

Combinatorial Group Theory

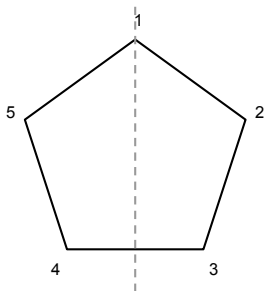
Dr Martin Edjvet, The University of Nottingham, Spring semester 2011

\LaTeX by Alexandra Surdina, last changes: April 18, 2011.

These are the lecture notes for the module *Combinatorial Group Theory* at the University of Nottingham by Dr Martin Edjvet, based on handwritten notes. I'm happy to correct any mistakes you find, just send me an email: alexandra.surdina@gmail.com

1 Free groups

By way of introduction consider the dihedral group D_{10} of order 10, the group of isometries of the regular 5-gon. It consists of five rotations and five reflections.



Let $x = (12345)$, $y = (25)(34)$. Then $|x| = 5$, $|y| = 2$, and

$$y^{-1}xy = (25)(34)(12345)(25)(34) = (15432) = x^{-1}$$

Therefore,

$$yx = y^{-1}x = x^{-1}y^{-1} = x^{-1}y$$

$$\text{and } y^{-1}x^{-1} = yx^{-1} = xy$$

(rewrite rules). Thus, all elements of D_{10} are of the form $x^i y^j$.

For example,

$$\begin{aligned} w &= xyx^2y^3x^3y^{-1}x^{-2}y^{11} = x(yx)xyx^3y^{-1}x^{-2}y \\ &= xx^{-1}yxyx^3y^{-1}x^{-2}y = (yx)yx^3y^{-1}x^{-2}y \\ &= (x^{-1}y)yx^3y^{-1}x^{-2}y = x^2y^{-1}x^{-2}y \\ &= x^2(y^{-1}x^{-1})x^{-1}y = x^2xyx^{-1}y \\ &= x^3(yx^{-1})y = x^4y^2 \\ &= x^4 \end{aligned}$$

$$\Rightarrow D_{10} = \{e, x, x^2, x^3, x^4, y, xy, x^2y, x^3y, x^4y\}$$

(Does D_{10} really contain ten elements? In other words: Could some of the elements above still be equal? No! Suppose for example $x^3 = x^4y \Rightarrow x^{-1} = y$.)

Definition. A group F is said to be free on $X \subseteq F$ if given any group G and any mapping $\theta : X \rightarrow G$ there exists a unique homomorphism $\theta' : F \rightarrow G$ extending θ , that is, having the property that $x\theta' = x\theta$ ($\forall x \in X$). That is, the diagram

$$\begin{array}{ccc} X & \xrightarrow{\iota} & F \\ \downarrow \theta & \searrow \theta' & \\ G & & \end{array}$$

commutes. Here $\iota : X \rightarrow F$ is the *inclusion* determined by $x\iota = x$ ($\forall x \in X$).

Remarks. (1) ι and θ are mappings; θ' is a homomorphism.

(2) This definition allows us to distinguish between words in F .

$$x_1x_2, x_1x_3 \in F \quad (x_i \in X)$$

$$\begin{array}{ccccccc} x_1 & & x_2 & & x_3 & & X \longrightarrow F \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \theta \quad \nearrow \theta' \\ (12) & & (123) & & (124) & & S_4 \end{array}$$

$$(x_1x_2)\theta' = (x_1)\theta'(x_2)\theta' = (12)(123)$$

$$(x_1x_3)\theta' = (x_1)\theta'(x_3)\theta' = (12)(124)$$

(3) If we replace “group” by “abelian group” in the above definition, we get a free abelian group on X .

Exercise. Show that every free abelian group A is a direct sum of copies of \mathbb{Z} :

$$A \cong \oplus \mathbb{Z}$$

Lemma 1.1. *If F is free on X then X generates F .*

Proof. Let $H = \langle X \rangle \subseteq F$ be the subgroup generated by X , and let $\theta : X \rightarrow H$ be the mapping $x\theta = x$ ($\forall x \in X$). Let $\theta' : F \rightarrow H$ be the corresponding extension. Let $\iota_2 : H \rightarrow F$ be defined by $h\iota_2 = h$ ($\forall h \in H$). Then $\theta'\iota_2$ extends θ . But so does id_F , and so $\theta'\iota_2 = id_F$ by uniqueness. Therefore $F = Im(id_F) = Im(\theta'\iota_2) \subseteq H \Rightarrow F = H = \langle X \rangle$. □

If F is free on X then X is a (free) basis for F and $|X| = r(F)$ is the rank of F .

Theorem 1.2. *If F_i is free on X_i ($i = 1, 2$) and $|X_1| = |X_2|$ then $F_1 \cong F_2$. (Free groups of the same rank are isomorphic.)*

Proof. Assume $|X_1| = |X_2|$. Let $\phi : X_1 \rightarrow X_2$ be a bijection. Let α, β be the following extensions (in which ι_1 and ι_2 are inclusions):

$$\begin{array}{ccc}
 X_1 & \xrightarrow{\iota_1} & F_1 \\
 \downarrow \phi & \nearrow \alpha & \\
 X_2 & & \\
 \downarrow \iota_2 & & \\
 F_2 & &
 \end{array}
 \quad
 \begin{array}{ccc}
 X_2 & \xrightarrow{\iota_2} & F_2 \\
 \downarrow \phi^{-1} & \nearrow \beta & \\
 X_1 & & \\
 \downarrow \iota_1 & & \\
 F_1 & &
 \end{array}$$

Now $\iota_1\alpha\beta = \phi\iota_2\beta = \phi\phi^{-1}\iota_1 = \iota_1$, so $\alpha\beta : F_1 \rightarrow F_1$ extends ι_1 .

$$\begin{array}{ccc}
 X_1 & \xrightarrow{\iota_1} & F_1 \\
 \downarrow \iota_1 & \nearrow \alpha\beta & \\
 F_1 & &
 \end{array}$$

By uniqueness, $\alpha\beta = id_{F_1}$, since id_{F_1} also extends ι_1 . Similarly $\beta\alpha = id_{F_2}$. This says that $\alpha : F_1 \rightarrow F_2$ and $\beta : F_2 \rightarrow F_1$ are bijective homomorphisms and so are inverse isomorphisms. □

Let F be a group and let $X \subseteq F$. For the group G let $Hom(F, G)$ denote the set of homomorphisms from $F \rightarrow G$, and let $Map(X, G)$ denote the set of mappings from $X \mapsto G$.

Define $\rho : Hom(F, G) \rightarrow Map(X, G)$ by $\phi\rho = \iota\phi$ where $\iota : X \rightarrow F$ is inclusion.

Exercise. (1) ρ is surjective iff for all maps $X \rightarrow G$ there exists θ' as in the definition of F being free on X .

(2) ρ is injective iff θ' , if it exists, is unique.

(3) F is free on X iff ρ is bijective \forall groups G .

Theorem 1.3. *If F_i is free on X_i ($i = 1, 2$) and $F_1 \cong F_2$ then $|X_1| = |X_2|$. (Free groups of different rank are not isomorphic.)*

Proof. Since $F_1 \cong F_2$ we have $|\text{Hom}(F_1, G)| = |\text{Hom}(F_2, G)|$ for any group G . Therefore $|\text{Map}(X_1, G)| = |\text{Map}(X_2, G)|$ for any group G . Let $G = C_2$ be the cyclic group of order two. Then $|\text{Map}(X_1, G)| = 2^{|X_1|} = |\text{Map}(X_2, G)| = 2^{|X_2|}$
 $\Rightarrow |X_1| = |X_2|$. □

Free groups are (isomorphic to): $\mathbb{Z}, F_2, F_3, \dots, F_n, \dots$ and F_∞ where F_n is the free group of rank n and F_∞ is the free group of X where X is infinite. Let X be an arbitrary non-empty set. We construct a free group $F(X)$ with X as a free basis.

Step 1. First form another copy of X ,

$$\hat{X} = \{\hat{x} : x \in X\}$$

where the elements of \hat{X} will later become the inverses of the elements of X . Let $X^{\pm 1} := X \cup \hat{X}$. Now form the sets of words W_n of length $n \geq 0$ in $X^{\pm 1}$ which are n -tuples of elements of $X^{\pm 1}$. Thus

- W_0 consists of $()$, the *empty word* (sometimes denoted by e).
- W_1 consists of $(x), (\hat{x}), x \in X$
- W_2 consists of $(x, y), x, y \in X^{\pm 1}$

and so on. Now discard all words containing an adjacent pair: $(\dots, x, \hat{x}, \dots)$ or $(\dots, \hat{x}, x, \dots)$ where $x \in X$. The remaining words are called *reduced* words. Let \widetilde{W}_n denote the set of reduced words of length n . Finally let $F(X) = \bigcup_{n \geq 0} \widetilde{W}_n$.

Notation: We are writing:

- x^{-1} for \hat{x}
- $x_1 x_2 \dots x_k$ for (x_1, x_2, \dots, x_k)
- x^n for $(x, \dots, x) \in \widetilde{W}_n$
- x^{-n} for $(\hat{x}, \dots, \hat{x}) \in \widetilde{W}_n$

(for $x, x_i \in X$).

Example. If $X = \{x, y\}$, $\widetilde{W}_2 = \{x^2, y^2, x^{-2}, y^{-2}, xy, xy^{-1}, x^{-1}y, x^{-1}y^{-1}, yx, y^{-1}x, y^{-1}x^{-1}, yx^{-1}\}$.

Step 2. “Juxtaposition plus cancellation” is the binary operation.

Given $a = (x_1, \dots, x_l) \in \widetilde{W}_l, b = (y_1, \dots, y_m) \in \widetilde{W}_m$,

$$ab := (x_1, \dots, x_{l-r}, y_{r+1}, \dots, y_m)$$

where r is the largest integer k such that none of $(x_l, y_1), (x_{l-1}, y_2), \dots, (x_{l-k+1}, y_k)$ is reduced. Thus $ab \in \widetilde{W}_{l+m-2r}$. Now we need to check the group axioms.

Closure: Immediate.

Identity: The empty word $()$.

Inverses: $(x_1, \dots, x_l)^{-1} = (\hat{x}_l, \dots, \hat{x}_1)$ with the understanding that $\hat{x} := x$ for $x \in X$.

Associativity: Let $c = (z_1, \dots, z_n) \in \widetilde{W}_1$ and let $bc = (y_1, \dots, y_{m-s}, z_{s+1}, \dots, z_n) \in \widetilde{W}_{m+n-2s}$. We want to show: $(ab)c = a(bc)$.

“We always prove $(ab)c = a(bc)$. Why is this enough to prove that it doesn’t matter how to bracket an arbitrary expression? We always take it for granted, don’t we? This is a hidden horrible exercise in group theory.”

If a, b or c is the empty word the result is obvious. So, assume that $l, m, n \geq 1$. Then there are three cases to consider:

Case 1.

$r + s < m$ (The cancellations in ab and bc are disjoint).

Then both sides of $(ab)c = a(bc)$ are equal to

$$(x_1, \dots, x_{l-r}, y_{r+1}, \dots, y_{m-s}, z_{s+1}, \dots, z_n) \in \widetilde{W}_{l+m+n-2(r+s)}$$

Example. $r = 2, s = 3, m = 6$

$a = xyxy^{-1}x^{-1}$ (which is equal to $(x, y, x, \hat{y}, \hat{x})$ but we won’t use this notation.)

$b = xyxy^{-1}xy^{-1}$ and $c = yx^{-1}yx$

$$\begin{aligned}(ab)c &= (xyxy^{-1}x^{-1}xyxy^{-1}xy^{-1})yx^{-1}yx \\ &= (xyxy^{-1}xy^{-1})yx^{-1}yx \\ &= xyxxx\end{aligned}$$

$$\begin{aligned}a(bc) &= xyxy^{-1}x^{-1}(xyxy^{-1}xy^{-1}yx^{-1}yx) \\ &= xyxy^{-1}x^{-1}(xyxx) \\ &= xyxxx\end{aligned}$$

Case 2. $r + s = m$ (The cancellations in ab and bc meet in exactly one place so that b is completely cancelled out.)

Here both sides equal $(x_1, \dots, x_{l-r}, z_{s+1}, \dots, z_n) \in W_{l+n-m}$.

Example. $r = 2, s = 2, m = 4$

$$a = yx^{-1}y^{-1} \quad (l = 4)$$

$$b = yxyx \quad (m = 4)$$

$$c = x^{-1}y^{-1}y^{-1}x \quad (n = 4)$$

$$\begin{aligned}(ab)c &= (yx^{-1}y^{-1}yxyx)x^{-1}y^{-1}y^{-1}x \\ &= (yxyx)x^{-1}y^{-1}y^{-1}x \\ &= xyx^{-1}x \in W_4\end{aligned}$$

$$\begin{aligned}a(bc) &= yx^{-1}y^{-1}(yxyxx^{-1}y^{-1}y^{-1}x) \\ &= yx^{-1}y^{-1}(yxy^{-1}x) \\ &= xyx^{-1}x \in W_4\end{aligned}$$

(Of course this word can be further reduced to $xx \in \widetilde{W}_2$ but we stop the reduction as soon as we arrive in \widetilde{W}_{l+m-n} . It's sufficient to know that we end up with the same *irreduced* word at some point since it would lead us to the same *reduced* word as well.)

Case 3. $r + s > m$ (The cancellations overlap).

In this case put $\beta = (y_1, \dots, y_{m-s}), \gamma = (y_{m-s+1}, \dots, y_r), \delta = (y_{r+1}, \dots, y_m)$, where

γ describes the overlapping part.

By hypothesis, γ has length $r - m + s - 1 + 1 = r - m + s > 0$ and $b = \beta\gamma\delta$,
 $a = \alpha\gamma^{-1}\beta^{-1}$ with $\alpha = (x_1, \dots, x_{l-r})$, $c = \delta^{-1}\gamma^{-1}\varepsilon$ with $\varepsilon = (z_{s+1}, \dots, z_n)$

Then,

$$\begin{aligned}(ab)c &= (\alpha\gamma^{-1}\beta^{-1}\beta\gamma\delta)(\delta^{-1}\gamma^{-1}\varepsilon) \\ &= (\alpha\delta)(\delta^{-1}\gamma^{-1}\varepsilon) \\ &= \alpha(\gamma^{-1}\varepsilon)\end{aligned}$$

$$\begin{aligned}a(bc) &= (\alpha\gamma^{-1}\beta^{-1})(\beta\gamma\delta\delta^{-1}\gamma^{-1}\varepsilon) \\ &= (\alpha\gamma^{-1}\beta^{-1})(\beta\varepsilon) \\ &= (\alpha\gamma^{-1})\varepsilon\end{aligned}$$

Since α and γ^{-1} are adjacent in the reduced word a there is no cancellation in forming their product. Similarly this is also the case for γ^{-1} and ε since they are adjacent in the reduced word c . Therefore:

$$a(bc) = a\gamma^{-1}\varepsilon = (ab)c$$

Example. Take $r = 4, s = 4, m = 5$.

$$a = xyxy^{-1}x^2y = (xyx)(y^{-1}x)(xy) = \alpha\gamma^{-1}\beta^{-1}$$

$$b = y^{-1}x^{-2}yx = (y^{-1}x^{-1})(x^{-1}y)(x) = \beta\gamma\delta$$

$$c = x^{-1}y^{-1}xyx^3 = (x^{-1})(y^{-1}x)(yx^3) = \delta^{-1}\gamma^{-1}\varepsilon$$

$$\text{Then } (ab)c = \alpha\gamma^{-1}\varepsilon = (xyx)(y^{-1}x)yx^3 = xyxy^{-1}xyx^3 = a(bc).$$

Step 3. Get rid of the brackets and commas.

$$x \rightarrow x$$

$$(x_1, \dots, x_l) = x_1 \dots x_l$$

and identify \hat{x} with x^{-1} . Note that $\langle X \rangle = F(X)$.

Step 4. Finally we show that $F(X)$ is free on X .

