A Combinatorial Proof of a generalization of a Theorem of Frobenius

Supravat Sarkar

Abstract
In this article, we shall generalize a theorem due to Frobenius in group theory, which asserts that if \( p \) is a prime and \( p^r \) divides the order of a finite group, then the number of subgroups of order \( p^r \) is \( \equiv 1 \pmod{p} \). Interestingly, our proof is purely combinatorial and does not use much group theory.

Keywords: Group, subgroup, prime, count.

MSC number: 20D15

1. Introduction
Although Sylow’s theorems are taught in almost all undergraduate courses in abstract algebra, a generalization due to Frobenius does not seem to be as well known as it ought to be. Frobenius’ generalization states that if \( p \) is a prime and \( p^r \) divides the order \( N \) of a finite group \( G \), the number of subgroups of \( G \) of order \( p^r \) is \( \equiv 1 \pmod{p} \). The special case when \( p^r \) is the largest power of \( p \) dividing \( N \) is part of Sylow’s third theorem. Many of the standard texts do not mention this theorem. One source is Ian Macdonald’s ‘Theory of Groups’ [1]. In fact, a further generalization due to Snapper [2] asserts that for any subgroup \( K \) of order \( p^r \) and for any \( s \geq r \) where \( p^s \) divides the order of \( G \), the number of subgroups of order \( p^s \) containing \( K \) is also \( \equiv 1 \pmod{p} \). In this article, we give a new proof of a further extension of Snapper’s result that is purely combinatorial and does not use much group theory. Thus, we have a new combinatorial proof of Frobenius’s theorem as well.

2. Main results

We initially started by giving a combinatorial proof of Frobenius’s result and, interestingly, our method of proof yields as a corollary an extension of Snapper’s Theorem. Our proof builds on the famous combinatorial proof of Cauchy’s theorem which asserts that if a prime divides the order of a group, there is an element of that prime order.
Theorem 1 Let $G$ be a finite group of order $N$, and let $p$ be a prime. Let $b_0 < b_1 < \cdots < b_r$ be nonnegative integers such that $p^{b_i}$ divides $N$ and $P_{b_i}$ be a subgroup of $G$ of order $p^{b_i}$. Then the number of ordered tuples $(P_{b_1}, P_{b_2}, \ldots, P_{b_r})$ such that each $P_{b_i}$ is subgroup of $G$ of order $p^{b_i}$ and

$$P_{b_0} \subset P_{b_1} \subset \cdots \subset P_{b_r}$$

is $1 \pmod{p}$.

The case $r = 1$ is a Theorem due to Snapper [2] which is itself an extension of Frobenius’s Theorem that corresponds to the case $r = 1, b_0 = 0$ in our Theorem. Let us recall here the simple results in finite group theory that we will need.

1. If $H$ is a subgroup of a finite group $G$ of order $N$, and the index $[G : H]$ is the smallest prime divisor of $N$, then $H$ is normal in $G$.
2. (Sylow’s first theorem) If $G$ is a finite group of order $N$, $p$ a prime, $i \geq 0$ is an integer, $p^{i+1}|N$ and $P$ is a subgroup of $G$ of order $p^i$, then there is a subgroup $Q$ of $G$ containing $P$ of order $p^{i+1}$.

We shall also use the following notations throughout.

1. For a finite set $S$, $|S|$ denotes the number of elements (cardinality) of $S$.
2. If $G, H$ are finite groups, $H \leq G$ means $H$ is a subgroup of $G$.
3. If $G, H$ are finite groups, $H \leq G$, $[G : H]$ denotes the index of $H$ in $G$.
4. If $G$ is a finite group, the order of $G$ is the number of elements of $G$.
5. If $H$ is a subgroup of a group $G$, $N_G(H)$ denotes the normalizer of $H$ in $G$.
6. For positive integers $a, b$, we write $a|b$ to mean $a$ divides $b$.

Proof of Theorem.

For ease of understanding, we divide the proof into three steps.

Step 1: We tackle the case $r = 1, b_0 = 0, b_1 = 1$ first, which just says that if $p$ divides the order of $G$, then the number of subgroups of $G$ of order $p$ is $1 \pmod{p}$.

Let $T = \{(a_1, a_2, ..., a_p) | a_i \in G \forall i, a_1a_2...a_p = 1\}$.

Observe that $|T| = N^{p-1} \equiv 0 \pmod{p}$, as any choice of $a_1, ..., a_{p-1}$ uniquely determines $a_p$. Also, if not all $a_i$’s are equal, then $(a_1, a_2, ..., a_p) \in T$ implies $(a_i, a_{i+1}, ..., a_{i+p-1})$ for $i = 1, 2, ..., p$ (indices are modulo $p$) are $p$ distinct elements of $T$. The reason is as follows:

If $(a_i, a_{i+1}, ..., a_{i+p-1}) = (a_j, a_{j+1}, ..., a_{j+p-1})$ for some $i \neq j$, then $a_k = a_{k+j-i} \forall k$.

