BACHELOR THESIS

Cayley-graphs

and

Free Groups

Author:	Martina Pflegpeter
Student Number:	0606219
Study:	A 033 621 Mathematik
Advisor:	Dr. Bernhard Krön

Vienna, 01.03.2010

Slovenian-Austrian Cooperation project (ÖAD)

Ljubljana, Leoben, Vienna

Bernhard Krön, Aleksander Malnič, Primož Potočnik, Norbert Seifter, Primož Šparl et al.

CONTENTS

1. CAYLEY-GRAPHS

In the following we establish the basics of Cayley graphs of a group. This first section is heavily based on Chapter 2.1 of Oleg Bogopolski‘s *Introduction of Group Theory* [1].

Definition 1.1. We say that a group G *acts on a set on the left* if for each $g \in G$ and $m \in M$, an element $gm \in M$ is defined such that $g_2(g_1x) = (g_2g_1)x$ and $1x = x$ for all $m \in M$, $g_1, g_2 \in G$.

Definition 1.2. A graph $X = (VX, EX)$ is a pair consisting of a nonempty set of vertices VX, a set of edges $EX$and three mappings $o : EX \to VX$, $t : EX \to VX$, $^{-} : EX \to EX$ such that $\bar{\bar{e}} = e$, $\bar{e} \neq e$ and $o(e) = t(\bar{e})$ for every $e \in EX$.

Let X and Y be graphs. Then $\varphi : (VX, EX) \to (VY, EY)$ is called a *(graph-) morphism* if for all edges e
$\varphi(o(e)) = o(\varphi(e))$, $\varphi(t(e)) = t(\varphi(e))$ and $\varphi(\bar{e}) = \overline{\varphi(e)}$.
If φ is bijective then it is called an *isomorphism*. An isomorphism of a graph to itself is called an *automorphism* and the set $\mathrm{Aut}(X)$ of all automorphisms forms a group by composition, the *automorpism group* of X.

A graph X is called *oriented* if in each pair of its mutually inverse edges $e, \bar{e}$ one edge is chosen to be called the *positively oriented* edge, while the other edge is called *negatively oriented*. We denote the set of all positively oriented edges by EX^+, the negatively oriented edges by EX^-, and call the set EX^+ an *orientation* of the graph X.

A sequence $p = e_1e_2 \dots e_n$ of edges is called a *walk* of length n if $t(e_i) = o(e_{i+1})$, where $i \in \{1, \dots, n-1\}$. A walk is called a *path* if $o(e_i) \neq o(e_j)$, where $i \neq j$, $i \in \{1, \dots, n\}$, $j \in \{1, \dots, n\}$. Any vertex v of X is a *(degenerate)* path of length 0 with the beginning and the end at v. A path p is called *reduced* if it is either degenerate or $p = e_1e_2 \dots e_n$, where $e_{i+1} \neq \overline{e_i}$ for $i \in \{1, \dots, n-1\}$, and *closed* if its beginning and end coincide. A closed path is also called a *circuit*. We define the *product* of a path $p = e_1 \dots e_n$ and another path $p' = e'_1 \dots e'_k$, where $t(p) = o(p')$, to be the path $pp' = e_1 \dots e_n e'_1 \dots e'_k$.

A graph X is connected if for any two vertices u and v of X there exists a path in X from u to v. A connected graph without circuits is a *tree*.

Definition 1.3. We say that a *group G acts on a graph* X (on the left) if (left) actions of G on the sets VX and EX are defined such that $go(e) = o(ge)$ and $g\bar{e} = \overline{ge}$ for all $g \in G$ and $e \in EX$. The neutral element 1 of G acts as identity

on VX. We say that G acts on X *without inversion of edges* if $ge \neq \bar{e}$ for all $e \in EX$ and $g \in G$.
The action is called *free* if $gv \neq v$ for all $v \in VX$ and all $g \in G \setminus \{1\}$.
Informally, we define a *barycentric subdivision* B_X of a graph X to be a graph, which can be obtained from X by a "subdivision" of each edge $e \in EX$ into two edges e_1 and e_2 and by adding a new vertex v_e corresponding to the "middle" of the edge e. According to this definition B_X satisfies the relations $(\bar{e})_2 = \bar{e}_1$, $(\bar{e})_1 = \bar{e}_2$ and $v_e = v_{\bar{e}}$.
An action of a group G on the graph B_X is defined by setting $ge_1 = (ge)_1$, $ge_2 = (ge)_2$ and $gv_e = v_{ge}$. The action of G on the vertices of B_X, which are the vertices of X, is preserved.

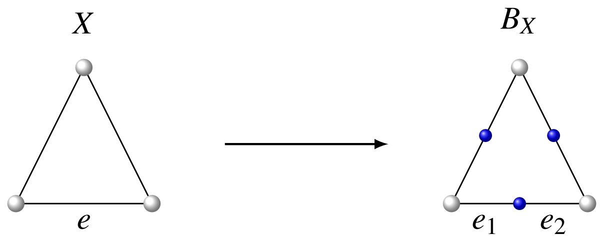


FIGURE 1. Barycentric subdivision of the graph X.

So, if G acts on a graph, then G acts without inversion of edges on its barycentric subdivision.

Definition 1.4. Let G be a group and $S \subseteq G$ be a subset of G. Then the oriented graph with set of vertices G, set of positively oriented edges $G \times S$, and functions o and t defined by $o((g,s)) = g$ and $t((g,s)) = gs$, where $(g,s) \in G \times S$, is denoted by $\mathrm{Cay}(G,S)$. The inverse of the edge (g,s) is the edge (gs, s^{-1}) and the *label* of an edge (g,t) is the element t.

The group G acts on $\mathrm{Cay}(G,S)$ by left multiplication. That is, an element $g_1 \in G$ maps a vertex g_2 to g_1g_2 and an edge (g_2,t) to (g_1g_2,t). This action is free.

