First Iso. Thm. for Groups

Last time: if $N \subset G$ is a normal subgroup
then $G/N = \{\text{left cosets } aN\} = \{\text{right cosets } Na\}$
inherits a well-defined mult.

↳ fails if it's not a normal subgroup:
let $G = D_5$
$H = \{1, s\}$
$sH = \{s, 1\}$ same as H

$rH = \{r, rs\} = \{r, sr^4\}$
$sr^4H = \{sr^4, sr^4s\} = \{sr^4, r\}$ same as rH

if we define $\underline{sH} \cdot \underline{rH} = srH = \{sr, srs\}$
$= \{sr, r^4\}$

then we'd run into trouble because
$\underline{1H} \cdot \underline{sr^4H} \neq (1 \cdot sr^4)H = sr^4H = \{sr^4, r\}$

same! same! different!

operation on G/H is well-def.
iff H is normal.

normal example:
$G = D_5 \qquad N = \langle r \rangle.$
how should we understand G/N?

as with rings, use the 1^{st} iso theorem.

Thm: a homomorphism $\varphi: G \to H$ induces an isomorphism $\bar{\varphi}: G/\ker\varphi \to \operatorname{im}\varphi$.

Recall that $\ker\varphi$ is a normal subgroup of G, $\operatorname{im}\varphi$ is a subgroup of H.

To understand $D_5/\langle r\rangle$, want a hom.

$$\varphi: D_5 \longrightarrow \text{some group}$$

with $\ker\varphi = \langle r\rangle$.

Then $D_5/\langle r\rangle \cong \operatorname{im}\varphi$.

Take $\varphi: D_5 \longrightarrow \{\pm 1\} \cong \mathbb{Z}_2$

$$\varphi(\text{rotation}) = 1$$
$$\varphi(\text{reflection}) = -1$$

Check: this is a hom.
once that's done, know that $D_5/\langle r\rangle \cong \mathbb{Z}_2$

(φ is surjective, so $\operatorname{im}\varphi$ = everything.)

---

had $\text{sign}: S_n \to \mathbb{Z}_2$
surjective. kernel = $\underbrace{\text{even permutations}}_{A_n = \text{alternating group}}$.

so $A_n \subset S_n$ is normal and $S_n/A_n \cong \mathbb{Z}_2$.

exercise: in D_4, $N = \{1, r^2\}$
$\boxed{I}$ $\boxed{180}$

this is normal

$|D_4| = 8$ $|N| = 2$

so $|D_4/N| = 4$

ask: is $D_4/N \cong \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$?

in D_6, $N = \{1, r^3\}$ is normal

is $D_6/N \cong \mathbb{Z}_6$ or S_3 ?

is there a geom. interpretation?

Thm: a homomorphism $\varphi: G \to H$ induces an isomorphism $\bar{\varphi}: G/_{\ker\varphi} \to \operatorname{im}\varphi$.

Pf. Let $K = \ker \varphi \subset G$

Given $aK \in G/K$, define $\bar{\varphi}(aK) = \varphi(a)$.

Is it well-defined? ✓

if $aK = bK$ then $a = bk$ for some $k \in K$.

So $\varphi(a) = \varphi(bk) = \varphi(b) \cdot \varphi(k)$
$= \varphi(b) \cdot 1$

So $\bar{\varphi}(aK) = \bar{\varphi}(bK)$

Is it a homomorphism? ✓

$$\bar{\varphi}(aK \cdot bK) = \bar{\varphi}(abK)$$
$$= \varphi(ab)$$
$$= \varphi(a)\varphi(b)$$
$$= \bar{\varphi}(aK)\,\bar{\varphi}(bK)$$

Is it injective? ✓

if $\bar{\varphi}(aK) = 1$ then $\varphi(a) = 1$

so $a \in K$

so $aK = K$

thus $\ker \bar{\varphi}$ = just the identity elt $K = 1K$

so $\bar{\varphi}$ is injective.

