ON A CONJECTURE OF FROBENIUS

NOBUO IYORI AND HIROYOSHI YAMAKI

ABSTRACT. Let $G$ be a finite group and $e$ be a positive integer dividing the order of $G$. Frobenius conjectured that if the number of elements whose orders divide $e$ equals $e$, then $G$ has a subgroup of order $e$. We announce that the Frobenius conjecture has been proved via the classification of finite simple groups.

Let $G$ be a finite group and $e$ be a positive integer dividing $|G|$, the order of $G$. Let $L_e(G) = \{x \in G | x^e = 1\}$. In 1895 Frobenius [4] proved the following result:

$$|L_e(G)| = ke$$

for an integer $k \geq 1$

and he made the following conjecture.

Frobenius conjecture. If $k = 1$, then the $e$ elements of $L_e(G)$ form a characteristic subgroup of $G$, that is, a subgroup of $G$ that is invariant under the automorphism group of $G$.

If the $e$ elements of $L_e(G)$ form a subgroup, then $L_e(G)$ is necessarily a characteristic subgroup by the definition of $L_e(G)$. If $e$ is a power of a prime, the conjecture is true by Sylow's theorem. M. Hall [6] gives a proof of the conjecture when $G$ is solvable. It is proved by Zemlin [16] that the minimal counterexample to the conjecture is a nonabelian simple group. The purpose of this note is to announce the following

Theorem. The conjecture of Frobenius is always true.

Because of the classification of finite simple groups we may assume that $G$ is isomorphic with

1. $A_n$ ($n \geq 5$), the alternating group on $n$ letters,
2. a simple group of Lie type, or
3. one of the twenty-six sporadic simple groups.
We refer to [11] for the alternating groups, [7, 8, 11, 15] for the simple groups of Lie type and [14] for the sporadic simple groups. In order to verify the conjecture two lemmas play crucial role.

**Lemma 1** [10, 11, 16]. Let $G$ be a finite group and $e$ be a positive integer dividing $|G|$. Assume that $e = |L_e(G)|$. If $p$ is a prime divisor of $e$ and $|G|/e$, then Sylow $p$-subgroups of $G$ are cyclic, generalized quaternion, dihedral, or quasidihedral.

**Lemma 2** [11, 15]. Let $G$ be a finite simple group and $S$ be a nilpotent Hall $n$-subgroup of $G$. Suppose that $S$ is disjoint from its distinct conjugates and $C_G(x)$ is contained in $SC_G(S)$ for all $x$ in $S^4$. If $e$ is minimal such that $e = |L_e(G)|$ divides $|G|$ and $e > 1$, then $|S|$ divides either $e$ or $|G|/e$.

**Remark.** We apply this lemma only when $S$ is abelian. Basic idea of the proof can be found in [15]. Let $e$ be minimal such that $e = |L_e(G)|$ divides $|G|$ and $1 < e < |G|$. Since $G$ is simple we have to prove that there exists no such $e$.

Suppose that there exists a prime $p$ that divides both $e$ and $|G|/e$. Let $P$ be a Sylow $p$-subgroup of $G$. If $p = 2$, then $P$ is dihedral or quasidihedral by Lemma 1 and $G$ is isomorphic with $A_7$, $M_{11}$, $L_2(q)$, $q \equiv 1(2)$, $q > 3$; $L_3(q)$, $q \equiv -1(4)$; or $U_3(q)$, $q \equiv 1(4)$ (see [5]). By [7, 11, 14, 15] the conjecture holds for these simple groups. If $p$ is an odd prime, then $P$ is cyclic by Lemma 1. Blau [1] yields that $P$ is disjoint from its distinct conjugates since $G$ is simple. Let $x$ be a nontrivial element of $P$. Then $C_G(x)$ is $p$-closed and every $p'$-element acts trivially on $\Omega_1(P)$. It follows that $C_G(x) = C_G(P)$. However Lemma 2 implies that $|P|$ divides either $e$ or $|G|/e$, which is a contradiction by the choice of $p$. It follows that $e$ is a Hall divisor of $|G|$, that is, $(e, |G|/e) = 1$. In order to illustrate briefly our proof we consider the cases that $G = E_7(q)$, the simple Chevalley group of type $E_7$ and $G = P\Omega_{2m}(-1, q)$, the orthogonal simple group with nonmaximal Witt index (see [7, 8]).

