M4P61 Infinite Groups

Lectured by Dr Isabel Müller
Typed by David Kurniadi Angdinata

Autumn 2019

Syllabus

Contents

0 Introduction

Lecture 1
Thursday
03/10/19

Groups are ubiquitous throughout almost all areas in mathematics and many areas in physics. They arise naturally as the symmetries of classical mathematical objects, that is bijective maps which preserve the structure of the object studied. Well known groups include $\mathcal{S}_n$, the group of symmetries of a set of size n, or $\mathcal{D}_n$, the group of symmetries of a regular n-gon. From linear algebra we also know $\mathrm{GL}_n(\mathbb{R})$, the group of all invertible linear transformations of the vector space $\mathbb{R}^n$, and $\mathrm{O}(n)$, its subgroup of isometries. Historically, groups appeared for the first time in the work of Galois, when he tried to understand solutions of polynomial equations by studying the group of symmetries of their roots. He was the first to use the word group in the modern sense and that work dates back to 1829, when he was 18 years old. Another main contribution to the study of groups in mathematics came from Felix Klein's Erlangen program in 1872, in which he aimed to understand and classify euclidean, affine, projective, etc geometries by studying their group of symmetries. A huge milestone in the study of groups has been the classification of finite simple groups, which is a result based on the accumulated work of more than 100 authors on tens of thousands of pages published between 1954 and 2004.
This course will focus on infinite groups. More specifically, we will aim to study and understand groups by their actions on geometric objects. In that sense, we can consider the course program as an inverse of Klein's Erlangen program. This area of mathematics goes back to the 1980s, hence is comparably new, and is nowadays wider known as geometric group theory. The two leading questions will roughly be the following.

- If we know that a given group G admits an action with properties P on a space of type T, what does this tell me about the group G itself?
- Assume we are given a group G. Does it act on a given space T with properties P?

Our main goal in the first part will be the fundamental theorem of Bass-Serre theory, which states that a group acting on a tree is the fundamental group of a graph of groups. We first will introduce the notion of graphs in the sense of Serre and study group actions on these graphs. Afterwards, we will introduce free groups as the universal object in the class of groups and study how groups can arise as fundamental groups of graphs. We will see that groups can be presented by giving a set of generators accompanied with a set of relators and point out advantages and disadvantages of this viewpoint on groups.
In the second chapter, we will learn how to construct new groups out of given data via free products, free amalgamated products and HNN extensions. The counterpoint to this, that is the question on whether a given group decomposes into the amalgamated product or HNN extension of other groups, will be of special interest and we will approach it by understanding their actions on trees. This second part concludes with the introduction of graphs of groups and the fundamental theorem of Bass-Serre theory.
In the last part, we will investigate the word problem and its solvability in specific classes of groups. The word problem asks if two words on the generators of some group G represent the same element in it. Even for finitely presentable groups, the word problem is not always solvable, that is decidable. We will get to know Hopfian and residually finite groups as examples of classes in which the words problem actually is solvable. If time permits, we will conclude the lecture with an introduction into hyperbolic groups.
The following are reading material.

- R C Lyndon and P E Schupp, Combinatorial group theory, 2001
- P de la Harpe, Topics in geometric group theory, 2000
- O Bogopolski, Introduction to group theory, 2008
- J Rotman, An introduction to the theory of groups, 1995
- W Magnus, A Karrass, and D Solitar, Combinatorial group theory, 2005
- D Robinson, A course in the theory of groups, 1993

1 Geometric group theory

1.1 Bass-Serre graphs

Definition 1.1.1. A **graph** X is a tuple consisting of a set of vertices X^0, a set of edges X^1, together with functions $\alpha, \omega : X^1 \to X^0$ and $\bar{\cdot} : X^1 \to X^1$, such that $\overline{\overline{e}} = e$ and $\alpha(\overline{e}) = \omega(e)$ for every $e \in X^1$. We call $\alpha(e)$ the **initial vertex**, $\omega(e)$ the **terminal vertex**, and $\overline{e}$ the **inverse vertex**.

A convention is that unless otherwise specified, we identify edges e and e' if $\alpha(e) = \alpha(e')$ and $\omega(e) = \omega(e')$. The following are translations of notions.

