ON P. HALL'S GENERALISATION OF A THEOREM OF FROBENIUS

by S. K. SEHGAL

(Received 20 July, 1960)

1. It is a well known theorem due to Frobenius that the number of solutions of the equation

$$x^n = 1$$

in a finite group G is a multiple of the greatest common divisor (n, g) of n and the order g of G. Frobenius himself proved later that the number of solutions of the equation

$$x^n = a,$$

where a is a fixed element of G, is a multiple of (n, g_a), g_a being the order of the centralizer $Z(a)$ of a in G.

P. Hall generalised the equation to an arbitrary system of general word equations in x and $a_1, \ldots, a_m$, where $a_1, \ldots, a_m$ are fixed elements of G, and found a modulus even better than the most natural generalisation of the above [1].

Following Hall's arguments we plan here to generalise the systems of equations to an arbitrary system of equations in n variables.

I wish to thank Professor Hans Zassenhaus for his aid in the preparation of this paper.

2. Let $f(x_1, \ldots, x_n;\ a_1, \ldots, a_r) = 1$ be a word equation in variables $x_1, \ldots, x_n$ and constants $a_1, \ldots, a_r$. By the *degree in x_i of f* we mean the absolute value of the sum of the exponents of x_i in f.

Let H be a subgroup of G and let k be a natural number. We define the function $m = m(G, H, k)$ of Hall to be the greatest of the numbers m_1, m_2, m_3 in so far as these are defined; where

(i) If G is finite and the Sylow p-subgroups of G are regular, then $m_1 = \rho_k$ where p^{ρ_k} is the order of $\Omega_k(J)$ and J is a Sylow p-subgroup of H. $\Omega_k(G) = \{g \in G \mid g^{p^k} = 1\}$;

(ii) if J is regular, then $m_2 = \min_{j=0}^{k}(\rho_j + p^{k-j} - 1)$;

(iii) in any case, $m_3 = \min(\rho_k, k(p-1))$ or $k(p-1)$ according as the solutions of $x^{p^k} = 1$ in J form a subgroup $\Omega_k(J)$ of order p^{ρ_k} or do not form a subgroup.

THEOREM. *Let G be a group. Let $f, g \ldots$ be a system of words in the symbols $x_1, x_2, \ldots, x_n$; $a_1, a_2, \ldots$, where the x_i are unknowns and the a_i are fixed elements of G. Let p be a prime and suppose that p^{k_i} divides the degree in x_i of each of the words $f, g, \ldots$ $(1 \leqq i \leqq n)$.*

Let H be a finite subgroup of the centralizer of the a_i in G and let $s_1, \ldots, s_n$ be given elements of G. Then the number of solutions $(x_1, \ldots, x_n)$ of the equations

$$f = g = \ldots = 1$$

for which $x_i \in Hs_iH$ $(1 \leqq i \leqq n)$ *is divisible by* p^m, *where* $m = m(G, H, k)$ *is the function of Hall and* $k = \max(k_1, \ldots, k_n)$.

We observe that by taking $n = 1$ we get Hall's result.

3. Proof of the theorem.

3.1. We shall use induction on the order $O(H)$ of H. When $O(H) = 1$, $m = 0$ and the result is clear. When H is not a p-group, we have $O(J) < O(H)$ and $m(G, J, k) = m(G, H, k)$.

Also, every double coset Hs_iH is then the union of a certain number of double cosets of J. So the result follows by induction. We therefore suppose that H is a p-group.

Since G can be embedded in a larger group in which H is a centralizer [**1,** p. 486], we may suppose that H is the centralizer of the a_i in G.

3.2. Any one of the words $f, g, \ldots$ may be written in the form $u_1v_1u_2v_2 \ldots u_sv_s$, where each u_i is an x-word and each v_i is an a-word. This may be rewritten as

$$u_1u_2 \ldots u_sv_1^{u_2 \cdots u_s}v_2^{u_3 \cdots u_s} \ldots v_s.$$

The transforms $v_i^{u_{i+1} \cdots u_s}$ which occur here are of degree 0 in each x_j. Hence the degree in x_j of the x-word $u_1u_2 \ldots u_s$ is a multiple of p^{k_j}. Since the derived group of the group generated by the x_j is generated by the commutators $(x_i, x_j) = x_i^{-1}x_j^{-1}x_ix_j$ and their transforms, it follows that each of the words $f, g, \ldots$ can be expressed in the form

$$f = x_1^{\lambda_1 p^{k_1}}x_2^{\lambda_2 p^{k_2}} \ldots x_n^{\lambda_n p^{k_n}}f_1f_2,$$

where f_1 is a product of terms of the form

$$u^{-1}(x_i, x_j)u,$$

and f_2 is a product of terms of the form

$$u^{-1}a_j^{\pm 1}u.$$

u is an x-word which may vary from term to term.