Let $G$ be a simple Chevalley group $E_7(q)$. By [2] $G$ contains Hall abelian subgroups $H$ in a maximal torus $T(E_7)$ and $K$ in a maximal torus $T(E_6(a_1))$ such that $|H| = (q^6 - q^3 + 1)(3, q+1)^{-1}$, $|K| = (q^6 + q^3 + 1)(3, q - 1)^{-1}$, $(N_G(H) : C_G(H)) = (N_G(K) : C_G(K)) = 18$, $|C_G(h)| = (q^6 - q^3 + 1)(q + 1)$, $h \in H^2$ and
\(|C_G(k)| = (q^6 + q^3 + 1)(q - 1), \ k \in K^d (\text{see also [9, 13]}). \ H \text{ and } K \text{ satisfy the condition of Lemma 2. It follows that either } L_e(G) \text{ contains all conjugates of } H \text{ or not and either } L_e(G) \text{ contains all conjugates of } K \text{ or not. Now we have four possibilities: (i) } e \equiv 0(|H||K|), \text{ (ii) } e \equiv 0(|H|) \text{ and } (e, |K|) = 1, \text{ (iii) } e \equiv 0(|K|) \text{ and } (e, |H|) = 1, \text{ (iv) } (e, |H||K|) = 1. \text{ Case (ii)} (\text{resp. case (iii)}) \text{ yields that } e = |L_e(G)| > |G|/19(q + 1) \text{ (resp. } e > |G|/19(q - 1)), \text{ a contradiction. Case (iv)} \text{ cannot happen since } G \text{ contains } (|G|^2 - q^{126} \text{ unipotent elements by [12].} \text{ In case (i)} \text{ let } \pi = (q - 1, |G|/e) \text{ and } \rho = (q + 1, |G|/e). \text{ If } \pi = 1 \text{ or } \rho = 1, \text{ then } e > |G|/20. \text{ This is impossible since } e \text{ is a Hall divisor of } |G|. \text{ If } \pi \neq 1 \neq \rho, \text{ the counting arguments, which are slightly more complicated than those of [15], yield that } e = |L_e(G)| > |G|/15 \text{Max}\{\pi, \rho\}. \text{ Now we can prove } e > |G|/11. \text{ This is a contradiction since } e \text{ is a Hall divisor of } |G|. \text{ This implies that } e = 1 \text{ or } e = |G|. \text{ Let } G \text{ be the orthogonal simple group } P\Omega_{2m}(-1, q). \text{ If } q = 2 \text{ and } m = 4 \text{ or } 5, \text{ then the conjecture holds by [3]. Thus we assume that } G \neq P\Omega_8(-1, 2), P\Omega_{10}(-1, 2). \text{ By [2] } G \text{ contains a torus } T(C_{m-i}) \text{ (}0 \leq i \leq [m/2]) \text{ of order } (q^m + 1)(q^m + 1, 4)^{-1} \text{ or } (q^{m-i} + 1) \text{ (see also [9, 13]). Let } g_j(q) = (q^j + 1, \prod_{k|j}(q^k + 1)^N) \text{ for a sufficiently large integer } N. \text{ Let } h_j(q) = (q^j + 1)/g_j(q). \text{ } T(C_{m-i}) \text{ contains a Hall subgroup } H_{m-i} \text{ (}0 \leq i \leq [m/2]) \text{ in } G \text{ with } h_{m-i}(q) = |H_{m-i}| \text{ and } C_G(H_{m-i}) \supseteq T(C_{m-i}). \text{ } H_{m-i} \text{ satisfies the condition of Lemma 2. It follows that either } L_e(G) \text{ contains all conjugates of } H_{m-i} \text{ or not. We note that } (N_G(H_m) : C_G(H_m)) \text{ divides } 2m. \text{ The counting arguments for } E_7(q) \text{ can be piled up using } H_{m-i}. \text{ If } h_m(q) \text{ divides } e, \text{ then } e = |L_e(G)| > (|H_m| - 1)|K|(G : N_G(H_m))/\nu \text{ where } C_G(H_m) = H_m \times K \text{ and } \nu = (|K|, |G|/e). \text{ We can easily get a contradiction, which yields that } h_m(q) \text{ divides } |G|/e. \text{ We can successfully prove that } e \text{ is a power of } 2 \text{ if } q \text{ is odd and } e = 1 \text{ if } q \text{ is even by the similar counting arguments. This contradiction shows that } e = 1 \text{ or } e = |G|. \text{ ACKNOWLEDGMENT} \text{ Both authors would like to thank the anonymous referees for suggestions that helped make the paper clearer and more readable.}
REFERENCES


Institute of Mathematics, University of Tsukuba, Ibaraki, 305 Japan