# Sections 4 & 5

31/1 I

Last time: "Group" is binary algebraic structure $(G, *)$ satisfying

$G_1$: $*$ is associative

$G_2$: There is an identity element $e \in G$ for $*$

$G_3$: For each $a \in G$, there is an inverse $a' \in G$, i.e.

$$a * a' = a' * a = e.$$

Examples $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}^n, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{Z}_n, +_n)$, $(U_n, \cdot)$, $(GL_n(\mathbb{R}), *)$ matrix multiplication.

## Properties of groups

Norsk: Kansellerings lover

**Cancellation laws**: Let $(G, *)$ be a group, $a, b, c \in G$.

① $a * b = a * c \implies b = c$ "left cancellation law"

② $b * a = c * a \implies b = c$ "right cancellation law"

Proof of ①: $a * b = a * c \overset{G_3}{\implies} a' * (a * b) = a' * (a * c)$

$\overset{G_1}{\implies} (a' * a) * b = (a' * a) * c \implies e * b = e * c \implies b = c$ □

Example • Consider equation $x + y = x + 5$, $x, y \in \mathbb{Z}$, this implies $y = 5$.

• Consider equation $xy = x \cdot 5$, $x, y \in \mathbb{Z}$, does not imply $y = 5$, since may have $x = 0$, $y =$ whatever.

• "Explanation": $(\mathbb{Z}, +)$ is a group, $(\mathbb{Z}, \cdot)$ is not.

**Proposition** Let $(G, *)$ be group, $a, b \in G$. Equations

$$\textcircled{1} \quad x * a = b \qquad x \in G$$
$$\textcircled{2} \quad a * y = b \qquad y \in G$$

each have exactly one solution.

**Proof of ①:** $x * a = b \Rightarrow (x * a) * a' = b * a' \Rightarrow x * (a * a') = b * a'$
$\Rightarrow x * e = b * a' \Rightarrow x = b * a'$.

Check $x = b * a'$ is solution:
$(b * a') * a = b * (a' * a) = b * e = b$. □

**Proposition** Let $(G, *)$ be group.

① There is exactly one identity element. $e \in G$
② For every $a \in G$, there is exactly one inverse $a' \in G$.

**Proof** ①, last lecture. For ②, inverse of $a$ solves equation

$$x * a = e,$$

hence is unique.

**Proposition** ("Sudoku property") Let $(G, *)$ be a finite group. In each row (or column) of the multiplication table for $G$, each element of $G$ appears exactly once.

Example:

$\mathbb{Z}_3$

| $+_3$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

Proof:

| $*$ | | $a$ |
|---|---|---|
| | | |
| | | |
| $b*a'$ | | $b$ |
| $e$? | | $b$? |

Let $a, b \in G$, consider column under $a$, to prove $b$ appears exactly once.

At least once: Yes $(b*a')*a = b$

Only once: If $b$ appears in row $c$, have

$$e*a = (b*a')*a = b$$

$\Downarrow$ ← right cancellation

$$c = b*a'.$$

□

Norsk: Ordenen til $G$.

Def The order of a group $G$ is the number of elements of $G$, denoted $|G|$.

The group of order 3: Assume $(G, *)$ has order 3, $G = \{e, a, b\}$. What is $*$?

| $*$ | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | ? | |
| $b$ | $b$ | | |

$?=e$ →

| $*$ | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | $e$ | |
| $b$ | $b$ | $b$ | |

impossible

$?=b$ →

| $*$ | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | $b$ | $e$ |
| $b$ | $b$ | $e$ | $a$ |

$\simeq$

| $+_3$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

$$(G, *) \simeq (\mathbb{Z}_3, +_3).$$

New notation: Usually don't write $a*b$, instead one of two notational conventions:

Multiplicative: $a, b \in G$, write $ab$ for $a*b$.

- $a^{-1} = a'$, the inverse
- For $n > 0$, $a^n = \underbrace{aa\cdots a}_{n \text{ times}}$* $a^{-n} = \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{n \text{ times}}$
- $a^0 = e$

*This makes sense because of associativity!

Fact: For $m, n \in \mathbb{Z}$, have

$$a^{m+n} = a^m a^n,$$

e.g.

$$a^3a^{-2} = aaa\,a^{-1}a^{-1} = aaea^{-1} = aaa^{-1} = a = a^{3-2}.$$

Additive (only if $G$ is abelian, $a*b = b*a$ for all $a, b \in G$)

- $a+b$ for $a*b$
- $0 = e$
- $-a = a'$, the inverse
- For $n > 0$, $na = \underbrace{a+a+\cdots+a}_{n \text{ times}}$, $-na = \underbrace{(-a)+\cdots+(-a)}_{n \text{ times}}$
- $0a = 0$

Fact: For $m, n \in \mathbb{Z}$, $(m+n)a = ma + na$.

