MA4F2 Braid Groups

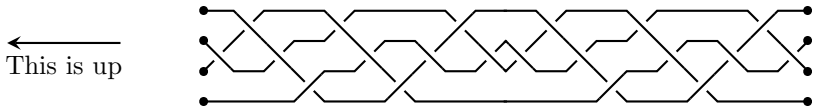
Daan Krammer

March 8, 2005

Contents

1 Vague definition of braid groups

Figure 1: A braid on 4 strings



1.1 This section is purposely vague. Later we'll do things more precisely.

1.2 Vague definition of braids. Fix $n \geq 1$. A *braid* on n strings, or an n-braid, is a collection of n disjoint 'strings' in 3-space like in figure 1 up to 'homotopy'. Two such collections of strings are *homotopic* if you can get from one to the other by only wiggling the strings. The endpoints of the strings cannot wiggle. Strings cannot wiggle through each other. Strings cannot wiggle over the top or below the bottom.

The set of n-braids is written B_n. It is called the *braid group* because we will soon prove that it is a group.

1.3 What is up? Our pictures may rotate over 90 degrees once in a while. If they do we indicate what's up. If up isn't up then it is the way it is in figure 1.

1.4 Multiplication of braids. The *multiplication* of braids is defined to be the map

$$\begin{aligned} B_n \times B_n &\longrightarrow B_n \\ (a, b) &\longmapsto ab := a \text{ on top of } b, \end{aligned}$$

see figure 2.

It is clear that $(ab)c = a(bc)$ for all $a, b, c \in B_n$: associativity holds. (What has this to do with wiggling strings?) In general we don't have $ab = ba$: commutativity fails.

1.5 Semigroups and monoids. We quickly review the basic definitions of semigroups and monoids. A *semigroup* is a pair $(G, *)$ of a set G and an associative multiplication $G \times G \to G$, $(a, b) \mapsto a * b = ab$. An *identity* in a semigroup G is an element 1 such that $1a = a1 = a$ for all $a \in G$. An identity is unique, if it exists. A *monoid* is a semigroup having an identity 1. An *inverse* of an element a in a monoid is an element b such that $ab = ba = 1$.

Figure 2: Multiplication of braids

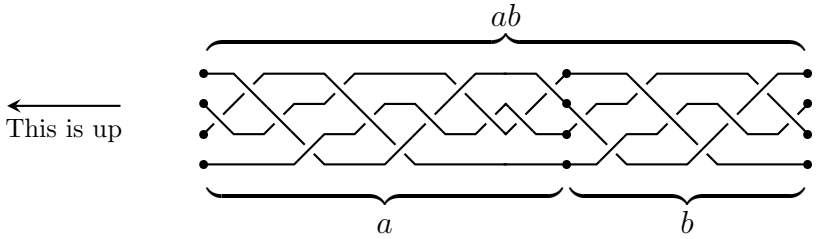


Figure 3: Generators

This is σ_i This is τ_i

An inverse of a is unique if it exists. An element which has an inverse is called *invertible*. A group is just a monoid all of whose elements are invertible. The set of invertible elements in a monoid is a group.

So we know now that B_n is a semigroup.

1.6 Identity braid. The identity braid in B_n, which is written 1 or $\varnothing$, consists of n perfectly vertical strings. We have $1a = a1 = a$ for all $a \in B_n$. So B_n is a monoid.

1.7 Generators. Figure 3 shows $2(n-1)$ braids

$$\sigma_1,\ \tau_1,\ \ldots,\ \sigma_{n-1},\ \tau_{n-1} \in B_n$$

(pronounciation: σ = sigma, τ = tau). The braid σ_i switches strings i and $i+1$ in one sense, τ_i in the other. By its very (vague) definition, B_n is generated[1], as a monoid, by the σ_i and τ_i. We call σ_i and τ_i *generators*. They cause *crossings*, which are the places where one string goes over another.

We often write i instead of σ_i; if we do then we write the identity element as $\varnothing$ because otherwise we would have a clash of notation with $1 = \sigma_1$.

1.8 Exercise. (a). The braids σ_i and τ_i are inverses of each other. Don't prove this, but make it plausible by drawing a picture. What has wiggling to do with this? (From now on we write σ_i^{-1} or i^{-1} instead of τ_i.)

(b). Prove that *every* braid has an inverse. (Use the fact that B_n is generated, as a monoid, by the σ_i and τ_i.)

1.9 Artin Relations. Figure 4 illustrates the fact that

$$\sigma_i\,\sigma_{i+1}\,\sigma_i = \sigma_{i+1}\,\sigma_i\,\sigma_{i+1} \qquad (1 \le i < n). \tag{1.10}$$

For example, $121 = 212$ in the short notation. We also have

$$\sigma_i\,\sigma_j = \sigma_j\,\sigma_i \qquad (1 \le i < j-1 < n-1). \tag{1.11}$$

(What pictures belong to this?) We call (1.10) and (1.11) the *Artin relations*. They are an algebraic version of wiggling strings.

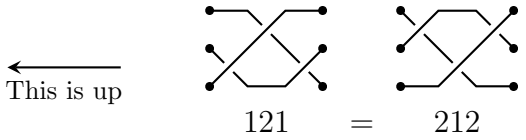
1.12 Example. Prove $213213 = 132132$.

Solution. We apply the Artin relations repeatedly, as well as the basic properties of groups, as follows:

$$\begin{aligned} 213213 &= 231213 = 232123 = 323123 \\ &= 321323 = 321232 = 312132 = 132132. \end{aligned}$$

[1]See exercise 1.16 for generators of semigroups and monoids

Figure 4: An Artin Relation



1.13 Exercise. Draw the pictures for the two braids 213213, 132132 of example 1.12. Decide whether your pictures count as a proof that they are equal. Answer:

If you've decided that the pictures lead to a faster proof that the braids are equal, as you probably have, then hold on for more difficult braids to come!

1.14 Exercise. Draw pictures of the following braids: $a = 231232$, $b = 213213$, $c = 123212$. Two of these braids are equal. Which are they? Prove that two of these are equal by connecting them by a sequence of Artin relations. (The third braid is different.)

1.15 Exercise. Prove the following identities for braids, by applying the Artin relations repeatedly:

(a) $(12)^3 = (21)^3$

(b) $12132 = 23123$

(c) $12^2 32^2 12^2 3 = 32^2 12^2 32^2 1$

(d) $(123)^4 = (321)^4$

(e) If $a = 1234123121$ then $1a = a4$.

1.16 Exercise. This exercise is about submonoids of monoids. Let M be a monoid.

(a). A subset $N \subset M$ is a *submonoid* if the following hold.

(1) Closure: $a, b \in N \Rightarrow ab \in N$.

(2) Identity: The identity of M is in N.

Show that if N is a submonoid of M, then N is a monoid itself.

(b). Give an example where $N \subset M$ satisfies (1) (so that N is a semigroup, don't prove this) and such that N, as a semigroup, contains an identity, while N does not satisfy (2).

(c). The *submonoid* $\langle S \rangle$ *of* M *generated by* S is by definition

$$\{ s_1 \cdots s_n \mid n \geq 0,\ s_i \in S \}.$$

Show that $\langle S \rangle$ is a submonoid. Show that $\langle S \rangle$ equals the intersection of all submonoids of M.

2 Fundamental groups and braid groups

2.1 In this section we learn what the fundamental group of a topological space[2] is, and a precise definition of braid groups. But not one after the other: we do them at the same time! If you want to read the topics separately watch the Fs and Bs in the margin!

[F]=fundamental group [B]=braid group

This section may be a bit technical on the analysis side. Don't worry — you're not expected to understand the analytic aspects very deeply. We are heading for the algebraic aspects of braid groups.

[B] **2.2 Braid space.** We define *braid space* to be

$$BS_n = \Big\{ X \subset \mathbb{C} : |X| = n \Big\},$$

the set of subsets of $\mathbb{C}$ of n elements. We have a *metric* d on braid space BS_n defined by

$$d(X,Y) = \min \Big\{ \sum_{x \in X} |x - fx| \;\Big|\; f\colon X \to Y \text{ a bijection} \Big\}.$$

Every metric induces a topology on BS_n, so the metric d gives us a topology on BS_n. (The metric is no longer relevant once we have the topology.)

We have a *base-point* $X_0 = \{1, 2, \ldots, n\} \in BS_n$.

[F] **2.3 Paths.** Let T be a topological space. A *path* in T is a triple (a, b, f) where $a, b \in \mathbb{R}$ and $a < b$ and

$$f\colon [a,b] \longrightarrow T$$

a continuous map. We say that this path runs from $f(a)$ to $f(b)$, and we call $f(a)$ and $f(b)$ the endpoints of the path.

It is common to write "$f\colon [a,b] \to T$ is a path" instead of "(a,b,f) is a path".

The space T is often equipped with a *base-point*. A path is said to be *based* if it starts and ends at the base-point.

[B] **2.4 Geometric braids.** Let $f\colon [a,b] \to BS_n$ be a based path in braid space BS_n (based means starting and ending at X_0). The *geometric braid* $\mathrm{GB}(f)$ associated with this path is

$$\mathrm{GB}(f) = \bigcup_{a \le t \le b} f(t) \times \{t\} = \left\{ (z,t) \;\middle|\; \begin{matrix} a \le t \le b \\ z \in f(t) \in \mathbb{C} \end{matrix} \right\} \subset \mathbb{C} \times \mathbb{R}.$$

A picture of a geometric braid consists of the points (x,t) where $(x+iy,t) \in \mathrm{GB}(f)$ and $x, y \in \mathbb{R}$. We need to ignore one coordinate because our paper is only 2-dimensional! We choose to drop the imaginary part y.

Now draw such a picture of a geometric braid. Such a picture looks just like the pictures of section 1! Of course, we also need to keep track, at crossings, which strings go over and which under — this is the distinction between σ_i and σ_i^{-1}. This information is thought of to be part of the picture.

[2] Don't worry if you don't know what a topological space is; think *metric space* every-time you read *topological space*.

[F] **2.5 Reparametrisation and concatenation.** Let (T, t_0) be a based topological space. Two based paths $f\colon [a,b] \to T$ and $g\colon [c,d] \to T$ are said to be *reparametrisations* of each other if there exists an increasing homeomorphism $r\colon [a,b] \to [c,d]$ with $g = fr$.

The *concatenation* $f * g$ is defined if $b = c$ and is then the (unique) path $e\colon [a,d] \to T$ satisfying

$$e|_{[a,b]} = f, \qquad e|_{[c,d]} = g,$$

that is, f and g are restrictions of e.

Of course, even if $f * g$ is not defined, $f * g'$ is defined for an appropriate reparametrisation g' of g.

[B] **2.6 Exercise.** Let f, g be two paths in braid space whose concatenation $f * g$ exists. Prove that $\mathrm{GB}(f * g)$ is the *union* $\mathrm{GB}(f) \cup \mathrm{GB}(g)$.

In a picture this means that $\mathrm{GB}(f)$ gets stacked on top of $\mathrm{GB}(g)$ as we already suspected from section 1. Notice the ordering: braids run from top to bottom.

[F] **2.7 Homotopy.** Let T be a topological space. Two paths $f, g\colon [a,b] \to T$ are said to be *strictly homotopic relative endpoints* if there exists a continuous map $h\colon [0,1] \times [a,b] \to T$ such that

- $h(0,x) = f(x)$ and $h(1,x) = g(x)$ for all $x \in [a,b]$, and
- the maps $t \mapsto h(t,a)$ and $t \mapsto h(t,b)$ are constant. (Therefore $f(a) = g(a)$ and $f(b) = g(b)$.)

We call two paths in a topological space *homotopic relative endpoints* if one is strictly homotopic relative endpoints to a reparametrisation of the other.

[B] **2.8 Exercise.** Let $f, g\colon [a,b] \to BS_n$ be based paths in braid space.

(a). Suppose g is a reparametrisation of f. Sketch the geometric braids of f and g in a typical case.

(b). Suppose f and g are strictly homotopic relative endpoints. Again, sketch the geometric braids of f and g in a typical case.

[F] **2.9 Exercise.** Prove that any two paths in $T = \mathbb{R}^m$ with the same endpoints are homotopic relative endpoints.

[F] **2.10 Exercise.** Prove that being homotopic relative endpoints is an equivalence relation.

[F] **2.11 Fundamental group.** Let T be a topological space and $t_0 \in T$ a basepoint. The *fundamental group* $\pi_1(T, t_0) = \pi_1(T)$ consists of the homotopy classes $[f]$ relative endpoints of based paths f in T. The *multiplication*

$$\begin{aligned} \pi_1(T) \times \pi_1(T) &\longrightarrow \pi_1(T) \\ ([f],[g]) &\longmapsto [f][g] \end{aligned}$$

is defined as follows. First choose a reparametrisation g' of g such that the concatenation $f * g$ exists. Then $[f][g] := [f * g']$.

It can be shown that $[f * g']$ depends only on $[f], [g]$ as it should.

[F] **2.12 Exercise.** In this exercise you prove some of the basic properties of fundamental groups.

(a) Prove that multiplication in fundamental groups is well-defined as explained in 2.11.

(b) Prove that multiplication in $\pi_1(T, t_0)$ is associative.

(c) Prove that $\pi_1(T, t_0)$ is a group.

(d) Prove that if there exists a path from t_0 to t_1 ($t_0, t_1 \in T$) then $\pi_1(T, t_0)$ and $\pi_1(T, t_0)$ are isomorphic.

[F] **2.13 Path-connected spaces.** A topological space is *path-connected* if any two points can be connected by a path, that is, any two points are the endpoints of some path.

In exercise 2.12(d) you've shown that if T is path-connected, then $\pi_1(T, t_0)$ does not depend on the base-point t_0, up to isomorphism. Somewhat loosely we write $\pi_1(T)$ and call it the fundamental group of T.

[B] **2.14 Exercise.** Prove that the following spaces are path-connected: $\mathbb{R}^m$, BS_n, $\mathbb{R}^2 - \mathbb{Q}^2$.

[B] **2.15 Braid groups: the official definition.** Recall braid space BS_n and its base-point $X_0 = \{1, \ldots, n\}$. The braid group is defined as the fundamental group of BS_n:

$$B_n = \pi_1(BS_n, X_0).$$

An element of the braid group B_n is of course called a braid.

2.16 Exercise. (a). Let $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ be the circle. Prove that $\pi_1(S^1)$ is isomorphic to $\mathbb{Z}$. This is very difficult at this stage! (Not examinable.)

(b). Prove that BS_2 is homeomorphic to $S^1 \times \mathbb{R}^3$ and deduce that $B_2 \cong \mathbb{Z}$.

2.17 Remark. Note that we haven't proved that B_n is generated by the σ_i (but it is true).

2.18 Remark. Continuous paths can be ugly things. Many people find it easier to require all paths and homotopies in braid space (or any manifold) to be piecewise linear, or differentiable. (We won't worry what these mean.) One can show that the resulting fundamental group is the same in all three approaches. (Beware that other invariants of manifolds than the fundamental group can feel the difference!)

3 Braid group actions and the Burau representation

3.1 In this section and the next section we look at some B_n-actions on various objects. These actions will not be used after that — they are just examples showing how to use the Artin relations and to have some fun.

The *symmetric group* of a set X will be written $\mathrm{Sym}(X)$.

3.2 Exercise. This exercise reviews group actions on sets and can probably be skipped by most of you.

Let G be a group and X a set. A *G-action* on X is a map $p\colon G\times X\to X$ such that, on writing gx instead of $p(g,x)$, one has

$$g(hx)=(gh)x \tag{3.3}$$

for all $(g,h,x)\in G\times G\times X$. Let A be the set of G-actions on X and B the set of homomorphisms $G\to\mathrm{Sym}(X)$. You will show that there exists a natural bijection between A and B. We define $\phi\colon A\to B$ and $\sigma\colon B\to A$ by

$$\big((\phi p)g\big)x=p(g,x),\qquad (\sigma f)(g,x)=(fg)x.$$

(a) Write (3.3) in terms of p alone, never using the notation gx but always $p(g,x)$.
(b) Show that $\phi A\subset B$, that is, ϕp is always a homomorphism.
(c) Show that $\sigma B\subset A$, that is, σf is always an action.
(d) Prove that $\phi\sigma=1_B$.
(e) Prove that $\sigma\phi=1_A$. Conclude that ϕ is a bijection.

3.4 Let $f\colon B_n\to G$ be a homomorphism of groups and put $A_i:=f(\sigma_i)$. We have

$$\text{hexagon relation: } A_iA_{i+1}A_i=A_{i+1}A_iA_{i+1}\ (1\le i<n) \tag{3.5}$$

$$\text{commutation relation: } A_iA_j=A_jA_i\ (1\le i<j-1<n-1), \tag{3.6}$$

that is, the A_i satisfy the Artin relations; this follows from the definition of group homomorphisms and the fact that the σ_i satisfy the Artin relations.

3.7 Theorem. *Conversely, given a group G and $A_i\in G$ $(1\le i<n)$ satisfying the Artin relations (3.5), (3.6) there exists a unique homomorphism $f\colon B_n\to G$ such that $f(\sigma_i)=A_i$ for all i.* □

3.8 Later we will discuss this theorem, but we will not prove it. Notice that the uniqueness in 3.7 is easily proved if one assumes that B_n is generated by the σ_i.

Theorem 3.7 helps us find homomorphisms from B_n to other groups. In this section and the following, we will use theorem 3.7 to construct B_n-actions on various objects. The first one is due to Burau (1936).

3.9 Burau representation. A *representation* of a group G is a homomorphism $G \to \mathrm{GL}(V)$ for some vector space V over some field, or some module V over some ring.

Let $R = \mathbb{Z}[q, q^{-1}]$ be the ring of Laurent polynomials in one variable q. Let $e_1, \ldots, e_n$ be the standard basis of R^n.

We define the elements $A_i \in \mathrm{GL}(n, R)$ by

$$\begin{aligned} A_i\, e_j &= e_j \qquad\qquad j \notin \{i, i+1\} \\ A_i\, e_i &= q\, e_{i+1} \\ A_i\, e_{i+1} &= e_i + (1-q)\, e_{i+1}. \end{aligned} \tag{3.10}$$

In matrix form we have

$$A_i = \begin{pmatrix} I_{i-1} & & & \\ & 0 & 1 & \\ & q & 1-q & \\ & & & I_{n-i-1} \end{pmatrix}$$

where I_j denotes the identity matrix of size j. We claim that there exists a unique representation

$$b\colon B_n \longrightarrow \mathrm{GL}(n, R)$$

called the *Burau representation* such that $b(\sigma_i) = A_i$ for all i. This will follow from 3.7 if we can show that the A_i satisfy the Artin relations (3.5) and (3.6).

3.11 We will now prove by a computation that the Artin relations are indeed satisfied. The commutation relations are clearly satisfied. Moreover, in order to prove the hexagon relations, it is clearly sufficient to prove $A_1A_2A_1 = A_2A_1A_2$ in the case $n = 3$. Then we are dealing with 3×3 matrices. We have

$$A_1 = \begin{pmatrix} 0 & 1 & 0 \\ q & 1-q & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & q & 1-q \end{pmatrix}$$

so

$$A_1A_2 = \begin{pmatrix} 0 & 0 & 1 \\ q & 0 & 1-q \\ 0 & q & 1-q \end{pmatrix}. \tag{3.12}$$

Using (3.12) twice we find

$$A_1A_2A_1 = (A_1A_2)A_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & q & 1-q \\ q^2 & q-q^2 & 1-q \end{pmatrix}$$

and

$$A_2A_1A_2 = A_2(A_1A_2) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & q & 1-q \\ q^2 & q-q^2 & q(1-q)+(1-q)^2 \end{pmatrix}.$$

It follows that $A_1A_2A_1 = A_2A_1A_2$ as promised. The construction of the Burau representation is complete. □

3.13 Remarks. It is known that the Burau representation is not faithful. There is a faithful representation of the braid group though. In exercise 3.24 you will construct this representation by computation.

3.14 Our aim will be to prove that the Burau representation has a preserved Hermitian form. In order to make the formulas simpler, we change to a different basis $(h_1, \dots, h_n)$ defined by

$$h_i := q^{-i} e_i.$$

Then

$$\begin{aligned} A_i\, h_j &= h_j && j \notin \{i, i+1\} \\ A_i\, h_i &= h_{i+1} \\ A_i\, h_{i+1} &= q\, h_i + (1-q)\, h_{i+1}. \end{aligned}$$

3.15 Hermitian forms. Let $x \mapsto \overline{x}$ denote the ring automorphism of R defined by $\overline{q} = q^{-1}$. A *Hermitian form* on an R-module W is a $\mathbb{Z}$-bilinear form $(\cdot,\cdot)\colon W \times W \to R$ such that

$$\text{bar-symmetry:} \quad (x,y) = \overline{(y,x)} \qquad \text{for all } x, y \in W \tag{3.16}$$

$$\text{linear/bar-linear:} \quad (ax, by) = a\overline{b}(x,y) \qquad \text{for all } a, b \in R,\ x, y \in W. \tag{3.17}$$

There is a more general notion of Hermitian forms for any commutative ring with an involution (=automorphism of order 2). The most famous instance is the complex numbers with complex conjugation as involution.

3.18 The Burau representation is Hermitian. There is a unique $\mathbb{Z}$-linear form $(\cdot,\cdot)$ on R^n satisfying (3.17) and

$$(h_i, h_j) = \begin{cases} q^{-1} & \text{if } i < j \\ -1 & \text{if } i = j \\ q & \text{if } i > j. \end{cases} \tag{3.19}$$

This is because h_i is an R-basis and (3.19) prescribes the form on pairs of basis vectors. But (3.19) is such that $(h_i, h_j) = \overline{(h_j, h_i)}$; this implies that bar-symmetry (3.16) is satisfied and therefore, $(\cdot,\cdot)$ is a Hermitian form.

We will prove that this Hermitian form is invariant under the Burau representation, that is,

$$(gx, gy) = (x, y)$$

for all $g \in b(B_n)$ and all $x, y \in R^n$. It is enough to show this for $g = A_k$ because they are the Burau matrices for the *generators* σ_k of B_n. Moreover, because of bar-symmetry, it is enough to prove this for $i \le j$.

We consider four cases, which may have subcases:

$$\begin{aligned} &\text{Case 1:} && A_k(h_i) = h_i, && A_k(h_j) = h_j \\ &\text{Case 2:} && A_k(h_i) \neq h_i, && A_k(h_j) = h_j \\ &\text{Case 3:} && A_k(h_i) = h_i, && A_k(h_j) \neq h_j \\ &\text{Case 4:} && A_k(h_i) \neq h_i, && A_k(h_j) \neq h_j. \end{aligned}$$

Case 1. In this case we clearly have $(A_k\, h_i, A_k\, h_j) = (h_i, h_j)$.

Case 2A: $k = i$. Then $A_k\, h_i = h_{i+1}$ and

$$(A_k\, h_i, A_k\, h_j) = (h_{i+1}, h_j) = q^{-1} = (h_i, h_j).$$

Case 2B: $k = i - 1$. Then $A_k\, h_i = qh_{i-1} + (1-q)h_i$ and

$$\begin{aligned}(A_k\, h_i, A_k\, h_j) &= (qh_{i-1} + (1-q)h_i, h_j) = q(h_{i-1}, h_j) + (1-q)(h_i, h_j)\\ &= q \cdot q^{-1} + (1-q) \cdot q^{-1} = q^{-1} = (h_i, h_j).\end{aligned}$$

Cases 3 and 4 are left as an exercise. □

3.20 Exercise. Finish cases 3 and 4 in 3.18.

3.21 Exercise. Compute the *determinant* of the Burau Hermitian form, that is, the determinant of the $n \times n$ matrix whose (i, j)-entry is (h_i, h_j).

3.22 Exercise.

(a) Prove that the Burau representation preserves $v_0 := e_1 + \cdots + e_n$.

(b) Put $V := R^n/Rv_0 \cong R^{n-1}$. From (a) it follows that there is a *reduced Burau representation* $c\colon B_n \to \mathrm{GL}(V) \cong \mathrm{GL}(n-1, R)$ defined by $(cx)(v + Rv_0) = (bx)v + Rv_0$. A basis for V is $(f_1, \ldots, f_{n-1})$ where $f_i = e_i - e_{i-1} + Rv_0$. (Don't prove these things.) Write down the matrices for $c\sigma_i$ with respect to the basis $(f_1, \ldots, f_{n-1})$ (or in algebraic form like we did in (3.10)).

3.23 Exercise. Compute the entries of the Burau matrix of $\sigma_1 \cdots \sigma_{n-1} \in B_n$. Hint: Once you have a conjectural answer, try to prove it by induction.

3.24 Exercise. Let V be a free $\mathbb{Z}[q, q^{-1}, t, t^{-1}]$-module with basis

$$\big\{x_{ij} = x_{ji} \;\big|\; 1 \le i < j \le n\big\}.$$

Prove that there exists a unique representation $B_n \to \mathrm{GL}(V)$ defined by

$$\begin{aligned}
\sigma_k\, x_{k,k+1} &= tq^2\, x_{k,k+1};\\
\sigma_k\, x_{ik} &= (1-q)\, x_{ik} + q\, x_{i,k+1}, && i < k;\\
\sigma_k\, x_{i,k+1} &= x_{ik} + tq^{k-i+1}(q-1)\, x_{k,k+1}, && i < k;\\
\sigma_k\, x_{kj} &= tq(q-1)\, x_{k,k+1} + q\, x_{k+1,j}, && k+1 < j;\\
\sigma_k\, x_{k+1,j} &= x_{kj} + (1-q)\, x_{k+1,j}, && k+1 < j;\\
\sigma_k\, x_{ij} &= x_{ij}, && i < j < k \;\text{ or }\; k+1 < i < j;\\
\sigma_k\, x_{ij} &= x_{ij} + tq^{k-i}(q-1)^2\, x_{k,k+1}, && i < k < k+1 < j.
\end{aligned}$$

3.25 Example. Here is another application of 3.7. We will show that there exists a unique automorphism f of B_n which takes σ_i to σ_i^{-1}, for all i.

