Orthogonality relations for characters and blocks

Benjamin Sambale TU Kaiserslautern

Mathematics & Statistics Colloquium, Maynooth

February 3, 2016

Representations

Let G be a finite group and let F be a field.

Definition

A representation of G over F is a group homomorphism

$$\Delta: G \to \mathrm{GL}(n, F)$$

for some $n \ge 1$.

These maps encode information about G. For example, if Δ is injective, then of course $G \cong \Delta(G)$. This makes it possible to work with concrete matrices instead of abstract group elements.

The symmetries of the cube

Example

Let G be the symmetry group of the cube in \mathbb{R}^3 . Then the elements of G can be realized as 3×3 matrices, i. e. there exists an injective representation $\Delta : G \to GL(3, \mathbb{R})$. For instance:



Characters

Definition

The map $\chi: G \to F$, $g \mapsto tr(\Delta(g))$ is called the character of Δ .

- The characters are the "shadows" of representations (we lose information by reducing the "dimension" of the objects).
- Since similar matrices have the same trace, characters are constant on conjugacy classes, i.e. $\chi(hgh^{-1}) = \chi(g)$ for all $g, h \in G$.
- The representation Δ and its character are called irreducible if there is no subspace $0 \subsetneq V \subsetneq F^n$ such that $\Delta(g)(V) \subseteq V$ for all $g \in G$.

Decomposition of characters

Proposition

Every character χ of G is a sum of irreducible characters χ_1, \ldots, χ_r , *i.e.*

$$\chi(g) = \chi_1(g) + \ldots + \chi_r(g) \qquad \forall g \in G.$$

Therefore, we are primarily interested in the irreducible characters of G.

Character tables

- Now assume that $F = \mathbb{C}$. Then the set Irr(G) of irreducible characters of G is finite.
- More precisely, the cardinality k := |Irr(G)| equals the number of conjugacy classes of G.
- Hence, the values of these characters can be given by the character table

$$T = (\chi_i(g_j))_{i,j=1}^k,$$

a square matrix of complex numbers.

• The character table still contains important information of G (e.g., it determines if G is abelian or solvable), but the isomorphism type of G is usually not preserved.

Ordinary orthogonality

Theorem (Orthogonality relations)

We have

$$T^{\mathsf{t}}\overline{T} = \begin{pmatrix} |\mathcal{C}_G(g_1)| & 0\\ & \ddots & \\ 0 & & |\mathcal{C}_G(g_k)| \end{pmatrix}$$

where $C_G(g_i) := \{x \in G : xg_i = g_ix\}$. It follows that

$$(\chi_i, \chi_j)_G := \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_j(g)} = \delta_{ij}.$$

The character table of A_6

Example

The character table of the alternating group $G = A_6$ of degree 6 is given by



Modular representation theory

In the following we fix a prime p.

Definition

Let $G_{p'}$ be the set of p'-elements of G. We define a graph \mathcal{G} with vertices $\mathrm{Irr}(G)$ such that $[\chi,\psi]$ is an edge iff

$$\sum_{\mathbf{g}\in G_{p'}}\chi(g)\overline{\psi(g)}\neq 0.$$

The connected components of \mathcal{G} are called the (*p*-)blocks of G.

If $p \nmid |G|$, then $G_{p'} = G$ and the orthogonality relations imply that every p-block is a singleton.

Block distribution for A_6

Example

Again let $G = A_6$. Then the *p*-blocks are given as follows:



Block distribution for A_6

Example

Again let $G = A_6$. Then the *p*-blocks are given as follows:



Block distribution for A_6

Example

Again let $G = A_6$. Then the *p*-blocks are given as follows:



Modular orthogonality

For $g \in G$, the abelian group $\langle g \rangle$ is a direct product of a *p*-group and a *p'*-group. Therefore, *g* can be written uniquely as $g = g_p g_{p'}$ where $g_p \in \langle g \rangle$ is a *p*-element and $g_{p'} \in G_{p'}$.