Is it surjective? ✓

Let $h \in \operatorname{im} \varphi \subset H$

choose $a \in G$ s.t. $\varphi(a) = h$.

then $\bar{\varphi}(aK) = h$

$\boxed{\text{Q.E.D.}}$

Application

Last quarter, Homework 8,

Challenge problem §3.3 #10:

$x^4 - 10x^2 + 1$ is irred in $\mathbb{Q}[x]$

but reducible in $\mathbb{Z}_p[x]$ $\forall p$

Key fact: if 2 is not a square in $\mathbb{Z}_p$
and 3 is not ― ― ― ―
then 6 <u>is</u> a square in $\mathbb{Z}_p$

Let $G = \mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ under mult.
$|G| = p-1$

consider $\varphi : G \to G$ this is a hom.
$a \longmapsto a^2$ bec. G is Abelian.

claim: if $2 \notin \operatorname{im} \varphi$ and $3 \notin \operatorname{im} \varphi$
then $6 \in \operatorname{im} \varphi$.

let $N = \operatorname{im} \varphi$.

know that $6N = N$ iff $6 \in N$
similarly with 2 and 3

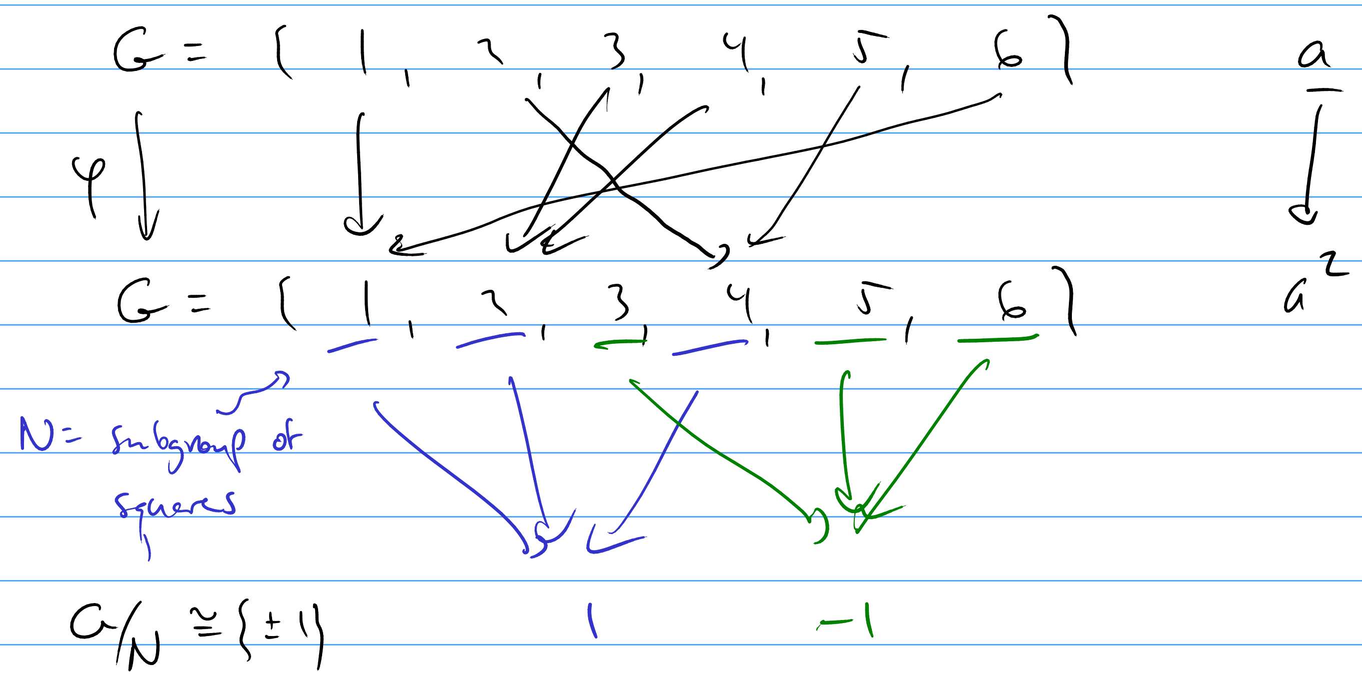
if we show that $[G:N] = 2$
i.e. $|N| = |G|/2 = \frac{p-1}{2}$ ☆

then we win, because G/N is a group with 2 elements,
so $G/N \cong \{\pm 1\} \cong \mathbb{Z}/2$

