Crash course in products of groups K and L

- **direct product** $K \times L = \{(k,l) \mid k \in K, l \in L\}$

  unit (e,e)

  inverse $(k,l)^{-1} = (k^{-1}, l^{-1})$

  product $(k_1,l_1)\cdot(k_2,l_2) = (k_1k_2, l_1l_2)$

Example: $\mathbb{Z} \times \mathbb{Z} = \{(a,b) \mid a,b \in \mathbb{Z}\}$ group w.r.t component-wise addition

- can one put any other group structures on the set $K \times L$?

Yes! **semidirect product** $K \rtimes L = \{(k,l) \mid k \in K, l \in L\}$

  unit (e,e)

  inverse $(k,l)^{-1} = (?, l^{-1})$

  product $(k_1,l_1)\cdot(k_2,l_2) = (?, l_1l_2)$

Above, ? and ? are heavily constrained by group axioms

The most general construction is to assume you are given

$$L \xrightarrow{\Phi} K \qquad \{\Phi_l : K \to K \text{ automorphism}\}_{\forall l \in L}$$

and set $? = \Phi_{l^{-1}}(k^{-1})$

$$? = \Phi_{l_1}(k_2)$$

Thus, for every action Φ $\exists$ a semi-direct product $K \rtimes L$

check associativity axiom:

$$\big((k_1,l_1)(k_2,l_2)\big)(k_3,l_3) = (k_1 \Phi_{l_1}(k_2), l_1 l_2)(k_3,l_3)$$
$$= (k_1 \Phi_{l_1}(k_2)\, \Phi_{l_1 l_2}(k_3), l_1 l_2 l_3)$$

$$(k_1,l_1)\big((k_2,l_2)(k_3,l_3)\big) = (k_1,l_1)(k_2 \Phi_{l_2}(k_3), l_2 l_3)$$
$$= (k_1 \Phi_{l_1}(k_2 \Phi_{l_2}(k_3)), l_1 l_2 l_3)$$

The equality of ____ and ____ uses both the fact that Φ is an action and that it is by automorphisms, i.e. $\Phi_\ell(xy) = \Phi_\ell(x)\,\Phi_\ell(y)$

Example: $\mathbb{Z}/2\mathbb{Z} \curvearrowright \mathbb{Z}/n\mathbb{Z}$ by automorphism $k \longmapsto -k$

Check (or ask on forum) that $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_{2n}$

Short exact sequences of groups
(suite exacte courte)

Def: given groups K, L, G, a s.e.s.

$$\underbrace{1}_{\text{trivial group}} \longrightarrow K \xrightarrow{f} G \xrightarrow{g} L \longrightarrow \underbrace{1}_{\text{trivial group}}$$

is the datum of two homomorphisms f, g as above

s.t. • f is injective

• g is surjective

• $\mathrm{Im}\, f = \ker g$ (which implies $g \circ f$ = trivial)

existence of a.s.e.s $\Longrightarrow$ $K \cong H \trianglelefteq G$

$\Longrightarrow$ $L \cong G/\ker g = G/H$

As a consequence, we call G an extension of L by K

(meaning: existence of a s.e.s. implies that G is bijective to $K \times L$ as sets; however extending this to a description of the group structure of G from that of K and L is tricky)

Ex: (let $m, n \in \mathbb{N}$) $1 \to \mathbb{Z}/m\mathbb{Z} \xrightarrow{f} \mathbb{Z}/mn\mathbb{Z} \xrightarrow{g} \mathbb{Z}/n\mathbb{Z} \to 1$

f = multiplication by n

g = remainder mod n

$\ker g = \{i \in \{0, \dots, mn-1\} \text{ s.t. } n \mid i\} = \{0, n, 2n, \dots, (m-1)n\} = \mathrm{Im}\, f$

Ex: (direct product) $\forall$ groups K, L, $\exists$ a s.e.s.

$$1 \to K \xrightarrow{f} K \times L \xrightarrow{g} L \to 1$$

$$k \rightsquigarrow (k, e)$$

$$(k, l) \rightsquigarrow l$$

$\ker g = \{(k,l) \mid l = e\} = \{(k,e) \mid k \in K\} = \mathrm{Im}\, f$

Ex: (semidirect product): $\forall$ groups K, L, $\forall$ $L \xrightarrow{\Phi} K$, $\exists$ s.e.s.

$$1 \longrightarrow K \xrightarrow{f} K \rtimes L \xrightarrow{g} L \longrightarrow 1$$

$$k \rightsquigarrow (k, e)$$
$$(k, l) \rightsquigarrow l$$

$$\operatorname{Ker} g = \{(k,l) \mid l = e\} = \{(k,e) \mid k \in K\} = \operatorname{Im} f$$

Why are f and g group homomorphisms?

