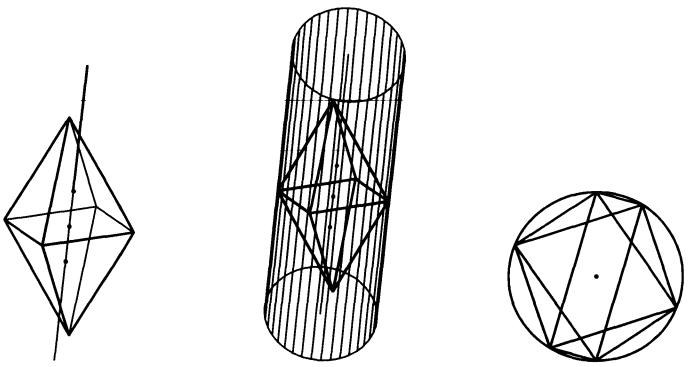
$(0, \pm 2/7, 0)$, and $(0, 0, \pm 1/4)$, and the outer 2-radius $R_2(K^0)$ is $2/\sqrt{69}$. FIGURE 7 shows this octahedron and the smallest cylinder that contains it.



(a) The polar dual (b) Smallest cylinder (c) Axial view

Figure 7 The octahedron in the smallest cylinder

REFERENCES

1. René Brandenberg, Radii of regular polytopes, *Discrete Comput. Geom.*, to appear.
2. H. S. M. Coxeter and S. L. Greitzer, *Geometry Revisited*, New Mathematics Library 19, Random House and L. W. Singer, 1967.
3. H. G. Eggleston, *Convexity*, Cambridge Univ. Press, 1958.
4. H. Everett, I. Stojmenović, P. Valtr, and S. Whitesides, The largest k-ball in a d-dimensional box, *Comput. Geom.* **11** (1998), 59–67.
5. A. M. Gleason, R. E. Greenwood, and L. M. Kelly, *The William Lowell Putnam Mathematical Competition Problems and Solutions: 1938–1964,* Mathematical Association of America, 1980.
6. P. Gritzmann and V. Klee, Inner and outer j-radii of convex bodies in finite-dimensional normed spaces, *Discrete Comput. Geom.* **7** (1992), 255–280.
7. R. P. Jerrard, J. Schneider, R. Smallberg, and J. E. Wetzel, Straw in a box, preprint.
8. K. A. Post, Triangle in a triangle: On a problem of Steinhaus, *Geom. Dedicata* **45** (1993), 115–20.
9. G. W. Mackey, The William Lowell Putnam Mathematical Competition, *Amer. Math. Monthly* **55** (1948), 630–633.
10. D. O. Shklarsky, N. N. Chentzov, I. M. Yaglom, *Geometric Inequalities and Problems on Maxima and Minima* (in Russian), Nauka, Moscow, 1970.

A Theorem of Frobenius and Its Applications

DINESH KHURANA
Panjab University
Chandigarh-160014, India
dkhurana@pu.ac.in

ANJANA KHURANA
Punjabi University
Patiala (Punjab), India
an14in@yahoo.com

In any finite cyclic group, there are exactly d elements x satisfying $x^d = 1$ for each divisor d of its order. Consequently, in any finite abelian group, the number of solutions of $x^d = 1$ is a multiple of d, since we can write the group as a direct sum of cyclic

groups. Remarkably, this result turns out to be true for *any* finite group. This is a fundamental theorem proved by Frobenius [**9**] more than hundred years ago, in 1895:

> *If d is a divisor of the order of a finite group G, then the number of solutions of $x^d = 1$ in G is a multiple of d.*

This result (which we call *the Frobenius theorem*) has stimulated widespread interest in counting solutions of equations in groups; details can be found in Finkelstein [**8**]. Many proofs and generalizations of the result are known [**1**; **2**, p. 49; **3**, p. 92; **11**; **12**, p. 136; **18**, p. 77]. A standard proof (Frobenius's original one) is a consequence of the character theory of finite groups (see, for instance, Serre [**20**, Corollary 2, p. 83]), but now many elementary proofs are known. In spite of its fundamental nature, Frobenius's theorem, unlike the Sylow theorems, has not found its well-deserved place in undergraduate texts in algebra. In fact, even most of the recent graduate texts in group theory do not include the Frobenius theorem.