In the notation of 3.7 we put $A_i = \sigma_i^{-1}$. We have the hexagon relation

$$\sigma_i\, \sigma_{i+1}\, \sigma_i = \sigma_{i+1}\, \sigma_i\, \sigma_{i+1}.$$

Taking inverses of both sides we find

$$\sigma_i^{-1}\,\sigma_{i+1}^{-1}\,\sigma_i^{-1} = \sigma_{i+1}^{-1}\,\sigma_i^{-1}\,\sigma_{i+1}^{-1}$$

and therefore

$$A_i\,A_{i+1}\,A_i = A_{i+1}\,A_i\,A_{i+1}$$

that is, the A_i satisfy the hexagon relation (3.5). They also satisfy the commutation relations (3.6) as one shows likewise. Using 3.7 we conclude that there is a unique homomorphism f taking σ_i to σ_i^{-1}. It is clear that $f^2 = 1$, so that in particular f is bijective, and an automorphism of B_n.

3.26 Exercise.

(a) Define a self-homeomorphism of BS_n which preserves X_0 and which induces the automorphism f from 3.25. A proof is not necessary.

(b) Prove that there exists an anti-automorphism[3] of B_n which takes σ_i to σ_i, for all i.

3.27 Exercise.

(a) Use 3.7 to show that there exists a homomorphism $f\colon B_{n-1} \to B_n$ defined by $f(\sigma_i) = \sigma_i$.

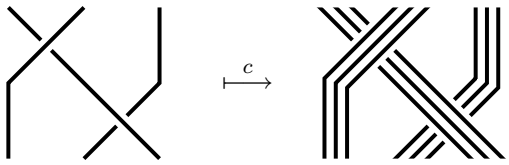
(b) Let $H = \{x \in B_n \mid (\pi x)n = n\}$. Use the vague definition of the braid group to define a homomorphism $g\colon H \to B_{n-1}$ such that $gf = 1$. Deduce that f is injective.

3.28 Exercise. There is a homomorphism called *cabling* $c\colon B_n \to B_{kn}$ which replaces each string by k strings. See figure 5. The k strings always stay neatly in line. Suppose now $k = 2$.

(a) Express $c(\sigma_i)$ in terms of the sigma-generators of B_{2n}.

(b) (Re)prove that c exists in an algebraic way, by using theorem 3.7 and proving that c takes any Artin relation in B_n to one of the consequences of the Artin relations in B_{2n}.

Figure 5: Cabling



[3]Let G, H be groups. A map $f\colon G \to H$ is called an *anti-homomorphism* if $f(xy) = (fy)(fx)$ for all $x, y \in G$. It is an *anti-isomorphism* if it is also bijective. An *anti-automorphism* of G is an anti-isomorphism from G to itself.

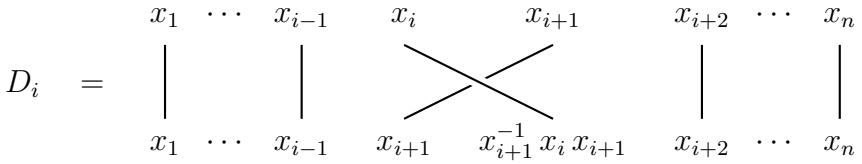
4 The action on the free group

4.1 Let G be any group. In what follows, we treat G^n as a set, not a group or anything else. We define $D_i \in \mathrm{Sym}(G^n)$ (acting on G^n on the right) by

$$(x_1,\ \ldots,\ x_n)D_i = (x_1,\ \ldots,\ x_{i-1},\ x_{i+1},\ x_{i+1}^{-1}\, x_i\, x_{i+1},\ x_{i+2},\ \ldots,\ x_n).$$

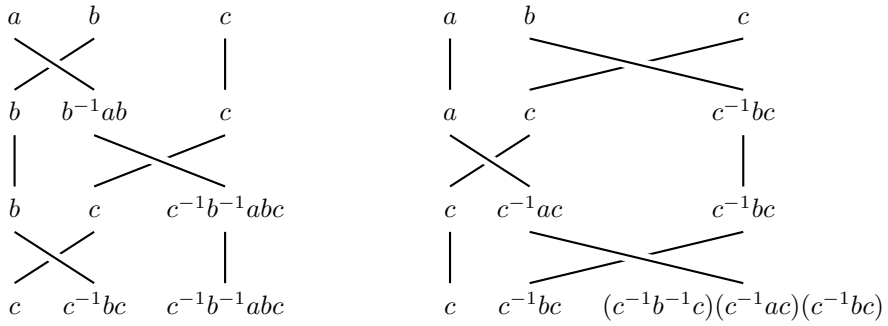
We claim that the D_i satisfy the Artin relations (3.5) and (3.6), so that we have a unique homomorphism $f\colon B_n \to \mathrm{Sym}(G^n)$ with $f(\sigma_i) = D_i$, by 3.7.

4.2 Diagrammatic notation. We have a diagrammatic notation for D_i as follows.



The strings depict σ_i, according to the fact that we want $f(\sigma_i) = D_i$. The n-tuple $(x_1, \ldots, x_n)$ in the top row denotes an element of G^n, and each entry of this tuple is attached to its own string. Sometimes we say that x_j is the *label* of string j (but the label of that string may change when passing from one horizontal line to the next). The main property of the diagrammatic notation is that the label of a string can only change at a crossing.

4.3 Proof of the Artin relations. It is clear that the commutation relations (3.6) are satisfied. In order to prove the hexagon relations (3.5) it is enough to do this for $n = 3$, $(i, j) = (1, 2)$. Using the diagrammatic notation we find the following.



The bottom rows are, respectively, $(a, b, c)D_1D_2D_1$ and $(a, b, c)D_2D_1D_2$. But they are also equal as our computation shows, which finishes the proof. □

4.4 As we said in 4.1, it follows that there exists a unique action $f\colon B_n \to \mathrm{Sym}(G^n)$ such that $f(\sigma_i) = D_i$. We will learn later that this is related to something called the *braid group action on the free group*.

The diagrammatic notation is not indispensable in the above but it is a crisp and clear notation of what is going on.

There is a topological explanation for the existence of the action f on the free group. It can be shown that f is injective if, for example, G is a free non-abelian group, or $G = \mathrm{SL}(2, \mathbb{Z})$.

4.5 Exercise. Let G be a group and $C \subset G$ a union of conjugacy classes. Show that the B_n-action on G^n preserves C^n.

4.6 Exercise. Define $p\colon G^n \to G$ by $p(x_1,\ \ldots,\ x_n) = x_1 \cdots x_n$. Prove that the braid group preserves p, that is, $p(xg) = p(x)$ for all $g \in B_n$, $x \in G^n$.

4.7 Exercise. Put $R = \mathbb{Z}[q, q^{-1}]$,

$$G = \left\{ \begin{pmatrix} q^k & x \\ 0 & 1 \end{pmatrix} : k \in \mathbb{Z},\ x \in R \right\}, \qquad C = \left\{ \begin{pmatrix} q & x \\ 0 & 1 \end{pmatrix} : x \in R \right\}.$$

So G is a subgroup of $\mathrm{GL}(2, R)$ and C is a subset of G.

(a) Prove that C is a union of conjugacy classes in G. In 4.5 we've seen that therefore B_n acts on C^n.

(b) On writing

$$\left(\begin{pmatrix} q & x_1 \\ 0 & 1 \end{pmatrix},\ \cdots,\ \begin{pmatrix} q & x_n \\ 0 & 1 \end{pmatrix} \right) D_i = \left(\begin{pmatrix} q & y_1 \\ 0 & 1 \end{pmatrix},\ \cdots,\ \begin{pmatrix} q & y_n \\ 0 & 1 \end{pmatrix} \right),$$

express $(y_1,\ \ldots,\ y_n)$ in terms of $(x_1,\ \ldots,\ x_n)$.

(c) Prove that this recovers the Burau representation.

(d) Devise a diagrammatic notation for the Burau representation and give the example for σ_i.

4.8 Exercise. Let G be a group, $k \in \mathbb{Z}$. Prove that there exist unique homomorphisms $a,\ b\colon B_n \to \mathrm{Sym}(G^n)$ such that the following hold.

(a) $(x_1,\ \ldots,\ x_n)(a\sigma_i) = (x_1,\ \ldots,\ x_{i-1},\ x_{i+1},\ x_{i+1}^{-k}\, x_i\, x_{i+1}^{k},\ x_{i+2},\ \ldots, x_n)$.

(b) $(x_1,\ \ldots,\ x_n)(b\sigma_i) = (x_1,\ \ldots,\ x_{i-1},\ x_{i+1}^{-1},\ x_{i+1}\, x_i\, x_{i+1},\ x_{i+2},\ \ldots, x_n)$.

5 Presentations of monoids

5.1 Maps of monoids. Let M, N be monoids. A set-map $f\colon M \to N$ is called a *homomorphism* or *map* (of monoids) if the following hold.

(1) $f(xy) = (fx)(fy)$ for all $x, y \in M$.

(2) $f(1_M) = 1_N$.

5.2 In group theory you've learned that every kernel of a group homomorphism is a normal subgroup of the source group. Conversely, every normal subgroup of a group is a kernel. The following proposition tells us what happens in the more general case of monoids.

5.3 Proposition. *Let M be a monoid and let $\approx$ be an equivalence relation on M. Then the following are equivalent.*

(1) *There exists a monoid N and a homomorphism $f\colon M \to N$ such that $x \approx y \Leftrightarrow fx = fy$, for all $x, y \in M$.*

(2) *For all $w, x, y, z \in M$, if $w \approx x$ and $y \approx z$ then $wy \approx xz$.*

5.4 Exercise. Prove 5.3.

5.5 Congruences. An equivalence relation $\approx$ on a monoid M satisfying the equivalent properties of 5.3 is called a *congruence*.

5.6 Let $\approx$ be a congruence on a monoid M. Then there exists a unique monoid structure on $M/\!\approx$ defined as follows, on writing $[x]$ for the $\approx$-class of x: $[x][y] = [xy]$. We have a *natural map* $M \to M/\!\approx$ defined by $x \mapsto [x]$ which is a homomorphism.

5.7 Relations. If S is any subset of a group G then there is a smallest normal subgroup of G containing S. We will now generalise this to monoids.

Recall that a *relation* on a set A is just a subset of $A \times A$. In particular, a congruence on M is some sort of subset of $M \times M$.

5.8 Proposition. Let R be a relation on a monoid M. Then there is a smallest congruence $\approx_{RM} = \approx_R$ on M containing R. It is also the intersection of all congruences on M containing R.

Proof. Let A be the set of congruences on M containing R. Then A is non-empty, because $(M \times M) \in A$. Let T denote the intersection of all elements of A. We have $R \subset T$, because each element of A contains R.

We claim that T is a congruence. Suppose $w, x, y, z \in M$ such that wTx and yTz. For any relation $U \in A$ we have wUx and yUz. But U is a congruence by assumption, so $wyUxz$. Since this is true for all $U \in A$ we get $wyTxz$. This proves our claim that T is a congruence.

Put $\approx_R := T$. This is indeed the smallest congruence on M containing R because it is a subset of any $U \in A$. □

5.9 Definition. We call $\approx_R$ the congruence *generated by* R. We often write M/R instead of $M/\approx_R$.

5.10 Free monoids. Let S be a set. The *standard free monoid* on S is

$$S^* := \coprod_{n\geq 0} S^n \qquad \text{(disjoint union)}.$$

We have a multiplication (or concatenation) on S^* defined by

$$(x_1, \ldots, x_k)(y_1, \ldots, y_\ell) := (x_1, \ldots, x_k, y_1, \ldots, y_\ell).$$

Multiplication is obviously associative and there is an identity $1 = \varnothing = () \in S^0$ (the empty string). So S^* is a monoid indeed.

We often write $x_1 \cdots x_k$ instead of $(x_1, \ldots, x_k)$.

In this context, S is called an *alphabet*, its elements *letters* or *generators* and the elements of S^* *words* or *strings*. A *subword* of a word $(x_1, \ldots, x_k)$ is a word of the form $(x_p, x_{p+1}, \ldots, x_{q-1})$ with $1 \leq p \leq q \leq k$.

A *free monoid* is a monoid isomorphic to a standard free monoid.

5.11 Let S be a set, M a monoid and $f\colon S \to M$ a set-map. It is clear that f can be extended, in a unique fashion, to a homomorphism of monoids $S^* \to M$ (we identify S with $S^1 \subset S^*$).

5.12 *Universal property. It can be shown that the property in 5.11 characterizes free monoids (we won't make this precise). It is known as the universal property.

5.13 Monoid presentations. A *monoid presentation* is a pair (S, R) where S is a set and R a relation on S^*, that is, a subset of $S^* \times S^*$.

Instead of $(x, y) \in R$ we will often write $(x = y) \in R$ and later also $(x \to y) \in R$. A shorter notation for $(x, 1) \in R$ is $x \in R$. Admittedly it's confusing to have these notations at the same time but all are usual so it's good if we are prepared for all of them.

Associated with a monoid presentation (S, R) is a monoid, namely $S^*/R := S^*/\approx_R$. We say that (S, R) *presents* this monoid (or any isomorphic monoid) with *generators* S and *relations* R.

Sometimes we write

$$(x_1, \ldots, x_k \mid r_1, \ldots, r_\ell)$$

for the presentation $(\{x_1, \ldots, x_k\} \mid \{r_1, \ldots, r_\ell\})$ and then we write

$$\langle x_1, \ldots, x_k \mid r_1, \ldots, r_\ell \rangle$$

for the monoid presented by it.

The $\approx_R$-equivalence class of $x \in S^*$ is written x_R or $[x]$ or even just x.

5.14 The following proposition is often useful.

5.15 Proposition. *Let (S, R) be a monoid presentation and M a monoid. Suppose we have a map $f\colon S^* \to M$ of monoids such that $fu = fv$ whenever $(u, v) \in R$. Then there exists a unique homomorphism of monoids $g\colon S/R \to M$ such that $g[x] = fx$ for all $x \in S$.* □

5.16 Exercise. Prove 5.15.

5.17 Corollary. *Let (S_1, R_1) and (S_2, R_2) be monoid presentations. Suppose we have a map $f\colon S_1^* \to S_2^*$ of free monoids such that $fu \approx_{R_2} fv$ whenever $(u, v) \in R_1$. Then there exists a unique homomorphism of monoids*

$$g\colon S_1/R_1 \longrightarrow S_2/R_2$$

such that $g[x] = [fx]$ for all $x \in S_1$. □

5.18 Example. Let $n > 0$. Then $\langle x \mid x^n \rangle \cong \mathbb{Z}_n$.

Solution. Put $G = \langle x \mid x^n \rangle$. There is a unique homomorphism $f\colon G \to \mathbb{Z}_n$ satisfying $f(x) = 1$, by 5.15 and because $f(x^n) = 0$ and x^n is the only relation for G. It is obvious that f is surjective. As to injectivity, we have $x^n \approx 1$ whence $x^{r+qn} \approx 1$ $(r, q \geq 0)$. It follows that G has at most n elements and therefore f is injective. □

5.19 Example. Prove that the presented monoids

$$M = \langle a, b \mid b = a^2b^2 \rangle, \qquad N = \langle a, c \mid c = a^2cac \rangle$$

are isomorphic.

First solution. Define $P = \{a, b\}^*$, $Q = \{a, c\}^*$. Define $f\colon P \to Q$ and $g\colon Q \to P$ by

$$f(a) = a, \quad f(b) = ac, \quad g(a) = a, \quad g(c) = ab^2.$$

The following calculation shows that f takes the relation for M to a consequence of relations for N:

$$f(a^2b^2) = a^2(ac)^2 = a^3cac = a(a^2cac) \approx ac = f(b)$$

where $\approx$ denotes the appropriate congruence. Therefore, f induces a homomorphism $f_*\colon M \to N$, by 5.17.

Conversely, g takes the relation for N to a consequence of relations for M because

$$g(a^2cac) = a^2(ab^2)a(ab^2) = a(a^2b^2)(a^2b^2) \approx ab^2 = g(c).$$

Therefore g induces a homomorphism $g_*\colon N \to M$.

Prove yourself that $f_*g_* = 1_N$ and $g_*f_* = 1_M$. It follows that f is bijective and therefore an isomorphism. □

Second solution. Define a third monoid

$$R = \langle a, b, c \mid b = ac,\ c = ab^2 \rangle.$$

This monoid can be rewritten in two ways. The first way is by eliminating c and writing ab^2 everywhere instead of c. This way one gets the presentation for M. The second way is by eliminating b and writing ac instead everywhere. One gets N which shows that M and N are isomorphic.

Elimination of a generator as above is an example of the *Tietze moves* which we will not study. Two finite presentations define isomorphic monoids if and only if one presentation can be obtained from the other by a sequence of Tietze moves. □

5.20 Algorithms. We will not define precisely what an algorithm is, but the following vague description should be sufficient. An algorithm is like a computer program, or a cooking recipy. It is a list of easy to perform steps leading to the desired result.

Many problems have been shown to have no algorithmic solution. For example, there is no algorithm which on input a finite monoid presentation, decides whether the presented monoid is trivial.

Much more important than the question whether an algorithmic solution exists, is the question whether a *fast* algorithmic solution exist. A slow algorithm is almost as worthless as no algorithm at all. Here is a precise definition of something like *fast*. An algorithm is *polynomial (time)* if the time taken by the algorithm is at most an^b where a, b are constants and n is the length of the input (say, number of bits). In by far most practical cases, polynomial algorithms are fast, and non-polynomial ones are not, but exceptions exist in either direction.

5.21 The word problem. Let (S, R) be a finite presentation of the monoid M. The *word problem* asks whether there exists an algorithm which, on input two words $u, v \in S^*$, decides whether $u \approx_R v$.

It is known that the answer to this question depends only on (the isomorphism class of) the monoid M.

Confusingly, we say that M has *solvable word problem* if the answer is "yes" (an algorithm exists) and otherwise it is said to have unsolvable word problem.

Monoids with unsolvable word problem exist and have been constructed.

5.22 Word problems and braid groups. The main aim of these lecture notes is a polynomial solution to the word problem in the braid group.

It is easy to see that if a group has solvable word problem, then so has every (finitely generated) subgroup. This is one of the reasons why one is interested in homomorphisms from the braid group to other groups G. If such a homomorphism is injective, and the word problem is solvable in G then it is in the braid group.

Of course, braids are closely related to knots and links. Even though links don't form a group, there is something like a word problem for them. It is the question whether there exists an algorithm which on input two links (say by pictures of them), decides if they are isotopic ("the same"). Such an algorithm exists, but it is not known whether a polynomial one exists.

6 Rewriting systems

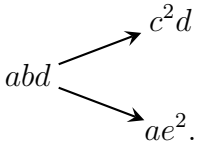
6.1 Example. We consider the word problem in the monoid

$$\langle S, R\rangle = \langle a, b, c, d, e \mid ab = c^2,\ bd = e^2\rangle.$$

Notice $c^2d = (ab)d = a(bd) = ae^2$. Consider the rewriting process which on input a word w, keeps doing the following replacements for subwords (that is, some letters may appear on the left or right of the letters below, but are untouched).

$$ab \longrightarrow c^2, \qquad bd \longrightarrow e^2, \qquad c^2d \longrightarrow ae^2 \tag{6.2}$$

The process terminates when none of these replacements are possible anymore. It is clear that the process terminates — either the number of b's goes down, or it stays at the same number while the number of c's goes down. The process is not unique, as is shown by the two reductions



We will later learn how to show that the final result of the process is not dependent of the process, that is, depends only on w. It will be written $N(w)$ and called the *normal form* for w. Moreover, we have

$$u \approx_R v \quad \Leftrightarrow \quad N(u) = N(v). \tag{6.3}$$

It follows that the word problem for this monoid is solvable. Given $u, v \in S^*$ compute $N(u)$ and $N(v)$; then (6.3) tells you how to decide whether $u \approx_R v$.

Exercise: Show that this would go wrong if we didn't add the third rewrite rule in (6.2).

To be continued in 6.13.

6.4 Orderings. Let R be a relation on a set A, that is, $R \subset A \times A$. Here are some properties R may or may not have:

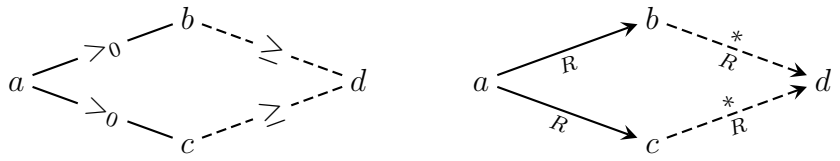
reflexive:	aRa for all $a \in A$.
anti-reflexive:	(not aRa) for all $a \in A$.
anti-symmetric:	aRb and $bRa \quad \Rightarrow \quad a = b$.
transitive:	aRb and $bRc \quad \Rightarrow \quad aRc$.

We call R an *ordering* (think: $\geq$) if it is reflexive, anti-symmetric and transitive. We call R a *strict ordering* (think: $>$) if it is anti-reflexive, anti-symmetric and transitive.

6.5 Least and greatest. Let $(L, \leq)$ be an ordered set[4]. A *least* element of L is an element $x \in L$ such that $x \leq y$ for all $y \in L$. A least element doesn't necessarily exist, but if it does, then it is unique. Likewise, a *greatest* element of L is an element $x \in L$ such that $y \leq x$ for all $y \in L$.

[4] An ordered set is never necessarily a total ordering, unless stated so.

Figure 6: The diamond property for $>_0$, respectively, $\xrightarrow[R]{}$



6.6 Transitive closures. Let R be a relation on a set A. The smallest transitive relation on A containing R is called the *transitive closure* of R and is clearly equal to

$$\left\{(x,y) \;\middle|\; \begin{array}{c} \exists n \geq 1,\ x_0,\ \ldots,\ x_n: \\ x = x_0 R x_1 R \cdots R x_n = y \end{array}\right\}.$$

Similarly, the smallest reflexive and transitive relation on A containing R is called the *reflexive-transitive closure* of R and is clearly equal to

$$\left\{(x,y) \;\middle|\; \begin{array}{c} \exists n \geq 0,\ x_0,\ \ldots,\ x_n: \\ x = x_0 R x_1 R \cdots R x_n = y \end{array}\right\}.$$

We call R *acyclic* if it is contained in an ordering. Equivalently, if

$$x_0 R x_1 R \cdots R x_n = x_0$$

then $x_i = x_0$ for all i. If R is acyclic then its reflexive-transitive closure is an ordering.

6.7 Diamond property. Let $>_0$ be an acyclic relation on a set L. Let $\geq$ denote its reflexive-transitive closure. We say that $>_0$ satisfies the *diamond property* if whenever $a, b, c \in L$ are such that $a >_0 b$ and $a >_0 c$, there exists $d \in L$ such that $b \geq d$ and $c \geq d$. See the diagram on the left in figure 6.

6.8 Diamond Lemma. *Let $>_0$ be an acyclic relation on a set L. Let $\geq$ denote its reflexive-transitive closure. Suppose that L has no infinite descending chains, that is, there are no $x_0,\ x_1,\ \ldots \in L$ with $x_0 > x_1 > \cdots$. Suppose also that $>_0$ has the diamond property. If L has a greatest element*[5]*, then it has a least element.*

6.9 Exercise. In this exercise you will prove the diamond lemma.

Retain the notation and assumptions of the diamond lemma. For $x \in L$, let $L(x) := \{y \in L \mid x \geq y\}$. Let L_0 be the set of elements $x \in L$ such that $L(x)$ has no least element. For $x \in L - L_0$ let $M(x)$ be the least element of $L(x)$. In parts (a), (b), (c), suppose L_0 is non-empty.

(a) Prove that L_0 has a minimal element a (that is, there is no $b \in L_0$ such that $a > b$).

(b) Let a be as before. Suppose $a >_0 b_i$ and $a \neq b_i$ $(i = 1, 2)$. Prove $b_i \notin L_0$ and $M(b_1) = M(b_2)$.

[5] A greatest element in L is an $x \in L$ such that $x \geq y$ for all $y \in L$.

(c) Deduce a contradiction.

(d) Finish the proof.

6.10 Rewriting systems. Let (S, R) be a monoid presentation. The *bi-invariant closure* of R is

$$\xrightarrow[R]{} := \big\{(axb, ayb) \;\big|\; (x, y) \in R,\ a, b \in S^*\big\}.$$

We call (S, R) a *rewriting system* if $\xrightarrow[R]{}$ is acyclic, that is, its reflexive-transitive closure

$$\xrightarrow[R]{*}$$

is an ordering. (Note: if $a \xrightarrow[R]{*} b$ and $a \neq b$ we'll say that a is greater than b, not less.) We say $x \in S^*$ is *R-minimal* if $x \xrightarrow[R]{} y$ implies $x = y$.

