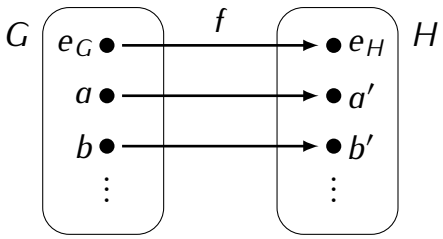
Definition 12.1

An *isomorphism of groups* is a group homomorphism which is both onto and 1-1.



Theorem 12.2

If $g: G \to H$ is an isomorphism then the inverse function $f^{-1}: H \to G$ is also an isomorphism.

Proof. The inverse function is 1-1 and onto, so it remains to prove that it is a homomorphism of groups.

Let $a', b' \in H$. We need to show that $f^{-1}(a'b') = f^{-1}(a')f^{-1}(b')$. Since f is a 1-1 function it will suffice to show that $f(f^{-1}(a'b')) = f(f^{-1}(a') \cdot f^{-1}(b'))$.

We have $f(f^{-1}(a'b')) = a'b'$. Also, since f is a homomorphism, we have

$$f(f^{-1}(a')f^{-1}(b')) = f(f^{-1}(a')) \cdot f(f^{-1}(b')) = a'b'$$

□

Theorem 12.3

A homorphism of groups $f: G \to H$ is an isomorphism if and only if $\mathrm{Im}(f) = H$ and $\mathrm{Ker}(f) = \{e\}$.

Definition 12.4

We say the group G is *isomorphic* to a group H if there exists an isomorphism $f\colon G \to H$. Then we write $G \cong H$.

Theorem 12.5

Isomorphism of groups is an equivalence relation:
1) For any group G we have $G \cong G$.
2) If G, H are groups such that $G \cong H$ then $H \cong G$.
3) If G, H, K are groups such that $G \cong H$ and $H \cong K$, then $G \cong K$.

Proof. 1) The identity function $\mathrm{id}\colon G \to G$, $\mathrm{id}(a) = a$ is an isomorphism, so $G \cong G$.

2) If $G \cong H$ then there is an isomorphism $f\colon G \to H$. In such case the function $f^{-1}\colon H \to G$ is also an isomorphism, so $H \cong G$.

3) If $G \cong H$ and $H \cong K$ then we have isomorphisms $f\colon G \to H$ and $g\colon H \to K$. Then the composition $g \circ f\colon G \to K$ is also an isomorphism and so $G \cong K$. □

Example. Recall that for a set A the group $S(A)$ of permutations of A consists of all permutations $f\colon A \to A$ with their composition as the group operation. We will show that if B is another set with the same number of elements as A then $S(A) \cong S(B)$. Indeed, let $\varphi\colon A \to B$ be a function which is onto and 1-1. We define

$$\Phi\colon S(A) \to S(B)$$

by $\Phi(\alpha) = \varphi \circ \alpha \circ \varphi^{-1}$. One can check that this is an isomorphism of groups.

In particular, recall that the symmetric group on n letters S_n is defined as the group of permutations of the set $\{1, 2, \ldots, n\}$. We obtain that if A is a set consists of n elements, then $S(A) \cong S_n$.

Example. If G, H are cyclic groups and $|G| = |H|$ then $G \cong H$. Indeed, let $G = \langle a \rangle$ and $H = \langle b \rangle$ then the function $f\colon G \to H$, $f(a^k) = b^k$ is an isomorphism.

As a consequence, we obtain that every cyclic group is isomorphic either to $\mathbb{Z}$ or to $\mathbb{Z}_n$ for some $n \geq 1$.

Example. Let $m, n > 0$ be integers such that $\gcd(m, n) = 1$. Recall that by Theorem 9.7 the group $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is cyclic of order mn. This gives: $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

Note. Let $f: G \to H$ be a homomorphism which is 1-1 (i.e. $\text{Ker}(f) = \{e\}$). Then we can obtain an isomorophism from f by replacing H with $\text{Im}(f)$:

$$f: G \to \text{Im}(f)$$

Thus any 1-1 homomorphism $f: G \to H$ defines an isomorphism between G and the subgroup $\text{Im}(f)$ of H.

Theorem 12.6 (Cayley's Theorem)

Let G be a finite group of order n. Then G is isomorphic to a subgroup of the symmetric group S_n.

Proof. Let $\overline{G}$ denote the set of elements of G. Since $\overline{G}$ consists of n elements, the symmetric group S_n is isomorphic to the group $S(\overline{G})$ of permutations of $\overline{G}$. Thus it will suffice to prove that G is isomorphic to a subgroup of $S(\overline{G})$.

To show this, it is enough to construct a 1-1 homomorphism $\Phi: G \to S(\overline{G})$. We will do it as follows. For an element $a \in G$ define a function $t_a: \overline{G} \to \overline{G}$ by $t_a(x) = ax$. This function is a permutation of the set $\overline{G}$, so it is an element of the group $S(\overline{G})$. We define: $\Phi(a) = t_a$.

We will show that the function Φ is a group homomorphism, i.e. that for any $a, b \in G$ we have $\Phi(ab) = \Phi(a) \circ \Phi(b)$. Indeed, $\Phi(ab) = t_{ab}$ and $t_{ab}: \overline{G} \to \overline{G}$ is the permutation given by $t_{ab}(x) = abx$. On the other hand,

$$\Phi(a) \circ \Phi(b) = t_a \circ t_b$$

where $t_a(x) = ax$ and $t_b(x) = bx$ We have

$$t_a \circ t_b(x) = t_a(bx) = abx = t_{ab}(x)$$

Therefore $\Phi(ab) = \Phi(a) \circ \Phi(b)$.

It remains to show that Φ is 1-1, i.e. that $\text{Ker}(\Phi) = \{e\}$. Assume then that $a \in \text{Ker}(\Phi)$. This means that $\Phi(a) = t_a$ is the identity permutation, $t_a(g) = g$ for $g \in G$. But then $ag = g$ for all $g \in G$, which means that $a = e$.

□

Definition 12.7

An *automophism* of a group G is an isomorphism $f: G \to G$.

Example. Given a group G and $a \in G$, define $f_a \colon G \to G$ by $f_a(g) = aga^{-1}$. This function is an automorphism of G. Automorphisms of this form are called *inner automorphisms*.

Note that if G is an abelian group then G for any $a \in G$ we have $f_a(g) = g$. Thus the only inner automorphism of G is the identity function.

Definition 12.8

Let G be a group. The *group of automorphisms* of G is the group $\mathrm{Aut}(G)$ whose elements are automorphisms of G and the group operation is given by composition of automorphisms.