Publicaciones Electrónicas
Sociedad Matemática Mexicana

An Introduction to Group Theory with applications to Mathematical Music Theory

Flor Aceff-Sánchez
Octavio A. Agustín-Aquino
Janine du Plessis
Emilio Lluis-Puebla
Mariana Montiel

www.smm.org.mx

Serie: Textos. Vol. 15 (2012)

An Introduction to Group Theory with applications in Mathematical Music Theory

Flor Aceff-Sánchez
Universidad Nacional Autónoma de México

Octavio A. Agustín-Aquino
Universidad de la Cañada

Janine du Plessis
Georgia State University

Emilio Lluis-Puebla
Universidad Nacional Autónoma de México

Mariana Montiel
Georgia State University

Contents

List of Figures

Preface

The success of Group Theory is impressive and extraordinary. It is, perhaps, the most powerful and influential branch of all Mathematics. Its influence is strongly felt in almost all scientific and artistic disciplines (in Music, in particular) and in Mathematics itself. Group Theory extracts the essential characteristics of diverse situations in which some type of *symmetry* or *transformation* appears. Given a non-empty set, a binary operation is defined on it such that certain axioms hold, that is, it possesses a structure (the group structure). The concept of structure, and the concepts related to structure such as isomorphism, play a decisive role in modern Mathematics.

The general theory of structures is a powerful tool. Whenever someone proves that his objects of study satisfy the axioms of a certain structure, he immediately obtains all the valid results of the theory for his objects. There is no need to prove each one of the results in particular. Indeed, it can be said that the structures allow the classification of the different branches of Mathematics (or even the different objects in Music (!)).

The present text is based on the book in Spanish "Teoría de Grupos: un primer curso" by Emilio Lluis-Puebla, published by the Sociedad Matemática Mexicana This new text contains the material that corresponds to a course on the subject that is offered in the Mathematics Department of the Facultad de Ciencias of the Universidad Nacional Autónoma de México plus optional introductory material for a basic course on Mathematical Music Theory.

This text follows the approach of other texts by Emilio Lluis-Puebla on Linear Algebra and Homological Algebra. A modern presentation is chosen, where the language of commutative diagrams and universal properties, so necessary in Modern Mathematics, in Physics and Computer Science, among other disciplines, is introduced.

This work consists of four chapters. Each section contains a series of problems that can be solved with creativity by using the content that is presented there; these problems form a fundamental part of the text. They also are designed with the objective of reinforcing students' mathematical writing. Throughout the first three chapters, representative examples (that are not numbered) of

applications of Group Theory to Mathematical Music Theory are included for students who already have some knowledge of Music Theory.

In chapter 4, elaborated by Mariana Montiel, the application of Group Theory to Music Theory is presented in detail. Some basic aspects of Mathematical Music Theory are explained and, in the process, some essential elements of both areas are given to readers with different backgrounds. For this reason, the examples follow from some of the outstanding theoretical aspects of the previous chapters; the musical terms are introduced as they are needed so that a reader without musical background can understand the essence of how Group Theory is used to explain certain pre-established musical relations. On the other hand, for the reader with knowledge of Music Theory only, this chapter provides concrete elements, as well as motivation, to begin to understand Group Theory.

The last four authors give a special acknowledge for the valuable help in the English edition to Dr. Flor Aceff-Sánchez who, in spite of her delicate health, put all her dedication and love in the elaboration of this text with many mathematical and musical comments. Without her, this text would never have come to life.

Flor Aceff-Sánchez
Universidad Nacional Autónoma de México

Octavio A. Agustín-Aquino
Universidad de la Cañada

Janine du Plessis
Georgia State University

Emilio Lluis-Puebla
Universidad Nacional Autónoma de México

Mariana Montiel
Georgia State University

Introduction

Mathematics exist from the initial stages of human existence. Practically every human being is a mathematician in some sense, from those that use mathematics to those that discover and create new mathematics. Everybody is also, to a certain extent, a philosopher of mathematics. Indeed, everyone who measures, recognizes people or things, counts, or says "as clear as two plus two is four" are mathematicians or philosophers of mathematics. However, only a very small number of people specialize in creating, teaching, researching or popularizing mathematics.

Mathematics is a pillar and foundation of our civilization. From the first half of the XIX century, due to the progress in different areas, mathematical sciences were unified, and the name of "Mathematics" as a single discipline was justified. According to the philologist Arrigo Coen, *mathema* means "erudition", *manthánein* is the infinitive "to learn", the root *mendh* means, in the passive tense, "knowledge". In other words, it is the relative to learning. In an implicit sense, Mathematics means "what is worth learning". It is also said that Mathematics is "a science par excellence".

However, it can also be said that there are very few people that posses correct and up-to-date information about the branches and sub-branches of Mathematics. Children and young adults of our time can have good approximated images of electrons, galaxies, black holes, the genetic code, etc. Nevertheless, they will find, with difficulty, mathematical concepts that go beyond the first half of the XIX century. This is due to the nature of mathematical concepts.

It is a very common belief that a mathematician is a person who carries out enormous sums of natural numbers during every day of his life. It is also true that people suppose that a mathematician knows how to add and multiply natural numbers at a great speed. If we think a little about the concepts that the majority of people have about mathematicians, we could reach the conclusion that mathematicians are not necessary, given that a pocket calculator can carry out this work.

When one asks "what is the difference between a mathematician and an accountant?", it is considered equivalent to the question "what is the difference between x and x?". That is, it is supposed that they do the same. If it is explained that only on rare occasions does a mathematician carry out sums or multiplications, it seems incredible. It also appears incredible that a great

number of advanced mathematics texts will not usually use numbers bigger than 10, with the exception, perhaps, of the page numbers.

During many years, the emphasis has been on teaching children to learn multiplication tables, on the calculation of enormous additions, subtractions, multiplications, divisions and square roots, but of very small numbers (as far as big numbers, the majority of people have little idea of their magnitude). After, as teenagers, those that could sum and multiply polynomials were considered geniuses by their classmates, in possession of a great mathematical talent and afterwords, if they were lucky, they were taught to add and multiply complex numbers.

It would seem, then, that a mathematician is a person that passes his life doing addition and multiplication (of small numbers), something like the person in charge of the banking aspect of a business. This impression exists in the majority of people. Nothing further than the truth. Mathematicians are not those who calculate or do arithmetic operations, but those who invent how to calculate or do operations. To do Mathematics is to imagine, to create, to reason.

To be able to count, it was somehow necessary to represent numbers, for example, with the fingers. Then the abacus embodied a step forward, although still tied to counting with the fingers, and is still used in some parts of the planet. Afterwards, the arithmetic machine that was invented by Pascal in 1642 allowed people to carry out addition and subtraction through a very ingenious system of gears. Today, the pocket calculators allow us to carry out, in seconds, calculations that would have taken years to do before, and have also allowed us to get rid of the logarithm tables and the slide rule.

However, in general, the students and graduates of any area will respond to the question "what is the sum?", or rather "what is addition?", by shrugging their shoulders, in spite of having spent twelve years doing sums, and that the sum is a primitive concept. It is also common that when a child, or a young person or an adult with a professional degree confronts a problem, he does not know whether to add, subtract, multply or cry.

The concept of binary operation, or law of composition, is one of the oldest in Mathematics and goes back to the ancient Egyptians and Babylonians [B] who already had methods to calculate addition and multiplication of positive integers and positive rational numbers (remember that they did not use the number system that we use). However, as time went on, mathematicians realized that the most important aspects were not the tables for adding or multplying certain "numbers", but the set itself and the binary operation defined on it. The binary operation, together with certain properties that must be satisfied, gave way to the fundamental concept of group.

Historically, the concept of binary operation, or law of composition, was extended in two ways, in which we can only find a certain resemblance with the numerical cases of the Egyptians and Babylonians [B].The first was by Gauss, when he studied quadratic forms with integer coefficients, and when he saw that the law of composition was compatible with particular equivalence classes. The second culminated in the concept of group, in the Theory of Substitutions (by

means of the development of the ideas of Lagrange, Vandermonde and Gauss in the solution of algebraic equations). However, these ideas remained superficial, with Galois being the real pioneer of Group Theory when he reduced the study of algebraic equations to the study of the permutation groups associated to them.

The English mathematicians of the first half of the XIX century isolated the concept of law of composition and extended the area of Algebra by applying it to Logic (Boole), vectors and quaternions (Hamilton) and matrices (Cayley). By the end of the XIX century, Algebra was focused on the study of algebraic structures, leaving behind the interest for the applications of the solutions to numerical equations. This orientation gave way to three fundamental trends [B]:

(i) Number Theory, that emerged from the German mathematicians Dirichlet, Kummer, Kronecker, Dedekind and Hilbert, based on the work of Gauss. The concept of field was fundamental.

(ii) The creation of Linear Algebra in England by Sylvester, Clifford; in the United States by Pierce, Dickson, Wedderburn; and in Germany and France by Weirstrass, Dedekind, Frobenius, Molien, Laguerre, Cartan.

(iii) Group Theory that, in the beginning, was focused on the study of permutation groups. It was Jordan who developed the work of Galois, Serret and other predessesors. He introduced the concept of homomorphism and was the first to study infinite groups. Later, Lie, Klein and Poincaré developed these studies considerably. Finally, it was seen that the fundamental and essential idea of group lay in its law of composition, or binary operation, and not in the nature of its objects.

The success of Group Theory is impressive and extraordinary. It suffices to mention its influence in almost all of Mathematics and in other areas of knowledge. The examples given in 1.1 could leave the non-mathematician perplex, with a false idea about the hobbies that mathematicians create, consisting of combining "numbers" in a strange perverse way. However, the examples considered in this section are vitally important for Number Theory (the number 3 can be replaced by any natural number n - if $n = 12$ we obtain clock arithmetic - or by a prime number p, obtaining important concepts and results), for Group Theory itself (dihedral or symmetric groups) or for Music, in relation to the chromatic scale. By observing this, it can be seen that what really is done in Group Theory, is extract the essential aspects from these examples, that is, given a non-empty set, we define a binary operation on it, such that certain axioms, postulates or properties hold, in other words, they possess a structure (the group structure). There exist several concepts linked to that of structure, one of the most important being isomorphism.

The concept of structure and those concepts related to it, such as isomorphism, play a decisive role in contemporary Mathematics. The general theories of the important structures are very powerful tools. Whenever someone proves that his objects of study satisfy the axioms of a certain structure, he immediately obtains all the valid results of the theory for his objects. There is no need to prove each one of the results in particular. One use of structures and

isomorphisms made in modern Mathematics is the classification of its different branches (the nature of the objects is not important, the essential aspect are their relations to each other).

In the Middle Ages, Mathematics was classified as Arithmetic, Music, Geometry and Astronomy, which composed the Quadrivium. Afterwards, and until the middle of the XIX century, the branches of Mathematics were distinguished by the objects they studied, for example, Arithmetic, Algebra, Analytic Geometry, Analysis, with some subdivisions. It was as if we said that, given that bats and eagles fly, they must both be birds. We now can see beyond the surface and extract the underlying structures from the mere appearance.

Currently there are 63 branches of mathematics with over 5000 sub-classifications. Among them are Algebraic Topology (composite structures), Homological Algebra (purification of the interaction between Algebra and Topology, created in the fifties), and Algebraic K-Theory (one of the most recent branches, created in the seventies).

The idea of the connection between Mathematics and Music has been present historically and the scope of this connection has been broadened significatively since it was made explicit, for the first time, by Pythagoras of Samos. Chapter 4 presents a facet of the modern development of Mathematical Music Theory, based in its transformational nature. In this context, Group Theory plays the role of protagonist.

The foundations of this application can be attributed, in particular, to David Lewin, who developed Transformational Theory and gave rise to a new form of music theory, designed for the analysis of modern music. This new theory is known as Neo-Riemannian Theory.

Neo-Riemannian Theory is inspired in the work of the German musical theorist Hugo Riemann, who contributed to the effort to establish relations between tones and intervals. The need of this change arose from the industrial, political and social changes that ocurred during the XIX century. It was inevitable that they would exercise an important effect on the music of that time, and these changes were frequently expressed by means of bold modulations, innovative chord progressions, dissonance and resolutions and, in general, much less preparation for abrupt changes. These radical transformations gave rise, in music, to postromanticism and, finally, to atonality. Naturally, tonal theory in music could not explain these developments, and new tools had to be contructed to analyze and explain the evolution of this music; thus the birth of Neo-Riemannian Theory.

While Riemann was fundamentally interested in substituting the existing system of chord labelling and musical events at the time, Lewin saw the potential of these labels to describe the movement between these musical events. Lewin's work takes form in his extensive contribution to the definition of the operations that describe musical movement (that is,Transformational Theory) and, going even further, he applied Group Theory to Music. These sets of transformation not only form groups, but they are isomophic to each other and to the dihedral group. What's more, they satisfy several properties that allow us to conclude that duality exists.

Some people think that Mathematics is only a game that interests the intellect in a detached, cold way. Poincaré affirmed that this way of thinking does not take into account the sensation of mathematical beauty, of the harmony of numbers and shapes, as well as geometric elegance. There is, certainly, a sensation of aesthetic pleasure that every real mathematician has felt and, of course, belongs to the category of sensitive emotions. The beauty and elegance of Mathematics consists of all the elements harmonically displayed such that our mind can embrace their totality while maintaining, at the same time, their details.

This harmony, continues Poincaré, is an immediate satisfaction of our aesthetic needs, and a help that sustains and guides the mind. At the same time, by placing an ordered totality in our sight, we can make out a mathematical law, or truth. This is the aesthetic sensitivity that plays the role of a delicate filter, which, Poincaré concludes, explains why the person that does not have will never be a true creator.

For the authors of this text, Mathematics is one of the Fine Arts, the purest of them, that has the gift of being the most precise, and the precision of the Sciences.

Chapter 1

1.1 Binary Operations

In this section we present one of the oldest concepts in Mathematics, the *binary operation* or *law of composition*. We will also see to what extent certain "popular sayings", for example "as clear as two plus two is four" and "the order of the factors does not change the product", are true.

We will review some elementary concepts.
First, recall the set of integers.

$$\mathbb{Z} = \{... - 5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, ...\}$$

Second, ask yourself: - how are two sets "properly" related"? Let A and B be two arbitrary sets. We say that $f : A \longrightarrow B$ is a **function** of A to B if, to each element of A, we associate a *unique* element of B.

For example, if $A = \{a, b, c\}$ and $B = \{p, q, r, s\}$ then $f : A \longrightarrow B$ given by the following association

$$\begin{array}{ccc} a & \longmapsto & p \\ b & \longmapsto & q \\ c & \longmapsto & r \end{array}$$

is a function, while the association

$$\begin{array}{ccc} a & \longmapsto & p \\ a & \longmapsto & q \\ b & \longmapsto & q \\ c & \longmapsto & r \end{array}$$

is not a function, given that we do not associate to an object A a unique element of B, (p and q are associated to a). The sets A and B are called, respectively, the **domain** and the **codomain** of the function f.

The subset of the codomain that consists of those elements associated to the domain is called the **range** of f. Thus, in the previous function, the range of f is the set $\{p, q, r\}$; the element s of B is not in the range of f, that is, it is not the image of any element of A under f.

We use the following notation to denote the images of the elements of A under f:

$$\begin{array}{rccc} f: & A & \longrightarrow & B \\ & a & \longmapsto & f(a) = p \\ & b & \longmapsto & f(b) = q \\ & c & \longmapsto & f(c) = r \end{array}$$

Third: consider the Cartesian product of a set A, denoted by $A \times A$, that consists of all ordered pairs of elements of A, that is,

$$A \times A = \{(a, b) | a, b \in A\}$$

Now we can define the important concept of binary operation, or law of composition. Let G be a non-empty set. A **binary operation** or **law of composition** on G is a function $f : G \times G \longrightarrow G$ where $(x, y) \longmapsto f(x, y)$.

It is obvious that we can denote a function with any symbol, for example $f, g, h, \blacklozenge, \blacktriangle, \clubsuit, \heartsuit, \times, \otimes, *$, etc. Hence, in $\mathbb{Z}$, we can have a binary operation

$$\begin{array}{rccc} f: & \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & (x, y) & \longmapsto & f(x, y) \end{array}$$

and, by abuse or convenience of notation, we can denote $f(x, y)$ as xfy. For example, $(3, 2) \longmapsto f(3, 2) = 3f2$.

If the binary operation f is denoted as $+$ (the usual sum in $\mathbb{Z}$) then $(3, 2) \longmapsto +(3, 2) = 3 + 2$ is equal to 5. If the binary operation f is denoted as $\cdot$ (the usual multiplication in $\mathbb{Z}$), then $(3, 2) \longmapsto \cdot(3, 2) = 3 \cdot 2$ is equal to 6. Observe that a binary operation is defined on a non-empty set G.

1.1 Example. Define a set in the following way: consider three boxes and distribute the integers in each box in an ordered way:

$\vdots$	$\vdots$	$\vdots$
-6	-5	-4
-3	-2	-1
0	1	2
3	4	5
6	7	8
9	10	11
$\vdots$	$\vdots$	$\vdots$

[0]	[1]	[2]

We will denote the boxes as follows: the first one as [0] because it contains zero, (or $0 + 3\mathbb{Z}$, that is, the multiples of 3), the second [1] because it contains the number one (or $1 + 3\mathbb{Z}$, that is, all multples of 3 plus 1), and the third box [2] because it contains the number two (or $2 + 3\mathbb{Z}$, that is, all multiples of 3 plus 2). We will assign the number 0 to the box [0] , because its elements have a remainder of 0 when divided by 3; analogously, we assign the number 1 to the box [1], and the number 2 to the box [2] , given that their elements have remainders 1 and 2 respectively when divided by 3. Consider the set $\mathbb{Z}_3 = \{0, 1, 2\}$ called **the complete set of remainders module** 3, because when dividing by 3 we get remainders $0, 1$ or 2. Define a binary operation that could be denoted by $f, g, h, \blacklozenge, \blacktriangle, \clubsuit, \heartsuit, \times, \otimes, *$, etc; we choose $+$. Thus,

$$+ : \mathbb{Z}_3 \times \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$$

with

$$(1,1) \longmapsto +(1,1) = 1 + 1 = 2$$

$$(0,1) \longmapsto +(0,1) = 0 + 1 = 1$$

$$(1,0) \longmapsto +(1,0) = 1 + 0 = 1$$

$$(2,1) \longmapsto +(2,1) = 2 + 1 = 0$$

$$(2,2) \longmapsto +(2,2) = 2 + 2 = 1$$

We write its addition table:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Let us examine another

1.2 Example. Consider the complete set of remainders modulo 5, that is, the possible remainders obtained by dividing any number by 5, which we will denote as $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Draw the boxes. Define a binary operation on $\mathbb{Z}_5$

$$\cdot : \mathbb{Z}_5 \times \mathbb{Z}_5 \longrightarrow \mathbb{Z}_5$$

in the following way:

$$\begin{array}{lcl} (2,2) & \longmapsto & \cdot(2,2) = 2{\cdot}2 = 4 \\ (2,1) & \longmapsto & \cdot(2,1) = 2{\cdot}1 = 2 \\ (2,3) & \longmapsto & \cdot(2,3) = 2{\cdot}3 = 1 \\ (3,4) & \longmapsto & \cdot(3,4) = 3{\cdot}4 = 2 \end{array}$$

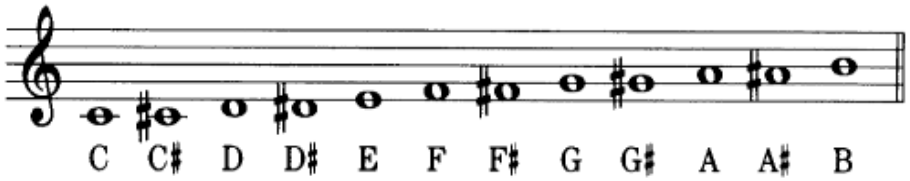


Figure 1.1: The chromatic scale

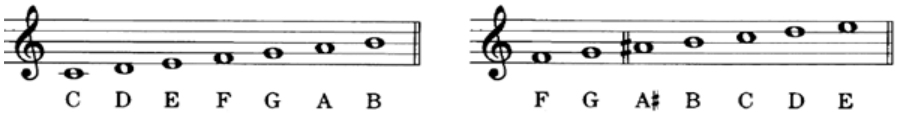


Figure 1.2: The C major (left) and F major (right) scales

Example. In Mathematical Music Theory it is very useful to interpret the chromatic equal tempered scale (figure 1.1) as the group $\mathbb{Z}_{12}$, with the associations

$$\begin{aligned} &\mathrm{C} \mapsto 0, \mathrm{C}\sharp \mapsto 1, \mathrm{D} \mapsto 2, \mathrm{D}\sharp \mapsto 3, \\ &\qquad \mathrm{E} \mapsto 4, \mathrm{F} \mapsto 5, \mathrm{F}\sharp \mapsto 6, \mathrm{G} \mapsto 7, \\ &\qquad\qquad \mathrm{G}\sharp \mapsto 8, \mathrm{A} \mapsto 9, \mathrm{A}\sharp \mapsto 10, \mathrm{B} \mapsto 11, \end{aligned}$$

if we are interested in the pitch of a note[1] without taking into account the octave[2] in which it is found.

This way it is easy to transpose melodies, scales or chords. For example, the C-major scale $\{\mathrm{C}, \mathrm{D}, \mathrm{E}, \mathrm{F}, \mathrm{G}, \mathrm{A}, \mathrm{B}\} = \{0, 2, 4, 5, 7, 9, 11\}$ can be transposed to the scale of F-major (figure 1.2) by adding 5 to each note. Explicitly, we have

$$\begin{aligned} &\{0+5, 2+5, 4+5, 5+5, 7+5, 9+5, 11+5\} \\ &\qquad = \{5, 7, 9, 10, 0, 2, 4\} = \{\mathrm{F}, \mathrm{G}, \mathrm{A}, \mathrm{A}\sharp, \mathrm{C}, \mathrm{D}, \mathrm{E}\}. \end{aligned}$$

It is common to hear the saying "as clear as two plus two is four". However, as we have seen in the previous examples, $2+2=1$, $2+1=0$, $2{\cdot}3=1$, $3{\cdot}4=2$, etc. and clearly $2+2 \neq 4$. In the previous examples we have considered the sets $\mathbb{Z}_3$ and $\mathbb{Z}_5$ on which we have defined a "sum" or binary operation. The

[1] **Pitch** is the perception that one has of the frequency of a sound. Fixed pitches are chosen in Music, so that they can be composed, such as in the case of the ones that make up the equal tempered scale. See chapter 4, section 1.

[2] An **octave** is the distance (or interval) that is percieved between a note and another with double (or half) its frequency. See chapter 4, section1.

usual sum in the natural and integer numbers is a binary operation, as is the multiplication defined on these sets. These are the binary operations considered in the saying. In the first years of school a special emphasis is made on the algorithms for adding and multiplying natural numbers(i.e. in the procedure or manner of adding and multplying these numbers). After several years emphasis is made on adding and multiplying integers, and on multiplying and dividing polynomials. In general, when one "adds", the set on which the binary operation is defined must always be specified.

It is also common to hear the saying that "the order of the factors does not change the product". Wll this always be true?

1.3 Example. Consider the set Δ_3 of the rigid movements of the equilateral triangle with vertices A, B, C, that is, the rotations about the baricenters of $0°$, $120°$ and $240°$ and the reflections about the medians. Denote these rigid movements in the following way:

$$0 = [ABC/ABC], 1 = [ABC/BCA], 2 = [ABC/CAB]$$

$$3 = [ABC/ACB], 4 = [ABC/CBA], 5 = [ABC/BAC]$$

The elements $0, 1$ and 2 correspond to the rotations. The elements $3, 4$ and 5 correspond to the reflections. Define a binary operation $\circ$ on Δ_3:

$$\begin{array}{rccc} \circ: & \Delta_3 \times \Delta_3 & \longrightarrow & \Delta_3 \\ & (x, y) & \longmapsto & \circ(x, y) = x \circ y \end{array}$$

Calculate:

$$[ABC/BCA] \circ [ABC/BCA] = [ABC/CAB]$$

that is

$$(1, 1) \longmapsto \circ(1, 1) = 1 \circ 1 = 2.$$

$$[ABC/CAB] \circ \ [ABC/ACB] = [ABC/BAC]$$

that is

$$(2, 3) \longmapsto \circ\,(2, 3) = 2 \circ 3 = 5.$$

$$[ABC/ACB] \circ \ [ABC/CAB] = [ABC/CBA]$$

that is

$$(3, 2) \longmapsto \circ\,(3, 2) = 3 \circ 2 = 4.$$

Observe that

$$2 \circ 3 \neq 3 \circ 2.$$

Now, $2 + 2 = 4$ and $2 \circ 3 = 3 \circ 2$?

The concept of binary operation, or law of composition, is one of the oldest in Mathematics and goes back to the ancient Egyptians and Babylonians who already had methods to calculate addition and multiplication of positive integers and positive rational numbers (recall that they did not use the number system

that we use). However, as time went on, mathematicians realized that the most important aspects were not the tables for adding or multplying certain "numbers", but the set itself and the binary operation defined on it. The binary operation, together with certain properties that must be satisfied, gave way to the fundamental concept of group.

We will say, in an informal manner that later on we will make precise, that a **group** is a non-empty set G together with a binary operation $f : G \times G \longrightarrow G$, denoted (G, f) which is associative, has an identity element and each member of the set has an inverse. The image of (x, y) in G will be denoted $(x, y) \longmapsto f(x, y)$. By abuse, or convenience of notation we will denote $f(x, y)$ as xfy and call it the **composition of** x and y.

It is easy to show (see the problems below) that the sets $\mathbb{Z}_3$, $\mathbb{Z}_5$ and Δ_3 with their respective binary operation, have a group structure. As can be seen in the case of $(\Delta_3, \circ)$, the group concept is closely linked to the concept of symmetry. The previous examples show some sets that posees a group structure, and how varied these can be.

We can define functions $f : G \longrightarrow G$, $g : G^2 = G \times G \longrightarrow G$, $h : G \times G \times G \longrightarrow G$ or $j : G^n = G \times ... \times G \longrightarrow G$ producing **unary operations**, **binary**, **ternary** or n**-ary**. The **null operation** is the function $i : \{e\} \longrightarrow G$.

An **algebraic structure** or **algebraic system** is a set C together with one or more n-ary operations. In the following section we will define some of them.

1.4 Definition. Consider H, a subset of a group $(G, \circ)$. We say that H es **stable** or **closed** with respect to the binary operation if $x \circ y \in H$, for all elements $x, y \in H$. Observe that the restriction of $\circ$ to a stable or closed subset H provides a binary operation for H called the **induced binary operation.** .

Problems

1.1 Construct a table that represents the multiplication of all the elements of $\mathbb{Z}_3$.

1.2 Construct a table that represents the sum of all the elements of $\mathbb{Z}_5$.

1.3 Construct a table that represents the multiplication of all the elements of $\mathbb{Z}_5$.

1.4 Show that Δ_3 with the binary operation defined in the Example 1.3 is a group.

1.5 Let Σ_3 be the set of all the permutations of $1, 2, 3$. Calculate the number of elements in Σ_3. Define a binary operation on Σ_3 and construct its table.

1.6 Let Σ_n be the set of all permutations of a set with n elements. Calculate the number of elements of Σ_n.

1.7 Construct a table that represents the sum of all the elements of $\mathbb{Z}_6$ and compare it with the tables Σ_3 and Δ_3. Observe that the tables of Σ_3 and Δ_3 are the same, except for the names and order of the elements. Show that these last two are groups and establish a bijective function between their elements. Observe that the table for $\mathbb{Z}_6$ allows you to show that it is a group, but that it is totally different from the other two.

1.2 Algebraic Structures

In this section we will define several algebraic structures, some of which already have been implicitly studied. The idea is to **present a brief panorama** of some of the algebraic structures (not the specific study of the category of groups), thereby situating the reader in a better position to understand the objects of study of Group Theory. We will suppose that the reader knows the foundations of Linear Algebra as in [Ll2] and we will use the same notation as used in that source.

Let $(V, +, \mu)$ be a vector space over a field K , as is defined in Linear Algebra. If we eliminate the scalar multiplication μ what remains is a set with a binary operation $+$, in which the four usual axioms hold. Then we say that $(V, +)$ is a **commutative group under** $+$. Formally, **with this notation and in this context** (in the next section we will give another, more general, definition of group) **we repeat** the definition of group given in the previous section, to connect it with the study of vector spaces.

2.1 Definition. A **group** is a pair $(G, +)$ where G is a non-empty set and

$$+\colon G \times G \to G$$

is a binary operation

$$(u, v) \longmapsto +(u, v)$$

and where, by convenience or abuse of notation we write

$$+(u, v) = u + v$$

such that

(i) $+(+(u, v), w) = +(u, +(v, w))$, that is, $(u + v) + w = u + (v + w)$

(ii) there exists an element $O \in G$, called the **identity element**, such that $+(v, O) = v + O = v$

(iii) for every $v \in G$ there exists an element, called **inverse**, denoted by $-v$, such that $+(v, -v) = v + (-v) = O$.

We say that a group is **commutative** if it also satisfies

(iv) $+(u, v) = +(v, u)$ that is, $u + v = v + u$.

If in the previous definition we consider a set E with a binary operation $+$ where none of the conditions hold, we say that $(E, +)$ is a **magma** (or **grupoid**).

If in the previous definition we consider a set S with a binary operation $+$ where (i) holds, we say that $(S, +)$ is a **semigroup**.

If in definition 2.1 we also consider a set M with a binary operation $+$ in which (i) and (ii) hold, we say that $(M, +)$ is a **monoid**.

2.2 Example. The set $\mathbb{N}$ of natural numbers with the usual sum is a semigroup but not a monoid because it has no identity element. $(\mathbb{Z},+)$ and $(\mathbb{Z}_n,+)$ (with $n \in \mathbb{N}$) are commutative monoids under the "sum" and $(\mathbb{N},\cdot),(\mathbb{Z},\cdot)$ and $(\mathbb{Z}_n,\cdot)$ are "multiplicative" monoids..

2.3 Example. The reader can prove that $(\mathbb{Z},+)$, $(n\mathbb{Z},+)$, $n \in \mathbb{Z}$, $(\mathbb{Q},+)$, $(\mathbb{Q}^* = \mathbb{Q}-\{0\},\cdot)$, $(\mathbb{R},+)$, $(\mathbb{R}^* = \mathbb{R}-\{0\},\cdot)$, $(\mathbb{C},+)$, $(\mathbb{C}^* = \mathbb{C}-\{0\},\cdot)$, $(\mathbb{Z}_n,+)$, $(\Delta_3,\circ)$, $(\Sigma_3,\circ)$, $(\Sigma_n,\circ)$, $(M_nK,+)$, where M_nK denotes the square matrices with $n\times n$ coefficients in a field K, $(GL_nK,+)$ and $(GL_nK,\cdot)$, where GL_nK denotes the square invertible matrices of dimension $n\times n$ ($n \in \mathbb{N}$) with coefficients in a field K, are groups (with the usual binary operations in each one of them).

Example. Composers frequently take a theme and apply different symmetries to it, to give variety to a musical creation.

Three common procedures are the **inversion** (I_s) respect to the pitch s, the **retrograde** (R) and the **retrograde with inversion** (RI_s). To fix ideas we define, provisionally, an n-**motive** as a sequence $\{x_i\}_{i=1}^n$ with $x_i \in \mathbb{Z}_{12}$ for evey i (taking into account the identification that we saw in the previous section). We denote as $\mathcal{T}(n)$ the set of all n-motives. We define the inversion, the retrogadation and the retrograde with inversion as

$$\begin{aligned} I_s : \mathcal{T}(n) &\mapsto \mathcal{T}(n), \\ \{x_i\}_{i=1}^n &\mapsto \{y_i = 2s - x_i\}_{i=1}^n, \end{aligned}$$

$$\begin{aligned} R : \mathcal{T}(n) &\mapsto \mathcal{T}(n), \\ \{x_i\}_{i=1}^n &\mapsto \{y_i = x_{n-i+1}\}_{i=1}^n, \end{aligned}$$

and

$$\begin{aligned} RI_s : \mathcal{T}(n) &\mapsto \mathcal{T}(n), \\ \{x_i\}_{i=1}^n &\mapsto \{y_i = 2s - x_{n-i+1}\}_{i=1}^n. \end{aligned}$$

Let s be a fixed pitch in the equal-tempered scale and $\{x_i\}_{i=1}^n \in \mathcal{T}(n)$. We see that

$$\begin{aligned} I_s \circ I_s(\{x_i\}_{i=1}^n) &= I_s(y_i = \{2s - x_i\}_{i=1}^n) \\ &= \{w_i = 2s - (2s - x_i)\}_{i=1}^n \\ &= \{w_i = 2s - 2s + x_i\}_{i=1}^n \\ &= \{w_i = x_i\}_{i=1}^n = \{x_i\}_{i=1}^n, \end{aligned}$$

that is, $I_s \circ I_s = \mathrm{id}_{\mathcal{T}(n)}$. In a similar way

$$\begin{aligned} R \circ R(\{x_i\}_{i=1}^n) &= R(\{y_i = x_{n-i+1}\}_{i=1}^n) \\ &= \{w_i = y_{n-i+1}\}_{i=1}^n \\ &= \{w_i = x_{n-(n-i+1)+1)}\}_{i=1}^n \\ &= \{w_i = x_{n-n+i-1+1}\}_{i=1}^n \\ &= \{w_i = x_i\}_{i=1}^n = \{x_i\}_{i=1}^n \end{aligned}$$

which indicates that $R \circ R = \mathrm{id}_{\mathcal{T}(n)}$. Finally,

$$\begin{aligned} I_s \circ R(\{x_i\}_{i=1}^n) &= I_s(\{y_i = x_{n-i+1}\}_{i=1}^n) \\ &= \{w_i = 2s - y_i\}_{i=1}^n \\ &= \{w_i = 2s - x_{n-i+1}\}_{i=1}^n = IR_s \\ &= \{w_i = y_{n-i+1}\}_{i=1}^n \\ &= R(\{y_i = 2s - x_i\}_{i=1}^n) = R \circ I_s(\{x_i\}_{i=1}^n) \end{aligned}$$

from where it can be concluded that

$$I_s \circ R = IR_s = R \circ I_s,$$

and also implies that

$$\begin{aligned} IR_s \circ IR_s &= (R \circ I_s) \circ (I_s \circ R) \\ &= R \circ (I_s \circ (I_s \circ R)) \\ &= R \circ ((I_s \circ I_s) \circ R) \\ &= R \circ (\mathrm{id}_{\mathcal{T}(n)} \circ R) \\ &= R \circ R \\ &= \mathrm{id}_{\mathcal{T}(n)}. \end{aligned}$$

the previous development shows that the composition of functions, when restricted to the subset

$$\mathcal{ST}_s = \{I_s, R, IR_s, \mathrm{id}_{\mathcal{T}(n)}\}$$

of the set of transformations of $\mathcal{T}(n)$ to itselfis closed. As the composition of functions is associative, it can be seen that $(\mathcal{ST}_s, \circ)$ is a group, whose identity is $\mathrm{id}_{\mathcal{T}(n)}$ and the inverses of I_s, R and IR_s are themselves.

For example, we can take the 5-motive

$$\{x_1 = \mathrm{A} = 9, x_2 = \mathrm{G} = 7, x_3 = \mathrm{F} = 5, x_4 = \mathrm{E} = 4, x_5 = \mathrm{G} = 7\}$$

that appears in the 29th bar of Fugue 6 in D minor from the first book of "Das Wohltemperierte Klavier" by J. S. Bach. If we invert it respect to the pitch $\mathrm{G} = 7$ (recalling that $2 \cdot 7 = 14 = 2$), obtenemos

$$\begin{aligned} \{y_1 = 2 - x_1 = 5, y_2 = 2 - x_2 = 7, \\ y_3 = 2 - x_3 = 9, y_4 = 2 - x_4 = 10, y_5 = 2 - x_5 = 7\} \end{aligned}$$

which is

$$\{y_1 = \mathrm{F}, y_2 = \mathrm{G}, y_3 = \mathrm{A}, y_4 = \mathrm{B}\flat, y_5 = \mathrm{G}\};$$

and is found in bar 33.

