Corollary 15.1

Character values are algebraic integers.

Proof: By the above, roots of unity are algebraic integers. Since the algebraic integers form a ring, so are sums of roots of unity. Hence the claim follows from Property 7.5(b). ■

16 Central Characters

We now extend representations/characters of finite groups to "representations/characters" of the centre of the group algebra $\mathbb{C}G$ in order to obtain further results on character values, which we will use in the next sections in order to prove Burnside's $p^a q^b$ theorem.

Definition 16.1 (*Class sums*)

The elements $\widehat{C_j} := \sum_{g\in C_j} g \in \mathbb{C}G$ $(1 \leqslant j \leqslant r)$ are called the **class sums** of G.

Lemma 16.2

The class sums $\{\widehat{C_j} \mid 1 \leqslant j \leqslant r\}$ form a $\mathbb{C}$-basis of $Z(\mathbb{C}G)$. In other words, $Z(\mathbb{C}G) = \bigoplus_{j=1}^r \mathbb{C}\widehat{C_j}$.

Proof: Notice that the class sums are clearly $\mathbb{C}$-linearly independent because the group elements are.

'$\supseteq$': $\forall\ 1 \leqslant j \leqslant r$ and $\forall\ g \in G$, we have

$$g \cdot \widehat{C_j} = g(g^{-1}\widehat{C_j}g) = \widehat{C_j} \cdot g\,.$$

Extending by $\mathbb{C}$-linearity, we get $a\cdot\widehat{C_j} = \widehat{C_j}\cdot a\ \ \forall\, 1 \leqslant j \leqslant r$ and $\forall\, a \in \mathbb{C}G$. Thus $\bigoplus_{j=1}^r \mathbb{C}\widehat{C_j} \subseteq Z(\mathbb{C}G)$.

'$\subseteq$': Let $a \in Z(\mathbb{C}G)$ and write $a = \sum_{g\in G} \lambda_g g$ with $\{\lambda_g\}_{g\in G} \subseteq \mathbb{C}$. Since a is central, for every $h \in G$, we have

$$\sum_{g\in G} \lambda_g g = a = hah^{-1} = \sum_{g\in G} \lambda_g (hgh^{-1})\,.$$

Comparing coefficients yield $\lambda_g = \lambda_{hgh^{-1}}\ \forall\ g, h \in G$. Namely, the coefficients λ_g are constant on the conjugacy classes of G, and hence

$$a = \sum_{j=1}^{r} \lambda_{g_j} \widehat{C_j} \in \bigoplus_{j=1}^{r} \mathbb{C}\widehat{C_j}\,.$$

■

Now, notice that by definition the class sums $\widehat{C_j}$ $(1 \leqslant j \leqslant r)$ are elements of the subring $\mathbb{Z}G$ of $\mathbb{C}G$, hence of the centre of $\mathbb{Z}G$.

Corollary 16.3

(a) $Z(\mathbb{Z}G)$ is finitely generated as a $\mathbb{Z}$-module.

(b) The centre $Z(\mathbb{Z}G)$ of the group ring $\mathbb{Z}G$ is integral over $\mathbb{Z}$; in particular the class sums $\widehat{C_j}$ $(1 \leqslant j \leqslant r)$ are integral over $\mathbb{Z}$.

Proof:

(a) It follows directly from the second part of the proof of Lemma 16.2 that the class sums $\widehat{C}_j$ $(1 \leqslant j \leqslant r)$ span $Z(\mathbb{Z}G)$ as a $\mathbb{Z}$-module.

(b) The centre $Z(\mathbb{Z}G)$ is integral over $\mathbb{Z}$ by Theorem D.2 because it is finitely generated as a $\mathbb{Z}$-module by (a). ■

Notation 16.4 (*Central characters*)

If $\chi \in \mathrm{Irr}(G)$, then we may consider a $\mathbb{C}$-representation affording χ, say $\rho^\chi : G \longrightarrow \mathrm{GL}(\mathbb{C}^{n(\chi)}) = \mathrm{Aut}_{\mathbb{C}}(\mathbb{C}^{n(\chi)})$ with $n(\chi) := \chi(1)$. This group homomorphism extends by $\mathbb{C}$-linearity to a $\mathbb{C}$-algebra homomorphism

$$\begin{array}{rccl} \widetilde{\rho}^\chi : & \mathbb{C}G & \longrightarrow & \mathrm{End}_{\mathbb{C}}(\mathbb{C}^{n(\chi)}) \\ & a = \sum_{g\in G} \lambda_g g & \mapsto & \widetilde{\rho}^\chi(a) = \sum_{g\in G} \lambda_g \rho^\chi(g)\,. \end{array}$$

