AUT Journal of Mathematics and Computing

AUT J. Math. Comput., 4(1) (2023) 99-103
DOI: 10.22060/AJMC.2022.21305.1085

Original Article

A new approach to character-free proof for Frobenius theorem

Seyedeh Fatemeh Arfaeezarandi*[a], Vahid Shahverdi[b]

[a] *Department of Mathematics, Stony Brook University, Stony Brook, New York, USA*
[b] *Department of Mathematics, KTH Royal Institute of Technology, Stockholm, Sweden*

ABSTRACT: Let G be a Frobenius group. Using character theory, it is proved that the Frobenius kernel of G is a normal subgroup of G, which is well-known as a Frobenius theorem. There is no known character-free proof for Frobenius theorem. In this note, we prove it, by assuming that Frobenius groups are non-simple. Also, we prove that whether K is a subgroup of G or not, Sylow 2-subgroups of G are either cyclic or generalized quaternion group. Also by assuming some additional arithmetical hypothesis on G we prove Frobenius theorem. We should mention that our proof is character-free.

Review History:

Received:16 April 2022
Revised:19 July 2022
Accepted:22 July 2022
Available Online:01 February 2023

Keywords:

Finite group
Frobenius group
Frobenius theorem

AMS Subject Classification (2010):

20D15; 20C20; 20C15

(*Dedicated to Professor Jamshid Moori*)

1. Introduction

Let G be a finite Frobenius group, that is G contains a proper nontrivial subgroup H such that $H \cap H^g = 1$ for all $g \in G \setminus H$. A subgroup with these properties is called a Frobenius complement of G. The Frobenius kernel of G, with respect to H, is defined by $K = (G \setminus (\cup_{g \in G} H^g)) \cup \{1\}$. Obviously, K is a normal subset of G. Using character theory it is proved that K is a subgroup of G (see [6]), which is well-known as a Frobenius theorem.

So far there has been elementary proof for Frobenius theorem, only in special cases: when the complement is solvable, or the complement is of even order (see [5, 8]). Also in [1], the authors tried to find a character-free proof for the theorem and in [2], the author proved that if G is a non-simple Frobenius group, then the Frobenius kernel of G is a normal subgroup of G.

It is easy to see that the Frobenius kernel K is a normal subset of Frbenius group G. In this short note, avoiding character theory, we prove the following theorem:

Theorem A. Assume that all Frobenius groups are not Simple. If G is a Frobenius group with Frobenius kernel K. Then K is a subgroup of G.

By knowing that the Frobenius Kernel K of a Frobenius group G is a subgroup, it has been proved that Sylow 2-subgroups H of G are either generalized quaternion or cyclic. In the next theorem, we show this result by taking out the assumption that K is a subgroup of G.

*Corresponding author.
E-mail addresses: seyedehfatemeh.arfaeezarandi@stonybrook.edu, vahidsha@kth.se

Theorem B. If G is a Frobenius group with Frobenius complement H of even order, then the Sylow 2-subgroups of H are cyclic or generalized quaternion group.

As K is a normal subset of G, K is a disjoint union of some conjugacy classes of G. We denote by $s(K)$ the number of disjoint G-conjugacy classes of G, whose union is $K \setminus \{1\}$. As another result of this paper we prove the following:

Theorem C. If G is a Frobenius group with Frobenius kernel K such that $s(K) \leq 2$, then K is a subgroup of G.

We denote by $n_G(H)$, the size of $S = \{HgH \mid g \in G \setminus H\}$. As our last result we prove the following:

Theorem D. Let G be a Frobenius group with Frobenius complement H. If $n_G(H) \leq 10$, then K, the Frobenius kernel of G, is a normal subgroup of G.

Throughout the paper, we denote by $\pi(G)$, the set of all prime divisors of $|G|$. All other notations are standard.

