Group actions and Sylow theorems

written by Night Shift in Math on Functor Network
original link: https://functor.network/user/854/entry/370

If a positive integer m divides the order of a finite group G, does G have a subgroup of order m? The answer is true for finite abelian groups, but it is not true for arbitrary groups. Sylow theorems discuss this situation when m is a prime power.

Before discussing Sylow theorems, we first discuss group actions.

Definition 1. *An action of a group G on a set S is a function $G \times S \to S$ denoted $(g, x) \mapsto gx$ such that $\forall x \in S, \forall g_1, g_2 \in G, ex = x$ and $(g_1 g_2)x = g_1(g_2 x)$. When such an action is given, we say that G acts on the set S.*

Let G is a group and $H \leq G$, the action of group H on the set G where $(h, x) \mapsto hx$ is the product on G is called a left translation. The action of H on G where $(h, x) \mapsto hxh^{-1}$ is called conjugation by h and the element hxh^{-1} is said to be a conjugate of x. If K is any subgroup of G and $h \in H$, $hKh^{-1} \cong K$. Thus H acts on the set S of all subgroups of G by conjugation $(h, K) \mapsto hKh^{-1}$. The group hKh^{-1} is said to be conjugate to K.

Lemma 1. *Let G be a group acting on a set S*

(i) The relation $\sim$ on S defined by $x \sim x' \iff \exists g \in G, gx = x'$ is an equivalence relation.

(ii) $\forall x \in S, G_x = \{g \in G \mid gx = x\}$ is a subgroup of G.

The equivalence classes are called the orbits of G on S, denoted by $\bar{x}$ for $x \in S$. The group G_x is called the stabilizer of x. If G acts on itself by conjugation, the orbits are called conjugacy classes. If a subgroup H acts on G by conjugation, $H_x = \{h \in H \mid hxh^{-1} = x\}$ is called the centralizer of x in H and is denoted $C_H(x)$. $C_G(x)$ is simply called the centralizer of x. If H acts by conjugation on the set S of subgroups of G, the subgroup of H fixing $k \in S$, $\{h \in H \mid hKh^{-1} = K\}$ is called the normalizer of K and is denoted $N_H(K)$. The group $N_G(K)$ is simply the normalizer of K. Every subgroup K is normal in $N_G(K)$ and K is normal iff $N_G(K) = G$.

Theorem 1. *If a group G acts on a set S, the cardinal number of the orbit of $x \in S$, is the index $[G : G_x]$.*

Proof. Let $g, h \in G$. Since $gx = hx \iff g^{-1}hx = x \iff hG_x = gG_x$ it follows that $gG_x \mapsto gx$ is a well-defined bijection of the set of cosets of G_x in G onto $\bar{x}$. Hence $[G : G_x] = |\bar{x}|$. □

Corollary 1. *Let G be a finite group and $K \leq G$.*

(i) The number of elements in the conjugacy class of $x \in G$ is $[G : C_G(x)]$ which divides $|G|$

(ii) If $\bar{x}_1, \cdots, \bar{x}_n$ are the distinct conjugacy classes of G, then

$$|G| = \sum_{i=1}^{n} [G : C_G(x_i)]$$

(iii) The number of subgroups of G conjugate to K is $[G : N_G(K)]$ which divides $|G|$.

Proof. (i) and (iii) follow from the previous theorem and Lagrange's theorem. Since conjugacy is an equivalence relation, (ii) follows from (i). □

Theorem 2. *If a group G acts on a set S, this induces a homomorphism $G \to A(S)$, where $A(S)$ is the group of permutations of S.*

Proof. If $g \in G$, define $\tau_g : S \to S$ by $\tau_g(x) = gx$. Since $x = g(g^{-1}x)$, τ_g is surjective. Similarly, $gx = gy$ implies $x = y$ whence τ_g is injective. Since $\tau_{gg'} = \tau_g \tau_{g'}$, the map $G \to A(S)$ given by $g \mapsto \tau_g$ is a homomorphism. □

Corollary 2. *If G is a group, there is a monomorphism $G \to A(G)$. Hence every group is isomorphic to a group of permutations. In particular, every finite group G is isomorphic to a subgroup of S_n with $n = |G|$.*

Proof. Let G act on itself by left translation and obtain $\tau : G \to A(G)$. If $\tau(g) = \mathrm{id}_G$, then $\forall x \in G, gx = x$. In particular, $ge = e$ whence $g = e$ and τ is a monomorphism. Note if $|G| = n$, $A(G) \cong S_n$. □

If G is a group, $\operatorname{Aut} G$, the set of all automorphisms of G is a group under composition.

Corollary 3. *Let G be a group.*

(i) $\forall g \in G$, conjugation by g induces an automorphism of G.

(ii) There is a homomorphism $G \to \operatorname{Aut} G$ whose kernel is $C(G) = \{g \in G \mid \forall x \in G, gx = xg\}$.

