1. Free groups and presentations

Let X be a subset of a group G. The subgroup generated by X, denoted $\langle X\rangle$, is the intersection of all subgroups of G containing X as a subset.

If $g \in G$, then $g \in \langle X\rangle \Leftrightarrow g$ can be written as $x_1^{e_1}\dots x_n^{e_n}$ where $x_i \in X$, $e_i = \pm 1$, $n \geq 0$. (When $n = 0$, this means $g = 1$.)

[Set of all such products is a subgp of G, and any subgp of G containing X contains all such products.]

Definition. *X generates G* if $G = \langle X\rangle$.

If $f : G \to H$ is a homom. and $G = \langle X\rangle$, then

$$f(x_1^{e_1}\dots x_n^{e_n}) = f(x_1)^{e_1}\dots f(x_n)^{e_n}$$

so f is determined by its restriction to X.

If $G = \langle X\rangle$ and $f : X \longrightarrow H$, is a map to a group H, f does not necessarily extend to a homom. $\tilde{f} : G \to H$.

Example. $G = \langle x\rangle$ cyclic of order 3, $H = \langle y\rangle$ cyclic of order 2
$f : X \longrightarrow H$, $f(x) = y \quad (X = \{x\})$.
If extension $\tilde{f}$ exists, then x^3=1, but

$$\tilde{f}(x^3) = \tilde{f}(x)^3 = y^3 = y \neq 1$$

contradiction.

In general, for an extension to exist, need:

$$x_1^{e_1}\dots x_n^{e_n} = 1 \ (x_i \in X,\ e_i = \pm 1) \Rightarrow f(x_1)^{e_1}\dots f(x_n)^{e_n} = 1.$$

Then can define $\tilde{f}(x_1^{e_1}\dots x_n^{e_n}) = f(x_1)^{e_1}\dots f(x_n)^{e_n}$, and this is a homom.

Free groups.

Definition. Let X be a subset of a group F. Then F is a *free group with basis X* if, for any map $f : X \to H$, where H is a group, there is a unique extension of f to a homom. $\tilde{f} : F \to H$.

Note. Follows that X generates F. For let $F_1 = \langle X\rangle$. Inclusion map $X \to F_1$ has an extension to a homom. $f_1 : F \to F_1$.
Let $f_2 : F_1 \to F$ be the inclusion map.
Then $f_2 f_1$ and id_F both extend the inclusion map $X \to F$, so $f_2 f_1 = \mathrm{id}_F$, hence f_2 is onto, i.e. $F = F_1$.

Proposition 1.1. *Let F_1, F_2 be free groups with bases X_1, X_2. Then F_1 is isomorphic to $F_2 \Leftrightarrow |X_1| = |X_2|$. ($|X_i|$ = cardinality of X_i.)*

Proof. $\Leftarrow$ Let $f : X_1 \to X_2$ is a bijective map. Viewed as a mapping $X_1 \to F_2$, there is an extension to a homom. $\tilde{f} : F_1 \to F_2$. Similarly, putting $g = f^{-1}$, g has an extension to a homom. $\tilde{g} : F_2 \to F_1$. Both $\tilde{g}\tilde{f}$ and $\mathrm{id}_{F_1} : F_1 \to F_1$

extend inclusion map $X_1 \to F_1$, so $\tilde{g}\tilde{f} = \mathrm{id}_{F_1}$. Similarly, $\tilde{f}\,\tilde{g} = \mathrm{id}_{F_2}$, hence $\tilde{f}$ is an isomorphism.
$\Rightarrow$ Let F be free with basis X, F^2 =subgp. gend. by $\{u^2 \mid u \in F\}$.
Let V be a vector space over $\mathbb{Z}/2\mathbb{Z}$ with basis X.
Inclusion mapping $X \to V$ extends to a homomorphism $F \to V$ of groups; kernel contains F^2, so there is an induced homomorphism $F/F^2 \to V$, which is a linear map of vector spaces.

Follows that the projection homom. $F \to F/F^2$ is injective on X and the image of X is a $\mathbb{Z}/2\mathbb{Z}$ basis for F/F^2. Hence $|X| = \dim_{\mathbb{Z}/2\mathbb{Z}}(F/F^2)$.

Now an isomorphism from F_1 to F_2 induces an isomorphism $F_1/F_1^2 \to F_2/F_2^2$ (of vector spaces), so $|X_1| = |X_2|$. □

Definition. If F is free with basis X, then $|X|$ is the *rank* of F.