If we use retrogade, the resulting motive is $\{y_1 = \mathrm{G}, y_2 = \mathrm{E}, y_3 = \mathrm{F}, y_4 = \mathrm{G}, y_5 = \mathrm{A}\}$ (it is just the original, but backwards) that appears between bars 7

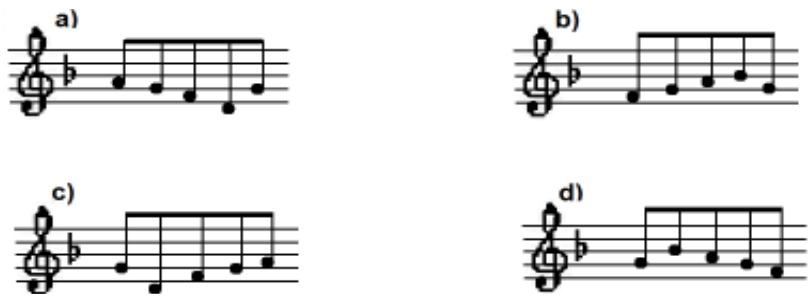


Figure 1.3: Motive with symmetries

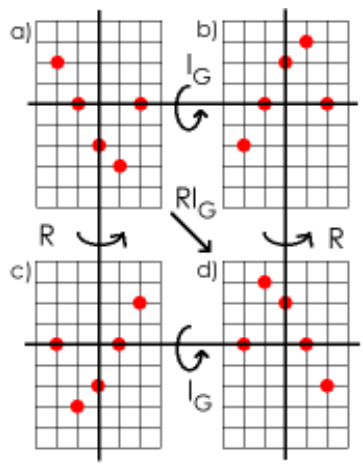


Figure 1.4: Geometric representation of the symmetries

and 8. If we apply a retrograde with inversion we obtain $\{y_1 = \mathrm{G}, y_2 = \mathrm{B}\flat, y_3 = \mathrm{A}, y_4 = \mathrm{G}, y_5 = \mathrm{F}\}$. A transposition of this set is seen in bar 36 of the work.

The transformations of the motive can be seen in the figure where **??**, a) is the original motive b) is its inversion with respect to G, c) is its retrograde and d) is its retrograde with inversion with respect to G. A more geometric presentation of Bach's motives is seen in the figure **??**.

recall that we denote the binary operation on a set with any symbol, for example $+, *, \circ, \diamond, \star, \theta, \bullet, \triangle$, etc, which is what we will do from here on. We say the the **order** of a group $(G, \cdot)$ is the number of elements of the set G and we will denote it with $o(G)$ or with $|G|$ indistinctly. Thus, the ways to write this are, for example: $(\mathbb{Z}_n, +)$ has order n, $o(\Delta_3, \circ) = 6$, $|\Sigma_3| = 6$, $o(\Sigma_n) = n!$. If $|G|$ is infinite (finite) we say that G es infinite (finite). Then, $\mathbb{Z}$ is infinite (forms an infinite group under the usual sum).

To relate two groups it is necessary to define a function that preserves the group structure.

2.4 Definition. Let $(G, \diamond)$ and $(G', \star)$ be two groups. A **homomorphism of groups** is a function $f\colon G \to G'$ such that $f(u \diamond v) = f(u) \star f(v)$.

Example. Consider the set of functions

$$T = \{e^t : t \in \mathbb{Z}_{12}\}$$

where we define

$$\begin{aligned} e^t : \mathbb{Z}_{12} &\to \mathbb{Z}_{12}, \\ a &\mapsto a + t. \end{aligned}$$

Then $(T, \circ)$ is a group, where $\circ$ is the composition of functions. This group is isomorphic to $(\mathbb{Z}_{12}, +)$, under the isomorphism

$$\begin{aligned} \phi : \mathbb{Z}_{12} &\to T, \\ x &\mapsto e^x. \end{aligned}$$

Indeed,

$$\phi(x + y) = e^{x+y} = e^x \circ e^y = \phi(x) \circ \phi(y);$$

we leave it to the reader to show that ϕ is bijective and that its inverse is also a homomorphism.

From the musical point of view, T is the group of all transpositions, and this shows that it is isomorphic to the equal tempered chromatic scale. For more details about transpositions, see chapter 4, section 4.2.

Now, we will recall the definition of action and define the concept of a group with operators:

2.5 Definition. Let Ω and A be two sets. An **action** of Ω on A is a function of $\Omega \times A$ on the set A.

2.6 Definition. Let Ω be a set. A group $(G, \cdot)$ together with an action on Ω in $(G, \cdot)$

$$\begin{array}{rcl} \circ : \Omega \times G & \longrightarrow & G, \\ (\alpha, x) & \mapsto & \circ(\alpha, x) = \alpha \circ x = x^\alpha, \end{array}$$

that is distributive with respect to the composition law of $(G, \cdot)$ is called a **group with operators** in Ω.

Example. Let $GL(\mathbb{Z}_{12}) = \{1, 5, 7, 11\} \subseteq \mathbb{Z}_{12}$ (the elements of $\mathbb{Z}_{12}$ with multiplicative inverse). If $G = (\mathbb{Z}_{12}, +)$, then by defining the action

$$\begin{aligned} \circ : GL(\mathbb{Z}_{12}) \times \mathbb{Z}_{12} &\to \mathbb{Z}_{12} \\ (u, x) &\mapsto ux \end{aligned}$$

we get $\mathbb{Z}_{12}$ as a group with operators on $GL(\mathbb{Z}_{12})$. Indeed,

$$\circ(u, x+y) = u(x+y) = ux + uy = \circ(u,x) + \circ(u,y).$$

The set of operators is, in fact, a group under multiplication in $\mathbb{Z}_{12}$. Recall that $\mathbb{Z}_{12}$ can be interpreted as the equal tempered scale modulo octaves and, for this reason, these operators are very important. They can be used to classify chords, scales or motives, by considering those that are transformed according to $GL(\mathbb{Z}_{12})$ as equivalent, and this has musical meaning. For example, if $11 \in GL(\mathbb{Z}_{12})$ acts on $\mathbb{Z}_{12}$ it inverts the pitches, a very useful operation in counterpoint and in the manipulation of motives.

The distributive law can be expressed as

$$(xy)^\alpha = x^\alpha y^\alpha$$

i.e.,

$$(\alpha, xy) \longmapsto \circ(\alpha, xy) = \alpha \circ (xy) = (\alpha \circ x)(\alpha \circ y).$$

2.7 Observation. In a group G with operators in Ω, each element of Ω (called **operator**) defines an endomorphism (i.e.a homomorphism from $G \longrightarrow G$) of the group G. Considere $\Omega = \mathbb{Z}$ and for $x \in G$, $n \in \mathbb{Z}$ define

$$\begin{array}{rcl} \circ : \mathbb{Z} \times G & \longrightarrow & G, \\ (n, x) & \mapsto & n \circ x = x^n. \end{array}$$

If G is abelian, we have

$$n(xy) = (xy)^n = x^n y^n = (nx)(ny).$$

Hence, every abelian group G can be seen as a group with operators in $\mathbb{Z}$.

2.8 Definition. A **ring** is a triple $(\Lambda, +, \cdot)$ where Λ is a set, $+$ and $\cdot$ are binary operations such that
(i) $(\Lambda, +)$ is a commutative group,
(ii) $(\Lambda, \cdot)$ is a semigroup,
(iii) $u(v+w) = uv + uw$ and $(u+v)w = uw + vw$.

The reader can show that $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$,$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(M_n K, +, \cdot)$, $(K, +, \cdot)$,$(K[x], +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are rings.

If a ring $(\Lambda, +, \cdot)$ satisfies:
(iv) $(\Lambda, \cdot)$ is a commutative semigroup, then $(\Lambda, +, \cdot)$ is called a **commutative ring**.

If $(\Lambda, \cdot)$ is monoid, we say that $(\Lambda, +, \cdot)$ is a **ring with identity** or **a unit ring**.

Recall that if the product of two elements different from zero of a ring Λ yields the zero element of the ring, then these two elements are caller **zero divisors.** If the ring $(\Delta, +, \cdot)$ with $1 \neq 0$ does not have zero divisors, it is called an **integral domain**. If an integral domain has a multiplicative inverse for every non-zero element, it is called a **division ring**.

Finally, a **field** is a commutative division ring.

How do we relate two rings? Through functions that preserve the ring structure. If $(\Lambda, \diamond, \star)$ and $(\Lambda', +, \cdot)$ are rings, a **ring homomorphism** is a function that is a homomorphism on the commutative group of Λ into the commutative group of Λ' and that is also a homomorphism of semigroups of Λ into semigroups of Λ', that is,

$$f(u \diamond v) = f(u) + f(v) \text{ and } f(u \star v) = f(u) \cdot f(v).$$

If we consider a commutative ring with identity, $(\Lambda, +, \cdot)$, instead of a field K, when defining a vector space, we obtain an algebraic structure called a **(left) Λ-module** . Then, as a particular case of the Λ-modules we have the K-modules, i.e. the vector spaces over a field K.

Many of the results for vector spaces are valid for Λ-modules, it is enough to take $K = \Lambda$, a commutative ring with an identity element. In particular, we relate two Λ-modules by means of a **homomorphism of Λ-modules**. Λ-modules are generalizations of the concepts of commutative group and vector space, and they are the objects of study of Homological Algebra (see [Ll1]). Imitating vector spaces, if a Λ-module has a *basis*, we call it a **free Λ-module** . Not every Λ-module has a basis, that is, not every Λ-module is free, but every vector space or K-module is free, that is, it has a basis. We say that a Λ-module is **projective** if it is the sumand of the direct sum of a free module, and it is **finitely generated** if it has a finite set of generators.

Example. The cartesian product $\mathcal{I} = \mathbb{Z}_{12} \times \mathbb{Z}_{12}$ can be seen as the set of all equal tempered **counterpoint intervals**: the first component represents the "base" pitch of the interval and the second its "length". For example, the pair $(0, 0)$ represents the zero interval (or octave, there is no difference) with base pitch C, whereas the pair $(2, 7)$ represents an ascending fifth over D (or, also, a descending fourth over D)[3].

We can define a sum on this set

$$+ : \mathcal{I} \times \mathcal{I} \to \mathcal{I},$$
$$((a, b), (c, d)) \mapsto (a + c, b + d).$$

[3] This ambiguity is resolved by giving an **orientation** to the counterpoint interval $\xi \in \mathcal{I}$, that is, $+$ if it is ascending and $-$ if it is descending, and it is written $(\xi, +)$ or $(\xi, -)$. If it is not specified, it is understood that the orientation is ascending.

and a multiplication by a scalar

$$\begin{aligned} \cdot : \mathbb{Z}_{12} \times \mathcal{I} &\to \mathcal{I}, \\ (k, (c, d)) &\mapsto (kc, kd). \end{aligned}$$

that converts it into a $\mathbb{Z}_{12}$-module. These operations have a musicological meaning. For example, multiplication by the scalar $-1 = 11 \in \mathbb{Z}_{12}$ is equivalent to inverting the intervals and reflecting the base point with respect to the pitch C. To sum $(c, 0)$ to any element of the form (a, b) is equivalent to transposing the base pitch a by c units, but preserving the distance of the interval. Such procedures are common in counterpoint.

An **algebra** over Λ (Λ is a commutative ring with identity) is a set A that is simultaneously a ring and a Λ-module. That is, an algebra $(A, +, \mu, \cdot)$ is a Λ-module with another binary operation called **multiplicación** with the extra condition that makes the binary operation and the scalar multiplication compatible, which is the following:

$(\lambda u + \lambda' v)w = \lambda(uw) + \lambda'(vw)$
$w(\lambda u + \lambda' v) = \lambda(wu) + \lambda'(wv) \quad$ for $\lambda, \lambda' \in \Lambda; u, v, w \in A$

In particular we see that $(\lambda u)v = \lambda(uv) = u(\lambda v)$, thus λuv is a well defined element of A. We leave it to the reader to provide the definition of a homorphism of algebras, and to recognize several examples of well known algebras that have been implicitly introduced..

Example. We can define a multiplication on $\mathcal{I}$ in the following way:

$$\begin{aligned} * : \mathcal{I} \times \mathcal{I} &\to \mathcal{I}, \\ ((a, b), (c, d)) &\mapsto (ac, ad + bc). \end{aligned}$$

This way $(\mathcal{I}, +, \cdot, *)$ is transformed into an algebra on $\mathbb{Z}_{12}$ because, on the one hand,

$$\begin{aligned} ((a, b) + (c, d)) * (u, v) &= (a + c, b + d) * (u, v) \\ &= ((a + c)u, (a + c)v + (b + d)u) \\ &= (au + cu, av + cv + bu + du) \\ &= (au, av + bu) + (cu, cv + du) \\ &= (a, b) * (u, v) + (c, d) * (u, v), \end{aligned}$$

and, on the other

$$\begin{aligned} (u, v) * ((a, b) + (c, d)) &= (u, v) * (a + c, b + d) \\ &= (u(a + c), u(b + d) + v(a + c)) \\ &= (ua + uc, ub + ud + va + vc) \\ &= (ua, va + ub) + (uc, ud + cv) \\ &= (u, v)(a, b) + (u, v)(c, d) \end{aligned}$$

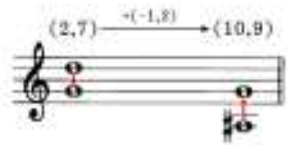


Figure 1.5: Multiplication of the descending interval $((2,7),-)$ by $(-1,2)$ to obtain $((10,9),+)$.

and also

$$\begin{aligned}(k\cdot(a,b))*(u,v) &= (ka,kb)*(u,v)\\ &= (kau, kav+kbu)\\ &= k(au, av+bu) = k\cdot((a,b)*(u,v)).\end{aligned}$$

This multiplication is meaningful from the musicological point of view. To show why, we first define the functions

$$\begin{aligned}\alpha_+ : \mathcal{I} &\mapsto \mathbb{Z}_{12},\\ (x,y) &\mapsto x+y,\end{aligned}$$

and

$$\begin{aligned}\alpha_- : \mathcal{I} &\mapsto \mathbb{Z}_{12},\\ (x,y) &\mapsto x-y.\end{aligned}$$

Given a counterpoint interval $(x,y)\in\mathcal{I}$, the functions α_+ and α_- allow us to recover the "endpoint" of the interval, depending on the orientation. For example, if $((7,7),+)$ is the *ascending* fifth over G, we can obtain the "endpoint" by summing the "length" of the interval to the base pitch.

$$\alpha_+(7,7) = 7+7 = 2$$

that is, the pitch D. Now, if $((2,7),-)$ is the *descending* fifth over D, the "endpoint" results from subtracting the "length" of the interval from the base pitch.

$$\alpha_-(2,7) = 2-7 = 7,$$

which is the pitch G.

We observe that

$$\begin{aligned}\alpha_+((-1,2)*(x,y)) &= \alpha_+(-x, 2x-y)\\ &= -x+(2x-y)\\ &= x-y = \alpha_-(x,y).\end{aligned}$$

this relation, in musical terms, tells us that, if we have a descending counterpoint interval $((x, y), -)$ with endpoint $x - y$, we can change it for the ascending counterpoint interval

$$((-1, 2) * (x, y), +) = ((-x, 2x - y), +)$$

if we are intereseted in preserving its "endpoint". For example, we change the descending fifth over D $((2, 7), -)$ for

$$((-1, 2) * (2, 7), +) = ((-2, 4 - 7), +) = ((10, 9), +),$$

which is the ascending major sixth over A♯. Both counterpoint intervals have the pitch G as their "endpoint" (figure **??**).

The previous development is important in counterpoint where, in general, it is required that the intervals between two voices have the same orientation (whether ascending or descending). If they have opposite directions at some point (as when the voices cross), we can change the orientation of some intervals through multiplication by $(-1, 2)$ until they are uniform, but maintaining one of the voices as invariant.

For more details about the musicological meaning of $\mathcal{I}$,seen as a $\mathbb{Z}_{12}$-algebra and its applications to counterpoint, consult [M], part VII.

If conditions are imposed on the multiplication of an algebra we can obtain **commutative algebras**, **associative algebras**, **algebras with identity**.

A associative algebra with identity, such that every element different from zero is invertible, is called a **division algebra**.

2.9 Example. $(M_nK, +, \cdot, \mu)$, where M_nK denotes the $n \times n$ square matrices with coefficients in a field K (μ denotes the scalar multiplication) is an algebra, the same as $(K, +, \cdot, \mu)$ and $(K[x], +, \cdot, \mu)$.

We define a **graduated algebra** as a sequence $A = (A_0, A_1, A_2, ...)$ of algebras A_i, one for each index $i \in N$.

For those who have studied, in an elementary Linear Algebra, or Multilinear Algebra course, recall the following concepts from Multilinear Algebra (as in [Ll2]), that are not requisites for this text.

2.10 Example. Let $T^k(V) = \otimes^k V = V \otimes_K \cdots \otimes_K V$ be the tensorial product of a vector space V on the field K, k times. We call $T^k(V)$ **the tensor space of degree** k of V. If we define a multiplication

$$\cdot : T^kV \times T^lV \to T^{k+l}V \text{ as}$$
$$(u_1 \otimes ... \otimes u_k) \cdot (v_1 \otimes ... \otimes v_l) = u_1 \otimes ... \otimes u_k \otimes v_1 \otimes ... \otimes v_l$$

we obtain a graduated algebra (where we define $T^0V = K$ and $T^1V = V$) $TV = (K, V, T^2V, T^3V, T^4V, \ldots)$ called the **tensor algebra** of V.

2.11 Example. Let $\bigwedge^k V = V \wedge ... \wedge V$ be the exterior product of a vector space V over a field K, k times. We consider the exterior multiplication defined as

$$\wedge : \bigwedge^k V \times \bigwedge^l V \to \bigwedge^{k+l} V.$$

Then we have a graduated algebra

$$\bigwedge V = (K, V, \bigwedge^2 V, \bigwedge^3 V, \ldots)$$

called **exterior algebra** or **Grassmann algebra** of V.

Problems

2.1 Prove that the sets in Example 2.2 , with their respective binary operations are, indeed, monoids.

2.2 Prove that the sets in Example 2.3 , with their respective binary operations are, indeed, groups.

2.3 Prove that the sets in Example 2.9 , with their respective binary operations are, indeed, algebras.

2.4 Prove that the complex numbers, under multiplication, form a monoid.

1.3 Elementary Properties

In this section we present some elementary properties of groups. To the particular case of Group Theory, what was mentioned previously in general terms will be applied; that is, every time a property is proved for a set with a binary operation that satisfies the group axioms, this property is immediately valid for all sets that satisfy the group axioms.

Consider a group $(G, \cdot)$. If x and y are elements of G, we denote $x \cdot y$ as xy, to simplify the notation. Let e be the identity element of G. With this notation, the generalized definition of group, that was promised in the previous section, is:

A **group** is a pair $(G, \cdot)$ where G is a non-empty set and

$$\cdot \colon G \times G \to G$$

is a binary operation

$$(x, y) \longmapsto \cdot(x, y)$$

where, by abuse or convenience of notation, we write

$$\cdot(x, y) = x \cdot y = xy$$

such that

(i) $(xy)z = x(yz)$; $x, y, z \in G$.

(ii) there exists an element $e \in G$ such that $ey = y$, for every $y \in G$.

(iii) for every $y \in G$ there exists an element, denoted y^{-1}, such that $(y^{-1})y = e$.

We say that a group is **commutative** or **abelian** if it also satisfies

(iv) $xy = yx$, for every $x, y \in G$, that is, its binary operation is commutative.

If the group is abelian, it is usual to denote its binary operation with the $+$ sign.

We can understand the concept of group as a special case of groups with operators in $\varnothing$ (and as an action, the only one possible of $\varnothing$ on G).

The element e will be called the **left identity element** or simply **left identity** of x and y^{-1}will be called the **left inverse** of y. Analogously, we have a **right identity element** and a **right inverse**. When the binary operation's notation is clear, frequently it is omitted and the group $(G, \cdot)$ is designated as G.

We will see that, in our definition of group, the stipulation of a left identity element and a left inverse implies the existence of a right identity and right inverse.

3.1 Proposition. In a group $(G, \cdot)$, if an element is a left inverse it is also a right inverse. If e is a left identity, then it is a right identity.
Proof. Consider $x^{-1}x = e$ for any element $x \in G$. Consider the left inverse element of x^{-1}, that is, $(x^{-1})^{-1}x^{-1} = e$. Then

$$xx^{-1} = e(xx^{-1}) = ((x^{-1})^{-1}x^{-1})(xx^{-1}) = (x^{-1})^{-1}ex^{-1} = (x^{-1})^{-1}x^{-1} = e.$$

Hence x^{-1} is a right inverse of x. Now, for any element x, consider the equalities

$$xe = x(x^{-1}x) = (xx^{-1})x = ex = x.$$

Thus e is a right identity.♦

We say that e is the **identity element** of a group G if e is a left or right identity element and we talk about the **inverse** of an element if its left or right inverse exist.

We will now see some elementary properties:

3.2 Proposition. The identity element e of a group G is unique.
Proof. Let e' be another identity element such that $e'e = e$. As e is also an identity, then $e'e = e'$. Thus $e = e'$.♦

3.3 Proposition. If $xy = xz$ in a group G, then $y = z$. Analogously, $yx = zx$, then $y = z$.
Proof. If $xy = xz$, then $x^{-1}(xy) = x^{-1}(xz)$. By associativity, $(x^{-1}x)y = (x^{-1}x)z$. Hence, $ey = ez$ and, finally, $y = z$. If $yx = zx$, then $y = z$, which can be proved in the same way.♦

3.4 Proposition. In an arbitrary group G, the inverse of any element is unique.
Proof. Let x' be another inverse element of the element x. Then, $x'x = e$. We also know that $x^{-1}x = e$. Thus, $x'x = x^{-1}x = e$. By the previous proposition, $x' = x^{-1}$.♦

3.5 Proposition. In an arbitrary group G, if $x, y \in G$, the equations $xa = y$ and $bx = y$ have a unique solution in G.
Proof. Let $x(x^{-1}y) = (xx^{-1})y = ey = y$. Hence, $a = x^{-1}y$ is a solution to $xa = y$. Suppose that there are two solutions, $xa = y$ and $xa' = y$. Then $xa = xa'$, and $a = a'$. Analogously for the other case.♦

3.6 Proposition. Let G be a group. For any elements x, y in G

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Proof. As

$$\begin{aligned}(xy)(y^{-1}x^{-1}) &= x(yy^{-1})x^{-1} = xx^{-1} = e,\\ (y^{-1}x^{-1})(xy) &= y^{-1}(x^{-1}x)y = y^{-1}y = e\end{aligned}$$

then $(xy)^{-1} = y^{-1}x^{-1}$.♦

Recall the definition of group homomorphism from the previous section with the following notation: Let $(G, +)$ and $(G', \cdot)$ be two groups. A **group homomorphism** is a function $f\colon G \to G'$ such that $f(u + v) = f(u) \cdot f(v)$.

Some examples follow.

3.7 Example. Let $G = \mathbb{R}^3$ and $G' = \mathbb{R}$ with the usual sum. We define $f : G \to G'$ by the rule $f(x, y, z) = 8x - 4y + 4z$. We will show that f is a homomorphism. As

$$\begin{aligned} f((x_1, y_1, z_1) + (x_2, y_2, z_2)) &= f(x_1 + x_2, y_1 + y_2, z_1 + z_2) \\ &= 8(x_1 + x_2) - 4(y_1 + y_2) + 4(z_1 + z_2) \text{ y} \\ f(x_1, y_1, z_1) + f(x_2, y_2, z_2) &= (8x_1, -4y_1 + 4z_1) + (8x_2 - 4y_2 + 4z_2), \end{aligned}$$

f is a homomorphism.

3.8 Proposition. Let $f : G \to G'$ be a homomorphism of groups. If e is an identity element of G then $f(e) = e'$ is the identity of G'.
Proof. Consider $e'f(x) = f(x) = f(ex) = f(e)f(x)$. Multiplying both sides by the inverse of $f(x)$ we obtain $e'f(x)f(x)^{-1} = f(e)f(x)f(x)^{-1}$. Then $e' = e'e' = f(e)e' = f(e)$. Thus $e' = f(e)$.♦

3.9 Example. Let $G = G' = \mathbb{R}^2$. We define $f : G \to G'$ by $f(x, y) = (x+8, y+2)$. As $f(0, 0) = (8, 2) \neq (0, 0)$, f is not a homomorphism, because all group homomorphisms send the identity element in the domain to the identity element in the codomain.

3.10 Proposition. The composition of two group homomorphisms is a group homomorphism.
Proof. Let $f : G' \to G$ and $g : G \to G''$ be group homomorphisms. Then $(g \circ f)(x+y) = g(f(x+y)) = g(f(x)+f(y)) = g(f(x))+g(f(y)) = (g \circ f)(x)+(g \circ f)(y)$. Hence $(g \circ f)$ is a homomorphism.♦

3.11 Definition. Let $f : G \to G'$ be a group homomorphism. We say that f es un **isomorphism**, and write $f : G \xrightarrow{\cong} G'$ if there exists a homomorphism $g : G' \to G$ such that $g \circ f = 1_G$ and $f \circ g = 1_{G'}$.

It is easy to show (Problem 3.13) that, if g exists, it is determined uniquely; We denote it by f^{-1} and it is called the **inverse** of f. Hence, $f : G \to G'$ is an isomorphism if and only if it is bijective. We say that two groups G and G' are **isomorphic** if there exists an isomorphism $f : G \xrightarrow{\cong} G'$ and we write $G \cong G'$.

3.12 Definition. Let $f : G \to G'$ be a group homomorphism. The **kernel** of f, denoted as $\ker f$, is the set of all elements $x \in G$ such that $f(x) = e'$ where

e' denotes the identity of G'. The **image** of f, denoted $im\ f$, is the set $\{\ f(x) : x \in G\}$.

If in the definition of homomorphism $\ker f = \{e\}$ we say that f is a **monomorphism** and we denote it by $f : G \rightarrowtail G'$; if $im\ f = G'$ we say that f is an **epimorphism** and we denote it by $f : G \twoheadrightarrow G'$ and if f is such that $\ker f = \{e\}$ and $im\ f = G'$ then we say that f is an **isomorphism**. In other words, f is a monomorphism when it is injective; it is an epimorphism when it is surjective (onto), and it is an isomorphism when it is bijective (Problem 3.13). A homorphism $f : G \to G$ will be called an **endomorphism** and, if f is bijective, we will call it an **automorphism**.

3.13 Proposition. Let $f\colon G' \to G$, $g\colon G \to G''$ be two group homomorphisms and $h = g \circ f$ the composition of the two. Then, (i) if h is a monomorphism, f is a monomorphism, and (ii) if h is an epimorphsm, g is an epimorphism.
Proof. (i) Suppose that h is a monomorphism. If $f(x) = f(y)$ then $h(x) = g(f(x)) = g(f(y)) = h(y)$. As h is a monomorphism, $x = y$. Hence f is a monomorphism. (ii) Suppose that h is an epimorphism. Then $h(G') = G''$. Thus, $G'' = h(G') = g(f(G')) \subset g(G) \subset G''$. Hence, $g(G) = G''$.♦

We say that a homomorphism $f\colon G \to G'$ is **trivial** if $f(x) = e'$ for every $x \in G$. That is, $im\ f = \{e'\}$. If f is trivial, we denote it as O (see Problem 3.9). Thus $f = O$ if and only if $\ker f = G$.

Now we will study those subsets of a group which are, also, groups themselves.

3.14 Definition. We say that a subset H of $(G, \cdot)$ is a **subgroup** of G if H is a stable group, that is, if H is closed under the induced binary operation. We denote this as $H < G$.

We will see a result that provides a way of showing that a subset of a group is a subgroup.

3.15 Proposition. A subset H of $(G, \cdot)$ is a subgroup of G if and only if the following three conditions are satisfied:
(i) H is stable or closed under $\cdot$.
(ii) the identity element e of G is in H.
(iii) if $x \in H$, then $x^{-1} \in H$.
Proof. See Problem 3.4.♦

3.16 Example. $(\mathbb{Z}, +)$ is a subgroupo of $(\mathbb{R}, +)$. $(\mathbb{Q}^+, \cdot)$ is a subgroup of $(\mathbb{R}^+, \cdot)$. $(\mathbb{Q}, +)$ is also a subgroup of $(\mathbb{R}, +)$, $(\mathbb{R}, +)$ is a subgroup of $(\mathbb{C}, +)$ and $(2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

3.17 Example. Let $(G, \cdot)$ be a group. Both G and $\{e\}$ are subgroups of $(G, \cdot)$, called **improper subgroups** . All other subgroups are called **proper**. The

subgroup $\{e\}$ is called the **trivial subgroup** and it is usual to denote it, by abuse of notation, only by e where e can also be denoted as 0 or 1 or any other notation that represents the identity element of the group under consideration.

3.18 Proposition. The intersection of subgroups of G is a subgroup of G.
Proof. Let $\{H_i\}_{i\in I}$ be a collection of subgroups of G, indexed by a set I of indices. We take $x, y \in \cap_i H_i$. As $\cap_i H_i \subset H_i$ for every i, we see that $x, y \in H_i$. As H_i is a subgroup of G, $x + y \in H_i$, $e \in H_i$, $x^{-1} \in H_i$ for every $i \in I$. Hence, $x + y \in \cap H_i, e \in \cap H_i, x^{-1} \in \cap H_i$.♦

3.19 Proposition. Let $f : G \to G'$ be a homomorphism of groups. Then, if H is a subgroup of G, $f(H)$ is subgroup of G' and if $H'$is a subgroup of G', $f^{-1}(H')$ is a subgroup of G.
Proof. We will show that $f(H) = \{f(x)|x \in H\}$ is a subgroup of G'. Let $v, w \in f(H)$; Then there exist $x, y \in H$ such that $f(x) = v$, $f(y) = w$. As H is a subgroup of G, $x + y \in H$. As f is a homomorphism, $f(e) = e' \in f(H)$, $v + w = f(x) + f(y) = f(x + y) \in f(H)$. If $x \in H$ then $f(x) \in f(H)$. As H is a subgroup of G, $x^{-1} \in H$. Then (Problem 3.18) $f(x^{-1}) = f(x)^{-1} \in f(H)$. Hence, $f(H)$ is a subgroup of G'.

Now, we will see that $f^{-1}(H') = \{x \in G|f(x) \in H'\}$ is a subgroup of G. Let $x, y \in f^{-1}(H')$, then $f(x)$ and $f(y)$ are in H'. As H' is a subgroup of G' and f is a homomorphism, $f(x + y) = f(x) + f(y) \in H'$ and $f(e) = e' \in H'$. Given that $f(x) \in H'$, as $f(x)^{-1} = f(x^{-1})$, $f(x)^{-1} \in H'$. Hence $f^{-1}(H')$ is a subgroup of G.♦

Observe that in the previous Proposition the inverse image is a subgroup of the domain, although there is not necessarily an inverse function f^{-1} for f. The inverse image of $\{e'\}$ is the kernel of f and the inverse image of any subgroup contains the kernel of f.

3.20 Corollary. Let $f : G \to G'$ be a group homomorphism. Then $im\ f$ is a subgroup of G' and $ker\ f$ is a subgroup of G.
Proof. Immediate from the previous proposition taking $H = G$ and $H' = e'$.♦

We will denote as $Hom(X, Y)$ the set of homomorphisms of an abelian group X in an abelian group Y. Let $f, g\colon X \longrightarrow Y$ be homomorphisms of abelian groups and define $f + g\colon X \longrightarrow Y$ by $(f + g)(x) = f(x) + g(x)$. It is easy to show that this definition makes $Hom(X, Y)$ an abelian group, (Problem 3.21).

Let $\psi\colon Y' \longrightarrow Y$ be a homomorphism of abelian groups and $(X \xrightarrow{f} Y')$ an element of $Hom(X, Y')$. We associate a homomorphism $(X \xrightarrow{g} Y) \in Hom(X, Y)$ to f by means of a function

$$\psi_* = Hom(X, \psi)\colon Hom(X, Y') \longrightarrow Hom(X, Y)$$

given by $\psi_*(f) = \psi \circ f$. Hence ψ_* is a homomorphism of abelian groups (Problem 3.22), called the **homomorphism induced by** ψ.

Let $\varphi\colon X' \longrightarrow X$ be a homomorphism of abelian groups and $(X \xrightarrow{g} Y) \in Hom(X,Y)$. We associate a homomorphism $(X' \xrightarrow{f} Y) \in Hom(X',Y)$ to g by means of a function

$$\varphi^* = Hom(\varphi, Y)\colon Hom(X,Y) \longrightarrow (X',Y)$$

given by $\varphi^*(g) = g \circ \varphi$. Then φ^* is a homomorphism of abelian groups (Problema 3.23), called the **homomorphism induced by** φ.

Let $\psi\colon Y' \longrightarrow Y$ and $\psi'\colon Y \longrightarrow Y''$ be homomorphisms of abelian groups and X an abelian group. If $1_Y\colon Y \longrightarrow Y$ is the identity, then $1_{Y_*}\colon Hom(X,Y) \longrightarrow Hom(X,Y)$ is the identity of $Hom(X,Y)$, and $(\psi' \circ \psi)_* = \psi'_* \circ \psi_*$. (Problem 3.24). We can visualize this by the following diagram:

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, equal] & Y'' \arrow[d, "\psi"] & \in & Hom\,(X,Y') \arrow[d, "\psi*"] & \\
\left(X \arrow[r, "g"] \arrow[d, equal] & Y\right) \arrow[d, "\psi'"] \arrow[loop left, "1_Y"] & \in & Hom\,(X,Y \arrow[loop right, "1_{Y_*}"] \arrow[d, "\psi*"] & \psi'_* \circ \psi^* \arrow[ddll, bend left] \\
X \arrow[r, "h"] & Y'' & \in & Hom\left(X,Y''\right) &
\end{tikzcd}$$

Let $\varphi\colon X' \longrightarrow X$ and $\varphi'\colon X \longrightarrow X''$ be homomorphisms of abelian groups and Y an abelian group. If $1_X\colon X \longrightarrow X$ is the identity, then $1_X^*\colon Hom(X,Y) \to Hom(X,Y)$ is the identity of $Hom(X,Y)$, and $(\varphi' \circ \varphi)^* = \varphi^* \circ \varphi'^*$. (Problem 3.25). We can visualize this by the following diagram:

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "\varphi"] & Y'' \arrow[d, equal] & \in & Hom\,(X,Y') & \\
\left(X \arrow[r, "g"] \arrow[d, "\varphi'"] & Y\right) \arrow[d, equal] \arrow[loop left, "1_X"] & \in & Hom\,(X,Y \arrow[loop right, "1_{X_*}"] \arrow[u, "\varphi*"] & (\varphi \circ \varphi\prime)^* \arrow[uull, bend left] \\
X \arrow[r, "h"] & Y'' & \in & Hom\left(X,Y''\right) \arrow[u, "\varphi*"] &
\end{tikzcd}$$

Problems

3.1 Using additive notation, write the definition of commutative group, and write the elementary properties that they possess (and that are given at the beginning of this section).

3.2 Show that $(x^{-1})^{-1} = x$ and that $e^{-1} = e$.

3.3 Show that if $xy = yx$ in a group G then $(xy)^n = x^n y^n$.

3.4 Show Proposition 3.15.

3.5 Show that there are two groups that have 4 elementos, write their tables, find their subgroups and their diagram of subgroups. One is $\mathbb{Z}_4$ and the other is known as the **Klein 4-group**, denoted with the letter V.

3.6 Prove the statements in Example 3.16.

3.7 The group of symmetries of a regular polygon of n sides is called **dihedral group** of degree n, denoted D_n. Write the multiplication tables for D_3 and D_4. Determine the order of D_n.

3.8 Let $G = G' = K^n$ where K is a field. Show that $f\colon G \to G'$ given by $f(u_1, \ldots, u_n) = (u_1, u_2, \ldots, u_{n-1}, 0)$ is a homomorphism.

3.9 Let G be a group. Show that the function $1_G\colon G \to G$ and the functions $O_G\colon G \to G$ given by $1_G(x) = x$ and $O_G(x) = O$ for every $x \in G$, are homomorphisms. 1_G is called the **identity homomorphism** on G and O_G is called the **trivial homomorphism**.

