# Understanding Burnside's Theorem

**Lily Zhang**

Macalester College
Math 476 – Representation Theory – Fall 2021 – Professor Tom Halverson

**Abstract**

William Burnside's $p^aq^b$ Theorem is a very important result in group theory, which states that any group $\mathsf{G}$ of order $p^aq^b$ is solvable. An interesting fact about this theorem is that it was originally proven through techniques from character theory, another branch of algebra. In fact, it was about seventy years before a group-theoretic proof of Burnside's Theorem was developed through the work of Goldschmidt, Matsuyama, Bender, and other mathematicians. This paper first reviews related terminology covered in the current semester and from an earlier course, MATH 376, and then states results such as Sylow's Theorem and introduces algebraic numbers, and finally elaborates a proof of Burnside's Theorem in a way that is accessible to all students in the MATH 476 course.

## 1 Introduction

### 1.1 Background

Burnside's Theorem was first proved by English mathematician William Burnside in 1904. While he is mainly known for his contributions to group theory, Burnside began his work in other areas of math, including elliptic functions and hydrodynamics. It was in 1893, as a Professor at the Royal Naval College in Greenwich, that Burnside published his first paper on group theory, and in 1897 he published the first edition of his book Theory of Groups of Finite Order.

### 1.2 Preliminary Definitions

To begin with, we first recall some important terminology, defining new terms that we learned over the semester and from MATH 376 that are necessary for the following sections.

**Definition 1.** *A group* $\mathsf{G}$ *is called* ***simple*** *if its only normal subgroups are* $\mathsf{G}$ *itself and* $\{1\}$.

Thus, we can think of a simple group as being a "building block" group that cannot be broken down any further with regards to normal subgroups.

**Definition 2.** *A group* $\mathsf{G}$ *is* ***solvable*** *if it has a chain of subgroups,* $\mathsf{G}_0, \mathsf{G}_1, \ldots, \mathsf{G}_r$ *with* $1 = \mathsf{G}_0 < \mathsf{G}_1 < \cdots < \mathsf{G}_r = \mathsf{G}$ *such that for* $1 \leq i \leq r$, $\mathsf{G}_{i-1} \lhd \mathsf{G}_i$ *and the factor group* $\mathsf{G}_i/\mathsf{G}_{i-1}$ *is cyclic of prime order.*

While the above definition appears technical, we can intuitively capture the idea of solvability as a condition that allows us to figuratively "pull apart" a group in order to analyze its components.

**Definition 3.** *A* ***p−group*** *is a group whose order is a power of the prime number p.*

**Definition 4.** *(The Class Equation) Let* $x_1, \ldots, x_l$ *be representatives of the conjugacy classes of* $\mathsf{G}$*. Then*

$$|\mathsf{G}| = |Z(\mathsf{G})| + \sum_{x_i \notin Z(\mathsf{G})} |x_i^{\mathsf{G}}|,$$

*where* $|x_i^{\mathsf{G}}| = |\mathsf{G} : C_{\mathsf{G}}(x_i)|$*, and both* $|Z(\mathsf{G})|$ *and* $|x_i^{\mathsf{G}}|$ *divide* $|\mathsf{G}|$*.*

# 2 Necessary Theorems

## 2.1 The Isomorphism Theorems

In this section we will recall the Isomorphism Theorems for groups that we learned from MATH 376, which serves as fundamental results in group theory, as well as crucial facts used in later proofs.

**Theorem 5.** *(First Isomorphism Theorem) Let* $\phi$ *be a group homomorphism from* $\mathsf{G}$ *to* $\overline{\mathsf{G}}$*. Then the mapping from* $\mathsf{G}/Ker\,\phi$ *to* $\phi(\mathsf{G})$*, given by* $gKer\,\phi \to \phi(g)$*, is an isomorphism. In symbols,* $\mathsf{G}/Ker\,\phi \cong \phi(\mathsf{G})$*.*

**Theorem 6.** *(Second Isomorphism Theorem) If* $\mathsf{K}$ *is a subgroup of* $\mathsf{G}$ *and* $\mathsf{N}$ *is a normal subgroup of* $\mathsf{G}$*, then* $\mathsf{K}/(\mathsf{K} \cap \mathsf{N})$ *is isomorphic to* $\mathsf{KN}/\mathsf{N}$*.*