## Subgroups

Def Let $G$ be a group. If $H \subseteq G$ is closed under the binary operation of $G$, and $H$ with the induced operation is a group, we call it a subgroup of $G$, written $H \leq G$.

Norsk: Undergruppe

Examples · Let $G=(\mathbb{C},+)$. Then $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are subgroups. $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$ are closed under $+$, but lack inverses, so are not subgroups.

Norsk

**Def** Let $G$ be a group, some special subgroups $H \leq G$:

Den uekte undergruppa — $H=G$: "the improper subgroup"

Triviell undergruppe — $H=\{e\}$: "the trivial subgroup"

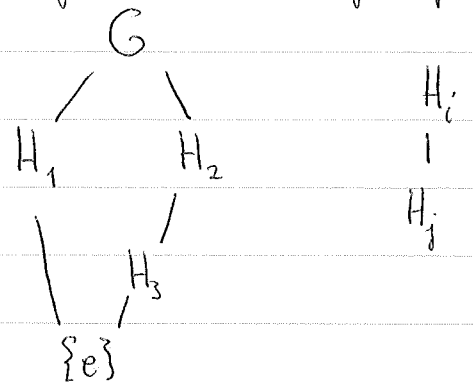
Ekte undergruppe — $H \neq G \iff H$ is a proper subgroup, write $H<G$

Ikketriviell undergruppe — $H \neq \{e\} \iff H$ is a nontrivial subgroup.

**Thm** Let $G$ be a group, $H \subseteq G$. $H$ is a subgroup if the following holds:

1. $H$ is closed under binary op. of $G$.
2. The identity element of $G$ lies in $H$
3. For all $a \in H$, we have $a^{-1} \in H$. ($a^{-1}$: the inverse in $G$.)

Subgroup diagrams: $G$ a group, $H_1, \ldots, H_r \leq G$, draw as




means $H_j < H_i$.

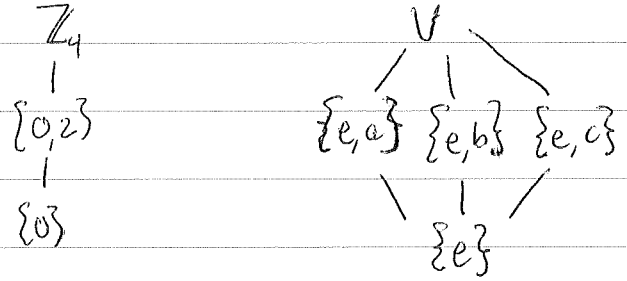
Example Groups of order 4, up to isomorphism 2 kinds, $(\mathbb{Z}_4, +_4)$ & $V$, "Klein 4-group"

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| V | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | a | e |

Subgroups of $\mathbb{Z}_4$: $\{0\}$, $\{0,2\}$, $\{0,1,2,3\}$

Subgroups of $V$: $\{e\}$, $\{e,a\}$, $\{e,b\}$, $\{e,c\}$, $V$




E.g. if $H \leq V$ contains $\{e,a,b$, it contains $ab=c$, so $H=V$.

## Cyclic (sub-)groups

Let $G$ be a group, $a \in G$. Let $H \leq G$, assume $a \in H$. Then
$aa = a^2 \in H$, $aa^2 = a^3 \in H$, ..., $a^n \in H$ for all $n > 0$.
$a^{-1} \in H$, $a^{-1}a^{-1} = a^{-2} \in H$, ..... $a^{-n} \in H$ for all $n > 0$.

$$\rightsquigarrow \{a^n \mid n \in \mathbb{Z}\} \subseteq H.$$

**Thm** Let $G$ be group, $a \in G$. Then

$$\langle a \rangle \overset{\text{def.}}{=} \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of $G$.

Pf Closed under operation: $a^m a^n = a^{m+n} \in \langle a \rangle$
Identity: $a^0 = e \in \langle a \rangle$
Inverses: $a^n$ has inverse $a^{-n} \in \langle a \rangle$.

Norsk: Syklisk

**Def** The group $\langle a \rangle$ is the cyclic subgroup of $G$ generated by $a$. If $G = \langle a \rangle$, say

- $G$ is a cyclic group
- $G$ is generated by $a$

Example: $\mathbb{Z}$ is cyclic, generated by either 1 or -1.

Example All subgroups of $\mathbb{Z}_4$ are cyclic:

$\mathbb{Z}_4 = \langle 1 \rangle = \langle 3 \rangle$

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

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

All proper subgroups of $V$ are cyclic:

$\{e,a\} = \langle a \rangle$

$\{e,b\} = \langle b \rangle$

$\{e,c\} = \langle c \rangle$

$\{e\} = \langle e \rangle$

$V$ is not cyclic.

Example In $\mathbb{Z}$, $\langle n \rangle = n\mathbb{Z} = \{ na \mid a \in \mathbb{Z} \}$.