Examples. (1) Trivial gp is free of rank 0 (basis the empty set).
(2) infinite cyclic gp is free of rank 1 (basis any of the two generators).

Existence. Let X be a set. Let X^{-1} be a set in 1-1 correspondence with X via a map $x \mapsto x^{-1}$, and with $X \cap X^{-1} = \emptyset$. Put $X^{\pm 1} = X \cup X^{-1}$ and define $(x^{-1})^{-1} = x$, for $x \in X$, to obtain an involution $X^{\pm 1} \to X^{\pm 1}$ without fixed points.

A *word* in $X^{\pm 1}$ is a finite sequence $w = (a_1, \ldots, a_n)$, where $a_i \in X^{\pm 1}$ for $1 \le i \le n$, and $n \ge 0$. (When $n = 0$, $w = 1$, the *empty word*.)
Length of w, denoted $|w|$, is n $\quad(|1| = 0)$.

Let W be the set of words. If $w' = (b_1, \ldots, b_m)$ is also in W, define

$$w.w' = (a_1, \ldots, a_n, b_1, \ldots, b_m)$$

$(1.w = w.1 = w)$, giving assoc. binary operation on W, with identity elt. 1.

Define $w^{-1} = (a_n^{-1}, \ldots, a_1^{-1})$ $\quad(1^{-1} = 1)$.
Then $(u.v)^{-1} = v^{-1}.u^{-1}$ $\ \forall u,\ v \in W$.

For $u,\ v \in W$, define $u \simeq v$ to mean v is obtained from u by inserting or deleting a part aa^{-1}, where $a \in X^{\pm 1}$.
(eg $xyzz^{-1}x \simeq xyx \simeq xz^{-1}zyx$.)
For $u,\ v \in W$, $u \sim v$ means there is a sequence $u = u_1, u_2, \ldots, u_k = v$, where $u_i \simeq u_{i+1}$ $(1 \le i \le k-1)$. Equivalence relation on W.

if $u \simeq v$ and $w \in W$, then $u.w \simeq v.w$, hence if $u \sim v$ then $u.w \sim v.w$. Similarly, $u \sim v$ implies $w.u \sim w.v$.

Hence, if $u \sim u_1$ and $v \sim v_1$, then $u.v \sim u.v_1$ and $u.v_1 \sim u_1.v_1$, so $u.v \sim u_1.v_1$.

If $u \sim v$ then $u^{-1} \sim v^{-1}$ and $u.u^{-1} \sim 1 \sim u^{-1}.u$.

Let $[u]$ denote the equivalence class of $u \in W$ and let F be the set of equiv classes.

Follows: F is a group, by defining

$$[u][v] = [u.v]$$

with identity elt. [1], and $[u]^{-1} = [u^{-1}]$.

Definition. Word $w \in W$ is *reduced* if it contains no part aa^{-1} with $a \in x^{\pm 1}$.

1.2 (Normal Form Theorem). *Every equivalence class contains a unique reduced word.*

Proof. At least one-take a word of minimal length in the equiv. class.

Suppose $[u] = [v]$, where u, v are reduced, so there is a sequence $u = u_1, \ldots, u_k = v$ with $u_i \simeq u_{i+1}$. To prove $u = v$, suffices to show: if $k \geq 2$, the sequence can be shortened. Note $k \neq 2$ as u, v are reduced, so assume $k > 2$.

Let u_i be a word of maximal length in the sequence. Then $1 < i < k$ since u, v are reduced. Further, u_i is obtained from u_{i-1} by inserting yy^{-1} for some $y \in X^{\pm 1}$, and u_{i+1} is obtained from u_i by deleting zz^{-1} for some $z \in X^{\pm 1}$. If the parts yy^{-1} and zz^{-1} of u_i coincide or overlap by a single letter, then $u_{i-1} = u_{i+1}$, and u_i, u_{i+1} can be omitted from the sequence.

Otherwise, can replace u_i by u_i', where u_i' is obtained from u_i by deleting zz^{-1}, and u_{i+1} is obtained from u_i' by inserting yy^{-1}. This reduces $\sum_{i=1}^{k} |u_i|$, so after finitely many such replacements we shall be able to shorten the derivation. □

Consequently, map $X \to F$, $x \mapsto [x]$ is injective, as (x) is a reduced word. Can identify x with $[x]$, for $x \in X$.