Proof. (i) If G acts on itself by conjugation, $\tau_g : G \to G$ given by $\tau_g(x) = gxg^{-1}$ is a bijection. τ_g is also a homomorphism and hence an automorphism. (ii) Let G act on itself by conjugation. The homomorphism $\tau : G \to A(G)$ has image contained in $\operatorname{Aut} G$. Clearly

$$g \in \ker \tau \iff \tau_g = \mathrm{id}_G \iff \forall x \in G, gxg^{-1} = x$$

whence $\ker \tau = C(G)$. □

The automorphism τ_g is called the inner automorphism induced by g. $C(G)$ is called the center of G. An element $g \in C(G)$ iff the conjugacy class of g consists of g alone. Thus if $x \in C(G)$, then $[G : C_G(x)] = 1$. Thus if G is finite, then

$$|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$$

where $\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_m$ are distinct conjugacy classes of G and each $[G : C_G(x_i)] > 1$. The above equation is called the class equation.

Proposition 1. *Let H be a subgroup of G and G act on S the set of all left cosets of H in G by left translation. The kernel of the induced homomorphism $G \to A(S)$ is contained in H.*

Proof. The induced homomorphism $\tau : G \to A(S)$ is given by $g \mapsto \tau_g$ where $\tau_g : S \to S$ and $\tau_g(xH) = gxH$. If $g \in \ker \tau, \tau_g = \mathrm{id}_S$ and $\forall x \in G, gxH = xH$. In particular, $geH = eH$ implying $g \in H$. □

Corollary 4. *If H is a subgroup of index n in a group G and no nontrivial normal subgroup of G is contained in H, then G is isomorphic to a subgroup of S_n.*

Proof. Apply the proposition. The kernel of the induced homomorphism $G \to A(S)$ is a normal subgroup of G contained in H and thus must be $\langle e \rangle$. Hence $G \to A(S)$ is a monomorphism. □

Corollary 5. *If H is a subgroup of a finite group G of index p, where p is the smallest prime dividing the order of G, then H is normal in G.*

Proof. Let S be the set of all left cosets of H in G. Then $A(S) \cong S_p$. If K is the kernel of the homomorphism $G \to A(S)$, $K \trianglelefteq G$ and $K \subseteq H$. Furthermore, G/K is isomorphic to a subgroup of S_p. Hence $|G/K|$ divides $p!$. But every divisor of $|G/K|$ must divide $|G|$. Thus $|G/K| = p$ or $|G/K| = 1$. However, $|G/K| = [G : H][H : K] = p[H : K] \geq p$. Thus $|G/K| = p$ and $[H : K] = 1$, whence $H = K$. But K is normal in G. □

We now discuss some lemmas that lead to the Sylow theorems.

Lemma 2. *If a group H of order p^n where p is a prime acts on a finite set S and if $S_0 = \{s \in S \mid \forall h \in H, hx = x\}$, $|S| \equiv |S_0| \pmod{p}$.*

Proof. An orbit $\bar{x}$ contains exactly one element iff $x \in S_0$. Hence S is a disjoint union $S = S_0 \sqcup \bigsqcup_{i=1}^{n} \bar{x}_i$ with $|\bar{x}_i| > 1$ for all i. Hence $|S| = |S_0| + \sum_{i=1}^{n} |\bar{x}_i|$. $p \mid |\bar{x}_i|$ for each i since $|\bar{x}_i| > 1$ and $|\bar{x}_i| = [H : H_{x_i}]$ divides $|H| = p^n$. Therefore $|S| \equiv |S_0| \pmod{p}$. □

Theorem 3 (Cauchy)**.** *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

Proof. Let S be the p-tuple of group elements $\{(a_1, a_2, \cdots, a_p) \mid a_i \in G, a_1a_2\cdots a_p = e\}$. Since $a_p = (a_1a_2\cdots a_{p-1})^{-1}$ necessarily, $|S| = n^{p-1}$, where $n = |G|$. Since $p \mid n, |S| \equiv 0 \pmod p$. Let $\mathbb{Z}_p$ act on S by cyclic permutations. $k(a_1, a_2, \cdots, a_p) = (a_{k+1}, a_{k+2}, \cdots, a_p, a_1, \cdots, a_k)$. Note $ab = e$ implies $ba = a^{-1}(ab)a = e$ so that $(a_{k+1}, a_{k+2}, \cdots, a_p, a_1, \cdots, a_k) \in S$. Verify that for $0, k, k' \in \mathbb{Z}_p, x \in S, 0x = x$ and $(k+k')x = k(k'x)$. Thus the action is well-defined. Now $(a_1, a_2, \cdots, a_p) \in S_0$ iff $a_1 = a_2 = \cdots = a_p$. Clearly $(e, e, \cdots, e) \in S_0$ so $|S_0| \neq 0$. $|S_0| \geq p$. There exists $a \neq e$ such that $(a, a, \cdots, a) \in S_0$ and hence $a^p = e$. Since p is prime, $|a| = p$. □

Definition 2. *A group in which every element has order a power of some fixed prime p is said to be a p-group. If H is a subgroup of a group G and H is a p-group, H is said to be a p-subgroup of G.*

In particular, $\langle e\rangle$ is always a p-subgroup of G for every prime p.