Theorem (Block orthogonality relations)

Let $g, h \in G$ such that g_p and h_p are not conjugate in G. Then

$$\sum_{\chi \in B} \chi(g) \overline{\chi(h)} = 0$$

for every block B of G.

A converse result

Since $g\in G_{p'}$ iff $g_p=1,$ the theorem applies for $g\in G_{p'}$ and $h\in G\setminus G_{p'}.$

Conjecture (Harada, 1981)

If $J \subseteq Irr(G)$ such that

$$\sum_{\chi \in J} \chi(1)\chi(h) = 0 \qquad \forall h \in G \setminus G_{p'},$$

then J is a union of blocks.

This conjecture holds if G is (p-)solvable or |J| = 1, i. e. $\{\chi\}$ is a block iff $\chi(g) = 0$ for all $g \in G \setminus G_{p'}$.

Block orthogonality for A_6

Example

Let
$$G = A_6$$
 and $p = 2$.



Brauer characters

- Now let F be an algebraically closed field of characteristic p.
- Then every character χ of G over F determines a Brauer character $\varphi: G_{p'} \to \mathbb{C}$ by "lifting" $\chi(g)$ to \mathbb{C} .
- The (finite) set of irreducible Brauer characters of G is denoted by $\operatorname{IBr}(G)$.
- The values of these functions can be expressed with the Brauer character table $T_p = (\varphi_i(g_j))_{i,j}$. This is again a complex square matrix.
- If $p \nmid |G|$, then Irr(G) = IBr(G) and $T_p = T$.

Generalized decomposition numbers

In the following let G_p be the set of *p*-elements of *G*.

Proposition

Let $u \in G_p$ and let $\chi \in Irr(G)$. Then there are uniquely determined algebraic integers $d^u_{\chi\varphi}$ in the cyclotomic field $\mathbb{Q}_{|\langle u \rangle|}$ such that

$$\chi(uv) = \sum_{\varphi \in \operatorname{IBr}(\mathcal{C}_G(u))} d^u_{\chi\varphi}\varphi(v) \qquad \forall v \in \mathcal{C}_G(u)_{p'}.$$

The numbers $d^u_{\chi \omega}$ are called generalized decomposition numbers.

For u = 1 we obtain a connection between Irr(G) and IBr(G).

Brauer characters of blocks

Definition

Let B be a block of G. We define

$$\operatorname{IBr}(B) := \{ \varphi \in \operatorname{IBr}(G) : d^1_{\chi \varphi} \neq 0 \text{ for some } \chi \in B \}.$$

- This yields a partition of $\mathrm{IBr}(G)$, i. e. every irreducible Brauer character belongs to exactly one block.
- In fact, the sets IBr(B) are precisely the connected components of the graph \mathcal{G}_p on IBr(G) with edges $[\varphi, \mu]$ where

$$\sum_{g \in G_{p'}} \varphi(g) \overline{\mu(g)} \neq 0.$$

9

The Brauer character table of A_6

Example

$$T_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 4 & 1 & -2 & -1 & -1 \\ 4 & -2 & 1 & -1 & -1 \\ 8 & -1 & -1 & \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \\ 8 & -1 & -1 & \frac{1-\sqrt{5}}{2} & \frac{1+\sqrt{5}}{2} \end{pmatrix}.$$

The Brauer character table of A_6

Example

$$T_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 3 & -1 & 1 & \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \\ 3 & -1 & 1 & \frac{1-\sqrt{5}}{2} & \frac{1+\sqrt{5}}{2} \\ 4 & . & -2 & -1 & -1 \\ 9 & 1 & 1 & -1 & -1 \end{pmatrix}.$$

The Brauer character table of A_6

Example

$$T_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 5 & 1 & 2 & -1 & -1 \\ 5 & 1 & -1 & 2 & -1 \\ 8 & . & -1 & -1 & . \\ 10 & -2 & 1 & 1 & . \end{pmatrix}.$$

Brauer correspondence

For a character χ of G and a subgroup $H \leq G$, the restriction $\chi_H : H \to \mathbb{C}$ is a character of H.

