

Last time: Modular Arithmetic

$(\mathbb{Z}, +)$ gp. Fix $n \neq 0$
 $n\mathbb{Z}$ subgp.

Cosets: $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}$
 n cosets

Set of cosets: $\mathbb{Z}/n\mathbb{Z}$

Equiv relⁿ $a \sim b$ if n divides $b-a$

$\mathbb{Z}/n\mathbb{Z}$: equiv classes for this equiv relⁿ

Defined: L.O.C. on $\mathbb{Z}/n\mathbb{Z}$ as

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a+b + n\mathbb{Z})$$

We proved: $\mathbb{Z}/n\mathbb{Z}$ with $+$ is a gp.

Today: We'll generalize

G arbitrary gp, $N \leq G$ a normal subgp

cosets: aN for $a \in G$

Notation: let $\bar{G} = G/N$ denote the set of cosets of N in G

(recall! left cosets of N and right cosets are the same)

$\bar{G}$ is the set of equivalence classes for the equivalence relⁿ

$\bar{G}$ is the set of equivalence classes for the equivalence relⁿ
 $b \sim a$ if $b = an$ for some $n \in N$.
 $a, b \in G$

If $a \in G$, denote $[aN]$ the associated elt of $\bar{a}$.

Well def: • We'll define a L.O.C. on $\bar{G}$
 • We'll prove this L.O.C. makes $\bar{G}$ a sp.

Define: $\cdot : \bar{G} \times \bar{G} \rightarrow \bar{G}$ as

$$[aN] \cdot [bN] = [abN] \quad *$$

Claim: This L.O.C. is well-defined.

I.e. if $\underline{aN = a'N}$ and $bN = \underline{b'N}$ then $\underline{abN = a'b'N}$.

Pf: $a' = an_1$ for some $n_1 \in N$
 $b' = bn_2$ for some $n_2 \in N$.

$$\Rightarrow a'b' = an_1bn_2 = ab(\underbrace{b^{-1}n_1}_{\in N} \underbrace{b}_{\in N})n_2$$

$\underbrace{\hspace{10em}}_{\in N}$

$$\Rightarrow a'b'N = abN$$

Thm $N, G, \bar{G}$ as above. Then L.O.C. on $\bar{G}$ just defined makes $\bar{G}$ into a sp. Moreover, the map

$$\pi: G \rightarrow \bar{G}$$

$$a \mapsto [aN]$$

is a surj. qd homom. w/ kernel N .

$\pi: G \rightarrow G/N$
is a surj. gp homom. w/ kernel N .

Remark: Every normal subgroup arises as the kernel of a gp homom.

Example $G = (\mathbb{Z}, +)$

$\cdot N = n\mathbb{Z} \quad n \neq 0$

$\cdot \bar{G} = G/N \text{ is } \mathbb{Z}/n\mathbb{Z}$

$\pi: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/n\mathbb{Z}, +) \text{ is a surj. gp homom.}$

Pf: 1) Kernel of π is N : $\pi: G \rightarrow \bar{G}$

Claim: $\pi(x) = [xN] = [1N] \iff x \in N$.

Pf: $[xN] = [1N]$ means $xN = 1N = N$, which happens precisely when $x \in N$.

$\cdot$ Also clear: π is a surjective map of sets.

Have: $\pi(xy) = [xyN] = [xN][yN]$
 $= \pi(x)\pi(y)$

Rest of Thm follows from

Lemma: Suppose G a gp, Y a set w/ a L.C.C. Suppose

$\varphi: G \rightarrow Y$ is surjective and satisfies $\varphi(ab) = \varphi(a)\varphi(b)$

$\forall a, b \in G$. Then Y is a gp and $\varphi: G \rightarrow Y$ is a gp homom.
□□

$\forall a, b \in G$. Then Γ is a gp and $\varphi: G \rightarrow Y$ is a gp homom.