**Theorem 7.** *(Third Isomorphism Theorem) Let* $\mathsf{N} \lhd \mathsf{G}$ *and let* $\mathsf{K}, \mathsf{H}$ *be subgroups with* $\mathsf{N} \leq \mathsf{K} \leq \mathsf{H} \leq \mathsf{G}$ *and* $\mathsf{K} \lhd \mathsf{H}$*. Then*

$$(\mathsf{H}/\mathsf{N})/(\mathsf{K}/\mathsf{N}) \;\cong\; \mathsf{H}/\mathsf{K}.$$

**Theorem 8.** *(Lattice Isomorphism Theorem) Let* $\mathsf{G}$ *be a group with* $\mathsf{N} \lhd \mathsf{G}$*. Then there is a bijection from the set of subgroups of* $\mathsf{G}$ *that contain* $\mathsf{N}$ *onto the set of subgroups of* $\mathsf{G}/\mathsf{N}$*. In particular, every subgroup* ***of*** $\mathsf{G}/\mathsf{N}$ *is of the form* $\mathsf{H}/\mathsf{N}$ *for some subgroup* $\mathsf{H}$ *of* $\mathsf{G}$ *containing* $\mathsf{N}$*.*

## 2.2 Lagrange's Theorem and Consequences

We begin by proving Lagrange's Theorem and Cauchy's Theorem, which give us information about the order of a group and its subgroups. We will then use these results to prove the existence of Sylow $p-$subgroups and show that $Z(\mathsf{G})$ is nontrivial for all $p-$groups $\mathsf{G}$. These results are all needed for the proof of Burnside's Theorem in the latter section.

**Theorem 9.** *(Lagrange's Theorem) Let* $\mathsf{G}$ *be a finite group and* $\mathsf{H} \leq \mathsf{G}$*. Then* $|\mathsf{H}|$ *divides* $|\mathsf{G}|$ *and* $|\mathsf{G} : \mathsf{H}| = \frac{|\mathsf{G}|}{|\mathsf{H}|}$*.*

*Proof.* Let $\mathsf{G}$ be a finite group and let $\mathsf{H} \leq \mathsf{G}$ such that $|\mathsf{H}| = m$ and $|\mathsf{G} : \mathsf{H}| = n$. Then for any $g \in G$, define the surjective mapping $\phi_g(h) = gh$. For any distinct $h_1 \neq h_2 \in \mathsf{H}$, we have $gh_1 \neq gh_2$. Thus $\phi_g$ is a bijection, so $|g\mathsf{H}| = |\mathsf{H}| = m$.

Observe that the set of left cosets of $\mathsf{H}$ in $\mathsf{G}$ forms a partition of $\mathsf{G}$. First note that for any $g \in \mathsf{G}$ and $g \in g\mathsf{H}$, we obtain $\mathsf{G} \subseteq \cup_{g\in\mathsf{G}} g\mathsf{H}$ and clearly $\cup_{g\in\mathsf{G}} g\mathsf{H} \subseteq \mathsf{G}$. Therefore, $\mathsf{G} = \cup_{g\in\mathsf{G}} g\mathsf{H}$. To show that left cosets are disjoint, suppose that for distinct cosets $g_1\mathsf{H} \neq g_2\mathsf{H} \in \mathsf{G}/\mathsf{H}$, there exists an element $x \in g_1\mathsf{H} \cap g_2\mathsf{H}$. Then there exist elements $h_1, h_2 \in \mathsf{H}$ such that $x = g_1h_1 = g_2h_2$. Therefore, $g_1 = g_2h_2h_1^{-1}$, so for any $g_1h \in g_1\mathsf{H}$, $g_1h = (g_2h_2h_1^{-1})h = g_2(h_2h_1^{-1}h) \in g_2\mathsf{H}$. Hence, $g_1\mathsf{H} \subseteq g_2\mathsf{H}$. But we have seen that $|g_1\mathsf{H}| = |g_2\mathsf{H}|$, so $g_1\mathsf{H} = g_2\mathsf{H}$, which is a contradiction. Thus, the $k$ left cosets of $\mathsf{H}$ in $\mathsf{G}$ are in fact disjoint and, hence, partition $\mathsf{G}$. Since each has cardinality $m$, it follows that $|\mathsf{G}| = km$. Therefore $|\mathsf{H}|$ divides $|\mathsf{G}|$ and $|\mathsf{G}|/|\mathsf{H}| = k$.

