BACHELOR

Linear representations of finite groups
some properties of braids

Onete, M.C.

Award date:
2007

LINEAR REPRESENTATIONS OF FINITE GROUPS; SOME PROPERTIES OF BRAIDS

CRISTINA ONETE

PROJECTCOORDINATOR: HANS CUYPERS

April 11, 2007

Abstract

This paper elaborates on two akin subjects, namely linear representations and braid groups. Linear representations are a manner of analyzing finite groups; they are defined as homomorphisms from the said finite groups to spaces of bijections from a space V onto itself. Any finite group may be characterized this way. Braid groups, however, are infinite, though finitely generated. They may only be analyzed as finite groups when additional conditions are imposed to their generators, so that only a finite section of a braid group is analyzed.

As a primary example, the symmetric group on 5 elements, S_5, is chosen. It is shown that it has seven conjugacy classes and, as such, seven linear representations. As the character of a representation is shown to be a categoric, definitive attribute that defines the representation, the representations of S_5 are primarily described by means of their characters. For the representations with orders 1 and 4, a concrete function form is found for the representations.

Braid groups are shown to be a model of the phenomenon of braiding, which has existed since ancient times. The necessity of braids has arisen from a wish to understand its twin domain, knot theory. Although braids, as described first by Emil Artin, have not given the expected benefits to knot theory, braids have evolved as a separate domain. Braid groups are an established algebraic structure with as parameter the number of strands. Although infinite, the group is finitely generated. The additional restriction of having only generators of order two, however, presents S_5 as a restriction to a finite group.

The domain of braids and braid groups is further analyzed from the perspective of its cryptographic benefits. Two methods of authentication are given, which use a relatively simple composition of braids. Patrick Dehornoy's work, which presents algorithms for reducing braids to a state where they are more easily comparable. With the aid of this method, two algorithms are presented and exemplified for authentication based on the relative easy of composing a braid, but the comparable difficulty of finding an original braid from a composition.

The knowledge of the protocol in the first method is wholly exposing; that is, an eavesdropper is able to fully penetrate the system. However, even knowledge of the system will provide only one chance in 2^k, where k is a positive integer decided upon by the two parties communicating, of the eavesdropper to successfully break the protocol.

Contents

1 **Introduction** *2*
2 **Linear Representations of Finite Groups** *4*
2.1 *Groups and Group Analysis* *4*
2.2 *Linear Representations* *5*
2.3 *Irreducibility; Irreducible Linear Representations* *7*
2.4 *Characters of Representations* *8*
2.5 *A Few Theorems* *10*
2.6 *Permutation Representations and the Frobenius Reciprocity* *15*
2.7 *The Symmetric Group S_5* *16*
2.7.1 The trivial and semi-trivial representations *17*
2.7.2 The Permutation Representation to $Sym(5)$; Representations of Order 4 *18*
2.7.3 Representations of Order 5 *20*
2.7.4 The Representation of Order 6 *20*
3 **Braids and Braid Groups** *22*
3.1 *Braids* *22*
3.2 *The Group B_n* *24*
3.3 *Reduced Forms and Dehornoy's Work* *28*
3.4 *Dehornoy's Algorithms* *32*
3.4.1 Full Reduction *32*
3.4.2 Greedy Reduction *33*
3.4.3 Convex Reduction *34*
3.5 *Braids and Cryptography* *35*
3.5.1 An outline of a first method *35*
3.5.2 An outline of a second method *36*
4 **Suggested Extensions and Improvements** *38*
A **Character Tableaux of S_3 and S_4** *40*
A.1 S_3 *40*
A.2 S_4 *40*

Chapter 1

Introduction

The present paper concerns two areas within group theory, namely linear representations and braid groups. Although these two parts are mostly separately treated, there are points in which they are related.

Groups, especially finite groups, are of interest to most mathematicians, both because of their intriguing, intrinsic form, and because of their uses in various domains, including in cryptography. It is habitual to view groups by means of linear representations, since they describe the groups by means of homomorphisms. Just as mathematicians like to find isomorphic, that is "similar", groups, they also like to transform them.

Linear representations may be given, like most functions, in a few ways. Given a finite group, it is enough to associate each of its conjugacy classes with a linear bijection defined on a space V. This function might, in turn, be given by an expression, or by a matrix.

In what follows in chapter 2, it is attempted to give a general background on linear representations and to exemplify this theory by means of an analysis of the group S_5.

A particular kind of groups, which might be of interest, are braid groups. The most intriguing factor about these groups is that they are both familiar and unknown. They represent a field in mathematics that was created as a basis to understand a completely different subject, knot theory. Since then, although not much progress was made within knot theory with the aid of braids, braid groups have evolved into a separate branch of mathematics.

Chapter 3 concerns braid groups entirely, explaining what braids are and how they may be used, in particular in cryptography. It is perhaps better if an introduction to braids is given here, from the perspective of knots and knot theory.

Knot is a relatively new branch in mathematics. The basics of the pillar-branches of mathematics, such as linear algebra, algebra itself, and calculus can trace their beginnings in the antiquity; most of these branches had a solid basis and commanded immense interest already around 1850. Knots themselves existed from the ancient times, having a strong background in reality and everyday life. It was only at the end of the nineteenth century, however, when a mathematical background was given to them and they became a branch of great interest.

The sudden interest in knot theory originated in practical sciences. The first impulse came from physics, from the times when it was believed that the universe was filled with a substance called ether. [KnotTheory] explains that it was Lord Kelvin who suggested that elements might have an unique signature, depending on how elements knotted the ether around them. This statement meant that atomic theory could be partly reduced to studying knots and knot theory. Mathematicians were asked to show tables of knots and what these knots looked like. With the dismissal of this idea by the new atomic theory, however, knot theory died down, only to be take up in the next century by geneticists.

Genetics and DNA have been very much in vogue for many years. It was not, however, until geneticists noticed that sometimes DNA becomes tangled that this new science was connected to knot theory.

Experiments were done on these tangled DNA strands and the results showed that the knots might have an impact on what the strand behaves like after replication.

We may begin by stating that braids are simply cut knots. A knot is defined as a simple, closed, three-dimensional curve. The term **simple** refers to the fact that the curve may not cross itself, although it might go over or under it. A braid is simply a knot which is not closed and its ends are bound to two parallel knitting needles.

To graphically illustrate this, let us consider the simples knot, which is named the **unknot**.

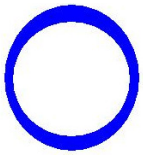


Figure 1.1: The Unknot

In a braid, this knot would become:

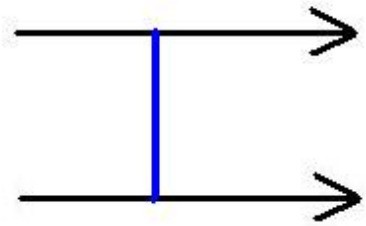


Figure 1.2: The Identity Braid

The concept of braids is further analyzed in chapter 3, from the perspective of braid groups. A connection between linear representations and braids is attempted in this chapter, stating that certain restrictions may connect finite groups to braid groups.

Finally, chapter 4 lists some suggestions of improvements for the expansion of this thesis.

Chapter 2

Linear Representations of Finite Groups

2.1 Groups and Group Analysis

We must begin by defining the term 'group'. On a set G of elements we define an operation denoted by '*', with $* : G \times G \longrightarrow G$. This operation must fulfill the following four conditions:

- Associativity: $\forall\, a, b, c \in G$: $(a * b) * c = a * (b * c)$;
- Neutral Element: $\exists\, e \in G$: $e * a = a * e = a\ \forall\, a \in G$;
- Inverse Element: $\forall\, a \in G\ \exists\, b \in G$: $a * b = b * a = e$, for e the neutral element of the previous clause;
- Closure: $\forall\, a, b \in G$, $a * b \in G$.

There are multiple manners in which a mathematician can look at a group and therefore can subsequently analyse it.

One manner is of course to view all its elements, where we use this term very loosely. Surely, if the group has a cardinality (i.e. a number of elements) greater than, say, 100, even writing down all the elements is not very practical. What is generally meant by viewing a group's elements is by separating them in **conjugacy classes** and viewing only a **representative** or two of each class.

Before we proceed to show other manners of representing a group, let us first define conjugacy classes and representatives, since they are essential to understanding representations and characters of representations.

- **Definition:**

  Two elements, t and t', with $t, t' \in G$ are said to be **conjugate** if there exists $s \in G$ such that: $t' = sts^{-1}$. All the elements in a group that are conjugates of each other form a **conjugacy class**.

Conjugacy is a so-called equivalence class, that is to say, it is *reflexive, symmetric,* and *transitive*. This can be easily shown:

- *Reflexivity:* For any $t \in G\ \exists \mathbf{1} \in G$ such that $t = \mathbf{1}t\mathbf{1}^{-1}$. By $\mathbf{1}$ we refer to the neutral element of the group. Therefore t is a conjugate of itself.

- *Symmetry:* Take $t, t' \in G$, conjugates of each other, so with a certain $s \in G$ such that $t' = sts^{-1}$. Define: $s' = s^{-1}$. From the definition of a group (see **??**), it follows that $s' \in G$.

Then: $t' = s't{s'}^{-1}$ Therefore, if t is a conjugate of t', then t' is also a conjugate of t.

- *Transitivity:* Take $t, t', t'' \in G$, with t a conjugate of t' and t' a conjugate of t''. Then there exist $s, s' \in G$ with $t' = sts^{-1}$ and $t'' = s't's'^{-1}$. Define $s'' = s's$. Then $s''^{-1} = (s's)^{-1} = s'^{-1}s^{-1} \in G$, and $t'' = s''ts''^{-1}$, and thus t is a conjugate of t''.

Because conjugacy is an equivalence relation, it follows that it *partitions* G into conjugacy classes, hence these classes are disjunct. We will return to the subject of conjugacy classes a little later.

Therefore, one way of looking at groups is to look at its elements. A different manner of looking at groups, however, is to notice that they have a lot in common with matrices. For instance, the multiplication of matrices is, similarly with the operation defined on groups, mostly invertible, has a neutral element, and is not necessarily commutative.

A third manner of looking at groups is to represent them in terms of representations in different spaces, such as function spaces. Linear functions on finitely-dimensional spaces can, naturally, also be expressed in terms of matrices.

2.2 Linear Representations

We now introduce the terms **linear representations** and **characters**. Representations connect groups in their initial form, i.e. as a set of elements with an operation defined on them, to function spaces and to matrices. A good treatment of this topic is found in [Serre, 1977].

It is assumed that the reader is familiar with terms such as homomorphisms, isomorphism, and fields. For further reading on the basics of algebra and groups, the reader is recommended [Artin, 1991] and [Rotman,1995].

