Review of 561/562

(1) Structure of Groups
(2) Symmetry
(3) Structure of Rings.

Today: (1)

DEF: A Group is a triple $(G, \circ, =)$ s.t.

(G1) $\forall a, b \in G, \quad a \circ b \in G$
(G2) $\forall a, b, c \in G, \quad a \circ (b \circ c) = (a \circ b) \circ c$
(G3) $\exists e \in G, \forall a \in G, \quad a \circ e = e \circ a = a$
(G4) $\forall a \in G, \exists b \in G, \quad a \circ b = b \circ a = e$.

The group is abelian if

(G5) $\forall a, b \in G, \quad a \circ b = b \circ a$.

Exercise: identity & inverses are unique.

eg. if $a \circ e = e \circ a = a \quad \forall a \in G$
& $a \circ f = f \circ a = a \quad \forall a \in G$.

Then $e = e \circ f = f$ $\boxtimes$

DEF: Say $H \subseteq G$ is a subgroup (write $H \leq G$) if $\forall a, b \in H$, $ab^{-1} \in H$.

DEF: Map $\varphi : (G, \circ, =) \to (G', \circ, \equiv)$ is a group homomorphism if $\forall a, b \in G$.

$$\underbrace{\varphi(a) \circ \varphi(b)}_{\text{in } G'} \underbrace{\equiv}_{\text{in } G'} \varphi(\underbrace{a \circ b}_{\text{in } G})$$

Thm: Given $H \leq G$, the relation

$$a \sim_H b \iff a^{-1} b \in H$$

is an equivalence on G. The $\sim_H$ classes

$$aH := \{ab : b \in H\} \subseteq G.$$

are called (left) H-cosets.

Exercise: $aH = bH \iff a^{-1} b \in H$

(see 561 Exam 2)

Theorem (Lagrange): Given $H \leq G$, define $G/H :=$ set of H-cosets. If $|G| < \infty$ then

$$|G/H| = |G| / |H|.$$

Cor: $|H|$ divides $|G|$

Exercise: prove it!

DEF: Given $H \leq G$ say H is normal (write $H \trianglelefteq G$) if $aH = Ha \quad \forall a \in G$.

Exercise: $H \trianglelefteq G \iff \exists$ group hom $\varphi : G \to G'$ with $H = \ker \varphi = \{a \in G : \varphi(a) = e_H\}$

Thm: If $H \trianglelefteq G$ then G/H is a group with operation

$$[aH] \cdot [bH] := [(ab)H]$$

Exercise (well-defined): If $aH = a'H$ and $bH = b'H$ show that

$$[aH] \cdot [bH] = [a'H] \cdot [b'H].$$

1st Iso. Thm: Given gp. hom $\varphi: G \to G'$ we have $\ker\varphi \trianglelefteq G$ and

$$G/\ker\varphi \cong \operatorname{im}\varphi \leq G' \quad \text{as groups.}$$

Proof: Define $\bar{\varphi}: G/\ker\varphi \to \operatorname{im}\varphi$

$$a(\ker\varphi) \mapsto \varphi(a).$$

Check well-defined ✓
injective ✓
surjective ✓
hom ✓

$\boxtimes$

Exercise: Given groups H, G we have H ($\cong$) subgroup of G $\iff$ $\exists$ injective gp. hom $\varphi: H \hookrightarrow G$.

DEF: Given $a \in G$ define $\langle a \rangle \leq G$ by

$$\langle a \rangle := \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$$

$|\langle a \rangle|$ = the order of a.

$|\langle a \rangle|$ divides $|G|$ by Lagrange.

Say G is cyclic if $G = \langle a \rangle$ for some $a \in G$.

