Frobenius groups of low rank

WOLFGANG KNAPP AND PETER SCHMID

Abstract. Let G be a finite Frobenius group of degree n. We show, by elementary means, that n is a power of some prime p provided the rank $\mathrm{rk}(G) \leq 3 + \sqrt{n+1}$. Then the Frobenius kernel of G agrees with the (unique) Sylow p-subgroup of G. So our result implies the celebrated theorems of Frobenius and Thompson in a special situation.

Mathematics Subject Classification. 20B05, 20B10.

Keywords. Frobenius groups, Sylow subgroups, Rank of a transitive permutation group.

1. Introduction. Throughout, G will be a finite Frobenius group with point stabilizer H and degree $n = |G : H|$ $(n > 2)$. Thus G is a transitive, nonregular permutation group where each element $\neq 1$ has at most one fixed point. In other words, $H \neq 1$ and $H \cap H^g = 1$ for all $g \in G \setminus H$ $(H^g = g^{-1}Hg)$. It follows that each nontrivial H-orbit has size $|H|$ and that there are just $s = \frac{n-1}{|H|}$ such orbits. Hence the (permutation) rank of G equals

$$\mathrm{rk}(G) = 1 + s = 1 + \frac{n-1}{|H|}.$$

Let $\widehat{H} = \bigcup_{g \in G} H^g$ and $F^\sharp = G \setminus \widehat{H}$. Thus $F^\sharp$ is the set of all *derangements* in G (acting fixed-point-freely). Let $F = F^\sharp \cup \{1\}$. By definition, $F^\sharp$ and F are normal subsets of G, and $|F| = n$ is the cardinality of F. By a theorem of Frobenius [4], F is always a (normal) subgroup of G, and Thompson [16] has shown that the *Frobenius kernel F* is nilpotent (confirming a longstanding conjecture). Combining these celebrated results, we will speak of the Frobenius–Thompson theorem in what follows.

Except for some special cases the known proofs for the theorem of Frobenius make use of character theory (or Fourier analysis). The Fourier-analytic approach given by Terry Tao in [15] is "character-free" but, as he conceded

in this blog post, it is "not all that far from character-based in spirit". One should compare this with the rather direct approach [11] of the present authors which uses only some basic facts on characters; see also [12].

Lemma 0. *The theorem of Frobenius has been proved without employing characters (or Fourier analysis) when H is solvable or $|H|$ is even, or when $\mathrm{rk}(G) \leq 3$. If $|H|$ is even or $\mathrm{rk}(G) \leq 3$, the Frobenius kernel F is an abelian subgroup of G.*

For proofs of this lemma, we refer to [1, Theorems 3.4A and 3.4B] (see also [8, Ex. 18 in Sect. V.8]). One knows that the Sylow subgroups of H are cyclic or generalized quaternion, so that H is solvable (metacyclic) when $|H|$ is odd. However, in order to prove this, one requires that F is a (normal) subgroup of G and that H acts freely on the group F [8, Satz V.8.15].

The following provides an elementary approach to the Frobenius–Thompson theorem in a special situation.

Theorem. *The degree n of the Frobenius group G is a power of some prime p if the rank $\mathrm{rk}(G) \leq 3 + \sqrt{n+1}$. In this case, the Frobenius kernel F is the unique Sylow p-subgroup of G.*

Since H is a Hall subgroup of G, in general, for every prime p dividing $|F| = n$, the Sylow p-subgroups of G are contained in F. Thus, for small rank as above, the Frobenius–Thompson theorem is just a consequence of Sylow's theorem. In a certain sense, the given upper bound is best possible. For instance, the dihedral group G of order $2 \cdot 15$ is a Frobenius group of degree $n = 15$ and rank $\mathrm{rk}(G) = 8$, whereas $3 + \sqrt{n+1} = 7$.

When G is a point stabilizer in a Zassenhaus group (of degree $n+1$), then, by the classification of these groups, indeed $\mathrm{rk}(G) \leq 3 + \sqrt{n+1}$. A crucial step towards this classification is a result by Feit [2] which in particular tells us that here n is always a prime power (see also [9, Theorem XI.6.1]). The largest rank (in relation to the degree) is obtained when G is a point stabilizer in the Suzuki group $Sz(q)$, where $n = q^2$ with $q = 2^{m+1}$ $(m \geq 1)$ and $\mathrm{rk}(G) = 2 + \sqrt{n}$.

