Week 13

Subgroups

Definition: Consider set $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n]\}$, where $[a] = \{a + kn : k \in \mathbb{Z}\}$, $n \in \mathbb{N}$. Define on $\mathbb{Z}_n$ the following binary operation
$[a] \circ [b] = [a] + [b] = [c]$, where $a + b = kn + c$, $0 \le c < n$.

For example, in $\mathbb{Z}_5$, $[2] + [4] = [1]$.

Ex. Prove that $\mathbb{Z}_n$ with binary operation introduced above is a commutative group.

Definition: Let G be a group and H be a subset of G ($H \subset G$), $H \neq \emptyset$. Then H is called a **subgroup** of G if H is a group under the binary operation of G.

Ex. $G = \mathbb{Z}_4 = \{[0], [1], [2], [3]\}$.

(i) $H_1 = \{[0], [2]\}$ is a subgroup of $\mathbb{Z}_4$

(ii) $H_2 = \{[0], [1], [2]\}$ is not a subgroup of $\mathbb{Z}_4$ since $[1] \in H_2$, $[2] \in H_2$ but $[1] \circ [2] = [1] + [2] = [3] \notin H_2$.

Theorem 2. Let G be a group, $H \subset G$. H is a subgroup of G if and only if (a) $\forall a, b \in H$, $a \circ b \in H$ and (b) $\forall a \in H, a^{-1} \in H$.

Proof: Straightforward.

Theorem 3. Let G be a group, $H \subset G$, $H \neq \emptyset$, $|H| < \infty$. H is a subgroup of G if and only if $\forall a, b \in H$, $a \circ b \in H$.

Proof. (i) Let H be a subgroup of $G \Rightarrow \forall a, b \in H$, $a \circ b \in H$.
(ii) Let $\forall a, b \in H$, $a \circ b \in H$. Let us show that H is a subgroup of G. By Theorem 2, it is enough to show that $\forall a \in H$, $a^{-1} \in H$. Take $a \in H$ and consider $aH = \{a \circ b : b \in H\}$. Clearly, $aH = H$. Then $\exists\, b \in H$ s.t. $a \circ b = a \Rightarrow b = e \in H$. Then, $\exists\, c \in H$ s.t. $a \circ c = e \Rightarrow c = a^{-1} \in H$. □

Definition. Group G is called finite if the number of elements in G is finite, i.e. $|G| < \infty$.

Remark: Let G be a finite group and $a \in G$. Then there is a positive integer n such that $a^n = e$.

Proof. Consider the powers of a:

$$a, a^2, a^3, \ldots$$

They all belong to G. Then, since G is finite, i.e. $|G| < \infty$, then there are positive numbers k and l, $k > l$ with $a^k = a^l$. Multiplying both sides by $(a^{-1})^l$ yields $a^{k-l} = e$. $\square$

Example: $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$, $[a]+[b]=[c]$, $a+b=4k+c$, $0 \le c < 3$, $k \in \mathbb{Z}$.

Take $a = [1]$. Then $[1]^4 = [1]+[1]+[1]+[1] = [0] = e$

$[2]^2 = [2]+[2] = [0] = e$

$[3] + [3] + [3] + [3] = [3]^4 = e$.

Let's explore the idea just introduced a little more. Let G be a group and let $g \in G$. Let $\langle g \rangle$ denote the set of all powers of g, i.e.

$$\langle g \rangle = \{ g^n : n \in \mathbb{Z} \}.$$

It is clear that $\langle g \rangle$ is a subgroup of G. Indeed, it is closed under the binary operation of G:

$$g^n \circ g^m = g^{n+m} \in \langle g \rangle.$$

This group $\langle g \rangle$ is called the cyclic subgroup generated by g. We saw in Remark above that if G is finite then $\exists\, n > 0$ s.t. $g^n = e$. Choose n to be the smallest positive integer with this property, then the powers of g are

$$g^0 = e, g^1 = g, g^2, \ldots, g^{n-1}, g^n = e, g^{n+1} = g, \ldots$$

with a similar progression for the negative powers

Thus the powers of g cycle among $e, g, \dots, g^{n-1}$; this is the reason for the name "cyclic".

Definition: The order of $g \in G$ is defined to be the smallest positive integer n with $g^n = e$ if such n exists, and to be ∞ otherwise. We denote the order of g by $\text{ord}(g)$.

Proposition: Let G be a group, $g \in G$.

(1) If $\text{ord}(g) = n$ is finite then $\langle g \rangle = \{e, g, \dots, g^{n-1}\}$ and all of these powers are distinct and $|\langle g \rangle| = n$.

(2) If $\text{ord}(g)$ is infinite, then all powers of g are distinct. Thus $|\langle g \rangle| = \infty$.

Definition: A group G is said to be cyclic if $G = \langle g \rangle$ for some $g \in G$, and such an element g is said to be a generator of G.

Remark: Note that a cyclic group can have more than one generator.

$G = \mathbb{Z}$, $\circ$ is usual addition:

$\mathbb{Z} = \langle 1 \rangle$, $\mathbb{Z} = \langle -1 \rangle$

Example. Show that any cyclic group is commutative.

Solution: Let G be a cyclic group with generator g, i.e. $G = \langle g \rangle$, i.e. $\forall\, a \in G \ \exists\, n \in \mathbb{Z}$ s.t. $a = g^n$.

Then $a \circ b = g^n \circ g^m = g^{n+m} = g^{m+n} = g^m \circ g^n = b \circ a$,

where $a = g^n$ and $b = g^m$ for some $m, n \in \mathbb{Z}$.

