0.1 Group actions

We teased the concept of group actions in **??**; now we come back to it. The abstract study of groups is a rather modern treatment. Historically, group theory only dealt with the theory of groups of permutations. However, it turns out that studying how a group acts on a set can be very insightful into the properties of groups. We already know of one example: Cayley's Theorem. We also can understand Lagrange's Theorem in the language of group actions. Later on, we will prove a partial converse to Lagrange's Theorem - the Sylow Theorems. All this is to say that the study of group actions is worthwhile.

For convenience, we shall restate the definition of a group action. At this point, the reader is likely to be sufficiently used to abstract concepts that there can be no confusion with the group action and the group multiplication.

Definition 0.1 (Group action)**.** A **group action** of G on a set S is a function $\cdot : G \times S \to S$ satisfying the following properties:

(1) **(Associativity)** For all $g, h \in G$ and $x \in S$, we have $gh \cdot x = g \cdot (h \cdot x)$.

(2) **(Identity)** For all $x \in S$, we have $e \cdot x = x$.

Sometimes, when it is clear, we will omit the use of $\cdot$, and just write gx to indicate $g \cdot x$. (Warning: Some authors such as [Jac09] are quite abusive with this notation.)

We wish to investigate further the properties of the function $\cdot$ which is defined by the action of G on S. Let G be a group and suppose G acts on S. The function $\cdot$ takes in 2 arguments; a group element and an element of S. To best investigate this function, we should probably do it by fixing one of the arguments. For now, fix some $g \in G$, and let $m_g : S \to S$ be the function given by $m_g(x) = g \cdot x$. Is m_g injective or surjective? Yes.
Exercise 0.2. Show that m_g is bijective.

The above discussion shows us that for each g, the function m_g is a bijection, hence a permutation. What we can do now is define a function $T : G \to \mathrm{Sym}(S)$ (here $\mathrm{Sym}(S)$ is the set of permutations on S), which takes $T(g) = m_g$. Both the domain and codomain of T are groups. Is T a group homomorphism? For that to hold we need $m_g \circ m_h = m_{gh}$. But this is immediate from the definition of a group action. Thus, we have a positive answer. We leave it for the reader to verify this claim.
Exercise 0.3. Check that T as defined above is indeed a group homomorphism.

After all that work, we can conclude that any group action induces a group homomorphism of G into $\mathrm{Sym}(S)$. In this case, we call the homomorphism T, the *homomorphism induced by the action of G on S*. If the context is clear, we shall simply say *action induced homomorphism* The image of the group G under T, $T[G] \subseteq \mathrm{Sym}(S)$, we shall call the *associated transformation group*.

All this discussion begs the following question: If we have a group G and a set S, and we are given a homomorphism $\varphi : G \to \mathrm{Sym}\, S$, is there some way we can define an action of G on S using φ? The answer is positive as well (see Exercise 0.22. If you think you have an idea of how to define it, don't go to the exercise yet. Try to come up with it yourself before looking at the exercise.)

Definition 0.4 (Effective action)**.** Let G act on S, and let T be the action induced homomorphism. Then we say that G **acts effectively on** S if T is injective.

Previously, we have defined the kernel of a group action to be the set

$$\{\, g \in G : g \cdot x = x \text{ for every } x \in S \,\}.$$

We will now show that the name "kernel" is not an abuse of notation - this set is exactly equal to the kernel of the homomorphism induced by the action of G.
Exercise 0.5. Let G act on S. Let $T : G \to \mathrm{Sym}(S)$ be the homomorphism induced by the action of G on S. Show that $\ker T$ is exactly equal to the kernel of the action of G on S.