6.11 Confluent, well-founded, complete. Let (S, R) be a rewriting system. We call R *confluent* if $\xrightarrow[R]{}$ has the diamond property (see the diagram on the right in figure 6). We call R *well-founded* if it has no descending chains, that is,

$$x_0 \xrightarrow[R]{} x_1 \xrightarrow[R]{} \cdots$$

implies that there exists n such that $x_i = x_{i+1}$ for $i > n$. We say that R is *complete* if it is confluent and well-founded.

6.12 Proposition. *Let (S, R) be a complete rewriting system. For any element $x \in S^*$ there is a unique R-minimal $y \in S^*$ such that $x \approx_R y$.*

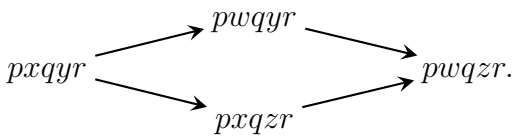
Proof. Let $z \in S^*$. Let $L(z) = \{w \in S^* \mid z \xrightarrow[R]{*} w\}$. Then $L(z)$ has a greatest element z. Moreover, $L(z)$ has no infinite descending chains, because R is well-founded. Moreover, $L(z)$ satisfies the diamond property, because R is confluent. Therefore, the diamond lemma 6.8 says that $L(z)$ has a least element $N(z)$. The existence of y follows by putting $y := N(x)$. The uniqueness is proved as follows. First, if $z \xrightarrow[R]{} w$ then $N(z) = N(w)$. Suppose that uniqueness is false, witnessed by two R-minimal elements y_1, y_2 with $x \approx_R y_1 \approx_R y_2$. Then y_1 and y_2 can be connected by a path of $\xrightarrow[R]{}$ in varying direction. So $N(y_1) = N(y_2)$. Also $y_i = N(y_i)$ which shows $y_1 = y_2$. □

6.13 Example. Continued from 6.1. We now know that

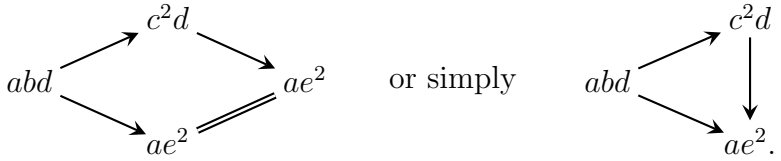
$$(S, R) = (a, b, c, d, e \mid ab \to c^2, \quad bd \to e^2, \quad c^2 d \to ae^2)$$

is a rewriting system. The same way one proves that it is acyclic, one also proves that it is well-founded. We will now prove that it is confluent. Write $\longrightarrow$, $\xrightarrow{*}$ instead of $\xrightarrow[R]{}$, $\xrightarrow[R]{*}$. Suppose $A \longrightarrow B$ and $A \longrightarrow C$. We need to prove $B \xrightarrow{*} D$ and $C \xrightarrow{*} D$ for some D.

Suppose first that the two subwords of A that are replaced here are disjoint, that is, $A = pxqyr$, $B = pwqyr$, $C = pxqzr$ and $x \longrightarrow w$, $y \longrightarrow z$. Then we can obviously finish a diamond as follows:



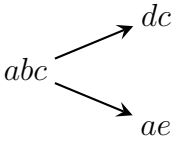
Suppose now the replaced subwords overlap. The only possible such overlap is abd; here ab can be replaced by c^2 or bd can be replaced by e^2. As before, we can ignore the letters not in the subword (here abd); we will not mention them anymore. We have



Notice that the equality sign in the left diamond is a special case of $\xrightarrow[R]{*}$ (we have $x \xrightarrow[R]{*} x$ for all x because $\xrightarrow[R]{*}$ is a reflexive-transitive closure). This proves that our rewriting system R is confluent and thereby complete.

Applying 6.12 tells us that every $\approx_R$-class contains a unique R-minimal element.

6.14 Remark. This remark reduces the calculations necessary for proving confluence for any rewriting system to a minimum. The reasoning of 6.13 shows that all one needs to do to prove confluence is to finish the diamond in the case of *overlapping* reductions, that is



where a, b, c, d, e are words and b is non-empty. (The rewrite rules applied here are $ab \to d$ and $bc \to e$.)

6.15 Example. Consider again the monoid M, which we also studied in 5.19, presented by (S, R) where $S = \{a, b\}$ and $R = \{b = a^2b^2\}$. It is immediately clear that R is a complete rewriting system, because overlapping reductions don't exist. It follows that each element of M is represented by a unique word (normal form) not containing a^2b^2 as a subword.

For $x \in M$, let $\ell(x)$ the length of the normal form for x, that is, the number of letters a and b. As an application, we want to compute the sum of all normal forms (the *total growth function*). The set of normal forms is

$$\Big\{ b^k \,(ab^{\ell+1} \text{ or } a^{\ell+2}b)^p \, a^n \;\Big|\; k, \ell, n, p \geq 0 \Big\}$$

where the "or" means a product of p factors where each factor can be $ab^{\ell+1}$ or $a^{\ell+2}b$. Moreover, each normal form is mentioned precisely once. Their sum is

$$\sum_{k,n,p\geq 0} b^k \Big(\sum_{\ell\geq 0} (a\, b^{\ell+1} + a^{\ell+2}\, b) \Big)^p a^n$$
$$= \frac{1}{1-b} \Big(1 - a\frac{b}{1-b} - \frac{a^2}{1-a} b \Big)^{-1} \frac{1}{1-a}.$$

Putting $a = b = t$ we find a formula for the *growth function*

$$\sum_{x\in M} t^{\ell(x)} = \frac{1}{(1-t)^3(1-t-t^2-t^3)}.$$

7 Presentations of groups

7.1 Group presentations – version 1. A *group presentation* (version 1) is a monoid presentation (S, R) such that for all $x \in S$ there exists $y \in S$ such that

$$\{xy = 1,\ yx = 1\} \subset R.$$

An example of a group presentation is

$$(a,\ b,\ A,\ B \mid aA,\ Aa,\ bB,\ Bb,\ aba = bab).$$

What group is presented by this example?

7.2 Exercise. If the monoid M is presented by a group presentation (version 1), then M is a group.

7.3 Warning. The converse is not true. A monoid presentation may present a group without being a group presentation (version 1). Here is an example: $(a,\ b \mid ab,\ bba)$.

7.4 Free groups. Let $S^{\pm}$ be a set of $2n$ elements x_i, y_i $(1 \leq i \leq n)$. Let R be the set of relations of the form $x_i y_i$ or $y_i x_i$ $(1 \leq i \leq n)$. (Recall that these mean, respectively, $x_i y_i = 1$ and $y_i x_i = 1$.) Then (S, R) is an example of a group presentation (version 1). The monoid S/R is a group by exercise 7.2, and it is called the *free group* (of rank n) on generators $S = \{x_1, \ldots, x_n\}$.

7.5 Groupification of monoid presentations. Let (S, R) be a monoid presentation. We can turn this into a group presentation $(S^{\pm}, R')$. First, let S^{-1} denote a disjoint copy of S, and let $x \mapsto x^{-1}$ denote an involution of $S^{\pm} := S \cup S^{-1}$ which takes S to S^{-1}. Put

$$R' := R \cup \{x^{-1}x = 1,\ xx^{-1} = 1 \mid x \in S\}.$$

It is clear that $(S^{\pm}, R')$ is a group presentation (version 1). We call it the *groupification* of the monoid presentation (S, R).

7.6 Group presentations – version 2. Sometimes one writes down a monoid presentation, and calls it a group presentation, even though it is not! What happens here is that one has the *groupification* of that monoid presentation in mind.

A typical example is

$$(a,\ b \mid aba = bab).$$

A formula like this can be a monoid presentation or a group presentation (version 2).

7.7 Group presentations – version 3. This is the most common notation for group presentations. Here the elements of S^{-1} are literally written as x^{-1} for some $x \in S$. Moreover, one doesn't necessarily mention the relations $xx^{-1} = 1$, $x^{-1}x = 1$ because they are obvious. A typical example is

$$(a,\ b \mid ab^{-1} = ba^{-2}).$$

It will become clear in 7.10 that another way of saying this is that a group presentation (version 3) is a pair (S, R) where S is a set and R a subset of the free group on S.

7.8 Exercise. Which of the following could be a monoid presentation? Which could be a group presentation and of which versions?

$$(a,\ b \mid ab,\ a^4b^5a^6 = b)$$
$$(a,\ b \mid a^{-3}b = b^{-5}a^2)$$
$$(a,\ b,\ c \mid ab,\ ba,\ c^2,\ cac = b)$$
$$(a,\ b,\ c,\ d \mid ab,\ ba,\ cd,\ dc,\ cac = d^{-1})$$

7.9 Reduced words. Let F be a free group on S. This was defined in 7.4 using version 1 of group presentations, but from now on we will use version 3. So our alphabet $S^{\pm}$ is a disjoint union $S \cup S^{-1}$. A word

$$z_1 \cdots z_k \in (S^{\pm})^* \qquad (\text{with } z_i \in S^{\pm})$$

is called *reduced* if none of the length 2 subwords z_iz_{i+1} is of the form xx^{-1} with $x \in S^{\pm}$.

It is obvious that every element of F can be represented by a reduced word[6]. The following proposition says that the converse holds.

7.10 Proposition. *Every element of a free group can be uniquely represented by a reduced word.*

Proof. A presentation (version 1) for the free group is with generators x_i, y_i $(i \in I)$ and relations $R = \{(x_iy_i, 1), (y_ix_i, 1)\}$. One shows that the very same relations R are also a complete rewriting system. (Do yourself.) It follows that every element of the free group is represented by a unique R-minimal word. But R-minimal words are precisely reduced words, and the proof is finished. □

7.11 Remark/Exercise. In 5.15 (respectively, 5.17) we saw how to characterize homomorphisms from a presented monoid to any monoid (respectively, another presented monoid). Of course, there are group analogues for these results. Exercise: Formulate them. *Exercise: Prove them.

7.12 Example. We will show that the presented groups $G = \langle 1, 2 \mid 121 = 212\rangle$ and $H = \langle a, b \mid a^3 = b^2\rangle$ are isomorphic. (Of course, $G = B_3$, the 3-string braid group.)

Let P be the free group on $1, 2$ and Q the free group on a, b.

Define $f\colon Q \to P$ by $f(a) = 12$, $f(b) = 121$. On denoting $\approx$ the appropriate congruences we have

$$f(a^3) = (12)^3 = (121)(212) \approx (121)(121) = f(b^2).$$

By the group analogue to 5.17 it follows that there is a homomorphism $f_*\colon H \to G$ with $f_*[x] = [fx]$.

[6]If there is a forbidden subword xx^{-1}, throw it away. This doesn't change the group element it represents. Keep throwing forbidden subwords away until you arrive at a reduced element.

Conversely, define $g\colon P \to Q$ by $g(1) = a^{-1}b$, $g(2) = b^{-1}a^2$. Then

$$\begin{aligned} g(121) &= (a^{-1}b)(b^{-1}a^2)(a^{-1}b) = b \approx b(b^{-2}a^3) \\ &= b^{-1}a^3 = (b^{-1}a^2)(a^{-1}b)(b^{-1}a^2) = g(212). \end{aligned}$$

By the group analogue to 5.17 there exists a homomorphism $g_*\colon G \to H$ with $g_*[x] = [gx]$.

Prove yourself that $f_*g_* = 1_G$ and $g_*f_* = 1_H$. Therefore, f, g are bijective and $G \cong H$. □

7.13 Now we can finally understand where theorem 3.7 comes from (the theorem which helps finding homomorphisms from braid groups to other groups). It is an immediate consequence of the group analogue to 5.15 and the presentation of braid groups, which we don't prove but state in the following.

7.14 Theorem/Definition. The braid group is presented by generators σ_i $(1 \le i < n)$ and the Artin relations (1.10), (1.11). This is called the *Artin presentation*. □

7.15 * Now that we know what free groups are, we can understand why section 4 was titled "the action on the free group" and not "the action on G^n". There exists an action $B_n \to \mathrm{Aut}(F_n)$ where F_n denotes the free group on n generators, and which is closely related to section 4. We won't go into the details.

7.16 *Some properties. Here are some important results which we shall not prove, and mostly not even use. Let (S, R) be a monoid presentation and $(S^{\pm}, R')$ its groupification. Then the isomorphism class of the group $S^{\pm}/R'$ depends only on the isomorphism class of the monoid S/R. We write $\mathrm{Gp}(S/R) := S^{\pm}/R'$ and it is called the *groupification* of the monoid S/R. The groupification of a group is the group itself. The process of going from a monoid to its groupification is a functor from the category of monoids to the category of groups. There is a natural homomorphism of monoids from any monoid M to $\mathrm{Gp}(M)$.

7.17 Exercise. Let B_3^+ be the monoid presented by $(S_1, R_1) = (1, 2 \mid 121 = 212)$. (Warning: $\varnothing$ is the identity, 1 is not.) Let B_3 be the group presented by the same presentation, regarded as a group presentation. From the general theory of presentations it follows that there is a natural homomorphism $f\colon B_3^+ \to B_3$. One of the things you prove in this exercise is that f is injective.

(a) Prove that B_3^+ is presented [7] by

$$(S_2, R_2) := \left(1, 2, \Delta \;\middle|\; \begin{array}{ll} 121 \to \Delta, & 212 \to \Delta, \\ 1\Delta \to \Delta 2, & 2\Delta \to \Delta 1 \end{array}\right)$$

[7] Recall our convention $xRy \Leftrightarrow (x, y) \in R \Leftrightarrow (x = y) \in R \Leftrightarrow (x \to y) \in R$, four notations for the same thing.

(b) Construct a map $g\colon S_2^* \to \mathbb{Z}_{\geq 0}$ such that $g(x) > g(y)$ if $x \xrightarrow[R]{} y$. You don't need to prove that g has this property. Deduce that (S_2, R_2) is a well-founded rewriting system for B_3^+.

(c) Prove that (S_2, R_2) is a complete rewriting system for B_3^+.

(d) Prove that you don't get a complete rewriting system for B_3^+ if you remove the last rewriting rule $2\Delta \to \Delta 1$.

(e) Compute the R_2-minimal form for 22121122121222121.

(f) Prove that

$$(S_3, R_3) := \left(1, 2, \Delta, \delta \;\middle|\; \begin{array}{ll} 121 \to \Delta, & 212 \to \Delta, \\ 1\Delta \to \Delta 2, & 2\Delta \to \Delta 1, \\ 1\delta \to \delta 2, & 2\delta \to \delta 1, \\ \Delta\delta \to \varnothing, & \delta\Delta \to \varnothing \end{array} \right)$$

is a monoid presentation for B_3.

(g) From now on you may assume without proving it that (S_3, R_3) is a well-founded rewriting system for B_3. Prove that (S_3, R_3) is a complete rewriting system for B_3.

(h) Prove that every R_2-minimal word in $\{1, 2, \Delta\}^*$ is also R_3-minimal. Deduce that f is injective.

(i) There is a homomorphism (called length) $\ell\colon B_3^+ \to \mathbb{Z}$, $\ell(1) = \ell(2) = 1$. (You don't need to prove this.) Clearly, the rewriting system (S_2, R_2) preserves the length, that is, for all $(x, y) \in R$ one has $\ell(x) = \ell(y)$. Use this to compute the formal power series

$$\sum_{x \in B_3^+} t^{\ell(x)}.$$

Hint: The R_2-minimal forms are as follows:

$$\Delta^k \, a^{k_1} \, b^{k_2} \, a^{k_3} \cdots (a \text{ or } b)^{k_n}$$

where $k \geq 0$, $\{a, b\} = \{1, 2\}$ and $(k_1, \ldots, k_n)$ satisfies some condition which you should find. Don't worry about the parity of n!

7.18 *Exercise. Let p be a prime number and let $\mathbb{F}_p$ or $\mathbb{Z}_p$ be the field of p elements. Prove that $\mathrm{SL}(2, \mathbb{F}_p)$ is presented by $(x, y \mid xyx = yxy,\ (xy)^6,\ x^p)$.

8 Cayley graphs

8.1 Graphs. A *graph* is a triple (V, E, ∂) where V is a set (of *vertices*), E is a set (of *edges*) and ∂: $E \to P(V)$ is a map such that $\partial(e)$ is a set of one or two vertices, for all edges $e \in E$. The elements of $\partial(e)$ are the *endpoints* of the edge e. An edge is called a *loop* if it has just one endpoint. Two distinct edges e, f are called *parallel* or *multiple* if $\partial(e) = \partial(f)$.

One of the best things about graphs is that one can draw pictures of them. Vertices are represented by dots and an edge e by an arc between the two elements of $\partial(e)$ (which will be equal if e is a loop).

A *directed graph* is a graph together with, for every edge e, an orientation on the drawing of that edge. If the endpoints of e are distinct, this is equivalent to choosing a total ordering on $\partial(e)$. If the edge e has just one endpoint, this doesn't work and one needs to rely on the drawing. In pictures of graphs, edge orientations are indicated by an arrow. If the vertices are distinct, then the arrow points from the smaller vertex to the bigger vertex.

8.2 Cayley graphs. Let G be a group and $S \subset G$ a generating set. The *Cayley graph* $\Gamma(G, S)$ has vertex set G and edge set

$$E = \Big\{ \{g, gs\} \;\Big|\; g \in G,\ s \in S \Big\}.$$

The map ∂ is just the inclusion $E \subset P(V)$.

8.3 Exercise. Prove that a Cayley graph has no multiple edges. Prove that it has loops if and only if $1 \in S$.

8.4 *Remark. For those who know the universal cover. If G is the fundamental group of a path-connected topological space T then $\Gamma(G, S)$ is an approximation to the universal cover of T.

8.5 Labels of edges. Let G be a group and $S \subset G$ a generating set. Let $g \in G$ and $x \in S^{\pm} = S \cup S^{-1}$. Then $\{g, gx\}$ is an edge of the Cayley graph. It is useful to equip the oriented edge (g, gx) with the *label* x and the reversely oriented edge (gx, g) with the inverse label x^{-1}.

8.6 Paths in the Cayley graph and the word metric. Let S be a generating set of a group G. A *path* in the Cayley graph $\Gamma(G, S)$ is a sequence

$$(g_0,\ x_1,\ g_1,\ x_2,\ g_2,\ \ldots,\ x_n,\ g_n)$$

where $g_i \in G$ are vertices and $x_i \in S \cup S^{-1}$ are generators, such that

$$g_i\, x_i = g_{i+1} \qquad \text{for all } i.$$

We say that this path starts at g_0 and finishes at g_n. The *label* of the path is $x_1 \cdots x_n \in (S^{\pm})^*$ (an element in the free monoid on $S^{\pm} = S \cup S^{-1}$).

The *length* of the path is n. For $g, h \in G$, we define $d_S(g, h)$ to be the smallest length of a path connecting g with h. Then d_S is a metric on G, called the *word metric* on G (with respect to the generating set S). We also write $\ell_S(g)$ instead of $d_S(g, 1)$.

8.7 Proposition. *In the Cayley graph $\Gamma(G,S)$ of a group presentation (S,R) the two endpoints of a path are equal if and only if its label represents the trivial element of the group.*

Proof. Consider the path described in 8.6. Applying the identity $g_{i-1}x_i = g_i$ repeatedly yields that $g_n = g_0\, x_1 \cdots x_n$. So the endpoints g_0, g_n are equal if and only if $x_1 \cdots x_n = 1$. □

8.8 Left and right multiplication in a Cayley graph. Consider a Cayley graph $\Gamma(G,S)$ and let $g \in G$. Then we have a permutation of the vertex set g_0: $x \mapsto gx$; and a permutation of the edge set g_1: $\{h, hs\} \mapsto \{gh, ghs\}$. Moreover, the vertex operator ∂ commutes with these operations, because ∂ is just the inclusion. For these reasons, we call (g_0, g_1) an *automorphism* of the Cayley graph. These automorphisms come from left multiplication. See exercise 8.14 for an automorphism not coming from left multiplication.

What about right multiplication? In general, the action on the vertex set $x \mapsto xg$ ($g \in G$) is *not* an automorphism of the Cayley graph. Still, it has a meaning: if $s \in S$ then the action on the vertex set $x \mapsto xs$ takes any vertex to one of its neighbours. More generally, if $g \in G$ and $\ell(g) = n$ then right multiplication with g takes any vertex to a vertex at distance no more than n.

8.9 Exercise. Let G be a group generated by $S \subset G$. Let $g, x, y \in G$. Prove $d_S(x,y) = d_S(gx, gy)$ and $d_S(x,y) = \ell_S(x^{-1}y)$.

8.10 We are mainly interested in Cayley graphs $\Gamma(S/R, S)$ for a presentation (S,R) (where we regard S as a generating subset of G). In that case, 8.7 implies that a path is closed as soon as its label is of the form xy^{-1} for some relations $(x = y) \in R$.

In practice one constructs the Cayley graph $\Gamma(G,S)$ as follows. (Examples will follow.) One starts with one vertex $1 \in G$. One continues by drawing an edge labelled $x \in S$ emanating from every vertex, adding the final vertex of such an edge if necessary. One makes sure that the condition of 8.7 is satisfied. Labels of edges are important and are indicated everywhere; the names of the vertices can be ignored.

Warning: It may happen that during the process, two vertices or two edges turn out to be equal even if they didn't appear to be at first. In that case the drawing should be simplified by identifying such.

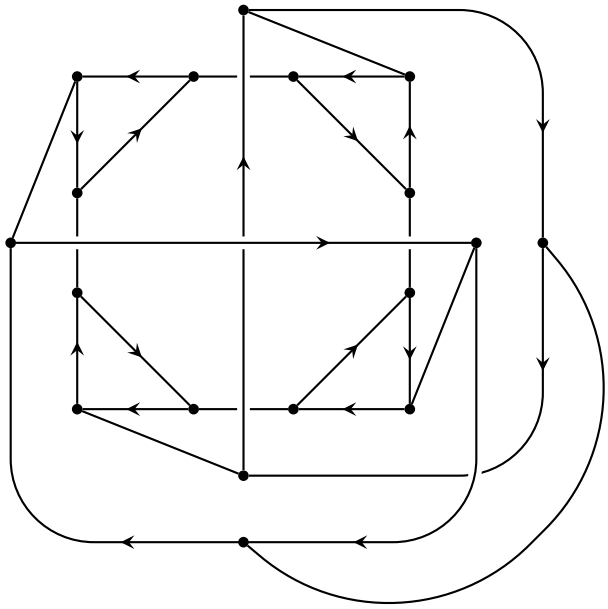
8.11 Example. Figure 7 shows the Cayley graph of the presentation

$$(x, y \mid xyxy = yxyx,\ x^3 = 1,\ y^2 = 1).$$

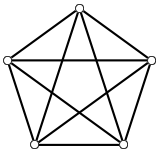
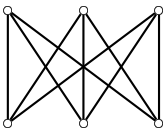
Note that, since y is an involution, if an oriented edge has label y, then the reversely oriented edge has the same label. Therefore, if an edge has label y, we needn't give the edge an orientation. Every edge with an arrow has label x, so we don't indicate their labels in the picture.

We conclude that the above group has 18 elements, because that's the number of vertices in the graph.

Figure 7: See example 8.11



8.12 Exercise. Prove that the Cayley graph of 8.11 can be drawn with just one crossing. Prove also that it cannot be drawn without crossings, that is, it is not planar. You may use *Kuratowski's theorem* which states that a graph is planar if and only if none of its quotients [8] contains one of the following graphs.

$K_5 =$  $K_{33} =$ 

8.13 Example. Figure 8 shows the Cayley graph of the presentation

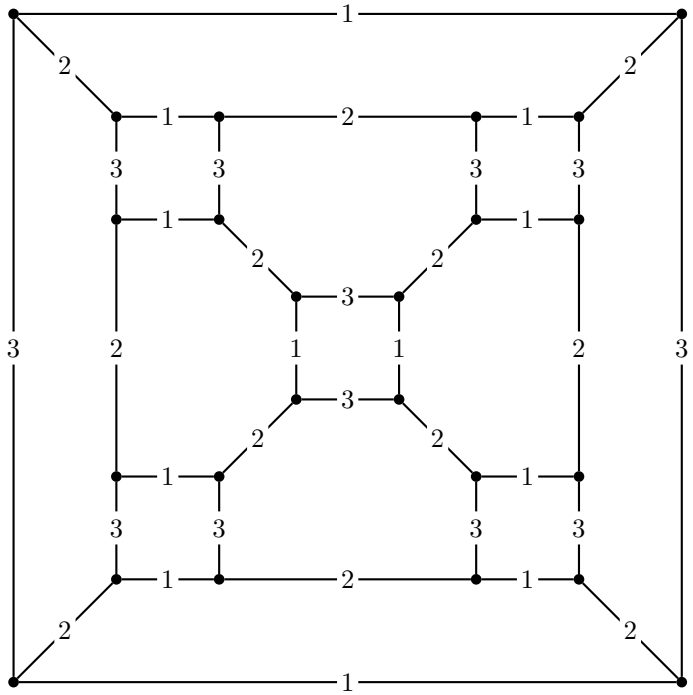
$$(1, 2, 3 \mid 1^2,\ 2^2,\ 3^2,\ (12)^3,\ (23)^3,\ (13)^2).$$

Let G denote the group presented by this presentation. Then G has 24 elements. Moreover, there is a surjective homomorphism $f\colon G \to \Sigma_4$ from G to the symmetric group defined by $f(i) = (i, i+1)$ (exercise). But Σ_4 also has 24 elements, so f is an isomorphism. We have shown that our presentation is in fact a presentation of Σ_4.