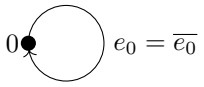
- A subgraph is an **induced** subgraph.
- A graph homomorphism ϕ from X to Y is a mapping from $X^i \to Y^i$ for $i = 0, 1$ such that $\phi(\alpha(e)) = \alpha(\phi(e))$ and $\phi(\overline{e}) = \overline{\phi(e)}$.
- Given $x \in X^0$, then we call the set $\{e \mid \alpha(e) = x\}$ the **star** of x, or $\operatorname{star} x$. The cardinality of $\operatorname{star} x$ is called the **valency** of x.
- A homomorphism $\phi : X \to Y$ is **locally injective** if and only if its restriction to $\operatorname{star} x$ is injective for all $x \in X^0$.
- An **orientation** of X is a choice of vertices $X^1_+ \subseteq X^1$ which picks exactly one of each pair $\{e, \overline{e}\}$.

Example 1.1.2.

- Fix $n \in \mathbb{N}_{\geq 1}$ for $n \neq 2$. Set

$$\mathcal{C}_n^0 = \{0, \dots, n-1\}, \qquad \mathcal{C}_n^1 = \{e_i, \overline{e_i} \mid i < n\}, \qquad \omega(e_i) = \alpha(e_{i+1}) = i + 1 \mod n_i, \qquad i < n.$$

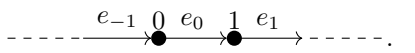
  Then $\mathcal{C}_1$ is



- $\mathcal{C}_\infty$ is given by

$$\mathcal{C}_\infty^0 = \mathbb{Z}, \qquad \mathcal{C}_\infty^1 = \{e_i, \overline{e_i} \mid i \in \mathbb{Z}\}, \qquad \omega(e_i) = \alpha(e_{i+1}).$$

  Then $\mathcal{C}_\infty$ is



The graphs $\mathcal{C}_n$ and $\mathcal{C}_\infty$ for $n \neq 2$ are called **circuits**.

Lecture 2
Tuesday
08/10/19

A sequence $p = e_1 \dots e_n$ with $e_i \in X^1$ is called a **path** from $\alpha(e_1) = x_0$ to $x_n = \omega(e_n)$ if and only if $\omega(e_i) = \alpha(e_{i+1})$ for all $i < n$. We consider vertices to be paths of length zero. A path is called **reduced** if $\overline{e_i} \neq e_{i+1}$. If p is a path, then $p^{-1} = \overline{e_n} \dots \overline{e_1}$ is called its **inverse path**. A path is called a **closed path** if $\omega(e_n) = \alpha(e_1)$.

Note.

- If we have a path p given, we can naturally consider it to be a subgraph via

$$X_p^0 = \{\alpha(e_i) \mid i < n\} \cup (\omega(e_n)), \qquad X_p^1 = \{e_1, \dots, e_n, \overline{e_1}, \dots, \overline{e_n}\}.$$

- If $p = e_1 \dots e_n$ is closed, then a permutation of the form

$$e_{i+1} \dots e_n e_1 \dots e_i$$

  is called a **cyclic permutation**. p is called **cyclically reduced** if every cyclic permutation is reduced.

Exercise 1.1.3.

- Let $\phi : X \to Y$ be a morphism of graphs. Then ϕ is locally injective if and only if the image of any reduced path is reduced.
- If p is closed and reduced, then it contains a circuit as a substructure.

If $p = e_1 \dots e_n$ and $q = f_1 \dots f_m$ such that $\omega(e_n) = \alpha(f_1)$ then we denote by

$$pq = e_1 \dots e_n f_1 \dots f_m.$$

A graph X is **connected** if for any $x, y \in X^0$ there is a path from x to y. A connected graph without circuits is called a **tree**.

Exercise 1.1.4.

- X is a tree if and only if for all $x, y \in X^0$ there is a unique reduced path from x to y.
- If X is connected and T is a tree, then any $\phi : X \to T$ locally injective is already injective and X is a tree.

