CATEGORY THEORY
SYLOW'S THEOREM

PAUL L. BAILEY

1. p-Groups

Definition 1. Let p be a prime integer. A *p-group* is a group such that the order of every element is a power of p.

Proposition 1. *Let G be a finite group and let p be a prime integer. Then G is a p-group if and only if $|G| = p^n$ for some $n \in \mathbb{N}$.*

Proof.

($\Rightarrow$) Suppose that $|G|$ is not a power of p. Then $q||G|$ for some prime $q \neq p$. Then by Cauchy's Theorem, G has an element of order q. Thus G is not a p-group.

($\Leftarrow$) Suppose that $|G| = p^n$ and let $g \in G$. Then by Lagrange's Theorem, the order of g divides p^n. Since p is prime, $\text{ord}(G) = p^m$ for some $m \leq n$. □

Proposition 2. *Let G be a finite p-group. Then G has a nontrivial center.*

Proof. We know that $|G| = p^n$ for some $n \in \mathbb{N}$.

Let G act on itself by conjugation. Then G is partitioned into disjoint orbits, and the order of G is the sum of the cardinalities of these orbits. The set of fixed points of this action is the center of G, so the order of G is equal to the order of $Z(G)$ plus the sum of the cardinalities of the nonsingleton orbits.

For $g \in G$, the stabilizer of g is $C_G(g)$. There is a correspondence between the points in $\text{orb}(g) = g^G$ and the cosets of $\text{stb}(g) = C_G(g)$ in G. This gives us the class equation

$$|G| = |Z(G)| + \sum [G : C_G(g)],$$

where the sum is taken over a set of representatives of the conjugacy classes of the noncentral elements of G.

Now p divides $|G|$ and p divides $[G : C_G(g)]$ for each $g \in G$; thus p divides $|Z(G)|$, and $Z(G)$ is nontrivial. □

Date: March 29, 1996.

2. Lifting

Proposition 3. *Let $\phi : G \to H$ be a group epimorphism with kernel K. Let $L \leq H$. Suppose that K has order n and L has order m. Then $\phi^{-1}(L)$ is a subgroup of G containing K of order mn. We call this subgroup the* lift *of L.*

Proof. Let $M = \phi^{-1}(L)$. That M is closed under multiplication and inverses is immediate from the fact that ϕ is a homomorphism, as is the fact that M contains K. So $|M| = |K|[M : K]$. But since $M/K \cong L$, $[M : K] = |L|$. □

Definition 2. Let $p \in \mathbb{N}$ be a prime integer. A *Sylow p*-subgroup of a group G is a maximal p-subgroup of G.

Lemma 1. *Let G be a group of order p^r where p is prime. Then for $s \in \mathbb{N}$, $0 \leq s \leq r$, G contains a subgroup of order p^s.*

Proof. Let $s = r - 1$ It suffices to show that G contains a subgroup of order p^s, for then it will have a subgroup of order p^{s-1} and so forth.

Since G has a nontrivial center, let g be a central element of order p and let $H = \langle g \rangle$. Then G/H is a group of order p^s and by induction has a subgroup of order p^{s-1}. Lifting this subgroup back to G yields a subgroup in G of order p^s. □

3. Sylow's Theorem

Theorem 1. *Let G be a finite group of order $p^r m$ where $p, m, r \in \mathbb{N}$, p is prime, and p^r is the maximum power of p which divides G. Then*

1. *for any $s \in \mathbb{N}$, $0 \leq s \leq r$, G contains a subgroup of order p^s;*
2. *the p-Sylow subgroups of G are conjugate;*
3. *the number of p-Sylows is congruent to 1 modulo p;*
4. *the number of p-Sylows divides m.*

Proof. By the lemma, to prove (1) it suffices to show that G contains a subgroup of order p^r.

Suppose that G has a nontrivial subgroup H whose index in G is relatively prime to p. Then p^r divides the order of H and by induction, H contains a subgroup of order p^r.

Thus we assume that for every subgroup H of G we have $p|[G : H]$. Let G act on itself by conjugation. Then

$$|G| = |Z(G)| + \sum [G : C_G(g)],$$

and p must divide the order of $Z(G)$. Now let g be a central element of order p whose existence is guaranteed by Cauchy's Theorem. Let $H = \langle g \rangle$. Then p^{r-1} divides the order of G/H, so by induction, G/H has a subgroup of order p^{r-1}. Lifting this subgroup back to G yields (1).

To prove (2) and (3), let P be a p-Sylow subgroup of G whose existence is guaranteed by (1).

First we claim that the only p-Sylow which normalizes P is P itself. Let Q be another p-Sylow subgroup of G and suppose that $Q \leq N_G(P)$. Then $P \lhd QP$ and since $QP/P \cong Q/(Q \cap P)$, we have that

$$|QP||Q \cap P| = |P||Q|.$$

Thus QP is a p-group, and by maximality we must have $Q = P$.