Definition

Let $u \in G_p$, let b be a block of $H := C_G(u)$ and let $\psi \in b$. Then the Brauer correspondent of b is the unique block $B := b^G$ of G such that the p-parts of $\sum_{\chi \in B} \chi(1)(\chi_H, \psi)_H$ and $|G : H|\psi(1)$ coincide.

Theorem (Brauer's second main theorem)

In the situation above we have $d^u_{\chi\varphi} = 0$ unless $\varphi \in \operatorname{IBr}(b)$ and $\chi \in \operatorname{Irr}(b^G)$.

Generalized decomposition matrices

Proposition

Let $u_1, \ldots, u_r \in G_p$ be representatives for the conjugacy classes in G_p . We define a matrix

$$Q_p := \left(d_{\chi\varphi}^{u_i} : \chi \in \operatorname{Irr}(G), \ i = 1, \dots, r, \ \varphi \in \operatorname{IBr}(\mathcal{C}_G(u_i)) \right)$$

whose rows are indexed by Irr(G) and the columns are indexed by pairs (i, φ) with $\varphi \in IBr(C_G(u_i))$. Then Q_p is invertible, in particular it has square shape.

Generalized decomposition matrices of blocks

According to Brauer's second main theorem, ${\cal Q}_p$ can be arranged in the form

$$Q_p = \begin{pmatrix} W_1 & 0 \\ & \ddots & \\ 0 & & W_n \end{pmatrix}$$

where the W_i correspond to the blocks B_i of G. We call W_i the generalized decomposition matrix of B_i .

The generalized decomposition matrix of A_6

Example

$$Q_2 = \begin{pmatrix} 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot \\ 1 & 1 & \cdot & 1 & -1 & \cdot & \cdot \\ 1 & \cdot & 1 & 1 & -1 & \cdot & \cdot \\ 1 & 1 & 1 & 1 & 1 & \cdot & \cdot \\ 2 & 1 & 1 & -2 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix}$$

The generalized decomposition matrix of A_6

Example



The generalized decomposition matrix of A_6

Example



Another orthogonality

Theorem (Orthogonality of generalized decomposition numbers)

The generalized decomposition matrix Q_B of a block B can be arranged such that

$$Q_B^t \overline{Q_B} = \begin{pmatrix} C_1 & 0 \\ & \ddots & \\ 0 & & C_l \end{pmatrix}$$

where each C_i is the Cartan matrix of a block b of $C_G(u)$ such that $b^G = B$. In particular, $Q_B^t \overline{Q_B}$ is integral and positive definite. Moreover, $\det(Q_B^t \overline{Q_B})$ is a p-power.

Another orthogonality of A_6

Example

Let
$$G = A_6$$
 and $p = 2$.

$$Q_2 = \begin{pmatrix} 1 & . & . & 1 & 1 & . & . \\ 1 & 1 & . & 1 & -1 & . & . \\ 1 & . & 1 & 1 & -1 & . & . \\ 1 & 1 & 1 & 1 & -1 & . & . \\ 2 & 1 & 1 & -2 & . & . & . \\ . & . & . & . & . & 1 & . \\ . & . & . & . & . & . & 1 \end{pmatrix}$$

Another orthogonality of A_6

Example

Let
$$G = A_6$$
 and $p = 2$.

$$Q_{2} = \begin{pmatrix} 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot \\ 1 & 1 & \cdot & 1 & -1 & \cdot & \cdot \\ 1 & \cdot & 1 & 1 & -1 & \cdot & \cdot \\ 1 & 1 & 1 & 1 & 1 & \cdot & \cdot \\ 2 & 1 & 1 & -2 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix}$$
$$-1 \cdot 1 + 1 \cdot 1 = 0$$

Refinements

• By the theorem above, we may restrict ourselves to the matrix

$$Q_B^{(u,b)} := (d^u_{\chi\varphi})_{\chi \in B, \varphi \in \mathrm{IBr}(b)}$$

where $u \in G_p$ and b is a block of $C_G(u)$ with $b^G = B$.