Definition 1.5. Let G be a group and S be a generating set of G. Then the graph $\mathrm{Cay}(G,S)$ constructed in Definition 1.4 is called the *Cayley graph of G with respect to S*.

2. FREE GROUPS

In this section we establish the existence of free groups with an arbitrary basis, as described in [1] Chapter 2.3. Free groups play an important role in combinatorial group theory, as we will begin to see in Section 3 discussing presentations. For example Theorem 2.10 says, that any group is a factor group of an appropriate free group, or that any group is obtainable as a homomorphic image of a free group, respectively.

Let A be an arbitrary set and $A^{-1} = \left\{a^{-1} \mid a \in A\right\}$. We assume that $A \cap A^{-1} = \emptyset$ and $(a^{-1})^{-1} = a$. The set $A^{\pm} = A \cup A^{-1}$ is called an *alphabet*. Its elements are called *letters*. A finite sequence of letters written in the form $a_1 a_2 \dots a_n$, $n \geq 0$, $a_i \in A^{\pm}$, is called a *word*, whereas for $n = 0$ we have the *empty word*. Any subsequence of consecutive letters of a word is a *subword*. Given a word $f = a_1 a_2 \dots a_n$, the number n is called the *lenght* of f and is denoted $|f|$.
Let W be the set of all words in the alphabet $A^{\pm}$. Given two words f and g of W, we define their product by juxtaposition (concatenation) as the word fg. If $A \neq \emptyset$ then W in combination with this composition is not a group since a nonempty word has no inverse. So we introduce an equivalence relation on W and define a product on the set of equivalence classes to obtain a group. Two words u, v are called equivalent if there exists a finite sequence of words $u = f_1, f_2, \dots, f_k = v$ such that each f_{j+1} can be obtained from f_j by insertion or deletion of subwords of the form aa^{-1}, where $a \in A^{\pm}$. We call such a sequence a *sequence connecting the word* u *and* v.
Let $[F]$ denote the set of equivalence classes of words of W and $[f]$ the class containing the word f. A word g is called *reduced* if it does not contain subwords of the form aa^{-1}, where $a \in A^{\pm}$.

Proposition 2.1. *Any class $[f]$ contains a unique reduced word.*

Proof. Since the existence of a reduced word in the class $[f]$ is evident, it is left to prove the uniqueness. We do so by using the so called *pick reduction method*.
Suppose there exist two different reduced words u, v in $[f]$. From all sequences connecting u with v, we choose a sequence $u = f_1, f_2, \dots, f_k = v$ with minimal sum $\sum_{i=1}^{k} |f_i|$. Since the words u, v are reduced and different, it follows that $|f_1| < |f_2|$ and $|f_k| > |f_{k-1}|$. Therefore there exists $i \in \{2, \dots, k-1\}$ such that $|f_{i-1}| < |f_i|$ and $|f_i| > |f_{i+1}|$. So f_{i+1} can be obtained from f_{i-1} in two steps: first we insert a subword aa^{-1} and get f_i, and then we delete a subword bb^{-1}. If these subwords have an empty intersection in f_i, we can interchange the steps, which means first we delete bb^{-1} and get a new word f_i', and then we insert aa^{-1}. Hence we can replace the triple f_{i-1}, f_i, f_{i+1} by f_{i-1}, f_i', f_{i+1} and get a new sequence connecting u and v with smaller sum of length, which is a contradiction. If the subwords aa^{-1} and bb^{-1} of f_i have a nonempty intersection, it follows that $f_{i-1} = f_{i+1}$ and

we can delete the words f_i and f_{i+1} from the chosen connecting sequence. Again this is a contradiction to the minimality of the sum of lengths. $\square$

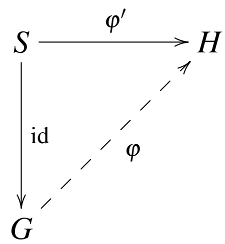
Definition 2.2. Let F be a group and let A be a linearly subset of F such that $A \cap A^{-1} = \emptyset$. The group F is called a *free group with the basis* A if every nontrivial element f can be uniquely represented as a product $f = a_1 a_2 \ldots a_n$, where $a_i \in A \cup A^{-1}$ and $a_i a_{i+1} \neq 1$ for all i. Such an expression is called *reduced with respect to* A. Further we assume that the trivial element is represented by the empty reduced expression.

Theorem 2.3. *For any set A there exists a free group with basis A.*

Proof. We define a multiplication on the set $[F]$ by $[f][g] = [fg]$ and prove that $[F]$ is a free group with basis $[A] = \{[a] \mid a \in A\}$:
The multiplication is associative, the identity element is the class $[\emptyset]$ and the inverse of the class $[f] = [a_1 \ldots a_n]$, where $a_i \in A^{\pm}$, is the class $[a_n^{-1} \ldots a_1^{-1}]$. Besides $[f] = [a_1] \ldots [a_n]$, and this expression is reduced with respect to $[A]$ if and only if the word $a_1 \ldots a_n$ is reduced. The fact that each class of $[F]$ contains exactly one reduced form (see Proposition 2.1) implies the uniqueness of the reduced form of elements of $[F]$ with respect to $[A]$. $\square$

We denote the free group with basis A by F_A and consider the elements of this group as words in the alphabet $A^{\pm}$, considering two words as equal if the corresponding reduced words are equal.

Definition 2.4. ***(Universal property)*** The group G satisfies the *universal property with respect to* S, $S \subset G$, if $\langle S \rangle = G$ and for all groups H and for all maps $\varphi' : S \to H$ there exists a homomorphism $\varphi : G \to H$ with $\varphi|_S = \varphi'$. A group is callend *free over* S if it satisfies the universal property with respect to S.



