5/21/14

Review of 561/562, May 2014

Today 5/21
Friday 5/23
Tues 5/27
Thurs 5/29
Prelim Exam on Friday 5/30.

A group is a structure $(G, \circ, 1)$ where

- $\circ$ is a function $G \times G \longrightarrow G$ written

$$(a, b) \longmapsto a \circ b.$$

- $\forall\, a, b, c \in G$ we have

$$a \circ (b \circ c) = (a \circ b) \circ c$$

- $\forall\, a \in G$ we have $a \circ 1 = 1 \circ a = a$.

- $\forall\, a \in G$ $\exists\, b \in G$ such that

$$a \circ b = b \circ a = 1.$$

The group is called abelian if

- $\forall a, b \in G$ we have $a \circ b = b \circ a$.

Exercise: Identity and inverses are unique.

If $a \circ 1 = 1 \circ a = a \quad \forall a \in G$

and $a \circ 1' = 1' \circ a = a \quad \forall a \in G$

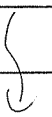
then $1 = 1 \circ 1' = 1'$

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

We say $\varphi : (G, \circ) \to (G', *)$ is a group homomorphism if $\forall a, b \in G$

$$\varphi(a) * \varphi(b) = \varphi(a \circ b).$$

($\varphi(a) * \varphi(b)$ in G'; $\varphi(a \circ b)$ in G.)



Exercise: Given $H \leq G$ prove that

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

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

$$\begin{aligned}[a]_H &= \{ b \in G : a^{-1}b = h \in H \} \\ &= \{ ah : h \in H \} \\ &= aH\end{aligned}$$

are called (left) H-cosets.

Exercise: Prove that

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

///

Theorem (Lagrange): Given $H \leq G$, let $G/H := \{ aH : a \in G \}$ be the set of left H-cosets. If $|G| < \infty$ then

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

Corollary: $|H|$ divides $|G|$.

Corollary: Given $a \in G$ we define the cyclic subgroup generated by a:

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

Call $|\langle a \rangle|$ the order of $a \in G$. By Lagrange we know that $|\langle a \rangle|$ divides $|G|$ and hence

$$a^{|G|} = a^{k|\langle a \rangle|} = \left(a^{|\langle a \rangle|}\right)^k = 1^k = 1.$$

Exercise: Prove Lagrange's Theorem.

We say $H \leq G$ is normal (and write $H \trianglelefteq G$) if $\forall\, a \in G$, $aH = Ha$, or equivalently if $\forall\, a \in G$, $h \in H$ we have $aha^{-1} \in H$

Q: Who cares?

A: The kernel of a group hom $\varphi: G \to G'$,

$$\ker \varphi := \{ g \in G : \varphi(g) = 1_{G'} \}$$

is a normal subgroup of G.

Conversely, if $H \trianglelefteq G$ is any normal subgroup then H is the kernel of a group hom $\varphi: G \to G'$ for some group G'.

Q: Which group G'?

A: We define an operation on the set G/H by

$$(aH) \circ (bH) := (ab)H.$$

Exercise: If $H \trianglelefteq G$ then this operation is well defined and makes G/H into a group so that

$$\begin{aligned} \varphi : G &\longrightarrow G/H \\ a &\longmapsto aH \end{aligned}$$

is a group hom with kernel H. ///

Note: The image of a group hom $\varphi: G \to G'$,

$$\text{im}\,\varphi := \{a' \in G' : \exists\, a \in G,\ \varphi(a) = a'\},$$

is a subgroup of G' but it need not be normal.

Compare:

	Group	Ring
image	subgroup	subring
kernel	normal subgroup	ideal

Noether's First Isomorphism Theorem:

Given any group homomorphism $\varphi: G \to G'$ we obtain a group isomorphism

$$G/\ker\varphi \cong \operatorname{im}\varphi$$

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

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

Then

$$\begin{aligned} a(\ker\varphi) = b(\ker\varphi) &\iff a^{-1}b \in \ker\varphi \\ &\iff \varphi(a^{-1}b) = 1 \\ &\iff \varphi(a)^{-1}\varphi(b) = 1 \\ &\iff \varphi(b) = \varphi(a). \end{aligned}$$

