USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

GRUPOS E MÚSICA: TRANSFORMACIÓNS DE ACORDES

Lucía González Iglesias

Xullo, 2022

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

GRUPOS E MÚSICA: TRANSFORMACIÓNS DE ACORDES

Lucía González Iglesias

Xullo, 2022

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: Grupos e música: transformacións de acordes
Breve descrición do contido
Neste traballo abordaranse algúns conceptos de teoría de grupos e as súas accións. O obxectivo principal é aplicalo á teoría de acordes musicais. En concreto estudaremos dous grupos que actúan sobre os acordes da escala diatónica e as relacións entre ambos.
Recomendacións
Coñecer os elementos básicos da linguaxe musical incluíndo a escala diatónica, intervalos e acordes.
Outras observacións

Índice

Resumo

O traballo consiste en ver a relación que hai entre a teoría de grupos e a teoría musical. Comézase estudando grupos, prestando especial atención ás accións de grupos en conxuntos e ós grupos libres. Posteriormente, aplícase o estudado ó caso do grupo simétrico. Identifícase o conxunto das 12 notas musicais da escala cromática co grupo cíclico de 12 elementos. A continuación, defínese o conxunto dos acordes de tres notas maiores e menores, e danse unha serie de transformacións no mesmo. Os acordes maiores e menores xunto con estas transformacións son a base da harmonía de moitas cancións e melodías. Próbase que o conxunto de dúas destas transformacións, as inversións e transposicións, forma un grupo que actúa sobre o conxunto dos acordes. Por outra banda, vese que o conxunto formado por outras tres delas, a paralela, relativa, e intercambio de sétima, forma outro grupo que tamén actúa sobre o conxunto dos acordes. Posteriormente, próbase que ámbolos dous grupos son isomorfos, e que ademais un é o centralizador do outro, chegando finalmente a que os grupos son duais como subgrupos do grupo de transformacións do conxunto de acordes.

Abstract

This work studies the relationship between group theory and music theory. We start presenting groups, with special emphasis on group actions on sets and free groups. Next, we apply the previous results to the symmetric group. We identify the set of 12 musical notes form the chromatic scale with the cyclic group of order 12. We also define the set of major and minor triads and present several transformations on the set they form. Major and minor chords and these transformations make part of the harmonic base of lots of songs and melodies. We show that the set of two kinds of transformations, namely inversions and transpositions make part of a group that acts on the set of chords. On the other hand, we see that the set formed by a different set of transformations, the parallel, relative and seventh interchange constitute another group that acts also on the set of chords. Finally, we prove that both groups are isomorphic and one is the centralizer of the other, concluding that both groups are dual subgroups of the permutation group of transformations on the set of chords.

Introdución

A noción de grupo codifica a idea matemática de conxunto de transformacións dun sistema que poden compoñerse. Unha fonte histórica da noción de grupo aparece na idea de Lagrange de considerar as permutacións das raíces dunha ecuación alxébrica. Esta idea levou a Galois á idea do grupo dunha ecuación polinómica e á solución do problema da resolubilidade por radicais dunha ecuación tal. Outra fonte de aparición da estrutura de grupo é a consideración de transformacións xeométricas que preservan certas propiedades xeométricas das figuras. Hoxe en día, a estrutura de grupo xoga un papel central nas matemáticas e nas súas aplicacións.

Neste traballo preséntanse algunhas aplicacións da teoría de grupos á teoría musical. En concreto vanse expoñer certas transformacións que rexen algunhas propiedades básicas da harmonía, e en particular certas simetrías do conxunto dos 24 acordes básicos: as 12 tríades maiores e as correspondentes 12 menores.

As notas musicais da escala dispóñense en 12 semitóns e presentan unha simetría básica gobernada polo grupo cíclico de 12 elementos. Os elementos deste grupo correspóndense cos intervalos da harmonía básica.

Nesta memoria considéranse dous grupos de simetrías do conxunto dos 24 acordes principais. O primeiro grupo, denominado TI, está formado polas transposicións e inversións diatónicas. É un subgrupo do grupo das permutacións do conxunto dos acordes, sendo as transposicións ciclos de orde 12 e as inversións ciclos de orde 2. A súa descrición mediante xeradores e relacións permite identificalo co grupo diédrico dos movementos dun dodecágono. O outro grupo, denominado PLR, está xerado por tres transformacións que son a súa propia inversa. A transformación P intercambia un acorde maior pola súa versión menor, L intercambia un acorde maior pola súa terceira menor (transformación ás veces chamada transposición de sétima) e R intercambia un acorde maior co seu relativo menor (sexta menor). Á súa vez, este grupo identifícase cun subgrupo do grupo de permutacións do conxunto dos acordes, e é tamén isomorfo ao grupo diédrico. Estas transformacións foron consideradas no século XIX polo musicólogo Hugo Riemann, polo que o grupo PLR se asocia a el, como se indica no texto de Crans, Fiore e Satyendra [4].

A xeometría subxacente ao grupo PLR pode apreciarse no diagrama "Tonnetz"de Riemann

que se reproduce na sección 3.2.2. Pese a que PLR e TI son isomorfos e ambos subgrupos do grupo de permutacións do conxunto dos acordes, non son coincidentes. No traballo probarase que ambos grupos son duais. En termos precisos, cada un deles é o centralizador do outro. Esta propiedade alxébrica capta a idea de que ambos grupos expoñen de formas matemáticas distintas a mesma simetría subxacente na colección de acordes formados polas tríades maiores e menores.

Pásase agora á descrición máis detallada do contido do traballo. O propósito do mesmo é facer un estudo da teoría de grupos e posteriormente relacionalo coa harmonía e cos acordes. Para elo, estruturarase a memoria do seguinte xeito:

O primeiro capítulo é en gran parte un resumo de resultados da teoría de grupos coa finalidade de que a memoria sexa autocontida. No último epígrafe introdúcese o concepto de grupo libre con base un conxunto e próbase a súa existencia, así como a súa unicidade salvo isomorfismos. Un resultado importante que se obtén é que todo grupo é o cociente dun grupo libre, o que permitirá falar de presentación dun grupo por xeradores e relacións. Finalmente, próbase o teorema de van Dyck, resultado que se ilustrará cun par de exemplos.

O segundo capítulo está dedicado ao estudo do grupo simétrico S_n. Deste xeito, concrétase o estudado no primeiro capítulo ao caso deste grupo. Así, dado un conxunto, analízanse as aplicacións bixectivas dentro do mesmo, o que se coñece como permutacións, e vense algunhas concretas: os chamados ciclos e as transposicións. A continuación, próbase que as permutacións se poden factorizar nun produto de ciclos, e que a súa vez os ciclos se poden factorizar nun produto de transposicións, sendo a paridade do número de transposicións na factorización sempre a mesma. Isto leva a distinguir entre dous tipos de permutacións: pares e impares. A continuación analízanse as clases de conxugación de S_n e finalízase o capítulo dando unha presentación do mesmo por xeradores e relacións.

O terceiro e último capítulo versa sobre a relación entre os grupos e as transformacións de acordes. Para iso, comézanse definindo os acordes de tres notas maiores e menores, e o conxunto formado por todos eles. A continuación, vense varias transformacións dentro deste conxunto que, como xa se dixo, forman dous grupos isomorfos. Ademais, son un o centralizador do outro, chegando a que son grupos duais.

A memoria remata coa bibliografía, na que aparecen as referencias empregadas para a realización do traballo. Debemos indicar que aínda que consultamos máis referencias das que figuran limitámonos a incluír as que citamos explicitamente no texto.

