Last time: · Cauchy's theorem: if G is a finite group, p a prime with $p \mid |G|$ then $\exists a \in G$, $a \neq e$ s.t. $a^p = e$

Thm 18.1 Let H, N be two groups, $\mu: H \to \mathrm{Aut}(N)$ a homomorphism and $H \times N \to N$, $h \circ n = (\mu(h))(n)$ the corresponding action. Then $*: (N \times H) \times (N \times H) \to N \times H$, $(n_1, h_1) * (n_2, h_2) = (n_1 (h_1 \circ n_2), h_1 h_2)$ is an associative binary operation that makes $N \times H$ into a group (denoted by $N \rtimes H$ or by $N \rtimes_\mu H$)
Moreover $N \times \{e\} \cong N$ and $N \times \{e\} \lhd (N \rtimes H)$.

Ex $H = GL(n, \mathbb{R})$, $N = \mathbb{R}^n$, H acts on $(\mathbb{R}^n, +)$ by $A \circ v = Av$

$$(v_1, A_1) * (v_2, A_2) = (v_1 + A_1 v_2, A_1 A_2)$$

We have an injective homomorphism

$$\mathbb{R}^n \rtimes GL(n, \mathbb{R}) \xrightarrow{\varphi} GL(n+1, \mathbb{R})$$

$$\varphi(v, A) = \left(\begin{array}{c|c} A & v \\ \hline 0 \cdots 0 & 1 \end{array}\right)$$

Check: $\varphi(v_1, A_1)\varphi(v_2, A_2) = \left(\begin{array}{c|c} A_1 & v_1 \\ \hline 0 \cdots 0 & 1 \end{array}\right)\left(\begin{array}{c|c} A_2 & v_2 \\ \hline 0 \cdots 0 & 1 \end{array}\right) = \left(\begin{array}{c|c} A_1 A_2 & A_1 v_2 + v_1 \\ \hline 0 \cdots 0 & 1 \end{array}\right)$

$\mathbb{R}^n \rtimes GL(n, \mathbb{R})$ (and $\varphi(\mathbb{R}^n \rtimes GL(n, \mathbb{R})) \subseteq GL(n+1, \mathbb{R})$) is called the group of affine transformations of $\mathbb{R}^n$.

Ex: $O(n) < GL(n, \mathbb{R})$, so $\mathbb{R}^n \rtimes O(n) < \mathbb{R}^n \rtimes GL(n, \mathbb{R})$

$$\mathbb{R}^n \rtimes O(n) =: \mathrm{Euc}(n)$$

The group of rigid motions (a.k.a isometries) of $\mathbb{R}^n$, the Euclidean group.

Proof of 18.1. Write (e, e) for (e_N, e_H).

Note $a \circ (n_1 n_2) = (a \circ n_1)(a \circ n_2)$ $\forall a \in H$ $\forall n_1, n_2 \in N$

Then $\forall (n, a) \in N \times H$

$$(e, e) * (n, a) = (e(e \circ n), ea) \overset{e \circ n = n \ \forall n}{=} (n, a)$$

$(n,a) * (e,e) = (n\,(a \bullet e),\, ae) \underset{\uparrow}{=} (ne, a) = (n, a)$

$a \cdot e = \mu(a)e = e$ since $\mu(a): N \to N$ is a homomorphism

(2) (associativity of $*$)

$((n_1,a_1) * (n_2,a_2)) * (n_3,a_3) = (n_1(a_1 \bullet n_2), a_1a_2) * (n_3, a_3) =$

$= (n_1\,(a_1 \bullet n_2)((a_1 a_2) \bullet n_3),\ (a_1 a_2) a_3)$ while

$(n_1, a_1) * ((n_2,a_2) * (n_3,a_3)) = (n_1, a_1) * (n_2\,(a_2 \bullet n_3),\ a_2 a_3)$

$= (n_1\,(a_1 \bullet (n_2 \cdot (a_2 \bullet n_3))),\ a_1(a_2a_3))$

$= (n_1 \cdot (a_1 \bullet n_2) \cdot (a_1 \bullet (a_2 \bullet n_3)),\ (a_1a_2)a_3)$

$= (n_1\,(a_1 \bullet (n_2 \cdot (a_2 \bullet n_3))),\ (a_1 a_2) a_3) = (n_1\,(a_1 \bullet n_2)((a_1 a_2) \bullet n_3),\ (a_1 a_2) a_3).$

(3) (inverses)

$(n,a) * (a^{-1} \bullet n^{-1}, a^{-1}) = (n\,(a \bullet (a^{-1} \bullet n^{-1})),\ aa^{-1}) = (n((aa^{-1}) \bullet n^{-1}),\ e)$