By induction, $a_k = a_{k+\alpha(j-i)}$ for any integer $\alpha$. But $i \neq j$ implies $gcd(j-i, p) =$
1, as $0 < |i - j| < p$ and $p$ is a prime. So, $j - i$ is invertible modulo $p$. So any $1 \leq l \leq p$ satisfies $l \equiv 1 + \alpha(j - i) \pmod{p}$ for some integer $\alpha$. So, $a_l = a_{1 + \alpha(j - i)} = a_1$ for any $1 \leq l \leq p$. So, $a_l$'s are all equal, which leads to a contradiction.

So, if $d$ is the number of elements of $G$ of order $p$, then $0 \equiv |T| \equiv (1 + d) \pmod{p}$. So, $d \equiv -1 \pmod{p}$ (as there are exactly $1 + d$ elements of $T$ with all $a_l$'s equal.) In each subgroup of order $p$, there are $p - 1$ elements of order $p$, different subgroups of order $p$ intersect at the identity. So,

$$-1 \equiv d = (p - 1)(\text{number of subgroups of order } p) \equiv -(\text{number of subgroups of order } p) \pmod{p}.$$ 

So, number of subgroups of order $p$ is $\equiv 1 \pmod{p}$, which finishes the proof for the case $r = 1, b_0 = 0, b_1 = 1$.

**Step 2:** Now come to a general case. First, we fix a notation. Let $H$ be any group of order $M$, $p^n|M, p^{n+1} \nmid M$, $0 \leq r \leq n$. Let $P_r$ be a subgroup of order $p^r$ in $H$. Define

$$S(P_r, H) = \{(P_{r+1}, P_{r+2}, \ldots, P_n)| P_i \leq H, |P_i| = p^i \forall i, P_r \leq P_{r+1} \leq \cdots \leq P_n \leq H\}.$$ 

So, $S(P_r, H)$ is a singleton set, by convention.

For $r \leq i < n$ and a subgroup $P_i$ of $H$ of order $p^i$, there is a subgroup $P_i^{r+1}$ of $H$ of order $p^{i+r}$ containing $P_i$, by Sylow’s theorems. $|P_i^{r+1} : P_i| = p$, which is the smallest prime divisor of $|P_i^{r+1}|$, so $P_i$ is normal in $P_i^{r+1}$. Hence $P_i^{r+1} \leq N_G(P_i)$. So, $P_i^{r+1}$ is a subgroup of order $p$ in $N_G(P_i)$. By the same reasoning, any subgroup $P_{i+1}$ of $H$ of order $p^{i+1}$ containing $P_i$ must be a subgroup of $N_G(P_i)$, and so $P_{i+1}$ is a subgroup of order $p$ in $N_G(P_i)$. Conversely, any subgroup of order $p$ in $N_G(P_i)$ gives rise via pullback to a subgroup $P_{i+1}$ of $N_G(P_i)$ (hence of $H$) of order $p^{i+1}$ containing $P_i$. So, there is a one-to-one correspondence between such $P_{i+1}$ (subgroups of $G$ of order $p^{i+1}$ containing $P_i$) and the subgroups of order $p$ of the quotient group $\frac{N_G(P_i)}{P_i}$.

So, the number of such $P_{i+1}$ is the number of subgroups of order $p$ in $\frac{N_G(P_i)}{P_i}$, which is $\equiv 1 \pmod{p}$, in view of Step 1. So, in mod $p$, we can choose $P_{r+1}$ in 1 way, after each such choice we can choose $P_{r+2}$ in 1 way, and so on. So, $|S(P_r, H)| \equiv 1 \pmod{p}$.

**Step 3:** Now come to the setup of our theorem. We have $|S(P_b, G)| \equiv 1 \pmod{p}$, by Step 2. Let us count $|S(P_b, G)|$ in another way. Let $x$ be the number of ordered tuples as in the statement of our theorem. After choosing any of such $x$ ordered tuples, we can choose $(P_{b_i+1}, \ldots, P_{b_i+1})$ in $|S(P_{b_i}, P_{b_i+1})| \equiv 1 \pmod{p}$ ways, for each $0 \leq i \leq r - 1$, and we can choose $(P_{b_i+1}, \ldots, P_n)$ in $|S(P_{b_i}, G)| \equiv 1 \pmod{p}$ ways.

Now, $p^n$ is the largest power of $p$ dividing $N$, each $P_i$ is a subgroup of $G$ of order $p^i$ and $P_r \leq P_{r+1}$ for all $b_0 \leq i < n$. So, we obtain $|S(P_b, G)| \equiv x \pmod{p}$. Hence finally we get $x \equiv 1 \pmod{p}$ which completes the proof.
Remarks
The case \( r = 1 \) is Snapper’s result and the further special case \( r = 1, b_0 = 0 \) corresponds to Frobenius’ theorem.

References

[1] Macdonald, Ian. Theory of Groups, Oxford University Press, 1968.

[2] Snapper, Ernst. Counting \( p \)-subgroups, Proc. Amer. Math. Society, Vol. 39 (1973), pp.81-82.