The map id in the diagram denotes the identity. We call G a free group with basis S (with respect to the universal property) if for any group H and any map $\varphi' : S \to H$ there exists a unique extension of φ' to a homomorphism $\varphi : G \to H$.

Theorem 2.5. *The Definitions 2.2 and 2.4 are equivalent.*

Proof. (⇐): Let F_A be a free group with a basis A in the sense of Definition 2.2 and let φ' be a map from A to a group G. We have to show that there is a unique way of extending φ' to a homomorphism φ from F_A to G. An arbitrary element $f \in F$ is of the form $f = a_1 \dots a_n$, where $a_1, \dots, a_n \in A^{\pm}$. This form is unique except for a finite number of insertions and deletions of words of the form $a_i a_i^{-1}$, where $a_i \in A^{\pm}$. Now we set

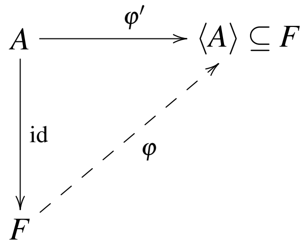
$$\varphi(f) = \varphi(a_1 \dots a_n) = \varphi(a_1) \dots \varphi(a_n)$$

and

$$\varphi(f^{-1}) = \varphi((a_1 \dots a_n)^{-1}) = \varphi((a_n^{-1}) \dots (a_1^{-1})) = \varphi((a_n)^1 \dots (a_1)^{-1}) =$$

$$= (\varphi(a_1) \dots \varphi(a_n))^{-1} = \varphi(a_1 \dots a_n)^{-1} = \varphi(f)^{-1}$$

(⇒): Let F be a free group with basis A in the sense of Definition 2.4 We can extend the identity embedding $A \to \langle A \rangle$ to a homomorphism $F \to \langle A \rangle$ and further to a homomorphism $F \to F$ with image $\langle A \rangle \subseteq F$. So the homomorphism φ and the identity homomorphism $F \to F$ both extend the identity embedding $A \to F$. But extensions are unique. Hence they must coincide, which implies that F equals $\langle X \rangle$.



Now it is left to show that the reduced form of elements in F with respect to A is unique. To do so we consider the homomorphism $F \to [F]$, which is an extension of the mapping $a \mapsto [a]$, where $a \in A$. Hence F with the universal property satisfies Definition 2.2.

□

Theorem 2.6. *All bases for a given free group F have the same cardinality.*

Proof. Let S be a basis of a free group F. To prove the theorem we will show that the cardinality of S only depends on F. Let therefore $\mathbb{Z}_2 = \{0, 1\}$ be the group of residues modulo 2 and H be the additive group consisting of all functions $f : S \to \mathbb{Z}_2$ with $f(x) = 1$ for only a finite number of $x \in S$. The addition in H is defined by $(f + g)(x) = f(x) + g(x)$, where $x \in S$. Then we associate with each $x \in S$ the function

$$f_x(y) = \begin{cases} 1 & y = x \\ 0 & y \neq x \end{cases}$$

and define $\varphi' : S \to H$, which maps x to f_x. We can extend φ' to an epimorphism $\varphi : F \to H$, whose kernel consists of all words in F in which for every $x \in S$ the total number of occurrences of x and x^{-1} is even.
We have to prove that $\ker\varphi = \langle w^2 \mid w \in F \rangle$. Evidently the right side of the equation only contains words with the required property that the total number of x and x^{-1} is even. The converse inclusion follows with the identities

$$xuxv = xux(uu^{-1})v = (xu)^2u^{-1}v\,,$$
$$x^{-1}uxv = x^{-1}(x^{-1}x)ux(uu^{-1})v = x^{-2}(xu)^2u^{-1}v\,,$$

as well as induction on the length n of a word from $\ker\varphi$. For $n = 2$ we have $xx = x^2$ or $xx^{-1} = id (= id^2)$. Let u and v be words with length $|u| = n-1$, $|v| \leq n-1$ and $u = u_1^2$, $v = v_1^2$ for some $u_1,\ v_1 \in F$. Now we have two choices of concatenating x, so that the total number of occurrences of x and x^{-1} in the new word is even . These are $xuxv$ and $x^{-1}uxv$. With the identities from above we see that $\ker\varphi \subseteq \langle w^2 \mid w \in F \rangle$. With the First Isomorphism Theorem, which can be found in [2], p. 19, we see that $H \cong F/\langle w^2 \mid w \in F \rangle$ and hence the cardinality of H does not depend on the choice of S.
On the other hand, from the definition of H it follows that $|H| = 2^{|S|}$ if S is finite, or $|H| = |S|$ if S is infinite respectively. So the cardinality of S only depends on F. □

Definition 2.7. The *rank* of a free group F, denoted $\mathrm{rk}(F)$, is the cardinality of some (equivalently, any) basis of F.

Corollary 2.8. *Two free groups are isomorphic if and only if their ranks coincide.*

Corollary 2.9. *If $\psi : F_Y \to F_X$ is an epimorphism, then $|Y| \geq |X|$.*

Proof. Let $\varphi : F_X \to H$ be the epimorphism from the proof of Theorem 2.6, where the group H can be considered as a vectorspace over $\mathbb{Z}_2$ with basis $\{f_x \mid x \in X\}$. The set $\varphi(\psi(Y))$ generates H. □

The following claim as well as a proof of it, can be found in [2] Chapter 1.3, p 15.
If H is a subgroup of a group G, the following statements about H are equivalent.

(i) $xH = Hx$ for all $x \in G$
(ii) $x^{-1}Hx = H$ for all $x \in G$
(iii) $x^{-1}hx \in H$ for all $x \in G$, $h \in H$

The notation $H \lhd G$ indicates that H is a normal subgroup of G. The quotient group (or factor group) of H in G, denoted by G/H, is the set of all cosets of H in G together with the group operation $(xH)(yH) = (xy)H$.

