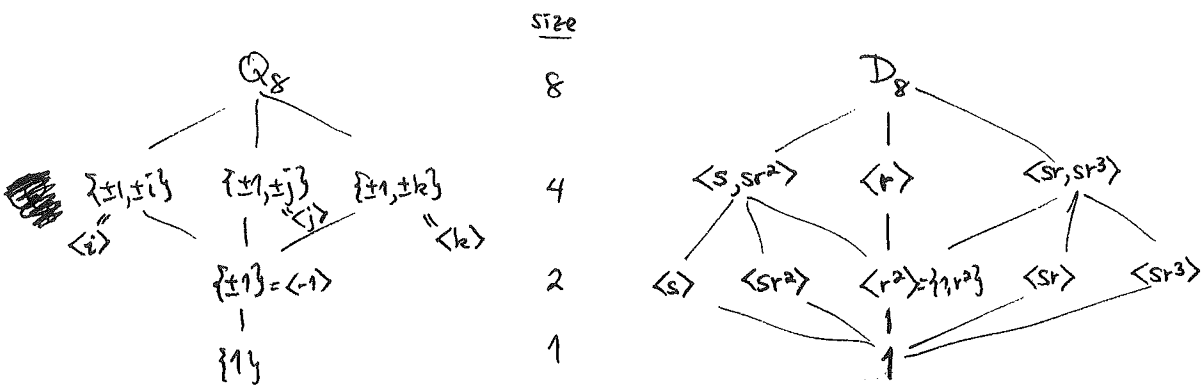
Infact, how do we even know $Q_8 \not\cong D_8$!?

They have the same class equation $\quad 8 = 1 + 1 + 2 + 2 + 2$

For D_8: $\quad \{1\} \quad \{r^2\} \quad \{r, r^3\} \quad \{s, sr^2\} \quad \{sr, sr^3\}$

For Q_8: $\quad \underbrace{\{1\} \quad \{-1\}}_{Z(Q_8) = \{\pm 1\}} \quad \{\pm i\} \quad \{\pm j\} \quad \{\pm k\}$

However, they have different numbers of subgroups of various sizes:



10/29/2018

§7.7 The Sylow theorems (1872)

These answer several questions about subgroups of G based on $|G|$.

Sylow's 1st Theorem: If $|G| = p^e m$ where $p \nmid m$ ("does not divide"), then G contains at least one subgroup P having $|P| = p^e$; these are called Sylow p-subgroups $P < G$.

Sylow's 2nd Theorem: For any finite group G,

(a) any two Sylow p-subgroups $P, P' < G$ are conjugate, i.e. $\exists g \in G$ with $P' = gPg^{-1}$, and

(b) every p-subgroup $H < G$ is contained in some Sylow p-subgroup P i.e. $H < P < G$.

Sylow's 3rd Theorem: If $|G| = p^e m$ where $p \nmid m$ as above, then the number of Sylow p-subgroups $P < G$ (call it s_p) satisfies

(a) $s_p \mid m$ ("divides")

and (b) $s_p \equiv 1 \bmod p$

EXAMPLE: $G = S_4$ has $|G| = 4! = 24 = 2^3 \cdot 3^1$

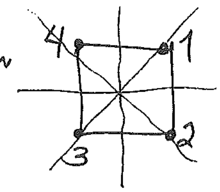
so the only relevant primes are $p=2$ and $p=3$

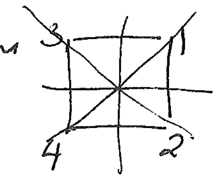
$\boxed{p=2:}$ Its Sylow 2-subgroups have $|P| = 2^3 = 8$ (and $m=3$ here)

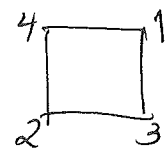
and are the subgroups isomorphic to D_4 that we have encountered earlier:

They exist! (Sylow's 1st)

$$\begin{cases} P_1 = \{1, (12)(34), (13)(24), (14)(23), (1234), (1432), (13), (24)\} \\ P_2 = \{ \text{———} \;''\; \text{———}, (1243), (1342), (14), (23)\} \\ P_3 = \{ \text{———} \;''\; \text{———}, (1324), (1423), (12), (34)\} \end{cases}$$







Note $\left.\begin{array}{l} P_2 = (34)P_1(34)^{-1} \\ P_3 = (23)P_1(23)^{-1} \end{array}\right\}$ Sylow's 2nd (a)

Note every 2-subgroup lies in some P_i, e.g. $\langle (12) \rangle < P_3$

(Sylow's 2nd (b))