3.3. We divide the solutions $(x_1, \ldots, x_n)$ of

$$f = g = \ldots = 1, \quad x_i \in Hs_iH \quad (1 \leqq i \leqq n) \tag{1}$$

into classes according to the values they give to the elements

$$x_i^{p^{k_i}}, \quad (x_i, a_j) \quad \text{and} \quad (x_i, x_j).$$

Consider the class for which

$$x_i^{p^{k_i}} = b_i, \quad (x_i, a_j) = c_{ij}, \quad (x_i, x_j) = e_{ij}, \tag{2}$$

where the b_i, c_{ij} and e_{ij} are fixed elements of G. Let K be the centralizer in H of these elements. If $K \neq H$, we say that the class is of the first kind; and if $K = H$, we say that it is of the second kind.

We shall prove that the number of solutions of each kind is divisible by p^m.

3.4. Consider a class of solutions of the first kind, for which $O(K) < O(H)$. The degree in x_i of each of the equations (2) is a multiple of p^{k_i}. From the induction hypotheses applied

to the system (1)+(2), it follows that the number of solutions of this system for which x_i lies in an assigned double coset of K $(1 \leqq i \leqq n)$ is a multiple of $p^{m'_1}$, where $m'_1 = m(G, K, k)$. Since Hs_iH is the union of a certain number of double cosets of K, the number of solutions in the given class will also be a multiple of $p^{m'_1}$. But for any solution $(x_1, \ldots, x_n)$ of (1) and any $h \in H$, $(x_1^h, \ldots, x_n^h)$ will also be a solution of (1). Transforming the solutions of the given class by the elements of H, we obtain $(H : K)$ disjoint classes each with the same number of members. So the solutions of the first kind fall into sets of classes and in each set the total number of solutions is a multiple of $p^{m'_1}(H : K)$. Since p^m divides $p^{m'_1}(H : K)$ [**1**, p. 489], we have proved that the number of solutions of the first kind is divisible by p^m.

3.5 Let us now consider a class of solutions of the second kind, for which $K = H$.

(*a*) We claim that, for any solution of this class, $x_i^{-1}Hx_i = H$ $(1 \leqq i \leqq n)$.

Since H is the centralizer of the a_j, $x_i^{-1}Hx_i$ will be the centralizer of the elements $x_i^{-1}a_jx_i$ $(j = 1, 2, \ldots)$. But H commutes elementwise with the (x_i, a_j) and therefore also with the $x_i^{-1}a_jx_i$. Since H is finite, it follows that $x_i^{-1}Hx_i = H$.

The double coset Hs_iH which contains x_i reduces to an ordinary coset $Hs_i = s_iH$.

(*b*) We prove next that the original equations (1) are now irrelevant. This is because every solution of (2) for which $x_i \in Hs_i$ $(1 \leqq i \leqq n)$ automatically satisfies (1) as well, so that the given class consists precisely of all such solutions of (2).

To see this, let $(x_1, \ldots, x_n)$ be any solution of (1), (2) and let $(x'_1, \ldots, x'_n)$ be any solution of (2) for which $x'_i = h_ix_i$ with $h_i \in H$ $(1 \leqq i \leqq n)$. Consider the effect of the substitution $x_i \to x'_i$ on one of the words f, which we take in the form given in §3.2. Since $x_i^{p^{k_i}} = (x'_i)^{p^{k_i}} = b_i$, the factors $x_i^{\lambda_i p^{k_i}}$ are unaffected. If u is any x-word and u' is the corresponding x'-word, we have $u' = hu$ for some $h \in H$, by (*a*). But $(x'_i, x'_j) = e_{ij} = (x_i, x_j)$ and h commutes with e_{ij}. Hence $(u')^{-1}(x'_i, x'_j)u' = u^{-1}(x_i, x_j)u$. Since h also commutes with a_j, we have

$$(u')^{-1}a_j^{\pm 1}u' = u^{-1}a_j^{\pm 1}u.$$

So the factors of f_1 and f_2 are also unaffected by the substitution. It follows that $(x'_1, \ldots, x'_n)$ is a solution of (1).

(*c*) We remark that the equations $(x_i, a_j) = c_{ij}$ of (2) are also irrelevant for the same reason, namely that $(x'_i, a_j) = (x_i, a_j)$.