8.14 Exercise. Prove that the Cayley graph $\Gamma(\Sigma_4, S)$ from example 8.13 (viewed as a graph (V, E, ∂)) has an automorphism which does not come from left multiplication by an element $h \in \Sigma_4$ (see 8.8). Don't use the picture of this graph in your proof.

[8] A *quotient* of a graph (V, E, ∂) is a graph (V', E, ∂') where $V' = V/\!\sim$ for some equivalence relation $\sim$ on V, and $\partial'(e)$ is the set of equivalence classes of elements of $\partial(e)$.

Figure 8: See example 8.13



8.15 Exercise. Draw the Cayley graph for the presentation $G = \langle x, y \mid x^3,\ y^2,\ xyxyx^{-1}y \rangle$. Make your drawing planar, that is, without crossings. Choose a vertex a and label each vertex b with the distance $d_S(a, b)$. You needn't prove that your drawing is correct. Prove that G is isomorphic to the alternating group A_4.

8.16 Exercise. Make a planar drawing of the Cayley graph for the presentation $\langle x, y \mid x^5,\ y^2, (xy)^3 \rangle$. (It has 60 vertices so you need to draw somewhat small to make it fit on one page.) You needn't prove that your drawing is correct.

9 The symmetric group

9.1 For $n \geq 1$, write $I_n = \{1, \ldots, n\}$ and $\Sigma_n = \mathrm{Sym}(I_n)$, the symmetric group on I_n. We agree that the Σ_n-action on I_n is from the left. As an example, we have $(12)(23) = (123)$, not (321).

9.2 Reflections. A *reflection* in S_n is an element (written (ij) or s_{ij}) which fixes all elements in I_n except $i, j \in I_n$. Some people call them transpositions. Every reflection is of order 2. The set of reflections in Σ_n will be denoted by Ref. The reflections $s_i := s_{i,i+1}$ are called *fundamental reflections*. The set of fundamental reflections in Σ_n is written S.

9.3 The aim of this section is to understand the Cayley graph $\Gamma(\Sigma_n, S)$. The word metric and word length are written D, L instead of d_S, ℓ_S.

9.4 We have a homomorphism $\pi\colon B_n \to \Sigma_n$ defined as follows. Let $x \in B_n$. Then $(\pi x)i = j$ if the string in position i at the bottom (counted from the left) is the string in position j at the top.

We follow the string from bottom to top rather than reversely because Σ_n acts on I_n on the left.

Note $\pi(\sigma_i) = s_i$.

9.5 Exercise. Prove that $\pi\colon B_n \to \Sigma_n$ is a homomorphism.

9.6 Theorem. *The symmetric group Σ_n is presented by generators s_i ($1 \leq i < n$) and the following relations for all appropriate indices.*

$$\begin{aligned} s_i\, s_{i+1}\, s_i &= s_{i+1}\, s_i\, s_{i+1} \\ s_i\, s_j &= s_j\, s_i \qquad (|i-j| > 1) \\ s_i^2 &= 1 \end{aligned}$$

Proof. It is clear that two braids have the same π-image if and only if one can be moved into the other by, not only the usual homotopy, but also moving one string through another. A basic example of one string moving through another is $\sigma_i^2 \to 1$. All other examples are conjugates of σ_i^2, so the kernel of π is generated, as normal subgroup, by all σ_i^2. In other words, a presentation for the symmetric group Σ_n is obtained from the presentation for the braid group B_n by adding the extra relations σ_i^2 (just one of them suffices). □

9.7 *Remark. The above proof is sketchy and depends on the presentation for the braid group, which we won't prove. But the symmetric group is a purely combinatorial thing, so one expects that a clean combinatorial proof of 9.6 exists. It exists indeed, see for example Johnson, Presentations of Groups, pages 61–64.

9.8 The standard representation. Put

$$E = \bigoplus_{i=1}^{n} \mathbb{R}e_i, \qquad V = \bigoplus_{i=1}^{n} \mathbb{R}v_i.$$

We define a bilinear map $\langle \cdot, \cdot \rangle$: $E \times V \to \mathbb{R}$ by $\langle e_i, v_j \rangle = \delta_{ij}$ which is 1 if $i = j$ and 0 otherwise. (The bilinear map $\langle \cdot, \cdot \rangle$ is an example of a pairing and makes E and V into each other's duals.) The symmetric group Σ_n acts on E and V by

$$f(e_i) = e_{f(i)}, \qquad f(v_i) = v_{f(i)}, \qquad (f \in \Sigma_n).$$

We call V the *standard representation* of Σ and E its dual.

9.9 * There is a Σ_n-invariant Euclidean metric on V, given by

$$m(\sum_i x_i\, v_i, \sum_i y_i\, v_i) = \Big(\sum_i (x_i - y_i)^2 \Big)^{1/2}.$$

We shall not use this metric anywhere.

9.10 Hyperplanes and chambers. For $1 \le i < j \le n$ we define a *hyperplane*

$$H_{ij} = H_{ji} = H_{(ij)} = \big\{ x \in V : \langle e_i - e_j, x \rangle = 0 \big\}.$$

Notice that (ij) preserves H_{ij} pointwise. It also interchanges the two sides of H_{ij}.

A *chamber* is a connected component of

$$V - \bigcup_{r \in \mathrm{Ref}} H_r. \tag{9.11}$$

9.12 *Exercise. Prove that a chamber is convex. Prove that every convex subset of (9.11) is contained in a chamber.

9.13 Lemma. *The symmetric group Σ_n acts simply transitively*[9] *on the set of chambers.*

Proof. Let C be a chamber and $(ij) \in \mathrm{Ref}$. Then either $\langle e_i - e_j, x \rangle > 0$ for all $x \in C$, or $\langle e_i - e_j, x \rangle < 0$ for all $x \in C$ (because C is connected and $C \cap H_{ij} = \varnothing$). Let us write $i <_C j$ if the former is the case. Clearly, $<_C$ is a total ordering. It is clear that $C \mapsto <_C$ is a bijection (from the set of chambers to the set of total orderings on I_n). It is known that Σ_n acts simply transitively on the set of total orderings on I_n. □

9.14 Separation of chambers. The complement $V - H_{ij}$ has precisely two connected components, which are called *half-spaces*. We say that H_{ij} and (ij) *separate* two chambers if they are in the two distinct connected components. In formula, H_{ij} and (ij) separate two chambers C_1, C_2 if

$$\langle e_i - e_j, x \rangle \langle e_i - e_j, y \rangle < 0$$

for one (hence all) $x \in C_1$, $y \in C_2$.

The number of reflections separating a chamber C_1 from a chamber C_2 is written $d(C_1, C_2)$. Then d is a metric on the set of chambers.

[9] If a group acts on a set X, we say that the action is *transitive* if one (hence any) *orbit* $Gx = \{gx \mid g \in G\}$ (with $x \in X$) equals X. The action is called *simply transitive* if it is transitive and $gx = x$ implies $g = 1$ ($g \in G$, $x \in X$).

9.15 Separation of permutations. From now on we fix a *fundamental chamber*

$$C = \Big\{ \sum_{i=1}^{n} x_i v_i \;\Big|\; i < j \Rightarrow x_i < x_j \Big\}.$$

If chambers can be separated then so can permutations, because there is a bijection from Σ_n to the set of chambers, taking $x \in \Sigma_n$ to xC (see 9.13). We say that H_{ij} and (ij) *separate* two permutations $x, y \in \Sigma_n$ if they separate xC from yC. Similarly, we define

$$d(x, y) = d(xC, yC) \qquad (x, y \in \Sigma_n).$$

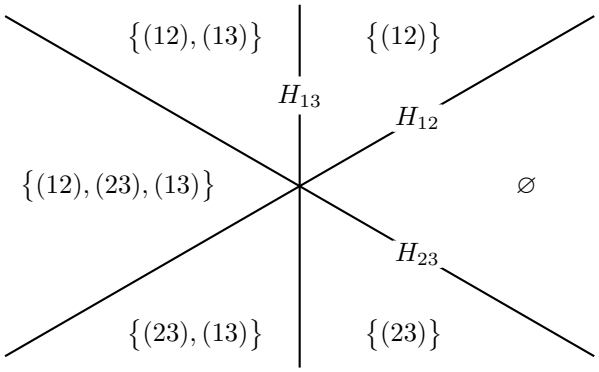
Then d is a metric on the symmetric group. We also define

$$\ell(x) = d(1, x) \qquad (x \in \Sigma_n). \tag{9.16}$$

9.17 Definition. Let $x \in \Sigma_n$. The set of reflections which separate x from 1 will be written $N(x)$. So clearly, $\ell(x) = |N(x)|$ for all $x \in \Sigma_n$.

9.18 Example. Figure 9 shows the situation for $n = 3$. The picture relies on the fact that we can reduce the dimension by one by dividing out $(\sum_i v_i)\mathbb{R}$. The fundamental chamber is labelled with $\varnothing$. In general the chamber xC $(x \in \Sigma_n)$ is labelled $N(x)$.

Figure 9: The $N(x)$ for $n = 3$



9.19 Exercise. Let $x \in \Sigma_n$ and $1 \le i < j \le n$. Then $(ij) \in N(x^{-1}) \Leftrightarrow xi > xj$.

9.20 Exercise. Compute $N(x)$ and $\ell_S(x)$ if $x = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 9 & 6 & 8 & 3 & 2 & 5 & 1 \end{smallmatrix}\right) \in \Sigma_9$.

9.21 Exercise.

(a) Let $r \in \mathrm{Ref}$, $g, a, b \in \Sigma_n$. Prove that r separates a from b if and only if grg^{-1} separates ga from gb.

(b) Prove that d is left-invariant, that is, $d(xy, xz) = d(y, z)$ for all $x, y, z \in \Sigma_n$.

(c) Let $x, y \in \Sigma_n$ be such that $N(x) \subset N(xy)$. Prove that $N(xy)$ is the disjoint union of $N(x)$ and $x\,N(y)\,x^{-1}$.

9.22 Lemma. *The metric d coincides with the word metric D of (Σ_n, S).*

Proof. First notice that both d and D are left-invariant. For you d you proved this in 9.21; and it is true for D because D is a word metric (see 8.9).

We claim $L(x) = 1 \Rightarrow \ell(x) = 1$. Indeed, if $L(x) = 1$ then $x = s_i$ for some i. Prove yourself that $\ell(s_i) = 1$, thus proving the claim. By left-invariance, it follows that $D(x, y) = 1 \Rightarrow d(x, y) = 1$.

Proof that $d \leq D$. Let $x, y \in \Sigma_n$ and write $k = D(x, y)$. But D is a word metric, so there are $x = x_0, \ldots, x_k = y$ such that $D(x_i, x_{i+1}) = 1$ for all appropriate i. By our above claim, it follows that $d(x_i, x_{i+1}) = 1$. Using the fact that d is a metric we find

$$d(x, y) = d(x_0, x_k) \leq \sum_i d(x_i, x_{i+1}) = k = D(x, y).$$

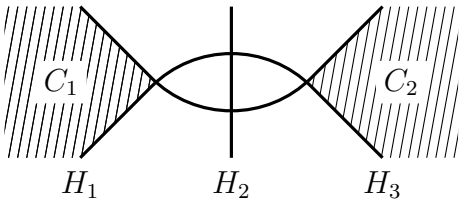
First proof that $D \leq d$. (Sketchy.) Let $x, y \in \Sigma_n$. We want to prove $D(x, y) \leq d(x, y)$. Choose points $p \in xC$, $q \in yC$. The straight line segment A from p to q passes through no $H_r \cap H_s$ $(r \neq s)$ if p, q are chosen appropriately; assume this is the case. By looking at the chambers which A passes through, one obtains an expression for $x^{-1}y$ in terms of the fundamental reflections S. But straight line segments pass through a hyperplane at most once; therefore the above word has length $d(x, y)$. This proves $D \leq d$.

Second proof that $D \leq d$. (Combinatorial.) Let $x \in \Sigma_n$. By induction on $\ell(x)$ we will prove $\ell(x) = L(x)$. If $\ell(x) = 0$ then $x = 1$, and our result holds. Assume now $\ell(x) > 0$. Then $x \neq 1$ so there exists i such that

$$x^{-1}(i) > x^{-1}(i + 1).$$

So $s_i \in N(x)$ and $\ell(x) = \ell(s_i) + \ell(s_i x) = 1 + \ell(s_i x)$ so $\ell(s_i) = L(s_i x)$ by the induction hypothesis. It follows that $L(x) \leq L(s_i) + L(s_i x) = 1 + \ell(s_i x) = 1 + \big(\ell(x) - 1\big) = \ell(x)$. □

9.23 Example. The first proof of $D \leq d$ in the above result suggests how to find examples of similar situations where $D \neq d$. Consider three curves H_1, H_2, H_3 ("curved hyperplanes") in the plane and two of the chambers C_1, C_2 defined by them as follows.



$$d(C_1, C_2) = 1$$
$$D(C_1, C_2) = 3$$

Then $d(C_1, C_2) = 1$ but $D(C_1, C_2) = 3$. The first proof of $D \leq d$ in the above doesn't work here because the H_i are not straight lines.

9.24 Lemma. *Let $x, y \in \Sigma_n$. Then*

$$\ell(xy) = \ell(x) + \ell(y) \quad \Leftrightarrow \quad N(x) \subset N(xy).$$

Proof. $\ell(xy) = \ell(x) + \ell(y) \Leftrightarrow d(1, xy) = d(1, x) + d(1, y)$
$\Leftrightarrow d(1, xy) = d(1, x) + d(x, xy)$
$\Leftrightarrow$ no reflection separates x from both 1 and xy
$\Leftrightarrow N(x) \subset N(xy)$. □

9.25 Definition. We define a relation $\leq$ on Σ_n by

$$x \leq xy \quad \Leftrightarrow \quad \ell(xy) = \ell(x) + \ell(y)$$

which is also equivalent to $N(x) \subset N(xy)$. Notice that $N\colon \Sigma_n \to P(\text{Ref})$ is injective. Therefore the relation $\leq$ on Σ_n is an ordering.

9.26 Exercise.

(a) Define $x, y \in \Sigma_n$ by $x = s_i$, $y = s_{i+1}$. Prove $1 < x < xy < xyx$.

(b) Define $x, y \in \Sigma_n$ by $x = s_i$, $y = s_j$ and suppose $|i - j| > 1$. Prove $1 < x < xy$.

9.27 Exercise. Prove that there exists $w_0 \in \Sigma_n$ such that $N(w_0) = \text{Ref}$. Give a formula for $w_0(i)$ for all $i \in I_n$. Show that $x \leq w_0$ for all $x \in \Sigma_n$.

9.28 Proposition. *Let $T \subset \text{Ref}$. Then the following are equivalent.*

(P) $T \in N(\Sigma_n)$.

(Q) Whenever $1 \leq i < j < k \leq n$ we have

$$\big[(ij) \in T \text{ and } (jk) \in T\big] \quad \Rightarrow \quad (ik) \in T \tag{9.29}$$

$$\big[(ij) \notin T \text{ and } (jk) \notin T\big] \quad \Rightarrow \quad (ik) \notin T. \tag{9.30}$$

Proof. For any $T \subset \text{Ref}$, we define a relation $<_T$ on I_n by

$$i <_T j \quad \Leftrightarrow \quad \Big[\big(i < j \text{ and } (ij) \notin T\big) \text{ or } \big(i > j \text{ and } (ij) \in T\big)\Big].$$

In order to prove the proposition, we introduce a third property

(R) The relation $<_T$ is a strict ordering.

We now prove (P) ⇒ (R). Put $T = N(x^{-1})$. We find

$$\begin{aligned} i <_T j &\Leftrightarrow \Big[\big(i < j \text{ and } (ij) \notin T\big) \text{ or } \big(i > j \text{ and } (ij) \in T\big)\Big] \\ &\Leftrightarrow \Big[\big(i < j \text{ and } xi < xj\big) \text{ or } \big(i > j \text{ and } xi < xj\big)\Big] \\ &\Leftrightarrow xi < xj, \end{aligned}$$

and hence $<_T$ is a strict ordering. We have proved (P) ⇒ (R). But (P) and (R) both occur $n!$ times; so (P) and (R) are equivalent.

We now prove (P) $\Rightarrow$ (Q). Suppose $T = N(x^{-1})$. By 9.19 we find

$$\begin{aligned}(ij) \in T \text{ and } (jk) \in T \quad &\Rightarrow \quad xi > xj \text{ and } xj > xk \\ &\Rightarrow \quad xi > xk \quad \Rightarrow \quad (ik) \in T\end{aligned}$$

which proves (9.29). Similarly

$$\begin{aligned}(ij) \notin T \text{ and } (jk) \notin T \quad &\Rightarrow \quad xi < xj \text{ and } xj < xk \\ &\Rightarrow \quad xi < xk \quad \Rightarrow \quad (ik) \notin T\end{aligned}$$

which proves (9.30) and thereby (P) $\Rightarrow$ (Q).

It remains to prove (Q) $\Rightarrow$ (R). There are $2^3 = 8$ possibilities for

$$T \cap \big\{(ij), (jk), (ki)\big\}$$

of which precisely $8 - 2 = 6$ satisfy (Q_{ijk}) and precisely $3! = 6$ satisfy (R_{ijk}). But we already proved (R) $\Rightarrow$ (Q) so the 6 cases coincide, that is, (R) is equivalent to (Q). □

9.31 *Exercise. Let $r \in \mathrm{Ref}$ and $x, y \in \Sigma_n$. Prove that r separates x from y if and only if $d(x, y) > d(x, ry)$.

9.32 Exercise. Let S denote the set of fundamental reflections in Σ_7 and write $s_i < s_j$ if and only if $i < j$. Find the lexicographically smallest minimal expression $(x_1, \ldots, x_k) \in S^k$ for

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix},$$

that is, with the property that there is no minimal expression of the form $(x_1, \ldots, x_{i-1}, y, \ldots)$ with $y < x_i$.

10 The symmetric group is a lattice

10.1 Meet and join. Let $(L, \leq)$ be an ordered set and $X \subset L$ a subset. If $\{y \in L \mid x \leq y \text{ for all } x \in X\}$ has a least element, then that is called the *join* or *least common upper bound* of X, and denoted $\vee X$. Likewise, if $\{y \in L \mid x \geq y \text{ for all } x \in X\}$ has a greatest element, then that is called the *meet* or *greatest common lower bound* of X, and denoted[10] $\wedge X$. We write

$$x \wedge y := \wedge\{x, y\}, \qquad x \vee y := \vee\{x, y\}.$$

10.2 Definition. A *lattice* is an ordered set in which any two elements have a meet and a join.

10.3 Exercise. In each of the following cases, L is a set of sets, and L will be ordered by inclusion (that is, $X \leq Y \Leftrightarrow X \subset Y$). Prove that L is a lattice.

(a) L is the set of subsets of a fixed set S.

(b) L is the set of subspaces of a fixed vector space V.

(c) L is the set of subgroups of a fixed group G.

10.4 Lemma. *Let $(L, \leq)$ be a finite ordered set. Suppose that L has a least element, and that any two elements of L have a join. Then L is a lattice.*

Proof. Let $x, y \in L$. We need to prove that x, y have a meet. Let

$$A = \{z \in L \mid z \leq x \text{ and } z \leq y\}.$$

The smallest element of L is in A, so A is non-empty. Also A is finite because L is. Since any two elements in L have a join, any finite number have as well; so the join $w := \vee A$ exists. We will prove $x \wedge y = w$. By construction x is an upper bound for A, so $x \geq w$. Likewise we have $y \geq w$. So $w \in A$. This proves $x \wedge y = w$. □

10.5 Theorem. *The ordered set $(\Sigma_n, \leq)$ is a lattice.*

Proof. We have an isomorphism of ordered sets $N\colon \Sigma_n \to N(\Sigma_n)$ (the latter ordered by inclusion) by 9.24 and 9.25. We will prove that $N(\Sigma_n)$ is a lattice.

Recall from 9.28 that $N(\Sigma_n)$ is precisely the set of subsets $A \subset \text{Ref}$ satisfying

$$\big[(ij) \in A \text{ and } (jk) \in A\big] \;\Rightarrow\; (ik) \in A \qquad (1 \leq i < j < k \leq n) \tag{10.6}$$

$$\big[(ij) \notin A \text{ and } (jk) \notin A\big] \;\Rightarrow\; (ik) \notin A \qquad (1 \leq i < j < k \leq n). \tag{10.7}$$

We will use this as our characterisation of $N(\Sigma_n)$.

It is clear that $N(\Sigma_n)$ has a least element $\varnothing = N(1)$, and that $N(\Sigma_n)$ is finite. By 10.4 we will be done if we can prove that any two elements of $N(\Sigma_n)$ have a join. We will now prove this.

[10] Here is a useful trick to tell the symbols apart: $\wedge$ looks like $\cap$ and $\vee$ looks like $\cup$.

Let $A, B \in N(\Sigma_n)$. Let C be the least subset of Ref containing $A \cup B$ and satisfying (10.6). Equivalently, for $1 \leq i < j \leq n$ we have $(ij) \in C$ if and only if there exist $i = \ell_0 < \cdots < \ell_p = j$ such that $(\ell_q \ell_{q+1}) \in A \cup B$ for all q.

We will prove $C \in N(\Sigma_n)$, that is, C satisfies (10.7). Let $1 \leq i < j < k \leq n$ and suppose $(ik) \in C$. We want to prove $(ij) \in C$ or $(jk) \in C$. By construction there are $i = \ell_0 < \cdots < \ell_p = k$ such that $(\ell_q \ell_{q+1}) \in A \cup B$ for all q.

Suppose first $\ell_q = j$ for some q. Then $(ij) = (\ell_0 \ell_q) \in C$.

Suppose next $\ell_q < j < \ell_{q+1}$ for some q. We know that $(\ell_q \ell_{q+1})$ is in $A \cup B$, say, in A. As A satisfies (10.7), A contains $(\ell_q j)$ or $(j \ell_{q+1})$, say, $(\ell_q j) \in A$. Then $(ij) = (\ell_0 \ell_q) \in C$ by construction. This proves that $C \in \Sigma_n$.

It is clear that $A \cup B \subset C$. Moreover, $C = A \vee B$ in $N(\Sigma_n)$ because if $D \in N(\Sigma_n)$ is any element containing A and B then D satisfies (10.6); but C is the smallest subset of Ref containing $A \cup B$ satisfying (10.6) and therefore $C \subset D$. □

10.8 Exercise. Put $x = s_i$, $y = s_j$. Prove that $x \vee y = xyx = yxy$ if $|i - j| = 1$ and $x \vee y = xy = yx$ if $|i - j| > 1$.

10.9 Definition. Let $\sim$ denote the congruence on S^* generated by the Artin relations in the s_i.

10.10 Minimal expressions. Let $x \in \Sigma_n$. A *minimal expression* for x is an element $(x_1, \ldots, x_k) \in S^k$ such that $x_1 \cdots x_k = x$ and with k as small as possible, that is, $k = \ell(x)$.

Notice that an element $(x_1, \ldots, x_k) \in S^k$ is a minimal expression if and only if

$$x_1 \cdots x_i < x_1 \cdots x_{i+1} \qquad \text{for all } i.$$

10.11 Corollary. *Let $(x_1, \ldots, x_k)$ be a minimal expression for $x \in S_n$. Then the $\sim$-class of $(x_1, \ldots, x_k)$ depends only on x.*

Proof. Let $x = (x_1, \ldots, x_k)$, $y = (y_1, \ldots, y_k)$ be two minimal words in S for $z \in \Sigma_n$. We must prove $(x_1, \ldots, x_k) \sim (y_1, \ldots, y_k)$. We will do this by induction on k.

For $k = 0$ this is obvious. Suppose now that the result is known for smaller k. We consider two cases.

Case 1: $x_1 = y_1$. Then $(x_2, \ldots, x_k)$ and $(y_2, \ldots, y_k)$ are two minimal words for the same permutation so that by the induction hypothesis, they are $\sim$-equivalent. Then so are x and y.

Case 2: $x_1 \neq y_1$. Let u, v be minimal expressions such that $(x_1, u) = (y_1, v)$ is an Artin relation. Then

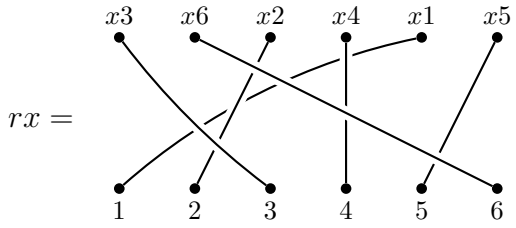
$$(x_1, u) \sim (y_1, v). \tag{10.12}$$

Choose a minimal expression w such that $z = (x_1 \vee y_1)[w] = x_1[uw] = y_1[vw]$. Then (x_1, u, w) and (y_1, v, w) are minimal expressions because Σ_n is a lattice. So

$$(x_1, \ldots, x_k) \sim (x_1, u, w) \sim (y_1, v, w) \sim (y_1, \ldots, y_k);$$

the middle equivalence is by (10.12) and the other two are by the induction hypothesis. □

Figure 10: A simple braid



10.13 Definition/Corollary. Define $t(s_i) = \sigma_i$ for all i. Let $(x_1, \ldots, x_k)$ be a minimal expression for $z \in S_n$. Then $(tx_1) \cdots (tx_k)$ depends only on z. It will be written $r(z)$.

Proof. Immediate from 10.11. □

10.14 Remark. The above result 10.13 is also obvious from the pictures. One of the reasons we proved it the way we did is because an algebraic proof is necessary in most other cases of Garside groups, including some finite type Artin groups.

