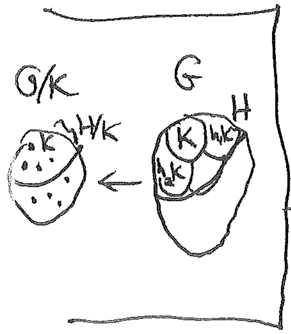
PROPOSITION: Given $K \lhd G$ and the quotient G/K with $\begin{array}{l} G \xrightarrow{\pi} G/K, \\ g \longmapsto gK \end{array}$
(THM 2.10.5)

one obtains a bijection



$$\left\{ \begin{array}{c} \text{subgroups} \\ \bar{H} \text{ of } G/K \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subgroups } H \text{ of } G \\ \text{with } K \leq H \leq G \end{array} \right\}$$

$$\pi(H) = \{hK : h \in H\} \longleftarrow\!\!\shortmid \; H$$

$$\begin{array}{c} \bar{H} \\ \shortparallel \\ \{K, h_1K, h_2K, \ldots\} \end{array} \longmapsto \{h \in G : hK \in \bar{H}\} = \bigsqcup_{h_iK \in \bar{H}} h_iK$$

with the property that $|H| = |\bar{H}| \cdot |K|$ (when G is finite).

proof: Try it yourself! ∎

10/31/2018 ≥

EXAMPLE: $G = \mathbb{Z}$, $K = 6\mathbb{Z}$ ($K \lhd G$)

$G/K = \mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$$\begin{tikzcd} & G/K \arrow[dl, dash] \arrow[dr, dash] & \\ \{\bar{0}, \bar{2}, \bar{4}\} \arrow[dr, dash] & & \{\bar{0}, \bar{3}\} \arrow[dl, dash] \\ & \{\bar{0}\} & \end{tikzcd}
\qquad
\begin{tikzcd} & G = \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \arrow[dl, dash] \arrow[dr, dash] & \\ 2\mathbb{Z} = \{\ldots, -2, 0, 2, 4, \ldots\} \arrow[dr, dash] & & 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, \ldots\} \arrow[dl, dash] \\ & K = 6\mathbb{Z} = \{\ldots, -12, -6, 0, 6, 12, \ldots\} & \end{tikzcd}$$

---

proof that a p-group P with $|P| = p^e$ has subgroups H with $|H| = p^k$ $\forall\, 1 \leq k \leq e$:

Induct on e. In the base case $e = 1$, $|P| = p$ so there's nothing to show.

In the inductive step, since P is a p-group, $\exists$ some $g \in Z(P) - \{1\}$, say with order $\mathrm{ord}(g) = p^{\ell}$, $\ell \geq 1$, and then another element $z = g^{p^{\ell-1}} \in Z(P)$ having $\mathrm{ord}(z) = p$. This z generates a cyclic subgroup $K = \langle z \rangle$ having $|K| = p$, and P/K is a p-group of size $|P/K| = p^{e-1}$. By induction on e, P/K contains subgroups $\bar{H}$ of all sizes $|\bar{H}| = p^{k'}$ with $0 \leq k' \leq e-1$, and then under the Correspondence Thm, they give subgroups H of P of sizes $|H| = p^k$ for $1 \leq k \leq e$ ∎

(100) <u>COROLLARY:</u> $|G| = 2p$, $p \neq 2$ prime

$\Rightarrow$ either $G \cong (\mathbb{Z}/2p\mathbb{Z})^+$ (cyclic)

or $G \cong D_p$ (dihedral)

<u>proof:</u> <u>CASE 1:</u> G cyclic. ✓

<u>CASE 2:</u> G not cyclic.

By Cauchy's Thm, $\exists\, r \in G$ with $\mathrm{ord}(r) = p$

We claim <u>any</u> $s \in G \setminus \langle r \rangle$ has $\mathrm{ord}(s) = 2$:

Any such s has prime order 2 or p (since G not cyclic),

so $\langle s \rangle \cap \langle r \rangle = \{1\}$ (Why?)

and hence the map $\langle s \rangle \times \langle r \rangle \xrightarrow{\mu} G$ is injective

$(h, k) \mapsto hk$

and would have $|\mathrm{Im}(\mu)| = |\langle s \rangle \times \langle r \rangle| = p \cdot p$ <u>too big</u>

if $\mathrm{ord}(s) = p$. Thus $\mathrm{ord}(s) = 2$.

Now pick any such $s \in G \setminus \langle r \rangle$.

Since $sr \notin \langle r \rangle$ also, $1 = (sr)^2 = srsr$

$$\Rightarrow \underset{srs^{-1}}{\underset{\shortparallel}{srs}} = r^{-1}$$

Thus we have $G = \langle s, r \rangle$ with $\boxed{s^2 = 1 = r^p}$

and $\boxed{srs^{-1} = r^{-1}}$

which one can see makes $G \cong D_p = \{1, r, r^2, \ldots, r^{p-1}, s, sr, sr^2, \ldots, sr^{p-1}\}$ ∎

Note that whenever $s_p (= \#\text{Sylow } p\text{-subgroups}) = 1$,

then Sylow's 2^{nd} Thm. implies that the unique Sylow p-subgroup P must be normal, i.e. $P \triangleleft G$, since $\forall g \in G$, $|gPg^{-1}| = |P|$

$\Rightarrow gPg^{-1}$ is a Sylow p-subgroup

$\Rightarrow gPg^{-1} = P$

COROLLARY: When $|G| = pq$ with p, q primes, $p < q$ and $p \nmid q-1$, then $G \cong (\mathbb{Z}/pq\mathbb{Z})^+$

i.e. G is cyclic.

EXAMPLES: (1) $|G| = 15 = \overset{p}{3} \cdot \overset{q}{5}$ $(3 \nmid 5-1=4)$ $\} \Rightarrow G \cong (\mathbb{Z}/15\mathbb{Z})^+$

(2) But $|G| = 21 = \overset{p}{3} \cdot \overset{q}{7}$ $(3 \mid 7-1=6)$ does not imply $G \cong (\mathbb{Z}/21\mathbb{Z})^+$;

(Artin analyzes the other possibility for $|G|=21$ as part of his PROP. 7.7.7)

11/2/2018

proof of COROLLARY: Note Sylow's $3^{rd} \Rightarrow s_q \mid p \Rightarrow s_q = 1$ or p

and $s_q \equiv 1 \mod q \Rightarrow \boxed{s_q = 1}$ (since $p < q$)

Also Sylow's $3^{rd} \Rightarrow s_p \mid q \Rightarrow s_p = 1$ or q

and $s_p \equiv 1 \mod p$

i.e. p divides $s_p - 1 \Rightarrow \boxed{s_p = 1}$ since $p \nmid q-1$

Hence there are unique Sylow p-subgroups P and Sylow q-subgroups Q, with $P \triangleleft G$, $Q \triangleleft G$

- One way to finish the proof argues $P \times Q \to PQ = G$, $(h, k) \mapsto hk$ is an isomorphism from this.
- Another way uses Sylow's 2^{nd} to say every element of order p must lie in P, of order q must lie in Q, and since $|G| = pq > p+q-1 = |P \cup Q|$, there must be elements of order pq. ∎