This operation is well-defined since for $x' = xa$ and $y' = yb$ with $a, b \in H$, $x'y' = xayb = xy(y^{-1}ay)b \in (xy)H$. Also this operation is associative, the inverse of xH is $x^{-1}H$ and the identity element is H. The cardinality of G/H is equal to $|G : H|$. Information about quotient groups can be found in [2], pp. 18.

Theorem 2.10. *An arbitrary group G is a factor group of an appropriate free group.*

Proof. Let Y be an arbitrary set generating the group G. By Theorem 2.5 there exists a homomorphism from the free group F_Y to the group G, extending the identity mapping $Y \to Y$. This homomorphism is an epimorphism. □

3. Presentations

We have seen that every group is a factor group of an appropriate free group. In this section we introduce presentations of groups as in [2], Chapter 2.2., pp. 50 and give some important examples.

Definition 3.1. A *(free) presentation* of a group G is an epimorphism $\pi : F \to G$, where F is a free group. If $\mathscr{R} = \ker \pi$ then $\mathscr{R} \lhd F$ and $F/\mathscr{R} \cong G$. The elements of $\mathscr{R}$ are called the *relators* of the presentation.

Choose a set of free generators Y of F, and a subset R of F such that $\langle R^F \rangle = \mathscr{R}$, where $R^F = \left\{ \prod_{i=1}^{k} f_i^{-1} r_i^{\pm 1} f_i \mid f_i \in F, r_i \in R, k \geq 0 \right\}$ is the normal closure of R in F. If $Y_\pi = \pi(Y)$, then Y_π is a set of generators of G. We denote the presentation π of the group G by

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

or

$$\langle Y_\pi \mid r(y) = 1, r \in R \rangle$$

respectively.

The following theorem is useful in the discussion of groups with similar presentations.

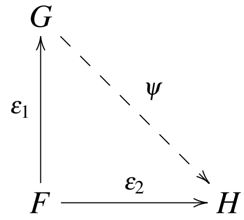
Theorem 3.2. (von Dyck) *Let G and H be groups with presentations* $\varepsilon_1 : F \to G$ *and* $\varepsilon_2 : F \to H$ *such that each relator of* ε_1 *is also a relator of* ε_2*. Then the function*

$$\psi : G \to H$$

$$\varepsilon_1(f) \mapsto \varepsilon_2(f)$$

is a well- definded epimorphism.

Proof. Supposse that $\ker \varepsilon_1 \leq \ker \varepsilon_2$.



If $g \in G$, then $g = \varepsilon_1(f)$ for some $f \in F$. If $g = \varepsilon_1(f_1)$ also, then $f = f_1 k$, where $k \in \ker \varepsilon_1 \leq \ker \varepsilon_2$. This implies $\varepsilon_1(f) = \varepsilon_2(f_1)$ and we see that $\psi : G \to H$ is an epimorphism. □

Example 3.3.

(i) $G = \langle x, y \mid x^2 = y^2 = (xy)^n = 1 \rangle$, where $n \geq 2$.
This group is called the *dihedral group* D_n *of order* $2n$. The dihedral group is the group of symmetries of a regular polygon, including rotations and reflections.

As an example consider the complete automorphism group of a cycle X of length 4:

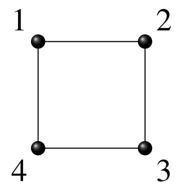


FIGURE 2. Cycle X of length 4.

Let a be the rotation for $-\frac{\pi}{2}$ and b be the reflection on the second median. Then the group $\mathrm{Aut}(X) = \langle a, b \mid a^4 = b^2 = (ba)^2 = e \rangle$ contains 8 elements and is isomorphic to D_4.

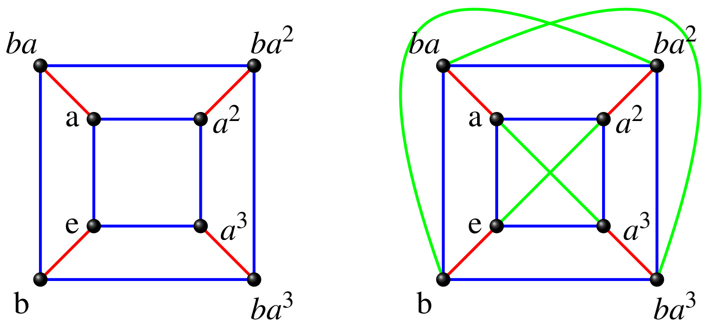
As we see in Figure 3.B, the elements $c = a^2$ und b generate a subgroup $H = \langle b, c \rangle$ of order 4 in $\mathrm{Aut}(X)$.
The previous example, as well as an table of the automorphism group of an regular quadrangle, can be found in [5], pp. 55.

(ii) $G = \langle x, y \mid x^2 = 1, y^2 = 1 \rangle$.
This group is called the *infinite dihedral group* D_∞ .

(iii) A presentation of the symmetric group:

Theorem 3.4. *If* $n > 1$*, there is a presentation of the symmetric group* S_n *with generators* $x_1, x_2, \ldots, x_{n-1}$ *and relations*

$$1 = x_i^2 = (x_j x_{j+1})^3 = (x_k x_l)^2 \tag{3.1}$$



(A) $\mathrm{Cay}(\mathrm{Aut}(X),\{a,b\})$ (B) $\mathrm{Cay}(\mathrm{Aut}(X),\{a,b,c\})$

FIGURE 3. Cayley graphs of $\mathrm{Aut}(X)$ with generating sets $\{a,b\}$ and $\{a,b,c\}$.