For a given group G and a mapping $\theta : X \rightarrow G$ define $\theta' : F(X) \rightarrow G$ as follows:

$$\begin{aligned} e_{F(X)}\theta' &= e_G \\ x\theta' &= x\theta \quad \forall x \in X \\ x^{-1}\theta' &= (x\theta)^{-1} \quad \forall x \in X \end{aligned}$$

and $(x_1, \dots, x_l)\theta' = (x_1\theta')(x_2\theta') \dots (x_l\theta')$ for $x_1, \dots, x_l \in \widetilde{W}_l$.

It is clear that θ' extends θ and if $\phi : F(X) \rightarrow G$ is another extension of θ then θ' and ϕ (given that θ' is a homomorphism) agree on the generating set X so $\theta' = \phi$ (uniqueness). (See Exercise Sheet 1, Question 1.)

It remains to show that θ' is homomorphism: Let $a = x_1 \dots x_l \in \widetilde{W}_l$ and $b = y_1 \dots y_m \in \widetilde{W}_m$ and $ab = x_1 \dots x_{l-r} y_{r+1} \dots y_m \in \widetilde{W}_{l+m-2r}$. By definition of ab we see that $y_i = x_{l-i+1}^{-1}$ for $1 \leq i \leq r$ (to get cancellations) and so by definition of θ' , $y_i\theta' = (x_{l-i+1}\theta)^{-1} = (x_{l-i+1}\theta')^{-1}$.

(To see this if $y_i \in X$, $x_{l-i+1}^{-1} \in X^{-1}$ then $y_i\theta' = y_i\theta = (y_i^{-1}\theta')^{-1} = (x_{l-i+1}\theta')^{-1}$; and if $y_i \in X^{-1}$, $x_{l-i+1}^{-1} \in X$ then $y_i\theta' = x_{l-i+1}^{-1}\theta' = (x_{l-i+1}\theta)^{-1} = (x_{l-i+1}\theta')^{-1}$.)

Therefore,

$$\begin{aligned} (a\theta')^{-1}((ab)\theta')(b\theta')^{-1} &= [x_1\theta' \dots x_l\theta'] [x_1\theta' \dots x_{l-r}\theta' y_{r+1}\theta' \dots y_m\theta'] [y_1\theta' \dots y_m\theta']^{-1} \\ &= (x_l\theta')^{-1} \dots (x_{l-r+1}\theta')^{-1} (y_r\theta')^{-1} \dots (y_1\theta')^{-1} \\ &= (y_1\theta') \dots (y_r\theta') (y_r\theta')^{-1} \dots (y_1\theta')^{-1} = e \end{aligned}$$

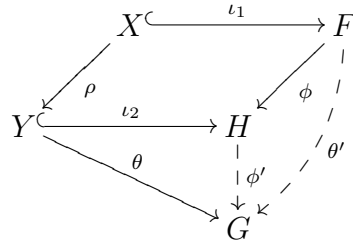
So $(a\theta')(b\theta') = ((ab)\theta') \Rightarrow \theta' \in \text{Hom}(F(X), G)$.

We have proved:

Theorem 1.4. *The group $F(X)$ of reduced words in $X^{\pm 1}$ is free on X .*

Lemma 1.5. *If F is free of rank r and $H \cong F$ then H is free of rank r .*

Proof. Let F be free on X with $|X| = r$. Let $\phi : F \rightarrow H$ be an isomorphism and let $Y = \{x\phi : x \in X\} \subseteq H$.



We claim that H is free on Y . Since $|Y| = r$ the result follows.

Let $\rho : X \rightarrow Y$ be the bijection $x\rho = x\phi$ ($\forall x \in X$). Let G be any group and θ any mapping from Y to G . Since F is free on X there exists a unique homomorphism $\theta' : F \rightarrow G$ extending $\rho\theta$. Let $\phi' : H \rightarrow G$ be the homomorphism defined by $\phi' = \phi^{-1}\theta'$. Clearly $\rho\iota_2 = \iota_1\phi$. Therefore $\rho\theta = \iota_1\theta' = \iota_1\phi\phi' = \rho\iota_2\phi'$. Now ρ is a bijection, so $\theta = \iota_2\phi'$, that is, ϕ' extends θ . Suppose now that $\theta = \iota_2\hat{\phi}$. Then $\rho\theta = \rho\iota_2\hat{\phi}$.
 $\Rightarrow \rho\theta = \iota_1\phi\hat{\phi} \Rightarrow \phi\hat{\phi}$ extends θ . Since θ' also extends θ and is unique, $\hat{\phi} = \phi^{-1}\theta' = \phi'$. □

(What we have proved here is that “being free” is an isomorphism invariant.)

Theorem 1.6. *A group F is free on a subset $X \subseteq F$ iff*

(i) X generates F , and

(ii) no reduced word in $X^{\pm 1}$ of positive length is equal to the identity in F .

Proof. Let θ' be the unique extension of the inclusion $\iota_2 : X \rightarrow F$.

$$\begin{array}{ccc}
X & \xrightarrow{\iota_1} & F(X) \\
\downarrow \iota_2 & \nearrow \theta' & \\
F & &
\end{array}$$

(\Leftarrow): If (i) holds then θ' is surjective. If (ii) holds then θ' is injective. Therefore θ' is an isomorphism and so F is free on X by 1.5.

(\Rightarrow): If F is free on X and $|X| = r$, then both F and $F(X)$ are free groups of rank r . Therefore by theorem 1.2, $F \cong F(X)$. Since (i) and (ii) hold in $F(X)$ it is clear that they also hold in F . □

Theorem 1.7. *Every group is isomorphic to a quotient group of a free group.*

Proof. Let G be a given group and let X be any generating set for G . Such an X always exists (take $X = G$ if necessary). Let θ' be the unique extension given by:

$$\begin{array}{ccc} X & \xrightarrow{\iota_1} & F(X) \\ \downarrow \iota_2 & \nearrow \theta' & \\ G & & \end{array}$$

Then (first isomorphism theorem) $F(X)/\ker\theta' \cong \text{Im}\theta'$.

But $X \subseteq \text{Im}\theta'$ and $\langle X \rangle = G$. Thus, $\text{Im}\theta' = G$.

□

We investigate **torsion** in free groups.

A reduced word

$$a = x_1 \dots x_l \quad (x_i \in X^{\pm 1}, a \in F(X))$$

is called *cyclically reduced* if $x_1 \neq x_l^{-1}$.

Example. The word $x^2y^{-1}xyx^{-1}$ is reduced but not cyclically reduced.

The word $yx^2y^3x^{-1}y$ is cyclically reduced.

Suppose $a = x_1 \dots x_l$ is reduced and $a^2 = x_1 \dots x_{l-r}x_{r+1} \dots x_l \in \widetilde{W}_{2l-2r}$. So $l(a) = 2l - 2r$. Question: How big can r be?

Example. Let's assume $l = 9$ and $r = 5$.

$$a = x_1x_2x_3x_4x_5x_6x_7x_8x_9x_1x_2x_3x_4x_5x_6x_7x_8x_9$$

But x_5x_5 is a reduced word of length 2, so $r = 5$ is impossible!

Example. What about $l = 8$ and $r = 5$?

$$a = x_1x_2x_3x_4x_5x_6x_7x_8x_1x_2x_3x_4x_5x_6x_7x_8$$

If $x_5x_4 = e$ then $x_4 = x_5^{-1} \Rightarrow x_4x_5 = e$ which contradicts the fact that a is reduced.

More generally, if $l = 2k + 1$ and $r > k$ then we get $x_{k+1}^2 = e$ (contradiction), and if $l = 2k$ and $r \geq k$ then we get “ a not reduced” (contradiction). Therefore $r < l(a)/2$.

Now let $a = u^{-1}\hat{a}u$ where \hat{a} is cyclically reduced.

$$a = (x_1 \dots x_r)^{-1} x_{r+1} \dots x_{l-r} (x_1 \dots x_r) \quad l(\hat{a}) > 0 \text{ for } a \neq e$$

Example.

$$a = x^{-1}y^{-1}x^2y^4xyx^{-2}yx$$

$$\hat{a} = y^4xy$$

Note that $l(a^2) = 2l(a) - 2r > 2l(a) - l(a) = l(a)$.

More generally,

$$a^n = (u^{-1}\hat{a}u)^n = u^{-1}\hat{a}^n u$$

$$\Rightarrow l(a^n) = l(u^{-1}\hat{a}^n u) = nl(\hat{a}) + 2r > (n-1)l(\hat{a}) + 2r = l(u^{-1}\hat{a}^{n-1}u) = l(a^{n-1}).$$

We have proved:

Theorem 1.8. $F(X)$ is torsion free (the only element of finite order is e).

Remark. $\langle \mathbb{Q} \setminus \{0\}, x \rangle$ has elements $+1$ and -1 of finite order so it is not torsion free – therefore it’s not free.

If $g \in G$ then the centralizer of g in G is the subgroup $C_G(g) = \{h \in G : hg = gh\} \leq G$.

Theorem 1.9. For any $w \in F(X) \setminus \{e\}$, $C_w = C_{F(X)}(w) \cong \mathbb{Z}$ (infinite cyclic group).

We will need some Lemmas:

Lemma 1.10. Let $a, b \in F(X)$. If $ab = ba$ then $\exists c \in F(X)$ such that $a = c^k$ and $b = c^h$ where $k, h \in \mathbb{Z}$.

Proof. The proof is by induction on $l(a) + l(b)$. The result is clear if $a = e$ or $b = e$, in particular, the result holds for $l(a) + l(b) = 1$.

Assume $a \neq e$ and $b \neq e$. Let $a = x_1 \dots x_l \in \widetilde{W}_l, b = y_1 \dots y_m \in \widetilde{W}_m$ and assume without loss of generality that $l \leq m$. Suppose in reduced form we have:

$$ab = x_1 \dots x_{l-r} y_{r+1} \dots y_m$$

$$ba = y_1 \dots y_{m-r} x_{r+1} \dots x_l$$

where $0 \leq r \leq l$.

(If we have r cancellations in ab we also have r cancellations in ba since $ab = ba$ so ab and ba have the same length.)

- If $r = 0$ then $x_i = y_i$ for $1 \leq i \leq l$ and so $b = au$ where $l(u) = m - l < l(b)$. Now $au = b \Rightarrow au = a^{-1}ab = a^{-1}ba = a^{-1}a u a = ua$. So by induction we see that a and u are powers of a common element. But then so is $au = b$.
- If $r = l$ then $b = a^{-1}v$ with $l(v) < l(b)$. Now $a^{-1}v = b \Rightarrow a^{-1}v = aa^{-1}b = aba^{-1} = aa^{-1}va^{-1} = va^{-1}$ (since $ab = ba \Leftrightarrow a^{-1}b = ba^{-1}$). $\Rightarrow a^{-1}$ and v are powers of a common element. But then, so is $a^{-1}v = b$.
- $0 < r < l$: See Exercise Sheet, question 5.

□

Lemma 1.11. (i) If $a, b \in F(X)$ and $a^n = b^n$ then $a = b$.

(ii) If $w \in F(X)$ then $|\{c \in F(X) : c^n = w \text{ for some } n \in \mathbb{N}\}| < \infty$.

Proof. (i) Write:

$$a = u^{-1} \hat{a} u \quad \Rightarrow l(a) = l(\hat{a}) + 2l(u)$$

$$b = v^{-1} \hat{b} v \quad \Rightarrow l(b) = l(\hat{b}) + 2l(v)$$

$$\begin{aligned}
a^n = b^n &\Rightarrow u^{-1}\hat{a}^n u = v^{-1}\hat{b}^n v \\
&\Rightarrow nl(\hat{a}) + 2l(u) = nl(\hat{b}) + 2l(v)
\end{aligned}$$

$$\begin{aligned}
a^n = b^n &\Rightarrow a^{2n} = b^{2n} \\
&\Rightarrow u^{-1}\hat{a}^{2n} u = v^{-1}\hat{b}^{2n} v \\
&\Rightarrow 2nl(\hat{a}) + 2l(u) = 2nl(\hat{b}) + 2l(v) \\
&\Rightarrow l(\hat{a}) = l(\hat{b}) \Rightarrow l(u) = l(v)
\end{aligned}$$

Therefore $u^{-1}\hat{a}^n u = v^{-1}\hat{b}^n v$ (reduced). $\Rightarrow u = v$ and $\hat{a} = \hat{b} \Rightarrow a = b$.

- (ii) Let $c^n = w$. If $w = e$ then $c = e$ by Theorem 1.8. Write $c = u^{-1}\hat{c}u$. If $w \neq e$ then $c \neq e$ and so $\hat{c} \neq e$. Now $l(w) = l(c^n) = l(u^{-1}\hat{c}u) = nl(\hat{c}) + 2l(u) \geq n$. But $l(w) \geq n$ for only finitely many n . Therefore, since w is an n^{th} power of at most one element for each fixed n by (i), the result follows. □

Lemma 1.12. *If $a^k b^h = b^h a^k$ for $a, b \in F(X)$, $h, k \in \mathbb{Z} \setminus \{0\}$ then $\exists c \in F(X)$ such that $a, b \in \langle c \rangle$ ($\Rightarrow ab = ba$ since they're both powers of a common element).*

Proof. Exercise. [Hint: Apply Lemma 1.11 (i) twice.] □

Lemma 1.13. *If $a \in F(X) \setminus \{e\}$ then $C = C_{F(X)}(a)$ is Abelian.*

Proof. Let $u, v \in C$. Then $ua = au$ and $va = av$. Assume without any loss that $u \neq e$ and $v \neq e$. By Lemma 1.10 there exist $b, d \in F(X)$ and $p, q, r, s \in \mathbb{Z} \setminus \{0\}$ such that:

$$\begin{aligned}
u &= b^p, & a &= b^q \\
v &= d^r, & a &= d^s
\end{aligned}$$

$\Rightarrow b^q d^s = d^s b^q \Rightarrow \exists c \in F(X)$ such that $b = c^h, d = c^k$ (by 1.12).

Therefore $u = c^{hp}$ and $v = c^{kr}$ commute. □

Proof of Theorem 1.9. Observe that $w^n \in C_w$ for all $n \in \mathbb{Z}$. By Theorem 1.7 it follows that C_w is infinite. Pick $d \in C_w \setminus \{e\}$ such that d has minimal length. Let $v \in C_w$. We claim that v is a power of d . Since d and v commute (by 1.13) we have $d = u^h, v = u^k$ for some $u \in F(X)$. Now $u^k \in C_w$ implies: u^k commutes with w and so u commutes with w by 1.12, that is, $u \in C_w$. Write $u = a^{-1}\hat{u}a$. Then:

$$\begin{aligned} l(d) &= l(u^h) = |h|l(\hat{u}) + 2l(a) \\ &= (|h| - 1)l(\hat{u}) + l(\hat{u}) + 2l(a) \\ &= (|h| - 1)l(\hat{u}) + l(u) \end{aligned}$$

By minimality we have $|h| = 1$ therefore $d = u^{\pm 1} \Rightarrow v = d^{\pm h}$ and we have shown that $C_w = \langle d \rangle$. □

Remark. $\langle w \rangle \leq C_{F(X)}(w)$, but equality does not always hold!

Take for example $X = \{x, y\}, w = x^4$. Here $C_w \neq \langle x^4 \rangle$.

2 Schreier's Method

Dedekind's Theorem tells us that if A is free Abelian and $B \leq A$ then B is free Abelian and $\text{rank} B \leq \text{rank} A$. In this section, we will prove that a subgroup of a free group is free. However there is no bound on the rank of a free subgroup.

Let $F = F(X)$ be the free group on X . Let $H \leq F$. We show that H is a free group.

1. The well-ordering of F

A partial ordering on a set S is a binary relation $<$ on S such that $<$ is

(01) irreflexive: $\neg(s < s) \quad (\forall s \in S)$

(02) transitive: $a < b \wedge b < c \Rightarrow a < c$

and $<$ is called a total ordering if also

(03) $(\forall s, t \in S) \quad s < t \text{ or } s = t \text{ or } t < s$

and $<$ is called a well-ordering if also

(04) any nonempty set T in S has a least element. That is, $\forall T \subseteq S : \exists t \in T$ such that $t < \hat{t} \quad \forall \hat{t} \in T \setminus \{t\}$.