3.6. We have now only to prove the following:

If the b_i and the e_{ij} centralize H and the s_i normalize H, then the number of solutions $(x_1, \ldots, x_n)$ of

$$x_i^{p^{k_i}} = b_i, \quad (x_i, x_j) = e_{ij}, \quad x_i \in Hs_i \quad (1 \leqq i, j \leqq n) \tag{3}$$

is divisible by p^m, where $m = m(G, H, k)$.

We take up the three cases of the definition of m separately and suppose without loss of generality that $k = k_n = \max(k_1, k_2, \ldots, k_n)$.

Case (i). Here G is finite and its Sylow p-subgroups are regular. We recall that, if $x^{p^k} = b$, where b commutes with every element of H, and $x^{-1}Hx = H$, then $(xh)^{p^k} = b$ for $h \in H$ if and only if $h \in \Omega_k(H)$ [**1**, pp. 490, 491]

Put two solutions of (3) in the same class if and only if there is an element $h_0 \in H$ such that $x'_i = h_0^{-1}x_ih_0$ $(1 \leqq i \leqq n-1)$. In the class containing a given solution $(x_1, \ldots, x_n)$, the

https://doi.org/10.1017/S2040618500034390 Published online by Cambridge University Press

first $n-1$ unknowns can be chosen in $(H : C)$ ways, where C is the centralizer of $x_1, \ldots, x_{n-1}$ in H. Fixing $x_1, \ldots, x_{n-1}$, we may replace x_n by hx_n with $h \in H$ if and only if $h \in \Omega_k(H)$ and $(x_i, x_n) = (x_i, hx_n)$ for $1 \leqq i \leqq n-1$, i.e. if and only if $h \in C \cap \Omega_k(H)$. Hence this class contains just

$$(H : C)(C \cap \Omega_k(H) : 1) = (H : C\Omega_k(H))(C\Omega_k(H) : C)(C \cap \Omega_k(H) : 1)$$
$$= (H : C\Omega_k(H))(\Omega_k(H) : 1) = p^{\rho_k}(H : C\Omega_k(H))$$

members and this number is a multiple of $p^{\rho_k} = p^{m_1}$.

Case (ii). Here $H = J$ is a regular p-group and there exists a normal subgroup M_m of H, of order p^{m_2}, such that $x_n{}^{p^k} = b_n$ implies that $(x_n h)^{p^k} = b_n$ for all $h \in M_n$. [**1**, p. 491]. The desired result now follows as in case (i), with M_m in place of $\Omega_k(H)$.

Case (iii). In the general case too, there exists a normal subgroup L_k of H, of order p^{m_3}, such that $x_n{}^{p^k} = b_n$ implies that $(x_n h)^{p^k} = b_n$ for all $h \in L_k$, [**1**, p. 492]. In this case the result follows by taking L_k in place of $\Omega_k(H)$.

COROLLARY 1. *The number of solutions* $(x_1, \ldots, x_n)$ *of*

$$f = g = \ldots = 1; \quad (x_i, x_j) = 1 \quad (1 \leqq i, j \leqq n)$$

with $x_i \in Hs_iH$ *is divisible by* p^m.

COROLLARY 2. *Suppose that* N_i *divides the degree in* x_i *of each of the words* $f, g, \ldots$ *and let* $N = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ *be the prime factorization of the l.c.m.* N *of the* N_i $(1 \leqq i \leqq n)$. *Then the number of solutions of* $f = g = \ldots = 1$ *with* $x_i \in Hs_iH$ $(1 \leqq i \leqq n)$ *is divisible by* $p_1^{m_1} \ldots p_r^{m_r}$, *where* $m_i = m(G, H, \alpha_i)$.

(This result was stated by A. N. Prokofyev [**2**].)

Here it is supposed as before that $s_1, \ldots, s_n$ are given elements of G and that H is a finite subgroup which commutes elementwise with all the constants a_j occurring in the given words.

I would like to express to the referee, Professor Philip Hall, my appreciation of his suggestions for the improvement of the presentation of this paper.

REFERENCES

1. P. Hall, On a theorem of Frobenius, *Proc. London Math. Soc.* **40** (1936), 468–501.

2. A. N. Prokofyev, On the fundamental theorem of Frobenius, *Doklady Akad. Nauk SSSR* (N.S.) **65** (1949), 801–804.

UNIVERSITY OF NOTRE DAME
NOTRE DAME, INDIANA, U.S.A.