Character Theory of Finite Groups

NZ Mathematics Research Institute
Summer Workshop

Day 2: The group algebra, divisibility and Burnside's $p^a q^b$ theorem

Don Taylor

The University of Sydney

Nelson, 7–13 January 2018

From yesterday: the essentials

First orthogonality relations

$$\langle \chi_i \mid \chi_j \rangle = \frac{1}{|G|} \sum_{x \in G} \chi_i(x)\overline{\chi_j(x)} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

Second orthogonality relations

$$\sum_{i=1}^{r} \chi_i(x)\overline{\chi}_i(y) = \begin{cases} |C_G(x)| & x \text{ is conjugate to } y \\ 0 & x \text{ is not conjugate to } y \end{cases}$$

Orthogonality revisited

Let x_1, x_2, ..., x_r represent the conjugacy classes of G and define $h_i = |\mathrm{ccl}_G(x_i)|$ for $1 \le i \le r$.

Because characters are constant on conjugacy classes, the first orthogonality relations can be written as

$$\sum_{k=1}^{r} h_k \chi_i(x_k)\overline{\chi}_j(x_k) = \delta_{ij}|G|.$$

In matrix form this is $XD\overline{X}^\top = |G|I$, where $X = \big(\chi_i(x_j)\big)$ is the *character table* and $D = \mathrm{diag}(h_1, h_2, \dots, h_r)$.

Consequently

$$\overline{X}^\top XD = \overline{X}^\top (XD\overline{X}^\top)\overline{X}^{-\top} = |G|I$$

and therefore $\overline{X}^\top X = |G|D^{-1}$, which is the matrix form of the second orthogonality relations.

Summary

In the character table

Class	C_1	$\dots$	C_j	$\dots$	C_r
Size	1	$\dots$	h_j	$\dots$	h_r
χ_1	1	$\dots$	1	$\dots$	1
	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
χ_i	n_i	$\dots$	$\chi_i(x_j)$	$\dots$	$\chi_r(x_r)$
	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
χ_r	n_r	$\dots$	$\chi_r(x_j)$	$\dots$	$\chi_r(x_r)$

we have

- $\sum_{k=1}^{r} h_k \chi_i(x_k)\overline{\chi}_j(x_k) = |G|\delta_{ij}$
- $\sum_{i=1}^{r} \chi_i(x_j)\overline{\chi}_i(x_k) = |C_G(x_j)|\delta_{jk}$

The alternating group Alt(4)

	1	$(12)(34)$	(123)	(132)
	1	3	4	4
	1	1	1	1
	1	1	ω	ω^2
	1	1	ω^2	ω
	3	-1	0	0

$\omega^3 = 1$

The group algebra $\mathbb{C}[G]$

The *group algebra* $\mathbb{C}[G]$ is the vector space of dimension $|G|$ with basis $(e_x)_{x \in G}$ and multiplication such that $e_x e_y = e_{xy}$.

Let $\rho_i : G \to \mathrm{GL}(W_i)$ for $1 \le i \le r$ be the distinct (up to isomorphism) irreducible representations of G, and put $n_i = \dim(W_i)$ so that the algebra $\mathrm{End}(W_i)$ of endomorphisms of W_i is isomorphic to $M_{n_i}(\mathbb{C})$, the algebra of all $n_i \times n_i$ complex matrices..

The map $\rho_i : G \to \mathrm{GL}(W_i)$ extends by linearity to an algebra homomorphism $\tilde{\rho}_i : \mathbb{C}[G] \to \mathrm{End}(W_i)$ such that $\tilde{\rho}_i(e_x) = \rho_i(x)$ and the family $(\tilde{\rho}_i)$ defines a homomorphism

$$\tilde{\rho} : \mathbb{C}[G] \to \prod_{i=1}^{r} \mathrm{End}(W_i) \simeq \prod_{i=1}^{r} M_{n_i}(\mathbb{C}).$$

Decomposition of $\mathbb{C}[G]$

$$\tilde{\rho} : \mathbb{C}[G] \to \prod_{i=1}^{r} \mathrm{End}(W_i) \simeq \prod_{i=1}^{r} M_{n_i}(\mathbb{C}).$$

Theorem

The homomorphism $\tilde{\rho}$ is an isomorphism.

