Lecture 17

Partitions of G $\rightsquigarrow$ There are two e.r on G $\rightsquigarrow$ $[a] = aH$ and $G/\sim_\ell = G/H$

G/H or $H \backslash G$

left $a \sim_\ell b \iff b^{-1}a \in H$

rigth $a \sim_r b \iff ab^{-1} \in H$ $\qquad [a] = Ha$ and $G/\sim_r = H\backslash G$

Corollary 30: Let G be a finite group

(a) If $a \in G$, then $|a|$ divides $|G|$

(b) $a^{|G|} = 1$ for all $a \in G$.

We didn't have this result before Lagrange's thm. We had

- $a \in G \implies |a| \leq |G|$
- Only for cyclic groups $|a| \mid |G|$ for all $a \in G = \langle x \rangle$

Proof:

(1) Let $a \in G$. Consider $\langle a \rangle \leq G$. By Lagrange's thm $|\langle a \rangle|$ divides $|G|$. From Prop 20, $|a| = |\langle a \rangle|$. The result follows.

(2) $a^{|G|} = a^{|a|[G:\langle a \rangle]} = 1$.

Corollary 31: Let G be a group of order p prime. Then G is cyclic, i.e. $G \cong \mathbb{Z}/p$.

Proof: Let $x \in G \setminus \{1\}$. Then $|\langle x \rangle| > 1$ and $|\langle x \rangle|$ divides $|G| = p$. Since p is prime and $\langle x \rangle \neq \{1\}$, $|\langle x \rangle| = p$. Given that $\langle x \rangle \subseteq G$, we have $\langle x \rangle = G$.

Hence, $G \cong \mathbb{Z}/p$.

⚠ Lagrange's thm is a subgroup candidate criterion. It provides a list of candidates for orders of subgroups of G. For instance, if $|G| = 10$, G can only have subgroups of orders $1, 2, 5$ and 10.

⚠ The converse of Lagrange's thm is FALSE. If $n \mid |G|$, it is not necessarily true that $\exists H \leq G$ with $|H| = n$. e.g. $|A_4| = 12$ and A_4 has no subgroup of order 6.

Normal Subgroups & Quotient Groups

Goal: Create a new group from G, $H \leq G$ and G/H (or $H \backslash G$).

Question: How do we give G/H or $H \backslash G$ the group structure? Let's focus on left cosets.

A natural way: $(aH) \bullet (bH) := (ab)H \quad \forall a,b \in G$

Problem ⇝

1. Well-defined? ✗ $\boxed{aH = bH \text{ and } cH = dH \Rightarrow (aH)\bullet(cH) = (bH)\bullet(dH)}$ $\iff$ $\boxed{gH = Hg \text{ for all } g \in G}$ ✱
2. Binary? ✓ Since $ab \in G$, then $(ab)H \in G/H$
3. Associative? ✓ Because G is a group
4. Identity? ✓ $e_{G/H} := H = eH$
5. Inverse? ✓ $(aH)^{-1} = a^{-1}H$ because $(aH) \bullet (a^{-1}H) = H$

⚠ Being well-defined is equivalent to having left cosets of H = rigth cosets of H. Remember that $gH = Hg$ for all $g \in H$ is not always true.

But, when ✱ is true, our new operation is well-defined.

Subgroups with property ✱ deserve a name!

Def: A subgroup N of G is said to be normal in G if

$$aN = Na \quad \text{for all } a \in G.$$

Notation: $N \trianglelefteq G$

⚠ $aN = Na$ does not imply $an = na$ for all $a \in G$. It means $an = ma$ for some $n, m \in N$.

Ex: 1) D_6 and $N = \{1, r, r^2\}$. N is normal in D_6 because

$$1N = N1 \qquad sN = \{s, sr, sr^2\} = \{s, rs, r^2s\} = Ns$$

$$rN = Nr \qquad srN = \{sr, sr^2, s\} = \{sr, rsr, r^2sr\} = Nsr$$

$$r^2N = Nr^2 \qquad sr^2N = \{sr^2, s, sr\} = \{sr^2, rsr^2, r^2sr^2\} = Nsr^2$$

D_6 and $H = \{1, s\}$. H is not normal in D_6 because $rH = \{r, rs\} \neq \{r, sr\} = Hr$.

These cosets are not equal as $rs = sr^{-1} = sr^2 \neq sr$.

2) Every subgroup of an abelian group is normal.

G abelian, $H \leq G$, $a \in G \implies aH = \{ah \mid h \in H\} \underset{\uparrow}{=} \{ha \mid h \in H\} = Ha \implies H \trianglelefteq G$

G is abelian

3) For all G, $Z(G) \trianglelefteq G$.

