1 and M_2 where e_1 acts by

$$T_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad T_2 = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

respectively. T_1 and T_2 are conjugate over $\mathbf{Q}$, and therefore the $\mathbf{Q}[G]$-modules M_1 and M_2 are isomorphic. However, taking $P = (2) \subset \mathbf{Z}$, we get non-isomorphic modules of $\mathbf{Z}/2\mathbf{Z}[G]$ (T_2 is not semisimple in characteristic 2!). Note, however, that they have the same composition factors.

Theorem 3.6 (Brauer and Nesbitt)**.** *Two* $\mathbf{k}[G]$*-modules associated to the same* $K[G]$*-module have the same composition factors.*

Proof. Let M_P and M'_P be a pair of $R_P[G]$-modules inside M, with R_P-bases $\{m_1, \ldots, m_r\}$ and $\{m'_1, \ldots, m'_r\}$ respectively. Then there exists a matrix $A = (a_{ij}) \in GL_r(K)$ such that

$$m'_i = a_{i1}m_1 + \cdots + a_{ir}m_r.$$

Replacing M'_P with the isomorphic R_P-module $\pi^a M'_P$ would result in replacing A by $\pi^a A$. We may therefore assume that A has all entries in R_P and that at least one entry is a unit. Replacing A by a matrix XAY, where $X, Y \in GL_r(R_P)$ amounts to changing bases for M_P and M'_P. Let $\overline{A}$ be the image of $A \in M_r(R_P)$ in $M_r(\mathbf{k})$. $\overline{A}$ is equivalent to a matrix of the form $\begin{pmatrix} \overline{B} & 0 \\ 0 & 0 \end{pmatrix}$, where $B \in GL_2(\mathbf{k})$. A little work shows that A is equivalent in $M_r(R_P)$ to a matrix of the form $\begin{pmatrix} B & 0 \\ 0 & \pi C \end{pmatrix}$, where $B \in GL_r(R_P)$. For each $x \in K[G]$ let $T(x)$ and $T'(x)$ denote the matrices for the action of x on M with respect to the bases $\{m_1, \ldots, m_r\}$ and $\{m'_1, \ldots, m'_r\}$ respectively. T and T' are matrix-valued functions on R. Decompose them as block matrices (of matrix-valued functions on R):

$$T = \begin{pmatrix} X & Y \\ Z & W \end{pmatrix} \quad \text{and} \quad T' = \begin{pmatrix} X' & Y' \\ Z' & W' \end{pmatrix}.$$

Substituting in $TA = AT'$, we get

$$\begin{pmatrix} XB & \pi YC \\ ZB & \pi WC \end{pmatrix} = \begin{pmatrix} BX' & BY' \\ \pi CZ' & \pi CW' \end{pmatrix}.$$

Consequently $\overline{Y}' = 0$ and $\overline{Z} = 0$, and

$$\overline{T} = \begin{pmatrix} \overline{X} & 0 \\ \overline{Z} & \overline{W} \end{pmatrix} \quad \text{and} \quad \overline{T}' = \begin{pmatrix} \overline{X}' & \overline{Y}' \\ 0 & \overline{W'} \end{pmatrix}.$$

An algebra homomorphism from any algebra into a matrix ring naturally defines a module for the algebra. If we denote by $\overline{M}$ and $\overline{M}'$ the $\mathbf{k}[G]$-modules M_P/PR_PM_P and $M'_P/PR_PM'_P$ respectively, then $\overline{M}$ is defined by $\overline{T}$ and $\overline{M}'$ is defined by $\overline{T}'$. The composition factors of $\overline{M}$ are those of the module defined by $\overline{X}$ together with those of the module defined by $\overline{Z}$. Likewise the composition factors of $\overline{M}'$ are those of the module defined by $\overline{X}'$ together with those of the module defined by $\overline{Z'}$. Since X is similar to X' the former pair are isomorphic $\mathbf{k}[G]$-modules. To see that the latter pair have the same composition factors one may use an induction hypothesis on the dimension of M over K (the theorem is clearly true when M is a one dimensional K-vector space). □

