§ 2 Co products and free grps

1. Review: products Let $I \neq \emptyset$ and let $(G_i)_{i \in I}$ be a family of groups. Put
$G = \prod_{i \in I} G_i$. The elements of G are thus infinite sequences $g = (g_i)_{i \in I}$, with $g_i \in G_i$, and G is a group, with product

$$gh = (g_i h_i)_{i \in I} \quad h_i, g_i \in G_i$$

For $j \in I$ define $pr_j(g) = g_j$, $pr_j : G \to G_j$

Then pr_j is a surjective group homomorphism.

The products has a universal property.

2. Theorem Let $I \neq \emptyset$, let $(G_i)_{i \in I}$ be a family of grps. Then there exist a group P, with homomorphisms $p_j : P \to G_j$ for all j, such that the following holds. If H is any group, with homomorphisms $f_j : H \to G_j$ for all j,

then there is a unique homomorphism $F : H \to P$ such that $f_j = p_j \circ f$ for all $j \in I$.

$$\begin{tikzcd} & P \arrow[d, "p_j"] \\ H \arrow[ur, "\exists ! F"] \arrow[r, "f_j"'] & G_j \end{tikzcd}$$

Pf Put $P = \prod_{j \in I} G_j$ and $p_j = pr_j$ and

$f(h) = (f_j(h))_{j \in J}$, then $p_j \circ f = f_j$. Moreover,

if $\tilde{f} : H \to P$ is a homomorphism with $p_j \circ \tilde{f} = f_j$,

$\tilde{f}(h) = (\tilde{f}_j(h))_{j \in J}$, then $\tilde{f}_j = f_j \Rightarrow \tilde{f} = f$. $\square$

<u>Addendum</u> The universal property characterizes the product <u>uniquely</u>: if P and $\tilde{P}$ both have the universal property, put $H = \tilde{P}$

$$\begin{tikzcd} & P \arrow[d, "p_j"] \\ \tilde{P} \arrow[ur, "\exists ! \varphi"] \arrow[r, "\tilde{p}_j"'] & G_j \end{tikzcd} \qquad \begin{tikzcd} & \tilde{P} \arrow[d, "\tilde{p}_j"] \\ P \arrow[ur, "\exists ! \psi"] \arrow[r, "p_j"'] & G_j \end{tikzcd}$$

$$\Rightarrow \quad \begin{tikzcd} & \tilde{P} \arrow[d, "\tilde{p}_j"] \\ \tilde{P} \arrow[ur, shift left, "\psi \circ \varphi"] \arrow[ur, shift right, "id_{\tilde{P}}"'] \arrow[r, "\tilde{p}_j"'] & G_j \end{tikzcd} \qquad \begin{tikzcd} & P \arrow[d, "p_j"] \\ P \arrow[ur, shift left, "\varphi \circ \psi"] \arrow[ur, shift right, "id"'] \arrow[r, "p_j"'] & G_j \end{tikzcd}$$

$\psi \circ \varphi = id$ $\qquad$ $\varphi \circ \psi = id$ $\square$

$\Rightarrow \tilde{p}_j = p_j \circ \varphi$

Now we "dualize" this (in the categorical sense).

3. <u>Def</u> Let $I \neq \emptyset$ and let $(G_i)_{i \in I}$ be a family of grps. A <u>coproduct</u> of this family is a grp C, with homomphisms

$\iota_j : G_j \to C$ for all $j \in I$, and the following

<u>universal property</u>: if H is any grp, with homomorphisms $f_j : G_j \to H$ for all j, then there is a unique homomphism $f : C \to H$ such that $f_j = f \circ \iota_j$ for all j,

$$\begin{tikzcd} H & G_j \arrow[l, "f_j"'] \arrow[d, "\iota_j"] \\ & C \arrow[ul, "\exists!\, f"] \end{tikzcd}$$

<u>If</u> the coproduct exists, then it is again unique up to isomorphism: if $\tilde{C}$ is another coproduct, with homomphism $\tilde{\iota}_j : G_j \to \tilde{C}$, consider again

$$\begin{tikzcd} \tilde{C} \arrow[dr, shift left, "\psi"] & G_j \arrow[l, "\tilde{\iota}_j"'] \arrow[d, "\iota_j"] \\ & C \arrow[ul, shift left, "\varphi"] \end{tikzcd}$$

$\rightsquigarrow$ as before $\varphi \circ \psi = id_{\tilde{C}}$

$\psi \circ \varphi = id_C$

$\tilde{\iota}_j = \varphi \circ \iota_j$

It remains to show the existence of coproducts.

