A PROOF OF BURNSIDE'S $p^a q^b$ THEOREM

OBOB

Abstract. We prove that if p and q are prime, then any group of order $p^a q^b$ is solvable.

Throughout this note, denote by $\mathbb{A}$ the set of algebraic numbers. We begin with some basic results from Galois theory which will be necessary later.

Proposition 1. *Let α, $\beta \in \mathbb{A}$, let p and q be polynomials with α and β as roots, and let r be the minimal (monic) polynomial for $\alpha + \beta$. If c is a root of r, then there are roots a and b of p and q, respectively, such that $c = a + b$.*

Proof. Let K be the splitting field for q. Since q is irreducible, $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the roots of q, so there is a $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\alpha + \beta) = c$. But σ is an automorphism, so $\sigma(\alpha) + \sigma(\beta) = c$. However, if $a(x)$ is any polynomial in $\mathbb{Q}[x]$, then an element of $\mathrm{Gal}(K/\mathbb{Q})$ must send roots of $a(x)$ to roots of $a(x)$. In particular, since α and β are roots of p and q, $\sigma(\alpha)$ and $\sigma(\beta)$ are roots of p and q as well. This completes the proof. $\square$

Proposition 2. *Let $\alpha \in \mathbb{A}$, let $r \in \mathbb{Q}$, let p be a polynomial with α as a root, and let q be the minimal (monic) polynomial for $r\alpha$, respectively. If b is a root of q, then there is a root a of p such that $b = ra$.*

Proof. We proceed as in the previous lemma. Let K be the splitting field for q. Since q is irreducible, there is a $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(r\alpha) = b$. Since σ is an automorphism fixing the base field $\mathbb{Q}$, we have $\sigma(r\alpha) = r\sigma(\alpha)$. But σ sends roots of p to roots of p, so $\sigma(\alpha)$ is a root of p, and $c = r\sigma(\alpha)$ as desired. $\square$

The following Corollary of the previous two propositions will be necessary in the proof of one of the main preliminary lemmas:

Corollary 3. *Let α, $\beta \in \mathbb{A}$. The conjugates of $\alpha + \beta$ are all of the form $\alpha' + \beta'$, where α' is a conjugate of α and β' is a conjugate of β. If $r \in \mathbb{Q}$, then the conjugates of $r\alpha$ are all of the form $r\alpha'$.*

Proof. Let p and q be the minimal polynomials of α and β, respectively. The result follows immediately from Propositions 1 and 2. $\square$

We will need another simple fact from the theory of polynomials, as follows.

Proposition 4. *The minimal polynomial of an algebraic integer lies in $\mathbb{Z}[x]$.*

Proof. Let α be an algebraic integer which is the root of a monic polynomial $p \in \mathbb{Z}[x]$. Let q be the minimal polynomial of α. Then q divides p, so there is a polynomial $s \in \mathbb{Z}[x]$ such that $p = q \cdot s$. Since p and q are monic, so is s. But now, from the theory of polynomial rings, there are polynomials Q and S in $\mathbb{Z}[x]$ which are integer multiples of q and s such that $p = Q \cdot S$. Since p is monic, the only way this can happen is if $q = Q$ and $s = S$. That is, q must have already been in $\mathbb{Z}[x]$, which completes the proof. □

We will also need one simple fact about complex roots of unity.

Proposition 5. *Let λ be a nth root of unity. Then all the conjugates of λ are also nth roots of unity.*

Proof. Suppose λ is an nth root of unity. Then λ is a root of the polynomial $z^n - 1$. The set of all polynomials in $\mathbb{Z}[x]$ for which $p(\lambda) = 0$ forms an ideal. But $\mathbb{Z}[x]$ is a principal ideal domain, so this ideal is principal, generated by the minimal polynomial of λ. In particular, this means that the minimal polynomial of λ divides $z^n - 1$. Hence every root of the minimal polynomial of λ is also a root of $z^n - 1$. Since all the roots of $z^n - 1$ are nth roots of unity, all the conjugates of λ are also nth roots of unity. □

There are two preliminary lemmas which will be needed in the proof of Burnside's Theorem. The first deals with a particular number constructed from a finite group G and one of its irreducible characters χ.

Lemma 6. *Let χ be an irreducible character of a finite group G, and let $g \in G$. Then*

$$\lambda = \frac{|G| \cdot \chi(g)}{|C_G(g)| \cdot \chi(1)}$$

is an algebraic integer.

Proof. Denote by $\overline{K}$ the sum of the elements of the conjugacy class K of g, and let U be an irreducible $\mathbb{C}G$-submodule of $\mathbb{C}G$ with character χ. First, we claim that $\overline{K}$ acts on U by multiplication by λ.