We now look at examples of group actions.
Example 0.6 (Group acting on itself by left translation)**.** This example really illustrates the power of group actions - it yields the proof of Cayley's Theorem (**??**). Let G be a group and let $S = G$. We shall define an action $\cdot : G \times S \to S$ by $g \cdot x = gx$. This action is called **the action of G on itself by left translation (or left multiplication)**. Note

that on the right side, gx is the group multiplication. On the left side, $g \cdot x$ is the group action. The proof of Cayley's Theorem yields the fact that the induced homomorphism $T : G \to \mathrm{Sym}(G)$ is injective. The group of symmetries which G is isomorphic to is actually its image $T[G]$. //

Example 0.7 (Group acting on itself by right translations)**.** We can let G act on itself with right multiplications in a similar way. However, we have to be careful. Notice if we define $g \cdot x = xg$, then we have $(gh) \cdot x = xgh$, and $g \cdot (h \cdot x) = xhg$. If G is not abelian then these may not be equal. However, we can repair the issue by instead defining $g \cdot x = xg^{-1}$. Then, we have $gh \cdot x = x(gh)^{-1} = xh^{-1}g^{-1} = g \cdot (h \cdot x)$. This action is called the **action of G on itself by right translations**. We leave it for the reader to verify that this action is effective. //

Example 0.8 (Group acting on itself by conjugations)**.** Another important action of G on itself is what we shall call G **acting on itself by conjugations**. This will be essential in our proof of the Sylow Theorems. Let $S = G$. Define an action $\cdot : G \times S \to S$ by $g \cdot x = gxg^{-1}$. We can also denote this with ${}^g x$. We leave it to the reader to check that conjugation is an action. We also leave it to the reader to verify that the kernel of this action is $Z(G)$ (see Exercise 0.20).

//

Example 0.9 (Restricting the action)**.** Let G be a group acting on a set S. If H is a subgroup of G, then H also acts on S, by restricting the action of G to H, i.e. $\cdot|_H : H \times S \to S$. //

Example 0.10 (Actions on coset space)**.** Let G be a group, and let H be a subgroup of G. Recall that G/H denotes the set of all left cosets of H, i.e. $G/H = \{\, xH : x \in G \,\}$. There is a canonical action of G on G/H given by setting $g \cdot xH = (gx)H$. We shall call this the **action of G on G/H by left translations**. We leave it to the reader to show that the kernel of this action is the set of all $g \in G$ such that $g \in \bigcap_{x \in G} xHx^{-1}$. //

Recall that we defined the

Definition 0.11 (Orbit of an element)**.** Let G act on a set S, and let $x \in S$. The **orbit of x (under the action of G)** is the set

$$\mathrm{Orb}_G(x) = \{\, g \cdot x : g \in G \,\}.$$

We will write $\mathrm{Orb}(x)$ whenever the group G is clear. This is sometimes denoted $\mathcal{O}_x$[1], or $G \cdot x$.

The orbits of Example 0.10 are rather interesting. Pick some $xH \in G/H$, and let us consider what $\mathrm{Orb}(xH)$ will be. If yH is any other coset, then we have $yx^{-1} \cdot xH = yH$. What this means is $\mathrm{Orb}(xH)$ is all of the coset space G/H. We call group actions where this happens transitive actions.

Definition 0.12 (Transitive group action)**.** Let G act on S. Then we say G **acts transitively on** S if there exists $x \in S$, such that $\mathrm{Orb}(x) = S$.

Notice that if there is a single $x \in S$ with orbit being all of S, then for any $x \in S$, $G \cdot x = S$.

Exercise 0.13. Show that if there is some $x \in S$ such that $G \cdot x = S$, then for every $y \in S$, $G \cdot y = S$.

We make a trivial but important observation that if Σ is some orbit, then G acts transitively on Σ. Let's take a look at some transitive actions.

Example 0.14. Let S_n act on the set $\{\, 1, \ldots, n \,\}$ in the obvious way (i.e. $\sigma \cdot x = \sigma(x)$). Then S_n acts transitively on this set, as you should verify. //

Example 0.15. Let G act on itself by left multiplications, as in Example 0.6. Then this action is transitive, since if $x \in G$, we have $yx^{-1} \cdot x = y$, so that $G \cdot x = G$. //

Example 0.16. Similarly, the action of G on itself by right translations is transitive. //

Of course, not all group actions are transitive.

