Last time G = finite group. Then

$$G = Z(G) \sqcup G\cdot x_1 \sqcup \cdots \sqcup G\cdot x_k$$

where $G\cdot x_i$, $i=1,\dots,k$ are disjoint conjugacy classes.

(here $\cdot$ is the conjugation action $G\times G\to G$, $g\cdot x = gxg^{-1}$)

$$\Rightarrow \quad |G| = |Z(G)| + \sum_{i=1}^{k} |G\cdot x_i| = |Z(G)| + \sum_{i=1}^{k} \frac{|G|}{|\mathrm{Cent}(x_i)|}$$

Prop 5.4.2 If $|G| = p^n$ for some prime p then $p \mid |Z(G)|$

In particular, $|Z(G)| > 1$.

We haven't finished proving:

Cor 5.4.3 If $|G| = p^2$ and p is prime, then either G is isomorphic to $\mathbb{Z}_{p^2}$ or to $\mathbb{Z}_p \times \mathbb{Z}_p$.

Proof We showed:

"if $\exists\, g \in G$ s.t. $|\langle g\rangle| = p^2$ then $G \cong \mathbb{Z}_{p^2}$" (isomorphic to)

Now suppose $\nexists\, g \in G$ with $|\langle g\rangle| \neq p^2$.

Then $\forall\, g \in G \smallsetminus \{e\}$, $|\langle g\rangle| = p$.

By 5.4.2, $|Z(G)| > 1$. So $\exists\, a \neq Z(G)$ with $a \neq e$.

Then $|\langle a\rangle| = p$ (it can't be 1 since $a \neq e$ and it can't be p^2).

Since $|G| = p^2 > p = |\langle a\rangle|$, $G \smallsetminus \langle a\rangle \neq \emptyset$.

Choose any $b \in G \smallsetminus \langle a\rangle$. Then $|\langle b\rangle| = p$.

Since $a \in Z(G)$, $bab^{-1} = a$, $\Rightarrow ab = ba$.

$\Rightarrow \forall\, k, \ell \in \mathbb{N}$ $\quad a^k b^\ell = b^\ell a^k$.

Claim 1 $f : \langle a\rangle \times \langle b\rangle \to G$, $f(a^k, b^\ell) = a^k b^\ell$ is a homomorphism.

Check $f((a^k, b^\ell)\cdot(a^r, b^s)) = f(a^{k+r}, b^{\ell+s}) =$

$= a^{k+r} b^{\ell+s} = a^k a^r b^\ell b^s = a^k b^\ell a^r b^s = f(a^k, b^\ell)\cdot f(a^r, b^s)$.

Claim 2 f is 1–1 (hence, since $|\langle a\rangle \times \langle b\rangle| = |\langle a\rangle|\,|\langle b\rangle| = p^2 = |G|$, f is onto hence an isomorphism).

Check $f(a^k, b^\ell) = f(a^r, b^s) \Leftrightarrow a^k b^\ell = a^r b^s$

$\Rightarrow a^{-r} a^k = b^s b^{-\ell} \in \langle a\rangle \cap \langle b\rangle$.

TOPS FORM
Litho in U.S.A.

$\langle a\rangle \cap \langle b\rangle$ is a subgroup of $\langle a\rangle$. $\Rightarrow |\langle a\rangle \cap \langle b\rangle| \mid |\langle a\rangle| = p$

$\Rightarrow |\langle a\rangle \cap \langle b\rangle| = 1$ or p. If $|\langle a\rangle \cap \langle b\rangle| = p$, $\langle a\rangle \cap \langle b\rangle = \langle a\rangle$.

$\Rightarrow b \in \langle a\rangle$. But $b \in G \setminus \langle a\rangle$. Contradiction.

Therefore $\langle a\rangle \cap \langle b\rangle = \{e\}$.

$\Rightarrow a^{k-r} = b^{s-\ell} = e$. $\Rightarrow a^k = a^r$, $b^s = b^r$

$\Rightarrow f$ is 1-1

$\Rightarrow f$ is an isomorphism.

Since $\langle a\rangle \cong \mathbb{Z}_p$, $\langle b\rangle \cong \mathbb{Z}_p$

$G \cong \langle a\rangle \times \langle b\rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$. ▷

Theorem 5.4.6 (Cauchy) Suppose G is a finite group, p is prime and $p \mid |G|$. Then G has an element of order p.

Ex $|S_7| = 7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$

$\Rightarrow S_7$ has elements of order 7, 5, 3, 2.

Proof of Cauchy's Theorem We want to show: $\exists\, a \in G$ s.t. $a \neq e$ and $a^p = e$.

Consider $X = \{(a_1, a_2, \ldots a_p) \in G^p \mid a_1 \cdot a_2 \cdot \cdots \cdot a_p = e\}$

We want to show: $\exists\, (a_1, \ldots a_p) \in X$ w.th $a_1 = a_2 = \cdots = a_p$ and $a_i \neq e$.

Note $\forall\, a, b \in G$ $ab = e \Rightarrow a = b^{-1} \Rightarrow ba = e$.