2. Preliminaries. We keep the assumptions and notation as introduced above. In particular, $n = |G : H| = |F|$ is the degree of G, with $|H|$ dividing $n - 1$. For a subgroup M of G, we have $M \subseteq F$ if and only if $|M|$ is a divisor of n because $|H|$ and n are relatively prime. Recall that F is a normal subset of G.

Lemma 1. *The Frobenius complement H acts semiregularly (via conjugation) on the set $F^\sharp$. For any $y \in F^\sharp$, the centralizer $C_G(y) \subseteq F$, and the conjugacy class y^G has cardinality $|y^G| = s_y|H|$ where $s_y = \frac{n}{|C_G(y)|}$ is an integer.*

Proof. For convenience, we include a proof of this lemma (which is probably well known). If $y^h = h^{-1}yh = y$ for some $h \in H$ $(y \in F^\sharp)$, then $yhy^{-1} = h \in H \cap H^{y^{-1}} = 1$ and therefore $h = 1$. If $x \in C_G(y)$ fixes some element α (in the underlying G-set), then $\beta = \alpha y^{-1} \neq \alpha$ and

$$\beta x = \alpha(y^{-1}x) = \alpha(xy^{-1}) = (\alpha x)y^{-1} = \alpha y^{-1} = \beta.$$

This forces that $x = 1$. Thus the subgroup $C_G(y)$ of G is contained in F, whence $|C_G(y)|$ is a divisor of n. It follows that $|y^G| = |G : C_G(y)| = s_y|H|$ is as asserted. $\square$

In particular, $s = \frac{n-1}{|H|}$ is just the number of distinct H-orbits on $F^\sharp$, each being of size $|H|$.

The set $\widehat{H} = \bigcup_{g \in G} H^g$ has cardinality $|\widehat{H}| = (n-s)|H|$, an integer multiple of $|H|$. This is not surprising because it is a consequence of another well known theorem of Frobenius [5] just noting that

$$\widehat{H} = \{x \in G|\ x^{|H|} = 1\}.$$

The following will play a crucial role in this paper.

Lemma 2. *Let m be a positive integer dividing $|F| = n$, or let M be a subgroup of G with order $|M| = m$ (dividing n). Defining $\widehat{M} = \{x \in G|\ x^m = 1\}$, the following hold:*

(i) $\widehat{M}$ is a normal subset of G with $\widehat{M} \subseteq F$, and $M \subseteq \widehat{M}$ in the latter case.
(ii) We have $|\widehat{M}| = k_m m$ for some positive integer $k_m \leq \frac{n}{m}$.

Proof. For (i), observe that $F^\sharp = G \setminus \widehat{H}$ and that each element of $\widehat{H}$ has order dividing $n-1$. We have $M \subseteq \widehat{M}$ by Lagrange's theorem. Statement (ii) follows from the result by Frobenius [5] mentioned above. We refer to Theorems 9.1.1 and 9.1.2 in M. Hall's monography [7] for a nice inductive approach (see also [10] and [13]; improvements can be found in the paper [6] by P. Hall). The upper bound on k_m is clear since $\widehat{M} \subseteq F$ by (i). $\square$

In particular, taking $m = n$ in Lemma 2, we get that $F = \{x \in G|\ x^n = 1\}$ (as already noted in [8, V.19.15]). It has been asked by Frobenius whether a set $\widehat{M}$ as introduced above is a (characteristic) subgroup of G provided $|\widehat{M}| = m$. This has been verified in some special cases (e.g. see [7, Theorem 9.4.1] and [3]), the general problem being settled now through the classification of the finite simple groups.