10.15 Definition. We write $\Omega := r(\Sigma_n)$. The elements of Ω are called *simple braids*. See figure 10.

10.16 Exercise. Let $x \in \Sigma_n$ and let $(y_1, \ldots, y_k) \in S^k$ be a minimal expression for x. Prove that no two strings in the permutation word $(y_1, \ldots, y_k)$ cross twice.

10.17 Exercise. Let $x, y \in \Sigma_n$, $x \leq xy$. Prove $r(xy) = (rx)(ry)$.

10.18 Proposition. *The braid group B_n is presented as follows.*

Generators:	$\{g(x) \mid x \in \Sigma_n\}$.
Relations:	$(gx)(gy) = g(xy)$ *whenever* $x \leq xy$.

Proof. We define two homomorphisms

$$u\colon G \longrightarrow B_n \qquad\qquad v\colon B_n \longrightarrow G$$
$$gx \longmapsto rx \qquad\qquad \sigma_i \longmapsto gs_i.$$

First we should prove that u, v are well-defined. (Note that a homomorphism of presented groups is well-defined if and only if it takes any relation for the source group to a consequence of the relations in the target group.)

The homomorphism u is well-defined by exercise 10.17.

We now prove that v is well-defined. Write $x = s_i$, $y = s_{i+1}$. Then

$$1 < x < xy < xyx$$

as we proved in 9.26. Therefore $g(xyx) = (g(xy))(gx) = (gx)(gy)(gx)$. For the same reason we also have $g(yxy) = (gy)(gx)(gy)$ so that $(gx)(gy)(gx) =$

$(gy)(gx)(gy)$. In a similar way, prove yourself that $(gs_i)(gs_j) = (gs_j)(gs_i)$ if $|i-j| > 1$. This proves that v is well-defined.

It is clear that $uv = 1$, so that in particular v is injective. It remains to show that v is surjective. Consider a generator gx for G ($x \in \Sigma_n$). Let $(x_1, \ldots, x_k)$ be a minimal expression for x. Then

$$x_1 \cdots x_i < x_1 \cdots x_{i+1} \qquad \text{for all } i. \tag{10.19}$$

By induction on i we will show that

$$g(x_1 \cdots x_i) = (gx_1) \cdots (gx_i). \tag{10.20}$$

For $i = 0$ this is clear. If it is true for i then by (10.19)

$$g(x_1 \cdots x_{i+1}) = g(x_1 \cdots x_i)\, g(x_{i+1}) = (gx_1) \cdots (gx_{i+1}).$$

We have proved (10.20). Therefore, $g(x_1 \cdots x_i)$ is in the image of v and in particular, so is gx. □

10.21 *Exercise. Let A be a non-empty subset of Σ_n satisfying the following.

(1) For all $a, b \in \Sigma_n$, if $a < b \in A$ then $a \in A$.

(2) For all $a \in \Sigma_n$ and $x, y \in S$, if $a < ax$ and $a < ay$ and $ax, ay \in A$ then $a(x \vee y) \in A$.

Prove that A has a greatest element.

10.22 Exercise. Put $x = s_1\, s_3 \cdots s_{2n-1}$ and $y = s_2\, s_4 \cdots s_{2n}$, two elements of Σ_{2n}. Prove that $x \vee y$ is the longest element w_0 of Σ_{2n} (which is defined by $w_0(i) = 2n + 1 - i$).

11 The greedy form for positive braids

11.1 Positive braids. The *positive braid monoid* B_n^+ is the monoid presented with generators σ_i $(1 \le i < n)$ and the Artin relations (1.10), (1.11) for relations. There is clearly a homomorphism e: $B_n^+ \to B_n$, $e(\sigma_i) = \sigma_i$. It is far from clear at this stage that e is injective; we will prove that later. The elements of B_n^+ are called *positive braids*.

11.2 Theorem. *The following presentation (Ω, R) is a complete rewriting system of the positive braid monoid: $\Omega = \{rx \mid x \in \Sigma_n\}$, and R consists of $r(1) \to 1$ as well as*

$$\big(ra, r(xb)\big) \longrightarrow \big(r(ax), rb\big) \qquad \text{whenever}$$
$$a < ax \text{ and } x < xb \text{ and } \ell(x) = 1 \ (a, x, b \in \Sigma_n).$$

11.3 Remarks. (a). The theorem consists of two statements. The first is that (Ω, R) is a presentation for B_n^+. The second is that it is a complete rewriting system (that is, acyclic, well-founded and confluent).

(b). The first relation is perhaps a bit confusing. The 'dummy' generator $r(1)$ in this presentation represents the trivial element in the monoid because $r(1)$ is itself a relation.

(c). The notation can be simplified a bit by writing x instead of rx $(x \in \Sigma_n)$ and $\varnothing$ for the trivial element in Ω^*. For example, the rewrite rules in R can then be written $1 \to \varnothing$ and $(a, xb) \to (ax, b)$ $(a < ax < axb$, $\ell(x) = 1)$. This notation doesn't cause ambiguity because the generators are still separated by commas.

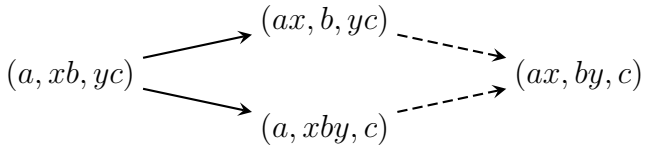
Proof. The proof that (Ω, R) is a presentation for B_n^+ is very similar to the proof of 10.18 (do yourself).

Prove yourself that R is acyclic and well-founded (it's not hard).

We will now prove that R is confluent. As we saw in 6.14, we need only consider overlapping reductions. There are three cases as follows.

$$\begin{aligned}
&\text{Case 1:} \quad (ax, b, yc) \longleftarrow (a, xb, yc) \longrightarrow (a, xby, c)\\
&\text{Case 2:} \quad (x, a) \longleftarrow (1, xa) \longrightarrow (xa)\\
&\text{Case 3:} \quad (ax, c) \longleftarrow (a, b) \longrightarrow (ay, d)
\end{aligned}$$

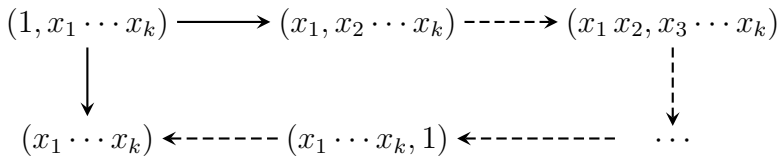
Case 1. In case 1, three consecutive generators are involved. Whenever the solid arrows in



are given one can finish the diamond with the dashed arrows. Here a, x, b, y, c are in Σ_n and $\ell(x) = \ell(y) = 1$ and $a < ax$, $xb < xby$. This settles case 1.

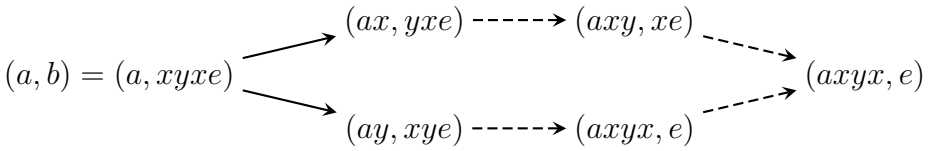
Case 2. In case 2, we consider the reductions $(1, xa) \to (x, a)$ and $(1, xa) \to (xa)$ where $x, a \in \Sigma_n$, $\ell(x) = 1$ and $x \le xa$. Write $x = x_1$

and let $(x_1, \ldots, x_k)$ be a minimal expression for xa. Then we can finish the diamond as follows.



Case 3. In case 3, we consider two rewrite rules $(a, b) \to (ax, c)$ and $(a, b) \to (ay, d)$. So $\ell(x) = \ell(y) = 1$, say, $x = s_i$, $y = s_j$. We have $x \leq b$ and $y \leq b$ and therefore $x \vee y \leq b$; write $b = (x \vee y)e$. Recall from exercise 10.8 that $x \vee y = xyx = yxy$ if $|i - j| = 1$ and $x \vee y = xy = yx$ if $|i - j| > 1$.

Let us consider the first case where $|i-j| = 1$. We claim that the following finishes the diamond.



In order to prove our claim, we need to prove $ax < axy < axyx$ and $ay < ayx < ayxy$ and $xyx < xyxe$. You will prove the first two of these in the following exercise 11.4; the last one is similar to the first two. The second case where $|i - j| > 1$ is similar. □

11.4 Exercise.

(a) Let $a \in \Sigma_n$ and $1 \leq i < n$. Prove that $a < as_i \Leftrightarrow a(i) < a(i + 1)$.

(b) Let $a \in \Sigma_n$ and write $x = s_i$ and $y = s_j$. Suppose $a < ax$ and $a < ay$. Prove the following. If $|i - j| = 1$ then $ax < axy < axyx$. If $|i - j| > 1$ then $ax < axy$.

11.5 Greedy form. It follows from 6.12 and 11.2 that every positive braid is represented by a unique R-minimal word in the generators Ω. This R-minimal word is called the *greedy form*.

11.6 Exercise. Let $n = 3$. Then the generators in our complete rewriting system for B_3^+ can be written $\Omega = \{1, \sigma_1, \sigma_2, \sigma_{12}, \sigma_{21}, \Delta\}$ where $\sigma_i = rs_i$ and $\sigma_{ij} = r(s_i s_j)$. Can you write down all rewriting rules explicitly? There are 25 of them.

11.7 Computing a greedy form. We will now see how to compute the greedy form of a positive braid in practice.

The generators are the simple braids $\Omega = \{rx \mid x \in \Sigma_n\}$, that is, they are in bijection with the permutations. In this theory, permutations $f \in \Omega$ are best written in *table form*

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}.$$

First we need to know how to multiply a permutation in table form with a fundamental reflection s_i on the left or right. As an example we multiply

$$x = \begin{pmatrix} 1 & \boxed{2} & \boxed{3} & 4 & 5 & 6 \\ \textcircled{3} & \boxed{4} & \boxed{6} & 1 & \textcircled{2} & 5 \end{pmatrix}$$

with s_2 on the left and right. We get

$$x\,s_2 = \begin{pmatrix} 1 & \boxed{2} & \boxed{3} & 4 & 5 & 6 \\ 3 & \boxed{6} & \boxed{4} & 1 & 2 & 5 \end{pmatrix}, \qquad s_2\,x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \textcircled{2} & 4 & 6 & 1 & \textcircled{3} & 5 \end{pmatrix}.$$

Recall that $(x, s_i y) \to (x s_i, y)$ is a rewriting rule if and only if $x < x s_i$ and $s_i < s_i y$. So we need to know how to read off from the table whether $x < x\,s_i$ and $s_i < x$. Well, in the above example both $x < x\,s_2$ and $s_2 < x$ are true. The general rule is found in 9.19.

Here is an example of an application of a single rewriting rule.

$$r\begin{pmatrix} 1 & 2 & \overline{3} & \overline{4} & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} r\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & \underline{4} & 5 & 1 & \underline{3} \end{pmatrix} \longrightarrow r\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix} r\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}$$

Crucial here are $|3 - 4| = 1$, the order of the underlined 3 and 4, and the order of 1 and 5.

Now we are ready for a computation of a greedy form.

$$\begin{aligned} & r\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} r\begin{pmatrix} 1 & \overline{2} & \overline{3} & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} r\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & \underline{3} & \underline{2} & 4 \end{pmatrix} \\ \longrightarrow\ & r\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} r\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} r\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\ \longrightarrow\ & r\begin{pmatrix} \overline{1} & \overline{2} & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} r\begin{pmatrix} 1 & 2 & 3 & 4 \\ \underline{2} & 3 & \underline{1} & 4 \end{pmatrix} \\ \longrightarrow\ & r\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} r\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \end{aligned}$$

The latter is an R-minimal word, that is, no more rewriting rules can be applied.

11.8 Exercise. Compute the greedy form of

$$r\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} r\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} r\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} r\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

11.9 Exercise. Prove that another complete rewriting system for B_n^+ is defined precisely as in 11.2 except that the condition $\ell(x) = 1$ is replaced by the condition $\ell(x) \geq 1$.

11.10 Exercise. Let $x_1, \ldots, x_k \in \Omega$. Prove that $(x_1, \ldots, x_k)$ is a greedy form if and only if (x_i, x_{i+1}) is a greedy form for all appropriate i.

12 The word problem in the braid group

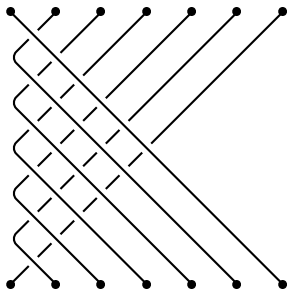
12.1 Definition. We define $w_0 \in \Sigma_n$ by

$$w_0(i) = n + 1 - i \qquad (1 \leq i \leq n).$$

We know that $(\Sigma_n, \leq)$ is a lattice so it must have a greatest element; it is precisely w_0. The usual name for w_0 is the *longest element* however — this refers to the length ℓ, as defined in (9.16).

We also define $\Delta = r(w_0)$, which is sometimes viewed as element of the braid group B_n, sometimes as element of the positive braid monoid B_n^+. Recall that we haven't proved yet that the homomorphism $e\colon B_n^+ \to B_n$ is injective! We call Δ the *half-twist* or *Garside braid*. See figure 11.

Figure 11: The Garside braid Δ



12.2 Lemma. *In B_n^+ as well as in B_n we have $\Delta\,\sigma_i = \sigma_{n-i}\,\Delta$. In particular, Δ^2 is central*[11] *in the braid group.*

Proof. For B_n this is obvious from the picture. For B_n^+ this can be proved algebraically. Do this yourself. □

12.3 Theorem. *Let (Ω, R) denote the complete rewriting system for B_n^+ from 11.2. Define $\overline{\Omega} = \Omega \cup \{\Delta^{-1}\}$, obtained by adding one abstract symbol Δ^{-1}. Let $\overline{R}$ denote the union of R with three extra kinds of rewriting rules*

$$\Delta^{-1}\Delta \longrightarrow \varnothing, \quad \Delta\Delta^{-1} \longrightarrow \varnothing, \quad a\Delta^{-1} \longrightarrow \Delta^{-2}a\Delta \quad (a \in \Omega).$$

Then $(\overline{\Omega}, \overline{R})$ is a complete rewriting system for B_n.

12.4 Remark. As in 11.2 this theorem consists of two statements. Firstly, $(\overline{\Omega}, \overline{R})$ is a presentation for the braid group; secondly, it is a complete rewriting system.

12.5 Exercise. Prove theorem 12.3.

12.6 It follows from 6.12 and 12.3 that every braid is represented by a unique $\overline{R}$-minimal word in the generators Ω. This $\overline{R}$-minimal word is called the *greedy form*.

[11] An element in a group is *central* if it commutes with all elements.

12.7 Corollary. *(a). Let $x \in B_n^+$. Then the greedy form of x is also the greedy form of $ex \in B_n$.*

(b). The homomorphism e: $B_n^+ \to B_n$ (see 11.1) is injective.

Proof. Obvious. □

12.8 Exercise. (a). Let $M = \{0, 1\}$ be equipped with the multiplication $xy = \max(x, y)$. Prove that M does not *embed* in a group (that is, there is no injective homomorphism from M to a group).

(b). Consider the monoid

$$S = \langle a, b, c, d, u, v, x, y \mid au = bv,\ cu = dv,\ cx = dy \rangle.$$

Prove that S is not embeddable in a group.

(c)*. Prove that S is *cancellative*, that is, for all $p, q, r \in S$, if $pr = qr$ or $rp = rq$ then $p = q$.

12.9 Definition. From now on we consider B_n^+ as a subset (submonoid) of B_n, which is justified by corollary 12.7. We define a relation $\leq$ on B_n by

$$x \leq xy \quad \Leftrightarrow \quad y \in B_n^+.$$

12.10 Exercise. Prove that the relation $\leq$ on B_n is an ordering. Prove that $\leq$ is left-invariant, that is, $xy \leq xz \Leftrightarrow y \leq z$ for all $x, y, z \in B_n$.

12.11 Lemma.

(1) *Let $x, y \in \Sigma_n$. Then $x \leq y \Leftrightarrow rx \leq ry$.*

(2) *Let $(y_1, \ldots, y_n)$ be the greedy form of $y \in B_n^+$ and let $x \in \Omega$. Then $x \leq y \Leftrightarrow x \leq y_1$.*

(3) *Let $x, y \in \Sigma_n$. Then $rx \vee ry$ exists in B_n and equals $r(x \vee y)$.*

Proof. (1). Proof of $\Rightarrow$. Define z by $y = xz$. Then $ry = (rx)(rz)$ by definition, so $rx \leq ry$.

Proof of $\Leftarrow$. Suppose $rx \leq ry$. Then there are $z_1, \ldots, z_k \in \Omega$ such that

$$ry = (rx)\, z_1\, z_2 \cdots z_k.$$

Imagine one applies the algorithm to turn the right hand side into the greedy form. During this algorithm, x can only grow, and finally takes the value y. This proves $x \leq y$.

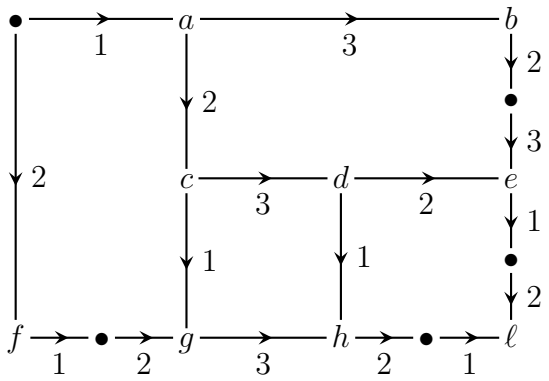
(2). The implication $\Leftarrow$ is obvious. Proof of $\Rightarrow$. Suppose $x \leq y$. Then there are $z_1, \ldots, z_k \in \Omega$ such that

$$y = x\, z_1\, z_2 \cdots z_k.$$

The remainder of the proof of (b) is similar to (a). Imagine one applies the algorithm to turn the right hand side into the greedy form. During this algorithm, x can only grow, and finally takes the value y. So $x \leq y$.

(3). By (a), $r(x \vee y)$ is an upper bound for x and y. Let $z \in B_n$ be such that $rx \leq z$ and $ry \leq z$. We need to prove that $r(x \vee y) \leq z$. We have $z \in B_n^+$. Let $(rz_1, \ldots, rz_k)$ be the greedy form for z. Then $rx \leq rz_1$ and $ry \leq rz_1$ by (b). By (a) we get $x \leq z_1$ and $y \leq z_1$. Therefore $x \vee y \leq z_1$. Therefore $r(x \vee y) \leq rz_1 \leq z$. □

Figure 12: The word reversing process



12.12 Theorem. *The ordered set $(B_n, \leq)$ is a lattice.* □

12.13 Word reversing – diagrammatic example. Instead of proving theorem 12.12 we will give an example how to compute the join of two braids in practice. A proof of theorem 12.12 can be given along the same lines but we won't do so.

Write i instead of σ_i. We will repeatedly use the fact, which is a special case of lemma 12.11(3), that the joins $\sigma_i \vee \sigma_j$ exist and are given by

$$\begin{aligned} \sigma_i \vee \sigma_j &= \sigma_i \sigma_j \sigma_i && |i-j| = 1 \\ \sigma_i \vee \sigma_j &= \sigma_i \sigma_j && |i-j| > 1 \end{aligned} \tag{12.14}$$

We write i for σ_i and aim to compute $2 \vee 13$ (and to prove that this join exists). See figure 12. By (12.14) we have

$$g = a \vee f, \quad e = c \vee b, \quad h = g \vee d, \quad \ell = h \vee e.$$

(In particular, these joins exist.) Going backwards through these identities, we find

$$\begin{aligned} \ell &= h \vee e = g \vee d \vee e = g \vee e \\ &= g \vee c \vee b = g \vee b = a \vee f \vee b = f \vee b. \end{aligned}$$

We conclude $2 \vee 13 = 132312$.

It should be clear how you find the diagram algorithmically: you start with the left and top edges and you work your way to the bottom right corner. This algorithm is called the *word reversing process* due to its symbolic form which is the next topic.

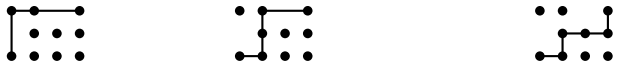
12.15 Word reversing – symbolic example. Let $S = \{\sigma_i \mid 1 \leq i < n\}$ and $S^{-1} = \{\sigma_i^{-1} \mid 1 \leq i < n\}$. Let R be the rewriting system on $(S \cup S^{-1})^*$ consisting of the following.

$$\begin{aligned} \sigma_i^{-1} \sigma_j &\longrightarrow \sigma_j \sigma_i \sigma_j^{-1} \sigma_i^{-1} && |i-j| = 1 \\ \sigma_i^{-1} \sigma_j &\longrightarrow \sigma_j \sigma_i^{-1} && |i-j| > 1 \\ \sigma_i^{-1} \sigma_i &\longrightarrow \varnothing \end{aligned}$$

It can be shown that R is a complete rewriting system, but the monoid it describes is far from being the braid group or so! The *word reversing process* is the algorithm to apply the rewriting rules from R repeatedly until one arrives at an R-minimal word. A word in $S \cup S^{-1}$ is R-minimal if and only if it does not contain a subword of the form $\sigma_i^{-1}\sigma_j$.

Here is the algebraic version of the example in figure 12 (the little pictures are there to help you make the connection with the diagrammatic version):

$$\underline{2^{-1}1}3 \longrightarrow 121^{-1}\underline{2^{-1}3} \longrightarrow 12\underline{1^{-1}3}23^{-1}2^{-1}$$



$$\longrightarrow 123\underline{1^{-1}2}3^{-1}2^{-1} \longrightarrow 12321^{-1}2^{-1}3^{-1}2^{-1}$$

In practice the symbolic approach to word reversing is usually faster than the diagrammatic approach.

12.16 Exercise. We write i for σ_i. Apply the word reversing process to $2^{-1}3^{-1}3^{-1}4^{-1}1223$. Use your result to give an expression for $4332 \vee 1223$.

13 Complements

13.1 Why Garside groups? This section and the next two, which are without proofs, are about a recent invention called Garside groups. We have two reasons for being interested in them:

(1) Garside groups generalise braid groups.

(2) The theory of Garside groups streamlines the proofs. In the case of the braid group, we had to work very hard on the symmetric group to get the greedy form right. Once you have the general theory of Garside groups, the proofs are often reduced to a small set of computations.

13.2 Words. We fix a finite set A called alphabet, whose elements are called letters. The empty word is written 1 or $\varnothing$. We fix a disjoint copy A^{-1} of A and an involution $x \mapsto x^{-1}$ of $A \cup A^{-1}$ such that $x \in A \Leftrightarrow x^{-1} \in A^{-1}$. Elements in the free monoid A^* on A are called *positive words* and elements of $(A \cup A^{-1})^*$ are called *words*. The *inverse* w^{-1} of a word $w \in (A \cup A^{-1})^*$ is obtained by inverting each letter of w and reversing the order in which they appear.

Warning: $(A \cup A^{-1})^*$ is not a group, and $ww^{-1} \neq 1$ for most words w.

We will use x, y, z to denote letters and u, v, w to denote words.

13.3 Complements. Let A be an alphabet. A *complement* on A is a partial mapping[12]

$$f\colon A \times A \longrightarrow A^*$$

such that $f(x, x) = 1$ for all $x \in A$, and such that $f(x, y)$ is defined whenever $f(y, x)$ is.

Every complement (A, f) gives rise to a monoid presentation called a *complemented presentation*

$$(A, R) = \big(A \;\big|\; xf(x,y) = yf(y,x) \text{ whenever } f(x,y) \text{ is defined}\big) \qquad (13.4)$$

and conversely, the complement is determined by this presentation.

Let M denote the monoid presented by (13.4) and G the group presented by it. By $x \mapsto [x]$ we will denote the two natural maps $A^* \to M$ and $(A \cup A^{-1})^* \to G$. Let $\equiv^+$ be the congruence on A^* generated by the set R of the relations in (13.4) and let $\equiv$ be the congruence on $(A \cup A^{-1})^*$ generated by

$$R \cup \big\{aa^{-1} = 1,\ a^{-1}a = 1 \;\big|\; a \in A\big\}.$$

So $M = A^*/\equiv^+$ and $G = (A \cup A^{-1})^*/\equiv$.

13.5 Example. The positive braid monoid B_n^+ is the monoid associated with the complement (A, f) where $A = \{\sigma_1, \ \ldots, \ \sigma_{n-1}\}$ and

$$f(\sigma_i, \sigma_j) = \begin{cases} \sigma_j\,\sigma_i & |i-j| = 1 \\ \sigma_j & |i-j| > 1. \end{cases}$$

The braid group B_n is the associated group.

[12] A partial mapping $X \to Y$ is a pair (Z, f) of a subset $Z \subset X$ and a mapping $f\colon Z \to Y$. We say that $f(x)$ is *not defined* if $x \in X - Z$.