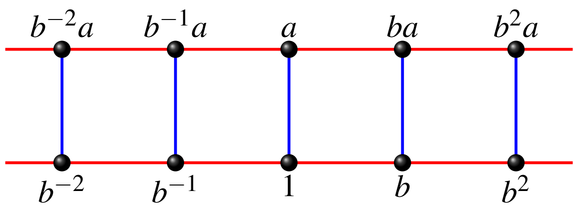


FIGURE 4. The Cayley graph of D_∞ with generating set $\{a,b\}$.

where $1 \le i \le n-1, 1 \le j \le n-2$, *and* $1 \le l < k-1 < n-1$.

Proof. Let G be a group with the generators and defining relations listed. First we show that $|G| \le n! = |S_n|$.
Let $H = \langle x_1, \dots, x_{n-2}\rangle$. By *von Dyck's* Theorem 3.2 and induction on n it follows that $|H| \le (n-1)!$, so it is enough to prove that $|G : H| \le n$.
Consider the n right cosets H, Hx_{n-1}, $\dots$, $Hx_{n-1}x_{n-2}\dots x_1$ and show that right multiplication by any x_j permutes these cosets. For $j < i-1$ we have $x_ix_j = (x_ix_j)^{-1} = x_jx_i$ by 3.1. Therefore $(Hx_{n-1}\dots x_i)x_j = Hx_jx_{n-1}\dots x_i = Hx_{n-1}\dots x_i$, since $x_j \in H$. Now let $j > i$. Since $x_kx_j = x_jx_k$ for $|j-k| > 1$, we have

$$(Hx_{n-1}\dots x_i)x_j = Hx_{n-1}\dots x_{j+1}(x_jx_{j-1}x_j)x_{j-2}\dots x_i.$$

By 3.1 we have the relation $(x_{j-1}x_j)^3 = 1$, which implies that $x_{j-1}x_jx_{j-1} = x_jx_{j-1}x_j$. So we have

$$(Hx_{n-1}\dots x_i)x_j = Hx_{n-1}\dots x_{j+1}(x_{j-1}x_jx_{j-1})x_{j-2}\dots x_i =$$
$$= Hx_{j-1}x_{n-1}\dots x_i = Hx_{n-1}\dots x_i.$$

At last

$$(Hx_{n-1}\dots x_i)x_i = Hx_{n-1}\dots x_{i+1}$$

and

$$(Hx_{n-1}\dots x_i)x_{i-1} = Hx_{n-1}\dots x_i x_{i-1}.$$

Since the x_j generate G, every element of G lies in one of these cosets and $|G:H| \le n$.

Finally we show that S_n actually realizes the presentation. Consider the $n-1$ adjacent transpositions $\pi_i = (i, i+1)$, $i \in \{1,\dots,n-1\}$. Every permutation is a product of transpositions and every transposition is a product of adjacent transpositions, as can be seen by repeated use of the formula

$$(i, j) = (j-1, j)(i, j-1)(j-1, j)$$

where $i < j-1$. So $S_n = \langle \pi_1,\dots,\pi_{n-1}\rangle$ and we just have to verify that $1 = \pi_i^2 = (\pi_j\pi_{j+1})^3 = (\pi_k\pi_l)^2$, with $1 \le i \le n-1, 1 \le j \le n-2$ and $1 \le l < k-1 < n-1$. By Theorem 3.2 there exists an epimorphism $\psi : G \to S_n$ which maps x_i to π_i. Since $|G : Ker\psi| = n!$ and $|G| \le n!$, we see that $Ker\psi = 1$ and ψ is an isomorphism.

□

In Figure 5 we see the Cayley graph of S_3 with respect to the generating set $\{(12),(123)\}$.

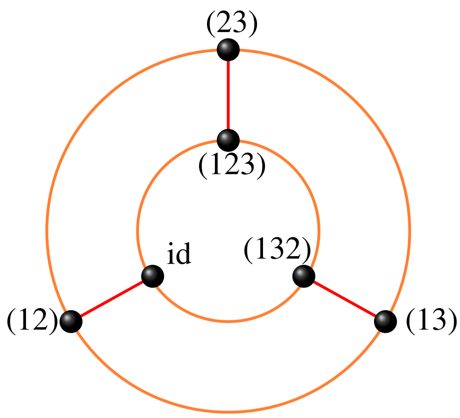
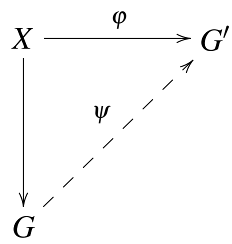


FIGURE 5. The Cayley graph of S_3 with generating set $\{(12),(123)\}$

The following two theorems can be found in [1], p. 60.

Theorem 3.5. *Let G be a group presented by generators and defining relations $\langle X \mid R\rangle$, and let G' be another group. Every map $\varphi : X \to G'$ such that $\varphi(r) = 1$ for all $r \in R$ can be extended to a homomorphism $\psi : G \to G'$.*

Proof.



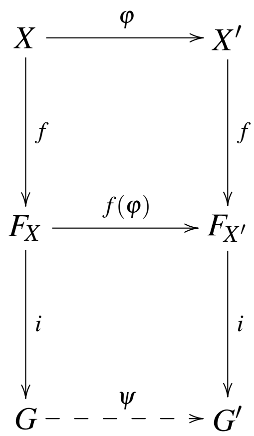
An arbitrary element $g \in G$ can be written as $g = x_1 \dots x_n$, $x_i \in X^+ \cup X^-$. The desired homomorphism ψ must be defined by $g \mapsto \varphi(x_1)\dots\varphi(x_n)$, so if $x_1 \dots x_n = 1 \in G$, then $\varphi(x_1)\dots\varphi(x_n) = 1 \in G'$ (because φ maps all words from the normal closure of R in F_X to 1).

□

A reformulation of this result is the following theorem.