Corollary 6. *A finite group G is a p-group iff $|G|$ is a power of p.*

Corollary 7. *The center $C(G)$ of a nontrivial finite p-group G contains more than one element.*

Proof. Consider the class equation $|G| = |C(G)| + \sum_i [G : C_G(x_i)]$. Since each $[G : C_G(x_i)] > 1$ and divides $|G|$, $p \mid [G : C_G(x_i)]$ and thus $p \mid |C(G)|$. □

Lemma 3. *If H is a p-subgroup of a finite group G, then $[N_G(H) : H] \equiv [G : H] \pmod p$.*

Proof. Let S be the set of left cosets of H in G and let H act on S by left translation. Then $|S| = [G : H]$. Also,

$$xH \in S_0 \iff \forall h \in H, hxH = xH \iff x^{-1}Hx = H \iff x \in N_G(H)$$

Thus $|S_0| = [N_G(H) : H]$. Then $[N_G(H) : H] = |S_0| \equiv |S| = [G : H] \pmod p$. □

Corollary 8. *If H is a p-subgroup of a finite group G such that $p \mid [G : H]$, then $N_G(H) \neq H$.*

Proof. $0 \equiv [G : H] \equiv [N_G(H) : H] \pmod p$. Since $[N_G(H) : H] \geq 1$, we must have $[N_G(H) : H] > 1$. Thus $N_G(H) \neq H$. □

Theorem 4 (First Sylow Theorem)**.** *Let G be a group of order $p^n m$ with $n \in \mathbb{N}$, p prime, and $(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of G of order p^i, for $i < n$ that is normal in some subgroup of order p^{i+1}.*

Proof. Since $p \mid |G|$, G contains an element of order p.Proceeding by induction, assume $H \leq G$ where $|H| = p^i$ for $1 \leq i < n$. Then $p \mid [G : H]$ and $H \triangleleft N_G(H), H \neq N_G(H)$ and $1 < |N_G(H)/H| = [N_G(H) : H] \equiv [G : H] \equiv 0 \pmod p$. Hence $p \mid |N_G(H)/H|$ and $N_G(H)/H$ contains a subgroup of order p.

This group is of the form H_1/H where H_1 is a subgroup of $N_G(H)$ containing H. Since H is normal in $N_G(H)$, H is necessarily normal in H_1. Finally, $|H_1| = |H||H_1/H| = p^{i+1}$. □

Definition 3. *A subgroup P of a group G is said to be a Sylow p-subgroup iff P is a maximal p-subgroup of G.*

Sylow p-subgroups always exist, though sometimes they may be trivial, and every p-subgroup is contained in a Sylow p-subgroup. The first Sylow theorem shows that a finite group has a nontrivial Sylow p-subgroup for every prime p that divides the order of G.

Corollary 9. *Let G be a group of order $p^n m$ with p prime, $n \in \mathbb{N}, (m, p) = 1$. Let H be a p-subgroup of G.*

(i) H is a Sylow p-subgroup of G iff $|H| = p^n$

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

(iii) If there is only one Sylow p-subgroup, it is normal in G.

Theorem 5 (Second Sylow Theorem)**.** *If H is a p-subgroup of a finite group G and P is any Sylow p-subgroup of G, $\exists x \in G, H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups are conjugate.*

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. $|S_0| \equiv |S| = [G : P] \pmod p$. But $p \nmid [G : P]$. Thus $|S_0| \neq 0$ and there exists $xP \in S_0$.

$$xP \in S_0 \iff \forall h \in H, hxP = xP \iff xHx^{-1} \leq P \iff H \leq x^{-1}Px$$

If H is a Sylow p-subgroup, $|H| = |P| = |x^{-1}Px|$ and hence $H = x^{-1}Px$. □

Theorem 6 (Third Sylow Theorem)**.** *If G is a finite group and p a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.*

Proof. By the second Sylow theorem, the number of Sylow p-subgroups is the number of conjugates of any one of them, say P. This number is $[G : N_G(P)]$, a divisor of $|G|$. Let S be the set of all Sylow p-subgroups of G and let P act on S by conjugation. Then $Q \in S_0 \iff \forall x \in P, xQx^{-1} = Q \iff P \leq N_G(Q)$. Both P and Q are Sylow p-subgroups of G and hence of $N_G(Q)$ and are therefore conjugate in $N_G(Q)$. But $Q \trianglelefteq N_G(Q)$ meaning $Q = P$. Thus $S_0 = \{P\}$ and $|S| \equiv |S_0| = 1 \pmod p$. □

Theorem 7. *If P is a Sylow p-subgroup of a finite group G, then $N_G(N_G(P)) = N_G(P)$.*

Proof.

$$x \in N_G(N_G(P)) \implies xPx^{-1} \leq xN_G(P)x^{-1} = N_G(P)$$
$$\exists y \in N_G(P), yPy^{-1} = xPx^{-1} \implies y^{-1}xPx^{-1}y = P \implies x \in N_G(P)$$

□