$\langle (1234) \rangle < P_1$

$\langle (12)(34) \rangle < P_1, P_2, P_3$

$V_4 = \{e, (12)(34), (13)(24), (14)(23)\} < P_1, P_2, P_3$

Note $\left.\begin{array}{l} s_2 = \#\text{ Sylow 2-subgroups} = 3 \text{ divides } m=3 \\ \text{and } s_2 = 3 \equiv 1 \bmod 2 \end{array}\right\}$ Sylow's 3rd

$\boxed{p=3:}$ Its Sylow 3-subgroups have $|P| = 3^1$ (and $m=8$ here),

so they are $\left.\begin{array}{l} P_1 = \langle (123) \rangle \ (= \langle (132) \rangle) \\ P_2 = \langle (124) \rangle \\ P_3 = \langle (134) \rangle \\ P_4 = \langle (234) \rangle \end{array}\right\}$ They exist! (Sylow's 1st)

$P_2 = (34)P_1(34)^{-1}$, etc (Sylow's 2nd (a)) [Sylow's 2nd (b) says little here]

$s_3 = \#$ Sylow 3-subgroups $= 4$ divides $m=8$

and $s_3 = 4 \equiv 1 \bmod 3$.

Before proving the Sylow Theorems, let's deduce some more consequences.

Cauchy's Theorem: If a prime p divides $|G|$ then $\exists$ a subgroup $H < G$ with $|H| = p$.

In fact, something much stronger holds:

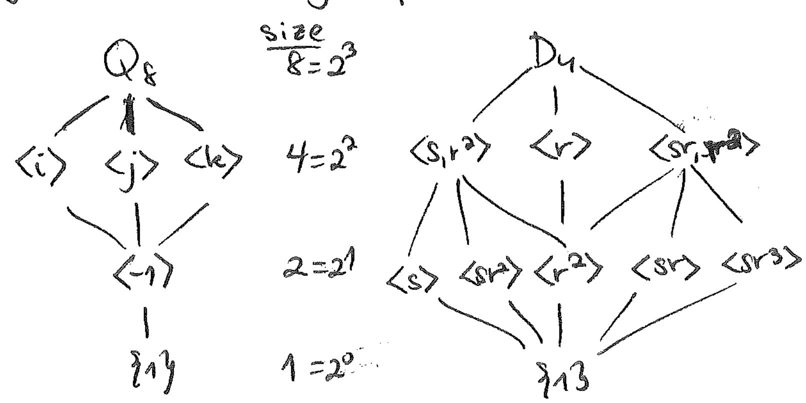
"Better-than-Cauchy's Theorem": If p^k divides $|G|$ then $\exists$ a subgroup $H < G$ with $|H| = p^k$.

Note that this would follow immediately from Sylow's 1st Theorem if we can prove this result:

PROPOSITION: A p-group P, say of cardinality $|P| = p^e$, contains subgroups H with every possible cardinality $|H| = p^k$ with $1 \leq k \leq e$.

---

e.g. we saw the 2-groups D_4 and Q_8 have this property:



This proposition is easy to prove if we go back and prove part of Noether's 3rd Isomorphism Thm, what Artin called the Correspondence Theorem in §2.10 ...

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

one obtains a bijection

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

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

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

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

proof: Try it yourself! ∎

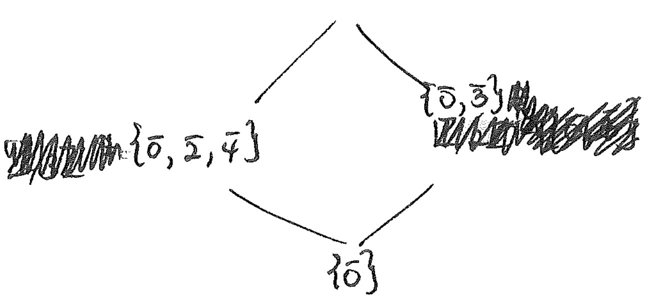
10/31/2018

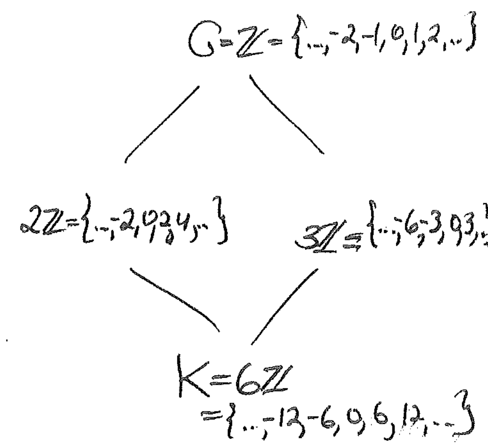
EXAMPLE: $G = \mathbb{Z}$

$\triangledown$

$K = 6\mathbb{Z}$

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





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 $1 \leq k \leq e$ ∎