A SIMPLE PROOF OF BURNSIDE'S CRITERION FOR ALL GROUPS OF ORDER n TO BE CYCLIC

SIDDHI PATHAK

ABSTRACT. This note gives a simple proof of a famous theorem of Burnside, namely, all groups of order n are cyclic if and only if $(n, \phi(n)) = 1$, where ϕ denotes the Euler totient function.

1. Introduction

The question of determining the number of isomorphism classes of groups of order n has long been of interest to mathematicians. One can ask a more basic question: For what natural numbers n, is there only one isomorphism class of groups of order n? Since we know that there exists a cyclic group of every order, this question reduces to finding natural numbers n such that all groups of order n are cyclic. The answer is given in the following well-known theorem by Burnside [1]. Let ϕ denote the Euler function.

Theorem 1.1. *All groups of order n are cyclic if and only if* $(n, \phi(n)) = 1$.

Many different proofs of this fact are available. Practically all of them are inaccessible to the undergraduate student since they use Burnside's transfer theorem and representation theory [2]. Here, we would like to give another proof of this theorem which is elementary and uses only basic Sylow theory. Throughout this note, n denotes a positive integer and C_n denotes the cyclic group of order n.

2. Groups of order pq

Let p and q be two distinct primes, $p < q$. In this section, we investigate the structure of groups of order pq. The two cases to be considered are when $p \mid q-1$ and $p \nmid q-1$.

First, let us suppose that $p \nmid q-1$. In this case, every group of order pq is cyclic. Indeed, let G be a group of order pq. Let n_p be the number of p-Sylow subgroups and n_q be the number of q-Sylow subgroups of G. Then, according to Sylow's theorem,

$$n_q \equiv 1 \bmod q \text{ and } n_q \mid p.$$

Since $p < q$, $n_q = 1$. Thus, the q-Sylow subgroup, say Q, is normal in G. Again by Sylow's theorem,

$$n_p \equiv 1 \bmod p \text{ and } n_p \mid q.$$

Since q is prime, either $n_p = 1$ or $n_p = q$. But $p \nmid q-1$. Hence, $n_p = 1$. Thus, the p-Sylow subgroup, say P, is also normal in G. Also, since the order of non-identity elements of P and Q are co-prime, $P \cap Q = \{e\}$. Thus, if $a \in P$ and $b \in Q$,

2010 *Mathematics Subject Classification.* 20D60, 20E99.
Key words and phrases. Number of groups of a given order, cyclic groups, Sylow theory.

then consider the element $c := aba^{-1}b^{-1} \in G$. The normality of Q implies that $aba^{-1} \in Q$ and hence, $c \in Q$. On the other hand, the normality of P implies that $ba^{-1}b^{-1} \in P$ and hence, $c \in P$. Thus, $c \in P \cap Q = \{e\}$. Therefore, the elements of P and Q commute with each other. This gives us a group homomorphism,

$$\Psi : P \times Q \to G,$$

such that $\Psi(a,b) = ab$. Since, $P \cap Q = \{e\}$, Ψ is injective. $|P \times Q| = |G|$ implies that Ψ is also surjective and hence, an isomorphism. As P and Q are cyclic groups of distinct prime order, $P \times Q$ is cyclic and so is G. Therefore, if $p \nmid q-1$, then all groups of order pq are cyclic.

Now, suppose $p \mid q-1$. We claim that in this case, there exists a group of order pq which is not cyclic.

Note that since $p \mid q-1$, there exists an element in $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ of order p, say α_p. To see this, note that

$$\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^* \simeq C_{q-1},$$

and a cyclic group of order n contains an element of order d, for every divisor d of n. Thus, we get a group homomorphism, say θ, from C_p to $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ by sending a generator of C_p to α_p. Denote $\theta(u)$ by θ_u. Clearly, θ is a non-trivial map. We define the semi-direct product, $C_p \ltimes_\theta C_q$ as follows:

As a set, $C_p \ltimes_\theta C_q := \{(u,v) : u \in C_p \text{ and } v \in C_q\}$. The group operation on this set is defined as

$$(u,v).(u',v') = (uu', \theta_u(v)v'). \tag{1}$$

One can check that this operation is indeed associative and makes $C_p \ltimes_\theta C_q$ into a group. To see that this group is non-abelian, consider (u,v) and (u',v') in $C_p \ltimes_\theta C_q$. Thus,

$$(u',v').(u,v) = (u'u, \theta_{u'}(v')v),$$

which is not equal to $(u,v).(u',v')$ as evaluated in (1) since θ is non-trivial. Thus, if $p \mid q-1$, then there exists a group of order pq which is not abelian, in particular, not cyclic.

Remark. *In fact, given any group G of order pq, one can show that it is either cyclic or isomorphic to the semi-direct product constructed above. Thus, if $p \mid q-1$, there are exactly two isomorphism classes of groups of order pq.*

3. Proof of the *only if* part

Suppose all groups of order n are cyclic, i.e, there is only one isomorphism class of groups of order n. Since $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ are 2 non-isomorphic groups of order p^2, we see that n is squarefree.