3.10 Verify which functions are homomorphisms and which are not:
(i) $f\colon K^n \to K^m$, $f(x) = Ax$ where A an $m \times n$ matrix with elements in a field K.
(ii) $f\colon K^2 \to K^2$, $f(x, y) = (4y, 0)$.
(iii) $f\colon K^3 \to K^3$, $f(x, y, z) = (-z, x, y)$.
(iv) $f\colon K^2 \to K^2$, $f(x, y) = (x^2, 2y)$.
(v) $f\colon K^5 \to K^4$, $f(u, v, x, y, z) = (2uy, 3xz, 0, 4u)$.
(vi) $f\colon K^3 \to K^3$, $f(x, y, z) = (x + 2, y + 2, z + 2)$.

3.11 Establish, if possible, nontrivial homomorphisms for the following cases:
(i) $1 \longrightarrow \mathbb{Z}_2$.
(ii) $\mathbb{Z}_2 \xrightarrow{\times 2} \mathbb{Z}_4$.
(iii) $\mathbb{Z}_4 \longrightarrow \mathbb{Z}_2$.
(iv) $\mathbb{Z}_2 \longrightarrow 1$.
(v) $\mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$.
(vi) $\mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$.
(vii) $\mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$.

3.12 We denote the set of homomorphisms of the group G into the abelian group G'as $Hom(G, G')$. Define $f + g\colon G \to G'$ as $(f + g)(x) = f(x) + g(x)$, $x \in G$. Show that $(Hom(G, G'), +)$ is a group.

3.13 Prove that if $f : G \to G'$ is an isomorphism of groups as in the Definición 3.11, g is determined uniquely and that f is an isomorphism if and only if it is bijective.

3.14 Let $f : G \to G'$ be a bijective group homomorphism. Show that the inverse function $f^{-1} : G' \to G$ is also a homomorphism.

3.15 Show Corollary 3.20 without using Proposición 3.19.

3.16 Show that a group homomorphism $f\colon G \to G'$ is injective if and only if $\ker f = \{e\}$.

3.17 In a group G, show that if an element x is idempotent ($x \cdot x = x$) then $x = e$, where e is the identity element of G. Use this to show that under a group homomorphism, the identity element in the domain is sent, under the homomorphism, to the identity element in the codomain.

3.18 Let $f : G \to G'$ be a group homomorphism. Show that if $x \in G$ then $f(x^{-1}) = f(x)^{-1}$.

3.19 Let X, Y and G be abelian groups. We say that $f\colon X \times Y \to G$ is a biadditive function if $f(x_1 + x_2, y) = f(x_1, y) + f(x_2, y)$ and $f(x, y_1 + y_2) = f(x, y_1) + f(x, y_2)$ for $x, x_1, x_2 \in X$, $y, y_1, y_2 \in Y$. Show that

(i) $f(\lambda x, y) = \lambda f(x, y) = f(x, \lambda y)$ for every $x \in X, y \in Y$ and $\lambda \in \mathbb{Z}$.

(ii)f is never injective unless $X = Y = 0$.

3.20 Show that the group $(\mathbb{Z}[x], +)$ is isomorphic to the group $(\mathbb{Q}^+, \cdot)$.

3.21 Consider $Hom(X, Y)$ as the set of homomorphisms of the abelian group X into the abelian groupo Y. Let $f, g\colon X \longrightarrow Y$ be group homomorphisms of abelian groups and define $f + g\colon X \longrightarrow Y$ by $(f + g)(x) = f(x) + g(x)$. Show that this definition makes $Hom(X, Y)$ an abelian group.

3.22 Let $\psi\colon Y' \longrightarrow Y$ be a homomorphism of abelian groups and $(X \xrightarrow{f} Y')$ an element of $Hom(X, Y')$. Associate a homomorphism $(X \xrightarrow{g} Y) \in Hom(X, Y)$ to f with a function given by

$$\psi_* = Hom(X, \psi)\colon Hom(X, Y') \longrightarrow Hom(X, Y)$$

where $\psi_*(f) = \psi \circ f$. Show that ψ_* is a homomorphism of abelian groups.

3.23 Let $\varphi\colon X' \longrightarrow X$ be a homomorphism of abelian groups and $(X \xrightarrow{g} Y) \in Hom(X, Y)$. Associate a homomorphism $(X' \xrightarrow{f} Y) \in Hom(X', Y)$ to g with a function given by $(\varphi, Y)\colon Hom(X, Y) \longrightarrow (X', Y)$ such that $\varphi^*(g) = g \circ \varphi$. Show that φ^* is a homomorphism of abelian groups.

3.24 Let $\psi\colon Y' \longrightarrow Y$ and $\psi'\colon Y \longrightarrow Y''$ be homomorphisms of abelian groups and X an abelian group. Show that if $1_Y\colon Y \longrightarrow Y$ is the identity, then $1_{Y_*} : Hom(X, Y) \longrightarrow Hom(X, Y)$ is the identity of $Hom(X, Y)$, and $(\psi' \circ \psi)_* = \psi'_* \circ \psi_*$.

3.25 Let $\varphi\colon X' \longrightarrow X$ and $\varphi'\colon X \longrightarrow X''$ be homomorphisms of abelian groups and Y an abelian group. Show that if $1_X\colon X \longrightarrow X$ is the identity, then $1_X^*\colon Hom(X,Y) \longrightarrow Hom(X,Y)$ is the identity of $Hom(X,Y)$, and $(\varphi' \circ \varphi)^* = \varphi^* \circ \varphi'^*$.

1.4 Cyclic Groups

Consider a multiplicative group $(G, \cdot)$ and the powers of a fixed element $x \in G$, that is, $\{x^n | n \in \mathbb{Z}\}$ where we define $x^0 = e$.

4.1 Proposition. The set $\{x^n | n \in \mathbb{Z}\}$ denoted (x) is a subgroup of G.
Proof. As $x^i x^j = x^{i+j}$, the product of two elements of the set is in the set; thus (x) is closed. As $x^0 = e$, $e \in (x)$. Finally, for x^n, we consider x^{-n}. Then, $x^n x^{-n} = e$.♦

4.2 Definition. The subgroup (x) will be called the **cyclic subgroup** of G generated by one of its elements x and we say that x is a **generator** of (x). If $(x) = G$ we say that G is a **cyclic group generated by** x.

If there does not exist a natural number n for the subgroup (x) such that $x^n = e$ we say that (x) is **infinite cyclic**. If n is the smallest natural such that $x^n = e$, then (x) consists of the elements $x^{n-1}, ...x^1, e = x^n$ and, in this case, we say that (x) is **cyclic group of order** n.

4.3 Example. $\mathbb{Z}$ and $\mathbb{Z}_n$ are cyclic groups, the first is infinite, and the second is finite. $3\mathbb{Z} = (3)$ is also cyclic and, in general, $n\mathbb{Z} = (n)$ are infinite cyclic groups, $n \in \mathbb{N}$. Observe that $(8) = 8\mathbb{Z} < (4) = 4\mathbb{Z} < (2) = 2\mathbb{Z}$.

4.4 Example. $(1) = (3) = \mathbb{Z}_4$, $(1) = (-1) = \mathbb{Z}$.

4.5 Proposition. If G is a cyclic group, then it is commutative (abelian).
Proof. Let $(x) = G$. Then $x^m x^r = x^{m+r} = x^{r+m} = x^r x^m$. Hence G is commutative (abelian).♦

4.6 Definition. Let G be any group and x an element of G. Let r be the smallest natural number such that $x^r = e$, then we say that x has **order** r. If there does not exist a natural number r such that $x^r = e$, we say that x has **infinite order**.

When we consider non abelian groups we will usually use the multiplicative notation and when the groups are abelian we will usually use additive notation. However, we will use multiplicative notation for cyclic groups (which are abelian).

We have the following properties (known as the laws of exponents) in multiplicative notation

$$x^n x^m = x^{n+m}, (x^n)^m = x^{nm}, x^{-n} = (x^n)^{-1}$$

and, in additive notation

$$nx + mx = (n+m)x, m(nx) = (mn)x, (-n)x = -(nx).$$

If a group G is abelian, the following holds

$$n(x+y) = nx + ny.$$

Observe that (once Problems 4.2 and 4.3 are solved) for each $n \in \mathbb{N}$ there is a cyclic group of order n, $(n) = n\mathbb{Z}$. Observe, as well, that if we have two cyclic groups of order n, when we take their generators, we can find a one-to-one correspondence with each power of the generator, which means that, essentially, there is only one cyclic group of order n structurally. In other words, two cyclic groups of the same order are isomorphic, as we will see below.

4.7 Theorem. Let $(G, \cdot)$ be a infinite cyclic group. Then the function

$$h : \mathbb{Z} \longrightarrow G$$

given by

$$n \longmapsto x^n$$

for a fixed element x of G is an isomorphism of groups.
Proof. $h(n+m) = x^{n+m} = x^n x^m = h(n)h(m)$, thus h is a homomorphism. If $h(n) = x^n = x^m = h(m)$, then $n = m$. thus h is injective. For every $x^n \in G$, the integer n goes to x^n under h. Hence, h is surjective.♦

Example. Consider the infinite cyclic subgroup of $(\mathbb{R}^*, \cdot)$ (the nonzero reals with the usual multiplication) generated by the element

$$x = \sqrt[12]{2} \tag{1.1}$$

The number x is, by definition, the quotient of the frequencies between a pitch and another that is a **semitone** above (see chapter 4, section 1). The numbers x^k (up to multplication by a constant) correspond to the hertzian frequencies of the pitches used in the music of equal tempered tuning.

By theorem 4.7 we see that (x) is isomorphic to $(\mathbb{Z}, +)$. We will abuse of this isomorphism and associate a pitch to each element of the group $(\mathbb{Z}, +)$ or to the group $(\mathbb{Z}_{12}, +)$, as can be seen in section 2 of chapter 3.

In addition, such an isomorphism reflects the way our brain interprets the musical distances, or intervals (for more details, see chapter 3, section 2 and chapter 4, section 1).

4.8 Theorem. Every finite cyclic group of order n, with a generator of order n, is isomorphic to $\mathbb{Z}_n$.
Proof. Let G be a cyclic group of order n. Let x be a generator of G such that $x^n = e$. We define

$$h : \mathbb{Z}_n \longrightarrow G$$

given by

$$[m] \longmapsto h([m]) = x^m.$$

Suppose that $h([j]) = h([k])$, then $x^j = x^k$. Hence, $x^{j-k} = e$. Thus, $j - k = rn$ and $n|j-k$. Therefore, $[j] = [k]$ in $\mathbb{Z}_n$.We can also suppose that the ker $h = \{[j]\}$. Then $h([j]) = e$. Hence $x^j = e = x^0$. Thus, $[j] = [0]$ in $\mathbb{Z}_n$. Therefore, h is injective. It is easy to see that h is well defined, it is a homomorphism and it is surjective, (Problem 4.5).♦

4.9 Observation. Consider a cyclic group generated by en element x of order n, and consider q an integer such that $n = mq$. The different powers of x, say

$$x^q, x^{2q}, x^{3q}, ..., x^{mq} = x^n = e,$$

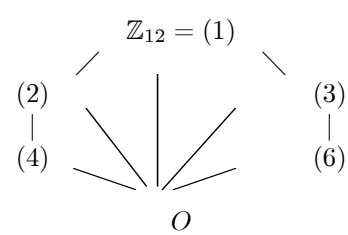
form a cyclic subgroup of (x) of order m.

Similarly, if N is a nontrivial subgroup of (x) we can take the least positive integer q such that $x^q \in N$. As $e = x^n = x^{mq}$, and $m|n$, it is clear that N has $m = n/q$ elements. Finally if $o(G) = n$, then x^j is a generator of G if and only if $(n, j) = 1$, (Problem 4.7).

4.10 Example. Consider $(\mathbb{Z}_{12}, +)$. The generators of $\mathbb{Z}_{12}$ are the elements j such that $(12, j) = 1$, that is, $j = 1, 5, 7$ and 11. Thus, $\mathbb{Z}_{12} = (1) = (5) = (7) = (11)$. The possibilities for q and m in $12 = qm$ are 1 and 12, 2 and 6, 3 and 4, 4 and 3, 6 and 2, 12 and 1 respectively. Hence, the different powers of a generator x,

$$x^{1q}, x^{2q}, x^{3q}, ..., x^{mq} = x^{12} = 0$$

form a cyclic subgroup of (x) of order m. If we take $x = 1$, which makes the calculations easy, we obtain the powers of 1: For $q = 1$, $m = 12$, $\{1^{1\cdot 1}, 1^{2\cdot 1}, 1^{3\cdot 1}, ..., 1^{12\cdot 1} = 1^{12} = 0\}$ which, in additive notation is $\{1\cdot 1, 2\cdot 1, 3\cdot 1, ..., 12\cdot 1 = 0\}$ and we get, exactly $(1) = \mathbb{Z}_{12}$. Analogously, for $q = 2$, $m = 6$, we obtain $\{1^{1\cdot 2}, 1^{2\cdot 2}, 1^{3\cdot 2}, ..., 1^{6\cdot 2} = 1^{12} = 0\}$ which, in additive notation is $\{2 \cdot 1, 4 \cdot 1, 6 \cdot 1, ..., 12 \cdot 1 = 0\} = \{2, 4, 6, 8, 10, 0\} = (2)$. For $q = 3$, $m = 4$, we get $\{1^{1\cdot 3}, 1^{2\cdot 3}, 1^{3\cdot 3}, 1^{4\cdot 3} = 1^{12} = 0\}$ which, in additive notation is $\{3 \cdot 1, 6 \cdot 1, 9 \cdot 1, 12 \cdot 1 = 0\} = \{3, 6, 9, 0\} = (3)$. For $q = 4$, $m = 3$, we obtain $\{1^{1\cdot 4}, 1^{2\cdot 4}, 1^{3\cdot 4} = 1^{12} = 0\}$ which, in additive notation is $\{4 \cdot 1, 8 \cdot 1, 12 \cdot 1 = 0\} = \{4, 8, 0\} = (4)$. For $q = 6$, $m = 2$, we get $\{1^{1\cdot 6}, 1^{2\cdot 6} = 1^{12} = 0\}$ which, in additive notation, is$\{6 \cdot 1, 12 \cdot 1 = 0\} = \{6, 0\} = (6)$. Finally, for $q = 12$, $m = 1$, we get $\{1^{1\cdot 12} = 0\}$ which, in additive notation, is $\{12 \cdot 1 = 0\} = \{0\} = (0) = O$. Thus we have a **subgroup diagram** of $\mathbb{Z}_{12}$:



Problems

4.1 Let $h : G \longrightarrow G'$ be a homomorphism of multiplicative groups. Show that $h(x^n) = (h(x))^n$, $n \in \mathbb{Z}$.

4.2 Show that the multiples of $\mathbb{Z}$, $n\mathbb{Z}$ with $n \in \mathbb{Z}$, are subgroups in $\mathbb{Z}$.

4.3 Show that every subgroup of $\mathbb{Z}$ es cyclic.

4.4 Show that any subgroup of a cyclic group is cyclic. Suggestion: use Problem 4.2 for the infinite case, and the observation 4.9 for the finite case.

4.5 Complete the proof of Theorem 4.8.

4.6 Show that there only exists (up to isomorphism) one group of order 1, 2 and 3; 2 groups of order 4 and 2 groups of order 6.

4.7 Let G be a cyclic group of order n generated by por x. Show that x^j is a generator of G if and only if $(n, j) = 1$.

4.8 Find the subgroups and the diagram of subgroups for $(\mathbb{Z}_{18}, +)$, $(\mathbb{Z}_{24}, +)$ and $(\mathbb{Z}_{31}, +)$. What do you suspect for $(\mathbb{Z}_p, +)$ with p prime?

Chapter 2

2.1 Exact Sequences

In this section we will study finite and infinite sequences of group homomorphisms.

$$\cdots \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow \cdots$$

We begin with the study of sequences where the kernel of the "outgoing" homomorphism contains the image of the "incoming" homomorphism.

1.1 Definition. We say that a sequence of groups

$$\cdots \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}} \cdots$$

is **semiexact** in G_i if $im\ f_{i-1} \subset \ker f_i$. If it is semiexact in each group, we call it a **semiexact sequence**.

This definition is equivalent, as we will soon see, to the composition of the two homomorphisms, the "outgoing" and the "incoming", being the trivial homomorphism. By abuse of notation, we denote the identity element of any group as e, or sometimes as e_{G_i} to specifiy the identity of the group G_i, and we denote the **trivial morphism** as O or "**zero**".

1.2 Proposition. A sequence of groups

$$\cdots \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}} \cdots$$

es semiexact in G_i if and only if the composition $f_i \circ f_{i-1} = O$.
Proof. Suppose that a sequence is semiexact in G_i. Then $im\ f_{i-1} \subset \ker f_i$. We see that the composition $[f_i \circ f_{i-1}](x) = O(x) = e_{G_{i+1}}$ for every $x \in G_{i-1}$. As $f_{i-1}(x) \in im\ f_{i-1} \subset \ker f_i$, we have $f_i(f_{i-1}(x)) = e_{G_{i+1}} = O(x)$. Thus, as x is arbitrary, $f_i \circ f_{i-1} = O$. Now, suppose $f_i \circ f_{i-1} = O$. Let $y \in im\ f_{i-1}$

be arbitrary. Then there exists an $x \in G_{i-1}$ such that $f_{i-1}(x) = y$. Then $f_i(y) = f_i(f_{i-1}(x)) = O(x) = e_{G_{i+1}}$, and $y \in f_i^{-1}(e) = \ker f_i$. We have shown that, if $y \in im\ f_{i-1}$, then $y \in \ker f_i$ for any y. Thus $im\ f_{i-1} \subset \ker f_i$.♦

1.3 Definition. We say that a sequence of groups

$$\cdots \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}} \cdots$$

is **exact** in G_i if it is semiexact and $im\ f_{i-1} \supset \ker f_i$. If it is exact in each group, we call it an **exact sequence**.

We will also say that such a sequence is exact in G_i if and only if $im\ f_{i-1} = \ker f_i$. Every exact sequence is semiexact, but not every semiexact sequence is exact. An exact sequence of the form

$$e \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow e$$

will be called a **short exact sequence**.

1.4 Example. Consider the sequence

$$O \xrightarrow{h} \mathbb{Z}_2 \xrightarrow{f=\times 2} \mathbb{Z}_4 \xrightarrow{g} \mathbb{Z}_2 \xrightarrow{k} O.$$

Here, f is given by $f(0) = 0$ and $f(1) = 2$; $g(0) = g(2) = 0$ and $g(1) = g(3) = 1$. It is easy to show that f and g, defined this way, are group homomorphisms. It is clear that $im\ h = \{0\} = \ker f$, $im\ f = \{0, 2\} = \ker g$, and $im\ g = \{0, 1\} = \ker k$. Thus, it is a short exact sequence.

1.5 Example. Consider the sequence

$$O \xrightarrow{h} \mathbb{Z}_2 \xrightarrow{f} \mathbb{Z}_2 \times \mathbb{Z}_2 \xrightarrow{g} \mathbb{Z}_2 \xrightarrow{k} O.$$

Here f is given by $f(0) = (0, 0)$ and $f(1) = (1, 0)$; $g(0, 0) = g(1, 0) = 0$ and $g(0, 1) = g(1, 1) = 1$. It is easy to prove that f and g defined this way are group homomorphisms. It is clear that $im\ h = \{0\} = \ker f$, $im\ f = \{(0, 0), (1, 0)\} = \ker g$, and $im\ g = \{0, 1\} = \ker k$. Hence, it is a short exact sequence.

Example. Let M be an R-module (that certainly is a group under addition), and

$$M^k = \underbrace{M \oplus M \oplus \cdots \oplus M}_{k}.$$

In a first approximation, the musical objects (whether a scale, a chord, a motif, a rhythm) can be seen as a subset of some appropriate M^k module. In Mathematical Music Theory, it is very interesting to classify the musical objects with musical meaning, up to isomorphism, of M^k. For example, how many different chords or scales are there if we consider all the transpositions as

equivalent? Or, how many motifs are there if the permutations of their elements are considered, essentially, as the same motif?

A short exact sequence that is used in the classification of musical objects is

$$0 \to M \xrightarrow{\Delta_{n+1}} M^{n+1} \xrightarrow{d_{n+1}} M^n \to 0$$

where Δ_k is the diagonal morphism

$$\begin{aligned} \Delta_k : M &\longrightarrow M^k, \\ m &\longmapsto (\underbrace{m, m, \ldots, m}_{k}) \end{aligned}$$

and d_{k+1} the difference morphismfism

$$\begin{aligned} d_{k+1} : M^{k+1} &\longrightarrow M, \\ (m_0, \ldots, m_k) &\longmapsto (m_1 - m_0, \ldots, m_k - m_0). \end{aligned}$$

As $\Delta_{n+1}(m) = 0$ if and only if $m = 0$, we have $\ker \Delta_{n+1} = 0$. Then

$$d_{n+1}(m_0, \ldots, m_n) = (m_1 - m_0, \ldots, m_n - m_0) = (0, \ldots, 0)$$

if and only if $m_k = m_0$ for $k = 1, \ldots, n$. Hence $\ker d_{n+1} = \operatorname{im} \Delta_{n+1}$. Finally, d_{n+1} is surjective, because for any $(m_1, \ldots, m_n)$ we can see that

$$d_{n+1}(0, m_1, \ldots, m_n) = (m_1 - 0, \ldots, m_n - 0) = (m_1, \ldots, m_n).$$

In other words, the $\operatorname{im} d_{n+1} = M^n$.

Often we elimnate the symbol $\circ$ from the notation $g \circ f$ and write, simply, gf. Consider an exact sequence of groups

$$H' \xrightarrow{f} H \xrightarrow{g} G \xrightarrow{h} G''$$

with f an epimorphism and h a monomorphism. Then $im\ f = H$ and $\ker h = e$. As the sequence is exact, $H = im\ f = \ker g$ and $im\ g = \ker h = e$; then, g is the trivial homomorphism. Inversely, if g is the trivial homomorphism, then f is an epimorphism and h is a monomorphism. Thus, we have

1.6 Proposition. If

$$H' \xrightarrow{f} H \xrightarrow{g} G \xrightarrow{h} G''$$

is an exact sequence of groups, h is monomorphism if and only if g is trivial; g is trivial if and only if f is an epimorphism.

So, when we have a short exact sequence as follows

$$e \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow e$$

we will write it, indistinctly, as

$$G' \overset{f}{\rightarrowtail} G \overset{g}{\twoheadrightarrow} G''$$

where $\rightarrowtail$ denotes injective and $\twoheadrightarrow$ surjective.

1.7 Definition. Let G, G', H, H' be groups, with f, f', g, g' group homomorphisms. We say that a **diagram**

$$\begin{array}{ccc} G & \xrightarrow{f'} & H \\ {\scriptstyle g'}\downarrow & & \downarrow{\scriptstyle f} \\ G' & \xrightarrow{g} & G'' \end{array}$$

commutes if $f \circ f' = g \circ g' \colon G \longrightarrow H'$.

1.8 Proposition. Let $G' \overset{f'}{\rightarrowtail} G \overset{f}{\twoheadrightarrow} G''$ and $H' \overset{g'}{\rightarrowtail} H \overset{g}{\twoheadrightarrow} H''$ be two short exact sequences, and suppose that, in the following commutative diagram

$$\begin{array}{ccccc} G' & \overset{f'}{\rightarrowtail} & G & \overset{f}{\twoheadrightarrow} & G'' \\ \downarrow{\scriptstyle h'} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle h''} \\ H' & \overset{g'}{\rightarrowtail} & H & \overset{g}{\twoheadrightarrow} & H'' \end{array}$$

two of the three homomorphisms h', h, h'' are isomorphisms. Then the third is also an isomorphism.

Proof. Suppose that h' and h'' are isomorphisms. We will show that h is a monomorfism: let $x \in \ker h$; then $gh(x) = g(e_H) = h''f(x) = e_{H''}$. As h'' is an isomorphism, then $f(x) = e_{G''}$. Thus there exists an $x' \in G'$ such that $f'(x') = x$, because the sequence on top is exact. Then $hf'(x') = h(x) = e_H = g'h'(x')$. As $g'h'$ is injective, then $x' = e_G$. Hence, $f'(x') = x = e_G$.

Now we will show that h is an epimorphism. Let $y \in H$. As $h''$is an isomorphism, there exists $x'' \in G''$ such that $g(y) = h''(x'')$. As f is surjective, there exists $z \in G$ such that $f(z) = x''$. Hence,

$$g(y-h(z)) = g(y)-gh(z) = g(y)-h''f(z) = g(y)-h''(x'') = g(y)-g(y) = e_{H''}.$$

Thus, $y - h(z) \in \ker g$. As the sequence on the bottom is exact, there exists $y' \in H'$ with $g'(y') = y - h(z)$. As h' is an isomorphism, there exists $x' \in G'$ such that $h'(x') = y'$. Thus,

$$h(f'(x') + z) = hf'(x') + h(z) = g'h'(x') + h(z) = g'(y') + y - g'(y') = y.$$

If we define $x = f'(x') + z$, we have $h(x) = y$. The other two possible cases are left as an exercise, see Problem 1.6.♦

Observe that the previous proposition establishes the isomorphisms only when there exists a function $h \colon G \longrightarrow H$ compatible with the given isomorphisms and the diagram commutes. For example, if we consider the following

diagram

$$\begin{array}{ccccccccc} e & \longrightarrow & Z_2 & \xrightarrow{\times_2} & Z_4 & \longrightarrow & Z_2 & \longrightarrow & e \\ & \| & & & \| & & \| & & \\ e & \longrightarrow & Z_2 & \longrightarrow & Z_2 \times Z_2 & \longrightarrow & Z_2 & \longrightarrow & e \end{array}$$

we know that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not isomorphic to a $\mathbb{Z}_4$.

Let $\{C_n\}_{n \in Z}$ be a family of abelian groups and $\{\partial_n : C_n \longrightarrow C_{n-1}\}_{n \in \mathbb{Z}}$ a family of homomorphisms of abelian groups such that $\partial_n \circ \partial_{n+1} = 0$. The pair $C = \{C_n, \partial_n\}$ will be called a **chain complex** (or **chain**) , and we write

$$C : \cdots \longrightarrow C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \longrightarrow \cdots$$

In other words, a chain complex (or chain) is a descending semiexact sequence of abelian groups with indices in $\mathbb{Z}$.

Let $C = \{C_n, \partial_n\}$ and $D = \{D_n, \partial'_n\}$ be two chain complexes of abelian groups. A **chain morphism** $\varphi : C \longrightarrow D$ is a family of group homomorphisms of abelian groups $\{\varphi_n : C_n \longrightarrow D_n\}$ such that the squares of the following diagram commute:

$$\begin{array}{ccccccccc} C : \cdots & \xrightarrow{\partial_{n+2}} & C_{n+1} & \xrightarrow{\partial_{n+1}} & C_n & \xrightarrow{\partial_n} & C_{n-1} & \xrightarrow{\partial_{n-1}} & \cdots \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ D : \cdots & \xrightarrow{\partial'_{n+2}} & D_{n+1} & \xrightarrow{\partial'_{n+1}} & D_n & \xrightarrow{\partial'_n} & D_{n-1} & \xrightarrow{\partial'_{n-1}} & \cdots \end{array}$$

Problems

1.1 Define appropriate homomorphisms so that, for a prime number p, the sequences

$$O \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}_{p^2} \longrightarrow \mathbb{Z}_p \longrightarrow O$$
$$O \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}_p \longrightarrow O$$

are short exact.

1.2 Prove that , in an exact sequence of groups,

$$G' \xrightarrow{f} G \xrightarrow{g} G'' \xrightarrow{h} H \xrightarrow{k} H'$$

f is an epimorphism and k is a monomorphism if and only if $G'' = e$.

1.3 Prove that if $e \longrightarrow G \longrightarrow e$ is an exact sequence of groups, then $G = e$.

1.4 Let

$$G' \xrightarrow{f} G \xrightarrow{g} G'' \xrightarrow{h} H' \xrightarrow{k} H \xrightarrow{q} H''$$

be an exact sequence of groups. Show that g, k are trivial homomorphisms if and only if h is an isomorphism, and h is an isomorphism if and only if f is an epimorphism and q a monomorphism.

1.5 Prove that if

$$e \longrightarrow H' \xrightarrow{h} G \longrightarrow e$$

is an exact sequence of groups then h is an isomorphism.

1.6 Prove the two cases that are left in Proposition 1.8.

1.7 Let $\{C^n\}_{n \in Z}$ be a family of abelian groups and $\{\delta^n : C^n \longrightarrow C^{n+1}\}_{n \in \mathbb{Z}}$ a family of homomorphisms of abelian groups such that $\delta^{n+1} \circ \delta^n = 0$. We will call the pair $C = \{C^n, \partial^n\}$ a **cochain complex** (or **cochain**) and we will write it as

$$C : \cdots \longrightarrow C^{n-1} \xrightarrow{\partial^{n-1}} C^n \xrightarrow{\partial^n} C^{n+1} \xrightarrow{\partial^{n+1}} \cdots$$

In other words, a cochain complex (or cochain), is an ascending semiexact sequence of abelian groups with indices in $\mathbb{Z}$. Define the concept of **morphism of cochains** $\Psi : C \longrightarrow D$.

2.2 Quotient Groups

Consider the first example of section 1. We distributed the integers in three boxes, where none of them were in two or more of the boxes, only in one of them. We labelled the boxes with three labels. We gave a group structure to the set of boxes by defining a binary operation. The reader verified that, indeed, we had a commutative group. We will call the boxes **cosets** and we will call the group a **quotient group**. In this case it is the quotient of $\mathbb{Z}$ "modulo" $3\mathbb{Z}$, which we will denote $\mathbb{Z}_3$.

Recall the concept of vector space quotient studied in Linear Algebra (see [Ll2]) and consider the additive part for the case in which G is an abelian group and H a subgroup of G, with $x \in G$; we denoted as $x + H$ the set $\{x + y | y \in H\}$. These elements, $x + H$, will be called **cosets** of H in G. As $0 \in H$ and $x = x + 0 \in x + H$, each $x \in G$ belongs to a coset. It was verified that any two cosets are either equal, or their intersection is empty (they are disjoint). The set of all cosets of H in G was denoted as G/H and G/H was given a group structure by

$$+ \colon G/H \times G/H \to G/H$$

such that

$$((x + H), (y + H)) \longmapsto ((x + y) + H).$$

It was also proved that this binary operation is well defined and that it defines an abelian group structure (the additive part of the vector space) in G/H. We wil call G/H, the **quotient group** of G modulo H.

It was also seen that H is a subgroup of the group G and if $y \in x + H$, then there exists $w \in H$ such that $y = x + w$. Hence $y - x = w \in H$. Therefore, if $y - x \in H$ then $y - x = w \in H$. Thus $y = x + w \in x + H$, and $y - x \in H \iff -(y - x) = x - y \in H \iff x \in y + H$. In synthesis,

$$y \in x + H \iff y - x \in H \iff x \in y + H.$$

Finally, we saw $p \colon G \to G/H$ given by $x \longmapsto x + H$. If $x, w \in G$, then

$$p(x + w) = (x + w) + H = (x + H) + (w + H) = p(x) + p(w).$$

Hence, p is a homomorphism called the **canonical projection**.

All of this was done for vector spaces over a field K. However, recall that the additive part of a vector space is an abelian group.

What about the non-commutative case? What happens? We will imitate the previous development and adjust it to the non-commutative context. To begin, we consider, once again, the first example of section 1. An equivalence relation called congruence modulo 3 was taken, where $x \equiv y \ (mod\ 3)$ if and only if $3| - x + y$, or, in other words, $-x + y \in 3\mathbb{Z}$. What we will do, is generalize

this equivalence relation to non abelian groups, using multiplicative notation as follows:

2.1 Definition. Consider the subgroup H of a group $(G, \cdot)$ and elements $x, y \in G$. We say that x is **congruent on the left with** y if $x^{-1}y \in H$ (that is, if $y = xh$ for some $h \in H$) and we denote it as $x \equiv_i y \ (mod\ H)$. Analogously, we say that x is **congruent on the right with** y if $xy^{-1} \in H$ and we denote it as $x \equiv_d y \ (mod\ H)$.

Observe that, in the abelian case, the concepts of left and right congruence coincide, given that $x^{-1}y \in H$ if and only if $(x^{-1}y)^{-1} = y^{-1}x = xy^{-1} \in H$.

2.2 Proposition. The left and right congruence relations are equivalence relations.
Proof. As $x \equiv_i x \ (mod\ H) \iff x^{-1}x = e \in H$, the relation is reflexive. As $x \equiv_i y \ (mod\ H) \iff x^{-1}y \in H \iff (x^{-1}y)^{-1} \in H \iff y^{-1}x \in H \iff y \equiv_i x \ (mod\ H)$ the relation is symmetric. Finally, if $x \equiv_i y \ (mod\ H)$ and $y \equiv_i z \ (mod\ H)$ then $x^{-1}y \in H$ and $y^{-1}z \in H$. Hence $(x^{-1}y)(y^{-1}z) \in H \iff x^{-1}ez = x^{-1}z \in H$. Thus $x \equiv_i z \ (mod\ H)$ and the relation is transitive. Analogously for the right congruence.♦

2.3 Proposition. The left and right equivalence clases $[x]$ of the relation defined can be expressed as

$$xH = \{xh | h \in H\}$$

and

$$Hx = \{hx | h \in H\}$$

respectively.
Proof. The equivalence classes of any element x of G can be expressed as (using the symmetry):

$$\begin{aligned}
[x] &= \{y \in G | y \equiv_i x \ (mod\ H)\} \\
&= \{y \in G | x \equiv_i y \ (mod\ H)\} \\
&= \{y \in G | x^{-1}y = h \in H\} \\
&= \{y \in G | y = xh; h \in xH\} \\
&= \{xh | h \in H\} = xH.
\end{aligned}$$

The same is true for the equivalence classes under the relation of right congruence modulo H .♦

Observe that a group G is the union of the left or right cosets of H in G. Similarly, two cosets are either disjoint or the same. We will call the equivalence clases xH and Hx the **left cosets and right cosets** respectively..

Consider the set of all left cosets, and denote it as G/H. We want to give the set a group structure and make the **natural or canonical projection** $p : G \longrightarrow G/H$ a homomorphism. This is not always possible, but we will see what conditions will allow it.

2.4 Definition. We say that a subgroup H of G is **normal** in G (denoted $H \lhd G$) if for every $x \in G$, $xHx^{-1} \subset H$ where $xHx^{-1} = \{xhx^{-1} | h \in H\}$.

Given that $xHx^{-1} \subset H$ holds for every element $x \in G$ by this definition, in particular it holds for $x^{-1} \in G$. Then, $x^{-1}Hx \subset H$. Thus, for every $h \in H$, $h = x(x^{-1}hx)x^{-1} \in xHx^{-1}$. Then $H \subset xHx^{-1}$ and $xHx^{-1} = H$. From here it is easy to see that every left coset is a right coset and that $xH = Hx$ for every $x \in G$ (Problema 2.4). We also observe that every subgroup of an abelian group is normal and that the trivial subgroups are normal in G (Problema 2.5).

2.5 Proposition. A subgroup H of G is normal if and only if $(xH)(yH) = (xy)H$ for every $x, y \in G$.
Proof. Suppose that H is normal and we take any two elements $x, y \in G$. It is easy to see that $(xH)(yH) = (xyH)$ Problem 2.9. Now, suppose that $(xH)(yH) = (xy)H$ for every $x, y \in G$. Let $h \in H$ and $x \in G$ be arbitrary. Then

$$xhx^{-1} = (xh)(x^{-1}e) \in (xH)(x^{-1}H) = eH = H,$$

and H is normal.♦

2.6 Theorem. Let H be a normal subgroup of G. Then G/H is a group with a binary operation

$$\cdot : G/H \times G/H \longrightarrow G/H$$

given by

$$((xH), (yH)) \mapsto \cdot((xH), (yH)) = (xH) \cdot (yH) = (xH)(yH) = (xy)H.$$

In addition, the canonical projection $p : G \longrightarrow G/H$ is an epimorphism whose kernel is H, i.e. $\ker p = H$.
Proof. It is immediate to see that the group axioms hold in G/H with $eH = H$ as the identity element and $x^{-1}H$ as the inverse of xH. As $p(xy) = (xy)H = (xH)(yH) = p(x)p(y)$ and p is surjective, then it is an epimorphism. Finally,

$$\begin{aligned} \ker(p) &= \{x \in G | p(x) = eH = H\} = \\ &= \{x \in G | xH = H\} = \{x \in G | x \in H\} \\ &= H. \blacklozenge \end{aligned}$$

2.7 Corollary. If $H \lhd G$ then H is the kernel of the homomorphism g from G into G' for a group G', i.e. $H = \ker(g : G \longrightarrow G')$ for a group G'.
Proof. As H is normal, then it is the kernel of an epimorphism, as in the previous theorem.♦

2.8 Proposition. If $H = \ker(g : G \longrightarrow G')$ for a group G' then $H \lhd G$.
Proof. Let $h \in H$ and $x \in G$ be arbitrary. Then

$$g(xhx^{-1}) = g(x)g(h)g(x^{-1}) = g(x)eg(x^{-1}) = g(x)(g(x))^{-1} = e.$$

Therefore, $xhx^{-1} \in \ker(g : G \longrightarrow G') = H$.♦

By the previous corollary and proposition, the normality condition is necessary, and sufficient, for the concept of quotient group.

