JOURNAL OF ALGEBRA 7, 363-371 (1967)

On the Number of Sylow Subgroups in a Finite Group*

MARSHALL HALL, JR.

California Institute of Technology, Pasadena, California 91109

Received March 22, 1967

1. INTRODUCTION

If the order g of a finite group G is divisible by p^r but no higher power of the prime p, then the classical theorems of Sylow [7] assert that there are subgroups of order p^r, the Sylow p-subgroups, forming a single conjugate class in G, and that the number of these, n_p is of the form $n_p = 1 + kp$ for some integer $k \geqslant 0$. If G is solvable, it was shown by P. Hall [5] that n_p is a product of factors of the form q^t, where q is a prime and $q^t \equiv 1 \pmod{p}$. For a simple group X the number s_p of Sylow p-subgroups need not be of this form. It is shown in this paper (Theorem 2.2) that the number n_p of Sylow p-subgroups in any finite group G is a product of factors of the form (*1*) s_p, where there is a simple group X with s_p Sylow p-subgroups and (*2*) a power q^t of a prime q, where $q^t \equiv 1 \pmod{p}$, and that an arbitrary product of factors of these two kinds is the n_p of some finite group. Thus the n_p's form a semigroup. A quotient of two n_p's which is an integer need not be an n_p, since $LF(2.7)$ has eight Sylow 7-subrgoups and A_7 has 120 Sylow 7-subgroups, but no group has 15 Sylow 7-subgroups, a fact proved in Theorem 3.1.

Any odd number may be the number of Sylow 2-subgroups in a finite group. But for every prime $p > 2$, not every integer $n \equiv 1 \pmod{p}$ is the n_p of a finite group. In particular Theorem 3.2 shows that there is no finite group with $n_3 = 22$, $n_5 = 21$, or $n_p = 1 + 3p$ for $p \geqslant 7$. As with so many questions, the mysterious part as to the possible values for n_p lies in the study of the finite simple groups.

2. THE NUMBER OF SYLOW SUBGROUPS IN A GROUP

If a group G_1 has n_1 Sylow p-subgroups and a group G_2 has n_2 Sylow p-subgroups, then the direct product $G_1 \otimes G_2$ has $n_1 n_2$ Sylow p-subgroups,

* This research was supported in part by NSF grant GP 3909 and in part by ONR contract ONR N 00014-67-A-0094-0010.

namely the direct products of the Sylow p-subgroups in G_1 with those of G_2. Hence the integers n_p for which there exists a group G with n_p Sylow p-subgroups form a semigroup. We know that $n_p \equiv 1 \pmod{p}$ ([4], p. 45), but not every integer congruent to one modulo p is an n_p.

Let q be a prime different from p and let t be an exponent such that $q^t \equiv 1 \pmod{p}$. Then the linear substitutions $x \to xm + b$ over $GF(q^t)$ with $m \neq 0$, b elements of $GF(q^t)$ form a group G of order $q^t(q^t - 1)$. The additive subgroup $x \to x + b$ is elementary Abelian of order q^t and normal in G. The multiplicative group $x \to xm$ is cyclic of order $q^t - 1$. Here, as $p \mid q^t - 1$, a Sylow p-subgroup $S(p)$ will have the multiplicative subgroup in its normalizer, and we can easily show that this is its complete normalizer. Thus $| N_G(p) | = q^t - 1$ and $[G : N_G(p)] = q^t$, whence G has q^t Sylow p-subgroups Hence prime powers q^t congruent to one modulo p are among the numbers n_p. It has been shown by Philip Hall [5] that only products of such prime powers arise as n_p for a solvable group. Other values may arise in simple groups, as for example $n_5 = 6$ in A_5. Thus the totality of n_p's includes numbers which are products of two kinds of numbers: (*1*) s_p, the number of Sylow p-subgroups in a simple group X, and (*2*) q^t, where q is a prime and $q^t \equiv 1 \pmod{p}$. We shall show here that these are all the possible values for n_p.

