Last time: • the class equation:

$$|G| = |Z(G)| + \sum_{i=1}^{n} \frac{|G|}{|\mathrm{Cent}(a_i)|}$$

- If $|G| = p^k$, p prime, $k \geq 1$, then $|Z(G)| > 1$ ∴
- If $|G| = p^2$ then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Theorem (Cauchy) Suppose G is a finite group, p is prime and $p \mid |G|$. Then $\exists a \in G$ s.t. $a \neq e$ and $a^p = e$.

Remarks If $\exists a \in G$ s.t. $a^p = e$ and $a \neq e$, then $|\langle a \rangle| = p$ and $p = |\langle a \rangle| \mid |G|$ by Lagrange's theorem. Cauchy's theorem proves a converse: if $p \mid |G|$ then $\exists a$ s.t. $|\langle a \rangle| = p$.

Proof of Cauchy's theorem

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

$X \neq \emptyset$ since $(e, \ldots e) \in X$

In fact $G^{p-1} \to X$, $(a_1, \ldots, a_{p-1}) \mapsto (a_1, \ldots, a_{p-1}, (a_1 \cdots a_{p-1})^{-1})$ is a bijection.

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

! Consequently $(a_1, \ldots a_p) \in X \Rightarrow a_p = (a_1 \cdots a_{p-1})^{-1} \Rightarrow (a_p, a_1, \ldots, a_{p-1}) \in X$

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

is a well-defined bijection ($f(a_1, \ldots a_p)$ is in X)

$\Rightarrow f \in \mathrm{Sym}(X)$

Note: $f \neq \mathrm{id}_X$ and $f^p := \underbrace{f \circ \cdots \circ f}_{p} = \mathrm{id}_X$.

$\Rightarrow f \in \mathrm{Sym}(X)$ has order p. ($|\langle f \rangle| = p$.) $\Rightarrow \langle f \rangle \cong \mathbb{Z}_p$.

$\Rightarrow \varphi: \mathbb{Z}_p \to \mathrm{Sym}(X)$, $\varphi([k]) = f^k$

is a well-defined injective homomorphism.

Recall A homomorphism $\varphi: G \to \mathrm{Sym}(X)$ "is" a left action of G on X:

$$g \cdot x := (\varphi(g))(x) \qquad \forall g \in G \ \forall x \in X$$

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

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

Consider $X^{\mathbb{Z}_p} := \{x \in X \mid \mathbb{Z}_p \cdot x = \{x\}\}$

Claim $|X^{\mathbb{Z}_p}| > 1$

Proof of claim Since p is prime and since $\forall H < \mathbb{Z}_p$, $|H| \mid |\mathbb{Z}_p| = p$

the only subgroups of $\mathbb{Z}_p$ are $\{[0]\}$ and $\mathbb{Z}_p$.

$\Rightarrow \forall x \in X \quad |\mathbb{Z}_p \cdot x| = |\mathbb{Z}_p / \text{Stab}(x)| = p$ or 1

(p if $\text{Stab}(x) = \{[0]\}$, 1 if $\text{Stab}(x) = \mathbb{Z}_p$)

Let $n = |X^{\mathbb{Z}_p}|$, number of fixed points,

let ℓ = # of orbits with p elements.

Then $|X| = n \cdot 1 + \ell \cdot p$.

On the other hand $|X| = |G^{p-1}| = |G|^{p-1}$.

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

$\Rightarrow p \mid (n + \ell p)$

$\Rightarrow p \mid n$.

$\Rightarrow n > 1$.

We know $(e, \dots e) \in X^{\mathbb{Z}_p}$ Since $|X^{\mathbb{Z}_p}| > 1$ $\exists (a_1, \dots a_p) \in X$

s.t $(a_1 \dots a_p) \neq (e, \dots e)$ and $(a_1, \dots, a_p) \in X^{\mathbb{Z}_p}$

$(a_1, \dots, a_p) \in X \Rightarrow a_1 \cdot \dots \cdot a_p = e$

$(a_1 \dots a_p) \in X^{\mathbb{Z}_p} \Rightarrow (a_1, \dots a_p) = (a_p, a_1, \dots a_{p-1})$

$\Rightarrow a_1 = a_p, a_2 = a_1, \dots \quad a_p = a_{p-1}$

$\therefore \Rightarrow a_1 = a_2 = \dots = a_p$.

$\therefore \exists a \in G$ s.t $a \neq e$ and $a^p = e$. D

Semi-direct products.