Define now a vector space V over the field of complex numbers, **C**. We consider isomorphisms of V onto itself and name the group of all such isomorphisms **GL(*V*)**. We define the elements of **GL(*V*)** as linear mappings with linear inverses, i.e.:

$$\mathbf{GL}(V) = \{\alpha : V \longrightarrow V | \alpha \text{is linear and } \alpha^{-1} \text{exists}\} \tag{2.1}$$

We restrict ourselves to finitely-generated vector spaces. In this case, the vector space V has a finite basis, let's say of n elements, which we label $\{e_i\}_{i=1}^{n}$. If that is the case, each linear map α is defined by a matrix, A. This matrix will be $n \times n$, with elements a_{ij}. We have considered V to be spanned over the complex numbers, therefore the matrix entries a_{ij} are complex numbers. They can be obtained by considering that the matrix transforms the basis vectors as follows:

$$A(e_j) = \sum_{i=1}^{n} a_{ij} e_i \tag{2.2}$$

Knowing that α represents an isomorphism automatically forms a restriction on the matrix A, namely that A is invertible, and hence that $det(A) \neq 0$. We can now identify $\mathbf{GL}(V)$ with the group of invertible matrices of order n, where n is, as it was earlier mentioned, the dimension of V. It will be easier now to understand the connection between linear representations and their matricial forms.

- **Definition:**

For G a finite group with neutral element **1** and composition $(s,t) \longrightarrow st$, we can define a **linear representation** of G in V as a homomorphism $\rho : G \longrightarrow \mathbf{GL}(V)$, such that we have:

$$\rho(st) = \rho(s)\rho(t) \tag{2.3}$$

It is trivial to show now that the following two equalities hold:

- $\rho(1) = 1$
- $\rho(s^{(-1)}) = (\rho(s))^{-1}$

If we have such a linear representation of G into V already given, we may call V the **representation space** of G. Serre ([Serre, 1977]) mentions that V is sometimes also called, by abuse of language, a **representation** of G.

A connection can now be established between linear representations, if V is finite, and matrices. For the sake of simplicity, we will denote $\rho(s)$ by ρ_s. The matrix of ρ_s with respect to the basis $\{e_i\}$ of V is labelled by R_s and must fulfil the following conditions:

- $det(R_s) \neq 0$, for all $s \in G$
- $R_{st} = R_s \cdot R_t$, for all $s, t \in G$

The representation and its matrix form are equivalent, meaning that given one, the other may be found. We define here the term **similarity** (or isomorphism) of two representations:

- **Definition:**

  Two representations, ρ with representation space V and ρ' in V' are **similar** or **isomorphic** if there exists a linear isomorphism, $\tau : V \longrightarrow V'$ such that:

$$\tau \circ \rho_s = \rho'_s \circ \tau, \forall s \in G \tag{2.4}$$

This definition translates into matrix-related terms as follows:

- **Definition:**

  Two representations, ρ with matrix R_s and ρ' with matrix form R'_s are **similar** or **isomorphic** if there exists an invertible $n \times n$ matrix, T, such that:

$$T \cdot R_s = R'_s \cdot T, \forall s \in G \tag{2.5}$$

A trivially-proven, but important consequence of this definition is that the two representations, whether as functions or in matrix form, have the same degree, n.

2.3 Irreducibility; Irreducible Linear Representations

Firstly, we must recall the term **direct sum** of two subsets. Consider a vector space V and U, $W \subseteq V$.

- **Definition:**

  We say V is the direct sum of U and W and we write $V = U \oplus W$ if any element $v \in V$ can be uniquely written in the form $v = u + w$, with $u \in U$ and $w \in W$.

It can be easily shown that this definition is equivalent with saying that $V = U \oplus W$ if and only if:

- $U \cap W = \{0\}$
- $dim(V) = dim(U) + dim(W)$

- *Example:*

  As an example, consider the two-dimensional space $V = \mathbf{R}^2$. We can write the elements of this space in the form (x, y), with $x, y \in \mathbf{R}$. Consider the following two spaces, $U =< (1, 0) >$ and $W =< (0, 1) >$. By this notation, we mean the space generated by $(1, 0)$ and $(0, 1)$ respectively. It is not difficult to notice that any element, (x, y) can be written in the form $\underline{u} + \underline{w}$, with $\underline{u} = x * (1, 0) \in V$ and $\underline{w} = y * (0, 1) \in W$. At the same time, $\underline{u} = \underline{w}$ if and only if $x = y = 0$; thus, $U \cap W = \{(0, 0)\}$. We can say that $V = U \oplus W$.

Consider a vector space V and a linear representation, $\rho : G \longrightarrow \mathbf{GL}(V)$. Let $W \subseteq V$. We name W **stable** (or **invariant**) under the action of G if $x \in W$ implies $\rho_s x \in W$, $\forall s \in G$. We have:

- **Definition:**

  A linear representation $\rho : G \longrightarrow \mathbf{GL(}V\mathbf{)}$ is **irreducible** or **simple** if $V \neq \{0\}$ and if no vector subspace $W \subseteq V$ is stable under G with the exceptions of V and $\{0\}$

Theorem 1 *(Theorem 2 in [Serre, 1977]):*

Every representation is a direct sum of irreducible representations.

It is not difficult to prove this if we consider an induction after the dimension of the vector space V. Indeed, this is done very clearly in [Serre, 1977]. We will not repeat this proof here. It is, however, important to notice that irreducible representations act like a basis for the set of representations. This idea will come back later, when we speak about characters.

Beside the direct sum of representations, there is one other term we must define, namely the **tensor product** of two representations. In order to do so, we must first look at the the tensor product of two vector spaces.

- **Definition:**

  Consider two vector spaces V_1 and V_2. A space $\mathbb{W}$ with a map $\sigma : V_1 \times V_2 \longrightarrow W, \sigma(x_1, x_2) = x_1 \cdot x_2$, is called the **tensor product** of V_1 and V_2 if the following conditions are satisfied:

  - $x_1 \cdot x_2$ is linear in both x_1 and x_2
  - If we have a basis of V_1, $\{e_{i1}\}$, and a basis of V_2, $\{e_{i2}\}$, then the products $\{e_{i1} \cdot e_{i2}\}$ forms a basis of W.

This space, which exists and is unique up to isomorphism, is denoted by $V_1 \otimes V_2$. Similarly to this, we can now define the tensor product of two representations:

- **Definition:**

  Take ρ^i, $i \in 1, 2$ to be two linear representations of G respectively in V_1 and V_2. For $s \in G$ define $\rho_s \in \mathbf{GL}(V_\mathbf{1} \otimes V_\mathbf{2})$ by means of the condition:

$$\rho_s(x_1 \cdot x_2) = \rho_s^1(x_1) \cdot \rho_s^2(x_2) \text{ for } x_1 \in V_1, x_2 \in V_2 \tag{2.6}$$

In matrix form, we denote bases of V_1 and of V_2 by $\{e_{i1}\}$ and $\{e_{i2}\}$ respectively. We label the matrices of ρ_s^1 and of ρ_s^2 with respect to these bases r_{i1j1} and r_{i2j2}. The definition in (2.2) implies:

$$\rho_s(e_{j1} \cdot e_{j2}) = \sum_{i(1),i(2)} r_{i1j1}(s) \cdot r_{i2j2}(s) \cdot e_{i1} \cdot e_{i2} \tag{2.7}$$

This above relation defines the tensor product of matrices. As ever when it comes to groups, this three-fold approach is closely related. The notion of characters again reflects the connection between representations and matrices. It is trivial to see by means of this relation between the matrices that the product of two linear representations will also be a linear representation of greater or equal order to the maximal order of the representations composing it.

2.4 Characters of Representations

We must firstly recall the definition for the **trace** of a matrix; this concept is essential to defining the **character** of a linear representation.

- **Definition:**

  We consider again a vector space V of dimension n, with basis $\{e_i\}_{i=1}^n$. Let α be a linear map of V onto itself, described in terms of the given basis by a matrix $A = (a_{ij})$. The **trace** of A is the number $Tr(a)$, defined as:

$$Tr(a) = \sum_{i=1}^{n} a_{ii} \tag{2.8}$$

This is the sum of the eigenvalues of A, with their respective multiplicities. It does not depend on the chosen basis.

Let us return to representations. For every $s \in G$, we have a linear map ρ_s that can be written in terms of a matrix, say R_s.

- **Definition:**

  We define the **character** of the representation as a function $\chi : G \longrightarrow \mathbf{C}$, with $\chi_\rho(s) = Tr(R_s)$. As it will be shown later, the character of a representation is essential, as it characterizes it.

It is interesting to list a few properties of a character of a representation.

Proposition 2 *(Proposition 1 in [Serre, 1977])*

Let ρ be a representation ρ of degree n, and let χ be its character. Then:

1. $\chi(1) = n$
2. $\chi(s^{-1}) = (\chi(s))^*$, *for* $s \in G$. *By* z^* *we indicate the complex conjugate of a number* $z \in \mathbf{C}$.
3. $\chi(tst^{-1}) = \chi(s)$, *for* $s, t \in G$.

Proof:

Point (1) is easy to ascertain. Indeed, as we have before said, we have $\chi(1) = 1$. Since $dim(V) = n$, the matrix R_1 has dimensions $n \times n$, with only the element 1 repeated on the diagonal. Hence, $Tr(R_1) = n$.

Point (2) is nearly as easily ascertained. For this, we must recall that the map ρ_s has finite order. Because of this, the eigenvalues $\lambda_1, \lambda_2, ...\lambda_n$ are also of finite order. Since they are complex numbers, their absolute value must all be equal to 1. Then:

$$\chi(s)^* = (Tr(R_s)^*) = \sum_{i=1}^{n} \lambda_i^* \tag{2.9}$$

A simple calculation will show that $z^* = \frac{||z||^2}{z}$. Hence,

$$\sum_{i=1}^{n} \lambda_i^* = \sum_{i=1}^{n} \lambda_i^{-1} = Tr((R_s)^{-1}) = Tr(\rho_{s^{-1}}) = \chi(s^{-1}) \tag{2.10}$$

Part (3) is merely a matter of rewriting the equation with $u = ts$ and $v = t^{-1}$. Then we must only prove that $\chi(uv) = \chi(vu)$. This is already known from matrices and from linear functions.

To get a better idea of how characters are connected to their respective representations, the following Proposition describes the connections between characters and the direct sum and the tensor product of two representations.

Proposition 3 *(Proposition 2 in [Serre, 1977])*

Consider two linear representations of G in V_1 *and* V_2 *respectively. Let these representations be labelled* ρ^1 *and* ρ^2*, with characters* χ_1 *and* χ_2*. Let* χ *be the character of the representation of G in* $V_1 \oplus V_2$ *and let* ψ *be the character of the representation of G in* $V_1 \otimes V_2$*. Then:*

- $\chi = \chi_1 + \chi_2$
- $\psi = \chi_1 \cdot \chi_2$

Proof:

The proof is easier if we consider representations and characters from the point of view of their matrices. Let s be an element of G and let R_s^1 and R_s^2 be the respective matrices of ρ_s^1 and ρ_s^2. Then the representation ρ_s^+ of G in $V_1 \oplus V_2$ has matrix R_s^+ given by:

$$\begin{pmatrix} R_s^1 & 0 \\ 0 & R_s^2 \end{pmatrix}$$

The trace of this matrix is then $Tr(R_s^1) + Tr(R_s^2)$, therefore we have: $\chi(s) = \chi_1(s) + \chi_2(s)$.