Hence G is commutative. □

Ex. Every group with 1, 2, or 3 elements is cyclic

Solution:

(i) $|G|=1 \Rightarrow G=\{e\} \Rightarrow G=\langle e\rangle$ is cyclic

(ii) $|G|=2 \Rightarrow G=\{e,a\}$ and $a=a^{-1}$, i.e. $a^2=e \Rightarrow$
$G=\langle a\rangle$ is cyclic

(iii) $|G|=3 \Rightarrow G=\{e,a,a^{-1}\}$ and

$a\circ a\neq e$ (otherwise $a=a^{-1}$). Then
$a\circ a=a^{-1} \Rightarrow a^3=e,\ a^2=a^{-1},\ a=a$. Hence
$G=\langle a\rangle$ is cyclic.

Ex. Prove that group $G=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix}\right\}$,
$\circ$ is usual multiplication is not cyclic.

Proof. If G is cyclic then G is commutative and G is commutative

But $\begin{pmatrix}-1&0\\0&1\end{pmatrix}\begin{pmatrix}-1&0\\0&+1\end{pmatrix}=\begin{pmatrix}+1&0\\0&+1\end{pmatrix}=e$

$\begin{pmatrix}+1&0\\0&-1\end{pmatrix}\begin{pmatrix}+1&0\\0&-1\end{pmatrix}=\begin{pmatrix}+1&0\\0&1\end{pmatrix}=e$

$\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\begin{pmatrix}-1&0\\0&-1\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}=e$

Hence any cyclic subgroup of G has 2 elements. It does not coincide with G since $|G|=4$.

Homomorphism, Isomorphism.

Definition: Let G be a group with $\circ$ binary operation (or simply $(G,\circ)$) and H be a group with $*$ binary operation (or simply $(H,*)$). Function $f: G\to H$ is called a group homomorphism if $\forall a,b\in G$ $f(a\circ b)=f(a)*f(b)$.

Ex. Let $G = \mathbb{Z} \times \mathbb{Z}$ with

$(a,b) \oplus (c,d) := (a+c,\ b+d)$, where

$a+c$, $b+d$ are computed using ordinary addition in $\mathbb{Z}$.

Let $H = \mathbb{Z}$ with usual addition. Are

$f_1 : G \to H$ given as $f_1((a,b)) = ab$

$f_2 : G \to H$ given as $f_2((a,b)) = a+2b$

homomorphisms?

Solution:

(i) $f_1((a,b)+(c,d)) \stackrel{?}{=} f_1(a,b) + f(c,d)$

$f_1((a+c),(b+d)) \stackrel{?}{=} ab+cd$

$(a+c)(b+d) \stackrel{?}{=} ab+cd$

$ab+cd+ad+cb \stackrel{?}{=} ab+cd$ $\forall a,b,c,d \in \mathbb{Z}$. No

Hence f_1 is not a group homomorphism from G to H.

(ii) $f_2((a,b)+(c,d)) \stackrel{?}{=} f_2((a,b)) + f_2((c,d))$

$f_2((a+c,\ b+d)) \stackrel{?}{=} a+2b+c+2d$

$a+c+2b+2d = a+c+2b+2d$. Yes,

f_2 is a group homomorphism from G to H.

Ex. Let G be a group as in Ex above and H be any commutative group. Let $f : G \to H$ be a group homomorphism s.t. $f(1,3) = g_1$ and $f(3,7) = g_2$. Express $f(4,6)$ in terms of g_2 and g_1.

Solution: Since $-5(1,3) + 3(3,7) = (4,6)$, then

$f(4,6) = f(-5(1,3)) + f(3(3,7)) = -5f(1,3) + 3f(3,7)$

$= -5g_1 + 3g_2$

Theorem Let $(G,\circ)$, $(H,*)$ be groups with respective identities e_G, e_H. Let $f: G \to H$ be a homomorphism. Then

(a) $f(e_G) = e_H$

(b) $f(a^{-1}) = (f(a))^{-1}$ $\forall a \in G$

(c) $f(a^n) = (f(a))^n$, $\forall a \in G$, $\forall n \in \mathbb{Z}$

(d) if S is a subgroup of G, then $f(S) = \{f(a) : a \in G\}$ is a subgroup of H.

Proof:

(a) $e_H * f(e_G) = f(e_G) = f(e_G \circ e_G) = f(e_G) * f(e_G)$

$\Rightarrow e_H = f(e_G)$.

(b) Take $a \in G$.

$f(a) * f(a^{-1}) = f(a \circ a^{-1}) = f(e_G) = e_H \Rightarrow$

$f(a^{-1}) = (f(a))^{-1}$

(c) $f(a \circ a) = f(a) * f(a) = (f(a))^2$, i.e.

$f(a^2) = (f(a))^2$. Let $n \geq 2$. By induction on n,

$f(a^n) = f(a^{n-1} \circ a) = f(a^{n-1}) * f(a) = (f(a))^{n-1} * f(a) =$

$= (f(a))^n$.

Let $n \leq -2$. Then $n = -m$, $m \geq 2$

$f(a^{-m}) = f((a^m)^{-1}) = (f(a^m))^{-1} = ((f(a))^m)^{-1} =$

$= (f(a))^{-m}$

(d) Let S be a subgroup of G. Let us show that $f(S)$ is a subgroup of H. Take $c, d \in f(S)$. They are $c = f(a)$, $d = f(b)$ for some $a, b \in G$. Then $c * d = f(a) * f(b) = f(a \circ b) \in f(S)$, i.e. $f(S)$ is closed under $*$, then it is a subgroup of H. $\square$