2. Preliminaries

Lemma 2.1 (Frobenius Theorem [3]). *If n divides the order of a finite group G, then the number of solutions of $x^n = 1$ is a multiple of n.*

Lemma 2.2 (Zsigmondy Theorem [9]). *Let p be a prime and let n be a positive integer. Then one of the following holds:*

(i) *There is a primitive prime p' for $p^n - 1$, that is , $p' \mid (p^n - 1)$ but $p' \nmid (p^m - 1)$, for every $1 \leq m < n$,*

(ii) *$p = 2$, $n = 1$ or 6,*

(iii) *p is a Mersenne prime and $n = 2$.*

Lemma 2.3 (see [7, 8.3.7]). *Let G be a Frobenius group, and K be a Frobenius kernel of G. If K is a normal subgroup of G. Then all Frobenius complements of G are conjugate.*

Lemma 2.4 (see [7, 8.1.12]). *Let G be the semidirect product of the nontrivial subgroup H with the normal subgroup K. Then the following statements are equivalent:*

(i) *G is a Frobenius group with a Frobenius complement H and a Frobenius kernel K.*

(ii) *$C_K(h) = 1$ for all $h \in H$.*

Lemma 2.5 (see [7, 4.1.8]). *Let G be a Frobenius group with Frobenius complement H and Frobenius kernel K.*

(a) *Let L be a subgroup of G such that $L \nsubseteq K$, and $x \in G$ such that $H^x \cap L \neq 1$. Then either $L \leq H^x$ or L is a Frobenius group with Frobenius complement $H^x \cap L$ and Frobenius kernel $L \cap K$.*

(b) *Let H_0 be another Frobenius complement of G such that $|H_0| \leq |H|$. Then H_0 is conjugate to a subgroup of H.*

Lemma 2.6 (see [4]). *Let G be a Frobenius group with the Frobenius kernel K and Frobenius complement H. Assume K is a normal subgroup of G and $|H|$ is even. Then K is abelian.*

3. Main results

Throughout this section, we assume G is a Frobenius group with Frobenius complement H. We denote by K, the Frobenius kernel of G with respect to H which is a normal subset of G. We assume these hypotheses for the following lemmas and theorems without further mentioning.

Lemma 3.1. $|G| = |H|(n_G(H)|H| + 1)$ *and* $|K| = n_G(H)|H| + 1$.

Proof. It is easy to see that $S = \{HgH | g \in G \setminus H\}$ forms a partition for $G \setminus H$. As H is a Frobenius complement of G, $|HaH| = |H|^2$, for $a \in G \setminus H$. Therefore, we conclude that $|G| = n_G(H)|H|^2 + |H| = |H|(n_G(H)|H| + 1)$. As $H = N_G(H)$, we deduce that the number of distinct subgroups of G conjugate to H is equal to $n_G(H)|H| + 1$. Hence, $|K| = |G| - (n_G(H)|H|) + 1)(|H| - 1) = n_G(H)|H| + 1$. □

Lemma 3.2. *Let $x \in K \setminus \{1\}$. Then the followings hold:*

(a) $C_G(x) \subseteq K$.

(b) $|x|$ *divides* $|K|$.

(c) *If a prime* p *divides* $|K|$, *then* K *contains* P, *where* $P \in Syl_p(G)$.

(d) $|C_G(x)|$ *divides* $|K|$.

Proof. Assume there exist $y, g \in G$ such that $y \in C_G(x) \cap H^g$. Then $y \in H^{gx} \cap H^g$ and so $x \in H^g \cap K = 1$. So, part (a) is proved.

Assume p is a prime divisor of $(|x|, |H|)$. Hence, there exists a power of x (whose order is p), say x^t, which belongs to P^g, for some $P \in Syl_p(H)$ and $g \in G$. Thus, $x^t \in H^g \cap C_G(x)$. Now using part(a), we get $x^t = 1$ that is a contradiction, so $|x|$ is a divisor of $|K|$, so part(b) is proved. The statement of part(c) is obvious.

First we prove $(|C_G(x)|, |H|) = 1$. On the contrary, assume q is a prime divisor of $(|C_G(x)|, |H|)$. Then there exists $y \in C_G(x)$ such that $|y| = q$. Therefore, by part(b), we get that $y \in H^g$, for some $g \in G$, a contradiction. Therefore, $|C_G(x)|$ divides $|K|$. □

Proposition 3.3. *Let* N *be a normal subgroup of* G. *Then either* N *is a Frobenius group with Frobenius complement* $N \cap H$ *and Frobenius kernel* K, *or* $N \subseteq K$.