What should C look like?

(a) it should contain a copy of each G_j:

$\left(\text{put } H = G_j, \quad f_j = id_{G_j}, \quad f_i(g) = e \text{ for } i \neq j \right)$

$$\begin{tikzcd} G_j & G_j \arrow[l, "f_j"'] \arrow[l, phantom, shift right=2, "="] \arrow[d, "\iota_j"] \\ & C \arrow[ul] \end{tikzcd}$$

(b) the subgroups $f_j(G_j) \subseteq H$ need not commute, so the copies of the G_j in C need not commute.

(so C is very different from $\prod_{i \in I} G_i$!)

Now we show the existence of coproducts by an explicit construction, the free product of groups.

4. <u>Free products</u> Let $I \neq \emptyset$ and let $(G_i)_{i \in I}$ be a family of groups. We assume that $G_i \cap G_j = \emptyset$ for $i \neq j$ for simplicity (we can make the groups disjoint by replacing G_i by $G_i \times \{i\}$). So for every $g \in V = \bigcup \{G_i \mid i \in I\}$ we know to which group G_i the element g belongs!

A <u>reduced word</u> is a tuple

identity in G_{j_k}

$w = (g_1, \dots, g_m)$ with $g_k \in G_{j_k} - \{e_{j_k}\}$

$m \geq 0$

such that consecutive elements ($\hat{=}$ letters) belong to <u>different groups</u>, $j_k \neq j_{k+1}$ $k = 1, \dots, m-1$

We allow the <u>empty word</u> $(\,)$ (no letters)

Let $\mathcal{W}$ denote the set of all reduced words.

We define a product $*$ on $\mathcal{W}$ recursively as follows:

(a) $(g_1, \dots, g_m) * (h_1, \dots, h_n)$

$= (g_1, \dots, g_m, h_1, \dots, h_n)$ if

g_m and h_1 belong to different groups

(b) $(g_1, \dots, g_m) * (h_1, \dots, h_n)$

$= (g_1, \dots, g_m h_1, h_2, \dots, h_n)$

if g_m, h_1 belong to the same group and if

$g_n \neq h_1^{-1}$

(c) $(g_1, \dots, g_m) * (h_1, \dots, h_n)$

$= (g_1, \dots, g_{m-1}) * (h_2, \dots, h_n)$ if

g_m, h_1 belong to the same group and if $g_m = h_1^{-1}$.

It is easy to see that the empty word $()$ is a neutral element and that $(g_m^{-1}, \dots, g_1^{-1})$ is an inverse of $(g_1, \dots, g_m)$. Associativity is "clear" but unpleasant to check. We take a different approach. #

Let $g \in G_j$. We define a map

$L_g : \mathcal{W} \to \mathcal{W}$ as follows.

- If g is the identity element, then $L_g = id_{\mathcal{W}}$

- If $g \neq e_j$, then we put

$$L_g(g_1, \ldots, g_m) = \begin{cases} (gg_1, g_2, \ldots, g_m) & \text{if } g_1 \in G_j \text{ and if } g_1 \neq g^{-1} \\ (g_2, \ldots, g_m) & \text{if } g_1 \in G_j \text{ and if } g_1 = g^{-1} \\ (g, g_1, g_2, \ldots, g_m) & \text{if } g_1 \notin G_j \end{cases}$$

For $h \in G_j$ we have then $L_g \circ L_h = L_{gh}$ (different cases to consider...), so we have an <u>action</u> $G_j \times \mathcal{W} \to \mathcal{W}$, for each j.

For $w \in \mathcal{W}$, $w = (g_1, \ldots, g_m)$ we define $L_w : \mathcal{W} \to \mathcal{W}$ via $L_w = L_{g_1} \circ L_{g_2} \circ \ldots \circ L_{g_m}$

It follows that $L_w \circ L_{\tilde{w}} = L_{w * \tilde{w}}$ for $w, \tilde{w} \in \mathcal{W}$. We note also that $L_w(\underset{\uparrow}{()}) = w$
empty word.