Example 0.17 (A non-transitive group action)**.** Let $O(n)$ be the orthogonal group of $\mathbb{R}^n$. Recall that elements of $O(n)$ are isometries (distance-preserving linear maps). Consider some vector $v \in \mathbb{R}^n$ with norm 1. Then for any $T \in O(n)$, it follows that $\|T(v)\| = 1$. Thus any vector with norm that is not 1 is not in the orbit of this v. //

0.1.1 Problems and Exercises

Exercise 0.18 (Left translations)**.** Check that Example 0.6 is indeed a group action. Also verify that

Exercise 0.19. Verify that the actions defined in Examples 0.6 to 0.10. are actually group actions.

[1] We will not use $\mathcal{O}_x$ since this notation is bad. However, [DF04] does.

Exercise 0.20 (Kernel of conjugation)**.** Prove that the kernel of the action of G on itself by conjugation as defined in Example 0.8 is the center of G, $Z(G)$. Conclude that this action is effective if and only if $Z(G)$ is trivial.

Exercise 0.21 (Action of a group on coset space)**.** Let G be a group and let H be a subgroup of G. Let G act on G/H canonically (as in Example 0.10).

(i) Check that this action is transitive.

(ii) Show that the kernel of this action is precisely $\bigcap_{x\in G} xHx^{-1}$. To get started, note that $gxH = xH$ if and only if $x^{-1}gx \in H$ for all x.

(iii) Show that G acts on G/H effectively if and only if H contains no nontrivial subgroups that are normal in G. (*Hint: The kernel of the action is the largest normal subgroup of G contained in H*)

Exercise 0.22 (Group actions induced by homomorphisms)**.** Let G be a group, and let S be a set. Let $\varphi : G \to \mathrm{Sym}(S)$ be a homomorphism of G into the group of symmetries on the set S.

Define the function $\cdot : G \times S \to S$ by $g \cdot x = \varphi(g)(x)$. Here, $\varphi(g)$ is a permutation on S. Verify that $\cdot$ is an action of G on S.

0.2 Transitive actions and counting

Transitive actions are special, in the sense that there is really only "one". In particular, if G acts on S transitively, then we can study this action by studying how G acts on a coset space G/H. To make this notion precise, we shall define essentially what is an "isomorphism" of group actions.

Definition 0.23 (Equivalent actions)**.** Let G act on S with $\cdot_1$ and S' with $\cdot_2$. We say that the actions of G on S and S' are **equivalent** if there is a bijection $\beta : S \to S'$ such that

$$g \cdot_2 \beta(x) = \beta(g \cdot_1 x).$$

We can express this diagramatically with

$$\begin{array}{ccc} S & \xrightarrow{g\cdot -} & S \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\beta} \\ S' & \xrightarrow[g\times -]{} & S' \end{array}$$

Here, g is fixed, and $\cdot, \times$ are actions of G on S and S' respectively. The map $g \cdot -$ is the map $s \mapsto g \cdot s$ (likewise with $g \times -$). We can understand this intuitively as saying that it does not matter whether we first do the action in S and move to S', or whether we first move over to S' and do the action in S'.

Recall we have defined the

Definition 0.24 (Stabilizer of an element)**.** Let G act on S and let $x \in S$. Then the **stabilizer of** x is the set

$$\mathrm{Stab}(x) = \{\, g \in G : g \cdot x = x \,\}.$$

The last use of stabilizers was in **??**. The ideas from this theorem will come to light in the proceeding discussion. It turns out that the stabilizer is exactly what we need to show that transitive actions are equivalent to the action of a group on some coset space.

