

The Banach–Tarski Paradox and Amenability

Lecture 3: Free Groups

7 August 2012

Paradoxical groups

Definition

Let G be a group. Subsets $A, B \subseteq G$ are said to be **equidecomposable**, denoted $A \sim B$, if A and B can each be partitioned into the same finite number of respectively G -congruent pieces.

Formally, $A = \cup_{i=1}^n A_i$ and $B = \cup_{i=1}^n B_i$ where for $1 \leq i < j \leq n$, $A_i \cap A_j = B_i \cap B_j = \emptyset$ and there are $g_1, \dots, g_n \in G$ such that for each $1 \leq i \leq n$, $g_i A_i = B_i$.

Definition

Let G be a group. Then G is **paradoxical** if one (hence both) of the following conditions hold:

1. There are two proper disjoint subsets A and B of G such that $A \sim G$ and $B \sim G$.
2. There are two proper disjoint subsets A and B of G such that $G = A \cup B$, $A \sim G$ and $B \sim G$.

Group presentations

Any group G has a presentation

$$G = \langle S \mid R \rangle$$

where S is a set of generators and R a set of relations.

Examples

1. $G = C_n$ the cyclic group of order n

$$G = \langle x \mid x^n = 1 \rangle$$

2. $G = D_{2n}$ the dihedral group of order $2n$

$$G = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$$

Informally, a free group is a group with no relations.

Group presentations

Care is needed with group presentations. For example consider

$$G_2 = \langle a, b \mid aba^{-1} = b^2 \rangle$$

$$G_3 = \langle a, b, c \mid aba^{-1} = b^2, bcb^{-1} = c^2, cac^{-1} = a^2 \rangle$$

$$G_4 = \langle a, b, c, d \mid aba^{-1} = b^2, bcb^{-1} = c^2, cdc^{-1} = d^2, dad^{-1} = a^2 \rangle$$

The groups G_2 and G_4 are infinite but G_3 is trivial (exercise).

Motivation: basis for a vector space

Let V be an n -dimensional vector space over a field K with basis $B = \{v_1, \dots, v_n\}$.

Theorem

If W is any vector space over K and $w_1, \dots, w_n \in W$, then there exists a unique linear transformation $T : V \rightarrow W$ such that $T(v_i) = w_i$ for $1 \leq i \leq n$.

Free abelian groups: definition via universal property

Definition

Let X be a subset of a group F . Then F is a **free abelian group** with **basis** X if, for every abelian group G and every function $f : X \rightarrow G$, there exists a unique homomorphism $\varphi : F \rightarrow G$ which extends f .

When X is a basis of the free abelian group F we have

$$F = \sum_{x \in X} \langle x \rangle \cong \mathbb{Z}^{|X|}$$

Theorem

Let F be a free abelian group with basis X and G a free abelian group with basis Y . Then $F \cong G$ if and only if $|X| = |Y|$.

The **rank** of a free abelian group with basis X is $|X|$, the cardinality of the set X .

Free groups: definition via universal property

Definition

Let X be a subset of a group F . Then F is a **free group** with **basis** X if, for every group G and every function $f : X \rightarrow G$, there exists a unique homomorphism $\varphi : F \rightarrow G$ which extends f .

We will show that X is a generating set for F and that every group G is the quotient of a free group, thus arriving at a rigorous definition of a group presentation.

Words

Notation

Let X be a set. Let X^{-1} be a set disjoint from X so that there is a bijection $X \rightarrow X^{-1}$ denoted $x \mapsto x^{-1}$. Let $1 \notin X \cup X^{-1}$.

Example

If $X = \{a\}$ then $X \cup X^{-1} \cup \{1\} = \{a, a^{-1}, 1\}$ has three elements.

Definition

A **word** on X is a sequence

$$w = (a_1, a_2, \dots)$$

where $a_i \in X \cup X^{-1} \cup \{1\}$ for all i , such that the sequence is eventually constant and equal to 1. More precisely, there is an $n \geq 0$ so that for all $i > n$, $a_i = 1$.

Example

The constant sequence $(1, 1, \dots)$ is a word called the **empty word**. It is also denoted by 1.

Words

Definition

A *word* on X is a sequence $w = (a_1, a_2, \dots)$ where $a_i \in X \cup X^{-1} \cup \{1\}$ for all i , such that the sequence is eventually constant and equal to 1.

Notation

A nonempty word will be written

$$w = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n}$$

where $a_i \in X$ for $1 \leq i \leq n$, $\varepsilon_i \in \{1, -1, 0\}$ for $1 \leq i < n$ and $\varepsilon_n \in \{\pm 1\}$.

Example

If $X = \{a\}$ and $w = (a, 1, a^{-1}, a, 1, 1, \dots)$ then write $w = a^1 a^0 a^{-1} a^1$.

Words

Notation

A nonempty word will be written $w = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n}$ where $a_i \in X$ for $1 \leq i \leq n$, $\varepsilon_i \in \{1, -1, 0\}$ for $1 \leq i < n$ and $\varepsilon_n \in \{\pm 1\}$.

Definitions

1. The **length** of the empty word $1 = (1, 1, \dots)$ is defined to be 0 and the **length** of $w = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n}$ is defined to be n .
2. If $w = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$ is a word then its **inverse** is the word $w^{-1} = a_n^{-\varepsilon_n} \cdots a_1^{-\varepsilon_1}$.
3. A word w is **reduced** if either w is empty or $w = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n}$ where all $a_i \in X$, all $\varepsilon_i \in \{\pm 1\}$ and a and a^{-1} are never adjacent.