We <u>define</u> then ~~a group~~ $C \subseteq \mathrm{Sym}(\mathcal{W})$ as

$$C = \langle \{ L_w \mid w \in \mathcal{W} \} \rangle \subseteq \mathrm{Sym}(\mathcal{W})$$

Then G acts transitively on $\mathcal{W}$, because $L_w() = w$. Since $L_w \circ L_{\tilde{w}} = L_{w * \tilde{w}}$, we have $G' = \{ L_w \mid w \in \mathcal{W} \}$. The stabiliser of $()$ is $\{L_{()}\} = \{id_{\mathcal{W}}\}$, hence G acts <u>sharply transitively</u> on $\mathcal{W}$ and we have a <u>bijection</u> $G \to \mathcal{W}$, $L_w \mapsto L_w() = w$.

This bijection maps the product $\circ$ in G to the product $*$ in $\mathcal{W}$, hence $(\mathcal{W}, *)$ is a group and $L_w \to w$ is a group isomorphism.

We put

$$\coprod_{i \in I} G_i = \mathcal{W} \cong (G, \circ)$$

the <u>free product</u> of the groups G_i.

For each $i \in I$ we have a homomorphism

$$\iota_i : G_i \to \mathcal{W}, \qquad \iota_i(e_i) = ()$$
$$\iota_i(g) = (g) \text{ if } g \neq e_i$$

5. <u>Prop</u> The free product $\coprod_{i\in I} G_i$ is a (the) coproduct (in the category of groups).

<u>pf</u> Let $f_i : G_i \to H$ be homomorphisms, for $i \in I$.

We define $f : \coprod_{i\in I} G_i \to H$ via

$$f(g_1, \dots, g_m) = f_{i_1}(g_1) \cdots f_{i_m}(g_m) \quad , \quad g_k \in G_{i_k}$$

Then $f \circ \iota_j = f_j$

$$\begin{tikzcd} \coprod_{i\in I} G_i \arrow[dr, "f"] & \\ G_j \arrow[u, "\iota_j"] \arrow[r, "f_j"'] & H \end{tikzcd}$$

If $\tilde{f} : \coprod_{i\in I} G_i \to H$ also has this property, then

$\tilde{f}(g) = f_j(g)$ for all $g \in G_j$, hence $\tilde{f} = f$ $\square$

<u>Convention</u>. One also writes $\ast_{i\in I} G_i = \coprod_{i\in I} G_i$

and if $I = \{1, \dots, m\}$ is finite

$$\coprod_{i\in I} G_i = G_1 * G_2 * \dots * G_2$$

The reduced words are written as $(g_1, \dots, g_m) =$

$g_1 * \dots * g_m = g_1 \cdots g_m$.

6. <u>Example</u> Let $G_1 \cong G_2 \cong \mathbb{Z}/2$

$G_1 = \{e_1, a\}$ $\quad G_2 = \{e_2, b\}$
$a^2 = e_1 \qquad b^2 = e_2$

Then $W = G_1 * G_2 = \{() = e, a, b, ab, ba, aba, bab, \ldots\}$

<u>Proposition</u> Let $(G_i)_{i \in I}$ be a family of groups. If at least two groups G_i, G_j are not trivial, then $\coprod_{i \in I} G_i$ is infinite (and not abelian).

Pf ($\to$ homework) $\square$

Now we consider free groups.

7. Let X be a set. For each $x \in X$, put $G_x = \mathbb{Z} \times \{x\}$ as an abelian group. We write $(n, x) = x^n$ for $n \in \mathbb{Z} \leadsto x^n \circ x^m = x^{n+m}$, $x = x^1$ for short

The free grp <u>$F(X)$</u> is defined as

$$F(X) = \coprod_{x \in X} G_x \qquad \text{if } X \neq \emptyset$$

$$F(\emptyset) = \{e\} \qquad \text{the trivial grp.}$$

The reduced words in $F(X)$ are thus of the form $x_1^{n_1} \cdots x_k^{n_k}$, $n_i \neq 0$, $x_i \neq x_{i+1}$.