$$(k,l)(k',l') = (k\,\Phi_e(k'), ll')$$

$$f(k)f(k') \quad (k,e)(k',e) = (k\,\Phi_e(k'), ee) = (kk', e) = f(kk')$$

$$g((k,l)(k',l')) = g((k\Phi_e(k'), ll')) = ll' = g((k,l))\,g((k',l'))$$

Def: Equivalences of s.e.s. (given K, L)

$$1 \longrightarrow K \xrightarrow{f} G \xrightarrow{g} L \longrightarrow 1$$

is said to be equivalent to

$$1 \longrightarrow K \xrightarrow{f'} G' \xrightarrow{g'} L \longrightarrow 1$$

if $\exists$ homomorphism $s: G \longrightarrow G'$ s.t. the following diagram commutes

$$\begin{array}{ccccccc} 1 & \longrightarrow & K & \xrightarrow{f} & G & \xrightarrow{g} & L \longrightarrow 1 \\ & & \downarrow \mathrm{Id}_K & \square & \downarrow s & \square & \downarrow \mathrm{Id}_L \\ 1 & \longrightarrow & K & \xrightarrow{f'} & G' & \xrightarrow{g'} & L \longrightarrow 1 \end{array}$$

$$1 \to K \xrightarrow{f'} G' \xrightarrow{g'} L \to 1$$

meaning of $\square$: composition $\begin{array}{c}\to\\ \downarrow\end{array}$ = composition $\begin{array}{c}\downarrow\\ \to\end{array}$, i.e. $s \circ f = f'$

meaning of $\square$: composition $\begin{array}{c}\to\\ \downarrow\end{array}$ = composition $\begin{array}{c}\downarrow\\ \to\end{array}$, i.e. $g = g' \circ s$

Why is the above an equivalence relation?

- $\to$ reflexive (obvious)
- $\to$ symmetric $\Leftarrow$ s is an isomorphism
- $\to$ transitive (easy, think about it)

Proof that s in

$$\begin{array}{ccccccccc} 1 & \to & K & \xrightarrow{f} & G & \xrightarrow{g} & L & \to & 1 \\ & & \downarrow Id_K & \square & \downarrow s & \square & \downarrow Id_L & & \\ 1 & \to & K & \xrightarrow{f'} & G' & \xrightarrow{g'} & L & \to & 1 \end{array}$$

is an isomorphism

- s inj: assume $x \in G$ s.t. $s(x) = e_{G'} \Rightarrow g(x) \overset{\square}{=} g' \circ s(x) = g'(e_{G'}) = e_L$

$\Rightarrow x \in \operatorname{Ker} g = \operatorname{Im} f \Rightarrow \exists\, k \in K$ s.t. $x = f(k)$

$\Rightarrow e_{G'} = s(x) = s \circ f(k) \overset{\square}{=} f'(k)$

$\Rightarrow k = e_K$ because f' inj $\Rightarrow x = f'(e_K) = e_{G'}$.

- s surj: take $x' \in G' \Rightarrow g'(x') \in L \Rightarrow \exists\, x \in G$ s.t. $g(x) = g'(x')$

but then $g'\left(x's(x)^{-1}\right) = g'(x')\, g'(s(x))^{-1}$

$= g'(x') \left(g' \circ s(x)\right)^{-1}$

$\overset{\square}{=} g'(x')\, g(x)^{-1} = e_{G'}$

$\Rightarrow x's(x)^{-1} \in \operatorname{Ker} g' = \operatorname{Im} f'$

$\Rightarrow \exists\, k \in K$ s.t. $x's(x)^{-1} = f'(k)$

$\Rightarrow x' = f'(k)\, s(x) \overset{\square}{=} s(f(k))\, s(x) = s(f(k)x) \in \operatorname{Im} s$

Big Question: when is a given s.e.s. $1 \to K \to G \to L \to 1$

equivalent to $1 \to K \xrightarrow{\text{inclusion}} K \times L \xrightarrow{\text{projection}} L \to 1$

or to $1 \to K \xrightarrow{\text{inclusion}} K \rtimes L \xrightarrow{\text{projection}} L \to 1$

for some action $L \overset{\Phi}{\curvearrowright} K$

Answer in the following theorems.

Thm 1: a given s.e.s. $1 \to K \xrightarrow{f} G \xrightarrow{g} L \to 1$ is equivalent to

$1 \longrightarrow K \longrightarrow K \times L \longrightarrow L \longrightarrow 1$

$\Longleftrightarrow$ f has a retraction, i.e. a homomorphism $K \xleftarrow{\phi} G$

such that $\phi \circ f = Id_K$

Thm 2: a given s.e.s. $1 \to K \xrightarrow{f} G \xrightarrow{g} L \to 1$ is equivalent to

$$1 \longrightarrow K \longrightarrow K \rtimes L \longrightarrow L \longrightarrow 1$$

for an arbitrary $L \xrightarrow{\Phi} K$

$\Longleftrightarrow$ g has a section, i.e. a homomorphism $G \xleftarrow{\psi} L$ such that $g \circ \psi = Id_L$

Proof of Thm 1: (Thm 2 done in Lecture Notes)

"only if":

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{f} & G & \longrightarrow & L & \longrightarrow & 1 \\ & & \| & & s \downarrow & & \| & & \\ 1 & \longrightarrow & K & \underset{\bar{f}}{\overset{\bar{\phi}}{\rightleftarrows}} & K \times L & \longrightarrow & L & \longrightarrow & 1 \end{array}$$

$k \mapsto (k, e)$

$k \in \ker(k,l) \mapsto l$

$\Longrightarrow$ f has a retraction

$\phi : G \to K$

$\phi := \bar{\phi} \circ s$

$\phi \circ f = \bar{\phi} \circ s \circ f = \bar{\phi} \circ \bar{f} = Id_K$.