Notes. 1. (04) \Rightarrow (03)

2. **Theorem.** Any set can be well-ordered.

Let $<$ be a well-ordering of $X^{\pm 1}$. Let $a = x_1 \dots x_l, b = y_1 \dots y_m \in F(X)$ where $x_i, x_j \in X^{\pm 1}$ and so that $l(a) = l$ and $l(b) = m$. Then write $a < b$ if either $l < m$ or $l = m$ and $x_r < y_r$ and $x_i = y_i$ for $1 \leq i \leq r - 1$.

Exercise. This yields a well-ordering on $F(X)$.

Example. Let $X = \{x, y\}$. Well-ordering of $X^{\pm 1}$: $x < y < x^{-1} < y^{-1}$ (Question: What is the 10th word in $F(X)$? — Answer: $e < x < y < x^{-1} < y^{-1} < xx < xy < xy^{-1} < yx < yy < \dots$)

Lemma 2.1. Let $w = x_1 \dots x_n$ be a reduced word in $X^{\pm 1}$ with $n > 1$ and let v be any element of $F = F(X)$. Then $v < x_1 \dots x_{n-1} \Rightarrow vx_n < w$.

Proof. If $l(v) < n - 1$ then $l(vx_n) < n = l(w)$ (Caution: this is the usual “less than”, not our ordering!) and $vx_n < w$ (this on the other hand *is* our well-ordering “less than”). Now suppose that $v = x_1 \dots x_{r-1} y_r \dots y_{n-1}$ where $y_r < x_r$.

If $x_n = y_{n-1}^{-1}$ then $l(vx_n) = n - 2 < l(w)$ and the result follows.

If $x_n \neq y_{n-1}^{-1}$ then $vx_n = x_1 \dots x_{r-1} y_r \dots y_{n-1} x_n < x_1 \dots x_n = w$. □

2. Schreier Transversal (1927)

We have H , our fixed subgroup of F . Let U be a right transversal for H in F . Then for any $w \in F$, $Hw \cap U$ consists of a single element that we denote \bar{w} .

Example (What is a transversal?). $C_{20} = \langle x \rangle$, $H = \langle x^5 \rangle = \{1, x^5, x^{10}, x^{15}\}$. Then the other partitions we get are Hx, Hx^2, Hx^3 and Hx^4 . Either two cosets are the same or their intersection is empty (since the partitions can be considered as equivalence classes with $a \sim b \Leftrightarrow a = b \pmod{H}$).

A *transversal* is a set of coset representatives. There are 4^5 transversals, e.g. $\{x^5, x^{11}, x^{12}, x^3, x^4\}$. Here, $\overline{x^{16}} = x^{11}$.

A subset S of F has the *Schreier property* (SP) if it contains all initial segments of all its elements, that is, $w = x_1 \dots x_n \in S \Rightarrow x_1 \dots x_{n-1} \in S$, where $l(w) \geq 1$.

A *Schreier transversal* for H in F is a transversal U with (SP). Note that this implies $e \in U$.

Lemma 2.2. *Every subgroup H of F has a Schreier transversal.*

Proof. Choose the least element of each right coset of H in F in the above well-ordering of F . Let U denote the resulting transversal. Suppose that $x_1 \dots x_{n-1} \notin U$ but $w = x_1 \dots x_n \in U$. Let v be the least element of $Hx_1 \dots x_{n-1}$.

Then $v < x_1 \dots x_{n-1}$ and this implies $vx_n < x_1 \dots x_{n-1}x_n = w$ by Lemma 2.1. But now $Hv = Hx_1 \dots Hx_{n-1} \Rightarrow Hvx_n = Hw \Rightarrow vx_n \in Hw$ and this contradicts the minimality of w in Hw . \square

Example. $X = \{x, y\}$, $F = F(X)$ ordered as above, $x < y < x^{-1} < y^{-1}$. Let H be the *normal closure* of $S = \{x^3, y^2, x^{-1}y^{-1}xy\}$ in F . Then H is the intersection of all the normal subgroups of F containing S . For example, $H \trianglelefteq F$ and $S \leq N \trianglelefteq F \Rightarrow H \trianglelefteq N$.

We show that $|F : H| = 6$.

Let $C_6 = \{e, a, a^2, a^3, a^4, a^5\} = \langle a \rangle$ and define $\theta : X \rightarrow C_6$ by $x\theta = a^2, y\theta = a^3$. Let $\theta' : F \rightarrow C_6$ be the unique extension of θ .

Then $(yx^{-1})\theta' = (y\theta')(x\theta')^{-1} = a \Rightarrow \theta'$ is onto. $x^3\theta' = y^2\theta' = x^{-1}y^{-1}xy\theta' = e \Rightarrow S \leq \ker \theta' \leq F \Rightarrow H \leq \ker \theta' \Rightarrow |F : H| = |F : \ker \theta'| \cdot |\ker \theta' : H| \geq |F : \ker \theta'| = |\text{Im } \theta'| = 6$ by the first isomorphism theorem.

On the other hand the quotient group F/H is generated by Hx and Hy and there $(Hx)^3 = (Hy)^2 = H, Hx^{-1}y^{-1}xy = H \Rightarrow HxHy = HyHx$.

(If N is a normal subgroup of G and $a \in G$, then $Na = aN, N^k = N, (Na)^k = Na^k$.

Normal subgroups make life much easier.)

$\Rightarrow F/H$ is Abelian of order $\leq 6 \Rightarrow |F : H| \leq 6 \Rightarrow |F : H| = 6$ since we already know that $|F : H| \geq 6$.

(The rearranging works like this:

$$\begin{aligned}
Hx^{-1}y^{-1}xy &= H \\
\Rightarrow x^{-1}y^{-1}Hxy &= H \\
\Rightarrow Hxy = yxH = Hyx \\
\Rightarrow H^2xy = H^2yx \\
\Rightarrow HxHy = HyHx
\end{aligned}$$

General observation: $N \trianglelefteq G$ normal, $[a, b] \in N \Leftrightarrow NaNb = NbNa$.)

The transversal $\{e, x, x^2, y, xy, x^2y\}$ has SP.

In general, take the **least-element approach**:

Take a look at the ordered elements.

$$e \ x \ y \ x^{-1} \ y^{-1} \ xx \ xy \ xy^{-1} \ yx \ yy \ yx^{-1} \dots$$

Now for each class we search for the element representing it. Clearly, $e \in H, x \in Hx, y \in Hy$. The next element is x^{-1} and it's in Hx^2 because $x^3 \in H$ iff $Hx^2 = H$, $y^{-1} \in Hy$ with a similar argument involving $y^2 \in H$. Of course the next elements $xx \in Hx^2$ and $xy \in Hxy$. Now, $Hxy^{-1} = HxHy^{-1} = HxHy = Hxy$ and $Hyx = HyHx = HxHy = Hxy$, and $Hyx^{-1} = HyHx^{-1} = HyHx^2 = Hx^2Hy = Hx^2y$ and so it completes our transversal.

Transversal: $\{e, x, y, x^{-1}, xy, yx^{-1}\}$.

3. The Schreier generators

Recall that $Hw \cap U = \bar{w}$ where U is a right Schreier transversal for H in $F = F(X)$.

Properties.

1. $\overline{\bar{w}} = \bar{w}$
2. $Hw = H\bar{w}$

3. $\bar{w} = w$ iff $w \in U$

4. $(\forall u \in U, x \in X^{\pm 1}) Hux = H\bar{u}\bar{x} \Rightarrow Hu = H\bar{u}\bar{x}x^{-1} \Rightarrow \overline{\bar{u}\bar{x}x^{-1}} = u$.

Lemma 2.3. H is generated by $A = \{ux(\bar{u}\bar{x})^{-1} | u \in U, x \in X^{\pm 1}\}$

Proof. Since $Hux = H\bar{u}\bar{x}$ we have $Hux\bar{u}\bar{x}^{-1} = H$, that is, $ux(\bar{u}\bar{x})^{-1} \in H$, so $A \subseteq H$. Now let $h \in H$ and write h as a reduced word $h = x_1 \dots x_n$ ($x_i \in X^{\pm 1}$). Define the following sequence of elements of U :

$$\begin{aligned} u_1 &= e \\ u_{i+1} &= \overline{u_i x_i} \quad (1 \leq i \leq n) \end{aligned}$$

and now put $a_i = u_i x_i u_{i+1}^{-1} = u_i x_i (\overline{u_i x_i})^{-1} \in A$ ($1 \leq i \leq n$). Then

$$\begin{aligned} a_1 a_2 \dots a_n &= (u_1 x_1 u_2^{-1})(u_2 x_2 u_3^{-1}) \dots (u_{n-1} x_{n-1} u_n^{-1})(u_n x_n u_{n+1}^{-1}) \\ &= u_1 x_1 x_2 \dots x_n u_{n+1}^{-1} = u_1 h u_{n+1}^{-1} \\ &= h u_{n+1}^{-1} \end{aligned}$$

Observe that $u_{n+1}^{-1} = h^{-1}(a_1 \dots a_n) \in H \Rightarrow u_{n+1}^{-1} \in H \cap U = \{e\} \Rightarrow h = a_1 \dots a_n$. □

Returning to the previous example we obtain:

$U \backslash X^{\pm 1}$	x	y	x^{-1}	y^{-1}
e	e	e	e	y^{-2}
x	x^3	e	e	$xy^{-2}x^{-1}$
x^{-1}	e	$x^{-1}yxy^{-1}$	x^{-3}	$x^{-1}y^{-1}xy^{-1}$
y	$xyy^{-1}x^{-1}$	y^2	e	e
xy	xyx^2y^{-1}	xy^2x^{-1}	$xyx^{-1}y^{-1}$	e
yx^{-1}	e	$yx^{-1}yx$	$yx^{-2}y^{-1}x^{-1}$	$yx^{-1}y^{-1}x$

The entries are: $ux\bar{u}\bar{x}^{-1}$, e.g. $ex\bar{e}\bar{x}^{-1} = e, Hx^3 = Hy^2 = Hx^{-1}y^{-1}xy = H, Hxy = Hyx$. (In example, for $x \in U, y^{-1} \in X^{\pm 1}$ we get $xy^{-1}(\overline{xy^{-1}})^{-1} = xy^{-1}(xy)^{-1} = xy^{-1}y^{-1}x^{-1}$.)

4. Decomposition of the set A .

Notice that in the previous table there are redundancies. In fact, $\{\text{column 1}\} \cup \{\text{column 2}\} = (\{\text{column 3}\} \cup \{\text{column 4}\})^{-1}$. Also, e appears at entry (u, x) iff $ux \in U$. It turns out that these are the only redundancies.

Let $B = \{b_1, b_2, b_3, b_4, b_5, b_6, b_7\} := \{x^3, yxy^{-1}x^{-1}, xyx^2y^{-1}, x^{-1}yxy^{-1}, y^2, xy^2x^{-1}, yx^{-1}yx\}$.

More generally put $B = \{ux\bar{u}x^{-1} : u \in U, x \in X, ux \notin U\}$.

Lemma 2.4. *The sets $\hat{B} = \{ux\bar{u}x^{-1} : u \in U, x \in X^{-1}, ux \notin U\}$ and $B^{-1} = \{b^{-1} : b \in B\}$ coincide. Moreover $A = B \cup \hat{B} \cup \{e\}$. (In other words, B generates H .)*

Proof.

$$\begin{aligned}
A \setminus \{e\} &= \{ux\bar{u}x^{-1} : u \in U, x \in X^{\pm 1}, ux\bar{u}x^{-1} \neq e\} \\
&= \{ux\bar{u}x^{-1} : u \in U, x \in X^{\pm 1}, ux \neq \bar{u}x\} \\
&= \{ux\bar{u}x^{-1} : u \in U, x \in X^{\pm 1}, ux \notin U\} \\
&= \{ux\bar{u}x^{-1} : u \in U, x \in X, ux \notin U\} \cup \{ux\bar{u}x^{-1} : u \in U, x \in X^{-1}, ux \notin U\} \\
&= B \cup \hat{B}
\end{aligned}$$

Now for $u \in U, x \in X^{\pm 1}$,

$$\begin{aligned}
(ux\bar{u}x^{-1})^{-1} &= \bar{u}xx^{-1}u^{-1} \\
&= \bar{u}xx^{-1}\overline{\bar{u}xx^{-1}}^{-1} \\
&= u'x^{-1}\overline{u'x^{-1}}^{-1}
\end{aligned}$$

where $u' = \bar{u}x \in U$. (Here we used the identity $u = \overline{\bar{u}xx^{-1}}$ which we noted earlier.)

Also:

$$\begin{aligned}
ux \notin U &\text{ iff } ux \neq \bar{u}x \\
&\text{ iff } u \neq \bar{u}xx^{-1} \\
&\text{ iff } \overline{\bar{u}xx^{-1}} \neq \bar{u}xx^{-1} \\
&\text{ iff } \bar{u}xx^{-1} \notin U \\
&\text{ iff } u'x^{-1} \notin U
\end{aligned}$$

In conclusion $\langle B \rangle = H$. Let $x \in X$ to get $B^{-1} \subseteq \hat{B}$ and let $x \in X^{-1}$ to get $\hat{B}^{-1} \subseteq B$ and result. \square

5. Freeness of the generators B .

Let $b = ux\overline{ux}^{-1}$ and $b' = vy\overline{vy}^{-1}$ be members of $B \cup B^{-1} = A \setminus \{e\}$. So $bb' = ux\overline{ux}^{-1}vy\overline{vy}^{-1}$.

Lemma 2.5. (i) ux when reduced retains the final x .

vy when reduced retains the final y .

(ii) $x\overline{ux}^{-1}$ when reduced retains the initial x .

$y\overline{vy}^{-1}$ when reduced retains the initial y .

(iii) $x\overline{ux}^{-1}v$ when reduced retains the initial x .

$\overline{ux}^{-1}vy$ when reduced retains the final y .

(iv) $bb' = e$ precisely when $v = \overline{ux}$, $x = y^{-1}$ and $u = \overline{vy}$, that is, $b' = \overline{ux}x^{-1}u^{-1}$ (i.e. b' is the free inverse of b).

Proof. (i) Let $v = y_1 \dots y_m$ be reduced where $y_i \in X^{\pm 1}$. If there is cancellation in forming vy then $y_m = y^{-1}$ and so $vy = y_1 \dots y_{m-1}$. If $m = 1$ then $vy = e$ and if $m > 1$ then $vy \in U$ (by (SP)) and in both cases $b' = vy\overline{vy}^{-1} = e$, a contradiction. Similarly ux retains the final x .

(ii) Let $\overline{ux} = x_1 \dots x_l$ ($x_i \in X^{\pm 1}$) be reduced. If x is cancelled in $x\overline{ux}^{-1} = xx_l^{-1} \dots x_1^{-1}$ then $x = x_l$. But then

$$\begin{aligned} ux &= \overline{\overline{ux}x^{-1}}x = \overline{x_1 \dots x_{l-1}}x \\ &= x_1 \dots x_{l-1}x \text{ by (SP)} \\ &= x_1 \dots x_{l-1}x_l = \overline{ux} \end{aligned}$$

$\Rightarrow b = e$. a contradiction. Similarly $y\overline{vy}^{-1}$ retains the initial y .

(iii) If $\overline{ux}^{-1}vy$ does not retain the final y then since vy retains y it follows that vy is an initial segment of \overline{ux} . But by (SP) $vy \in U$ and so $vy = \overline{vy} \Rightarrow b' = e$, a

contradiction.

If $x\overline{ux}^{-1}v$ does not retain the initial x then $(x\overline{ux}^{-1})^{-1} = \overline{ux}x^{-1}$ must be an initial segment of v . So it is in U by (SP). But then $ux = \overline{ux}x^{-1}x = \overline{ux}x^{-1}x = \overline{ux} \Rightarrow b = e$, a contradiction.