For all $a \in G$, $aZ(G) = \{az \mid z \in Z(G)\} \underset{\uparrow}{=} \{za \mid z \in Z(G)\} = Z(G)a \implies Z(G) \trianglelefteq G$

$z \in Z(G)$

Theorem: Normal Subgroup Test Let $N \leq G$. The following are equivalent

(1) $N \trianglelefteq G$.

(2) $aNa^{-1} \subseteq N$ for all $a \in G$.

(3) $aNa^{-1} = N$ for all $a \in G$.

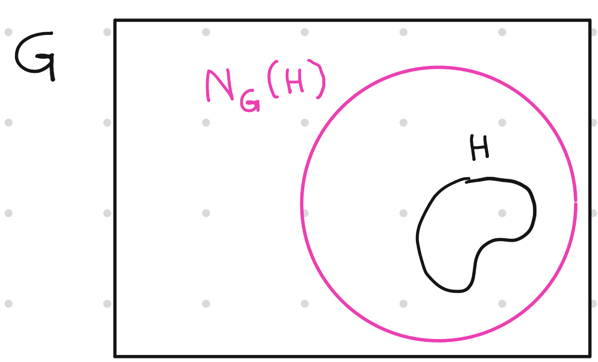
(4) $N_G(N) = G$.

Observation: Now the concept of normalizer will make more sense!

If $H \leq G$, then $N_G(H)$ measures "how close" H is to be normal in G.

If H is not normal in G, the normalizer provides a "bubble" where "H can be normal", i.e.

$N_G(H)$ is the largest subgroup of G containing H where H is normal.



$H \trianglelefteq N_G(H) \leq G$

⚠ The normalizer is NOT normal in G.

Find examples!

⚠ "Being normal" is not a transitive relation.

Proof:

(1) $\Rightarrow$ (2) Let $ana^{-1} \in aNa^{-1}$. WTS: $ana^{-1} \in N$

Observe that $na^{-1} \in Na^{-1}$. Since $N \trianglelefteq G$, $Na^{-1} = a^{-1}N$. Thus, $na^{-1} \in a^{-1}N$, i.e. $na^{-1} = a^{-1}m$ for some $m \in N$. Consequently, $ana^{-1} = aa^{-1}m = m \in N$.

(2) $\Rightarrow$ (3) WTS: $aNa^{-1} = N$

($\subseteq$) By hypothesis.

($\supseteq$) Let $n \in N$, then $n = a(a^{-1}na)a^{-1}$.

by hyp $gNg^{-1} \subseteq N \ \forall g \in G$.

Observe that $a^{-1}na \in (a^{-1})N(a^{-1})^{-1} \subseteq N$, then $a^{-1}na = m \in N$. Thus $n = a(a^{-1}na)a^{-1} = ama^{-1} \in aNa^{-1}$.

(3) $\Rightarrow$ (4) By definition of $N_G(N)$.

(4) $\Rightarrow$ (1) $\forall a \in G$, $\quad aN = (aN)a^{-1}a = (aNa^{-1})a \underset{\text{by hyp } N_G(N) = G}{=} Na.$

Theorem 32: $N \trianglelefteq G \iff \big($ If $aN = bN$ and $cN = dN$, then $(ac)N = (bd)N \big)$.

Proof:

($\Rightarrow$) Suppose $aN = bN$ and $cN = dN$, i.e. $b^{-1}a \in N$ and $d^{-1}c \in N$ by Lemma 27.

WTS: $(bd)^{-1}(ac) \in N$.

We have that $b^{-1}a = m$ and $d^{-1}c = n$ with $m, n \in N$. Then

$(bd)^{-1}(ac) = d^{-1}b^{-1}ac = d^{-1}mc$. Notice that $mc \in Nc \underset{N \trianglelefteq G}{=} cN$, then $mc = cn'$

For some $n' \in N$. Hence, $(bd)^{-1}(ac) = d^{-1}cn' = nn' \in N$.

By Lemma 27, $(ac)N = (bd)N$.

($\Leftarrow$) If we prove that $aNa^{-1} \subseteq N$ for all $a \in G$ then by the Normal Subgroup Test $N \trianglelefteq G$.

Let $ana^{-1} \in aNa^{-1}$. Since $n \in N$, by Lemma 27 $nN = N$. Also, $a^{-1}N = a^{-1}N$. Thus, by hypothesis, $(na^{-1})N = a^{-1}N$. By Lemma 27, $ana^{-1} = (a^{-1})^{-1}na \in N$.

Corollary 33: Let $N \trianglelefteq (G, \bullet)$, then $G/N = N\backslash G$ and G/N is a group under the operation $(aN) \bullet (bN) := (a \bullet b)N$.

Proof: From Thm 32, $\bullet$ is well-defined.

Def: Let $N \trianglelefteq G$.

(1) G/N is the quotient group of G by H

read G mod N.

(2) The homomorphism $\pi : G \longrightarrow G/N$, given by $\pi(a) = aN$ is called the natural projection of G onto N.