Can get a hom. $\psi : G \to \{\pm 1\}$
with $\ker \psi = N = \{\text{squares}\}$

if 2 and 3 are not squares then
$\psi(2) = -1 \quad \psi(3) = -1$
so $\psi(6) = \psi(2)\,\psi(3) = (-1)\cdot(-1) = 1$
so 6 is a square.

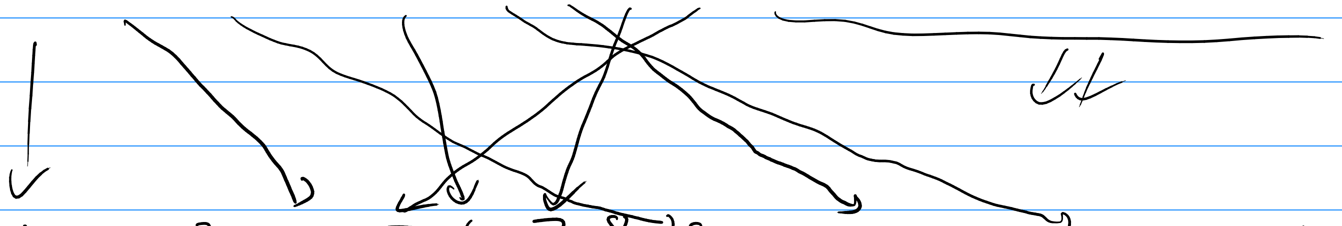
Example: $p = 7$



Another example: $p = 19$

$G =$ $\qquad$ $10 = -9 \qquad 10^2 = 9^2$ etc

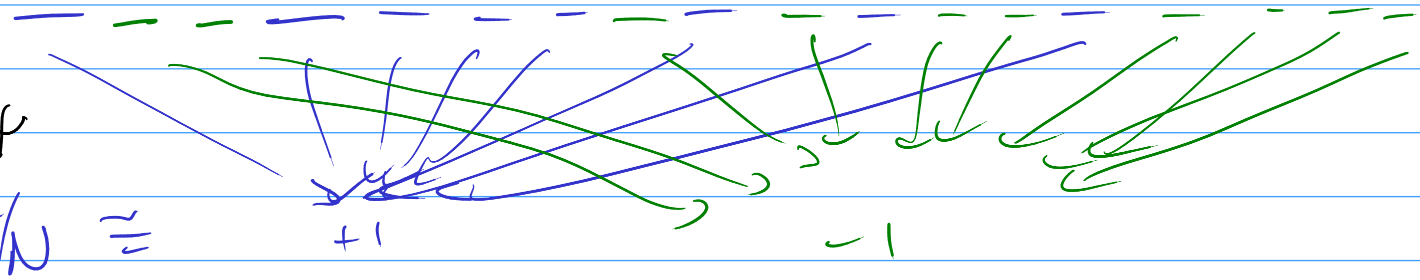
$\{1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\}$



$\{1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\}$

ψ

$G/N \cong$



$\psi(2) = -1 \qquad \psi(3) = -1 \qquad \psi(6) = 1$

Remains to see that $|N| = |G|/2$.

$$G \xrightarrow{\varphi} G$$

$N = \operatorname{im} \varphi \cong G/\ker \varphi$.

$\ker \varphi$?: $a \in G = \mathbb{Z}_p^\times$ with $a^2 = 1$

if p is odd then then $a = \pm 1$

So $|\ker| = 2$ so $|N| = |G|/2$ $\blacksquare$

(if p is even, don't need a fancy argument...)