# Lecture 11

## Isomorphisms

We see that cyclic group of order $d$ looks very similar to the group $(\mathbb{Z}_d, +)$. In some sense this is the same group, and to make this claim precise we introduce a new notion.

**Definition 1: Isomorphism**

A group *isomorphism* between groups $(G_1, *_1)$ and $(G_2, *_2)$ is a bijection

$$\varphi\colon G_1 \to G_2$$

which *respects* operations $*_1$ and $*_2$, i.e., for any $x, y \in G_1$ we have

$$\varphi(x *_1 y) = \varphi(x) *_2 \varphi(y).$$

**Proposition 1**

Let $\varphi : G_1 \to G_2$ be an isomorphism. Then $\varphi^{-1} : G_2 \to G_1$ is also an isomorphism.

*Proof.* Since $\varphi$ is a bijection, $\varphi^{-1}$ is also a bijection.
It remains to check that $\varphi^{-1}$ respects multiplication. Let $a, b, \in G_2$ be any two elements. Since $\varphi$ is a bijection, we can uniquely write

$$a = \varphi(x) \quad b = \varphi(y)$$

for the corresponding $x$ and $y$ in $G_1$. Then

$$\varphi^{-1}(a) *_1 \varphi^{-1}(b) = \varphi^{-1}(\varphi(x)) *_1 \varphi^{-1}(\varphi(y)) = x *_1 y$$

Applying bijection $\varphi$ to the right hand side we would get

$$\varphi(x *_1 y) = a *_2 b$$

since $\varphi$ respects multiplication. Thus $x *_1 y = \varphi^{-1}(a *_2 b)$, so we conclude

$$\varphi^{-1}(a) *_1 \varphi^{-1}(b) = \varphi^{-1}(a *_2 b)$$

proving that $\varphi^{-1}$ also respects multiplication. □

**Example 1**

1. The exponential function defines an isomorphism $(\mathbb{R}^*, \cdot) \to (\mathbb{R}, +)$.
2. We have encountered at least two groups of order two, namely $(\mathbb{Z}_2, +)$ and $(\{1, -1\}, \cdot)$. The map

$$\mathbb{Z}_2 \to \{1, -1\}$$

   sending 0 to 1 and 1 to $-1$ gives an isomorphism between the two.

**Definition 2**

Two groups $G$ and $G'$ are said to be isomorphic if there exists an isomorphism $\varphi : G \to G'$.

Isomorphic groups have exactly the same properties (same order, isomorphic cyclic subgroups etc.), so we often can identify them with each other.

**Claim.** Being isomorphic is an equivalence relation on the set of all groups.

The main problem of the group theory is classification of groups up to the isomorphism equivalence relation.

**Proposition 2**

A cyclic group of infinite order is isomorphic to $\mathbb{Z}$.

**Proposition 3**

Let $n \geqslant 2$ be an integer. Any cyclic group of order $n$ is isomorphic to $\mathbb{Z}_n$.

**Example 2: Direct product $\mathbb{Z}_2 \times \mathbb{Z}_2$**

The simplest example of this construction is the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ with respect to addition in both factors. It has elements

$$\{(0,0),(0,1),(1,0),(1,1)\}$$

and the operation on the above pairs via the coordinate-wise addition modulo 2.

**Example 3**

Let us now give some examples of how to prove that two groups are not isomorphic.

1. The groups $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are not isomorphic the first one being cyclic of order 4, whereas the second one has only elements of order at most 2.

2. The groups $\mathbb{Q}$ and $\mathbb{Z}$ are not isomorphic. Indeed, assume we have an isomorphism $\varphi : \mathbb{Z} \to \mathbb{Q}$ and denote $\varphi(1) = a$. By surjectivity of $\varphi$, there exists an integer $n$ such that $\varphi(n) = \frac{a}{2}$. But since $\varphi$ is a homomorphism, we must have $\varphi(2n) = 2\varphi(n) = a$, so that by injectivity of $\varphi$, $2n = 1$, which is a contradiction. Note that here the argument relied on the fact that in the group $\mathbb{Q}$ one can divide by 2 indefinitely, whereas this is not possible in $\mathbb{Z}$.

   Another way of seeing this is by remarking that for all $n \in \mathbb{Z}$, we have $\varphi(n) = n\varphi(1)$. This means that the denominator of the rational number $n\varphi(1)$ is at most the denominator of $\varphi(1)$. Since the denominators of elements of $\mathbb{Q}$ can be arbitrarily large, this means that $\varphi$ cannot be surjective.

3. The additive group $(\mathbb{Q},+)$ is not isomorphic to the multiplicative group $(\mathbb{Q}^\times,\cdot)$. Indeed, let $\varphi : (\mathbb{Q}^\times,\cdot) \to (\mathbb{Q},+)$ be an isomorphism. Put $\varphi(2) = a$. By surjectivity of $\varphi$, there is a rational number $x$ such that $\varphi(x) = \frac{a}{2}$. Then $\varphi(x \cdot x) = \varphi(x)+\varphi(x) = a$, so by injectivity, $x^2 = 2$. This is impossible since there is no rational number $x$ satisfying this. This argument is similar to the one in the previous example: here we used that dividing by 2 in the additive setting corresponded to taking square roots in the multiplicative setting, which is not always possible in the rationals.

# Cosets and Lagrange's theorem

## Left and right cosets

**Definition 3**

Let $G$ be a group and $H$ a subgroup of $G$. A *left coset* of $H$ is a subset of $G$ of the form

$$gH = \{gh,\ h \in H\}.$$

In the same way, we can define right cosets to be $Hg = \{hg,\ h \in H\}$ for $g \in G$.

**Remark 1**

The group $G$ itself is both its a left coset and a right coset, for $g = e$ the identity element of $G$: $G = eG = Ge$. More generally, for all $g \in G$, we have $G = gG = Gg$.

**Remark 2**

Left and right cosets of $H$ are the same if the group $G$ is abelian, but in general they may be different. For an abelian group, we will often use additive notation and write both types of cosets in the form $g + H$.

**Example 4**

The cosets of $H = \{0, 3\}$ in $\mathbb{Z}_6$ are

$$0 + H = 3 + H = \{0, 3\}$$

$$1 + H = 4 + H = \{1, 4\}$$

$$2 + H = 5 + H = \{2, 5\}.$$