Theorem 1.3. *The gp F is free with basis X.*

Proof. let $f : X \to H$ be a map, H a gp. Extend f to $\bar{f} : W \to H$ by:

$$\bar{f}(x_1^{e_1}, \ldots, x_n^{e_n}) = f(x_1)^{e_1} \ldots f(x_n)^{e_n}$$

($x_i \in X$, $e_i = \pm 1$) and $\bar{f}(1) = 1$. If $u \simeq v$ then $\bar{f}(u) = \bar{f}(v)$, so if $u \sim v$ then $\bar{f}(u) = \bar{f}(v)$. So can define $\tilde{f} : F \to H$ by $\tilde{f}([u]) = \bar{f}(u)$. If u, $v \in W$ then $\bar{f}(u.v) = \bar{f}(u)\bar{f}(v)$, hence $\tilde{f}$ is a homom. extending f.

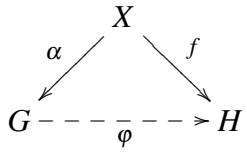
Finally, X generates F, so extension of f is unique. □

Presentations. Let X be a set, W the set of words in $X^{\pm 1}$, G a gp, $\alpha : X \to G$ a map. Extend α to $\bar{\alpha} : W \to G$ by $\bar{\alpha}(x_1^{e_1}, \ldots, x_n^{e_n}) = \alpha(x_1)^{e_1} \ldots \alpha(x_n)^{e_n}$.

Definition. R a subset of W. The gp G has presentation $\langle X \mid R \rangle$ (via α) if

(1) $\bar{\alpha}(w) = 1$ for all $w \in R$;

(2) given a gp H and map $f : X \to H$, s.t. $\bar{f}(w) = 1$ for all $w \in R$, $\exists$ a unique homom. $\varphi : G \to H$ such that $\varphi\alpha = f$.



Elts of R are called *relators* of the presn. If $w \in R$, often write $w = 1$ instead of w. More generally, if $w = w_1.w_2^{-1}$, write $w_1 = w_2$ instead of w. Call this a *relation*.
Map α often suppressed, but can't assume it's injective (eg R might contain $x.y^{-1}$, where $x, y \in X$, $y \neq x$).

Remarks.

(1) Requirement that φ is unique$\equiv\alpha(X)$ generates G.
(2) If G, H both have presn $\langle X \mid R\rangle$ via suitable maps, then $G \cong H$, and if $G \cong H$, any presn for G is one for H.
(3) For any X and $R \subseteq W$, $\exists$ a gp with presn $\langle X \mid R\rangle$. Let F be free with basis X; then R represents a subset of F. Let N be the normal subgp of F gend by R (i.e. subgp gend by all conjugates of elts of R), let $G = F/N$, $\alpha : X \to G$ restriction of projection $F \to F/N$ to X. Then $\langle X \mid R\rangle$ is a presn of G via α.
(4) Any gp has a presn. Let X be a set of generators for G, Let F be free with basis X, $f : F \to G$ extn of inclusion map $X \to G$ to F. Let $N = \ker(f)$, viewed as a set of reduced words. Then $\langle X \mid N\rangle$ is a presn of G via inclusion map $X \to G$.

Examples. (1) If G has presn $\langle x \mid x^n\rangle$, then G is cyclic of order n. Clearly cyclic of order $\leq n$, and if $\langle a\rangle$ is cyclic of order n, $x \mapsto a$ extends to a homom. $G \xrightarrow{\text{onto}} \langle a\rangle$, so $|G| \geq n$.

(2) Let $n \geq 2$; let a be a rotation of the plane $\mathbb{R}^2 = \mathbb{C}$ anticlockwise through $2\pi/n$ ($z \mapsto ze^{2\pi i/n}$).
Let b be reflection in the real axis ($z \mapsto \bar{z}$), so a has order n, b has order 2, and $bab^{-1} = a^{-1}$
Let $D_n = \langle a, b\rangle$ (subgp gend by a, b in the group of isometries of $\mathbb{R}^2$).
Let $A = \langle a\rangle$, $B = \langle b\rangle$; then $A \trianglelefteq D_n$, so $D_n = AB$, and $A \cap B = \{1\}$. Hence $|D_n| = |A||B| = 2n$.

[D_n, sometimes written D_{2n}, is the *dihedral group* of order $2n$. It is the set of all isometries of $\mathbb{R}^2$ which map the set $\left\{e^{2\pi ik/n}\right\}$ of complex nth roots of 1 onto itself, equivalently the polygon with these points as vertices if $n \geq 3$.]