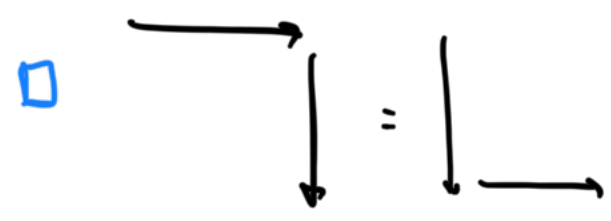
"if" given a retraction $K \underset{\phi}{\overset{f}{\rightleftarrows}} G$ $\Longrightarrow$

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{k} & G & \xrightarrow{g} & L & \longrightarrow & 1 \\ & & \| & \square & \vdots s & \square & \| & & \\ 1 & \longrightarrow & K & \xrightarrow{\bar{f}} & K \times L & \xrightarrow{\bar{g}} & L & \longrightarrow & 1 \end{array}$$

To construct s, define $\forall x \in G$ $s(x) = (\phi(x), g(x)) \in K \times L$; clearly s is homomorphism

$\square$ reads $s \circ f = \bar{f}$; to check this, note that $\forall k \in K$

$$s(f(k)) = (\phi(f(k)), g(f(k))) = (k, e) = \bar{f}(k)$$



reads $\bar{g} \circ s = g$; to check this, note that $\forall x \in G$

$$\bar{g}(s(x)) = \bar{g}((\phi(x), g(x))) = g(x)$$

The case of abelian groups

recall that G is called abelian $\iff$ $xy = yx$, $\forall x, y \in G$

when x is abelian we write "$x+y$" instead of xy

"$-x$" instead of x^{-1}

"0" instead of e_G

moreover, 0 will denote the trivial abelian group, even though it is the same thing as the trivial group 1

Lemma: if $L \overset{\Phi}{\curvearrowright} K$ and K, L are abelian,

then $K \rtimes L$ is abelian $\iff$ Φ = trivial action

$\iff$ $K \rtimes L = K \times L$

Proof:

$$\begin{array}{ccc} (k,l)(k',l') & = & (k',l')(k,l) \\ \| & & \| \\ (k\,\Phi_l(k'), ll') & & (k'\,\Phi_{l'}(k), ll') \end{array}$$

so $\forall k, k' \in K$, $\forall l, l' \in L$, we have $k\,\Phi_{l}(k') = k'\,\Phi_{l'}(k)$

choose $k' = e_K =$ "0", $l = e_L =$ "0"

$k\,\underbrace{\Phi_{e_L}(e_K)}_{e_K} = e_K\,\Phi_{l'}(k)$

$\Phi_{l'}(k) = k$, $\forall k \in K$, $\forall l' \in L$ $\Rightarrow$ Φ trivial

by the way, it suffices for G to be abelian as all subs and quotients of an abelian group (such as K and L) must also be abelian

Corollary: suppose $0 \to K \xrightarrow{f} G \xrightarrow{g} L \to 0$ is a s.e.s. of abelian groups

It is equivalent to $0 \to K \to K \times L \to L \to 0$ $\Leftrightarrow$ $\exists$ retraction $K \underset{\phi}{\overset{f}{\rightleftarrows}} G$

it is equivalent to $0 \to K \to K \times L \to L \to 0$ $\Leftrightarrow$ $\exists$ section $G \underset{\psi}{\overset{g}{\rightleftarrows}} L$

So, in the abelian world, $\exists$ retraction $\Leftrightarrow$ $\exists$ section

(and when this happens, we call $0 \to K \to G \to L \to 0$ split)

Exercise: show that $0 \to \mathbb{Z}/n\mathbb{Z} \xrightarrow{f} \mathbb{Z}/mn\mathbb{Z} \xrightarrow{g} \mathbb{Z}/n\mathbb{Z} \to 0$

Ex: show that $\mathbb{Z}/mn\mathbb{Z}$ $\mathbb{Z}/m\mathbb{Z}$ $\mathbb{Z}/n\mathbb{Z}$

ϕ ψ

$f(k) = nk$ $\quad$ $g(x) = x \bmod n$

is split if $\gcd(m,n) = 1$ (in which case $\exists a, b$ s.t. $am + bn = 1$)

Pick $\phi(x) = xb \bmod m$ and let's check they are retraction section

$\psi(L) = amL$

$\phi \circ f(k) = \phi(nk) = bnk \bmod m = k \bmod m$ because $bn = 1 - am$

$g \circ \psi(L) = g(aLm) = amL \bmod n = L \bmod n$ $\quad$ $am = 1 - bn$