Proof. First, assume N is not a subset of K. Therefore, $N \cap H \neq 1$. So N is a Frobenius group by Lemma 2.5 and the number of conjugate subgroups of $N \cap H$ in N is equal to:

$$\frac{|N|}{|N \cap H|} = \frac{|N \cap K| + (|K|)(|N \cap H| - 1)}{|N \cap H|}.$$

Also, $|NH|$ divides $|G|$, which implies that $|N|/|N \cap H|$ divides $|K|$. This fact leads us to conclude that

$$|K| - (\frac{|K| - |N \cap K|}{|N \cap H|}) \mid (\frac{|K| - |N \cap K|}{|N \cap H|}).$$

If $|K| - |N \cap K| > 0$, then we deduce that $|K||N \cap H| \leq 2(|K| - |N \cap K|)$, and so $|K|(|N \cap H| - 2) < 0$, a contradiction. So we may assume $|K| = |N \cap K|$, which implies that $K \subseteq N$. Hence, $|N| = |K||N \cap H|$ and this means that the Frobenius kernel of N is K, that is our desired result. □

Proposition 3.4. *Let* N *be a normal subgroup of* G *contained in* K. *Then* G/N *is a Frobenius group and* K/N *and* HN/N *are Frobenius kernel and Frobenius complement of* G/N, *respectively.*

Proof. Note that by Lemma 2.5, NH and NH^x are Frobenius groups, for each $x \in G \setminus NH$. By the structure of a Frobenius group we get that $NH \cap NH^x = (N \cup (\bigcup_{n \in N} H^n)) \cap (N \cup (\bigcup_{n \in N} H^{xn}))$. Therefore, it is obvious that $NH \cap NH^x = N$.

For more convenient, we use the bar to work on the group $\overline{G} = G/N$ and the subgroups of $\overline{G}$. For every $\overline{x} \in \overline{G} \setminus \overline{H}$, we have $\overline{H} \cap \overline{H}^{\overline{x}} = N/N$, as $x \notin NH$, by the above discussion.

Let $\overline{F}$ be the Frobenius kernel of $\overline{G}$. It is obvious that $\overline{F} = \{xN \mid xN \notin H^g N \text{ for every } g \in G\} \subseteq \overline{K} = \{kN \mid k \in K\}$ and $|\overline{F}| = |\overline{G}|/|\overline{H}| = |K|/|N| = |\overline{K}|$, by Lemma 3.1. So we have $\overline{F} = \overline{K}$, hence G/N is a Frobenius group with Frobenius kernel and Frobenius complement K/N and HN/N, respectively. □

Now we are ready to prove Theorem A.

Proof of Theorem A. On the contrary, we assume G is a counterexample with minimal order $|G|$. As G is not simple, G has a nontrivial proper normal subgroup N. By Proposition 3.3, either $N \subseteq K$ or $K \subseteq N$. First, assume the latter case holds and $K \subseteq N$. Then by Proposition 3.3, N is a Frobenius group, with Frobenius kernel K and so, by minimality of G, K is a subgroup of N and so it is a subgroup of G that is a contradiction. So we may assume the former case holds, it means $N \subseteq K$. By Proposition 3.4, G/N is a Frobenius group with Frobenius kernel and Frobenius complement K/N and HN/N, respectively. Again using minimality of G, we conclude that K/N is a normal subgroup of G/N, which implies that K is a subgroup of G which is a contradiction.

Proof of Theorem B. We claim that each right coset of H contains at most one involution. First assume there exist $x, y \in aH$, such that $|x| = |y| = 2$, for some $a \in G \setminus H$. If $x = ah_1$ and $y = ah_2$, for some h_1 and $h_2 \in H$, then $h_1ah_1 = h_2ah_2$. Hence, $h_2^{-1}h_1 = ah_2h_1^{-1}a^{-1}$. As H is a Frobenius complement, we conclude that $a \in H$ which is a contradiction.