13.6 Word reversing. Let (A, f) be a complement. By $\curvearrowright = \curvearrowright_f$ we will denote the reflexive-transitive closure of

$$X = \left\{ ua^{-1}bv \to uf(a,b)f(b,a)^{-1}v \;\middle|\; \begin{array}{l} a, b \in A,\ f(a,b) \text{ defined}, \\ u, v \in (A \cup A^{-1})^* \end{array} \right\},$$

that is, we write $u \curvearrowright v$ if and only if there exist $u = u_0,\ u_1,\ \ldots,\ u_k = v$ such that $(u_i, u_{i+1}) \in X$ for all i. The process of finding a chain $u_1 \curvearrowright u_2 \curvearrowright \cdots$ when u_1 is given is called *word reversing*. As we're not doing proofs we won't need X, only $\curvearrowright$. A word $v \in (A \cup A^{-1})^*$ is said to be $\curvearrowright$*-minimal* if $v \curvearrowright w$ implies $v = w$, in other words, nontrivial word reversing cannot be applied to v. We say that (A, f) is *convergent* if for any $u \in (A \cup A^{-1})^*$ there exists $\curvearrowright$-minimal v with $u \curvearrowright v$.

Warning: $xx^{-1} \curvearrowright 1$ is not true for $x \in A$!

If word reversing is acyclic (it isn't always) then it is an example of a rewriting system. As we have seen in examples 12.13 and 12.15, the aim of word reversing is roughly to find the join of two elements, which is very different from the aim of the rewriting systems we have seen before, namely, to solve the word problem in a monoid.

13.7 Proposition. *Suppose $u \curvearrowright v$ and $u \curvearrowright w$ with v, w $\curvearrowright$-minimal. Then $v = w$. Moreover, these assumptions imply that there is no infinite chain*

$$u = u_0 \curvearrowright u_1 \curvearrowright \cdots$$

except where $u_i = u_{i+1}$ for big i. (In particular, (A, f) is convergent if and only if $\curvearrowright$ is a well-founded complete rewriting system.)

13.8 Partial identity convention. According to the *partial identity convention* (pic) an identity $A = B$ or $A \equiv^+ B$ or $A \equiv^{++} B$ means that either both sides are defined and the identity is true, or neither is defined. We will follow this convention even if we don't always mention it.

13.9 The operation \. For $u \in (A \cup A^{-1})^*$, we define u^+ to be the unique word $v \in A^*$ such that $u \curvearrowright vw^{-1}$ for some $w \in A^*$, if such words v, w exist; otherwise u^+ is not defined. For $u, v \in A^*$ we put $u\backslash v := (u^{-1}v)^+$ ("u under v").

Notice that $f(x, y) = x\backslash y$ (under the partial identity convention). So $\backslash$ generalises f.

13.10 Example. This example is just about the notation we've just introduced. Consider the complemented presentation

$$(a, b, c \mid abb = bbc,\ bcc = cca,\ caa = aab).$$

Examples of f are

$$f(a, b) = bb, \qquad f(b, a) = bc$$

and examples of single rewriting rules are

$$a^{-1}b \longrightarrow bbc^{-1}b^{-1}, \qquad b^{-1}a \longrightarrow bcb^{-1}b^{-1}.$$

(To be continued in 14.8.)

13.11 Example. Consider the presentation

$$(x, y \mid x^2 y = y)$$

associated with an appropriate complement. Then

$$y^{-1}xy \curvearrowright y^{-1}x^{-1}y \curvearrowright y^{-1}xy.$$

The first and last words are equal, so $\curvearrowright$ is not acyclic, and certainly not convergent.

13.12 Example. Here is an example where f is acyclic but not convergent. Consider the presentation

$$(1, 2, 3 \mid 121 = 212,\ 131 = 313,\ 232 = 323)$$

which is associated to an appropriate complement (A, f). (In fact this presents what is called the infinite type *Artin group* of type $\tilde{A}_2$.) Notice the S_3-symmetry. Then

$$\underline{1^{-1}2}3 \curvearrowright 21\underline{2^{-1}1^{-1}}3 \curvearrowright 21\underline{2^{-1}31}3^{-1}1^{-1}.$$

The latter word contains $2^{-1}31$ which equals the initial word $1^{-1}23$ up to an automorphism of (A, f). It follows that $\curvearrowright$ is not convergent (apply the same line to the subword $2^{-1}31$ and keep going). It can be shown however that $\curvearrowright$ is acyclic.

13.13 Exercise. Consider the complement f on $A = \{a, b\}$ associated with the presentation $(a, b \mid abb = bba)$. Prove that $(a^{-1}ba)^+$ is not defined.

14 Norms and coherence

14.1 We fix $A, f, M, G, \curvearrowright, \backslash$ as before.

14.2 Norms. A *norm* for f is a map $\lambda\colon A^* \to \mathbb{Z}_{\geq 0}$ (pronounciation: λ = lambda) such that

$$\lambda(xv) > \lambda(v)$$
$$\lambda(vx) \geq \lambda(v)$$
$$x \equiv^+ y \Rightarrow \lambda(x) = \lambda(y)$$

for all $x \in A$, $u, v \in A^*$. We say that f is normed if a norm for f exists.

One can show that if f is normed then the relation $\leq$ on M defined by $x \geq y \Leftrightarrow x = yz$ for some z is an ordering.

Here is a practical method of proving that a norm exists. If there is a monoid homomorphism $\lambda\colon M \to \mathbb{Z}_{\geq 0}$ with $\lambda(x) > 0$ for all $x \in A$ then this λ is a norm.

14.3 Definition. For $u, v \in A^*$ we write $u \equiv^{++} v$ if and only if $u^{-1}v \curvearrowright 1$.

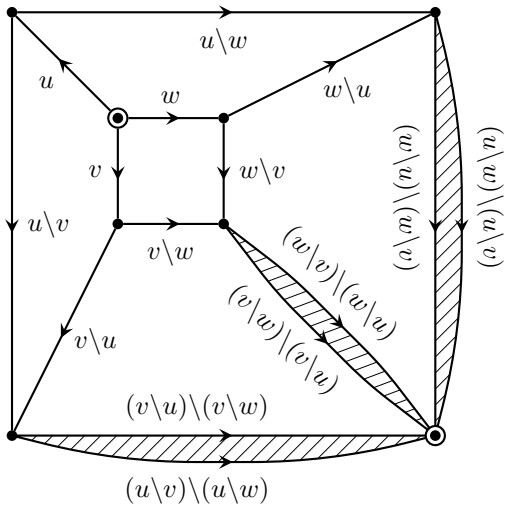
14.4 Coherence. We say f is *coherent* on $B \subset A^*$ if

$$(u\backslash v)\backslash(u\backslash w) \equiv^{++} (v\backslash u)\backslash(v\backslash w) \qquad \text{(pic)} \qquad (14.5)$$

for all $u, v, w \in B$. We say f is *coherent* if it is coherent on A^* and *locally coherent* if it is coherent on A.

In figure 13 you can find the diagrammatic interpretation of (14.5).

Figure 13: Coherence



Here is the main theorem on norms and coherence.

14.6 Theorem/Definition. Suppose f is normed and locally coherent. Then the following hold.

(1) The complement f is coherent.

(2) For all $u, v \in A^*$, we have $u \equiv^+ v \Leftrightarrow u \equiv^{++} v$.

(3) If $u \equiv^+ u_1$ and $v \equiv^+ v_1$ then $u\backslash v = u_1\backslash v_1$. Therefore, we may define $[u]\backslash[v] := [u\backslash v]$ where $x \mapsto [x]$ denotes the natural map $A^* \to M$.

(4) The monoid M is left cancellative ($rp = rq \Rightarrow p = q$). Any two elements of M have a meet. If two elements of M have a common upper bound then they have a least such (that is, a join). For $p, q \in M$ we have $p \vee y = p(p\backslash q)$.

14.7 Due to 14.6(3) we can ignore A^* most of the time and work in M instead, as we shall do from now on.

14.8 Example. (Continuation from 13.10.) Consider the complement f on $A = \{a, b, c\}$ associated with the presentation

$$(a, b, c \mid abb = bbc,\ bcc = cca,\ caa = aab).$$

(a) Prove that f is normed.

(b) Prove that f is coherent.

(c) Prove that the join $a \vee b \vee c$ exists and compute it. (As explained in 14.7 we work entirely in M here.)

(d) Prove that the join $ac \vee cb$ exists and compute it.

Solution. (a). A norm is given by the monoid homomorphism $\lambda\colon M \to \mathbb{Z}_{\geq 0}$, $\lambda(a) = \lambda(b) = \lambda(c) = 1$.

(b). We have

$$(a\backslash b)\backslash(a\backslash c) = bb\backslash ab = (b^{-1}\underline{b^{-1}a}b)^+ = (\underline{b^{-1}b}cb^{-1}\underline{b^{-1}b})^+ = (cb^{-1})^+ = c,$$
$$(b\backslash a)\backslash(b\backslash c) = bc\backslash cc = (c^{-1}\underline{b^{-1}c}c)^+ = (\underline{c^{-1}c}ca^{-1}\underline{c^{-1}c})^+ = (ca^{-1})^+ = c,$$

which proves

$$(a\backslash b)\backslash(a\backslash c) = (b\backslash a)\backslash(b\backslash c).$$

Since the presentation is symmetric under the permutation (abc) we have proved local coherence. Since f is normed, theorem 14.6(1) tells us that f is coherent.

(c). Following the partial identity convention we have by 14.6(4)

$$\begin{aligned} a \vee b \vee c = a \vee (b \vee c) = a \vee b\,c\,c = a\,(\underline{a^{-1}\,b}\,c\,c)^+ = a\,(b\,b\,c^{-1}\,\underline{b^{-1}\,c}\,c)^+ \\ = a\,(b\,b\,\underline{c^{-1}\,c}\,c\,a^{-1}\,\underline{c^{-1}\,c})^+ = a\,(b\,b\,c\,a^{-1})^+ = a\,b\,b\,c. \end{aligned}$$

We have proved much more than $x \leq abbc$ for all $x \in \{a, b, c\}$, namely that (1) the expression $a \vee b \vee c$ exists, and (2) it equals $abbc$.

(d). We have

$$\begin{aligned} ac\backslash cb &= (c^{-1}\,\underline{a^{-1}\,c}\,b)^+ = (\underline{c^{-1}\,a}\,b\,a^{-1}\,\underline{a^{-1}\,b})^+ \\ &= (a\,a\,b^{-1}\,\underline{a^{-1}\,b}\,\underline{a^{-1}\,b}\,b\,\underline{c^{-1}\,b^{-1}})^+ \\ &= (a\,a\,\underline{b^{-1}\,b}\,b\,\underline{c^{-1}\,b^{-1}\,b\,b}\,\underline{c^{-1}\,b^{-1}\,b})^+ = (a\,a\,b\,c\,a\,\underline{c^{-1}\,c^{-1}})^+ = aabca \end{aligned}$$

so $ac \vee cb = ac(ac\backslash cb) = acaabca$.

To be continued in 15.4.

15 Garside elements

15.1 Definition. Let f be a normed and coherent complement on a set A which is defined everywhere. A *Garside element* is an element $\Delta \in M$ such that the following hold.

(a) We have $x \leq \Delta$ for all $x \in A$ where we identify A with its image in M.

(b) There exists an automorphism[13] ϕ of (A, f) such that (in M) $x\Delta = \Delta\phi(x)$ for all $x \in A$.

Given a Garside element Δ, we say that the elements of

$$\Omega := \{x \in M \mid 1 \leq x \leq \Delta\}$$

are the Δ-*simple elements*. Note $A \subset \Omega$. The automorphism ϕ of (A, f) induces an automorphism of $(A, f, M, G, \leq)$ which is still written ϕ.

If $\vee A$ (the join of all generators) does not exist, then a Garside element does not exist. If $\vee A$ exists it is a good first candidate for being a Garside element.

15.2 Dehornoy graphs. See figure 14. Suppose (A, f) is normed and coherent and f is defined everywhere. A *generalised Dehornoy graph* is a graph Γ (often a subgraph of the Cayley graph of (G, A)) with the following properties.

(a) The vertex set V is a subset of M containing A. If $u \in M$, $v \in V$ and $u \leq v$ then $u \in V$. Let $u, v \in V$. If $u \vee v$ exists then it is also in V.

(b) The edge set of Γ is precisely $\{(u, ux) \mid x \in A,\ u, ux \in V\}$.

It can be shown that there is a smallest generalised Dehornoy graph; we call it simply the Dehornoy graph. The Dehornoy graph is finite if and only if $\vee A$ (the join of all generators) exists; if it does then the vertex set of the Dehornoy graph is $[1, \vee A]$.

Let $\Delta \in M$ be such that $x \leq \Delta$ for all $x \in A$. Then $[1, \Delta] := \{u \in M \mid u \leq \Delta\}$ is the vertex set of a generalised Dehornoy graph. Such generalised Dehornoy graphs may be called *principal*. In particular, this condition is fulfilled by a Garside element.

Drawing Dehornoy graphs in practice is similar to drawing Cayley graphs.

15.3 Theorem/Definition. Let f be a normed and coherent complement on A. Let Δ be a Garside element and let Ω, ϕ be as in the defition of Garside elements. Then the following hold.

(1) Word reversing is convergent. The expressions u^+ and $u\backslash v$ and $u \vee v$ are defined for all $u, v \in A^*$.

(2) We have a complete rewriting system (Ω, R) for M where

$$R = \Big\{(1) \to \varnothing\Big\} \cup \Big\{(a, xb) \to (ax, b) \;\Big|\; x \in A,\ a, b, xb, ax \in \Omega\Big\}.$$

[13] Pronounciation: ϕ = phi. Handwritten it looks like φ.

(3) We have a complete rewriting system $(\overline{\Omega}, \overline{R})$ for G where

$$\overline{\Omega} = \Omega \cup \{\Delta^{-1}\}$$
$$\overline{R} = R \cup \left\{ \begin{array}{l} \Delta\Delta^{-1} \to \varnothing,\ \Delta^{-1}\Delta \to \varnothing, \\ a\Delta^{-1} \to \Delta^{-1}\phi(a) \end{array} \middle|\ a \in \Omega \right\}.$$

(4) The $\overline{R}$-minimal form (respectively, R-minimal form) of an element of G (respectively, M) is called the *greedy form*. The greedy form of an element $u \in M$ is also the greedy form of $e(u)$ where $e\colon M \to G$ is the natural map. In particular, e is injective. We will henceforth consider M to be a subset (submonoid) of G.

(5) Define an ordering on G by $x \leq xy \Leftrightarrow y \in M$. Then the ordered set $(G, \leq)$ is a lattice.

15.4 Example. (Continuation from 14.8.) We have shown that

$$(a, b, c \mid abb = bbc,\ bcc = cca,\ caa = aab)$$

is normed and coherent, and that $a \vee b \vee c$ exists and equals $abbc$. The fact that it exists implies that the Dehornoy graph is finite. It is drawn in figure 14(a). From the Dehornoy graph one easily reads off more expressions for Δ such as $\Delta = aabb$.

We will now prove that Δ is a Garside element. We have

$$a\Delta = a(abbc) = (aabb)c = \Delta c.$$

By the (abc) symmetry we have $b\Delta = \Delta a$ and $c\Delta = \Delta b$. So Δ is a Garside element and $\phi = (cba)$.

Using the Dehornoy graph or otherwise one can compute a greedy form with respect to Δ. For example the greedy form for $abbacaaca$ is the last entry in

$$\begin{aligned} abbacaaca &= (abb)(a)(\underline{caa})(ca) \\ &= (abb)(\underline{a})(\underline{aab})(ca) = (abb)(aa)(ab)(ca). \end{aligned}$$

15.5 Example.

(a) Prove that the complement associated with the presentation

$$(a, b, c \mid abb = bbc,\ cbb = bba,\ aa = cc)$$

is normed and coherent.

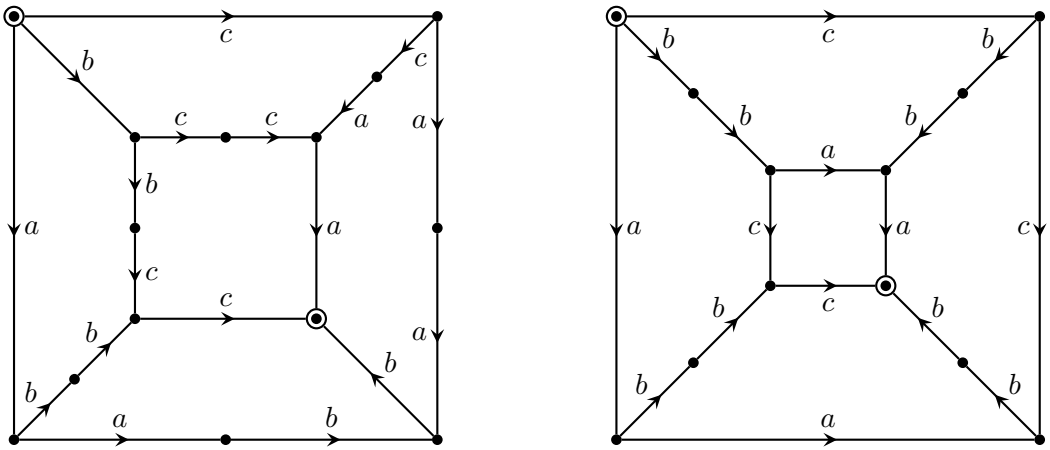
(b) Show that $\Delta := a \vee b \vee c$ exists and compute it.

(c) Draw the Dehornoy graph.

(d) Prove that Δ is not a Garside element.

(e) Prove that a Garside element does not exist.

Figure 14: Two Dehornoy graphs



Solution. **(a).** We have

$$(a\backslash c)\backslash(a\backslash b) = a\backslash bb = (\underline{a^{-1}\,b}\,b)^+ = (b\,b\,c^{-1}\,\underline{b^{-1}\,b})^+ = (b\,b\,c^{-1})^+ = bb$$

so that $(a\backslash c)\backslash(a\backslash b) = (c\backslash a)\backslash(c\backslash b)$ by the (ac)-symmetry. We also have

$$\begin{aligned}(a\backslash b)\backslash(a\backslash c) &= bb\backslash a = (b^{-1}\,\underline{b^{-1}\,a})^+\\ &= (\underline{b^{-1}\,b}\,c\,b^{-1}\,b^{-1})^+ = (c\,b^{-1}\,b^{-1})^+ = c\\ (b\backslash a)\backslash(b\backslash c) &= bc\backslash ba\\ &= (c^{-1}\,\underline{b^{-1}\,b}\,a)^+ = (\underline{c^{-1}\,a})^+ = (c\,a^{-1})^+ = c\end{aligned}$$

which proves

$$(a\backslash b)\backslash(a\backslash c) = (b\backslash a)\backslash(b\backslash c). \tag{15.6}$$

The last identity needed follows from (15.6) by another use of the (ac)-symmetry.

(b). Under the partial identity convention we have

$$\begin{aligned}a\vee b\vee c = b\vee(a\vee c) = b\vee aa &= b\,(b\backslash aa)\\ &= b\,(\underline{b^{-1}\,a}\,a)^+ = b\,(b\,c\,b^{-1}\,\underline{b^{-1}\,a})^+\\ &= bbc\,(\underline{b^{-1}\,b}\,c\,b^{-1}\,b^{-1})^+ = bbc\,(c\,b^{-1}\,b^{-1})^+ = bbcc.\end{aligned}$$

(c). See figure 14(b).

(d). Suppose that Δ is a Garside element. We will use theorem 15.3(4) which states that M embeds into a group, and in particular, is cancellative.

By the definition of Garside elements, there exists an automorphism ϕ of (A, f) such that we have $x\Delta = \Delta\phi(x)$ for all $x \in A$. Every automorphism of (A, f) fixes b, so we must have $b\Delta = \Delta b$. By (b) we have $b(bbcc) = b\Delta = \Delta b = (bbcc)b$. By cancellation in M we find $bcc = ccb$. This however cannot be true in M because the only words $\equiv^+ bcc$ are bcc itself and baa. This contradiction proves that Δ is not a Garside element.

(e). We have

$$\underline{a^{-1}\,b}\,a \;\curvearrowright\; b\,b\,c^{-1}\,\underline{b^{-1}\,a} \;\curvearrowright\; b\,b\,(c^{-1}\,b\,c)\,b^{-1}\,b^{-1}.$$

The latter word contains $c^{-1}bc$ which is the initial word $a^{-1}ba$ up to an automorphism of (A, f). So word reversing is not convergent. By theorem 15.3(1), a Garside element does not exist.

15.7 Exercise. Consider the complemented presentation

$$(a, b, c \mid bab = aaa,\ bac = cba,\ abc = cab).$$

(a) Prove that the associated complement f on $A = \{a, b, c\}$ is normed and coherent.
(b) Prove that $\Delta := a \vee b \vee c$ exists and give a representative in A^* for it.
(c) Draw the Dehornoy graph.
(d) Prove that Δ is not a Garside element (without using the following parts of the exercise).
(e) Prove that f is not convergent, by showing that the word reversing process applied to $c^{-1}b^{-1}ac$ does not terminate.
(f) Prove that a Garside element does not exist.

15.8 Exercise. Consider the complemented presentation

$$(a, b, c \mid acab = bcaa,\ bcaac = cabca,\ cabca = acabc).$$

You may assume that the associated complement f on $A = \{a, b, c\}$ is normed and coherent.

(a) Draw the Dehornoy graph. Hint: Your graph should be closed under "replacing a word $xf(x, y)$ by $yf(y, x)$". This fact was not necessarily used in the examples of the lectures, but it is needed here.
(b) Use the Dehornoy graph to prove that $D := a \vee b \vee c$ exists and to compute it.
(c) Prove that D is not a Garside element.
(d) Prove that $\Delta := Da$ is a Garside element.
(e) Draw the generalised Dehornoy graph with vertex set $[1, \Delta] = \{u \in M \mid 1 \leq u \leq \Delta\}$.
(f) Compute the greedy form (with respect to Δ) for $cbabcaac$.

15.9 *Exercise. Find a Garside group with 3 generators whose Dehornoy graph is not planar.

15.10 *Exercise. It's easy to prove that the complemented presentation

$$(a, b, c \mid ab = ccc,\ bc = aaa,\ ca = bbb)$$

is coherent and has a Garside element. A bar of chocolate for the first person to prove that it's normed!

16 The BKL Garside structure

16.1 The Garside structure on the braid group which we learned in section 12 is not the only one. Let's call it the *classical* Garside structure so that we can distinguish it from another Garside structure on the braid group, discovered in 1998 by Birman-Ko-Lee (BKL), and which is the topic of this section.

16.2 We identify $\mathbb{Z}_n = \mathbb{Z}/n$ with $I_n = \{1, \ldots, n\}$ in the obvious way. For each $a \in \mathbb{Z}/n$ we define a total ordering $<_a$ on $\mathbb{Z}/n$ by

$$a <_a a+1 <_a a+2 <_a \cdots <_a a-1.$$

16.3 Proposition. *The braid group B_n is presented by the generators $a_{ij} = a_{ji}$ $(1 \le i < j \le n)$ and relations*

$$a_{ij}\, a_{k\ell} = a_{k\ell}\, a_{ij} \qquad (i <_i j <_i k <_i \ell) \tag{16.4}$$

$$a_{ij}\, a_{jk} = a_{jk}\, a_{ij} \qquad (i <_i j <_i k). \tag{16.5}$$

Proof. Let G denote the group thus presented. We *define* the braid group B_n by the Artin presentation. So we want to prove $G \cong B_n$.

Let P denote the free group on $\{\sigma_1, \ldots, \sigma_{n-1}\}$ and Q the free group on $\{a_{ij} \mid 1 \le i < j \le n\}$. Let $\approx$ denote the appropriate congruences on P and Q. Define homomorphisms

$$\begin{aligned} u\colon P &\longrightarrow Q & \qquad v\colon Q &\longrightarrow P \\ \sigma_i &\longmapsto a_{i,i+1} & a_{ij} &\longmapsto (\sigma_i \cdots \sigma_{j-1})(\sigma_{j-2}^{-1} \cdots \sigma_i^{-1}). \end{aligned}$$

See figure 15(a) for a picture of $v(a_{ij})$.

Claim 1: For all $x, y \in P$, if $x \approx y$ then $ux \approx uy$.

First consider the case $x = \sigma_i\sigma_j$, $y = \sigma_j\sigma_i$ with $|i-j| > 1$. We have

$$ux = u(\sigma_i\sigma_j) = a_{i,i+1}\, a_{j,j+1} \approx a_{j,j+1}\, a_{i,i+1} = u(\sigma_j\sigma_i) = uy.$$

Next consider the hexagon relation. We put

$$a := a_{i,i+1}, \quad b := a_{i+1,i+2}, \quad c := a_{i+2,i}.$$

From (16.5) applied to $(i, i+1, i+2)$ instead of (i, j, k) we have

$$ab \approx bc. \tag{16.6}$$

Applied to $(i+2, i, i+1)$ instead of (i, j, k) however we also find

$$ca \approx ab. \tag{16.7}$$

Using (16.6) we can express c in terms of a, b by $c \approx b^{-1}ab$. Plugging this into (16.7) gives $b^{-1}aba \approx ab$, that is, $aba \approx bab$. Therefore

$$u(\sigma_i\sigma_j\sigma_i(\sigma_j\sigma_i\sigma_j)^{-1}) = aba(bab)^{-1} \approx 1$$

which finishes the proof of claim 1.

Claim 2: For all $x, y \in G$, if $x \approx y$ then $vx \approx vy$.

There are two cases of the relation (16.4). The first is where $i < j < k < \ell$. In that case, the elements

$$va_{ij} = (\sigma_i \cdots \sigma_{j-1})(\sigma_{j-2}^{-1} \cdots \sigma_i^{-1}) \tag{16.8}$$

$$va_{k\ell} = (\sigma_k \cdots \sigma_{\ell-1})(\sigma_{\ell-2}^{-1} \cdots \sigma_k^{-1}) \tag{16.9}$$

commute up to $\approx$ because any generator on the right in (16.8) commutes with any generator on the right in (16.9).

