$\boxed{\text{Subgroups}}$ Let G be a group. $H \subseteq G$ is a "subgroup" of G if H is a group (w.r.t. the same operation)

Notation: $H \leq G$

Test for subgroup: a.) $H \subseteq G$ b.) $x, y \in H \Rightarrow xy^{-1} \in H$

<u>Coset decomposition</u> Let $H \leq G$.

$x \sim y \Leftrightarrow x^{-1}y \in H \Leftrightarrow y \in xH$ is an equ. relation

proof:
- $x \sim x$ since $x^{-1}x = e \in H$
- $x \sim y \Rightarrow x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} = y^{-1}x \in H \Rightarrow y \sim x$
- $x \sim y, y \sim z \Rightarrow x^{-1}y, y^{-1}z \in H \Rightarrow x^{-1}yy^{-1}z = x^{-1}z \in H \Rightarrow x \sim z$

Note: the proof needs e, inverse $\in H$ and closed under "$\cdot$". hence only subgroups make $\sim$ an equ. relation.

- $[x] = xH$ is called "left coset"
- notation: $G/\sim \; = G/H$
- $|xH| = |yH| = |H|$ for $x, y \in G$
- if $|G/H|$ finite: $G = x_1 H \cup \ldots \cup x_n H$ (one of these is $= H$)
  "coset decomposition"

- analogously: define right cosets via $x \sim y \Leftrightarrow xy^{-1} \in H$

<u>Lemma:</u> $|G| = \underbrace{|G/H|}_{\text{index of } H \text{ in } G} \cdot |H|$

We have decomposed G into the subgroup H and G/H. Ideally, G/H is also a group w.r.t.:

$$[x] \cdot [y] = [xy]$$

$$xH \cdot yH = xy \cdot H$$

Need to assure well-defined. Other group properties are straightforward.

Check: $a \sim x,\ b \sim y \Rightarrow ab \sim xy$

$a = xh,\ b = yh' \quad h, h' \in H$

$\Rightarrow ab = xhyh' = \underbrace{xyy^{-1}hyh'}_{\in xyH \iff y^{-1}hy \in H}$

Result: "$\cdot$" well-defined $\iff$ for all $h \in H, y \in G: y^{-1}hy \in H$

$\iff$ for all $y \in G: y^{-1}Hy \subseteq H$

$\iff$ " $\quad y^{-1}Hy = H$

or $\quad Hy = yH$

<u>Definition:</u> $H \leq G$ is called a "normal subgroup" if for all $y \in G$, $y^{-1}Hy = H$. Notation: $H \trianglelefteq G$.

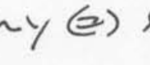
<u>Lemma:</u> If $N \trianglelefteq G$, then G/N is a group called a "factor group."
If G is abelian then every subgroup is normal.

$$\boxed{G/H \text{ a group} \iff H \trianglelefteq G}$$

Brief discussion on the classification of groups and especially simple groups (groups without normal subgroups) which was finished ~ 2000.

Examples:

a.) $C_4 = \langle x \mid x^4 = 1 \rangle = \{1, x, x^2, x^3\}$, $H = \langle x^2 \rangle = \{1, x^2\} \trianglelefteq C_4$
$\Rightarrow H$ is a C_2 and C_4/C_2 is a group (of size 2)

b.) $G = \mathbb{R}$ (with $+$), $H = \mathbb{Z} \trianglelefteq \mathbb{R}$, $x \sim y \iff x - y \in \mathbb{Z}$
$\mathbb{R}/\mathbb{Z}$ is the group $\{[\alpha] \mid \alpha \in [0,1)\}$:  or better since $0 \sim 1$

c.) $(n\mathbb{Z}, +) \trianglelefteq (\mathbb{Z}, +) \Rightarrow (\mathbb{Z}/n\mathbb{Z}, +)$ is a group,

In fact a cyclic group of size n.

$\boxed{\text{group homomorphism}}$ greek: homo – same
morphos – shape

<u>Definition</u>: A group homomorphism is a mapping $\varphi: G \to H$ (G, H groups) s.t. $\varphi(xy) = \varphi(x)\varphi(y)$, $x, y \in G$.