Theorem 3.6. *Let G and G' be groups presented by generators and defining relations $\langle X \mid R\rangle$ and $\langle X' \mid R'\rangle$. Then every map $\varphi : X \to X'$ with the property that all words $\varphi(r)$, $r \in R$, lie in the normal closure of the set R' in $F_{X'}$ can be extended to a homomorphism $\psi : G \to G'$.*

Proof.



□

4. Free Groups and Cayleygraphs

Sabidussi‘s Theorem, but without proof, can be found in [5], p. 57.

Theorem 4.1. (Sabidussi) *A graph X is a Cayley graph of a group G if and only if it admits a free and transitive action of G on X.*

Proof. Let S be a generating set of the group G.

(⇒): The group G acts on the Cayley graph $X(G,S)$ by left multiplication. This action is free and transitiv.

(⇐): We have a free and transitive action of G on X. First we identify the vertices VX of X with group elements of G. Choose $id \in VX$, where id is the identiy. We map id to an arbitrary $x \in VX$ and transcribe the colouring of the edges, which means we identify each edge $e \in EX$ with an element $s \in S$. Each $s \in S$ is allowed to be identified with more than one edge in X, but each edge $e \in EX$ has a unique color. Suppose that there exist group elements $g_1, g_2 \in G$ and x, y with $x^{-1}y \in S$. Then

$$x = g_1(id) = g_2(id)$$
$$g_1^{-1}(y) \neq g_2^{-1}(y)$$

which means g_1 and g_2 map different $s_i \in S$ to the pair (x, y).
But that leads to a contradiction. Consider $h = g_1^{-1}g_2$. Then

$$h(id) = g_1^{-1}g_2(id) = g_2^{-1}(x) = id$$

and

$$h(v) = g_1^{-1}g_2(v) = g_1^{-1}g_2(g_2^{-1}(y)) = g_1^{-1}(y).$$

So $h(id) = id$, but $h(g_2^{-1}(y)) \neq g_2^{-1}(y)$.
Finally we have to show that X with that colouring is $\mathrm{Cay}(G, S)$.

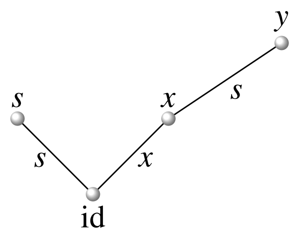


FIGURE 6

G has to act on X by left multiplication. So X has to satisfy $s(x) = xs = y$, where $s \in S, x, y \in G$, by Definition 1.5. Suppose $x \in S \subseteq G$. We see that $x = x(id)$ and $s(x) = xs = y$.

□

Not every transitive graph is a Cayley graph of a group. For example we consider the *Peterson graph P*. Let $G := \left\langle Rot_{-\frac{2\pi}{5}}, \psi, s \right\rangle$ be the group generated by rotation of $-\frac{2\pi}{5}$, ψ, where ψ means "evert" , and s, where s means fixing four vertices and flipping the others.

Although G acts transitive on P, the Peterson graph is not the Cayley graph of G. The group G, the automorphism group of P, is isomorphic to S_5, so it has $5! = 120$ elements. The order of the element $Rot_{-\frac{2\pi}{5}}$ is 5, the order of ψ is 4 and s is an involution, so its order is 2. There are

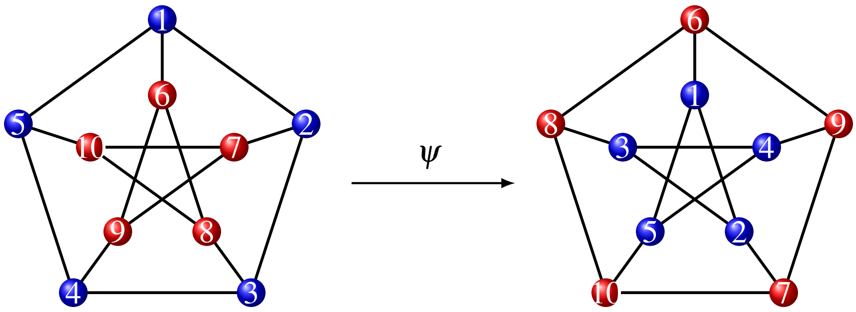


FIGURE 7. The operation ψ on the Peterson graph P.

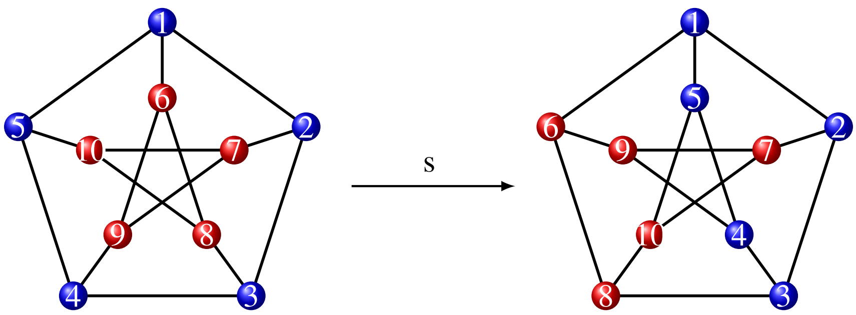


FIGURE 8. The operation s on the Peterson graph P.

5 different ways of fixing four elements and flipping the others from the inner circle to the outer circle and vice versa. All these permutations can be obtained by our generators. So the group G contains 20 elements generated by $Rot_{-\frac{2\pi}{5}}$ and ψ and five times an inner/outer-circle-permutation applied to these elements. So the entire sum of elements of G is 120. This implies that G contains far too many elements to have P as its Cayley graph, respectively to act free on P.
On the other hand, the group we are searching for has cardinality 10. This criterion is satisfied by two groups, namely $\mathbb{Z}_{10}$ and the dihedral group D_5. But neither $\mathbb{Z}_{10}$ nor D_5 acts transitive on the Peterson graph. So we see that P is no Cayley graph.

