Definition 15.1

Let G be a group and X be a set. Given a function

$$\mu\colon G \times X \to X$$

denote $g \cdot x := \mu(g, x)$. We say that μ is a *group action* of G on the set X if the following conditions are satisfied:

1) $(gh) \cdot x = g \cdot (h \cdot x)$ for any $g, h \in G$ and $x \in X$.
2) $e \cdot x = x$ for any $x \in X$.

Note. Let $\mu\colon G \times X \to X$ be a group action and let $g \in G$, Define a function $\varphi_g\colon X \to X$ by $\varphi_g(x) = g \cdot x$. This function is a bijection. Indeed, it is onto, since if $y \in X$, then $y = \varphi_g(g^{-1} \cdot y)$. Also, it is 1-1, since if $\varphi_g(x) = \varphi_g(x')$, then $g \cdot x = g \cdot x'$, which gives

$$x = e \cdot x = g^{-1}g \cdot x = g^{-1}g \cdot x' = e \cdot x' = x'$$

This shows that a group action μ associates to each element $g \in G$ a permutation φ_g of the set X. The property 1) in Definiton 15.1 implies that multiplication in G corresponds to composition of permutations:

$$\varphi_{gh} = \varphi_g \circ \varphi_h$$

As a consequence, we obtain a homomorphism of groups:

$$\Phi\colon G \to S(X)$$

where $S(X)$ is the group of permutations of the set X and $\Phi(g) = \varphi_g$.

Definition 15.2

Let $\mu\colon G \times X \to X$ be a group action.

- The *orbit* of an element $x \in X$ is the subset of X given by

$$\mathrm{Orb}(x) = \{gx \mid g \in G\}$$

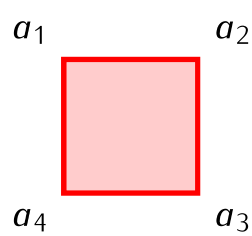
- The *stabilizer* of an element $x \in X$ is the subset of G given by

$$\mathrm{Stab}(x) = \{g \in G \mid gx = x\}$$

Example. Take the dihedral group D_4:

$\circ$	I	R_{90}	R_{180}	R_{270}	H	V	D	D'
I	I	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	I	D'	D	H	V
R_{180}	R_{180}	R_{270}	I	R_{90}	V	H	D'	D
R_{270}	R_{270}	I	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	I	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	I	R_{270}	R_{90}
D	D	H	D'	V	R_{270}	R_{90}	I	R_{180}
D'	D'	V	D	H	R_{90}	R_{270}	R_{180}	I

Elements of this group are symmetries of a square.



Let $X = \{a_1, a_2, a_3, a_4\}$ be the set of vertices of the square. For each $g \in D_4$ let $g \cdot a_i := g(a_i)$. This defines an action of D_4 on X. Since $a_1 = Ia_1$, $a_2 = R_{90}a_1$, $a_3 = R_{180}a_1$ and $a_4 = R_{270}a_1$, this action has only one orbit:

$$\mathrm{Orb}(a_1) = \{a_1, a_2, a_3, a_4\}$$

The stabilizer of the vertex a_1 consists of elements of D_4 that do not move a_1. We get $\mathrm{Stab}(a_1) = \{I, D'\}$. On the other hand, $\mathrm{Stab}(a_2) = \{I, D\}$.

Example. Let $G = \langle a \rangle$ be a cyclic group of order 2, so that $a^2 = e$. Define an action of G on the set of integers by $e \cdot n = n$ and $a \cdot n = -n$ for any $n \in \mathbb{Z}$. If $n \neq 0$ then $\mathrm{Orb}(n) = \{n, -n\}$ and $\mathrm{Stab}(n) = \{e\}$, Also, $\mathrm{Orb}(0) = \{0\}$ and $\mathrm{Stab}(0) = \{e, a\}$. Notice that for each $n \in \mathbb{Z}$ we have $\mathrm{Orb}(n) = \mathrm{Orb}(-n)$.

Example. If G is a group the we can define an action of G on itself by $g \cdot x := gxg^{-1}$. Take for example $G = D_4$. We have $\mathrm{Orb}(I) = \{gIg^{-1} \mid g \in D_4\} = \{I\}$ and $\mathrm{Stab}(I) = D_4$. On the other hand $\mathrm{Orb}(R_{90}) = \{R_{90}, R_{270}\}$ and $\mathrm{Stab}(R_{90}) = \{I, R_{90}, R_{180}, R_{270}\}$.

