Algebra I: Lecture 2

Recall what a subgp. is. *(already done)*

<u>Ex</u>: $\langle r\rangle, \langle s\rangle < D_{2n}$.

<u>Non-ex</u>: $\mathbb{N} \not< \mathbb{Z}$, as it's not closed under inverses.

The subgp criterion isn't usually so bad.

<u>Ex</u>: $\varphi : G \to H$ <u>hom</u>.

$im(\varphi) \leq H$ as

1). $\varphi(e_G) (= e_H) \in H \Rightarrow im(\varphi) \neq \emptyset$

2). $a = \varphi(g_1)$, $b = \varphi(g_2) \Rightarrow \varphi(ab^{-1}) = ab^{-1} \Rightarrow ab^{-1} \in im(\varphi)$ ✓ ($g_1 g_2^{-1}$) (same before) (up to here)

<u>Ex</u>: $\alpha \in I$, $H_\alpha \leq G \Rightarrow H = \bigcap_{\alpha \in I} H_\alpha \leq G$; it contains e, $a \in H, b \in H \Rightarrow ab^{-1} \in H_\alpha \ \forall \alpha$.

<u>But</u> $\bigcup_{\alpha \in I} H_\alpha$ may <u>not</u> be a subgp. Ex: $\langle r\rangle \cup \langle s\rangle \not\leq D_{2n}$ as $rs \notin \langle r\rangle \cup \langle s\rangle \Rightarrow$ not <u>closed</u>.

<u>Quotients</u>: $H \leq G$

<u>Def^n</u> The (left) coset space G/H

is the set of equiv. classes of the rel^n

$$g_1 \sim g_2 \Leftrightarrow g_1^{-1} g_2 \in H. \Leftrightarrow g_2 = g_1 h,\ h \in H.$$

~~The left~~ (Equiv. rel^n: $g = ge \Rightarrow g \sim g$

$g_1 \sim g_2 \Rightarrow g_2 = g_1 h \Rightarrow g_1 = g_2 h^{-1} \Rightarrow g_2 \sim g_1$

$g_1 \sim g_2,\ g_2 \sim g_3 \Rightarrow g_2 = g_1 h,\ g_3 = g_2 h' = g_1 (hh')$
$\Rightarrow g_1 \sim g_3$

$\Rightarrow$ they are distinct (partition as equiv. rel^n)

That is, the coset containing g is $gH = \{gh : h \in H\}$.

<u>Ex</u>: $G = \mathbb{Z}$, $H = m\mathbb{Z}$, $G/H = \mathbb{Z}/n\mathbb{Z}$. A coset containing $m \in \mathbb{Z}$ is $\{r \in \mathbb{Z} \mid r \equiv a \pmod n\}$. i.e., the cosets are <u>congruence classes</u>.

Note that here, they are a <u>group</u> ($a \equiv b$, $c \equiv d$ $\Rightarrow a + c \equiv b + d$, so well-definedness (adding is)

Lemma: All cosets have the same size.

Pf: We have a bijection $g_1 H \to g_2 H$ (follow your nose!)

$g \mapsto g_2 g_1^{-1} g$ (injectivity, as often, comes from inverses in the gp.)

surj: $g_2 h \leftarrow g_1 h$

~~All cosets distinct~~

Lagrange's Thm: $|G| < \infty$

$\Rightarrow |G| = |G/H| \cdot |H|$. In particular, $|H| \mid |G|$. ($\frac{|G|}{|H|} = |G/H|$)

trivial coset! $\to |H|$ $=: [G:H] =$ index.

(# of cosets) $\cdot |H| = |G|$

↑ size of aH coset

Cor: $|g| \mid |G|$ (as $|g| = |\langle g \rangle|$).

Cor (Fermat's Little Thm)

p prime, $(a,p) = 1 \Rightarrow a^{p-1} \equiv 1 \ (p)$.

(as then $a \in \mathbb{Z}/p\mathbb{Z}^*$, and ~~$|a| = 1$ or p, so $a = a^{p-1} = 1$~~ $a^{|\mathbb{Z}/p\mathbb{Z}^*|} = a^{p-1} = 1$ in $\mathbb{Z}/p\mathbb{Z}^*$.)

Also Euler's (totient) Thm ~

Q: When does G/H have the full group structure? (already wrestling to use ring theory)

On $\mathbb{Z}/n\mathbb{Z}$, the structure of a group is.

take a representative of each coset ($1, \ldots$ to $\mathbb{Z}$) add, then reduce mod n.

e.g. $n = 7$, ~~$\bar{3} + \bar{5} = \ldots$~~

$(3 + 7\mathbb{Z}) + (5 + 7\mathbb{Z}) = 8 + 7\mathbb{Z} = 1 + 7\mathbb{Z}$.

$\bar{3} + \bar{5} = \bar{1}$

Try in general:

try to set $(g_1 H)(g_2 H) = (g_1 g_2) H$. only natural choice

well-defined?

replace g_1 by $g_1 h_1$ (picking different representatives)

want $g_1 g_2 H = g_1 h_1 g_2 h_2 H \Leftrightarrow g_2^{-1} h_1 g_2 h_2 H = H$

(h_2 absorbs ($g_2^{-1} h_1 g_2$ permutes them around))

$\Leftarrow g_2^{-1} h_1 g_2 \in H \quad \forall g_2 \in G, h_1 \in H$.