Let $G = \langle a \rangle$ and consider group hom

$$\varphi : (\mathbb{Z}, +) \to \langle a \rangle$$
$$k \longmapsto a^k$$

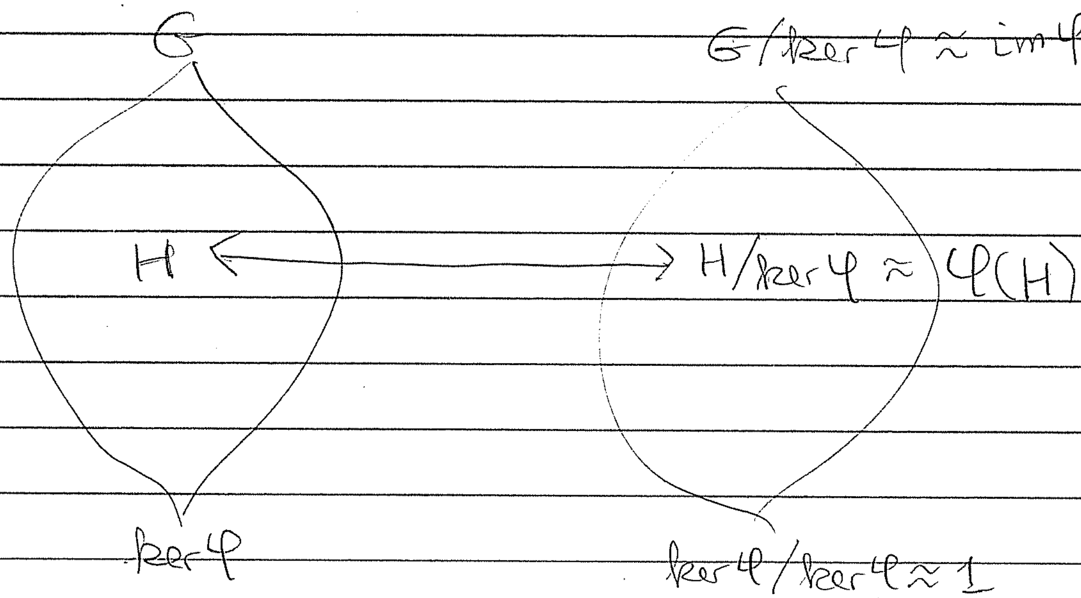
Note: $\operatorname{im} \varphi = \langle a \rangle$ (surjective)
$\ker \varphi = n\mathbb{Z}$ where $n = |\langle a \rangle|$.

Hence (1st Iso Thm):

$$\langle a \rangle = \operatorname{im} \varphi \cong \mathbb{Z}/\ker \varphi = \mathbb{Z}/n\mathbb{Z}.$$

But Wait!

Thm (Correspondence): Given gp. hom $\varphi : G \to G'$, $\exists$ lattice isomorphism



Apply to Cyclic Groups.

Thm: Every subgroup of $(\mathbb{Z}, +)$ is $a\mathbb{Z}$ for some $a \in \{0, 1, 2, \dots\}$

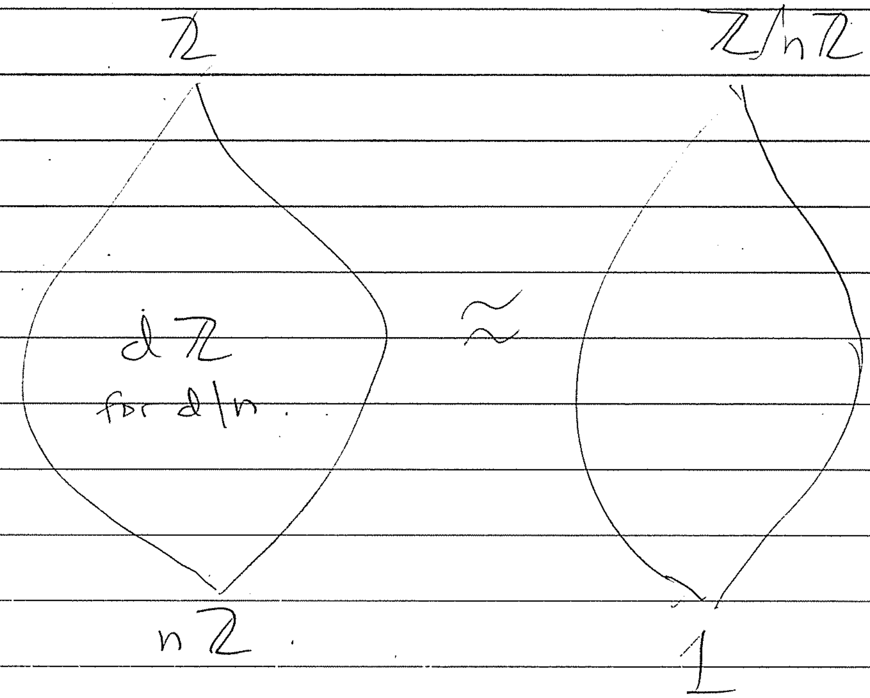
Proof: Exercise.

Note $a\mathbb{Z} \leq b\mathbb{Z} \iff b$ divides a.

Thm (FTCG):

$\mathcal{L}(\mathbb{Z}/n\mathbb{Z}) \approx$ lattice of divisors of n.

Proof: $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.



∎

Appendix: Group Products

If $H, K \leq G$ with $K \trianglelefteq G$ then

1) $HK = \{hk : h \in H, k \in K\} \leq G$.

2) $K \trianglelefteq HK$ and $H \cap K \trianglelefteq H$ with

$$\frac{H}{H \cap K} \cong \frac{HK}{K} \quad \text{(2nd Iso Thm)}.$$

3) By Lagrange,

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}$$

4) What if $H \cap K = 1$?

Then $G = HK$ as <u>sets</u>

Structure? Say $G = H \times K \quad H \trianglelefteq G$

$= H \rtimes K \quad H \ntrianglelefteq G$.

//