Proof. [d'après J.-P. Serre].

Claim: $\tilde{\rho}$ is surjective. Suppose that f is a linear functional defined on $\prod_i M_{n_i}(\mathbb{C})$, which is zero on the image of $\tilde{\rho}$. This gives a linear relation between the functions $a_{jk}^{(i)}$, where $\left(a_{jk}^{(i)}(x)\right)_{j,k}$ is the matrix of $\rho_i(x)$. It follows from the Schur relations that $f = 0$ and hence $\tilde{\rho}$ is surjective.

On the other hand, $\mathbb{C}[G]$ and $\prod_i M_{n_i}(\mathbb{C})$ both have dimension $|G| = \sum_{i=1}^{r} n_i^2$ and since $\tilde{\rho}$ is surjective it is bijective. □

The inverse of $\tilde{\rho}$

Theorem (Fourier inversion)

Let $(u_i)_{1 \le i \le r} \in \prod_i \mathrm{End}(W_i)$ and $u = \sum_x u(x) e_x \in \mathbb{C}[G]$ be such that $\tilde{\rho}_i(u) = u_i$ for all i. Then

$$u(x) = \frac{1}{|G|} \sum_{i=1}^{r} n_i \mathrm{Tr}_{W_i}(\rho_i(x^{-1}) u_i), \quad \text{where } n_i = \dim W_i.$$

Proof.

By linearity it suffices to take $u = y$ in G. Then $u(x) = \delta_{xy}$ and hence $\mathrm{Tr}_{W_i}(\rho_i(x^{-1} u_i) = \chi_i(x^{-1} y)$, where χ_i is the character of ρ_i. This reduces us to proving

$$\delta_{xy} = \frac{1}{|G|} \sum_{i=1}^{r} n_i \chi_i(x^{-1} y),$$

which is a consequence of the orthogonality relations (equivalently r_G). □

Central idempotents in $\mathbb{C}[G]$

An element $E \in \mathbb{C}[G]$ is *idempotent* if $E^2 = E$. Idempotents E and E' are *orthogonal* if $EE' = 0 = E'E$.

The identity transformations $I_i \in \mathrm{End}(W_i)$ are idempotents and their inverse images $E_i = \tilde{\rho}^{-1}(I_i)$ are orthogonal idempotents in the centre $Z(\mathbb{C}[G])$ of $\mathbb{C}[G]$:

$$E_i E_j = \delta_{ij} E_i \quad \text{and} \quad E_1 + E_2 + \cdots + E_r = 1.$$

By Fourier inversion we have

$$E_i = \frac{\chi_i(1)}{|G|} \sum_{x \in G} \overline{\chi}_i(x) e_x$$

and the formula $E_i E_j = \delta_{ij} E_i$ is equivalent to

$$\frac{1}{|G|} \sum_{y \in G} \chi_i(xy^{-1}) \chi_j(y) = \frac{\chi_i(x)}{\chi_i(1)} \delta_{ij}.$$

The centre of $\mathbb{C}[G]$

The central idempotents $E_1, E_2, \ldots, E_r$ form a basis for $Z(\mathbb{C}[G])$.

If $C_1, C_2, \ldots, C_r$ are the conjugacy classes of G, the elements $\hat{C}_i = \sum_{x \in C_i} e_x$ are another basis. (We always suppose that $C_1 = \{1\}$.)

The restriction of $\tilde{\rho}_i$ to $Z(\mathbb{C}[G])$ is a homomorphism whose image is contained in the scalar matrices of $M_{n_i}(\mathbb{C})$; that is, it defines a homomorphism $\omega_i : Z(\mathbb{C}[G]) \to \mathbb{C}$ such that for $u = \sum_{x \in G} u(x) e_x$ in $Z(\mathbb{C}[G])$ and $n_i = \chi_i(1)$,

$$\omega_i(u) = \frac{1}{n_i} \sum_{x \in G} u(x) \chi_i(x). \qquad \frac{1}{n_i} \mathrm{Tr}_{W_i} \rho_i(u)$$

(u is a class function and we proved this in the previous lecture.)

