Normal Subgroups and Quotient Groups

2013 02 11

Def Let $H \leq G$. We say H is a normal subgroup (and write $H \trianglelefteq G$) if $gH = Hg$ $\forall g \in G$.

ex If G is abelian and $H \leq G$, then H is normal.

Note $n \geq 3$

ex Consider $G = D_{2n} = \langle r, s \rangle = \{1, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}$

$H_1 = \langle r \rangle$, has two cosets ($|G|/|H_1| = 2$). $sH_1 = \{s, sr, \dots\}$ $H_1 s = \{s, rs, \dots\} = \{s, sr^{n-1}, \dots, sr\}$

$\therefore sH_1 = H_1 s$ and $H_1 = H_1$, so H_1 is normal

$H_2 = \langle s \rangle$ has $|G|/|H| = 2n/2 = n$ cosests (n left, n right)

Note $rH_2 = \{r, rs = sr^{n-1}\} \neq \{r, sr\} = H_2 r$ $\therefore$ H_2 not normal, $H_2 \ntrianglelefteq D_{2n}$

If $n = 2k$, $r^k H_2 = H_2 r^k$

Theorem: Let $H \leq G$. Then TFAE:

1) $H \trianglelefteq G$; 2) $gHg^{-1} = H$ $\forall g \in G$; 3) $gHg^{-1} \subseteq H$ $\forall g \in G$.

Pf: For 1)$\Leftrightarrow$2), note $gHg^{-1} = H \Leftrightarrow gH = Hg$. 2)$\Rightarrow$3) is trivial.

3)$\Rightarrow$1): $gHg^{-1} \subseteq H \Rightarrow gH \subseteq Hg$. $(g^{-1})H(g^{-1})^{-1} \subseteq H \Rightarrow Hg \subseteq gH \Rightarrow Hg = gH$.

Lemma: Let G_1, G_2 be groups, let $\varphi: G_1 \to G_2$ be a group homomorphism. Then $\ker(\varphi) \trianglelefteq G_1$.

Pf: By the Thm, it suffices to show that $g\ker(\varphi)g^{-1} \subseteq \ker(\varphi)$ $\forall g \in G$.

Let $x \in g\ker(\varphi)g^{-1}$. So $x = ghg^{-1}$ for $h \in \ker(\varphi)$.

Then $\varphi(ghg^{-1}) = \varphi(g)\underbrace{\varphi(h)}_{e}\varphi(g)^{-1} = e$, so $x \in \ker(\varphi)$. $\blacksquare$

Def Let $H \leq G$ Define $G/H = \{gH ; g \in G\}$.

works iff $H \trianglelefteq G$

Rmk: Can try $(aH)(bH) = (ab)H$ or $(aH)(bH) = aHbH$.

Prop. Let $N \trianglelefteq G$. Then $a_1N = a_2N$, $b_1N = b_2N \Rightarrow a_1b_1N = a_2b_2N$ and $a_1Nb_1N = a_1b_1N$.

Proof: $a_1Nb_1N = a_1b_1NN = a_1b_1N$, N normal $\Rightarrow Nb_1 = b_1N$, $N \leq G \Rightarrow NN = N$.

Then $a_1b_1N = a_1Nb_1N = a_2Nb_2N = a_2b_2N$ by the first part of pf. $\blacksquare$

Theorem: Let $N \trianglelefteq G$. Then $(G/N, \cdot)$ is a group.

Pf: Associativity: easy, follows from G. Identity: $eN \overset{=N}{:}$ $NaN = aNN = aN$, $aNN = aN$ ✓

Inverse: $(aN)(a^{-1}N) = aa^{-1}N = eN = N$.

ex [illegible]

Midterm: end of today + A5

2013 02 13

Observation: If $N \trianglelefteq G$ then the map $\gamma_N : G \to G/N$, given by $\gamma_N(a) = aN$, is a group *homomorphism*. Also, $\ker(\gamma_N) = N$

Lemma 1: Let $N \trianglelefteq G$, $[G:N] = k$. Then $a^k \in N$ $\forall a \in G$.
Proof: Note $|G/N| = k$ and $\gamma_N(a^k) = \gamma(a)^k = e_{G/N} = N$
$\Rightarrow a^k \in \ker(\gamma_N) = N$. ∎

ex S_3, $H = \{id, (1,2)\}$, $[G:H] = 6/2 = 3$, $(2\ 3)^3 = (2\ 3) \notin H$.