Lemma 1.1.5. *Let X be a connected graph and $T \subseteq X$ a maximal subtree of X, then $T^0 = X^0$.*

Proof. Otherwise, there is some $x \in X^0 \setminus T^0$. As X is connected, there is some path p starting in T, ending in x. As $x \notin T^0$, there exists an edge in p such that $\alpha(e) \in T^0$ and $\omega(e) \notin T^0$. But then

$$T' = \left(T^0 \cup \{\omega(e)\}, T^1 \cup \{e\}\right)$$

is again a tree, a contradiction. □

Such a tree T is called a **spanning tree** for X.

1.2 Cayley graphs

Definition 1.2.1. Let G be a group and X a graph. We say that G **acts** on X if and only if it acts on X^0 and X^1 as sets, such that

- $g \cdot \alpha(e) = \alpha(g \cdot e)$, and
- $g \cdot \overline{e} = \overline{g \cdot e}$.

Note. This just means that

$$\begin{array}{rccc} \phi_g & : & X^0 & \longrightarrow & X^0 \\ & & x & \longmapsto & g \cdot x \end{array}$$

is a morphism of graphs for any $g \in G$.

Notation. gh is multiplication and $g \cdot h$ is action.

Remark. Given G and X arbitrary, then G acts on X by $g \cdot x = x$ and $g \cdot e = e$. Hence we will ask for nice properties of the action.

Definition 1.2.2. Assume G acts on a graph X. Then we say that G **acts without inversion of edges**, if $g \cdot e \neq \overline{e}$ for all $e \in X^1$. We say that G **acts freely** on X, if $g \cdot x = x$ if and only if $g = e_G$.

Definition 1.2.3. Let G be a group and $S \subseteq G \setminus \{e_G\}$.

- We say that S **generates** G, or G is **generated** by S, if there is no proper subgroup of G containing S. That is, the smallest subgroup H containing S equals G.
- If S has some property P, then we say that G is **P-ly generated**. For example, if S is finite, then G is finitely generated.
- If P is a property of subgroups, then S **P-ly generates** G, if the smallest subgroup of G containing S with property P, is already G. For example, if the smallest normal subgroup of G containing S is already G, then S normally generates G.

Example 1.2.4. $(\mathbb{Z}, +)$ is generated by $\{1\}$ or $\{-1\}$ or $\{-1, 1\}$ or $\{2, 3\}$ or $\mathbb{Z} \setminus \{0\}$.

Example 1.2.5. Let G be an infinite simple group. Then it is normally generated by any $g \in G \setminus \{e_G\}$. A question is can it be generated by g? No. G is cyclic and simple if and only if $G = \mathbb{Z}/p\mathbb{Z}$ for p prime. [1] A_∞ is an infinite simple group.

Lecture 3
Wednesday
09/10/19

Definition 1.2.6. Assume G is a group and $S \subseteq G \setminus \{e_G\}$. Then we define the graph $\Gamma(G, S)$ via

- the vertex set is $\Gamma(G, S)^0 = G$,
- the set of positive edges is $\Gamma(G, S)^1_+ = G \times S$,
- for e an edge, we have $\alpha((g, s)) = g$ and $\omega((g, s)) = gs$, and
- the inverse of (g, s) is $\overline{(g, s)} = \left(gs, s^{-1}\right)$, where

$$S^{-1} = \left\{s^{-1} \mid s \in S\right\}$$

is a set of new formal symbols. Thus $\left(g, s^{-1}\right) \notin G \times S$, even if as elements $s^{-1} = s' \in S$. If $s = s^{-1}$, this avoids troubles.

We consider $\Gamma(G, S)$ to be a labelled graph, where the label of (g, s) is s.

Exercise 1.2.7.

- $\Gamma(G, S)$ is connected if and only if S is a generating set for G.
- Otherwise set $H = \langle S \rangle \subsetneq G$. How does H relate to $\Gamma(G, S)$?

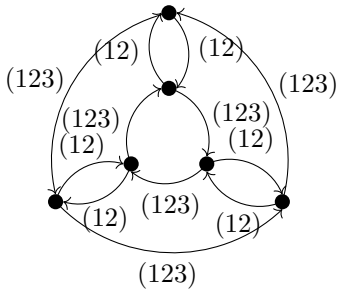
Definition 1.2.8. If G is a group and $S \subseteq G \setminus \{e_G\}$ generates G, then $\Gamma(G, S)$ is called the **Cayley graph** of G with respect to S.