□

**Corollary 10.** *(Cauchy's Theorem) Let* $\mathsf{G}$ *be a finite abelian group, and let* $p \in \mathbb{N}$ *be a prime dividing* $|\mathsf{G}|$*. Then* $\mathsf{G}$ *has an element of order* $p$*.*

*Proof.* We prove this by induction on $|\mathsf{G}|$. Take any non-identity element $g \in \mathsf{G}$. If $|\mathsf{G}| = p$, then by *Theorem 9*, $g$ has order $p$. Now assume that $|\mathsf{G}| > p$ and that all subgroups of order less than $|\mathsf{G}|$ whose orders are divisible by $p$ have an element of order $p$. First consider the case where $p$ divides the order of $g$. Then we can write $|g| = np$, for some $n \in \mathbb{N}$. Thus, $1 = g^{np} = (g^n)^p$, so the order of $g^n$ must divide $p$. But $p$ is a prime, so $|g^n| = p$.

So we now consider the case where $p$ does not divide the order of $g$. Let $\mathsf{H} = \langle g\rangle$, which is a normal subgroup of $\mathsf{G}$, since $\mathsf{G}$ is abelian. By *Theorem 9*, $|\mathsf{G}/\mathsf{H}| < |\mathsf{G}|$, since $\mathsf{H}$ is nontrivial. Moreover, it must hold that $p$ divides $|\mathsf{G}/\mathsf{H}|$, because $p$ divides $|\mathsf{G}|$, but does not divide $|\mathsf{H}|$. Hence, by induction, $\mathsf{G}/\mathsf{H}$ contains an element of order $p$, say $x\mathsf{H}$. We have that $x^p \in \mathsf{H}$, but $x \notin \mathsf{H}$, so $\langle x^p\rangle \neq \langle x\rangle$, giving that $|x^p| < |x|$. Again, by *Theorem 9*, we can find that $|x^p|$ divides $|x|$, so we have $p$ divides $|x|$. This brings us back to the previous case. So, by induction, $\mathsf{G}$ has an element of order $p$. □

**Theorem 11.** *(Sylow's Theorem) Let* $p$ *be a prime number, and let* $\mathsf{G}$ *be a finite group of order* $p^a b$*, where* $a$*,* $b$ *are positive integers and* $p \nmid b$*. Then* $\mathsf{G}$ *contains a subgroup of order* $p^a$*; such a subgroup is called a Sylow* $p-$*subgroup of* $\mathsf{G}$*.*

*Proof.* We prove this by induction on $|\mathsf{G}|$. If $|\mathsf{G}| = 1$, the result is trivially true. Assume that Sylow $p-$subgroups exist for all groups of order less than $|\mathsf{G}|$. First consider the case where $p$ divides $|Z(\mathsf{G})|$. Since $Z(\mathsf{G})$ is an abelian group, then by *Corollary 10*, $Z(\mathsf{G})$ has a cyclic subgroup, $\mathsf{N}$, of order $p$. So by *Theorem 9*, $|\mathsf{G}/\mathsf{N}| = p^{a-1}b$. Therefore, by induction, $\mathsf{G}/\mathsf{N}$ has a Sylow $p-$subgroup, $\overline{P}$, of order $p^{a-1}$. Now define $P = \{g \in \mathsf{G} \,|\, gN \in \overline{P}\}$. To show $P$ is a subgroup of $\mathsf{G}$, first note that $1 \in P$ and $P \neq \emptyset$, since $1\mathsf{N}$ is the identity in $\mathsf{G}/\mathsf{N}$. Next, suppose $g_1, g_2 \in P$, i.e. $g_1\mathsf{N}, g_2\mathsf{N} \in \overline{P}$. Then $(g_1 g_2^{-1})\mathsf{N} = (g_1\mathsf{N})(g_2\mathsf{N})^{-1} \in \overline{P}$ since $\overline{P}$ is closed under inverses and multiplication; thus, $g_1 g_2^{-1} \in P$. Also note that $\mathsf{N}$ is a subgroup of $P$, since for all $n \in \mathsf{N}$, $n\mathsf{N} = \mathsf{N} \in \overline{P}$. Therefore, by construction, $\phi : g \mapsto g\mathsf{N}$ is a surjective homomorphism from $P$ into $\overline{P}$, and it follows that Ker $\phi = P \cap \mathsf{N} = \mathsf{N}$. By *Theorem 5*, we have $P/\mathsf{N} \cong \overline{P}$. Hence $|\overline{P}| = |P|/|\mathsf{N}|$, which implies that $|P| = |\overline{P}||\mathsf{N}| = p^{a-1}p = p^a$. Therefore, $P$ is a Sylow $p-$subgroup of $\mathsf{G}$.