Via the map $i_X : X \to F(X)$, $x \longmapsto x^1 = x$ we may view X as a <u>sub set</u> of $F(X)$. Then

$$\langle X \rangle = F(X) \quad , \quad X \text{ generates } F(X).$$

8. <u>Theorem</u> (The universal property of the free group)

Let X be a set, let $i_X : X \to F(X)$ as above. Then $(F(X), i_X)$ has the following universal property. For every group H and every map $\varphi : X \to H$, there is a <u>unique</u> homomorphism $F(\varphi) : F(X) \to H$ such that $F(\varphi) \circ i_X = \varphi$

$$\begin{tikzcd} X \arrow[r, "i_X"] \arrow[d, "\varphi"'] & F(X) \arrow[dl, "F(\varphi)"] \\ H & \end{tikzcd}$$

<u>pf</u> For each $x \in X$ consider the homomorphism $\lambda_x : G_x \to H$, $\lambda_x(x^n) = \varphi(x)^n$. We obtain a homomorphism

$$F(X) = \coprod_{x \in X} G_x \xrightarrow{F(\varphi)} H$$

with $F(\varphi)(x) = f(x)$

If $f: F(X) \to H$ is any homomorphism with $F \circ i_X = \varphi$, then $f(x) = \varphi(x)$ for all $x \in X$, hence

$$F(x_1^{n_1} \dots x_k^{n_k}) = \varphi(x_1)^{n_1} \dots \varphi(x_k^{n_k}) = F(\varphi)(x_1^{n_1} \dots x_k^{n_k})$$

$\Rightarrow f = F(\varphi)$ $\square$

<u>Corollary</u> A For every map of <u>sets</u> $X \xrightarrow{\varphi} Y$, there is a <u>unique</u> homomorphism $F(\varphi): F(X) \to F(Y)$ such that $i_Y \circ \varphi = F(\varphi) \circ i_X$

$$\begin{tikzcd} X \arrow[r, "i_X"] \arrow[d, "\varphi"'] & F(X) \arrow[d, "F(\varphi)"] \\ Y \arrow[r, "i_Y"] & F(Y) \end{tikzcd}$$

#

pf Apply the theorem to $i_Y \circ \varphi : X \to F(Y)$ $\square$

<u>Corollary</u> B The assignment
$$X \longmapsto F(X)$$
$$\varphi \longmapsto F(\varphi)$$
is a <u>functor</u> from the category of sets and maps to the category of groups and homomorphisms, ie:

$$F(id_X) = id_{F(X)}$$

$$F(\psi \circ \varphi) = F(\psi) \circ F(\varphi)$$

for $X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z$

pf This follows from the uniqueness of $F(\varphi)$. $\square$

Corollary C Let G be a group. Then there is a free grp $F(X)$ and a surjective homomorphism $\varphi: F(X) \to G$.

Every group is a quotient of some free group.

pf Let $X \subseteq G$ be a generating set (for example $X = G$). The inclusion $X \subseteq G$ extends to a homomphm $\varphi: F(X) \to G$.

Since $\varphi(X)$ generates G, φ is surjective $\square$

If there is a bijection $X \xrightarrow{\varphi} Y$, then $F(\varphi)$ is also a bijective homomorphism $F(X) \to F(Y)$ (by the uniqueness in Cor A). Hence $F(X)$ depends only on the cardinality of the set X. If $\# X = n < \infty$, one writes therefore

$F_n = F(X)$, the free group in

n generators.

If $F(X) \cong F(Y)$, do X and Y have the same number of elements? This needs some preparation.

9. <u>Def</u> Let G be a grp, and $a, b \in G$. The <u>commutator</u> of a and b is $[a,b] = aba^{-1}b^{-1}$
$= ab(ba)^{-1}$

$[a,b] = e \iff ab = ba$

$[a,b]^{-1} = [b,a]$

The <u>commutator grp</u> of G is the subgrp

$$DG = \langle \{[a,b] \mid a,b \in G\} \rangle.$$

Note: the product of commutators is <u>not</u> always a commutator, hence $DG \supseteq \{[a,b] \mid a,b \in G\}$.

<u>Lemma</u> Let G be a group. Then the following hold. (i) $DG \trianglelefteq G$

(ii) $DG = \{e\} \iff G$ is abelian

(iii) G/DG is abelian

(iv) If A is an abelian grp and if $\varphi : G \to A$ is a homomorphism, then $DG \subseteq \ker(\varphi)$.

pf (i) $g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}]$, hence

$g(DG)g^{-1} = DG$

(ii) G is abelian $\Leftrightarrow$ $ab = ba$ for all $a,b \in G$

$\Leftrightarrow$ $[a,b] = e$ for all $a,b \in G$ $\Leftrightarrow$ $DG = \{e\}$

(iii) $ab = [a,b]\,ba$, hence $ab \in DG\,ba = ba\,DG$

$\Rightarrow$ $ab\,DG = ba\,DG$ $\Rightarrow$ G/DG abelian.

