Last time: A subgroup N of a group G is normal (notation: $N \trianglelefteq G$)
iff $\forall g \in G$, $\forall n \in N$ $\quad gng^{-1} \in N$.

We proved: $N \trianglelefteq G \iff \forall g \in G \quad gN = Ng$.

Theorem 14.1 (compare: Thm 1 on p132 of Nicholson)
Let N be a normal subgroup of the group G. Then set of (left) cosets $G/N := \{gN\}_{g \in G}$ of N has a unique binary operation $*$ which makes G/N into a group and $\pi: G \to G/N$ into a homomorphism.

Proof (uniqueness) If $*$ exists and $\pi: G \to G/N$ is a homomorphism then $\forall a, b \in G$ $\quad \pi(ab) = \pi(a) * \pi(b)$
Since π is onto, there is only one choice for $*$; namely

$$(\star) \quad (aN) * (bN) = (ab)N$$

for all $aG = \pi(a)$, $bG = \pi(b) \in G/N$.

(existence)
We should define $*$ by $\quad aN * bN := abN$.
We need to check that this makes sense; that is, if
$aN = a'N$, $\quad bN = b'N$ then $(ab)N = (a'b')N$.
Now $aN = a'N \Rightarrow a = a'n_1$ for some $n_1 \in N$
$\qquad bN = b'N \Rightarrow b = b'n_2$ for some $n_2 \in N$
Hence $\quad ab = a'n_1 b'n_2 = a'b' \underbrace{(b')^{-1} n_1 b'}_{\in N} n_2 \in a'b'N$

$\Rightarrow \quad abN = a'b'N$.
$\therefore$ $*$ is well-defined

Note: $\forall aN \in G/N$ $\quad (aN) * (eN) = (ae)N = aN$
and $(eN) * aN = (ea)N = aN$

Remains to check: $(G/N, *, eN)$ is a group:
$*$ is associative and $\forall aN \in G/N$ $\exists bN \in G/N$ s.t.
$(aN) * (bN) = eN = (bN) * (aN)$)

Now $(aN)*(a^{-1}N) = aa^{-1}N = eN$

and similarly $(a^{-1}N)*aN = eN$

$\therefore \quad (aN)^{-1} = a^{-1}N.$

Also $\forall a,b,c \in G$

$$((aN)*(bN))*cN = (abN)*cN = ((ab)c)N$$
$$= (a(bc))N = \cdots = aN*(bN*cN). \qquad \square$$

"Example" $G = (\mathbb{Z},+,0)$ $\quad H = n\mathbb{Z} \trianglelefteq \mathbb{Z}$ since $\mathbb{Z}$ is abelian

$\Rightarrow G/H = (\mathbb{Z}/n\mathbb{Z}, \text{"}+\text{"}, [0])$

Recall Given a homomorphism $f: G \to H$, $K = \ker f$ is a normal subgroup and we have a well-defined map $\bar{f}: G/K \to H$, $\bar{f}(gK) = f(g)$. which is injective. Note $\operatorname{im}\bar{f} = \operatorname{im} f$

$(\operatorname{im} f = \{f(g) \mid g \in G\}$, $\operatorname{im}\bar{f} = \{\bar{f}(gK) \mid g \in G\} = \{f(g) \mid g \in G\})$

Recall also: $\operatorname{im} f$ is a subgroup of H

We just proved: G/K is a group

1st isomorphism theorem Let $f: G \to H$ be a homomorphism Then $\bar{f}: G/K \to \operatorname{im} f$ is an isomorphism (where $K = \ker f$).

Proof We know that $\bar{f}$ is a bijection. Moreover

$$\bar{f}((aK)*(bK)) = \bar{f}(abK) = f(ab) = f(a)f(b) = \bar{f}(aK)\cdot\bar{f}(bK) \qquad \square$$

Example $f: \mathbb{R} \to \mathbb{C}^\times$, $f(\theta) = e^{2\pi i\theta}$ is a homomorphism.

$\operatorname{im} f = \{e^{2\pi i\theta} \mid \theta \in \mathbb{R}\} = \{\lambda \in \mathbb{C}^\times \mid |\lambda| = 1\} = U(1) = S^1$.