2.9 Theorem. (**Lagrange**) If G is a group of order n and $H < G$, then $o(H)|o(G)$.
Proof. As G is the union of its left cosets, the number of elements n of G, is equal to the product of the number of left cosets r times the number of elements of each set $m = o(H)$ because the cosets of H has the same number of elements m (Problem 2.2) and they are either disjoint or equal. Thus, $n = rm$, that is, $o(H)|o(G)$.♦

The number of left (or right) cosets of a subgroup $H < G$ will be denoted $(G : H)$ and we will call it the **índex** of H in G, that is, $(G : H) = o(G/H)$. By Problem 2.4, the index of H in G does not depend if left or right cosets are considered, and it can be finite or infinite. Clearly, as each coset has $o(H)$ elements, $(G : H) = o(G)/o(H)$.

2.10 Corollary. If the order of a group G es prime, then G is cyclic.
Proof. Let $p = o(G)$ and (x) the cyclic subgroup generated by the element $x \neq e \in G$. By the Theorem of Lagrange $2 \leq o((x))$, and $o((x))|p$. Then, $o((x)) = p$, thus $(x) = G$ and G is cyclic.♦

From the previous corollary we can infer that there exists one, and only one, group (up to isomorphism) of prime order.Observe that a group of prime order cannot have nontrivial proper subgroups. The trivial subgroups G and e are normal in G. Hence G/G is the trivial group e and G/e is isomorphic to G. We say that a group G is **simple** if its only normal subgroups are trivial. The alternating group A_n is simple for $n \geq 5$ as we will see in the following chapter.

Finally we have the following

2.11 Theorem. Let (x) be a cyclic group generated by x and $h : (x) \longrightarrow H$ a group homomorphism. Then $im\ h = h((x))$ is a cyclic subgroup of H.
Proof. Suppose that (x) has order n. If h is a homomorphism and x generates (x), as $h(x^r) = [h(x)]^r$ (Problem 2.13), then $h(x)$ generates $im\ h$ because $h(e) = (h(x^n) = [h(x)]^n = e$.♦

Example. The human brain perceives two pitches as essentially identical when their frequencies have a ratio equal to 2^r with $r \in \mathbb{Z}$. That is, it "identifies" two

frequencies $u, w \in (x) < (\mathbb{R}^*, \cdot)$ when $u^{-1}w \in (x^{12})$, where x is the real number given by the equation (**??**). Indeed,

$$x^{12} = (\sqrt[12]{2})^{12} = 2$$

and $u^{-1}w = \frac{w}{u} \in (2) = (x^{12})$ means that $\frac{w}{u} = 2^r$ for some $r \in \mathbb{Z}$.

Given that

$$\begin{aligned} h : \mathbb{Z} &\to (x), \\ n &\mapsto x^n, \end{aligned}$$

defines an isomorphism between $\mathbb{Z}$ and (x), the pitches which are essentially different to the human ear happen to be those whose quotient is

$$\frac{(x)}{(x^{12})} \cong \frac{\mathbb{Z}}{12\mathbb{Z}} = \mathbb{Z}_{12};$$

the reader should verify that, indeed, $(x^{12}) \cong 12\mathbb{Z}$ under the isomorphism h.

This way one justifies the abuse of nomenclature committed when identifying elements of $\mathbb{Z}$ and $\mathbb{Z}_{12}$ with pitches. It is also very useful for defining the concept of scale in a rigurous manner. A **scale** E is a subset of $\mathbb{Z}$ (which we see as pitches) such that

$$e^{12}(E) = E + 12 = E$$

that is, $x + 12 \in E$ for every $x \in E$.

The scales are well behaved under the canonical projection $p : \mathbb{Z} \to \mathbb{Z}_{12} = \frac{\mathbb{Z}}{12\mathbb{Z}}$, in the sense that

$$p^{-1}(p(E)) = E.$$

The set $p(E) \subseteq \mathbb{Z}_{12}$ is called the **chord of the scale**[1]. Generally the abuse of nomenclature is committed when referring to a scale by its chord, as in the example from Chapter 1, Section 1.

In fact, given a subset $S \subseteq \mathbb{Z}_{12}$, we define a scale as

$$E = p^{-1}(S);$$

the reader should prove that this, indeed, defines a scale and that the chord of this scale is S. For example, the scale that comes from $S = \mathbb{Z}_{12}$ is exactly the chormatic scale.

Let $C = \{C_n, \partial_n\}$ be a chain complex, or chain. The **homology group of degree** nC, $H_n(C)$ is defined as the quotient $H_n(C) = \ker \partial_n / im\ \partial_{n+1}$. That is, given a chain

$$C : \cdots \longrightarrow C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \longrightarrow \cdots$$

we consider the kernel of $\partial_n, \ker \partial_n \subset C_n$, and the image of $im\ \partial_{n+1} \subset C_n$, and we form the quotient $\ker \partial_n / im\ \partial_{n+1}$. Note that C is a semiexact sequence,

[1] In chapter 3, section 2, we will see that this is a very appropriate name.

that is, $im\ \partial_{n+1} \subset \ker \partial_n$, and that the quotient $H_n(C) = \ker\ \partial_n / im\ \partial_{n+1}$ measures the inexactness of C. Indeed, if C is exact, then $im\ \partial_{n+1} = \ker \partial_n$ and $H_n(C) = 0$.

The elements of C_n are known as **chains of degree** n, and the homomorphisms ∂_n are called **diferentials** or **boundary operators** . The elements of the kernel of ∂_n are called **cycles of degree** n, denoted as $Z_n(C)$ and the elements of the image of ∂_{n+1} are called **boundaries of degree** n, denoted as $B_n(C)$. Thus, $H_n(C) = Z_n(C)/B_n(C)$.

We say that two elements of $H_n(C)$ are **homologous** if they belong to the same coset. The element of $H_n(C)$, determined by the cycle c of degree n, is called the **homology class** of c and is denoted by $[c]$. Then, for each $n \in Z$, we define a homology group $H_n(C)$. We call $H_*(C) = \{H_n(C)\}$ the **homology of the chain** C.

Problems

2.1 Prove that the right congruence relation is an equivalence relation.

2.2 Show that all the cosets of a subgroup H of a group G have the same number of elements, that is $o(xH) = o(H) = o(Hx)$ for every $x \in G$.

2.3 Find all the cosets of the subgroup $H = \{0, 3\}$ of Δ_3 of the rigid movements of the equilateral triangle.

2.4 Show that if $xHx^{-1} = H$, every left coset is a right coset and that $xH = Hx$ for every $x \in G$. Deduce that this implies that, for every $x \in G$, $xHx^{-1} \subset H$.

2.5 Prove that every subgroup of an abelian group is normal.

2.6 Prove that under a group homomorphism the homomorphic image of a normal subgroup is normal.

2.7 Prove that under a homomorphism, the inverse image of a normal subgroup is a normal subgroup in the domain.

2.8 Show that a group G is the union of its left or right cosets of H in G and that two cosets are either disjoint or equal.

2.9 Verify that $(xH)(yH) = (xyH)$ in proof 2.5.

2.10 Prove that the order of an element x of a finite group G divides the order of the group.

2.11 Prove that if N, H, G are groups such that $N < H < G$, then $(G : N) = (G : H)(H : N)$ and that if two of these indices are finite, then the third also is.

2.12 Prove that a quotient group of cyclic group is cyclic.

2.13 Prove that $h(x^r) = [h(x)]^r$, in the proof of the last theorem of this section.

2.14 In a group G, an element $xyx^{-1}y^{-1}$ is called a **commutator**. Prove that the set of commutators generates a normal subgroup of G, denoted a G' and that the quotient G/G' is abelian.

2.15 Let $C = \{C^n, \delta^n\}$ be a complex of cochains. Define the **cohomology group of degree** n **of** C, $H^n(C)$.

2.3 Isomorphism Theorems

3.1 Definition. An **automorphism** of a group G is an isomorphism of G into G.

For every element $x \in G$, the function

$$\begin{array}{rl} \iota_x : & G \longrightarrow G \text{ given by} \\ & y \longmapsto xyx^{-1} \end{array}$$

is an automorphism of G, see Problem 3.1, called **inner automorphism**. In these terms we can say that H is a normal (or invariant) subgroup if and only if H is invariant under every inner automorphism of G.

3.2 Proposition. Let $H \lhd G$ and $H' \lhd G'$. Consider the cannonical projections to the corresponding quotients $p : G \longrightarrow G/H$ y $p' : G' \longrightarrow G'/H'$. If $g : G \longrightarrow G'$ is a group homomorphism such that $g(H) \subset H'$, then $g^* : G/H \longrightarrow G'/H'$ given by $xH \mapsto g^*(xH) = g(x)H'$ is well defined and is a group homomorphism called the **homomorphism induced by g in the quotient groups**. The following square is also commutative

$$\begin{array}{ccc} G & \xrightarrow{g} & G' \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p'} \\ G/H & \xrightarrow{g^*} & G'/H' \end{array}$$

and $im\ g^* = p'(im\ g)$ and $\ker g^* = p(g^{-1}(H'))$.

Proof. If $x \in G$ and $y \in H$ are arbitrary, given that $g(xy) = g(x)g(y) \in g(x)g(H) \subset g(x)H'$, the image of xH under g is contained in a unique coset of H', say $g(xH) \subset g(x)H'$. Then, we define

$$\begin{array}{rccl} g^* : & G/H & \longrightarrow & G'/H' \text{ such that} \\ & xH & \longrightarrow & g^*(xH) = g(x)H'. \end{array}$$

It is immediate to prove that g^* is well defined and to prove it is a homomorphism, consider any cosets xH and $x'H$. Then,

$$\begin{aligned} g^*((xH)(x'H)) &= g^*((xx')H)) \\ &= g(xx')H' \\ &= (g(x)g(x'))H' \\ &= (g(x)H')(g(x')H') \\ &= g^*(xH)g^*(x'H). \end{aligned}$$

We will show that the square commutes: consider and element x of G. Then $(p' \circ g)(x) = p'(g(x)) = g(x)H' = g^*(xH) = g^*(p(x)) = (g^* \circ p)(x)$. Thus $(p' \circ g) = (g^* \circ p)$. As p and p' are epimorphisms, it is also clear that $im\ g^* = p'(im\ g)$ y $\ker\ g^* = p(g^{-1}(H'))$.♦

3.3 Theorem. Under the same hypothesis of the previous proposition, in particular, if g is an epimorphism with $H' = e$ and $H = \ker\ g$ then $G'/H' \cong G'$ and g^* is an isomorphism in the following commutative diagram:

$$\begin{array}{ccc} G & \overset{g}{\twoheadrightarrow} & G' \\ {\scriptstyle p}\downarrow & & \cong\downarrow{\scriptstyle p'} \\ G/\ker g & \overset{g*}{\longrightarrow} & G' \end{array}$$

Proof. If g is an epimorphism with $H' = e$ and $H = \ker\ g$ then $G' = G'/H'$ and g^* is an isomorphism. As $\ker\ g^* = p(g^{-1}(e)) = p(\ker g) = p(H) = eH = e_{G/H} = e$, then g^* is a monomorphism and as $im\ g^* = p'(im\ g) = G'$ then g^* is an epimorphism, hence an isomorphism.

Thus we have the following commutative diagram

$$\begin{array}{ccc} G & \overset{g}{\twoheadrightarrow} & G' \\ {\scriptstyle p}\downarrow & & \cong\downarrow{\scriptstyle I_{G'}} \\ G/\ker g & \overset{g*}{\longrightarrow} & G' \end{array} \quad ♦$$

3.4 Theorem. Let $H \lhd G$ and, as a particular case of the previous theorem, $e = H' \lhd G'$ with $H \subset \ker g$. Then there is a unique homomorphism $g^* : G/H \longrightarrow G'$ given by $xH \mapsto g^*(xH) = g(x)H' = g(x)$. Also, $\ker g^* = \ker g/H$ and $im\ g = im\ g^*$. g^* is an isomorphism if and only if, g is an epimorphism and $H = \ker g$.

Proof. By the previous theorem, g is a homomorphism. It is unique since it is determined by g. Also, $xH \in \ker g^*$ if and only if $g(x) = e$, which happens if and only if $x \in \ker g$. So, $\ker g^* = \{xH | x \in \ker g\} = \ker g/H$. Clearly $im\ g = im\ g^*$. Finaly, g^* is an epimorphism if and only if g is an epimorphism and g^* is a monomorphism if and only if $\ker g^* = \ker g/H$ is the trivial subgroup of G/H which happens when $\ker g = H$.♦

3.5 Corollary. (**First Isomorphism Theorem**). Under the same hipotheses as the previous theorem $G/\ker\ g \cong im\ g$.
Proof. As g is an epimorphism, $im\ g = G'$, then $G/\ker\ g \cong im\ g$.♦

In other words, if $g : G \twoheadrightarrow G'$ is an epimorphism of groups with kernel $\ker g$, then there exists a unique isomorphism $g^* : G/\ker g \cong G'$, such that $g = g^* \circ p$, that is, any homomorpism of G with kernel $\ker g$ has an image that is isomorphic to $G/\ker g$. Even more, it tells us that any epimorphism $g : G \twoheadrightarrow G'$ has as its codomain a quotient group, that is, the codomain of g is the quotient of the domain of g modulo the kernel of g. It also tells us which isomorphism: that in which $im\ g = im\ g^*$. This result, $G/\ker g \cong im\ g$ is known as the **First Isomorphism Theorem.** Given a group and a normal subgroup we can "determine" the quotient group without having to establish the cosets, as we will see later on.

3.6 Example. Let H be a normal subgroup of a group G. Consider the quotient group G/H. Let $i\colon H \longrightarrow G$ be an inclusion monomorphism and $p\colon G \longrightarrow G/H$ the projection epimorphism. Then $im\ i = H = \ker\ p$, hence:

$$e \longrightarrow H \xrightarrow{i} G \xrightarrow{p} G/H \longrightarrow e$$

is a short exact sequence. Consider now a short exact sequence

$$e \xrightarrow{h} G' \xrightarrow{f} G \xrightarrow{g} G'' \xrightarrow{k} e.$$

Then $im\ f = \ker g$, f is a monomorphism (because $e = im\ h = \ker f$) and g is an epimorphism (because $im\ g = \ker k = G''$). Let $H = im\ f = \ker g$ which is a normal subgroup of G, then f establishes an isomorphism $H \xrightarrow{\cong} G'$ and g establishes another isomorphism $G/H \xrightarrow{\cong} G''$ by the first isomorphism theorem. Hence a short exact sequence is equivalent to a sequence of a subgroup and a quotient group of a group.

3.7 Example. $g : G \twoheadrightarrow G'$ where $G = \mathbb{Z}$ and $G' = \mathbb{Z}_n$ is an epimorphism with the kernel being the subgroup $n\mathbb{Z}$, that is,

$$e \longrightarrow n\mathbb{Z} \longrightarrow \mathbb{Z} \xrightarrow{g} \mathbb{Z}_n \longrightarrow e$$

is a short exact sequence. Then, by the previous theorem, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

3.8 Example. Let G be the multiplicative group of real numbers different from zero $\mathbb{R}^*$ and G' is the multiplicative group of the positive reals $\mathbb{P}^*$. Consider the epimorphism $g : G \twoheadrightarrow G'$ given by $x \mapsto g(x) = |x|$ where $|x|$ denotes the absolute value of x. The kernel of g is $\{\pm 1\}$. Then the sequence

$$e \longrightarrow \{\pm 1\} \longrightarrow \mathbb{R}^* \xrightarrow{g} \mathbb{P}^* \longrightarrow e$$

is exact. By the previous theorem, the quotien group $\mathbb{R}^*/\{\pm 1\}$ is isomorphic to $\mathbb{P}^*$.

3.9 Example. Let G be the additive group of the real numbers $\mathbb{R}$ and G' the multiplicative group of complex numbers $\mathbb{S}^1$ with absolute value equal to 1. Let

$g : G \twoheadrightarrow G'$ be the epimorphism given by $\theta \mapsto g(\theta) = e^{2\pi i\theta}$. Its kernel is $\mathbb{Z}$. Then the sequence

$$e \longrightarrow \mathbb{Z} \longrightarrow \mathbb{R} \xrightarrow{g} \mathbb{S}^1 \longrightarrow e$$

is exact and by the previous theorem, $\mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1$.

We will generalize the concept of coset:

3.10 Definition. Let H and N be any two subgroups of a group G. The **product** of H and N is $HN = \{xy | x \in H, y \in N\}$.

Thus, a left coset is $xH = \{x\}H$, for $x \in G$. We can generalize this concept and define, for a family of subgroups $\{H_i | i \in I\}$ with I a set of linearly ordered indices

$$\prod_{i \in I} H_i = \{x_1 x_2 x_3 \cdots x_j | x_k \in H_{i_k}, i_1 < i_2 < \cdots < i_j, j \geq 0\}.$$

Observe that HN is not necessarily a subgroup of G because the product of the multiplication of two of its elements is not necessarily in HN. If G is abelian then it is a subgroup of G.

3.11 Theorem. (**Second Isomorphism Theorem**). Let $H < G$, $N \lhd G$. Then $(HN)/N \cong H/(H \cap N)$.

Proof. As $N \lhd G$, it is easy to see that $(H \cap N) \lhd H$. Define

$$h : HN \longrightarrow H/(H \cap N) \text{ given by } xy \mapsto h(xy) = x(H \cap N).$$

We will see that h is well defined: Suppose that $x_1 y_1 = xy$, then $x^{-1}x_1 = yy_1^{-1}$. Thus, $x^{-1}x_1 \in H$ and $x^{-1}x_1 \in N$, then $x^{-1}x_1 \in H \cap N$. Hence, in $H/(H \cap N)$, $x(H \cap N) = x_1(H \cap N)$ and $h(xy) = h(x_1 y_1)$.

We will verify that h is a homomorphism. As $N \lhd G$, $x_1 y_2 = y_2 x_3$. Then, $h((x_1 y_1)(x_2 y_2)) = h((x_1 x_2)(y_3 y_2)) = x_1 x_2 (H \cap N) = x_1(H \cap N) x_2 (H \cap N) = h(x_1 y_1) h(x_2 y_2)$.

As $ker\ h = \{xy \in HN | x \in H \cap N\} = N$ and as $h(xe) = x(H \cap N)$ for every $x \in H$, using the First Isomorphism Theorem, $HN/N \cong H/(H \cap N)$.♦

3.12 Ejemplo. Consider

$$\begin{aligned} G &= \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}, \\ H &= \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \{0\} \text{ y} \\ N &= \{0\} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}. \end{aligned}$$

Then

$$\begin{aligned} HN &= \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \text{ y} \\ H \cap N &= \{0\} \times \mathbb{Z} \times \mathbb{Z} \times \{0\}. \end{aligned}$$

Therefore,

$$HN/N \cong \mathbb{Z} \cong H/(H \cap N).$$

3.13 Theorem. (**Third Isomorphism Theorem**). Let $H \lhd G$ and $N \lhd G$ with $N < H$. Then, $G/H \cong (G/N)/(H/N)$.
Proof. We define

$$\begin{array}{rl} h: & G \longrightarrow (G/N)/(H/N) \text{ by} \\ & x \longmapsto (xN)(H/N). \end{array}$$

As

$$\begin{aligned} h(xy) &= ((xy)N)(H/N) = ((xN)(yN))(H/N) \\ &= [(xN)(H/N)][(yN)(H/N)] = h(x)h(y), \end{aligned}$$

h is a homomorphism. Its kernel is $\ker h = \{k \in G | h(k) = H/N\}$. These are, exactly, the elements of H. Using the First Isomorphism Theorem, $G/H \cong (G/N)/(H/N)$.

$$\begin{array}{ccccc} \ker h & \hookrightarrow & G & \longrightarrow & G/H \\ \| & & \downarrow & & \downarrow \cong \\ H & & G/N & \longrightarrow & (G/N)\,/\,(H/N) \end{array} \quad \blacklozenge$$

3.14 Example. Consider $N = 6\mathbb{Z} < H = 2\mathbb{Z} < G = \mathbb{Z}$. Then $G/H = \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$. $G/N = \mathbb{Z}/6\mathbb{Z}$. We can see that , $(\mathbb{Z}/6\mathbb{Z})/(2\mathbb{Z}/6\mathbb{Z})$ also has 2 elements and is isomorfic to $\mathbb{Z}_2$.

Problems

3.1 Prove that for every element $x \in G$, the homomorphism

$$\begin{array}{rl} \iota_x: & G \longrightarrow G \text{ given by} \\ & y \mapsto xyx^{-1} \end{array}$$

is an automorphism of G, called the **inner automorphism**.

3.2 Consider the set of all inner automorphisms of a group G, denoted $In(G)$. Prove that it is a group under the operation of composition.

3.3 Consider the set $Aut(G)$ of all automorphisms of the group G. Prove that $Aut(G)$ is a group under composition and that $In(G) \lhd Aut(G)$. Two automorphisms f, g are said to belong to the same "**automorphism class**" if $f = h \circ g$ for some automorphism h. Prove that the automorphism classes form a group $Aut(G)/In(G)$ called "**outer automorphisms** of G".

3.4 Provide the details, in the proof of Theorem 3.2, which show that g^* is well defined. Prove, as well, that $im\ g^* = p'(im\ g)$ and $\ker g^* = p(g^{-1}(H'))$.

3.5 Provide the complete details of the proof of Theorem 3.4.

3.6 We will call the quotient groups of a homomorphism of abelian groups $g : G \longrightarrow G''$, the **coimage** and **cokernel**, if

$$\begin{aligned} coim\ g &= G/\ker\ g \\ \operatorname{coker}\ g &= G''/im\ g. \end{aligned}$$

Let $g\colon G \longrightarrow G''$ be a homomorphism of abelin groups. Prove that the sequence

$$e \longrightarrow \ker g \longrightarrow G \longrightarrow G'' \longrightarrow \operatorname{coker}\ g \longrightarrow e$$

is exact. Observe that, in this context, the First Isomorphism Theorem says that $coim\ g \cong im\ g$.

3.7 Prove that a group homomorphism $g : G \to G''$ is a monomorphism if and only if $\ker\ g = e$ and is a epimorphism if and only if $\operatorname{coker}\ g = e$.

3.8 Verify that the sequences shown in the examples are, indeed, short exact sequences.

2.4 Products

Recall that if H and N are any two subgroups of a group G, the product of H and N is $HN = \{xy|x \in H, y \in N\}$ and for a family of subgroups $\{H_i|i \in I\}$ with I a set of linearly ordered indices

$$\prod_{i\in I} H_i = \{x_1x_2x_{3...}x_j|x_k \in H_{i_k}, i_1 < i_2 < \cdots < i_j, j \geq 0\}.$$

Recall that HN is not necessarily a subgroup of G because, if we multiply two of its elements, we do not always obtain an element in HN. If G is abelian then HN is a subgroup of G.

Consider a family of groups $\{G_i\}$. The **external direct product** of this family is

$$\prod_{i\in I} G_i = \{(x_1, ..., x_n)|x_i \in G_i\}$$

which has a group structure given by

$$(x_1, ..., x_n)(y_1, ..., y_n) = (x_1y_1, ..., x_ny_n).$$

If we use additive notation, we write $\underset{i\in I}{\oplus} G_i$ and we call it the **external direct sum**.

Example. The external direct sum

$$\mathbb{Z}_m \oplus \mathbb{Z}_n$$

is used in Mathematical Music Theory to study the motifs in n-tempered scales with m-cyclic onsets. Specifically,

$$\begin{aligned} p_1 : \mathbb{Z}_m \oplus \mathbb{Z}_n &\to \mathbb{Z}_m, \\ (x, y) &\mapsto x \end{aligned}$$

is the first projection, a **motif** μ in $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is an element of the power set[2] $\wp(\mathbb{Z}_m \oplus \mathbb{Z}_n)$ of $\mathbb{Z}_m \oplus \mathbb{Z}_n$ such that $p_1(u) \neq p_1(v)$ for every $u, v \in \mu$. The idea is that, given an onset t, they should not coincide in more than one note.

For example, $\{(0, 0), (1, 2), (2, 4)\} \subseteq \mathbb{Z}_3 \oplus \mathbb{Z}_{12}$ represent thel motif C, D, E (in this order) in a time signature of three, as can be seen in figure **??**. On the other hand, the set $\{(0, 0), (1, 2), (1, 4)\} \subseteq \mathbb{Z}_3 \oplus \mathbb{Z}_{12}$ is not a motif because $p_1(1, 2) = 1 = p_1(1, 4)$, which means that at the onset 1 the pitches D and E coincide.

Recall that the Cartesian product $\prod_{i\in I} X_i$ of a family of sets $\{X_i\}_{i\in I}$ is the set of functions $h : I \longrightarrow \underset{i\in I}{\cup} X_i$ such that $h(i) = h_i \in X_i$ for every $i \in I$.

[2] The symbol $\wp X$ denotes the power set of X.

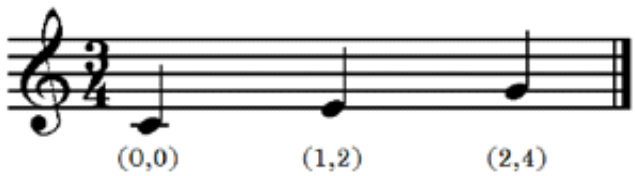


Figure 2.1: A motif of three notes

Let G_1 and G_2 be two groups. Their **product** $G_1 \times G_2$ consists of the set of all the pairs (x, y) with $x \in G_1$, $y \in G_2$ and binary operation

$$\begin{array}{rcl} \cdot & : & (G_1 \times G_2) \times (G_1 \times G_2) \longrightarrow (G_1 \times G_2) \\ ((x_1, y_1), (x_2, y_2)) & \mapsto & \cdot((x_1, y_1), (x_2, y_2)) = (x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2) \end{array}$$

This binary operation gives it a group structure. The **projections** $(x, y) \mapsto x$ and $(x, y) \mapsto y$ are group homomorphisms.

$$\begin{array}{ccc} & G_1 \times G_2 & \\ & \swarrow \quad \searrow & \\ G_1 & & G_2 \end{array}$$

Observe that every function $h : \{1, 2\} \longrightarrow G_1 \cup G_2$ such that $h(1) \in G_1$ and $h(2) \in G_2$ determines an element $(x_1, x_2) = (h(1),\ h(2)) \in G_1 \times G_2$ and that, inversely, a pair $(x_1, x_2) \in G_1 \times G_2$ determines a function $h : \{1, 2\} \longrightarrow G_1 \cup G_2$ given by $h(1) = x_1$ and $h(2) = x_2$. Thus, there exists a one to one correspondence between the set of all functions defined this way, and the group $G_1 \times G_2$.

4.1 Theorem. Let G be a group. Consider a family of groups $\{G_i\}_{i \in I}$ and a family of homomorphisms $\{\varphi_i : G \longrightarrow G_i\}_{i \in I}$. Then there exists a unique homomorphism $\varphi : G \longrightarrow \prod_{i \in I} G_i$ such that $p_i \circ \varphi = \varphi_i$ for every $i \in I$.

Proof. Consider the product $P = \prod_{i \in I} G_i$ with projections $p_i : \prod_{i \in I} G_i \longrightarrow G_i$. Given $(G, \varphi_i : G \longrightarrow G_i)$, define $\varphi : G \longrightarrow \prod_{i \in I} G_i$ by

$$\begin{array}{l} g \mapsto h_g : I \longrightarrow \cup G_i \\ \qquad\qquad\quad i \longmapsto h_g(i) = \varphi_i(g) \in G_i. \end{array}$$

It is easy to see that φ is a homomorphism of groups. It is also clear that $p_i \circ \varphi = \varphi_i$ for every $i \in I$.

$$\begin{array}{ccc} & G & \\ {}^{\varphi_i}\swarrow & & \searrow^{\varphi} \\ G_i & \xleftarrow{p_i} & \prod_{i \in I} G_i \end{array}$$

Suppose $\varphi' : G \longrightarrow \prod_{i\in I} G_i$ is another homomorphism such that $p_i \circ \varphi' = \varphi_i$ for every $i \in I$. However

$$(\varphi'(g))(i) = p_i\varphi'(g) = \varphi_i(g) = h_g(i) = (\varphi(g))(i).$$

Hence $\varphi = \varphi'$.♦

Suppose that there exists another group P' with $p'_i : P' \longrightarrow G_i$ such that $p'_i \circ \varphi = \varphi_i$ for every $i \in I$. Consider the following diagrams that represent the property applied to what it corresponds:

$$\begin{tikzcd}
 & P' \arrow[dl, "p'_i"'] \arrow[dr, "\varphi"] & \\
G_i & & P = \prod_{i\in I} G_i \arrow[ll, "p_i"']
\end{tikzcd}$$

$$\begin{tikzcd}
 & P = \prod_{i\in I} G_i \arrow[dl, "p_i"'] \arrow[dr, "\rho"] & \\
G_i & & P' \arrow[ll, "p'_i"']
\end{tikzcd}$$

$$\begin{tikzcd}
 & P = \prod_{i\in I} G_i \arrow[dl, "p_i"'] \arrow[dr, "\rho\circ\varphi"] & \\
G_i & & P = \prod_{i\in I} G_i \arrow[ll, "p_i"']
\end{tikzcd}$$

As $I_P : P \longrightarrow P$ does the same as $\rho \circ \varphi$, by the uniqueness of the identity, $I_P = \rho \circ \varphi$. Analagously, $\rho \circ \varphi = I_{P'}$. Thus, φ is bijective (it is easy to verify that all the functions are, indeed, group homomorphisms) and, therefore, is an isomorphism.

This **universal property of the direct product** determines the product $\prod_{i\in I} G_i$ uniquely up to isomorphism.

Consider a family of groups $\{G_i\}$. The **weak external direct product** of this family is

$$\prod_{i\in I}^{d} G_i = \{f \in \prod_{i\in I} G_i | f(i) = e_i \in G_i \text{ for almost every } i \in I\}.$$

In the case that there are only abelian groups we will call it **external direct sum** and we will denote it by $\sum_{i\in I} G_i$. If I is finite, the external and weak direct products coincide.

4.2 Theorem. Let G be an abelian group. Consider a family of additive abelian groups $\{G_i\}$ and a family of homomorphisms $\{\gamma_i : G_i \longrightarrow G\}_{i\in I}$. Then

there exists a unique homomorphism $\gamma : \sum_{i\in I} G_i \longrightarrow G$ such that $\gamma \circ \iota_i = \gamma_i$ for every $i \in I$.

Proof. Consider elements different from zero $g_{i_1}, ..., g_{i_s} = \{g_{i_j}\} \in \sum_{i\in I} G_i$ and define

$$\begin{aligned} \gamma : \sum_{i\in I} G_i &\longrightarrow G \quad \text{by} \\ 0 &\longmapsto 0, \\ \{g_i\} &\longmapsto \gamma(\{g_i\}) = \gamma_{i_1}(g_{i_1}) + ... + \gamma_{i_s}(g_{i_s}) = \sum_{j=1}^{s} \gamma_{ij}(g_{ij}), \end{aligned}$$

this last sum over the indices where $g_i \neq 0$, which is a finite number. It can be easily shown that γ is a homomorphism such that $\gamma \circ \iota_i = \gamma_i$ for every $i \in I$ because G is commutative.

$$\begin{tikzcd} & G \arrow[dl, "\gamma_i"'] & \\ G_i & & \prod_{i\in I} G_i \arrow[ll, "\iota_i"'] \arrow[ul, "\gamma"'] \end{tikzcd}$$

Observe that $\{g_i\} \in \sum_{i\in I} G_i, \{g_i\} = \sum \iota_j(g_j)$, this last sum over the indices where $g_i \neq 0$ which is a finite number. If $\eta : \sum_{i\in I} G_i \longrightarrow G$ is such that $\eta \circ \iota_i = \gamma_i$ for every $i \in I$ then $(\{g_i\}) = \eta\left(\sum \iota_j(g_j)\right) = \sum \gamma_i(g_i) = \sum \gamma\iota_i(g_i) = \gamma\left(\sum \iota_i(g_i)\right) = \gamma(\{g_i\})$.

Thus $\eta = \gamma$ and,γ is unique.♦

This theorem determines $\sum_{i\in I} G_i$ uniquely up to isomorphism.

We will now see the case of two factors, in which a group G is isomorphic to the weak external product of one of its subgroups.

4.3 Proposition. Let H and N be any two normal subgroups of a group G. If $HN = G$ and $H \cap N = e$ then $H \times N \cong G$.

Proof. As $HN = G$, if $g \in G$, $xy = g$ with $x \in H, y \in N$. We will see that x and y are determined in a unique way by g: because if $g = x_1y_1$ then $xy = x_1y_1$. Hence, $x^{-1}x_1 = yy_1^{-1}$. As this element is in the intersection of H and N, $x^{-1}x_1 = yy_1^{-1} = e$. Therefore, $x = x_1$ and $y = y_1$.

Now we establish an isomorphism between $H \times N$ and G. Define $h : H \times N \longrightarrow G$ given by $(x, y) \longmapsto h(x, y) = xy$. h is a homomorphism because if we consider the commutator $x^{-1}y^{-1}xy$ then $(x^{-1}y^{-1}x)y \in N$ because N is normal in G and $x^{-1}(y^{-1}xy) \in H$ because H is normal in G. Hence, as $x^{-1}y^{-1}xy$ is in the intersection of H and N, $x^{-1}y^{-1}xy = e$, then $xy = yx$. Thus, $h((x_1, y_1)(x_2, y_2)) = h(x_1x_2, y_1y_2) = x_1x_2y_1y_2 = x_1y_1x_2y_2 = h(x_1, y_1)h(x_2, y_2)$. Finally, it is easy to see that h is bijective (Problem 4.12).♦

4.4 Definition. We will say that a group G is a **direct product (internal)** of H and N if H and N are normal subgroups of G such that $HN = G$ and $H \cap N = e$.

Observe that in this definition H and N are subgroups of G. If $G = H \times N$ as the external direct product, we can consider G as an internal direct product by the subgroups that are images of H and N, that is, $H \times \{1\}$ and $\{1\} \times N$, but not of H and N. Then it is clear the the two types of products provide, in reality, isomorphic groups and we just call it direct product.

4.5 Proposition. Let $\{X_i\}_{i\in I}$ and $\{Y_i\}_{i\in I}$ be families of abelian groups, X and Y abelian groups. Then $Hom(\sum\limits_{i\in I} X_i, Y) \cong \prod_{i\in I} Hom(X_i, Y)$.

Proof.. Define ρ by $\rho(\varphi) = (\varphi\iota_i)_{i\in I}$. It is clear that ρ is a homomorphism. We will show that ρ is a monomorphism: suppose that $\rho(\varphi) = 0$; then $(\varphi\iota_i) = 0$ for each $i \in I$. That is, in the following diagram:

$$\begin{tikzcd}
 & Y & \\
X_i \arrow[ur, "0"] & & \sum\limits_{i\in I} X_i \arrow[ul, "\varphi"'] \arrow[ll, "\iota_i"']
\end{tikzcd}$$

the homomorphism $0\colon X_i \longrightarrow Y$ is such that $0 = \varphi \circ \iota_i$. Hence, $\varphi = 0$. Therefore, $\ker \rho = \{0\}$. We will show that ρ is an epimorphism: let $(\varphi_i)_{i\in I} \in \prod_{i\in I} Hom(X_i, Y)$. Then we have $\varphi_i\colon X_i \longrightarrow Y$ for every $i \in I$. By the universal property of the direct sum, there exists a homomorphism $\varphi\colon \sum\limits_{i\in I} X_i \longrightarrow Y$ such that $\varphi\iota_i = \varphi_i$ for each $i \in I$. Thus, $\rho(\varphi) = (\varphi_i)_{i\in I}$.♦

Problems

4.1 Prove that if $H \lhd G$ and $N \lhd G$, then $HN \lhd G$.

4.2 Let G_1, G_2 and G_3 be three groups. (i) Prove that the product $G_1 \times G_2$ with the binary operation defined above is, indeed, a group.(ii) Prove that $G_1 \times G_2 \cong G_2 \times G_1$.(iii) Prove that $G_1 \times (G_2 \times G_3) \cong (G_1 \times G_2) \times G_3$.

