Isomorphism of groups

Informally speaking: two groups are isomorphic if they have the exact same structures; only the names of the group elements (and perhaps of the operations) are different.

Definition. *Two groups* $(G, \circ)$ *and* $(H, *)$ *are* **isomorphic** *if there is a bijection* $f : G \to H$ *such that*

$$f(x \circ y) = f(x) * f(y) \quad \textit{for all} \;\; x, y \in G.$$

Such a bijection f *is sometimes called an isomorphism between* G *and* H*.*

In other words, if the images of some $a, b, c \in G$ are $a', b', c' \in H$ and $c = a \circ b$, then we must have $c' = a' * b'$. We sometimes express this as "f respects the given group operations".

While this definition seems to be one-sided – so we should say G is isomorphic *to* H –, it is easy to see that given such a bijection $f : G \to H$, the bijection $f^{-1} : H \to G$ also satisfies a similar property, and so being isomorphic is a symmetric relation. It is equally obvious that this relation is also transitive and reflexive, so group isomorphism is an equivalence relation.

Let f be an isomorphism between $(G, \circ)$ and $(H, *)$. The following properties are easily seen (we write e_G and e_H for the respective identities in the groups):

- $f(e_G) = e_H$
- $f(a^{-1}) = (f(a))^{-1}$ for all $a \in G$.

Examples. Let $G = \{e, a\}$ with operation $e \circ e = e,\; e \circ a = a \circ e = a,\; a \circ a = e$, and let $H = \{c, d\}$ with operation $c \circ c = c,\; c \circ d = d \circ c = d,\; d \circ d = c$.
Clearly, these two groups are isomorphic; we simply renamed e to c and a to d.

But they are also isomorphic to the following two groups:

Let $U = \{1, -1\}$ with operation $1 \cdot 1 = 1,\; 1 \cdot (-1) = (-1) \cdot 1 = -1,\; (-1) \cdot (-1) = 1.$

Let $\mathbb{Z}_2 = \{0, 1\}$ with operation $0 + 0 = 0,\; 0 + 1 = 1 + 0 = 1,\; 1 + 1 = 0.$

Here is a simple bijection between the last two groups which respects the operations:

$$f : \mathbb{Z}_2 \to U : x \mapsto (-1)^x$$

Homework: Find a simple (and familiar) isomorphism between the groups $(\mathbb{R}^+, \cdot)$ and $(\mathbb{R}, +)$ (the former being the set of all positive reals under multiplication).

It is easy to see that any cyclic group is Abelian and is isomorphic to one of the following: $(\mathbb{Z}, +)$, or $(\mathbb{Z}_n, +)$ for some non-negative integer n.

It is also easy to see (using Lagrange's theorem) that if the order n of a group is prime, then the group is cyclic and hence isomorphic to $(\mathbb{Z}_n, +)$.