Example

The inverse of $w = a^1 a^0 a^{-1} a^1$ is $w^{-1} = a^{-1} a^1 a^0 a^{-1}$. This word is not reduced.

Words

Definition

A word w is *reduced* if either w is empty or $w = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n}$ where all $a_i \in X$, all $\varepsilon_i \in \{\pm 1\}$ and a and a^{-1} are never adjacent.

Definition

A **subword** of $w = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n}$ is either the empty word or a word of the form $v = a_i^{\varepsilon_i} \cdots a_j^{\varepsilon_j}$ where $1 \leq i \leq j \leq n$.

So a nonempty word is reduced if and only if has no subwords $a^\varepsilon a^{-\varepsilon}$ or a^0 .

Multiplication of words

First we define multiplication on the set of all words:

if $w = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n}$ and $u = b_1^{\delta_1} b_2^{\delta_2} \cdots b_m^{\delta_m}$ then

$$wu := a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n} b_1^{\delta_1} b_2^{\delta_2} \cdots b_m^{\delta_m}$$

The product wu need not be reduced, even when both w and u are reduced.

To define multiplication of two **reduced** words w and u , we carry out all possible cancellations on wu . More precisely, we can write $w = w'v$ and $u = v^{-1}u'$ where v is a possibly empty word, such that $w'u'$ is reduced, and define the **juxtaposition** $wu := w'u'$.

Existence of free groups

Definition

Let X be a subset of a group F . Then F is a **free group** with **basis** X if, for every group G and every function $f : X \rightarrow G$, there exists a unique homomorphism $\varphi : F \rightarrow G$ which extends f .

Theorem

Given any set X there exists a free group $F = F(X)$ with basis X .

The free group $F(X)$ will be the set of all reduced words on X , under juxtaposition.

Examples of free groups

Examples

1. Let $X = \{a\}$. Then a reduced word on X is either empty or has the form $w = a^{\varepsilon_1} a^{\varepsilon_2} \cdots a^{\varepsilon_n}$ where either all $\varepsilon_i = 1$ or all $\varepsilon_i = -1$. If all $\varepsilon_i = 1$ denote w by a^n and if all $\varepsilon_i = -1$ denote w by a^{-n} . Then multiplication of reduced words $w = a^k$ and $u = a^l$ where $k, l \in \mathbb{Z}$ is given by $wu = a^{k+l} = a^{l+k} = uw$. So the free group $F(a)$ on $X = \{a\}$ is just the infinite cyclic group generated by a .
2. Let $X = \{a, b\}$. Then a reduced word on X is either empty or has the form $w = a^{k_1} b^{l_1} a^{k_2} b^{l_2} \cdots a^{k_n} b^{l_n}$ where each $k_i, l_i \in \mathbb{Z}$, possibly $k_1 = 0$ and possibly $l_n = 0$ but all other $k_i, l_i \neq 0$. The free group $F(a, b)$ on $X = \{a, b\}$ is nonabelian.

Definition

The **rank** of the free group on X is the cardinality of the set X .

Aside on free groups

Free groups are important in topology as the fundamental groups of graphs and of punctured surfaces. Algebraic topology can be used to give a short proof of:

Theorem

Every subgroup of a free group is free.

The following conjecture was posed in 1957 and proved by Mineyev (Annals 2012).

Hanna Neumann Conjecture

Let H and K be two nontrivial finitely generated subgroups of a free group F and let $L = H \cap K$. Then

$$\text{rank}(L) - 1 \leq (\text{rank}(H) - 1)(\text{rank}(K) - 1)$$

Free groups are also important in logic.

Group presentations

Definition

Let X be a subset of a group F . Then F is a **free group** with **basis** X if, for every group G and every function $f : X \rightarrow G$, there exists a unique homomorphism $\varphi : F \rightarrow G$ which extends f .

Theorem

Given any set X there exists a free group F with basis X .

Corollary

Every group G is a quotient of a free group.

Proof.

Let $X = \{a_g : g \in G\}$ so that $f : a_g \rightarrow g$ is a bijection $X \rightarrow G$. Then by definition there exists a (unique) homomorphism $\varphi : F(X) \rightarrow G$ such that $\varphi(a_g) = f(a_g) = g$ for all $g \in G$. Then φ is surjective, and so $G \cong F(X)/\ker(\varphi)$. □

Group presentations

Theorem

Given any set X there exists a free group $F(X)$ with basis X .

Corollary

Every group G is a quotient of a free group.

Definition

Let X be a set and let R be a family of words on X . A group G has **generators** X and **relations** R if

$$G \cong F(X)/\langle\langle R \rangle\rangle$$

where $\langle\langle R \rangle\rangle$ is the normal subgroup of $F(X)$ generated by R . The ordered pair $G = \langle X \mid R \rangle$ is called a **presentation** of G .

Group presentations

Examples

1. Let $X = \{a\}$ and $R = \{a^5\}$ (say). Then

$$G = F(X)/\langle\langle R \rangle\rangle = \langle a \mid a^5 = 1 \rangle$$

is the cyclic group of order 5.

2. Let $X = \{r, s\}$ and $R = \{r^n, s^2, rsrs\}$ for $n \geq 2$ an integer. Then

$$G = F(X)/\langle\langle R \rangle\rangle = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$$

is the dihedral group of order $2n$.