Proof. Let us note that if $n = \prod_{i=1}^k p_i$ where, $p_1, \ldots, p_k$ are distinct primes and $p_1 < \cdots < p_k$, then $(n, \phi(n)) = 1 \iff p_i \nmid (p_j - 1)$, for all $1 \le i < j \le k$.

Now, suppose n is squarefree and $(n, \phi(n)) > 1$, i.e, there exists a p_i such that $p_i \mid (p_j - 1)$ for some $1 \le i < j \le k$. As seen in the earlier section, there exists a group, $\mathcal{G}$ of order $p_i p_j$ that is not cyclic. Thus, $\mathcal{G} \times C_{n/p_ip_j}$ is a group of order n and is not cyclic. This contradicts our assumption that all groups of order n are cyclic. Hence, n and $\phi(n)$ must be coprime. $\square$

4. **Proof of the *if* part**

The condition that $(n, \phi(n)) = 1$ helps us to infer that it is enough to consider only those n that are squarefree.

Our proof hinges upon the following crucial lemma.

Lemma 4.1. *Let G be a finite group such that every proper subgroup of G is abelian. Then either G has prime order, or G has a non-trivial, proper, normal subgroup i.e, G is not simple.*

Proof. Let G be a group of order n. By a maximal subgroup of G, we will mean a nontrivial proper subgroup H of G such that, for any subgroup H' of G that contains H, either $H' = G$ or $H' = H$ itself.

Let M denote a maximal subgroup of G. Let $|M| = m$. Suppose $M = \{e\}$,i.e, G contains no nontrivial proper subgroup. Sylow's first theorem thus implies that the order of G must be prime.

Suppose n is not prime. Hence, $m \geq 2$. Let $N_G(M)$ denote the normalizer of M in G. Recall that

$$N_G(M) = \{g \in G : gMg^{-1} = M\}.$$

If M is normal in G, then clearly G is not simple. Therefore, let us suppose that M is not normal. Hence, $N_G(M) \neq G$. Since $M \subseteq N_G(M)$ and M is maximal, $N_G(M) = M$. Let the number of conjugates of M in G be r, $r > 1$. The number of conjugates of a subgroup in a group is equal to the index of its normalizer. Therefore,

$$\begin{aligned} r &= [G : N_G(M)] \\ &= [G : M] \\ &= \frac{n}{m}. \end{aligned}$$

Let $\{M_1, \cdots, M_r\}$ be the set of distinct conjugates of M. Suppose $M_i \cap M_j \neq \{e\}$ for some $1 \leq i < j \leq r$. Let $K_1 := M_i \cap M_j$. Since M_i and M_j are abelian by hypothesis,

$$K_1 \triangleleft M_i \quad , K_1 \triangleleft M_j. \tag{2}$$

Therefore K_1 is normal in the group generated by M_i and M_j. Since conjugates of maximal subgroups are themselves maximal, the group generated by M_i and M_j is G. Thus, K_1 is normal in G and hence G is not simple.

Therefore, we suppose that all the conjugates of M intersect trivially. Let $V := \cup_{i=1}^{r} M_i$. Then,

$$\begin{aligned} |V| &= r(m-1) + 1 \\ &= n - \left[\frac{n}{m} - 1\right] < n. \end{aligned}$$

Thus, $\exists\ y \in G$, $y \notin V$.

If G is a cyclic group generated by y (of composite order), then the subgroup of G generated by y^k for any $k|n$, $k \neq 1, n$ is a non-trivial normal subgroup. So we can assume that the group generated by y is a proper subgroup of G. Let L be a maximal subgroup containing the subgroup of G generated by y. Since, $y \notin V, L \neq M_i\ \forall\ 1 \leq i \leq r$. If L is normal in G, then G is clearly not simple. Therefore, suppose that L is not normal in G.

Let the number of conjugates of L in G be s, $s > 1$. Let $\{L_1, \cdots, L_s\}$ be the set of distinct conjugates of L in G. If any two distinct conjugates of L or a conjugate of L and a conjugate of M intersect non-trivially, then the corresponding intersection is a normal subgroup of G by an argument similar to the one given above. Thus, G is not simple. Hence, it suffices to assume that

$$M_i \cap M_j = \{e\}, \tag{3}$$

$$M_i \cap L_q = \{e\}, \tag{4}$$

$$L_p \cap L_q = \{e\}, \tag{5}$$

for all $1 \leq i < j \leq r$, for all $1 \leq p < q \leq s$.

Let $|L| = l$, $l \geq 2$. Since L is not normal in G but is maximal, $N_G(L) = L$. Thus, the number of conjugates of L in G is

$$\begin{aligned} s &= [G : N_G(L)] \\ &= [G : L] \\ &= \frac{n}{l}. \end{aligned}$$

Let $W := \cup_{p=1}^{s} L_p$. By (3), (4) and (5),

$$\begin{aligned} |V \cup W| &= r(m-1) + s(l-1) + 1 \\ &= n - \frac{n}{m} + n - \frac{n}{l} + 1 \\ &= 2n - n(\frac{1}{m} + \frac{1}{l}) + 1 \\ &\geq 2n - n + 1 \\ &> n, \end{aligned}$$

since $m, l \geq 2$. But $V \cup W \subseteq G$. Therefore, $|V \cup W| \leq n$. This is a contradiction. Hence, G must have a nontrivial proper normal subgroup. □

We will now prove that if $(n, \phi(n)) = 1$, then all groups of order n are cyclic. As seen earlier, we are reduced to the case when n is squarefree.