$= (n\,(e \bullet n^{-1}),\ e) = (nn^{-1}, e) = (e,e).$

Similarly

$(a^{-1} \bullet n^{-1}, a^{-1}) * (n,a) = ((a^{-1} \bullet n^{-1})(a^{-1} \bullet n),\ a^{-1}a) = (a^{-1} \bullet (n^{-1}n),\ e)$

$= (a^{-1} \bullet e, e) = (e,e)$ (since $b \bullet e = \mu(b)(e) = e \quad \forall b \in H.$)

Note: $\forall\, n_1, n_2 \in N \quad (n_1, e) * (n_2, e) = (n_1\,(e \bullet n_2),\ ee) = (n_1 n_2, e)$

Hence $\varphi: N \to N \rtimes H$, $\varphi(n) = (n, e)$, is an (injective) homomorphism

and $\varphi(N) = N \times \{e\}$.

Similarly $\forall\, a, b \in H \quad (e,a) * (e,b) = (e\,(a \bullet e), ab) = (ee, ab) = (e, ab)$

$\Rightarrow \quad H \cong \{e\} \times H < N \rtimes H.$

Finally, $(e,a) * (n,e) * (e,a)^{-1} = (e(a \cdot n), ae) * (a^{-1} \bullet e^{-1}, a^{-1})$

$= (a \cdot n, a) * (e, a^{-1}) = ((a \bullet n)\underbrace{(a \bullet e)}_{=e},\ aa^{-1}) = (a \bullet n, e)$

$\Rightarrow \quad N \times \{e\} \triangleleft (N \rtimes H)$ and conjugation by elements of $H \cong \{e\} \times H$ recovers the action of H on N $\square$

Sylow Theorems

Recall A group G acts on itself by conjugation: $g\cdot x := gxg^{-1}$.
Equivalently there is a homomorphism

$$c: G \to \mathrm{Aut}(G), \quad g \mapsto c_g, \quad c_g(x) := gxg^{-1}.$$

Note $c_g(xy) = g(xy)g^{-1} = gxg^{-1}gyg = c_g(x)c_g(y)$
So c is a homomorphism.

Note If $H < G$ and $\varphi: G \to G$ is an isomorphism, i.e., if $\varphi \in \mathrm{Aut}(G)$, then $\varphi(H)$ is a subgroup of G and $\varphi|_H : H \to \varphi(H)$ is an isomorphism.

Hence $\forall g \in G$ $\forall H < G$ $c_g(H)$ is a subgroup of G isomorphic to H. We write gHg^{-1} for $c_g(H)$.

Def Let G be a group. $H_1, H_2 < G$ are conjugate subgroups if $\exists g \in G$ s.t. $gH_1g^{-1} = H_2$.

Ex In S_n for any two r-cycles $\sigma, \tau \in S_n$ $\langle\sigma\rangle$ and $\langle\tau\rangle$ are conjugate since $\exists \mu \in S_n$ st $\tau = \mu\sigma\mu^{-1}$.
(recall: $\mu(i_1 \dots i_r)\mu^{-1} = (i_{\mu(1)}, \dots i_{\mu(r)})$)

Definition The normalizer of a subgroup H of a group G is
$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Note $N_G(H)$ is a subgroup of G
This can be either checked directly or we can observe that G acts on the set $\mathcal{P}(G)$ of subsets of G by

$$(\star)\quad g\cdot S = gSg^{-1} \quad (= c_g(S))$$

and $N_G(H) = \mathrm{Stab}(H)$ for the action $(\star)$.

<u>Definition</u> Let G be a finite group, p prime, $|G| = p^n m$
s.t $\gcd(p^n, m) = 1$ (p^n is the max power of p that divides $|G|$)
A subgroup $H < G$ is a <u>p-subgroup</u> if $|H| = p^k$ for some $k \leq n$
A subgroup $P < G$ is a p-Sylow subgroup if $|P| = p^n$
(i.e., P is a p-subgroup of maximal size)

<u>Theorem</u> (Sylow theorems #1, 2 and 3) Let G be a finite group, p prime, $p \mid |G|$.

1) if $p^k \mid |G|$ then there is a subgroup H of G with $|H| = p^k$
(In particular p-Sylow subgroups of G exist.

2) Let $H < G$ be a p-subgroup, $P < G$ p-Sylow subgroup.
Then $\exists a \in G$ s.t $aHa^{-1} \subseteq P$

In particular any two p-Sylow subgroups are conjugate

3) Let $n_p = \#$ of p-Sylow subgroups of G, $P < G$ p-Sylow subgroup.
Then (i) $n_p \mid |G/P|$
(ii) $n_p \equiv 1 \mod p$
(iii) $n_p = |G/N_G(P)|$ where as before
$N_G(P)$ = the normalizer of P in G.