Now assume H contains s involutions. So by Lemma 3.2 the number of involutions out of H is exactly equal to $s|H|n_G(H)$. Therefore $s|H|n_G(H) \leq |H|n_G(H)$, implying $s \in \{0, 1\}$. It is well-known that a 2-group with only one involution is either a cyclic group or a generalized quaternion group, which is our desired result.

Proof of Theorem C. By our assumption, $|K|$ is divided by at most two primes. If $|K| = p^n$ for some prime p, then K is a Sylow p-subgroup of G by Lemma 3.2 and we are done. So we may assume $|K| = p^\alpha q^\beta$ and also every element of K has prime order and every element in K with the same order are G-conjugate.

Let $x, y \in K$ where $|x| = p$ and $|y| = q$. Then $|y^G| = |H|p^\alpha$ and $|x^G| = |H|q^\beta$, as G does not have any element of order pq. Therefore

$$|H|(p^\alpha + q^\beta) + 1 = |K| = p^\alpha q^\beta. \quad (*)$$

Let $r \in \{p, q\}$. Then by the above discussion for every $R \in Syl_r(G)$ there exists $z \in K$ such that $R = C_G(z)$ and so $\{\mathbf{Z}(R) \setminus \{1\} | R \in Syl_r(G)\}$ partition x^G, where x is a nontrivial r-element of G. Therefore $|G|(|\mathbf{Z}(R)| - 1)/|N_G(R)| = |x^G| = |G|/|R|$ implying that $|N_G(R)| = |R|(|\mathbf{Z}(R)| - 1)$. Note that by Lemma 2.4, $N_G(R)$ is a Frobenius group whose Frobenius complement is an r-complement of $N_G(R)$.

If $r \neq 2$, then $2 \mid (|\mathbf{Z}(R)| - 1)$ and so the order of Frobenius complements of $N_G(R)$ is even. Using Lemma 2.6, the Sylow r-subgroups of G are abelian. Also, if $r = 2$, the fact that the exponent of every Sylow 2-subgroup of G is 2 implies that Sylow 2-subgroups of G are abelian. Therefore the Sylow r-subgroups of G are elementary abelian for $r \in \{p, q\}$.

Assume $p < q$. We know $|\mathbf{Z}(P)| - 1 = p^\alpha - 1$ divides $|H|q^\beta$, where $P \in Syl_p(G)$. If $d = (|H|, p^\alpha - 1) = 1$ we conclude that $p^\alpha - 1$ is a power of q. Hence, $q = 2^\alpha - 1$ and $p = 2$ by Lemma 2.2. On the other hand $q - 1$ divides $|\mathbf{Z}(Q)| - 1$, for $Q \in Syl_q(G)$, and so $q - 1$ divides $p^\alpha|H|$. By $(*)$ and some easy calculation we get that $q - 1$ is a divisor of $p^\alpha(p^\alpha - 1)$. As $q - 1 = 2^\alpha - 2$ and $p = 2$, the only possibility is $(\alpha, q) = (2, 3)$.

As $|H| = \frac{2^2 3^\beta - 1}{2^2 + 3^\beta} < 2^2$ we deduce that $|H| = 1$ which is a contradiction. Thus, $d > 1$ and without loss of generality we assume $|H \cap N_G(P)| > 1$. Therefore, by Lemma 2.5, $N_G(P)$ is a Frobenius group with Frobenius complement $H \cap N_G(P)$. Also by Lemma 2.4, $N_G(P)$ is a Frobenius group whose p-complement is a Frobenius complement. Hence, by Lemma 2.3, we realize $H \cap N_G(P)$ is a p-complement of $N_G(P)$. Therefore, $p^\alpha - 1$ is a divisor of $|H|$. Thus, $(p^\alpha - 1)(p^\alpha + q^\beta) \mid p^\alpha q^\beta - 1$ and hence $p^{2\alpha} - p^\alpha + 1 \leq q^\beta$. On the other hand $(p^\alpha - 1)(p^\alpha + q^\beta) \mid p^\alpha q^\beta - 1 - (p^\alpha - 1)(p^\alpha + q^\beta)$, whence $p^\alpha + q^\beta \mid p^{2\alpha} + 1$. Therefore $q^\beta = p^{2\alpha} - p^\alpha + 1$ and $|H| = p^\alpha - 1$.