Now consider the case where $p$ does not divide $|Z(\mathsf{G})|$. By the Class Equation (*Definition 4*), we have that $|\mathsf{G}| = |Z(\mathsf{G})| + \sum_{i=1}^{n} |\mathsf{G} : C_{\mathsf{G}}(g_i)|$, where $g_1, g_2, \ldots, g_n$ are representatives of the distinct conjugacy classes of $\mathsf{G}$ that are not contained in $Z(\mathsf{G})$. Reducing this congruence modulo $p$, if every term $|\mathsf{G} : C_{\mathsf{G}}(g_i)|$ were divisible by $p$ then $|Z(\mathsf{G})|$ would also be divisible by $p$, contrary to assumption. Hence for some $1 \leq i \leq n$, $p \nmid |\mathsf{G} : C_{\mathsf{G}}(g_i)|$, so $|C_{\mathsf{G}}(g_i)| = p^a k$ for some $k \in \mathbb{N}$ with $p \nmid k$. Moreover, since $g_i \notin Z(\mathsf{G})$, then $C_{\mathsf{G}}(g_i) \neq \mathsf{G}$, so $|C_{\mathsf{G}}(g_i)| < |\mathsf{G}|$. Therefore, by induction, $C_{\mathsf{G}}(g_i)$ has a Sylow $p-$subgroup, $P$, of order $p^a$, which is also a subgroup of $\mathsf{G}$. Thus, $P$ is a Sylow $p-$subgroup of $\mathsf{G}$. □

**Lemma 12.** *Let $\mathsf{G}$ be a group of order $p^n$ with $n \geq 1$. If $\{1\} \neq \mathsf{H} \lhd \mathsf{G}$ then $\mathsf{H} \cap Z(\mathsf{G}) \neq \{1\}$. In particular, $Z(\mathsf{G}) \neq \{1\}$.*

*Proof.* Since $\mathsf{H} \lhd \mathsf{G}$, $\mathsf{H}$ is a union of conjugacy classes of $\mathsf{G}$, all of which have size a power $p$; and $\mathsf{H} \cap Z(\mathsf{G})$ consists of those conjugacy classes in $\mathsf{H}$ which have size 1. Therefore

$$|\mathsf{H}| = |\mathsf{H} \cap Z(\mathsf{G})| + (\text{a multiple of } p).$$

Since $1 \in \mathsf{H} \cap Z(\mathsf{G})$, we have $|\mathsf{H} \cap Z(\mathsf{G})| \geq 1$. Reducing the displayed equality modulo $p$ gives $|\mathsf{H} \cap Z(\mathsf{G})| \equiv 0 \pmod{p}$, hence $|\mathsf{H} \cap Z(\mathsf{G})| \geq p$. Thus $\mathsf{H} \cap Z(\mathsf{G}) \neq \{1\}$. □

## 2.3 Characters

Although we all get quite familiar with the characters over the semester, it would be better to highlight some pivotal theorems that support the proof of Burnside's Theorem. *Throughout this subsection, all representations are over $\mathbb{C}$.*

**Proposition 13.** *Let $\chi$ be the character of a $d-$dimensional representation, then $\chi(g)$ is a sum of $d$ $m$th roots of unity where $|g| = m$.*

*Proof.* Since $g$ has finite order $m$, $\rho(g)$ satisfies $x^m - 1 = 0$. Over $\mathbb{C}$, the polynomial $x^m - 1$ has distinct roots, so $\rho(g)$ is diagonalizable with $m$th roots of unity on the diagonal. Hence $\chi(g) = \omega_1 + \ldots + \omega_d$ is a sum of $m$th roots of unity. □

**Theorem 14.** *Let $\chi_1, \ldots, \chi_k$ be the irreducible characters of $\mathsf{G}$, and let $g_1, \ldots, g_k$ be representatives of the conjugacy classes of $\mathsf{G}$. Then the column orthogonality relations:*

$$\sum_{i=1}^{k} \chi_i(g_r)\overline{\chi_i(g_s)} = \delta_{rs}|C_{\mathsf{G}}(g_s)|,$$