LEMMA 2.1. *Let G have a normal subgroup K, and let P be a Sylow p-subgroup of G. Then $K \cap P$ is a Sylow p-subgroup of K and PK/K is a Sylow p-subgroup of G/K.*

Proof. As P is a Sylow p-subgroup of G it is *a fortiori* a Sylow p-subgroup of $P \cup K = PK$. Since $K \lhd G$, then $K \cap P \lhd P$ and by the isomorphism theorem $PK/K \cong P/K \cap P$. Hence if $P/K \cap P$ is of order p^r and $K \cap P)$ is of order p^s, then P is of order p^{r+s} and PK/K is a subgroup of G/K of order p^r and $K \cap P$ is a subgroup of K of order p^s. Since p^{r+s} is the highest power of p dividing the order of G it follows that PK/K is a Sylow p-subgroup of G/K and $K \cap P$ is a Sylow p-subgroup of K.

THEOREM 2.1. *Let G have a normal subgroup K and let P be a Sylow p-subgroup of G. Then if n_p is the number of Sylow p-subgroups in G, $n_p = a_p b_p c_p$ where a_p is the number of Sylow p-subgroups in G/K, b_p is the number of Sylow p-subgroups in K and c_p is the number of Sylow p-subgroups in $N_{PK}(P \cap K)/P \cap K$.*

Proof. By the second Sylow theorem ([4], p. 45) $n_p = [G : N_G(P)]$. Now, as K is normal in G, $N_G(PK) \supseteq N_G(P)\ K \supseteq N_G(P)$. Hence

$$n_p = [G : N_G(P)] = [G : N_G(PK)]\ [N_G(PK) : N_G(P)]. \tag{2.1}$$

In the factor group $H = G/K$, $P^* = PK/K$ is a Sylow p-subgroup and in G

the inverse image of $N_H(P^*)$ is $N_G(PK)$. But for a_p the number of Sylow p-subgroups in $H = G/H$ we have $a_p = [H : N_H(P^*)] = [G : N_G(PK)]$. Thus from 2.1,

$$n_p = a_p[N_G(PK) : N_G(P)]. \tag{2.2}$$

Now P is a Sylow p-subgroup of PK which is therefore of index prime to p in $N_G(PK)$. Hence the number of Sylow p-subgroups in $N_G(PK)$ is the same as the number of Sylow p-subgroups in PK. This means

$$[N_G(PK) : N_G(P)] = [PK : N_{PK}(P)], \tag{2.3}$$

and so substituting in (2.2),

$$n_p = a_p[PK : N_{PK}(P)]. \tag{2.4}$$

As K is normal in G and $N_{PK}(P) \geqslant P$, we have

$$\begin{aligned} &P \cup (N_{PK}(P) \cap K) = N_{PK}(P) \cap (P \cup K) = N_{PK}(P), \\ &P \cap (N_{PK}(P) \cap K) = P \cap K, \end{aligned} \tag{2.5}$$

where the first of these is an application of the modular law and the second is trivial. As $N_{PK}(P) \cap K \lhd N_{PK}(P)$, it follows that

$$[N_{PK}(P) : K \cap N_{PK}(P)] = [P : P \cap K]$$

and, from (2.5), that

$$[N_{PK}(P) : P] = [K \cap N_{PK}(P) : P \cap K]. \tag{2.6}$$

Also, since $[PK : P] = [K : P \cap K]$, we have

$$[PK : N_{PK}(P)] = [K : K \cap N_{PK}(P)]. \tag{2.7}$$

If an element $y \in K$, $y \in PK$ and $y^{-1}Py = P$ then

$$y^{-1}(P \cap K)y = y^{-1}Py \cap y^{-1}Ky = P \cap K.$$

Thus

$$N_K(P \cap K) = K \cap N_{PK}(P \cap K) \geqslant K \cap N_{PK}(P) \tag{2.8}$$

and so

$$[K : K \cap N_{PK}(P)] = [K : N_K(P \cap K)]\,[K \cap N_{PK}(P \cap K) : K \cap N_{PK}(P)]. \tag{2.9}$$

Here $[K : N_K(P \cap K)] = b_p$ is the number of Sylow p-subgroups in K. Substituting from (2.7) and (2.9) into (2.6), we have

$$n_p = a_p b_p [K \cap N_{PK}(P \cap K) : K \cap N_{PK}(P)] = a_p b_p c_p . \tag{2.10}$$