Suppose G acts transitively on S. Pick some element $x \in S$, and let $H = \mathrm{Stab}(x)$. What do the left cosets of H represent? Well, if $h \in H$, then $h \cdot x = x$. So given some $g \in G$, then $(gh) \cdot x = g \cdot x$. Now, suppose that $g' \in G$ has the property that $g' \cdot x = g \cdot x$. This tells us that $g^{-1}g' \cdot x = x$, so that $g^{-1}g' \in H$. Equivalently, this means $g' \in gH$. We thus see that gH is the set of all the $g' \in G$ that takes x to $g \cdot x$, (i.e. $g' \cdot x = g \cdot x$ for all $g' \in H$). Now, for each $gH \in G/H$, let's associate to it the element of S, $g \cdot x$. This actually defines a map $gH \mapsto g \cdot x$ (which is well-defined, of course), with codomain in S. Does this map hit everything in S? Well, since G acts transitively on S, given any element $y \in S$, there is some g' such that $g' \cdot x = y$. This g' lives in some left coset of H. This shows that the map is actually surjective. At this point we may have an inkling that a coset gH represents exactly one element of S, namely the element $g \cdot x$. Is that true? Suppose that aH and bH both represent the element $y \in S$. This means that

$a \cdot y = b \cdot y$. Now, using the same line of reasoning as above, when investigating what left cosets of H represent, we see that $b^{-1}a \cdot y = y$, so that $a \in bH$. This means $aH = bH$.

The discussion above has proven the following

Theorem 0.25 (Transitive actions are equivalent to actions on coset space)**.** Let G act on S transitively. Let $x \in S$ be some element, and let $H = \mathrm{Stab}(x)$. Then, the action of G on S is equivalent to the action of G on G/H.

Proof. Fix $x \in S$, and let $\alpha : G \to S$ be defined by $\alpha(g) = g \cdot x$. Note that α is surjective, since the action is transitive. Thus let $\overline{G} = \{\, \alpha^{-1}(x) : x \in S \,\}$. An element $\overline{g} \in \overline{G}$ is the set $\overline{g} = \{\, a \in G : \alpha(a) = \alpha(g) \,\} = \{\, a \in G : a \cdot x = g \cdot x \,\}$. We now let $\overline{\alpha} : \overline{G} \to S$ be the map defined by $\overline{\alpha}(\overline{g}) = \alpha(g)$. This map is obviously well-defined. We claim that $\overline{\alpha}$ is bijective. Surjectivity is due to surjectivity of α. We leave it for the reader to check injectivity.

We next check that $\overline{g}$ is the left coset $g\,\mathrm{Stab}(x)$. This will show that $\overline{G} = G/\mathrm{Stab}(x)$ and so the map $\overline{\alpha}$ takes $g\,\mathrm{Stab}(x)$ to $g \cdot x$. An element a is in $\overline{g}$ if and only if $a \cdot x = g \cdot x$ if and only if $g^{-1}a \cdot x = x$, which is equivalent to $g^{-1}a \in \mathrm{Stab}(x)$. This is equivalent to $a \in g\,\mathrm{Stab}(x)$.

All that remains is to check that $\overline{\alpha}$ is indeed an equivalence of actions. We leave this for the reader. □

Exercise 0.26. Complete the proof of Theorem 0.25.

If G is a finite group, then we obtain an important

Corollary 0.27. Let G be a finite group acting transitively on a set S. Then, for any $x \in S$,

$$|S| = [G : \mathrm{Stab}(x)].$$

Proof. This follows immediately since $\overline{\alpha}$ is a bijection of G/H to S. □

