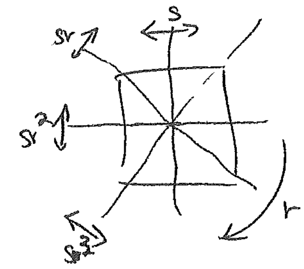
(93)

EXAMPLE: $D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$



has $Z(G) = \{e, r^2\}$

and conjugacy classes
$\{e\}$
$\{r, \underset{r^{-1}}{\overset{\shortparallel}{r^3}}\}$ since $srs^{-1} = srs = r^3 = r^{-1}$
$\{r^2\}$
$\{s, sr^2\}$ since $rsr^{-1} = sr^3r^{-1} = sr^2$
$\{sr, sr^3\}$

and class equation $\underset{|D_4|}{\overset{\shortparallel}{8}} = \underbrace{\underset{\{e\}}{1}} + 2 + \underbrace{\underset{\{r^2\}}{1}} + 2 + 2$

$Z(D_4)$

§7.3 p-Groups

The class equation has an interesting consequence for **p-groups** G, defined to be groups G with $|G| = p^k$ a prime power, $k \geq 1$.

10/26/2018 >

PROPOSITION: A p-group G always has center $Z(G) \overset{?}{\neq} \{1\}$,
(PROP 7.3.1) i.e. a nontrivial subgroup

proof: Assume for the sake of contradiction that G has $|G| = p^k$ and trivial center $Z(G) = \{1\}$. Then its class equation looks like

$$p^k = |G| = \sum_{\substack{\text{Conjugacy}\\ \text{class } C(h)}} |C(h)| = 1 + \sum_{\substack{\text{Conj.}\\ \text{classes } C(h) \neq \{1\}}} |C(h)|$$

p^k: equals 0 mod p (since $k \geq 1$)

1: equals 1 mod p

$|C(h)|$: equals 0 mod p since $|C(h)| = \frac{|G|}{|Z(h)|} = \frac{p^k}{p^{k'}} = p^{k-k'}$, $k' \neq k$ since $1 \neq$, $h \notin Z(G)$

$\underbrace{1 + \sum |C(h)|}_{\text{equals 1 mod } p}$

CONTRADICTION

■

EXAMPLE: D_4 is a 2-group since $|D_4| = 8 = 2^3$,

and it has nontrivial center $Z(D_4) = \{1, r^2\} \supsetneqq \{1\}$.

This has an interesting corollary. Recall $|G| = p \Rightarrow G \cong (\mathbb{Z}/p\mathbb{Z})^+$.
p prime, $\|$ is cyclic $\{e, g, g^2, \ldots, g^{p-1}\}$

COROLLARY: (PROP 7.3.3) A group G with $|G| = p^2$ for p prime is always abelian, and in fact

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

or $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

(but false for $|G| = p^3$, e.g. $|D_4| = 2^3$ and D_4 is not abelian!)

proof: Assume $|G| = p^2$.

CASE 1: $G = \langle g \rangle$ is cyclic
$= \{e, g, g^2, \ldots, g^{p^2-1}\}$

and then we're done.

CASE 2: G is not cyclic.

Since G is a p-group, we know $Z(G) \supsetneqq \{1\}$,

so pick $h \in Z(G) - \{1\}$, and let $H := \langle h \rangle$.

$|H|$ divides $|G| = p^2$, so $|H| = \cancel{1}, p$ or $\cancel{p^2}$

impossible since $h \neq 1$ — impossible since G not cyclic $\Rightarrow G \neq H$

Thus $|H| = p$, so we can find some $k \in G - H$

and let $K := \langle k \rangle$. Again we claim $|K| = p$ for same reason.

But now we know that H, K commute since $h \in H < Z(G)$ implies $hk = kh$.

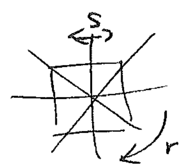
Hence $H \times K \xrightarrow{\mu} G$, $(h^i, k^j) \longmapsto h^i k^j$ is a homomorphism with image HK, which properly contains H, so $HK = G$. $|H \times K| = p^2 = |G|$ then forces μ to be an isomorphism ∎

<u>EXAMPLE</u>: Who are <u>all</u> of groups G with $|G| = 8 = 2^3$, up to isomorphism?

