Math 4550
9/15/25

Theorem (Division algorithm)

Let $m, n \in \mathbb{Z}$ with $m > 0$.
Then there exist unique integers q and r where

$$n = mq + r \quad \text{and} \quad 0 \le r < m$$

proof:
See my 3450 or 4460 notes. $\blacksquare$

Ex: $n = 38$, $m = 4$

$$\underbrace{38 = 4 \cdot 9 + 2}_{n = mq + r}$$

$$0 \le r < 4$$

$$\begin{array}{r|l} & \;\;9 \leftarrow \boxed{q} \\ 4 & \;38 \\ & -36 \\ \hline & \;\;\;2 \leftarrow \boxed{r} \end{array}$$

Ex: $n = 40, \ m = 10$

$$\begin{array}{r} 4 \\ 10\,\overline{)\,40} \\ -40 \\ \hline 0 \end{array}$$

$\boxed{q}$ $\boxed{r}$

$$\underbrace{40 = 10 \cdot 4 + 0}_{n = m \cdot q + r}$$

$$0 \le r < 10$$

Theorem: Let G be a group. Let $x \in G$.

(a) If x has finite order n, then

$$\langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}$$

and $x^{k_1} \neq x^{k_2}$ if $0 \leq k_1 < k_2 \leq n-1$.

Thus, $|\langle x \rangle| = n$

(b) If x has infinite order, then

$$\langle x \rangle = \{\dots, x^{-3}, x^{-2}, x^{-1}, e, x, x^2, x^3, \dots\}$$

and $x^{k_1} \neq x^{k_2}$ if $k_1 \neq k_2$.

Proof:

(a) Let x have order n.

Let $S = \{e, x, x^2, \dots, x^{n-1}\}$.

We want to show

that $\underbrace{S = \langle x \rangle}$

$\langle x \rangle = \{\dots, x^{-2}, x^{-1}, e, x, x^2, \dots\}$

Clearly, $S \subseteq \langle x \rangle$.

Let's show $\langle x \rangle \subseteq S$.

Let $y \in \langle x \rangle$.

Then, $y = x^a$ where $a \in \mathbb{Z}$.

Divide n into a to get

$a = nq + r$ and $0 \leq r < n$

where $q, r \in \mathbb{Z}$.

We get

$$x^a = x^{nq+r} = x^{nq} x^r$$
$$= (x^n)^q x^r$$
$$= (e)^q x^r$$
$$= e x^r$$
$$= x^r$$

x has order n

Since $0 \leq r < n$ we get

$$y = x^a = x^r \in S$$

Thus, $\langle x \rangle \subseteq S$. $\boxed{S = \{e, x, x^2, \ldots, x^{n-1}\}}$

So, $\langle x \rangle = S$.

Now suppose $x^{k_1} = x^{k_2}$ with $0 \leq k_1 < k_2 \leq n-1$.

Then, $e = x^{k_2 - k_1}$ with $0 < k_2 - k_1 < n$.

But this would contradict the fact that x has order n.

So, $x^{k_1} \neq x^{k_2}$ if $0 \leq k_1 < k_2 \leq n-1$.

(b) Suppose x has infinite order and $\boxed{x^{k_1} = x^{k_2}}$ with $k_1 \neq k_2$.

Let's show this is a contradiction.

Suppose $k_2 > k_1$.

Then, $e = x^{k_2 - k_1}$

with $0 < k_2 - k_1$.

This contradicts x having infinite order.

So, $x^{k_1} \neq x^{k_2}$ if $k_1 \neq k_2$.