For the second part of the proof, with the notation given in 2.3, we have:

$$\begin{aligned} \chi_1(s) &= \sum_{i(1)} r_{i1i1}(s) \\ \chi_2(s) &= \sum_{i(2)} r_{i2i2}(s) \\ \psi(s) = \sum_{i1,i2} r_{i1i(1)} r_{i2i2} &= \chi_1(s) \cdot \chi_2(s) \end{aligned} \tag{2.11}$$

The Proposition is thus proved.

2.5 A Few Theorems

The general purpose of this document is to give background information of linear representations and to exemplify how to find these representations if a given group G is considered. In this section, a few theorems and lemmas are given, some without their proofs. For the interested reader, we recommend Serre's book, [Serre, 1977].

Lemma 4 *(Schur's Lemma: Proposition 4 in [Serre, 1977])*

Consider two irreducible representations in two vector spaces, V_1 *and* V_2*; let them be labelled* ρ^1 *and* ρ^2*. Let furthermore* f *be a linear mapping of* V_1 *into* V_2*, such that* $\rho_s^2 \circ f = f \circ \rho_s^1$*, for all* $s \in G$*. Then:*

1. *If ρ^1 and ρ^2 are not isomorphic, then f is uniformly 0.*
2. *If V_1=V_2 and $\rho^1 = \rho^2$, f is a homothety.*

In Serre's book, [Serre, 1977], is a clear proof of this theorem. We leave it to the reader. Instead, it is interesting to state two consequences of this theorem, which are of great importance in deriving an important property of irreducible characters:

Corollary 5 *Corollary 2 to Proposition 4 in [Serre, 1977]*

In the above-stated situation, if ρ_1 is not isomorphic to ρ_2 and if $card(G) = g$, then:

$$\frac{1}{g}\sum_{t\in G} r_{i2j2}(t^{-1})r_{i1j1}(t) = 0, \tag{2.12}$$

for arbitrarily-chosen $i1, i2, j1, j2$.

The second corollary refers to the second alternative to Schur's Lemma:

Corollary 6 *Corollary 3 to Proposition 4 in [Serre, 1977]*

In the above-stated situation, if V_1=V_2, n =$dim(V_1)$ and $\rho^1 = \rho^2$, and if $card(G) = g$, then:

$$\frac{1}{g}\sum_{t\in G} r_{i2j2}(t^{-1})r_{i1j1}(t) = \frac{1}{n}\delta_{i2i1}\delta_{j2j1} \tag{2.13}$$

As a consequence, this product has the value $\frac{1}{n}$ if $i1 = i2$ and $j1 = j2$, and it is equal to 0 otherwise.

An essential theorem follows from these relations. However, we must first define a function that could be consider an inner product of two characters. First consider two functions $\phi, \psi : G \longrightarrow \mathbf{C}$ and define:

$$(\phi|\psi) = \frac{1}{g}\sum_{t\in G} \phi(t)\psi(t)^* \tag{2.14}$$

Again, we denote the cardinal of G by g. This function is a scalar product, because it is linear in ϕ, it is semilinear in ψ, and $(\phi, \phi) > 0$ if $\phi \neq 0$.

- *Example:*

Consider instead of two functions, two representations of the symmetric group S_5 (see 2.6 and 2.7 for further reading on the symmetric group S_5). These characters may be written in the following tableau:

χ	s_0	s_1	s_2	s_3	s_4	s_5	s_6
χ_0	1	1	1	1	1	1	1
χ_1	1	-1	1	-1	1	1	-1
(s_i)	1	10	20	30	24	15	20

The elements listed at the top of the tableau are the conjugacy classes of this particular group. For each class i, $c(s_i)$ is the number of elements in that class. We therefore have:

$$(\chi_0|\chi_0) = \frac{1}{g}\sum_{i=0}^{6} c(s_i) * \chi_0(s_i) * \chi_0(s_i)^*(\chi_0|\chi_1) = \frac{1}{g}\sum_{i=0}^{6} c(s_i) * \chi_0(s_i) * \chi_1(s_i)^*$$

The two characters form an orthonormal system, that is $(\chi_0|\chi_0) = 1$ and $(\chi_0|\chi_1) = 0$

Let us define now:

$$< \phi, \psi >= \frac{1}{g}\sum_{t\in G} \phi(t^{-1})\psi(t) = \frac{1}{g}\sum_{t\in G} \phi(t)\psi(t^{-1}) \tag{2.15}$$

The connection between these two expressions becomes apparent if we denote $\psi(t^{-1})^*$ by $\psi'(t)$. It becomes now easy to see that:

$$(\phi|\psi) =< \phi, \psi' > \tag{2.16}$$

If we now consider, instead of a random function ψ, a character χ of a representation of G, then, by Proposition 2, it follows that $\chi' = \chi$, and thus that $(\phi|\chi) =< \phi, \chi' >$ for any function ϕ on G. An essential theorem now follows regarding characters; this gives the orhonormality of characters of irreducible representations.

Theorem 7 *(Theorem 3 in [Serre, 1977])*

- *If χ is the character of an irreducible representations of G, then $(\chi|\chi) = 1$. (We also say that χ is **of norm** 1)*
- *If χ and χ' are the characters of two nonisomorphic, irreducible representations of G, then $(\chi|\chi') = 0$ (This means that χ and χ' are orthogonal).*

Proof:

The proof follows easily from the corollaries 5 and 6. We can write ρ, the irreducible representation with character χ in matrix form, with the matrix of ρ_s being represented by $R_s = (r_{ij}(s))$. Then: $\chi(s) = \sum r_{ii}(t)$. It follows that $(\chi|\chi) =< \chi, \chi >= \sum_{i,j} < r_{ii}, r_{jj} >$.

Now, by using the values we have for $< r_{ii}, r_{jj} >$ by the two corollaries, we obtain the results in this theorem.

Serre ([Serre, 1977]) discusses characters and representations in detail. However, we only present a few more theorems and proposition that will later be needed for the identification of irreducible representations. The proofs of these theorems can be found in Serre's work.

Theorem 8 *(Theorem 5 in [Serre, 1977])*

If χ is the character of a representation ρ of a group G in a vector space V*, then $(\chi|\chi) \in \mathbf{Z}^+$, with $(\chi|\chi) = 1$ if and only if ρ is irreducible.*

Lemma 9 *(Corollary 2 to Proposition 5 in [Serre, 1977])*

Consider the h irreducible, linear representations of a group G of cardinality g, with respective degrees $n_1, n_2, ...n_h$. Then:

$$\sum_{i=1}^{h} (n_i)^2 = g \tag{2.17}$$

This lemma gives already a hint towards the number of irreducible representations that a certain group has. The following theorems further consolidate the basis that the results so far have given us. However, it is important to draw the reader's attention to the following problem: the construction of the characters of the irreducible representations of a group is being now reduced to a problem of partitioning the cardinal of g into a sum of squares that must fulfil some additional properties. This hints towards a method that becomes easier once the first few representations are found.

Before we progress any further, it is important to define **class functions**.

- **Definition:**

  Let us consider a function f on a group G, with the following property:

  $$f(tst^{-1}) = f(s), \text{ for all } s, t \in G \tag{2.18}$$

  Such a function is called a **class function**.

It must be immediately noted that characters are class functions (this follows from Proposition 2). We also know that they form an orthonormal set. In fact, as it is shown in [Serre, 1977]:

Theorem 10 *(Theorem 6 in [Serre, 1977])*

Let H be the space of the class functions of a group G. Then the characters $\chi_1, \chi_2, ...\chi_h$ form an orthonormal basis of H.

An essential theorem follows from this result, indicating exactly how many irreducible representations a group G has.

Theorem 11 *(Theorem 7 in [Serre, 1977])*

G has as many non-isomorphic irreducible representations as it has conjugacy classes.

Proof:

Consider a group that has k conjugacy classes, $C_1, ...C_k$. Consider a class function $f \in H$. This class function must remain constant on each of the conjugacy classes, since, assuming an $s \in C_i$ is chosen, for all $s' \in C_i$, we have the same value $f(s)$, which we denote by λ_i. Therefore, the dimension of the space of all class functions is k. This dimension is, by Theorem 9, equal to the number of irreducible representations, up to isomorphism.

Finally, we give a lemma which facilitates the computation of the characters of irreducible representations of a group G.

Lemma 12 *(Proposition 7 in [Serre, 1977])*

Define for every $s \in G$ $c(s)$ as the number of elements in the conjugacy class of s. Then:

1. $\sum_{i=1}^{h} \chi_i(s)^* \chi_i(s) = \frac{g}{c(s)}$ *for all* $s \in G$
2. $\sum_{i=1}^{h} \chi_i(s)^* \chi_i(t) = 0$, *for all* $t \in G$ *not in the conjugacy class of* s.

Proof:

Let g be the cardinality of G. Consider the identity function on the class of s, I_s, which takes the value 1 for all the elements in the conjugacy class of s and is 0 everywhere else. This function is a class function and therefore it can be written in terms of the basis of characters of H as follows:

$$I_s(t) = \sum_{i=1}^{h} \lambda_i \chi_i(t), \text{ for all } t \in G \tag{2.19}$$

Herein, the coefficients of this function are:

$$\lambda_i = (f_s | \chi_i) = \frac{c(s)}{g} \chi_i(s)^* \tag{2.20}$$

This translates to:

$$I_s(t) = \frac{c(s)}{g} \sum_{i=1}^{h} \chi(s)^* \chi_i(t) \tag{2.21}$$

Given the values that I_s by definition takes, the lemma now follows.

2.6 Permutation Representations and the Frobenius Reciprocity

We have spoken thus far of characters of representations. In the analysis of some symmetric groups, representations may be visualized by means of permutation representations. Firstly let us first define symmetric groups in general. Consider a group V with n elements.

- **Definition:**

  The **symmetric group on V**, $Sym(V)$, consists of all the bijections $\rho : V \longrightarrow V$ from V to V. In the particular case $V = \{1, 2, 3, ..., n\}$, we denote this group by S_n.

Now we can define permutation representations.

- **Definition:**

  A **permutation representation** ϕ of G in a set V is a homomorphism $\phi : G \longrightarrow Sym(V)$

The Frobenius Reciprocity may be formulated within a lemma. For this purpose, however, further notations are necessary. For those interested, a more complete treatment of permutation representations may be found in [Cohen, 1980].