Next we show that the number of p-Sylows conjugate to a given p-Sylow is not divisible by p. Let $\mathcal{S}$ be the set of p-Sylow subgroups of G which are conjugate to P. Note that G acts transitively on $\mathcal{S}$ by conjugation. Since $N_G(P)$ is the stabilizer of P under this action, we have $[G : N_G(P)] = |\mathcal{S}|$. But since $P \leq N_G(P)$, p^r divides $N_G(P)$ and so p does not divide $[G : N_G(P)]$, that is, p does not divide $|\mathcal{S}|$.

Now let Q be another p-Sylow subgroup of G and let Q act on $\mathcal{S}$ by conjugation. Then $|\mathcal{S}|$ is equal to the number of fixed points of this action plus the sum of the sizes of the orbits of the nonfixed points. The stabilizer of this action on $R \in \mathcal{S}$ is $N_Q(R)$; thus these orbits have cardinality $[Q : N_Q(R)]$. But $|Q| = p^r$ so p divides $[Q : N_Q(R)]$ if R is not fixed, that is, unless Q normalizes R. Thus p divides the sum of the sizes of the orbits of the nonfixed points, and since p does not divide $|\mathcal{S}|$, some point must be fixed.

However, the only p-Sylow fixed by the action of Q is Q itself. Thus $Q \in \mathcal{S}$, proving (2). That Q is the only fixed point proves (3).

To prove (4), note that $\mathcal{S}$ is the set of p-Sylow subgroups of G by (2). Then $|\mathcal{S}| = [G : N_G(P)]$ divides $|G| = p^r m$; since p does not divide $[G : N_G(P)]$, then $[G : N_G(P)]$ divides m. This proves (4). □

4. An Application of Sylow Theorem

We will show that all groups of order < 60 are solvable.

First note that this is equivalent to showing that there are no nonabelian simple groups of order < 60.

Suppose that there are no non-abelian, simple groups of order < 60. If the order of G is less than 60, then it is either abelian and hence solvable, or has a normal subgroup H. Then by induction, both G/H and H are solvable, so G is solvable.

On the other hand, suppose that all groups of order < 60 are solvable. Then each one has a normal series with abelian factors. If it is simple, it must be abelian.

We proceed with a sequence of lemmas. If p is a prime which divides the order of a group, let s_p denote the number of p-Sylows in that group.

Lemma 2. *If p is a prime, then a group of order p is cyclic, and thence abelian.*

Lemma 3. *If p is a prime, then a group of order p^2 is abelian.*

Proof. Since G is a p-group, it has a nontrivial center. Then $\overline{G} = G/Z(G)$ has order either p or 1. Suppose $|\overline{G}| = p$. Then $\overline{G}$ is cyclic. Let $\overline{g}$ generate $\overline{G}$. Let $a, b \in G$. Let $\overline{a} = \overline{g^m}, \overline{b} = \overline{g^n}$. That is, $a = g^m z_1$ and $b = g^n z_2$ for some $z_1, z_2 \in Z(G)$. Then $[a, b] = [g^m, g^n] = 1$.

This actually shows that any group of the form central by cyclic is abelian. □

Lemma 4. *Every p-group is solvable.*

Lemma 5. *If p and q are two primes then a group of order pq cannot be simple.*

Proof. Let s_p be the number of Sylow p-subgroups of a group G. By Sylow's Theorem, $s_p \cong 1(p)$ and $s_p || G|$.

If $|G| = pq$, then by the second condition, $s_p = 1$ or q and $s_q = 1$ or p. Suppose that $s_p = q$ and $s_q = p$. Then $q \cong 1(p)$ and $p \cong 1(q)$. This says that $q = kp + 1$ and $p = lq + 1$, where k and l are positive. Thus $q = klq + k + 1$ and $q(1 - kl) = k + 1$. The left side must be positive, so $kl = 0$. Thus either k or l is zero, a contradiction.

Therefore, either $s_p = 1$ or $s_q = 1$. A unique Sylow subgroup is normal, so G is not simple. □

Lemma 6. *If p and q are two primes then a group of order p^2q cannot be simple.*

Proof. Let G be a group of order p^2q.

If $p = q$, then G is a p-group and has a nontrivial center, so G is nonsimple.

Next assume that $p > q$. Since $s_p | q$, $s_p = 1$ or $s_p = q$. Suppose that $s_p = q$. Then $s_p \cong 1(p)$, so $p | s_p - 1$. Thus $p \leq s_p - 1 < s_p = q$; but $p > q$, a contradiction. Thus $s_p = 1$ and the p-Sylow is normal.

Now assume that $q > p$. Since $s_q | p^2$, either $s_q = 1$, $s_q = p$, or $s_q = p^2$. If $s_q = 1$, we are done. Suppose $s_q = p$. Then $s_q \cong 1(q)$, so $q | s_q - 1$. Thus $q \leq s_q - 1 < s_q = p$; but $q > p$, a contradiction. Thus $s_p \neq q$.

