Geometric Group Theory

Cornelia Druțu

University of Oxford

Part C course HT 2024

Construction of a free group

Given n, we want to construct "the largest infinite group" generated by n elements.
This must be a group with no prescribed relation ("free").

Take $X \neq \emptyset$. Its elements = letters/symbols.
Take inverse letters/symbols $X^{-1} = \{a^{-1} \mid a \in X\}$.
We call $\mathcal{A} = X \sqcup X^{-1}$ an alphabet.
A word w in $\mathcal{A}$ is a finite (possibly empty) string of letters in $\mathcal{A}$

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

where $a_i \in X, \epsilon_i = \pm 1$. The length of w is k.
We use the notation 1 for the empty word (the word with no letters).
We say it has length 0.

$X^* =$ the set of words in the alphabet $\mathcal{A} = X \sqcup X^{-1}$, empty word included.

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 $a^{-1}a$.

$F(X) =$ the set of reduced words in $\mathcal{A}$, empty word included.

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

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

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.

Proposition

$\forall w \in X^*$, there exists a unique $u \in F(X)$ such that $w \sim u$.

Construction of a free group, Ping-pong lemma

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.

Example

Take $r \in \mathbb{R}$, $r \geq 2$,

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

$SL(2, \mathbb{R})$ acts by isometries on $\mathbb{H}^2 = \{z \in \mathbb{C} : Im(z) > 0\}$, *via*

$$g \cdot z = \frac{az+b}{cz+d}, \qquad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{R}).$$

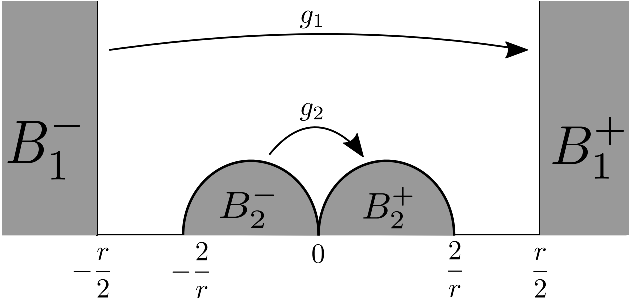
Why is $\langle g_1, g_2 \rangle$ free 1

Statement: We have that $\langle g_1, g_2 \rangle \leq SL(2, \mathbb{R})$ is isomorphic to $F(\{g_1, g_2\})$

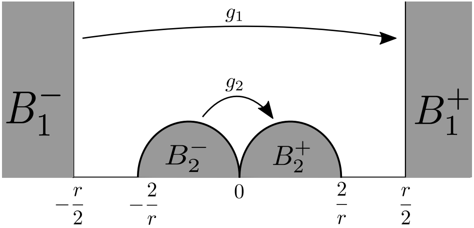
Proof

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

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



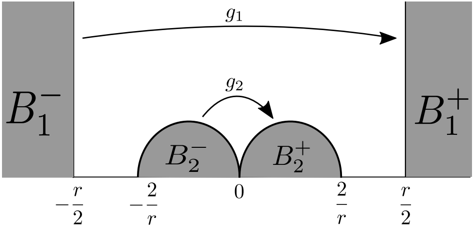
Why is $\langle g_1, g_2 \rangle$ free 2



$g_1(\mathbb{H}^2 \setminus B_1^-) \subset B_1^+$, $g_1^{-1}(\mathbb{H}^2 \setminus B_1^+) \subset B_1^-$.
g_2 does the same for $B_2^- = I(B_1^+)$, $B_2^+ = I(B_1^-)$.
Let $w = a_1 ... a_k$, $a_i \in \{g_1^{\pm}, g_2^{\pm}\}$, w in $F(\{g_1^{\pm}, g_2^{\pm}\}) \setminus \{1\}$.

Test 1: $\forall z \in \mathbb{H}^2 \setminus \bigcup_{i=1}^2 B_i^{\pm}$, $w(z) \in \bigcup_{i=1}^2 B_i^{\pm}$. And so $w(z) \neq z$.

Why is $\langle g_1, g_2 \rangle$ free 3



Test 2: Take $M = B_1^- \cup B_1^+$, $N = B_2^- \cup B_2^+$. Then $M \cap N = \emptyset$ and $g_1^n(N) \subset M$, $g_2^n(M) \subset N$.

Ping-Pong Lemma: Let G be a group acting on a set S and $a, b \in G$. If $\exists A, B$ non empty disjoint subsets of S s. t. $a^n B \subseteq A$ and $b^n A \subseteq B$, $\forall n \in \mathbb{Z} \setminus \{0\}$ then $\langle \{a, b\} \rangle \simeq F(\{a, b\})$. (Problem Sheet 1, Ex. 3). □

Free groups are the largest

Proposition (Universal Property of free groups)

Let X be a set and let G be a group. A map $\varphi : X \to G$ has a unique extension

$$\Phi : F(X) \to G$$

that is a group homomorphism.

Proof

- 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.

Free groups are the largest

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

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

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

□

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.

Example

$\{g_1, g_2\}$ freely generate $\langle g_1, g_2 \rangle \leq SL(2, \mathbb{R})$.

Free groups are the largest

Corollary

Every group $G = \langle X \rangle$, $\# X = n$, *is a quotient of a free group* $F(X)$.

Proof.

$X \hookrightarrow G$ extends to $\Phi : F(X) \to G$. Since $X \subset Im(\Phi)$, we have that

$$G \leq Im(\Phi) \leq G$$

and so Φ is onto. □

Rank of a free group

Corollary

Consider two groups G and H, $G = \langle X \rangle$.

1. *Every homomorphism $\phi : G \to H$ is uniquely determined by $\phi\big|_X : X \to H$. In particular there are at most $|H|^{|X|}$ homomorphisms.*
2. *If moreover $G = F(X)$ then there are exactly $|H|^{|X|}$ homomorphisms.*

Proof.

