Recap:

$H, K \leq G$

- $H \vee K = \langle HK \rangle$ join of H and K

if $N \trianglelefteq G$ then $H \vee N = NH = HN$.

The second Isomorphism explores the relationship between $H, N, HN, H \cap N$.

$$\begin{tikzcd}[column sep=small] & HN \arrow[dl, dash] \arrow[dr, dash] & \\ N \arrow[dr, dash] & & H \arrow[dl, dash] \\ & H \cap N & \end{tikzcd}$$

Second Isomorphism Theorem: If $H \leq G$, $N \trianglelefteq G$, then

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

$ghH = \{gh\tilde{h} \mid \tilde{h} \in H\}$ equal!
$gH = \{gh' \mid h' \in H\}$
$h' = h\tilde{h}$ $\quad \tilde{h} = h^{-1}h'$

Proof:
$$H \longrightarrow HN \xrightarrow{\pi} HN/N$$
$$h \longmapsto h \longmapsto hN$$

$$\boxed{\begin{array}{l} \text{If } H < G \\ ghH = gH \\ \forall g \in G,\ h \in H \end{array}}$$

$$\phi : H \to HN/N$$
$$h \mapsto hN.$$

Claim 1: ϕ is surjective!

Proof: Take $\underbrace{h}_{\in H}\underbrace{n}_{\in N}N \in HN/N$. Then $hnN = hN$

and thus $hnN = \phi(h)$.

Claim 2: $\ker \phi = N \cap H$

<u>Proof</u>: S'pose $h \in \ker\phi$.

Then $\phi(h) = N$

$$\phi(h) = hN.$$

$$hN = N$$

True if $h = e$ or
more generally when $h \in N$!

If $hN = N$ then $hn = e$ for some $n \in N$
$\overset{\in}{e}$ $\quad h = n^{-1} \in N.$ $\therefore$ $hN = N \Leftrightarrow h \in N.$

$\Updownarrow$

$h \in \ker\phi$

$\therefore \ker\phi = N \cap H.$

G/N

$aN \quad bN \quad eN = N$

$(aN)(bN) = abN$

$(aN)(eN) = aeN = aN$

$nN = N$

Thus $\phi : H \to HN/N$ epimorphism
$\ker\phi = H \cap N.$ 1st Iso. Theorem:

$$\tilde{\phi} : H/(H \cap N) \xrightarrow{\cong} HN/N$$

$\square$

<u>Theorem</u>: Let a, b be positive integers.
Then

$$\frac{ab}{\gcd(a,b)} = \operatorname{lcm}(a,b)$$

<u>Proof</u>: Will work with subgroups of $\mathbb{Z}$ w/ $+$.

$$(H+N)/N \cong H/(H \cap N)$$

$$\left.\begin{array}{l} H = a\mathbb{Z} \\ N = b\mathbb{Z} \end{array}\right\} \quad H+N = a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b)\mathbb{Z}$$

why???

$\exists\, m, n$ s.t. $am + bn = \gcd(m,n)$
also if $k = au + bv$

then since $\gcd(a,b) \mid a$ and $\mid b$ $\Rightarrow \gcd(a,b) \mid au+bv$
$\Rightarrow \gcd(a,b) \mid k$

$$H \cap N = a\mathbb{Z} \cap b\mathbb{Z} = \operatorname{lcm}(a,b)\mathbb{Z}$$

$$\therefore \quad \underbrace{\frac{\gcd(a,b)\mathbb{Z}}{b\mathbb{Z}}}_{\substack{\text{order}\\ \text{is } b/\gcd(a,b)}} = \frac{(H+N)}{N} \cong \frac{H}{H\cap N} = \underbrace{\frac{a\mathbb{Z}}{\operatorname{lcm}(a,b)\mathbb{Z}}}_{\substack{\text{order}\\ \text{is } \operatorname{lcm}(a,b)/a}}$$

Quick note if $r \mid s$ then $s\mathbb{Z} \leq r\mathbb{Z}$ and $\left|\frac{r\mathbb{Z}}{s\mathbb{Z}}\right| = \frac{s}{r}$

$$\frac{b}{\gcd(a,b)} = \frac{\operatorname{lcm}(a,b)}{a}$$

$\square$

Third Isomorphism Theorem:

Let $H, K \trianglelefteq G$ with $K \leq H$.
Then
$$(G/K)/(H/K) \cong G/H$$

Proof: $G \xrightarrow{\pi} G/H$ surjection

$K \subseteq \ker(\pi) = H$ so π descends to the quotient

$G/K \xrightarrow{\tilde{\pi}} G/H$ surjection!