Consequently, if a finite group acts transitively on a set, then the set is finite, and the cardinality of that set divides $|G|$. Of course, not all actions are transitive. Let G be a finite group acting on a finite set S. We have previously shown in **??** that orbits partition S. Since S is finite we can write

$$S = \mathrm{Orb}(x_1) \cup \mathrm{Orb}(x_2) \cup \cdots \cup \mathrm{Orb}(x_k), \tag{1}$$

where x_k are representatives of orbits. We have previously remarked that G acts transitively on $\mathrm{Orb}(x_i)$, so in particular for any $y \in \mathrm{Orb}(x_i)$, then $|\mathrm{Orb}(x_i)| = [G : \mathrm{Stab}(y)]$. Since $x_i \in \mathrm{Orb}(x_i)$ we can simply say $|\mathrm{Orb}(x_i)| = [G : \mathrm{Stab}(x_i)]$. As such, we can say that

$$|S| = \sum_{x_i \in \{\, x_1, \ldots, x_k \,\}} [G : \mathrm{Stab}(x_i)] \tag{2}$$

where the set $\{\, x_1, \ldots, x_k \,\}$ is a set of representatives of the orbits. We also remark that each term we sum over, the $[G : \mathrm{Stab}(x_i)]$'s are divisors of $|G|$.

At this point, the reader is likely curious how stabilizers of different elements within an orbit are related. Let O be some orbit and say we had $x, y \in O$. How is $\mathrm{Stab}(x)$ related to $\mathrm{Stab}(y)$? Since x and y lie in the same orbit, we have $y = g \cdot x$ for some g. Now, $a \cdot y = y$ if and only if $a \cdot (g \cdot x) = y$. We can apply g^{-1} on both sides to obtain $(g^{-1}ag) \cdot x = g^{-1} \cdot y = x$. So, $a \in \mathrm{Stab}(y)$ if and only if $g^{-1}ag \in \mathrm{Stab}(x)$. This is equivalent to saying that $a \in g\,\mathrm{Stab}(x)g^{-1}$. We shall write this as

$$\mathrm{Stab}(g \cdot x) = g\,\mathrm{Stab}(x)g^{-1}. \tag{3}$$

As such, if x and y lie in the same orbit, then their stabilizers are conjugate. Consequently, if the action is transitive, all stabilizers are conjugate to each other.

Exercise 0.28. Prove the claim in Equation (3).

0.2.1 Problems and exercises

Exercise 0.29 (Orbit-stabilizer is a corollary)**.** Show how the Orbit-Stabilizer Theorem (**??**) can be obtained as a corollary to Theorem 0.25.

Exercise 0.30. Let G be a finite group and let H be a subgroup of G such that $[G : H] = n$. Show that there is a normal subgroup N of G such that $N \subseteq H$ and $[G : N]$ is a divisor of $n!$. *(Hint: Let G act on G/H by left translations. See Example 0.10)*

Exercise 0.31 (Generalization of index 2 subgroups are normal)**.** Let G be a finite group. Let p be the *smallest* prime dividing $|G|$. Show that if H is a subgroup of G such that $[G : H] = p$, then H is normal. *(Hint: Again let G act on G/H by left translations.)*

Exercise 0.32 (Classification of groups of order p^2)**.** Let p be a prime. Prove that if G has order p^2, G is abelian. Show that there are only 2 groups of order p^2 up to isomorphism.

Exercise 0.33 (Semidirect products)**.** Let H, K be groups. We say that H *acts on K by automorphisms* if H acts on K with $\cdot$, and for every $h \in H$, the map $k \mapsto h \cdot k$ is an automorphism of K.

Suppose H acts on K by automorphisms. Let $G = K \times H$ (cartesian product). Define a binary operation on G by

$$(k_1, h_1)(k_2, h_2) = (k_1(h_1 \cdot k_2), h_1 h_2),$$

with $e_G = (e_K, e_H)$.

(i) Show that G is a group under the operation defined above.

(ii) Show that the map $h \mapsto (e_K, h)$ from H into $K \times H$ is an injective homomorphism.

(iii) Show that the map $k \mapsto (k, e_H)$ from K to $K \times H$ is an injective homomorphism, and that the image of K under this map is a normal subgroup.

(iv) Suppose H, K are finite. Show that $|G| = |K||H|$.

The construction above is called the **semi-direct product** of K and H. We will see this construction soon.