- Let p^r be the order of u, and let $\zeta := e^{\frac{2\pi i}{p^r}} \in \mathbb{C}$.
- Then $1, \zeta, \ldots, \zeta^s$ where $s := p^{r-1}(p-1) 1$ is an integral basis for \mathbb{Q}_{p^r} .
- Hence, for $\chi \in B$ and $\varphi \in \text{IBr}(b)$ there exist integers $a_i(\chi, \varphi)$ such that $d^u_{\chi\varphi} = \sum_{i=0}^s a_i(\chi, \varphi)\zeta^i$.

Discrete Fourier transformation

- Consequently, $Q_B^{(u,b)}$ can be represented by an integral matrix A of size $|B| \times s |\text{IBr}(b)|$. This can be understood as a discrete Fourier transformation.
- By the results above, it is natural to ask if $A^{\rm t}A$ actually depends on $Q_B^{(u,b)}.$

Theorem (S. 2015)

The matrix $A^{t}A$ only depends on the following local invariants:

• the Cartan matrix C_b of b,

2 the group
$$\mathcal{N} := \operatorname{N}_G(\langle u \rangle, b) / \operatorname{C}_G(u)$$
,

③ the action of \mathcal{N} on $\operatorname{IBr}(b)$ by conjugation.

A special case

Unfortunately, $A^{t}A$ does not have a "nice" shape in terms of these three ingredients (it is usually not invertible). But in a special case things behave better.

Proposition (S. 2015)

Suppose that \mathcal{N} acts trivially on $\operatorname{IBr}(b)$. Then $A^{t}A$ is a Kronecker product of the form $C_{b} \otimes S$ where S is related to the semidirect product $\langle u \rangle \rtimes \mathcal{N}$.

A trivial case

For u = 1, $Q_B^{(1,B)}$ is already integral and $A^{t}A = C_B$. Here the following is of interest.

Basic set conjecture (≤ 1991)

There exists $J \subseteq \operatorname{Irr}(B)$ such that $|J| = |\operatorname{IBr}(B)|$ and the matrix $(d^1_{\chi\varphi})_{\chi\in J,\varphi\in\operatorname{IBr}(B)}$ has determinant ± 1 .

This conjecture is satisfied if G is (p-)solvable or |IBr(B)| = 1 (Malle-Navarro-Späth 2015).

The number of characters in a block

For $\chi \in Irr(G)$ it is known that $\chi(1) \in \mathbb{N}$ divides |G|.

Definition

Let B be a p-block of G. Then the largest integer d such that $p^d \mid \frac{|G|}{\chi(1)}$ for some $\chi \in B$ is called the defect of B. We write d(B) := d.

Conjecture (Brauer, 1954)

For every block B we have $|B| \leq p^{d(B)}$.

Theorem (Brauer-Feit)

For every block B we have $|B| \leq p^{2d(B)}$.

Non-zero decomposition numbers

Proposition

Let b be a block of $C_G(u)$ such that b and $B := b^G$ have the same defect. Then for every $\chi \in B$ there exists a $\varphi \in IBr(b)$ such that $d^u_{\chi\varphi} \neq 0$.

• It follows that

$$|B| \le \sum_{\chi \in B} \sum_{\varphi \in \mathrm{IBr}(b)} |d^u_{\chi \varphi}|^2 = \mathrm{tr}(C_b).$$

- The proposition applies with u = 1 and B = b. In this case we also have $|B| \leq \det(C_B)$ (S. 2015).
- To improve these bounds we apply the discrete Fourier transformation introduced earlier.

