Last time. Finished proving: if $|G| = p^2$, p prime, then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

- Cauchy's theorem: if a prime p divides $|G|$ then the group G has an element of order p.

Semi-direct products

Recall the correspondence

$\{$action of G on a set $X\} \longleftrightarrow \{$homomorphisms $G \to Sym(X)\}$

In particular given a homomorphism $\varphi : G \to Sym(X)$
G acts on X by $g \cdot x := \varphi(g)x$

Now suppose X is a group and $\varphi : G \to Aut(X)$ a homomorphism. Then G acts on X by homomorphisms

$$g \cdot x = \varphi(g)x$$

And $g \cdot (x_1 \cdot x_2) = \varphi(g)(x_1 x_2) = (\varphi(g)x_1) \cdot (\varphi(g)x_2) = (g \cdot x_1)(g \cdot x_2)$

Ex $G = \{\pm 1\}$, $X = \{e^{2\pi k i/n} \mid 0 \leq k \leq n\} = \langle e^{2\pi i/n} \rangle$
G acts on X: $(-1) \cdot e^{2\pi k i/n} = -e^{2\pi k i/n}$

Ex $X = A_n = \ker(\text{sign} : S_n \to \{\pm 1\})$, a normal subgroup of S_n
$G = \langle (12) \rangle$.

$\forall \sigma \in S_n$, $(12) \cdot \sigma = (12)\,\sigma\,(12)$

$(12) \cdot (\sigma_1 \sigma_2) = (12)\,\sigma_1 (12)(12)\,\sigma_2\,(12) = ((12)\cdot\sigma_1)((12)\cdot\sigma_2)$.

This corresponds to $\varphi : \langle (12) \rangle \to Aut(A_n)$ $\varphi(12) = C_{(12)}$ ← conj by (12).

Ex $G = O(n)$ $X = \mathbb{R}^n$
$\forall A \in O(n)$, $\forall v_1, v_2 \in \mathbb{R}^n$

$$A(v_1 + v_2) = Av_1 + Av_2.$$

This corresponds to $\varphi : O(n) \to Aut(\mathbb{R}^n_+)$

Theorem 23.1 (compare with 3.2.3 in Goodman)

Let A be a group acting on a group N by homomorphisms:

$$a * (\underbrace{n_1 n_2}_{\text{mult in } N}) = \underbrace{(a*n_1)(a*n_2)}_{\text{mult. in } N} \quad \forall a \in A,\ n_1, n_2 \in N.$$

Then

1) $G = N \times A$ with the multiplication defined by

(★) $(n_1, a_1)(n_2, a_2) = (n_1(a_1 * n_2), a_1 a_2)$

for all $n_1, n_2 \in N$, $a_1, a_2 \in A$ is a group

(2) $N' = N \times \{e_A\}$ is a normal subgroup of G

(3) $A' = \{e_N\} \times A$ acts on N' by conjugation and

$(e_N, a)(n, e_A)\cdot(e_N, a)^{-1} = (a*n, e_A)$. In particular $N' \trianglelefteq G$.

Notation: $G = N \rtimes A$

Proof We abbreviate both $e_N \in N$ and $e_A \in A$ as e.

i) $\forall (n,a) \in N \times A$. Note: $e_A * n = n \ \forall n \in N$, $a * e_N = e_N \ \forall a \in A$.

$(e,e)(n,a) = (e(e*n), ea) = (en, ea) = (n,a)$.

and $(n,a)(e,e) = (n(a*e), ae) = (ne, a) = (n,a)$

$\Rightarrow (e,e) \in N \times A$ is the identity element.

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

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

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

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

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

$\therefore$ the multiplication in $G = N \rtimes A$ is associative.

(iii) [inverses] $(n,a)(a^{-1} * n^{-1}, a^{-1}) = (n \cdot (a * (a^{-1} * n^{-1})), aa^{-1})$

$= (n \cdot ((aa^{-1}) * n^{-1}), e) = (n \cdot (e * n^{-1}), e) = (nn^{-1}, e) = (e,e)$.