Ex Recall $D_n = \langle \rho, \tau \mid \rho^n = e = \tau^2 \quad \tau\rho = \rho^{-1}\tau \rangle$

$H = \langle \tau \rangle = \{e, \tau\}$, $N = \langle \rho \rangle = \{\rho^k \mid k \in \mathbb{Z}\} \lhd D_n$

and $\forall g \in D_n$ $\exists!$ $\rho^k \in \langle \rho \rangle$ ($=N$) $\tau^l \in \langle \tau \rangle$ ($=H$) s.t. $g = \rho^k \tau^l$.

ie $f: \langle \rho \rangle \times \langle \tau \rangle \longrightarrow D_n$ $f(\rho^k, \tau^l) = \rho^k \tau^l$ is a bijection. Note: f is not a homomorphism

---

Set up Suppose G is a group ($e.g.\ D_n$) $H, N < G$, $N \triangleleft G$ s.t. $f: N \times H \to G$, $f(n,h) = nh$ is a bijection.

Q Can we define a multiplication $*$ on $N \times H$ so that f is an isomorphism? We would need:

$$f((n_1,h_1) * (n_2,h_2)) = f(n_1,h_1)\, f(n_2,h_2)$$

Now $f(n_1,h_1) \cdot f(n_2,h_2) = n_1 h_1 n_2 h_2 = n_1 \underbrace{h_1 n_2 h_1^{-1}}_{\in N} h_1 h_2$

So define

$$(n_1,h_1) * (n_2,h_2) = (n_1 (h_1 n_2 h_1^{-1}),\ h_1 h_2)$$

One can check: $(N \times H, *, (e,e))$ is a group.

And then, by construction

$$f: (N \times H, *) \to G, \quad f(n,h) = nh$$

is an isomorphism.

The definition of $*$ on $N \times H$ used the fact that hnh^{-1} makes sense for $h \in H$, $n \in N$ (since $H, N < G$)

Theorem 18.1 Let H, N be two groups, $\mu: H \to \mathrm{Aut}(N)$ a homomorphism and $H \times N \to N$, $h \cdot n = \mu(h)(n)$ the corresponding action of H on N. Then

$$*: (N \times H) \times (N \times H) \to N \times H$$

$$(n_1,h_1) * (n_2,h_2) := (n_1 (h_1 \cdot n_2),\ h_1 h_2)$$

is an associative binary operation that makes $N \times H$ into a group. Moreover $H \cong \{e_N\} \times H$, $N \cong N \times \{e_H\}$ and $N \times \{e_H\} \triangleleft (N \times H, *)$.

Notation

The group $(N \times H, *)$ is usually denoted by $N \rtimes H$ (or by $N \rtimes_\mu H$ if we want to specify $\mu: H \to \mathrm{Aut}(N)$). It's called the semi-direct product of N and H.

Ex $H = \mathbb{R}^\times = \{a \in \mathbb{R} \mid a \neq 0\}$ $\quad N = (\mathbb{R}, +)$

$\mu: \mathbb{R}^\times \to \mathrm{Aut}(\mathbb{R})$ is $\mu(a)x := ax$

Since $a \cdot (x+y) = (a \cdot x) + (a \cdot y)$ $\mu(a)$ is in $\mathrm{Aut}(\mathbb{R})$.

And μ is a homomorphism since $\forall x \in \mathbb{R}$ $\forall a, b \in \mathbb{R}^\times$

$$\mu(ab)x = (ab)x = a(bx) = \mu(a)(\mu(b)x)$$

$$\Rightarrow \mu(ab) = \mu(a) \circ \mu(b).$$

Then by 18.1 $\mathbb{R} \rtimes \mathbb{R}^\times$ is a group:

$$(x, a) * (y, b) = (x + ay, ab)$$

Note

$$\mathbb{R} \rtimes \mathbb{R}^\times \xrightarrow{\cong} \left\{ \begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} \mid a \neq 0 \right\} \subset GL(2, \mathbb{R})$$

since $\begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ab & ay + x \\ 0 & 1 \end{pmatrix}$.

Ex A = abelian group. Then $\forall a, b \in A$

$$(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$$

$\Rightarrow$ $\mathrm{inv}: A \to A$ is a homomorphism and $\mathrm{inv} \circ \mathrm{inv} = \mathrm{id}$

$\Rightarrow$ $\mathrm{inv} \in \mathrm{Aut}(A)$ and $|\langle \mathrm{inv} \rangle| = 2$

$\Rightarrow$ We get a homomorphism $\mathbb{Z}_2 \to \mathrm{Aut}(A)$, $[k] \mapsto (\mathrm{inv})^k$

hence an action $\mathbb{Z}_2 \times A \to A$, $[0] \cdot a = a$ $\quad \forall a \in A$.

$[1] \cdot a = a^{-1}$

We get a group $A \rtimes \mathbb{Z}_2$

If $A = \mathbb{Z}_n$, we get $\mathbb{Z}_n \rtimes \mathbb{Z}_2 \cong D_n$.