- (iv) If $bb' = e$ then x must cancel with y . For this to happen we must have $\overline{ux} = v$, then $x = y^{-1}$ and $u = \overline{vy}$. So $b' = vy\overline{vy}^{-1} = uxx^{-1}u^{-1} = b^{-1}$ is freely the inverse of b .

□

Example.

$$\begin{aligned}
z &:= \overbrace{(u_1x_1\overline{u_1x_1}^{-1})}^{b_1} \overbrace{(u_2x_2\overline{u_2x_2}^{-1})}^{b_2} \overbrace{(u_3x_3\overline{u_3x_3}^{-1})}^{b_3} \overbrace{(u_4x_4\overline{u_4x_4}^{-1})}^{b_4} \\
&= w_1 \underbrace{x_1\overline{u_1x_1}^{-1}u_2x_2\overline{u_2x_2}^{-1}}_{b_1b_2} b_3b_4 \\
&= w_1x_1w_2 \underbrace{x_2\overline{u_2x_2}^{-1}u_3x_3\overline{u_3x_3}^{-1}}_{b_2b_3} u_4x_4\overline{u_4x_4}^{-1} \\
&= w_1x_1w_2x_2w_3 \underbrace{x_3\overline{u_3x_3}^{-1}u_4x_4\overline{u_4x_4}^{-1}}_{b_3b_4} \\
&= w_1x_1w_2x_2w_3x_3w_4 \underbrace{x_4\overline{u_4x_4}^{-1}}_{b_4} \\
&= w_1x_1w_2x_2w_3x_3w_4x_4w_5
\end{aligned}$$

where $l(w_i) \geq 0$ with relation to $X^{\pm 1}$.

Note that lengths are relative: $l(z) = 4$ relative to B but $l(z) \geq 4$ relative to $X^{\pm 1}$.

IMPORTANT: When we talk of a reduced word we always mean *reduced relative to some given set of generators*.

Example. $X = \{x, y\}$, $B \leq F(X)$, $B = \langle b_i : 1 \leq i \leq 5 \rangle$ where

$$\begin{aligned}
b_1 &= x^2yx^{-2} \\
b_2 &= x^{-1}yx^3y \\
b_3 &= y^4 \\
b_4 &= y^{-1}x^{-1}y^{-1}x^{-2} \\
b_5 &= y^{-1}x
\end{aligned}$$

Here $b_1 b_2 b_2^{-1} b_3$ is NOT REDUCED relative to B or to X .

The word $b_1 b_2^2 b_3 = x^2 y x^{-2} x^{-1} y x^3 y x^{-1} y x^3 y y^4$ is REDUCED relative to B and to X .

However, the word

$$b_2 b_3 b_4 = x^{-1} y x^3 y \underbrace{y^4 y^{-1}} x^{-1} y^{-1} x^2$$

is REDUCED relative to B but NOT REDUCED relative to X .

Also:

$$b_2 b_4 b_1 b_5 = x^{-1} \underbrace{y x^3 y y^{-1} x^{-1} y^{-1} x^{-2} x^2 y x^{-2} y^{-1} x}_{\text{reduced to } x^{-1} y x^3 y y^{-1} x^{-1} y^{-1} x^{-2} x^2 y x^{-2} y^{-1} x}$$

$\Rightarrow \{b_1, \dots, b_5\}$ is *not* a free basis for B .

(Question: Is $\{b_1, \dots, b_4\}$ a free basis for B ?)

6. Proof of Theorem

Theorem 2.6 (Nielsen-Schreier Theorem). *Let F be a free group and $H \leq F$. Then H is free. Moreover if $|F : H| = g$ and $\text{rank } F = r$ are both finite then*

$$\text{rank } H = (\text{rank } F - 1)|F : H| + 1 = (r - 1)g + 1$$

Proof. Let X be a set of free generators for F . Let U be a Schreier transversal for H and let B be the set of generators for H as constructed above. It follows from Lemma 2.5 that if $w = b_1 \dots b_n$ is a word reduced relative to B then after reducing we get a reduced word in X of length at least n and so $w \neq e$. Therefore B is a free basis for H . For the last statement, observe that B is indexed by the pairs $(u, x) \in U \times X$ with $ux \notin U$ and so $\text{rank } H = |U| \times |X| - b = gr - b$ where $b = |\{(u, x, v) \in U \times X \times U : ux = v\}|$. It remains to prove $b = g - 1$. Let T denote the graph with g vertices labelled by the elements of U and having a directed edge from u to v labelled x iff $ux = v$ where $x \in X$. By (SP) every vertex of T is connected by a path to e . In particular, T is connected. Also T has no circuits since F is free on X . Therefore T is a tree with $g - 1$ edges. Since there is a bijection between edges of T , $E(T)$, and $\{(u, x, v) \in U \times X \times U : ux = v\}$ it follows that $b = g - 1$.

□

Example. Let $F = F(X)$ be the free group on $X = \{x, y\}$, N the normal closure of $\{x^5, y^2, (yx)^2\}$ in F . Then $|F/N| = 10$, $|Nx| = 5$ and $|Ny| = 2$ (see later).

Now let $H = \langle N, y \rangle \leq F(X)$. Then $N \trianglelefteq H$ and $H = N \cup Ny \Rightarrow |H : N| = 2$ so $|F : H| \cdot |H : N| = |F : N| \Rightarrow |F : H| = 5$. Thus $\text{rank } H = (2 - 1)5 + 1 = 6$.

However H is *not* a normal subgroup of F .

We obtain Schreier generators for H . As before $x < y < x^{-1} < y^{-1}$. Observe that a Schreier transversal for H in F is $U = \{e, x, x^{-1}, x^2, x^{-2}\}$. Since $|Nx| = 5$ in F/N it follows that $H, Hx, Hx^{-1}, Hx^2, Hx^{-2}$ are distinct.

If $Hx^i = Hx^j$ for $i \neq j$ it follows that $x^{j-i} \in H = N \cup Ny$, a contradiction.

Certainly $x^{j-i} \notin N$ and $x^{j-i} \in Ny \Rightarrow \underbrace{Nx^{j-i}}_{\text{order } 5} = \underbrace{Ny}_{\text{order } 2}$, a contradiction.

u	x	ux	\overline{ux}	$ux\overline{ux}^{-1}$
e	x	x	x	e
e	y	y	e	$?$
x	x	x^2	x^2	e
x	y	xy	x^{-1}	xyx
x^{-1}	x	e	e	e
x^{-1}	y	$x^{-1}y$	$?$	$?$
x^2	x	x^3	x^{-2}	x^5
x^2	y	x^2y	$?$	$?$
x^{-2}	x	x^{-1}	x^{-1}	e
x^{-2}	y	$x^{-2}y$	$?$	$?$

$$yxyx \in N \Rightarrow yxyx \in H \Rightarrow Hyxyx = H$$

$$\Rightarrow Hxyx = H \Rightarrow Hxy = Hx^{-1}$$

In general, if N is a normal subgroup then every cyclic permutation of elements and inverses belongs to N . (If $x_1x_2 \dots x_k$ is in a normal subgroup then so is $(x_i \dots x_k x_1 \dots x_{i-1})^{\pm 1}$.) For example, $yxyx \in N$

$$\Rightarrow Nyxy = Nx^{-1}$$

$$\Rightarrow (Nyxy)^2 = (Nx^{-1})^2$$

$$\Rightarrow Nyxy^2xy = Nx^{-2}$$

$Nyx^2y = Nx^{-2}$ since N is normal. Therefore $yx^2yx^2 \in N \leq H \Rightarrow Hyx^2yx^2 = H \Rightarrow Hx^2yx^2 = H \Rightarrow Hx^2y = Hx^{-2} \Rightarrow \overline{x^2y} = x^{-2}$.

3 Presentations

Let X be a set, $F = F(X)$ the free group on X , $R \subseteq F$, N the normal closure of R in F (denoted by \overline{R} or \overline{R}^F). Put $G \cong F/N$.

When we have this situation we write

$$G = \langle X | R \rangle$$

and call this a *presentation* of the group G . The elements of X are called *generators*, and the elements of R are called *defining relators*. A group G is said to be *finitely presented* if $G = \langle X | R \rangle$ where $|X| < \infty$ and $|R| < \infty$.

IMPORTANT: $G = \langle X | R \rangle$. The elements of G are cosets Nw of N in F where $w \in F(X)$. However we often write w for Nw . Thus “ $w = 1$ in G ” iff $w \in N$ iff $N = Nw$. $G = \langle Nx : x \in X \rangle$ but we usually use $G = \langle X \rangle$ to mean this.

The identity in G is denoted by: $1, e, 1_G, e_g$.

Exercise. Let $g \in F(X)$. Show that $g \in N = \overline{R}$ iff $g = \prod_{i=1}^k h_i^{-1} r_i^{\varepsilon_i} h_i$ where $h_i \in F(X), r_i \in R, \varepsilon_i = \pm 1$.

Notation: $\langle x, y | \underbrace{x^2y^{-2}}_{\text{relator}} \rangle = \langle x, y | \underbrace{x^2y^{-2} = 1}_{\text{relation}} \rangle = \langle x, y | \underbrace{x^2 = y^2}_{\text{relation}} \rangle$

Example. $F(X) = \langle X | \ \rangle$ is the free group on X .

$G = \langle X | X \rangle$ is the trivial group.

If $G = \langle x, y | x^3, y^2, x^{-1}y^{-1}xy \rangle = \langle x, y | x^3 = y^2 = 1, xy = yx \rangle$ then (we get an Abelian group since the two generators commute and) $G \cong C_3 \times C_2 = C_6$, the cyclic group of order 6.

Example. Let $G = \langle x | x^n \rangle$ where $n \geq 1$. Then $g = 1$ in G iff $g \in \{\overline{x^n}\}$ iff $g = \prod_{i=1}^k w_i x^{\pm n} w_i$ where $w_i \in F(\{x\})$.

$\Rightarrow g = x^{qn}$ for some $q \in \mathbb{Z}$.

It follows that the elements of G are $1, x, x^2, \dots, x^{n-1}$.

$\Rightarrow G \cong C_n$.

Moreover every finite cyclic group is a homomorphic image of the infinite cyclic group $\mathbb{Z} = \langle x \mid \rangle$. The kernel is again cyclic and is the normal closure of x^n for some $n \geq 1$.

Cyclic groups: $\mathbb{Z} = \langle x \mid \rangle, C_n = \langle x \mid x^n \rangle, n \geq 1$.

Theorem 3.1. *Every group has a presentation and every finite group can be finitely presented.*

Proof. Let G be any group and $X \subseteq G$ be a set of generators for G . Then $G = \langle x \mid \ker \theta' \rangle$ where $\theta' : F(X) \rightarrow G$ is the unique homomorphism extending $\iota : X \rightarrow G$. If G is finite, $|G| = l < \infty$, say, then so is X , $|X| = r$, say. Then $\ker \theta'$ is generated by a set B of cardinality $(r - 1)l + 1$ by Nielsen-Schreier.

Since $\langle B \rangle = \ker \theta' \trianglelefteq F(X)$ it follows that:

$\bar{B} = \langle B \rangle$ (since $\bar{B} \subseteq \langle B \rangle$ by definition of normal closure but $\langle B \rangle \subseteq \bar{B}$ because it's the smallest subgroup containing B).

$\Rightarrow G = \langle X \mid B \rangle$, a finite presentation. □

Remarks. 1. Every group has infinitely many presentations.

(For example, $\langle x \mid B \rangle = \langle x, y \mid B, y = 1 \rangle$ and so on.)

2. Some infinite groups can be finitely presented. (Uncountable groups can't.)

3. If $G = \langle X \mid K \rangle$ where $K \trianglelefteq F(X)$ and $\langle S \rangle = K$ then $G = \langle X \mid S \rangle$.

Lemma 3.2. *If F, G, H are groups and $\nu : F \rightarrow G, \alpha : F \rightarrow H$ are homomorphisms such that*

(i) $\text{Im } \nu = G$

(ii) $\ker \nu \subseteq \ker \alpha$

then there exists a homomorphism $\alpha' : G \rightarrow H$ such that $\nu\alpha' = \alpha$.

$$\begin{array}{ccc}
 F & \xrightarrow{\alpha} & H \\
 \searrow \nu & & \nearrow \alpha' \\
 & G &
 \end{array}
 \quad \text{“}\alpha \text{ factors through } G\text{”}$$

Proof. Given $g \in G$, (i) allows us to pick $f \in F$ such that $f\nu = g$. Define $g\alpha' := f\alpha$.

WELL-DEFINED: If $f\nu = f'\nu = g$ then $f^{-1}f' \in \ker \nu \subseteq \ker \alpha$.

$\Rightarrow f\alpha = f'\alpha$.

COMMUTING: $f(\nu\alpha') = (f\nu)\alpha' = g\alpha' = f\alpha$

HOMOMORPHISM: Let $f\nu = g$ and $f^*\nu = g^*$ so that $g^*\alpha' = f^*\alpha$.

Then $(gg^*)\alpha' = (f\nu f^*\nu)\alpha' \stackrel{\nu \text{ hom.}}{=} (ff^*)\nu\alpha' = (ff^*)\alpha \stackrel{\alpha \text{ hom.}}{=} f\alpha f^*\alpha = g\alpha' g^*\alpha'$. \square

Theorem 3.3 (von Dyck). *If $G = \langle X|R \rangle$ and $H = \langle X|S \rangle$ where $R \subseteq S \subseteq G(X)$ then \exists epimorphism $\phi : G \rightarrow H$ fixing X elementwise ($\forall x \in X$) and such that $\ker \phi = \overline{S \setminus R}$. Conversely every quotient group of $G = \langle X|R \rangle$ has a presentation $\langle X|S \rangle$ where $R \subseteq S$.*

Proof. Let $\nu : F(X) \rightarrow G$ and $\alpha : F(X) \rightarrow H$ denote the natural homomorphisms ($w \xrightarrow{\nu} \overline{R}w, w \xrightarrow{\alpha} \overline{S}w$). Since ν is onto and $\ker \nu = \overline{R} \subseteq \overline{S} = \ker \alpha$ we get $\alpha' : G \rightarrow H$ such that $\nu\alpha' = \alpha$.

$$\begin{array}{ccc}
 F & \xrightarrow{\alpha} & H \\
 \searrow \nu & & \nearrow \alpha' = \phi \\
 & G &
 \end{array}$$

Since ν and α fix $x \in X$, so does α' . Moreover α' is onto since $\nu\alpha' = \alpha$ which is onto; and $\ker \alpha' = (\ker \alpha)\nu$. To see this let $w \in \ker \alpha'$. Then $w \in G$ and so there exists $f \in F(X)$ such that $f\nu = w \Rightarrow f\nu\alpha' = w\alpha' = e_H \Rightarrow f\alpha = e_H \Rightarrow f \in \ker \alpha \Rightarrow w \in (\ker \alpha)\nu$.

Conversely if $u \in (\ker \alpha)\nu$ then $u = f\nu$ where $f\alpha = e_H$. But $u = f\nu \Rightarrow u\alpha' = f\nu\alpha' \Rightarrow u\alpha' = f\alpha = e_H \Rightarrow u \in \ker \alpha'$.

But $(\ker \alpha)\nu = \overline{S}\nu = \overline{S \setminus R}$ as required.

For the converse: If H is a quotient group of G let θ be the composite of the natural maps $F(X) \rightarrow G \rightarrow H$ so that $\ker \theta \supseteq R$ and $H = \langle X | \ker \theta \rangle$. \square

Remark. This theorem says that “adding relators to a presentation for G ” is the same as “taking quotients of G ”.

Example. $C_6 = \langle x | x^6 \rangle, H = \langle x | x^6, x^4 \rangle$.

$(x^6 = 1, x^4 = 1 \Rightarrow x^2 = 1)$. Or: $C_6 = \langle x \rangle, C_3 = \langle x^4 \rangle, C_6/C_3$.