Exercise 1.2.9. Given S a connected graph. Is there a group G and $S \subseteq G \setminus \{e_G\}$ such that $X \cong \Gamma(G, S)$, where S is a generating set?

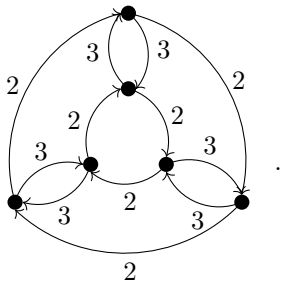
Example 1.2.10.

- Recall $\mathcal{C}_n$ and $\mathcal{C}_\infty$. Then
$$\mathcal{C}_n \cong \Gamma(\mathbb{Z}/n\mathbb{Z}, \{1\}), \qquad \mathcal{C}_\infty \cong \Gamma(\mathbb{Z}, \{1\}).$$
- Careful. Cayley graphs depend heavily on the choice of S. It is not always easy to determine whether it is cyclic. Consider
$$\Gamma_1 = \Gamma(\mathcal{S}_3, \{(123), (12)\}), \qquad \Gamma_2 = \Gamma(\mathbb{Z}/6\mathbb{Z}, \{2, 3\}).$$

Then



Γ_1



.

Γ_2

Given Γ_i, is the group abelian? A group is abelian if and only if all its generators commute, that is $ab = ba$. For Γ_2, if $a = 2$ and $b = 3$, then $(2)(3) = (3)(2)$.

[1] Exercise

Lemma 1.2.11. *Every group G acts on its Cayley graph by left multiplication. The multiplication is free, label-preserving, and without inversion of edges. Furthermore, every ϕ_g is a label-preserving automorphism of $\Gamma(G,S)$.*

Proof. Define the action via $h \cdot g = hg$ for all $h \in G$ and all $g \in \Gamma(G,S)^0$, and $h \cdot (g,s) = (hg,s)$. One checks easily that this defines an action. It is obviously label-preserving and hence without inversion of edges, as positive and negative edges have disjoint label sets. Now, if $h \cdot g = g$, then $hg = g$ and this $h = e_G$. Hence the action is free. Clearly, ϕ_h is injective, as $\phi_h(g_1) = \phi_h(g_2)$ if and only if $hg_1 = hg_2$ if and only if $g_1 = g_2$. For surjectivity, note that $g = hh^{-1}g$ and hence $g = h \cdot \left(h^{-1}g\right) = \phi_h\left(h^{-1}g\right)$. □

Lecture 4
Thursday
10/10/19

Lemma 1.2.12. *Let G be some group and $S \subseteq G \setminus \{e_G\}$ a generating set. Denote by $\mathrm{Aut}_L\,\Gamma(G,S)$ the label-preserving automorphism group of its Cayley graph. Then*

$$G \cong \mathrm{Aut}_L\,\Gamma(G,S).$$

Proof. By 1.2.11 we know that

$$\begin{array}{rccc} \Phi & : & G & \longrightarrow & \mathrm{Aut}_L\,\Gamma(G,S) \\ & & h & \longmapsto & \phi_h \end{array}.$$

One easily checks that this is a group homomorphism. If $\phi_h = \phi_g$, then in particular they agree on the vertex e_G, that is $h = \phi_h(e_G) = \phi_g(e_G) = g$, so $g = h$ and Φ is injective. Now consider $\phi \in \mathrm{Aut}_L\,\Gamma(G,S)$ arbitrary. We claim that $\phi = \phi_h$ with $h = \phi(e_G)$. As ϕ is label-preserving and every vertex has exactly one outgoing and one incoming edge with label s, we know that $\phi((g,s)) = (\phi(g),s)$. Hence

$$\phi(\omega((g,s))) = \omega(\phi((g,s))) = \omega((\phi(g),s)) = \phi(g)\,s.$$

As $\Gamma(G,S)$ is connected, we get that two label-preserving automorphisms agree if and only if they agree on one vertex. Now, $\phi(e_G) = h = \phi_h(e_G)$, so $\phi = \phi_h$. □

Example 1.2.13. The group of all automorphisms of $\mathcal{C}_n$ is called the **dihedral group** and denoted by $\mathcal{D}_n$. Note that every such automorphism is uniquely determined by its image on e_0. Hence if we consider $\alpha(e_0) = e_1$ and $\beta(e_0) = \overline{e_{n-1}}$, then

$$\mathcal{D}_n = \left\{a^k, a^k b \;\middle|\; k < n\right\}, \qquad \mathcal{D}_\infty = \left\{a^k, a^k b \;\middle|\; k \in \mathbb{Z}\right\}.$$

Exercise 1.2.14.