Corollary 3.7. *If $(p, |G|) = 1$, M is a $K[G]$-module and P is a prime ideal containing p, then all $\mathbf{k}[G]$-modules associated to M are isomorphic.*

Proof. This follows from Theorem 3.6 and Maschke's theorem. □

4. Decomposition Numbers

Let G be a finite group and K be a splitting field for G. Denote by R the ring of integers in K. Fix a prime ideal P in R. Denote by $\mathbf{k}$ the field R/P. Given an irreducible $\mathbf{C}[G]$-module, we know from Prop 2.11 that it is isomorphic to $M \otimes_K \mathbf{C}$ for some irreducible $K[G]$-module. By Proposition 3.4, there is an $R_P[G]$-module M_P such that $M = KM_P$. Let $\overline{M}$ denote the $\mathbf{k}[G]$-module M_P/PR_PM_P. By Theorem 3.6, the composition factors of $\overline{M}$ and their multiplicities do not depend on the choice of M_P above.

Let $M_1, \ldots, M_c$ be a complete set of representatives for the isomorphism classes of irreducible representations of $\mathbf{C}[G]$. Likewise, denote by $N_1, \dots, N_d$ a complete set of representatives for the irreducible representations of $\mathbf{k}[G]$. By the theorems of Frobenius and of Brauer and Nesbitt, we know that c is the number of conjugacy classes in G and d is the number of p-regular conjugacy classes in G, provided that $\mathbf{k}$ is a splitting field for G.

Definition 4.1 (Decomposition matrix)**.** The *decomposition matrix of G with respect to P* is the $d \times c$ matrix $D = (d_{ij})$ given by

$$d_{ij} = [\overline{M}_j : N_i].$$

The preceding discussion shows that D is well-defined.

5. Brauer-Nesbitt theorem

Let $1 = \epsilon_1 + \dots + \epsilon_r$ be pairwise orthogonal idempotents in $\mathbf{k}[G]$.

Lemma 5.1. *Let $\epsilon \in \mathbf{k}[G]$ be an idempotent. There exists and idempotent $e \in \widehat{R}_P[G]$ such that $\overline{e} = \epsilon$.*

Proof. Consider the identity

$$1 = (x + (1-x))^{2n} = \sum_{i=0}^{2n} \binom{2n}{r} x^{2n-j}(1-x)^j.$$

Define

$$f_n(x) = \sum_{i=0}^{n} \binom{n}{r} x^{2n-j}(1-x)^j.$$

It follows that

$$f_n(x) \equiv 0 \mod x^n \text{ and } f_n(x) \equiv 1 \mod (1-x)^n.$$

Since $f(x)^2$ satisfies the same congruences,

$$f_n(x)^2 \cong f(x) \mod x^n(1-x)^n. \tag{5.2}$$

Replacing n by $n-1$ gives

$$f_n(x) \cong f_{n-1}(x) \mod x^{n-1}(1-x)^{n-1}. \tag{5.3}$$

Finally a direct computation yields

$$f_1(x) \cong x \mod x^2 - x. \tag{5.4}$$

Choose any $a \in R_P[G]$ such that $\overline{e} = \epsilon$. Then $a^2 - a \in PR_P[G]$. By (5.3)

$$f_n(a) - f_{n-1}(a) \in P^{n-1}R_P[G],$$

whence $f_n(a)$ is a P-Cauchy sequence. Let $e = \lim_{n\to\infty} f_n(a)$ (this is an element of $\widehat{R}_P[G]$). It follows from (5.2) that e is idempotent, and from (5.4) that $\overline{e} = \epsilon$. □