Now, if $z \in Z(\mathbb{C}G)$, then for each $g \in G$, we have

$$\widetilde{\rho}^\chi(z)\widetilde{\rho}^\chi(g) = \widetilde{\rho}^\chi(zg) = \widetilde{\rho}^\chi(gz) = \widetilde{\rho}^\chi(g)\widetilde{\rho}^\chi(z)\,.$$

As we have already seen in Chapter 2 on Schur's Lemma this means that $\widetilde{\rho}^\chi(z)$ is $\mathbb{C}G$-linear. This holds in particular if z is a class sum. Therefore, by Schur's Lemma, for each $1 \leqslant j \leqslant r$ there exists a scalar $\omega_\chi(\widehat{C}_j) \in \mathbb{C}$ such that

$$\widetilde{\rho}^\chi(\widehat{C}_j) = \omega_\chi(\widehat{C}_j) \cdot I_{n(\chi)}\,.$$

The functions defined by

$$\begin{array}{rccc} \omega_\chi : & Z(\mathbb{C}G) & \longrightarrow & \mathbb{C} \\ & \widehat{C}_j & \mapsto & \omega_\chi(\widehat{C}_j) \end{array}$$

and extended by $\mathbb{C}$-linearity to the whole of $Z(\mathbb{C}G)$, where χ runs through $\mathrm{Irr}(G)$, are called the **central characters** of $\mathbb{C}G$ (or simply of G).

Remark 16.5

If $z \in Z(G)$, then $[z] = \{z\}$ and therefore the corresponding class sum is z itself. Therefore, we may see the functions $\omega_\chi|_{Z(G)} : Z(G) \longrightarrow \mathbb{C}$ as representations of $Z(G)$ of degree 1, or equivalently as linear characters of $Z(G)$.

Theorem 16.6 (*Integrality Theorem*)

The values $\omega_\chi(\widehat{C}_j)$ $(\chi \in \mathrm{Irr}(G),\ 1 \leqslant j \leqslant r)$ of the central characters of G are algebraic integers. Moreover,

$$\omega_\chi(\widehat{C}_j) = \frac{|C_j|}{\chi(1)}\chi(g_j) \qquad \forall\, \chi \in \mathrm{Irr}(G),\ \forall\, 1 \leqslant j \leqslant r\,.$$

Proof: Let $\chi \in \mathrm{Irr}(G)$ and $1 \leqslant j \leqslant r$. By Corollary 16.3 the class sum $\widehat{C}_j$ is an algebraic integer. Thus there exist integers $n \in \mathbb{Z}_{>0}$ and $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ such that $\widehat{C}_j^n + a_{n-1}\widehat{C}_j^{n-1} + \ldots + a_0 = 0$. Applying ω_χ yields $\omega_\chi(\widehat{C}_j)^n + a_{n-1}\omega_\chi(\widehat{C}_j)^{n-1} + \ldots + a_0 = \omega_\chi(0) = 0$, so that $\omega_\chi(\widehat{C}_j)$ is also an algebraic integer.
Now, according to Notation 16.4 we have

$$\chi(1)\omega_\chi(\widehat{C}_j) = \mathrm{Tr}\left(\widetilde{\rho}^\chi(\widehat{C}_j)\right) = \mathrm{Tr}\Big(\sum_{g\in C_j} \rho^\chi(g)\Big) = \sum_{g\in C_j} \mathrm{Tr}\left(\rho^\chi(g)\right) = \sum_{g\in C_j} \chi(g) = |C_j|\chi(g_j)\,,$$

where the last equality holds because characters are class functions. The claim follows. ■

Corollary 16.7

If $\chi \in \mathrm{Irr}(G)$, then $\chi(1)$ divides $|G|$.

Proof: By the 1st Orthogonality Relations we have

$$\frac{|G|}{\chi(1)} = \frac{|G|}{\chi(1)}\langle \chi, \chi\rangle_G = \frac{1}{\chi(1)}\sum_{g\in G}\chi(g)\chi(g^{-1}) = \frac{1}{\chi(1)}\sum_{j=1}^{r}|C_j|\chi(g_j)\chi(g_j^{-1}) = \sum_{j=1}^{r}\underbrace{\frac{|C_j|}{\chi(1)}\chi(g_j)}_{\omega_\chi(\hat{C}_j)}\chi(g_j^{-1})\,.$$