Suppose that $s_q = p^2$. Then $q | p^2 - 1$, so $q | p + 1$ or $q | p - 1$. By the preceeding argument, we cannot have $q | p - 1$. Thus $q | p + 1$. Since $q > p$, $q = p + 1$. The only primes for which this is true are $p = 2$ and $q = 3$.

In this case, G has order 12 and $s_3 = 4$, so G contains 8 distinct elements of order 3. The other four elements of G must be a unique 2-Sylow; hence, G is nonsimple. □

Lemma 7. *Let p be prime where $p > m > 1$. A group of order $p^n m$ cannot be simple.*

Proof. Since $s_p | m$, $s_p = 1$ or $s_p | m$. Suppose that $s_p | m$. Then $s_p \leq m$. Then $s_p \cong 1(p)$, so $p | s_p - 1$. Thus $p \leq s_p - 1 < s_p \leq m$; but $p > m$, a contradiction. Thus $s_p = 1$ and the p-Sylow is normal. □

Lemma 8. *Let q be prime. A group of order $2q^n$ cannot be simple.*

Proof. If $q = 2$, then the group is a p-group. Otherwise, the q-Sylow has index 2 and is normal. □

Lemma 9. *Let q be prime. A group of order $3q^n$ cannot be simple.*

Proof. If $q = 3$, then the group is a p-group. Assume that $q \neq 3$.

Let G be a group of order $3q^n$ and let H be a Sylow q-subgroup of G. Let $X = G/H$ be the left coset space of H in G. Then $|X| = 3$. Since G acts on X by left multiplication, we have a homomorphism $G \mapsto S_3$.

Suppose that G is simple. Then this map in injective, so G is a subgroup of S_3. Since the order of G is $3q^n$, then $q = 2$, $n = 1$, and $G \cong S_3$. But S_3 is nonsimple, a contradiction. □

Lemma 10. *Let q be prime. A group of order $4q^n$ cannot be simple.*

Proof. If $q = 2$, then the group is a $p - group$. Assume that $q \neq 2$.

Let G be a group of order $4q^n$ and let H be a Sylow q-subgroup of G. Let $X = G/H$ be the left coset space of H in G. Then $|X| = 4$. Since G acts on X by left multiplication, we have a homomorphism $G \mapsto S_4$.

Suppose that G is simple. Then this map in injective, so G is a subgroup of S_4, and the order of G divides 24. Since the order of G is $4q^n$, then $q = 3$, $n = 1$ and G has order 12. Then G is a $p^2 q$ group and is nonsimple, a contradiction. □

Lemma 11. *A group of order 30 is not simple.*

Proof. Let G be a group of order 30. We have that $30 = 2 \cdot 3 \cdot 5$.

Suppose that G has no normal Sylow subgroups. Then $s_2 \geq 3$, $s_3 \geq 4$, and $s_5 \geq 6$. This gives us 3 elements of order 2, 8 elements of order 3, and 25 elements of order 5 for a total of at least 36 elements, a contradiction. □

Lemma 12. *A group of order 40 is not simple.*

Proof. Let G be a group of order 40. We have that $40 = 2^8 \cdot 5$.

Now $s_5 | 8$ so $s_5 \in \{1, 2, 4, 8\}$. Also $s_5 \cong 1(5)$ so $s_5 \in \{1, 6, 11, \dots\}$. This only possibility is $s_5 = 1$, so the 5-Sylow is normal. □

Lemma 13. *A group of order* 56 *is not simple.*

Proof. Let G be a group of order $56 = 2^3 \cdot 7$.

Now $s_7|8$ so $s_7 \in \{1, 2, 4, 8\}$. Also $s_7 \cong 1(7)$ so $s_7 \in \{1, 8, \dots\}$. Then either $s_7 = 1$, in which case the 7-Sylow is normal, or $s_7 = 8$.

Suppose that $s_7 = 8$. Then G contains 48 elements of order 7. The other 8 elements in G must form a unique 2-Sylow, which is normal. □

Order	Type	Order	Type	Order	Type
1	TRIV	21	pq	41	p
2	p	22	pq	42	pm
3	p	23	p	43	p
4	p^2	24	$3q^3$	44	p^2q
5	p	25	p^2	45	p^2q
6	pq	26	pq	46	pq
7	p	27	p^3	47	p
8	p^3	28	p^2q	48	$3q^4$
9	p^2	29	p	49	p^2
10	pq	30	pqr (*)	50	p^2q
11	p	31	p	51	p
12	p^2q	32	p^5	52	p^2q
13	p	33	pq	53	p
14	pq	34	pq	54	p^3m
15	pq	35	pq	55	pq
16	p^4	36	$4q^2$	56	p^3q (*)
17	p	37	p	57	p
18	p^2q	38	pq	58	pq
19	p	39	p	59	p
20	p^2q	40	p^3q (*)	60	SIMP

Department of Mathematics, University of California, Irvine
Email address: pbailey@math.uci.edu