Thus $\omega_i(E_j) = \delta_{ij}$ and if $C_j = \mathrm{ccl}_G(x_j)$, then $\omega_i(\hat{C}_j) = \dfrac{|C_j| \chi_i(x_j)}{n_i}$.

Products of class sums

For $z \in C_k$, define

$$a_{ijk} = \left|\{(x,y) \in C_i \times C_j \mid xy = z\}\right|.$$

Then a_{ijk} is independent of the choice of $z \in C_k$.

Theorem

$$\hat{C}_i \hat{C}_j = \sum_{k=1}^{r} a_{ijk} \hat{C}_k$$

$$\omega_t(\hat{C}_i)\omega_t(\hat{C}_j) = \sum_{k=1}^{r} a_{ijk} \omega_t(\hat{C}_k)$$

Burnside's formula

Theorem

$$a_{ijk} = \frac{h_i h_j}{|G|} \sum_{t=1}^{r} \frac{\chi_t(x_i)\chi_t(x_j)\overline{\chi_t(x_k)}}{n_t} \qquad (\textit{where } h_i = |C_i|)$$

Proof.

Expand $\omega_t(\hat{C}_i)\omega_t(\hat{C}_j) = \sum_{\ell=1}^{r} a_{ij\ell}\omega_t(\hat{C}_\ell)$.

$$\frac{h_i\chi_t(x_i)}{n_t}\frac{h_j\chi_t(x_j)}{n_t} = \sum_{\ell=1}^{r} a_{ij\ell}\frac{h_\ell\chi_t(x_\ell)}{n_t}.$$

Multiply by $n_t\overline{\chi_t(x_k)}$, sum over t, then use the second orthogonality relations.

$$h_i h_j \sum_{t=1}^{r} \frac{\chi_t(x_i)\chi_t(x_j)\overline{\chi_t(x_k)}}{n_t} = \sum_{t,\ell} a_{ij\ell} h_\ell \chi_t(x_\ell)\overline{\chi_t(x_k)}$$
$$= \sum_{\ell} a_{ij\ell} h_\ell |C_G(x_k)| \delta_{k\ell} = a_{ijk}|G|.$$

□

Algebraic integers

An element of a commutative ring B is *integral* over a subring A if it is a root of a *monic* polynomial with coefficients from A.

A complex number which is integral over $\mathbb{Z}$ is an *algebraic integer*. If $z \in \mathbb{Q}$ is an algebraic integer, then $z \in \mathbb{Z}$.

Theorem

The following are equivalent:

1. $x \in B$ *is integral over* A.
2. *The subring* $A[x]$ *of* B *is a finitely generated* A*-module.*
3. $A[x]$ *is contained in a subring* C *of* B *such that* C *is a finitely generated* A*-module.*

Corollary

The elements of B *which are integral over* A *form a submodule of* B.

$\therefore$ *If* χ *is a character,* $\chi(x)$ *is an algebraic integer*

Right eigenvectors of the class matrices

For $1 \le i \le r$ let A_i be the $r \times r$ matrix $\left(a_{ijk}\right)_{j,k}$. $\longleftarrow$ *class matrix*

Theorem

The eigenvalues of A_i *are the quantities* $\omega_t(\hat{C}_i)$ *for* $1 \le t \le r$*, hence the* $\omega_t(\hat{C}_i)$ *are algebraic integers.*

Proof.