We present our own proof of the Frobenius theorem and some of its applications in a way that uses only elementary knowledge of group theory. For this purpose, we refer the reader to Herstein's book [**13**]. In the last section, we also discuss some applications of Frobenius's theorem to number theory.

Comparison with Sylow theory To show how useful the theorem may be, let us recall some standard results normally proved using the Sylow theorems in most undergraduate texts in algebra.

It is well known that every group of prime order is cyclic. Are there other natural numbers n such that, if G is a group of order n, then G is cyclic? Here is a typical approach using Sylow theory: Let $n = pq$, where $p < q$ are primes. The number of Sylow q-subgroups is $1 + kq$, for some k such that $1 + kq$ divides p. As $q > p$, $k = 0$ and so there is a unique subgroup of order q and which, therefore, is normal. If $p \nmid q - 1$, the subgroup of order p is also normal and G, being their direct sum, is cyclic. The Frobenius theorem gives a stronger result, allowing us to characterize all such values of n. These turn out to be precisely those n for which n and $\phi(n)$ are relatively prime (where $\phi(n)$ is the number of positive integers less than n that are relatively prime to n).

A group G is called *simple* if its only normal subgroups are G and $\{1\}$. For instance, abelian simple groups are just the cyclic groups of prime order. A group is said to be *solvable* if it contains a sequence of normal subgroups $\{1\} = N_0 \lhd N_1 \lhd \cdots \lhd G$ such that each quotient N_{j+1}/N_j is abelian. In particular, a solvable nonabelian group is not simple.

As noted above, in a group G of order pq, where $p < q$ are primes, the Sylow q-subgroup is normal and thus G is not simple. With a little more effort the Sylow theory shows that the Sylow r-subgroup is normal in a group of order pqr, where $p < q < r$ are primes. But Sylow theorems do not work for this purpose if the order of the group is a product of more than three distinct primes. Using the Frobenius theorem, it can be easily proved that if every Sylow p-subgroup of G is cyclic (for instance, if the order of the group is squarefree) and q is the largest prime divisor of the order of group, then the Sylow q-subgroup is normal and thus G is not simple. Burnside [**2**, p. 503] remarked, "... simple (nonabelian) groups of odd order do not exist." His claim was proved in 1963 by Feit and Thompson [**7**] when they showed that every group of odd order is solvable. Indeed, if G is a nonabelian group of odd order, then the commutator subgroup G' is a proper normal subgroup showing that G is not simple.

Using the Frobenius theorem, one can easily prove that a group, all of whose Sylow subgroups are cyclic, is solvable.

The Frobenius Theorem Throughout, G denotes a finite group and $o(g)$ the order of $g \in G$. By $|S|$, we mean the number of elements in a finite set S. By $H \leq G$ (resp. $H \trianglelefteq G$) we mean that H is a subgroup (normal subgroup) of G. If d divides $|G|$, then

$$A_d = \{x \in G : x^d = 1\}.$$

If $S \subseteq G$, then $\langle S \rangle$ will denote the subgroup of G generated by S. We denote the greatest common divisor and least common multiple of m and n by $\gcd(m, n)$ and $\operatorname{lcm}(m, n)$, respectively. For an element $a \in G$, $N(a) = \{g \in G : ag = ga\}$ is the *centralizer* of a and $C(a) = \{gag^{-1} : g \in G\}$ is the conjugacy class of a. We begin with the following lemma, which we shall use repeatedly in the paper.

LEMMA. *For any n, the number of elements of order n in G is either 0 or a nonzero multiple of $\phi(n)$. Furthermore, if a divisor of $|G|$ has the form $d = p^\alpha s$, where $p^{\alpha+1}$ divides $|G|$ and $\gcd(p, s) = 1$, then the set $A = A_{dp} \backslash A_d$ is either empty or has cardinality a multiple of $\phi(p^{\alpha+1})$.*

Proof. We define a relation on the elements of G as follows: x is related to y if and only if they generate the same subgroup, that is, $\langle x \rangle = \langle y \rangle$. Clearly this is an equivalence relation. As $o(x) = o(x^t)$ if and only if $\gcd(t, o(x)) = 1$, the equivalence class of x has $\phi(o(x))$ elements. Writing G as a disjoint union of its equivalence classes, it follows that the set of elements of a given order n is a union of equivalence classes and, thus, its cardinality is a multiple of $\phi(n)$.

