$\chi_1(1)$	$\chi_2(1)$	$\chi_3(1)$	$\chi_4(1)$	$\chi_5(1)$	$\chi_6(1)$
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 apply [Exercise 21(b), Sheet 6] saying 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 (*Exercise 22, Sheet 6*)

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 with character χ and $g \in G$, then:

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

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

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 $\varepsilon_1, \ldots, \varepsilon_n$ which are $o(g)$-th roots of unity. Hence $\varepsilon_1, \ldots, \varepsilon_n$ are the eigenvalues of $\rho(g)$. Applying the Cauchy-Schwartz inequality to the vectors $v := (\varepsilon_1, \ldots, \varepsilon_n)$ and $w := (1, \ldots, 1)$ in $\mathbb{C}^n$ yields

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

and equality implies that v and w are $\mathbb{C}$-linearly dependent so that $\varepsilon_1 = \ldots = \varepsilon_n =: \varepsilon$. Therefore $\rho(g) \in \mathbb{C}^\times \mathrm{Id}_V$. Conversely, if $\rho(g) \in \mathbb{C}^\times \mathrm{Id}_V$, then there exists $\lambda \in \mathbb{C}^\times$ such that $\rho(g) = \lambda \mathrm{Id}_V$. Therefore the eigenvalues of $\rho(g)$ are all equal to λ, i.e. $\lambda = \varepsilon_1 = \ldots = \varepsilon_n$ 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 $\rho : G \longrightarrow \mathrm{GL}(V)$ be a $\mathbb{C}$-representation affording χ and set $n := \chi(1)$.

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

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

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). If $g \in Z(\chi)$, then by Lemma 17.2 restriction to $Z(\chi)$ yields a group homomorphism

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

with kernel $\ker(\chi)$. Therefore, by the 1st ismomorphism theorem, $Z(\chi)/\ker(\chi)$ is isomorphic to a finite subgroup of $\mathbb{C}^\times \mathrm{Id}_V \cong \mathbb{C}^\times$, 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 $\overline{g} = g\ker(\chi) \in Z(G/\ker(\chi))$. As χ is irreducible, $\rho(g) = \lambda \mathrm{Id}_V$ for some $\lambda \in \mathbb{C}^\times$ by Schur's Lemma. Thus $g \in Z(\chi)$ and it follows that

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

■

Exercise 17.4 (*Exercise 23, Sheet 6*)

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

Remark 17.5 (*See* [Exercise 24, Sheet 6])

If χ is an irreducible character of degree n then n divides $|G : Z(\chi)|$, and hence divides $|G : Z(G)|$.

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 7.4(c) we must have $|\chi(g)| < \chi(1)$ and hence $|\alpha| < 1$. Now, again by Property 7.4(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

In the situation of Theorem 17.6 if moreover $\chi(1) > 1$ and $C \neq \{1\}$, then either $\chi(g) = 0$ or $Z(\chi)$ is a non-trivial normal subgroup of G. In particular, if G is non-abelian simple then it is always the case that $\chi(g) = 0$.

Proof: Indeed, if $\chi(g) \neq 0$, then Theorem 17.6 implies that $g \in Z(\chi)$, so $Z(\chi) \neq 1$. Now, if G is non-abelian simple, then $Z(\chi) = G$. 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. ∎

18 Burnside's $p^a q^b$-Theorem

Character theory has many possible applications to the to the structure of finite groups. We consider in this section on of the most famous of these: the proof of Burnside's $p^a q^b$ theorem.

Example 10

To begin with we consider two possible minor applications of character theory to finite groups. Both are results of the *Einfürung in die Algebra*, for which you have already seen purely group-theoretic proofs.

(a) G finite group such that $|G| = p^2$ for some prime number $p \implies G$ is abelian.

· **Proof using character theory**. By Corollary 16.7 we have $\chi(1) \mid |G|$ for each $\chi \in \mathrm{Irr}(G)$. Thus

$$\chi(1) \in \{1, p, p^2\}\,.$$

Therefore the class equation reads

$$p^2 = |G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = \underbrace{\mathbf{1}_G(1)^2}_{=1} + \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi \neq \mathbf{1}_G}} \chi(1)^2\,,$$

which implies that it is not possible that the degree of an irreducible character of G is p or p^2. In other words, all the irreducible characters of G are linear, and thus G is abelian by Corollary 14.8.

(b) G is a non-trivial p-group $\implies G$ is soluble.

[Recall from the *Einfürung in die Algebra* that a finite group G is **soluble** if it admits a chain of subgroups

$$1 = G_0 < G_1 < \ldots < G_s = G$$

such that for $1 \leqslant i \leqslant s$, $G_{i-1} \lhd G_i$ and G_i/G_{i-1} is cyclic of prime order. Moreover, we have the following very useful *solubility criterion*, sometimes coined "the sandwich principle": if $H \trianglelefteq G$ is a normal subgroup, then the group G is soluble if and only if both G and G/H are soluble.]