- Draw the Cayley graphs of $\mathcal{D}_n$ with respect to $S = \{a,b\}$.
- Prove that $\mathcal{D}_3 \cong \mathcal{S}_3$.
- Determine the axis of the reflection and the representation a^k and $a^k b$ for given ϕ just by using $\omega(\phi(e_0))$ and $\alpha(\phi(e_0))$.

1.3 Words and paths

Note. If for some group element g, both $g = s_1$ and $g^{-1} = s_2$ are in S, then we distinguish the edges $e_1 = (e_G, s_1)$ and $e_2 = \left(e_G, s_2^{-1}\right)$ even though $\alpha(e_1) = e_G = \alpha(e_2)$ and $\omega(e_1) = s_1 = g = s_2^{-1} = \omega(e_2)$.

Definition 1.3.1. Let S be any set. We say that w is a **word** on S if and only if it is a finite sequence of the form

$$w = s_1^{\epsilon_1} \dots s_n^{\epsilon_n}, \qquad s_i \in S, \qquad \epsilon_i = -1, 1.$$

We call S an **alphabet** and elements of S are **letters**. If $S \subseteq G$, then every word in S considered as a product, defines some group element. We write

$$w \underset{G}{=} s_1^{\epsilon_1} \dots s_n^{\epsilon_n} \underset{G}{=} g,$$

and we say that w **represents** G.

Example 1.3.2. Consider $\mathbb{Z}$ with $S = \{s_0 = -1, s_1 = 1\}$. Then $w_1 = s_0 s_1 \neq s_1^{-1} s_1 = w_2$ but $w_1 \underset{G}{=} w_2$.

Remark 1.3.3. If S is a generating set for G, then for every $g \in G$, every word in S corresponds to a unique path $p_w(g)$ in the Cayley graph starting at g and ending at gh, where $h \underset{G}{=} w$.

Example 1.3.4. Let $\mathbb{Z} \times \mathbb{Z}$ and $S = \{a = (1,0), b = (0,1)\}$. Consider

$$w_1 = aabbab^{-1}, \qquad w_2 = baaa, \qquad w_3 = aba^{-1}a^{-1}.$$

Then $w_1 \underset{G}{=} w_2$ and $w_3 \underset{G}{=} ba^{-1} \underset{G}{=} a^{-1}b$.

Definition 1.3.5. A word $w = s_1^{\epsilon_1} \dots s_n^{\epsilon_n}$ on S is called **reduced** if and only if $s_i = s_{i+1}$ implies that $\epsilon_i = \epsilon_{i+1}$.

Consider $s \in G$ with $s^2 = 1$. Then $s \underset{G}{=} s^{-1}$ and $w = ss^{-1}$ is not reduced. But $w' = ss$ is reduced.

1.4 Free groups

Lecture 5
Tuesday
15/10/19

Fact 1.4.1 (Tits alternative)**.** If G is an infinite linear group, then either it is virtually solvable, that is there is a finite index subgroup which is solvable, or it contains a non-abelian free group as a subgroup.

Definition 1.4.2 (Free groups I)**.** Let G be a group and $S \subseteq G \setminus \{e_G\}$ be any subset of G. Then G is called **free on** S, or a **free group with basis** S, if and only if every element of G can be represented uniquely as a reduced word on S.

Remark. This implies that S generates G.

Example. Let G be finite. Then for all $s \in S$ there exists $n \in \mathbb{N}_{>0}$ such that $s^n \underset{G}{=} e_G$, so not unique.