Capítulo 1

Teoría de grupos

Neste primeiro capítulo preténdese levar a cabo unha revisión dalgúns dos aspectos fundamentais da teoría de grupos, que permiten encamiñar o tema en cuestión. En primeiro lugar, defínese o concepto de grupo e introdúcense nocións básicas a partir do mesmo, tales como as súas propiedades e aplicacións. A continuación, estúdase un tipo de grupos particulares: os cíclicos. Posteriormente, defínese o concepto de subgrupo normal e establécense as condicións para que un subgrupo sexa tal. Ademais, estúdanse as aplicacións entre grupos que conservan as operacións dos mesmos, denominadas homomorfismos. Enúncianse o teorema de Lagrange e os de isomorfía de Noether e recóllense algúns resultados deducidos dos mesmos. Determínase a idea de acción de grupos en conxuntos, cuxos resultados se relacionarán, máis adiante, coa teoría musical. Finalmente, estúdanse os conceptos de grupo libre, xeradores e relacións, nocións necesarias para ver presentacións de grupos. Os contidos do capítulo seguen os textos de Rotman [12], Cohn [3] e Hungerford [8].

1.1. Xeneralidades sobre grupos

Comézase pois, como xa se dixo, coa noción de grupo:

Definición 1.1. Un **grupo** é un par $(G, \cdot)$, onde G é un conxunto cunha operación interna, $\cdot$

$$\begin{array}{rccc} \cdot : & G \times G & \longrightarrow & G \\ & (x, y) & \longmapsto & x \cdot y \end{array}$$

verificando as seguintes propiedades:

- Asociativa: $\forall x, y, z \in G,\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
- Existencia de elemento neutro: $\exists e \in G$ tal que $x \cdot e = x = e \cdot x,\ \forall x \in G$.

- Existencia de elemento simétrico: $\forall x \in G$, $\exists x' \in G$ tal que $x \cdot x' = e = x' \cdot x$.

Se, ademais, se verifica que $\forall x, y \in G$, $x \cdot y = y \cdot x$, o grupo G dise **conmutativo** ou **abeliano**.

Pola definición, dedúcese que nun grupo G se verifican as seguintes **propiedades**:

- O neutro é único.
- O simétrico dun elemento é único.
- $(x \cdot y)' = y' \cdot x'$, $\forall x, y \in G$.
- $(x')' = x$, $\forall x \in G$.
- $x \cdot y = x \cdot z \Rightarrow y = z$, $\forall x, y, z \in G$.
- $x \cdot y = e \Rightarrow x = y'$ e $y = x'$.

Para denotar un grupo poden utilizarse dúas notacións distintas:

- **Multiplicativa**: denótase $(G, \cdot)$, o neutro por 1, e o elemento simétrico (ou inverso) de x por x^{-1}. Ademais, por simplificar, tense que $x \cdot y = xy$.
- **Aditiva**: denótase $(G, +)$, o neutro por 0, e o simétrico dun elemento x por $-x$.

En xeral, a segunda utilízase cando o grupo é conmutativo.

Vexamos agora uns primeiros exemplos de grupos:

Exemplo 1.2. Os exemplos máis clásicos de grupos son os números enteiros $\mathbb{Z}$, os racionais $\mathbb{Q}$, os reais $\mathbb{R}$ e os complexos $\mathbb{C}$ coa suma; así como os racionais sen o cero $\mathbb{Q}^*$, os reais sen o cero $\mathbb{R}^*$ e os complexos sen o cero $\mathbb{C}^*$, coa multiplicación.

Exemplo 1.3. Un **anel** é unha terna $(R, +, \cdot)$, onde $(R, +)$ é un grupo, $(R, \cdot)$ é un monoide ($\cdot$ é asociativa e ten elemento neutro 1) e verificando a propiedade distributiva de $\cdot$ respecto de $+$. Pode verse que, dado un anel R, o conxunto das súas unidades, que se define como $U(R) := \{a \in R \mid \exists a^{-1} \in R \,, aa^{-1} = a^{-1}a = 1\}$, é un grupo coa multiplicación.

Exemplo 1.4. Outro exemplo é o grupo linear xeral $GL(n, K)$, que é o conxunto das matrices de orde $n \times n$ non singulares sobre un corpo K (un anel onde todo elemento distinto de 0 é unha unidade), coa operación a multiplicación de matrices. Este é un exemplo de grupo non conmutativo, debido a que o produto de matrices non ten por que selo.

Exemplo 1.5. O grupo diédrico D_n con $n \in \mathbb{N}$ é o grupo simétrico dun polígono regular de n lados e ten $2n$ elementos.

Por exemplo, D_3 é o grupo simétrico dun triángulo equilátero. Considérase un triángulo de vértices A, B e C. Téñense entón os xiros no sentido contrario ao das agullas do reloxo de $120°, 240°$ e $360°$ ($G_{120}, G_{240}, G_{360}$) así como as simetrías sobre cada un dos vértices do triángulo: S_A, S_B e S_C. O grupo G é entón $G = \{G_{120}, G_{240}, G_{360}, S_A, S_B, S_C\}$. Se se fai a composición entre cada par de transformacións, obtense a táboa seguinte:

	G_{120}	G_{240}	G_{360}	S_A	S_B	S_C
G_{120}	G_{240}	G_{360}	G_{120}	S_B	S_C	S_A
G_{240}	G_{360}	G_{120}	G_{240}	S_C	S_A	S_B
G_{360}	G_{120}	G_{240}	G_{360}	S_A	S_B	S_C
S_A	S_C	S_B	S_A	G_{360}	G_{240}	G_{120}
S_B	S_A	S_C	S_B	G_{120}	G_{360}	G_{240}
S_C	S_B	S_A	S_C	G_{240}	G_{120}	G_{360}

Introdúcese agora o concepto de subgrupo.

Definición 1.6. Un **subgrupo** dun grupo $(G, \cdot)$ é un subconxunto $H \subset G$, $H \neq \emptyset$ de xeito que $(H, \cdot)$ é un grupo. É dicir, $1 \in H$ e para todo par de elementos $x, y \in H$, tense que $xy \in H$ e $x^{-1} \in H$. Denótase por $H < G$. Obviamente, $\{1\} < G$ e $G < G$.

Outros exemplos sinxelos son os seguintes.

Exemplo 1.7. Xa se dixo que $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ e $(\mathbb{C}, +)$ son grupos. Entón, é claro que $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$.

Exemplo 1.8. Se $n\mathbb{Z}$, con $n \in \mathbb{N}$ é o grupo formado polos múltiplos de n en $\mathbb{Z}$, terase que $(n\mathbb{Z}, +) < (\mathbb{Z}, +)$.

Exemplo 1.9. Como xa se dixo no Exemplo 1.4, o grupo linear xeral $GL(n, K)$ é un grupo, sendo K un corpo. En concreto, $GL(2, \mathbb{C})$ é o grupo das matrices 2×2 invertibles con entradas en $\mathbb{C}$. Considéranse dúas matrices neste grupo:

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

A partir destas dúas matrices, defínese a continuación o chamado grupo dos cuaternios Q_8, que está formado polos 8 elementos: $Q_8 = \{A, A^2, A^3, A^4 = I, B, AB, A^2B, A^3B\}$.

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \qquad A^3 = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

$$AB = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \qquad A^2B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad A^3B = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

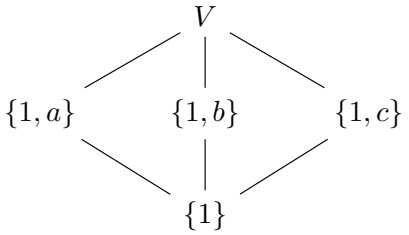
Téñense cinco subgrupos neste grupo. En primeiro lugar tense o subgrupo trivial $\{A^4 = I\}$. En segundo lugar, o subgrupo de dous elementos $N = \{I, A^2\}$. Finalmente, tres subgrupos de catro elementos $H_1 = \{A, A^2, A^3, A^4\}$, $H_2 = \{B, B^2, B^3, B^4 = I\}$ e $H_3 = \{AB, (AB)^2, (AB^3), I\}$.

Cabe destacar que, dado un grupo cun número finito de elementos, pode representarse graficamente o seu retículo de subgrupos, como se ve a continuación.