Let us write $G_1 = N_{PK}(P \cap K)$. As K is normal in G,

$$G_1 = N_{PK}(P \cap K) \geqslant N_{PK}(P) \geqslant P.$$

Thus

$$G_1 \cup K = N_{PK}(P) \cup K = P \cup K = PK.$$

By the normality of K,

$$[PK : K] = [G_1 : G_1 \cap K] = [N_{PK}(P) : N_{PK}(P) \cap K] = [P : P \cap K]. \tag{2.11}$$

From this it follows that

$$[PK : G_1] = [K : G_1 \cap K], \qquad [G_1 : N_{PK}(P)] = [G_1 \cap K : N_{PK}(P) \cap K]$$
$$[N_{PK}(P) : P] = [N_{PK}(P) \cap K : P \cap K]. \tag{2.12}$$

In particular,

$$c_p = [K \cap N_{PK}(P \cap K) : K \cap N_{PK}(P)] = [G_1 \cap K : N_{PK}(P \cap K)]$$
$$= [G_1 : N_{PK}(P)] = [G_1 : N_{G_1}(P)], \tag{2.13}$$

where since $N_{PK}(P) \subseteq G_1$ it follows that $N_{PK}(P) = N_{G_1}(P)$. Thus c_p is the number of Sylow p-subgroups in G_1. Since $P \cap K$ is a p-group normal in $G_1 = N_{PK}(P \cap K)$, it is contained in every Sylow p-subgroup of G_1, and so the number c_p of Sylow p-subgroups in G_1 is the same as the number of Sylow p-subgroups in $G_1/P \cap K = N_{PK}(P \cap K)/P \cap K$. This completes the proof of our theorem.

We can now give an exact description of the number of Sylow p-subgroups in any group.

THEOREM 2.2. *The number n_p of Sylow p-subgroups $S(p)$ in a finite group G is the product of factors of the following two kinds:* (1) *the number s_p of Sylow p subgroups in a simple group X; and* (2) *a prime power q^t where $q^t \equiv 1 \pmod{p}$.*

Proof. We proceed by induction on the order of G, the theorem being trivial if G is a p-group or of order prime to p. If G is simple there is nothing to prove as this is part (1) of the theorem. Hence we may suppose that G has a proper normal subgroup K. From Theorem 2.1, $n_p = a_p b_p c_p$ where a_p is the number of Sylow p-subgroups in G/K, b_p is the number of Sylow

p-subgroups in K and c_p is the number of Sylow p-subgroups in $N_{PK}(P \cap K)/P \cap K$ where P is a Sylow p-subgroup of G. If all three of these groups are of order less than G, then the theorem follows by induction. K and G/K are certainly of order less than G and so we must consider the case in which $G = N_{PK}(P \cap K)/P \cap K$. Here $P \cap K = 1$, which means that K is a p'-group (i.e., of order prime to p) and also $G \subseteq PK$ whence $G = PK$ and so $G/K \cong P$. Here if $|P| = p^r$ with $r > 1$ let P_1 be a subgroup of P of order p^{r-1} and so maximal and normal in P. If we now take $K_1 = KP_1$, we have $K_1 \lhd G$ and $P \cap K_1 = P_1 \supset 1$ and in application of Theorem 2.1 all three groups are of order less than G and our theorem holds by induction. We are left to consider cases in which P is of order p, and $K \lhd G$ with $[G : K] = p$, K a p'-group.

Let $P = \langle a \rangle$ with $a^p = 1$, and let $\alpha : x \to a^{-1}xa = x^a$ be the automorphism of K induced by conjugation by the element a. If $x \in N_{PK}(P) \cap K$, then $x^{-1}(a^{-1}xa) = (x^{-1}a^{-1}x)\, a \in P \cap K = 1$, and so $x^{-1}a^{-1}xa = 1$, $a^{-1}xa = x$. Thus $N_{PK}(P) \cap K = F$ where $F = F^a$ is the subgroup of K fixed by the automorphism α. Here $N_{PK}(P) = PF$. If PK has $n_p S(p)$'s then $n_p = [PK : PF] = [K : F]$. Hence if the order of K is $q_1^{e_1}q_2^{e_2} \cdots q_r^{e_r}$ and the order of F is $q_1^{f_1}q_2^{f_2} \cdots q_r^{f_r}$, then