5. FREE GROUPS AND TREES

In this section be discuss the classifying property of the Cayley graph of a free group. Further we discuss subgroups of free groups. By doing so, we follow the first part of [1], Chapter 2.8.

Proposition 5.1. *Let* $\mathrm{Cay}(G,S)$ *be the Cayley graph defined by a group* G *and a subset* S *of* G*. Then* $\mathrm{Cay}(G,S)$ *is a tree if and only if* G *is a free group with basis* S*.*

Before we prove the previous proposition we note the following:

Remark 5.2. The graph $\mathrm{Cay}(G,S)$ is connected if and only if S is a generating set of G.
If $\mathrm{Cay}(G,S)$ is connected, then every vertex of $\mathrm{Cay}(G,S)$ can be obtained by actions of elements of S. So every group element of G can be generated by combining elements of S. Hence S is a generating set of G.
On the other hand, if S is a generating set of G, we construct a Cayley graph as in the proof of Sabidussi‘s Theorem 4.1.

Proof of Proposition 5.1. For an edge (g,t) with $t \in S^{\pm}$ we define its label to be $s(e) = t$. Then $t(e) = o(t)s(e)$ and $t(e_n) = o(e_1)s(e_1)\dots s(e_n)$ for any path $e_1 \dots e_n$.

- ($\Leftarrow$): Let G be a free group with basis S. Then the graph $\mathrm{Cay}(G,S)$ is connected by Remark 5.2. Suppose there exists a closed reduced path $e_1 \dots e_n$ in $\mathrm{Cay}(G,S)$. Then $t(e_n) = o(e_1)$ by definition and therefore $s(e_1)\dots s(e_n) = 1$. Because S is a basis of G, there exists an index i such that $s(e_i) = (s(e_{i+1}))^{-1}$. But then the edge $e_k = \overline{e_{k+1}}$, wich is a contradiction. So the graph $\mathrm{Cay}(G,S)$ is a tree.
- ($\Rightarrow$): The Cayley graph of the group G with basis S is a tree. Since relations between generators take shape in cycles in the corresponding Cayleygraph, there are no relations between the generating elements S of G.

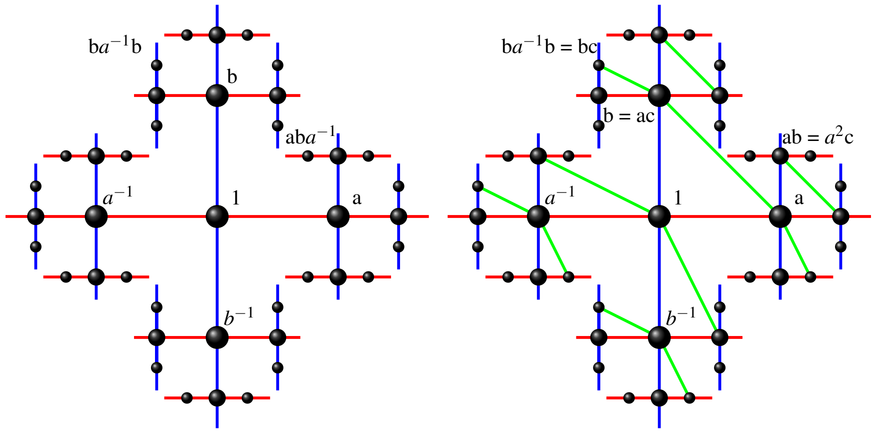
$\square$

If we consider the group F_2 with two different generating sets, we see that $\mathrm{Cay}(F_2,S)$ is a tree only if F_2 is free with respect to S. So $\mathrm{Cay}(F_2,\{a,b\})$ is a tree, while for $c = ab$ the Cayley graph $\mathrm{Cay}(F_2,\{a,b,c\})$ is not.

Corollary 5.3. *Any free group acts freely and without inversion of edges on a tree.*

Proof. Let F be a free group with a basis S. The group F acts by left multiplication on its Caley graph $\mathrm{Cay}(F,S)$. This action is free and without inversion of edges, and $\mathrm{Cay}(F,S)$ is a tree. $\square$

Before we discuss subgroups of free groups, we have to give some further definitions and claims. See [1], p. 48.
Let G be a group acting on a graph X without inversion of edges. For $x \in VX \cup EX$, the orbit of x with respect to this action is denoted by $\mathcal{O}(x) = \{gx \mid g \in G\}$. We define the *factor graph* X/G as the graph with vertices $\mathcal{O}(v)$, where $v \in VX$, and edges $\mathcal{O}(e)$, where $e \in EX$, such that:



(A) $\langle a,b \rangle$

(B) $\langle a,b,c \mid ac = b \rangle$ $\langle a,b,c \mid acb^{-1} \rangle$

FIGURE 9. The Cayley graph of F_2 with two different generating sets

(i) $\mathscr{O}(v)$ is the beginning of the edge $\mathscr{O}(e)$ if there exists $g \in G$ such that gv is the beginning of e

(ii) the inverse of the edge $\mathscr{O}(e)$ is the edge $\mathscr{O}(\bar{e})$

Since G acts on X without inversion of edges, $\mathscr{O}(e)$ and $\mathscr{O}(\bar{e})$ do not coincide. The morphism $p : X \to X/G$ given by $p(x) = \mathscr{O}(x)$, where $x \in VX \cup EX$, is called a *projection*. Any preimage of y with respect to p, where y is a vertex or an edge of the factor graph X/G, is called a *lift* of y in X.

As an example, the following figure shows a factor graph of the Cayley graph of S_3.

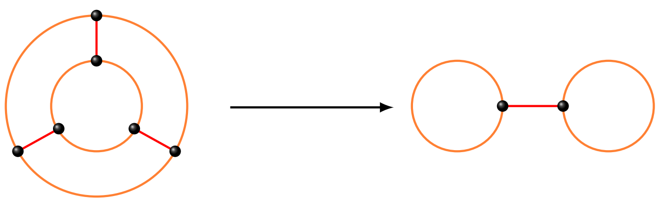


FIGURE 10. A factor graph of $\mathrm{Cay}(S_3, \langle (123) \rangle)$

We have to consider the following claims.