We may write $\omega_t(\hat{C}_i)\omega_t(\hat{C}_j) = \sum_{k=1}^{r} a_{ijk}\omega_t(\hat{C}_k)$ as

$$\sum_{k=1}^{r} \left(\omega_t(\hat{C}_i)\delta_{jk} - a_{ijk}\right)\omega_t(\hat{C}_k) = 0.$$

That is, the column vector $(\omega_t(\hat{C}_1), \ldots, \omega_t(\hat{C}_r))^\top$ is an eigenvector of A_i; it is non-zero because $\omega_t(\hat{C}_1) = |C_1| = 1$.

Thus $\det(\omega_t(\hat{C}_i)I - A_i) = 0$ and the $\omega_t(\hat{C}_i)$ are eigenvalues of A_i.

Moreover they satisfy a monic polynomial with integer coefficients; i.e., they are algebraic integers. □

Left eigenvectors of the class matrices

We have

$$a_{ijk}|C_k| = \left|\{(x,y) \in C_i \times C_j \mid xy \in C_k\}\right|$$

and therefore

$$a_{ijk}|C_k| = a_{i'kj}|C_j|$$

where $C_{i'} = \{x^{-1} \mid x \in C_i\}$.

Thus $\omega_t(\hat{C}_{i'})\omega_t(\hat{C}_k) = \sum_{j=1}^{r} a_{i'kj}\omega_t(\hat{C}_j)$ becomes

$$\sum_{j=1}^{r} \chi_t(x_j)\left(\omega_t(\hat{C}_{i'})\delta_{jk} - a_{ijk}\right) = 0$$

and so $(\chi_t(x_1), \chi_t(x_2), \ldots, \chi_t(x_r))$ is a left eigenvector of A_i.

Divisibility

Theorem

The degrees of the irreducible characters of G divide $|G|$.

Proof.

Suppose that χ_t is an irreducible character of degree n_t and that for $1 \le i \le r$, $C_i = \mathrm{ccl}_G(x_i)$. Then

$$\sum_{i=1}^{r} \omega_t(\hat{C}_i)\overline{\chi}_t(x_i) = \frac{1}{n_t}\sum_{i=1}^{r} |C_i|\chi_t(x_i)\overline{\chi}_t(x_i) = \frac{1}{n_t}\sum_{x \in G} \chi_t(x)\overline{\chi}_t(x)$$
$$= \frac{|G|}{n_t}\langle \chi_t \mid \chi_t \rangle = \frac{|G|}{n_t},$$

whence $|G|/n_t$ is an algebraic integer. Since this is a rational number it must belong to $\mathbb{Z}$; that is, n_t divides $|G|$. □

Further properties of characters

Theorem

Let ρ be a linear representation of G with character χ. For all $x \in G$

1. $|\chi(x)| \le \chi(1)$,
2. $|\chi(x)| = \chi(1)$ *if and only if* $\rho(x) = \lambda I$ *for some* $\lambda \in \mathbb{C}^\times$,
3. $\chi(x) = \chi(1)$ *if and only if* $\rho(x) = I$.

Proof.

We have $x^d = 1$ for some divisor d of $|G|$. Thus the eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_k$ of $\rho(x)$ are dth roots of unity and

$$|\chi(x)| = |\lambda_1 + \lambda_2 + \cdots + \lambda_k| \le k = \chi(1).$$

If $|\chi(x)| = \chi(1)$, then $\lambda_1 = \lambda_2 = \cdots = \lambda_k$.
If $\chi(x) = \chi(1)$, then $\lambda_i = 1$ for all i. The minimal polynomial of $\rho(x)$ divides $X^d - 1$ and therefore has distinct roots, whence $\rho(x) = I$.
The converse implications of 2 and 3 are clear. □

The kernel of a character

From 2 of the theorem $\{x \in G \mid \chi(x) = \chi(1)\} = \ker \rho$ and for convenience we also refer to it as $\ker \chi$.

The character χ is said to be *faithful* if $\ker \chi = 1$.

(Recall that the *centre* of a group H is $Z(H) = \{x \in H \mid xy = yx \text{ for all } y \in H\}$.)

If $N \trianglelefteq G$, define $Z(G \bmod N) = \{x \in G \mid xN \in Z(G/N)\}$.