$$n_p = q_1^{e_1-f_1}q_2^{e_2-f_2} \cdots q_r^{e_r-f_r}$$

and we must show $q_i^{e_i-f_i} \equiv 1 \pmod{p}$ for $i = 1, \ldots, r$. Let Q_1 be a Sylow q_i-subgroup of F. If Q_1 is a Sylow q_i-subgroup of K then $q^{e_i-f_i} = 1 \equiv 1 \pmod{p}$ and we have the desired result. Suppose Q_1 is not a Sylow q_i-subgroup of F (including the possibility $Q_1 = 1$). Then there is a group Q^* such that $[Q^* : Q_1] = q_i$ and $Q_1 \lhd Q^*$, and so $[N_K(Q_1) : Q_1] \equiv 0 \pmod{q_i}$. Now if $y^{-1}Q_1y = Q_1$, then since ${Q_1}^a = Q_1$ it follows that $(y^a)^{-1}Q_1y^a = Q$, and we conclude that $N_K(Q_1)^a = N_K(Q_1)$. Now any subgroup H of K, including K itself which admits the automorphism α, has a Sylow q_i-subgroup which admits α, since the number of $S_H(q_i)$'s (Sylow q_i-subgroups of H) is a divisor of the order of H and so not a multiple of p. As the automorphism α permutes the $S_H(q_i)$'s that it does not fix in cycles of length p, there must be at least one that α fixes.

In this way we may find a chain of q_i-subgroups, $Q_1 \subset Q_2 \subset \cdots \subset Q_s$, in which each Q_j is a Sylow q_i-subgroup of $N_K(Q_{j-1})$ and each Q_j is fixed by α, and finally $Q_s = Q$ is a Sylow q_i-subgroup of K. Since Q_1 is a Sylow q_i subgroup of F, the group fixed by α, there can be no larger subgroup of Q fixed by α, and so the $q_i^{e_i} - q_i^{f_i}$ elements of $Q - Q_1$ are permuted in cycles of length p, whence $q_i^{e_i} - q_i^{f_i} \equiv 0 \pmod{p}$ and so $q_i^{e_i-f_i} \equiv 1 \pmod{p}$, as we wished to prove. This completes the proof of our theorem.

3. Impossible Values for n_p

If $p = 2$ then every odd prime q satisfies $q \equiv 1 \pmod 2$ and so by Theorem 2.2 every odd number n is an n_2. More directly we may observe that if n is any odd number the dihedral group of order $2n$ has n $S(2)$'s. But for every other prime p, there are numbers $n \equiv 1 \pmod p$ that are not n_p's.

THEOREM 3.1. *If $n = 1 + rp$, with $1 < r < (p + 3)/2$ there is not a group G with $nS(p)$'s unless $n = q^t$ where q is a prime, or $r = (p - 3)/2$ and $p > 3$ is a Fermat prime.*

Proof. Since $1 < r < p$, we cannot have

$$n = 1 + rp = (1 + r_1 p)(1 + r_2 p) = n_1 n_2$$

with $n_1 > 1$, $n_2 > 1$. Hence by Theorem 2.2 if there is a group with $1 + rpS(p)$'s we either have $1 + rp = q^t$ or $1 + rp$ is the number of $S(p)$'s in a simple group X. Consider the case of a simple group X with $1 + rp$ $S(p)$'s. The representation of X on cosets of $N_G(p)$ is on $1 + rp < p^2$ letters. Here the representation of $S(p)$ is on orbits of length p or 1 and so $S(p)$ is elementary Abelian. If an $S(p)$ is of order p^2 or greater, if two distinct $S(p)$'s are P_1 and P_2 then the number of conjugates of P_2 under P_1 is $[P_1 : P_1 \cap P_2] < 1 + rp < p^2$. Hence $[P_1 : P_1 \cap P_2] = p$. Hence any two $S(p)$'s have a nontrivial intersection and as they are Abelian it follows from a theorem of Brodkey [3] that all $S(p)$'s have a common nontrivial intersection V. But then $1 \subset V \lhd X$, contrary to the fact that X is simple. Hence $S(p)$ is of order p.

