Recall

$$Z(G) = \{ a \in G \mid ag = ga \quad \forall g \in G \}$$

$$C(a) = \{ g \in G \mid ag = ga \}$$

Theorem 13

The centre $Z(a)$ of a group is a subgroup of G

Similar proof to $C(a)$ being a subgroup, page 67

Definition

Let G be a group and $a \in G$

i) $\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$ is the set generated by a.

ii) If there is an element in G such that $\langle a \rangle = G$, then G is called a cyclic group, and a is a generator of G

Example 23

Is $\mathbb{Z}_6$ a cyclic group? $\{0, 1, 2, 3, 4, 5\}$

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \{1, 2, 3, 4, 5, 0\}$

$\langle 2 \rangle = \{2, 4, 0\}$

$\langle 3 \rangle = \{3, 0\}$

$\langle 4 \rangle = \{4, 2, 0\}$

$\langle 5 \rangle = \{5, 4, 3, 2, 1, 0\}$

$\therefore \langle 1 \rangle$ and $\langle 5 \rangle$ are equal to $\mathbb{Z}_6$, therefore the group is cyclic.

Remark

If $m \in \mathbb{Z}^+$ then $\mathbb{Z}_m$, so $\mathbb{Z}$ is cyclic for all $m \in \mathbb{Z}^+$, those are the most important cyclic groups

Proposition 14

Every cyclic group is abelian

Suppose $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$, and $g, h \in G$, WTS $gh = hg$

Then $g = a^n$, $h = a^m$ for some $n, m \in \mathbb{Z}$

$$gh = a^n a^m = \underbrace{a\,a\,a \ldots a}_{n \text{ times}}\ \underbrace{aaa \ldots a}_{m \text{ times}} = \underbrace{(aaa \ldots a)}_{m \text{ times}} \cdot \underbrace{(aaa \ldots a)}_{n \text{ times}}$$

$$= a^m a^n = hg$$

Corollary 15

D_n is not cyclic for any $n \geq 3$

We showed that D_n is not Abelian, so if D_n was cyclic, it would have to be Abelian, which is a contradiction

Example 26

What is the symmetry group of each picture? Is it cyclic?

a) Periwinkle Rotations, Cyclic $\mathbb{Z}_5$

b) Thornside Rotations, Flips D_7

c) Boric Acid Rotations, Cyclic (order 3) $\mathbb{Z}_3$

b) Snowflake Rotations, Flips D_6

Example 27

In R_{12} find $a, b \in \mathbb{Z}$ s.t. $\langle 0 \rangle \subset \langle a \rangle \subset \langle b \rangle \subset \mathbb{Z}_{12}$

Recall $\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$

$\langle 0 \rangle = \{0\}$

$\langle 2 \rangle = \{2, 4, 6, 8, 10, 0\}$

$\langle 4 \rangle = \{4, 8, 0\}$

So we could let $a = \langle 4 \rangle$ and $b = \langle 2 \rangle$

Proposition 16

Let $a \in G$, then $\langle a \rangle$ is a subgroup of G.

i) $\langle a \rangle \neq 0$ since $a \in \langle a \rangle$, and its a subset of G since $a^n \in G$ and G is closed.

ii) Suppose $g, h \in \langle a \rangle$, then $g = a^i$ $h = a^j$ for some $i, j \in \mathbb{Z}$

So $gh = a^i * a^j = a^{i+j} \in \langle a \rangle$ since $i + j \in \mathbb{Z}$

iii) Suppose $g \in \langle a \rangle$ so $g = a^i$ for some $i \in \mathbb{Z}$.

Then $g^{-1} = \bar{g}^i \in \langle a \rangle$ since $-i \in \mathbb{Z}$

Chapter 4: Cyclic Groups

What is the order of $\langle a \rangle$?

Example 28

In $U(15)$ find

a) $|7|$

$|g| = n$ means that n is the smallest positive integer s.t. $g^n = e$

$|7| = ?$ $\quad e = 1$

$7 \neq 1$

$7^2 = 49 \equiv 4 \neq 1 \pmod{15}$

$7^3 = 343 \equiv 13 \neq 1 \pmod{15}$

$7^4 = 7 \cdot 13 = 91 \equiv 1$

So $|7| = 4$

$|G| = n$ # elements in G is n

b) $\langle 7 \rangle = \{ \overset{7^1}{7}, \overset{7^2}{4}, \overset{7^3}{13}, \overset{7^4}{1}, \overset{7^5}{7}, \overset{7^6}{4}, \ldots$
$\overset{7^0}{1}, \overset{7^{-1}}{13}, \overset{7^{-2}}{4}, \overset{7^{-3}}{7}, \ldots \}$

$|\langle 7 \rangle| = 4$

Theorem 17

Let G be a group and $a \in G$

i) If a has an infinite order then $a^i = a^j$ iff $i = j$ so $|\langle a \rangle|$ is infinite

ii) If a has a finite order n, then $a^i = a^j$ iff $n | i-j$.

