Group Theory
Week #6, Lecture #22

Prop G finite group, $H, K \leq G$ subgroups $\Rightarrow |HK| = \frac{|H|\,|K|}{|H \cap K|}$

Proof The multiplication map $\mu: G \times G \to G$, $\mu(a,b) = ab$ restricts to a map $\varphi: H \times K \to G$, $\varphi(h,k) = hk$ (in general, this is not a homomorphism)

Note that $\operatorname{im}(\varphi) = \{x \in G : x = \varphi(h,k) \text{ for some } h \in H, k \in K\}$
$= \{x : x = hk\}$
$=: HK$

[this is not a subgroup in general, so φ is not a hom in such cases, since φ hom $\Rightarrow \operatorname{im}(\varphi)$ subgroup]

Also note that $|H \times K| = |H| \cdot |K|$

To finish the proof, it is enough to show

$$\boxed{\varphi^{-1}(\{x\}) = \{(hz, z^{-1}k) : z \in H \cap K\}} \quad (*)$$

for all $x = hk \in HK = \operatorname{im}(\varphi)$. Indeed

$|\varphi^{-1}(\{x\})| = |H \cap K|$,

and so $|H \times K| = |\operatorname{im}(\varphi)| \cdot |\varphi^{-1}(\{x\})|$
$= |HK| \cdot |H \cap K|$

$\subseteq$ Let $(a,b) \in \varphi^{-1}(\{x\})$, $(a',b') \in \varphi^{-1}(\{x\})$. Then $ab = x$ $(= \varphi(a,b))$, $a'b' = x$ $(= \varphi(a',b'))$

$\therefore$ $ab = a'b' \Rightarrow \underbrace{a^{-1}a'}_{\in H} = \underbrace{b(b')^{-1}}_{\in K}$ $\leftarrow$ since $H, K \leq G$

$\therefore$ if we set $z := a^{-1}a' = b(b')^{-1}$, then $z \in H \cap K$

Moreover, $az = a'$, $zb' = b$ $\Rightarrow (a,b) = (a'z^{-1}, zb')$ and $(a',b') = (az, z^{-1}b)$

$\supseteq$ If $g = (hz, z^{-1}k)$, then $\varphi(g) = (hz)(z^{-1}k) = hk = x$
$\therefore g \in \varphi^{-1}(\{x\})$

QED

Lemma Let G be a finite group, and $S, T \subseteq G$ two subsets. Then:

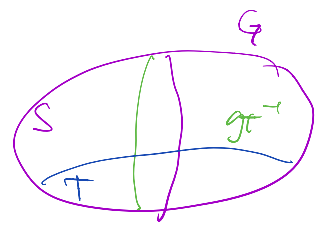
$$\boxed{|S| + |T| > |G| \Rightarrow ST = G}$$

Proof By def, $ST \subseteq G$. So we need to show $G \subseteq ST$.
Let $g \in G$. Consider the subset $gT^{-1} \subseteq G$, where $T^{-1} := \{t^{-1} : t \in T\}$ and $gT^{-1} := \{g\} \cdot T^{-1} = \{gt^{-1} : t \in T\}$

Then: $\boxed{|gT^{-1}| = |T|}$ $\quad \left(\begin{matrix} T & \overset{\text{bij}}{\longleftrightarrow} & gT^{-1} \\ t & \longmapsto & gt^{-1} \end{matrix} \right)$

Hence, by the assumption of the lemma:

$$\boxed{|S| + |gT^{-1}| > |G|}$$



Hence

$$S \cap gT^{-1} \neq \emptyset$$

(otherwise, if $S \cap gT^{-1} = \emptyset$, then $\underset{= |S \cup gT^{-1}| \leq |G|}{|S| + |gT^{-1}|}$)

and so, $\exists s \in S$ of the form

$$s = gt^{-1}, \text{ for some } t \in T$$

$$\therefore \quad g = st \in ST$$

QED

→ **Application of the Lemma to Fields & Groups**

Corollary Every element in a finite field is a sum of two squares.

Proof (only for the field $F = \mathbb{Z}_p$, though same proof works for arbitrary finite field $F = \mathbb{F}_q$, $q = p^n$)

* First some intuition: (for $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$)

$p=2$: $0 = 0^2$, $1 = 1^2$ ✓ $(x = a^2 \Rightarrow x = a^2 + 0^2)$

$p=3$: $0 = 0^2$, $1 = 1^2$, $2 = 1^2 + 1^2$ ✓

$p=5$: $0 = 0^2$, $1 = 1^2$, $2 = 1^2 + 1^2$, $3 = 2^2 + 2^2$, $4 = 2^2$ ✓

$\underbrace{2 \quad 4}_{\equiv 3}$

* Step 1 First we work in the multiplicative group

$$\boxed{\mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}} \quad \text{(of order } p-1)$$

Write $\mathbb{Z}_p^\times = \{\underset{1}{e}, a, a^2, \ldots, a^{p-1}\} = \langle a \rangle$

[where a is a generator of the cyclic group $\mathbb{Z}_p^\times$ (there are $\phi(p-1)$ of those]

WLOG, we may assume $p > 2$.