As $q^\beta = p^\alpha(p^\alpha - 1) + 1 = p^\alpha|H| + 1$, we deduce that the conjugacy class of G containing the q-elements of G has exactly $q^\beta - 1$ elements, implying that G contains a normal Sylow q-subgroup. Hence, $QP = K$ is a subgroup of G, where $Q \in Syl_q(G)$ and $P \in Syl_p(G)$, as we desired. So by normality of K as a subset, it is a normal subgroup of G.

Lemma 3.5. *Let p be the smallest prime divisor of $|K|$. If $s(K) > n_G(H)/p$, then K is a subgroup of G.*

Proof. On the contrary assume that K is not a subgroup of G. Hence,

$$|x^G| = |G|/|C_G(x)) = |H||K|/|C_G(x)| \geq p|H|$$

for every $x \in K \setminus \{1\}$. Thus, $p|H|s(K) \leq |H|n_G(H)$ and $s(K) \leq n_G(H)/p$ which is a contradiction. □

Proof of Theorem D. On the contrary, we suppose K is not a subgroup. So, by Lemma 3.5, $s(K) \leq n_G(H)/p$ where p is the smallest prime divisor of $|K|$. Note that $|H|n_G(H) = \Sigma_{i=1}^{s(K)} |x_i^G|$, where x_i^G's are disjoint G-conjugacy classes contained in K. Let $|x_i^G| = |H|t_i$, for $1 \leq i \leq s(K)$, where t_i is a divisor of $|K|$. So there is a partition for $n_G(H)$ with $s(K)$ parts such that all parts $2 \leq t_i$, for each $i \in \{1, \cdots, s(K)\}$, (as otherwise $K = C_G(x_i)$ for some $i \in \{1, \cdots, s(K)\}$). By Theorem C, we get the desired result for $i \in \{1, 2, 3, 4, 5, 6\}$.

- Let $n_G(H) = 7$. Obviously $s(K) \leq 3$. We only need to exclude the case $s(K) = 3$. Assume $K \setminus \{1\} = x_1^G \cup x_2^G \cup x_3^G$. Let $|x_i^G| = |H|t_i$, for $1 \leq i \leq 3$. Hence, $t_1 + t_2 + t_3 = 7$ and $2 \leq t_i$, for each $i \in \{1, 2, 3\}$. Note that t_i's are divisors of K, as explained. Therefore, we may assume $(t_1, t_2, t_3) = (2, 2, 3)$. Obviously 6 divides K and $|\pi(K)| \leq 3$. First, assume $\pi(K) = \{2, 3, p\}$, for some prime $p \notin \{2, 3\}$. Then $|K| = 7|H| + 1 = 2^\alpha 3^\beta p^\gamma$. By Lemma 2.1, for $1 \leq i \leq 3$, there exist natural numbers s_i's such that

$$s_1 p^\gamma = t_1|H| + 1, s_2 3^\beta = t_2|H| + 1, s_3 2^\alpha = t_3|H| + 1.$$

  Hence, $7|H| + 1$ divides $(3|H| + 1)(2|H| + 1)^2$. By easy calculation we obtain $|H| = 7$, a contradiction, as $|K| = 50$ is not divided by 3. So, we may assume $|K| = 2^\alpha 3^\beta$. Suppose there exists an element of order 6 in G. In this case, all p-elements are G-conjugate for each $p \in \{2, 3\}$. Then, by Lemma 2.1 we have $2^\alpha \mid 3|H| + 1$ and $3^\beta \mid 2|H| + 1$. This implies that $|K| = 7|H| + 1$ is a divisor of $6|H|^2 + 5|H| + 1$, which leads to a contradiction.

  So we may assume there is no element of order 6. Therefore one nontrivial conjugacy class contains p-elements and the union of two other nontrivial conjugacy classes contains $\{\{2, 3\} - \{p\}\}$-elements, for some $p \in \{2, 3\}$. Then, either 2^α divides $5|H| + 1$ and 3^β is a divisor of $2|H| + 1$, or 2^α divides $3|H| + 1$ and $3^\beta \mid 4|H| + 1$. In the former case, $|K| = 7|H| + 1 \mid 10|H|^2 + 7|H| + 1$, implying $7|H| + 1$ divides 10, that is a contradiction. Then we assume the latter case occurs. This case lead us to contradiction, as $7|H| + 1$ divides $12|H|^2 + 7|H| + 1$ and so $7|H| + 1 \mid 12$. Therefore $s(K) \leq 2$, and we are done by Theorem C.