Also $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $|\langle a \rangle| = |a|$

Proof

i) Assume a has infinite order, ie $a^n = e$ for any positive integer n

Suppose $a^i = a^j$, WTS $i = j$, and suppose $i \neq j$ so w.l.o.g. $i > j$ $\Rightarrow$

Then $a^i a^{-i} = a^j a^{-i}$

$a^{i-j} = e$

$i - j$ positive integer, contradiction

$\therefore i = j$

Suppose $i = j$ Then $a^i = a^j$ $\Leftarrow$

ii) Suppose a has finite order $|a| = n$, ie n is the smallest positive integer such that $a^n = e$.

$\Leftarrow$ Suppose $n | i-j$, WTS $a^i = a^j$

Then $i - j = qn$ for some $q \in \mathbb{Z}$

So $a^{i-j} = a^{qn} = (a^n)^q = (e)^q = e$

$a^{i-j} = e$ so $a^i a^{-j} = e$

$a^i = a^j$ as we wanted

$\Rightarrow$ Suppose $a^i = a^j$, WTS $n | i-j$

Then $a^{i-j} = e$, then $i - j = qn + r$ for some $q, r \in \mathbb{Z}$

Where $0 \leq r \leq n-1$, WTS $r = 0$

$e = a^{i-j} = a^{qn+r} = a^{qn} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$ so $a^r = e$

$\therefore r = 0$ since n is the smallest positive integer s.t $a^n = e$

So $r = 0$, which means $i - j = qn$ so $n | i-j$

iii) Claim $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$

$\{a^n \mid n \in \mathbb{Z}\}$

Proof of Claim: Obviously $\{e, a, a^2, \ldots, a^{n-1}\}$ is a subset of $\langle a \rangle$ by definition of $\langle a \rangle$, WTS $\langle a \rangle \subseteq \{e, a, a^2, \ldots, a^{n-1}\}$

Let $x \in \langle a \rangle$ so $x = a^m$ for some $m \in \mathbb{Z}$, then $m = qn + r$ where $q, r \in \mathbb{Z}$ $0 \leq r \leq n-1$. Then $x = a^m = a^{qn+r} = a^{qn} \cdot a^r = (a^n)^q \cdot a^r$

$= e^q \cdot a^r = a^r$

So $x = a^r \in \{e, a, a^2, \ldots, a^{n-1}\}$, so $\langle a \rangle \subseteq \{e, a, \ldots, a^{n-1}\}$ $0 \leq r \leq n-1$

$\therefore \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$

iv) Claim $|\langle a \rangle| = |a|$

$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$

so $|\langle a \rangle| = |\{e, a, a^2, \ldots, a^{n-1}\}|$

Recall $|a| = n$

Also if $a^i = a^j$ then $n \mid i - j$ so all of $e, a, a^2, \ldots, a^{n-1}$ are different elements, so $|\langle a \rangle| = |\{e, a, a^2, \ldots, a^{n-1}\}| = n$

$n = |a|$

Corollary 18

For any element a in a group G, $|\langle a \rangle| = |a|$

Corollary 19

Let $a \in G$ with $|a| = n$, if $a^k = e$ then $n \mid k$, $k \in \mathbb{Z}$

Suppose $a^k = e$, and $a^0 = e$, so $a^k = a^0 \Rightarrow n \mid k-0 \Rightarrow n \mid k$

$a^i = a^j \Rightarrow n \mid i-j$

Example 29

Is $(\mathbb{Z}, +)$ cyclic ?

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

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

$-7 = 1^{-7} = -1 - 1 - 1 - 1 - 1 - 1 - 1$

$1^0 = 0 \qquad 0 = e$

$a^0 = e$

So $(\mathbb{Z}, +)$ is an infinite cyclic group

Note: $\langle -1 \rangle = \mathbb{Z}$ as well

What are the subgroups of $(\mathbb{Z}, +)$

- $H = \{$even numbers$\}$ ✓
- $\{$odd numbers$\}$ ✗
- $\{$multiples of 4$\}$ ✓
- $\{$multiples of any integer$\}$ ✓

$\{0\} = \langle 0 \rangle \quad \mathbb{Z} = \langle 1 \rangle$

Proposition 20

H is a subgroup of $(\mathbb{Z}, +)$ iff $H = \langle d \rangle$ for some integer $d \geq 0$

$\langle d \rangle = \{ n \cdot d \mid n \in \mathbb{Z} \}$

Theorem 21

Every subgroup of a cyclic group must be cyclic

A generalization of the proof of prop 20 (Th 4.3)

Proposition 22

In a finite cyclic group, the order of an element divides the order of the group