Group Actions

Patrick J. Morandi

There are a number of results of group theory presented in Herstein [1] (the counting principles in Sections 2.5 and 2.11, Cayley's theorem in Section 2.9 and the Sylow theorems of Section 2.12, among others) whose proofs follow similar ideas. However, it is not apparent that this is so. This handout covers the ideas necessary to tie these results together. The important idea is that of an action of a group on a set.

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

There can be different ways for a group to act on a set. The notation gs for the image of (g, s) is ambiguous, but won't cause problems since we will not consider two different actions of a group on a set at a time. Before we get into properties of group actions, we give many examples. Most of these examples will lead to a theorem in group theory. Note that you have seen examples where you multiply one type of object by another, such as scalar multiplication of vectors. In fact, this will lead off our examples.

Example 2 Let G be the group of nonzero real numbers under multiplication, and let S be the set of all vectors in 3–space. Thus $S = \{(a, b, c) \mid a, b, c \in \mathbf{R}\}$. Then G acts on S via scalar multiplication. That is, $g(a, b, c) = (ga, gb, gc)$ if g is a nonzero real number. Then for any vector $\overrightarrow{v}$, we have $1\overrightarrow{v} = \overrightarrow{v}$, and if g, $h \in G$ then $(gh)\overrightarrow{v} = g(h\overrightarrow{v})$, since if $\overrightarrow{v} = (a, b, c)$ then $(gh)\overrightarrow{v} = (gha, ghb, ghc) = g(ha, hb, hc) = g(h\overrightarrow{v})$.

Example 3 Let G be a group and $S = G$. Then G acts on S by left multiplication. That is, gs is defined to be the ordinary product of g and s in G. Associativity of multiplication in G and properties of the identity then show this is an action of G on S. This example will lead to a proof of Cayley's theorem [1, Thm. 2.9.1].

Example 4 Let G be a group and $S = G$. Let us define an action of G on S by conjugation. That is, if $g \in G$ and $s \in S$ (so $s \in G$), then we define the function by $(g, s) \mapsto gsg^{-1}$. To see that this is an action of G on S, we check the definition. If $s \in S$ then $(e, s) \mapsto ese^{-1} = s$, so the first property is satisfied. Second, if g, $h \in G$ and $s \in S$ then $((gh), s) \mapsto (gh)s(gh)^{-1} = ghsh^{-1}g^{-1}$, and $(g, (h, s)) \mapsto g(hsh^{-1})g^{-1} = g(hsh^{-1})g^{-1}$. These are then equal, so this is an action. This example will yield a proof of the counting principle in Section 2.11 of [1].

Example 5 Let G be a group and H a subgroup of G. Let S be the set of all left cosets of H in G. So $S = \{aH \mid a \in G\}$. Then G acts on S by $g(aH) = gaH$. That this definition is well defined is left to the reader. To check that this is an action, we see that $e(aH) = eaH = aH$, and if g, $h \in G$, then $(gh)(aH) = ghaH = g(haH)$. Therefore this is an action of G on the set of left cosets of H. The two results in Section 2.9 of [1] after Cayley's theorem can and will be proved by using this example.

Example 6 Let G be a group and S the set of all subsets of G with n elements (here n can be any positive integer with $n \leq |G|$). Then G acts on S via $(g, X) \mapsto gX = \{gx \mid x \in X\}$. Note that gX is a subset of G with n elements. To verify this is an action, we see that $eX = \{ex \mid x \in X\} = X$, and if g, $h \in G$ then $(gh)X = \{ghx \mid x \in X\} = g(hX)$. This example will be used in the proof of the first Sylow theorem.

Example 7 Let H and K be subgroups of a group G, and let $S = \{aK \mid a \in G\}$, the set of left cosets of K in G. Then H acts on S by left multiplication, as in Example 4. That is, H acts on S via $(h, aK) \mapsto haK$. That this is a group action follows from the same reasons as in Example 4. This example will lead us to a proof of the counting principle of 2.5.

Example 8 Let G be a group and H a subgroup of G. Let $S = \{aHa^{-1} \mid a \in G\}$, a collection of subgroups of G. Then G acts on S via conjugation: $(g, K) \mapsto gKg^{-1}$. If $K \in S$ then $K = aHa^{-1}$for some $a \in G$, so $(g, K) \mapsto gaHa^{-1}g^{-1} = (ga)H(ga)^{-1}$, so the result lands in S. That this is an action can be verified by similar arguments to those given in Example 4. This example will be used in the proof of the third Sylow theorem.

