- There's a very powerful technique where groups come into play, and that's where the group *acts* on a set, for example, a group of rotations acting on points in the plane by moving them around. We make this precise as follows.

- Let G be a group and Ω a set. We define the *action* of G on Ω as a function $\sigma : G \times \Omega \longrightarrow \Omega$ satisfying
  - $\sigma(1, x) = x$ and $\sigma(a, \sigma(b, x)) = \sigma(ab, x)$ $\forall\, x \in \Omega$, $\forall\, a, b \in G$.
  - since this gets messy enough to hide the simplicity of what's going on, we abuse notation to write $\sigma(a, x) = ax$, making our conditions $1x = x$ and $a(bx) = (ab)x$.

- Examples

  1. $\Omega = \mathbb{R}^2$, $G = \langle\, r \mid r$ is a rotation 45 degrees anticlockwise about the origin$\rangle$
  2. $\Omega = \{w_1, w_2, \ldots, w_n\}$, $G = S_n$, namely the group of permutations of n objects.
  3. G = any group, Ω = G , and define $\sigma(a, x) = a * x$, i.e., left multiplication by a.
  4. G = any group, Ω = G , and define $\sigma(a, x) = axa^{-1}$, i.e., conjugation of x by a. We wrote conjugation in the order axa^{-1} to preserve the left-right order of reading actions so that $a(bx) = (ab)x$.
  5. G = any group, $\Omega = \mathscr{P}(G)$, i.e., all subsets of G, and define $\sigma(a, H) = aH = \{ah \mid h \in H\}$. If H happens to be a subgroup, we call the set aH the *left coset* of H by a.*
  6. G = any group, $\Omega = \mathscr{P}(G)$, and define $\sigma(a, H) = a^{-1}Ha = \{a^{-1}ha \mid h \in H\}$.

- Define the *stabilizer* of $x \in \Omega$ as $G_x = \{g \in G \mid gx = x\}$, and similarly $G_A = \{g \in G \mid gA = A\}$ for $A \subseteq \Omega$, it's the set of elements of G that leave x (or similarly the set A) fixed.**

* Notice that the set of all left cosets of H *partitions* G. The same could be said of *right cosets.* If G is Abelian then aH = Ha, but that's more aggressive than needed since it enforces $ah = ha$. Allowing a to 'stir' H around a bit, so that $ah = h'a$ is all that's needed for aH = Ha ... such a subgroup H is said to be *normal*, albeit actually somewhat rare within a non-Abelian group!

** Notice that in saying that a *set* A is fixed, we do not mean that each point in it stays fixed under the action of the relevant elements of G. Rather we mean that the set A *as a whole* stays within itself; the points within it may well move around under G's provocation, but they stay within the confines of the set A. This is a very important distinction to be aware of.

- It's a fairly quick exercise (*you should do it!*) to show that the stabilizer of a point or of a subset is actually a subgroup of G. Referring back to our examples of group actions ....
- Examples
  1. $G_{(0.0)} = G$, and $G_P = \{ I \}$ for *P* any point other than the origin.
  2. $G_w = S_{n-1}$, since we can fix any particular $w \in \Omega$ and move the remaining $(n - 1)$ things around freely.
  3. $G_a = \{ I \}$ since $Ia = a$ and I is unique.
  4. $G_a = \{ g \in G \mid gag^{-1} = a \} = \mathcal{C}_G(a)$, the *centralizer* of $a \in G$, i.e., everything in G which commutes with the element *a*. (Do the elements of $\mathcal{C}_G(a)$ commute with each other, i.e., is it Abelian?)
  5. $G_H = \{ g \in G \mid gH = H \} = H$, after all, H is a group itself
  6. $G_H = \{ g \in G \mid g^{-1}Hg = H \} = \mathcal{N}_G(H)$, the *normalizer* of $H \subseteq G$, which must contain H itself, of course. Notice that $N = \mathcal{N}_G(H)$ has the property that $gN = Ng \ \forall g \in G$, so its left and right cosets coincide.
- Define $\sim$ on Ω by $a \sim b$ iff $\exists\, g \in G$ such that $b = ga$. Note that $\sim$ is an equivalence relation (reflexivity: $Ia = a$, symmetry: $g^{-1}(ga) = (g^{-1}g)a$, transitivity: $g(ha) = (gh)a$), so we define the *orbit* of $w \in \Omega$ to be $\text{orb}(w) = \{ gw \mid g \in G \} = [w]$, the equivalence class of *w*.
- Examples
  1. orb(*origin*) = {*origin*}, and orb(*P*) = circle passing through *P* and centred at the origin.
  2. $\text{orb}(w_i) = \Omega$. In such cases, where the orbit is the entire set, G is said to be *transitive*.
  3. $\text{orb}(a) = G$. Again, G is transitive.
  4. $\text{orb}(a)$ in this example is called the *conjugacy class* of $a \in G$.
  5. $\text{orb}(H) = \{ gH \mid g \in G \}$, the set of all the left cosets of H, we denote its size by $|G : H|$.
  6. $\text{orb}(H) = \{ g^{-1}Hg \mid g \in G \}$.