From 3 of the theorem

$$\{x \in G \mid |\chi(x)| = \chi(1)\} \subseteq Z(G \bmod \ker \chi).$$

and if χ is irreducible it follows from Schur's lemma that equality holds.

Solubility

A group G is *soluble* if there is a sequence of subgroups

$$G_0 = 1 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_\ell = G,$$

each normal in the next, such that all G_{i+1}/G_i are abelian.

Lemma

If $G \neq 1$ is a p-group, $Z(G) \neq 1$, hence G is soluble.

Proof.

Let $x_1 = 1$, x_2, ..., x_r represent the conjugacy classe of G. Then

$$|G| = 1 + \sum_{i \neq 1} |\mathrm{ccl}_G(x_i)|.$$

Thus there exists $i \neq 1$ such that $|\mathrm{ccl}_G(x_i)|$ is not divisible by p. But then $|\mathrm{ccl}_G(x_i)| = 1$ and hence $G = C_G(x_i)$; that is, $x_i \in Z(G)$.
The fact that G is soluble follows by induction. □

A lemma of Burnside

Lemma

Suppose χ is an irreducible character of G and that $\gcd(\chi(1), |\mathrm{ccl}_G(x)|) = 1$ for $x \in G$. Then either $\chi(x) = 0$ or $x \in Z(G \bmod \ker \chi)$.

Proof.

There exist integers a and b such that $a\chi(1) + b|\mathrm{ccl}_G(x)| = 1$. Thus

$$\frac{\chi(x)}{\chi(1)} = a\chi(x) + b\frac{|\mathrm{ccl}_G(x)|\chi(x)}{\chi(1)} = a\chi(x) + b\omega_\chi(\widehat{\mathrm{ccl}_G(x)})$$

and so $\alpha = \chi(x)/\chi(1)$ is an algebraic integer. Let α_1, ..., α_m be the algebraic conjugates of α. Then $\chi(1)\alpha_i$ is a sum of $\chi(1)$ roots of unity and hence $|\alpha_i| \leq 1$ and thus $|\prod_i \alpha_i| \leq 1$. This is a rational number and therefore it is either 0 or 1. In the first case $\chi(x) = 0$ and in the second case $|\chi(x)| = 1$, whence $x \in Z(G \bmod \ker \chi)$. □

Burnside's nonsimplicity criterion

Theorem

Suppose that $|\mathrm{ccl}_G(x)| = p^a$ *for some* $x \in G$*, where* $x \neq 1$ *and* p *is a prime. If* G *is a simple group, then* G *is cyclic of prime order.*

Proof.

If $a = 0$, then $x \in Z(G)$ and the result follows.
Let $\chi_1 = 1_G$, χ_2, ..., χ_r be the irreducible characters of G. If $a > 0$ and G is a noncyclic simple group, every nonprincipal character is faithful. From the second orthogonality relations we have

$$1 + \sum_{i \neq 1} \chi_i(1)\chi_i(x) = 0.$$

If for $i \neq 1$, $p \nmid \chi_i(1)$ implies $\chi_i(x) = 0$, the equation becomes $1 + p\alpha = 0$ for some algebraic integer α, which is impossible. Thus for some i, $\gcd(|\mathrm{ccl}_G(x)|, \chi_i(1)) = 1$ and $\chi_i(x) \neq 0$. Therefore, by the previous lemma, $x \in Z(G)$, contrary to our assumption. □

Burnside's $p^a q^b$ theorem

Theorem

Every group of order $p^a q^b$ *(*p *and* q *primes) is soluble.*

Proof.

Let Q be a Sylow q-subgroup of G and choose $x \in Z(Q)$, $x \neq 1$. Then $Q \subseteq C_G(x)$ and thus $|\mathrm{ccl}_G(x)| = p^c$ for some $c \leq a$.
By Burnside's non-simplicity criterion G is either of prime order or G has a normal subgroup $1 \neq N \neq G$.
A group of prime order is soluble and by induction N and G/N are soluble. Therefore G is soluble. □