Example 9 The group S_n acts on $S = \{1, 2, \ldots, n\}$ by $\sigma n = \sigma(n)$. This is an action since for any $r \in \{1, 2, \ldots, n\}$, then $er = e(r) = r$, and if σ, $\tau \in S_n$ then $(\sigma\tau)r = (\sigma\tau)(r) = \sigma(\tau(r)) = \sigma(\tau r)$. Therefore S_n acts on $\{1, 2, \ldots, r\}$. This example can yield the unique cycle decomposition of a permutation.

Now that we have a bunch of examples, let us develop the theory of group actions. Applying the theory to these special cases will lead to some theorems, such as Cayley's theorem and the counting principles of Sections 2.5 and 2.11 of [1].

Definition 10 *Suppose G is a group which acts on a set S. If $s \in S$, let $\mathcal{O}(s) = \{gs \mid g \in G\}$. The set $\mathcal{O}(s)$ is called the* orbit *of s. The* stabilizer *of s is the subset $G_s = \{g \in G \mid gs = s\}$ of G.*

Let us record the basic properties of these concepts. One small point to start with. If $gs = t$ then $s = es = (g^{-1}g)s = g^{-1}(gs) = g^{-1}t$. We now consider the stabilizer of an element.

Lemma 11 *Let G act on a set S. If $s \in S$, then the stabilizer G_s of s is a subgroup of G.*

Proof. Note that G_s is nonempty since $e \in G_s$. Furthermore, if g, $h \in G_s$ then $gs = hs = s$, so $(gh)s = g(hs) = gs = s$, so $gh \in G_s$. Finally, if $g \in G_s$ then $g^{-1}s = g^{-1}(gs) = (g^{-1}g)s = es = s$. Thus $g^{-1} \in G_s$. Therefore G_s is a subgroup of G. ■

The orbits $\mathcal{O}(s)$ are subsets of S. The significant fact about these subsets is they form a partition of S, which is proved in the next lemma.

Lemma 12 *Let G act on a set S. If the relation $\sim$ on S is defined by $s \sim t$ if $s = gt$ for some $g \in G$, then $\sim$ is an equivalence relation. Furthermore, the equivalence class of any $s \in S$ is the orbit $\mathcal{O}(s)$.*

Proof. We need to verify the three properties of an equivalence relation. If $s \in S$ then $s \sim s$ since $s = es$. If $s \sim t$ then $s = gt$ for some g. It then follows that $t = g^{-1}s$, so $t \sim s$. Finally, if $s \sim t$ and $t \sim r$ then $s = gt$ and $t = hr$ for some g, $h \in G$. Then $s = g(hr) = (gh)r$, so $g \sim r$. Thus $\sim$ is an equivalence relation on S. For any $s \in S$, the equivalence class of s is the set $\{t \in S \mid t \sim s\} = \{t \in S \mid t = gs\} = \mathcal{O}(s)$. ■

We will use group actions primarily to obtain information about finite groups. The following result gives the basic numerical information about group actions of finite groups.

Lemma 13 *Let G be a finite group acting on a set S. If $s \in S$ then $|\mathcal{O}(s)| = [G : G_s]$, the index of G_s in G.*

Proof. We prove this by producing a 1–1 correspondence between $\mathcal{O}(s)$ and the set of left cosets of G_s. Given a coset gG_s, we associate this coset to the element gs of $\mathcal{O}(s)$. Is this a function? We must show this correspondence is well defined. If $gG_s = hG_s$ then $g^{-1}h \in G_s$, so $(g^{-1}h)s = s$. Then $hs = gs$, so this is indeed well defined. To see this function is 1–1, suppose $gs = hs$. Then $g^{-1}(hs) = s$, so $(g^{-1}h)s = s$. Hence $g^{-1}h \in G_s$, so $gG_s = hG_s$. Therefore our function is 1–1. As for onto, if $t \in \mathcal{O}(s)$ then $t = gs$ for some g, and so t is the image of gG_s. Therefore our function is indeed a 1–1 correspondence between $\mathcal{O}(s)$ and the set of left cosets of G_s. Since these two sets are finite, this means they have the same number of elements. ■