Exemplo 1.10. Considérese o grupo de Klein, un grupo de 4 elementos, $V = \{1, a, b, c\}$, cuxa operación interna vén dada pola seguinte táboa:

·	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

É un grupo conmutativo no que hai tres subgrupos non triviais: $\{1, a\}$, $\{1, b\}$ e $\{1, c\}$. Non obstante, $\{1, a, c\}$ non é un subgrupo, xa que $ac = b \notin \{1, a, c\}$. Obtense, entón, o seguinte retículo de subgrupos:



Vese agora un resultado sobre a intersección de subgrupos.

Proposición 1.11. *Dado un grupo G, a intersección de subgrupos de G é un subgrupo de G:* $H_i < G, i \in I \Rightarrow \bigcap_{i \in I} H_i < G$.

Este resultado xeral que se verifica coa intersección de subgrupos non ten por que cumprirse coa unión, como se pode ver a continuación.

Exemplo 1.12. Sexa o grupo $\mathbb{Z}$, e sexan $3\mathbb{Z} < \mathbb{Z}$ e $4\mathbb{Z} < \mathbb{Z}$. Obsérvase facilmente que $3 \in 3\mathbb{Z}$ e $4 \in 4\mathbb{Z}$. Non obstante, $3 + 4 = 7 \notin 3\mathbb{Z} \cup 4\mathbb{Z}$, e polo tanto $3\mathbb{Z} \cup 4\mathbb{Z} \not< \mathbb{Z}$.

Deste xeito, aínda que a unión de subgrupos non sexa en xeral un subgrupo, pode definirse o menor subgrupo que contén á unión. De xeito aínda máis xeral, defínese a continuación o menor subgrupo contendo a un subconxunto.

Definición 1.13. O **subgrupo xerado por X**, sendo G un grupo e X un subconxunto de G, é o menor subgrupo de G contendo a X, e denótase por $\langle X\rangle$. Polo visto anteriormente, pode afirmarse que $\langle X\rangle = \bigcap\{H \mid H < G, X \subset H\}$.

A proposición seguinte dinos como son os elementos do subgrupo que se acaba de definir.

Proposición 1.14. *Se $X \neq \emptyset, X \subset G$ con G grupo, tense que $\langle X\rangle = \{a_1 \cdots a_n \mid n \in \mathbb{N}$ e para cada $i, a_i \in X$ ou $a_i^{-1} \in X\}$.*

1.2. Grupos cíclicos

Poden agora introducirse os conceptos de subgrupo e grupo cíclicos.

Definición 1.15. Dado $a \in G$, o **subgrupo cíclico xerado por a** é $\langle a\rangle := \{a^n \mid n \in \mathbb{Z}\}$. Así, dise que un grupo G é **cíclico** se $\exists a \in G$ tal que $G = \langle a\rangle$.

Cabe destacar que todo grupo cíclico é abeliano, e que todo subgrupo dun grupo cíclico é cíclico.

Entón, un grupo dise cíclico se pode xerarse por un solo elemento del. Vexamos un exemplo sinxelo de grupo cíclico.

Exemplo 1.16. Considerando $\mathbb{Z}$ coa suma, é un grupo cíclico: $\mathbb{Z} = \langle 1\rangle$, e tamén $\mathbb{Z} = \langle -1\rangle$.

Exemplo 1.17. Pola súa banda, pode definirse en $\mathbb{Z}$ unha relación de equivalencia mediante a congruencia $a \equiv b (\text{mód } m)$, onde $a, b, m \in \mathbb{Z}$. Entón, polo algoritmo da división en $\mathbb{Z}$, fixado $m \in \mathbb{N}$, tense que para todo $a \in \mathbb{Z}$ se verifica $a = mq + r$, onde $0 \leq r < m$. É dicir, cada $a \in \mathbb{Z}$ é congruente módulo m a r, isto é, a $0, 1, 2, ..., m-1$. Estes números son os residuos módulo m, que son as clases da relación de equivalencia. O conxunto das clases é $\mathbb{Z}_m = \{\overline{1}, \overline{2}, ..., \overline{m-1}\}$, que é un grupo coa suma. Ademais, resulta ser un grupo cíclico, pois $\mathbb{Z}_m = \langle\overline{1}\rangle$. Posteriormente, estudarase o grupo $\mathbb{Z}_{12}$ polo seu significado musical, xa que é un xeito sinxelo de representar a escala cromática equitemperada.

Nunha sección posterior verase que tódolos grupos cíclicos son como $\mathbb{Z}$ ou $\mathbb{Z}_m$, para $m \in \mathbb{N}$.

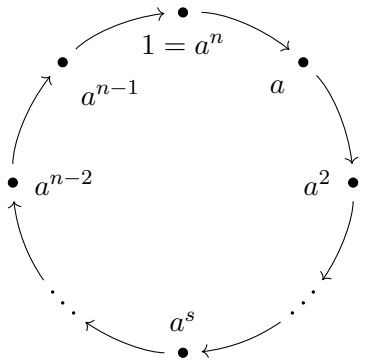
Introdúcese a continuación o concepto de orde dun grupo e orde dun elemento do grupo.

Definición 1.18. Sexa G un grupo. A súa **orde**, $|G|$, é o número de elementos que ten se o conxunto G é finito. Noutro caso, dise que G é de orde infinita. Ademais, se $a \in G$, defínese a súa **orde**, $|a|$, como a orde de $\langle a \rangle$.

Proposición 1.19. *Dado un grupo G, $a \in G$, $|a| = n$:*

1. *Os elementos $1, a, ..., a^{n-1}$ son todos distintos; $\langle a \rangle = \{1, a, ..., a^{n-1}\}$ e $a^n = 1$.*
2. *Sexa $m \in \mathbb{Z}$. Entón, $a^m = 1 \Leftrightarrow m = \dot{n}$. En particular, n é o menor enteiro positivo non nulo de xeito que $a^n = 1$.*

Unha forma sinxela de visualizar un grupo cíclico finito nas hipóteses da proposición anterior consiste en representar nun círculo os elementos $1, a, ..., a^{n-1}$ do seguinte xeito:



Así, obsérvase que un elemento a^s se atopa situado a s unidades, medidas no sentido das agullas do reloxo, do elemento $a^n = 1$. Pode verse facilmente no seguinte exemplo.

Exemplo 1.20. Tomando U_n o conxunto das raíces n-ésimas da unidade, tense que é un grupo multiplicativo cíclico de orde n que está xerado por $\alpha = \cos\frac{2\pi}{n} + i\,\mathrm{sen}\,\frac{2\pi}{n}$. Represéntanse no círculo de raio unidade, dende $\alpha^n = 1$ situado no punto $(1, 0)$, co resto situados equidistantes no sentido contrario ás agullas do reloxo.

Proposición 1.21. *Sexa G un grupo cíclico de orde n, $G = \langle a \rangle$. Entón:*

1. *$|a^r| = \frac{n}{(n,r)}$, onde (n, r) denota o máximo común divisor de n e de r.*
2. *$\langle a^r \rangle = G \Leftrightarrow (n, r) = 1$*

Un grupo cíclico pode ter máis dun xerador como xa se viu con $\mathbb{Z}$. A proposición anterior determina as potencias de a que xeran o grupo $\langle a \rangle$.

Introdúcese a continuación a función φ de Euler, que servirá para enunciar unha serie de resultados que caracterizan ós grupos cíclicos finitos.

Definición 1.22. A función φ de Euler defínese como segue: $\varphi(n) := |\{a \leq n \mid a \in \mathbb{Z}^+ \text{ e } (a,n) = 1\}|$, para $n \in \mathbb{Z}^+$ e onde $|\cdot|$ representa o cardinal.

Esta función é importante en teoría de números e proporciona o tamaño do grupo multiplicativo de enteiros módulo n. Máis precisamente, $\varphi(n)$ é a orde do grupo de unidades do anel $\mathbb{Z}_n$.