Hence if g is the order of X, g is divisible by exactly the first power of p. By Brauer and Reynolds ([2], Theorem 2*), either $r = (p - 3)/2$ where $p = 2^m + 1 > 3$ is a Fermat prime and $X \cong LF(2, 2^m)$ or r has a representation

$$r = \frac{hup + u^2 + u + h}{u + 1} \tag{3.1}$$

with integers $h > 0$, $u > 0$. But as $r > hup/(u + 1) > hp/2$ and $r < (p + 3)/2$ we must have $h = 1$. If $h = 1$ and $u \geqslant 2$ then

$$r \geqslant \frac{up}{u + 1} + u \geqslant \frac{2p}{3} + 2 > \frac{p + 3}{2}.$$

Here $h = 1$ and $u = 1$ give $r = (p + 3)/2$. Hence with $r < (p + 3)/2$ the representation is not possible. This proves our theorem.

THEOREM 3.2. *There is no group G with $n_3 = 22$, with $n_5 = 21$, or with $n_p = 1 + 3p$ for $p \geqslant 7$.*

Proof. We prove the statements of the Theorems in reverse order. For $p \geqslant 7$ $1 < 3 < (p + 3)/2$ and Theorem 3.1 is applicable. Now $1 + 3p \equiv 0 \pmod 2$ and so if $1 + 3p$ is a prime power, it is a power of 2. Suppose $1 + 3p = 2^t$. Then t must be even. With $t = 2s$, $2^{2s} - 1 = 3p = (2^a - 1)(2^s + 1)$. Here $2^s - 1 = 1$ or 3 and so $s = 1$ or 2. But $2^2 - 1 = 3$ and $2^4 - 1 = 3.5$. Hence 2^t is of the form $1 + 3p$ only when $p = 5$. Thus Theorem 3.1 tells us that there is no group with $n_p = 1 + 3p$ for $p \geqslant 7$.

Suppose there is a group G with $n_5 = 21$. From Theorem 2.2 this is only possible if there is a simple group G with $21 S(5)$'s. The representation of G on $N(5) = N_G(S(5))$ is on 21 letters and so $S(5)$ is represented on orbits of 1 and 5 letters and so is elementary Abelian. By Brodkey [3] if the order of $S(5)$ is 5^2 or greater then all $S(5)$'s have a common non-trivial intersection which is normal in G, contrary to the simplicity of G. Hence $S(5)$ is of order 5. Then $| N(5) | = 5qw$, where $q = 2$ or 4 is the order of the automorphism induced in $S(5)$ in $N(5)$ and w is the order of a group $V(5)$ centralizing $S(5)$. By Brauer [1] the degrees z_i of the irreducible ordinary characters in the principal block $B_1(5)$ divide $q(1 + rp)$ in this case $2 \cdot 21 = 42$ or $4 \cdot 21 = 84$ and satisfy

$$z_i \equiv \delta_i = \pm 1 \pmod p \tag{3.2}$$

for the q nonexceptional characters $\zeta_1, \ldots, \zeta_q$ including the identity characters ζ_1 and

$$z_0 \equiv -\delta_0 q \equiv \pm q \pmod p \tag{3.3}$$

for the $(p - 1)/q$ p-conjugate exceptional characters, if $q \neq p - 1$. If $q = p - 1$, the character ζ_0 is not exceptional.

$$\delta_0 z_0 + \delta_1 z_1 + \cdots + \delta_q z_q = 0. \tag{3.4}$$

Here the δ's are ± 1 and for $i = 1, \ldots, q$ $\zeta_i(b) = \delta_i$ where b is a generator of $S(p)$. As G is simple the only character of degree 1 is the identity character ζ_1. For $q = 2$ the only divisors of 42 satisfying the conditions (3.2), (3.3) and (3.4) are

$$\delta_1 z_1 = 1, \qquad \delta_2 z_2 = 6, \qquad \delta_0 z_0 = -7. \tag{3.5}$$

For $q = 4$ the only divisors of 84 satisfying the conditions are

$$\delta_0 z \delta = 21, \qquad \delta_1 z_1 = 1, \qquad \delta_2 z_2 = -14, \qquad \delta_3 z_3 = -14, \qquad \delta_4 z_j = 6 \tag{3.6}$$

or

$$\delta_0 z_0 = 21, \qquad \delta_1 z_1 = 1, \qquad \delta_2 z_2 = -14, \qquad \delta_3 z_3 = -4, \qquad \delta_4 z_4 = -4. \tag{3.7}$$

Since in all three cases there is a character of degree less than $2p + 1 = 11$, it follows from Lemma 4 of Stanton [6] that $S(5)$ must be its own centralizer and so $w = 1$. Hence for $q = 2$ the order of G is $21 \cdot 10 = 210$. But it is well known [4, p. 204] that there is no simple group whose order if divisible by 2 but not by 4. Thus $q = 2$ is impossible. If $q = 4$, $w = 1$ then G is of order 420. But, from (3.6) or (3.7), G has an irreducible character of degree 21 and, since $21^2 = 441 > 420$, this leads to a conflict, because the sum of the squares of the degrees of the irreducible characters of a group is its order. Hence there is no simple group with 21 $S(5)$'s and so, from Theorem 2.2, no group with $n_5 = 21$.