For the rest of the section, we will refer to permutation characters codomain as X. We will write the permutation character in the form χ^X. We must also define the **stabilizer** of an element group v with respect to a permutation representation ϕ on G.

- **Definition:**

  Assume the existence of a homomorphism $\phi : G \longrightarrow Sym(V)$ for certain sets G and V with G a group. For an element $v \in V$ we can now define the **stabilizer** of v in G is:

$$G_V^{\phi} := \{g \in G | \phi(g)(v) = v\} \tag{2.22}$$

We must now define the term **orbit** of an element x under a permutation group $H \subset Sym(V)$ as the subset $Hx = \{h(x) | h \in H\} subset V$.

The Frobenius Reciprocity may be formulated as follows:

Theorem 13 *(Proposition* 4.3.4 *in [Cohen, 1980])*

Let H be a subgroup of G. Assume that χ is a character of H and ϕ is a character of G. It follows then that:

$$< \chi^G | \phi >=< \chi | \phi_H > \tag{2.23}$$

A proof of this theorem is given in [Cohen, 1980]. A more interesting consequence of this theorem is given in the Corollary below.

Corollary 14 *Let G be a permutation group on X; let χ^X be the character of the corresponding linear representation. . Then:*

$$(\chi^X|1) \text{ is the number of orbits of } G \text{ in } X. \tag{2.24}$$

An application of this corollary is finding how many irreducible representations are contained within a reducible representation. We consider two transitive permutation representations of G on X, respectively Y with characters χ and ψ. We have from the corollary that:

$$(\chi^X|1) \text{ is the number of orbits of G on X} \tag{2.25}$$

We now take $H = G_x$ the stabilizer of x in G. $\chi = \mathbf{1}^G$ induced by the stabilizer G_x of x. We write this $\mathbf{1}^G_{G_x}$. It follows that:

$$(\chi|1) = (\mathbf{1}^G_{G_x}|1) = (1_{G_x}|1_{G_x}) = 1 \tag{2.26}$$

This is the number of orbits of G_x on X. Then:

$$(\chi|\psi) = (\mathbf{1}^G_{G_x}|\psi) = (1_{G_x}|\psi_{G_x}) = (\psi_{G_x}|1)_{G_x} \tag{2.27}$$

This number represents, by the previous corollary, the number of orbits of ψ on G_x, so the number of orbits of ψ in G made by χ. Once we have such a representation and its character, therefore, we can calculate the function $(\phi|\phi)$, as defined in section 2.5. This will indicate the number of irreducible representations included in the permutation representation.

2.7 The Symmetric Group S_5

The elements of S_5 may be divided into seven conjugacy classes labelled s_0, s_1, s_2, ..., s_6, thus, by theorem 13, there are seven irreducible representations of S_5. The order of this group is $5! = 120$, therefore we can write the following equation:

$$\sum_{i=0}^{6} c(s_i)\chi(s_i)^2 = 120, \text{ where } c(s_i) \text{ is the number of elements of the class } s_i \tag{2.28}$$

1. The unit element, {1}. We have $c(\{1\}) = 1$. We name this class s_0.

2. Elements of the form (12). The number of ways to form such elements (regardless of the order the elements are in) is equal to the number of ways two numbers may be picked out of five. We have thus $c(\{(12)\}) = 10$. We name this class s_1.

3. Elements of the form (123). In this case, the order of the numbers does matter. If we pick three numbers, say (123), we may also arrange them into a second, different combination, namely (132). We have $c(\{(123)\}) = 2 * 10 = 20$. We name this class s_2.

4. Elements of the form (1234). There are six ways of rearranging four picked numbers into different permutations. For example, we have: (1234), (1324), (1243), (1423), (1432), and (1342). We have $c(\{(1234)\}) = 5 * 6 = 30$. We name this class s_3.

5. Elements of the form (12345). This is equal to the number of ways 5 people can be seated around a circular table, thus $c(\{(12345)\}) = 4! = 24$. We name this class s_4.

6. Elements of the form (12)(34). If we have the first pair fixed, say (12), there are three options left for the second pair. On the other hand, because the elements are symmetric, ((12)(34)=(34)(12)), we only have $\frac{10}{2} = 5$ ways of picking the first pair. There are $c(\{(12)(34)\}) = 15$ elements of this type. We name this class s_5.

7. Elements of the form (123)(34). There are 10 ways of choosing the loose pair. The triplet may be written in two ways, like for the elements in s_2 We have $c(\{(123)(45)\}) = 10 * 2 = 20$. We name this class s_6.

For this group, it is attempted in what follows to give the character tableau and some of the irreducible, linear representations that may be associated with it. For the interested reader, the character tableaux of some smaller symmetric groups, S_4 and S_3 are given in the Appendix.

2.7.1 The trivial and semi-trivial representations

Firstly, we must draw the attention to the fact that there are two rather trivial representations. One such representation is the 'identity' representation, whose character is identically 1:

χ	1	(12)	(123)	(1234)	(12345)	(12)(34)	(123)(45)
χ_0	1	1	1	1	1	1	1

We must have orthogonality of the characters, by virtue of theorem 7. A semi-trivial representation follows as shown below, the sign representation.

χ	1	(12)	(123)	(1234)	(12345)	(12)(34)	(123)(45)
χ_1	1	-1	1	-1	1	1	-1

The fact that these truly are representations applying to S_5 may be easier visualized as functions, like it is described in section 2.2. For the trivial and for the semi-trivial representations as shown above, these functions are as follows.

The Trivial Representation

Firstly, we must consider that the group is generated by the elements in the class of (12). A linear representation is characterized by the fact that $\chi(st) = \chi(s)\chi(t)$. We take:

1. $V = \{1\}$
2. Consider $f \in GL(V)$, with $f(x) = 1 \forall x \in V$
3. Consider the homomorphism: $\chi_0 : S_5 \longrightarrow GL(V)$, with $\chi_0((12)) = f$, with the property: $\chi(st) = \chi(s)\chi(t)$

It is not very difficult now to show that indeed all the elements of the group are mapped to f and that the character table is indeed correct.

The Semi-Trivial Representation

Similarly, by taking the generators of the group, we consider the following, semi-trivial representation:

- $V = \{-1, 1\}$
- Consider $g \in GL(V)$, with $g(x) = -1 \forall x \in V$
- Finally, consider the homomorphism $\chi_1 : S_5 \longrightarrow GL(V)$, with $\chi_1((12)) = -1$ and the property $\chi_1(st) = \chi_1(s)\chi_1(t)$

If we consider all the seven conjugacy classes, we may find this is the sign function, sgn, of a permutation.

2.7.2 The Permutation Representation to $Sym(5)$; Representations of Order 4

Let us consider a permutation representation to $Sym(5)$. We know already that there exists such a homomorphism to $Sym(5)$, since $S_5 \cong Sym(5)$. We have to calculate the character of the representation, ϕ. For the seven conjugacy classes, s_i, $0 \leq i \leq 6$, $\phi(s_i)$ is the number of fixed points the homomorphism leaves.

- $\phi((1)) = 5$
- $\phi((12)) = 3$
- $\phi((123)) = 2$
- $\phi((1234)) = 1$
- $\phi((12345)) = 0$
- $\phi((12)(34)) = 1$
- $\phi((123)(45)) = 0$

We now have $(\phi|\phi) = \frac{1}{120} * \sum_{i=0}^{6} c(s_i) * \phi(s_i)^2 = \frac{240}{120} = 2$. This indicates that $\phi = \chi_0 + \chi_2$, where χ_0 is the character of the trivial representation of degree 1. Both χ_0 and χ_2 are the characters of irreducible representations. Thus:

$$\chi_2(t) = \psi(t) - \chi_0(t) \tag{2.29}$$

We now have the following:

χ	1	(12)	(123)	(1234)	(12345)	(12)(34)	(123)(45)
χ_2	4	2	1	0	-1	0	-1

Indeed, we have $\sum_{i=0}^{6} \chi_2(s_i)^2 = 120$ A second irreducible representation may be found by considering the tensor product of χ_1 and χ_4, leading to another irreducible representation, namely:

χ	1	(12)	(123)	(1234)	(12345)	(12)(34)	(123)(45)
χ_3	4	-2	1	0	-1	0	1

For this representation, too, we have $\sum_{i=0}^{6} \chi_3(s_i)^2 = 120$. It is left to the reader to verify that indeed we have orthogonality.

In order to now find these representations in function form, we must take a more abstract approach than for the trivial and semi-trivial representations. This approach is shown below.

The representation with character χ_2

We consider a five-dimensional space W, with a basis $\{w_1, w_2, w_3, w_4, w_5\}$. For every element, $\sigma \in S_5$, we define $f : V \longrightarrow V$, with $f(e_i) = e_{\sigma^{-1}(i)}$.

We can also look at this function from the perspective of matrices, by looking at how the basis vectors are changed by the permutation, σ. For instance, for $\sigma = (12)$:

$$M(12) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

This function is indeed linear; the proof is trivial if one looks at this function from the perspective of matrices. It is true that:

$$f(A * e_i + B * e_j) = Af(e_i) + Bf(e_j) \tag{2.30}$$

This ascertains that indeed $f \in GL(W)$.

However, the space W is not four-dimensional. On closer examination, it is noticeable, however, that $\sum_{i=1}^{5} w_i$ is invariant under the given function. ($f(\sum_{i=1}^{5} w_i) = \sum_{i=1}^{5} w_i$) We can now restrict f to $V = W/ < \sum_{i=1}^{5} w_i >$. We can now define, as before:

- $\chi_2 : S_5 \longrightarrow GL(V)$, with $\chi_2(\sigma) = f(\sigma)$.

The representation with character χ_3

As mentioned before, the representation with character χ_3 is the tensor product of the representations with character χ_1 and χ_2 respectively. We define then:

$$\begin{aligned} V_1 &= \{-1\} \\ V_2 &= V, \text{ with V as mentioned above} \end{aligned} \tag{2.31}$$

We have:

1. $\chi_3 : S_5 \longrightarrow V_1 \otimes V_2$, with $\chi_3(t) = \chi_1(t) \cdot \chi_2(t)$.

2.7.3 Representations of Order 5

Similarly, we may introduce a homomorphism, Ψ, to all the doubles of the form $\{i, j\}$, with $i, j \in \{1, 2, 3, 4, 5\}$ and $i \neq j$. As before, we must find $\psi(s_i)$, $0 \leq i \leq 6$, which are the fixed elements under the homomorphism.