*hold for any $r, s \in \{1, \ldots, k\}$.*

*Proof.* For $1 \leq s \leq k$, let $\psi_s$ be the class function which satisfies

$$\psi_s(g_r) = \delta_{rs} \qquad (1 \leq r \leq k).$$

We know that $\psi_s$ can be written in a linear combination of $\chi_1, \ldots, \chi_k$, say

$$\psi_s = \sum_{i=1}^{k} \lambda_i \chi_i (\lambda_i \in \mathbb{C}).$$

Since $\langle \chi_i, \chi_j \rangle = \delta_{ij}$, so

$$\lambda_i = \langle \psi_s, \chi_i \rangle = \frac{1}{|\mathsf{G}|} \sum_{g \in \mathsf{G}} \psi_s(g)\overline{\chi_i(g)}.$$

Now $\psi_s(g) = 1$ if $g$ is conjugate to $g_s$, and $\psi_s(g) = 0$ otherwise; also there are $|\mathsf{G}|/|C_{\mathsf{G}}(g_s)|$ elements of $\mathsf{G}$ which are conjugate to $g_s$, by the orbit stabilizer theorem. Hence

$$\lambda_i = \frac{1}{|\mathsf{G}|} \sum_{g \in g_s^{\mathsf{G}}} \psi_s(g)\overline{\chi_i(g)} = \frac{\overline{\chi_i(g_s)}}{|C_{\mathsf{G}}(g_s)|}.$$

Therefore,

$$\delta_{rs} = \psi_s(g_r) = \sum_{i=1}^{k} \lambda_i \chi_i(g_r) = \sum_{i=1}^{k} \frac{\chi_i(g_r)\overline{\chi_i(g_s)}}{|C_{\mathsf{G}}(g_s)|},$$

and the column orthogonality relations follow. □

# 3 Algebraic Integers and Algebraic Numbers

Understanding algebraic integers and numbers will be essential in the proof of one of the main preliminary lemmas, and a couple preliminary lemmas which will be needed in the proof of Burnside's Theorem. For example, *Corollary 19* deals with a particular number constructed from a finite group $\mathsf{G}$ and one of its irreducible characters $\chi$.

### 3.1 Facts about Algebraic Integers

**Definition 15.** *$\lambda$ is an **algebraic integer** if and only if $\lambda$ is a root of a polynomial of the form $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$, where $a_0, \ldots, a_{n-1}$ are integers.*

Some examples of algebraic integers are $i$, $\sqrt{2}$, $\sqrt[3]{10}$, and $(1+\sqrt{5})/2$.

**Proposition 16.** *If $\lambda$ is both a rational number and an algebraic integer, then $\lambda$ is an integer.*

**Theorem 17.** *If $\lambda$ and $\mu$ are algebraic integers, then $\lambda\mu$ and $\lambda + \mu$ are also algebraic integers.*

**Corollary 18.** *If $\chi$ is a character of $\mathsf{G}$ and $g \in \mathsf{G}$, then $\chi(g)$ is an algebraic integer.*

**Corollary 19.** *If $\chi$ is an irreducible character of $\mathsf{G}$ and $g \in \mathsf{G}$, then*

$$\lambda = \frac{|\mathsf{G}|}{|C_{\mathsf{G}}(g)|}\frac{\chi(g)}{\chi(1)}$$

*is an algebraic integer.*

### 3.2 Facts about Algebraic Numbers

**Definition 20.** *Similarly, an **algebraic number** is a root of a polynomial equation with rational coefficients, i.e., $\beta$ is an algebraic number if and only if there exist $b_1, b_2, \ldots, b_m \in \mathbb{Q}$ with $\beta^m + b_1\beta^{m-1} + b_2\beta^{m-2} + \cdots + b_{m-1}\beta + b_m = 0$.*

The algebraic numbers include $(1+i)/2$, $\sqrt{1/5}$, and $\sin(2\pi/7)$.

**Definition 21.** *We call a polynomial in $x$ **monic** if the coefficient of the highest power of $x$ in it is 1.*

**Definition 22.** *Let $\alpha$ be an algebraic number; and let $p(x)$ be a monic polynomial over $\mathbb{Q}$ of smallest possible degree having $\alpha$ as a root. Then $p(x)$ is unique and irreducible; it is called the **minimal polynomial** of $\alpha$. The roots of $p(x)$ are called the **conjugates** of $\alpha$.*

**Theorem 23.** *Let $\alpha$ and $\beta$ be algebraic numbers. Then every conjugate of $\alpha + \beta$ is of the form $\alpha' + \beta'$, where $\alpha'$ is a conjugate of $\alpha$ and $\beta'$ is a conjugate of $\beta$.*

## 4 Proofs of Burnside's Theorem

The next lemma demonstrates the final result on algebraic integers necessary before the proof of the main theorem can proceed.