Then: $H \cong C_2$.

Theorem 3.4 (Substitution Test). *Suppose we are given a presentation $G = \langle X | R \rangle$, a group H and a mapping $\theta : X \rightarrow H$. Then θ extends to a homomorphism $\theta'' : G \rightarrow H$ iff $(\forall x \in X, \forall r \in R)$ the result of substituting $x\theta$ for x in r yields the identity in H .*

Proof. Consider the commutative diagram where ι_1, ι_2 are inclusions and $\nu : F(X) \rightarrow G$ is the natural map ($w \xrightarrow{\nu} \overline{R}w$). Let $\theta' : F(X) \rightarrow H$ extend θ .

$$\begin{array}{ccccc}
 & & R & & \\
 & & \downarrow \iota_2 & & \\
 X & \xrightarrow{\iota_1} & F(X) & \xrightarrow{\nu} & G & \quad x \longmapsto x \longmapsto x\overline{R} \\
 & \searrow \theta & \downarrow \theta' & \swarrow \theta'' & \\
 & & H & &
 \end{array}$$

(\Leftarrow): The substitution condition can be *rephrased* as $R \subseteq \ker \theta' \trianglelefteq F(X)$. Now $\ker \nu = \overline{R} \subseteq \overline{\ker \theta'} = \ker \theta''$. Now apply (3.2) to get $\theta'' : G \rightarrow H$. Observe that $\theta = \iota_1 \theta' = \iota_1 \nu \theta'' \Rightarrow \theta''$ extends θ .

(\Rightarrow): For the converse the existence of such a θ'' entails that $R \subseteq \overline{R} = \ker \nu \subseteq \ker(\nu \theta'') = \ker \theta'$. \square

NOTE: θ'' is onto iff $\langle X\theta \rangle = H$.

Example. $G = \langle a, b, c | a^2 b^2 a^{-2} b^{-1} c^{-1} b^{-1} c \rangle$,

$H = \langle x, y, z | [x, y], [y, z], [z, x] \rangle$

$\theta : \{a, b, c\} \rightarrow H, \quad a\theta = x, \quad b\theta = y, \quad c\theta = z$

Check: $x^2y^2x^{-2}y^{-1}z^{-1}y^{-1}z \stackrel{\text{group Abelian}}{=} x^{2-2}y^{2-1-1}z^{-1+1} = 1.$

$\Rightarrow \theta$ extends to a homomorphism $\theta'' : G \rightarrow H, a\theta'' = x, b\theta'' = y, c\theta'' = z.$

Theorem 3.5. *If $G = \langle X|R \rangle$ and $H = \langle Y|S \rangle$ then $G \times H = \langle X, Y|R, S, [X, Y] \rangle$ where $[X, Y] = \{[x, y] : x \in X, y \in Y\}$*

Proof. Let $D = \langle X, Y|R, S, [X, Y] \rangle.$ We must show that $D \cong G \times H.$ The inclusions $X \hookrightarrow D, Y \hookrightarrow D$ induce homomorphisms $\theta : G \rightarrow D, \phi : H \rightarrow D$ by substitution test. Define $\alpha : G \times H \rightarrow D$ by $(g, h)\alpha = g\theta h\phi.$ Notice that $(x, 1)\alpha = x\theta 1\phi = x$ and $(1, y)\alpha = y.$ Moreover $(g_1, h_1)(g_2, h_2)\alpha = (g_1g_2h_1h_2)\alpha = (g_1g_2)\theta(h_1h_2)\phi = g_2\theta g_2\theta h_1\phi h_2\phi = g_1\theta h_1\phi g_2\theta h_2\phi$ (since $[X, Y]$ are relators in D) $= (g_1, h_1)\alpha(g_2, h_2)\alpha \Rightarrow \alpha \in \text{Hom}(G \times H, D).$

On the other hand the mapping of $X \cup Y$ into $G \times H$ sending x to $(x, 1)$ and y to $(1, y)$ extends by the substitution test to a homomorphism $\beta : D \rightarrow G \times H.$ Since $[x, y]$ in D rewrites to $[(x, 1), (1, y)]$ in $G \times H$ and $(x, 1)(1, y) = (x, y) = (1, y)(x, 1).$ Finally $\alpha\beta : G \times H \rightarrow G \times H$ sends $(x, 1)$ to $(x, 1)\alpha\beta = x\beta = (x, 1)$ and sends $(1, y)$ to $(1, y)$ and $x\beta\alpha = x, y\beta\alpha = y.$ It follows that α and β are mutually inverse isomorphisms. \square

Example. $C_3 = \langle x \rangle, C_4 = \langle y \rangle.$

$$\begin{aligned} C_3 \times C_4 &= \langle x, y|x^3, y^4, [x, y] \rangle \\ C_2 \times C_5 \times C_{10} &= \langle x, y, z|x^2, y^5, z^{10}, [x, y], [y, z], [z, x] \rangle \\ C_2 \times C_2 \times C_2 &= \langle a, b, c|a^2, b^2, c^2, [a, b], [b, c], [c, a] \rangle \\ &= \langle a, b, c|a^2, b^2, c^2, (ab)^2, (bc)^2, (ca)^2 \rangle \end{aligned}$$

Recall that the *commutator subgroup* or *derived subgroup* G' or $[G, G]$ of a given group G is the subgroup of G generated by $\{[g, h] : g, h \in G\}.$

Remarks. (1) $G' \trianglelefteq G$

(2) $G_{ab} := G/G'$ is Abelian.

(3) G/N is Abelian iff $G' \subseteq N, N$ normal subgroup.

(4) In General, $G' \neq \{[g, h] : g, h \in G\}.$ (But the equality often holds.)

Theorem 3.6. *If $G = \langle X|R \rangle$ then $G_{ab} = \langle X|R, [X, X] \rangle$ where $[X, X] = \{[x, y] : x, y \in X\}$.*

Proof. Let $D = \langle X|R, [X, X] \rangle$. We must prove that $D \cong G_{ab}$. By von Dyck there exists an epimorphism $\theta : G \rightarrow D$ with $\ker \theta = \overline{[X, X]}$. It remains to show that $G' = \overline{[X, X]}$. Since the generators of $D \cong G/\ker \theta$ is Abelian it follows that $G' \subseteq \ker \theta$. On the other hand $[X, X] \subseteq G \Rightarrow \overline{[X, X]} \subseteq \overline{G'} = G'$ and so $G' = \overline{[X, X]}$. \square

Example. 1. $G = \langle x, y, z | x^2yz^{-1}yz^{-1} \rangle$

$$G_{ab} = \langle x, y, z | [x, y], [y, z], [z, x], x^2y^2z^{-2} \rangle.$$

2. $G = \langle x, y | xyx^{-2}yxy^{-2} \rangle$

$$G_{ab} = \langle x, y | [x, y] \rangle \text{ infinite}$$

3. $G = \langle x, y | x^4y^{-2}x^{-2}y, y^3x^{-1}y^{-2}x \rangle$

$$G_{ab} = \langle x, y | [x, y], x, y \rangle \text{ trivial}$$

4. $G = \langle x, y, z, t | x^2y^2zy^{-2}, x^3t^4x^{-2}t^{-1}, txyt^{-1}x^{-5}, yt^2y^{-1}t^{-1} \rangle$

$$G_{ab} = \langle x, y, z, t | [X, X], x^2z, xt^3, x^{-4}y, t \rangle$$

$$[= \langle x, y, z | [X, X], x^2z, x, yx^{-4} \rangle = \langle y, z | [y, z], z, y \rangle = \{1\}].$$

Since $G \twoheadrightarrow G_{ab}$ it follows that if G_{ab} is infinite G is also infinite. We describe the so-called **Tietze transformations** which allow us to pass from one presentation of a group G to another.

Lemma 3.7. *Let $F = \langle X | \rangle, G = \langle X|R \rangle$ and suppose that $w \in F$ and $r \in \overline{R} \setminus R \subseteq F$. Let y be a symbol not in X . Then both of the inclusions*

$$\alpha_1 : X \rightarrow \langle X|R, r \rangle$$

$$\beta_1 : X \rightarrow \langle X, y|R, y^{-1}w \rangle$$

extend to isomorphisms with domain G .

Proof. The fact that these mappings extend to homomorphisms with domain G is immediate from the substitution test. Now observe that the maps $\alpha_2 : X \rightarrow \langle X|R \rangle$ and $\beta_2 : X \rightarrow \langle X|R \rangle$ which fix elementwise and where $y\beta_2 = w$ extend, again by the substitution test, to homomorphisms.

Now $\hat{\alpha}_1\hat{\alpha}_2$ and $\hat{\beta}_1\hat{\beta}_2$ (where $\hat{}$ denotes extension) fix the generating set X , and so both equal id_G . Therefore $\hat{\alpha}_i, \hat{\beta}_i$ are isomorphisms. \square

NOTE 1.

We say that $r \in \overline{R} \setminus R$ is a *consequence* of the relators R .

NOTE 2.

The four isomorphisms of 3.7 are the so-called **Tietze transformations**:

R^+ : adjoining a relator: $\langle X|R \rangle \rightarrow \langle X|R, r \rangle$ where $r \in \overline{R} \setminus R$

R^- : removing a relator: $\langle X|R \rangle \rightarrow \langle X|R - \{r'\} \rangle$ where $r' \in R \cap \overline{R} \setminus \{r'\}$

X^+ : adjoining a generator: $\langle X|R \rangle \rightarrow \langle X, y|R, y^{-1}w \rangle$ where $y \notin X, w \in F$.

X^- : removing a generator: $\langle X|R \rangle \rightarrow \langle X - \{y\}|R - \{y^{-1}w\} \rangle$ where $y \in X, w \in F(X \setminus \{y\})$ and $y^{-1}w$ is the only relator of R that involves y .

Example.

$$\begin{aligned}
R^+ &: \langle x, y, z | z^{-1}xyz = y, y^3 = 1 \rangle \\
&= \langle x, y, z | z^{-1}xyz = y, y^3 = 1, (xy)^3 = 1 \rangle \\
R^- &: \langle a, b, c | a^4, a^8, abc \rangle \\
&= \langle a, b, c | a^4, abc \rangle \\
X^+ &: \langle x, y, z | x^2 = y^2 = z^4 = 1, (xyz)^4 = 1 \rangle \\
&= \langle x, y, z, t | y^2 = z^4 = 1, (xyz)^4 = 1, t = xyz^2xyz \rangle \\
&\text{(or choose any other word in } x, y, z \text{)} \\
X^- &: \langle x, y, z, t | t = z^3x, y^4 = 1 \rangle \\
&= \langle x, y, z | y^4 = 1 \rangle
\end{aligned}$$

In practice we do many transformations at the same time.

$$\begin{aligned}
& \langle x, y | x^l, y^m, (xy)^n \rangle \\
&= \langle x, y, a | x^l, y^m, (xy)^n, a^{-1}xy \rangle \\
&= \langle x, y, a | x^l, y^m, a^n, a^{-1}xy \rangle \\
&= \langle y, a | (ay^{-1})^l, y^m, a^n \rangle \\
&= \langle y, a, b | (ay^{-1})^l, y^m, a^n, b^{-1}y^{-1} \rangle \\
&= \langle a, b | (ab)^l, b^m, a^n \rangle
\end{aligned}$$

Example.

$$\begin{aligned}
& \langle x, y, z | x = yzy^{-1}, y = zxz^{-1}, z = xyx^{-1} \rangle \\
&= \langle x, z | x = yxyx^{-1}y^{-1}, y = xyx^{-1}xy^{-1}x^{-1} \rangle \\
&= \langle x, y | xyx = yxy \rangle \\
&= \langle x, y, a | ax = ya, a = xy \rangle \\
&= \langle x, a | ax = x^{-1}a^2 \rangle \\
&= \langle x, a, b | ax = x^{-1}a^2, b = ax \rangle \\
&= \langle a, b | b^2 = a^3 \rangle
\end{aligned}$$

Remark. Let $G = \langle Y | S \rangle$ and suppose that $s \in S$ is of the form $s_1 y^{\pm 1} s_2$ where $y \in Y$ and y is *not* included in either s_1 or s_2 . Then $y = (s_1^{-1} s_2^{-1})^{\pm 1}$, a word not involving y . So $G = \langle Y - \{y\} | \widehat{S} \rangle$ where \widehat{S} consists of all relators in $S - \{s\}$ in which y is replaced by $(s_1^{-1} s_2^{-1})^{\pm 1}$ wherever it appears.

Example. $\langle x, y, z, t | t^3 y t x^{-1} z, z^2 y t y, x^3 y t z^2, x^5 \rangle$

$$t^3 y t x^{-1} z = 1 \Rightarrow y = t^{-3} z^{-1} x t^{-1}$$

$$G = \langle x, z, t | z^2 (t^{-3} z^{-1} x t^{-1}) t (t^{-3} z^{-1} x t^{-1}), x^3 (t^{-3} z^{-1} x t^{-1}), x^5 \rangle$$

Theorem 3.8. *Given two presentations of the same group, one can be obtained from the other by a finite sequence of Tietze transformations.*

Proof. Suppose $G = \langle x | R(x) = 1 \rangle = \langle Y | S(y) = 1 \rangle$. Let $X = X(Y)$ and $Y = Y(X)$ be two systems of equations expressing the X in terms of Y and the Y in terms of

X . We can do this since $G = \langle X \rangle = \langle Y \rangle$.

Now

$$\langle X | R(X) = 1 \rangle$$

$$X^+ : = \langle X, Y | R(X) = 1, Y = Y(X) \rangle$$

$$R^+ : = \langle X, Y | R(X) = 1, Y = Y(X), X = X(Y) \rangle$$

$$R^+ : = \langle X, Y | R(X) = 1, Y = Y(X), X = X(Y), R(X(Y)) = 1 \rangle$$

$$R^- : = \langle X, Y | Y = Y(X), X = X(Y), R(X(Y)) = 1 \rangle$$

$$R^+ : = \langle X, Y | Y = Y(X), X = X(Y), R(X(Y)) = 1, Y = Y(X(Y)) \rangle$$

$$R^- : = \langle X, Y | X = X(Y), R(X(Y)) = 1, Y = Y(X(Y)) \rangle$$

$$X^- : = \langle Y | R(X(Y)) = 1, Y = Y(X(Y)) \rangle$$

$$R^+ : = \langle Y | R(X(Y)) = 1, Y = Y(X(Y)), S(Y) = 1 \rangle$$

$$= \langle Y | S(Y) = 1 \rangle$$

□

Example. If $A = \langle x | x^{12}, x^{30} \rangle$ then $|A| = 6 = \gcd(12, 30)$ (If $x^{12} = 1$ then $x^{24} = 1$. If $x^{24} = x^{30} = 1$ it follows that $x^6 = 1$. $\Rightarrow A = \langle x | x^{12}, x^{30}, x^6 \rangle = \langle x | x^6 \rangle$.)

Example. $C_m \times C_n \cong C_{mn}$ iff $\gcd(m, n) = 1$.

(\Rightarrow): Let p be prime, $p|m$ and $p|n$. Then $C_m \times C_n = \langle a \rangle \times \langle b \rangle$ contains the subgroup $\langle a^{m/p} \rangle \times \langle b^{n/p} \rangle \cong C_p \times C_p$ a non-cyclic group (since every element has order p). This contradicts our assumption that $C_m \times C_n$ is cyclic (all subgroups of a cyclic group are cyclic).

($C_p = \langle x \rangle, C_p = \langle y \rangle \Rightarrow (x, y)^m = (x^m, y^m) \Rightarrow |(x, y)| \leq p < p^2$. If $|G| = n$ and $g \in G$ then $g^n = 1$ so here either a^p or b^p equals 1.)

