

Group Actions, p -Groups, and the Sylow Theorems

Patrick J. Morandi

September 18, 1998

In this note we introduce the notion of a group action on a set and use it to prove a number of theorems about p -groups and the Sylow theorems. For undefined terms see any decent book on group theory. The theory of p -groups and the Sylow theorems have a number of applications in Galois theory. The nice structure of p -groups will translate via the fundamental theorem of Galois theory to nice structure of Galois extensions of degree a power of a prime. The first application of the Sylow theorems to Galois theory we will see will be to give an algebraic proof that \mathbb{C} is algebraically closed.

1 Group Actions

Definition 1 *Let G be a group and S a nonempty set. Then G is said to act on S if there is an operation $G \times S \rightarrow S$ (usually denoted by $(g, s) \mapsto gs$) such that $es = s$ and $(gh)s = g(hs)$ for all $s \in S$ and $g, h \in G$.*

Note that if $gs = t$ then $g^{-1}t = s$ since $g^{-1}t = g^{-1}(gs) = (g^{-1}g)s = es = s$.

If G acts on S and \sum_S is the group of all permutations of S then there is a homomorphism $\phi: G \rightarrow \sum_S$ given by $\phi(g)(s) = gs$. Thus $\phi(g)$ is the permutation that sends s to gs . This is a homomorphism because for all $s \in S$ we have $\phi(g) \circ \phi(h)(s) = \phi(g)(\phi(h)(s)) = g(hs) = (gh)s = \phi(gh)(s)$. Thus $\phi(gh) = \phi(g) \circ \phi(h)$. Conversely, if S is a set and $\tau: G \rightarrow \sum_S$ is a homomorphism then we can define an action of G on S by $gs = \tau(g)(s)$. Thus the existence of a homomorphism from G to \sum_S is equivalent to having an action of G on S .

Here are some examples of group actions.

Example 2 S_n acts on $\{1, 2, \dots, n\}$ by $(\sigma, i) \mapsto \sigma(i)$.

Example 3 If G is a group then G acts on itself by left translation: $(g, s) \mapsto gs$.

Example 4 If H is a subgroup of G and S the set of left cosets of H in G then G acts on S by left translation: $(g, xH) \mapsto gxH$.

Example 5 If G is a group then G acts on itself by conjugation: $(g, s) \mapsto gsg^{-1}$.

Example 6 Let G be a finite group and S the set of all subsets of G of cardinality n . Then G acts on S by $(g, X) \mapsto gX$, where $gX = \{gx \mid x \in X\}$ for $X \subseteq G$ with $|X| = n$.

If G acts on a set S , let $\phi : G \rightarrow \sum_S$ be the corresponding homomorphism. Then the kernel K of ϕ is given by $K = \{g \in G \mid gs = s \text{ for all } s \in S\}$. In Example 3 we see that $K = \{g \in G \mid gh = h \text{ for all } h \in G\} = (e)$.

Proposition 7 (Cayley) *Every group G is isomorphic to a subgroup of \sum_S for some set S .*

Proof. If G acts on itself by left multiplication, let ϕ be the corresponding homomorphism from G to \sum_G . As noted above the kernel of this homomorphism is (e) , so ϕ is 1 – 1. Thus G is isomorphic to $\phi(G)$, a subgroup of \sum_G . In particular, if $|G| = n$ then G is isomorphic to a subgroup of $S_n \cong \sum_G$. \square

Definition 8 *Let G act on S . For any $s \in S$ let $\mathcal{O}(s) = \{t \in S \mid t = gs \text{ for some } g \in G\}$. The set $\mathcal{O}(s)$ is called the orbit of s .*

Proposition 9 *If G acts on S then the relation \sim defined by $s \sim t$ if $t = gs$ for some $g \in G$ is an equivalence relation on S and the equivalence class of s is $\mathcal{O}(s)$.*

Definition 10 *If G acts on S , for $s \in S$ let $G(s) = \{g \in G \mid gs = s\}$.*

Note that $G(s)$ is a subgroup of G , which is called the *stabilizer group* of s .