Lema 1.23. *Sexa un grupo cíclico G de orde n. Entón, para cada divisor d de n existe un único subgrupo de G de orde d.*

Demostración. Supoñamos $|G| = n < \infty$, $G = \langle a \rangle$ e sexa d dividindo a n. Entón denotemos $t = \frac{n}{d}$. Pola Proposición 1.21, tense que $|a^t| = d$, polo que existe un subgrupo $\langle a^t \rangle < G$ de orde d. Vexamos agora que este subgrupo de G é o único de orde d.

Sexa H outro subgrupo de G de orde d. Entón, $H = \langle a^s \rangle$, sendo s o mínimo enteiro positivo verificando $a^s \in H$. De novo pola Proposición 1.21, $\frac{n}{(n,s)} = |a^s| = |H| = d = \frac{n}{t}$, de onde se deduce que $t = (n,s)$. Así, t divide a s, e polo tanto $a^s \in \langle a^t \rangle$. Entón, $H = \langle a^s \rangle < \langle a^t \rangle$, pero tamén se tiña $|a^t| = d = |H|$, o que implica que $H = \langle a^t \rangle$. □

Teorema 1.24. *Dado un enteiro positivo n, verifícase que $n = \sum_{d|n} \varphi(d)$, onde d son os divisores de n tales que $1 \leq d \leq n$.*

Demostración. Se C é un subgrupo cíclico do grupo G, denótase por $\text{xen}(C)$ o conxunto dos seus xeradores. Deste xeito, G pode escribirse como a unión disxunta $G = \bigcup \text{xen}(C)$, onde C percorre tódolos subgrupos cíclicos de G. Entón, como se dixo no lema, se G é un grupo cíclico de orde n, hai un único subgrupo C_d cíclico de orde d para cada divisor d de n. Polo tanto, terase que $n = |G| = \sum_{d|n} |\text{xen}(C_d)|$. Ademais, dado un grupo cíclico G de orde n de xeito que $G = \langle a \rangle$, tense que $G = \langle a^k \rangle$ se, e só se, $(k,n) = 1$. Así, o número de xeradores de G é $\varphi(n)$. Conclúese entón que $|\text{xen}(C_d)| = \varphi(d)$, de onde se segue o resultado do teorema. □

Teorema 1.25. *Un grupo G de orde n é cíclico se, e só se, existe ao sumo un subgrupo cíclico de G de orde d para cada divisor d de n.*

Demostración. A implicación cara a dereita séguese do lema anterior (Lema 1.23). Lembremos agora que, pola proba anterior, o grupo G é a unión disxunta $G = \bigcup \text{xen}(C)$, con C os distintos subgrupos cíclicos de G. Agora, polo teorema anterior, $n = |G| = \sum |\text{xen}(C_d)| \leq \sum_{d|n} \varphi(d) = n$. Conclúese entón que, para cada divisor d de n, se ten un subgrupo cíclico de orde d. En particular, tomando $d = n$, G é cíclico. □

1.3. Teorema de Lagrange

Nesta sección enúnciase o Teorema de Lagrange e algún resultado que se deduce a partir del. Dado un grupo G e $H < G$, defínese unha relación de equivalencia:

$$x, y \in G, x \sim y :\Leftrightarrow x^{-1}y \in H$$

As clases da relación de equivalencia son: $[a] = \{b \in G \mid a^{-1}b \in H\} = aH$ para $a \in G$. En particular, $[1] = H$, e tense así unha partición de G dada pola unión disxunta das clases.

Definamos unha serie de conceptos necesarios para enunciar o teorema de Lagrange.

Definición 1.26. O **conxunto cociente de G por H** é o conxunto das clases de equivalencia anteriores, e denótase por G/H.

Definición 1.27. O **índice de H en G**, $(G : H)$, denota o cardinal de G/H.

Teorema 1.28. *(**Teorema de Lagrange**) Se G é un grupo finito, entón $|G| = |H|(G : H)$.*

Do teorema de Lagrange séguense os seguintes resultados:

Corolario 1.29. *Dado un grupo G finito, verifícase:*

1. $H < G \Rightarrow |H| \mid |G|$.
2. $a \in G \Rightarrow |a| \mid |G|$.
3. $a \in G \Rightarrow a^{|G|} = 1$.
4. *Se $|G|$ é un número primo, entón G é cíclico.*

É de interese mencionar que se ben o teorema de Lagrange di que se G é un grupo finito de orde n e H é un subgrupo de G, a orde de H divide a n, non se ten asegurada a existencia dun subgrupo de orde d para d un divisor de n. Este resultado é certo para os grupos cíclicos finitos e tal subgrupo tamén é cíclico como se viu no Lema 1.23 e tamén para as potencias de primos que dividen a n, resultado que está asegurado polo teorema de Sylow. No capítulo seguinte darase un exemplo dun grupo de orde 12 que non ten ningún subgrupo de orde 6.

1.4. Subgrupos normais

Séguese a continuación o estudo dun tipo de subgrupos N que permiten reflectir no cociente G/N a estrutura de grupo de G.

Definición 1.30. Dado un grupo G, dise que un subgrupo $N < G$ é **normal** e denótase $N \triangleleft G$ se $aNa^{-1} \subset N \ \ \forall a \in G$, onde $aNa^{-1} = \{ana^{-1} \mid n \in N\}$.

Vexamos unha caracterización dos subgrupos normais.

Proposición 1.31. *Sexa N un subgrupo dun grupo G. Equivalen:*

1. $N \triangleleft G$.
2. $aN = Na \ \ \forall a \in G$.
3. $aNbN = abN \ \ \forall a, b \in G$.
4. $aNa^{-1} = N \ \ \forall a \in G$.

Poden verse uns primeiros exemplos de subgrupos normais dun grupo G.

Exemplo 1.32. Sexa G un grupo. Entón, obviamente G e $\{1\}$ son subgrupos normais de G.

Definición 1.33. Dados dous elementos $a, b \in G$ con G grupo, dise que son **conxugados** se $\exists x \in G$ tal que $b = x^{-1}ax$. A relación "ser conxugados" é unha relación de equivalencia en G, e denótase por $\overset{c}{\sim}$. Deste xeito, a clase de conxugación dun elemento $a \in G$ está formada por tódolos elementos de G que son conxugados con a.

Así, pode dicirse que un subgrupo H dun grupo G é normal se, e soamente se, H contén ós conxugados de tódolos seus elementos:

$$H \triangleleft G \Leftrightarrow [x \in H, y \overset{c}{\sim} x \Rightarrow y \in H]$$

É dicir, un subgrupo é normal se contén tódalas clases de conxugación de tódolos seus elementos.

Vexamos unha condición suficiente para que un subgrupo sexa normal.

Proposición 1.34. *Sexa N un subgrupo de G. Entón $(G : N) = 2 \Rightarrow N \triangleleft G$.*

Defínense a continuación dous subgrupos dun grupo G, que se verifica que son normais.

Definición 1.35.

1. O **centro** de G é $Z(G) := \{x \in G \mid xy = yx \ \ \forall y \in G\}$.
2. Dados $a, b \in G$, o **conmutador** de a e b é o elemento $[a, b] := aba^{-1}b^{-1}$. Entón, o **conmutador** de G é o subgrupo xerado por tódolos conmutadores de elementos de G, é dicir, $[G, G] := \langle aba^{-1}b^{-1} \mid a, b \in G\rangle$. Ademais, $[G, G]$ queda caracterizado do xeito seguinte:

   a) $[G, G]$ é subgrupo normal de G.

b) $G/[G,G]$ é abeliano.

c) Se $H \triangleleft G$ de xeito que G/H é abeliano, entón $[G,G] \subset H$.

Obsérvese que dado un grupo G conmutativo e $N < G$, tense trivialmente que $N \triangleleft G$.