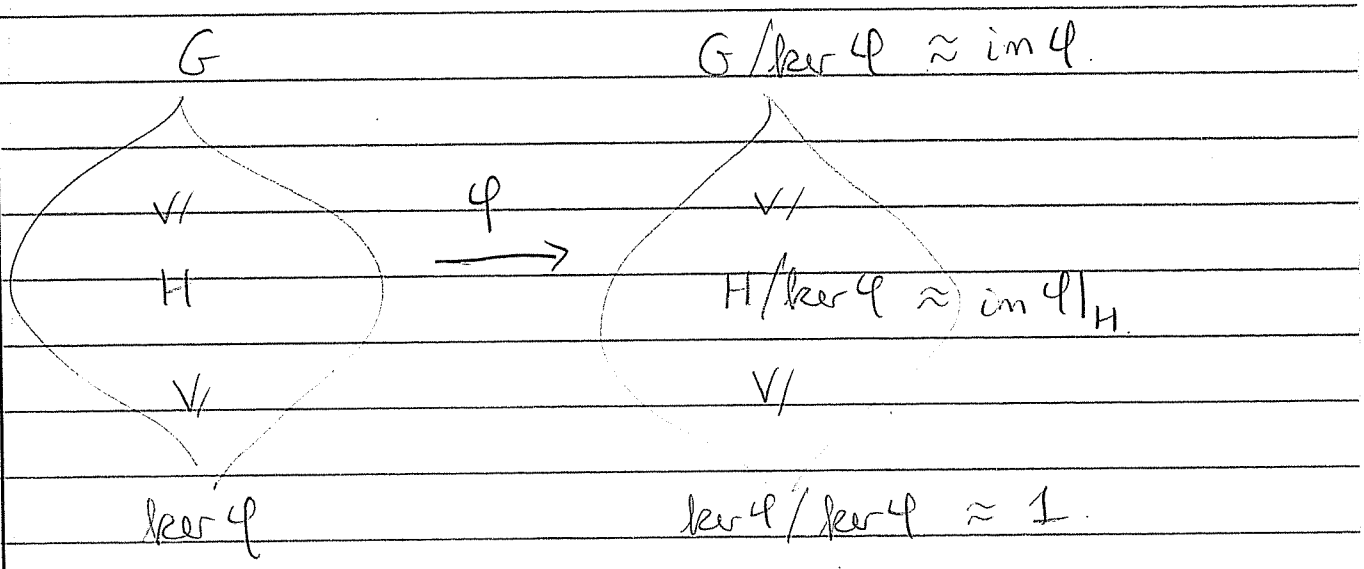
$\Rightarrow$ proves well defined

$\Leftarrow$ proves injective. //

More generally we have the

Correspondence Theorem: Given a group hom $\varphi: G \to G'$ we have an isomorphism of lattices

$$\mathcal{L}(G, \ker\varphi) \approx \mathcal{L}(G/\ker\varphi)$$



Application to Cyclic Groups:

We say group G is <u>cyclic</u> if $\exists\, g \in G$ such that

$$\langle g \rangle = G.$$

Then we have a surjective group hom

$$\varphi : (\mathbb{Z}, +) \to G.$$
$$k \longmapsto g^k$$

The kernel is $n\mathbb{Z}$ where $n = |\langle g \rangle|$, and hence

$$\mathbb{Z}/n\mathbb{Z} \approx G.$$

More generally, recall that every subgroup of $(\mathbb{Z}, +)$ has the form $a\mathbb{Z}$ for some $a \in \mathbb{Z}$ (Proof: Division with Remainder) and that

$$a\mathbb{Z} \leq b\mathbb{Z} \iff b \mid a.$$

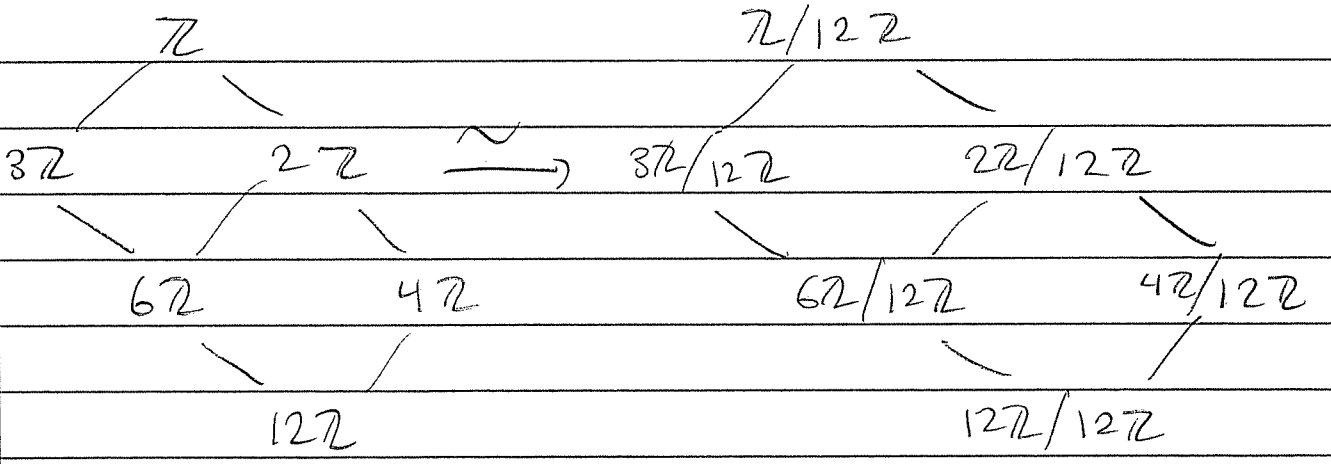
Thus we obtain the Fundamental Theorem of Cyclic Groups:

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

Proof: Correspondence Theorem. //

Example: $n = 12$.

$\mathcal{L}(\mathbb{Z}, 12\mathbb{Z}) \xrightarrow{\sim} \mathcal{L}(\mathbb{Z}/12\mathbb{Z})$.



Since $|d\mathbb{Z}/n\mathbb{Z}| = n/d$ we obtain exactly one subgroup of $\mathbb{Z}/12\mathbb{Z}$ for each divisor of 12.

Remark:

$$\frac{d\mathbb{Z}}{n\mathbb{Z}} \cong \frac{\mathbb{Z}/n\mathbb{Z}}{\mathbb{Z}/d\mathbb{Z}}.$$

by 2nd or 3rd Isomorphism Thm. I forget which one.