Thus, for $\psi((1))$, there are 10 fixed elements, namely any combination of two elements taken out of the list of five. On the other hand $\psi((12))$. Fixed elements are in this case $\{12\}$ and any set i, j with $i, j \in \{3, 4, 5\}$. We have thus $\psi((12)) = 4$. We can thus write the following regarding the character of this representation:

1. $\psi((1)) = 10$
2. $\psi((12)) = 4$
3. $\psi((123)) = 1$
4. $\psi((1234)) = 0$
5. $\psi((12345)) = 0$
6. $\psi((12)(34)) = 2$
7. $\psi((123)(45)) = 1$

For this representation, we have $(\psi|\psi) = \frac{1}{120}\sum_{i=0}^{6} c(s_i)\psi(s_i)^2 = \frac{360}{120} = 3$. We also have $(\phi|\psi) = \frac{1}{120}\sum_{i=0}^{6} c(s_i)\phi(s_i)\psi(s_i)^* = 2$. Therefore, we have $\Psi = \chi_0 + \chi_2 + \chi_4$, where χ_0 is the character of the trivial irreducible representation and χ_2 is the character of the degree 4 representation as shown above. We now have:

χ	1	(12)	(123)	(1234)	(12345)	(12)(34)	(123)(45)
χ_4	5	1	−1	−1	0	1	1

χ_4 is the character of an irreducible representation. Indeed, $\sum_{i=0}^{6} c(s_i)\chi_4(s_i)^2 = 120$. The corresponding tensor product is given by the following character:

χ	1	(12)	(123)	(1234)	(12345)	(12)(34)	(123)(45)
χ_5	5	−1	−1	1	0	1	−1

2.7.4 The Representation of Order 6

So far, we have found six irreducible representations of S_5. As stated before, there are seven conjugacy classes of S_5, hence seven irreducible representations. The sixth is now easy to find by means of a system of equations dictated by the orthonormality of the system with respect to the $(*|*)$ metric.

A simple Mathematica routine provides the character of the last irreducible representation:

χ	1	(12)	(123)	(1234)	(12345)	(12)(34)	(123)(45)
χ_6	6	0	0	0	1	−2	0

Orthonormality may be easily tested for this seventh representation.

The corresponding concrete representation can be imagined as follows. We take a four-dimensional space V. A basis of this space may be imagined as $\{e_1, e_2, e_3, e_4\}$. The tensor product of V with itself is 16−dimensional. We are looking for a 6−dimensional space for the representation. The extra ten dimensions may be eliminated by taking out the space spanned by $v \otimes v' + v' \otimes v | v, v' \in V$.

The remaining space may be denoted by $\wedge^2 V$ and which is an antisymmetric difference of V and itself. In this space, we have that $e_i \otimes e_j = -e_j \otimes e_i$. The base of the remaining space, $\wedge^2 V$ is then six-dimensional, with base $\{e_i \otimes e_j | i < j\}$. There are six such elements, $e_1 \otimes e_2$, $e_1 \otimes e_3$, $e_1 \otimes e_4$, $e_2 \otimes e_3$, $e_2 \otimes e_4$, $e_3 \otimes e_4$. Their independence is easily proved, based on the definition of tensor products. They also span the entire space.

We have then the sixth-order linear representation of S_5. It can be easily verified that this representation is irreducible and that the character tableau of this representation matches the one above.

Chapter 3

Braids and Braid Groups

Braid Groups are placed at the limit between abstract algebra, namely group theory, and topology. The subject is deeply connected to knots and knot theory (see chapter **??**); however, for smaller braid groups, it is perhaps easier to picture braid groups than corresponding knot groups and knot-related problems. In this chapter, braids are first defined (in 3.1), then they are characterized as groups in 3.2. This introduction is, in essence, based on Emil Artin's work, [Artin, 1965]. A further addition on braid isotopy and on Dehornoy's work ([Dehornoy, 1997]) is given in 3.3.

3.1 Braids

In order to define a braid, one must first define a **weaving pattern of order n** and a **deformation of the pattern**. In what follows, the basic notions are given regarding weaving patterns and their connection to braids will be given. Finally, the braid group of order n, $\mathbf{B_n}$, will be defined.

Firstly, two parallel lines in space; the distance between them does not matter. Let us label these lines L_1 and L_2. If we took a randomly chosen points $P \in L_1$ and $Q \in L_2$, fixed. A curve s can be drawn in space, connecting these two points; the projection of the curve s on the plane given by L_1 and L_2 is labelled c.

In weaving patterns, any projected curves c must be somewhat restricted, enabling them to fall into a category that [Artin, 1965] names *normal curves*. This condition is shown below:

- Take a mobile point $R \in c$. We introduce an orientation of the curve c, from P to Q. As R now moves along the curve in this orientation, we condition that the distance from R to L_1 should be a strictly increasing function.

For instance, figure 3.1 shows a setting which does not fulfil this condition. In this example, the curve moves from P to Q as indicated above, but the distance R_1L_1 is greater than the distance R_2L_1, although R_2 is farther along the curve than R_1 on the oriented curve c:

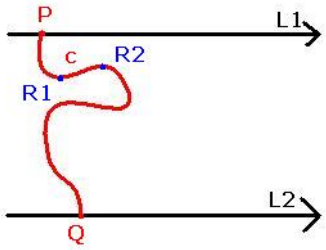


Figure 3.1: c is here not a normal curve

Secondly, a positive integer n is considered. Consider orientations of L_1 and L_2; consider n points on each of these two lines, with $\{P_i\}_{i=1}^n \in L_1$ and $\{Q_i\}_{i=1}^n \in L_2$, such that P_i always comes before P_{i+1} along the oriented L_1 line and similarly Q_j always comes before Q_{j+1} along the oriented L_2.

In this setting, we now draw curves between each P_i on the L_1 and a certain Q_j with j not necessarily equal to i. The curve between P_i and Q_j (in space) is labelled s_i. Let us label the projections of these curves on the L_1L_2 plane c_i as before. We also set the condition no two curves s_1 and s_2 may intersect (in space). That, of course, does not mean that their projections might not intersect, but it does condition that no two curves end in the same point Q_j if they begin from P_{i1} and P_{i2} respectively, with $i1 \neq i2$.

We make the following convention: if the curve s_i passes underneath another curve s_j, their projections will intersect. In this case, the projection c_1 of s_1 will be interrupted before it crosses the projection c_2 of s_2. An example of a weaving pattern of degree 3 is shown below, with the respective curves between the points:

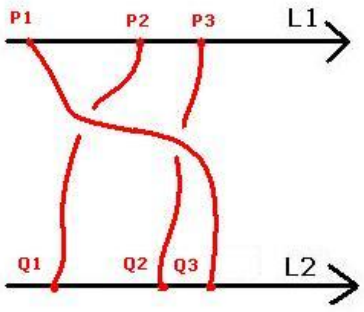


Figure 3.2: A weaving pattern of degree 3

The entire system, including the oriented lines L_1 and L_2, the points $\{P_i\}$ and $\{Q_i\}$, and the pairs of curves $\{s_i\}$ and $\{c_i\}$, is what Artin names a **weaving pattern of degree n**.

To obtain a braid, we must now introduce the notion of **deformation**. This is the definition that Artin uses in [Artin, 1965]. As the name suggests, this is an alteration of a weaving pattern of degree n; however, this alteration is limited by three, essential conditions:

1. The oriented lines L_1 and L_2 remain parallel throughout and after the deformation. Note that there are no conditions regarding the distance between the lines; this may change or may remain the same - it is irrelevant.

2. No two curves s_i may intersect during a deformation.

3. The curves c_i remain normal throughout and after the deformation.

This is perhaps better explained by the image below, which shows two equivalent weaving patterns:

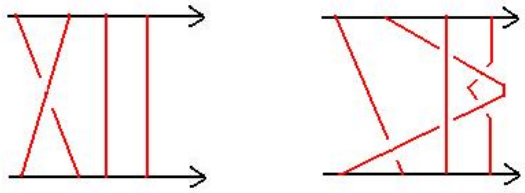


Figure 3.3: The two weaving patterns are equivalent

A weaving pattern coupled with the permission to be deformed as defined above forms a **braid of order n**. In what follows, unless specifically stated, the term 'braid' will refer to a braid of degree n for a certain, chosen n. It must be observed that a single weaving pattern identifies a single braid, but a braid encompasses infinitely many weaving patterns, all deformed from one another.

3.2 The Group B_n

The definition of a group has already been given in section 2.1. We must now define a group B_n of braids. We consider B_n the set of all the braids of order n; we must first properly define an operation on this set and then prove that it is, indeed, a group.

The principle by which the multiplication operation is defined here is similar to the composition of functions. In the rest of this chapter, we will refer to a braid with a fixed pattern simply as a braid. Let us consider two braids, **A** and **B**. **A** comprises the parallel, oriented lines L_1 and L_2, and points $P_1 \in L_1$ and $Q_1 \in L_2$, bound by the projected curve c_1. Similarly, **B** has parallel lines L_1' and L_2', and points $P_1' \in L_1'$ and $Q_1' \in L_2'$, bound by the projected curve c_1'.

The product $\mathbf{A} * \mathbf{B}$, also written as **AB**, may be imagined as follows: we shift **B** towards **A** such that L_1' moves upwards towards L_2. The points on L_2 are shifted (but kept in order), so as to coincide with the points Q_i on L_2. The line L_2, which now coincides to L_1' is then removed, resulting in another braid of degree n. This resulting braid might be denoted by **C**. Figure 3.5 illustrates this:

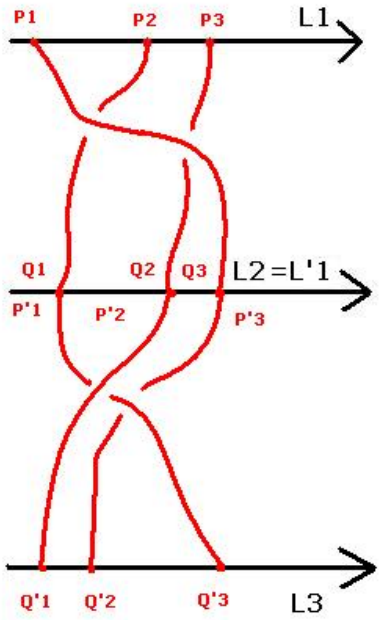


Figure 3.4: Multiplying braids

The associativity rule is clear in this case. It does not matter if we first 'melt' one braid together with the another, and then with a third, or if we first attach the latter two (in the same order), and then move this resulting thread towards the first one. It is, however, also visible, that in general it is not true that $\mathbf{AB} = \mathbf{BA}$.

As a neutral element, we present the following braid:

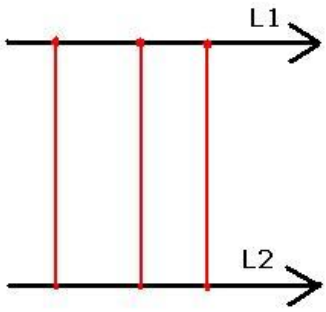


Figure 3.5: The Neutral Braid

It is trivial to notice that this braid indeed fulfils the requirements of a neutral element. To make a parallel to matrices, this would be the identity matrix, and is indeed denoted by $\mathbf{I}$. Naturally, the order of the identity braid is given by the order of the group.