The second case is where $j < k < \ell < i$. In that case an algebraic proof that $v(a_{ij}a_{k\ell}) \approx v(a_{k\ell}a_{ij})$ is tedious though easy; instead we refer to the picture of a_{ij} in figure 15(a) from which it is immediately clear that va_{ij} and $va_{k\ell}$ commute up to $\approx$.

Finally we consider the relation (16.5). A completely algebraic proof is somewhat cumbersome. Instead we use the picture of a_{ij} as follows. It is clear that the perfectly vertical strings in the background have no influence, and we may as well remove them. In other words, we need only prove $v(a_{ij}a_{jk}) \approx v(a_{jk}a_{ki}) \approx v(a_{ki}a_{ij})$ for $(i, j, k) = (i, i+1, i+2)$. Well, we have

$$\begin{aligned} v(a_{ij}\, a_{jk}) &= \sigma_i\, \sigma_{i+1} \\ v(a_{jk}\, a_{ki}) &= \sigma_{i+1}\, (\sigma_i\, \sigma_{i+1}\, \sigma_i^{-1}) \approx \sigma_i\, \sigma_{i+1}\, \sigma_i\, \sigma_i^{-1} = \sigma_i\, \sigma_{i+1} \\ v(a_{ki}\, a_{ij}) &= (\sigma_i\, \sigma_{i+1}\, \sigma_i^{-1})\, \sigma_i = \sigma_i\, \sigma_{i+1}. \end{aligned}$$

This finishes the proof of claim 2.

By claims 1 and 2, we have two homomorphisms $U\colon B_n \to G$ and $V\colon G \to B_n$ induced by u and v. We have $VU(\sigma_i) = V(a_{i,i+1}) = \sigma_i$, that is, $VU = 1_{B_n}$, and in particular, U is injective. It remains to prove that U is surjective. By induction on $|i-k|$ we will show that a_{ik} is in the image of U. For $k = i+1$ this is clear. Suppose $k > i+1$ and choose any j with $i < j < k$. Then

$$a_{ik} \approx a_{ij}\, a_{jk}\, a_{ij}^{-1}$$

by (16.5). But a_{ij} and a_{jk} are in the image of U by the induction hypothesis and therefore so is a_{ik}. □

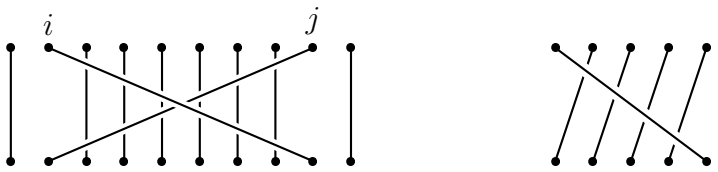
16.10 Exercise. Give a purely algebraic proof of $v(a_{ij}a_{k\ell}) \approx v(a_{k\ell}a_{ij})$ if $j < k < \ell < i$ (see the proof of 16.3 for the notation).

16.11 Let $1 \le i < j < k < \ell \le n$. There is no relation among (16.4) and (16.5) in which one side starts with a_{ik} and the other with $a_{j\ell}$. But we can make such a relation as a consequence of (16.4) and (16.5). We have

$$a_{ik}\, a_{ij}\, a_{k\ell} = a_{j\ell}\, a_{jk}\, a_{i\ell} \tag{16.12}$$

because $a_{ik}\, a_{ij}\, a_{k\ell} = a_{jk}\, a_{ik}\, a_{k\ell} = a_{jk}\, a_{k\ell}\, a_{i\ell} = a_{j\ell}\, a_{jk}\, a_{i\ell}$.

Figure 15:



(a): a_{ij} (b): δ

16.13 Exercise. Suppose $j < k < \ell < i$. We made a relation (16.12) as a consequence of the relations (16.4) and (16.5) and whose left hand side starts with a_{ik} and its right hand side with $a_{j\ell}$. Find a similar relation whose left hand side *ends* with a_{ik} and its right hand side with $a_{j\ell}$.

16.14 Theorem/Definition. *Let f be the complement on*

$$A = \{a_{ij} \mid 1 \leq i < j \leq n\}$$

associated to the presentation with relations (16.4), (16.5) and (16.12). Then f is normed, coherent, and admits a Garside element

$$\delta := \sigma_1 \cdots \sigma_{n-1}. \tag{16.15}$$

This Garside structure on the braid group is called the BKL Garside structure (Birman/Ko/Lee, 1998). □

16.16 Exercise. Prove theorem 16.14 for $n = 3$.

16.17 Exercise. Prove the coherence identity (14.5)

$$(u\backslash v)\backslash(u\backslash w) \equiv^{++} (v\backslash u)\backslash(v\backslash w)$$

for $n = 6$ and $(u, v, w) = (a_{14}, a_{25}, a_{36})$.

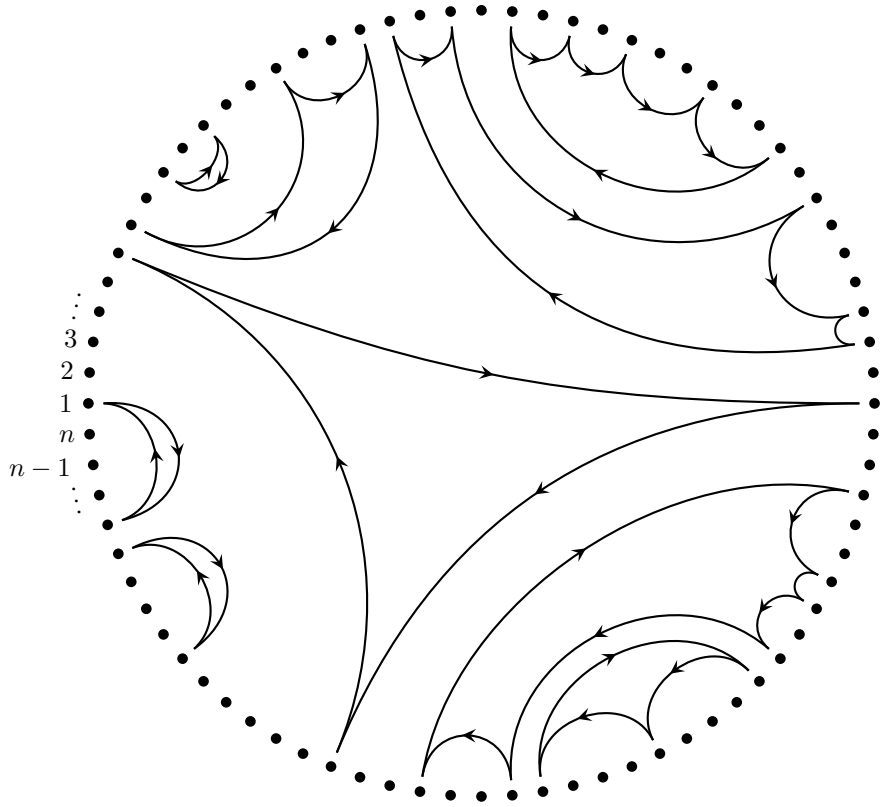
16.18 Exercise. Define the following BKL elements in B_4: $a = a_{12}$, $b = a_{23}$, $c = a_{34}$, $d = a_{13}$. Put $A = \{a, b, c, d\}$, let B_4^+ be the submonoid of B_4 generated by A and let $\leq$ be the ordering on B_4^+ defined by $x \leq z \Leftrightarrow \exists y \in B_4^+ : xy = z$. Prove that $(B_4^+, \leq)$ is not a lattice. Deduce that B_4^+ is not a Garside monoid, not even if one replaces A with another set of generators.

16.19 Let ℓ_R denote the length in Σ_n with respect to all reflections. Let $\leq_R$ denote the ordering on Σ_n defined by

$$x \leq_R xy \quad \Leftrightarrow \quad \ell_R(xy) = \ell_R(x) + \ell_R(y).$$

Define the *Coxeter element* $c = (12 \cdots n) \in \Sigma_n$, that is, $c(i) = i + 1$ for all $i \in \mathbb{Z}/n$ (remember that we identified $I_n = \mathbb{Z}_n$). Put $P = \{x \in \Sigma_n \mid x \leq_R c\}$. See figure 16 for a picture of a general element of P.

Figure 16: A general element of P



16.20 Theorem.

(1) *The braid group B_n is presented by generators $\{gx \mid x \in P\}$ and relations $g(xy) = (gx)(gy)$ whenever $x \leq_R xy$. We have $g(ij) = a_{ij}$.*

(2) *We have $[1, \delta] := \{x \in B_n \mid 1 \leq x \leq \delta\} = g(P)$.*

(3) *Let $x \in \Sigma_n$. Then $x \in P$ if and only if the following hold.*

  (a) *Let $i \in \mathbb{Z}/n$ and let k be the cardinality of its x-orbit $\langle x \rangle i$. Then*
  $$i <_i x(i) <_i x^2(i) <_i \cdots <_i x^{k-1}(i).$$

  (b) *Suppose $i < j < k < \ell$ and suppose that $\{i, k\}$ is in an x-orbit and $\{j, \ell\}$ too. Then $\{i, j, k, \ell\}$ is in an x-orbit.*

(4) *Let $x, y \in P$. Then $x \leq_R y$ is equivalent to the following. For all $i, j \in \mathbb{Z}/n$, if i, j are in the same x-orbit then they are in the same y-orbit.* □

17 Counting braids

17.1 There is a homomorphism $\ell\colon B_n \to \mathbb{Z}$ such that $\ell(\sigma_i) = 1$ for all i. One of the things we learn in this section is that the formal power series

$$\sum_{x \in B_n^+} t^{\ell(x)} \in \mathbb{Z}[[t]]$$

is a rational function.

Möbius functions

17.2 Formal power series. You will know the formal power series in one variable t which are the formal infinite sums

$$\sum_{n \geq 0} a_n \, t^n, \qquad a_n \in \mathbb{C}.$$

One can add and multiply formal power series: they form a commutative ring, which is written $\mathbb{C}[[t]]$.

A formal power series in one variable is a sum over the infinite monoid $\{t^n \mid n \geq 0\} \cong \mathbb{Z}_{\geq 0}$. We will consider a generalisation where this monoid is replaced by certain other monoids.

17.3 Good monoids. Let M be a monoid. We call M *good* if for all $x \in M$ there are only finitely many tuples $(x_1, \ldots, x_k) \in M^k$ $(k \geq 0)$ such that $x_1 \cdots x_k = x$ and $x_i \neq 1$ for all i.

For $x, y \in M$, we write $x \leq z$ if and only if there exists y with $xy = z$. It can be shown that this is an ordering if M is good. An *interval* in M is

$$[a, c] := \{b \in M \mid a \leq b \leq c\}$$

where $a, c \in M$.

17.4 Exercise. Let M be a cancellative monoid. Prove that the following are equivalent.

(1) M is good.

(2) (a) For any $z \in M$ there are only finitely many $(x, y) \in M^2$ such that $xy = z$.

(b) For all $x, y \in M$, if $xy = 1$ then $x = y = 1$.

17.5 A *Garside monoid* is a monoid M such that for some A, f, Δ the conditions of theorem 15.3 are satisfied.

Every Garside monoid is good.

17.6 Formal power series for good monoids. Let M be a good monoid. By $\mathbb{C}[[M]]$ we will denote the set of formal series

$$\sum_{x \in M} a_x \, x$$

with $a_x \in \mathbb{C}$. We define addition in $\mathbb{C}[[M]]$ by

$$\Big(\sum_x a_x\, x\Big) + \Big(\sum_x b_x\, x\Big) = \sum_x (a_x + b_x)\, x$$

and multiplication by

$$\Big(\sum_x a_x\, x\Big)\Big(\sum_y b_y\, y\Big) = \sum_z c_z\, z \quad \text{where} \quad c_z = \sum_{\substack{x,y\in M\\ xy=z}} a_x\, b_y.$$

Note that c_z is well-defined, that is, this is only a finite sum.

It follows that $\mathbb{C}[[M]]$ is an associative ring.

For example, if $M = \mathbb{Z}_{\geq 0}$ then $\mathbb{C}[[M]] \cong \mathbb{C}[[t]]$, the ring of formal power series in one variable.

17.7 Exercise (Invertibility). Let M be a good monoid. In this exercise you will prove that an element

$$a = \sum_x a_x\, x \in \mathbb{C}[[M]]$$

is invertible if and only if $a_1 \neq 0$.

(a) Prove that there is a homomorphism of rings $f\colon \mathbb{C}[[M]] \to \mathbb{C}$ defined by

$$f\Big(\sum_x a_x\, x\Big) = a_1.$$

Deduce the implication $\Rightarrow$.

(b) Prove $\Leftarrow$. Hint: Why can you assume $a_1 = 1$? Then use the geometric series.

17.8 The Möbius function. Suppose M is a good monoid. We define the *zeta series* or *total growth function* Z by

$$Z = \sum_{x\in M} a_x\, x \in \mathbb{C}[[M]]$$

and the *Möbius function* $\mu\colon M \to \mathbb{Z}$ (pronounciation: $\mu =$ mu) by

$$\sum_{x\in M} \mu(x)\, x = Z^{-1} = \Big(\sum_{x\in M} x\Big)^{-1}.$$

Note that this inverse exists by exercise 17.7.

By taking the coefficient of z in the identity

$$\Big(\sum_x \mu(x)\, x\Big)\, Z = 1$$

we find

$$\sum_{xy=z} \mu(x) = \delta_{z,1}.$$

Moreover, if M is cancellative then the left hand side can be rewritten so that we have

$$\sum_{x\in[1,z]} \mu(x) = \delta_{z,1}. \tag{17.9}$$

In practice one computes the values of a Möbius function recursively using (17.9).

17.10 Lemma. *Let G be a Garside group. Let $x \in M$ and suppose that the greedy form for x starts with x_1. Then $[1, x] \cap \Omega = [1, x_1]$.* □

17.11 Proposition. *Suppose that M is a Garside monoid. Suppose $x \in M$ is such that $\mu(x) \neq 0$. Then $x \in \Omega$.*

Proof. If there is a counterexample to our proposition, then there is a minimal counterexample x, meaning that there is no counterexample y with $y \leq x$. This is so because M has no infinite descending chains because of its norm.

Let $x \in M$ be a minimal counterexample to our proposition. We will be done if we can deduce a contradiction. (This argument is similar to induction.)

We have $x \neq 1$ because $1 \in \Omega$. Therefore $x_1 \neq 1$. We find

$$\begin{aligned}
0 &= \sum_{y \in [1,x]} \mu(y) && \text{by (17.9) as } x \neq 1 \\
&= \mu(x) + \sum_{y \in [1,x] \cap \Omega} \mu(y) && \text{since } x \text{ is a minimal counterexample} \\
&= \mu(x) + \sum_{y \in [1,x_1]} \mu(y) && \text{by lemma 17.10} \\
&= \mu(x) && \text{by (17.9) as } x_1 \neq 1.
\end{aligned}$$

This is the required contradiction, and the proof is finished. □

17.12 Corollary. *The inverse of the zeta series is a polynomial, that is, a formal power series over M with only finitely many terms:*

$$Z^{-1} = \sum_{x \in \Omega} \mu(x)\, x.$$ □

17.13 Exercise. In the following cases, let M be the monoid given by the presentation. You already know that M is a Garside monoid in cases (a), (b), and you may assume it is in case (c). Each time, $\ell\colon M \to \mathbb{Z}$ will denote the homomorphism such that $\ell(a) = \ell(b) = \ell(c) = 1$. Draw the Dehornoy graph and label each vertex x with $\mu(x)$. Compute

$$\sum_{x \in M} t^{\ell(x)}.$$

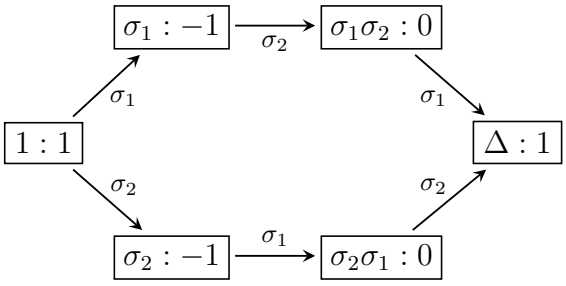
Proofs are not necessary.

(a) $(a, b, c \mid abb = bbc,\ bcc = cca,\ caa = aab)$.

(b) $(a, b, c \mid acab = bcaa,\ bcaac = cabca,\ cabca = acabc)$.

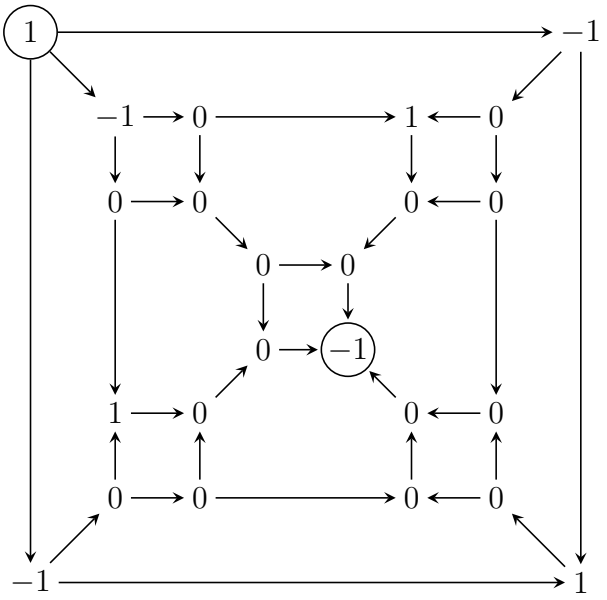
(c) $(a, b, c \mid ab = bc = ca)$.

Figure 17: The Möbius functions for B_3 and B_4



Meaning of a box: $\boxed{x : \mu(x)}$

x	$\mu(x)$
1	1
$\sigma_1,\ \sigma_2$	-1
$\sigma_1\sigma_2,\ \sigma_2\sigma_1$	0
Δ	1



The Möbius function for the classical positive braids

17.14 We will now study the Möbius function more closely in the case of the classical Garside structure on the braid group B_n.

17.15 Using (17.9) we can compute the Möbius function for B_3 and B_4. See figure 17. (One starts by drawing the Dehornoy graph, then labels each vertex x with the value $\mu(x)$.) This leads us to conjecture proposition 17.17.

17.16 For $I \subset S$ we write $w_I = \vee I$ and $\Delta_I = r(w_I) = \vee(rI)$. (So $w_0 = w_S$ and $\Delta = \Delta_S$.)

17.17 Proposition. *Let $x \in \Omega$. Then*

$$\mu(x) = \begin{cases} (-1)^{\#I} & \text{if } x = \Delta_I \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Put $J := S \cap N(x)$. We claim that for all $I \subset S$, one has

$$w_I \leq x \quad \Leftrightarrow \quad I \subset J. \tag{17.18}$$

Proof of $\Rightarrow$. $w_I \le x \Rightarrow N(w_I) \subset N(x) \Rightarrow N(w_I) \cap S \subset N(x) \cap S \Rightarrow I \subset J$ by 17.19.

Proof of $\Leftarrow$. For all $s \in J$ we have $s \in N(x)$ and therefore $s \le x$ by 17.20. Therefore $\vee J \le x$ and

$$I \subset J \Rightarrow \vee I \le \vee J \Rightarrow \vee I \le x \Rightarrow w_I \le x.$$

This proves (17.18).

For $x \in \Sigma_n$, put

$$f(x) = \begin{cases} (-1)^{\#I} & \text{if } x = w_I \\ 0 & \text{otherwise.} \end{cases}$$

Since $(\Sigma_n, \le)$ and $(\Omega, \le)$ are isomorphic ordered sets, we will be done if we can prove

$$\sum_{y \le x} f(y) = \delta_{x,1} \qquad (x \in \Sigma_n).$$

This is clear for $x = 1$ so suppose now $x \ne 1$. Then $J \ne \varnothing$. Using (17.18) and the fact that all w_I are distinct (by lemma 17.19) we find

$$\sum_{y \le x} f(y) = \sum_{w_I \le x} (-1)^{\#I} = \sum_{I \subset J} (-1)^{\#I} = 0 \qquad \square$$

17.19 Lemma. *Let $I \subset S$. Then $N(w_I) \cap S = I$. In particular, all w_I are distinct.* $\square$

17.20 Lemma. *Let $s \in S$, $x \in \Sigma_n$. Then $s \in N(x) \Leftrightarrow s \le x$.* $\square$

17.21 Examples.

$n = 2$: $Z^{-1} = 1 - \sigma_1$

$n = 3$: $Z^{-1} = 1 - \sigma_1 - \sigma_2 + \Delta_{12} = 1 - \sigma_1 - \sigma_2 + \sigma_1\,\sigma_2\,\sigma_1$

$n = 4$: $Z^{-1} = 1 - (\Delta_1 + \Delta_2 + \Delta_3) + (\Delta_{12} + \Delta_{23} + \Delta_{13}) - \Delta_{123}$.

We have a homomorphism $h\colon \mathbb{C}[[B_n^+]] \to \mathbb{C}[[t]]$ defined[14] by $h(\sigma_i) = t$. We find

$n = 2$: $hZ^{-1} = 1 - t$

$n = 3$: $hZ^{-1} = 1 - 2t + t^3$

$n = 4$: $hZ^{-1} = 1 - 3t + t^2 + 2t^3 - t^6$.

17.22 Exercise. Prove lemma 17.19. Hint: The proof of theorem 10.5 (Σ_n is a lattice) shows that $N(w_I)$ is the smallest set A of reflections containing I and such that

$$\big[(ij) \in A \text{ and } (jk) \in A\big] \;\Rightarrow\; (ik) \in A \qquad (1 \le i < j < k \le n).$$

[14]The definition is only complete if one also assumes that h is *continuous*, that is, h commutes with infinite formal sums.

17.23 *Exercise. Let $\ell\colon \Sigma_n \to \mathbb{Z}$ be the length with respect to S, the set of fundamental reflections. Prove:

$$\sum_{x\in\Sigma_n} q^{\ell(x)} = \prod_{k=1}^{n} \frac{1-q^k}{1-q}.$$

The Möbius function for the BKL positive braids

17.24 Next, we turn to the case of the BKL Garside structure on the braid group B_m.

17.25 For an n-cycle $x \in P$, write $a_n := \mu(rx)$.

It is clear that if $x \in P$ is any element, then on writing $f(k)$ for the number of k-cycles in x one has

$$\mu(rx) = \prod_k a_k^{f(k)}.$$

Our problem of determining the Möbius function is thus reduced to finding the numbers a_n.

17.26 Catalan numbers. We will soon need to know about the *Catalan numbers*

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

Here are some values of the Catalan numbers.

n	0	1	2	3	4	5
C_n	1	1	2	5	14	42

17.27 After some experimenting one may conjecture the following result. The proof will depend on two lemmas.

17.28 Proposition. $a_n = (-1)^{n-1}C_{n-1}$.

17.29 Lemma. *For $n \geq 2$ we have*

$$\sum_{k=0}^{n-1} \binom{n-k}{k} a_{n-k} = 0.$$

Proof. We simplify notation by writing $\mu(x)$ instead of $\mu(rx)$. Suppose $\vee P$ is an n-cycle. Put $P = P_1 \coprod P_2$ (we use $\coprod$ to denote the disjoint union) where $P_1 = \{x \in P \mid x(n) = n\}$. Then P_1 is like P for $n-1$ instead of n, so

$$\sum_{x\in P_1} \mu(x) = 0$$

and therefore

$$0 = \sum_{x\in P} \mu(x) = \sum_{x\in P_2} \mu(x). \tag{17.30}$$

Let Q_2 be the set of cycles in P_2. Let $f\colon P_2 \to Q_2$ be the map which takes $x \in P_2$ to its cycle containing n. Then

$$\sum_{x\in P_2} \mu(x) = \sum_{y\in Q_2} S(y) \tag{17.31}$$

where

$$S(y) := \sum_{x\in f^{-1}y} \mu(x).$$

Claim: We have $S(y) = 0$ unless

(H): there exists no i such that $y(i) = i,\ y(i+1) = i+1$.

In order to prove this claim, suppose that y fixes $J := \{j+1, j+2, \ldots, j+k\}$ pointwise ($k \geq 2$) but not j or $j+k+1$. Let A_0 denote those $x_0 \in f^{-1}(y)$ which fix J pointwise. Let A_1 denote those $x_1 \in f^{-1}(y)$ which fix $I_n - J$ pointwise. Then A_1 is a copy of P with $k \geq 2$ dots, so

$$\sum_{x_1\in A_1} \mu(x_1) = 0. \tag{17.32}$$

Now every element of $f^{-1}(y)$ can uniquely be written $x_0x_1 = x_1x_0$ with $(x_0, x_1) \in A_0 \times A_1$. It follows that

$$\sum_{x\in f^{-1}y} \mu(x) = \sum_{x_0\in A_0} \mu(x_0)\Big(\sum_{x_1\in A_1} \mu(x_1)\Big) = 0$$

by (17.32). Our claim is proved.