- We can show that $|\,\mathrm{orb}(x)\,| = |\,G : G_x\,|$ ....

  Proof: Define $\psi : \mathrm{orb}(x) \longrightarrow \{\, gG_x \mid g \in G \,\}$ by $\varphi(gx) = gG_x$.
  Is ψ well-defined? * Let $gx = hx$, then $\psi(gx) = gG_x$ and $\psi(hx) = hG_x \Longrightarrow h^{-1}g\,x = x$,
  hence $h^{-1}g \in G_x$ and so $gG_x = hG_x$.
  Furthermore, ψ is onto (by construction) and 1-1 (straightforward exercise).

- Notice that if H is a subgroup of G, then the set of left cosets of H partitions G since each left coset is itself an equivalence class within G under the relation $a \sim b \Leftrightarrow b^{-1}a \in H$ for $a, b \in G$.

- Moreover, the function $f : H \longrightarrow gH$ is a bijection, so each coset is the same size. Hence we get *Lagrange's Theorem*: $|\,G\,| = |\,G : H\,|\,|\,H\,|$, which makes most sense when G is finite, and which in the context of orbits and stabilizers is $|\,G\,| = |\,\mathrm{orb}(x)\,|\,|\,G_x\,|$. You can think of this as splitting G up into the stuff that fixes x and the stuff that moves x around.

- The analogous statements can be made for orbits and stabilizers of subsets within themselves, and here it has enormous value, not only for counting stuff (which *block* is it in, and how many *blocks* are there?), but also for writing programs which *do* things (write stuff which does things *within* some chunk, and then write stuff which *moves* that chunk around).

- As a quick application of Lagrange's Theorem, consider $G = \mathbb{Z}_p$, for p a prime. It's a group under addition, but also (if one removes the 0), a group under multiplication. Label this multiplicative group $G^\times$, then $|G^\times| = p - 1$. If $a \in G^\times$ then the size of the group generated by a, namely $\langle\, a \,\rangle = \{\, a, a^2, a^3, \ldots \,\}$, must divide $p - 1$, so $a^{p-1} = 1$, and hence $a^p = a$, or equivalently, $a^p \equiv a \pmod{p}$. This is often called *Fermat's little theorem*.**

---

* We need to check this in this case since we have *defined* what φ does by saying where it sends any particular member y of that orbit. However, that y in the orbit of x might have been possible to describe in multiple ways (e.g., as $y = gx$ or $y = hx$), yet we described where it was sent by using the g or h explicitly in saying it went to the coset gG_x or the coset hG_x. So it's important to check that *however* we *labeled* the *same* point in the domain, it ended up going to the *same* thing in the range, even if that thing is *labeled* differently.

** His 'big' theorem, stated as an extension of Pythagorus' and famous for the proclaimed proof that wouldn't fit in the margin, kept mathematicians busy for nearly 4 centuries, and was only solved 10 years ago by Andrew Wiles.