<u>Lemma</u>: a.) e, e' neutral elements of G, H, resp.
$\Rightarrow \varphi(e) = e'$
b.) $\varphi(x)^{-1} = \varphi(x^{-1})$

$\varphi: G \to H$ hom. + bij.
$\Rightarrow \varphi$ "isomorphism"
(greek: iso – equal)
Then: $G \cong H$
(G isomorphic to H)

Examples:
- $\varphi: (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$
  $x \mapsto \log_2(x)$
- $H \leq G$, $\varepsilon: H \to G$, $x \mapsto G$ called "embedding" (injective)
- $N \trianglelefteq G$, $\kappa: G \to G/N$, $x \mapsto xN$ called "canonical (surjective) projection"

$\boxed{\text{Kernel}}$ $\varphi: G \to H$ hom. $\mathrm{Ker}(\varphi) = \{x \in G \mid \varphi(x) = \underset{\uparrow}{e'}\}$ is called "kernel of φ." neutral element in H

<u>Lemma</u>: a.) $\ker\varphi \trianglelefteq G$
b.) Every $N \trianglelefteq G$ is kernel of a suitable hom.
c.) $G/\varphi = G/\ker\varphi$

proof: a.) - $\ker\varphi \subseteq G$ ✓
- $x, y \in \ker\varphi \Rightarrow \varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = e'e'^{-1} = e' \Rightarrow xy^{-1} \in \ker\varphi \Rightarrow \ker\varphi \leq G$.
- $x \in \ker\varphi$, $y \in G \Rightarrow \varphi(y^{-1}xy) = \varphi(y)^{-1}\varphi(x)\varphi(y)$
$= \varphi(y)^{-1}e'\varphi(y) = e' \Rightarrow \ker\varphi \trianglelefteq G$.

b.) Choose $\varphi: G \to G/N$

c.) Equ. rel induced by φ: $x \sim y \Leftrightarrow \varphi(x) = \varphi(y)$
" " by $\ker\varphi$: $x \sim y \Leftrightarrow x^{-1}y \in \ker\varphi$
$\Leftrightarrow y = xk, k \in \ker\varphi$
$\Leftrightarrow \varphi(y) = \varphi(xk) = \varphi(x)\varphi(k) = \varphi(x)$ ∎

As a consequence of c.) we get the canonical factorization:

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, "\pi:\, x \mapsto [x]", "\text{surj.}"'] & H \\
G/\ker\varphi = G/\varphi \arrow[r, "\bar\varphi:\, [x] \mapsto \varphi(x)"', "\text{bijective}"] & \varphi(G) \arrow[u, "\varepsilon:\, x \mapsto x \;\; \text{inj.}"']
\end{tikzcd}$$

$$\Rightarrow |G/\ker\varphi| = |\varphi(G)|$$

But $\bar\varphi$ is also a hom:

$$[x], [y] \in G/\ker\varphi \xrightarrow{\text{map}} \bar\varphi([x]), \bar\varphi([y]) \xrightarrow{\text{mult}} \bar\varphi([x])\bar\varphi([y]) \overset{\text{def}}{=} \varphi(x)\varphi(y)$$

$$[x], [y] \in G/\ker\varphi \xrightarrow{\text{mult}} [xy] \xrightarrow{\text{map}} \bar\varphi([xy]) \overset{\text{def}}{=} \varphi(xy) \quad \Big\| \text{ since } \varphi \text{ is a hom}$$

<u>Theorem:</u> $\varphi: G \to H$ a hom. Then

$$\boxed{G/\ker\varphi \cong \varphi(G)} \qquad \text{hom. theorem}$$

Summary: What we did

general	groups
definition	group def.
generators	group generators $\langle \dots \rangle$
substructure	subgroup H
homomorphism	group hom. φ
kernels of homs	normal subgroups N
factor structures	factor groups G/N
hom. theorem	$G/\ker\varphi \cong \varphi(G)$

Little history of group theory

- one origin: study of symmetries by the Moors (13th century)
- groups to solve polynomial equations: Evariste Galois (1811–1832) in 1829. Termed "group" and "normal subgroup".
- Study of groups: Arthur Cayley (1821–1895) in the 1850s
- First complete def. of an abstract group (as taught today): Heinrich Weber (1842–1913) in 1882. Termed "abelian".

More info: Wikipedia