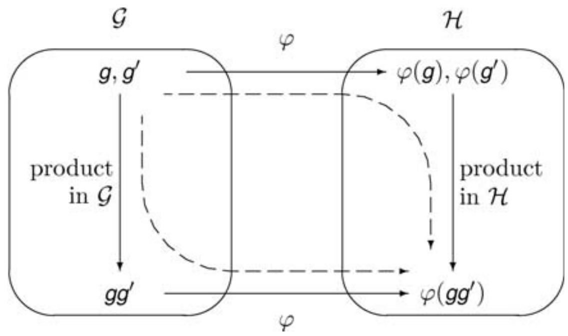

Figure 1.1.6.1
Schematic description of a homomorphism.

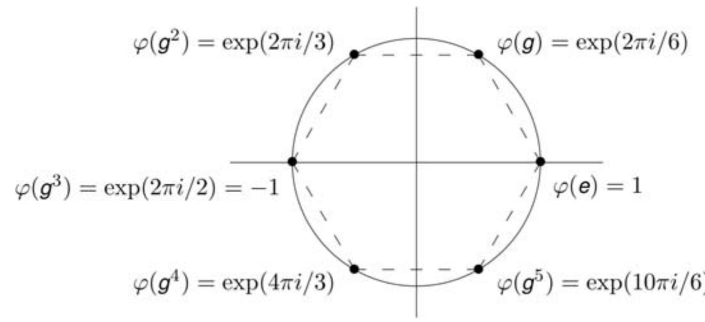

Figure 1.1.6.2
Cyclic group of order 6 embedded in the group of the unit circle.

Definition. Let φ be a group homomorphism from $\mathcal{G}$ to $\mathcal{H}$.

(i) The set $\{g \in \mathcal{G} \mid \varphi(g) = e\}$ of elements mapped to the identity element of $\mathcal{H}$ is called the *kernel* of φ, denoted by $\ker \varphi$.

(ii) The set $\varphi(\mathcal{G}) := \{\varphi(g) \mid g \in \mathcal{G}\}$ is called the *image of* $\mathcal{G}$ *under* φ.

In the case where only the identity element of $\mathcal{G}$ lies in the kernel of φ, one can conclude that $\varphi(g) = \varphi(g')$ implies $g = g'$ and φ is called an *injective homomorphism*. In this situation no information about the group $\mathcal{G}$ is lost and the homomorphism φ can be regarded as an *embedding* of $\mathcal{G}$ into $\mathcal{H}$.

The image $\varphi(\mathcal{G})$ of any homomorphism from $\mathcal{G}$ to $\mathcal{H}$ forms not just a subset, but a subgroup of $\mathcal{H}$. It is not required that $\varphi(\mathcal{G})$ is all of $\mathcal{H}$, but if this happens to be the case, φ is called a *surjective homomorphism*.

Examples

(i) For the symmetry group $4mm$ of the square a homomorphism φ to a cyclic group $\mathcal{C}_2 = \{e, g\}$ of two elements is given by $\varphi(1) = \varphi(4^+) = \varphi(2) = \varphi(4^-) = e$ and $\varphi(m_{10}) = \varphi(m_{01}) = \varphi(m_{11}) = \varphi(m_{1\bar{1}}) = g$, *i.e.* by mapping the rotations in $4mm$ to the identity element of $\mathcal{C}_2$ and the reflections to the non-trivial element.
Since every element of $\mathcal{C}_2$ is the image of some element of $4mm$, φ is a surjective homomorphism, but it is not injective because the kernel consists of all rotations in $4mm$ and not only of the identity element.