(iv) If A is abelian, then $\varphi([a,b]) = \varphi(e) = e$

for all $a,b \in G$, hence $DG \subseteq \ker(\varphi)$ $\square$

The quotient $G_{ab} = G/DG$ is called the

<u>abelianization</u> or the first <u>homology group</u>

of G. [This is a functor: a homomorphism

$\varphi: G \to H$ induces a <u>unique</u> homomorphism

$\varphi_{ab}: G_{ab} \to H_{ab}$, such that the diagram commutes

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d] & H \arrow[d] \\ G_{ab} \arrow[r, "\varphi_{ab}"] & H_{ab} \end{tikzcd}$$

(use the homomorphism theorem)]

<u>Cor</u> If $G \xrightarrow{\varphi} H \xrightarrow{\psi} K$ are group homomorphisms, then $(\psi \circ \varphi)_{ab} = \psi_{ab} \circ \varphi_{ab}$ $\square$

10. <u>Free abelian groups</u>. Let X be a set. If $X = \emptyset$, put $FA(\emptyset) = \{0\}$ (trivial group).

Else, put $G_z = \mathbb{Z} \times \{z\}$ for $z \in X$, write $(k, z) = k_z$

$$FA(X) = \bigoplus_{z \in X} G_z \subseteq \prod_{z \in X} G_z$$

$$\bigoplus_{z \in X} G_z = \{ (k_z)_{z \in X} \mid k_z = 0 \text{ for } \underbrace{\text{almost all}}_{\text{only finitely many exceptions}} z \in X \}$$

For $z \in X$, put $\hat{z} = (k_x)$ $\quad k_x = \begin{cases} 1 & x = z \\ 0 & \text{else} \end{cases}$

Each $a \in FA(X)$ is a <u>finite</u> linear combination

$$a = \sum_{z \in X} a_z \hat{z}$$

finite sum, since only finitely many $a_z \neq 0$!

$\leadsto$ we have an injection $j_X : X \longrightarrow FA(X)$
$z \longmapsto \hat{z}$

11. <u>Theorem</u> (The universal property of the free abelian group)

Let $(A,+)$ be an <u>abelian</u> gp. For every map $X \xrightarrow{\varphi} A$, there is a unique homomorphism $FA(\varphi) : FA(X) \to A$ such that $j_X \circ FA(\varphi) = \varphi$

$$\begin{tikzcd} X \arrow[r, "j_X"] \arrow[dr, "\varphi"'] & FA(X) \arrow[d, "FA(\varphi)\ \exists!"] \\ & A \end{tikzcd}$$

<u>pf</u> <u>Existence.</u> For $a = \sum_{z \in X} a_z \hat{z}$, put
$\uparrow$ finite sum

$$FA(\varphi)(a) = \sum_{z\in X} a_z \varphi(z)$$
$\uparrow$ finite sum

<u>Uniqueness.</u> Suppose that $\tilde{f} : FA(X) \to A$ is a homomorphism, with $\varphi = \tilde{f} \circ j_X$. Then

$\varphi(z) = \tilde{f}(\hat{z})$, hence $\tilde{f}\left(\sum_{z\in X} a_z \hat{z}\right) = \sum_{z\in X} a_z \tilde{f}(\hat{z})$

$= \sum_{z \in X} a_z \varphi(z) = FA(\varphi)\left(\sum_{z\in X} a_z \hat{z}\right)$ $\square$

<u>Corollary</u> Put $\pi: F(X) \to F(X)_{ab}$. There is a unique isomorphism $FA(X) \xrightarrow{\cong} F(X)_{ab}$ such that the diagram

$$\begin{tikzcd} X \arrow[r, "i_X"] \arrow[d, "j_X"'] & F(X) \arrow[d, "\pi"] \\ FA(X) \arrow[r, "\cong"] & F(X)_{ab} \end{tikzcd}$$

commutes.

<u>pf</u> We show that $(F(X)_{ab}, \pi \circ i_X)$ has the same universal property as $(FA(X), j_X)$.