Pf:

Assoc $y_1, y_2, y_3 \in Y$.

$$(y_1 y_2) y_3 \stackrel{?}{=} y_1 (y_2 y_3)$$

Take $x_1, x_2, x_3 \in G$ with $\varphi(x_1) = y_1, \varphi(x_2) = y_2, \varphi(x_3) = y_3$.

$$\begin{aligned}(y_1 y_2) y_3 &= (\varphi(x_1) \varphi(x_2)) \varphi(x_3) = \varphi(x_1 x_2) \varphi(x_3) \\ &= \varphi((x_1 x_2) x_3) = \varphi(x_1 (x_2 x_3))\end{aligned}$$

$$= \varphi(x_1) \varphi(x_2 x_3)$$

$$= \varphi(x_1) (\varphi(x_2) \varphi(x_3))$$

$$= y_1 (y_2 y_3) \quad \checkmark$$

Identity: Define $1_Y = \varphi(1_G)$.

Suppose $y \in Y, y = \varphi(x), x \in G$.

$$1_Y \cdot y = \varphi(1) \varphi(x) = \varphi(1 \cdot x) = \varphi(x) = y$$

Similarly, $y \cdot 1_Y = y$.

Inverses Suppose $y \in Y, y = \varphi(x), x \in G$.

Define $y' = \varphi(x^{-1})$.

$$y y' = \varphi(x) \varphi(x^{-1}) = \varphi(x \cdot x^{-1}) = \varphi(1) = 1_Y$$

$$\text{Similarly, } y' y = \varphi(x^{-1}) \varphi(x) = \varphi(x^{-1} x) = \varphi(1) = 1_Y.$$

$\Rightarrow Y$ a gp: $\varphi: G \rightarrow Y$ is a gp homom

$\Rightarrow$ a sp: $\varphi: G \rightarrow Y$ is a gp homom
 b/c our assumption is $\varphi(ab) = \varphi(a)\varphi(b) \quad \forall a, b \in G$.

Thm (First Isom Thm)

Suppose • $G \xrightarrow{\varphi} G'$ a sp homom.

• $N \subseteq \ker(\varphi)$ is a normal subgroup

• $\pi: G \rightarrow \bar{G} = G/N$ be the canonical map, i.e.
 $\pi(x) = [xN]$.

$$\begin{array}{ccc}
 G & \xrightarrow{\varphi} & G' \\
 \pi \searrow & \nearrow \bar{\varphi} & \\
 & \bar{G} &
 \end{array}$$

Then, $\exists$ a unique gp homom $\bar{\varphi}: \bar{G} \rightarrow G'$ so that

$$\varphi = \bar{\varphi} \circ \pi.$$

Moreover, if $\ker(\varphi) = N$ and φ is surjective, then

$\bar{\varphi}$ is an isom and $\bar{G} \cong G'$.

Pf: Define $\bar{\varphi}: \bar{G} \rightarrow G'$ as
 $\bar{\varphi}([aN]) = \varphi(a).$

Claim: This is well-defined. I.e., if $aN = a'N$ then
 $\varphi(a) = \varphi(a').$

Pf: $aN = a'N \Rightarrow a' = an$ for some $n \in N.$

$$\Rightarrow \varphi(a') = \varphi(a)\varphi(n) = \varphi(a) \cdot 1 = \varphi(a).$$

$$\underline{\text{II:}} \quad uv = uN = u \quad \text{for some } u \in G.$$

$$\Rightarrow \varphi(a') = \varphi(a)\varphi(u) = \varphi(a) \cdot 1 = \varphi(a),$$

$$u \in N \subseteq \ker(\varphi)$$

Clear: $\boxed{\varphi = \bar{\varphi} \circ \pi}$ as a map of sets and also clear that $\bar{\varphi}$ is unique with this property

Must check: $\bar{\varphi}$ is a gp homom.

$$\begin{aligned} \bar{\varphi}([aN][bN]) &= \bar{\varphi}([abN]) = \varphi(ab) \\ &= \varphi(a)\varphi(b) \\ &= \bar{\varphi}([aN])\bar{\varphi}([bN]). \end{aligned}$$

Suppose $\ker(\varphi) = N$ and φ is surjective.

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \pi \downarrow & & \uparrow \bar{\varphi} \\ & \bar{G} & \end{array}$$

But now: φ surj with kernel $N \Rightarrow$ fibers of φ are exactly the cosets aN for $a \in G$

$\Rightarrow \bar{\varphi}$ is a bijection. $\Rightarrow \bar{\varphi}$ is an isom. $\square$

Cor: $\varphi: G \rightarrow G'$ is a gp homom w/ kernel N . Then $\varphi(G) = \text{Im}(\varphi) \leq G'$ is isomorphic to $G/N = \bar{G}$.