**Lemma 24.** *Let $\chi$ be a character of a finite group $\mathsf{G}$, and let $g \in \mathsf{G}$. Then $|\chi(g)/\chi(1)| \leq 1$, and if $0 < |\chi(g)/\chi(1)| < 1$ then $\chi(g)/\chi(1)$ is not an algebraic integer.*

*Proof.* Let $\chi(1) = d$. By *Proposition 13*, we have $\chi(g) = \omega_1 + \ldots + \omega_d$, where each $\omega_i$ is a root of unity. So, we write

$$\frac{\chi(g)}{\chi(1)} = \frac{\omega_1 + \ldots + \omega_d}{d}.$$

By the triangle inequality, $|\chi(g)| = |\omega_1 + \ldots + \omega_d| \leq |\omega_1| + \ldots + |\omega_d| = d$, which implies that $|\chi(g)/\chi(1)| \leq 1$. Now suppose that $\chi(g)/\chi(1)$ is an algebraic integer, and $|\chi(g)/\chi(1)| < 1$. Our next goal is to show $\chi(g) = 0$. Write $\alpha = \chi(g)/\chi(1)$, and let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be the minimal polynomial of $\alpha$, where $a_i \in \mathbb{Z}$ for all $i$. By *Theorem 23*, each conjugate of $\alpha$ is of the form

$$\alpha' = \frac{\omega_1' + \ldots + \omega_d'}{d} = \frac{\omega_1'}{d} + \ldots + \frac{\omega_d'}{d},$$

where $\omega_1', \ldots, \omega_d'$ are conjugate to $\omega_1, \ldots, \omega_d$. The minimal polynomial of $\omega_i$ divides $x^\ell - 1$ for some $\ell$, since each $\omega_i$ is a root of unity. So, all the conjugates of $\omega_i$ are roots of unity and therefore they have norm 1. It follows that if $\alpha'$ is a root of $p$, then

$$|\alpha'| = \left|\frac{\omega_1'}{d} + \ldots + \frac{\omega_d'}{d}\right| \leq \left|\frac{\omega_1'}{d}\right| + \ldots + \left|\frac{\omega_d'}{d}\right| = \frac{1}{d} + \ldots + \frac{1}{d} = 1.$$

But the conjugates of $\alpha$ are, by definition, the roots of the polynomial $p(x)$, and the product of all these roots is equal to $\pm a_0$. Therefore $|a_0| < 1$ since $|\alpha'| \leq 1$ for all the roots of $p$ and $|\alpha| < 1$. Since $a_0 \in \mathbb{Z}$, it must be that $a_0 = 0$. As $p(x)$ is irreducible, this implies that $p(x) = x$, which in turn forces $\alpha := \chi(g)/\chi(1) = 0$, contradicting $0 < |\chi(g)/\chi(1)| < 1$. Hence $\chi(g)/\chi(1)$ is not an algebraic integer. □

We deduce the main result (*Theorem 26*) from another interesting theorem of Burnside.

**Theorem 25.** *Let $p$ be a prime number and let $r$ be an integer with $r \geq 1$. Suppose that $\mathsf{G}$ is a finite group with a conjugacy class of size $p^r$. Then $\mathsf{G}$ is not simple.*

*Proof.* First, let $g \in \mathsf{G}$ with $|g^{\mathsf{G}}| = p^r$. Since $|g^{\mathsf{G}}| = p^r > 1$, we know that $g \notin Z(\mathsf{G})$. Thus, $\mathsf{G}$ is not abelian and $g \neq 1$. Then, let $\chi_1, \ldots, \chi_k$ be the irreducible characters of $\mathsf{G}$ and take $\chi_1$ to be the trivial character. Applying *Theorem 14* (column orthogonality) to the columns corresponding to 1 and $g$ in the character table of $\mathsf{G}$, we have

$$\sum_{i=1}^{k} \chi_i(1)\,\overline{\chi_i(g)} = 1 + \sum_{i=2}^{k} \chi_i(1)\,\overline{\chi_i(g)} = 0,$$

or, dividing by $p$,

$$\sum_{i=2}^{k} \overline{\chi_i(g)} \cdot \frac{\chi_i(1)}{p} = -\frac{1}{p}.$$