Theorem 15.3

Let $\mu\colon G \times X \to X$ be a group action and let $x, y \in X$. Then:

1) $x \in \mathrm{Orb}(x)$.
2) Either $\mathrm{Orb}(x) = \mathrm{Orb}(y)$ or $\mathrm{Orb}(x) \cap \mathrm{Orb}(y) = \varnothing$.
3) $\mathrm{Orb}(x) = \mathrm{Orb}(y)$ if and only if $y = gx$ for some $g \in G$.

Proof.

1) We have $x = e \cdot x \in \mathrm{Orb}(x)$.

2) Assume that $\mathrm{Orb}(x) \cap \mathrm{Orb}(y) \neq \varnothing$ and $z \in \mathrm{Orb}(x) \cap \mathrm{Orb}(y)$. Then $z = g_1 \cdot x$ and $z = g_2 \cdot y$ for some $g_1, g_2 \in G$. Then, for any $h \in G$ we obtain:

$$h \cdot x = (hg_1^{-1}) \cdot (g_1 x) = (hg_1^{-1}) \cdot (g_2 y) \in \mathrm{Orb}(y)$$

and so $\mathrm{Orb}(x) \subseteq \mathrm{Orb}(y)$. By the same argument $\mathrm{Orb}(y) \subseteq \mathrm{Orb}(x)$, and so $\mathrm{Orb}(x) = \mathrm{Orb}(y)$.

3) If $y = g \cdot x$ then $y \in \mathrm{Orb}(y) \cap \mathrm{Orb}(x)$, and so $\mathrm{Orb}(x) = \mathrm{Orb}(y)$ by 2). Conversely, if $\mathrm{Orb}(x) = \mathrm{Orb}(y)$ then $y \in \mathrm{Orb}(x)$, so $y = g \cdot x$ for some $g \in G$. $\square$

Corollary 15.4

If $\mu\colon G \times X \to X$ is a group action and X is a finite set, then

$$|X| = |\mathrm{Orb}(x_1)| + |\mathrm{Orb}(x_2)| + \cdots + |\mathrm{Orb}(x_m)|$$

where $\mathrm{Orb}(x_1), \mathrm{Orb}(x_2), \ldots, \mathrm{Orb}(x_m)$ are all different orbits of the action.

Theorem 15.5

Let $\mu\colon G \times X \to X$ be a group action and let $x \in X$.

1) $\operatorname{Stab}(x)$ is a subgroup of G.

2) If $y = gx$ then $\operatorname{Stab}(y) = g\operatorname{Stab}(x)g^{-1}$.

3) If G is a finite group then $|G| = |\operatorname{Orb}(x)| \cdot |\operatorname{Stab}(x)|$

Proof.

1) Since $ex = x$, so $e \in \operatorname{Stab}(x)$. If $g, h \in \operatorname{Stab}(x)$ then $(gh)x = g(hx) = gx = x$, so $gh \in \operatorname{Stab}(x)$. Finally, if $g \in \operatorname{Stab}(x)$ then $g^{-1}x = g^{-1}gx = ex = x$, which gives $g^{-1} \in \operatorname{Stab}(x)$.

2) Let $h \in \operatorname{Stab}(x)$. Then

$$(ghg^{-1})y = ghg^{-1}gx = ghx = gx = y$$

so $g\operatorname{Stab}(x)g^{-1} \subseteq \operatorname{Stab}(y)$. Since $x = g^{-1}y$, this also gives $g^{-1}\operatorname{Stab}(y)g \subseteq \operatorname{Stab}(y)$, or equivalently $\operatorname{Stab}(y) \subseteq g\operatorname{Stab}(x)g^{-1}$. Therefore we obtain $\operatorname{Stab}(y) = g\operatorname{Stab}(x)g^{-1}$.