Theorem 11 *For any $s \in S$, $|\mathcal{O}(s)| = |G : G(s)|$.*

Proof. If $g, h \in G$ then $gs = hs$ iff $h^{-1}gs = s$ iff $h^{-1}g \in G(s)$ iff $gG(s) = hG(s)$. Thus the cosets of $G(s)$ in G are in 1 – 1 correspondence with the elements of $\mathcal{O}(s)$ by $gs \longleftrightarrow gG(s)$. Thus $|\mathcal{O}(s)| = |G : G(s)|$. \square

Let G act on itself by conjugation. For $s \in G$ we have $\mathcal{O}(s) = \{gsg^{-1} \mid g \in G\}$, the *conjugacy class* of s . The stabilizer group $G(s)$ is the set $G(s) = \{g \in G \mid gsg^{-1} = s\} = \{g \in G \mid gs = sg\} = C(s)$, the *centralizer* of s in G . Thus we have $|\mathcal{O}(s)| = |G : C(s)|$, so if G is a finite group we get $|\mathcal{O}(s)| = |G|/|C(s)|$. The kernel of the corresponding homomorphism $G \rightarrow \sum_G$ is $\{g \in G \mid gsg^{-1} = s \text{ for all } s \in G\} = Z(G)$, the *center* of G .

Definition 12 *If G acts on S then $s \in S$ is G -stable if $\mathcal{O}(s) = \{s\}$, that is, if $gs = s$ for all $g \in G$.*

Thus if G acts on itself by conjugation the G -stable elements are precisely the elements of $Z(G)$.

Proposition 13 *Let G be a finite group. Let a_1, \dots, a_n be elements whose conjugacy classes are the distinct conjugacy classes containing more than one element. Then $|G| = |Z(G)| + \sum |G : C(a_i)|$.*

Proof. The conjugacy classes form a partition of G and $Z(G)$ consists of those elements whose conjugacy classes contain only themselves. Thus we have $|G| = |Z(G)| + \sum |\mathcal{O}(a_i)| = |Z(G)| + \sum |G : C(a_i)|$. \square

This equation is called the *class equation* for G .

2 p -Groups

Definition 14 *A finite group G is a p -group if $|G| = p^n$ for some prime p .*

Lemma 15 *Let G be a p -group that acts on a finite set S . If X is the set of G -stable elements of S then $|S| \equiv |X| \pmod{p}$.*

Proof. Let s_1, \dots, s_n be representatives of the disjoint orbits under G containing more than one element. Then S is the disjoint union $S = X \cup \mathcal{O}(s_1) \cup \dots \cup \mathcal{O}(s_n)$, and so $|S| = |X| + \sum |\mathcal{O}(s_i)|$. But $|\mathcal{O}(s_i)| = |G : G(s_i)| > 1$, so since G is a p -group, p divides $|G : G(s_i)|$. Thus $|S| \equiv |X| \pmod{p}$. \square

Proposition 16 *If G is a p -group then $|Z(G)| > 1$.*

Proof. If G acts on itself by conjugation then $Z(G)$ is the set of G -stable elements. Thus by Lemma 15 we have $|G| \equiv |Z(G)| \pmod{p}$. But p divides $|G|$, so p divides $|Z(G)|$, hence $|Z(G)| > 1$. \square