Exercise 0.34 (Primitive actions)**.** Let G be a group acting on S. Let S be a set with at least 2 elements, and let $\pi(S)$ be a partition of S. We shall say that $\pi(S)$ is **stabilized by the action of G on S** if for every $A \in \pi(S)$ and $g \in G$, then $gA = \{ g \cdot a : a \in A \} \in \pi(S)$.

There are always at least 2 partitions of S that have this property: The trivial partition of S given by $\pi_0(S) = \{ S \}$ and the partition of S into singletons, given by $\pi_1(S) = \{ s : s \in S \}$. Let us call an action of G on S **primitive** if $\pi_0(S)$ and $\pi_1(S)$ are the only partitions with this property.

(i) Show that G acts imprimitively on S if and only if there is an $A \subset S$ with at least 2 elements such that for any $g \in G$, either $gA = A$ or $gA \cap A = \varnothing$. Such a proper subset of S is called a **block**.

(ii) Show that G acts primitively on S if and only if the only blocks of S are singletons or S itself.

0.3 The class equation and Sylow theorems

Our study into group actions has proven rather fruitful into extracting insights about the structure of a group, especially when the group is finite. We first observed that if G acts on itself by left translations, we have Cayley's Theorem, telling us that every group is really just a group of permutations. Now, we shall let G act on itself by conjugations. We have lightly explored this in Example 0.8. This action will be immensely useful for us when we prove the Sylow Theorems.

Recall that Lagrange's theorem states if we have a finite group, the order of any of its subgroups must divide the order of the group. The converse is not true: given some divisor of the order of a finite group, there may not necessarily be a subgroup of that order. Not to be discourage, we shall relax the conditions on the converse slightly, and ask a weaker question: Given some prime p that divides the order of a finite group G, is there necessarily a subgroup of that order? We know this question is answered positively if G is abelian by Cauchy's Theorem for finite abelian groups (**??**). But it turns out it is true for all groups in general. In fact, something much more can be said. Namely, if p^k is a divisor of the order of a finite group G, then there is a subgroup of order p^k. This is the content of Sylow's first theorem.

Given a group action of G on a set S, we have a partitioning of S into orbits. In the finite case we can write it as in Equation (1). We shall study the orbits of G when it acts on itself by conjugation. This orbit is so important, it gets its own name,

Definition 0.35 (Conjugacy class). Let G act on itself by conjugation and let $x \in G$. The **conjugacy class of** x is the orbit of x under the action of conjugation, i.e.

$$\{ gxg^{-1} : g \in G \}.$$

The collection of all these orbits is called the set of conjugacy classes of G.

From the previous section, we have an enumeration of the set G acts on (Equation (2)). Let G be a finite group, and let G act on itself by conjugations. Given some $x \in G$, what is $\mathrm{Stab}(x)$? An element $g \in G$ stabilizes x if and only if $gxg^{-1} = x$. From **??**, this is equivalent to $g \in C(x)$. Thus $\mathrm{Stab}(x)$ is exactly equal to $C(x)$. We can thus rewrite Equation (2) as

$$|G| = \sum_{x_i \in \{ x_1, \ldots, x_k \}} [G : C(x_i)], \tag{4}$$

where $\{ x_1, \ldots, x_k \}$ is a set of representatives of all the conjugacy classes of G. However, this formula has some redundancy. It is quite possible that $C(x_i) = G$, in which case we have $[G : C(x_i)] = 1$. However, notice that $C(x_i) = G$ is equivalent to saying that x_i commutes with everything in G. This means that $x_i \in Z(G)$ if and only if $C(x_i) = G$. Actually, this means that every element of $Z(G)$ represents a conjugacy class. So instead of adding a bunch of ones (caused by $[G : C(x_i)] = 1$) for each $x_i \in Z(G)$, we might as well remove those x_i's from our set of representatives and just add $|Z(G)|$ all at once. This leaves us with the **class equation of the finite group** G.

$$|G| = |C| + \sum_{y_i \in \{ y_1, \ldots, y_m \}} [G : C(y_i)]. \tag{5}$$

Note that the set $\{ y_1, \ldots, y_m \}$ is a set of representatives of conjugacy classes of G such that the conjugacy class determined by y_i has more than one element, i.e. the orbit of y_i under the action of conjugation has more than one element. In particular, that means $[G : C(y_i)] > 1$.