Proof. We will proceed by induction on the number of prime factors of n. For the base case, assume that n is prime. Lagrange's theorem implies that any group of prime order is cyclic. Thus, the base case of our induction is true.

Now suppose that the result holds for all n with at most $k-1$ distinct prime factors, for some $k > 1$. Let $n = p_1 \cdots p_k$ for distinct primes $p_1, \cdots, p_k$ and $p_1 < p_2 < ... < p_k$. Since $k \geq 2$, Sylow's first theorem implies that G has nontrivial proper subgroups. Let P be a proper subgroup of G. Hence, $|P|$ has fewer prime factors than k. Therefore, by induction hypothesis, P is cyclic and hence abelian. Thus, every proper subgroup of G is abelian. By Lemma 4.1, G has a nontrivial proper normal subgroup, say N. The induction hypothesis implies that G/N is cyclic. Therefore, G/N has a subgroup of index p_i for some $1 \leq i \leq k$. Let this subgroup be denoted by $\mathfrak{H}$. By the correspondence theorem of groups, all subgroups of G/N correspond to subgroups of G containing N. Let the subgroup of G corresponding to $\mathfrak{H}$ via the above correspondence be H, i.e, $\mathfrak{H} = H/N$. Since G/N is abelian, $\mathfrak{H} \triangleleft G/N$ and hence, $H \triangleleft G$. By the third isomorphism theorem of groups,

$$G/N \Big/ H/N \simeq G/H.$$

Since, $[G/N : \mathfrak{H}] = p_i$, $[G : H] = p_i$. Thus, G has a normal subgroup of index p_i, namely, H. Note that H is cyclic. In particular,

$$H \simeq C_a, \tag{6}$$

where $a = p_1 \cdots p_{i-1} p_{i+1} \cdots p_k$. Let K be a p_i- Sylow subgroup of G. Thus,

$$K \simeq C_{p_i}. \tag{7}$$

Consider the map $\Phi : K \to \mathrm{Aut}(H)$ that sends an element $k \in K$ to the automorphism γ_k where, γ_k is conjugation by k. Since $H \triangleleft G$, γ_k is a well-defined map from H to H. Therefore, Φ is a well-defined group homomorphism. Since, $ker(\Phi)$ is a subgroup of K and K has prime order, either $ker(\Phi) = \{e\}$ or $ker(\Phi) = K$. Suppose, $ker(\Phi) = \{e\}$. Then, $\Phi(K)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. By the induction hypothesis, H is isomorphic to the cyclic group of order $|H| = p_1 \cdots p_{i-1} p_{i+1} \cdots p_k$. Thus,

$$H \simeq \prod_{j=1, j \neq i}^{k} \mathbb{Z}/p_j\mathbb{Z}.$$

For any prime p,

$$\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^*.$$

Therefore,

$$\mathrm{Aut}(H) \simeq \prod_{j=1, j \neq i}^{k} (\mathbb{Z}/p_j\mathbb{Z})^*.$$

Hence,

$$|\mathrm{Aut}(H)| = \prod_{j=1, j \neq i}^{k} (p_j - 1).$$

Thus, by Lagrange's theorem, $|K|$ divides $|\mathrm{Aut}(H)|$, i.e,

$$p_i \Bigg| \prod_{j=1, j \neq i}^{k} (p_j - 1).$$

Since $(n, \phi(n)) = 1$, we see that $p_i \nmid (p_j - 1)$ for any $1 \leq i, j \leq k$. We thus arrive at a contradiction. Hence, $ker(\Phi) = K$. Let $k \in ker(\Phi)$ i.e, γ_k is the identity homomorphism. Since $ker(\Phi) = K$, $kh = hk$ for all $h \in H$ and for all $k \in K$. We now claim that $G \simeq H \times K$. To prove this claim, consider the map $\Psi : H \times K \to G$ sending a tuple (h, k) to the product hk. Since the elements of H and K commute with each other, Ψ is a group homomorphism. H has no element of order p_i. Thus, $H \cap K = \{e\}$. This implies that Ψ is injective and hence surjective as $|H \times K| = |G|$. Thus Ψ is the desired isomorphism. By (6) and (7),

$$G \simeq C_n.$$

Thus, every group of order n is cyclic. □

Acknowledgement

The above proof was a result of a long discussion with Prof. M. Ram Murty. I would like to thank him profusely for his guidance and help in writing the note. I would also like to thank the referee for useful comments on an earlier version of this note.

References

[1] J. Dixon, *Problems in Group Theory*, Dover Books, 1973, pg. **92**, **2.55**.
[2] W. R. Scott, *Group Theory*, Prentice Hall, 1964, pg. **217**.

(Siddhi Pathak) Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada, K7L3N6.
E-mail address, Siddhi Pathak: siddhi@mast.queensu.ca