Claim: $\langle x,y \mid x^n, y^2, yxy^{-1} = x^{-1}\rangle$ is a presentation of D_n, via $\alpha : x \mapsto a,\ y \mapsto b$. For let G be the group with this presentation.
α extends to a homom. $G \xrightarrow{\text{onto}} D_n$, so enough to show $|G| \leq 2n$.
Let H be the subgp of G gend by x; since $x^n = 1$ in G, $|H| \leq n$.
Consider cosets $H,\ Hy$.

$$Hx = H, \quad Hyx \quad = Hx^{-1}y = Hy$$
$$Hy = Hy, \quad (Hy)y \quad = Hy^2 = H$$

G is gend by $\{x,y\}$, so any elt of G permutes $\{H, Hy\}$ by right mult. This action on cosets of H is transitive, so $\{H, Hy\}$ is a complete list of the cosets. Hence $(G:H) \leq 2$, so $|G| = |H|(G:H) \leq 2n$.

(3) $\langle X \mid \emptyset\rangle$ is a presn of the free gp on X.

(4) G any gp, $X = \{x_g \mid g \in G\}$ a set in 1-1 corr. with G via $g \mapsto x_g$. Let $R = \left\{x_g.x_h.x_{gh}^{-1} \mid g,\ h \in G\right\}$. Let H have presn $\langle X \mid R\rangle$.

$\exists$ homom. $H \xrightarrow{\text{onto}} G$ induced by $x_g \mapsto g$ ($g \in G$), and this is an isom. [Hint: in H, $x_{g_1}^{e_1} \ldots x_{g_n}^{e_n} = x_{g_1{}^{e_1} \ldots g_n{}^{e_n}}$.]

Hence $\langle X \mid R\rangle$ is a presentation of G, called the *standard presentation* of G, denoted $\langle G \mid \text{rel}(G)\rangle$.

Tietze transformations. Let $\langle X \mid R\rangle$ be a presn of G via α. Let F be free on X, N the normal subgp of F gend by R. Words in $X^{\pm 1}$ representing elts of N are called *consequences* of R.
w is a consequence of $R \Leftrightarrow \bar{\alpha}(w) = 1$.

Definition. A *Tietze transformation* of $\langle X \mid R\rangle$ is one of the following.

(T1) replace $\langle X \mid R\rangle$ by $\langle X \cup Y \mid R \cup \{y = w_y \mid y \in Y\}\rangle$, where Y is a set with $X \cap Y = \emptyset$ and for each $y \in Y$, w_y is a word in $X^{\pm 1}$.
(T2) The inverse of T1.
(T3) Replace $\langle X \mid R\rangle$ by $\langle X \mid R \cup S\rangle$, where S is a set of words in $X^{\pm 1}$ which are consequences of R.
(T4) The inverse of T3.

Theorem 1.4. *Two presentations $\langle X \mid R\rangle$ and $\langle Y \mid S\rangle$ are presentations of the same group if and only if one can be obtained from the other by a finite succession of Tietze transformations.*

Proof. Omitted. □

Example. The presentation $\langle x,y \mid yxy^{-1}x,\ x^n,y^2\rangle$ of D_n can be transformed as follows.

$$
\begin{aligned}
&\overset{\text{T1}}{\Longrightarrow} && \langle x,y,u \mid yxy^{-1}x,\ x^n,\ y^2,\ u=yx\rangle\\
&\overset{\text{T3}}{\Longrightarrow} && \langle x,y,u \mid yxy^{-1}x,\ x^n,\ y^2,\ u=yx,\ u^2=1\rangle\\
&\overset{\text{T4}}{\Longrightarrow} && \langle x,y,u \mid x^n,\ y^2,\ u=yx,\ u^2=1\rangle\\
&\overset{\text{T3\& T4}}{\Longrightarrow} && \langle x,y,u \mid x^n,\ y^2,\ u^2,\ x=y^{-1}u\rangle\\
&\overset{\text{T3\& T4}}{\Longrightarrow} && \langle x,y,u \mid (y^{-1}u)^n,\ y^2,\ u^2,\ x=y^{-1}u\rangle\\
&\overset{\text{T2}}{\Longrightarrow} && \langle y,u \mid (y^{-1}u)^n,\ y^2,\ u^2\rangle\\
&\overset{\text{T3\& T4}}{\Longrightarrow} && \langle y,u \mid y^2,\ u^2,\ (yu)^n\rangle\\
&\Longrightarrow && \langle a,b \mid a^2,\ b^2,\ (ab)^n\rangle
\end{aligned}
$$