Corollary 17 *If $|G| = p^2$ then G is abelian.*

Proof. We have $|G| = |Z(G)| + \sum |G : C(a_i)|$, where the a_i are representatives of conjugacy classes containing more than one element. By Proposition 16 we have $|Z(G)| = p$ or p^2 . If $|Z(G)| = p^2$ then $G = Z(G)$, so G is abelian. So suppose $|Z(G)| = p$. Then $|G/Z(G)| = p$, so $G/Z(G)$ is cyclic, say generated by gZ ($Z = Z(G)$). If $h \in G$ then $h \in g^i Z$ for some i , say $h = g^i z$. Then $ghg^{-1} = gg^i z g^{-1} = g^i z = h$ as $z \in Z(G)$. Thus $g \in Z(G)$, so $G/Z(G)$ is the trivial group. Thus we get a contradiction to $|Z(G)| = p$. Therefore $|Z(G)| = p^2$, and so G is abelian. \square

If H is a subgroup of a group G , let $N(H) = \{g \in G \mid gHg^{-1} = H\}$, the *normalizer* of H in G . Then $N(H)$ is the largest subgroup of G containing H such that H is normal in $N(H)$. Let S be the set of subgroups of G . Then G acts on S by conjugation: $(g, K) \mapsto gKg^{-1}$. Thus $\mathcal{O}(H) = \{gHg^{-1} \mid g \in G\}$ and the stabilizer group $G(H) = \{g \in G \mid gHg^{-1} = H\} = N(H)$. Therefore $|\mathcal{O}(H)| = |G : N(H)|$.

Proposition 18 *Let G be a p -group. If H is a proper subgroup of G then $H \subsetneq N(H)$.*

Proof. Say $|G| = p^n$. We use induction on n . If $n = 1$ the result is clear. So suppose $n > 1$ and the result is true for all $m < n$. If $Z(G) \not\subseteq H$ then since $Z(G) \subseteq N(H)$ we see $H \subsetneq N(H)$. So we may suppose $Z(G) \subseteq H$. By Proposition 16, $|Z(G)| > 1$, so $|G/Z(G)| = p^m$ for some $m < n$. By induction $H/Z(G) \subsetneq N(H/Z(G))$. It is not hard to see that $N(H) = \{g \in G \mid gZ(G) \in N(H/Z(G))\}$ and $H = \{g \in G \mid gZ(G) \in H/Z(G)\}$ as $Z(G)$ is contained in both H and $N(H)$. Thus $H \subsetneq N(H)$ as $H/Z(G) \subsetneq N(H)/Z(G)$. \square

Definition 19 *A subgroup M is a maximal subgroup of G if $M \neq G$ and if H is a subgroup of G with $M \subseteq H \subseteq G$ then either $H = M$ or $H = G$.*

Note that maximal subgroups exist inside any finite group by the following argument. If H is a subgroup of G which is not maximal then there is a subgroup $H_1 \supsetneq H$. If H_1 is not maximal then there is a $H_2 \supsetneq H_1$. We can continue this process as long as H_i is not maximal. But since $|G| < \infty$ this process cannot continue indefinitely. Thus the sequence of H_i must terminate, and so there is a maximal subgroup of G . Note that this is not true in general, as the group $\mathbb{Z}_p^\infty = \{a/p^n \in \mathbb{Q} \mid a, n \in \mathbb{Z}\}$ has no maximal subgroups.

Proposition 20 *If G is a p -group and M a maximal subgroup of G then M is normal in G and $|G : M| = p$.*

Proof. By Proposition 18, $M \subsetneq N(M) \subseteq G$. By maximality we see $N(M) = G$, so M is normal in G . Since M is maximal the group G/M has no nontrivial subgroups, thus G/M has prime order. The only possibility is then $|G/M| = |G : M| = p$. \square

Corollary 21 *If $|G| = p^n$ and $m \leq n$ then G has a subgroup of order p^m . In fact, there is a normal subgroup of G of order p^m for any $m \leq n$.*