A global-local bound

Theorem (S. 2015)

Let $A^{t}A$ be the integral matrix coming from the discrete Fourier transformation of $Q_{B}^{(u,b)}$. Let $m \in \mathbb{N}$ be maximal with the property that there exists an integral matrix M with m non-zero rows such that $M^{t}M = A^{t}A$. Then $|B| \leq m$.

- The importance of the theorem is that $A^{t}A$ is locally determined and thus easier to compute than A itself.
- There is an algorithm by Plesken which finds all matrices M such that $M^{t}M = A^{t}A$. This can be used to compute m in the theorem above.

A bigger example

Example

• Let $G = {}^{2}F_{4}(2)'$. This is a simple group of Lie type of order

$$|G| = 17,971,200 = 2^{11} \cdot 3^3 \cdot 5^2 \cdot 13.$$

- Let B be the 3-block containing the trivial character χ (i.e. $\chi(g)=1$ for all $g\in G$).
- Then d(B) = 3 and Brauer's conjecture asserts that $|B| \le 27$.
- Let $u \in G$ be of order 3 and let b be a block of $C_G(u)$ such that $b^G = B$.

A bigger example

Example (continued)

• Then d(b) = 3 and

$$C_b = 3 \begin{pmatrix} 3 & 2 & 2 & 2 \\ 2 & 3 & 2 & 2 \\ 2 & 2 & 3 & 2 \\ 2 & 2 & 2 & 3 \end{pmatrix}$$

- In fact, C_b is determined by $C_G(u)/\langle u \rangle \cong Z_3^2 \rtimes Z_4$, a group with only 36 elements.
- This implies $|B| \leq 18$ (use something more clever than $tr(C_b)$).

A bigger example

Example (continued)

The matrix $A^{t}A$ is given by

$$A^{\mathsf{t}}A = \begin{pmatrix} 8 & 1 & 7 & -1 & 6 & . & 6 & . \\ 1 & 2 & -1 & -2 & . & . & . \\ 7 & -1 & 8 & 1 & 6 & . & 6 & . \\ -1 & -2 & 1 & 2 & . & . & . & . \\ 6 & . & 6 & . & 9 & . & 6 & . \\ . & . & . & . & . & . & . & . \\ 6 & . & 6 & . & 6 & . & 9 & . \\ . & . & . & . & . & . & . & . \end{pmatrix}$$

Plesken's algorithm gives $|B| \le 15$. In fact, it is known that |B| = 13.

Applications

An application of the global-local bound together with other ideas leads to the following.

Theorem (S. 2015)

Let B be a p-block with $d(B) \leq 3$ (or $d(B) \leq 5$ if p = 2). Then $|B| \leq p^{d(B)}$, i. e. Brauer's conjecture holds for B.

Defect groups

Definition

Let B be a block of G. A defect group of B is a maximal p-subgroup $D \leq G$ such that B has a Brauer correspondent in $N_G(D)$.

- One can show that D is unique up to conjugation and $|D|=p^{d(B)}.$
- When we study the matrix $Q_B^{(u,b)}$, we may always assume that u lies in a defect group of B.

Abelian defect groups

For a group H we define $Z(H) := \{x \in H : xy = yx \ \forall y \in H\}.$

Proposition

Let B be a block with defect group D, let $u \in Z(D)$ and let b be a block of $C_G(u)$ such that $b^G = B$. Then d(b) = d(B) and the global-local bound established above applies.

If D is abelian, then $\mathbf{Z}(D)=D$ and the methods are particularly strong.

Theorem (S. 2014)

Let B be a block with abelian defect group. Then $|B| \leq p^{3d(B)/2}$.

Abelian defect groups

Theorem (S. 2015)

Let B be a block with abelian defect group of rank ≤ 3 (or ≤ 7 if p = 2). Then $|B| \leq p^{d(B)}$.

Both results rely implicitly on the classification of the finite simple groups.