Lemma 2: Let $N \trianglelefteq G$, $a, x \in G$. If $x \in aN$ then $x^{-1} \in a^{-1}N$.
Proof: $x \in aN \Rightarrow xN = aN \Rightarrow \gamma_N(x) = \gamma_N(a) \Rightarrow \gamma_N(x^{-1}) = \gamma_N(a^{-1})$
$\Rightarrow x^{-1}N = a^{-1}N \Rightarrow x^{-1} \in a^{-1}N$ ∎

Lemma 3: Let $H \leq G$, $N \trianglelefteq G$. Then $NH = HN \leq G$.
Proof: $HN = \bigcup_{h \in H} hN = \bigcup_{h \in H} Nh = NH$.
Clearly $HN \neq \emptyset$. Suppose $hn, h'n' \in HN$. so $hn \in hN$, $h'n' \in h'N$.
Then $hnh'n' \in hNh'N = hh'NN = hh'N \subseteq HN$.
And ~~$(hn)^{-1} = n^{-1}h^{-1}$~~ if $x \in HN$, $x \in hN \Rightarrow x^{-1} \in h^{-1}N \subseteq HN$. ∎

Theorem (Cauchy): Let G be a finite abelian group. If a prime p is s.t. $p \mid |G|$ then $\exists$ an element of order p.
Pf: Clear if G is cyclic.. Proceed by induction. (on what???)
Base-case: $|G| = p \Rightarrow G$ cyclic as above.
Inductive step: $|G| = mp$, $m > 1$. Pick $a \in G \setminus \{e\}$
Case 1: $p \mid |a|$. Then $\langle a \rangle$ contains an element of order p.
Case 2: $p \nmid |a|$. Note $\{e\} < \langle a \rangle < G$. As G is abelian, $\langle a \rangle \trianglelefteq G$.
As $|G/H| \cdot |H| = |G|$ and $p \mid |G|$ and $p \nmid |\langle a \rangle|$, $p \mid |G/\langle a \rangle|$.
Note $|G/H| < |G|$ and G/H satisfies conditions, so $\exists\ gH \in G/H$ of order p. Let $n = |g^p|$. Claim: $|g^n| = p$.

show $|g^n| \in \{1, p\}$ get X

(fill in!) ← see midterm sols

$\varphi < \varphi$

1st ?

2013 02 15

☆☆☆ Midterm: Friday March 2nd, 8:30am
LJES
- no regurgitated proofs
- do know definitions
- know lots of examples *
- up to 2013 02 13 lecture, and up to assignment 5 ☆☆☆

Recall: If $N \triangleleft G$ then we have the surjective homomorphism $\nu_N : G \to G/N$, with $\ker(\nu_N) = N$.

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\nu"'] & \varphi(G) \\ G/N \arrow[ur, dashed, "\cong"'] & \end{tikzcd}$$

Theorem (First Isomorphism Theorem): Let $\varphi: G \to H$ be a group homomorphism. Then $\varphi(G) \leq H$ and $\varphi(G) \cong G/\ker(\varphi)$.

Proof: Exercise: Show $\varphi(G) \leq H$.

(apparently $N = \ker(\varphi)$)

Define $\psi: G/N \to \varphi(G)$ by $\psi(aN) = \varphi(a)$.

First we show this is well-defined. Suppose $aN = bN$. Then $a^{-1}b \in N$, so $\varphi(a^{-1}b) = e \Rightarrow \varphi(a)^{-1}\varphi(b) = e \Rightarrow \varphi(a) = \varphi(b)$, as required.

Now we show ψ is a homomorphism. Let $a, b \in G$. Then $\psi(aN\,bN) = \psi(abN) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(aN)\psi(bN)$.

Finally, ψ is clearly surjective, and (it is easy to show) $\ker(\psi) = \{e\}$, so ψ is a group isomorphism.

ex Consider $G = (\mathbb{C}^\times, \cdot)$ and $H = \{z \in \mathbb{C}^\times ; |z| = 1\}$. Then $H \triangleleft \mathbb{C}$ since $\mathbb{C}$ is abelian. We saw (A3) the cosets of H are circles.

What is $\mathbb{C}^\times/H$?