(ii) The cyclic group $\mathcal{C}_n = \{e, g, g^2, \ldots, g^{n-1}\}$ of order n is mapped into the (multiplicative) group S^1 of the unit circle in the complex plane by mapping g^k to $\exp(2\pi ik/n)$. As displayed in Fig. 1.1.6.2, the image of $\mathcal{C}_n$ under this homomorphism are points on the unit circle which form the corners of a regular n-gon.
This is an injective homomorphism because the smallest $k > 0$ with $\exp(2\pi ik/n) = 1$ is $k = n$ and $g^n = e$ in $\mathcal{C}_n$, thus by this homomorphism $\mathcal{C}_n$ can be regarded as a subgroup of S^1. It is clear that φ cannot be surjective, because S^1 is an infinite group and the image $\varphi(\mathcal{C}_n)$ consists of only finitely many elements.

(iii) For the additive group $(\mathbb{Z}, +)$ of integers and a cyclic group $\mathcal{C}_n = \{e, g, g^2, \ldots, g^{n-1}\}$, for every integer q a homomorphism φ is defined by mapping $1 \in \mathbb{Z}$ to g^q, which gives $\varphi(a) = g^{qa}$ for $a \in \mathbb{Z}$. This is never an injective homomorphism, because $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ is contained in the kernel of φ. Whether or not φ is surjective depends on whether g^q is a generator of $\mathcal{C}_n$. This is the case if and only if n and q have no non-trivial common divisors.

Definition. A homomorphism φ from $\mathcal{G}$ to $\mathcal{H}$ is called an *isomorphism* if $\ker \varphi = \{e\}$ and $\varphi(\mathcal{G}) = \mathcal{H}$, *i.e.* if φ is both injective and surjective. An isomorphism is thus a one-to-one mapping between the elements of $\mathcal{G}$ and $\mathcal{H}$ which is also a homomorphism.

Groups $\mathcal{G}$ and $\mathcal{H}$ between which an isomorphism exist are called *isomorphic groups*, this is denoted by $\mathcal{G} \cong \mathcal{H}$.

Isomorphic groups may differ in the way they are realized, but they coincide in their structure. In essence, one can regard isomorphic groups as the same group with different names or labels for the group elements. For example, isomorphic groups have the same multiplication table if the elements are relabelled according to the isomorphism identifying the elements of the first group with those of the second. If one wants to stress that a certain property of a group $\mathcal{G}$ will be the same for all groups which are isomorphic to $\mathcal{G}$, one speaks of $\mathcal{G}$ as an *abstract group*.

Examples

(i) The symmetry group $3m$ of an equilateral triangle is isomorphic to the group S_3 of all permutations of $\{1, 2, 3\}$. This can be seen as follows: labelling the corners of the triangle by $1, 2, 3$, each element of $3m$ gives rise to a permutation of the labels and mapping an element to the corresponding permutation is a homomorphism. The only element fixing all three corners of the triangle is the identity element of $3m$, thus the homomorphism is injective. On the other hand, the groups $3m$ and S_3 both have 6 elements, hence the homomorphism is also surjective, and thus it is an isomorphism.

(ii) For the symmetry group $\mathcal{G} = 4mm$ of the square and its normal subgroup $\mathcal{H}$ generated by the fourfold rotation, the factor group $\mathcal{G}/\mathcal{H}$ is isomorphic to a cyclic group $\mathcal{C}_2 = \{e, g\}$ of order 2. The trivial coset (containing the rotations in $4mm$) corresponds to the identity element e, the other coset (containing the reflections) corresponds to g.

(iii) The real numbers $\mathbb{R}$ form a group with addition as operation and the positive real numbers $\mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\}$ form a group with multiplication as operation. The exponential mapping $x \longmapsto \exp(x)$ is a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_{>0}, \cdot)$ because $\exp(x + y) = \exp(x) \cdot \exp(y)$. It is an injective homomorphisms because $\exp(x) = 1$ only for $x = 0$ [which is the identity element in $(\mathbb{R}, +)$] and it is a surjective homomorphism because for any $y > 0$ there is an $x \in \mathbb{R}$ with $\exp(x) = y$, namely $x = \log(y)$. The exponential mapping therefore provides an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_{>0}, \cdot)$.

The kernel of a homomorphism φ is always a normal subgroup, since for $h \in \ker \varphi$ and $g \in \mathcal{G}$ one has $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = e$. The information about the