1. The map $\mathrm{Hom}(G, H) \to \mathrm{Map}(X, H), \phi \mapsto \phi\big|_X$ is injective. NB. It is not in general onto.
2. For $G = F(X)$ it is onto (by the Universal Property).

□

Rank of a free group

Proposition

$F(X) \simeq F(Y) \iff |X| = |Y|$ (X and Y can have any cardinality).

Proof.

$\Leftarrow$: Obvious. A bijection $f: X \to Y$ extends to an isomorphism.

$\Rightarrow$: If $|X| = \infty$, then $|X| = |F(X)| = |F(Y)| = |Y|$.

If $|X| < \infty$, then $|\mathrm{Hom}(F(X), \mathbb{Z}_2)| = 2^{|X|}$. Now, $F(X) \simeq F(Y)$ implies that there exists an isomorphism $\phi : F(X) \to F(Y)$. This induces a bijection

$$\mathrm{Hom}(F(Y), \mathbb{Z}_2) \to \mathrm{Hom}(F(X), \mathbb{Z}_2) \quad f \mapsto f \circ \phi$$

Hence $2^{|X|} = 2^{|Y|}$. So Y must also be finite and $|X| = |Y|$. □

Rank of a free group

Proposition

The rank of $F(X)$ is $|X|$.

Proof.

Suppose that $F(X) = \langle Y \rangle$, $|Y| < |X|$. Then

$$2^{|X|} = |\mathrm{Hom}(F(X), \mathbb{Z}_2)| \leq |\mathrm{Hom}(Y, \mathbb{Z}_2)| = 2^{|Y|}$$

Hence, $|X| \leq |Y|$ and we have a contradiction. □

Algorithmic problems for infinite groups

We begin with a loose formulation of some algorithmic problems (to be made more precise).

Word problem: Given a group $G = \langle X \rangle$, describe an algorithm or construct a Turing machine that would recognise when a word $w \in X^*$ satisfies $w = 1$ in G.

Example

$G = F(X)$. Given $w \in X^*$, reduce w to $u \in F(X)$. If $u \neq w_\emptyset$ then $w \neq 1$ in G.

Algorithmic problems for infinite groups

Conjugacy problem: Given $G = \langle X \rangle$, describe an algorithm that can recognise when $w, w' \in X^*$ are conjugate in G, i.e. there exists $g \in G$ such that $w = gw'g^{-1}$ in G.

Example: $G = F(X)$. Let $w, w' \in X^*$ and let $u, v \in F(X)$ be such that $w \sim u$, $w' \sim v$.

$u = a_1 ... a_n \in F(X)$ is cyclically reduced if all its cyclic permutations

$$a_1 ... a_n, \quad a_2 ... a_n a_1, \quad a_3 ... a_n a_1 a_2, \quad ..., \quad a_n a_1 ... a_{n-1}$$

are reduced. Equivalently, if $u \neq axa^{-1}$ where $a \in X \sqcup X^{-1}$.

Algorithmic problems for infinite groups

Proposition

1. *Every $u \in F(X)$ is conjugate to a cyclically reduced word.*
2. *If $u, v \in F(X)$ are cyclically reduced then they are conjugate if and only if they are cyclic permutations of each other.*

Proof: (1): Take $r \sim gug^{-1}$, $g \in F(X)$, r of minimal length. Then $r \neq axa^{-1}$.
(2): $(\Leftarrow)$ $a_2 ... a_n a_1 = a_1^{-1}(a_1 ... a_n)a_1$.

Algorithmic problems for infinite groups

Proposition

1. *Every $u \in F(X)$ is conjugate to a cyclically reduced word.*
2. *If $u, v \in F(X)$ are cyclically reduced then they are conjugate if and only if they are cyclic permutations of each other.*

($\Rightarrow$) Take u cyclically reduced. We will prove that if v is cyclically reduced and $v \sim gug^{-1}$ then v is a cyclic permutation of u. Argue by contradiction: let $g \in F(X)$ be of minimal length such that $v \sim gug^{-1}$ is not a cyclic permutation of u. So $u \sim g^{-1}vg$. First assume $g^{-1}vg$ is reduced. Then $u = g^{-1}vg$ in $F(X)$, contradicting the assumption that u was cyclically reduced. So $g^{-1}vg$ is not reduced, i.e. if $g = a_1 \dots a_n$ either $v = xa_1^{-1}$ or $v = a_1x$. In the first case, (the second case is similar) we have

$$g^{-1}vg = a_k^{-1} \dots a_2^{-1} a_1^{-1} x a_2 \dots a_n$$

By the minimal length assumption on g, $a_1^{-1}x$ is a cyclic permutation of u. Hence, $v = xa_1^{-1}$ is a cyclic permutation of u. Contradiction. □

Algorithmic problems for infinite groups

Using the previous proposition it is easy to solve algorithmically the conjugacy problem in $F(X)$:

1. Given $u, v \in F(X)$ find their conjugates $u', v' \in F(X)$ that are cyclically reduced (whenever a is the first letter and a^{-1} the last, delete both).

2. For $u', v' \in F(X)$ cyclically reduced thus found, check if they are cyclic permutations of each other.

Algorithmic problems for infinite groups

The previous proposition solves the conjugacy problem for $F(X)$ and also implies

Corollary

All non-trivial elements in $F(X)$ have infinite order.

Proof.

For all non-trivial $w \in F(X)$, $w = gug^{-1}$, u cyclically reduced and non-trivial. And for all cyclically reduced non-trivial u, u^n is reduced and hence $\neq w_\emptyset$. □

Corollary

If $g, h \in F(X)$ are such that $g^k = h^k$ for some k then $g = h$.