Lemma 5.5. *Let ϵ_1 and ϵ_2 be orthogonal idempotents in $\mathbf{k}[G]$ and let e be any idempotent in $\widehat{R}_P[G]$ such that $\overline{e} = \epsilon_1 + \epsilon_2$. Then there exist orthogonal idempotents $e_1, e_2 \in \widehat{R}_P[G]$ such that $\overline{e}_i = \epsilon_i$.*

Proof. Choose any $a \in \widehat{R}_P[G]$ such that $\overline{a} = \epsilon_1$. Set $b = eae$. Then $\overline{b} = \overline{eae} = (\epsilon_1 + \epsilon_2)\epsilon_1(\epsilon_1 + \epsilon_2) = \epsilon_1$. Also, $be = eb = b$. Therefore, $b^2 - b \in P\widehat{R}_P[G]$, whence $\{f_n(b)\}$ converges to an idempotent $e_1 \in \widehat{R}_P[G]$ such that

$$\overline{e}_1 = \overline{b}_1 = \epsilon_1, \quad e_1 e = e e_1 = e_1.$$

Set $e_2 = e - e_1$, then e_2 is idempotent, and $e_1 e_2 = e_2 e_1 = 0$ and $\overline{e}_2 = \overline{e} - \overline{e}_1 = \epsilon_2$, proving the result. □

Lemma 5.6. *There exist pairwise orthogonal idempotents $e_1, \ldots, e_r \in \widehat{R}_P[G]$ such that $\overline{e}_i = \epsilon_1$ and $1 = e_1 + \cdots + e_r$.*

Proof. For $r = 1$ the result is trivial. Assume therefore, that $r > 1$ and that the result holds for $r - 1$. Set $\delta = \epsilon_{r-1} + \epsilon_r$. Then

$$1 = \epsilon_1 + \cdots + \epsilon_{r-2} + \delta \tag{5.7}$$

is an orthogonal decomposition. By the induction hypothesis, there exist $1 = e_1 + \ldots + e_{r-2} + d$ in $\widehat{R}_P[G]$ lifting (5.7). The lemma now follows from Lemma 5.5. □

Now assume that $1 = \epsilon_1 + \cdots + \epsilon_r$ is a decomposition into pairwise orthogonal *primitive* idempotents. Fix a lifting $1 = e_1 + \cdots + e_r$ in $\widehat{R}_P[G]$ of orthogonal idempotents. Let $M_1, \ldots, M_s$ denote the isomorphism classes of irreducible $K[G]$-modules. Then $[K[G]e_i, M_j] =$ [2] $\dim_K e_i M_j = \dim_{\mathbf{k}} \epsilon_i \overline{M}_j =$ [3] $\overline{M}_j, N_i] = d_{ij}$. Consequently,

$$K[G]e_j \sim \sum_{i=1}^{s} d_{ij} M_j.$$

Passing to associated $\mathbf{k}[G]$-modules,

$$\begin{aligned} P_j &\sim \sum_{i=1}^{s} d_{ij} \overline{M}_i \\ &\sim \sum_{i=1}^{s} d_{ij} \sum_{k=1}^{r} d_{ik} N_k. \end{aligned}$$

On the other hand

$$P_j \sim \sum_{k=1}^{r} c_{jk} N_k.$$

[2]Suppose $M = K[G]e$ for some primitive idempotent e. Then $\dim_K \mathrm{Hom}_{K[G]}(M_j, K[G]e_i) = \dim_K e_i K[G] f = \dim_K e_i M_j$

[3]Theorem 2.12.

Comparing the two expressions for P_j above shows that

$$c_{jk} = \sum_{i=1}^{s} d_{ij} d_{ik},$$

or that $C = D^t D$.

References

[Ser68] Jean-Pierre Serre. *Corps locaux.* Hermann, Paris, 1968. Troisième édition, Publications de l'Université de Nancago, No. VIII.

The Institute of Mathematical Sciences, Chennai.
URL: http://www.imsc.res.in/~amri