The technique of using Equation (2) yields many rather useful results. We shall demonstrate the utility of the technique by using the class equation (Equation (5)) to prove the following rather useful

Proposition 0.36. If G is a finite group and G has prime power order, then $Z(G)$ is nontrivial

Proof. Suppose that $|G| = p^k$ for some $k > 0$. We consider the class equation Equation (5). On the left side, we have $|G|$ being divisible by p. On the right side, all the terms must be a power of p, since C is a subgroup of G, and each $C(y_j)$ is also a subgroup of G. Now, since $[G : C(y_j)] > 1$, we know that each of those terms is divisible by p. We can rearrange it and we have

$$|G| - \sum [G : C(y_j)] = |C|.$$

Thus p divides $|C|$, so the conclusion follows. □

We now use the class equation to prove

Theorem 0.37 (Sylow's First Theorem). Let G be a finite group. Let p be a prime, let $k \geq 0$, and suppose that p^k divides $|G|$. Then, G has a subgroup of order p^k.

Proof. Let G have order n. We shall induct on the order of G. Clearly if G has order 1 it is trivial. Suppose the result is true for all groups of order $< n$. Consider the class equation Equation (5): $|G| = |C| + \sum [G : C(y_j)]$. If p does not divide $|C|$, then there is some j such that p does not divide $[G : C(y_j)]$. This implies that p^k divides $|C(y_j)|$, since $|G| = |C(y_j)| \cdot [G : C(y_j)]$. Since $C(y_j)$ is not all of G, it has order $< n$ and so it contains a subgroup of order p^k. If p does divide $|C|$, then by **??**, there is some element $z \in C$ such that $|z| = p$. Now, $\langle z \rangle$ is normal in G (since any subgroup of C is normal), and $G/\langle z \rangle$ has order n/p, which is divisible by p^{k-1}[2]. By induction, $G/\langle z \rangle$ has a subgroup of order p^{k-1}, which is of the form $H/\langle z \rangle$ for some $H \leq G$, such that $H \supseteq \langle c \rangle$. Then we have

$$|H| = [H : \langle z \rangle] \cdot |\langle z \rangle| = p^{k-1} \cdot p = p^k.$$

[2]There is a small technicality here since we only assumed $k \geq 0$, and so p^{0-1} is nonsense. However the case when $k = 0$ is a triviality, so it is ignored. We might as well say $k > 0$, but eh.

□

A useful corollary is

Corollary 0.38 (Cauchy's Theorem for finite groups)**.** Let G be a finite group and p a prime dividing the order of G. Then, G contains an element of order p.

Proof. Immediate. □

With this theorem, we are now allowed to define what is known as a

Definition 0.39 (Sylow p-subgroup)**.** Let G be a finite group and suppose p^m is the largest power of p that divides $|G|$, i.e. $p^m \mid |G|$ and $p^{m+1} \nmid |G|$. If H is a subgroup of G of order p^m, then H is called a **Sylow p-subgroup** of G.

These are the largest subgroups of prime power order contained in G. We know these must exist because of Theorem 0.37. Sylow's Second Theorem gives us some insight into the properties of these subgroups.

Theorem 0.40 (Sylow's Second Theorem)**.** Let G be a finite group.

(1) Sylow p-subgroups of G are conjugates; that is, given Sylow p-subgroups P_1, P_2, there is some $a \in G$ such that $P_2 = aP_1a^{-1}$.

(2) If P is *any* Sylow p-subgroup, then the number of Sylow p-subgroups divides $[G : P]$. Additionally, this number is congruent to 1 modulo p.