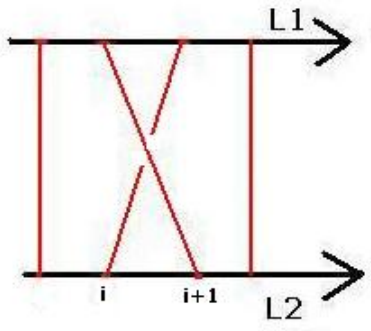
In view of this neutral element, we find an easy manner to define inverse braids. Given a certain braid

A, we consider the curve c_i binding P_i and Q_j. In the inverse braid, denoted by $\mathbf{A}^{-1}$, the curve c'_j would go from P'_j to Q'_i. Moreover, if in the initial braid c_i goes under any other c_k, the inverse braid woud go over the corresponding curve c'_l (the indices here are not the same, because the index of a curve is denoted by its starting point and not by its end point).

Finally, the fact that from two braids of degree n we obtain by multiplication another braid of the same degree n is rather trivial, considering the manner in which multiplication is defined.

Thus, we may affirm that indeed, the combination $(B_n, *)$ forms a group. This is not always an Abelian group, that is to say, it is not true that $\mathbf{AB} = \mathbf{BA}$, for all $A, B \in B_n$.

Now let us consider the following braid, which we label σ_i:

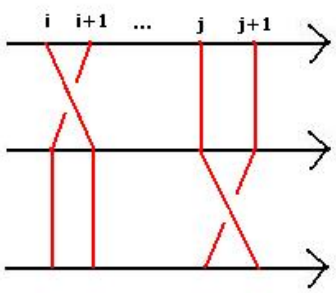


In figure 3.2, the curve c_i passes over c_{i+1} and the rest of the curves are vertical lines. Let us note that the inverse braid, σ_i^{-1}, is the same braid, only with curve c_i passing under c_{i+1} instead of over it.

It is not difficult to notice that the set $\{\sigma_1, \sigma_2, ...\sigma_{n-1}\}$ generates the group, as any braid can be composed of this set and the set of their inverses. We can also deduce that, because of the definition of these braids, we have the following:

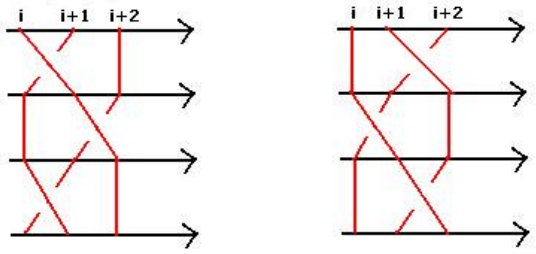
1. $\sigma_i\sigma_j = \sigma_j\sigma_i, \forall j \geq i+2$;

   This can be viewed from the following image of $\sigma_i\sigma_j$, for $j \geq i+2$. The equality results from the fact that it does not matter in which order the strands are braided; the two generating braids are disjunct, i.e. they have no common strand.

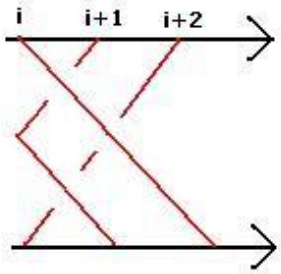


2. $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$.

The two terms are shown below:



Both these patterns have the same resulting braid:



These properties lead to an easy reduction of the set of generators, as Artin indicates ([Artin, 1965]). Having them in mind, we can now prove that the group B_n is generated by σ_1 and:

$$\alpha = \sigma_1\sigma_2...\sigma_{n-1} \tag{3.1}$$

Indeed, by an easy argument, we can prove that:

$$\sigma_i = \alpha^{i-1}\sigma_1\alpha^{-(i-1)} \tag{3.2}$$

Proof:

This statement may be proven by induction to n.

It is trivial that $\sigma_1 = \alpha^0\sigma_1\alpha^{-0}$. Now let us assume that it is true for a given k. It follows that:

$$\alpha\sigma_k = \prod_{i=1}^{n-1}\sigma_i\sigma_k \tag{3.3}$$

By repeatedly using the relation 1 listed above, we can shift the tail of this product as follows:

$$\prod_{i=1}^{n-1}\sigma_i\sigma_k = \prod_{i=1}^{n-2}\sigma_i\sigma_k\sigma_{n-1} = \ldots = \prod_{i=1}^{k-1}\sigma_i\sigma_k\sigma_{k+1}\sigma_k \prod_{i=k+2}^{n-1}\sigma_i \tag{3.4}$$

By using the fact that $\sigma_k\sigma_{k+1}\sigma_k = \sigma_{k+1}\sigma_k\sigma_{k+1}$, we write:

$$\alpha\sigma_k = \prod_{i=1}^{k-1}\sigma_i\sigma_k\sigma_{k+1}\sigma_k \prod_{i=k+2}^{n-1}\sigma_i = \prod_{i=1}^{k-1}\sigma_i\sigma_{k+1}\sigma_k\sigma_{k+1} \prod_{i=k+2}^{n-1}\sigma_i \tag{3.5}$$

Again, by repeated use of 1, we now have:

$$\alpha\sigma_k = \sigma_{k+1}\alpha \tag{3.6}$$

It follows then, by the induction step, that:

$$\sigma_{k+1} = \alpha\sigma_k\alpha^{-1} = \alpha^k\sigma_1\alpha^{-k} \tag{3.7}$$

Relations 1 and 2 therefore define the generators of a braid group. Furthermore, this braid group, B_n, is infinite, consisting of all the braids on n strands. however, a braid with n strands may be, for instance, formed by infinitely twirling the first two strands around each other. There is no finitude to the number of braids that one can obtain on a set number of strands. This can also be shown by remembering that we have $n-1$ generators, each of which can be taken to any integer power.

However, although the group itself is infinite, we may, be setting further restrictions on the generators, arrive at a familiar finite group. If we set the number of strands to 5 for instance, we may generate the group with the four classical generators, σ_1, σ_2, σ_3, and σ_4. Further requesting that $\sigma_i^2 = 1$ for all i restricts the group to S_5, which is analyzed in 2.7.

3.3 Reduced Forms and Dehornoy's Work

This section is of primary importance to braids, although it bears less bearing on braid representations. Instead, beside having intrinsic importance, it is crucial to the uses of braids in cryptography, as shown in section 3.5. Central to this part is the work of Patrick Dehornoy, who studied braids and developed an efficient method for deciding whether two braids are **isotopes** of each other or not, i.e. if they can be turned from one into the other by deformations. The method that Dehornoy used is summarized here, and the algorithm is shown at the end. For further reading, we recommend his paper, [Dehornoy, 1997].

Dehornoy considers the generators of Artin's B_n group slightly differently from the way they are presented above. Indeed, Dehornoy considers the crossing precisely opposite, for all the σ_i's, as follows:

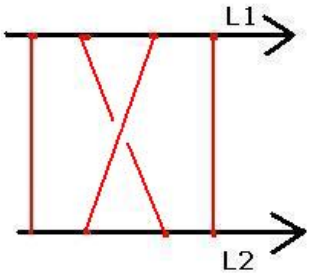


Figure 3.6: Dehornoy's σ_i

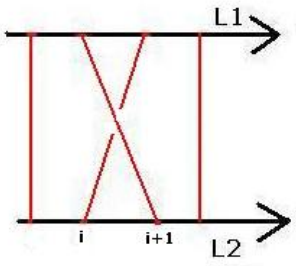


Figure 3.7: Dehornoy's σ_i^{-1}

This does not change the relations that Artin showed, regarding these generators. In view of this, we define a braid as a **word** involving **letters** of the form σ_i^k or σ_i^{-k}. Two such words are equivalent, by Artin's theory, if and only if an isomorphism can be found that preserves the characteristic generator equivalences:

$$\begin{aligned} \sigma_i\sigma_j &\equiv \sigma_j\sigma_i, \ |i-j| \geq 2 \\ \sigma_i\sigma_{i+1}\sigma_i &\equiv \sigma_{i+1}\sigma_i\sigma_{i+1} \end{aligned} \tag{3.8}$$

Dehornoy does not consider braid groups with a finite number of generators. Indeed, he refers in the case of his paper to what he names B_∞, namely the group generated by infinitely many generators under the conditions stated in 3.8. This generalization is used because the method described by Dehornoy is useful for any n, but it is better understood if infinitely many strands are used.

The paper presented by Dehornoy defines a few parameters for braid words. Thus, we denote the class of a word w by $\overline{w}$. $\overline{(w)}$ might be called a representative of its group class. We say that the word w is a decomposition for a braid β if β is in $\overline{w}$. We define, for every word, a **length**, which is the number of letters occurring in a word, and a **width**, which is the smallest domain to contain the non-trivial part of the word, meaning all the indexes between and including the lowest and the highest index of the generators in the word. Dehornoy notes that the width of a word which has a maximum difference between letter indices of $n-1$ is n. For instance, the braid word $\sigma_2\sigma_5\sigma_1^{-2}$. Here, we have a difference of 4, between 1 and 5 thus the width is 5.

We define **free reduction** as the operation that removes subwords of the form $\sigma_i \sigma_i^{-1}$; these words are referred to as **freely reduced**. We define **positive occurrences** the occurrences of letters of the form σ_i and **negative occurrences** the occurrences of inverses, of the form σ_i^{-1}. A **main generator** of a braid word w is the generator with the lowest index.

Dehornoy's work focuses on the introduction of an Noetherian ordering on braids. This is done by first defining an operation called **reduction**.

- **Definition:** (Present in [Dehornoy, 1997])

  We call a braid word w **reduced** either if it is the null string, or the empty braid, or if the main generator of w occurs only positively or only negatively. When the main generator occurs only positively, we speak of a **reduced decomposition of a positive type**; a **reduced decomposition of a negative type** refers then to the main generator occurring negatively.

Dehornoy founds his theory on this operation of reducing braid words. He states that there is no manner in which reduction would lead a non-empty word to the nullstring and that every braid admits decomposition. This can be reduced to saying that braids are only reduced in the true sense of the word, and not altered, by the decomposition. His reducing algorithms form inverse weaving patterns, by which the weaving patter, or word, in question is reduced to a simple form of the same braid class.

Having these aspects defined and stated, Dehornoy introduces an ordering on braids as follows:

- **Definition:** (Corollary 1.3 in [Dehornoy, 1997])

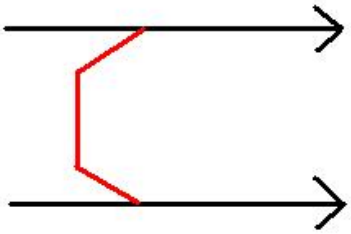
  For braids β and β', we say that $\beta < \beta'$ if and only if the braid $\beta^{-1}\beta'$ admits a reduced decomposition of positive type.

A first notice that we must make is that not all braids can be reduced.