Q: what is $\ker(\tilde{\pi})$?

A: $\tilde{\pi}(gK) = H \Leftrightarrow \pi(g) = H \Leftrightarrow gH = H \Leftrightarrow g \in H$.

$\ker(\tilde{\pi}) = \{hK \mid h \in H\} = H/K$

By 1st Isomorphism theorem

$$\tilde{\tilde{\pi}} : (G/K)/(H/K) \xrightarrow{\cong} G/H$$

$\square$

Group Actions:

G-set

Def: A group action of a group G on a set X is a function $G \times X \to X$
$$(g, x) \mapsto g \cdot x$$
satisfying two rules

- $e \cdot x = x \quad \forall x \in X$
- $a \cdot (b \cdot x) = (ab) \cdot x \quad \forall a, b \in G, x \in X.$

Def: The orbit of $x \in X$ is $\text{orb}(x) = \{g \cdot x \mid g \in G\}$

Prop: The relation $x \sim y \Leftrightarrow y \in \text{orb}(x)$ is an equivalence relation on X. Thus the orbits form a partition of x.
$$X/G = \{\text{orb}(x) \mid x \in X\}.$$

Def: Let $S \subseteq X$. The stabilizer subgroup or isotropy subgroup of S is
$$G_S = \{g \in G : g \cdot x = x \ \forall x \in S\}$$
Special case G_x to mean $G_{\{x\}}$

Orbit-Stabilizer Theorem: $|G| = |G_x| \cdot |\text{orb}(x)|$

equivalently $|\text{orb}(x)| = [G : G_x]$.

Cool consequence!

$$|G| = \sum_{[x] \in X/G} |\text{orb}(x)| = \sum_{[x] \in X/G} [G : G_x]$$

$$X_G = \{x \in X \mid g \cdot x = x \ \forall g \in G\} = \{x \in X \mid |\text{orb}(x)| = 1\}$$

$$\boxed{|G| = |X_G| + \sum_{\substack{[x] \in X/G \\ |\text{orb}(x)| > 1}} [G : G_x]}$$

Theorem: If G is a group and $|G| = p^r$ for p prime then G has a non-trivial center.

Proof:

Take $X = G$.

Define the action by $g \cdot x = gxg^{-1}$

$$\underbrace{|X|}_{p^r} = |X_G| + \sum_{\substack{[x] \in X/G \\ |orb(x)| > 1}} \underbrace{[G : G_x]}_{\text{multiples of } p}$$

$\therefore |X_G|$ must also be a multiple of p.

$$X_G = \{x \in X \mid g \cdot x = x \ \forall g \in G\}$$
$$= \{x \in X \mid gxg^{-1} = x \ \forall g \in G\}$$
$$= \{x \in G \mid gxg^{-1} = x \ \forall g \in G\} = \text{center of } G$$

$gx = xg$

$|X_G| \geq 1$ and $|X_G| \neq 1$ so $X_G \neq \{e\}$ $\square$

Corollary: If $|G| = p^2$ then G is abelian.

Proof: S'pose G not abelian. G has a nontrivial element x in its center. $|\langle x \rangle| \mid |G|$. so $|\langle x \rangle| = p$

$e, x, x^2, x^3, \dots, x^{p-1}$

Take $y \in G$ not in the center. Then

$y, xy, x^2y, x^3y, \dots, x^{p-1}y, \ y^2, xy^2, \dots, x^{p-1}y^2$

$G = \{x^m y^n \mid 0 \leq m, n < p\}$ $\quad$ p^2-many diff. elements

$$(x^m y^n)(x^k y^l) = x^m (y^n x^k) y^l = x^m x^k y^n y^l$$
$$= x^k x^m y^l y^n$$
$$= (x^k y^l)(x^m y^n)$$

$\Rightarrow\!\Leftarrow$.

$\square$