Let Q_3 denote set of those y which satisfy (H). So, by our proved claim, $S(y) = 0$ for all $y \in Q_2 - Q_3$. Let $Q_3(k)$ denote the set of those $y \in Q_3$ having precisely k fixed points. Note now the equivalences

$$\text{(H)} \quad \Leftrightarrow \quad \#f^{-1}(y) = 1 \quad \Leftrightarrow \quad f^{-1}(y) = \{y\}. \tag{17.33}$$

We find

$$\begin{aligned}
\sum_{y\in Q_2} S(y) = \sum_{y\in Q_3} S(y) = \sum_{y\in Q_3}\sum_{x\in f^{-1}y} \mu(x) &\overset{(17.33)}{=} \sum_{y\in Q_3} \mu(y) \\
= \sum_{k=0}^{n-1} \sum_{y\in Q_3(k)} \mu(y) = \sum_{k=0}^{n-1} \sum_{y\in Q_3(k)} a_{n-k} &\qquad (17.34)\\
= \sum_{k=0}^{n-1} \#Q_3(k)\cdot a_{n-k} = \sum_{k=0}^{n-1} \binom{n-k}{k} a_{n-k}&
\end{aligned}$$

where the last equality follows from the bijection

$$Q_3(k) \longrightarrow \Big\{m\text{-element subsets of } I_{n-k}\Big\}$$

$$\begin{pmatrix}\text{unique element}\\ \text{of fixed points}\\ x_0 < \cdots < x_{k-1}\end{pmatrix} \longmapsto \Big\{x_0,\ x_1 - 1,\ x_2 - 2,\ \ldots,\ x_{k-1} - (k-1)\Big\}.$$

The proof is finished by chaining (17.30), (17.31), (17.34). □

17.35 Lemma. *For $n \geq 2$ we have* $\displaystyle\sum_{k=0}^{n-1} \binom{n-k}{k} (-1)^{n-k-1} C_{n-k-1} = 0.$

Proof. Let $x^k * f$ denote the coefficient of x^k in f. We have

$$\begin{aligned}
\sum_{k=0}^{n-1} \binom{n-k}{k} C_{n-k-1} (-1)^{n-k} &= \sum_{k=1}^{n} \binom{k}{n-k} C_{k-1} (-1)^k \\
&= \sum_{k=1}^{n} \binom{k}{n-k} \binom{2k-2}{k-1} \frac{(-1)^k}{k} \\
&= \sum_{k=1}^{n} \frac{k!}{(n-k)!\,(2k-n)!} \frac{(2k-2)!}{(k-1)!\,k!} (-1)^k \\
&= \sum_{k=1}^{n} \frac{(n-1)!}{(k-1)!\,(n-k)!} \frac{(2k-2)!}{(n-2)!\,(2k-n)!} \frac{(-1)^k}{n-1} \\
&= \sum_{k=1}^{n} \binom{n-1}{k-1} \binom{2k-2}{n-2} \frac{(-1)^k}{n-1} \\
&= x^0 * \left[\sum_{k\in\mathbb{Z}} \binom{n-1}{k-1} \frac{(-1)^k x^{-2k}}{n-1} \right] \left[\sum_{\ell\in\mathbb{Z}} \binom{\ell-2}{n-2} x^\ell \right] \\
&= x^0 * \frac{(1-x^2)^{n-1}}{n-1} \frac{x^n}{(1-x)^{n-1}} = x^0 * \frac{(1+x)^{n-1}\, x^n}{n-1} = 0. \qquad \square
\end{aligned}$$

Proof of proposition 17.28. The recursion formulas 17.29 (for a_n) and 17.35 (for $(-1)^{n-1}C_{n-1}$) are identical. This suggests a proof by induction on n as follows. For $n < 2$ it is easy. Now let $n \geq 2$. Then the recursion formulas express a_n and $(-1)^{n-1}C_{n-1}$ in terms of the previous values. The induction step follows because the two recursion formulas are identical. $\square$

17.36 Example. Consider the homomorphism $h\colon \mathbb{C}[[B_m^+]] \to \mathbb{C}[[t]]$ defined by $h(\sigma_i) = t$ for all i. Then we have the following for the zeta series of the BKL positive braid monoids B_m^+:

$$\begin{aligned}
m = 2\colon &\quad hZ^{-1} = 1 - t \\
m = 3\colon &\quad hZ^{-1} = 1 - 3t + 2t^2 \\
m = 4\colon &\quad hZ^{-1} = 1 - 6t + 10t^2 - 5t^3
\end{aligned}$$

17.37 *Exercise. Prove the following formula for hZ^{-1} in the case of the BKL positive braid monoid B_m, valid for any m:

$$h\Big(\sum_{x\in B_m^+} x \Big)^{-1} = hZ^{-1} = \sum_{k=0}^{m-1} \frac{(m-1+k)!\,(-t)^k}{(m-1-k)!\,k!\,(k+1)!}.$$

18 The pure braid group

18.1 The aims of this section are the following.

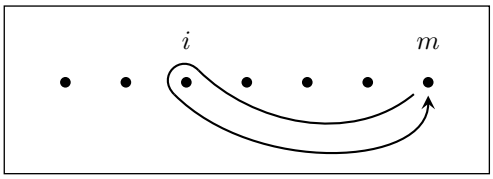
(1) A presentation for the pure braid group P_n.

(2) To learn semi-direct products and that P_{n+1} is a semi-direct product $P_n \ltimes F_n$.

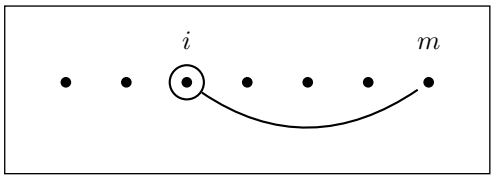
(3) A modest amount of the topology behind the groups, which mainly means that we draw some pictures.

(4) To learn the origin of the braid group action on the free group which we learned in section 4.

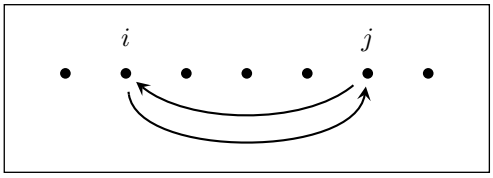
Figure 18: p_{km} and a_{ij} and the action $p_{km} \mapsto a_{ij} \rhd p_{km}$



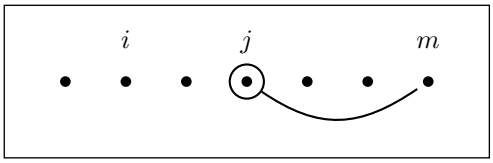
(a1) p_{im}

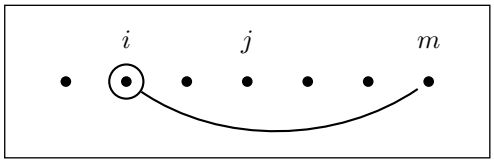


(a2) p_{im} symbolically

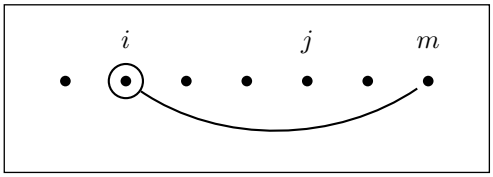


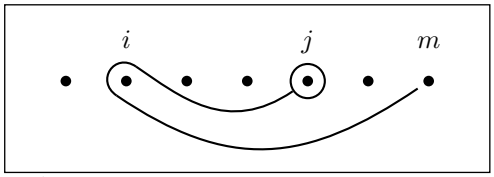
(b) a_{ij}



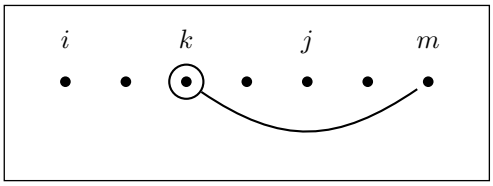


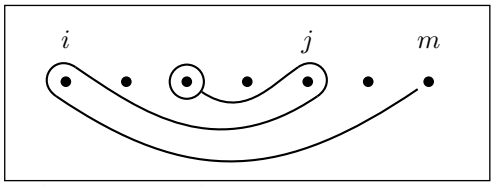
(c) $p_{jm} \mapsto p_{im}$





(d) $p_{im} \mapsto p_{im}^{-1} p_{jm} p_{im}$





(e) $p_{km} \mapsto p_{im}^{-1} p_{jm} p_{km} p_{jm}^{-1} p_{im}$

The punctured plane

18.2 The punctured plane. The *n times punctured plane* is $D_n = \mathbb{C} - \{1, \ldots, n\}$. We equip D_n with a *base point* $n+1$. We will write F_n for the fundamental group $\pi_1(D_n, n+1)$. We define elements $p_i = p_{i,n+1} \in F_n$ by figure 18(a1) though in the remaining drawings we shall simplify this as in figure 18(a2).

18.3 Proposition. *The group F_n is generated by $p_1, \ldots, p_n$ and moreover is a free group on these generators.* □

18.4 Action on F_n. Consider a based path $f\colon [a,b] \to BS_n$ in braid space BS_n (which, of course, represents a braid $g \in \pi_1(BS_n) = B_n$). As time t runs from a to b, the n points in $f(t)$ move through the plane. At some point they will hit the paths of figure 18(a) representing the p_i. We decide to avoid a collision by deforming the paths for p_i. At the end of the journey, $t = b$ and we have n new generators $(g^{-1} \rhd p_1, \ldots, g^{-1} \rhd p_n)$ of F_n obtained by deforming the paths for p_i. By construction (of course we are skipping many details here) this yields a B_n-action on F_n on the left.

Figure 18(cde) shows the paths for $a_{ij} \rhd p_{km}$.

Since $g \rhd p_i$ is an element of F_n, it can be expressed in terms of $(p_1, \ldots, p_n)$. From the pictures in figure 18 we deduce that, on writing m instead of $n+1$,

$$\left.\begin{array}{lll} & a_{ij} \rhd p_{km} = p_{km} & \left\{\begin{array}{l} i<j<k<m \\ \text{or}\ \ k<i<j<m \end{array}\right. \\ \text{(c)} & a_{ij} \rhd p_{jm} = p_{im} & i<j<m \\ \text{(d)} & a_{ij} \rhd p_{im} = p_{im}^{-1}\, p_{jm}\, p_{im} & i<j<m \\ \text{(e)} & a_{ik} \rhd p_{jm} = p_{im}^{-1}\, p_{km}\, p_{jm}\, p_{km}^{-1}\, p_{im} & i<j<k<m. \end{array}\right\} \quad (18.5)$$

18.6 Notice how important the pictures are in our deduction of (18.5). Later, in 18.27, we will see how one can find or prove these equations algebraically — but the pictures remain the only way to avoid long calculations!

18.7 Note that $p_m\, p_{m-1} \cdots p_1 \in F_n$ is a circle around all of $\{1, \ldots, n\}$ and is invariant under the B_n-action.

18.8 Exercise. An alternative, purely algebraic approach to the B_n-action on F_n takes (18.5) as starting point, forgetting that this formula comes from pictures or topology. Then one applies 5.15 to show that (18.5) defines a homomorphism $B_n \to \operatorname{Aut} F_n$. Can you do this?

18.9 Exercise.

(a) Let G be any group. Prove that there exists a set-theoretic bijection $\phi\colon \operatorname{Hom}(F_n, G) \to G^n$ defined by $\phi(f) = (fp_1, \ldots, fp_n)$.

(b) Let $\theta\colon B_n \times F_n \to F_n$ (pronounciation: θ = theta) denote the above constructed action. By (a) we have a B_n-action on G^n on the left by

$$\begin{aligned} B_n \times G^n &\longrightarrow G^n \\ (g, \phi f) &\longmapsto g(\phi f) := \phi\big(\theta(g,f)\big). \end{aligned}$$

Find a formula for $\sigma_i(x_1, \ldots, x_n)$.

Semi-direct products

18.10 Semi-direct products. Let G, H be a groups and let f be a G-action on H on the right:

$$\begin{aligned} f\colon H \times G &\longrightarrow H & (x^g)^h &= x^{(gh)} \\ (x, g) &\longmapsto x^g & (x^g)(y^g) &= (xy)^g \end{aligned} \tag{18.11}$$

One can show that the multiplication

$$(a, b)(c, d) := (ac, b^c d)$$

defines a group structure on the set $G \times H$. The group so created is called a *semi-direct product* and written $H \rtimes G$ or $H \rtimes_f G$.

We will be mainly dealing with left actions $G \times H \to H$ which we prefer to write as $(g, x) \mapsto g \rhd x$. In this case the semi-direct product is written $G \ltimes H$.

18.12 Split short exact sequences. Let

$$1 \longrightarrow H \xrightarrow{i} P \xrightarrow{p} G \longrightarrow 1 \tag{18.13}$$

be an short exact sequence[15] of groups. A *section* or *splitting* is a homomorphism $s\colon G \to P$ such that $ps = 1_G$. We say that (18.13) *splits* if a splitting exists.

Note that in the notation of 18.10,

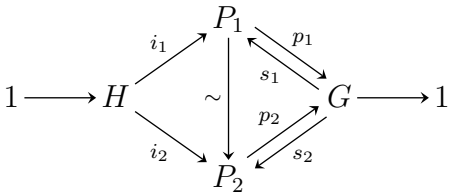
$$\begin{aligned} &1 \longrightarrow H \xrightarrow{i} G \ltimes_f H \underset{s}{\overset{p}{\rightleftarrows}} G \longrightarrow 1 \\ &i(b) = (1, b), \qquad p(a, b) = a, \qquad s(a) = (a, 1) \end{aligned} \tag{18.14}$$

is a split exact sequence. The following proposition says that semi-direct products and split short exact sequences are essentially the same thing in a precise sense.

18.15 *Proposition. *Let G, H be groups. There exists a bijection from* $\mathrm{Hom}(G, \mathrm{Aut}\, H)$ *to the set of split exact sequences*

$$1 \longrightarrow H \xrightarrow{i} P \underset{s}{\overset{p}{\rightleftarrows}} G \longrightarrow 1$$

up to isomorphism, where two such split exact sequences are called isomorphic if they combine into a commuting diagram



where the vertical arrow is an isomorphism. Under this bijection, a homomorphism $f\colon G \to \mathrm{Aut}\, H$ corresponds to the split short exact sequence (18.14).

[15] In this situation, exactness is equivalent to saying that i is injective and p surjective.

18.16 The following proposition tells us how to obtain a presentation (generators and relations) of a semi-direct product $G \ltimes_f H$ if f and presentations for G and H are known.

18.17 Proposition. *Let G, H be groups, and assume that G acts on H on the right written as in (18.11). Let (S_G, R_G) be a presentation for G and (S_H, R_H) one for H with S_G disjoint from S_H. For each $(x, y) \in S_G \times S_H$ choose a word $w(x, y) \in (S_H^{\pm})^*$ representing $x^y \in H$. Then a presentation for $G \ltimes H$ is $(S_G \cup S_H, R_G \cup R_H \cup R)$ where*

$$R = \big\{ y^{-1}xy = w(x,y) \;\big|\; x \in S_G,\ y \in S_H \big\}. \qquad \square$$

18.18 The B_n-action on F_n from 18.4 gives rise to a semi-direct product $B_n \ltimes F_n$. Using 18.17 and (18.5) (=formulas for the B_n-action on F_n) we immediately get a presentation for this semi-direct product as follows.

18.19 Proposition. *The group $B_n \ltimes F_n$ is presented by generators a_{ij} $(1 \le i < j \le n)$ and p_i $(1 \le i \le n)$ and the BKL relations (16.4), (16.5) and*

$$\begin{aligned}
a_{ij}\, p_{km}\, a_{ij}^{-1} &= p_{km} && \begin{cases} i<j<k<m \\ \text{or}\ \ k<i<j<m \end{cases} \\
a_{ij}\, p_{jm}\, a_{ij}^{-1} &= p_{im} && i<j<m \\
a_{ij}\, p_{im}\, a_{ij}^{-1} &= p_{im}^{-1}\, p_{jm}\, p_{im} && i<j<m \\
a_{ik}\, p_{jm}\, a_{ik}^{-1} &= p_{im}^{-1}\, p_{km}\, p_{jm}\, p_{km}^{-1}\, p_{im} && i<j<k<m. \qquad \square
\end{aligned}$$

18.20 *There's topology in the background. One can show that pairs of maps of topological spaces

$$A \xrightarrow{\ f\ } B \xleftarrow{\ g\ } C$$

with favourable properties which we don't make precise here give rise to a split short exact sequence

$$1 \longrightarrow \pi_1 A \longrightarrow \pi_1 B \longrightarrow \pi_1 C \longrightarrow 1.$$

Certain pairs (f, g) of this kind are behind the group theory in this section but we ignore it except that we like drawing pictures.

Adding and removing strings

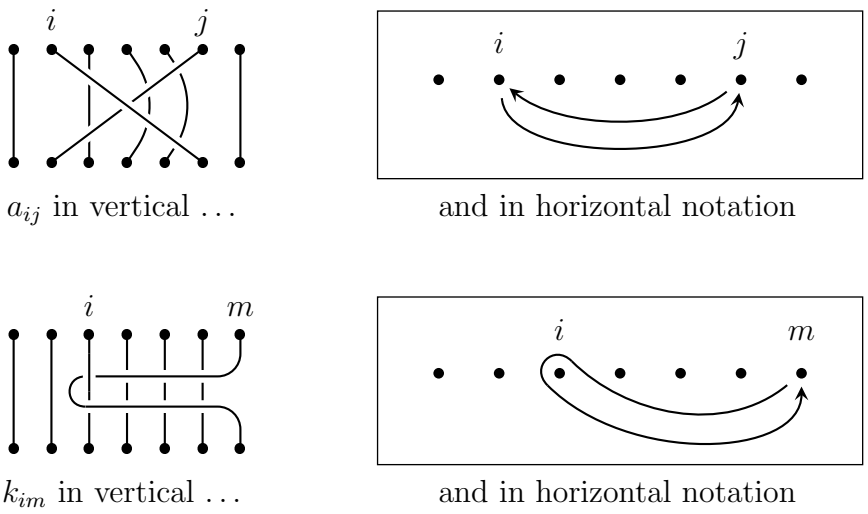
18.21 The B_n-action on F_n leads to a semi-direct product $B_n \ltimes F_n$. Does this group have any topological meaning? Yes! We will see that it can be embedded into B_{n+1} as a subgroup of index $n + 1$.

18.22 Horizontal diagrams. The diagrams by which we used to depict braids in section 1 are said to be in *vertical notation* (even after rotating them!) as opposed to the *horizontal notation* which we introduce now.

Recall that the braid group is the fundamental group of braid space

$$BS_n = \big\{ X \subset \mathbb{C} : |X| = n \big\}.$$

Figure 19: a_{ij} and $k_{im} = p_{im}$ in vertical and horizontal notation



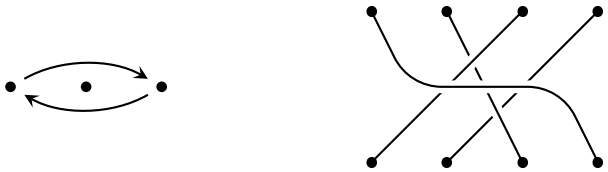
(a) a_{ij} in vertical ... and in horizontal notation

(b) k_{im} in vertical ... and in horizontal notation

The horizontal notation, whch is only somewhat loosely defined, consists in drawing the complex plane with the base-point of braid space $X_0 = \{1, \ldots, n\}$ and some arrows indicating how the points move around in the complex plane during the braid. As to the orientation of the arrows: in the vertical notation the arrows go down!

As an example, figure 19(a) shows the BKL braid a_{ij} in horizontal and vertical notation.

18.23 Exercise. Below a braid x is given in horizontal notation and a braid y in vertical. Sketch x in vertical notation and y in horizontal.



x y

18.24 The semi-direct product $B_n \ltimes K_n$. Recall the homomorphism $\pi\colon B_n \to \Sigma_n$ from 9.4. We define a group T_{n+1} by

$$T_{n+1} = \big\{ g \in B_{n+1} \;\big|\; (\pi g)(n+1) = n+1 \big\}.$$

In words, T_{n+1} is the group of $(n+1)$-braids such that the right most string at the bottom is also right most at the top.

We have a homomorphism $p\colon T_{n+1} \to B_n$ defined by removing the last string. We also have a homomorphism $s\colon B_n \to T_{n+1}$ defined by adding a vertical string to the right of everything. Moreover, we have $ps = 1_{B_n}$. Let K_n denote the kernel of p. Later on, we will see that $K_n = F_n$.

We can collect these groups and maps in a single diagram

$$1 \longrightarrow K_n \longrightarrow T_{n+1} \underset{s}{\overset{p}{\rightleftarrows}} B_n \longrightarrow 1. \tag{18.25}$$

This is clearly a split short exact sequence so T_{n+1} is a semi-direct product $B_n \ltimes K_n$. In particular, there is an action

$$\begin{aligned} B_n \times K_n &\longrightarrow K_n \\ (x, y) &\longmapsto x \rhd y := (sx)\, y\, (sx)^{-1}. \end{aligned}$$

It is clear that K_n is generated by the braids $k_i = k_{i,n+1} := a_{i,n+1}^2$ for $1 \leq i \leq n$. See figure 19(b) for vertical and horizontal diagrams of k_i. But wait a minute, it looks just like p_i!

18.26 Proposition/Definition. There is an isomorphism

$$\begin{aligned} F_n &\longrightarrow K_n \\ p_i &\longmapsto k_i \end{aligned}$$

which identifies the B_n-actions on F_n and K_n. So the semi-direct product $B_n \ltimes F_n$ from 18.18 is isomorphic to T_{n+1}. From now on we will write F_n and p_i rather than K_n and k_i. □

18.27 Algebraic deduction. In 18.4 we constructed a braid group action on F_n. But in 18.26 we saw that this action is just conjugacy in a braid group of one more string. As a consequence it should be possible to deduce the action from any presentation of the braid group, say, the BKL one. This is useful, because while drawing pictures remains the quickest way of computing the formulas, it is easy to confuse signs or directions of arrows that way. You get the signs right by doing just one formula the algebraic way, for example the following one. One of the BKL relations states

$$a_{ij}\, a_{jm}\, a_{ij}^{-1} = a_{im} \qquad (i < j < m).$$

On taking squares of both sides and recalling that $a_{jm}^2 = p_{jm}$ one finds

$$a_{ij}\, p_{jm}\, a_{ij}^{-1} = p_{im}$$

which agrees with 18.19.

The pure braid group

18.28 The *pure braid group* P_n is the kernel of π. So we have an exact sequence

$$1 \longrightarrow P_n \longrightarrow B_n \xrightarrow{\pi} \Sigma_n \longrightarrow 1.$$

We can play the game of 18.24 with P_n instead of B_n and P_{n+1} instead of T_{n+1}. Here's the result.

18.29 Proposition. $P_{n+1} = P_n \ltimes F_n$. □

18.30 Proposition/Exercise. The P_n-action on F_n by conjugation is as follows, where $m = n + 1$.

$$\left.\begin{array}{lll} (1) & p_{ij}\, p_{km}\, p_{ij}^{-1} = p_{km} & \left\{\begin{array}{l} i<j<k<m \\ \text{or}\quad k<i<j<m \end{array}\right. \\ (2) & p_{ij}\, p_{jm}\, p_{ij}^{-1} = p_{im}^{-1}\, p_{jm}\, p_{im} & i<j<m \\ (3) & p_{ij}\, p_{im}\, p_{ij}^{-1} = p_{im}^{-1}\, p_{jm}^{-1}\, p_{im}\, p_{jm}\, p_{im} & i<j<m \\ (4) & p_{ik}\, p_{jm}\, p_{ik}^{-1} = \text{exercise} & i<j<k<m \end{array}\right\} \quad (18.31)$$

Proof. This is an easy but tedious calculation which uses the identities displayed in 18.19 repeatedly. Equation (1) is easy. We prove (2) by

$$p_{ij}\, p_{jm}\, p_{ij} = a_{ij}\, (a_{ij}\, p_{jm}\, a_{ij}^{-1})\, a_{ij}^{-1} = a_{ij}\, p_{im}\, a_{ij}^{-1} = p_{im}^{-1}\, p_{jm}\, p_{im}$$

and (3) by

$$\begin{aligned} p_{ij}\, p_{im}\, p_{ij} &= a_{ij}\, (a_{ij}\, p_{im}\, a_{ij}^{-1})\, a_{ij}^{-1} = a_{ij}\, (p_{im}^{-1}\, p_{jm}\, p_{im})\, a_{ij}^{-1} \\ &= (a_{ij}\, p_{im}\, a_{ij}^{-1})^{-1} (a_{ij}\, p_{jm}\, a_{ij}^{-1})(a_{ij}\, p_{im}\, a_{ij}^{-1}) \\ &= (p_{im}^{-1}\, p_{jm}^{-1}\, p_{im})(p_{im})(p_{im}^{-1}\, p_{jm}\, p_{im}) \\ &= p_{im}^{-1}\, p_{jm}\, p_{im}\, p_{jm}\, p_{im}. \end{aligned}$$

Equation (4) is left as an exercise. □

18.32 Proposition. *The pure braid group P_n is presented by generators $p_{ij} = p_{ji}$ $(1 \le i < j \le n)$ and relations (18.31) for all values $i, j, k, m \in \{1, \ldots, n\}$ satisfying the indicated inequalities.*

Proof. Induction on n. For $n = 0$ this is obvious. Assume it's true for P_n. By 18.29, P_{n+1} is a semi-direct product $P_n \ltimes F_n$. Proposition 18.17 tells us that a presentation for P_{n+1} can be obtained from the one for P_n by adding generators for F_n (that's $p_{i,n+1}$ for $1 \le i \le n$) and relations for F_n (that's none) and relations stating how P_n acts on F_n (that's the relations 18.31 with $m = n + 1$). The result follows. □

Index

List of notations