Now, for each $1 \leqslant j \leqslant r$, $\omega_\chi(g_j)$ is an algebraic integer by the Integrality Theorem and $\chi(g_j^{-1})$ is an algebraic integer by Corollary 15.1. Hence $|G|/\chi(1)$ is an algebraic integer because these form a subring of $\mathbb{C}$. Moroever, clearly $|G|/\chi(1) \in \mathbb{Q}$. As the algebraic integers in $\mathbb{Q}$ are just the elements of $\mathbb{Z}$, we obtain that $|G|/\chi(1) \in \mathbb{Z}$, as claimed. ■

Example 8 (*The degrees of the irreducible characters of* $\mathrm{GL}_3(\mathbb{F}_2)$)

The group $G := \mathrm{GL}_3(\mathbb{F}_2)$ is a simple group of oder

$$|G| = \#\,\mathbb{F}_2\text{-bases of } \mathbb{F}_2^3 = (2^3-1)(2^3-2)(2^3-2^2) = 168 = 2^3\cdot 3\cdot 7\,.$$

For the purpose of this example we accept without proof that G is simple and that it has 6 conjugacy classes.

Question: can we compute the degrees of the irreducible characters of $\mathrm{GL}_3(\mathbb{F}_2)$?

(1) By the above $|\mathrm{Irr}(G)| = |C(G)| = 6$ and the degree formula yields:

$$1 + \sum_{i=2}^{6}\chi_i(1)^2 = |G| = 168\,.$$

(2) Next, as G is simple non-abelian, $G = G'$ and therfeore G has $|G : G'| = 1$ linear characters by Corollary 14.8, namely

$$\chi_i(1) \geqslant 2 \text{ for each } 2 \leqslant i \leqslant 6\,.$$

Thus, at this stage, we would have the following possibilities for the degrees of the 6 irreducible characters of G:

$\chi_1(1)$	$\chi_2(1)$	$\chi_3(1)$	$\chi_4(1)$	$\chi_5(1)$	$\chi_6(1)$
1	2	4	5	6	9
1	2	3	3	8	9
1	2	5	5	7	8
1	2	4	7	7	7
1	3	3	6	7	8

(3) By Corollary 16.7 we now know that $\chi_i(1) \mid |G|$ for each $2 \leqslant i \leqslant 6$. Therefore, as $5 \nmid |G|$ and $9 \nmid |G|$, the first three rows can already be discarded:

$\chi_1(1)$	$\chi_2(1)$	$\chi_3(1)$	$\chi_4(1)$	$\chi_5(1)$	$\chi_6(1)$
1	2	4	5	6	~~9~~
1	2	3	3	8	~~9~~
1	2	~~5~~	~~5~~	7	8
1	2	4	7	7	7
1	3	3	6	7	8

(4) In order to eliminate the last-but-one possibility, we use Exercise 14.14 telling us that a simple group cannot have an irreducible character of degree 2. Hence

$$\chi_1(1) = 1\,,\ \chi_2(1) = 3\,,\ \chi_3(1) = 3\,,\ \chi_4(1) = 6\,,\ \chi_5(1) = 7\,,\ \chi_6(1) = 8\,.$$

Exercise 16.8

Let G be a finite group of odd order and, as usual, let r denote the number of conjugacy classes of G. Use character theory to prove that

$$r \equiv |G| \pmod{16}\,.$$

[Hint: Label the set $\mathrm{Irr}(G)$ of irreducible characters taking dual characters into account. Use the divisibility property of Corollary 16.7]

17 The Centre of a Character

Definition 17.1 (*Centre of a character*)

The **centre** of a character χ of G is $Z(\chi) := \{g \in G \mid |\chi(g)| = \chi(1)\}$.

Note: Recall that in contrast, $\chi(g) = \chi(1) \ \Leftrightarrow\ g \in \ker(\chi)$.

Example 9

Recall from Example 5 that the character table of $G = S_3$ is

	Id	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Hence $Z(\chi_1) = Z(\chi_2) = G$ and $Z(\chi_3) = \{\mathrm{Id}\}$.

Lemma 17.2

If $\rho : G \longrightarrow \mathrm{GL}(V)$ is a $\mathbb{C}$-representation affording the character χ and $g \in G$, then:

$$|\chi(g)| = \chi(1) \quad\Longleftrightarrow\quad \rho(g) \in \mathbb{C}^\times\,\mathrm{Id}_V\,.$$

In other words $Z(\chi) = \rho^{-1}(\mathbb{C}^\times\,\mathrm{Id}_V)$.