Similarly

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

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

$\Rightarrow \quad G = N \rtimes A$ is a group

(iv) $N' = N \times \{e\} \cong N$ is normal in G:

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

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

<u>Corollary 3.2.5</u> Suppose G is a group, $N \trianglelefteq G$ a normal subgroup, $A < G$ a subgroup with $A \cap N = \{e\}$ and $G = NA$. Let $\varphi: A \to \mathrm{Aut}(N)$ be the homomorphism defined by

$$\varphi(a)\,(n) = ana^{-1}$$

Then $f: N \rtimes A \longrightarrow G$, $f(n,a) = na$ is an isomorphism.

—

<u>Ex</u> $G = D_n = \langle \rho, \tau \mid \rho^n = e,\ \tau^2 = e,\ \tau\rho = \rho^{-1}\tau \rangle$

$N = \langle \rho \rangle, \quad A = \langle \tau \rangle$

$\tau\rho\tau^{-1} = \rho^{-1}. \quad \Rightarrow \quad \tau\rho^k\tau^{-1} = \rho^{-k}.$

$D_n \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$ by Cor 3.2.5.

<u>Ex</u> $G = \mathrm{Euc}(\mathbb{R}^n) = \{ f: \mathbb{R}^n \to \mathbb{R}^n \mid f \text{ preserves distance} \}$.

<u>Recall:</u> $\forall f \in G$ there are unique $A \in O(n)$, $v \in \mathbb{R}^n$ s.t.

$f(w) = Aw + v \quad \forall w \in \mathbb{R}^n.$

$O(n) \leq \mathrm{Euc}(\mathbb{R}^n)$ is a subgroup

Every $v \in \mathbb{R}^n$ defines a <u>translation</u> $T_v: \mathbb{R}^n \to \mathbb{R}^n$

$$T_v(w) = v + w$$

The map $v \longmapsto T_v$, $\mathbb{R}^n \to \mathrm{Euc}(\mathbb{R}^n)$ is an injective group homomorphism. Proof:

$T_{v+v'}(w) = (v+v') + w = v + (v'+w) = T_v(T_{v'}(w))$

$= (T_v \circ T_{v'})(w)$

$T_v = \mathrm{id}_{\mathbb{R}^n} \iff v + w = w \quad \forall w \in \mathbb{R}^n$

$\iff v = 0.$

We have the bijection $\mathbb{R}^n \times O(n) \to Euc(\mathbb{R}^n)$

$$(v, A) \longmapsto T_v \circ A$$

Note $\forall w \in \mathbb{R}^n$ $(T_v \circ A)(w) = T_v(Aw) = Aw + v.$

Let $Trans(\mathbb{R}^n) = \{T_v \mid v \in \mathbb{R}^n\}$, the subgroup of translations

Claim $Trans(\mathbb{R}^n) \trianglelefteq Euc(\mathbb{R}^n)$

Proof $(A \circ T_v \circ A^{-1})(w) = A(A^{-1}w + v) = w + Av$

$$= T_{Av}(w).$$

$$\Rightarrow A \circ T_v \circ A^{-1} = T_{Av}.$$

Cor 3.2.5 $\Rightarrow$ $\mathbb{R}^n \rtimes O(n) \to Euc(\mathbb{R}^n)$

$$(v, A) \longmapsto T_v \circ A$$

is an isomorphism where $O(n)$ acts on $\mathbb{R}^n$ by

$$A \cdot v = Av$$

Ex $S_n \cong A_n \rtimes \mathbb{Z}_2.$

Reason Since $A_n = \ker(\text{sign})$, $A_n \trianglelefteq S_n$.

Since $\text{sign}(12) = -1$, $\langle(12)\rangle \cap A_n = \{e\}.$

Finally $S_n = A_n\langle(12)\rangle$ since $\forall \mu \in S_n$ with $\mu \notin A_n$,

$\text{sign}(\mu(12)) = \text{sign}(\mu)\,\text{sign}(12) = (-1)\cdot(-1) = 1.$ $\Rightarrow$ $\mu\cdot(12) \in A_n$.

$$\Rightarrow \quad \mu = \underbrace{(\mu(12))}_{\in A_n} \cdot \underbrace{(12)}_{\in \langle(12)\rangle}.$$

$$\Rightarrow \quad S_n = A_n \cdot \langle(12)\rangle.$$