Let A be an abelian gp, let $\varphi: X \to A$ be a map. Then is a unique homomorphism $F(\varphi): F(X) \to A$ such that $\varphi = F(\varphi) \circ i_X$. Since A is abelian, $F(\varphi)$ factors as $F(\varphi) = F(\varphi)_{ab} \circ \pi$

$$\begin{tikzcd} X \arrow[r, "i_X"] \arrow[d, "\varphi"'] & F(X) \arrow[d, "\pi"] \arrow[dl, "F(\varphi)"'] \\ A & F(X)_{ab} \arrow[l, "F(\varphi)_{ab}"] \end{tikzcd}$$

If $\tilde{F}: F(X) \to A$ is any other homomorphism with $\tilde{\tilde{f}} \circ \pi \circ i_X = \varphi$, then $\tilde{f} \circ \pi = F(\varphi)$ (uniqueness of $F(\varphi)$) and hence $\tilde{\tilde{f}} = F(\varphi)_{ab}$ (homomorphism theorem). $\square$

11. Proposition Let X, Y be sets. If there is an isomorphism $FA(X) \cong FA(Y)$, then both sets have the same cardinalities, $\# X = \# Y$.

For the proof we use the following Lemma.

Lemma Let $(A, +)$ be an abelian grp, let $m \in \mathbb{N}$. Then $mA = \{ ma \mid a \in A \}$ is a subgrp of A

pf The map $a \mapsto ma$ is an endomorphism of A. $\square$

pf of the proposition. Let p be a prime, eg $p = 2$. Then $FA(X) / pFA(X) \cong \bigoplus_{x \in X} H_x \qquad H_x \cong \mathbb{Z}/p$.

This abelian grp is an $\mathbb{F}_p$-vector space ($\mathbb{F}_p$ acts via $(l, \sum_{x \in X} a_x \hat{x}) \longmapsto \sum_{x \in X} l a_x \hat{x}$, $l, a_x \in \mathbb{Z}/p = \mathbb{F}_p$, $x \in X$) of dimension $\# X$. By Steinitz' Exchange Lemma, all bases have length $\# X$. Hence $\# X = \# Y$ $\square$

Corollary Let X, Y be sets. If there is an isomorphism $F(X) \cong F(Y)$, then $\# X = \# Y$.

pf $F(X) \cong F(Y) \Rightarrow F(X)_{ab} \cong F(Y)_{ab} \Rightarrow$
$FA(X) \cong FA(Y) \Rightarrow \# X = \# Y$. $\square$ #

In particular, we have for $m, n \in \mathbb{N}$

$$F_m \cong F_n \Rightarrow m = n$$

But we will see that there are injective homomorphisms
$F_m \rightarrow F_n$ for all $m, n \geq 2$!

Observation If $Y \subseteq X$ is a subset, then
$F(Y) \rightarrow F(X)$ is injective. We can show this, using only the universal property. Let $r: X \rightarrow Y$ be a left inverse of the inclusion $i: Y \rightarrow X$, i.e.
$r \circ i = \mathrm{id}_Y$

$$\begin{tikzcd} Y \arrow[r, "i"] \arrow[dr, equal] & X \arrow[d, "r"] \\ & Y \end{tikzcd} \quad \curvearrowright \quad \begin{tikzcd} F(Y) \arrow[r, "F(i)"] \arrow[dr, equal] & F(X) \arrow[d, "F(r)"] \\ & F(Y) \end{tikzcd}$$

$\Rightarrow F(i)$ has a left inverse $\Rightarrow F(i)$ injective.

Some properties of free groups / free products follow directly from the universal properties.
But: sometimes reduced words are needed.

The following is useful for recognizing free products.

12. <u>Lemma</u> (The Ping-Pong Lemma)
Let G be a grp with subgrps $A, B \leq G$, such that $G = \langle A \cup B \rangle$, with $\#A \geq 2$, $\#B \geq 3$.

Suppose that G acts on a set X, that $P, Q \subseteq X$ with $Q \nsubseteq P$ and that the following hold:

$$a \in A - \{e\} \Rightarrow a(Q) \subseteq P$$
$$b \in B - \{e\} \Rightarrow b(P) \subseteq Q$$

Then the canonical map $A * B \xrightarrow{\varphi} G$ is an isomorphism.

pf Since $G = \langle A \cup B \rangle$, the map $A * B \xrightarrow{\varphi} G$ is surjective. Let $w \in W$ with $\varphi(w) = e$.

<u>Claim:</u> $w = ()$. We view A, B as being disjoint!