$\blacksquare$

Ex: Consider $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

Let's find all the cyclic subgroups of $\mathbb{Z}_6$

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

$\bar{0}$ has order 1

$$\langle \bar{1} \rangle = \{\bar{0}, \bar{1}, \underset{\bar{1}+\bar{1}}{\bar{2}}, \overset{\bar{1}+\bar{1}+\bar{1}}{\bar{3}}, \underset{\bar{1}+\bar{1}+\bar{1}+\bar{1}}{\bar{4}}, \overset{\bar{1}+\bar{1}+\bar{1}+\bar{1}+\bar{1}}{\bar{5}}\}$$

$\bar{1}$ has order 6

$$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \underset{\bar{2}+\bar{2}}{\bar{4}}\}$$

$\bar{2}$ has order 3

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

$\bar{3}$ has order 2

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

$\bar{4}$ has order 3

$\boxed{\bar{4} + \bar{4} = \bar{8} = \bar{2}}$

$\boxed{\bar{4} + \bar{4} + \bar{4} = \overline{12} = \bar{0}}$

$\boxed{\bar{5} + \bar{5} + \bar{5} = \overline{15} = \bar{3}}$

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

$\boxed{\bar{5} + \bar{5} = \overline{10} = \bar{4}}$

$$\underbrace{\bar{5} + \bar{5} + \bar{5}} + \bar{5}$$
$$= \bar{3} + \bar{5}$$
$$= \bar{8} = \bar{2}$$

$$\underbrace{\bar{5} + \bar{5} + \bar{5} + \bar{5}}_{\bar{2}} + \bar{5} = \bar{7}$$
$$= \bar{1}$$

$\bar{5}$ has order 6 :

$$\underbrace{\bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5}}_{\bar{1}} + \bar{5} = \bar{6} = \bar{0}$$

Cyclic subgroups of $\mathbb{Z}_6$:

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

$\langle \bar{1} \rangle = \langle \bar{5} \rangle = \mathbb{Z}_6$

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

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

$$\begin{tikzcd}
 & \mathbb{Z}_6 \arrow[dl, dash] \arrow[dr, dash] & \\
\{\bar{0}, \bar{2}, \bar{4}\} \arrow[dr, dash] & & \{\bar{0}, \bar{3}\} \arrow[dl, dash] \\
 & \{\bar{0}\} &
\end{tikzcd}$$

later we will see these are all the subgroups of $\mathbb{Z}_6$

Fast method:

HW: G is a group, $x \in G$.

Then, $\langle x \rangle = \langle x^{-1} \rangle$

So in the above $\mathbb{Z}_6$ example

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

$\bar{5} + \bar{1} = \bar{0}$

So, $\bar{5}^{-1} = \bar{1}$

Def: We say that a group G is cyclic if there exists $x \in G$ with $G = \langle x \rangle$.

Ex: $\mathbb{Z}_6 = \langle \bar{1} \rangle$

So, $\mathbb{Z}_6$ is cyclic.

In general $\mathbb{Z}_n$ is cyclic since $\mathbb{Z}_n = \langle \bar{1} \rangle$.

Ex: $U_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$

$= \langle \zeta \rangle$ is cyclic

where $\zeta = e^{2\pi i/n}$

Ex:

$$\mathbb{Z} = \langle 1 \rangle = \{\ldots, \underbrace{-3}_{(-1)+(-1)+(-1)}, \overbrace{-2}^{(-1)+(-1)}, -1, 0, 1, \overbrace{2}^{1+1}, \underbrace{3}_{1+1+1}, \ldots\}$$

$\mathbb{Z}$ is cyclic

Theorem: If G is a cyclic group, then G is abelian

Proof:

Let G be a cyclic group.

Then there exists $x \in G$ where $G = \langle x \rangle$.

Let $a, b \in G$.

Then, $a = x^{n_1}$ and $b = x^{n_2}$ where $n_1, n_2 \in \mathbb{Z}$.

So,

$$
\begin{aligned}
ab = x^{n_1} x^{n_2} &= x^{n_1 + n_2} \\
&= x^{n_2 + n_1} \\
&= x^{n_2} x^{n_1} = ba.
\end{aligned}
$$

So, G is abelian. $\blacksquare$