Finally let us suppose there is a group G with $n_3 = 22$. Since 22 does not have a proper factorization of the form $(1 + 3r)(1 + 3s)$ and is not a prime power, it follows from Theorem 2.2 that if there is such a group, then there is a simple group G with $n_3 = 22$. Here $[G : N(3)] = 22$. If there were a subgroup H with $G \supset H \supset N(3)$ as $22 = 2 \cdot 11$, then either $[G : H] = 2$ and H is normal in G, contrary to the simplicity of G, or $[H : N(3)] = 2$ and $N(3)$ is normal in H. This too is a conflict, since the normalizer of a Sylow subgroup is its own normalizer ([4], p. 46). Hence the representation of G on the 22 cosets of $N(3)$ is primitive. Since $22 = 2 \cdot 11$ and $22 \neq a^2 + 1$, it follows from Wielandt [8] that a primitive group on 22 letters is doubly transitive. Here G_1 the subgroup of G fixing a letter is $N(3)$. As $N(3)$ is transitive on 21 letters it follows that every orbit of $S(3)$ on the 21 letters is of the same length. Hence every orbit length of $S(3)$, being a power of 3 dividing 21, is 3 and it follows that $S(3)$ is elementary Abelian. If G permutes 1, 2,..., 22, for each $i = 1,..., 22$ there is exactly one $S(3)$ fixing i. As the orbits are of length 3 the $S(3)$ fixing i has a subgroup of index 3 fixing a further letter j, and so contained in the jth $S(3)$. Hence if $S(3)$ is of order 3^t with $t \geqslant 2$ any two $S(3)$'s have a non-trivial intersection and so by Brodkey [3] all $S(3)$'s intersect in a group of order 3^{t-1}, which is normal in G, a conflict since G is simple. Hence $S(3)$ is of order 3. By Brauer [1], the degrees of the characters in the principal block $B_1(3)$ are divisors z_0, z_2 of $2 \cdot 22 = 44$ such that $1 + \delta_0 z_0 + \delta_2 z_2 = 0$. But no such degrees with $z_0 > 1$, $z_2 > 1$ exist. Hence we have reached a final conflict and conclude that there is no simple group with 22 $S(3)$'s and so by Theorem 2.2, no group with $n_3 = 22$. This finishes the proof of our theorem.

We note in passing that A_5 has $n_5 = 6$ and $n_3 = 10$. Also $n_5 = 11$ and $n_5 = 16$ are prime powers, while $n_3 = 4, 7, 13, 16, 19$ are prime powers and so, for $p = 5$ and $p = 3$, respectively, 21 and 22 are the smallest numbers $n \equiv 1 \pmod{p}$ which are not n_p's.

References

1. Brauer, R. On Groups whose order contains a prime number to the first power. I. *Am. J. Math.* **64** (1942), 401-420.
2. Brauer, R. and Reynolds, W. F. On a problem of E. Artin. *Annals Math.* **68** (1958), 713-720.
3. Brodkey, J. S. A Note on finite groups with an Abelian Sylow group. *Proc. Am. Math. Soc.* **14** (1963), 132-133.
4. Hall, Marshall, Jr. "The Theory of Groups." Macmillan, New York, 1959.
5. Hall, Philip A note on soluble groups. *J. London Math. Soc.* **3** (1928), 98-105.
6. Stanton, R. G. The Mathieu Groups. *Canadian J. Math.* **3** (1951), 164-174.
7. Sylow, L. Théorèmes sur les groupes de substitutions. *Math. Ann.* **5** (1872), 584-594.
8. Wielandt, H. Primitive Permutations, gruppen vom Grad 2p. **63** (1956), 478-485.