To prove the second statement, we note that the set A can also be written as $\{x : o(x) = p^{\alpha+1}s_1,\ s_1 \mid s\}$. If $A \neq \emptyset$, then it is a union of equivalence classes and the equivalence class of any element x with $o(x) = p^{\alpha+1}s_1$ has cardinality a multiple of $\phi(p^{\alpha+1})$, since $\phi(p^{\alpha+1}s_1) = \phi(p^{\alpha+1})\phi(s_1)$. It follows that $|A|$ has cardinality a multiple of $\phi(p^{\alpha+1})$. ∎

We recall one well-known fact before proving the Frobenius theorem. This is:

If $x \in G$ has $o(x) = mn$, where $\gcd(m, n) = 1$, then $x = yz$ for some y, z in G with $o(y) = m$, $o(z) = n$, and $yz = zy$.

(Hint for proof: Find integers a and b with $am + bn = 1$. Set $y = x^{bn}$, etc.)

THEOREM. (FROBENIUS) *If d divides $|G|$ then d divides $|A_d|$.*

Proof. We proceed by double induction on $|G|$ and d. Note that the induction is started trivially with $|G| = d = 1$. Assume $|G| > 1$ and $d < |G|$ (since the case $d = |G|$ is evident) and, that the result holds for larger divisors of $|G|$ and groups with order $< |G|$.

Let p be any prime divisor of $|G|/d$ and let $d = p^\alpha s$, where $\gcd(p, s) = 1$. Let $A = A_{dp} \backslash A_d$. Note that $|A_{dp}| = |A_d| + |A|$ and as d divides $|A_{dp}|$ (by the induction hypothesis), it is enough to show that d divides $|A|$. If $A = \emptyset$, then we are through, so we assume that $A \neq \emptyset$. By the lemma, $|A|$ is a multiple of $\phi(p^{\alpha+1}) = p^\alpha(p - 1)$. Thus we only have to show that s divides $|A|$.

Since $A = \{x : o(x) = p^{\alpha+1}s_1,\ s_1 \mid s\}$, the fact noted above shows that every element x of A has the form $yz = zy$, where $o(y) = p^{\alpha+1}$ and $z^s = 1$.

For $a \in G$ of order $p^{\alpha+1}$, let us define $S_a = \{ab : b \in N(a) \text{ and } b^s = 1\}$. Define $S_{C(a)} = \cup\{S_x : x \in C(a)\}$. Then A is a union of the sets S_a. We now show that the union is disjoint. Let $o(a) = o(a_1) = p^{\alpha+1}$ and $ab = a_1b_1$ with $b^s = b_1^s = 1$, where $ab = ba$ and $a_1b_1 = b_1a_1$. Note that $(ab)^s = (a_1b_1)^s$ implies that $a^s = a_1^s$. Since

$a^{p^{\alpha+1}} = a_1^{p^{\alpha+1}}$ and $\gcd(p^{\alpha+1}, s) = 1$, we have $a = a_1$ showing that A is a *disjoint* union of the sets S_a. So it is enough to show that s divides $|S_{C(a)}|$.

Note that $ab \to xax^{-1}xbx^{-1}$ is a bijection from $S_a \to S_{xax^{-1}}$. Thus $|S_{C(a)}| = |C(a)||S_a|$. Let $o(N(a)/\langle a\rangle) = k$ and $m = \gcd(s, k)$. Then $ab \to b\langle a\rangle$ is a bijection from

$$S_a \to \{y \in N(a)/\langle a\rangle : y^s = 1\} = \{y \in N(a)/\langle a\rangle : y^m = 1\}.$$

As $|N(a)/\langle a\rangle| < |G|$, the induction hypothesis implies that

$$\left|\{y \in N(a)/\langle a\rangle : y^m = 1\}\right| = |S_a| = cm \quad \text{for some natural number } c.$$