(\Leftarrow): $(m, n) = 1 \iff \exists u, v \in \mathbb{Z}$ s.t. $um + vn = 1$.

$$\begin{aligned}
C_{mn} &= \langle a | a^{mn} = 1 \rangle \\
&= \langle a, x, y | a^{mn} = 1, x = a^m, y = a^n \rangle \\
&= \langle a, x, y | a^{mn} = 1, x = a^m, y = a^n, [x, y] = 1, x^n = 1, y^m = 1, x^u y^v = a^{um+vn} = a \rangle \\
&= \langle x, y | (x^u y^v)^{mn} = 1, x = (x^u y^v)^m, y = (x^u y^v)^n, [x, y] = x^n = y^m = 1 \rangle \\
&= \langle x, y | (x^n)^{um} (y^m)^{vn} = 1, x = x^{um} y^{vm}, y = x^{un} y^{vn}, [x, y] = x^n = y^m = 1 \rangle \\
&= \langle x, y | x = x^{um}, y = y^{vn}, [x, y] = x^n = y^m = 1 \rangle
\end{aligned}$$

But $x^n = 1 \Rightarrow x^{vn} = 1 \Rightarrow x^{1-um} = 1 \Rightarrow x = x^{um}$ and $y^m = 1 \Rightarrow y = y^{vn}$.

So we get $C_{mn} = \langle x, y | x^n = y^m = [x, y] = 1 \rangle = C_m \times C_n$. \square

Strategy:

abstract presentations $\xleftarrow{\text{subst. test}}$ concrete groups

Example (The dihedral group). Let D_{2n} denote the dihedral group of order $2n$, the $2n$ symmetries of the regular n -gon. This n rotations and n reflections. Let $H = \langle x, y | x^n = y^2 = 1, y^{-1}xy = x^{-1} \rangle$. Define a mapping $\theta : \{x, y\} \rightarrow D_{2n}$ by $x\theta =$ rotation of order n and $y\theta =$ any reflection. Then $H = \langle x\theta, y\theta \rangle$ and $(x\theta)^n = 1, (y\theta)^2 = 1$, and $(y\theta)^{-1}(x\theta)(y\theta) = (x\theta)^{-1}$. Therefore θ extends to a homomorphism $\hat{\theta} : H \rightarrow D_{2n}$ by the substitution test. Now $\hat{\theta}$ is onto so it remains to show that $\hat{\theta}$ is injective.

Example (The quaternions). Let \mathbb{H} denote the subgroup of $\text{GL}(2, \mathbb{C})$ generated by

$$A = \begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ where } \omega = e^{i\pi/n}$$

Claim: $\mathbb{H} \cong Q_{2n} = \langle x, y | x^n = y^2, x^{2n} = 1, y^{-1}xy = x^{-1} \rangle$

Note that $B \notin \langle A \rangle \Rightarrow |\mathbb{H}| \geq 4n$

$$H = \{I, A \dots A^{2n-1}, B, BA \dots BA^{2n-1}\}.$$

Define $\theta : \{x, y\} \rightarrow \langle A, B \rangle$ by $x\theta = A, y\theta = B$.

Since $A^n = B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, A^{2n} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A^{-1}BA = B^{-1}$, we get $\hat{\theta} : Q_{2n} \xrightarrow{\text{onto}} \mathbb{H}$

extending θ by the substitution test. It remains to show that $|Q_{2n}| \leq 4n$.

Now $y^{-1}xy = x^{-1} \in \langle x \rangle, yxy = x^{-1} \in \langle x \rangle \implies \langle x \rangle \trianglelefteq Q_{2n}$.

But $Q_{2n}/\langle x \rangle = \langle y | y^2 = 1 \rangle$.

$$\implies |Q_{2n}| = |\langle y | y^2 = 1 \rangle| |\langle x \rangle| \leq 2 \cdot 2n = 4n.$$

Note that $Q_{2n} = \langle x, y | y^n = y^2, y^{-1}xy = x^{-1} \rangle$ since $y^{-1}xy = x^{-1} \implies (y^{-1}xy)^n = x^{-n} \implies y^{-1}x^ny = x^{-n} \implies x^n = x^{-n}$.

Example (Groups of order 8). Let G be a group of order 8 and let $x \in G$ have maximal order so that $|x| \in \{2, 4, 8\}$.

If $|x| = 8$ then $G \cong C_8$.

If $|x| = 2$ then $G \cong C_2 \times C_2 \times C_2$.

If $|x| = 4$ let $y \in G \setminus \langle x \rangle$. Then $y^{-1}xy \in \langle x \rangle \trianglelefteq G$ so $y^{-1}xy \in \{e, x, x^2, x^3\}$. Clearly $y^{-1}xy \notin \{e, x^2\}$. If $y^{-1}xy = x$ then $G \cong C_2 \times C_4$ so let $y^{-1}xy = x^3$. If $y^2 = 1$ then we get D_8 . If $y^2 \neq 1$ then $y^2 \in \langle x \rangle$ (otherwise we could write down more than 8 distinct elements). This forces $y^2 = x^2$ and $G \cong Q_4$.

Thus the groups of order 8 are:

$$\langle x | x^8 \rangle, \langle x, y | x^4, y^2, [x, y] \rangle, \langle x, y, z | x^2, y^2, z^2, [x, y], [y, z], [z, x] \rangle,$$

$$D_8 = \langle a, b | a^4 = b^2 = (ab)^2 = 1 \rangle, Q_4 = \langle a, b | a^2 = b^2, b^{-1}ab = a^{-1} \rangle$$

Example (The Heisenberg group).

H is the group of matrices of the form $\begin{pmatrix} 1 & r & s \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}, r, s, t \in \mathbb{Z}$.

$$\text{Put } A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, C = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\text{Then } A^k = \begin{pmatrix} 1 & k & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, B^l = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & l \\ 0 & 0 & 1 \end{pmatrix}, C^m = \begin{pmatrix} 1 & 0 & m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\text{and } A^k \cdot B^l \cdot C^m = \begin{pmatrix} 1 & k & m + kl \\ 0 & 1 & l \\ 0 & 0 & 1 \end{pmatrix}.$$

$$\implies H = \langle A, B, C \rangle.$$

Let $G = \langle a, b, c \mid [a, b] = c, [c, a] = 1, [c, b] = 1 \rangle$ and define $\theta : \{a, b, c\} \rightarrow H$ by

$a\theta = A, b\theta = B, c\theta = C$. Now $[A, B] = C, [C, A] = [C, B] = 1$. So θ extends to $\hat{\theta} \in \text{Hom}(G, H)$ by the substitution test. Clearly $\hat{\theta}$ is surjective.

Now let $L = \{n = a^k b^l c^m : k, l, m \in \mathbb{Z}\} \subseteq G$. Observe that $e_G \in L$ ($k = l = m = 0$).

We claim that $L_g \subseteq L$ ($\forall g \in G$). It would then follow that $L = G$.

To prove the claim it is enough to consider $a^{\pm 1}, b^{\pm 1}$ and $c^{\pm 1}$ and show that each of

$$ua, ua^{-1}, ub, ub^{-1}, uc, uc^{-1}$$

is in L .

Now

$$uc^{\pm 1} = a^k b^l c^{m \pm 1} \in L$$

$$ub^{\pm 1} = a^k b^l c^m b^{\pm 1} = a^k b^{l \pm 1} c^m \in L \quad ([c, b] = 1)$$

Observe that

$$\begin{aligned} [a, b] = c &\Leftrightarrow a^{-1} b^{-1} a b = c \\ &\Leftrightarrow a^{-1} b^{-1} a = c b^{-1} \\ &\Leftrightarrow a^{-1} b a = b c^{-1} \end{aligned}$$

and so

$$a^{-1} b^l a = (b c^{-1})^l = b^l c^{-l}$$

Similarly $ab^l a^{-1} = b^l c^l$.

Therefore

$$\begin{aligned} ua^{\pm 1} &= a^k b^l c^m a^{\pm 1} \\ &= a^k b^l a^{\pm 1} c^m \quad ([c, a] = 1) \\ &= a^k a^{\pm 1} b^l c^{\pm 1} c^m \in L \end{aligned}$$

But now distinct members of L are sent by $\hat{\theta}$ to distinct matrices in H which means $\hat{\theta}$ is injective, so $G \cong H$.

NOTE. $a^k b^l c^m$ is a *normal form* for G .

Symmetric groups.

Let S_n denote the symmetric group of degree n so that $|S_n| = n!$ and $S_n = \langle (i, i+1) : 1 \leq i \leq n \rangle$.

Put

$$\begin{aligned} G_n &= \langle x_1, \dots, x_n | R, S, T \rangle \\ R &= \{x_i^2 = 1 : 1 \leq i \leq n-1\} \\ S &= \{(x_i x_{i+1})^3 = 1 : 1 \leq i \leq n-2\} \\ T &= \{[x_i, x_j] = 1 : 1 \leq i < j-1 < n-1\} \end{aligned}$$

Claim: $S_n \cong G_n$.

Define $\theta : \{x_1, \dots, x_{n-1}\} \rightarrow S_n$ by $x_i \theta = (i, i+1)$. Then θ extends to a homomorphism $\hat{\theta} : G_n \rightarrow S_n$ by the substitution test and $\hat{\theta}$ is injective so $|G_n| \geq |S_n| = n!$. We show by induction on n that $|G_n| \leq n!$ and so $\hat{\theta}$ is an isomorphism.

Proceed by induction on n .

If $n = 1$ then $G_n = \{e\}$ and $|G_{n-1}| \leq (n-1)!$. Let H be the subgroup of G_n generated by x_1, \dots, x_{n-2} and define

$$\begin{aligned} y_0 &= 1 \\ y_i &= y_{n-1} \dots y_{n-i} \end{aligned}$$

Consider the subset $A = \{hy_i : h \in H, 0 \leq i \leq n-1\}$ of G_n . Observe that $H \leq A$ and $e_G \in A$.

We show that $hy_i x_j \in A$.

There are six possibilities:

- (i) $i = 0, j < n-1$: $hy_i x_j = hx_j \in H \subseteq A$
- (ii) $i = 0, j = n-1$: $hy_i x_j = hx_{n-1} = hy_i \in A$
- (iii) $i > 0, j > n-i$: exercise
- (iv) $i > 0, j = n-i$: $hy_i x_j = hx_{n-1} \dots x_{n-i} x_{n-i} \stackrel{(R)}{=} hx_{n-1} \dots x_{n-i+1} = hy_{i-1} \in A$
- (v) $i > 0, j = n-i-1$: $hy_i x_j = hy_{i+1} \in A$
- (vi) $i > 0, j < n-i-1$: $hy_i x_j \stackrel{(T)}{=} (hx_j)y_i = h'y_i \in A$.

It follows that $A = G_n$ and $|G_n| = |A| \leq n \times |H|$. Now since the relations in G_n that involve x_1, \dots, x_{n-2} are precisely those in G_{n-1} we get the homomorphism $\phi : G_{n-1} \rightarrow G_n$ where $x_i \phi = x_i$ ($1 \leq i \leq n-2$).

Now $\text{Im } \phi = H \Rightarrow (n-1)! \geq |G_{n-1}|$ (induction) $\geq |\text{Im } \phi| = |H|$.
 $\Rightarrow n! = n(n-1)! \geq n \cdot |H| \geq |G_n|$.

Example (The rationals $\langle \mathbb{Q}, + \rangle$). If $\frac{a}{b} \in \mathbb{Q}$ then $\frac{a}{b} = \frac{a(b-1)!}{b} = \underbrace{\frac{1}{b!} + \frac{1}{b!} + \dots + \frac{1}{b!}}_{a(b-1)! \text{ times}}$

Hence $\langle \mathbb{Q}, + \rangle = \langle \frac{1}{n!} : n \geq 1 \rangle$

Put $G = \langle t_n (n \geq 1) | t_n^n = t_{n-1} \ (n \geq 2) \rangle$.

Claim: $\langle \mathbb{Q}, + \rangle \cong G$.

For convenience we write additively so that

$$G = \langle x_n \ (n \geq 1) | nx_n = x_{n-1} \ (n \geq 2) \rangle$$

Define $\theta : \{x_n : n \geq 1\} \rightarrow \mathbb{Q}$ by $x_n \theta = \frac{1}{n!}$. By the substitution test θ extends to a surjective homomorphism $\hat{\theta} : G \rightarrow \mathbb{Q}$. We must check that $\hat{\theta}$ is injective.

Let $w \in G$. Then $w = a_1 x_1 + a_2 x_2 + \dots + a_N x_N$ where $a_i \in \mathbb{Z}$ for some $N \geq 1$. So $\hat{\theta}(w) = \sum_{n=1}^N \frac{a_n}{n!}$.

We say that w has *normal form* if:

- 1) $a_N \neq 0$
- 2) $0 \leq a_n \leq n-1$ for $2 \leq n \leq N$
- 3) a_1 is arbitrary.

Any word can be put into normal form. To do this we work from a_N . Suppose that we have got as far as k where $N \geq k \geq 2$.

Then $a_k = qk + a'_k$ where $0 \leq a'_k < k$. Then $a_k \cdot x_k = (qk + a'_k)x_k = qkx_k + a'_k x_k = qx_{k-1} + a'_k x_k$ and $w = a'_N x_N + \dots + a'_k x_k + (a_{k-1} + q)x_{k-1} + a_1 x_1$.

Suppose now that w, w' are in normal form and $\theta(w) = \sum_{n=1}^N \frac{a_n}{n!}$ and $\theta(w') = \sum_{n=1}^M \frac{b_n}{n!}$. Suppose that $a_j = b_j$ for all $1 \leq j \leq k-1$ but $a_k > b_k$. (If $k=1$ then this is strictly speaking the empty set.)

Then

$$\frac{a_k}{k!} + \sum_{n=k+1}^N \frac{a_n}{n!} = \frac{b_k}{k!} + \sum_{n=k+1}^M \frac{b_n}{n!}$$

$$\frac{1}{k!} \leq \frac{a_k - b_k}{k!} \leq \frac{a_k - b_k}{k!} + \sum_{n=k+1}^N \frac{a_n}{n!} = \sum_{n=k+1}^M \frac{b_n}{n!} \leq \frac{1}{k!} - \frac{1}{M!}$$

(for the last step see below) which gives a contradiction. It follows that $\hat{\theta}$ is injective.

NOTE. To prove $\sum_{n=k+1}^M \frac{b_n}{n!} \leq \frac{1}{k!} - \frac{1}{M!}$ we fix k and proceed by induction on $M \geq k + 1$.

If $M = k + 1$ we get $\frac{b_{k+1}}{(k+1)!}$ on the left hand side. But $b_{k+1} < k + 1$ and this implies $\frac{b_{k+1}}{k+1} \leq \frac{1}{k!} - \frac{1}{(k+1)!}$.

Assume that is true for $M - 1$. Then

$$\sum_{n=k+1}^M \frac{b_n}{n!} = \sum_{n=k+1}^{M-1} \frac{b_n}{n!} + \frac{b_M}{M!} \leq \left(\frac{1}{k!} - \frac{1}{(M-1)!} \right) + \frac{M-1}{M!} = \frac{1}{k!} - \frac{1}{M!}$$

4 Finitely generated Abelian groups

Recall that if $G = \langle X|R \rangle$ and $H = \langle Y|S \rangle$ then

$$G \times H = \langle X, Y | R, S, [X, Y] \rangle$$

$$G_{ab} = G/G' = \langle X | R, [X, X] \rangle$$

Proposition 4.1. *Let $F = F(X)$ be free of rank r .*

(i) $F_{ab} = \langle X | [X, X] \rangle$

(ii) $F_{ab} \cong \mathbb{Z}^r$

(iii) $F_{ab} \cong$ free Abelian group of rank r .

Proof. (i) is known and (ii) \Rightarrow (iii).

We prove (ii) by induction on r . If $r = 1$ then $F_{ab} = \langle x | \rangle = \mathbb{Z}$. Assume the claim is true for $1 \leq k < r$. Then

$$\begin{aligned} F_{ab} &= \langle x_1, \dots, x_r | [x_i, x_j] (i \neq j) \rangle \\ &= \langle x_1, \dots, x_{r-1} | [x_i, x_j] (i \neq j) \rangle \times \langle x_r | \rangle \\ &= \mathbb{Z}^{r-1} \times \mathbb{Z} = \mathbb{Z}^r \end{aligned}$$

□

NOTATION. $A = A(X)$ is free Abelian group on X . We will write additively.