Def^n: $H \leq G$ is *normal*, written $H \trianglelefteq G$, if

$g^{-1}hg \in H \quad \forall g \in G, h \in H$

i.e., H is closed/invariant under *conjugation*.

Prop: $H \trianglelefteq G \Rightarrow G/H$ is a group with the op. above

Pf: We checked well-definedness.

Associativity is clear. The id. is $eH = H$, and $(aH)^{-1} = a^{-1}H$.

(all gp. structure is naturally inherited)

In fact, this is *iff* (otherwise, not well-defined).

That's not to say there may not be other *unnatural* gp. structures on G/H...

Another characterization:

Natural map: $H \trianglelefteq G$

(projection) $\varphi: G \to G/H$.

$g \mapsto gH$.

is clearly *surjective*. $\ker(\varphi) = \{g \in G \mid gH = H\} = H$.

Thus, H is the *kernel* of a gp. hom.

Conversely, if $\varphi: G \to H$, then if $x \in \ker\varphi$, $g \in G$,

$\varphi(g^{-1}xg) = \varphi(g^{-1})\varphi(x)\varphi(g) = \varphi(g^{-1}g) = e_H$

$g^{-1}xg \Rightarrow g^{-1}xg \in \ker\varphi \Rightarrow \ker\varphi \trianglelefteq G$.

So, $H \trianglelefteq G$ *iff* it's a kernel of a *hom*.

Another useful property:

(E-Z Exercise) (E) $H \trianglelefteq G \Leftrightarrow gH = Hg \ \forall g \in G$ (left cosets = right cosets)

Rmk: While $\leq$ is transitive, $\trianglelefteq$ is *not*!

Ex: $\langle 5 \rangle \trianglelefteq \langle 5, r^2 \rangle \trianglelefteq D_8$, (check!) and the following (up)

$\langle 5 \rangle$: 2; $\langle 5, r^2 \rangle$: $\{5, r^2, r^4, r^6\}$; D_8: all

But $\langle s \rangle \not\trianglelefteq D_4$ as $rsr^{-1} = sr^2 \notin \langle s \rangle$. ($= sr^{-3}$) (sgs^{-1} send | to different places)

Prop: $|G/H| = 2 \Rightarrow H \trianglelefteq G$. ($H \leq G$)

pf: Pick $g \in G \setminus H \Rightarrow$ so $G/H = \{H, gH\}$. $\Rightarrow gH = G \setminus H$.
Similarly for Hg, $\Rightarrow G \setminus H = Hg = gH \Rightarrow H \trianglelefteq G$. (not much room for stuff to happen)

~~Notation~~. Terminology: gng^{-1} is the conjugate of n by g.

The set gNg^{-1} is the conjugate of N by g.

we say g normalizes N if $gNg^{-1} = N$. (more on these later).

Ex: In GL_n, conjugation is a change of basis.

Ex: If G is abelian, then all subgps are normal as

$$gng^{-1} = gg^{-1}n = n \quad \forall\, n \in N, g \in G.$$

Ex: Center $Z(G) = \{g \in G \mid gg' = g'g \ \forall g' \in G\}$ (commutes with everything)

For the same reason,

$$H \leq G, H \leq Z(G) \Rightarrow H \trianglelefteq G.$$

Ex: Prop: If G has prime order p, then $G \cong \mathbb{Z}/p\mathbb{Z}$.

pf: $\forall\, g \in G \setminus \{e\} \Rightarrow |g| \neq 1 \Rightarrow |g| = p \Rightarrow g, \dots, g^{p-1}$ distinct (Lagrange) (p prime)

$\Rightarrow |\langle g \rangle| = |G|$, but $\langle g \rangle \leq G \Rightarrow \langle g \rangle = G \Rightarrow G \hookrightarrow \mathbb{Z}/n\mathbb{Z}$

But all cyclic gps of the same order are $\cong$:

Indeed, In this case, define $\varphi: G \to \mathbb{Z}/p\mathbb{Z} = \langle 1 \rangle$

$g \mapsto 1$

and extend $g^k \mapsto k$. (like for linearity) (4)

$0 \leq k \leq p-1$

It's a hom: $\varphi(g^m \cdot g^n) = \varphi(g^{m+n}) = m+n = \varphi(g^m)+\varphi(g^n)$

Note: Can divide any $n \in \mathbb{Z}$ by p & remainder to get

$n = qp + r$, $0 \le r < p$. (Euclidean division)

So $a^n = a^{qp+r} = a^r$, and $\varphi(a^n) = r \equiv n \pmod p$, so φ holds for all $n \in \mathbb{Z}$

Now for $a, b \in G$, say $a = g^x$, $b = g^y$

$\Rightarrow \varphi(ab) = \varphi(g^{x+y}) = x+y = \varphi(g^x)+\varphi(g^y)$.