Also $|S_{C(a)}| = |C(a)||S_a| = |G||S_a|/|N(a)| = |G|cm/kp^{\alpha+1}$. Since both k and s divide $|G|$, so does $\operatorname{lcm}(k, s) = ks/m$, showing that s divides $|G|cm/k$. Finally, as $p^{\alpha+1}$ divides $|G|cm/k$ and $\gcd(p, s) = 1$, we see that s divides $|S_{C(a)}|$. ∎

Some applications in group theory In this section, we give some group-theoretic applications of the Frobenius theorem, including those stated in the introduction. We shall tacitly use the following fact: *If d divides $|G|$ and $|A_d| = d$, then any subgroup H of order d coincides with A_d and is thus normal in G.*

APPLICATION 1. *Let $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where $p_1 < p_2 < \cdots < p_r$ are primes. If every Sylow p-subgroup of G is cyclic, then a Sylow p_r-subgroup is normal in G (and is thus unique). Moreover, G is solvable. In particular, if $|G|$ is squarefree and p is the largest prime divisor of $|G|$, then the Sylow p-subgroup is normal in G and G is solvable.*

Proof. We show that $|A_d| = d$ for every divisor d of $|G|$ that can be written in a particular form, namely $d = p_k^{\beta_k} p_{k+1}^{\alpha_{k+1}} \dots p_r^{\alpha_r}$, $1 \le k \le r$ and $\beta_k \le \alpha_k$. We proceed by induction on d. For $d = |G|$, the result follows trivially. Assume $d < |G|$ and that the result holds for larger divisors of the given type. Let p be the largest prime divisor of $|G|/d$ and $A = A_{dp} \backslash A_d$. As a Sylow p-subgroup is cyclic, $A \neq \emptyset$. By our assumption, $|A_{dp}| = dp$ and by the Frobenius theorem, $|A_d| = dt$ for some $1 \le t < p$. By the lemma, $p - 1$ divides $dp - dt = d(p - t)$. As every prime divisor of d is greater than or equal to p, $\gcd(p - 1, d) = 1$ and so $p - 1 | p - t$, implying that $t = 1$. Thus $|A_d| = d$ and, in particular, $|A_{p_r^{\alpha_r}}| = p_r^{\alpha_r}$ implying that a Sylow p_r-subgroup N is normal. Now by induction on the size of the group, N and G/N are solvable and thus G is solvable.

As every group of prime order is cyclic, the "in particular" part is now clear. ∎

APPLICATION 2. *Let n be a positive integer. Then every group of order n is cyclic if and only if* $\gcd(n, \phi(n)) = 1$.

Proof. One can easily check that $\gcd(n, \phi(n)) = 1$ if and only if n is squarefree and $p \nmid q - 1$, where p and q are prime divisors of n.

Necessity We exhibit a noncyclic group for each n where $\gcd(n, \phi(n)) \neq 1$. If $p^2 \mid n$, for some prime p, then $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{n/p^2}$ is a noncyclic group of order n (recall that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if $\gcd(m, n) = 1$). Now suppose n is squarefree and $p < q$ are two prime divisors of n such that $p \mid q - 1$. As $\mathbb{Z}_q \backslash \{0\}$ is group under multiplication modulo q and $p \mid q - 1$, there exists a subgroup, say H, of order p. Define an operation on elements of $\mathbb{Z}_q \times H$ by $(x, h)(y, k) = (x + hy, hk)$. Then $\mathbb{Z}_q \times H$ is a group with identity $(0, 1)$ in which $(x, h)^{-1} = (-h^{-1}x, h^{-1})$. Note that if $h \neq 1$, then $(1, h)(1, 1) \neq (1, 1)(1, h)$ showing that $G = \mathbb{Z}_q \times H$ is nonabelian. Thus $G \times \mathbb{Z}_{n/pq}$ is a nonabelian group of order n.