The final property of group actions will be to relate a group acting on a set with the group of permutations on a set. Let G be a group acting on a set S. Let $A(S)$ be the group of all permutations of S. Then we can define a function from G to $A(S)$ with the use of the action. Let $f : G \to A(S)$ be given by $f(a)$ is the permutation that sends s to as. Let us denote this function by f_a. First, let's show this function exists, i.e., show f_a is in fact a permutation of S. That f_a is a function from S to S is clear, so we need to check that it is 1–1 and onto. For 1–1, suppose s and t are elements of S with $f_a(s) = f_a(t)$. So $as = at$. Then

$$s = es = (a^{-1}a)s = a^{-1}(as) = a^{-1}(at) = (a^{-1}a)t = et = t.$$

Therefore f_a is 1–1. For onto, suppose $t \in S$. Let $s = a^{-1}t$. Then

$$f_a(s) = as = a(a^{-1}t) = (aa^{-1})t = et = t.$$

Thus f_a is also onto. Hence f_a is a permutation of S, so lies in $A(S)$. Therefore f is a function from G to $A(S)$.

Lemma 14 *Let G act on a set S. Define $f : G \to A(S)$ as above by $f(a) = f_a$, where $f_a(s) = as$. Then f is a group homomorphism. The kernel of f consists of all $g \in G$ with $gs = s$ for all $s \in S$. Therefore $\{g \in G \mid gs = s \text{ for all } s \in S\}$ is a normal subgroup of G.*

Proof. We have verified that f is indeed a function from G to $A(S)$. To show f is a homomorphism, we need to show $f(ab) = f(a) \circ f(b)$ for all a, $b \in G$. That is, we need to show $f_{ab} = f_a \circ f_b$. To show these functions are equal we check that they have the same function value at each $s \in S$. Given $s \in S$, we have

$$\begin{aligned} f_{ab}(s) &= (ab)s = a(bs) = f_a(bs) = f_a(f_b(s)) \\ &= (f_a \circ f_b)(s). \end{aligned}$$

Therefore these two functions are indeed equal. Thus f is a homomorphism. An element $g \in G$ is in the kernel of f iff f_g is the identity function. This is true iff $f_g(s) = s$ for all $s \in S$. But since $f_g(s) = gs$, this means $g \in \ker(f)$ iff $gs = s$ for all $s \in S$. The kernel of a group homomorphism is a normal subgroup of G, which proves the final statement of the lemma. ■

The function in the proposition above will be useful to us for a couple different reasons which we will see below. But first, let us notice that the existence of a group action is in fact equivalent to the existence of a homomorphism from G to $A(S)$. One direction we have seen; given a group action of G on S we obtain a homomorphism from G to $A(S)$. Conversely, suppose S is a set such that there is a homomorphism $f : G \to A(S)$. We define a group action of G on S by $gs := f(g)(s)$. To verify that this is indeed an action, if $s \in S$ then $es = f(e)(s) = s$, since $f(e)$ is the identity function (since f is a group homomorphism, it takes the identity of G to the identity of $A(S)$). Second, if g, $h \in G$, we want to show $(gh)s = g(hs)$. Let us denote $f(a)$ by f_a for $a \in G$. Then $f_{gh} = f_g \circ f_h$ since f is a homomorphism. Therefore

$$(gh)(s) = f_{gh}(s) = (f_g \circ f_h)(s) = f_g(f_h(s)) = f_g(hs) = g(hs).$$

This definition is then an action on S. It is not hard to see that given this action, f is then the function obtained in Lemma 14.

We now utilize the theory of group actions to obtain results about groups. The first of these is Cayley's theorem [1, Thm. 2.9.1].

Proposition 15 (Cayley) *Let G be a group. Then G is isomorphic to a subgroup of $A(G)$. In particular, if G is a finite group of order n, then G is isomorphic to a subgroup of S_n.*

Proof. Let G act on itself by left multiplication as in Example 3. Then by Lemma 14, there is a homomorphism $f : G \to A(G)$, where $f(g)$ is the permutation of G that sends h to gh for any $h \in G$. Let us determine $\ker(f)$. We have that $a \in \ker(f)$ iff $ah = h$ for all $h \in G$, from the description of the kernel in Lemma 14, together with the description of the action. But if $ah = h$, cancellation gives $a = e$. Thus the kernel is trivial, so f is 1–1. Therefore f is an isomorphism from G to the image $f(G)$, a subgroup of $A(G)$. If $|G| = n$ then $A(G)$ is isomorphic to S_n, so G is isomorphic to a subgroup of S_n. ■

A counting principle (Section 2.5). Let H and K be subgroups of a group G. Let $HK = \{hk \mid h \in H, k \in K\}$. In general HK is not a subgroup of G (see [1, Lemma 2.5.1]). However, knowing the size of HK can be useful in working with finite groups. We will use the group action of Example 7 to prove the following theorem.