(3) If H is a subgroup of prime power order, then it is contained in a Sylow p-subgroup.

Before we embark on the proof, let's discuss the strategy. The first part of Theorem 0.40 seems to suggest that we should consider the action of G on Sylow p-subgroups of G by conjugation. But is this even a valid action?

Let's consider the general situation. Let Γ be the set of all subgroups of G. Can we let G act on Γ by conjugation? Well, if $g \in G$, and H is a subgroup of G, then gHg^{-1} is still a subgroup of G. From here, it is not too hard to see that conjugation defines an action of G on Γ. Moreover, $\left|gHg^{-1}\right| = |H|$, since conjugation by a fixed element is an automorphism. This shows that the conjugate of a Sylow p-subgroup remains a Sylow p-subgroup (Exercise 0.42). Hence the action of G on Γ by conjugation induces an action of G on Π.

Anyway, before we proceed with the proof, we will need the following
Lemma 0.41. *Let P be a Sylow p-subgroup of G, and $H \leq G$ have order p^j such that $H \subseteq N(P)$. Then $H \subseteq P$.*

Proof. We have H being a subgroup of $N(P)$, and P is normal in $N(P)$. This implies HP is a subgroup with $HP/P \cong H/H \cap P$. Hence HP is isomorphic to a factor grop of H, so HP has prime power order p^k. Moreover, $|HP| = p^k|P|$. But P is a Sylow p-subgroup so we must have $k = 0$. This implies HP is P, and so $H \subseteq P$. □

If P is a Sylow p-subgroup of G, then P is the only Sylow p-subgroup of $N(P)$, by the lemma.

Proof of Theorem 0.40. Let Π be the set of Sylow p-subgroups of G. Consider the action of G on Π by conjugation. Let $\Sigma = G \cdot P$ be an orbit under this action, and consider the action of P on Σ. This partitions Σ into P-orbits. Call the set of these P-orbits $\mathcal{U}$. Notice that $\{P\} \in \mathcal{U}$. We next claim that this orbit is the only singleton P-orbit in Σ; if $\{P'\} \in \Sigma$, then conjugation by elements of P fixes P', hence $P \subseteq N(P')$. Thus $P = P'$ since P is the only Sylow p-subgroup of $N(P')$. Now let $\mathcal{O} \in \mathcal{U}$, and consider $|\mathcal{O}|$. It must be a power of p, since $|\mathcal{O}|$ divides $|P|$. This proves that $|\Sigma| \equiv 1 \pmod{p}$. We now show that $\Pi = \Sigma$, which will prove (2). If not, there is a $Q \in \Pi \notin \Sigma$. Use the argument above on this Q; this shows there are no Q-orbits in Σ of cardinality 1, giving $|\Sigma| \equiv 0 \pmod{p}$. This contradicts $|\Sigma| \equiv 1 \pmod{p}$. Hence $\Sigma = \Pi$ and so G acts transitively on Π. We have now proven (1). (2) is proven with the additional observation that $|\Pi| = [G : N(P)]$. To prove (3), let $H \leq G$ with order p^k. Restrict the action of G on Π to H acting on Π. The H-orbits have cardinality a power of p, and since $|\Pi| \equiv 1 \pmod{p}$, there is a singleton orbit $\{P\}$. Then $H \subseteq N(P)$ and by Lemma 0.41, $H \subseteq P$. □

0.3.1 Problems and exercises

Exercise 0.42 (Conjugate of Sylow p-subgroup is a Sylow p-subgroup)**.** Let G be a finite group, let $g \in G$ and let P be a Sylow p-subgroup. Show that gPg^{-1} is a Sylow p-subgroup.
Exercise 0.43. Show that there are no simple groups of order 148 or of order 56.
Exercise 0.44. Show that there is no simple group of order pq where p, q are primes (not necessarily distinct).
Exercise 0.45. Classify all groups of order 15.