$K = \ker f = \{\theta \mid e^{2\pi i\theta} = 1\} = \mathbb{Z}$. $\quad$ 1st iso Thm $\Rightarrow$

$$\bar{f}: \mathbb{R}/\mathbb{Z} \to U(1) \qquad \bar{f}(\theta + \mathbb{Z}) = e^{2\pi i\theta}$$

is an isomorphism of groups.

<u>Ex</u> $\det : O(n) \to \mathbb{R}^\times = \{x \in \mathbb{R} \mid x \neq 0\}$, $A \mapsto \det A$
$\mathrm{Im}(\det) = \{\pm 1\}$ $\quad$ $\ker \det = \{A \in O(n) \mid \det A = 1\} \equiv SO(n)$.
Hence $SO(n) \trianglelefteq O(n)$ and by 1^{st} iso theorem

$$O(n)/SO(n) \simeq \{\pm 1\}$$
$$A\,SO(n) \longmapsto \det A \quad \text{is an iso.}$$

"<u>Ex</u>" G a group, $g \in G$, $f : \mathbb{Z} \to G$, $f(n) = g^n$ is a homomorphism
$\mathrm{Im}\, f = \langle g \rangle$ $\quad$ $\ker f = n\mathbb{Z}$ for some $n \geq 0$
$\Rightarrow \bar{f} : \mathbb{Z}/n\mathbb{Z} \to \langle g \rangle$ $\quad$ $\bar{f}(k + n\mathbb{Z}) = g^k$
is an isomorphism of groups

There is a diagram associated to the 1^{st} iso theorem

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \pi \downarrow & & \uparrow i \\ G/\ker f & \xrightarrow[\bar{f}]{} & \mathrm{Im} f \end{array}$$

which <u>commutes</u>, meaning

$f(g) = i \circ \bar{f} \circ \pi$ where $i : \mathrm{Im} f \to H$ is the inclusion,
$\pi : G \to G/\ker f$ is $\pi(g) = g \ker f$
and $\bar{f}(g \ker f) = f(g)$.

<u>Products of groups</u>

Let G and H be two groups. Their Cartesian product is the set
$G \times H = \{(g,h) \mid g \in G, h \in H\}$ of all ordered pairs.
By HWS #1, $G \times H$ is a group: the multiplication
is defined by

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2) \qquad \forall (g_1, h_1), (g_2, h_2) \in G \times H$$

the identity $e_{G \times H} = (e_G, e_H)$

The inverses are defined by $(g,h)^{-1} = (g^{-1}, h^{-1})$.

Ex $\mathbb{Z}_6$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Reason:

Consider $f: \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_3$, $f(n) = ([n]_2, [n]_3)$

Since $k: \mathbb{Z} \to \mathbb{Z}_2$, $k(a) = [a]_2$, $\ell: \mathbb{Z} \to \mathbb{Z}_3$ $\ell(b) = [b]_3$

are homomorphisms, $f(n) = (k(n), \ell(n))$ is

also a homomorphism (HW5 #5)

$\ker f = \{ a \in \mathbb{Z} \mid ([a]_2, [a]_3) = ([0]_2, [0]_3) \}$

$= \{ a \in \mathbb{Z} \mid 2 \mid a \text{ and } 3 \mid a \} = \{ 2k \mid 3 \mid 2k, k \in \mathbb{Z} \}$

$= \{ 2 \cdot 3\ell \mid \ell \in \mathbb{Z} \} = 6\mathbb{Z}$.

By the first isomorphism Theorem we get a well-defined injective homomorphism

$$\bar{f}: \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$$

$$\bar{f}([a]_6) = ([a]_2, [a]_3)$$

Now $|\mathbb{Z}_6| = 6$, $|\mathbb{Z}_2 \times \mathbb{Z}_3| = |\mathbb{Z}_2| \times |\mathbb{Z}_3| = 2 \cdot 3 = 6$

Any <u>injective</u> map from a 6 element set to a 6-element set is onto.

$\therefore$ $\bar{f}: \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$, $\bar{f}([a]_6) = ([a]_2, [a]_3)$

is an isomorphism of groups

The example generalizes: $\forall\, n, m \in \mathbb{N}$ s.t. $\gcd(n,m) = 1$

$\mathbb{Z}_{nm} \simeq \mathbb{Z}_n \times \mathbb{Z}_m$ ($\simeq$ = "isomorphic to")

The proof is "the same"

At some point one needs: $n \mid km$, $\gcd(n,m) = 1 \Rightarrow n \mid k$.