Infinite Groups

Cornelia Druțu

University of Oxford

Part C course MT 2023, Oxford

Please note that the deadline for handing in your solutions to the Ex. Sheets has changed. In particular, for Sheet 1 it is next Monday.

Free groups

What is "the largest infinite group" generated by n elements ?

Finite sets: A larger than $B \Leftrightarrow \mathrm{card}(A) \geq \mathrm{card}(B) \Leftrightarrow$ there exists $f : A \to B$ onto.

Infinite groups: We look for a group $G = \langle X \rangle$, $\mathrm{card}(X) = n$, such that for every group $H = \langle Y \rangle$, $\mathrm{card}(Y) = n$, a bijection $X \to Y$ extends to an onto group homomorphism.

Clearly this cannot be done for any group G: if G is abelian then H would have to be abelian.

So G must be a group with no prescribed relation ("free").

Construction of a free group

$X \neq \emptyset$. Its elements = letters/symbols.

Take inverse letters/symbols $X^{-1} = \{a^{-1} \mid a \in X\}$.

We call $X \sqcup X^{-1}$ an alphabet.

A word w in $X \cup X^{-1}$ = a finite (possibly empty) string of letters in $X \cup X^{-1}$

$$a_{i_1}^{\epsilon_1} a_{i_2}^{\epsilon_2} \cdots a_{i_k}^{\epsilon_k},$$

where $a_i \in X, \epsilon_i = \pm 1$.

The length of w is k.

We will use the notation 1 for the empty word (the word with no letters). We say the empty word has length 0.

Construction of a free group 2

A word w is reduced if it contains no pair of consecutive letters of the form aa^{-1} or $a^{-1}a$.

The reduction of a word w is the deletion of all pairs of consecutive letters of the form aa^{-1} or $a^{-1}a$.

An insertion is the opposite operation: insert one or several pairs of consecutive letters of the form aa^{-1} or $a^{-1}a$.

Denote by X^* the set of words in the alphabet $X \cup X^{-1}$, empty word included.

Denote by $F(X)$ the set of reduced words in $X \cup X^{-1}$, empty word included.

We define an equivalence relation on X^* by $w \sim w'$ if w can be obtained from w' by a finite sequence of reductions and insertions.

Construction of a free group 3

Proposition

Any word $w \in X^*$ is equivalent to a unique reduced word.

Proof. Existence: By induction on the length of a word.

- For words of length 0 and 1, clearly true.
- Assume true for words of length n and consider a word of length $n+1$, $w = a_1 \cdots a_n a_{n+1}$, where $a_i \in X \cup X^{-1}$.
- By the induction assumption, there exists a reduced word $u = b_1 \cdots b_k$ with $b_j \in X \cup X^{-1}$ such that $a_2 \cdots a_{n+1} \sim u$.
- If $a_1 \neq b_1^{-1}$ then $a_1 u$ is reduced.
  If $a_1 = b_1^{-1}$ then $a_1 u \sim b_2 \cdots b_k$ and the latter word is reduced.

Construction of a free group 4

Uniqueness:

- For every $a \in X \cup X^{-1}$ we define a map $L_a : F(X) \to F(X)$ by

$$L_a(b_1 \cdots b_k) = \begin{cases} ab_1 \cdots b_k & \text{if} \quad a \neq b_1^{-1}\,, \\ b_2 \cdots b_k & \text{if} \quad a = b_1^{-1}\,. \end{cases}$$

- For every word $w = a_1 \cdots a_n$ define $L_w = L_{a_1} \circ \cdots \circ L_{a_n}$. For the empty word 1 define $L_1 = \mathrm{id}$.
- $L_a \circ L_{a^{-1}} = \mathrm{id}$ for every $a \in X \cup X^{-1}$. Hence $v \sim w$ implies $L_v = L_w$.
- If w is reduced then $w = L_w(1)$ (proof by induction on the length of w).
- If $v \sim w$ and w reduced then $w = L_v(1)$.
- This proves uniqueness. □

Construction of a free group 5

Definition

The free group over X is the set $F(X)$ endowed with the product $*$ defined by: $w * w'$ is the unique reduced word equivalent to the word ww'. The unit is the empty word.

Exercise

$F(X)$ is non-abelian if and only if $\mathrm{card}(X) \geq 2$.

Terminology: We call free non-abelian group a group $F(X)$ with $\mathrm{card}(X) \geq 2$.

Universal property of free groups

Proposition (Universal property of free groups)

A map $\varphi : X \to G$ from the set X to a group G can be extended to a homomorphism $\Phi : F(X) \to G$ and this extension is unique.

Proof. Existence.

- φ can be extended to a map on $X \cup X^{-1}$ by $\varphi(a^{-1}) = \varphi(a)^{-1}$.
- For every reduced word $w = a_1 \cdots a_n$ in $F = F(X)$ define

$$\Phi(a_1 \cdots a_n) = \varphi(a_1) \cdots \varphi(a_n).$$

- Set $\Phi(1_F) := 1_G$, the identity element of G.
- Exercise: check that Φ is a homomorphism.

Universal property of free groups

Uniqueness. Let $\Psi : F(X) \to G$ be a homomorphism such that $\Psi(x) = \varphi(x)$ for every $x \in X$.

Then $\Psi(x) = \varphi(x)$ for every $x \in X \cup X^{-1}$.

Hence for every reduced word $w = a_1 \cdots a_n$ in $F(X)$,

$$\Psi(w) = \Psi(a_1) \cdots \Psi(a_n) = \varphi(a_1) \cdots \varphi(a_n) = \Phi(w).$$

This finishes the proof. □

Terminology: If $\varphi(X) = Y$ is such that Φ is an injective homomorphism, $\Phi(F(X)) = H$, we say that $Y \subset G$ generates a free subgroup or that Y freely generates H.