Theorem 4.2. *If X generates an Abelian group G then there exists an epimorphism (that is: a surjective homomorphism) $A(X) \rightarrow G$ fixing X elementwise: Every Abelian group is the homomorphis image of some free Abelian group.*

Proof. If $G = \langle X|R \rangle$ is Abelian then $G = G_{ab} = \langle X|R, [X, X] \rangle$. By von Dyck G is a factor of $A(X) = \langle X|[X, X] \rangle$ by the normal closure of R . \square

Theorem 4.3 (Dedekind). *If $A = A(X)$ is free Abelian of rank r and $B \leq A$ then B is free Abelian of rank $\leq r$. (Think subspaces of vector spaces.)*

Proof. If $r = 1$ then $A \cong \mathbb{Z}$ and the result is known. Assume $r > 1$ and result true for $1 \leq k < r$. Let $X = \{x_1, \dots, x_r\}$ and define the subgroups $H = \langle x_1, \dots, x_{r-1} \rangle$ and $C = \langle x_r \rangle$ of A . Then H is free Abelian of rank $r - 1$ and $A \cong H \oplus C$. By induction $B \cap H \leq H$ is free Abelian on y_1, \dots, y_s , say, where $s \leq r - 1$. Also

$$B/(B \cap H) \cong (B + H)/H \leq A/H \cong C$$

(the product of Abelian groups is the same as the sum). So $B/(B \cap H)$ is either trivial or infinite cyclic.

If trivial then $B = B \cap H$ and result follows.

So assume $B/(B \cap H) = \langle b + B \cap H \rangle$ where $b \in B \setminus H$.

Now $b = h + l \cdot x_r$ where $h \in H, l \in \mathbb{Z} \setminus \{0\}$.

We claim that B is free Abelian on $\{y_1, \dots, y_s, b\}$ and so has rank $s + 1 \leq r$, as required. Clearly $B = \langle Y \rangle$. Now suppose that $\sum_{i=1}^s k_i y_i + kb = 0$ ($k_i, k \in \mathbb{Z}$). Then $k \cdot l \cdot x_r = k(b - h) = -\sum_{i=1}^s k_i y_i - kh \in H \Rightarrow k \cdot l \cdot x_r \in H \cap C = \{0\}$.

Since $l \neq 0$ this forces $k = 0 \Rightarrow \sum_{i=1}^s k_i y_i = 0 \Rightarrow k_i = 0$ ($1 \leq i \leq s$) since $\{y_1, \dots, y_s\}$ is a basis.

Thus every element of B is uniquely a \mathbb{Z} -linear combination of the elements of Y , so Y is a free basis for B . \square

(This is equivalent to saying $B \cong \mathbb{Z}^{s+1}$.)

Change of generators.

We know that a finitely generated Abelian group is of the form $A(X)/B$ where $A = A(X)$ is free Abelian on $X = \{x_1, \dots, x_r\}$ and B is free Abelian on $Y = \{y_1, \dots, y_s\}$ where $s \leq r$. Let $Y = Y(X)$ be the elements of Y written as words in X .

Then $A(X)/B = \langle X | [X, X], Y(X) \rangle$.

Suppose that $\{u_1, \dots, u_n\}$ is another set of generators for A . Then we get $X = X(U)$ and $U = U(X)$, in which

$$(1) \quad x_i = \sum_{j=1}^n p_{ij} u_j \text{ for } 1 \leq i \leq r$$

$$(2) \quad u_j = \sum_{k=1}^r q_{jk} x_k \text{ for } 1 \leq j \leq n$$

($p_{ij}, q_{jk} \in \mathbb{Z}$). Substituting (2) into (1) yields

$$\sum_{j=1}^r p_{ij} q_{jk} = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

by uniqueness.

So if $P = [p_{ij}]_{r \times n}$ and $Q = [q_{jk}]_{n \times r}$ then $PQ = I_r$.

Substituting (1) into (2) yields $QP = I_n$.

If $n \geq r$ then $n = \text{rank}(I_n) = \text{rank}(QP) \leq \text{rank} Q \leq r$. So $n = r$ and $Q = P^{-1}$.

Conversely any transformation of type (2) with $[q_{jk}]$ invertible over \mathbb{Z} will yield a new set of generators for A .

Now let $B \leq A$. So B is free on $Y = \{y_1, \dots, y_s\}$ where $s \leq r$ and we get

$$(3) \quad y_k = \sum_{i=1}^r m_{ki} x_i \text{ for } 1 \leq k \leq s$$

Thus B is determined by the matrix $M = [m_{ki}]_{s \times r}$ relative to Y and X .

If we change to generators U of A instead of X then we must substitute (1) into (3).

In matrix terms we change from M to $MP = MQ^{-1}$. If Y is changed to another set V of free generators for B using an $s \times s$ -matrix T invertible over \mathbb{Z} then B is now determined by

TM relative to V, X

TMQ^{-1} relative to V, U

Theorem 4.4. *The subgroup $B = \langle Y \rangle_s$ of $A = \langle X \rangle_r$ is determined by the $s \times r$ coefficient matrix $M = [m_{ki}]_{s \times r}$. Changing the free generators X and Y corresponds to post- and pre-multiplication of M by matrices over \mathbb{Z} . Conversely if T and Q are invertible over \mathbb{Z} , the coefficient matrix TMQ^{-1} determines the same subgroup of A as does M .*

Example.

$$G = \langle x, y, z, t \mid (xyz)^6 = 1, t^2 = (xz)^2, (xy^3zt^2)^2 = 1, (yt^2)^2 = x^2z^3, (xyz)^4(yt)^2 = 1 \rangle$$

$$G_{ab} = \langle x, y, z, t \mid [x, y], [x, z], [x, t], [y, z], [y, t], [z, t], x^6y^6z^6 = 1, x^2z^2t^{-2} = 1, \\ x^2y^6z^2t^4 = 1, x^{-2}z^{-3}y^2t^4 = 1, x^4y^6z^4t^2 = 1 \rangle$$

$$G_{ab} \cong A(X)/B(Y)$$

where $X = \{x, y, z, t\}, Y = \{6x + 6y + 6z, 2x + 2z - 2t, 2x + 6y + 2z + 4t, -2x - 3z + 2y + 4t, 4x + 6y + 4z + 2t\}$

$$M = \begin{pmatrix} 6 & 6 & 6 & 0 \\ 2 & 0 & 2 & -2 \\ 2 & 6 & 2 & 3 \\ -2 & 2 & -3 & 4 \\ 4 & 6 & 4 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} d_1 & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 \\ 0 & 0 & d_3 & 0 \\ 0 & 0 & 0 & d_4 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Relation matrix: By performing row and column operations (which correspond to pre- and post-multiplication by invertible matrices) we can reduce M to a *canonical form* (Smith normal form) from which

- (i) free generators for the subgroup B can be read off
- (ii) $A(X)/B(Y)$ can be identified as a product of cyclic groups.

Row operations.

P: permuting rows

M: multiplying a row by ± 1

A: adding an *integer* multiple of one row to another

(Column operations are similarly defined.)

We now describe an algorithm (see handout) for reducing any $s \times r$ matrix M over \mathbb{Z} to the canonical form $D = \text{diag}(d_1, \dots, d_k)$ where $k = \min(r, s)$ and d_i is a non-negative integer ($1 \leq i \leq k$) such that $d_i | d_{i+1}$ for $1 \leq i \leq k - 1$.

Remarks. 1. The divisibility condition implies that any 1's that occur amongst the d_i occur at the beginning and any 0's occur at the end.

2. $d_1 = \text{hcf}(\text{entries of } M)$

3. Those d_i 's not equal to 0 or 1 are called the *invariant factors* or *torsion coefficients*.

4. The number of 0's is the *rank*.

5. The uniqueness of the invariant factors and rank follows from linear algebra.

Returning to Example (*): See Handout ($d_1 = 1, d_2 = 2, d_3 = 6, d_4 = 0$).

Exercise. Reduce this matrix to Smith normal form:

$$\begin{bmatrix} 132 & 68 & 68 \\ 78 & 76 & 40 \\ 78 & 112 & 40 \end{bmatrix}$$

Translating all this into group theory we obtain:

$$\begin{aligned} A(X)/B &= \frac{A(\{x_1, \dots, x_r\})}{\langle d_1x_1, \dots, d_kx_k \rangle} \\ &= \frac{A(\{x_1, \dots, x_r\})}{\langle d_1x_1, \dots, d_lx_l \rangle} \text{ where } l \leq k, d_i > 0 \\ &= \frac{\langle x_1 \rangle \times \dots \times \langle x_r \rangle}{\langle d_1x_1 \rangle \times \dots \times \langle d_lx_l \rangle} \\ &= \langle x_1 | d_1x_1 \rangle \times \langle x_2 | d_2x_2 \rangle \times \dots \times \langle x_l | d_lx_l \rangle \times \mathbb{Z}^{r-l} \end{aligned}$$

Returning to Example (*)

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

we get:

$$G_{ab} = \langle x|x \rangle \times \langle y|2y \rangle \times \langle z|6z \rangle \times \mathbb{Z} \cong C_2 \times C_6 \times \mathbb{Z}$$

rank = 1, invariant factors = $\{2, 6\}$.

Examples. (i)

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 16 & 0 & 0 \end{bmatrix}$$

$$C_2 \times C_{16} \times C_{16} \times \mathbb{Z}^2$$

$$\langle x_1, \dots, x_6 | x_1, x_2^2, x_3^{16}, x_4^{16}, [x_i, x_j] \rangle$$

(ii)

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$C_2 \times C_4 \times \mathbb{Z}^2$$

(iii)

$$\begin{bmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 9 \end{bmatrix}$$

$$C_3 \times C_3 \times C_9$$

Theorem 4.5 (Basis theorem for finitely generated Abelian groups). *Given a finitely generated Abelian group G there are integers $k, m \geq 0$ and integers $d_i \geq 2$ ($1 \leq i \leq k$) such that $d_i | d_{i+1}$ for $1 \leq i \leq k - 1$, and*

$$G \cong C_{d_1} \times \dots \times C_{d_k} \times \mathbb{Z}^m$$

Moreover each (d_1, \dots, d_k, m) uniquely determines G .

Example. $C_6 \times C_{10} \cong (C_2 \times C_3) \times C_{10} \cong C_2 \times (C_3 \times C_{10}) \cong C_2 \times C_{30}$

$$\begin{bmatrix} 6 & 0 \\ 0 & 10 \end{bmatrix} \rightarrow \begin{bmatrix} 6 & 6 \\ 0 & 10 \end{bmatrix} \rightarrow \begin{bmatrix} 6 & 6 \\ -12 & -2 \end{bmatrix} \rightarrow \begin{bmatrix} -30 & 0 \\ -12 & -2 \end{bmatrix} \rightarrow \begin{bmatrix} 2 & 0 \\ 0 & 30 \end{bmatrix}$$

Remark. Let $P(n)$ denote the number of partitions of $n \geq 1$. For example $P(5) = 7$:

$$5, 1 + 4, 2 + 3, 1 + 1 + 3, 1 + 2 + 2, 1 + 1 + 1 + 2, 1 + 1 + 1 + 1 + 1.$$

It follows from the theorem that the number of Abelian groups of order $n (= p_1^{k_1} \cdot \dots \cdot p_k^{k_r}, p_i$ distinct primes, $k_i \geq 1)$ equals $\prod_{i=1}^r P(k_i)$.

Example. How many Abelian groups are there of order $n = 71906968240509600$?

Answer: $n = 2^5 3^3 5^2 11^2 31^7$, the number of groups is $P(5) \cdot P(3) \cdot P(2) \cdot P(2) \cdot P(7) = 7 \cdot 3 \cdot 2 \cdot 2 \cdot 15 = 1260$.

Example. List the Abelian groups of order 144.

Suppose that the relation matrix M is a square matrix. Then the row and column operations only alter $\det M$ up to a factor of ± 1 .

Corollary. If $G = \langle X | R \rangle$ is a finite presentation and $|X| = |R|$ then

$$|G_{ab}| = \pm \det M$$

Corollary. If $G = \langle X | R \rangle$ is a finite presentation and $|X| > |R|$ then G is an infinite group.

Proof. Since $|X| > |R|$ the relation matrix has more columns than rows. So the normal form of M must contain at least $|X| - |R|$ columns of zeroes. It follows that G_{ab} is infinite. But G_{ab} is a quotient of G so G is infinite. \square

Example.

$$C_n = \langle x | x^n = 1 \rangle$$

$$Q_{2n} = \langle x, y | x^n = y^2, y^{-1}xy = x^{-1} \rangle$$

$$G = \langle x, y, z | y^{-1}xy = x^a, z^{-1}yz = y^a, x^{-1}zx = z^a \rangle$$

then $|G| < \infty$ for $a \geq 3$. Also: G cannot be 2-generated.

Example. List the Abelian groups of order 144.

OPEN PROBLEM: Is there a group G having a presentation $G = \langle X | R \rangle$ where

- (1) $|G| < \infty$,
- (2) $|X| = |R| = 4$, and
- (3) G can not be generated by fewer than 4 generators?

5 Group Extensions

The group G is said to *act* on the group A if for each $g \in G, a \in A$ there exists a unique element $a^g \in A$ such that

$$\begin{aligned} a^{e_A} &= a \quad (\forall a \in A) \\ (a^{g_1})^{g_2} &= a^{g_1 g_2} \quad (\forall a \in A, g_1, g_2 \in G) \\ (a_1 a_2)^g &= a_1^g a_2^g \quad (\forall a_1, a_2 \in A, g \in G) \end{aligned}$$

Example. If $A \subseteq G$ and we know $g^{-1}ag \in A \quad (\forall a \in A, g \in G)$ then

$$a^g := g^{-1}ag$$

is an action of G on A (conjugation).

$$\begin{aligned} a^{e_G} &= e_G^{-1}ae_G = a \\ (a^{g_1})^{g_2} &= (g_1^{-1}ag_1)^{g_2} = g_2^{-1}(g_1^{-1}ag_1)g_2 = a^{g_1 g_2} \\ (a_1 a_2)^g &= g^{-1}a_1 a_2 g = g^{-1}a_1 g g^{-1}a_2 g = a_1^g a_2^g \end{aligned}$$

Definition. An *automorphism* of A is an isomorphism $A \rightarrow A$. $\text{Aut}(A)$ is the group of all automorphisms of A with composition of maps.

Theorem 5.1. *Let G act on A (as groups). Then for each $g \in G$ there corresponds a mapping $\phi_g : A \rightarrow A$ defined by $\phi_g(a) = a^g \quad (\forall a \in A)$, and moreover $\phi_g \in \text{Aut}(A)$. The mapping $\phi : G \rightarrow \text{Aut}(A)$ defined by $g\phi = \phi_g \quad (\forall g \in G)$ is a homomorphism and we call ϕ the action.*

Conversely let $\phi \in \text{Hom}(G, \text{Aut}(A))$. Then G acts on A (with action ϕ) if we define $a^g := a(g\phi) \in A$.

Proof. We prove only the last statement.

$$\begin{aligned}
a^{e_G} &= a(e_G\phi) = a(e_{\text{Aut}(A)}) = a(\text{id}_A) = a \\
(a_1a_2)^g &= (a_1a_2)(g\phi) \\
&= a_1(g\phi)a_2(g\phi) \quad (\text{since } g\phi \in \text{Hom}(A, A)) \\
&= a_1^g a_2^g \\
a^{g_1g_2} &= a((g_1g_2)\phi) \\
&= a((g_1\phi)(g_2\phi)) \\
&= (a(g_1\phi))(g_2\phi) \\
&= (a^{g_1})^{g_2}
\end{aligned}$$

□

Suppose G acts on A (with action ϕ). Consider $K = G \times A$ (Cartesian product) with the binary operation

$$(x, a)(y, b) = (xy, a^yb) \quad (\forall x, y \in G)(\forall a, b \in A).$$

(Note: $a^y = a(y\phi)$.)