Analicemos agora exemplos de subgrupos normais, comezando co grupo dos cuaternios, e seguindo co grupo simétrico dun triángulo equilátero.

Exemplo 1.36. Considérese o grupo dos cuaternios, do que xa se falou no Exemplo 1.9. Pode verse que é un exemplo de grupo non conmutativo que ten tódolos subgrupos normais:

Xa se dixo que os subgrupos son o trivial, e os subgrupos $N = \{I, A\}$, $H_1 = \{I, A, A^2, A^3\}$, $H_2 = \{I, B, B^2, B^3\}$ e $H_3 = \{I, AB, (AB)^2, (AB)^3\}$. O subgrupo trivial sempre é normal. Por outra banda, os subgrupos de catro elementos son normais porque, por exemplo tomando H_1, tense que $(Q_8 : H_1) = 2 \Rightarrow H_1 \triangleleft Q_8$. Finalmente, o subgrupo de 2 elementos $N = \{1, A\}$ tamén é normal, como se pode ver tomando calquera $C \in Q_8$ facendo $C^{-1}A^2C = A^2$.

Exemplo 1.37. Centrémonos no grupo D_3 (Exemplo 1.5). Observamos que hai catro subgrupos distintos (que non son nin o trivial nin o propio grupo G).

$N = \{G_{360}, G_{120}, G_{240}\} = \langle\{G_{120}\}\rangle = \langle\{G_{240}\}\rangle = \langle\{G_{120}, G_{240}\}\rangle$,

$H_1 = \{G_{360}, S_A\} = \langle\{S_A\}\rangle$, $H_2 = \{G_{360}, S_B\} = \langle\{S_B\}\rangle$, $H_3 = \{G_{360}, S_C\} = \langle\{S_C\}\rangle$.

Como $|N| = |G_{120}| = |G_{240}| = 3$ e $|G| = 6$, entón $(G : N) = \frac{6}{3} = 2$, e así $N \triangleleft G$. Por outra banda, tomando por exemplo $S_B \in G$, $S_B S_A S_B^{-1} = S_B S_A S_B = G_{120} S_B = S_C \notin H_1$, e polo tanto H_1 non é subgrupo normal de G. O mesmo sucede con H_2 e H_3.

A seguinte proposición garante que o cociente dun grupo por un subgrupo normal ten estrutura de grupo.

Proposición 1.38. *Se $N \triangleleft G$, entón G/N será un grupo, denominado* ***grupo cociente de*** *G* ***por*** *N, de orde $(G : N)$, e que está dado pola operación $(aN)(bN) = abN$. O neutro é N e o simétrico dun elemento aN é $a^{-1}N$.*

1.5. Homomorfismos de grupos

Esta sección céntrase nas aplicacións entre grupos que son compatibles coas operacións dos grupos, e que serán denominadas homomorfismos de grupos.

Definición 1.39. Dados dous grupos $(G_1, *)$ e $(G_2, \circ)$, un **homomorfismo de grupos** é unha aplicación $f : G_1 \longrightarrow G_2$ de xeito que $\forall a, b \in G_1$,

$$f(a * b) = f(a) \circ f(b).$$

Segundo a aplicación sexa inxectiva, sobrexectiva ou bixectiva, teranse distintos tipos de homomorfismos, que se definen a continuación.

Definición 1.40. Un **monomorfismo** é un homomorfismo inxectivo, e un **epimorfismo** é un homomorfismo sobrexectivo.

Definición 1.41. Un **isomorfismo** é un homomorfismo que tamén é unha bixección. Se existe un isomorfismo entre dous grupos G_1 e G_2, dirase que son isomorfos e denotarase por $G_1 \cong G_2$.

Exemplo 1.42. Considérese agora o grupo de Klein de catro elementos, do que xa se falou no Exemplo 1.10, e compárese co grupo cíclico de catro elementos (táboa da dereita).

·	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

·	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

As dúas táboas son distintas, e así dannos un exemplo de dous grupos de catro elementos non isomorfos.

Estudemos unha serie de propiedades que verifican os homomorfismos de grupos.

Proposición 1.43. *Sexa $f : (G_1, *) \longrightarrow (G_2, \circ)$ un homomorfismo de grupos. Entón verifícase:*

1. $f(1) = 1$, *onde, por abuso de notación, se denota por 1 o neutro en ámbolos dous grupos.*
2. $f(a^{-1}) = f(a)^{-1}$ *para todo* $a \in G_1$.
3. $f(a^n) = f(a)^n$ *para todos* $a \in G_1$ *e* $n \in \mathbb{Z}$.

Vexamos algún exemplo de homomorfismo de grupos.

Exemplo 1.44. Sexa $\mathbb{S}^1$ o grupo do círculo de raio 1, é dicir, o grupo multiplicativo de tódolos números complexos de módulo 1. Entón, para un número real fixado y:

$$\begin{array}{rccc} f_y\colon & \mathbb{R} & \longrightarrow & \mathbb{S}^1 \\ & x & \longmapsto & f_y(x) = e^{iyx} \end{array}$$

é un homomorfismo. De feito, as funcións f_y son os únicos homomorfismos continuos $\mathbb{R} \to \mathbb{S}^1$.

Exemplo 1.45. Nun grupo G, é sinxelo ver que a conxugación por un elemento $a \in G$ é un homomorfismo de grupos $c_a : G \to G$, onde $c_a(x) = axa^{-1} \ \ \forall x \in G$. Observamos que non só é un homomorfismo, se non que ao ser unha aplicación bixectiva, tamén é un isomorfismo.

Definición 1.46. Dado un homomorfismo de grupos $f : G_1, \longrightarrow G_2$, defínese o seu **núcleo** como $\ker f = \{x \in G_1 \mid f(x) = 1\}$.

Definición 1.47. Se $f : G_1 \to G_2$ é un homomorfismo de grupos, $f(G_1)$ denótase por $\operatorname{Im} f$.

A partir destas definicións pode verse unha caracterización sinxela dos monomorfismos e epimorfismos.

Proposición 1.48. *Sexa un homomorfismo de grupos $f : G_1 \to G_2$. f é un monomorfismo se, e só se,* $\ker f = \{1\}$. *De xeito análogo, f é un epimorfimso se, e só se,* $\operatorname{Im} f = G_2$.

Proposición 1.49. *Dado un homomorfismo de grupos $f : G_1, \longrightarrow G_2$:*

1. $H_1 < G_1 \Rightarrow f(H_1) < G_2$.
2. $H_2 < G_2 \Rightarrow f^{-1}(H_2) < G_1$.
3. $N_2 \triangleleft G_2 \Rightarrow f^{-1}(N_2) \triangleleft G_1$.
4. $N_1 \triangleleft G_1$, *f sobrexectiva* $\Rightarrow f(N_1) \triangleleft G_2$.

Pode deducirse que $\operatorname{Im} f$ é un subgrupo de G_2. Obsérvese ademais que, como $\{1\} \triangleleft G_2$, terase que $\ker f = f^{-1}(\{1\}) \triangleleft G_1$. É dicir, os núcleos dos homomorfismos de grupos son subgrupos normais. Cabe destacar que tamén se verifica o recíproco, é dicir, os subgrupos normais son núcleos de homomorfismos de grupos, resultado que se reflicte na seguinte proposición.

Proposición 1.50. *Sexa un grupo G e $N \triangleleft G$. Entón a* ***proxección canónica*** $\pi : G \to G/N$, *dada por $\pi(x) = xN \ \ \forall x \in G$, é un epimorfismo cuxo núcleo é N.*

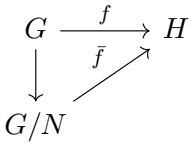
Demostración. En primeiro lugar, $\pi(xy) = xyN = (xN)(yN) = \pi(x)\pi(y)$. Entón, como a proxección canónica é sobrexectiva, π será un epimorfismo. Agora, pode calcularse $\ker \pi$ como $\ker \pi = \{a \in G \mid \pi(a) = 1N = N\} = \{a \in G \mid aN = N\} = \{a \in G \mid a \in N\} = N$, o que conclúe a proba. □

1.6. Teoremas de isomorfía

Nesta sección centrarémonos nos teoremas de isomorfía de Noether, así como nos resultados que se deducen a partir deles.