If we now consider this order with $\beta = \beta'$ only if they are the same braid, we may say that $\leq$ is a partial order in the case of braids. Indeed, this ordering exhibits the following properties:

- *Reflexivity:* For a braid A, we have $A \leq A$.
- *Antisymmetry:* For two braids, A and B, if $A \leq B$ and $B \leq A$, then either $A = B$ or both $B^{-1}A$ and $A^{-1}B$ admit reduced decompositions of the positive type. Since they are inverses of each other, that is not possible, so it only follows that A must be equivalent to B.
- *Transitivity:* Let us assume that A, B, and C are all braids and that we have $A \leq B$ and $B \leq C$. This means that $B^{-1}A$ and $C^{-1}B$ both admit reduced decompositions of a positive type. It follows that the product of these two, $C^{-1}BB^{-1}A = C^{-1}A$ also admits a reduced decomposition of a positive type. Therefore, $A \leq C$.

The question is now how to reduce braids according to this order. Remembering free reduction, we now wish to consider a generalized reduction, when we eliminate any occurrences of the form $\sigma_i^1 ... \sigma_i^{-1}$ or $\sigma_i^{-1} ... \sigma_i^1$, for σ_i the main generator of the word. Dehornoy's method reduces words by eliminating what he calls **handle**. A left handle is for instance a strand with the following shape:



We can define a σ_j**-handle** as a braid of the form $\sigma_j^e v \sigma_j^{-e}$, where $e \in \{-1, +1\}$ and v is a word that does not contain as generators σ_j or σ_{j+1}. Dehornoy suggests the reduction of handles may be done with the aid of what he names a **local reduction**. This is a homomorphism $\phi_{j,e}$, defined by:

$$\begin{aligned} \phi_{j,e}(\sigma_j^{\pm 1}) &= \varepsilon \\ \phi_{j,e}(\sigma_{j+1}^{\pm 1}) &= \sigma_{j+1}^{-e} \sigma_j^{\pm 1} \sigma_{j+1}^{e} \\ \phi_{j,e}(\sigma_k^{\pm 1}) &= \sigma_k^{\pm 1} \end{aligned} \tag{3.9}$$

- *Example:*

  Consider a word $w = \sigma_1\sigma_2\sigma_3\sigma_2^{-1}\sigma_1^{-1}$. The only main handle in w is w itself, as the main generator of w is σ_1. Applying local reduction to w yields the braid word $\sigma_2^{-1} w \sigma_2$. Any repeated reductions will only give words of the form $\sigma_2^{-k} w \sigma_2^k$.

Dehornoy shows that the only possible problem that might occur if repeated reducing occurs is that what he names the **median factor** is not reduced. The **median factor** is defined as the factor between the first and the last appearances of the main generator. To this effect, Dehornoy defines **permitted handles** and deduction using **one step of handle reduction** as follows:

- **Definition:**

  A σ_j-handle $\sigma_j^e v \sigma_j^{-e}$ is **permitted** if it includes no σ_{j+1}-handle.

- **Definition:**

  The word w' is deduced from word w with **one step of handle reduction** if a single application of the homomorphism $\phi_{j,e}$ is needed for it.

By extension, a reduction using **N steps of handle reduction** is obtained by repeating the **one handle** process N times. Dehornoy notes that handle reduction is Noetherian, with a bound to the number of possible steps. This is shown in [Dehornoy, 1997]. One last definition now gives us equivalences between terminality and handles.

- **Definition:**

  The word w is **fully reduced** if at least one letter $\sigma_{j-1}^{\pm 1}$ separates σ_j and its inverse.

Lemma 15 *(Lemma 1.5 in [Dehornoy, 1997])*

For any braid word w we have equivalence between the following:

1. *w is fully reduced.*
2. *w contains no handle.*
3. *w is terminal with respect to handle reduction.*

The proof can be found in [Dehornoy, 1997]. Furthermore, he shows that any braid in the Artin B_n groups has a fully reduced decomposition of width n.

3.4 Dehornoy's Algorithms

Based on his methods, Dehornoy builds a few algorithms for different levels of reduction. These algorithms are presented, with the adequate definitions. Thus, section 3.4.1 presents full reduction, section 3.4.2 depicts a greedy algorithm for a partial reduction, and finally 3.4.3 explains convex reduction. For further explanations and reading, the reader is strongly recommended [Dehornoy, 1997].

3.4.1 Full Reduction

A full reduction is the reduction of all the main handles; because of the distinction between permitted and general handles, however, other handles are reduced in the process. We must also recall the process of free reduction, which can be considered as a 'free' action at the end of each reduction round. Dehornoy gives the following definition, therefore:

- **Definition:**

  We speak of **one step of HF-reduction** if the braid w' is obtained from w by reducing a permitted handle of w and then freely reducing the resulting word.

As such, Dehornoy formulates a first algorithm as follows:

- **Algorithm:**

  - Start with a braid word w.
  - HF-Reduce the left-most handle.
  - Repeat this process until a fully-reduced word is obtained.

Note: From the previous section, it is known that the word w' that is obtained after this process is equivalent with the original word w. It is also known that w is trivial if and only if w' is the nullstring.

- *Example:*

  Let us consider the initial word $w_0 = \sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1\sigma_3^{-1}\sigma_2\sigma_1^2$. Successive reductions using the algorithm described above give the following (the handles that will be reduced are underlined):

  1. $\underline{\sigma_1^{-1}\sigma_2^{-1}\sigma_1}\ \sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1\sigma_3^{-1}\sigma_2\sigma_1^2$
  2. $\sigma_2\ \underline{\sigma_1^{-1}\sigma_2^{-1}}\sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1\ \sigma_3^{-1}\sigma_2\sigma_1^2$
  3. $\sigma_2^2\underline{\sigma_1^{-1}\ \sigma_2^{-1}\sigma_3\sigma_2}\ \sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_2\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_2\sigma_1^2$
  4. $\sigma_2^2\sigma_1^{-1}\sigma_3\sigma_2\sigma_3^{-1}\sigma_1^{-1}\ \underline{\sigma_2^{-1}\sigma_3^{-1}\sigma_2}\ \sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_2\sigma_1^2$
  5. $\sigma_2^2\sigma_1^{-1}\sigma_3\sigma_2\ \underline{\sigma_3^{-1}\sigma_1^{-1}\sigma_3}\ \sigma_2^{-1}\sigma_3^{-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_2\sigma_1^2$
  6. $\sigma_2^2\sigma_1^{-1}\sigma_3\sigma_2\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_1^{-1}\ \underline{\sigma_2^{-1}\sigma_3^{-1}\sigma_2}\ \sigma_1^2$
  7. $\sigma_2^2\sigma_1^{-1}\sigma_3\sigma_2\sigma_1^{-1}\sigma_2^{-1}\ \underline{\sigma_3^{-1}\sigma_1^{-1}\sigma_3}\ \sigma_2^{-1}\sigma_3^{-1}\sigma_1^2$
  8. $\sigma_2^2\sigma_1^{-1}\sigma_3\sigma_2\sigma_1^{-1}\sigma_2^{-1}\ \underline{\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_1}\ \sigma_1$
  9. $\sigma_2^2\sigma_1^{-1}\sigma_3\sigma_2\sigma_1^{-1}\ \underline{\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_1}$
  10. $\sigma_2^2\sigma_1^{-1}\sigma_3\sigma_2\sigma_1^{-1}\underline{\sigma_2\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}}$

3.4.2 Greedy Reduction

The full reduction algorithm is rather complex compared to, say, the needs of solving the word problem for braids, i.e. decide if two braids are equivalent. In this case simple reduction is needed only, and thus Dehornoy proposes what he names a 'greedy' algorithm for reducing words so they may easily be compared. Thus, only the main handles need to be reduced for these braid words; some secondary handles will need to be similarly reduced in order to permit the solving of the main handles.

- **Definition:**

  For a braid w assume that σ_i is its main generator. We name a σ_j-handle of w lying between positions p and q **nested** if we have a sequence of nested intervals:

$$(p_j, q_j) = (p, q) \subset (p_{j-1}, q_{j-1}) \subset \ldots \subset (p_i, q_i) \tag{3.10}$$

  such that the sub-word of w between p_k and q_k is a $\sigma_{i+k}handle$ for every k.

The subsequent algorithm is therefore:

- **Algorithm:**

  - Start with a braid word w.
  - HF-Reduce the left-most nested handle.
  - Repeat this process until a reduced word is obtained.

Note: The same note as in the previous subsection applies to this algorithm; the resulting braid word w' is equivalent to w and w is trivial if and only if w' is the nullstring.

- *Example:*

  Let us consider the initial word $w_0 = \sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1\sigma_3^{-1}\sigma_2\sigma_1^2$. Successive reductions using the algorithm described above give the following (the handles that will be reduced are underlined):

  1. $\underline{\sigma_1^{-1}\sigma_2^{-1}\sigma_1}\ \sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1\sigma_3^{-1}\sigma_2\sigma_1^2$
  2. $\sigma_2\ \underline{\sigma_1^{-1}\sigma_2^{-1}\sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1}\ \sigma_3^{-1}\sigma_2\sigma_1^2$
  3. $\sigma_2^2\sigma_1^{-1}\sigma_2^{-1}\sigma_3\sigma_2\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_2\sigma_1^{-1}\ \underline{\sigma_2^{-1}\sigma_3^{-1}\sigma_2}\ \sigma_1^2$
  4. $\sigma_2^2\sigma_1^{-1}\sigma_2^{-1}\sigma_3\sigma_2\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_2\ \underline{\sigma_1^{-1}\sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_1}\ \sigma_1$
  5. $\sigma_2^2\sigma_1^{-1}\sigma_2^{-1}\sigma_3\sigma_2\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_2\sigma_3\sigma_2\ \underline{\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_1}$
  6. $\sigma_2^2\sigma_1^{-1}\sigma_2^{-1}\sigma_3\sigma_2\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_2\sigma_3\sigma_2^2\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}$

3.4.3 Convex Reduction

The convex reduction is not, in itself, an algorithm, but a time-reduction of the previous algorithms. It is based on the fact that reducing handles may be done in any order and that, as Dehornoy states, it is not difficult to predict the effect of reducing off a certain permitted handle. A clever reduction, which Dehornoy compares to a convex hull, reduces the number of steps the algorithms need.

Firstly, however, we must consider the following terminology. For every braid w we define the unique (see [Dehornoy, 1997]), positive braid words $N_R(w)$ and $D_R(w)$ to be those words for which $N_R(w)D_R(w)^{-1}$ can be obtained from w using right reduction. Similarly, $N_L(w)$ and $D_L(w)$ are defined in the case of left reduction. We define furthermore $S(w)$ to be the set of all positive braid words equivalent to $D_L(w)N_R(w)$. Finally, the **rank** of w is the maximal number (taken over i) of letters σ_i^e in a σ_i-reduced word traced in $S(w)$.