<u>Case 1</u> $w = a_1 b_1 a_2 b_2 \dots a_s$, $s \geq 1$ $\Big|$ $a_i, b_j \neq e$, $a_i \in A - \{e\}$, $b_j \in B - \{e\}$

Then $\varphi(w)(Q) \subseteq P$. Since $Q \nsubseteq P$, $\varphi(w) \neq e$

Case 2 $\quad \omega = b_1 a_1 b_2 a_2 \dots b_s$, $s \geq 1$. Choose $a \in A - \{e\}$

$\Rightarrow \varphi(a \omega a^{-1}) \neq e$ by case 1, hence $\varphi(\omega) \neq e$

Case 3 $\quad w = a_1 b_1 \cdots a_s b_s$, $s \geq 1$. Choose $b \in B$, $b \neq e, b_s$

$\Rightarrow \varphi(b w b^{-1}) \neq e$ by case 2

hence $\varphi(\omega) \neq e$

Case 4 $\quad \omega = b_1 a_1 \cdots b_s a_s$, $s \geq 1$. Choose $b \in B$ $b \neq e, b_1$

$\varphi(b^{-1} \omega b) \neq e$ by case 2,

hence $\varphi(\omega) \neq e$ $\square$

13. Example

Recall $\quad SL_2\mathbb{Z} = \{ g \in \mathbb{Z}^{2\times 2} \mid \det(g) = 1 \}$

This is a grp: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Put $\quad a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

Lemma A $\quad \langle \{a, b\} \rangle = SL_2\mathbb{Z}$

pf $\quad$ Suppose $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2\mathbb{Z}$

case 1 $\quad \gamma = 0 \rightsquigarrow \alpha\delta = 1 \rightsquigarrow \alpha = \delta = \pm 1$

$$\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} = b^{\beta} \qquad (\checkmark)$$

$$\begin{pmatrix} -1 & \beta \\ 0 & -1 \end{pmatrix} = \underbrace{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}}_{=a^2} \underbrace{\begin{pmatrix} 1 & -\beta \\ 0 & 1 \end{pmatrix}}_{b^{-\beta}} \qquad (\checkmark)$$

Case 2 $\quad |\alpha| = |\gamma| \leadsto \gamma \neq 0$

$$\alpha = \gamma \leadsto aba\,g = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \alpha & \delta \end{pmatrix} = \underbrace{\begin{pmatrix} -\alpha & ? \\ 0 & ? \end{pmatrix}}_{\substack{\in \langle\{a,b\}\rangle \\ \text{by case 1}}}$$

$$\alpha = -\gamma \leadsto a^{-1}b\,g = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ -\alpha & \delta \end{pmatrix} = \underbrace{\begin{pmatrix} \gamma & ? \\ 0 & ? \end{pmatrix}}_{\in \langle\{a,b\}\rangle}$$

Case 3 $\quad \alpha = 0$

$$a\,g = \begin{pmatrix} -\gamma & -\delta \\ 0 & \beta \end{pmatrix} \in \langle\{a,b\}\rangle$$

Case 4 $\quad 0 < |\alpha| < |\gamma|$

$$a\,g = \begin{pmatrix} -\gamma & -\delta \\ \alpha & \beta \end{pmatrix} \leadsto \text{in case } 0 < |\gamma| < |\alpha|$$

Case 5 $\quad 0 < |\gamma| < |\alpha| \qquad \alpha = \lambda \cdot \gamma + \mu \qquad 0 < \mu \le |\gamma|$

$$b^{-\lambda} g = \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \mu & ? \\ \gamma & ? \end{pmatrix}$$

If $|\gamma| = \mu \rightsquigarrow$ case 2

If $|\gamma| > \mu \rightsquigarrow$ case 4 $\rightsquigarrow$ case 5, but the absolute value of the upper left corner has dropped ($|\gamma| < |\alpha|$). This can happen only finitely many times $\rightsquigarrow$ at some point we end up in case 1, 2, 3 $\square$

Lemma B The gp $SL_2(\mathbb{Z})$ acts on the projective line $\mathbb{R}P^1 = \mathbb{R} \cup \{\infty\}$ via

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}(x) = \frac{\alpha x + \beta}{\gamma x + \delta} \qquad \left(\text{with } \frac{1}{\infty} = 0,\ \frac{1}{0} = \infty,\ a + \infty = \infty\ a \in \mathbb{R} \ldots\right)$$

