Corollary. If $p = |G|$ is a prime number, then $G \cong Z_p$.

Proof. Pick $g \in G$, $g \neq e$, denote the order of the element g by m. Then $H = \{e, g, \dots g^{m-1}\} \cong Z_m$ is a subgroup of G. But according to Lagrange's theorem $|G| = nm$. For this to be prime, $n = 1$ or $m = 1$. But $g \neq e$, so $m > 1$ so $n = 1$ and $|G| = |H|$. But then it must be $H = G$.

Definition. Let group G act on a set X. The **little group** of $x \in X$ is the subgroup $G_x = \{g \in G |\ L_g(x) = x\}$ of G. It contains all elements of G which leave x invariant. It obviously contains the unit element e, you can easily show the other properties of a subgroup. The little group is also sometimes called the **isotropy group, stabilizer** or **stability group**.

For some points x it may turn out that $G_x = G$: $L_g(x) = x\ \forall g \in G$. In this case we call x a **fixed point** under the action of G. Example: let $G = SO(2, \mathbb{R})$ act as anticlockwise rotations about the origin on the Euclidean plane $\mathbb{R}^2$. Then the origin $0 \in \mathbb{R}^2$ is a fixed point.

We may also be interested in the converse problem: finding all the points that are left invariant by the action of a given element g of a group G.

Definition. Let g be an element of a group G acting on a set X. We denote by X^g the set of points left invariant by the (left) action of g:

$$X^g = \{x \in X | L_g(x) = x\}\ .$$

Note: for the unit element e, $X^e = X$ since e is always represented by the identity map.

Back to cosets. The set of cosets G/H is a G-space, if we define the left action $l_g : G/H \to G/H$, $l_g(g'H) = gg'H$. The action is transitive: if $g_1H \neq g_2H$, then $l_{g_1 g_2^{-1}}(g_2H) = g_1H$. The inverse is also true:

Theorem 2.3 *Let group G act transitively on a set X. Then there exists a subgroup H such that X can be identified with G/H. In other words, there exists a bijection $i : G/H \to X$ such that the diagram*

$$\begin{array}{ccc} G/H & \xrightarrow{i} & X \\ l_g \downarrow & \searrow & \downarrow L_g \\ G/H & \xrightarrow{i} & X \end{array}$$

commutes.

Proof. Choose a point $x \in X$, denote its isotropy group G_x by H. Define a map $i : G/H \to X$, $i(gH) = L_g(x)$. It is well defined: if $gH = g'H$, then $g = g'h$ with some $h \in H$ and $L_g(x) = L_{g'h}(x) = L_{g'}(L_h(x)) = L_{g'}(x)$. It is an injection: $i(gH) = i(g'H) \Rightarrow L_g(x) = L_{g'}(x) \Rightarrow x = L_{g^{-1}}(L_{g'}(x)) = L_{g^{-1}g'}(x) \Rightarrow g^{-1}g' \in H \Rightarrow g' = gh \Rightarrow gH = g'H$. It is also a surjection: G acts transitively so for all $x' \in X$ there exists g s.t. $x' = L_g(x) = i(gH)$. The diagram commutes: $(L_g \circ i)(g'H) = L_g(L_{g'}(x)) = L_{gg'}(x) = i(gg'H) = (i \circ l_g)(g'H)$.

Corollary. A consequence of the proof is that the orbit of a point $x \in X$, O_x, can be identified with G/G_x since G acts transitively on its orbits. Thus the orbits are determined by the subgroups of G, in other words the action of G on X is determined by the subgroup structure.

Example. $G = SO(3, R)$ acts on $\mathbb{R}^3$, the orbits are the spheres $|x|^2 = x_1^2 + x_2^2 + x_3^2 = r^2$, *i.e.* S^2 when $r > 0$. Choose the point $x =$ north pole $= (0, 0, r)$ on every orbit $r > 0$. Its little group is

$$G_x = \left\{ \begin{pmatrix} A_{2\times 2} & 0 \\ 0 & 1 \end{pmatrix} \mid A_{2\times 2} \in SO(2, R) \right\} \cong SO(2, R) \ .$$

By Theorem 2.3 and its Corollary, $SO(3, R)/SO(2, R) = S^2$.

If G is a finite group acting on a finite set X, by a similar argument as the proof of Lagrange's theorem it follows that

$$|O_x| = \frac{|G|}{|G_x|}$$

where $|O_x|$ denotes the number of elements in the orbit of x. This is known as the **orbit-stabilizer theorem**.

The following theorem is sometimes useful in combinatorial problems, such as establishing how many different cubes can be obtained with n possible color choices for its faces, or how many necklaces or bracelets can be built with a given choice of coloured beads.

Theorem 2.4 (Burnside's lemma) *Let G be a finite group acting on a finite set X. The number of orbits, $|X/G|$, can be counted as follows:*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g| \ .$$

Proof. On the right hand side of the equation there is a sum which can be rewritten, by reversing the order of counting as follows:

$$\sum_{g\in G}|X^g| = |\{(g,x)\in G\times X|\ L_g(x)=x\}| = \sum_{x\in X}|G_x|\ ,$$

i.e., instead of counting first the elements x left invariant by an element g and then repeating the count for all g, we first count the elements g which leave a given x invariant and then repeat the count for all x. On the other hand, according to the orbit-stabilizer theorem

$$|G_x| = \frac{|G|}{|O_x|}\ .$$

In fact, all orbits A in X have the same number of elements: $|A| = |O_x|$ for all $A\in X/G$. Furthermore, we can break up the sum over all elements $x\in X$ into two separate sums: first sum over all elements x belonging to a given orbit A and then repeat this sum for all orbits A. So we can rewrite:

$$\sum_{x\in X}|G_x| = |G|\sum_{x\in X}\frac{1}{|O_x|} = |G|\sum_{A\in X/G}\sum_{x\in A}\frac{1}{|A|} = |G|\sum_{A\in X/G}1 = |G||X/G|\ ,$$

which concludes the proof.

2.4.2 Normal subgroups and quotient groups

Since the quotient space G/H is constructed out of a group and its subgroup, it is natural to ask if it can also be a group. The first guess for a multiplication law would be

$$(g_1H)(g_2H) = g_1g_2H\ .$$

This definition would be well defined if the right hand side is independent of the labeling of the cosets. For example $g_1H = g_1hH$, so we then need $g_1g_2H = g_1hg_2H$ *i.e.* find $h'\in H$ s.t. $g_1g_2h' = g_1hg_2$. But this is not always true. We can circumvent the problem if H belongs to a particular class of subgroups, so called *normal* (also called *invariant, selfconjugate*) subgroups.

Definition. A **normal subgroup** H of G is one which satisfies $gHg^{-1} = \{ghg^{-1}|\ h\in H\} = H$ for all $g\in G$.

Another way to say this is that H is a normal subgroup, if for all $g\in G, h\in H$ there exists a $h'\in H$ such that $gh = h'g$.

Consider again the problem in defining a product for cosets. If H is a normal subgroup, then $g_1hg_2 = g_1(hg_2) = g_1(g_2h') = g_1g_2h'$ is possible. One can show that the above multiplication satisfies associativity, existence of identity (it is eH) and existence of inverse $(gH)^{-1} = g^{-1}H$. Hence G/H is a group if H is a normal subgroup. When G/H is a group, it is called a **quotient group**.