Note that $-1/p$ is in $\mathbb{Q}$ and not in $\mathbb{Z}$, so it is not an algebraic integer, by *Proposition 16*. Hence at least one term on the left is not an algebraic integer (*Theorem 17*). By *Corollary 18*, each $\chi_i(g)$ is an algebraic integer, so it follows that for some $i \geq 2$, $\chi_i(1)/p$ is not an algebraic integer. In particular, $p$ does not divide $\chi_i(1)$. Thus, $\chi_i(g) \neq 0$ and $p \nmid \chi_i(1)$. Hence $|g^{\mathsf{G}}| = p^r$ and $\chi_i(1)$ are relatively prime, so we can find $a, b \in \mathbb{Z}$ such that

$$a|g^{\mathsf{G}}| + b\chi_i(1) = 1,$$

and therefore, using $|g^{\mathsf{G}}| = |\mathsf{G} : C_{\mathsf{G}}(g)|$,

$$a\frac{|\mathsf{G}|}{|C_{\mathsf{G}}(g)|}\frac{\chi_i(g)}{\chi_i(1)} + b\,\chi_i(g) = \frac{\chi_i(g)}{\chi_i(1)}.$$

By *Corollaries 19 and 18*, the left-hand side is an algebraic integer. But the right-hand side is nonzero since $\chi_i(g) \neq 0$, so, by *Lemma 24*, we have $|\chi_i(g)/\chi_i(1)| = 1$. Equality in the triangle inequality forces all eigenvalues of $\rho(g)$ to be equal, hence $g$ acts as a scalar multiple of the identity under the corresponding representation $\rho$. Let $\mathsf{K} = \operatorname{Ker}\rho$, so that $\mathsf{K}$ is a normal subgroup of $\mathsf{G}$. Since $\chi_i$ is not the trivial character, $\mathsf{K} \neq \mathsf{G}$. Moreover, if $\mathsf{K} \neq \{1\}$, then $\mathsf{G}$ is not simple, and we are done. Therefore we may assume that $\mathsf{K} = \{1\}$, so that the associated representation $\rho$ is faithful. Since $\rho(g)$ is a scalar, it commutes with $\rho(h)$ for every $h \in \mathsf{G}$. As $\rho$ is faithful, this implies $g \in Z(\mathsf{G})$, so $Z(\mathsf{G}) \neq \{1\}$. As $Z(\mathsf{G})$ is a normal subgroup of $G$ and $Z(\mathsf{G}) \neq \mathsf{G}$, we conclude that $\mathsf{G}$ is not simple. □

**Theorem 26.** ***(No simple groups of order*** $p^aq^b$***.)*** *Let $p$ and $q$ be prime numbers, and let $a$ and $b$ be non-negative integers with $a + b \geq 2$. If $\mathsf{G}$ is a group of order $p^aq^b$, then $\mathsf{G}$ is not simple.*

*Proof.* First suppose that either $a = 0$ or $b = 0$. Then the order of $\mathsf{G}$ is a power of a prime, so by *Lemma 12* we have $Z(\mathsf{G}) \neq \{1\}$. Choose $g \in Z(\mathsf{G})$ of prime order. Then $\langle g\rangle \lhd \mathsf{G}$ and $\langle g\rangle$ is not equal to $\{1\}$ or $\mathsf{G}$. Hence $\mathsf{G}$ is not simple. Now assume that $a > 0$ and $b > 0$. By *Theorem 11*, $\mathsf{G}$ has a subgroup $\mathsf{Q}$ of order $q^b$. We have $Z(\mathsf{Q}) \neq \{1\}$ by *Lemma 12*. Let $g \in Z(\mathsf{Q})$ with $g \neq 1$. Then $\mathsf{Q} \leq C_{\mathsf{G}}(g)$, so $|g^{\mathsf{G}}| = |\mathsf{G} : C_{\mathsf{G}}(g)| = p^r$ for some $r$. If $p^r = 1$ then $g \in Z(\mathsf{G})$, so $Z(\mathsf{G}) \neq \{1\}$ and $\mathsf{G}$ is not simple as before. And if $p^r > 1$ then $\mathsf{G}$ is not simple, by *Theorem 25*. □

As a corollary, we have the following:

**Corollary 27.** *Let $p, q \in \mathbb{N}$ be prime, and let $a$ and $b$ be nonnegative integers. If $\mathsf{G}$ is a group of order $p^aq^b$, then $\mathsf{G}$ is solvable.*