· **Proof using character theory**. By induction on $|G| =: p^a$ ($a \in \mathbb{Z}_{>0}$). If $|G| = p$ or $|G| = p^2$, then G is abelian (cyclic in the former case). Finite abelian groups are clearly soluble because they are products of cyclic groups of prime power order.
Therefore, we may assume that $|G| \geqslant p^3$. As in (a) Corollary 16.7 implies that

$$\chi(1) \in \{1, p, p^2, \ldots, p^a\} \quad \text{for each } \chi \in \mathrm{Irr}(G)\,.$$

Now, again the degree formula yields

$$p^a = |G| = 1 + \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi \neq \mathbf{1}_G}} \chi(1)^2\,.$$

and for this equality to hold, there must be at least p linear characters of G (including the trivial character). Thus it follows from Corollary 14.8 that $G' \lneq G$. Hence both G' and G/G' are soluble by the induction hypothesis $\Rightarrow G$ is soluble by the *sandwich principle*.

Theorem 18.1 (*Burnside*)

Let G be a finite non-abelian simple group. If C is a conjugacy class of G such that $|C| = p^a$ with p prime and $a \in \mathbb{Z}_{\geqslant 0}$, then $C = \{1\}$.

Proof: Assume ab absurdo that $C \neq \{1\}$ and choose $g \in C$. In particular $g \neq 1$. Since G is non-abelian simple $G = G'$ and it follows from Corollary 14.8 that the unique linear character of G is the trivial character. Hence for each $\chi \in \mathrm{Irr}(G)\backslash\{\mathbf{1}_G\}$ we have either $p \mid \chi(1)$ or $\gcd(\chi(1), |C|) = 1$. Thus $\chi(g) = 0$ if $p \nmid \chi(1)$ and $\chi \neq \mathbf{1}_G$ by Corollary 17.7. Therefore the Second Orthogonality Relations read

$$0 = 1 + \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi \neq \mathbf{1}_G}} \underbrace{\chi(g)}_{\substack{=0 \text{ if} \\ p \nmid \chi(1)}} \underbrace{\overline{\chi(1)}}_{=\chi(1)} = 1 + \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ p \mid \chi(1)}} \chi(g)\chi(1)$$

and dividing by p yields

$$\underbrace{\sum_{\substack{\chi \in \mathrm{Irr}(G) \\ p \mid \chi(1)}} \underbrace{\frac{\chi(1)}{p}}_{\in \mathbb{Z}} \underbrace{\chi(g)}_{\substack{\text{algebraic} \\ \text{integer}}}}_{\text{algebraic integer}} = -\frac{1}{p} \in \mathbb{Q}\backslash\mathbb{Z}\,.$$

This contradicts the fact that rational numbers which are algebraic integers are integers. It follows that $g = 1$ is the only possibility and hence $C = \{1\}$. ∎

As a consequence, we obtain Burnside's $p^a q^b$ theorem, which can be found in the literature under two different forms. The first version provides us with a "non-simplicity" criterion and the second version with a solubility criterion, which is extremely hard to prove by purely group theoretic methods.

Theorem 18.2 (*Burnside's $p^a q^b$ Theorem, "simple" version*)

Let p, q be prime numbers and let $a, b \in \mathbb{Z}_{\geqslant 0}$ be integers such that $a + b \geqslant 2$. If G is a finite group of order $p^a q^b$, then G is not simple.

Proof: First assume that $a = 0$ or $b = 0$. Then G is a q-group with $q^2 \mid |G|$, resp. a p-group with $p^2 \mid |G|$. Therefore the centre of G is non-trivial (*Einführung in die Algebra*), thus of non-trivial prime power order. Therefore there exists an element $g \in Z(G)$ of order q (resp. p) and $1 \neq \langle g \rangle \lhd G$ is a proper non-trivial normal subgroup. Hence G is not simple.
We may now assume that $a \neq 0 \neq b$. Let $Q \in \mathrm{Syl}_q(G)$ be a Sylow q-subgroup of G (i.e. $|Q| = q^b$). Again, as Q is a q-group, we have $Z(Q) \neq \{1\}$ and we can choose $g \in Z(Q)\backslash\{1\}$. Then

$$Q \leqslant C_G(g)$$

and therefore the Orbit-Stabiliser Theorem yields

$$|[g]| = |G : C_G(g)| = p^r$$

for some non-negative integer $r \leqslant a$. If $r = 0$, then $p^r = 1$ and $G = C_G(g)$, so that $g \in Z(G)$. Hence $Z(G) \neq \{1\}$ and G is not simple by the same argument as above. If $p^r > 1$, then G cannot be simple by Theorem 18.1. ∎

Theorem 18.3 (*Burnside's $p^a q^b$ Theorem, "soluble" version*)

Let p, q be prime numbers and $a, b \in \mathbb{Z}_{\geqslant 0}$. Then any finite group of order $p^a q^b$ is soluble.

Proof: Let G be a finite group of order $p^a q^b$. We proceed by induction on $a + b$.

· $a + b \in \{0, 1\} \implies G$ is either trivial or cyclic of prime order, hence clearly soluble.

- $a + b \geqslant 2 \implies G$ is not simple by the "simple" version of Burnside's $p^a q^b$ theorem. Hence there exists a proper non-trivial normal subgroup H in G and both $|H|, |G/H| < p^a q^b$. Therefore both H and G/H are soluble by the induction hypothesis. Thus G is soluble by the sandwich principle. ■