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

Let G be finite group, and let $\mathrm{Irr}(G)$ denote the set of complex irreducible characters of G. Also, let $\chi \in \mathrm{Irr}(G)$.

Central characters: Let V be a $\mathbb{C}G$-module affording χ. By Schur's lemma, any $z \in Z(\mathbb{C}G)$ acts as a scalar on V. This scalar is $\frac{\chi(z)}{\chi(1)} =: \omega_\chi(z)$. The ω_ψ, where ψ runs the irreducible characters of G, form a complete set of isomorphism classes of the irreducible representations of $Z(\mathbb{C}G)$. They are called the central characters of G.

Let $\mathcal{C} \subseteq G$ be a conjugacy class, and let $C := \sum_{g \in \mathcal{C}} g$ be the corresponding class sum. Recall that the class sums form a basis of $Z(\mathbb{C}G)$.

Proposition 1
Pick $g \in \mathcal{C}$. Then $\omega_\chi(C) = \frac{|\mathcal{C}|}{\chi(1)}\chi(g)$ is an algebraic integer.

Proof: Let $C_1, \ldots, C_r$ be the class sums of G. Then $C_i C_j = \sum_{l=1}^r a_{ijl} C_l$ with

$$a_{ijl} = |\{(x, y) \in \mathcal{C}_i \times \mathcal{C}_j \mid xy = z\}| \in \mathbb{N}_0$$

for any $z \in \mathcal{C}_l$. Since $\omega_\chi(C_i C_j) = \sum_{l=1}^r a_{ijl}\omega_\chi(C_l)$, the $\mathbb{Z}$-span $\langle \omega_\chi(C_i) \mid 1 \le i \le r\rangle_{\mathbb{Z}}$ is a subring of $\mathbb{C}$ (which contains 1 as $\omega_\chi(1) = 1$). $\square$

Corollary 2
$\chi(1)$ divides $|G|$.

Proof: By the first orthogonality relation, $|G| = \sum_{g \in G} \chi(g)\chi(g^{-1}) = \sum_{i=1}^r \chi(1)\omega_\chi(C_i)\chi(g_i^{-1})$, where $g_i \in \mathcal{C}_i$. Character values are sums of roots of unity, hence algebraic integers. This implies that $\frac{|G|}{\chi(1)} = \sum_{i=1}^r \omega_\chi(C_i)\chi(g_i^{-1})$ is an algebraic integer. $\square$

Definition 3
$Z(\chi) := \{g \in G \mid |\chi(g)| = \chi(1)\}$ is called the centre of G. $\square$

Since $\chi(g)$ is a sum of $\chi(1)$ roots of unity, $Z(\chi)$ consists of those elements of G which act as scalars on the module V affording χ. In particular, $Z(G) \le Z(\chi)$.

Proposition 4
$Z(G) = \bigcap_{\psi \in \mathrm{Irr}(G)} Z(\psi)$.

Proof: Pick $g \in \bigcap_{\psi \in \mathrm{Irr}(G)} Z(\psi)$. By the second orthogonality relation,

$$|C_G(g)| = \sum_{\psi \in \mathrm{Irr}(G)} |\psi(g)|^2 = \sum_{\psi \in \mathrm{Irr}(G)} |\psi(1)|^2 = |G|.$$

Hence $g \in Z(G)$. $\square$

Theorem 5 (Burnside, 1904)
Let $\mathcal{C} \subseteq G$ be a conjugacy class. If $|\mathcal{C}|$ and $\chi(1)$ are coprime, then either $\mathcal{C} \subseteq Z(\chi)$ or χ vanishes on $\mathcal{C}$.

Proof: Pick $a, b \in \mathbb{Z}$ such that $1 = a\chi(1) + b|\mathcal{C}|$. Then

$$b\omega_\chi(C) = (1 - a\chi(1))\frac{\chi(g)}{\chi(1)} = \frac{\chi(g)}{\chi(1)} - a\chi(g)$$

is an algebraic integer, where $g \in \mathcal{C}$ and $C := \sum_{x\in\mathcal{C}} x$. Hence $\frac{\chi(g)}{\chi(1)}$ is an algebraic integer. Suppose that $g \notin Z(\chi)$. Then $|\chi(g)| < \chi(1)$. Hence $|\prod_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\chi(g))/\mathbb{Q})} \sigma(\frac{\chi(g)}{\chi(1)})| < 1$. But $\prod_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\chi(g))/\mathbb{Q})} \sigma(\frac{\chi(g)}{\chi(1)})$ is an algebraic integer and lies in $\mathbb{Q}$, thus it this an integer. Hence it is zero, which is only possible if $\chi(g) = 0$, as desired. □

Corollary 6
If G is simple and for some $1 \neq g \in G$, the size of ${}^G g$ is a power of a prime p, then G is the group of order p.

Proof: Suppose not. Let $1 \neq \chi$ be an irreducible character of G. Then $Z(\chi)$ is trivial, since it is a proper normal subgroup of G. If $p \nmid \chi(1)$, then $\chi(g) = 0$. Thus

$$0 = \varrho(g) = \sum_{\chi\in\mathrm{Irr}(G)} \chi(1)\chi(g) = 1 + \sum_{\chi\in\mathrm{Irr}(G),\ p|\chi(1)} \chi(1)\chi(g),$$

where $\varrho = \chi_{\mathbb{C}G}$ denotes the regular character of G. But this implies $-\frac{1}{p} = \sum_{\chi\in\mathrm{Irr}(G),\ p|\chi(1)} \frac{\chi(1)}{p}\chi(g)$ which is impossible, since the right hand side is an algebraic integer. □

Theorem 7 (Burnside, 1904)
If $|G| = p^a q^b$ for some primes p, q, then G is solvable.

Proof: If G has a non-trivial normal subgroup, the claim follows by induction. Assume G to be simple. Let $1 \neq P \leq G$ be a Sylow subgroup of G. Since the centre of P is non-trivial, we may pick $1 \neq g \in Z(P)$. Then $|{}^G g| = [G : C_G(g)] | [G : P]$ is a prime power, and the claim follows, using the above corollary. □

Not only the theorem is due to Burnside, the above proof is as well. It is still the standard proof one finds in any textbook. The first purely group-theoretic proof of the $p^a q^b$-theorem is due to Bender and appeared in 1972. Some simplifications of Bender's proof were found, but it is still way more complicated than Burnside's argument.