Theorem 16 *Let H and K be finite subgroups of a group G. Then*

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

Proof. Let us consider the group action of Example 7. In that example, H acts on the set of left cosets $\{gK \mid g \in G\}$. We prove the result by analyzing the orbit of $K = eK$ under this action of H. We have $\mathcal{O}(eK) = \{h(eK) = hK \mid h \in H\}$. Notice that the union of the distinct cosets in $\mathcal{O}(eK)$ is precisely HK. Since $|hK| = |K|$ for each $h \in H$, that these cosets are pairwise disjoint implies $|HK| = |K| \cdot |\mathcal{O}(eK)|$. By Lemma 13, $\mathcal{O}(eK) = [H : H_{eK}]$. (Note that the group that is acting on S is H, therefore the notation H_{eK} instead of G_{eK}.) The stabilizer H_{eK} is equal to the set

$$\{h \in H \mid heK = eK = K\} = \{h \in H \mid h \in K\} = H \cap K.$$

Therefore $|\mathcal{O}(eK)| = |H| \,/\, |H \cap K|$. But this gives $|HK| = |K|\,|H| \,/\, |H \cap K|$. ■

Another counting principle (Section 2.11). This next counting principle will be used to help determine the structure of groups of prime power order. These groups arise in the Sylow theorems, and in the description of finite abelian groups, and so are worth studying. A few of the most important results of groups of prime power order fall out from this counting principle. Recall [1, p. 47, problem 13] that the *normalizer* $N(a)$ of an element $a \in G$ is the set $N(a) = \{g \in G \mid ga = ag\}$. This is a subgroup of G. Consider the action of Example 4. That is, if G is a group then G acts on itself by conjugation. If $a \in G$ then the stabilizer G_a is given by $G_a = \{g \in G \mid gag^{-1} = a\}$. But $gag^{-1} = a$ iff $ga = ag$. thus $G_a = N(a)$. Recall that the center $Z(G)$ of G is the subgroup $\{x \in G \mid xg = gx \text{ for all } g \in G\}$. The elements of $Z(G)$ can be characterized in the following way: $x \in Z(G)$ iff $N(x) = G$.

Theorem 17 (Class Equation) *Let G be a finite group. Then*

$$|G| = \sum \frac{|G|}{|N(a)|},$$

where this sum runs over one element a from each conjugacy class. In particular,

$$|G| = |Z(G)| + \sum_{N(a) \neq G} \frac{|G|}{|N(a)|},$$

where the sum runs over one element a from each conjugacy class with $N(a) \neq G$.

Proof. Let $\mathcal{O}(a_1), \ldots, \mathcal{O}(a_r)$ be the distinct orbits of G under the conjugation action of G on itself. Since these orbits form the equivalence classes of an equivalence relation on G by Lemma 12, we have $|G| = |\mathcal{O}(a_1)| + \cdots + |\mathcal{O}(a_r)|$. By Lemma 13, $|\mathcal{O}(a_i)| = [G : N(a_i)]$, since $N(a_i)$ is the stabilizer of a_i. But by Lagrange's theorem, $[G : N(a_i)] = |G| \,/\, |N(a_i)|$. Therefore the first formula of the theorem is proved. ■

Let us now look a little more closely at the formula we just proved. If $x \in G$ then $\mathcal{O}(x) = \{gxg^{-1} \mid g \in G\}$. But if $x \in Z(G)$ then $gxg^{-1} = x$ for all g. Therefore $\mathcal{O}(x) = \{x\}$ for any $x \in Z(G)$. Note that the converse is also true: if $\mathcal{O}(x) = \{x\}$ then $x \in Z(G)$. The a_i are then subdivided into two parts. The first part is those a_i which $\mathcal{O}(a_i) = \{a_i\}$. This consists of all elements of $Z(G)$. The second part is all other a_i, so all a_i with $N(a_i) \neq G$. By breaking the sum above into two pieces, once piece for those a_i in $Z(G)$ and another piece for those a_i with $N(a_i) \neq G$, we see that the second formula is true.

Two results from Section 2.9. The group action of Example 5 will be used to prove Theorem 2.9.2 and Lemma 2.9.1 in [1]. In fact, he uses group actions without explicitly saying so. Let H be a subgroup of a group G, and let S be the set of all left cosets of H. Let us consider the function f defined by this group action. Then the function f is defined by $f(g) : aH \mapsto gaH$. We will obtain these two results by considering the kernel of f.