*Proof.* We proceed by induction on $a + b$. If $a + b \leq 1$ then $\mathsf{G}$ is cyclic of prime order, hence abelian, and therefore solvable since its commutator subgroup is trivial. Now if $\mathsf{G}$ is of order $p^aq^b$ then, by *Theorem 26*, there is a normal subgroup $\mathsf{H}$ of $\mathsf{G}$. By the inductive

hypothesis, both $\mathsf{H}$ and $\mathsf{G}/\mathsf{H}$ are solvable since they are groups of order of the form $p^{a'}q^{b'}$ where $a'+b' < a+b$, so there are subgroups

$$\mathsf{H} = A_0 \geq A_1 \geq \ldots \geq A_s = 1,$$

$$\mathsf{G}/\mathsf{H} = B_0 \geq B_1 \geq \ldots \geq B_t = 1.$$

By *Theorem 8*, the $B_i$ correspond to subgroups $C_i$ of $\mathsf{G}$ containing $\mathsf{H}$ such that $C_i/\mathsf{H} = B_i$ for each $i$. It is easy to see that $C_{i+1}$ is normal in $C_i$ for each $i$ since $B_{i+1}$ is normal in $B_i$, and by *Theorem 7*, $C_i/C_{i+1} \cong (C_i/\mathsf{H})/(C_{i+1}/\mathsf{H}) \cong B_i/B_{i+1}$ for each $i$, so each quotient $C_i/C_{i+1}$ is abelian. Finally, $B_t = \{1\}$ corresponds to $C_t = \mathsf{H}$, so we have that $C_t/A_0 = \{1\}$ is abelian. Then the series

$$\mathsf{G} = C_0 \geq C_1 \geq \ldots \geq C_t \geq A_0 \geq A_1 \geq \cdots \geq A_s = 1$$

shows that $\mathsf{G}$ is solvable. □

## 5 An Illustration to Burnside's Theorem

**Example 28.** *Prove that if* $\mathsf{G}$ *is a non-abelian simple group of order less than 80, then* $|\mathsf{G}| = 60$.

*Solution:* By *Theorem 26*, $|\mathsf{G}|$ is not of the form $p^aq^b$, so it is divisible by at least three distinct primes. Since $3 \cdot 5 \cdot 7 > 80$, $|\mathsf{G}|$ is even. A non-abelian simple group cannot have a cyclic Sylow 2-subgroup; if $v_2(|\mathsf{G}|) = 1$ then the Sylow 2-subgroup has order 2 (cyclic), a contradiction. Hence $4 \mid |\mathsf{G}|$. Since $4 \cdot 3 \cdot 7 > 80$, the only possibility is that $|\mathsf{G}| = 4 \cdot 3 \cdot 5 = 60$. □

## 6 Some Comments and Extensions of Burnside's Results

1. Although Burnside's theorems are important applications of character and representation theory, attempts have been made to give purely group theoretic derivations. Bender has given a proof of the Burnside's $p^aq^b$ theorem which does not use character theory, it is long and quite difficult; versions are given in Huppert and Blackburn III (1982b) and Isaacs (2008). No non-character theory proof of the first Burnside Theorem (*Theorem 25*) is known.

2. Burnside, with some later corrections, showed that this holds in most cases. The exceptions make use of some primes which arise in elementary number theory and are somewhat surprising. Assume that $p^a > q^b$, then the order of $\mathsf{G}$ not equal to 1, except possibly in the following cases:

(a) $p = 2$ and $q = 2n + 1$ where this number is a 'Fermat' prime (and so $n$ is a power of 2), only five of which are known at the present time; they are 3, 5, 17, 257 and 65537.

(b) $p = 2m - 1$ and $q = 2$. Here $p$ must be a 'Mersenne' prime (and so $m$ is also prime), at the present time 40 are known.

(c) $p = 2$ and $q = 7$. In this case an example has been given for a group with order $2^{23} \cdot 7^8$.

## References


[1] Bender, H. (1972). A group theoretic proof of the $p^\alpha q^\beta$ theorem. *Math. Z.*, pp. 327-338.

[2] Burnside, W. (1904). On groups of order $p^\alpha q^\beta$. London, UK: Proc. London Math Soc. (2), pp. 388-391.

[3] Fulton W., Harris J. (2004). *Representation Theory, A First Course*. New York, NY: Springer Science+Business Media, LLC.

[4] James G., M. Liebeck. (2001). *Representations and Characters of Groups, Second Edition*. New York, NY: Cambridge University Press.

[5] Linman, J., Swisher, H. (2010). Burnside's Theorem. sites.science.oregonstate.edu/∼ swisherh/JulieLinman.pdf

[6] Rose, H. E. (2010). *A course on finite groups*. New York, NY: Springer Science+Business Media, LLC.