Geometric Group Theory

Cornelia Druţu

University of Oxford

Part C course HT 2023

About Mathematics

D. Hilbert, talking about an ex-student: "You know, for a mathematician, he did not have enough imagination. But he has become a poet and now he is fine."

Lucien Szpiro: "The difference between mathematicians and physicists is that after physicists prove a big result they think it is fantastic, but after mathematicians prove a big result they think it is trivial."

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): $(\Leftarrow)$ $a_2 \dots a_n a_1 = a_1^{-1}(a_1 \dots a_n)a_1$.

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 $g = a_1 ... a_n$ either $v = xa_1^{-1}$ or $v = a_1 x$. In the first case, (the second case is similar) we have

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

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 of 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 $g = h$.

Proof.

If both g, h are cyclically reduced then this is obvious.

Assume that g is not cyclically reduced and $g = xg_1x^{-1}$ with g_1 cyclically reduced. Then $g_1^k = h_1^k$ where h_1 is the reduced word $\sim x^{-1}hx$.

$$g_1 \text{ cyclically reduced } \Leftrightarrow g_1^k \text{ cyclically reduced}$$

Since $h_1^k = g_1^k$ we must also have that h_1 is cyclically reduced. So $h_1 = g_1$. Hence $h = g$. □