4.3 Establish a definition of the external direct product in terms of the observation previous to Theorem 4.1.

4.4 Prove that $\iota_j : G_j \longrightarrow \prod\limits_{i\in I}^{d} G_i$ given by $\iota_j(g) = \{g_i\}_{i\in I}$ where

$$g_i = \begin{cases} e, & \text{para } i \neq j, \\ g, & \text{para } i = j, \end{cases}$$

is a group monomorphism called the **canonical injection**, that $\iota_i(G_i) \lhd \prod_{i\in I} G_i$ and that $\prod_{i\in I}^{d} G_i \lhd \prod_{i\in I} G_i$.

4.5 Prove that the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to the 4 Klein group V. (Hint: Prove that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic).

4.6 Prove that $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.(Hint: prove that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic by finding a generator and, as there is only one cyclic group of each order, the result follows).

4.7 Prove that $\mathbb{Z}_3 \times \mathbb{Z}_3 \ncong \mathbb{Z}_9$.(Hint: verify that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not cyclic).

4.8 Prove that the external direct product of a family of groups $\{G_i\}$, $\prod_{i\in I} G_i = \{(x_1, ..., x_n) | x_i \in G_i\}$ has a group structure given by

$$(x_1, ..., x_n)(y_1, ..., y_n) = (x_1y_1, ..., x_ny_n)$$

and that it is abelian if each group of the family is abelian.

4.9 Prove that $\mathbb{Z}_i \times \mathbb{Z}_j \cong \mathbb{Z}_{i,j}$ if and only if the greatest common divisor is $(i, j) = 1$.

4.10 Prove that for every $j \in I$ l the **canonical projection**

$$p_j : \prod_{i\in I} G_i \longrightarrow G_j$$

given by $f \longmapsto f(j)$ is a group epimorphism.

4.11 Provide all the details of the proof of Theorem 4.1.

4.12 Provide all the details of the proof of Proposition 4.3.

4.13 Prove that if $G = H \times N$, then $G/(H \times \{1\}) \cong N$.

4.14 Generalize the previous problem.

4.15 Let $H_1 \lhd G_1$ and $H_2 \lhd G_2$ be normal subgroups. Prove that $H_1 \times H_2 \lhd G_1 \times G_2$ and that $G_1 \times G_2/H_1 \times H_2 \cong G_1/H_1 \times G_2/H_2$.

4.16 Provide a generalization of the Proposition 4.3.

4.17 Let $\{X_i\}_{i\in I}$ and $\{Y_i\}_{i\in I}$ be families of abelian groups. Let X and Y be abelian groups. Prove that $Hom(X, \prod_{i\in I} Y_i) \cong \prod_{i\in I} Hom(X, Y_i)$.

Chapter 3

3.1 Finitely Generated Abelian Groups

We will say that a group G is **finitely generated** if it has a finite set of generators. The most important result about finitely generated abelian groups can be formulated in two ways, such that they provide "invariants"; then two groups will be isomorphic if and only if they have the same numerical invariants.

1.1 Theorem. Every finitely generated abelian group G is isomorphic to the direct product of n cyclic groups of order $p_i^{\lambda_i}$ with r infinite cyclic groups, where the p_i are prime numbers, not necessarily distinct, and the λ_i are positive integers. The direct product is unique up to the order of its factors.

This means that G looks like:

$$G \cong \mathbb{Z}_{p_1^{\lambda_1}} \times ... \times \mathbb{Z}_{p_n^{\lambda_n}} \times \mathbb{Z} \times ... \times \mathbb{Z}.$$

The second way of establishing this important result is:

1.2 Theorem. Every finitely generated abelian group G is isomorphic to the direct product of n cyclic groups of order m_i with r infinite cyclic groups, where $m_i | m_{i+1}$ for $1 \leq i \leq n-1$.

This means that G looks like:

$$G \cong \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n} \times \mathbb{Z} \times ... \times \mathbb{Z}.$$

The integers m_i are called **torsion coefficients** of G. These two theorems provide us with a classification, up to isomorphism, of all finitely generated abelian groups, that is, if we have a finitely generated abelian group, this should have the structure defined in the two previous theorems. As special cases, we have the following:

1.3 Theorem. (i) If G is a finitely generated abelian group that does not have elements of finite order, then it is isomorphic to the direct product of a finite number of copies of $\mathbb{Z}$ and (ii) If G is a finite abelian group then it is isomorphic to a direct product of finite cyclic groups of order m_i where $m_i|m_{i+1}$ for $1 \leq i \leq n-1$.

That is, in the case (i) $G \cong \mathbb{Z} \times ... \times \mathbb{Z}$ with r copies of $\mathbb{Z}$ we say that G is a **free abelian group of rank** r. In the case (ii) $G \cong \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n}$ where $m_i|m_{i+1}$ for $1 \leq i \leq n-1$ the elements of the list $m_1, ..., m_n$ are called **invariant factors**of the group G. Two finite abelian groups are isomorphic if and only if they have the same invariant factors. A list can be made of all the non-isomorphic abelian groups of a certain order n. It is enough to find all the possible lists $m_1, ..., m_n$ such that $m_i|m_{i+1}$ for $1 \leq i \leq n-1$ with product n. In conclusion, we have:

1.4 Theorem. Let $G \cong \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n} \times \mathbb{Z} \times ... \times \mathbb{Z}$, with r copies of $\mathbb{Z}$, where $m_i|m_{i+1}$ for $1 \leq i \leq n-1$ y $G' \cong \mathbb{Z}_{k_1} \times ... \times \mathbb{Z}_{k_j} \times \mathbb{Z} \times ... \times \mathbb{Z}$, with s copies of $\mathbb{Z}$, where $k_i|k_{i+1}$ for $1 \leq i \leq j-1$. If $G \cong G'$ then $m_i = k_i$ for $1 \leq i \leq n$, $n = j$ and $r = s$.

Although the Primary Decomposition Theorem is studied in a Linear Algebra course (as in [Ll2]), due to the approach of this presentation of Group Theory (as a first course), directed towards the study of Homological Algebra and Algebraic Topology, we prefer to postpone the proofs of these theorems for a future course on Module Theory, and see these theorems as special cases of the corresponding theorems for finitely generated modules over a prinicpal ideal ring. This way we can present other topics that are usually excluded from an introductory text on Group Theory. The reader who is interested can consult the proofs in [B-M, Cap. X] or [H, Cap. II y IV]. Now we will see how these theorems are used.

1.5 Example. All the possible finitely generated abelian groups of order 36 are obtained, using the first theorem, in the following manner: decompose 36 in powers of primes, such as $36 = 2^2 \cdot 3^2$. Then all the possible groups of the first way, (not isomorphic one to the other) are

$$\begin{aligned}
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3,\\
&\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3,\\
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9,\\
&\mathbb{Z}_4 \times \mathbb{Z}_9
\end{aligned}$$

and, by the second way (not isomorphic one to the other) they are:

$$\begin{aligned}
&\mathbb{Z}_6 \times \mathbb{Z}_6,\\
&\mathbb{Z}_3 \times \mathbb{Z}_{12},\\
&\mathbb{Z}_2 \times \mathbb{Z}_{18},\\
&\mathbb{Z}_{36}.
\end{aligned}$$

In summary, we have four abelian groups (up to isomorphism) of order 36. The first ones on the list correspond to the order of those written in the second list.

1.6 Example. All possible finitely generated abelian groups of order 540 are obtained, the first way, by decomposing 540 in powers of primes as $540 = 2^2 \cdot 3^3 \cdot 5$. Then, the possible groups (not isomorphic one to the other) are:

$$\begin{aligned}
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5,\\
&\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5,\\
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5,\\
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5,\\
&\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5,\\
&\mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_5
\end{aligned}$$

and, by the second way (not isomorphic one to the other) are:

$$\begin{aligned}
&\mathbb{Z}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_{30},\\
&\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{60},\\
&\mathbb{Z}_2 \times \mathbb{Z}_{270},\\
&\mathbb{Z}_6 \times \mathbb{Z}_{90},\\
&\mathbb{Z}_3 \times \mathbb{Z}_{180},\\
&\mathbb{Z}_{540}.
\end{aligned}$$

Thus, we have six abelian groups (up to isomorphism) of order 540. The ones in the first list correspond to the order of those written in the second list.

Consider a chain $C = \{C_n, \partial_n\}$ of finitely generated abelian groups and the homology group of degree n of C, $H_n(C) = \ker \partial_n / im\ \partial_{n+1} = Z_n(C)/B_n(C)$. The subgroups $Z_n(C)$ and $B_n(C)$ of C_n are finitely generated, hence $H_n(C)$ is finitely generated. The torsion coefficients of $H_n(C)$ are called **torsion coefficients of degree n of C** and the rank of $H_n(C)$ is called the **Betti number $\beta_n(C)$ of degree n of C**. The integer $\chi(C) = \sum_n (-1)^n \beta_n(C)$ is called **The Euler-Poincaré characteristic of the chain C**.

Problems

1.1 Find the possible abelian groups, up to isomorphism, of order 8, 10.

1.2 Find the possible abelian groups, up to isomorphism, of order12, 16.

1.3 Find the possible abelian groups, up to isomorphism, of order 32.

1.4 Find the possible abelian groups, up to isomorphism, of order 720.

1.5 Find the possible abelian groups, up to isomorphism, of order 860.

1.6 Find the possible abelian groups, up to isomorphism, of order 1150.

3.2 Permutations, Orbits and Sylow Theorems

Consider the set Σ_n that consists of all the permutations of the set $I_n = \{1, ..., n\}$, that is, Σ_n consists of all the bijective functions of I_n onto I_n. In I.2 we saw that Σ_n is a grup under the binary operation $\circ$ and that $|\Sigma_n| = n!$ Recall Σ_3 and its corresponding table as in I.1. Its elements are:

$$\begin{aligned} \iota &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \\ \eta_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \eta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \eta_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \end{aligned}$$

The calculation of the composition of two permutations will be made following the same order as in functions, for example:

$$\rho_1 \circ \eta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \eta_3$$

that is, first consider η_1 and then ρ_1. Thus,

$$\eta_1 \circ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \eta_2.$$

Its table is (considering the way we compose two functions, first the right (left column) and then the left (top row)):

$\circ$	ι	ρ_1	ρ_2	η_1	η_2	η_3
ι	ι	ρ_1	ρ_2	η_1	η_2	η_3
ρ_1	ρ_1	ρ_2	ι	η_2	η_3	η_1
ρ_2	ρ_2	ι	ρ_1	η_3	η_1	η_2
η_1	η_1	η_3	η_2	ι	ρ_2	ρ_1
η_2	η_2	η_1	η_3	ρ_1	ι	ρ_2
η_3	η_3	η_2	η_1	ρ_2	ρ_1	ι

We have written for $I_n = \{1, ..., n\}$ a permutation $\sigma : I_n \longrightarrow I_n$ as

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}.$$

We say that a permutation σ of I_n is a **cycle of length** r (or r-cycle) if there exist integers $i_1, ...i_r$ in I_n such that

$$\sigma(i) = \begin{cases} i_{j+1}, & \text{si } i = i_j \text{ y } 1 \leq j < r, \\ i_1, & \text{si } i = i_r, \\ i, & \text{si } i \neq i_j \text{ y } 1 \neq j \leq r, \end{cases}$$

and we denote it by $\sigma = (i_1, i_2, ..., i_r)$. For example,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3)$$

is a cycle of length 3. Observe that $(1,2,3) = (2,3,1) = (3,1,2)$, that is, there are 3 notations for this cycle and, in general, see Problem 2.3.

We say that a cycle of length 2 is a **transposition**. We will usually omit a cycle of length 1 when we have a product of cycles.

For example:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 6 & 5 & 4 & 7 \end{pmatrix} = (1,3,2)(4,6)(5)(7)$$

where $(1,3,2)$ is a tricycle, $(4,6)$ is a transposition, (5) and (7) are cycles of length one and it is usual to omit them.

Let σ be a permutation of Σ_n and define in $I_n = \{1,...,n\}$ a relation given by $i \equiv j$ if and only if $\sigma^r(i) = j$, for some integer r. It can be easily verified that this is an equivalence relation in I_n (Problem 2.4). The equivalence classes are called **orbits** of σ. For example, the orbit of the element 1 of the permutacion

$$\begin{aligned} & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 5 & 6 & 11 & 2 & 4 & 9 & 7 & 10 & 12 & 8 & 1 \end{pmatrix} \\ = \quad & (1,3,6,4,11,8,7,9,10,12)(2,5) \end{aligned}$$

is $\{1,3,6,4,11,8,7,9,10,12\}$, and that of the element 2 is $\{2,5\}$. Observe that if an orbit has more than one element, it then forms a cycle of length equal to the number of the elements in the orbit. Thus, if $O_1,...,O_k$ are the orbits (which are disjoint) of a permutation σ and $c_1,...,c_k$ are the cycles (disjoint) given by $c_j(i) = \sigma(i)$ if $i \in O_j$ or i if $i \notin O_j$ then $\sigma = c_1c_2\cdots c_k$. Hence, we have the following

2.1 Proposition. Every permutation σ can be written as the product of disjoint cycles.♦

Observe that the representation as a product of disjoint cycles is unique up to the order in which they are written. Clearly, the composition of two disjoint cycles is commutative and as every cycle can be expressed as $(i_1,i_2,...,i_r) = (i_1,i_r)(i_1,i_{r-1})\cdots(i_1,i_3)(i_1,i_2)$ we have the following

2.2 Corollary. Every permutation $\sigma \in \Sigma_n$ for $n \geq 2$ is a product of transpositions, not necessarily disjoint.♦

For example,

$$\begin{aligned} & (1,3,6,4,11,8,7,9,10,12)(2,5) \\ = \quad & (1,12)(1,10)(1,9)(1,7)(1,8)(1,11)(1,4)(1,6)(1,3)(2,5). \end{aligned}$$

Observe that, by decomposing a permutation as a product of transpositions, we can always add the identity transformation, written as$(i_j,i_k)(i_j,i_k)$, in such a way that the decomposition is not unique.

2.3 Definition. We say that a group G **acts** (on the left) on a set X if there exists a function

$$\begin{array}{rccc} a: & G \times X & \longrightarrow & X, \\ & (g,x) & \mapsto & a(g,x), \end{array}$$

where $a(g,x)$ will be denoted gx, such that $(e,x) \mapsto a(e,x) = ex = x$ and $(gg',x) \mapsto a(gg',x) = (gg')x = g(g'x)$ hold.

If G acts on X we say that X is a G**-set**. In the notation $(g,x) \mapsto a(g,x) = gx$, writing gx is a common abuse of notation and is defined in a particular way in every case. An analogous definition can be given of a right action.

We will see some examples.

2.4 Example. Every group G is a G-set with the binary operation seen as an action. Every group can be considered an H-set as well, with H a subgroup of G, and here we have $H \times G \longrightarrow G$ given by $(h,x) \mapsto a(h,x) = hx$. This action is called **translation** (on the left). Every vector space V over a field K can be seen as a K-set where the multiplicative part of K acts on V.

2.5 Example. I_n is a Σ_n-set with the action $a : \Sigma_n \times I_n \longrightarrow I_n$ given by $(\sigma, i) \mapsto a(\sigma, i) = \sigma(i)$.

2.6 Example. Considere an action of a subgroup H of G, $a : H \times G \longrightarrow G$ given by $(h,x) \mapsto a(h,x) = hxh^{-1}$. This action is called **conjugation** by h. The element hxh^{-1} is called a **conjugate** of x.

Let X be a G-set with $a : G \times X \longrightarrow X$. We say that two elements $x, y \in X$ are **related** and we write $x \sim y$ if and only if there exists $g \in G$ such that $a(g,x) = gx = y$ for some $g \in G$.

2.7 Proposition. $\sim$ is an equivalence relation and the set

$$G_x = \{g \in G | gx = x\}$$

is a subgroup of G.

Proof. As, for every $x \in X$, $ex = x$, then $x \sim x$. If $x \sim y$ then there exists $g \in G$ such that $gx = y$ for some $g \in G$. Then, $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}y$, thus $y \sim x$. If $x \sim y$ and $y \sim z$ then there exist $g, g' \in G$ such that $gx = y$ y $g'y = z$. Then $(g'g)x = g'(gx) = g'y = z$, thus $x \sim z$. Consider $g, g' \in G_x$. Then $gx = x$ and $g'x = x$. Hence, $(gg')x = g(g'x) = gx = x$. Therefore, $gg' \in G_x$. Clearly $ex = x$, so $e \in G_x$. Finally, if $g \in G_x$ then $gx = x$ and $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x$. Thus, $g^{-1} \in G_x$. Hence G_x is a subgroup of G.♦

The subgroup G_x is called **isotropy subgroup** of x or **stabilizer** of x. We will call each class of the equivalence relation ˜ the **orbit** of X under G. If $x \in X$ we will call the equivalence class of x the **orbit** of x and we will denote it as Gx.

We will give names to specific orbits:

(i) If a group G acts on itself under conjugation, the orbit $\{gxg^{-1}\}$ with $g \in G$ will be called the **conjugate class** of x.

(ii) If the subgroup $H < G$ acts on G by conjugation, the isotropy group $H_x = \{h \in H : hx = xh\}$ is called the **centralizer** of x in H and we will denote it as $C_H(x)$.

(iii) If $H = G$, $C_G(x)$ it will be called the **centralizer of** x.

(iv) If $H < G$ acts on the set of subgroups of G by conjugation, then the subgroup of H that leaves K fixed is called the **normalizer of** K **in** H, denoted as $N_H(K) = \{h \in H | hKh^{-1} = K\}$.

(v) In particular, if we have the case in which $H = G$, that is, $N_G(K)$ we will just call it the **normalizer of** K.

2.8 Theorem. Let X be a G-set $a : G \times X \longrightarrow X$. If $x \in X$, then the number of equivalence classes, or orbits, is equal to the index of G_x in G, that is, $|Gx| = (G : G_x)$.
Proof. Define a function

$$\begin{array}{cccc} \omega : & Gx & \longrightarrow & G/G_x \\ & a(g,x) = gx = y & \mapsto & \omega(a(g,x)) = \omega(gx) = gG_x. \end{array} \quad \text{given by}$$

We will see that ω is well defined: suppose that $a(h,x) = hx = y$ for $h \in G$ as well. Then $gx = hx$, $g^{-1}(gx) = g^{-1}(hx)$ and $x = (g^{-1}h)x$. Thus, $g^{-1}h \in G_x$, $h \in gG_x$ and $gG_x = hG_x$.

Now we will see that ω is injective: if $y, z \in Gx$ and $\omega(y) = \omega(z)$. Then there exists $h, k \in G$ such that $a(h,x) = hx = y$ and $a(k,x) = kx = z$, with $k \in hG_x$. Then $k = hg$ for some $g \in G_x$, then $z = kx = (hg)x = h(gx) = hx = y$. Therefore, ω is injective.

We will see that ω is surjective: let hG_x be a left coset. Then if $hx = y$, we have $hG_x = \omega(y)$. Thus ω is surjective. Therefore, $|Gx| = (G : G_x)$.♦

2.9 Corollary. If $o(G)$ is finite, then $o(Gx)|o(G)$.
Proof. As $o(G)$ Then $o(G) = o(Gx)o(G_x)$.♦

Example. Define a **chord** S as a subset of the scale $\mathbb{Z}_{12}$, that is $S \in \wp(\mathbb{Z}_{12})$. The group

$$\overrightarrow{GL}(\mathbb{Z}_{12}) = \{e^t \cdot u : t \in \mathbb{Z}_{12}, u \in GL(\mathbb{Z}_{12})\}$$

is called the **general affine group** of $\mathbb{Z}_{12}$ (or **group of affine symmetries** of $\mathbb{Z}_{12}$) and acts on $\wp(\mathbb{Z}_{12})$ as

$$\begin{aligned} \alpha : \overrightarrow{GL}(\mathbb{Z}_{12}) \times \wp(\mathbb{Z}_{12}) &\to \wp(\mathbb{Z}_{12}), \\ (e^t \cdot u, \{x\}) &\mapsto \{e^t \cdot u(x)\} = \{ux + t\}. \end{aligned}$$

For example, the D minor chord[1] $\{D, F, A\} = \{2, 5, 9\}$ can be transposed to E minor using $e^2 \cdot 1$, that is

$$\begin{aligned} e^2 \cdot 1(\{D, F, A\}) &= e^2 \cdot 1(\{2, 5, 9\}) \\ &= \{e^2 \cdot 1(2), e^2 \cdot 1(5), e^2 \cdot 1(9)\} \\ &= \{4, 7, 11\} = \{E, G, B\}. \end{aligned}$$

Guerino Mazzola has calculated all the isotropy groups of the chords in $\mathbb{Z}_{12}$, and a table that summarizes this information can be found in the book *The Topos of Music* [M], in the appendix L. In particular, the isotropy group of a major chord is always trivial (that is, it is $\{e^0 \cdot 1\}$), and the cardinality of its orbit is $|\overrightarrow{GL}(\mathbb{Z}_{12})| = 48$, with the same happening in the case of the minor chords. This means that, from the affine point of view, there are 48 major and minor chords in the orbit of each one of them or that, at the end, there really only exists one major (or minor) chord. On the other hand, an augmented chord $\mathcal{A}$ (for example, $\mathrm{C}^{\mathrm{aug}} = \{0, 4, 8\}$) has an isotropy group of cardinality 12. Thus, there are

$$o(\overrightarrow{GL}(\mathbb{Z}_{12})\mathcal{A}) = \frac{o(\overrightarrow{GL}(\mathbb{Z}_{12}))}{o(\overrightarrow{GL}(\mathbb{Z}_{12})_{\mathcal{A}})} = \frac{48}{12} = 4$$

elements in its orbit, and really twelve augmented chords from the affine point of view.

2.10 Theorem. Let G be a finite group, $g \in G$ and $X_g = \{x \in X | gx = x\}$. If n is the number of orbits of X in G then $n = \sum_{g \in G} |X_g| o(G)^{-1}$.

Proof. Let r be the number of pairs (g, x) such that $gx = x$. There are $|X_g|$ pairs for every g and $|G_x|$ for every x. Then

$$r = \sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|.$$

As $o(Gx) = (G : G_x) = o(G)/o(G_x)$ by the previous theorem, then $o(G_x) = o(G)/o(Gx)$. Hence, $r = \sum_{x \in X} (|G|/|Gx|) = |G| \sum_{x \in X} (1/|Gx|)$. However, $1/|Gx|$ is the same for every x in the same orbit and if O denotes any orbit, then $\sum_{x \in O} (1/|Gx|) = \sum_{x \in O} (1/|O|) = 1$. Substituting, we obtain $r = o(G)n$.♦

Example. We denote $\mathbb{Z}_{12} \oplus \mathbb{Z}_{12}$ as $\mathbb{Z}_{12}^2$ and consider the group

$$\overrightarrow{GL}(\mathbb{Z}_{12}^2) = \{e^{(s,t)} \cdot (u, v) : s, t \in \mathbb{Z}_{12}, u, v \in GL(\mathbb{Z}_{12})\}$$

and its action on the motifs in $\mathbb{Z}_{12}^2$. Harald Fripertinger (see [M]) has calculated the number of orbits of this action on these motifs and, in particular, the number

[1] For the definition of major and minor chorse, see chapter 4.

of classes of the 72 element motifs. According to his calculations, this number is

$$2\,230\,741\,522\,540\,743\,033\,415\,296\,821\,609\,381\,912 = 2.23\ldots \times 10^{23}.$$

which exceeds the approximate amount of stars in the Milky Way, which is 10^{11}.

2.11 Proposition. Let X be a G-set. The function

$$\begin{array}{rccl} \omega: & G & \longrightarrow & \Sigma_X \\ & g & \mapsto & \omega(g) = \sigma_g(x) = gx \end{array}$$

is a homomorphism.
Proof. We will see that $\sigma_g : X \longrightarrow X$ is, indeed, a permutation: If $\sigma_g(x) = \sigma_g(y)$, then $gx = gy$. Thus $g^{-1}(gx) = g^{-1}(gy)$ and $(g^{-1}g)x = (g^{-1}g)y$. Hence, $ex = ey$ and $x = y$. Therefore, σ_g is injective.

As $\sigma_g(g^{-1}x) = g(g^{-1}x) = (gg^{-1})x = ex = x$, for each x there exists $g^{-1}x$ such that $\sigma_g(g^{-1}x) = x$. Thus, σ_g is surjective. ω is a homomorphism since

$$\begin{array}{rcl} \omega(gg') & = & \sigma_{gg'}(x) = (gg')x = g(g'x) = g\sigma_{g'}(x) \\ & = & \sigma_g(\sigma_{g'}(x)) = \omega(g)(\sigma_{g'}(x)) = \omega(g)\omega(g'). \blacklozenge \end{array}$$

2.12 Corollary. (**Cayley**) If G is a group then there exists a monomorphism $G \longrightarrow \Sigma_G$, that is, every group is isomorphic to a group of permutations. If G is a finite group of order n then it is isomorphic to a subgroup of Σ_n.
Proof. Consider the action of G on itself by left translation and apply the previous proposition, obtaining

$$\begin{array}{rccl} \omega: & G & \longrightarrow & \Sigma_G \text{ given by} \\ & g & \mapsto & \omega(g) = \sigma_g(x) = gx. \end{array}$$

If $\omega(g) = \sigma_g(x) = gx = I_G$, then $\sigma_g(x) = gx = x$ for every $x \in G$. If we take $x = e$ then $ge = e$ and $g = e$. Thus, ω is a monomorfphism. As a particular case, if $o(G) = n$ then $\Sigma_G = \Sigma_n$.

Another way of writing this is the following: Let

$$H = \{\sigma_g : G \longrightarrow G | x \mapsto \sigma_g(x) = gx, \text{ for every fixed } g \in G\ \}$$

be a candidate for the subgroup of Σ_G. $\sigma_g : G \longrightarrow G$ is clearly a permutation of G, because if $\sigma_g(x) = \sigma_g(y)$ then $gx = gy$ and $x = y$; also, if $x \in G$ then $\sigma_g(g^{-1}x) = gg^{-1}x = x$. It can be verified immediately that H is a subgroup of Σ_G because $\sigma_g \circ \sigma_{g'}(x)) = \sigma_g(g'x) = g(g'x) = (gg')x = \sigma_{gg'}(x)$ for every $x \in G$, as $\sigma_e(x) = ex = x$ for every $x \in G$, H contains the identity permutation and, finally, as $\sigma_g\sigma_{g'} = \sigma_{gg'}, \sigma_g\sigma_{g^{-1}} = \sigma_{gg^{-1}} = \sigma_e$ y $\sigma_{g^{-1}}\sigma_g = \sigma_{g^{-1}g} = \sigma_e$ we see that $\sigma_{g^{-1}} = (\sigma_g)^{-1}$. Now, define

$$\begin{array}{rcl} h & : & G \longrightarrow H \text{ by} \\ g & \mapsto & h(g) = \sigma_g. \end{array}$$

As

$$h(gg')(x) = \sigma_{gg'}(x) = (gg')x = g(g'x) = \sigma_g(\sigma_{g'}(x)) = (\sigma_g\sigma_{g'})(x)) = h(g)h(g')$$

h is a homomorphism. If $h(g) = h(g')$ then, in particular, $\sigma_g(e) = ge = g = g' = g'e = \sigma_{g'}(e)$, thus $g = g'$ and h es inyective. Hence h is an isomorphism.♦

The Sylow theorems provide us with important information about finite non-commutative groups. They tell us, among other things, that if the power of a prime divides the order of a group, this group has a subgroup of that order.
2.13 Definition. A group G is called a p**-group** (p a prime number), if all the elements of G have the order of a power of p.

2.14 Theorem. (**First Sylow Theorem)**) Let G be a group of order $p^n m$ where p is prime, $n \geq 1$ and such that $p \nmid m$. Then, G contains a subgroup of order p^i for every i such that $1 \leq i \leq n$, and every subgroup H of G of order p^i is a normal subgroup of a subgroup of order p^{i+1} for $1 \leq i < n$.

2.15 Definition. Let p be prime number. We say that P is a **Sylow p-subgrupo of** G if P is a maximum p-subgroup of G, i.e., if K is a p-group such that $P < K < G$ then $P = K$.

2.16 Theorem. (**Second Sylow Theorem**) Two Sylow p-subgroups of a finite group G are conjugates.

2.17Theorem. (**Third Sylow Theorem**) If G is a finite group and $p|o(G)$ (p prime), then the number of Sylow p-subgroups of G divides the order of G and is congruent with 1 modulo p.

See [A] or [F] for the proofs of the Sylow theorems.

Problems

2.1 Verify that $a : \mathbb{Z} \times \mathbb{R} \longrightarrow \mathbb{R}$ given by $(g, x) \mapsto a(g, x) = gx$ is an action of $\mathbb{Z}$ in $\mathbb{R}$ called **translation**.

2.2 Consider the action $a : H \times s(G) \longrightarrow s(G)$ of a subgroup H of a group G in the set $s(G)$ that consists of all subgroupo of G given by $(h, K) \longmapsto hKh^{-1}$. Show that hKh^{-1} is a subgroup of G isomorphic to K. hKh^{-1} we say that it is a **conjugate subgroup** of K.

2.3 Prove that for a cycle of length r there are exactly r notations in cycle form.

2.4 Prove that if σ is a permutation of Σ_n and in $I_n = \{1, ..., n\}$, $i \equiv j$ if and only if $\sigma^r(i) = j$, for some integer r, then $\equiv$ is an equivalence relation in I_n.

2.5 Define the **sign of a permutation** $\sigma \in \Sigma_n$ as

$$sg(\sigma) = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Prove that if σ' is another permutation, then $sg(\sigma' \circ \sigma) = sg(\sigma')sg(\sigma)$ and that if τ is a transposition, then $sg(\tau) = -1$. We say that a permutation is **even** or **odd** if its sign is 1 or -1 respectively. Conclude that if $n > 1$, the set of even permutation of I_n form a subgroup A_n of Σ_n called the **alternating group of degree n**.

2.6 Define a homomorphism $h : \Sigma_n \longrightarrow \{1, -1\}$ given by $h(\sigma)$ equal to 1 if σ is even and -1 if σ is odd. Prove that A_n is the kernel of h and, hence, is a normal subgroup of Σ_n such that $o(A_n) = \frac{n!}{2}$.

2.7 Prove that if a prime number p divides the order of a finite group $o(G)$, then G possesses elements of order p and, hence, is a subgroup of order p. (**Cauchy's Theorem**)

2.8 Prove that a finite group is a p-group if and only if the order of G is a power of p.

2.9 Prove that if $o(G) = p^n$, p a prime number, then it possesses a non-trivial center.

2.10 Show that if $o(G) = p^2$ for p a prime number, then G is cyclic or isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

2.11 Show that the subgroup K is normal in $N_G(K)$.

2.12 Prove that K is normal in G if and only if $N_G(K) = G$. Verify that the Sylow 2-subgroups of Σ_3 have order 2 and that these are conjugates to each other.

2.13 Prove that there only is one group of order 15.

2.14 Prove that there do not exist simple groups of orders 15, 20, 30, 36, 48 and 255.

3.3 Free Groups

Consider the Cartesian product $A = X \times \mathbb{Z}_2$ where X denotes any set and $\mathbb{Z}_2 = \{-1, 1\}$. For each element x of X we will use the notation $x^1 = (x, 1)$ and $x^{-1} = (x, -1)$. Consider the set K of all the finite sequences of elements with repetition of the set A. Define a binary operation on K

$$\begin{array}{rcl} K \times K & \to & K, \\ (x_1, ..., x_r)(y_1, ..., y_s) & \mapsto & (x_1, ..., x_r, y_1, ..., y_s). \end{array}$$

We will call the elements of A the **alphabet**, and the elements of K **words**, which are formal products of the elements of A.

3.1 Example. Take $X = \{x_1, x_2, x_3, x_4\}$. The following expressions are words: $x_1^1 x_2^{-1} x_1^1 x_2^{-1} x_3^1 x_4^{-1} x_2^{-1} x_3^1$, $x_2^{-1} x_3^1 x_4^{-1} x_1^1 x_2^{-1} x_3^1 x_3^1 x_4^{-1}$, $x_3^1 x_4^{-1} x_1^1 x_2^{-1} x_3^1$.

We say that a word is **reduced** if, for every element x of X, x^1 is never next to x^{-1} or viceversa. Let L be the set of all reduced words of K and add the empty word (which is not in K) and which we will denote as 1.

Now we will define a binary operation on L with the following conditions: if one of the elements x or y is 1, then their product is x or y; if this is not the case, their product is a reduced word xy. It can be proved that this binary operation provides L with a group structure.

3.2 Definition. A **free group on a set** X is a pair (L, f) where L is a group and $f : X \longrightarrow L$ is a function such that, for any function $g : X \longrightarrow G$, G some group, there exists a unique homomorphism $h : L \longrightarrow G$ such that the following triangle is commutative:

$$\begin{array}{ccc} X & \xrightarrow{f} & L \\ {\scriptstyle g}\searrow & & \swarrow{\scriptstyle h} \\ & G & \end{array}$$

We define a function $f : X \longrightarrow L$ by $f(x) = x^1 \in L$. Suppose that $g : X \longrightarrow G$ is any function of X into a group G. Define a function $h : L \longrightarrow G$ by

$$\begin{array}{rcl} h(k) & = & e_G \text{ if } k \text{ is the empty word}, \\ h(k) & = & g(x_1)^{\eta_1} g(x_2)^{\eta_2} \cdots g(x_n)^{\eta_n} \text{ if } k = x_1^{\eta_1} x_2^{\eta_2} \cdots x_n^{\eta_n}\ , \\ \text{for } \eta_i & = & \pm 1,\ 1 \leq i \leq n. \end{array}$$

It is easy to prove that h is a group homomorphism such that $h \circ f = g$. If $h' : L \longrightarrow G$ is another group homomorphism such that $h' \circ f = g$ then, for the word $k = x_1^{\eta_1} x_2^{\eta_2} \cdots x_n^{\eta_n}$, we see that $h'(k) = h'(x_1)^{\eta_1} h'(x_2)^{\eta_2} \cdots h'(x_n)^{\eta_n} = g(x_1)^{\eta_1} g(x_2)^{\eta_2} \cdots g(x_n)^{\eta_n}$.Hence, $h = h'$. Thus we have the following

3.3 Theorem. For every set X there always exists a free group on X.♦

Consider a free group on the set X denoted (L, f), where $f : X \longrightarrow L$ is a function. We see that such a function f is injective: Suppose that $x, y \in X$ with $x \neq y$. Consider a group G and $g : X \longrightarrow G$ a function such that $g(x) \neq g(y)$. As $h(f(x)) = g(x) \neq g(y) = h(f(y))$ we see that $f(x) \neq f(y)$. We can also see that $f(X)$ generates L: let H be the subgroup of L generated by $f(X)$. Then f defines a function $g : X \longrightarrow H$ with $i \circ g = f$, where i denotes the inclusion of H in L. As L is free, there exists a homomorphism $h : L \longrightarrow H$ such that $h \circ f = g$.

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "g"'] & & L \arrow[dl, shift left, "h"] \\ & H \arrow[ul, shift left, "i"] & \end{tikzcd}$$

Consider the diagram

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "g"'] & & L \arrow[dl, shift left, "I_L"] \\ & H \arrow[ul, shift left, "i \circ h"] & \end{tikzcd}$$

It is clear that $I_L \circ f = f$, and $i \circ h \circ f = i \circ g = f$. By uniqueness, $i \circ h = I_L$. Thus, i is surjective. Thus, $H = G$ and $f(X)$ generates L.