The kernel of this action is $\left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$

Pf $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}(x) = x \iff \alpha x + \beta = \gamma x^2 + \delta x$

$\iff \gamma x^2 + (\delta - \alpha)x - \beta = 0$

If this holds for all x, then $\gamma = \gamma = 0$ and $\alpha = \delta$. $\square$

We put $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z}) / \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$

For $g \in SL_2\mathbb{Z}$ we denote its image in $PSL_2\mathbb{Z}$ by $\bar{g} = \{\pm g\}$

Put $A = \langle \bar{a} \rangle$ $\quad B = \langle \overline{ab} \rangle$

$a^2 = -\mathbb{1} \Rightarrow \bar{a}^2 = e \rightsquigarrow A \cong \mathbb{Z}/2$

$ab = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, (ab)^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, (ab)^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

$\rightsquigarrow B \cong \mathbb{Z}/3$

<u>Lemma C</u> $\quad PSL_2\mathbb{Z} \cong A * B$

pf We use the Ping-Pong Lemma, with

$P = \mathbb{R}_{>0} \subseteq \mathbb{R}P^1$

$Q = \mathbb{R}_{<0} \subseteq \mathbb{R}P^1$

$ab(x) = \frac{-1}{x+1} \rightsquigarrow \overline{ab}(P) \subseteq Q$

$(ab)^2(x) = -\frac{x+1}{x} \rightsquigarrow \overline{ab}^2(P) \subseteq Q$

$a(x) = \frac{-1}{x} \rightsquigarrow \bar{a}(Q) \subseteq P$

Hence $PSL_2(\mathbb{Z}) \cong A * B$ $\qquad \square$

14. Lemma (The Ping-Pong Lemma, II).

Suppose that $G \times X \to X$ is an action and that $P, Q \subseteq X$, $P \not\subseteq Q \not\subseteq P$. Suppose $a, b \in G$ are elements with

$$a^n(Q) \subseteq P \quad \text{for all } n \neq 0, n \in \mathbb{Z}$$
$$b^n(P) \subseteq Q \quad \text{for all } n \neq 0, n \in \mathbb{Z}$$

Then the canonical homomorphism
$$F(\{a,b\}) \to G, \quad a \mapsto a, \quad b \mapsto b$$
is injective.

Pf We have $a^n \neq e \neq b^n$ for all $n \neq 0$. Hence

$A = \langle a \rangle \cong \mathbb{Z}$ Put $H = \langle A \cup B \rangle$

$B = \langle b \rangle \cong \mathbb{Z}$

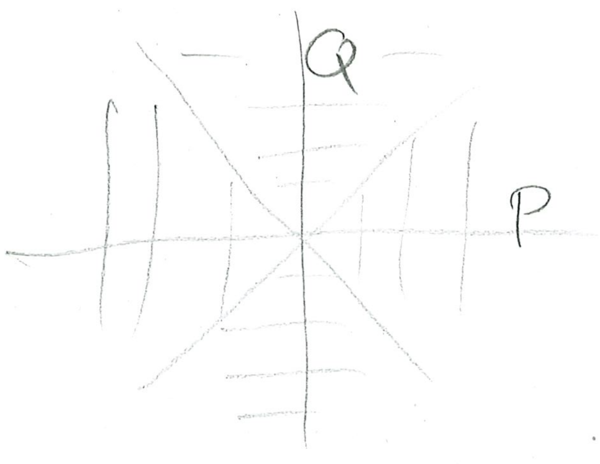
Now apply §2.12 $\rightsquigarrow$ $H \cong A * B$ $\square$

15. Example (Free groups in $SL_2\mathbb{Z}$)

Put $G = SL_2\mathbb{Z}$, $a = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ $b = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$

$X = \mathbb{R}^2$ $P = \{(x,y) \mid |x| > |y|\}$

$Q = \{(x,y) \mid |y| > |x|\}$



$a^k = \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix}$ If $|x| < |y|$, then

$|x + 2ky| \geq 2|k||y| - |x| > |y|$

for $k \neq 0$

$\Rightarrow a^k(Q) \subseteq P$

similarly $b^k(P) \subseteq Q$ if $k \neq 0$.

Hence $F_2 \cong \langle \{a, b\} \rangle \leq SL_2 \mathbb{Z}$ $\square$

#