Proposición 1.51. *Sexa $f : G \to H$ un homomorfismo de grupos e $N \triangleleft G$ tal que $N \subset \ker f$. Entón, existe un homomorfismo único $\bar{f} : G/N \to H$ de xeito que $\bar{f}(aN) = f(a) \ \ \forall a \in G$,*

$\operatorname{Im} f = \operatorname{Im} \bar{f}$ *e* $\ker \bar{f} = (\ker f)/N$. *Ademais,* $\bar{f}$ *é un isomorfismo se, e só se,* $N = \ker f$ *e* f *é sobrexectivo. É dicir, hai un único homomorfismo* $\bar{f} : G/N \to H$ *facendo conmutativo o diagrama:*



Demostración. Dado $b \in aN$, entón $\exists n \in N$ tal que $b = an$, e así, $f(b) = f(an) = f(a)f(n) = f(a)1 = f(a)$, dado que $N < \ker f$. Así, $\bar{f} : G/N \to H$, dada por $\bar{f}(aN) = f(a)$ está ben definida. Ademais, é un homomorfismo: $\bar{f}(aNbN) = \bar{f}(abN) = f(ab) = f(a)f(b) = \bar{f}(aN)\bar{f}(bN)$. Tense que $\operatorname{Im} f = \operatorname{Im} \bar{f}$ e $aN \in \ker \bar{f} \Leftrightarrow f(a) = 1 \Leftrightarrow a \in \ker f$, e así $\ker \bar{f} = \{aN \mid a \in \ker f\} = (\ker f)/N$. Como $\bar{f}$ está completamente determinado por f, é único.

Finalmente, $\bar{f}$ é un epimorfismo se, e só se, f o é. Sábese que $\bar{f}$ é un monomorfismo se, e só se, $\ker \bar{f} = (\ker f)/N$ é o subgrupo trivial de G/N, o que ocorre se, e só se, $\ker f = N$. □

Deste xeito, como consecuencia deste teorema, séguense os teoremas de isomorfía.

Corolario 1.52. *(**Primeiro Teorema de Isomorfía**) Sexa* $f : G \to H$ *un homomorfismo de grupos. Entón* $G/\ker f \cong \operatorname{Im} f$.

Corolario 1.53. *(**Segundo Teorema de Isomorfía**) Dado un grupo* G *de xeito que* $K < G$ *e* $N \triangleleft G$ *tense que* $K/(N \cap K) \cong NK/N$.

Corolario 1.54. *(**Terceiro Teorema de Isomorfía**) Se* G *é un grupo e* $H \triangleleft G$, $K \triangleleft G$ *tales que* $K < H$, *entón* $H/K \triangleleft G/K$ *e* $(G/K)/(H/K) \cong G/H$.

Do primeiro teorema de isomorfía séguese un importante resultado sobre grupos cíclicos.

Corolario 1.55. *Sexa* G *un grupo cíclico. Se é infinito,* $G \cong \mathbb{Z}$, *mentres que se a orde de* G *é* n, $G \cong \mathbb{Z}_n$.

Finalmente, vexamos o teorema de correspondencia, así como un resultado que pode deducirse a partir del.

Teorema 1.56. *(**Teorema de correspondencia**) Dado* $f : G \to H$ *un epimorfismo de grupos, existe unha correspondencia biunívoca entre o conxunto de subgrupos de* G *contendo a* $\ker f$ *e o conxunto de tódolos subgrupos de* H. *Defínese a correspondencia do seguinte xeito:*

$$\begin{array}{rccl} \alpha\colon & \{T \mid T < G, \ker f \subset T\} & \longrightarrow & \{\textit{subgrupos de } H\} \\ & T & \longmapsto & \alpha(T) = f(T) \end{array}$$

Baixo esta correspondencia, os subgrupos normais correspóndense con subgrupos normais.

Como consecuencia deste teorema pode saberse como son os subgrupos dun grupo cociente, feito que queda reflectido no seguinte corolario.

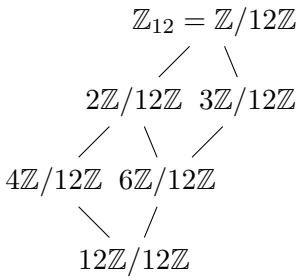
Corolario 1.57. *Se $N \triangleleft G$ con G un grupo, cada subgrupo de G/N é da forma K/N, onde $K < G$ e $N \subset K$. Ademais, K/N é normal en G/N se, e só se, K é normal en G, e neste caso, $(G/N)/(K/N) \cong G/K$.*

Así, por exemplo, pode dicirse como son os subgrupos de $\mathbb{Z}/12\mathbb{Z}$.

Exemplo 1.58. Tense o epimorfismo do paso ao cociente $\pi : \mathbb{Z} \to 12\mathbb{Z}$, que induce entón a correspondencia:

$$\{\text{subgrupos de } \mathbb{Z}/12\mathbb{Z}\} \leftrightarrow \{\text{subgrupos de } \mathbb{Z} \text{ que conteñen a } 12\mathbb{Z}\}$$

Agora ben, os subgrupos de $\mathbb{Z}$ contendo a $12\mathbb{Z}$ son: $T < \mathbb{Z} : T = m\mathbb{Z}$, $12\mathbb{Z} \subset m\mathbb{Z}$, é dicir, $T = m\mathbb{Z}$ con $m|12 \Leftrightarrow m \in \{1, 2, 3, 4, 6, 12\}$. Entón, $T = \{\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}, 12\mathbb{Z}\}$, e deste xeito os subgrupos de $\mathbb{Z}/12\mathbb{Z}$ son:



1.7. Accións de grupos

Analicemos agora algúns conceptos sobre accións de grupos en conxuntos. Posteriormente, relacionaranse estes resultados coa teoría musical. Defínese, pois, que é unha acción dun grupo nun conxunto.

Definición 1.59. Sexa G un grupo e X un conxunto. Unha **acción de G en X** pola esquerda é unha aplicación

$$\begin{array}{rccc} \alpha\colon & G \times X & \longrightarrow & X \\ & (g, x) & \longmapsto & gx \end{array}$$

verificando:

1. 1x=x $\forall x \in X$.
2. $g(hx) = (gh)x \quad \forall x \in X$ e $g, h \in G$.

Tamén se di que X é un G-conxunto.

Observamos que a definición feita é pola esquerda. Non obstante, tamén se pode definir de xeito totalmente análogo a acción dun grupo nun conxunto pola dereita.

Veranse a continuación uns primeiros exemplos.

Exemplo 1.60. É claro que a conxugación nun grupo G é unha acción do grupo en si mesmo:

$$\begin{array}{rccc} \alpha\colon & G \times G & \longrightarrow & G \\ & (g, x) & \longmapsto & gxg^{-1} \end{array}$$

Exemplo 1.61. O grupo G actuando sobre o conxunto $\{H \subset G \mid H < G\}$ coa conxugación:

$$\begin{array}{rccc} \alpha\colon & G \times \{H \subset G \mid H < G\} & \longrightarrow & X \\ & (g, H) & \longmapsto & gHg^{-1} \end{array}$$

O resultado desta operación é o subgrupo conxugado de H por g.

Defínense agora, dada unha acción de G en X, un subconxunto de X e un subgrupo de G, dous conceptos moi importantes na teoría de accións.

Definición 1.62. Sexa unha acción dun grupo G nun conxunto X e $x \in X$. O **subgrupo de isotropía** ou **estabilizador de** x é $G_x := \{g \in G \mid gx = x\}$.