We have encountered most of them already ....

abelian
$$\begin{cases} (\mathbb{Z}/8\mathbb{Z})^+ \\ (\mathbb{Z}/4\mathbb{Z})^+ \times (\mathbb{Z}/2\mathbb{Z})^+ \\ (\mathbb{Z}/2\mathbb{Z})^+ \times (\mathbb{Z}/2\mathbb{Z})^+ \times (\mathbb{Z}/2\mathbb{Z})^+ \end{cases}$$

non-abelian

D_4 = symmetries of square  $sr = r^{-1}s$

Q_8 = <u>quaternion</u> <u>group</u> (NEW?)
$= \{\pm 1, \pm i, \pm j, \pm k\}$ with $i^2 = j^2 = k^2 = -1$

$ij = k = -ji \qquad jk = i = -kj \qquad ki = j = -ik$

(see §2.4 p.47 of Artin)

(<u>Q</u>: Who is i^{-1}, j^{-1}, k^{-1}?)

- Q_8 can be thought of as a subgroup of $GL_2(\mathbb{R})$ via an injective homomorphism $Q_8 \to GL_2(\mathbb{C})$

$$\pm 1 \mapsto \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$\pm i \mapsto \pm \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$
$$\pm j \mapsto \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$
$$\pm k \mapsto \pm \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

- Q_8 can also be thought of as the group of units $(\mathbb{H}_\mathbb{Z})^\times$

where $\mathbb{H}_\mathbb{Z} = \{a+bi+cj+dk : a,b,c,d \in \mathbb{Z}\}$ $\subset$ $\mathbb{H}$:= Hamilton's <u>quaternions</u>
$= \{a+bi+cj+dk : a,b,c,d \in \mathbb{R}\}$

$i^2 = j^2 = k^2 = -1$
$ij = k = -ji$
$jk = i = -kj$
$ki = j = -ik$

(an <u>associative</u> but <u>non-commutative</u> ring!)

$\cup$

$\mathbb{C} = \{a+bi : a,b \in \mathbb{R}\}$

$\cup$

$\mathbb{R} = \{a : a \in \mathbb{R}\}$

- It takes a bit of work to show there are no other groups G up to isomorphism with $|G| = 8$.

(96)

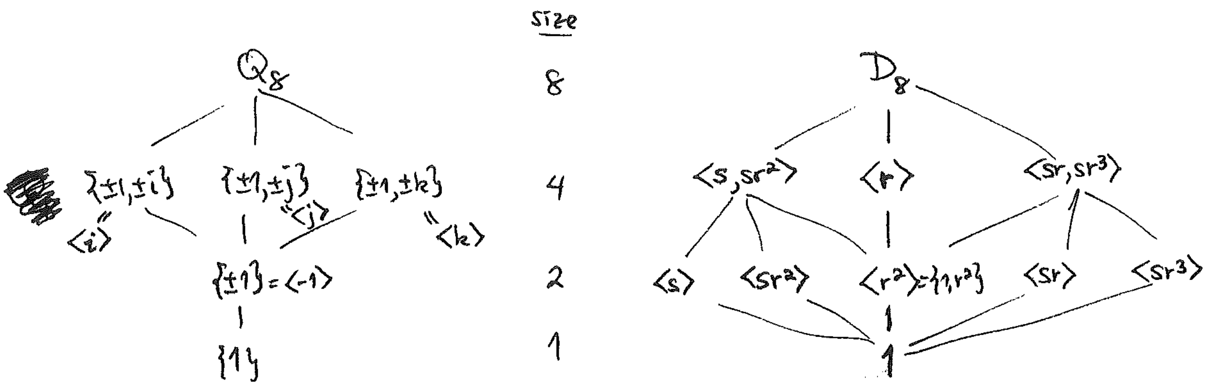
Infact, how do we even know $Q_8 \not\cong D_8$!?

They have the <u>same class equation</u> $8 = 1 + 1 + 2 + 2 + 2$

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

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

However, they have <u>different numbers of subgroups of various sizes</u>:



10/31/2018

§7.7 The Sylow theorems (1872)

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

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

<u>Sylow's 2nd Theorem</u>: 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. $H < P < G$.

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

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

and (b) $s \equiv 1 \mod p$