Dehornoy's upper bound proposition is stated below:

Proposition 16 *(Proposition 4.2 in [Dehornoy, 1997])*

Considering a length l, a width n, and a rank r of a braid word w, the convex versions of the Full Reduction and Greedy Reduction algorithms return reduced words (sometimes even fully reduced words) in a maximum of $l(2r)^{n+1}$ steps.

3.5 Braids and Cryptography

Knots, as described in chapter 1, behave much like numbers and discrete logarithms. That, coupled with the fact that knot theory is not well known, makes knots a rather difficult instrument in encryption/decryption. This does not apply to braids. Indeed, Marc Girault, Jean-Francois Misarsky, Patrick Dehornoy, and Herve Silbert ([US Patent, 2004]) have already forwarded a patent application publication on braids-based cryptography.

Much like with Elliptic Curve Cryptography, this application is based on the fact that, for instance, knowing a braid $T(S) = S^p$, with p an integer, it is very difficult to reverse the operation, that is to find a representative of the braid S. In order to understand the algorithm of this invention, it is important to recall a few details about braids.

Each braid consists of infinitely many weaving patterns, isomorphic with one another by means of deformations. We name one such weaving patterns a representative of a braid. The representatives of the neutral braids are named **pure braids**.

The cryptography method consists of a secret key defined by a representative s of a braid S, a public key identifiable with a representative of the braid $T(S)$, where T is an operator defined, for instance, as above, and a method of finding whether two braid representatives are equivalent or not.

There are two definitions of the operator T given in the patent application [US Patent, 2004]. One such definition is the one given above, with $T(S) = S^p$, $p \geq 2$. Another is $T(S) = SWS^{-1}$, where W is a braid in a group G_m, with representative w. We are speaking now of conjugacy. The problem of finding a representative for the braid S once a representative v of the conjugate braid $V = T(S)$ is known is also rather difficult to solve.

The attention is now recalled to Dehornoy's algorithms, as described in section 3.3. Reducing braids according to Dehornoy's methods provide a method of comparing braids relatively easily. This is necessary for the decryption of any cryptographic scheme proposed on the basis of braid groups.

The patent application [US Patent, 2004] is very general in that it does not necessarily give more specific information about exactly the method employed. Some methods, are, however, mentioned as examples, since the generality of the application allows for numerous cryptography methods. Two of these are described below.

3.5.1 An outline of a first method

This method is set within the group G_x of braids containing braids on $n = p + q$ strands. We have $G_x \subset G_n$ Two types of braids are considered within this group: those that use only the first p left-hand strands, and can therefore be generated by $p - 1$ generators and their inverses, and braids that use only the last q right-hand strands, generated by $q - 1$ generators and their inverses. Because they have no strands in common, it is easy to show that a p-braid commutes with a q-braid.

Consider now the users Alice and Bob, in short A and B. A wishes to send a message to B; for this, A has as secret key a representative s of a p-braid S. The public key is a pair (v, w). Herein, w is the representative of a braid $W \in G_x$ and v is a representative of $V = T(S) = SWS^{-1}$.

Authentication is now achieved by means of two exchanges.

1. B takes a representative z of a q-braid Z. B then calculates a representative of the braid $C = ZWZ^{-1}$. He chooses a representative, c, (for the sake of security, this second representative is generally chosen to be different from the first representative) of the same braid and sends it to A.

2. A calculates a representative y of the braid $Y = SCS^{-1}$ by using the received representative of C, namely c. A sends this result to B. B verifies the equivalence $Y \sim ZVZ^{-1}$.

In [US Patent, 2004], it is stipulated that equivalence results from the commutativity of S and Z, which results in:

$$Y = SCS^{-1} = S(ZWZ^{-1})S^{-1} = ZS(W)S^{-1}Z^{-1} = ZVZ^{-1} \tag{3.11}$$

The equivalence is easily verified by means of Dehornoy's method. In this method, it is not necessary, but it might be recommendable to choose reduced form representatives of C and of Y. Similarly, a pure braid is preferable for W.

- *Example:*

  Let us take the example of $G_x \subset G_5$, with $p = 3$ and $q = 2$. A picks a representative of a p-braid $S = \sigma_1\sigma_2$. The key is a double (V, W), with $W = \sigma_2\sigma_4$ and $V = \sigma_1\sigma_2\sigma_2\sigma_4\sigma_2^{-1}\sigma_1^{-1}$. By recalling the two basic properties of braid generators, we may shorten this to $V = \sigma_1\sigma_2\sigma_4\sigma_2\sigma_2^{-1}\sigma_1^{-1} = \sigma_1\sigma_2\sigma_4\sigma_1^{-1}$

  B takes a representative of the q-braid $Z = \sigma_4$ and sends a representative of $C = \sigma_4\sigma_2\sigma_4\sigma_4^{-1} = \sigma_4\sigma_2$.

  A calculates a representative of $Y = \sigma_1\sigma_2\sigma_4\sigma_2\sigma_2^{-1}\sigma_1^{-1} = \sigma_1\sigma_2\sigma_4\sigma_1^{-1}$ and sends it over to B.

  B now has a positive authentication of A.

3.5.2 An outline of a second method

The second authentication protocol considers a group G_{x2} of braids on n strands. This protocol consists of k iterations of a three-message exchange, each iteration giving a chance in two for the detection of an impostor (or eavesdropper) C. After k steps, the chance of C to pass undetected is one in 2^k.

The authors of the patent application [US Patent, 2004] denote this class of protocols by the term **zero-knowledge protocols**.

This system consists of the same elements as the previous protocol, namely the secret key s and the authentication pair (v, w). The protocol, however, is modified to three steps.

1. A selects a braid R and holds a representative r of it. A then keeps a representative of the braid $X = RWR^{-1}$. A representative (for the sake of security, it is preferable that the representative is different) of this same braid, x, is then sent to B.

2. B draws a bit at random, c, and sends it to A.

3. This step has two substeps:

   - a If $c = 0$, then A sends $y = r$ to B. B then verifies $x \sim ywy^{-1}$

   - b If $c = 1$, A calculates a representative y of RS^{-1} and sends y over. B verifies $x \sim yvy^{-1}$ by Dehornoy's Reduced Form method.

The equivalence in 3*a* can be shown by recalling that:

$$YVY^{-1} = (RS^{-1})SWS^{-1}(SR^{-1}) = RWR^{-1} \tag{3.12}$$

Braid equivalence is again found by using Dehornoy's method (3.3). It is recommendable to use reduce forms for the braid representatives exchanged between the two users.

- *Example:*

  Let us consider the example with $k = 2$ and $n = 5$. We assume $S = \sigma_1$ and $W = \sigma_2\sigma_4$. Then $V = \sigma_1\sigma_2\sigma_4\sigma_1^{-1}$. The public key is (V, W)

  A takes a representative $R = \sigma_1\sigma_2$ and sends a representative of the braid $X = \sigma_1\sigma_2\sigma_2\sigma_4\sigma_2^{-1}\sigma_1^{-1}$ to B. By relation 1 regarding braid generators, we have: $X = \sigma_1\sigma_2\sigma_4\sigma_2\sigma_2^{-1}\sigma_1^{-1} = \sigma_1\sigma_2\sigma_4\sigma_1^{-1}$.

  In the first round, B chooses $c = 0$ and sends it to A. A sends $Y = R = \sigma_1\sigma_2$ to B. B verifies that $YWY^{-1} = \sigma_1\sigma_2\sigma_2\sigma_4\sigma_2^{-1}\sigma_1^{-1} = \sigma_1\sigma_2\sigma_4\sigma_2\sigma_2^{-1}\sigma_1^{-1} = \sigma_1\sigma_2\sigma_4\sigma_1^{-1}$ is indeed equivalent to the representative of X they received. The first, partial authentication is completed, with the eavesdropper C having only one chance in 2 to guess the bit that was sent.

  In the second round, B chooses 1. In this case, $Y = RS^{-1} = \sigma_1\sigma_2\sigma_1^{-1}$ is sent from A back to B. B completes and accepts authentication because $YVY^{-1} = \sigma_1\sigma_2\sigma_1^{-1}\sigma_1\sigma_2\sigma_4\sigma_1^{-1}\sigma_1\sigma_2^{-1}\sigma_1^{-1} = \sigma_1\sigma_2^2\sigma_4\sigma_2^{-1}\sigma_1^{-1} = \sigma_1\sigma_2\sigma_4\sigma_2\sigma_2^{-1}\sigma_1^{-1} = \sigma_1\sigma_2\sigma_4\sigma_1^{-1}$ is identical to X. The eavesdropper has now only one chance in $4 = 2^2$ to break the code.

Chapter 4

Suggested Extensions and Improvements

Of the two subjects described by the present paper, the part about braids includes the most unknowns. It is in this area that most further inquiries are suggested. The list below may be expanded upon at free will.

- The concept of **knot** is introduced in chapter 1. It would be interesting to investigate exactly how far the theory of knots influences braids and viceversa.
- Knots and braids are connected to handlebodies and manifolds. A suggestion would be to present this subject further and show the connection between these subjects.
- It would be interesting to analyze the groups defined by braid generators with the additional conditions of $\sigma_i^3 = 1$ for the generators σ_1, σ_2, σ_3, and σ_4.

Bibliography

[Artin, 1965] Emil Artin, Serge Lang, John T. Tate "The Collected Papers of Emil Artin", Addison-Wesley Publishing Company Inc., 1965

[Serre, 1977] J.-P. Serre, "Linear Representations of Finite Groups", Springer-Verlag, 1977

[Artin, 1991] Michael Artin, "Algebra", Prentice Hall, 1991

[Rotman,1995] Joseph J. Rotman, "An Introduction to the Theory of Groups", Springer-Verlag, 1995

[KnotTheory] http://www.freelearning.com/knots/history.htm

[US Patent, 2004] US Patent 2004/0240672 A1, Marc Girault, Jean-Francois Misarsky, Patrick Dehornoy, Herve Silbert, Public Key Cryptografic Method Based on Braid Groups

[Dehornoy, 1997] Patrick Dehornoy, "A Fast Method for Comparing Braid Groups", Advances in Mathematics, No. 125, pages 200-235, 1997, also to be found at http://www.math.unicaen.fr/~dehornoy/Papers/Dfo.pdf

[Cohen, 1980] A. M. Cohen and H. A. Wilbrink "Eindige Groepen", Mathematisch Centrum Amsterdam, 1980.

Appendix A

Character Tableaux of S_3 and S_4

A.1 S_3

χ	1	(12)	(123)
χ_0	1	1	1
χ_1	1	-1	1
χ_2	2	0	1

A.2 S_4

χ	1	(12)	(123)	(1234)	(12)(34)
χ_0	1	1	1	1	1
χ_1	1	-1	1	-1	1
χ_2	2	0	-1	0	0
χ_3	3	1	0	-1	-1
χ_4	3	-1	0	1	-1