Theorem 18 *Let H be a subgroup of a group G, and let S be the set of left cosets of H in G. Let f be the homomorphism from G to $A(S)$ obtained from the action of G on S as in Example 5. Then* $\ker(f) = \bigcap_{a \in G} aHa^{-1}$. *Moreover, this is the largest normal subgroup of G which is contained in H. Furthermore, if G is a finite group such that $|G|$ does not divide $[G : H]!$ then* $\ker(f) \neq \{e\}$. *When this occurs, H contains a nontrivial normal subgroup of G.*

Proof. Let us determine $\ker(f)$. We have $g \in \ker(f)$ iff $f(g)$ is the identity function on S iff $gaH = aH$ for all $a \in G$. But $gaH = aH$ iff $a^{-1}ga \in H$ (recall that left cosets are equivalence classes for the congruence relation $a \sim b$ iff $a^{-1}b \in H$). Thus $g \in \ker(f)$ iff $g \in aHa^{-1}$ for all a. Therefore $\ker(f) = \bigcap_{a \in G} aHa^{-1}$. To see that $\ker(f)$ is the largest

normal subgroup of G contained in H, suppose $K \subseteq H$ is a normal subgroup. Then $K = aKa^{-1} \subseteq aHa^{-1}$ for all a, so $K \subseteq \ker(f)$.

For the last part of the theorem, suppose G is finite, and let n be the index of H in G. Then we can view f as a homomorphism from G to S_n. If $\ker(f) = \{e\}$ then f is 1–1, so G is isomorphic to a subgroup of S_n. By Lagrange's theorem, $|G|$ divides $|S_n| = n!$. If $|G|$ does not divide $n!$ then $\ker(f)$ is necessarily nontrivial. Therefore there is a nontrivial normal subgroup of G which is contained in H, namely $\ker(f) = \bigcap_{a \in G} aHa^{-1}$. ■

The final application we will give of group actions is to prove the Sylow theorems. Let G be a finite group. If p is a prime number dividing $|G|$, say $|G| = p^n q$ with p not dividing q. A subgroup of G of order p^n is called a p–Sylow subgroup of G. By Lagrange's theorem, the largest possible size of a subgroup of G of order a power of p is p^n. The Sylow theorems give the existence of, and properties of p–Sylow subgroups of G.

Theorem 19 (First Sylow Theorem) *Let G be a finite group. If p is a prime divisor of $|G|$ then there exists a p–Sylow subgroup of G.*

Proof. Let $|G| = p^n q$ with p not dividing q. Let S be the set of all subsets of G of size p^n. Then G acts on S via Example 6. That is, G acts on S via $(g, A) \mapsto gA = \{ga \mid a \in A\}$, if A is a subset of G of size p^n. The number of elements of S is equal to the number of ways of choosing p^n elements out of a set of size $p^n q = |G|$. Therefore

$$|S| = \binom{p^n q}{p^n}.$$

What is significant about this binomial coefficient is that it is not divisible by p. For a proof of this, see [1, p. 92]. Therefore the number of elements of S is not divisible by p. Since S is the union of the distinct orbits, there is some orbit whose size is not divisible by p. Suppose A is an element of S with $|\mathcal{O}(A)|$ not divisible by p. Let P be the stabilizer G_A of A. We claim that P is our desired p–Sylow subgroup. To verify this we need to show $|P| = p^n$. By Lemma 13, $|\mathcal{O}(A)| = [G : P] = |G| / |P|$. Since $|G| = p^n q$, the only way for p not to divide $[G : P]$ is for $|P|$ to be a multiple of p^n. Now, $P = \{g \in G \mid gA = A\}$. So if $x \in P$ and $a \in A$ then $xa \in A$. This says the right coset Pa consists of elements of A. Therefore $|Pa| \leq |A| = p^n$. Since $|Pa| = |P|$, we obtain $|P| \leq p^n$. Since we have already seen that p^n divides $|P|$, we conclude that $|P| = p^n$. Therefore P is a p–Sylow subgroup of G. ■

The second and third Sylow theorems are concerned with the structure of and number of Sylow subgroups. We shall see that the formula for the number of Sylow subgroups will allow us to characterize finite groups of some particular sizes. Note that if P is a p–Sylow subgroup of a group G and $x \in G$ then xPx^{-1} is a subgroup of G with $|xPx^{-1}| = |P|$. Therefore xPx^{-1} is also a p–Sylow subgroup of G. We prove the second Sylow theorem by applying the group action of Example 7. We need a preliminary lemma. If G acts on a set S, then an element $s \in S$ is called *G–stable* if $gs = s$ for all $g \in G$. That is, s is G–stable if $\mathcal{O}(s) = \{s\}$.