In what follows, we fix a prime p dividing $|F| = n$ and a Sylow p-subgroup P of G, and we let $m = n_{p'} = \frac{n}{|P|}$ be the p'-part of n. According to Lemma 2, we define $\widehat{M}$ for this m. So $\widehat{M}$ is the set of all p'-elements in F, and $|\widehat{M}| = k_{p'}m$ for some positive integer $k_{p'} = k_m \leq |P|$. We have $k_{p'} < |P|$ as p is a divisor of n. We also define $\widehat{P} = \{x \in G|\ x^{|P|} = 1\}$. By Lemma 2, we have $P \subseteq \widehat{P} \subseteq F$ and $|\widehat{P}| = k_p|P|$ for some positive integer $k_p \leq m$. By Sylow's theorem, $\widehat{P} = \bigcup_{g \in G} P^g$ is the set of all p-elements in G, and $k_p = 1$ if and only if $P = \widehat{P}$ is normal in G.

Lemma 3. *Let p be a prime dividing $|F| = n$, and define P, $m = \frac{n}{|P|}$, k_p, and $k_{p'}$ as above. Then $|H|$ is a divisor of $k_p|P| - 1$ and of $|P| - k_{p'}$ (where $1 \leq k_p \leq m$ and $1 \leq k_{p'} < |P|$). We have $k_p = m$ if and only if $m = 1$ ($P = F$), and $\mathrm{rk}(G) > m + 1$ unless $m = 1$ and G is 2-transitive.*

Proof. The set $\widehat{P}^\sharp = \widehat{P} \setminus \{1\}$ is a G-invariant subset of $F^\sharp$. By Lemma 1, all H-orbits on $\widehat{P}^\sharp$ have size $|H|$, so $|\widehat{P}^\sharp| = k_p|P| - 1$ is divisible by $|H|$. We have $k_p = m$ if and only if $\widehat{P} = F$, in which case F consists merely of p-elements, and this forces that $m = 1$ and $P = F$. As before, $\widehat{M}$ is the set of all p'-elements in F (so that $|\widehat{M}| = k_{p'}m$). By Lemmas 1 and 2, we know that $|H|$ is a divisor of $k_{p'}m - 1$. Similarly, each H-orbit on $F \setminus \widehat{M}$ has size $|H|$ and therefore

$$|F \setminus \widehat{M}| = n - k_{p'}m = m(|P| - k_{p'})$$

is divisible by $|H|$. Since $|H|$ is relatively prime to n and hence to m, we get that $|H|$ is a divisor of $|P| - k_{p'}$. Consequently

$$s = \frac{n-1}{|H|} = m\frac{|P| - k_{p'}}{|H|} + \frac{k_{p'}m - 1}{|H|}.$$

This gives the last statement (noting that $\mathrm{rk}(G) = s + 1$ and that $k_{p'} = 1$ if $m = 1$). $\qquad\square$

Lemma 4. *Suppose that $n = p^a q^b$ where $p \neq q$ are primes and a, b are positive integers. Assume that $p^a + 1 = q^b$. Then one of the following holds:*

(i) $n = 2^3 \cdot 3^2$.

(ii) $p = 2$ and $b = 1$ (so that $q = 2^a + 1$ is a Fermat prime).

(iii) $q = 2$ and $a = 1$ (so that $p = 2^b - 1$ is a Mersenne prime).

This seems to be "folklore"; a proof can be found in Suzuki [14, Theorem III.2]. On the basis of Lemma 3, we will actually prove below that none of the statements (i), (ii), (iii) can occur in the Frobenius group G, thus refuting the assumption that $p^a + 1 = q^b$.

3. Proof of the theorem. Assume that n is not a prime power. Let p be that prime divisor of n for which a corresponding Sylow p-subgroup P of G has least possible order. Let $|P| = p^a$. Recall that $P \subseteq F$. Let $m = \frac{n}{|P|}$. By Lemma 3, there is a positive integer $k_{p'} < |P|$ such that $|H|$ is a divisor of $|P| - k_{p'}$. We get the estimate $|H| \leq |P| - k_{p'} \leq |P| - 1$. By our choice of the prime p, we certainly have $p^a \leq m - 1$.