Exercise 1.4.3 (Free groups II)**.** A group G is **free on** $S \subseteq G$ if and only if $\Gamma(G, S)$ of G with respect to S is a tree and $S \cap S^{-1} = \emptyset$, considered as an intersection in G.

Example 1.4.4. Consider the subgroup $F \subseteq \mathrm{SL}_2(\mathbb{Z})$ generated by

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

Then F is free on $S = \{A, B\}$. First note that

$$A^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}, \qquad B^n = \begin{pmatrix} 1 & 0 \\ 2n & 1 \end{pmatrix}.$$

Clearly, F acts on $\mathbb{R}^2$. Set

$$U = \{(x, y) \mid |x| < |y|\}, \qquad V = \{(x, y) \mid |x| > |y|\}.$$

Then

$$\begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 2ny \\ y \end{pmatrix},$$

so $A^n(U) \subseteq V$ for all $n \geq 1$. Similarly, $B^n(V) \subseteq V$. Assume

$$w = A^{k_0} B^{l_0} \dots A^{k_{n-1}} B^{k_{n-1}} A^{k_n}, \qquad |k_i|, |l_i| > 0, \qquad k_0, l_0, k_n \geq 0$$

is an arbitrary word on S. Assume $w \underset{G}{=} e_G = I$. Now, if $|k_n|, |k_0| > 0$ then $w(U) \subseteq V$. But $U \cap V = \emptyset$, a contradiction. Otherwise consider w', the word which arises by conjugating by a high enough power of A, so $w' = A^N w A^{-N}$. Then w' is of the above form. But $w' \underset{G}{=} e_G$ if and only if $w \underset{G}{=} e_G$, a contradiction.

Remark. This proof generalises to the so-called ping-pong lemma, telling when two subgroups $\langle A \rangle$ and $\langle B \rangle$ appear as a free product $\langle A \rangle * \langle B \rangle$.

Lecture 6 is a problem class.

Lecture 6
Wednesday
16/10/19

Lecture 7
Thursday
17/10/19

Proposition 1.4.5 (Free groups III)**.** *Let S be an arbitrary non-empty set. Then there is a* ***group*** $\mathrm{F}(S)$ ***which is free on*** S*.*

Proof.

- Set $S^{\pm} = \{s^{\epsilon} \mid \epsilon = -1, 1\}$. If $s_1 = s_2^{-1} \in S^{\pm}$, identify $s_1^{-1} = \left(s_2^{-1}\right)^{-1} = s_2$. Set $\mathrm{F}'(S)$ to be the set of all words on S. As usual, we denote the empty word by ϵ. Further, for two words u_1 and u_2 given by $u_i = s_{i,1}^{\epsilon_{i,1}} \dots s_{i,n_i}^{\epsilon_{i,n_i}}$ let $u_1 u_2 = s_{1,1}^{\epsilon_{1,1}} \dots s_{1,n_1}^{\epsilon_{1,n_1}} s_{2,1}^{\epsilon_{2,1}} \dots s_{2,n_2}^{\epsilon_{2,n_2}}$. Note that this is not a group, since no inverses.
- We will define an equivalence relation on $\mathrm{F}'(S)$. Say that $u \sim v$ if and only if there exists a finite sequence of words such that $u = u_0, \dots, u_n = v$ and each u_{i+1} arises from u_i by inserting or deleting a subword of the form ss^{-1} for $s \in S^{\pm}$. We say that u is reduced, if it does not contain a subword ss^{-1}.
- Claim that every equivalence class contains exactly one reduced word. Assume $u \sim v$. Then there exists $u = u_0, \dots, u_n = v$. Choose this sequence such that $\sum_{i=0}^{n} |u_i|$ is minimal, where $|u_i|$ denotes the word length of u_i. As u and v are reduced, we know that $|u_0| < |u_1|$ and $|u_n| < |u_{n-1}|$. Then there exists $0 < i < n$ such that $|u_{i-1}| < |u_i|$ and $|u_{i+1}| < |u_i|$. Say, u_i arises from u_{i-1} by adding ss^{-1} and u_{i+1} from u_i by deleting tt^{-1}. Now either ss^{-1} and tt^{-1} are disjoint in u_i, then replace the sequence $u_{i-1}u_iu_{i+1}$ by $u_{i-1}u_i'u_{i+1}$ where u_i' arises from u_{i-1} by deleting tt^{-1}, or not, then cancelling the subsequence u_iu_{i+1} still gives a connecting sequence from u to v. In both cases we obtain a sequence of smaller length, a contradiction.
- Denote by $[u]$ the class $u/\sim$. We set $[u][v] = [uv]$. This is clearly independent of choice, that is if $u' \sim u$, then $u'v \sim uv$. Hence associativity is clear. Also, if $w = s_1^{\epsilon_1} \dots s_n^{\epsilon_n}$, then $[w] = [s_1^{\epsilon_1}] \dots [s_n^{\epsilon_n}]$. Hence $[S] = \{[s] \mid s \in S\}$ generates $\mathrm{F}(S)$. By the claim, every word has a unique reduced representation in $[S]$. Hence $\mathrm{F}(S)$ is free on $[S]$.