Suppose that (L', g) is another free group on the same set X as L. Then we can consider the following diagram:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, equal] \arrow[dr, "g"] & L \arrow[d, "h"] \\ X \arrow[r, "f"'] & L' \arrow[d, "h'"] \\ & L \end{tikzcd} \qquad \begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "g"'] & & L \arrow[dl, shift right, "h"'] \\ & L' \arrow[ul, shift right, "h'"'] & \end{tikzcd}$$

Here, as L is free, there exists a unique homomorphism h such that $g = h \circ f$ and as L' is also free, there exists a unique homomorphism h' such that $f = h' \circ g$. By uniqueness, $I_L = h' \circ h$. Analogously we can consider the diagram

$$\begin{tikzcd} X \arrow[r, "g"] \arrow[d, equal] \arrow[dr, "f"] & L' \arrow[d, "h'"] \\ X \arrow[r, "g"'] & L \arrow[d, "h"] \\ & L' \end{tikzcd} \qquad \begin{tikzcd} X \arrow[rr, "g"] \arrow[dr, "f"'] & & L' \arrow[dl, shift right, "h"'] \\ & L \arrow[ul, shift right, "h'"'] & \end{tikzcd}$$

and obtain $I_{L'} = h \circ h'$. Thus, $L \cong L'$. We can summarize the preceeding analysis in the following

3.4 Theorem. Let (L, f) be a free group on X. Then f is injective and $f(X)$ generates L. (L, f) is unique up to isomorphism.♦

Observe that every set X determines a unique free group. As f is injective, identify X with its image and $f(X)$ is a subset generated by L. We can say that every function $g : X \longrightarrow G$ **extends to a** unique homomorphism $h : L \longrightarrow G$.

We will call L the **free group generated by the elements of the set** X. Observe that every free group is infinite.

Let G be any group. We can choose a subset X of G that generates G. We always can, because we can choose $X = G$. Consider the free group generated by X. Then the inclusion function $g : X \longrightarrow G$ extends to a homomorphism $h : L \longrightarrow G$. h is surjective because X generates G and $X = g(X) \subset h(L)$. If N is the kernel of h, by the first isomorphism theorem, $G \cong L/N$. We can summarize this in the following

3.5 Theorem. Every group is isomorphic to the quotient of a free group.♦

Denote the set of generators of a subgroup N of a free group L, as R . As the group L is totally determined by the set X and the normal subgroup N is determined by the set R, the group $G \cong L/N$ can be defined by a set whose elements we will call **generators** of G and by a set R whose elements we will call **relations** that define G.

Consider a reduced word $k = x_1^{\eta_1} x_2^{\eta_2} \cdots x_n^{\eta_n} \neq 1$, that is, an element of R such that, if N is not a trivial subgroup, we will omit the identity (1) from the set R. As $k \in N$, it represents the identity element in the quotient. We will denote it by the expression $x_1^{\eta_1} x_2^{\eta_2} \cdots x_n^{\eta_n} = 1$.

We will say that the sets X and R form a **presentation** $(X|R)$ of the group $G \cong L/N$. There can be different presentations of the same group. In such cases we will call them **isomorphic presentations**.

3.6 Example. The dihedral group D_n $n \geq 2$, is the group of order $2n$ generated by two elements a and b with relations $a^n = 1, b^2 = 1$ and $bab = a^{-1}$.

3.7 Example. $(x|\_)$ is a presentation of the free group $\mathbb{Z}$. That is, a generator, but no relations. That is the reason behind the term **free**, that is, free of relations.

3.8 Example. $(x|x^n = e)$ is a presentation of the cyclic group $\mathbb{Z}_n$.

3.9 Definition. A free abelian group in the set X is a pair (L, f) where L is an abelian group and $f : X \longrightarrow L$ is a function such that, for any function $g : X \longrightarrow G$, G any abelian group, there exists a unique homomorphism $h : L \longrightarrow G$ such that the following triangle commutes:

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "g"'] & & L \arrow[dl, "h"] \\ & G & \end{tikzcd}$$

The following two theorems are proved in the same way as those that correspond to free groups:

3.10 Theorem. Let (L, f) be a free abelian group on X. Then f is injective and $f(X)$ generates L. (L, f) is unique up to isomorphism.♦

3.11 Theorem. Any abelian group is isomorphic to the quotient of a free abelian group.♦

3.12 Theorem. For any set X there always exists a free abelian group on X.
Proof. Let $(K, i : X \to K)$ be a free group on a set X. Consider the quotient group $L = K/K'$where K' denotes the commutator subgroup, and the projection of this quotient group $p : K \to K/K'$. We see that (L, f) is a free abelian group on X, $f = p \circ i$.

Let $g : X \to G$ be any function of X into an abelian group G. As K is a free group on X, there exists a homomorphism $k : K \to G$ such that $k \circ i = g$. As G is an abelian group, k sends the commutator subgroup K' of K to the element 0 of G. Thus, k induces a homomorphism $h : L \to G$ such that $h \circ p = k$. Hence $h \circ p \circ i = k \circ i = g$. The uniqueness is immediate and we leave it as an exercise.♦

As the function $f = p \circ i$ is injective, we can identify X with its image $f(X)$ in L. Then X is a subset of L that generates L. We say that a **function** g **extends** to a unique homomorphism h and we call L a **free abelian group generated by (the elements) of the set** X. We assert that any group G is a **free abelian group**, if it is isomorphic to a free abelian group L generated by a set X. If $f' : L \to G$ and we denote the restriction of f to X as f, then (G, f) is a free abelian group on the set X. We call the image $f(X)$ the **basis of the free abelian group** G. It is clear that every function $g : f(X) \to H$, where H is any abelian group, extends to a unique homomorphism $h : G \to H$. (Problem 3.3).

3.13 Example. Consider the group that consists of the direct sum of n copies of $\mathbb{Z}$. Then $(1, 0, ..., 0)$, $(0, 1, 0, ...0)$,..., $(0, ..., 0, 1)$ is a basis of that free abelian group. The group of the integers modulo n is not free abelian.

Problems

3.1 Let L be the set of all reduced words of K and add the empty word (which is not in K) that we will denote as 1. Define a binary operation on L with the following conditions: if one of the elements x or y is 1, then the product is x or y, and in any other case the product is the reduced word xy. Show that this binary operation provides a group structure to L.

3.2 Consider the function $h : L \longrightarrow G$ defined as

$$\begin{aligned} h(k) &= e_G \text{ if } k \text{ is the empty word,} \\ h(k) &= g(x_1)^{\eta_1} g(x_2)^{\eta_2} \cdots g(x_n)^{\eta_n} \text{ if } k = x_1^{\eta_1} x_2^{\eta_2} \cdots x_n^{\eta_n} \ , \\ \text{for } \eta_i &= \pm 1,\ 1 \leq i \leq n. \end{aligned}$$

Verify that h is a group homomorphism such that $h \circ f = g$ in the context of Theorem 3.3.

3.3 We say that any group G is a **free abelian group**, if it is isomorphic to a free abelian group L generated by a set X. If $f' : L \to G$ and we denote the restriction of f' to X as f, then (G, f) is a free abelian group on the set X. We will call the image $f(X)$ the **basis of the free abelian group** G . Prove that every function $g : f(X) \to H$ where H is any abelian group extends to a unique homomorphism $h : G \to H$.

3.4 We say that a free abelian group has **finite or infinite rank** if it has a finite or infinite basis, respectively. Show that if a basis is finite with n elements (infinite), then any other basis is also finite with n elements (infinite).

3.5 Let L and L' be isomorphic abelian groups generated by X and X' respectively. Show that if X consists of a finite number of elements, then X' consists of the same number of elements..

3.6 Let $\{G_j\}_{j \in X}$ be a family of abelian groups indexed by the set X with every $G_j \cong \mathbb{Z}, j \in X$. Define $L = \{\alpha : X \to \mathbb{Z} \mid \alpha(j) = 0$ for almost every $j \in X\}$ together with a binary operation given by $(\alpha + \beta)(j) = \alpha(j) + \beta(j)$ $j \in X$.

(i) Prove that L is an abelian group.

(ii) Define $f : X \to L$ as $j \mapsto f(j)(i) = 1$ if $i = j, 0$ if $i \neq j$. Show that (L, f) is a free abelian group on X.

(iii) Prove that $\sum_{j \in X} G_j \cong (L, f)$.

(iv) Conclude that an abelian group has rank m if and only if it is isomorphic to the direct sum of m infinite cyclic groups.

The following problems are optional (it is not expected that they will be solve without outside help) and will establish (together with the problems of previous sections and chapters) the **groups with order less than** 16, that is:

Order	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Number	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1

where the upper row indicates the order of the group and the lower row indicates the number of groups, up to isomorphismo, of that order.

3.7 Prove that if p is a prime number that divides the order of a group, then the group contains an element of order p. This is **Cauchy's Theorem**.

3.8 Prove that there only exist two groups of order $2p$ for every prime number p, one is cyclic and the other is D_p.

3.9 Write down all the groups, up to isomorphism, of every order less than 16.

3.10 Determine all the groups, up to isomorphism, of order 10.

3.11 Verify that the following presentations of $\mathbb{Z}_6$ are isomorphic:

$$(x, y | xyx^{-1}y^{-1} = e, x^2 = e, y^3 = e) \text{ and } (x | x^6 = e).$$

3.12 Determine all the groups, up to isomorphism, of order 8. (There are five, of which three are abelian and two are not abelian).

3.13 Determine all the groups, up to isomorphism, of order 12. (There are five, two are abelian and three are not abelian. Hint: use the Sylow Theorems and similar arguments as those used in the previous problem).

3.4 Tensor Product

We will define an abelian group in which there are only biadditive relations.

4.1 Definition. Let X and Y be abelian groups. The **tensor product** of X and Y is the pair (T, f), where T is an abelian group and $f\colon X \times Y \to T$ is a biadditive function, such that, if G is an abelian group and $g\colon X \times Y \to G$ is biadditive, then there exists a unique homomorphism $h\colon T \to G$ such that $g = h \circ f$.

The condition $g = h \circ f$ can be represented by the diagram

$$\begin{array}{ccc} X \times Y & \xrightarrow{f} & T \\ {}^{g}\searrow & & \swarrow^{h} \\ & G & \end{array}$$

The previous definition tells us that any biadditive function $g\colon X \times Y \to G$ can be expressed in terms of $f\colon X \times Y \to T$ as $g(x, y) = h(f(x, y))$ for a unique homomorphism $h\colon T \to G$.

We will see that the tensor product of two abelian groups, if it exists, is unique. That is, given two tensor products (T, f) and (T', f') of X and Y there exists an isomorphism between T and T'. This is immediate because, as T is a tensor product, there exists $h\colon T \to T'$ such that $f' = h \circ f$. Analogously, as T' is a tensor product, there exists $h'\colon T' \to T$ such that $f = h' \circ f'$. Consider the following diagrams

$$\begin{array}{ccc} & & T \\ & {}^{f}\nearrow & \downarrow^{h} \\ X \times Y & \xrightarrow{f'} & T' \\ & {}^{f}\searrow & \downarrow^{h'} \\ & & T \end{array}$$

$$\begin{array}{ccc} & & T' \\ & {}^{f}\nearrow & \downarrow^{h'} \\ X \times Y & \xrightarrow{f} & T \\ & {}^{f'}\searrow & \downarrow^{h} \\ & & T' \end{array}$$

As T is a tensor product, and $1_T\colon T \to T$ is such that $1_T \circ f = f$ we see that $h' \circ h \circ f = f$ as well. Thus, by uniqueness, we have $h' \circ h = 1_T$. Similarly, as T' is a tensor product, and $1_{T'}\colon T' \to T'$ is such that $1_{T'} \circ f' = f'$ and $h \circ h' \circ f' = f'$ as well, by uniqueness we see that $h \circ h' = 1_{T'}$. Hence, h is an isomorphism. Then we can identify the tensor product of T of X and denote it as $T = X \otimes Y$ or, simply, $X \otimes Y$.

Now we will see that, given two abelian groups, their tensor product always exists

4.2 Proposition. Let X and Y be two abelian groups. Then there exists and abelian group T that fulfills the previous definition.
Proof. Let L be a free abelian group with basis $X \times Y$ and let G be a subgroup of L generared by the elements $(x + x', y) - (x, y) - (x', y)$ and $(x, y + y') - (x, y) - (x, y')$ where $x, x' \in X$ and $y, y' \in Y$. Define $X \otimes Y = T = L/G$. Denote as $x \otimes y$ the coset $(x, y) + G$. It can be shown immediately that $X \times Y \to X \otimes Y$, given by $f(x, y) = x \otimes y$ is biadditive, (Problem 4.1). We will se that $X \otimes Y$ is, indeed, a tensor product. Let G' be an abelian group. Consider the triangle

$$\begin{array}{ccc} X \times Y & \xrightarrow{f} & T \\ {\scriptstyle g}\searrow & & \swarrow{\scriptstyle h'} \\ & G' & \end{array}$$

where g is biadditive. As L is free with basis $X \times Y$, there exists a homomorphism $h' \colon L \to G$ such that $g = h' \circ f$. It is easy to see that h' is annihilated by the generators of G. Hence, $G \subset \ker h'$, and induces a homomorphism $h \colon L/G \to G'$ such that the following triangle commutes:

$$\begin{array}{ccc} X \times Y & \xrightarrow{f} & L/G = X \otimes Y \\ {\scriptstyle g}\searrow & & \swarrow{\scriptstyle h} \\ & G' & \end{array}$$

It is easy to show that h is unique (Problem 4.1).♦

For every $x \in X$ and $y \in Y$, the element $f(x, y)$ will be written as $x \otimes y$. It can be shown (Problem 4.2) that $f(X \times Y)$ generates the tensor product T, which we will denote as $X \otimes Y$. Then, every element of $X \otimes Y$ can be written as $\sum_{i=1}^{r} \lambda_i (x_i \otimes y_i)$ with $\lambda_i \in \mathbb{Z}$, $x_i \in X$, $y_i \in Y$. This expression is not unique because different representatives can be chosen from a coset. Due to this, we can define $X \otimes Y$ alternatively as the abelian group generated by all the symbols $x \otimes y$, $x \in X$, $y \in Y$, subject to the relations

$$\begin{aligned} (x_1 + x_2) \otimes y &= x_1 \otimes y + x_2 \otimes y, \\ x \otimes (y_1 + y_2) &= x \otimes y_1 + x \otimes y_2. \end{aligned}$$

This expression is not unique because, by the biadditivity of f, we have

$$\begin{aligned} (x_1 + x_2) \otimes y &= (x_1 \otimes y) + (x_2 \otimes y), \\ x \otimes (y_1 + y_2) &= (x \otimes y_1) + (x \otimes y_2), \end{aligned}$$

where $x_1, x_2, x \in X$ and $y_1, y_2, y \in Y$. As a particular case we have that, for $\lambda \in \mathbb{Z}, (\lambda x) \otimes y = \lambda(x \otimes y) = x \otimes (\lambda y)$. If $\lambda = -1$ we can see that

$(-x)\otimes y = -(x\otimes y) = x\otimes(-y)$ and if $\lambda = 0$ it can be seen that $0\otimes y = 0 = x\otimes 0$. Hence, any element of $X \otimes Y$ can be written as

$$\sum_{i=1}^{r}(x_i \otimes y_i)$$

where $x_i \in X$, $y_i \in Y$.

The biadditive function f is called the **universal biadditive function** (any other biadditive function $g\colon X \times Y \to G$ is obtained from f). We say the due to the universal property, the abelian group $X \otimes Y$ is determined uniquely up to isomorphism.

Let $\varphi\colon X' \to X$, $\psi\colon Y' \to Y$ be homomorphisms of abelian groups

$$\varphi \times \psi\colon X' \times Y' \to X \times Y$$

given by

$$(\varphi \times \psi)(x, y) = (\varphi(x), \psi(y)).$$

Let $f\colon X' \times Y' \to X' \otimes Y'$ and $g\colon X \times Y \to X \otimes Y$ be biadditive functions. Consider the biadditive function

$$g \circ (\varphi \times \psi)\colon X' \times Y' \to X \otimes Y.$$

As $X' \otimes Y'$ is the tensor product, there exists a unique homomorphism

$$h\colon X' \otimes Y' \to X \otimes Y$$

that we will denote as $\varphi \otimes \psi$ such the the following diagram commutes:

$$\begin{array}{ccc} X' \times Y' & \xrightarrow{f} & X' \otimes Y' \\ {\scriptstyle \varphi\times\psi}\downarrow & & \downarrow{\scriptstyle \varphi\otimes\psi} \\ X \times Y & \xrightarrow{g} & X \otimes Y \end{array}$$

i.e.,

$$(\varphi \otimes \psi) \circ f(x, y) = g \circ (\varphi \times \psi)(x, y); (x, y) \in X' \times Y'.$$

Thus

$$(\varphi \otimes \psi)(x \otimes y) = \varphi(x) \otimes \psi(y), x \in X', y \in Y'.$$

As a consecuence of the uniqueness of $\varphi\otimes\psi$ we have that if $X' \xrightarrow{\varphi} X \xrightarrow{\varphi'} X''$ and $Y' \xrightarrow{\psi} Y \xrightarrow{\psi'} Y''$ are homomorphisms of abelian groups, then

$$(\varphi' \circ \varphi) \otimes (\psi' \circ \psi) = (\varphi' \otimes \psi') \circ (\varphi \otimes \psi).$$

In particular, the following propositions are immediate.

4.3 Proposition. Let $\psi\colon Y' \to Y$ and $\psi'\colon Y \to Y''$ be homomorphisms of abelian groups and X an abelian group. Then

(i) if $1_X\colon X \to X$ and $1_Y\colon Y \to Y$ are identity homomorphisms then $1_X \otimes 1_Y$ is the identity of $X \otimes Y$, and

(ii) $(1_X \otimes \psi') \circ (1_X \otimes \psi) = (1_X \otimes (\psi' \circ \psi))$.♦

We can show these properties with the following diagram:

$$\begin{tikzcd}
Y' \arrow[d, "\psi"] \arrow[dd, bend right=60, "\psi'\circ\psi"'] & X\otimes Y' \arrow[d, "1_X\otimes\psi"] \arrow[dd, bend left=60, "1_X\otimes\psi'\circ\psi"] \\
Y \arrow[d, "\psi'"] \arrow[r, "X\otimes ?"] \arrow[dr, bend left, "1_Y"] & X\otimes Y \arrow[d, "1_X\otimes\psi'"] \arrow[dl, bend right, "1_X\otimes 1_Y"'] \\
Y'' & X\otimes Y''
\end{tikzcd}$$

Analogously, we have the following

4.4 Proposition. Let $\varphi\colon X' \to X$ and $\varphi'\colon X \to X''$ be homomorphisms of abelian groups and Y an abelian group. Then

(i) if $1_X\colon X \to X$ and $1_Y\colon Y \to Y$ are the identity homomorphisms, then $1_X \otimes 1_Y$ is the identity on $X \otimes Y$, and

(ii) $(\varphi' \otimes 1_Y) \circ (\varphi \otimes 1_Y) = ((\varphi' \circ \varphi) \otimes 1_Y)$.♦

We can also show these properties by the following diagram:

$$\begin{tikzcd}
X' \arrow[d, "\varphi"] \arrow[dd, bend right=60, "\varphi'\circ\varphi"'] & X'\otimes Y \arrow[d, "\varphi\otimes 1_Y"'] \arrow[dd, bend left=60, "(\varphi'\circ\varphi)\otimes 1_Y"] \\
X \arrow[d, "\varphi'"] \arrow[r, "?\otimes Y"] \arrow[dr, bend left, "1_X"] & X\otimes Y \arrow[d, "\varphi'\otimes 1_Y"'] \arrow[dl, bend right, "1_X\otimes 1_Y"'] \\
X'' & X''\otimes Y
\end{tikzcd}$$

The following is a result about the tensor product of a direct sum of abelian groups:

4.5 Proposition. (i) Let X and Y be abelians groups with $Y = \sum_{i\in I} Y_i$. Then

$$X \otimes \left(\sum_{i\in I} Y_i\right) \cong \sum_{i\in I} (X \otimes Y_i)$$

(ii) Let X and Y be abelian groups and $X = \sum_{i\in I} X_i$. Then

$$\left(\sum_{i\in I} X_i\right) \otimes Y \cong \sum_{i\in I}(X_i \otimes Y)$$

Proof. Let $g\colon X \times (\sum_{i\in I} Y_i) \to \sum_{i\in I}(X \otimes Y_i)$ given by $g(x,(y_i)) = (x \otimes y_i)$. It is easy to show that g es biadditive. Then there exists

$$h\colon M \otimes (N_i) \to (M \otimes N_i)$$

such that the following diagram commutes:

$$\begin{array}{ccc} X \times \left(\sum_{i\in I} Y_i\right) & \xrightarrow{f} & X \otimes \left(\sum_{i\in I} Y_i\right) \\ {\scriptstyle g}\searrow & & \swarrow{\scriptstyle h} \\ & \sum_{i\in I}(X \otimes Y_i) & \end{array}$$

Let $\varphi_i\colon X \otimes Y_i \to X \otimes (\sum_{i\in I} Y_i)$ be given by $\varphi_i(x \otimes y_i) = x \otimes \iota_{Y_i}(y_i)$ where $\iota_{Y_i}\colon Y_i \to \sum_{i\in I} Y_i$ is the inclusion. Then, by the universal property of the direct sum, there exists a unique homomorphism

$$\varphi : \sum_{i\in I}(X \otimes Y_i) \to X \otimes \left(\sum_{i\in I} Y_i\right)$$

such that if $\iota_{X\otimes Y_i}\colon X \otimes Y_i \to \sum_{i\in I}(X \otimes Y_i)$ is the inclusion then $\varphi_i = \varphi \circ \iota_{X\otimes Y_i}$, that is, the following diagram commutes for every $i \in I$

$$\begin{array}{ccc} & X \otimes \left(\sum_{i\in I} Y_i\right) & \\ {\scriptstyle \varphi_i}\nearrow & & \nwarrow{\scriptstyle \varphi} \\ X \times Y_i & \xrightarrow{\iota_X \otimes Y_i} & \bigoplus_{i\in I}(X \otimes Y_i) \end{array}$$

It is easy to verify that $\varphi \circ h = 1_{X\otimes(\sum_{i\in I} Y_i)}$ and that $h \circ \varphi = 1_{\oplus_{i\in I}(X\otimes Y_i)}$. The proof of (ii) is analogous.♦

4.6 Proposition. (i) If $Y' \overset{\psi}{\rightarrowtail} Y \overset{\psi}{\twoheadrightarrow} Y''$ is an exact sequence of abelian groups and X an abelian group, then

$$X \otimes Y' \xrightarrow{1_X\otimes\psi} X \otimes Y \xrightarrow{1_X\otimes\psi'} X \otimes Y'' \longrightarrow 0$$

is an exact sequence. (ii) If $X' \overset{\varphi}{\rightarrowtail} X \overset{\varphi'}{\twoheadrightarrow} X''$ is an exact sequence of abelian groups and Y an abelian groups, then

$$X' \otimes Y \xrightarrow{\varphi\otimes 1_Y} X \otimes Y \xrightarrow{\varphi'\otimes 1_Y} X'' \otimes Y \longrightarrow 0$$

is an exact sequence..
Proof. (i) We will see that $1_X \otimes \psi'$ is an epimorphism: let $t'' = \sum(x_i \otimes y_i'') \in X \otimes Y''$, $x_i \in X$, $y_i'' \in Y''$. As ψ' is an epimorphism, there exists $y_i \in Y$ such that $\psi'(y_i) = y_i''$ for every i. Thus,,

$$(1_X \otimes \psi')\left(\sum(x_i \otimes y_i)\right) = \sum(x_i \otimes y_i'').$$

As

$$(1_X \otimes \psi')(1_X \otimes \psi) = (1_X \otimes \psi'\psi) = 1_X \otimes 0 = 0$$

we can see that $im(1_X \otimes \psi) \subset \ker(1_X \otimes \psi')$. It remains to verify that $(1_X \otimes \psi) \supset \ker(1_X \otimes \psi')$, which we will leave to the reader, as well as part (ii).♦

The previous result is the best we can obtain. For example, is we consider an exact sequence

$$\mathbb{Z} \overset{2.\_}{\rightarrowtail} \mathbb{Z} \twoheadrightarrow \mathbb{Z}/2$$

where 2._ denotes the multiplication by two, when the tensor product is constructed with $Y = Z/2$ we obtain

$$\mathbb{Z} \otimes \mathbb{Z}/2 \xrightarrow{2_*} \mathbb{Z} \otimes \mathbb{Z}/2 \twoheadrightarrow \mathbb{Z}/2 \otimes \mathbb{Z}/2$$

which is equivalent to

$$\mathbb{Z}/2 \xrightarrow{2_*} \mathbb{Z}/2 \twoheadrightarrow \mathbb{Z}/2$$

but 2_* is not injective..

Now we will establish some **properties of the tensor product**.

4.7 Proposition. Let Y be an abelian group. Then $Y \otimes \mathbb{Z} \cong Y \cong \mathbb{Z} \otimes Y$.
Proof. Let $g\colon Y \times \mathbb{Z} \to Y$ be the biadditive function given by $g(y, \lambda) = \lambda y$, $\lambda \in \mathbb{Z}$, $y \in Y$. Then there exists a unique homomorphism $h\colon Y \otimes \mathbb{Z} \to Y$ such that $h \circ f = g$, that is, the following diagram commutes:

$$\begin{array}{ccc} Y \times \mathbb{Z} & \xrightarrow{f} & Y \otimes \mathbb{Z} \\ {\scriptstyle g}\searrow & & \swarrow{\scriptstyle h} \\ & Y & \end{array}$$

The biadditive function g is surjective because $g(y, 1) = 1 \cdot y = y$. As $h \circ f = g$ then h is surjective.

We will see that h is injective: sea $x \in Y \otimes \mathbb{Z}$. Then there exist elements $\{y_i\}_{i=1}^n$ in Y and $\{\lambda_i\}_{i=1}^n$ in $\mathbb{Z}$ such that x is $\sum_{i=1}^n (y_i \otimes \lambda_i)$ for $y_i \in Y$, $\lambda_i \in \mathbb{Z}$. However,

$$x = \sum_{i=1}^n (y_i \otimes \lambda_i) = \sum_{i=1}^n (\lambda_i y_i \otimes 1) = (\sum_{i=1}^n \lambda_i y_i) \otimes 1 = y \otimes 1,$$

thus

$$h(x) = h(y \otimes 1) = h(f(y,1)) = g(y,1) = 1 \cdot y = y.$$

If $h(y \otimes 1) = 0$ then $y = 0$ and $x = y \otimes 1 = 0$. Hence, h es inyective. The proof that $Y \cong \mathbb{Z} \otimes Y$ is left to the reader(Problem 4.5).♦

4.8 Proposition. Let X, Y, Z be abelian groups. Then

$$(X \otimes Y) \otimes Z \cong X \otimes (Y \otimes Z) \cong X \otimes Y \otimes Z$$

Proof. Consider the biadditive function

$$g'' \colon X \times Y \to X \otimes Y \otimes Z$$

given by $g''(x,y) = x \otimes y \otimes w$ for $w \in Z$ fixed, which induces a homomorphism

$$h_w \colon X \otimes Y \to X \otimes Y \otimes Z$$

such that

$$h_w(x \otimes y) = x \otimes y \otimes w.$$

Let

$$g \colon (X \otimes Y) \times Z \to X \otimes Y \otimes Z$$

given by

$$g(t,w) = h_w(t).$$

The function g is biadditive and induces a homomorphism $h \colon (X \otimes Y) \otimes Z \to X \otimes Y \otimes Z$

such that.

$$h((x \otimes y) \otimes w) = x \otimes y \otimes w.$$

We now construct a function

$$h' \colon X \otimes Y \otimes Z \to (X \otimes Y) \otimes Z$$

such that $h' \circ h = 1_{(X \otimes Y) \otimes Z}$ and $h \circ h' = 1_{X \otimes Y \otimes Z}$. To construct h' consider the function

$$g' \colon X \times Y \times Z \to (X \otimes Y) \otimes Z$$

given by

$$g'(x,y,w) = (x \otimes y) \otimes w.$$

g' is linear in each variable, thus induces a homomorphism

$$h' \colon X \otimes Y \otimes Z \to (X \otimes Y) \otimes Z$$

such that

$$h(x \otimes y \otimes w) = (x \otimes y) \otimes w.$$

It is easily verified that $h' \circ h = 1_{(X \otimes Y) \otimes Z}$ and that $h \circ h' = 1_{X \otimes Y \otimes Z}$ thus, h and h' are isomorphisms. The proof that $X \otimes (Y \otimes Z) \cong X \otimes Y \otimes Z$ is analogous.♦

Problems

4.1 Show that in Proposition 4.2 $f\colon X \times Y \to X \otimes Y$, given by $f(x,y) = x \otimes y$ is biadditive, h' is annihilated in the generators of G and h is unique.

4.2 Verify that $f(X \times Y)$ generates $X \otimes Y$. (Hint:define a homomorphism $i\colon X \times Y \to X \otimes Y$ and use the uniqueness to show that i is surjective).

4.3 Let $g\colon X \times (\sum_{i\in I} Y_i) \to \sum_{i\in I}(X \otimes Y_i)$ given by $g(x,(y_i)) = (x \otimes y_i)$ as in Proposition 4.5. Verify that g is biadditive. Verify that $\varphi \circ h = 1_{X\otimes(\sum_{i\in I} Y_i)}$ and that $h \circ \varphi = 1_{\oplus_{i\in I}(X\otimes Y_i)}$ as well. Prove part (ii).

4.4 In Proposition 4.6 show that $(1_X \otimes \psi) \supset \ker(1_X \otimes \psi')$, as well as part (ii).

4.5 Prove that $Y \cong \mathbb{Z} \otimes Y$.

4.6 Prove that $X \otimes Y \cong Y \otimes X$.

4.7 Prove that $X \otimes (Y \otimes Z) \cong X \otimes Y \otimes Z$.

4.8 Prove that if $X' \overset{\varphi}{\rightarrowtail} X \overset{\varphi'}{\twoheadrightarrow} X''$ is an exact sequence of abelian groups that **splits** (that is, $X \cong X' \oplus X''$) and Y an abelian group, then

$$0 \to X' \otimes Y \xrightarrow{\varphi\otimes 1_Y} X \otimes Y \xrightarrow{\varphi'\otimes 1_Y} X'' \otimes Y \to 0$$

is an exact sequence that splits (that is, $X \otimes Y \cong X' \otimes Y \oplus X'' \otimes Y$).

Chapter 4

A detailed exposition of some applications of Group Theory to Music Theory will be made in this chapter. Some basic applications of Mathematical Music Theory will be explained and, in the process, we hope to contribute theoretical and analytical elements to readers with different backgrounds, both in Mathematics as well as Music. With this in mind, the examples follow from some of the most important theoretical aspects of the previous chapters; the musical terms and concepts are introduced as they are needed, so that a reader, without a musical background can understand the essence of how Group Theory is used to explain certain pre-established musical relations. For the reader with knowledge of Music Theory, this chapter provides concrete elements, as well as motivation, to begin to comprehend Group Theory.

A goal of Music Theory is to describe the possibilities of a pitch system. A pitch is the sound that is heard and that, usually, is associated to frequencies of vibrations. Traditionally, the study of the intervals between pitches was done using the frequency ratios of the powers of small integers. Modern Mathematical Music Theory offers an independent way of understanding pich systems by considering the intervals as transformations. In this chapter we will explore and develop some aspects of Neo-Riemannian Theory, in particular the duality of the TI and PLR groups. The content of this chapter is based on [CFS] and [DP].

4.1 Musical Background

The twelve pitches of our modern system use the names of the first 7 letters of the alphabet. Each letter represents a different frequency and the letters are repeated when the frequency of a pitch is doubled. The range of pitches which begin with a frequencey, until it is doubled, is known as an **octave**. By convention, the octave is divided into 12 equal intervals, from which we obtain a set of 12 pitches, such that the frequency of each pitch results from multiplying

Note	Frecuency (Hz)	Note	Frecuency (Hz)
C_4	261.63	$F\sharp_4/G\flat_4$	369.99
$C\sharp_4/D\flat_4$	277.18	G_4	392.00
D_4	293.66	$A\flat_4/G\sharp_4$	415.30
$E\flat_4/D\sharp_4$	311.10	A_4	440.00
E_4	329.63	$B\flat_4/A\sharp_4$	466.16
F_4	349.23	B_4	493.88

Table 4.1: Frecuencies of the notes in the central octave.

the previous one by $\sqrt[12]{2}$[1]. This is known as **equal tempered tuning**. Previous to equal tempered tuning, musicians used, among others, just tuning, which is a system whose notes have frequencies that are related by ratios of integers. In equal tempered tuning, the difference in frequency between each note is called a **semitone**. With only 7 letters and 12 notes, the symbol $\sharp$ is used to denote a pitch that is a semitone above the original and the symbol $\flat$ to denote a pitch that is a semitone below the original. For example, if we take the pitch G, then the note that is above by a semitone would be $G\sharp$ and the note that is below by a semitone would be $G\flat$. The complete set of twelve notes is called the **chromatic scale** and is denoted, musically, as follows:

$$C, C\sharp, D, D\sharp, E, F, F\sharp, G, G\sharp, A, A\sharp, B.$$

As was previously mentioned, two successive notes differ by a semitone. The note that is a semitone above G is $G\sharp$, although this same note is a semitone below A and can be denoted as $A\flat$. This property of notes possessing multiple names in equal tempered tuning is known as **harmonic equivalence**. This is shown together with the frequency values of each pitch (beginning with middle C[2] and the eleven notes that follow it) in the table 4.1.

As all multiples of a certain frequency are represented by the same letter, it is mathematically convenient to represent the set of twelve notes by the integers modulo 12 ($\mathbb{Z}_{12}$), where each element is a class and represents an infinite set of numbers. According to the literature on Mathematical Music Theory, we will assign number to the letters, as is shown in the figure 4.1.

[1] The human brain interprets the distances between the pitches logarithmically. That is, the distance (in octaves) between a pitch of frequency F_1 and another with frequency F_2 is perceived as

$$|\log_2(F_1) - \log_2(F_2)|.$$

For this reason, if $F_2 = 2F_1$, then the distance is

$$|\log_2(F_1) - \log_2(F_2)| = |\log_2(F_1) - \log_2(2F_1)| = |\log_2(\tfrac{F_1}{2F_1})| = |\log_2 \tfrac{1}{2}| = |-1| = 1.$$

The reader can verify that if the distance between F_1 and $2F_2$ is divided in twelve equal parts, the frequencies of the resulting pitches are the same as those obtained by multplying F_1 by successive powers of $2^{\frac{1}{12}}$.

[2] In the scientific notation of pitch, middle C is located in the fourth octave. That is why it is denoted C_4.

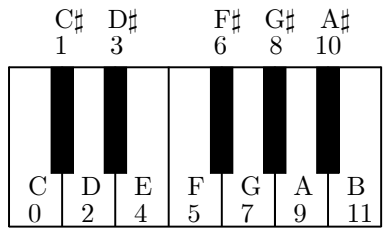


Figure 4.1: Notes assigned to the elements of $\mathbb{Z}_{12}$.

This assignment is not rigid, and it is valid to assign 0 to any of the 12 notes. In this chapter, we are interested in sets of notes that are played simultaneously. These sets of notes are known as **chords**. We will concentrate, in particular, on the group of chords known as **triads**, that is, sets of 3 notes that are played simultaneously.

Now, there are $\binom{12}{3} = 220$ subsets of 3 notes of the set of 12 notes. However, we will limit ourselves to the study of sets of 3 elements that are known as major and minor chords.

The three notes of a triad are called the root, the third and the fifth, respectively. Each triad has the name of its root. However, in our work the triads are sets and the order is not important (except to identify the root, of course). The major and minor chords are defined as follows:

Definition 1 *We will say the the chord $\{a, b, c\} \in \wp(\mathbb{Z}_{12})$ is a **major chord** if $b = a + 4$ and $c = a + 7$.*

The major chords, in this order, are in the root position and are designated with upper case letters, such as $G\sharp = \{8, 0, 3\}$.In the case of G♯, the root is G♯ = 8, the third is B♯ = 0, and the fifth is D♯ = 3.