Proof. If we weren't concerned about normality we could inductively construct the subgroups as follows. Suppose we have constructed a subgroup H_m of G of order p^m . If H_{m-1} is a maximal subgroup of H_m then from Proposition 20 we see that $|H_{m-1}| = p^{m-1}$. However, to get normal subgroups of any order we argue by induction on n . If $n = 1$ the result is

trivial. Suppose $n > 1$ and that the result is true for groups of order p^{n-1} . By Proposition 16 there is a $b \in Z(G)$ with $b \neq e$. If the order of b is p^l then $a = b^{p^{l-1}}$ has order p . Let N be the cyclic subgroup generated by a . Since $a \in Z(G)$, N is a normal subgroup of G , and $|G/N| = p^{n-1}$. By induction, since $m - 1 \leq n - 1$ there is a normal subgroup \mathcal{H} of G/N of order p^{m-1} . Let $H = \{g \in G \mid gN \in \mathcal{H}\}$. Then H is a normal subgroup of G containing N with $H/N = \mathcal{H}$, so $|H|/|N| = p^{m-1}$. Thus $|H| = p^m$. Therefore by induction the corollary is proven. \square

3 The Sylow Theorems

Let G be a finite group, p a prime and say $|G| = p^n q$ with p not dividing q .

Definition 22 *A p -Sylow subgroup of G is a subgroup of order p^n .*

Thus a p -Sylow subgroup of G is a p -subgroup of G of maximum possible order by Lagrange's theorem.

Theorem 23 (First Sylow Theorem) *Let G be a finite group. Then there exists a p -Sylow subgroup of G .*

Proof. Let $|G| = p^n q$ where q is not divisible by p . Let S be the set of all subsets of G containing p^n elements. Then $|S| = \binom{p^n q}{p^n}$. We will use the fact that p does not divide this binomial coefficient, which you can find in most books on group theory (but not Hungerford). Let G act on S by left multiplication. Since S is the disjoint union of the distinct orbits, there must be some orbit whose size is not divisible by p . Thus there is some subset T of G with $|T| = p^n$ such that $|\mathcal{O}(T)|$ is not divisible by p . Let $P = G(T)$, the stabilizer group of T . We have $|\mathcal{O}(T)| = |G : P| = |G|/|P|$, so since p does not divide $|\mathcal{O}(T)|$ we see p^n divides $|P|$. However $P = \{g \in G \mid gT = T\}$. But if $t \in T$ then $ht \in T$ for $h \in P$. Thus $Pt = \{ht \mid h \in P\} \subseteq T$ and $|Pt| = |P|$, so $|P| \leq |T| = p^n$. Thus we see $|P| = p^n$, so P is a p -Sylow subgroup of G . \square

Corollary 24 (Cauchy) *If p divides the order of G then there exists an $a \in G$ of order p .*

Proof. Let P be a p -Sylow subgroup of G and $b \in P$ a non-identity element. Then b has order p^m for some m by Lagrange's theorem. Then $a = b^{p^{m-1}}$ has order p . \square

Note that if P is a p -Sylow subgroup of G and $g \in G$ then gPg^{-1} is also a p -Sylow subgroup of G . Hence if G contains only one p -Sylow subgroup P then P is normal in G . We shall see from the second Sylow theorem that all p -Sylow subgroups are conjugate. Thus G has a normal p -Sylow subgroup iff G has only one p -Sylow subgroup.

Theorem 25 (Second Sylow Theorem) *If P is a p -Sylow subgroup of G and H is any p -subgroup of G then $H \subseteq xPx^{-1}$ for some $x \in G$. In particular, any two p -Sylow subgroups of G are conjugate.*

Proof. Let S be the left cosets of P in G and let H act on S by left multiplication. If X is the set of H -stable elements of S then since H is a p -group we have $|S| \equiv |X| \pmod{p}$ by Lemma 15. Since $|S| = |G : P|$ is not divisible by p , neither is $|X|$. Thus $X \neq \emptyset$. Let $xP \in X$. Then $hxP = xP$ for all $h \in H$. That is $hx \in xP$, or $h \in xPx^{-1}$. So $H \subseteq xPx^{-1}$, another p -Sylow subgroup of G .