Since the map $U \to U$ defined by $u \mapsto \overline{K}u$ is a $\mathbb{C}G$-homomorphism (since $\overline{K} \in Z(\mathbb{C}G)$), Schur's Lemma asserts that $\overline{K}$ acts on U by multiplication by some $\alpha \in \mathbb{C}$; we aim to show that $\alpha = \lambda$. Let $\mathscr{B}$ be a basis of U. Since $\overline{K}$ acts by scalar multiplication, the matrix corresponding to the endomorphism $u \mapsto \overline{K}u$ is a scalar matrix. That is, $[\overline{K}]_{\mathscr{B}} = \alpha I$. But

$$\alpha I = [\overline{K}]_{\mathscr{B}} = \left[\sum_{k \in K} k\right]_{\mathscr{B}} = \sum_{k \in K} [k]_{\mathscr{B}}.$$

Taking the trace of both sides, we have

$$\alpha\chi(1) = \sum_{k \in K} \chi(k).$$

But K is a conjugacy class of G, and characters are constant on conjugacy classes, so

$$\alpha\chi(1) = \sum_{k\in K} \chi(k) = |K| \cdot \chi(g) = [G : C_G(g)] \cdot \chi(G).$$

Accordingly,

$$\alpha = \frac{[G : C_G(g)] \cdot \chi(G)}{\chi(1)} = \frac{|G| \cdot \chi(g)}{|C_G(g)| \cdot \chi(1)} = \lambda.$$

We now set out to show that λ is an algebraic integer. Consider the endomorphism of U defined by $u \mapsto \overline{K}u$. Now λ is an eigenvalue of this endomorphism since $\overline{K}u = \lambda u$ for any $u \in U$. Let us extend this endomorphism to an endomorphism of $\mathbb{C}G$ in the natural way, by $r \mapsto \overline{K}r$. With respect to the standard basis of $\mathbb{C}G$, this matrix is clearly integral, as it is a sum of permutation matrices since each element of k acts on G by a permutation. But λ is clearly also an eigenvalue of the endomorphism $r \mapsto \overline{K}r$, so λ must be an algebraic integer. □

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

Lemma 7. *Let χ be a character of a finite group G, and let $g \in G$. Then $|\chi(g)/\chi(1)| \leq 1$, and if $|\chi(g)/\chi(1)|$ is neither 0 nor 1 then then $\chi(g)/\chi(1)$ is not an algebraic integer.*

Proof. Since $\chi(g)$ is a sum of $n = \chi(1)$ roots of unity, we have

$$\left|\frac{\chi(g)}{\chi(1)}\right| = \left|\frac{\sum_{i=1}^n \lambda_i}{\chi(1)}\right| \leq \frac{1}{n}\sum_{i=1}^n |\lambda_i| = 1,$$

where each λ_i is a root of unity.

Let $\gamma = \chi(g)/n$, and suppose that γ is an algebraic integer with $|\gamma| < 1$. Let p be the minimal polynomial of γ, with constant term $p(0) = a_0$. By Proposition 4, $p \in \mathbb{Z}[x]$, so $a_0 \in \mathbb{Z}$. By Corollary 3 and Proposition 5, we know that the conjugates of γ are all of the form

$$\frac{\lambda_1' + \cdots + \lambda_n'}{n},$$

where λ_i' is a complex root of unity. In particular, by the triangle inequality, all the conjugates of γ have absolute value at most 1. Since γ itself has absolute value strictly less than 1, it therefore follows that the product of all the roots of p has absolute value strictly less than 1. But for any monic polynomial, the product of all the roots of that polynomial must be equal to either the constant term or the additive inverse of the constant term. Hence $|a_0| < 1$. As $a_0 \in \mathbb{Z}$, we have $a_0 = 0$. Therefore the constant polynomial x divides p, so since p is irreducible this necessitates $p(x) = x$. But γ is a root of p, so $p(\gamma) = 0$, $\gamma = 0$, and $\chi(g) = 0$. Thus γ is an algebraic integer iff $|\gamma| = 1$ or $\gamma = 0$, which completes the proof. □

After the following major theorem, Burnside's Theorem will follow easily.

Theorem 8. *If a finite group G has a conjugacy class of prime power order p^r $(r \geq 1)$, then G is not simple.*

Proof. Let $g \in G$ be an element of g whose conjugacy class has p^r elements. Clearly $g \neq 1$. Let $\chi_1, \ldots, \chi_k$ be the set of irreducible characters of G, with χ_1 the principal character.