Also, φ is clearly a bijection. (i.e. it's a surjection between finite sets of the same size)

$\Rightarrow$ φ is an isomorphism

When is the converse to Lagrange true?

i.e. if $d \mid |G|$, does $\exists\ H \le G$ s.t. $|H| = d$?

Sometimes:

Ex: If G is cyclic, $|g| = n$, then $\forall\ d \mid n$

$G = \langle g \rangle$

$\langle g^{\frac{n}{d}} \rangle$ has size d. (see before)

$=:$

It's also true for abelian gps (follows from the Fundamental Theorem, more on this later)

False in general: [Let's see this now!]

Consider A_4, the alternating group in S_4. (will see more on later).

This is the kernel of $\operatorname{sgn}: S_4 \to \{\pm 1\}$ which sends:

$e \mapsto +1$

3 pairs of disjoint transpositions: $(12)(34), (13)(24), (14)(23)$ $\mapsto +1$ } V.

8 3-cycles: $(123), (124), \dots \mapsto +1$.

all else go to -1 (tedious this way, but is a hom!).

(5)

$\S$. $H \subset A_4$ has order $6 \mid 12$, set $H' := H \cap V$, where $V = \{e, \text{prod. of disjoint trans.}\}$ (Klein 4-group! all order 2!)

Lagrange $\Rightarrow |H'| \mid 4$ and $|H'| \mid 6 \Rightarrow |H'| = 1, 2$.

If $|H'| = 1$, then map $\varphi: H \times V \to A_4$

$(h, v) \mapsto h \cdot v$. is injective,

as: if $hv = hv'$ then $v = v'$

as $\ker \varphi = \{(e, e)\}$, as: if $\varphi(h, v) = e$, then $hv = e \Rightarrow h = v^{-1} \Rightarrow h \in H \cap V = H' \Rightarrow h = e \Rightarrow v = e$.

Recall: $\ker(\varphi) = e \Rightarrow$ injective

$\Rightarrow |H \times V| = 24 \leq |A_4| = 12$ $\#$.

Now $|H'| = 2$, and $H = \{e, v\}$ where $v =$ product of two disjoint trans. (already seen w/ three 4-cycles.)

$[G : H] = 2 \Rightarrow H \trianglelefteq G$

Say $v = (i\,j)(k\,\ell)$, and set $t = (i\,j\,k)$. $\left(= (i\,j\,k)(i\,j)(k\,\ell)(i\,j)\right)$

then $tvt^{-1} = (j\,k)(i\,\ell) \neq (i\,j)(k\,\ell) = v$

and $tvt^{-1} \in H$ by normality. Contradicts $|H'| = 2$.

That is, we found another prod. of 2 trans. in there does not exist!

However, we shall see!

Th$^{\underline{m}}$ (Cauchy)

p prime $p \mid |G| \Rightarrow G$ has an $\in H$ of order p.

(on HW)

Better:

Th$^{\underline{m}}$ (Sylow):

$|G| = p^r m$, $p \nmid m$, then G has a subgp. of order p^r.

(stuff at end of §3.2 maybe add to next on normalizers etc.)

all about gp. actions!

$HK = \{hk \mid h \in H, k \in K\}$.

Prop: $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$

Pf: $HK = \bigcup_{h \in H} hK$. each coset has size $|K|$

how many distinct? $hK = h'K \iff h^{-1}h' \in K \iff h^{-1}h' \in H \cap K$

$\iff h(H \cap K) = h'(H \cap K)$

# of cosets here is $|H|/|H \cap K|$ by Lagrange $\Rightarrow$ ∎.

Thm: If $H, K \leq G$, then $HK \leq G \iff HK = KH$

Pf: $\Leftarrow$ $HK = KH$. HK nonempty as $e \in HK$ ✓.

If $a, b \in HK \Rightarrow a = h_1k_1$, $b = h_2k_2$

$ab^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1k_3h_2^{-1}$ (for some $k_3 \in K$)

$= h_1(k_3h_2^{-1}) = h_1h_4k_4 \in HK$.

Conversely: If $HK \leq G$, then $H, K \leq HK \Rightarrow KH \leq HK$ (as (HK) is a gp).

Now let $hk \in HK$, say $hk = a^{-1}$ for $a = h_1'k_1'$

Moreover $\Rightarrow hk = (h_1'k_1')^{-1} = k_1'^{-1}h_1'^{-1} \in KH \Rightarrow HK \leq KH \Rightarrow$ ∎.

(Not automatic after noncommutative)

Cor: $H, K \leq G$, $H \leq N_G(K)$, then $HK \leq G$.

Exercise: i.e. put N: $K \leq G$ then $HK \leq G$ $\forall H \leq G$

Pf: Show $HK = KH$ If $h \in H$, $k \in K$

$hkh^{-1} \in K$

$\Rightarrow hk = (hkh^{-1})h \in KH \Rightarrow HK \leq KH$.

Also $kh = h(h^{-1}kh) \in HK \Rightarrow$ ∎

mention this part for HW!

Next time: Constructions, examples