□

Proposition 1.4.6 (Free groups IV)**.** *Assume F is a group and $S \subseteq F$ is any set. Then F is a* ***free group with basis*** *S if and only if F is the universal object in the class of groups with respect to S, that is whenever G is a group and $f : S \to G$ is any map, there exists a unique group homomorphism $\phi : F \to G$ extending f, so*

$$\begin{array}{ccc} S & \xrightarrow{f} & G \\ {\scriptstyle \mathrm{id}}\uparrow & \nearrow_{\exists! f} & \\ F & & \end{array} .$$

Proof.

$\Longrightarrow$ Assume F is free on S and $f : S \to G$ is any map. We first prove uniqueness of ϕ. By definition, for any $g \in F$ there exists a unique reduced word on S such that $w \underset{F}{=} g$, say $w = s_1^{\epsilon_1} \dots s_n^{\epsilon_n}$. Then, if $\phi : S \to G$ is a homomorphism of groups extending f, clearly,

$$\phi(g) = f(s_1)^{\epsilon_1} \dots f(s_n)^{\epsilon_n}.$$

Hence unique. Now for existence we prove that this actually is a homomorphism of groups, that is $\phi(gh) = \phi(g)\phi(h)$. Let $w_g \underset{F}{=} g$ and $w_h \underset{F}{=} h$ be reduced. Then $w_g w_h \underset{F}{=} gh$, but maybe not reduced. Say w_{gh} is the reduced word. If $w_g w_h$ is not reduced, then $w_g = w_g^1 w_g^2$ and $w_h = w_h^1 w_h^2$ such that $w_g^2 = \left(w_h^1\right)^{-1}$. Then clearly

$$\phi(gh) = f\left(w_g^1 w_h^2\right) = f\left(w_g^1\right) f\left(w_g^2\right) f\left(w_h^1\right)^{-1} f\left(w_h^2\right) = \phi(g)\phi(h).$$

Hence ϕ is indeed a group homomorphism.

$\Longleftarrow$ Let F be any group and $S \subseteq F$ such that for any group G and $f : S \to G$ there exists a unique homomorphism $\phi : F \to G$ extending f. First, consider $G_1 = \langle S \rangle \leq F$. Then the map $f : S \to F$ sending S to itself extends to some $\phi : F \to F$ with image G_1. But also, the homomorphism $\mathrm{id}_F : F \to F$ is a homomorphism extending f. By uniqueness, $\phi = \mathrm{id}_F$ whence $\langle S \rangle = G_1 = F$. Hence S generates F. Next, consider $G = \mathrm{F}(S)$ and $f : S \to \mathrm{F}(S)$ the natural embedding from S into $\mathrm{F}(S)$. We want to show that any element in F has a unique reduced representation on S. Indeed, assume $w = s_1^{\epsilon_1} \dots s_n^{\epsilon_n}$ is reduced for $n > 0$, but $w \underset{F}{=} e_F$. Then any homomorphism $\phi : F \to \mathrm{F}(S)$ extending f has to send w_G simultaneously to $e_{\mathrm{F}(S)}$ and to $w_{\mathrm{F}(S)}$, hence $e_{\mathrm{F}(S)} \underset{\mathrm{F}(S)}{=} w$, a contradiction.

□