- Let $n_G(H) = 8$. As $s(K) \leq 8/3$, we have $s(K) \leq 2$, which is done by the Theorem C.

- Let $n_G(H) = 9$. Then $s(K) \leq 9/2$. Note that $s(K)$ can not be 4, because there is just one partition for 9 with 4 parts greater than 1 and one of the parts is 3, which is not a divisor of $9|H| + 1$ (all parts divide $|K|$). So it remains to exclude the case $s(K) = 3$. The only possible partition of 9 with exactly three parts greater than 1, whose parts are coprime to 3 is $9 = 2 + 2 + 5$.

  First assume $|\pi(K)| = 3$. Then, by similar argument as we have in the case $n_G(H) = 7$, $9|H| + 1$ is a divisor of $(5|H|+1)(2|H|+1)^2$. Thus, by easy calculation we have $9|H|+1$ divides $20|H|+24$ and so $9|H|+1$ divides $2|H| + 22$. This implies that $|H| = 3$ and $|K| = 28$, contradicting the fact that 5 is a divisor of $|K|$.

  So, we may assume $\pi(K) = \{2, 5\}$ and $9|H| + 1 = 2^\alpha 5^\beta$.

  First, suppose there is an element of order 10 in G. Then, 2^α is a divisor of $5|H| + 1$ and 5^β divides $2|H| + 1$. Then $9|H| + 1$ divides $20|H|^2 + 9|H| + 1$, hence $9|H| + 1 \mid 20$, that is a contradiction.

  So we may assume there is no element of order 10 in G. Again by a similar argument as we have in case $n_G(H) = 7$, we have either 2^α divides $7|H| + 1$ and 5^β is a divisor of $2|H| + 1$, or 2^α divides $5|H| + 1$ and $5^\beta \mid 4|H|+1$. In the former case, $|K| = 9|H|+1 \mid 14|H|^2+9|H|+1$ that is a contradiction, as $|K| \mid 14$. Then we assume the latter case occurs. This case leads us to a contradiction, as $9|H|+1$ divides $20|H|^2+9|H|+1$, implying $|K| \mid 20$ and $|H| = 1$. So $s(K) \leq 2$ and we are done.

- Let $n_G(H) = 10$. So $s(K) \leq 10/3$. Let $s(K) = 3$. But there is no partition of 10, with 3 parts, whose parts are divisor of $10|H| + 1 = |K|$. Therefore $s(K) \leq 2$ and we are done by Theorem C.

References

[1] K. Corrádi and E. Horváth, *Steps towards an elementary proof of Frobenius' theorem*, Comm. Algebra, 24 (1996), pp. 2285–2292.

[2] P. Flavell, *A note on Frobenius groups*, J. Algebra, 228 (2000), pp. 367–376.

[3] G. Frobenius, *Über einen Fundamentalsatz der Gruppentheorie.*, Berl. Ber., 1903 (1903), pp. 987–991.

[4] L. C. Grove, *Groups and characters*, Pure and Applied Mathematics (New York), John Wiley & Sons, Inc., New York, 1997. A Wiley-Interscience Publication.

[5] B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin-New York, 1967.

[6] B. Huppert and N. Blackburn, *Finite groups. III*, vol. 243 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin-New York, 1982.

[7] H. Kurzweil and B. Stellmacher, *The theory of finite groups*, Universitext, Springer-Verlag, New York, 2004. An introduction, Translated from the 1998 German original.

[8] D. Passman, *Permutation groups*, W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[9] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys., 3 (1892), pp. 265–284.

Please cite this article using:

Seyedeh Fatemeh Arfaeezarandi, Vahid Shahverdi, A new approach to character-free proof for Frobenius theorem, AUT J. Math. Comput., 4(1) (2023) 99-103
DOI: 10.22060/AJMC.2022.21305.1085