Lemma 20 *Let G be a group with $|G| = p^r$ for some prime p. If G acts on a set S and X is the set of all G–stable elements in S then $|X| \equiv |S| \bmod p$.*

Proof. Let $s_1, \ldots, s_m$ be representatives of the disjoint orbits under G containing more than one element. Then S is the disjoint union $S = X \cup \mathcal{O}(s_1) \cup \cdots \cup \mathcal{O}(s_m)$, and so $|S| = |X| + \sum_i |\mathcal{O}(s_i)|$. By Lemma 13, $|\mathcal{O}(s_i)| = [G : G_{s_i}]$, which by Lagrange's theorem is a divisor of $|G|$. Therefore, since $\mathcal{O}(s_i)$ contains more than one element, $|\mathcal{O}(s_i)|$ is divisible by p. Therefore $|S| \equiv |X| \bmod p$. ■

Theorem 21 (Second Sylow Theorem) *Let G be a group of order $p^n q$, where p is a prime and p does not divide q. If P is a p–Sylow subgroup of G and H is any subgroup of G of order a power of p 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 set of left cosets of P in G and let H act on S as in Example 7. Let X be the set of all H–stable elements of S. By Lemma 20, $|S| \equiv |X| \bmod p$. Since $|S| = |G| / |P| = q$ is not divisible by p, $|X| \not\equiv 0 \bmod p$, so X is not the empty set. Suppose $aP \in X$. The orbit of aP is the set $\{haP \mid h \in H\}$. Since this orbit has only one element, $haP = aP$ for each $h \in H$. So $ha \in aP$, or $h \in aPa^{-1}$ for each h. Therefore $H \subseteq aPa^{-1}$. This proves the first statement of the theorem. For the second statement, suppose P' is another p–Sylow subgroup of G. Then by the first part of the theorem, $P' \subseteq aPa^{-1}$ for some $a \in G$. But $|P'| = p^n = |P| = |aPa^{-1}|$. Therefore $P' = aPa^{-1}$. ■

A consequence of the second Sylow theorem, which we will use in the proof of the third Sylow theorem, is that a p–Sylow subgroup P of G is a normal subgroup of G iff P is the unique p–Sylow subgroup of G. For, P is normal in G iff $xPx^{-1} = P$ for each $x \in G$. Therefore P is normal in G iff P is the unique p–Sylow subgroup of G, by the second Sylow theorem. We will prove the third Sylow theorem by using some of the ideas in the proof of the second Sylow theorem.

Theorem 22 (Third Sylow Theorem) *The number of p–Sylow subgroups of G divides $|G|$ and is of the form $1 + kp$ for some nonnegative integer k.*

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. That is, G acts on S via $(g, Q) \mapsto gQg^{-1}$ for $Q = aPa^{-1} \in S$, as in Example 8. The orbit of P is S, and the stabilizer of P is $\{g \in G \mid gPg^{-1} = P\} = N(P)$, the normalizer of P. Therefore by Lemma 13, $|S| = [G : (N(P)] = |G| / |N(P)|$. Therefore the number of p–Sylow subgroups of G divides $|G|$, and this number is not divisible by p since $|G| / |N(P)|$ divides $|G| / |P| = q$ by Lagrange's theorem (applied to $P \subseteq N(P)$). Let us now let P act on S by conjugation. If X is the set of P–stable elements of S, then $|S| \equiv |X| \bmod p$ by Lemma 20. Since $|S|$ is not divisible by p, the set X is nonempty. Thus there is a p–Sylow subgroup $Q \in S$ such that under the action of P, the orbit of Q consists of only Q itself. This means $xQx^{-1} = Q$ for all $x \in P$. Then $P \subseteq N(Q)$. Therefore P and Q are subgroups

of $N(Q)$. But in fact, P and Q are both p–Sylow subgroups of $N(Q)$, since $|N(Q)| = p^n q'$ for some divisor q' of q. However, since Q is normal in $N(Q)$, there is a unique p–Sylow subgroup of $N(Q)$. Thus $Q = P$. This says X has only one element. But since $|X| \equiv |S|$ mod p, we obtain $|S| \equiv 1$ mod p. Therefore $|S| = 1 + kp$ for some k. This completes the proof of the third Sylow theorem. ■

References

[1] I. N. Herstein, *Topics in algebra*, Xerox College Publishing, Lexington, Mass., 1975.