Assume that $p^a + 1 = m$. Then necessarily $m = q^b$ is a power of some prime $q \neq p$ (and $n = p^a q^b$). We now apply Lemma 4. We cannot have $n = 2^3 \cdot 3^2$ ($|P| = 2^3$) because then $|H| \leq 7$. However $|H|$ is a (nontrivial) divisor of the prime $n - 1 = 71$. Consider next statement (ii) of Lemma 4, where $p = 2$ and $q = q^b = 2^a + 1$ is a Fermat prime. Now we may write $k_q = k_{p'}$, and $|H|$ is a divisor of $k_q q - 1$ by Lemma 3. Let Q be a Sylow q-subgroup of G. We assert that Q is normal in G, whence $k_q = 1$. Otherwise there are at least $q + 1$ (conjugate) Sylow q-subgroups in G, all pairwise with trivial intersection, so that there are $|\widehat{Q}| \geq (q+1)(q-1) + 1 = q^2$ q-elements in F (and G). However $q^2 > n$, giving the desired contradiction. Therefore $k_q = 1$ and $|H|$ is a divisor of $q - 1 = 2^a$. But $|H|$ is relatively prime to $n = 2^a q$.

Now consider part (iii) of Lemma 4. Here $q = 2$ and $|P| = p = 2^b - 1$ is a Mersenne prime. We assert that P is normal in G. Otherwise there are at least

$|\widehat{P}| \geq (p+1)(p-1)+1 = p^2$ p-elements in F. There are at least $2^b - 1 = p$ 2-elements in $F^\sharp$, and $p^2 + p = p(p+1) = n$. If the Sylow 2-subgroup Q of G is not normal in G, then $|\widehat{P^\sharp}| + |\widehat{Q}| > n$, which is impossible as $\widehat{P^\sharp}$ and $\widehat{Q}$ are disjoint subsets of F. Hence $Q = \widehat{Q}$ is normal in G and $|H|$ a (nontrivial) divisor of $|Q| - 1 = 2^b - 1 = p$. But $|H|$ is relatively prime to $n = p \cdot 2^b$. Thus P is a normal Sylow p-subgroup of G, as asserted. Now PQ is a subgroup of G of order $n = |F|$ and therefore $F = PQ$ by co-primeness of $|H|$ and n (or by Lemma 2). Moreover G/P is a Frobenius group with kernel F/P and complement $HP/P \cong H$ (by a known property of Frobenius groups; use [8, V.8.5 and I.18.6]). Hence $|H|$ is a (nontrivial) divisor of $|F/P| - 1 = 2^b - 1 = p$, which again cannot happen.

Consequently $|P| + 1 < m$. Since $|H| + 1 \leq |P|$, this yields that $|H| + 3 \leq m$ and

$$(|H| + 1)(|H| + 3) \leq |P|m = n.$$

Therefore $|H|^2 + 4|H| - (n-3) \leq 0$ and so $|H| \leq \sqrt{n+1} - 2$. It follows that

$$\mathrm{rk}(G) \geq 1 + \frac{n-1}{\sqrt{n+1}-2} > 1 + \frac{n-3}{\sqrt{n+1}-2} = 3 + \sqrt{n+1}.$$

Hence, if $\mathrm{rk}(G) \leq 3 + \sqrt{n+1}$, then n must be a prime power.

4. Remarks. The Frobenius–Thompson theorem just tells us that, for every prime p dividing the degree n of the Frobenius group G, there is a unique (normal) Sylow p-subgroup of G (F being the direct product of these Sylow subgroups). One may ask whether it is possible to settle this by the methods used in the present paper.

(1) For $y \in F^\sharp$, let $s_y = \frac{n}{|C_G(y)|}$ be as in Lemma 1. If one can prove, by elementary arguments, that there is always such an element y with $s_y = 1$, then one would get an inductive approach to the Frobenius–Thompson theorem. For then, $F = C_G(y)$ and $Y = \langle y^G \rangle$ are normal subgroups of G, with Y in the centre of F. Either $Y = F$ or G/Y is a Frobenius group with kernel F/Y. Observe that

$$s = \frac{n-1}{|H|} = \sum_y s_y$$

when y varies over a set of representatives for the conjugacy classes of G contained in $F^\sharp$. The greatest common divisor of these s_y is 1 since they divide n whereas s is a divisor of $n-1$. Hence $s_y = 1$ for all y if $s = 1$ or 2 (see Lemma 0), and there is y with $s_y = 1$ if $s \leq 2 + \sqrt{n+1}$ by our theorem (and in general by the Frobenius–Thompson theorem).