3) Take the set of left cosets $G/\operatorname{Stab}(x)$. Let $f\colon G/\operatorname{Stab}(x) \to \operatorname{Orb}(x)$ be a function given by $f(g\operatorname{Stab}(x)) = gx$. Notice that f is well defined: if $g\operatorname{Stab}(x) = h\operatorname{Stab}(x)$ then $h = ga$ for some $a \in \operatorname{Stab}(x)$, so $hx = gax = gx$. Next, we show that the function f is 1-1. If $f(g\operatorname{Stab}(x)) = f(h\operatorname{Stab}(x))$ then $gx = hx$ so $g^{-1}h \in \operatorname{Stab}(x)$, which means that $g\operatorname{Stab}(x) = h\operatorname{Stab}(x)$. Also, f is onto, since if $y \in \operatorname{Orb}(x)$ then $y = gx = f(g\operatorname{Stab}(x))$.

This shows that f is a bijection and so $|G/\operatorname{Stab}(x)| = |\operatorname{Orb}(x)|$. By Lagrange Theorem 13.6 we obtain

$$|G| = |G/\operatorname{Stab}(x)| \cdot |\operatorname{Stab}(x)| = |\operatorname{Orb}(x)| \cdot |\operatorname{Stab}(x)|.$$

$\square$

Theorem 15.6 (Cauchy Theorem)

If G is a finite group and p is a prime that divides $|G|$ then there exists an element of order p in G.

Proof. Take X to be the set of all p-tuples of elements of G such the product of the p-tuple is the identity element:

$$X = \{(g_0, g_1, \ldots, g_{p-1}) \mid g_0 g_1 \cdot \ldots \cdot g_{p-1} = e\}$$

Notice that $|X| = |G|^{p-1}$, since in a tuple $(g_0, g_1, \ldots, g_{p-1})$ the elements $g_1, g_2, \ldots, g_{p-1}$ are arbitrary and $g_0 = (g_1 g_2 \cdot \ldots \cdot g_{p-1})^{-1}$. Define an action of $\mathbb{Z}_p$ on X by

$$k \cdot (g_0, g_1, \ldots, g_{p-1}) = (g_{0+k}, g_{1+k}, \ldots, g_{(p-1)+k})$$

where addition of indices is taken mod p (exercise: check that if $(g_0, g_1, \ldots, g_{p-1}) \in X$ then $(g_{0+k}, g_{1+k}, \ldots, g_{(p-1)+k}) \in X$). By Theorem 15.5 every orbit of this action divides $|\mathbb{Z}_p| = p$, so it must contain either 1 or p elements. Notice also that $|\operatorname{Orb}((g_0, g_1, \ldots, g_{p-1}))| = 1$ if and only if $g_0 = g_1 = \ldots = g_{p-1}$. One such orbit is the orbit of the tuple $(e, e, \ldots, e)$. If all other orbits consisted of p elements, then the set X would consists of $pq + 1$ elements for some q. This is however impossible, since $|X| = |G|^{p-1}$ is divisible by p. This means that there is some element $g \neq e$ such that $(g, g, \ldots, g) \in X$. Then $g^p = e$, and so $|g| = p$. $\square$

Definition 15.7

If p is a prime number then a p-group is a finite group of order p^r for some $r \geq 0$.

Corollary 15.8

A finite group G is a p-group if and only if the order of every element of G is a power of p

Proof. Let G be a p-group, $|G| = p^r$. If $g \in G$ then $|g|$ divides p^r so $|g| = p^i$ for some i.

Conversely, if G is not a p-group then there is some prime $q \neq p$ which divides $|G|$. Then by Theorem 15.6 G contains an element of order q. $\square$

Theorem 15.9

If G is a p-group then there exists an element $a \in G$ such that $a \neq e$ and $ag = ga$ for all $g \in G$.

Proof. Let $|G| = p^r$. Define an action of G on itself by $g \cdot x = gxg^{-1}$. By Theorem 15.5 every orbit $\mathrm{Orb}(x)$ of this action divides p^r, so $\mathrm{Orb}(x) = p^i$ for some $i \geq 0$. Also, $|\mathrm{Orb}(x)| = 1$ (i.e. $\mathrm{Orb}(x) = \{x\}$) if and only if $gx = xg$ for all $g \in G$. We have $\mathrm{Orb}(e) = \{e\}$. It all other orbits have more than one element, then we would have $|G| = pq + 1$ for some $q \geq 0$. This is impossible since p divides $|G|$. Thererefore there exists some element $a \neq e$ such that $\mathrm{Orb}(a) = \{a\}$. $\square$