In spite of this musical observation, in the mathematical work with the triads (that are sets of three elements) we insist that the order does not matter: sometimes it will be more useful to refer to G♯ as, say, $\{3, 0, 8\}$. The same is true for the minor chords that are defined as follows.

Definition 2 *We say that a chord $\{a, b, c\} \in \wp(\mathbb{Z}_{12})$ is a **minor chord** if $b = a + 3$ and $c = a + 7$.*

The minor chords in this order are also in root position, and will be denoted with lower case letters, for example, f = $\{5, 8, 0\}$. Now that we have defined the elements, we will refer to them as **pitch class triads**.

Definition 3 *The complete set of the 24 major and minor chords will be denoted as $\mathcal{M}$. Specifically,*

$$\mathcal{M} = \{\{x, x+3, x+7\}, \{X, X+4, X+7\} | x, X \in \mathbb{Z}_{12}\}.$$

We willl emphasize, once again, that chords are sets and, for this reason, are not ordered. In other words: by definitions 1 and 2 if the set $\{5, 8, 0\}$ is written in another order, say,$\{0, 8, 5\}$, there is no difference because both sets represent the F minor chord. The F minor chord is formed by playing the notes F, A♭, and C simultaneously. If we take $\{0, 8, 5\}$, we are still be indicating that the notes C, A♭, and F will be played together, forming the F minor chord. Hence, the root position of the chord (as in the definitions **??** and **??**) shows how the components of the chord will be included, but the individual notes can be distributed many ways without changing the identity of the chord.

There is a detail that should be considered with respect to the term "triad of pitch classes". It should be clear with which elements we are working because, up until now, we have refered to the triad of pitch classes just as a triad. However, an element x in $\mathcal{M}$ is a tríad, where $x = \{a, b, c\}$, and $a, b, c \in \mathbb{Z}_{12}$. This notation is used because it is comfortable and simple, but to be precise we must remember that $\mathbb{Z}_{12}$ is a set of cosets:

$$\mathbb{Z}_{12} = \{[0], [1], \ldots, [11]\},$$

where

$$[0] = \{\ldots, -24, -12, 0, 12, 24, \ldots\},$$
$$\vdots$$
$$[11] = \{\ldots, -13, -1, 11, 23, \ldots\}.$$

Therefore, $a \in \mathbb{Z}_{12}$, really means that $[a] \in \mathbb{Z}_{12}$. We call them pitch classes because every note from C to B represents all multiples of those pitches, in the same way that every coset in $\mathbb{Z}_{12}$ represents all the numbers modulo 12 of which they are multiples. For this reason, when reading $x = \{a, b, c\}$, we are really reading $[x] = \{[a], [b], [c]\}$. Hence, this idea is extended from pitch classes to triads of pitch classes, where all the elements in $\mathcal{M}$ are also classes. As an example, take the C major chord, $x = \{0, 4, 7\}$. If C major is seen as a class of triads, it whould be represented in the following way:

$$\mathrm{C} = [x] = \{[0], [4], [7]\} = \{\ldots, \{-12, -8, -5\}, \{0, 4, 7\}, \{12, 16, 19\}, \cdots\}.$$

Now that we have clarified the difference between the basic elements and the classes, we will continure denoting $[x]$ with x, for simplicity.

4.2 The T and I Transformations.

In Music Theory, transposition refers to the process of translating a pitch, or set of pitches, by a constant interval. The musical definition of this transformation can be translated directly into the definition of a mathematical transformation.

2.1 Definition. Let $x \in \mathcal{M}$, where $x = \{a, b, c\}$. A **transposition** is a function $T_n : \mathcal{M} \to \mathcal{M}$ given by

$$T_n(x) = x + n = \{a + n, b + n, c + n\},$$

where $n \in \mathbb{Z}$.

T_n can only be applied to the 24 elements (triads) in $\mathcal{M}$, but there is an infinite amount of transpositions of any triad because $n \in \mathbb{Z}$. However, after having transposed any triad 12 times, the same sequence of triads is obtained once again. For example:

$$\begin{array}{cc}
T_0(C) & T_0(\{0,4,7\}) = \{0,4,7\} \\
T_1(C) & T_1(\{0,4,7\}) = \{1,5,8\} \\
\vdots & \\
T_{12}(C) & T_{12}(\{0,4,7\}) = \{0,4,7\} = T_0(C) \\
T_{13}(C) & T_{13}(\{0,4,7\}) = \{1,5,8\} = T_1(C) \\
\vdots &
\end{array}$$

T_0 behaves like the identity function and, for every triad, there are at most 12 different transpositions.

We can see the transpositions, geometrically, as the rotations of a triangle through 12 points equally distributed in a circle. The three vertices of the triangle represent all the pitches of the triad. For example,the C major chord $\{0, 4, 7\}$ is situated in the upper left corner of the figure 4.2 . Then the three vertices, or pitches, are rotated towards the right, one by one. The figure 4.2 presents the process of applying $T_n(\{0, 4, 7\})$, for every $0 \leq n < 12$, to the C major chord.

2.2 Definition. Let $x \in \mathcal{M}$, where $x = \{a, b, c\}$. An **inversion** is a function $I_n : \mathcal{M} \to \mathcal{M}$ given by

$$I_n(x) = -x + n = \{-A + n, -B + n, -C + n\}$$

where $n \in \mathbb{Z}$.

As in the case of the transpositions, there are 24 tríads to invert and an infinite number of inversions of each triad. However, once again, when we invert a triad and then transpose it 12 times, we are back to the starting point, and

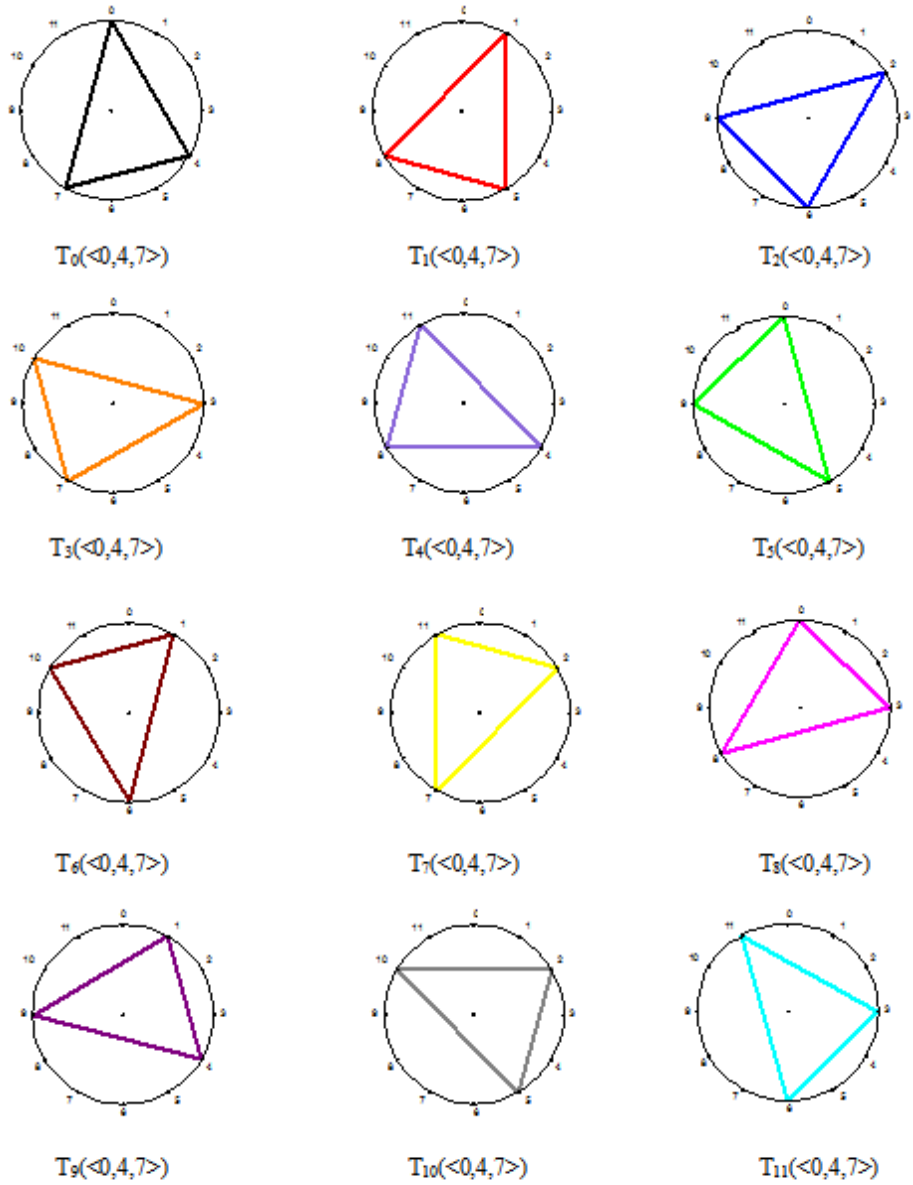


Figure 4.2: The twelve transpositions of the C major $\{0, 4, 7\}$ triad.

the same sequence is obtained when we begin again. For example:

$$\begin{aligned} I_0(C) &= I_0(\{0,4,7\}) = \{0,8,5\} \\ I_1(C) &= I_1(\{0,4,7\}) = \{1,9,6\} \\ &\vdots \\ I_{12}(C) &= I_{12}(\{0,4,7\}) = \{0,8,5\} = I_0(C) \\ I_{13}(C) &= I_{13}(\{0,4,7\}) = \{1,9,6\} = I_1(C) \\ &\vdots \end{aligned}$$

Once again it can be seen that for each triad there are no more than 12 different inversions. In contrast with the geometric representation of the transposition, the representation that corresponds to the inversion is relatively more descriptive. All the inversions can be ilustrated as reflections of triangles with respect to the vertical axis that passes through 0 and 6 in the circle. At first sight, thefigure 4.3 does not present the 12 inversions of $\{0,4,7\}$. With the intention of illustrating the reflections, the figure presents the inverted form of every major triad. However, each one of these triads is, at the end, a transposition of the original triad $\{0,4,7\}$. In other words, if each one of the triads of the figure 4.2 is reflected, the ones from the figure 4.3are obtained.

2.3 Proposition. For every $n, k \in \mathbb{Z}$, such that $n \equiv k \mod 12$,

$$T_n = T_k \quad \text{and} \quad I_n = I_k$$

Proof. As $n \equiv k \mod 12$, then $n = 12q + k$, for some $q \in \mathbb{Z}$. Hence

$$T_n = T_{12q+k} = T_{12q} \circ T_k = (T_0)^q \circ T_k = (i)^q \circ T_k = T_k$$

where i is the identity transformation (or the translation by 0) and

$$I_n = I_{12q+k} \overset{*}{=} T_{12q} \circ I_k = (T_0)^q \circ I_k = (i)^q \circ I_k = I_k;$$

the equality marked with an asterisc will be shown in lemma 4.2.♦

2.4 Definition. The set of all the transposition and inversion functions is denote as TI, and is defined as:

$$\mathrm{TI} = \{T_n, I_n | n = 0, \ldots, 11\}.$$

It turns out that we can represent all these elements in a more compact form if we analyze the four possibile compositions of the T and I functions.

2.5 Lemma. In the TI set there exist the following relations:

$$\begin{aligned} T_m \circ T_n &= T_{m+n \bmod 12}, \\ T_m \circ I_n &= I_{m+n \bmod 12}, \\ I_m \circ T_n &= I_{m-n \bmod 12}, \\ I_m \circ I_n &= T_{m-n \bmod 12}. \end{aligned}$$

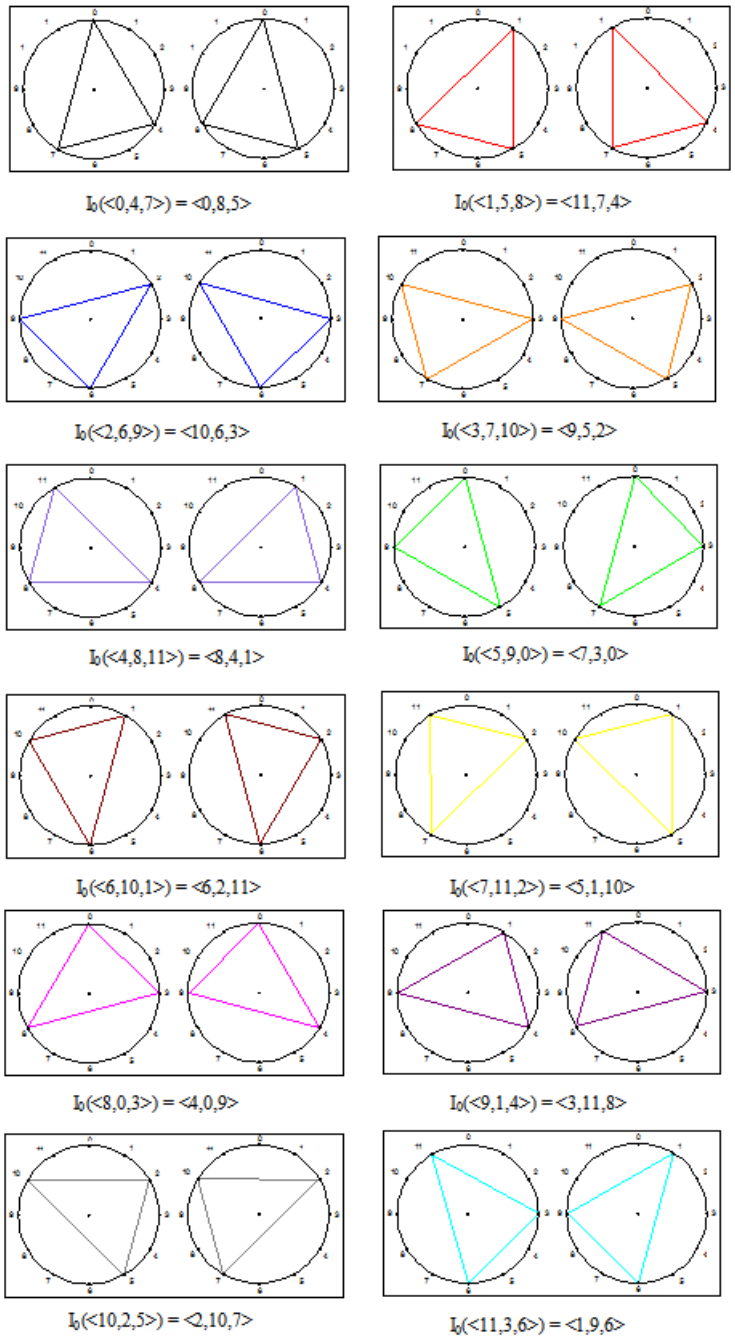


Figure 4.3: The twelve inversions of the C major $\{0, 4, 7\}$ triad.

Proof. For the first equality we have

$$\begin{aligned} T_m \circ T_n &= T_m(T_n(\{a,b,c\})) \\ &= T_m(\{a+n, b+n, c+n\}) \\ &= \{a+n+m, b+n+m, c+n+m\} \\ &= \{a+(m+n), b+(m+n), c+(m+n)\} \\ &= T_{m+n \bmod 12} \end{aligned}$$

whereas for the second

$$\begin{aligned} T_m \circ I_n &= T_m(I_n(\{a,b,c\})) \\ &= T_m(\{-a+n, -b+n, -c+n\}) \\ &= \{-a+n+m, -b+n+m, -c+n+m\} \\ &= \{-a+(m+n), -b+(m+n), -c+(m+n)\} \\ &= I_{m+n \bmod 12}. \end{aligned}$$

The proof of the other two equalities is left as an exercise for the reader. ♦

If the functions of the TI set are applied consecutively to any triad in $\mathcal{M}$, all of the set $\mathcal{M}$ is reproduced. We reiterate that the figures 4.2 and 4.3 show the result of applying all the functions of T and I to C $= \{0, 4, 7\}$.

It is left to the reader to show, in the exercises, that the functions in T and I are well defined.

2.6 Theorem. The TI set forms a group under composition.
Proof.

1. For all $f, g \in TI$, $f \circ g = h \in TI$, by the lemma 4.2, then TI is closed under composition.

2. The following is satisfied

$$\begin{aligned} T_0 \circ T_n &= T_{0+n} = T_n, \\ T_n \circ T_0 &= T_{n+0} = T_n, \\ T_0 \circ I_n &= I_{0+n} = I_n, \\ I_n \circ T_0 &= I_{n-0} = I_n. \end{aligned}$$

   Hence, $T_0 = i \in TI$ (i.e. T_0 is the identity element).

3. On the one hand the relationships:

$$\begin{aligned} T_n \circ T_{12-n} &= T_{n+12-n} = T_{12} = T_0, \\ T_{12-n} \circ T_n &= T_{12-n+n} = T_{12} = T_0, \end{aligned}$$

   implied $T_n^{-1} = T_{12-n}$ and on the other we have $I_n \circ I_n = T_{n-n} = T_0$; this shows that $I_n^{-1} = I_n$.

4. By the properties of the composition of functions, the operation $\circ$ is associative.

Then TI is a group under composition.♦

Problems

2.1 Show that the operations on T are well defined. That is, if $[x]$ is a triad of pitch classes in M, for every $x_1, x_2 \in [x]$ we have: $T_n(x_1) \equiv T_n(x_2)$, i.e. $T_n(\{a_1, b_1, c_1\}) \equiv T_n(\{a_2, b_2, c_2\})$.

2.2 Show that the operations on I are well defined. That is, if $[x]$ is a triad of pitch classes in M, for every $x_1, x_2 \in [x]$ we have: $I_n(x_1) \equiv I_n(x_2)$, i.e. $I_n(\{a_1, b_1, c_1\}) \equiv I_n(\{a_2, b_2, c_2\})$.

2.3 Prove the last two equalities of Lemma 4.2.

4.3 The P, L and R Transformations

In addition to the T and I transformations that we apply to the set $\mathcal{M}$, we also have the parallel (P), leading tone exchange (L), and relative (R) functions. Analogously to what occurs with the T and I functions, there are musical, group theoretic and geometric descriptions of the P, L and R functions. The descriptions and definitions of these three will not be separated, as with the T and I functions, and several examples will be provided after the formal definition.

Two triads are said to be **parallel** if they have the same letter name, but are of opposite parity (**parity** meaning major or minor). For instance, the parallel minor of F major, $F = \{5, 9, 0\}$, is f-minor $f = \{5, 8, 0\}$. Both triads are named with the letter F but one is major and the other is minor.

Two triads are said to be **relative** if they are again of opposite parity, and if the root of the minor triad is three semitones below the root of major triad. To illustrate, we take F-major $\{5, 9, 0\}$ and count three semitones below 5, which is 2 and then build a minor chord on 2. This yields the d-minor chord $\{2, 5, 9\}$, and d minor is the relative minor of F-major.

Lastly, the **leading tone exchange** is derived from the fact that a semitone below any pitch is called the leading tone of that pitch. Therefore, the leading tone exchange of any triad is also of opposite parity, and the root of the major triad is replaced with its leading tone. We use F-major $\{5, 9, 0\}$once again to illustrate. The root of F is 5, which is replaced with its leading tone, 4. It suffices for now to say that the only minor chord with the pitches 4, 9, and 0 is the a-minor chord, $\{4, 0, 9\}$.

Below are the mathematical definitions of P, L, and R which are then followed by examples .

3.1 Definition. Let $x, Y \in \mathcal{M}$, where $x = \{a, b, c\}$ is a minor triad and $Y = \{A, B, C\}$ is a major triad. Then

$$\begin{aligned}
P(x) &= P(\{a, b, c\}) = \{a, b + 1, c\}, \\
P(Y) &= P(\{A, B, C\}) = \{A, B - 1, C\}, \\
L(x) &= L(\{a, b, c\}) = \{c + 1, a, b\}, \\
L(Y) &= L(\{A, B, C\}) = \{B, C, A - 1\}, \\
R(x) &= R(\{a, b, c\}) = \{b, c, a - 2\}, \\
R(Y) &= R(\{A, B, C\}) = \{C + 2, A, B\}.
\end{aligned}$$

For example,

$$\begin{aligned}
P(c) = P(\{0, 3, 7\}) = \{0, 4, 7\} = C \text{ and } P(F) = P(\{5, 9, 0\}) = \{5, 8, 0\} = f, \\
L(e) = L(\{4, 7, 11\}) = \{0, 4, 7\} = C \text{ and } L(G) = L(\{7, 11, 2\}) = \{11, 2, 6\} = b, \\
R(b) = R(\{11, 2, 6\}) = \{2, 6, 9\} = D \text{ and } R(A) = R(\{9, 1, 4\}) = \{6, 1, 9\} = f\sharp.
\end{aligned}$$

We now explore what the set of P, L, and R functions looks like and we will start with the geometric representation. As with the T and I functions, there is

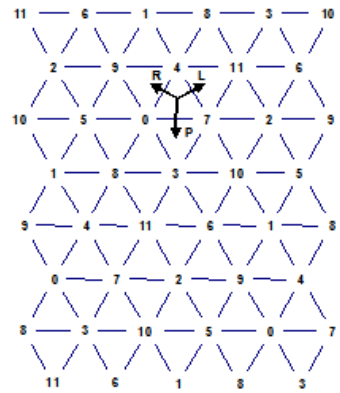


Figure 4.4: Oettingen/Riemann *Tonnetz*

a rather interesting representation of the P, L, and R functions, known as the *Tonnetz*.

The word *Tonnetz* is German for "tone network" and was invented by Leonhard Euler. It was Hugo Riemann that explored its capacity to chart harmonic motion, that is,the movement from one pitch or triad to another. The original *Tonnetz* has undergone various alterations, but we will use the version shown in figure 4.4 . Note that the vertices are pitch classes and the triangles represent major and minor triads. As mentioned before, the P, L, and R transformations preserve 2 pitches when applied to any triad in $\mathcal{M}$. Therefore, the rotation of a triangle about any one of its edges yields another triangle which is equivalent to one of the three triads that P, L, or R would produce. Notice that if we expand the diagram with more vertices, we see that they start repeating vertically and horizontally and, in effect, the grid wraps around and therefore lies on a torus.

Now we will analyze the compositions of the functions P, L, and R and the powers of these compositions, to determine all the elements of the set. Note that P, L, y R are involutive. That is:

$$P^2 = L^2 = R^2 = i.$$

We will show this for the function P, as the L and R functions behave in the same way.

$$P \circ P(\{a, b, c\}) = P(\{a, b+1, c\}) = \{a, (b+1)-1, c\} = \{a, b, c\} = i(\{a, b, c\})$$

By consecutively applying R to any triad and then L to the result, the following sequence of triads is produced (again, upper case representing major triads and lower case representing minor triads):

$$\mathrm{C, a, F, d, B\flat, g, E\flat, c, A\flat, f, D\flat, b\flat, G\flat, e\flat, B, g\sharp, E, c\sharp, A, f\sharp, D, b, G, e, C} \qquad (4.1)$$

This sequence is a famous progression in Beethoven's Ninth Symphony, first observed by Cohn [C]. To follow the first step in the construction of the sequence, we take C $= \{0, 4, 7\}$ and apply the functions R and L, obtaining:

$$R(\{0, 4, 7\}) = \{4, 0, 9\} = a.$$

Hence, C is taken to its relative minor, which is a. After that, we get:

$$L \circ R(\{0, 4, 7\}) = L(\{4, 0, 9\}) = \{5, 9, 0\} = \mathrm{F},$$

which shows that it is taken to its leading tone exchange, which is F major. By continuing this way, the row of triads shown above is produced. Even more, when the functions R and L are applied to any major triad of $\mathcal{M}$, in this order, the same cyclic sequence of triads results. On the other hand, the sequence is produced in reverse order when applied to any minor triad. In general, we can observe that:

$$\begin{aligned}(L \circ R)^3(\{A, B, C\}) &= (L \circ R)^2(L \circ R(\{A, B, C\})) \\ &= (L \circ R)^2(\{B + 1, C + 2, A\}) \\ &= (L \circ R)(C + 3, A + 2, B + 1) \\ &= \{A + 3, B + 3, C + 3\}\end{aligned}$$

and this pattern can be used four times to obtain:

$$\begin{aligned}(L \circ R)^{12}(\{A, B, C\}) &= (L \circ R)^9((L \circ R)^3(\{A, B, C\}) \\ &= (L \circ R)^9(\{A + 3, B + 3, C + 3\}) \\ &= (L \circ R)^6((L \circ R)^3(\{A + 3, B + 3, C + 3\})) \\ &= (L \circ R)^6(\{A + 6, B + 6, C + 6\}) \\ &= (L \circ R)^3((L \circ R)^3(\{A + 6, B + 6, C + 6\})) \\ &= (L \circ R)^3(\{A + 9, B + 9, C + 9\}) \\ &= \{A + 12, B + 12, C + 12\} \\ &= \{A, B, C\} = i(\{A, B, C\}).\end{aligned}$$

Analogously, if $(L \circ R)^{12} = (L \circ R) \circ (L \circ R)^{11}$ is applied to a minor triad, the same triad results. The following step in the process of calculating the effect of the powers of $L \circ R$ is $R \circ (L \circ R)^{13}$. First we have:

$$R \circ (L \circ R)^{12}(\{A, B, C\}) = \{C + 2, B, A\} = R(\{A, B, C\}).$$

If we calculate $L \circ R \circ (L \circ R)^{12} = (L \circ R)^{13}$ we obtain

$$(L \circ R)^{13}(\{A, B, C\}) = \{A + 1, C + 2, B\} = L \circ R(\{A, B, C\})$$

and the pattern repeats itself.

This way it can be verified that $(L \circ R)^{12}$ behaves as the identity and we can assert that:

$$(L \circ R)^{12} = i = (L \circ R)^0.$$

Once again it can be observed that any arbitrary exponent of the function will always be contained in the set:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}.$$

This fact can be treated formally in a proposition.

3.2 Proposition. For $n, k \in \mathbb{Z}$ such that $n \equiv k \mod 12$

$$(L \circ R)^n = (L \circ R)^k$$

and

$$R \circ (L \circ R)^n = R \circ (L \circ R)^k.$$

Proof. Remembering that $(L \circ R)^{12} = (L \circ R)^0 = i$, we have

$$\begin{aligned}
(L \circ R)^n &= (L \circ R)^{12q+k} \\
&= (L \circ R)^{12q}(LR)^k \\
&= ((L \circ R)^0)^q (L \circ R)^k \\
&= i^q (LR)^k = (L \circ R)^k.
\end{aligned}$$

The second equality it follows inmmediatly from the first.♦

3.3 Definition. The set of parallel, relative and leading tone exchange functions is denoted as PLR. Specífically,

$$\text{PLR} = \{(L \circ R)^n, R \circ (L \circ R)^n | n = 0, \ldots, 11\}.$$

It seems curious that the P and L functions are not explicitly mentioned in the definition of the PLR set, but we can generate the whole set $\mathcal{M}$ without using them. However, both P and L are represented, because the reader can show that

$$P = R \circ (L \circ R)^3 \tag{4.2}$$

and

$$L = R \circ (L \circ R)^{11}. \tag{4.3}$$

These equalities hold whether applied to a major or minor triad.

Another possible issue is that the functions $R \circ L$ might introduce additional functions to the set. However, as the functions P, L and R are involutive, when L is applied first, followed by R, in a consecutive manner, the same sequence is obtained, just in reverse order. The table 4.2 shows the relations between the functions $L \circ R$ and $R \circ L$

$R \circ (RL)^0 = R = L \circ (LR)^{11}$	$L \circ (LR)^6 = L \circ (RL)^5$
$LR = (RL)^{11}$	$(LR)^7 = (RL)^5$
$R \circ (RL) = L \circ (LR)^{10}$	$L \circ (LR)^7 = L \circ (RL)^4$
$(LR)^2 = (RL)^{10}$	$(LR)^8 = (RL)^4$
$R \circ (RL)^2 = L \circ (LR)^9$	$L \circ (LR)^8 = L \circ (RL)^3$
$(LR)^3 = (RL)^9$	$(LR)^9 = (RL)^3$
$R \circ (RL)^3 = L \circ (LR)^8$	$L \circ (LR)^9 = L \circ (RL)^2$
$(LR)^4 = (RL)^8$	$(LR)^{10} = (RL)^2$
$R \circ (RL)^4 = L \circ (LR)^7$	$L \circ (LR)^{10} = L \circ (RL)$
$(LR)^5 = (RL)^7$	$(LR)^{11} = RL$
$R \circ (RL)^5 = L \circ (LR)^6$	$L \circ (LR)^{11} = L(RL)^0 = L$
$(LR)^6 = (RL)^6$	$(LR)^0 = (RL)^0$

Table 4.2: Equivalences between the LR and RL functions.

Now we can conclude that the list of all functions $(L \circ R)^n$ and $R \circ (L \circ R)^m$ is much more exhaustive than it might appear. It contains the set of compositions that include the P, L and R functions, as well as the compositions $L \circ R$ and $R \circ L$. Moreover, these 24 different functions transform any element of $\mathcal{M}$ into a distinct element of $\mathcal{M}$.

We will denote the compositions $L \circ R$ and $R \circ L$, from here on, simply as LR and RL, respectively.

3.4 Lemma. The set is closed under composition $\circ$.
Proof. It is left to the reader to show, as an exercise, that the P, L and R operations are well defined, and that all the possible compositions of P, L and R are in the PLR set.♦

3.5 Theorem. The PLR set forms a group under composition. In particular,

$$(R(LR)^n)^{-1} = R(LR)^n \quad \text{and} \quad ((LR)^n)^{-1} = (LR)^k$$

where $k = -n \bmod 12$.

Proof. The lemma 4.3 proves that every possible composition, including the inverses, are in the PLR set.

Therefore, the P, L and R functions satisfy the group properties, as associativity is a property of the functions. Although we know the existence of the inverses, it is interesting see the generators of the inverses in the PLR group.

For the lemma 4.3 proof, for all functions of the form $R \circ (LR)^n$ we have

$$R \circ (LR)^n \circ R \circ (LR)^n = i.$$

Therefore, $(R \circ (LR)^n)^{-1} = R \circ (LR)^n$.

For the functions that appear as $(LR)^n$,

$$((LR)^n)^{-1} = (LR)^{-n} = (LR)^{-n \bmod 12} = (LR)^k.$$

where $k = -n \bmod 12$.♦

Problems

3.1 Exhibit a trajectory on the *Tonnetz* such that a sequence of R and L functions transform the triad $\{5, 9, 0\}$ into itself, after passing through all the other triads of $\mathcal{M}$ in the process.

3.2 Show that the P, L and R operations are well defined. That is, if $[x]$ is a triad of pitch classes in $\mathcal{M}$ then, for every $x_1, x_2 \in [x]$ we have:

$$\begin{aligned} P(x_1) &\equiv P(x_2), \quad \text{i.e.} \quad P(\{a_1, b_1, c_1\}) \equiv P(\{a_2, b_2, c_2\}), \\ L(x_1) &\equiv L(x_2), \quad \text{i.e.} \quad L(\{a_1, b_1, c_1\}) \equiv L(\{a_2, b_2, c_2\}), \\ R(x_1) &\equiv R(x_2), \quad \text{i.e.} \quad R(\{a_1, b_1, c_1\}) \equiv R(\{a_2, b_2, c_2\}). \end{aligned}$$

4.4 The Isomorphism between PLR and TI

Now we will exhibit an explicit isomorphism between the TI and PLR groups although, as both are isomophic to the group of symmetries of the dodecagon (see the exercises 4.4 and 4.4), they are isomorphic by transitivity.

The isomorphism we are interested in between the TI and PLR groups does not send (as one might think) a function in one of the groups to a function in the other, such that both transform a triad x into the same triad y. Consider the transformation denoted by ϕ, in the table 4.3. This is, exactly, the isomorphism that will be verified in the theorem 4.

$R \longmapsto I_0$	$R \circ (LR)^4 \longmapsto I_8$	$R \circ (LR)^8 \longmapsto I_4$
$LR \longmapsto T_1$	$(LR)^5 \longmapsto T_5$	$(LR)^9 \longmapsto T_9$
$R \circ (LR) \longmapsto I_{11}$	$R \circ (LR)^5 \longmapsto I_7$	$R \circ (LR)^9 \longmapsto I_3$
$(LR)^2 \longmapsto T_2$	$(LR)^6 \longmapsto T_6$	$(LR)^{10} \longmapsto T_{10}$
$R \circ (LR)^2 \longmapsto I_{10}$	$R \circ (LR)^6 \longmapsto I_6$	$R \circ (LR)^{10} \longmapsto I_2$
$(LR)^3 \longmapsto T_3$	$(LR)^7 \longmapsto T_7$	$(LR)^{11} \longmapsto T_{11}$
$R \circ (LR)^3 \longmapsto I_9$	$R \circ (LR)^7 \longmapsto I_5$	$R \circ (LR)^{11} \longmapsto I_1$
$(LR)^4 \longmapsto T_4$	$(LR)^8 \longmapsto T_8$	$(LR)^0 \longmapsto T_0$

Table 4.3: The isomorphism $\phi : \mathrm{PLR} \mapsto \mathrm{TI}$.

The isomorphism is constructed in the following way. First the generators and the identities of the TI and PLR groups are exhibited. For example, the generators of TI are T_1 and I_0, with the relations

$$(T_1)^{12} = i \quad \text{and} \quad (I_0)^2 = i.$$

The generators of the the PLR group are LR and R, with the relations

$$(LR)^{12} = i \quad \text{and} \quad R^2 = i.$$

This suggests the following: take T_1 to LR and I_0 to R. The identity T_0 is taken to the identity $(LR)^0$. The other functions reveal a pattern between the powers of RL and the subindices of the functions T and I.

Theorem 4 *There exists a bijective homorphism* $\phi : \mathrm{PLR} \to \mathrm{TI}$ *such that*

$$\phi((LR)^x) = T_x, \quad \phi(R \circ (LR)^x) = I_n,$$

where $n = -x \bmod 12$.

Proof. By using the table 4.3 we can conclude that the function is bijective. Now we will carry out a pointwise evaluation of all the possible combinations of

the generators of the PLR group. We will show that for every $g, h \in \mathcal{PLR}$ and all $x \in \mathcal{M}$,

$$\phi(g \circ h)(x) = \phi(g)(\phi(h)(x)).$$

Let $x = \{a, b, c\} \in \mathcal{M}$, and let $g = LR$ and $h = R$. Then the left side of the equation is:

$$\begin{aligned}
\phi(g \circ h)(\{a,b,c\}) &= \phi((LR) \circ R)(\{a,b,c\}) \\
&= \phi(L \circ R \circ R)(\{a,b,c\}) \\
&= \phi(L)(\{a,b,c\}) \qquad \text{(because } R^2 = i\text{)} \\
&= \phi(R \circ (LR)^{11})(\{a,b,c\}) \qquad \text{(using 4.3)} \\
&= I_1(\{a,b,c\}) \qquad \text{(by 4.2)} \\
&= \{-a+1, -b+1, -c+1\},
\end{aligned}$$

whereas the right side is:

$$\begin{aligned}
\phi(g)(\phi(h)(\{a,b,c\})) &= \phi(LR)(\phi(R)(\{a,b,c\})) \\
&= T_1(I_0(\{a,b,c\})) \qquad \text{(by 4.2)} \\
&= I_{1+0}(\{a,b,c\}) \qquad \text{(by lemma 4.2)} \\
&= I_1(\{a,b,c\}) \\
&= \{-a+1, -b+1, -c+1\}.
\end{aligned} \tag{4.4}$$

Now let $g = R$ and $h = LR$; then the left side of the equation is:

$$\begin{aligned}
\phi(g \circ h)(\{a,b,c\}) &= \phi(R \circ LR)(\{a,b,c\}) \\
&= I_{11}(\{a,b,c\}) \qquad \text{(by 4.2)} \\
&= \{-a+11, -b+11, -c+11\} \quad \text{(by 4.2)}
\end{aligned}$$

whereas the right side is:

$$\begin{aligned}
\phi(g)\,(\phi(h)(\{a,b,c\})) &= \phi(R)\,(\phi(LR)(\{a,b,c\})) \\
&= I_0\,(T_1\,(\{a,b,c\})) \\
&= I_{0-1}(\{a,b,c\}) \qquad \text{(by 4.2)} \\
&= I_{-1}(\{a,b,c\}) \\
&= I_{11}(\{a,b,c\}) \\
&= \{-a+11, -b+11, -c+11\}.
\end{aligned}$$

Now let $g = LR$ and $h = LR$; then the left side of the equation is:

$$\begin{aligned}
\phi(g \circ h)(\{a,b,c\}) &= \phi((LR) \circ (LR))(\{a,b,c\}) \\
&= \phi((LR)^2)(\{a,b,c\}) \\
&= T_2(\{a,b,c\}) \qquad \text{(by 4.2)} \\
&= \{a+2, b+2, c+2\}
\end{aligned}$$

wheras the right side is:

$$\begin{aligned}
\phi(g)(\phi(h)(\{a,b,c\})) &= \phi(LR)(\phi(LR)(\{a,b,c\})) \\
&= T_1(T_1(\{a,b,c\})) \qquad \text{(by 4.2)} \\
&= T_{1+1}(\{a,b,c\}) \qquad \text{(by lemma 4.2)} \\
&= T_2(\{a,b,c\}) \\
&= \{a+2, b+2, c+2\}.
\end{aligned}$$

Finaly let $g = R$ and $h = L$; then the left side of the equation is:

$$\begin{aligned}
\phi(g \circ h)(\{a,b,c\}) &= \phi(R \circ R)(\{a,b,c\}) \\
&= \phi(i)(\{a,b,c\}) \qquad \text{(because } R^2 = i\text{)} \\
&= \phi((LR)^0)(\{a,b,c\}) \qquad \text{(by 4.2)} \\
&= T_0(\{a,b,c\}) \qquad \text{(by 4.2)} \\
&= \{a,b,c\}
\end{aligned}$$

wheras the right side is:

$$\begin{aligned}
\phi(g)(\phi(h)(\{a,b,c\})) &= \phi(R)(\phi(R)(\{a,b,c\})) \\
&= I_0(I_0(\{a,b,c\})) \qquad \text{(by 4.2)} \\
&= T_{0+0}(\{a,b,c\}) \qquad \text{(by lemma 4.2)} \\
&= T_0(\{a,b,c\}) \\
&= \{a,b,c\}.
\end{aligned}$$

Hence $\phi(g \circ h)(x) = \phi(g)(\phi(h)(x))$ for every $g, h \in \mathcal{PLR}$ and for every $x \in \mathcal{M}$.