Proof: Let $n := \chi(1)$. Recall that we can find a $\mathbb{C}$-basis B of V such that $(\rho(g))_B$ is a diagonal matrix with diagonal entries $\varepsilon_1, \dots, \varepsilon_n$ which are $o(g)$-th roots of unity. Hence $\varepsilon_1, \dots, \varepsilon_n$ are the eigenvalues of $\rho(g)$. Applying the Cauchy-Schwarz inequality to the vectors $v := (\varepsilon_1, \dots, \varepsilon_n)$ and $w := (1, \dots, 1)$ in $\mathbb{C}^n$ yields

$$|\chi(g)| = |\varepsilon_1 + \dots + \varepsilon_n| = |\langle v, w\rangle| \leqslant ||v|| \cdot ||w|| = \sqrt{n}\sqrt{n} = n = \chi(1)$$

and equality implies that v and w are $\mathbb{C}$-linearly dependent so that $\varepsilon_1 = \dots = \varepsilon_n =: \varepsilon$. Therefore $\rho(g) \in \mathbb{C}^\times \operatorname{Id}_V$. Conversely, if $\rho(g) \in \mathbb{C}^\times \operatorname{Id}_V$, then there exists $\lambda \in \mathbb{C}^\times$ such that $\rho(g) = \lambda \operatorname{Id}_V$. Therefore the eigenvalues of $\rho(g)$ are all equal to λ, i.e. $\lambda = \varepsilon_1 = \dots = \varepsilon_n$ and therefore

$$|\chi(g)| = |n\lambda| = n|\lambda| = n \cdot 1 = n\,.$$

■

Proposition 17.3

Let χ be a character of G. Then:

(a) $Z(\chi) \trianglelefteq G$;

(b) $\ker(\chi) \trianglelefteq Z(\chi)$ and $Z(\chi)/\ker(\chi)$ is a cyclic group;

(c) if χ is irreducible, then $Z(\chi)/\ker(\chi) = Z(G/\ker(\chi))$.

Proof: Let $\rho : G \longrightarrow \operatorname{GL}(V)$ be a $\mathbb{C}$-representation affording χ and set $n := \chi(1)$.

(a) Clearly $\mathbb{C}^\times \operatorname{Id}_V \leqslant Z(\operatorname{GL}(V))$ and hence $\mathbb{C}^\times \operatorname{Id}_V \trianglelefteq \operatorname{GL}(V)$. Therefore, by Lemma 17.2,

$$Z(\chi) = \rho^{-1}\big(\mathbb{C}^\times \operatorname{Id}_V\big) \trianglelefteq G$$

as the pre-image under a group homomorphism of a normal subgroup.

(b) By the definitions of the kernel and of the centre of a character, we have $\ker(\chi) \subseteq Z(\chi)$. Therefore $\ker(\chi) \trianglelefteq Z(\chi)$ by (a). By Lemma 17.2 restriction to $Z(\chi)$ yields a group homomorphism

$$\rho|_{Z(\chi)} : Z(\chi) \longrightarrow \mathbb{C}^\times \operatorname{Id}_V$$

with kernel $\ker(\chi)$. Therefore, by the 1st ismomorphism theorem, $Z(\chi)/\ker(\chi)$ is isomorphic to a finite subgroup of $\mathbb{C}^\times \operatorname{Id}_V \cong \mathbb{C}^\times$, hence is cyclic (c.f. e.g. EZT).

(c) By the arguments of (a) and (b) we have

$$Z(\chi)/\ker(\chi) \cong \rho\big(Z(\chi)\big) \leqslant Z\big(\rho(G)\big)\,.$$

Applying again the first isomorphism theorem we have $\rho(G) \cong G/\ker(\rho)$, hence

$$Z\big(\rho(G)\big) \cong Z\big(G/\ker(\rho)\big) = Z\big(G/\ker(\chi)\big)\,.$$

Now let $g\ker(\chi) \in Z(G/\ker(\chi))$, where $g \in G$. As χ is irreducible, by Schur's Lemma, there exists $\lambda \in \mathbb{C}^\times$ such that $\rho(g) = \lambda \operatorname{Id}_V$. Thus $g \in Z(\chi)$ and it follows that

$$Z\big(G/\ker(\chi)\big) \leqslant Z(\chi)/\ker(\chi)\,.$$

■

Exercise 17.4

Prove that if $\chi \in \operatorname{Irr}(G)$, then $Z(G) \leqslant Z(\chi)$. Deduce that $\bigcap_{\chi \in \operatorname{Irr}(G)} Z(\chi) = Z(G)$.

Remark 17.5

Prove that, if $\chi \in \mathrm{Irr}(G)$, then $\chi(1) \mid |G : Z(\chi)|$. Deduce that $\chi(1) \mid |G : Z(G)|$.

This allows us to prove an important criterion, due to Burnside, for character values to be zero.