Set

$$\boxed{S := \langle a^2 \rangle = \{e, a^2, a^4, \ldots, a^{p-1}\} \quad \text{squares}}$$

$$T := \mathbb{Z}_p^\times \setminus S = \{a, a^3, a^5, \ldots, a^{p-2}\} \quad \text{non-squares}$$

note that: $|S| = \frac{p-1}{2}$ and so $|T| = \frac{p-1}{2}$

eg: for $p=7$ and $a=3$: $S = \{\underset{e}{1}, \underset{a^2}{2}, \underset{a^4}{4}\}$, $T = \{\underset{a}{3}, \underset{a^5}{5}, \underset{a^3}{6}\}$

* Step 2 Now we work in the full additive group $\mathbb{Z}_p$

Write $S' = S \cup \{0\}$ so that $|S'| = \frac{p-1}{2} + 1 = \frac{p+1}{2}$

$0 = 0^2$ is also a square

Then: $|S'| + |S'| = \frac{p+1}{2} + \frac{p+1}{2} = p + 1 > p = |\mathbb{Z}_p|$

Hence, by the Lemma:

$$\boxed{\mathbb{Z}_p = S' + S'} \quad \text{(product of two sets, written additively)}$$

elements in here are all squares!

QED

Isomorphism Theorems for Groups

Theorem Let G be a group, $H \leq G$ a subgroup and $N \trianglelefteq G$ a normal subgroup. Then:

(i) $HN \leq G$

(ii) $H \cap N \trianglelefteq H$

(iii) $\boxed{HN/N \cong H/H \cap N}$

Proof (i) — done in last lecture ($N \trianglelefteq G \Rightarrow H \leq N(N) = G \Rightarrow HN \leq G$)

(ii) Consider the projection homomorphism

(use $N \trianglelefteq G$) $\qquad G \xrightarrow{\pi} G/N \qquad \pi(g) = gN, \ \forall g \in G$

and let $\boxed{\varphi : H \longrightarrow G/N}$ be its restriction to H, so that $\boxed{\varphi(h) = hN}$, $\forall h \in H$ — also a homomorphism.

Then:

$*$ $$\begin{aligned} \mathrm{im}(\varphi) &= \{ gN : gN = hN \text{ for some } h \in H \} \\ &= \{ gN : g \in HN \} \quad g = g \cdot e = hn, \text{ for some } h \in H \\ &= HN/N \end{aligned}$$

$*$ $$\begin{aligned} \ker(\varphi) &:= \{ h \in H : \varphi(h) = e_{G/N} \} \\ &= \{ h \in H : \underset{hN}{\varphi(h)} = N \} \quad \begin{pmatrix} g_1 N = g_2 N \\ \Updownarrow \\ g_2^{-1} g_1 \in N \end{pmatrix} \\ &= \{ h \in H : h \in N \} \\ &= H \cap N \end{aligned}$$

By the FTH:

$$H/\ker\varphi \xrightarrow{\overline{\varphi}} \mathrm{im}(\varphi) \quad \text{is an iso}$$

$$\therefore \quad H/H \cap N \cong HN/N$$

QED

Quick example

Let: $G = D_8 = \{e, a, \dots, a^7, b, \dots, ba^7\}$ $\quad a^8 = b^2 = 1,\ ba = a^{-1}b$

$N = \langle a^2 \rangle \cong \mathbb{Z}_4$ (normal subgroup)

$H = \{e, a^4, b, a^4 b\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (subgroup)

Then: $HN = \{e, a^2, a^4, a^6, b, a^2 b, a^4 b, a^6 b\} \cong D_4$

$H \cap N = \{e, a^4\} \cong \mathbb{Z}_2$

1st Iso Theorem says: $HN/N \cong H/H\cap N$

$D_4/\mathbb{Z}_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2/\mathbb{Z}_2 \quad (\cong \mathbb{Z}_2)$ ✓

Theorem (2nd Iso Thm) Let H and N be two normal subgroups of G, with $N \subseteq H$. Then

(i) $H/N \triangleleft G/N$

(ii) $\boxed{{}^{G/N}\big/_{H/N} \cong G/H}$

(Proof next time)

Quick example If $m|n$, then $\mathbb{Z}_n/m\mathbb{Z}_n \cong \mathbb{Z}_m$.

Reason: Take $G = \mathbb{Z}$
$N = n\mathbb{Z}$
$H = m\mathbb{Z}$

$m|n \Rightarrow \underset{N}{n\mathbb{Z}} \subseteq \underset{H}{m\mathbb{Z}}$

Then: ${}^{G/N}\big/_{H/N} \cong G/H$

${}^{\mathbb{Z}/n\mathbb{Z}}\big/_{m\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/m\mathbb{Z}$

$\mathbb{Z}_n/m\mathbb{Z}_n \cong \mathbb{Z}_m$ ✓