Hence $(a_1, \ldots a_p) \in X \Rightarrow (a_1 \cdots a_{p-1}) \cdot a_p = e \Rightarrow a_p \cdot (a_1 \cdots a_{p-1}) = e$

$\Rightarrow (a_p, a_1, \ldots, a_{p-1}) \in X$.

Clearly $f: X \to X$, $f(a_1 \ldots a_p) = (a_p, a_1 \ldots a_{p-1})$

is a bijection and $\underbrace{f \circ \cdots \circ f}_{p \text{ times}} = id \Rightarrow \langle f\rangle \leq Sym(X)$ is a subgroup of order p.

We have a well-defined homomorphism

$$\mathbb{Z}_p \longrightarrow Sym(X), \quad [k] \longmapsto f^k = \overbrace{f \circ \cdots \circ f}^{k},$$

hence an action of $\mathbb{Z}_p$ on X.

Explicitly $[1]\cdot(a_1 \cdots a_p) = (a_p, a_1, \cdots a_{p-1})$

$[2]\cdot(a_1 \cdots a_p) = (a_{p-1}, a_p, a_1 \cdots a_{p-2})$ etc.

Claim $\exists\, x \in X$, $x \neq (e, \cdots, e)$ s.t.

$[k]\cdot x = x$ for all $[k] \in \mathbb{Z}_p$.

Proof of claim

Note first: $(a_1 \cdots a_p) \in X \Leftrightarrow a_p = (a_1 \cdots a_{p-1})^{-1}$.

Hence the map $G^{p-1} \to X$, $(a_1, \cdots, a_{p-1}) \mapsto (a_1, \cdots, a_{p-1}, (a_1 \cdots a_{p-1})^{-1})$ a a bijection. $\Rightarrow |X| = |G^{p-1}| = |G|^{p-1}$.

Next recall that $\forall x \in X$ $|\mathbb{Z}_p \cdot x \,||\, |\mathbb{Z}_p| = p$

$\Rightarrow |\mathbb{Z}_p \cdot x| = 1$ or p.

Let n = # of orbits of $\mathbb{Z}_p$ with 1 element

k = # of orbits of $\mathbb{Z}_p$ with p elements.

Then $|G|^{p-1} = |X| = n \cdot 1 + p \cdot k$

Since $p \,||\, |G|$, $p \,||\, |G|^{p-1} = |X|$.

$\Rightarrow p \,||\, (|X| - p \cdot k) = n$

$\Rightarrow n > 1$

$\Rightarrow \exists\, (a_1, \cdots a_p) \in X$ s.t. $(a_1, \cdots a_p) \neq (e, \cdots e)$

and $(a_p, a_1, \cdots a_{p-1}) = (a_1, a_2, \cdots a_p)$

$\Rightarrow a_1 = a_2,\ a_2 = a_3, \cdots, a_{p-1} = a_p,\ a_p = a_1$

$\Rightarrow \exists\, a \in G$ s.t. $a \neq e$ and $\underbrace{a \cdots a}_{p} = e$. $\square$

Semi-direct products.

Recall If A, B are two groups then we can turn $A \times B$ into a group with the multiplication given by

$$(a_1, b_1)\cdot(a_2, b_2) = (a_1 a_2, b_1 b_2)$$

Then $A' = A \times \{e_B\} \leq A \times B$ is isomorphic to A

$B' = \{e_A\} \times B \leq A \times B$ is isomorphic to B

A', B' are normal in $A \times B$ and $(A \times B)/A' \cong B$
$(A \times B)/B' \cong A$.

(Big idea) Given a homomorphism $\varphi: A \to \mathrm{Aut}(B)$ we can turn $A \times B$ into a group with a more "interesting" multiplication (that depends on φ).

This group is often denoted by $A \ltimes B$ or $A \ltimes_\varphi B$.

$A' = A \times \{e_B\}$, $B' = \{e_A\} \times B$ are subgroups of $A \ltimes B$

B' is normal, A' usually not.

$A \ltimes B$ is called the semi-direct product of A and B.

We'll see: the dihedral group D_n and the Euclidean group $\mathrm{Euc}(n)$ are (isomorphic to) semi-direct products.

Note A homomorphism $\varphi: A \to \mathrm{Aut}(B)$ defines an action of A on B, $(a, b) \mapsto a * b$ with the extra property:

$$a * (b_1 \cdot b_2) = (a * b_1) \cdot (a * b_2)$$

This is because $a * b = (\varphi(a))(b)$

and $\varphi(a)(b_1 b_2) = (\varphi(a)(b_1)) \cdot (\varphi(a)(b_2))$. $\forall\, a \in A,\ b_1, b_2 \in B$

Ex $A = \{\pm 1\}$ acts on $\mathbb{Z}_n$ by isomorphisms

$$1 * [k] = [k] \quad \forall\, [k] \in \mathbb{Z}_n$$
$$(-1) * [k] = [-k] \quad \forall\, [k] \in \mathbb{Z}_n$$

Note $\{\pm 1\} \cong \mathbb{Z}_2$

$$1 \longleftrightarrow [0]$$
$$-1 \longleftrightarrow [1]$$

We'll see

$$\{\pm 1\} \ltimes \mathbb{Z}_n \cong \mathbb{Z}_2 \ltimes \mathbb{Z}_n \cong D_n.$$