Theorem 17.6 (*Burnside*)

Let $\chi \in \mathrm{Irr}(G)$ and let $C = [g]$ be a conjugacy class of G such that $\gcd(\chi(1), |C|) = 1$. Then $\chi(g) = 0$ or $g \in Z(\chi)$.

Proof: As $\gcd(\chi(1), |C|) = 1$, there exist $u, v \in \mathbb{Z}$ such that $u\chi(1) + v|C| = 1$ Set $\alpha := \frac{\chi(g)}{\chi(1)}$. Then

$$\alpha = \frac{\chi(g)}{\chi(1)} \cdot 1 = \frac{\chi(g)}{\chi(1)}\big(u\chi(1) + v|C|\big) = u\chi(g) + v\frac{|C|\chi(g)}{\chi(1)} = u\chi(g) + v\omega_\chi(C)$$

is an algebraic integer because both $\chi(g)$ and $\omega_\chi(C)$ are. Now, set $m := |\langle g\rangle|$ and let $\zeta_m := e^{\frac{2\pi i}{m}}$. As $\chi(g)$ is a sum of m-th roots of unity, certainly $\chi(g) \in \mathbb{Q}(\zeta_m)$. Let $\mathcal{G}$ be the Galois group of the Galois extension $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_m)$. Then for each field automorphism $\sigma \in \mathcal{G}$, $\sigma(\alpha)$ is also an algebraic integer because α and $\sigma(\alpha)$ are roots of the same monic integral polynomial. Hence $\beta := \prod_{\sigma\in\mathcal{G}} \sigma(\alpha)$ is also an algebaric integer and because $\sigma(\beta) = \beta$ for every $\sigma \in \mathcal{G}$, β is an element of the fixed field of $\mathcal{G}$, namely $\beta \in \mathbb{Q}$ (Galois theory). Therefore $\beta \in \mathbb{Z}$.

If $g \in Z(\chi)$, then there is nothing to do. Thus we may assume that $g \notin Z(\chi)$. Then $|\chi(g)| \neq \chi(1)$, so that by Property 7.5(c) we must have $|\chi(g)| < \chi(1)$ and hence $|\alpha| < 1$. Now, again by Property 7.5(b), $\chi(g) = \varepsilon_1 + \ldots + \varepsilon_n$ with $n = \chi(1)$ and $\varepsilon_1, \ldots, \varepsilon_n$ m-th roots of unity. Therefore, for each $\sigma \in \mathcal{G}\backslash\{\mathrm{Id}\}$, we have $\sigma(\chi(g)) = \sigma(\varepsilon_1) + \ldots + \sigma(\varepsilon_n)$ with $\sigma(\varepsilon_1), \ldots, \sigma(\varepsilon_n)$ m-th roots of unity, because $\varepsilon_1, \ldots, \varepsilon_n$ are. It follows that

$$|\sigma(\chi(g))| = |\sigma(\varepsilon_1) + \ldots + \sigma(\varepsilon_n)| \leqslant |\sigma(\varepsilon_1)| + \ldots + |\sigma(\varepsilon_n)| = n = \chi(1)$$

and hence

$$|\sigma(\alpha)| = \frac{1}{\chi(1)}|\sigma(\chi(g))| \leqslant \frac{\chi(1)}{\chi(1)} = 1\,.$$

Thus

$$|\beta| = |\prod_{\sigma\in\mathcal{G}} \sigma(\alpha)| = \underbrace{|\alpha|}_{<1} \cdot \prod_{\sigma\in\mathcal{G}\backslash\{\mathrm{Id}\}} \underbrace{|\sigma(\alpha)|}_{\leqslant 1} < 1\,.$$

The only way an integer satisfies this inequality is $\beta = 0$. Thus $\alpha = 0$ as well, which implies that $\chi(g) = 0$. ■

Corollary 17.7

Assume now that G is a non-abelian simple group. In the situation of Theorem 17.6 if we assume moreover that $\chi(1) > 1$ and $C \neq \{1\}$, then it is always the case that $\chi(g) = 0$.

Proof: We see that then either $\chi(g) = 0$ or $Z(\chi)$ is a non-trivial proper normal subgroup of G. Indeed, if $\chi(g) \neq 0$, then Theorem 17.6 implies that $g \in Z(\chi)$, so $Z(\chi) \neq 1$. Now, as G is non-abelian simple we have $Z(\chi) = G$. On the other hand, the fact that G is simple also tells us that $\ker(\chi) = 1$ (if it were G, then χ would be reducible). Then it follows from Proposition 17.3 that

$$G = Z(\chi)/\ker(\chi) = Z(G/\ker(\chi)) = Z(G) = 1\,.$$

A contradiction. ■