Sufficiency We show that $|A_d| = d$ for every divisor d of $|G|$. We proceed by induction on d. For $d = |G|$, the result follows trivially. Assume $d < |G|$ and that the result holds for all divisors greater than d. Let p be any prime divisor of $|G|/d$ and $A = A_{dp} \backslash A_d$. Clearly $A \neq \phi$. By our assumption, $|A_{dp}| = dp$ and by the theorem, $|A_d| = dt$ for some $1 \leq t < p$. Arguing just as in Application 1, we see that that $t = 1$ and so $|A_d| = d$. In particular, $|A_p| = p$ for every prime divisor of $|G|$, which implies that every Sylow p-subgroup is normal. Thus G, being direct sum of its cyclic Sylow p-subgroups of co-prime order, is cyclic. ■

Dickson [**6**] characterized $n \in \mathbb{N}$ such that every group of order n is abelian. Miller and Moreno [**17**] studied nonabelian groups in which every subgroup is abelian. They proved that the order of a nonabelian group whose every proper subgroup is abelian can have at most two distinct prime factors.

As already mentioned, if $|A_d| = d$, then every subgroup of order d coincides with A_d and is thus normal. But the converse is not true; a normal subgroup of order d may not coincide with A_d. For example, if $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $N = \langle (1, 0) \rangle$, then $N \trianglelefteq G$ and $|N| = 2$, but $|A_2| = 4$. But if $N \trianglelefteq G$ and $\gcd(|N|, |G/N|) = 1$, then $N = A_{|N|}$. To see this let $a \in A_{|N|}$. Now $aN \in G/N$ implies $a^{|G/N|} \in N$ and $a \in A_{|N|}$ implies $a^{|N|} = 1 \in N$. This, in light of $\gcd(|N|, |G/N|) = 1$, implies that $a \in N$.

A similar argument shows that if $K \trianglelefteq N \trianglelefteq G$ with $\gcd(|K|, |N|/|K|) = 1$, then $K \trianglelefteq G$. For if $k \in K$ and $g \in G$, then $x = gkg^{-1} \in N$. Thus $x^{|N/K|} \in K$ and $x^{|K|} = 1 \in K \Rightarrow x \in K$. But this is not true for any chain of normal subgroups. For example, if we take $G = A_4$, $N = V_4 = \{I, (12)(34), (13)(24), (23)(14)\}$, and $K = \{I, (12)(34)\}$, then $K \trianglelefteq N \trianglelefteq G$ but K is not normal in G. What went wrong here is the fact that $\gcd(|K|, |N/K|) \neq 1$.

In 1895, Frobenius conjectured (in the same paper where he proved the theorem that bears his name [**9**]) that if $|A_d| = d$, then A_d forms a subgroup. The work of many group theorists went into proving the conjecture. Its final proof was announced in 1991 [**14**] and the details appeared later [**15**].

Let $|G| = p^\alpha m$, where p is the smallest prime divisor of $|G|$ and $\gcd(p, m) = 1$. If the Sylow p-subgroup is cyclic, then, as argued in Application 1, $|A_{n/p^\beta}| = n/p^\beta$, for all $1 \leq \beta \leq \alpha$. Thus, it follows from Frobenius's conjecture that G has subgroups of order n/p^β, for all $1 \leq \beta \leq \alpha$.

Some applications in number theory Many authors have studied A_d in symmetric groups [**4, 5, 16, 19**]. It is well known that two elements in S_n are conjugate if and only if they have the same cyclic decomposition [**13**, p. 88]. So if the cyclic decomposition of $\sigma \in S_n$ into m cycles has n_i cycles of length l_i with $l_i \geq 1$ and $\sum_i l_i n_i = n$, then one can show that the size of the conjugacy class of σ in S_n is

$$n! \Big/ \prod_{i=1}^{m} l_i^{n_i} \prod_{i=1}^{m} n_i! \tag{1}$$

and that the number of r-cycles in S_n is $n!/r(n-r)!$. The Frobenius theorem gives us many useful number-theoretic identities just by finding suitable $|A_d|$ for appropriate values of d in symmetric groups.

APPLICATION 3. *For any prime p and any natural number $n \geq p$, we have*

$$\sum_{k=1}^{t} \frac{n!}{p^k (n - kp)!\, k!} \equiv -1 \pmod{p},$$

where t is the largest natural number such that $tp \leq n$.