Then we get a group K called the *semi-direct product* of G on A ; and we write

$$K = G \times_{\phi} A \text{ or } A \rtimes_{\phi} G$$

For example

$$\begin{aligned}
(x, a)(x^{-1}, (a^{-1})^{x^{-1}}) &= (xx^{-1}, a^{x^{-1}}(a^{-1})^{x^{-1}}) = (e_G, (aa^{-1})^{x^{-1}}) \\
&= (e_G, e_a^{x^{-1}}) = (e_G, e_a)
\end{aligned}$$

So $(x, a)^{-1} = (x^{-1}, (a^{-1})^{x^{-1}})$.

NOTE. $e_A^y = e_A(y\phi) = e_A$.

NOTE. Direct product of G, A is obtained when $a^y = a \quad (\forall a \in A, \forall y \in G)$, that is, $a(y\phi) = a \quad (\forall a \in A, \forall y \in G)$, that is, $y\phi = \text{id}_A \quad (\forall y \in G)$, that is, $\phi : G \rightarrow \text{Aut}(A)$ is defined by $y\phi = \text{id}_A \quad (\forall y \in G)$.

The mappings

$$A \rightarrow K \quad a \mapsto (e_G, a)$$

$$G \rightarrow K \quad g \mapsto (g, e_A)$$

give injective homomorphisms. (Check!)

It is customary to identify A, G with their isomorphic images in K , that is, regard them as subgroups of K .

Observe that

$$\begin{aligned} (x, b)^{-1}(e_G, a)(x, b) &= (x^{-1}, (b^{-1})^{x^{-1}})(x, a^x b) \\ &= (e_G, ((b^{-1})^{x^{-1}})^x a^x b) = (e_G, b^{-1} a^x b) \in A \end{aligned}$$

Thus: $A \trianglelefteq K, G \leq K, A \cap G = \{(e_G, e_A)\}$ and $K/A \cong G$ (*)

Pictorially:

$$1 \longrightarrow A \longrightarrow K \longrightarrow G \longrightarrow 1$$

Definition. An *extension* of a group G by a group A is a group \tilde{G} having a normal subgroup N such that $A \cong N$ and $\tilde{G}/N \cong G$.

Example. If $\theta : \tilde{G} \rightarrow G$ is an epimorphism then \tilde{G} is an extension of G by $\ker \theta$.

Example. $K = A \downarrow_{\phi} G$ is an extension of G by A .

Pictorially:

$$1 \longrightarrow A \xrightarrow{\beta_1} \tilde{G} \xrightarrow{\beta_2} G \longrightarrow 1$$

where $\ker \beta_1 = \{e_A\}, \text{Im } \beta_1 = \ker \beta_2, \text{Im } \beta_2 = G$.

Definition. A sequence of groups A_i and homomorphisms α_j

$$A_0 \xrightarrow{\alpha_0} A_1 \xrightarrow{\alpha_1} A_2 \xrightarrow{\alpha_2} \cdots \xrightarrow{\alpha_{n-1}} A_n$$

is called *exact* if $\text{Im}(\alpha_{i-1}) = \ker(\alpha_i)$ for each i .

A *short exact sequence* is an exact sequence where $n = 4$ and $A_0 = A_4 = 1$.

Therefore group extensions \equiv short exact sequences.

$$1 \longrightarrow A_1 \xrightarrow{\text{inj.}} A_2 \xrightarrow{\text{surj.}} A_3 \longrightarrow 1$$

A *diagram* is a directed graph whose edges are homomorphisms between the end points and whose vertices are groups.

A diagram is called *commutative* if given any two vertices and any two paths between them the corresponding composite homomorphisms coincide.

Lemma 5.2 (The Five Lemma).

Let

$$\begin{array}{ccccccccc} A_0 & \xrightarrow{\alpha_0} & A_1 & \xrightarrow{\alpha_1} & A_2 & \xrightarrow{\alpha_2} & A_3 & \xrightarrow{\alpha_3} & A_4 \\ \phi_0 \downarrow & & \phi_1 \downarrow & & \phi_2 \downarrow & & \phi_3 \downarrow & & \phi_4 \downarrow \\ B_0 & \xrightarrow{\beta_0} & B_1 & \xrightarrow{\beta_1} & B_2 & \xrightarrow{\beta_2} & B_3 & \xrightarrow{\beta_3} & B_4 \end{array}$$

be a commutative diagram with exact rows. If ϕ_0, ϕ_1, ϕ_3 and ϕ_4 are isomorphisms then so is ϕ_2 .

Proof.

(ϕ_2 injective)

Let $a \in \ker \phi_2$. We show that $a = 0$.

$$\text{Then } a\alpha_2\phi_3 = a\phi_2\beta_2 = e\beta_2 = e$$

$$\Rightarrow a\alpha_2 \in \ker \phi_3 = e \quad (\phi_3 \text{ injective})$$

$$\Rightarrow a \in \ker \alpha_2 = \text{Im } \alpha_1 \quad (\text{exact})$$

$$\Rightarrow a = a_1\alpha_1 \text{ for some } a_1 \in A_1$$

$$\Rightarrow e = a\phi_2 = a_1\alpha_1\phi_2 = a_1\phi_1\beta_1$$

$$\Rightarrow a_1\phi_1 \in \ker \beta_1 = \text{Im } \beta_0 \text{ (exact)}$$

$$\Rightarrow a_1\phi_1 = b_0\beta_0 \text{ for some } b_0 \in B_0$$

Since ϕ_0 is surjective $\exists a_0 \in A_0$ s.t. $a_0\phi_0 = b_0$

$$\Rightarrow a_1\phi_1 = a_0\phi_0\beta_0 = a_0\alpha_0\beta_1$$

$$\Rightarrow a_1 = a_0\alpha_0 \quad (\phi_1 \text{ injective})$$

$\Rightarrow a_1 \in \text{Im } \alpha_0 = \ker \alpha_1$ (exact)

$\Rightarrow a = a_1 \alpha_1 = e$

$\Rightarrow \ker \phi_2 = \{e\}$.

(ϕ_2 surjective)

Exercise. □

Suppose now that we are given an extension

$$1 \longrightarrow A \xrightarrow{\iota} \tilde{G} \xrightarrow{\nu} G \longrightarrow 1 \text{ exact}$$

and presentations $G = \langle X|R \rangle$ and $A = \langle Y|S \rangle$. Our aim is to obtain a presentation for \tilde{G} .

Let $\tilde{Y} = \{y\iota = \tilde{y} : y \in Y\} \subseteq \tilde{G}$ and let $\tilde{S} = \{\tilde{s} : s \in S\} \subseteq \tilde{G}$ where \tilde{s} is obtained from $s \in S$ by replacing each occurrence of y in s by \tilde{y} . Now let $\tilde{X} = \{\tilde{x} : x \in X^{\pm 1}\} \subseteq \tilde{G}$ be members of a transversal for the image of ι in \tilde{G} such that $\tilde{x}\nu = x$.

NOTE.

$$G \cong \tilde{G} / \ker \nu = \tilde{G} / \text{Im } \iota$$

and

$$\begin{aligned} \tilde{x}_1\nu = \tilde{x}_2\nu & \text{ iff } \tilde{x}_1^{-1}\tilde{x}_2 \in \ker \nu \\ & \text{ iff } \tilde{x}_1^{-1}\tilde{x}_2 \in \text{Im } \iota \\ & \text{ iff } \tilde{x}_1\text{Im } \iota = \tilde{x}_2\text{Im } \iota. \end{aligned}$$

For each $r \in R$ let \tilde{r} be the word in \tilde{X} obtained from r by replacing each x with \tilde{x} .

Now $\tilde{r} \in \ker \nu = \text{Im } \iota$ so each \tilde{r} can be written as a word v_r in the \tilde{y} .

Put $\tilde{R} = \{\tilde{r}v_r^{-1} : r \in R\} \subseteq \tilde{G}$. Finally $\text{Im } \iota \trianglelefteq \tilde{G}$ and so each conjugate $\tilde{x}^{-1}\tilde{y}\tilde{x}$, $\tilde{x}\tilde{y}\tilde{x}^{-1} \in \text{Im } \iota$ and so is a word $w_{x,y}, w_{x^{-1},y}$ in \tilde{Y} . Put $\tilde{T} = \{\tilde{x}^{-1}\tilde{y}\tilde{x}w_{x,y}^{-1} : x \in X^{\pm 1}, y \in Y\} \subseteq \tilde{G}$.

Theorem 5.3.

$$\tilde{G} = \langle \tilde{X}, \tilde{Y} | \tilde{R}, \tilde{S}, \tilde{T} \rangle$$

Proof. Let $D = \langle \tilde{X}, \tilde{Y} | \tilde{R}, \tilde{S}, \tilde{T} \rangle$. We must show that $\tilde{G} \cong D$.

Define $\theta : \tilde{X} \cup \tilde{Y} \rightarrow \tilde{G}$ by

$$\tilde{x}\theta = \tilde{x} \quad \tilde{y}\theta = \tilde{y}$$

Then θ extends to a homomorphism $\hat{\theta} : D \rightarrow \tilde{G}$. The restriction of $\hat{\theta}$ to $\langle \tilde{Y} \rangle \leq D$ gives rise to the composite homomorphism $\theta_1 : \langle \tilde{Y} \rangle \rightarrow \text{Im } \iota \cong A$ where $\tilde{y}\theta_1 = y$. Since all the defining relators S of A with each y replaced by \tilde{y} yield the identity in $\langle \tilde{Y} \rangle$ then using the substitution test the mapping $Y \rightarrow \langle \tilde{Y} \rangle, y \mapsto \tilde{y}$ extends to a homomorphism $A \rightarrow \langle \tilde{Y} \rangle$ inverse to θ_1 . So θ_1 is an isomorphism. \square

The presence of \tilde{T} in the presentation for D implies that $\langle \tilde{Y} \rangle \trianglelefteq D$. So we have the commutative diagram

$$\begin{array}{ccc} D & \xrightarrow{\hat{\theta}} & \tilde{G} & \xrightarrow{\nu} & G \\ & \searrow \nu_1 & & \nearrow \theta_2 & \\ & & D/\langle \tilde{Y} \rangle & & \end{array}$$

where $\text{Im } \nu_1 = D/\langle \tilde{Y} \rangle$, $\ker \nu_1 = \langle \tilde{Y} \rangle$ and since $\langle \tilde{Y} \rangle \hat{\theta} \nu \subseteq (\text{Im } \iota) \nu = (\ker \nu) \nu = e_G \Rightarrow \ker \nu_1 = \langle \tilde{Y} \rangle \subseteq \ker(\hat{\theta} \nu)$ and so we can apply Lemma 3.2 to obtain

$$\begin{aligned} \theta_2 : D/\langle \tilde{Y} \rangle &\rightarrow G \\ \tilde{x}\langle \tilde{Y} \rangle \theta_2 &= \tilde{x} \nu_1 \theta_2 = \tilde{x} \hat{\theta} \nu = \tilde{x} \nu = x \end{aligned}$$

But the relators R of G with each x replaced by $\tilde{x}\langle \tilde{Y} \rangle$ all held in $D/\langle \tilde{Y} \rangle$ so applying the substitution test we obtain a homomorphism $G \rightarrow D/\langle \tilde{Y} \rangle$, $x \mapsto \tilde{x}\langle \tilde{Y} \rangle$, inverse to θ_2 . So θ_2 is an isomorphism.

We now have:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & \tilde{G} & \longrightarrow & G & \longrightarrow & 1 \\ \uparrow \theta_0 & & \uparrow \theta_1 & & \uparrow \hat{\theta} & & \uparrow \theta_2 & & \uparrow \theta_3 \\ 1 & \longrightarrow & \langle \tilde{Y} \rangle & \longrightarrow & D & \longrightarrow & D/\langle \tilde{Y} \rangle & \longrightarrow & 1 \end{array}$$

where the rows are exact and each θ_i is an isomorphism.

Corollary. Let $G = \langle X|R \rangle$ and $A = \langle Y|S \rangle$. Let $\alpha : G \rightarrow \text{Aut}(A)$ be a homomorphism such that

$$y(x\alpha) = w_{x,y} \in \langle Y \rangle = A \quad (\forall x \in X, \forall y \in Y)$$

Then the semi-direct product $A \downarrow_{\alpha} G$ has a presentation

$$A \downarrow_{\alpha} G = \langle X, Y | R, S, x^{-1}yxw_{x,y}^{-1} \quad (x \in X, y \in Y) \rangle$$

Proof. Apply 5.3 to the extension $1 \longrightarrow A \longrightarrow A \downarrow_{\alpha} G \longrightarrow G \longrightarrow 1$. Since $G \leq A \downarrow_{\alpha} G$ it follows that all the v_r are trivial. Remove the tildas to get result. \square

Also note that we use X instead of $X^{\pm 1}$ for $x^{-1}yxw_{x,y}^{-1}$. Since $x\alpha \in \text{Aut}(A)$ it follows that $\{w_{x,y} : y \in Y\}$ generates A .

Suppose we know that $x^{-1}yx = w_{x,y}$ then $xw_{x,y}x^{-1} = y \in A$. So $y = w_{x,y_1}^{n_1} \dots w_{x,y_k}^{n_k}$ and $xyx^{-1} = (xw_{x,y_1}x^{-1})^{n_1} (xw_{x,y_2}x^{-1})^{n_2} \dots (xw_{x,y_k}x^{-1})^{n_k} = y_1 \dots y_k \in A = \langle Y \rangle$

Example.

$$A = C_n = \langle y | y^n = 1 \rangle, G = C_m = \langle x | x^m = 1 \rangle$$

When does G act on A ?

We want G to act with action α , say, $\alpha : G \rightarrow \text{Aut}(A)$, where

$$(*) \quad y(x\alpha) = y^l$$

for some $l \in \{1, \dots, n-1\}$.

Since $x\alpha \in \text{Aut}(A)$ we must have $\langle y^l \rangle = A \Leftrightarrow \text{hcf}(l, n) = 1$.

Also since $(x\alpha)^m = x^m\alpha = e_G\alpha = e_{\text{Aut}(A)} = \text{id}_A$ we have $y(x\alpha)^m = y \Leftrightarrow y^{l^m} = y \Leftrightarrow l^m \equiv 1 \pmod n$ (**) ($\Rightarrow \text{hcf}(l, n) = 1$).

Subject to (**), (*) completely determines α since

$$y^r(x^s\alpha) = (y(x\alpha)^s)^r = y^{r \cdot l^s}$$

By corollary 5.4

$$A \downarrow_{\alpha} G = \langle x, y | x^m, y^n, x^{-1}yx = y^l \rangle$$

Example. $A = C_5 = \langle y | y^5 = 1 \rangle$, $G = \langle x | x^4 = 1 \rangle$, $l \in \{1, 2, 3, 4\}$, $m = 4$, $n = 5$, $l^4 \equiv 1 \pmod 5$.

In fact this is true for all values of l .

$$\begin{aligned} \langle x, y | x^4, y^5, x^{-1}yx = y \rangle &= C_4 \times C_5 \cong C_{20} \\ \langle x, y | x^4, y^5, x^{-1}yx = y^2 \rangle & \\ \langle x, y | x^4, y^5, x^{-1}yx = y^3 \rangle & \\ \langle x, y | x^4, y^5, x^{-1}yx = y^4 \rangle &. \end{aligned}$$

Example. $A = \langle y | y^6 = 1 \rangle$, $G = \langle x | x^2 = 1 \rangle$, $l \in \{1, 2, 3, 4, 5\}$,
 $m = 2$, $n = 6$, $l^2 = 1 \pmod{6}$

$$1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 3, 4^2 \equiv 4, 5^2 \equiv 1$$

$$\langle x, y | x^2, y^6, x^{-1}yx = y \rangle = C_2 \times C_6$$

$$\langle x, y | x^2, y^6, x^{-1}yx = y^{-1} \rangle = D_{12}$$