(2) Assuming that $|H|$ is odd (in view of Lemma 0) the proof for the Frobenius theorem is readily reduced to the case where H is a maximal subgroup of G. (Otherwise we get a Frobenius group G_0 which is a proper subgroup of G having the Frobenius complement H and the kernel $F_0 \subset F$. By induction, F_0 is a normal subgroup of G_0 and so H solvable (metacyclic) as it acts freely on the group F_0.) So let G be primitive. Then the Frobenius–Thompson theorem implies that F is an elementary abelian p-group for some prime p on which

H acts irreducibly (and freely). This can be deduced from our theorem in the cases where $|H| \geq \frac{n-1}{2+\sqrt{n+1}}$ (e.g. when $|H| \geq \sqrt{n-1}$). $< 3 + \sqrt{n+1}$.

(3) Bounding the rank of the Frobenius group G gives rise to an upper bound on the number of primes dividing the degree n of G. This is clear from the proof of the theorem. In fact, let $n = \prod_{i=1}^{t} p_i^{a_i}$ with $t \geq 2$ distinct prime divisors. By Lemma 3, we have $|H| \leq p_i^{a_i} - 1$ for each i. We obtain the crude estimate $|H|^t \leq \prod_{i=1}^{t}(p_i^{a_i} - 1) < n - 1$. Hence, if $|H| \geq (n-1)^{\frac{1}{t}}$, then n is divisible by at most $t - 1$ distinct primes. We have $|H| \geq (n-1)^{\frac{1}{t}}$ if and only if $\mathrm{rk}(G) \leq 1 + (n-1)^{\frac{t-1}{t}}$.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

[1] Dixon, J.D., Mortimer, B.: Permutation Groups. Springer, Berlin (1996)

[2] Feit, W.: On a class of doubly transitive permutation groups. Illinois J. Math. **4**, 170–186 (1960)

[3] Ferguson, P.A.: On a problem of Frobenius. J. Algebra **56**, 436–456 (1979)

[4] Frobenius, G.: Über auflösbare Gruppen IV. Sitz. Akad. Wiss. Berlin, 1216–1230 (1901)

[5] Frobenius, G.: Über einen Fundamentalsatz der Gruppentheorie II. Berliner Ber., 428–437 (1907)

[6] Hall, P.: On a theorem of Frobenius. Proc. Lond. Math. Soc. **40**, 468–501 (1936)

[7] Hall, M.: The Theory of Groups. MacMillan Company, New York (1959)

[8] Huppert, B.: Endliche Gruppen I. Springer, Berlin (1967)

[9] Huppert, B., Blackburn, N.: Finite Groups III. Springer, Berlin (1982)

[10] Isaacs, I.M., Robinson, G.R.: On a theorem of Frobenius: solutions of $x^n = 1$ in finite groups. Amer. Math. Mon. **99**, 352–354 (1992)

[11] Knapp, W., Schmid, P.: A note on Frobenius groups. J. Group Theory **12**, 393–400 (2009)

[12] Knapp, W., Schmid, P.: Some generalized characters associated to a transitive permutation group. J. Group Theory **23**, 393–397 (2020)

[13] Speyer, D.E.: A counting proof of a theorem of Frobenius. Amer. Math. Mon. **124**, 357–359 (2017)

[14] Suzuki, M.: Finite groups with nilpotent centralizers. Trans. Amer. Math. Soc. **99**, 452–470 (1961)

[15] Tao, T.C.: A Fourier-analytic proof of Frobenius' theorem. WordPress, Monthly Archive for May 2013

[16] Thompson, J.G.: Finite groups with fixed point free automorphisms of prime order. Proc. Nat. Acad. Sci. US **45**, 578–581 (1959)

Wolfgang Knapp and Peter Schmid
Mathematisches Institut der Universität Tübingen
Auf der Morgenstelle 10
72076 Tübingen
Germany
e-mail: `wolfgang.knapp@uni-tuebingen.de`

Peter Schmid
e-mail: `peter.schmid@uni-tuebingen.de`