Consider the group homomorphism $\varphi: \mathbb{C}^\times \to (\mathbb{R}^+, \cdot)$ given by $\varphi(z) = |z|$. Note $\varphi(ab) = |ab| = |a||b| = \varphi(a)\varphi(b)$. (or $\mathbb{R}^\times$)

We note $\ker(\varphi) = H$ and $\operatorname{im}(\varphi) = \varphi(\mathbb{C}^\times) = \mathbb{R}^+$, so by the First Isomorphism Theorem, $\mathbb{R}^+ \cong \mathbb{C}^\times/H$.

ex $\{e\}, G \triangleleft G$, and $G/\{e\} = \{\{a\} ; a \in G\} \cong G$, $G/G = \{G\} \cong \{e\}$.

ex Consider the cyclic group $(\mathbb{Z},+)$.
Recall (from Jan 16) that every subgroup is cyclic.
The subgroups are $n\mathbb{Z}$ $\quad \forall n \in \mathbb{N}\cup\{0\}$
The quotients are $\mathbb{Z}/n\mathbb{Z} =: \mathbb{Z}_n$.

Let G be any group, $a \in G$. Define $\varphi: \mathbb{Z} \to G$ by $\varphi(n) = a^n$.
Check this is a homomorphism.
Note $\varphi(\mathbb{Z}) = \langle a \rangle$.
By 1st iso thm, $\mathbb{Z}/\ker(\varphi) \cong \langle a \rangle$, a cyclic group.

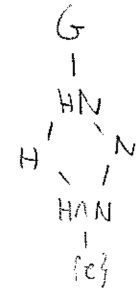
This proves:

Theorem: Every cyclic group is isomorphic to $\mathbb{Z}_n$, $n \in \mathbb{N}\cup\{0\}$.

Recall the first isomorphism theorem.

Lemma: Suppose $H \leq G$, $N \triangleleft G$. Then $HN = NH \leq G$ (recall from 0213)

Remark: HN is the smallest subgroup containing H and N



Theorem (Second Isomorphism Theorem): Suppose $A \leq G$, $B \triangleleft G$.
Then $B \triangleleft AB$, $A \cap B \triangleleft A$, and $AB/B \cong A/A\cap B$

Proof: Exercises. Define $\varphi: AB \to A/A\cap B$ by $\varphi(ab) = a(A\cap B)$.
First we show well-defined. Suppose $a_1b_1 = a_2b_2$. Then $a_2^{-1}a_1 = b_2b_1^{-1} \in A\cap B$.
So $a_2^{-1}a_1 \in A\cap B \Rightarrow a_1(A\cap B) = a_2(A\cap B)$.
Next we show φ is a group homomorphism. Let $a_1b_1, a_2b_2 \in AB$. As $b_1a_2 \in Ba_2 = a_2B$, $\exists b_3 \in B$ st $b_1a_2 = a_2b_3$.
So $\varphi(a_1b_1a_2b_2) = \varphi(a_1a_2b_3b_2) = a_1a_2(A\cap B)$
and $\varphi(a_1b_1)\varphi(a_2b_2) = (a_1(A\cap B))(a_2(A\cap B)) = a_1a_2(A\cap B)$. So φ is a group hom.
Remains to show $\ker(\varphi) = B$, $\operatorname{im}(\varphi) = A/A\cap B$.
Well for $a(A\cap B) \in A/A\cap B$, $\varphi(ae) = a(A\cap B) \Rightarrow \operatorname{im}(\varphi) = A/A\cap B$
Suppose $\varphi(ab) = A\cap B$. Then $aA\cap B = eA\cap B$ so $a \in A\cap B \Rightarrow a \in B \Rightarrow ab \in B$. (Note these are iff's so $\ker(\varphi) = B$).
By first isomorphism theorem, done. ∎

Theorem (Third Isomorphism Theorem): Suppose $H \triangleleft G$, $H \leq K \leq G$.
Then $K \triangleleft G$ iff $K/H \triangleleft G/H$. If so, $K/H \,/\, G/H \cong G/K$.

Proof: Exercises Now assume $K \triangleleft G$. Define $\varphi: G/H \to G/K$ by $\varphi(aH) = aK$.
First show well-defined. $a_1H = a_2H \Rightarrow a_1^{-1}a_2 \in H \subseteq K \Rightarrow a_1K = a_2K$.
Next show group homomorphism. Easy.
Next show $\operatorname{im}(\varphi) = G/K$. Easy
Finally $\varphi(aH) = K$ iff $aK = K$ iff $a \in K$ iff $aH \in K/H$
So apply first isomorphism to get done ∎