Universal property of free groups

Corollary

An onto map $\varphi : X \to Y$, where Y is a generating set of a group G has a unique extension $\Phi : F(X) \to G$ that is an onto group homomorphism.

Corollary

Every group is a quotient of a free group.

Proof. Let $G = \langle X \rangle$. There exists $\Phi : F(X) \to G$ onto homomorphism. □

Always split

Proposition

Every short exact sequence as below splits

$$\{1\} \longrightarrow N \xrightarrow{\varphi} G \xrightarrow{\psi} F(X) \longrightarrow \{1\}\,. \tag{1}$$

Proof. Ex. Sheet 1.

Corollary

Every short exact sequence as below splits

$$\{1\} \longrightarrow N \xrightarrow{\varphi} G \xrightarrow{\psi} \mathbb{Z} \longrightarrow \{1\}\,. \tag{2}$$

A main source of free groups: ping-pong

The ping-pong lemma is a simple, yet powerful, tool for constructing free groups acting on sets.

Before formulating it, we will illustrate how it works on an example.

Example

For any real number $r \geqslant 2$ the matrices

$$g_1 = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \text{ and } g_2 = \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$$

generate a free subgroup of $SL(2, \mathbb{R})$.

Why is $\langle g_1, g_2\rangle$ free.

The group $SL(2,\mathbb{R})$ acts on the upper half plane $\mathbb{H}^2 = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ by linear fractional transformations

$$z \mapsto \frac{az+b}{cz+d}\,.$$

$g_1(z) = z + r,\ g_2(z) = \frac{z}{rz+1}$.

$I(z) = -\frac{1}{z} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} z$, $g_2 = I \circ g_1^{-1} \circ I^{-1}$.

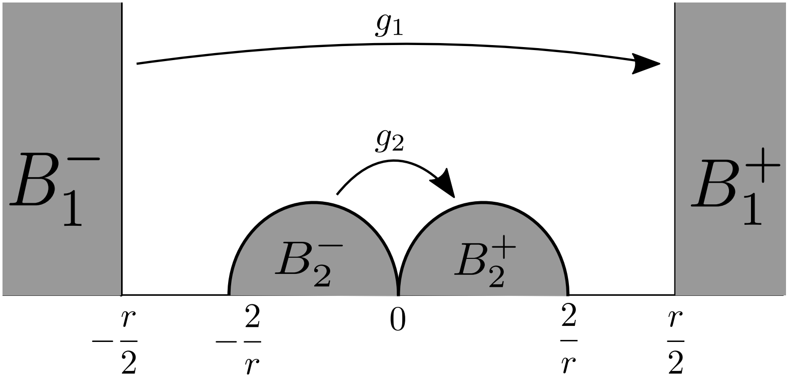
Define quarter-planes

$$B_1^+ = \{z \in \mathbb{H}^2 : \Re(z) \geqslant r/2\}, \quad B_1^- = \{z \in \mathbb{H}^2 : \Re(z) \leqslant -r/2\}$$

and half-disks $B_2^+ := \left\{z \in \mathbb{H}^2 : |z - \frac{1}{r}| \leqslant \frac{1}{r}\right\} = I(B_1^-)$ and

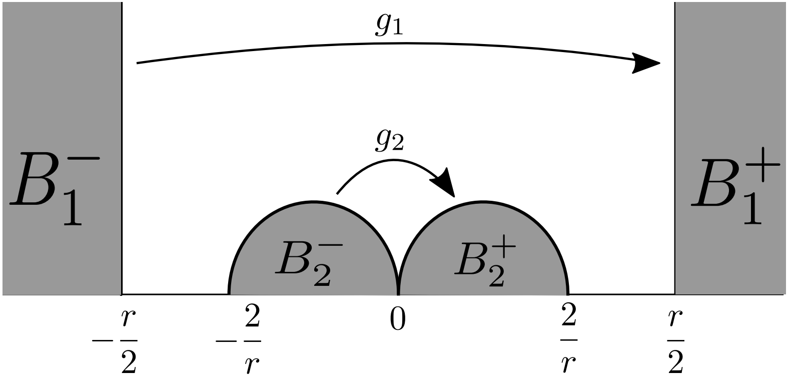
$$B_2^- := \left\{z \in \mathbb{H}^2 : |z + \frac{1}{r}| \leqslant \frac{1}{r}\right\} = I(B_1^+).$$

Example of ping-pong.



$g_1(\mathbb{H}^2 \setminus B_1^-) \subset B_1^+$, $g_1^{-1}(\mathbb{H}^2 \setminus B_1^+) \subset B_1^-$.
$g_2 = I \circ g_1^{-1} \circ I^{-1}$. $I(B_1^+) = B_2^-$ and $I(B_1^-) = B_2^+$. Therefore
$g_2(\mathbb{H}^2 \setminus B_2^-) \subset B_2^+$, $g_2^{-1}(\mathbb{H}^2 \setminus B_2^+) \subset B_2^-$.

Example of ping-pong.



Take a reduced word in $\{g_1^{\pm 1}, g_2^{\pm 1}\}$, say $g_1 g_2^{-1} g_1 g_2$.

$B_2^+ \sqcup B_1^- \sqcup B_1^+ \xrightarrow{g_2} B_2^+ \xrightarrow{g_1} B_1^+ \xrightarrow{g_2^{-1}} B_2^- \xrightarrow{g_1} B_1^+$