Lecture 10

Order of an element

Recall that the order of an element a in group $(G,*)$ is the smallest positive integer such that $a^d = e$. In this case element a generates cyclic subgroup of size d:

$$\langle a\rangle = \{e, a, a^2, \dots, a^{d-1}\}.$$

Proposition 1

Element $b = a^k \in \langle a\rangle_n$ can be taken as a generator of $\langle a\rangle_n$ if and only if $\gcd(n,k) = 1$.

Proof. First we note that a has order exactly n.
Element b generates the whole group, if and only if $a \in \langle b\rangle$, i.e., for some $l > 0$ we have

$$b^l = a^{lk} = a.$$

But this happens if and only if $lk \equiv 1 \mod n$ or equivalently $a^{lk-1} = e$.
This happens if and only if element $k \in \mathbb{Z}_n$ is multiplicatively invertible (is a unit), which is equivalent to $\gcd(n,k) = 1$. □

Example 1

We saw that $\mathbb{Z}_9^\times$ is a cyclic group with generator $a = 2$ and is of order $\varphi(9) = 6$. By the above example, all other generators are 2^k, where k is any number coprime with 6, i.e., $k = 1$ and $k = 5$:

$$2^1 = 2, 2^5 = 5$$

With a slight modification to the above argument, we can answer the second question

Proposition 2

Consider any element $b = a^k \in \langle a\rangle_n$. Then

$$\langle b\rangle = \langle a^{\gcd(n,k)}\rangle_{n/\gcd(n,k)} = \{a^0, a^{\gcd(n,k)}, a^{2\gcd(n,k)}, \dots, a^{n-\gcd(n,k)}\},$$

i.e., a^k generates a cyclic subgroup of order $n/\gcd(n,k)$ which can also be generated by $a^{\gcd(n,k)}$.

Problem 1: Every cyclic subgroup is abelian.

Proposition 3

Every subgroup of a cyclic group is cyclic.

Proof. We have already proved it for infinite cyclic group (see the statement about subgroups of $\mathbb{Z}$). Now let $H \subset \langle a\rangle_n$. Choose an element $a^k \in H$ with the smallest possible $k > 0$.
It is an exercise to check that $H = \langle a^k\rangle$. □

Problem 2: Let S^3 be a group of symmetries of an equilateral triangle. Find orders of all its elements.

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 $(G,*)$ and $(G',*')$ is a bijection

$$\varphi\colon G \to G'$$

which *respects* operations $*$ and $*'$, i.e., for any $x,y \in G$ we have

$$\varphi(x*y) = \varphi(x)*'\varphi(y).$$

Problem 3: Prove that if $\varphi\colon G \to G'$ is an isomorphism, then $\varphi^{-1}\colon G' \to G$ is also an isomorphism.

Proposition 4

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

Example 2

1. The exponential function defines an isomorphism $(\mathbb{R},+) \to (\mathbb{R}_{>0},\cdot)$.
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 etc.), so we can identify them to each other.

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

Proposition 5

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

Proposition 6

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

Definition 3: Product of groups

If $(G,*)$ and $(H,*)$ are two groups, we can define a group operation on the produce $G \times H$ by setting for any $(g_1,h_1) \in G \times H$ and $(g_2,h_2) \in G \times H$

$$(g_1,h_1) \times (g_2,h_2) := (g_1 * g_2, h_1 * h_2).$$

Example 3

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 ia the coordinate-wise addition modulo 2.

Example 4

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 since, 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 φ, there exists an integer n such that $\varphi(n) = \frac{a}{2}$. But since φ is a homomorphism, we must have $\varphi(2n) = 2\varphi(n) = a$, so that by injectivity of φ, $2n = 1$, 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 φ 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 φ, 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.