Definición 1.63. Dada unha acción dun grupo G nun conxunto X e $x \in X$, defínese a **órbita de** x como $Gx := \{gx \mid g \in G\}$.

Entón, efectivamente, o subgrupo de isotropía ou estabilizador dun elemento de X é un subgrupo de G; e a órbita dun elemento de X é un subconxunto de X.

Podemos ver cales son o estabilizador e as órbitas nos exemplos dados.

Exemplo 1.64. Con respecto á conxugación por un elemento x do grupo G (Exemplo 1.60), a órbita de x, $Gx = \{gxg^{-1} \mid g \in G\}$, non é máis que a clase de conxugación de x. Pola súa banda, o subgrupo de isotropía de x é $G_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}$, que coincide co **centralizador** de $\{x\}$ en G, entendendo por centralizador dun subconxunto non baleiro X de G o subgrupo $C_G(X) = \{g \in G | gxg^{-1} = x \ \forall x \in X\}$. É dicir, neste caso G_x é o subgrupo de G que deixa invariante x pola conxugación.

Exemplo 1.65. Con respecto ao Exemplo 1.61, o subgrupo de isotropía dun subgrupo H de G é $G_H = \{g \in G \mid gHg^{-1} = H\} = \{g \in G \mid gH = Hg\} = N_G(H)$. É dicir, é o **normalizador** de H en G (subgrupo de G que deixa invariante H pola conxugación). Por outra banda, a órbita de H é $GH = \{\text{conxugados de } H\}$.

Ademais, dada unha acción dun grupo G nun conxunto X pode definirse a relación de equivalencia: $x, y \in X$, $x \sim y \Leftrightarrow \exists g \in G$ tal que $gx = y$. Deste xeito, a órbita dun elemento x é a clase de equivalencia da relación que se acaba de definir $[x] = Gx$. Así, o conxunto das órbitas forma unha partición de X.

Estúdase agora unha relación entre a órbita dun elemento co índice do subgrupo de isotropía de dito elemento no grupo.

Proposición 1.66. *Sexa unha acción de G en X e $x \in X$. Entón, verifícase $|Gx| = (G : G_x)$.*

Agora ben, se o grupo G é finito e actúa sobre X, o seguinte resultado importante dá unha descomposición nas órbitas dos elementos de X.

Proposición 1.67. ***(Fórmula das clases ou descomposición en órbitas)*** *Sexa un grupo G finito actuando sobre X, un conxunto finito. Entón, $|X| = \sum |Gx|$.*

Pode verse como é esta fórmula no Exemplo 1.60.

Exemplo 1.68. Como xa se dixo, tense $Gx = \{gxg^{-1} | g \in G\}$ e $G_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} = C_G(x)$. Agora ben, distínguense dous casos:

- $x \in Z(G) \Rightarrow Gx = \{x\}$ e $G_x = G$.
- $x \notin Z(G) \Rightarrow G_x = C_G(x) = N_{\{x\}}$.

Deste xeito, utilizando que $|X| = \sum |Gx|$ e que $|Gx| = (G : G_x)$, a fórmula será da forma $|G| = |Z(G)| + \sum_{x \in C}(G : N_{\{x\}})$. C é o conxunto de representantes de clases de elementos que non pertencen ao centro de x e $N_{\{x\}} = C_G(x)$ é o centralizador ou normalizador de $\{x\}$.

Para finalizar esta sección, veranse algunhas definicións que resultarán de utilidade no último capítulo.

Definición 1.69. Sexa G un grupo e X un conxunto. Dise que unha acción de G en X é **fiel** se verifica que o único elemento de G con puntos fixos é a identidade. É dicir, se se ten que para $x \in X$ e $g \in G$, $gx = x$ implica que g é o elemento neutro de G.

Pola definición de subgrupo de isotropía dun elemento $x \in X$, nunha acción fiel de G en X, o estabilizador de x é o subgrupo trivial de G. Vexamos un exemplo dunha acción deste tipo.

Exemplo 1.70. Sexa X un conxunto con algunha estrutura. Sexa ademais $Aut(X)$ o grupo de permutacións de X conservando esa estrutura. Entón, a acción $\alpha : Aut(X) \times X \to X$ dada por $\alpha(\sigma, x) = \sigma(x)$ é fiel.

Definición 1.71. Defínese unha **acción transitiva** como unha acción dun grupo G sobre un conxunto X tal que $\forall x_1, x_2 \in X\ \exists g \in G$ de xeito que $gx_1 = x_2$.

Obsérvese que unha acción será entón transitiva cando defina unha única órbita.

Exemplo 1.72. A acción $\alpha : G \times G \to G$ definida por $\alpha(x, y) = xy$ con G grupo é transitiva.

Definición 1.73. Se unha acción dun grupo G nun conxunto X é transitiva e fiel dise que é **regular**.

Exemplo 1.74. Volvendo á acción do exemplo anterior (Exemplo 1.72), tíñase que a acción é transitiva. Ademais, é claro que se $xy = y$, entón x é 1, a identidade do grupo, polo que tamén e fiel. Polo tanto, esta acción é tamén regular.

1.8. Xeradores e relacións. Grupos libres

Nesta última sección, verase como caracterizar un grupo que vén dado de xeito abstracto, é dicir, coa lista dos seus elementos e a táboa multiplicativa. Non obstante, esta descrición do grupo pode sintetizarse de xeito que en vez de tomar todos os seus elementos, tomarase un conxunto de xeradores, e en vez de dar a táboa multiplicativa completa, darase un conxunto de produtos dos que derivarán o resto. Así, chámanse **relacións que definen ao grupo** a este conxunto de ecuacións entre os xeradores, das que resulta a táboa multiplicativa completa. A descrición feita así do grupo denomínase a **presentación do grupo por xeradores e relacións**.

Comézase definindo un grupo libre coma un grupo que verifica unha propiedade universal.

Definición 1.75. Un grupo F dise **libre** con **base** X se $X \subset F$ e ademais se verifica a seguinte propiedade universal: dada unha aplicación $f : X \to G$ con G grupo, existe un único homomorfismo $h : F \to G$ tal que $hi = f$, con i a inclusión de X en F. É dicir, existe un único homomorfismo h que estende f e fai conmutativo o diagrama:

$$\begin{array}{ccc} X & \xhookrightarrow{i} & F \\ & \searrow^{f} & \swarrow_{h} \\ & G & \end{array}$$

En primeiro lugar, verase que o grupo libre definido así é único.

Proposición 1.76. *Sexan F e F' grupos libres con base o conxunto X. Verifícase que F e F' son isomorfos.*

Demostración. Tomando na definición anterior como grupo G o grupo F' e como aplicación f a inclusión i' de X en F', por ser F libre de base X, existe un único homomorfismo $h : F \to F'$ de xeito que $hi = i'$, sendo i a inclusión de X en F.

Razoando de xeito análogo, tómase como grupo G o grupo F, e como aplicación f a inclusión i de X en F. De novo a propiedade universal do grupo libre F' dá a existencia dun único homomorfismo $h' : F' \to F$ tal que $h'i' = i$.

Entón, $hi = i'$ e $h'i' = i$, polo que substituíndo en ambas ecuacións tense $hh'i' = i'$ e $h'hi = i$. Así, hh' e $h'h$ son ambas a identidade, e entón h e h' son isomorfismos. □

A continuación, farase unha construción que proba a existencia de grupos libres. Comézanse dando unha serie de definicións que resultarán de utilidade.

Ao longo desta sección, X será un conxunto, X^{-1} outro conxunto bixectivo con el e disxunto, e $\{1\}$ un conxunto unitario de xeito que $\{1\} \cap (X \cup X^{-1}) = \emptyset$.