(i) Let e be an edge of a factor graph X/G and v be a lift of $o(e)$. Then there exists a lift of e with initial vertex v. By definition of the factor graph X/G $o(e)$ is the beginning of e if there exists a $l \in G$ such that

lv is the beginning of the lift of e. So l is the lift of e that we were looking for.

(ii) The cardinality of the set of edges of a connected graph X lying outside some maximal subtree T_X does not depend on the choice of T_X. If X is a finite connected graph with an orientation EX_+, then the number of positively oriented edges of X not belonging to T_X equals $|EX_+| - |VX| + 1$.

Theorem 5.4. *Let F be a group acting freely and without inversion of edges on a tree X. Then F is free and its rank is equal to the cardinality of the set of positively oriented edges of the factor graph $Y := X/F$ (for any choice of its orientation) lying outside some maximal tree. In particular, if Y is finite, then*

$$rk(F) = |EY_+| - |VY| + 1$$

Proof. Let $p : X \to Y$ be the canonical projection of the tree X onto the factor graph $Y = X/F$. In Y we choose a maximal subtree T_Y and lift it to a subtree T_X in X. Distinct vertices of T_X are not equivalent under the action of F and each vertex of X is equivalent to some uniquely defined vertex of T_X.We define in Y an arbitrary orientation and lift this orientation to X, that is we assume that an edge of X is positively oriented if and only if its image in Y is.
Let E_Y be the set of positively oriented edges of Y outside T_Y. By claim (i), for each $e_Y \in E_Y$ there exists a lift l of e_Y with initial vertex $o(e_Y) \in T_X$. The freeness of the action implies that such a lift is unique. Since if we suppose, from an arbitrary vertex of T_X would emanate two distinct but equivalent edges, the element carrying one edge to the other would fix this vertex. The end of l lies outside T_X, otherwise l would lie in T_X and so e_Y in T_Y. Let E_X be the set of all positively oriented edges in X with initial vertices in T_X and terminal vertices outside T_X. Then the projection p is a bijective mapping from E_X onto E_Y. The terminal vertex of each edge $e \in E_X$ is equivalent to a unique vertex v_e from T_X. The element f_e of F mapping v_e to the terminal vertex $t(e)$ of e is unique, again by the freeness of the action of F on X.
We will show that F with basis $S = \{f_e \mid e \in E_X\}$ is a free group. Subtrees fT_X, where $f \in F$, are disjoint and the set of their vertices coincides with the set of vertices VX of the tree X. Let h be a positively oriented edge from X lying outside the union of these subtrees. Then h connects two of these subtrees. Let these be (f_1T_X) and (f_2T_X). Then we contract each subtree fT_X onto one vertex and denote it by (fT_X). So we are able to form a new subtree X_{T_X}, in which the edge h connects the vertices (f_1T_X) and $f_2T_X)$. By Proposition 5.1 it is sufficient to show that X_{T_X} is isomorph to $\mathrm{Cay}(F,S)$. So we define an isomorphism on VX_{T_X} by $(hT_X) \mapsto h$, and on EX_{T_X} by $h \mapsto (f_1, f_1^{-1}f_2)$ if h connects the vertices (f_1T_X) and (f_2,T_X). The element $f_1^{-1}f_2$ is contained in S, because the edge $f_1^{-1}h$ connects the subtrees T_X and $f_1^{-1}T_X$. By claim (ii) the cardinality of S equals $|EY_+| - |VY| + 1$. □

Corollary 5.5. (Nielsen- Schreier) *Any subgroup of a free group is free.*

Proof. Let F be a free group with basis S. By Corollary 5.3 the group F acts freely and without inversion of edges on the tree $\mathrm{Cay}(G,S)$. If $H \leq F$ is a subgroup of F then H also acts freely and without inversion of edges on this tree. By Theorem 5.4 the group H is free. □

Corollary 5.6. (Schreier‘s formula) *If F is a free group of a finite rank and H is its subgroup of finite index n, then*

$$\mathrm{rk}(H) - 1 = n(\mathrm{rk}(F) - 1).$$

Proof. Let S be a basis of a group F and F/H be the set of right cosets of H in F. H acts on $\mathrm{Cay}(F,S)$ by $h(x) = hx$ and $h(x,s) = (hx,s)$, where $h \in H$, $x \in F$ and $s \in S$.
The factor graph $Y := H/\mathrm{Cay}(F,S)$ is given by $VY = F/H$ and $EY_+ = F \times S/H$ - the edge (Hx,s) connects the vertices Hx and Hxs. By Theorem 5.4 we know that the cardinality of H is given by

$$\mathrm{rk}(H) = |EY_+| - |VY| + 1.$$

Since we assumed that $[F : H] = n$ the claim follows, namely

$$\mathrm{rk}(H) = n\,\mathrm{rk}(G) - n + 1.$$

□

REFERENCES

[1] O. Bogopolski, Introduction to Group Theory, EMS Textbooks in Mathematics, 2008.

[2] D.J.S. Robinson, A Course in the Theory of Groups, Springer, 1996.

[3] M. A. Armstrong, Groups and Symmetry, Undergraduate Texts in Mathematics, Springer, 1988.

[4] T. Camps, V. große Rebel, G. Rosenberger, Einführung in die kombinatorische und die geometrische Gruppentheorie, Berliner Studienreihe zur Mathematik (Band 19), Heldermann Verlag, 2008.

[5] C. Marx, Vorlesungsmitschrift Kombinatorik von B. Krön, Univ. Wien, Sommersmester 2008.