This shows that ϕ is an isomorphism.♦

Problems

4.1 Given the lemma:

Let $x \in \{(LR)^n, R \circ (LR)^n\}$, and $y = a \circ x$, where $a \in \{P, L, R\}$. Then $y = a \circ x \in$ PLR.

Show by induction that all possible compositions of P, L and R are in the PLR set. (Hint: express P as $R \circ (LR)^3$, and L as $R \circ (LR)^{11}$ and, together with R, it can be verified for $n = 1$, that $x \in$ PLR in the three cases. Then suppose that x has length k, at the most).

4.2 Show that the TI group is isomorphic to the dihedral group of order $n = 12$, that is, that

$$(T_1)^n = i, \quad (I_0)^2 = i, \tag{4.5}$$

$$I_0 \circ T_1 = T_1^{n-1} \circ I_0, \tag{4.6}$$

$$\text{TI} = \{i, T_1, T_2, \ldots, T_{n-1}, I_0, I_1, \ldots, I_{n-1}\}. \tag{4.7}$$

4.3 Show that the PLR group is isomorphic to the dihedral group of order $n = 12$, that is,

$$(LR)^n = i, \quad R^2 = i, \tag{4.8}$$

$$R \circ (LR) = (LR)^{n-1} \circ R, \tag{4.9}$$

$$\text{PLR} = \{i, (LR), (LR)^2, \ldots, (LR)^{11}, R, R \circ (LR), \ldots, R \circ (LR)^{11}\}. \tag{4.10}$$

4.5 The Duality of the TI and PLR Groups

We know from chapter 3, definition 2.3, what it means for a group G to act on a set X.

5.1 Lemma. The set $\mathcal{M}$ is a TI-set. In other words, the TI group acts on $\mathcal{M}$.
Proof. We define the action of $T_m, I_n \in \mathrm{TI}$ on $x \in \mathcal{M}$ through the evaluation, ie

$$\phi(T_m, x) = T_m * x = T_m(x) \quad y \quad \phi(I_n, x) = I_n * x = I_n(x).$$

Since for any functions $f, g \in \mathrm{TI}$ we have:

$$(f \circ g) * x = (f \circ g)(x) = f(g(x)) = f * (g * x)$$

as well as $i * x = T_0 * x = T_0(x) = x = i(x)$, it follows that IT acts on $\mathcal{M}$.♦

5.2 Lemma. The set $\mathcal{M}$ is a PLR-set. In other words, the PLR group acts on $\mathcal{M}$.

Proof. Defining the action through the evaluation, the proof is essentially the same as the previous lemma.♦

Recall, also from chapter 3, the definition of the orbit of X under G.

5.3 Lemma. For every $x \in \mathcal{M}$, the orbit TIx of x is $\mathcal{M}$.

Proof. As illustrated in figures 4.2 and 4.3, where all the functions are applied to a single triad, the entire set $\mathcal{M}$ is generated. Even thought the table shows only the functions applied to the C major chord, it can be easily verified that the functions act in the same manner on any major or minor triad. So the orbit of the TI group is:

$$\mathrm{TI}x = \{f * x \mid f \in \mathrm{TI}\} = \mathcal{M}.♦$$

We leave it as an exercise to show that, for every $x \in \mathcal{M}$, the orbit PLRx is also $\mathcal{M}$. Recall the definition of isotropic subgroup (or stabilizer) from chapter 3, as well as the orbit-stabilizer theorem (theorem 2.8).

5.4 Lemma. Let $x \in \mathcal{M}$. Then the stabilizer of x under PLR is

$$\mathrm{PLR}_x = \{f \in \mathrm{PLR} | f * x = x\} = i = (LR)^0$$

Proof. We use Theorem 3.2.8. to see that

$$|\mathrm{PLR}_x| = \frac{|\mathrm{PLR}|}{|\mathrm{PLR}x|}.$$

But $|\mathrm{PLR}| = 24$ as there are 24 functions in PLR and $|\mathrm{PLR}x| = 24$ since $\mathrm{PLR}x = \mathcal{M}$. This gives us

$$|\mathrm{PLR}_x| = \frac{24}{24} = 1.$$

Naturally, $i * x = x$, so PLR_$i \in \{x\}$ and is the only member of the set. Therefore, the stabilizer is trivial.♦

We leave it as an exercise to show that if $x \in \mathcal{M}$, then the stabilizer of x under TI is

$$\mathrm{TI}_x = \{f \in \mathrm{TI} \mid f * x = x\} = i = T_0.$$

5.5 Definition. An action of a group G on a set X is **free** if for any $g, h \in G$ and $x \in X$ $g * x \neq f * x$. This condition is equivalent to $g * x = x$ if and only if g is the identity element of G.

5.6 Corollary. The TI and PLR groups act freely on $\mathcal{M}$.

Proof. We've already established that for all $x \in \mathcal{M}$ $\mathrm{TI}_x\{x\} = i$ and $\mathrm{PLR}_x = i$ are the stabilizers. Therefore, the actions of TI and PLR groups on $\mathcal{M}$ meet the definition of free action.♦

5.7 Definition. An action of a group G on a set X is **transitive** if for any $x, y \in X$ there exists $g \in G$ such that $g * x = y$.

5.8 Definition. An action of a group G on a set X is **regular** if it is transitive and free (also called "simply transitive").

Now we will show that the TI and PLR groups act regularly on $\mathcal{M}$.

5.9 Proposition. The actions of the TI and PLR groups on $\mathcal{M}$ are regular, that is, they are transitive and free.

Proof. We can deduce the regularity from figures 4.2 and 4.3 and the equation(4.1). First, we see that all functions acting on any x produce the entire set $\mathcal{M}$. In other words, for every y in $\mathcal{M}$ always exists a function g such that $g(x) = y$. Moreover, this happens without a repeat occurrence of triads, which means that only one function transforms any triad in any other triad. Therefore, g is unique.

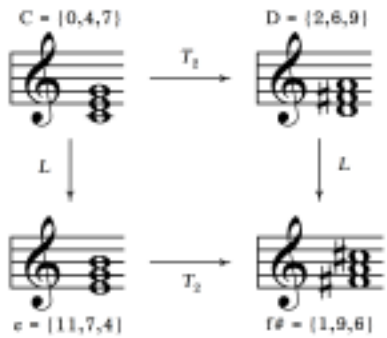


Figure 4.5: Musical illustration of $T_2 \circ L(\mathrm{C}) = L \circ T_2(\mathrm{C})$.

Therefore, the findings can be used to infer the regularity. Since, for all x, it holds that $\mathrm{TI}x = M$, then given $z, y \in \mathcal{M}$ there are $f, g \in \mathrm{TI}$ such that $f * x = z$ and $g * x = y$. This means that

$$f^{-1}(z) = f^{-1} * (f * x) = (f^{-1} \circ f) * x = i * x = x$$

and

$$(g \circ f^{-1}) * z = g * (f^{-1}(z)) = g * x = y$$

so that $g \circ f^{-1}$ is an element of the group that sends z to y by means of this action. Finally, if there are $g_1, g_2 \in \mathrm{TI}$ such that $g_2^{-1} \circ g_1 = i$ then $g_2 = g_1$. But the stabilizer of x is trivial, so $g_2 = g_1$and therefore $g_2 = g_1$. This demonstrates that TI is regular. The PLR case is analogous.♦

Recall the definition of the centralizer of a group from chapter 3. The concept of centralizer is based on commutativity and, because of this, we will examine the commutativity between elements of TI and PLR.

5.10 Lemma. All the elements of the PLR and TI groups commute.

We should show the commutativity of the generators of each group, that is,

$$T_1 \circ (LR) = (LR) \circ T_1, \tag{4.11}$$
$$T_1 \circ R = R \circ T_1, \tag{4.12}$$
$$I_0 \circ (LR) = (LR) \circ I_0, \tag{4.13}$$
$$I_0 \circ R = R \circ I_0. \tag{4.14}$$

It is left as an exercise complete the proof of this lemma.♦

The figures 4.5 y 4.6 provide musical examples of commutativity with the use of commutative diagrams.

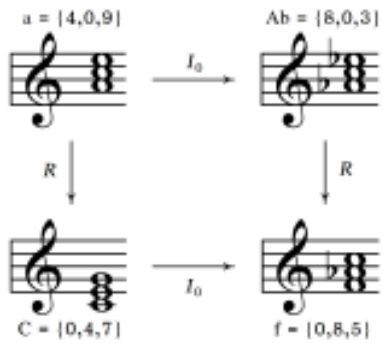


Figure 4.6: Musical illustration of $I_0 \circ R(\mathrm{a}) = R \circ I_0(\mathrm{a})$.

Given that the commutative relations are valid when any element of $\mathcal{M}$ is evaluated, for every f in TI and for every g in PLR, the commutative diagram is always valid.

$$\begin{array}{ccc} \mathcal{M} & \xrightarrow{f} & \mathcal{M} \\ g \downarrow & & \downarrow g \\ \mathcal{M} & \xrightarrow[f]{} & \mathcal{M} \end{array}$$

For example,

$$\begin{array}{ccc} \mathcal{M} & \xrightarrow{T_n} & \mathcal{M} \\ L \downarrow & & \downarrow L \\ \mathcal{M} & \xrightarrow[T_n]{} & \mathcal{M} \end{array}$$

means that $L \circ T_n = T_n \circ L$.

The commutative nature of the TI and PLR groups brings us to the last notion we need for duality.

As the TI and PLR groups are transformations of $\mathcal{M}$ into itself, they are permutation groups and, consequently, subgroups of the symmetric group of $\mathcal{M}$ (i.e. $\mathrm{Sym}(\mathcal{M})$, which is the group of all bijections of $\mathcal{M}$ into itself under function composition). Recall the definition of centralizer from chapter 3. We will examine the centralizers of each group (TI and PLR) as subgroups of the big group $\mathrm{Sym}(\mathcal{M})$.

5.11 Lemma. It holds that:

$$C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI}) = \mathrm{PLR} \quad \text{y} \quad C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{PLR}) = \mathrm{TI}.$$

Proof. First we consider the centralizer of the TI group,

$$C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI}) = \{g \in \mathrm{Sym}(\mathcal{M}) | fg = gf, \forall f \in \mathrm{TI}\}.$$

By lemma 4.5 we have that for every $g \in \mathrm{PLR}$ and $f \in \mathrm{TI}$, $f \circ g = g \circ f$. Then the PLR group is contained in $C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})$. We should verify that there do not exist other functions that do no belong to the PLR group in $C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})$. We begin by looking at the stabilizer of x in $C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})$. Suppose that $h \in C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})$ and that it fixes $x \in \mathcal{M}$. Let $g \in \mathrm{TI}$. Then:

$$\begin{aligned} h(x) &= x, \\ g(h(x)) &= g(x), \\ h(g(x)) &= g(x), \end{aligned}$$

where the last equality follows from the fact that h is in the centralizer. By proposition 4.5 we know that TI acts regularly, hence for every $y \in \mathcal{M}$ there exists a g such that $y = g(x)$. This shows that for every $x, y \in \mathcal{M}$

$$h(y) = h(g(x)) = g(x) = y.$$

In particular, $h(y) = y$ for every $y \in \mathcal{M}$. However, the only element in $C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})$ that fixes all elements in $C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})$ is i, hence h is the identity element. Thus, $C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})_x = i$.

By applying theorem 2.8 from Chapter 3 (the orbit-stabilizer theorem) to $C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})_x$ we obtain:

$$\begin{aligned} |C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})x| &= \frac{|C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})|}{|C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})_x|} \\ &= |C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})| \leq |\mathcal{M}| = 24, \end{aligned}$$

given that the orbit of x under $C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})$ is contained in $\mathcal{M}$. On the other hand, $\mathrm{PLR} \subseteq C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})$, giving us:

$$|\mathrm{PLR}| \leq |C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})|.$$

Combining these inequalities, we see that $|C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{TI})| = 24$ and the centralizer of TI must be the group PLR. We still must show that the centralizer of the PLR goupr is the TI group. However, we only have to interchange the roles of the TI group with the PLR group from the beginning of the proof to show that $C_{\mathrm{Sym}(\mathcal{M})}(\mathrm{PLR}) = \mathrm{TI}$.

5.12 Definition. Let H and K be subgroups of the symmetric group $\mathrm{Sym}(X)$ (i.e. H and K are permutation groups on the set X). Then H and K are said to be **dual** if each one acts regularly on X and one is the centralizer of the other in $\mathrm{Sym}(X)$.

The multiple lemmas and theorems that have been seen are used to deduce the duality of the TI and PLR groups.

5.13 Theorem. The TI and PLR groups are dual.

Proof. The statement follows from Proposition 4.5 and Lemma 4.5.

Problems

5.1 Show that for all $x \in \mathcal{M}$, the orbit of x is $PLR_x = \mathcal{M}$.

5.2 Show that if $x \in \mathcal{M}$, and $\mathcal{M}$ is a set-T/I, then the stabilizer of x is

$$T/I_x = \{f \in T/I \mid fx = x\} = T_0$$

5.3 Show the lemma 5.10. All the elements of the PLR and TI groups commute.

4.6 Solutions to the Problems of Chapter 4

2.1 Let $x_1, x_2 \in [x] \in \mathcal{M}$, where $x_1 = \langle a_1, b_1, c_1\rangle$ and $x_2 = \langle a_2, b_2, c_2\rangle$. Then x_1 and x_2 are elements in the class of triads $[x] = \langle [a], [b], [c]\rangle$. We see that a_1, $a_2 \in [a] \in \mathbb{Z}_{12}$, b_1, $b_2 \in [b] \in \mathbb{Z}_{12}$, and c_1, $c_2 \in [c] \in \mathbb{Z}_{12}$, then: $T_n(\langle a_1, b_1, c_1\rangle) = \langle a_1 + n, b_1 + n, c_1 + n\rangle$ and, $T_n(\langle a_2, b_2, c_2\rangle) = \langle a_2 + n, b_2 + n, c_2 + n\rangle$ as, $a_1 \in [a]$, then $(a_1 + n) \in [a + n]$ and $a_2 \in [a]$, then $(a_2 + n) \in [a + n]$.

Similarly $(b_1 + n), (b_2 + n) \in [b + n]$ and $(c_1 + n), (c_2 + n) \in [c + n]$ which gives us:

$$\begin{aligned} T_n(x_1) &= T_n(\langle a_1, b_1, c_1\rangle) \\ &= \langle a_1 + n, b_1 + n, c_1 + n\rangle \\ &\equiv \langle a_2 + n, b_2 + n, c_2 + n\rangle \\ &\equiv T_n(\langle a_2, b_2, c_2\rangle) \\ &\equiv T_n(x_2). \end{aligned}$$

Hence T_n is well defined.

2.2 iii.

$$\begin{aligned} I_m \circ T_n &= I_m(T_n(\langle a, b, c\rangle)) \\ &= I_m(\langle a + n, b + n, c + n\rangle) \\ &= \langle -a - n + m, -b - n + m, -c - n + m\rangle \\ &= \langle -a + (m - n), -b + (m - n), -c + (m - n)\rangle \\ &= I_{m-n \bmod 12} \end{aligned}$$

iv.

$$\begin{aligned} I_m \circ I_n &= I_m(I_n(\langle a, b, c\rangle)) \\ &= I_m(\langle -a + n, -b + n, -c + n\rangle) \\ &= \langle a - n + m, b - n + m, c - n + m\rangle \\ &= \langle a + (m - n), b + (m - n), c + (m - n)\rangle \\ &= T_{m-n \bmod 12} \end{aligned}$$

3.1 Let $x_1, x_2 \in [x] \in M$, where $x_1 = \langle a_1, b_1, c_1\rangle$and $x_2 = \langle a_2, b_2, c_2\rangle$. Then x_1 and x_2 are elements in the class of triads $[x] = \langle [a], [b], [c]\rangle$. We see that if $a_1, a_2 \in [a] \in \mathbb{Z}_{12}$, $b_1, b_2 \in [b] \in \mathbb{Z}_{12}$, and $c_1, c_2 \in [c] \in \mathbb{Z}_{12}$, then: $I_n(\langle a_1, b_1, c_1\rangle) = \langle -a_1 + n, -b_1 + n, -c_1 + n\rangle$and $I_n(\langle a_2, b_2, c_2\rangle) = \langle -a_2 + n, -b_2 + n, -c_2 + n\rangle$.

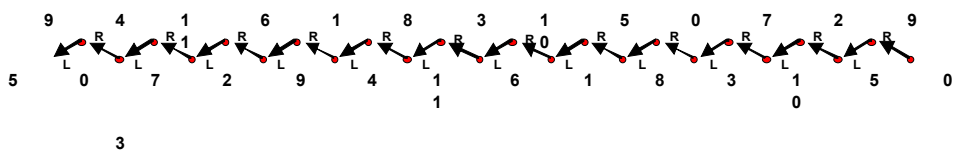
As, $-a_1 \in [a]$, then $(-a_1 + n) \in [a + n]$ and $-a_2 \in [a]$, hence $(-a_2 + n) \in [a+n]$. Similarly, $(-b_1+n), (-b_2+n) \in [b+n]$ and $(-c_1+n)$, $(-c_2+n) \in [c+n]$

which gives us

$$\begin{aligned} I_n(x_1) &= I_n(\langle a_1, b_1, c_1\rangle) \\ &= \langle -a_1+n, -b_1+n, -c_1+n\rangle \\ &\equiv \langle -a_2+n, -b_2+n, -c_2+n\rangle \\ &\equiv I_n(\langle a_2, b_2, c_2\rangle) \\ &\equiv I_n(x_2). \end{aligned}$$

Thus I_n is well defined.♦

3.2



3.3 Let $x_1, x_2 \in [x] \in \mathcal{M}$, where $x_1 = \langle a_1, b_1, c_1\rangle$and $x_2 = \langle a_2, b_2, c_2\rangle$. Then x_1 and x_2 are elements in of the class of triads $[x] = \langle [a], [b], [c]\rangle$and $a_1, a_2 \in [a] \in \mathbb{Z}_{12}$, $b_1, b_2 \in [b] \in Z_{12}$, $c_1, c_2 \in [c] \in \mathbb{Z}_{12}$.
i) $P(\langle a_1, b_1, c_1\rangle) = \langle C_1, B_1+1, A_1\rangle$and $P(\langle a_2, b_2, c_2\rangle) = \langle C_2, B_2+1, A_2\rangle$. As $A_1 \in [A]$, then $(A_1+n) \in [A+n]$ and $A_2 \in [A]$. Thus $(A_2+n) \in [A+n]$. Analogously, $(B_1+n), (B_2+n) \in [B+n]$ and $(C_1+n), (C_2+n) \in [C+n]$. Then:

$$\begin{aligned} P(x_1) &= P(\langle a_1, b_1, c_1\rangle) \\ &= \langle C_1, B_1+_1, A_1\rangle \\ &\equiv \langle C_2, B_2+1, A_2\rangle \\ &\equiv P(\langle a_2, b_2, c_2\rangle) \\ &\equiv P(x_2). \end{aligned}$$

Therefore, P is well defined.

3.4 $L(\langle a_1, b_1, c_1\rangle) = \langle A_1+1, C_1, B_1\rangle$ and $L(\langle a_2, b_2, c_2\rangle) = \langle A_2+1, C_2, B_2\rangle$. As $A_1 \in [A]$, then $(A_1+n) \in [A+n]$ and $A_2 \in [A]$. Thus $(A_2+n) \in [A+n]$. Similarly, $(B_1+n), (B_2+n) \in [B+n]$ and $(C_1+n), (C_2+n) \in [C+n]$ then:

$$\begin{aligned} L(x_1) &= L(\langle a_1, b_1, c_1\rangle) \\ &= \langle A_1+1, C_1, B_1\rangle \\ &\equiv \langle A_2+1, C_2, B_2\rangle \\ &\equiv L(\langle a_2, b_2, c_2\rangle) \\ &\equiv L(x_2) \end{aligned}$$

Hence L is well defined.

3.5 $R(\langle a_1, b_1, c_1\rangle) = \langle B_1, A_1, C_1 - 2\rangle$ and $R(\langle a_2, b_2, c_2\rangle) = \langle B_2, A_2, C_2 - 2\rangle$. As $A_1 \in [A]$, then $(A_1 + n) \in [A + n]$ and $A_2 \in [A]$. Hence $(A_2 + n) \in [A + n]$. Similarly $(B_1 + n)$, $(B_2 + n)$ $[B + n]$ and $(C_1 + n)$, $(C_2 + n)[C + n]$. Then

$$\begin{aligned} R(x_1) &= R(\langle a_1, b_1, c_1\rangle) \\ &= \langle B_1, A_1, C_1 - 2\rangle \\ &\equiv \langle B_2, A_2, C_2 - 2\rangle \\ &\equiv R(\langle a_2, b_2, c_2\rangle) \\ &\equiv R(x_2). \end{aligned}$$

Thus R is well defined. ♦

4.1 Let x be any composition of P, L and R functions. We say that x has length of, at the most n, if there exists a decomposition of x as the composition of, at the most, n functions of P, L and R. We will prove by induction that any composition of P, L and R functions is in the PLR set.

The *base case*: verify that, for any x of length $n = 1$, x is in the PLR set.

Case 1: If $x = P = R(LR)^3$, then $x \in$ PLR.

Case 2: If $x = L = R(LR)^{11}$, then $x \in$ PLR.

Case 3: If $x = R$, then $x \in$ PLR.

We assume that, if x has at most length k for every $k \geq 1$, then $x \in$ PLR.

Induction step: Verify that, for any x of length $k + 1$, $x \in$ PLR.

Let y be of length $k + 1$; then, by definition, y is a composition of $k + 1$ P, L and R functions. Let "a" be the first function of the composition; then $a \in \{P, L, R\}$, and $y = a * x$. Now, the length of x is $\leq k$ and we know that $x \in$ PLR. Hence, there exists an n such that $x = (LR)^n$ or $x = R(LR)^n$.

Now, applying the lema, it can be seen that $a * x = y \in$ PLR.

4.2 i.

$$\begin{aligned} (T_1)^n &= (T_1)^{12} && \text{as } n = 12 \\ &= \underbrace{(T_1)(T_1)\cdots(T_1)(T_1)}_{12 \text{ times}} \\ &= T_{\underbrace{1+1+\ldots+1+1}_{12 \text{ times}}} \\ &= T_{12} \\ &= T_0 \\ &= i \end{aligned}$$

and $(I_0)^2 = (I_0)(I_0) = T_{0+0} = T_0 = i$.

ii.

$$\begin{aligned}(I_0)(T_1) &= I_{0-1} = I_{-1} \\ &= I_{11} && \text{as } 11 = -1 \bmod 12 \\ &= I_{12-1+0} \\ &= (T_{12-1})(I_0) \\ &= (T_1)^{12-1}(I_0) \\ &= (T_1)^{n-1}(I_0)\end{aligned}$$

iii. The elements of the T/I group are

$$\begin{aligned}& \{i, T_1, (T)^2, \ldots, (T_1)^{11}, I_0, (I_0)(T_1), \ldots, (I_0)(T_1)^{11}\} \\ = \; & \{i, T_1, T_2, \ldots, T_{11}, I_0, I_{0-1}, \ldots, I_{0-11}\} && \begin{array}{l}\text{as } (T_1)^m = T_m, \\ \text{and } (I_n)(T_m) = I_{n-m}\end{array} \\ = \; & \{i, T_1, T_2, \ldots, T_{11}, I_0, I_1, \ldots, I_{11}\} && \text{as } I_k = I_{-n \bmod 12}\end{aligned}$$

Hence, the T/I group is isomorphic to the group of symmetries of the dodecagon. ♦

4.3 i.

$$\begin{aligned}(LR)^n &= (LR)^{12} && \text{as } n = 12 \\ &= (LR)^0 && \text{as } 12 = 0 \bmod 12 \\ &= i\end{aligned}$$

and $(R)^2 = i$ as R is involutive.

ii.

$$\begin{aligned}R(LR) &= L(LR)^{10} && \text{by table 2.5} \\ &= L(LR)^{10}(RR) && \text{as } (R)^2 = i \\ &= (L(LR)^{10}R)R \\ &= (LR)^{11}R \\ &= (LR)^{12-1}R \\ &= (LR)^{n-1}R\end{aligned}$$

iii. The elements of the PLR group are

$$\{i, (LR), (LR)^2, \ldots, (LR)^{n-1}, R, R(LR), \ldots, R(LR)^{n-1}\}.$$

Hence, the PLR group is isomorphic to the dihedral group of the dodecagon. ♦

5.1 As illustrated in table 2.3, all the functions, when applied to one triad, generate the complete set $\mathcal{M}$. The orbit of x in the PLR group is

$$\text{PLR}x = \{fx \mid f \in \text{PLR}\} = \mathcal{M}$$

Once more, there is only one orbit for every $x \in \mathcal{M}$, given that the complete set $\mathcal{M}$ results from the application of all the functions in the PLR group to any triad. ♦

5.2 Proposition 2.8 from Chapter 3 is used to see that: $|T/I_x| = |T/I| \diagup |T/Ix|$ where $|T/I| = 24$ as there are 24 functions in T/I and $|T/Ix| = 24$ as $T/Ix = \mathcal{M}$ This gives us: $|T/I_x| = 24/24 = 1$.Then $T/I_x = \{T_0\} = \{i\}$ as $T_0(x) = x$ Therefore, the stabilizer is trivial. ♦

5.3 i.

$$\begin{aligned} T_1 \circ (LR)(\langle A, B, C\rangle &= T_1(L(\langle b, a, c+2\rangle)) \\ &= T_1 \langle B-1, C+2, A\rangle \\ &= \langle B, C+3, A+1\rangle \\ (LR) \circ T_1(\langle A, B, C\rangle &= (LR)(\langle A+1, B+1, C+1\rangle) \\ &= L(\langle b+1, a+1, c+3\rangle \\ &= \langle B-1, C+3, A+1\rangle \end{aligned}$$

ii.

$$\begin{aligned} T_1 \circ (R)(\langle A, B, C\rangle &= T_1(\langle b, a, c+2\rangle) \\ &= \langle b+1, a+1, c+3\rangle \\ (R) \circ T_1(\langle A, B, C\rangle &= R(\langle A+1, B+1, C+1\rangle) \\ &= \langle b+1, a+1, c+3\rangle \end{aligned}$$

iii.

$$\begin{aligned} I_0 \circ (LR)(\langle A, B, C\rangle &= I_0(\langle B-1, C+2, A\rangle) \\ &= \langle 1-b, 10-c, -a\rangle \\ (LR) \circ I_0(\langle A, B, C\rangle &= (LR)(\langle -a, -b, -c\rangle) \\ &= L(\langle -B, -A, -C-2\rangle) \\ &= \langle 1-b, -c+10, -a\rangle \end{aligned}$$

iv.

$$\begin{aligned} I_0 \circ (R)(\langle A, B, C\rangle &= I_0(\langle b, a, c+2\rangle) \\ &= \langle -B, -A, -C-2\rangle \\ (R) \circ I_0(\langle A, B, C\rangle &= R(\langle -a, -b, -c\rangle) \\ &= \langle -B, -A, -C-2\rangle \end{aligned}$$

Thus, for every $f \in T/I$, and for every $g \in$ PLR, $fg = gf$. ♦

List of Symbols

Index

Bibliografy and References

[A] Armstrong, M. A. *Groups and Symmetry.* UTM. Springer. 1988.

[B] Bourbaki, N. *Algebra I.* Addison Wesley. 1973.

[B-M] Birkhoff, G. and MacLane, S. *Algebra.* Macmillan. 1968.

[C] Cohn, R. *Neo-Riemannian operations, parsimonious trichords and their Tonnetz representations.* Journal of Music Theory, 41 (1997), 1-66.

[CFS] Crans, A., Fiore, T. and Satyendra, R. *Musical Actions of Dihedral Groups.*
`http://arxiv.org/PS_cache/arxiv/pdf/0711/0711.1873v2.pdf`, 2008.

[DP] Du Plessis, J. *Transformation Groups and Duality in the Analysis of Musical Structure.* Masters thesis, Georgia State University (EU), 2008.

[F] Fraleigh, J.B. *Abstract Algebra.* Addison Wesley. 2003.

Hu, S-T. *Elements of Modern Algebra.* Holden-Day. 1965.

[H] Hungerford, T.W. *Algebra.* Springer. 1980.

Lang, S. *Algebra.* Addison Wesley. 1965.

[Ll1] Lluis-Puebla, E. *Álgebra Homológica, Cohomología de Grupos y K-Teoría Algebraica Clásica.* Segunda Edición. Publicaciones Electrónicas. Sociedad Matemática Mexicana. Serie: Textos. Vol. 5. 2005.

[Ll2] Lluis-Puebla, E. *Álgebra Lineal, Álgebra Multilineal, y K-Teoría Algebraica Clásica.* Segunda Edición. Publicaciones Electrónicas. Sociedad Matemática Mexicana. Serie: Textos. Vol. 9. 2008.

[M] Mazzola, G. *The Topos of Music.* Birkhäuser-Verlag. 2002.

Robinson, J.S. *A Course in the Theory of Groups.* Springer. 1980.

Rotman, J.J. *The Theory of groups.* Allyn and Bacon. 1976.

The Authors

Flor Aceff-Sánchez

Flor Aceff-Sánchez obtained the Professor of Primary Education degree at the Escuela Nacional de Maestros in 1982. In 1989 obtained her undergraduate degree in Mathematics, in 1990 graduated as Master in Mathematics and obtained a Ph.D. in Mathematics in 1995 at the Faculty of Sciences of the Universidad Nacional Autónoma de México. She is currently Full Time Professor at the Faculty of Sciences of the Universidad Nacional Autónoma de México both in Professional and Posgraduate Studies. She was National Researcher (1995-1998).

She is member of various scientific associations such as: the Mexican Institute of Sciences and Humanities, the Royal Spanish Mathematical Society, the American Mathematical Society, the Mexican Society of Geography and Statistics, the Mathematical Society of Mexico and is president of the Council on Accreditation of Educational Programs in Mathematics.

Octavio A. Agustín-Aquino

Octavio Alberto Agustín Aquino studied his undergraduate degree in Applied Mathematics at the Universidad Tecnológica de la Mixteca in Huajuapan de León, Oaxaca, and the Masters in Mathematical Sciences at the Universidad Nacional Autónoma de México. He obtained his Ph.D. in 2011 at the Universidad Nacional Autónoma de México under the joint direction of Emilio Lluis-Puebla, Guerino Mazzola and Rodolfo San Agustín Chi. His research is aimed at extending the Mathematical Theory of Counterpoint developed by Guerino Mazzola.

Janine du Plessis

Janine du Plessis is originally from South Africa and did her undergraduate and Masters in Mathematics at Georgia State University, where she wrote her thesis under the direction of Mariana Montiel. She also studied Music at the same University. She presently teaches Mathematics at Georgia Perimeter College and Chattahoochee Technical College.

Emilio Lluis-Puebla

Emilio Lluis-Puebla completed his Professional and Master Studies in Mathematics in Mexico. In 1980 he obtained his Ph.D. in Mathematics in Canada. He is professor at the National Autonomous University of Mexico in their Professional and Graduate divisions for over thirty years. He has formed several professors and researchers who work in Mexico and abroad. His mathematical work has been established in his research articles published on Algebraic K-theory and Cohomology of Groups in the most prestigious national and international journals. He has been Visiting Professor in Canada.

He received several academic awards, among others, Gabino Barreda Medal for the highest average in the Masters, National Researcher (1984-1990) and Endowed Chair of Excellence Conacyt (1992-1993). He is the author of several books on Algebraic K-Theory, Homological Algebra, Linear Algebra and Mathematical Music Theory published worldwide by Addison Wesley, Springer Verlag, Birkhäuser, AMS, SMM, among others.

He is a member of several scientific associations such as the Royal Spanish Mathematical Society and the American Mathematical Society. He is president of the Academy of Sciences of the Mexican Institute of Sciences and Humanities, president of the Academy of Mathematics of the Mexican Society of Geography and Statistics and president 2000-2002 of the Mathematical Society of Mexico.

Mariana Montiel

Mariana Montiel did her undergraduate and Masters in Mathematics at the National Autonomous University of Mexico. In 2005 she obtained her Ph.D. in Mathematics in the United States. She is professor at Georgia State University, in the Department of Mathematics and Statistics, since 2006. Her research is focused on Mathematical Music Theory and Mathematics as a semiotic system, with emphasis in the aspect of language.

She has directed theses and research projects in Mexico and the United States in the area of Mathematical Music Theory. She has published articles and collaborated in books about the application of Category Theory to Mathematical Music Theory.

She has received several scholarships and grants from foundations and institutes in Mexico and the United States, such as the National Council of Science and Technology, The UNAM Foundation, the University of New Hampshire and the Research Foundation of Georgia State University. She collaborates internationally and does translations of articles on Mathematics and Mathematics Education. Some of her publications are found in Birkhäuser and Springer Verlag.

The success of Group Theory is impressive and extraordinary. It is, perhaps, the most powerful and influential branch of all Mathematics. Its influence is strongly felt in almost all scientific and artistic disciplines (in Music, in particular) and in Mathematics itself. Group Theory extracts the essential characteristics of diverse situations in which some type of *symmetry* or *transformation* appears. The concept of structure, and the concepts related to structure such as isomorphism, play a decisive role in modern Mathematics.

In this text, a modern presentation is chosen, where the language of commutative diagrams and universal properties, so necessary in Modern Mathematics, in Physics and Computer Science, among other disciplines, is introduced.

This text consists of four chapters. Each section contains a series of problems that can be solved with creativity by using the content that is presented there; these problems form a fundamental part of the text. They also are designed with the objective of reinforcing students' mathematical writing. Throughout the first three chapters, representative examples (that are not numbered) of applications of Group Theory to Mathematical Music Theory are included for students who already have some knowledge of Music Theory.

In chapter 4, the application of Group Theory to Music Theory is presented in detail. Some basic aspects of Mathematical Music Theory are explained and, in the process, some essential elements of both areas are given to readers with different backgrounds. For this reason, the examples follow from some of the outstanding theoretical aspects of the previous chapters; the musical terms are introduced as they are needed so that a reader without musical background can understand the essence of how Group Theory is used to explain certain preestablished musical relations. On the other hand, for the reader with knowledge of Music Theory only, this chapter provides concrete elements, as well as motivation, to begin to understand Group Theory.