Proof. As A_p in S_n contains only those elements that are products of p-cycles and 1-cycles (fixed points), then by equation (1)

$$|A_p| = 1 + \sum_{k=1}^{t} \frac{n!}{p^k(n-kp)!\,k!},$$

where the summand counts those permutations that are the product of k p-cycles and $n - kp$ fixed points, and the initial 1 counts the identity permutation. Thus, the result follows from the Frobenius theorem. ∎

Note that by putting $n = p$ in Application 3, we get Wilson's theorem (that is, $(p-1)! \equiv -1 \pmod{p}$ for any prime p).

APPLICATION 4. *If $n/2 < p_1 < p_2 < \cdots < p_k \leq n$, where $n \in \mathbb{N}$ and each p_i is prime, then*

$$\sum_{t=1}^{k} \frac{n!}{p_t(n-p_t)!} \equiv -1 \pmod{p_1 p_2 \ldots p_k}.$$

Proof. Find $|A_{p_1 p_2 \ldots p_k}|$ in S_n as in Application 3 above. ∎

Proceeding along the same lines one may obtain many such identities.

Acknowledgment. We thank Professor Bhandari and Professor Gupta for some useful discussions. We are highly indebted to Professor B. Sury for many suggestions to improve the quality of the paper. Thanks are also due to the referees for their helpful comments.

REFERENCES

1. R. Brauer, On a theorem of Frobenius, *Amer. Math. Monthly* **76** (1969), 12–15.
2. W. Burnside, *The Theory of Groups of Finite Order*, 2nd ed., Dover, New York, 1955.
3. R. D. Carmichael, *Introduction to the Theory of Groups of Finite Order*, Dover, New York, 1956.
4. S. Chowla, I. N. Herstein, and W. K. Moore, On recursions connected with symmetric groups I, *Canad. J. Math.* **3** (1951), 328–334.
5. S. Chowla, I. N. Herstein, and W. R. Scott, The solutions of $X^d = 1$ in symmetric groups, *Norske Vid. Selsk. Forh. (Trondheim)* **25** (1952), 29–31.
6. L. E. Dickson, Definitions of a group and a field by independent postulates, *Trans. Amer. Math. Soc.* **6** (1905), 198–204.
7. W. Feit and J. G. Thompson, Solvability of groups of odd orders, *Pacific J. Math.* **13** (1963), 775–1029.
8. H. Finkelstein, Solving Equations in groups, *Period. Math. Hungar.* **9** (1978), 187–204.
9. F. G. Frobenius, Verallgemeinerung des Sylowschen Satzes, *Berliner Sitz.* (1895), 981–993.
10. ———, Über endliche gruppen, *Berliner Sitz.* (1895), 81–112.
11. ———, Über einen Fundamentalsatz der Gruppentheorie, *Berliner Sitz.* (1903), 987–991.
12. M. Hall, *The Theory of Groups*, Macmillan, New York, 1959.
13. I. N. Herstein, *Topics in Algebra*, Blaisdell, New York, 1964.
14. N. Iiyori and H. Yamaki, On a conjecture of Frobenius, *Bull. Amer. Math. Soc.* **25** (1991), 413–416.
15. N. Iiyori, A conjecture of Frobenius and the simple groups of Lie type IV, *J. Algebra* **154** (1993), 188–214.
16. E. Jacobstal, Sur le nombre d'éléments du groupe symétrique S_n dont l'ordre est un nombre premier, *Norske Vid. Selsk. Forh. (Trondheim)* **21** (1949), 49–51.
17. G. A. Miller and H. C. Moreno, Non-abelian groups in which every subgroup is abelian, *Trans. Amer. Math. Soc.* **4** (1903), 398–404.
18. G. A. Miller, H. F. Blichfeldt, and L. E. Dickson, *Theory and Application of Finite Groups*, Dover, New York, 1961.
19. L. Moser and M. Wyman, On solutions of $X^d = 1$ in symmetric groups, *Canad. J. Math.* **7** (1955), 159–168.
20. J. P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag GTM **42**, 1997.