If Q is a p -Sylow subgroup of G then from the above argument we see that $Q \subseteq xPx^{-1}$ for some $x \in G$. Thus $Q = xPx^{-1}$ since $|Q| = |P| = |xPx^{-1}|$. \square

Theorem 26 (Third Sylow Theorem) *The number of p -Sylow subgroups of G divides $|G|$ and is of the form $kp + 1$.*

Proof. Let P be a p -Sylow subgroup of G . Then by the second Sylow theorem the set S of all p -Sylow subgroups of G is $S = \{gPg^{-1} \mid g \in G\}$. The group G acts on S by conjugation, and $S = \mathcal{O}(P)$ and $G(P) = N(P)$, so $|S| = |\mathcal{O}(P)| = |G : N(P)|$ which divides $|G|$. Let X be the set of P -stable elements of S . Since P is a p -group, $|S| \equiv |X| \pmod{p}$ by Lemma 15. Note that $P \in X$ since $xPx^{-1} = P$ for all $x \in P$. Suppose $Q \in X$. Then $xQx^{-1} = Q$ for all $x \in P$, so $P \subseteq N(Q)$. However, Q is the unique p -Sylow subgroup of $N(Q)$ since Q is normal in $N(Q)$. But $P \subseteq N(Q)$ is another p -Sylow subgroup of $N(Q)$, so $Q = P$. Thus $|X| = 1$. So $|S| \equiv 1 \pmod{p}$, so $|S| = kp + 1$ for some k . \square

In fact, we can say a little more about the number of p -Sylow subgroups of G . If $|G| = p^n q$ where p does not divide q then since the number of p -Sylow subgroups ($kp + 1$) is relatively prime to p , this number must divide q , not just $|G|$. This also follows from the argument in the above proof, since the number of p -Sylow subgroups is equal to $|G : N(P)|$, which divides $|G : P| = q$ as $P \subseteq N(P)$.

Corollary 27 *If P is a p -Sylow subgroup of G then $N(N(P)) = N(P)$.*

Proof. Since P is normal in $N(P)$ it is the unique p -Sylow subgroup of $N(P)$. However if $x \in N(N(P))$ then $xN(P)x^{-1} = N(P)$, so $xPx^{-1} \subseteq xN(P)x^{-1} = N(P)$. This forces $xPx^{-1} = P$, so $x \in N(P)$. Hence $N(N(P)) \subseteq N(P)$. But $N(P) \subseteq N(N(P))$, so $N(N(P)) = N(P)$. \square

There are a number of applications of p -groups to Galois theory. Just to mention one, suppose K is a Galois extension of F with $[K : F] = p^n$. Then $G = \text{Gal}(K/F)$ is a p -group. Therefore from Corollary 21 there is a subgroup H of G of order p^{n-m} for any $m \leq n$. If L is

the fixed field of H then $[L : F] = |G : H|$, so $[L : F] = p^m$. Furthermore, we can choose H to be normal in G , so L is Galois over F . Thus we have a tower $F = L_0 \subset L_1 \subset \cdots \subset L_n = K$ where L_i is Galois over F of degree p^i . Since each L_{i+1} is Galois over L_i of degree p , we see that $\text{Gal}(L_{i+1}/L_i)$ is a cyclic group of order p . Therefore by analyzing cyclic Galois extensions we can use this tower of fields to give descriptions of K . In particular, if F contains a primitive p -th root of unity, that is an element ω with $\omega \neq 1$ and $\omega^p = 1$ then we will show soon that $L_{i+1} = L_i(\sqrt[p]{a_i})$ for some $a_i \in L_i$. In particular, K is a *radical* extension of F (which we will discuss later). If K is the splitting field of a separable polynomial $f(x) \in F[x]$ with $[K : F] = p^n$ then we shall show that K/F being a radical extension will imply that f is solvable by radicals. This roughly means there is a formula for the roots of f that only requires the operations on F together with the extraction of roots of elements of F .