From the column orthogonality relations, we obtain

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

so

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

Since $-1/p$ is not an algebraic integer, one of the numbers $\chi_i(g)\chi_i(1)/p$ is not an algebraic integer. As 0 is an algebraic integer, $\chi_i(g)$ must be nonzero. Since $\chi_i(g)$ is an algebraic integer, it must follow that $\chi_i(1)/p$ is not an algebraic integer. Since $\chi_i(1)$ is an ordinary integer, this means that $\chi_i(1)/p \in \mathbb{Z} - \mathbb{Q}$, and therefore that $p \nmid \chi_i(1)$. Hence p and $\chi_i(1)$ are relatively prime, so p^r and $\chi_i(1)$ are relatively prime as well. As $[G : C_G(g)] = p^r$, this means that there exist integers a and b for which the equality

$$a[G : C_G(g)] + b\chi_i(1) = 1$$

holds. Multiplying through by $\chi(g)/\chi(1)$, we have that

$$a\frac{|G| \cdot \chi_i(g)}{|C_G(g)| \cdot \chi_i(1)} + b\chi_i(g) = \frac{\chi_i(g)}{\chi_i(1)}.$$

By Lemma 6, the left hand side of this equation is an algebraic integer since $\chi_i(g)$ is an algebraic integer. But the right hand side of this equation is nonzero since $\chi_i(g) \neq 0$, so, by Lemma 7, we have $|\chi_i(g)/\chi_i(1)| = 1$. Hence $|\chi_i(g)| = |\chi_i(1)| = \chi_i(1)$, and g acts as a scalar multiple of the identity under the corresponding representation ρ.

Since χ_i is not the principal character, $\ker \chi_i \neq G$. Moreover, if $\ker \chi_i$ is not trivial, then this implies that $\ker \chi_i$ is a proper normal subgroup of G, and we are done. Therefore we may assume that $\ker \chi_i$ is trivial, so that the associated representation ρ is faithful. But g is a scalar multiple of the identity, so $\rho(g)$ is a scalar matrix, and $\rho(g)$ commutes with $\rho(h)$ for every $h \in G$. Now ρ is faithful, hence an isomorphism between G and $\operatorname{Im} \rho$, so $g \in Z(G)$, and the center of G is nontrivial. As $Z(G) \trianglelefteq G$ and G is nonabelian (since it has a nontrivial conjugacy class), it must be the case that $Z(G)$ is a proper normal subgroup of G, and that G is not simple. $\square$

Theorem 9 (Burnside)**.** *If G is a group of order $p^a q^b$, where p and q are distinct primes and a and b are nonnegative integers with $a + b \geq 2$, then G is not simple.*

Proof. If b is zero, then G is a p-group, and so has nontrivial center. By Cauchy's Theorem, there is a $g \in Z(G)$ of order p. The subgroup $\langle g \rangle$ is normal and of order $p < |G|$. The case $a = 0$ is identical.

Now suppose both a and b are positive. Let Q be a Sylow q-subgroup of G, and let g be a nonidentity element of the (nontrivial) center $Z(Q)$. Since $g \in Z(Q)$, for every $q \in Q$ we have $qgq^{-1} = g$, so $Q \leq C_G(g)$. Therefore the size of the conjugacy class of g is

$$[G : C_G(g)] \leq [G : Q] = p^a,$$

and since the size of the conjugacy class of g divides $[G : Q]$, we have $[G : C_G(g)] = p^r$ for some r. Now if r is zero then $g \in Z(G)$, so $Z(G)$ must have either an element of order p or an element of order q, and the cyclic group generated by that element is a normal subgroup of G. But if r is greater than zero then G has a conjugacy class of order p^r with $r > 0$, and so Theorem 8 asserts that G is not simple. □

As a corollary of Burnside's Theorem, we have the following:

Corollary 10. *Any group G of order $p^a q^b$ is solvable.*

Proof. We proceed by induction on $a + b$. If $a + b \leq 1$ then G is cyclic of prime order, hence abelian, and therefore solvable since its commutator subgroup is trivial. Now if G is of order $p^a q^b$ then, by Burnside's Theorem 9, there is a normal subgroup H of G. By the inductive hypothesis, both H and G/H are solvable since they are groups of order of the form $p^{a'} q^{b'}$ where $a' + b' < a + b$, so there are abelian normal towers

$$H = A_0 \geq A_1 \geq \cdots \geq A_s = \{1\}$$

and

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

By the Lattice Isomorphism Theorem the B_i correspond to subgroups C_i of G containing H such that $C_i/H = B_i$ 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 the Second Isomorphism Theorem asserts that $C_i/C_{i+1} \cong (C_i/H)/(C_{i+1}/H) \cong B_i/B_{i+1}$ for each i, so each quotient C_i/C_{i+1} is abelian. Finally, $B_t = \{1\}$ corresponds to $C_t = H$, so we have that $C_t/A_0 = \{1\}$ is abelian. Therefore

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

is an abelian normal tower for G, and G is solvable. □