Definición 1.77. Unha sucesión $(x_1, x_2, ...)$ con $x_i \in \{1\} \cup X \cup X^{-1}$ e de xeito que $\exists n \in \mathbb{N}$ tal que $x_i = 1$ para todo $i \geq n$ denomínase unha **palabra en** X. En particular, a **palabra baleira** será aquela formada pola sucesión constante $(1, 1, ...)$ e denotarase por 1. Poden pensarse as palabras da forma $x_1^{\lambda_1} \cdots x_n^{\lambda_n}$, onde $x_i \in X$, $\lambda \in \{1, -1, 0\}$ se $1 \leq n - 1$ e $\lambda_n \in \{1, -1\}$.

Obsérvese que esta ortografía dunha palabra é única, xa que dúas series (a_i) e (b_i) son iguais se o son termo a termo.

Definición 1.78. Unha palabra dise que é **reducida** se é a palabra baleira ou é da forma $x_1^{\lambda_1} \cdots x_r^{\lambda_r}$ con $x_i \in X$, $\lambda_i = \pm 1$ e x_i e x_i^{-1} nunca son adxacentes.

Visualicemos estas dúas definicións nun exemplo.

Exemplo 1.79. Se $X = \{x, y, z\}$, xyx e $x^{-1}yzz^{-1}y^{-1}zxz$ son palabras, das cales a primeira é reducida e a segunda non. A palabra reducida desta é $x^{-1}zxz$.

Dúas palabras $u = x_1^{\lambda_1} \cdots x_n^{\lambda_n}$ e $v = y_1^{\mu_1} \cdots y_l^{\mu_l}$ poden multiplicarse definindo o produto de ambas como $uv = x_1^{\lambda_1} \cdots x_n^{\lambda_n} y_1^{\mu_1} \cdots y_l^{\mu_l}$. Pero hai un problema, e é que esta multiplicación non define un produto como tal no conxunto das palabras reducidas sobre X, posto que o produto de dúas palabras reducidas non ten por que selo tamén. Para emendar isto defínese unha nova multiplicación de palabras reducidas, o que se coñece por **xustaposición**, entendendo por tal pegar dúas palabras reducidas e facer a reducida da palabra resultante. Vexámolo nun exemplo.

Exemplo 1.80. Sexa $X = \{x, y, z\}$, e considérense as palabras xyx, $x^{-1}yx^{-1}z$ e $z^{-1}xy^{-1}$. Entón, terase que o produto da primeira e da segunda sería $xyxx^{-1}yx^{-1}z$, que non é unha palabra reducida, pero a xustaposición desas dúas palabras sería $xyyx^{-1}z$, que si que é reducida. A xustaposición da segunda e da terceira será, de xeito análogo, x^{-1}.

Imos probar que o conxunto de palabras reducidas con esta operación que se acaba de definir é un grupo.

Teorema 1.81. *Para cada conxunto X, existe un grupo libre F de base X.*

Demostración. Denótase por F o conxunto das palabras reducidas sobre o conxunto e como operación en F considérase a xustaposición. A palabra baleira é a identidade para a xustaposición, e a inversa dunha palabra reducida $x_1^{\lambda_1} \cdots x_n^{\lambda_n}$ sería $x_n^{-\lambda_n} \cdots x_1^{-\lambda_1}$, que é tamén reducida, polo que só falta probar a asociatividade. Esta proba podería facerse por indución distinguindo casos como fai o texto de Carstensen, Fine e Rosenberger [2]. Porén, resulta unha demostración pesada, e por iso se fará seguindo a idea de van der Waerden.

Sexa $x \in X$ arbitrario e $(x_1^{\lambda_1}, ..., x_n^{\lambda_n}) \in F$, é dicir, unha palabra reducida. Entón, tómanse as funcións $|x^\lambda| : F \to F$, con $\lambda = \pm 1$ que se definen do seguinte xeito:

$$|x^\lambda|(x_1^{\lambda_1}, ..., x_n^{\lambda_n}) = \begin{cases} x^\lambda x_1^{\lambda_1} \cdots x_n^{\lambda_n}, \text{ se } x^\lambda \neq x_1^{-\lambda_1} \\ x_2^{\lambda_2} \cdots x_n^{\lambda_n}, \text{ se } x^\lambda = x_1^{-\lambda_1} \end{cases}$$

Observamos que $|x| \circ |x^{-1}| = |x^{-1}| \circ |x| = 1_F$, é dicir, son a identidade en F. Entón, $|x|$ e $|x^{-1}|$ son permutacións de F que ademais son inversas entre si. Consideremos o grupo simétrico de F, S_F, e F_0 o subgrupo de S_F xerado por $\{|x| : x \in X\}$. Veremos que F_0 é libre con base $\{|x| : x \in X\}$.

Tense unha bixección $\chi : \{|x| : x \in X\} \to X$ dada por $\chi(|x|) = x$. En primeiro lugar, un elemento $h \in F_0$ arbitrario, con $h \neq 1_F$, pode factorizarse da forma

$$g = |x_1^{\lambda_1}| \circ |x_2^{\lambda_2}| \circ \cdots \circ |x_n^{\lambda_n}| \tag{1.1}$$

cos elementos $|x^{\lambda_i}|$ e $|x^{-\lambda_i}|$ nunca adxacentes e $\lambda_i = \pm 1$. Como $g(1) = x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$ e como a ortografía dunha palabra reducida é única, esta factorización é única.

Agora, para ver que F_0 é un grupo libre con base $\{|x| : x \in X\}$, consideremos unha aplicación $f : \{|x| : x \in X\} \to G$ con G grupo. Defínese unha aplicación $h : F_0 \to G$ que virá dada por $f(|x_1^{\lambda_1}| \circ \cdots \circ |x_n^{\lambda_n}|) = f(|x_1|)^{\lambda_1} \cdots f(|x_n|)^{\lambda_n}$. Pola unicidade de factorización dun elemento $g \in F_0$ dada pola ecuación 1.1, a función h está ben definida e estende f.

Tense entón o seguinte diagrama conmutativo.

$$\begin{array}{ccc} \{|x| : x \in X\} & \xhookrightarrow{i} & F_0 \\ \downarrow{\scriptstyle f} & \swarrow{\scriptstyle h} & \\ G & & \end{array}$$

Agora ben, como F_0 está xerado por $\{|x| : x \in X\}$, é suficiente probar que h é un homomorfismo. A unicidade deducirase de que dous homomorfismos que coinciden nun conxunto de xeradores son o mesmo.

Sexan, pois, u e v elementos de F_0, é dicir, palabras reducidas sobre $\{|x| : x \in X\}$. Se uv é reducida, é claro que $h(uv) = h(u)h(v)$. Se non, u e v son da forma $u = u' \circ w$ e $v = w^{-1} \circ v'$ con $u'v'$ reducida. Por ser u e v reducidas, $h(u) = h(u')h(w)$ e $h(v) = h(w^{-1})h(v') = h(w)^{-1}h(v')$, e así $h(u)h(v) = h(u')h(w)h(w)^{-1}h(v') = h(u')h(v')$. Agora ben, por ser $u'v'$ reducida, $h(u')h(v') = h(u'v') = h(uv)$. Entón chégase a que, efectivamente, h é un homomorfismo.

Como se verifica a propiedade universal da Definición 1.75, viuse que F_0 é un grupo libre con base $\{|x| : x \in X\}$.

Por outra banda, sexa $\bar{\chi} : F_0 \to F$ con $\bar{\chi}(|x_1^{\lambda_1}| \circ |x_2^{\lambda_2}| \circ \cdots \circ |x_n^{\lambda_n}|) = x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$. $\bar{\chi}$ é bixectiva, e ademais $\bar{\chi}(\{|x| : x \in X\}) = \chi(\{|x| : x \in X\}) = X$.

$$\begin{array}{ccc} \{|x| : x \in X\} & \xhookrightarrow{i'} & F_0 \\ \downarrow{\scriptstyle \chi} & & \downarrow{\scriptstyle \bar{\chi}} \\ X & \xhookrightarrow{i} & F \end{array}$$

Sábese que se G é un grupo, X un conxunto e $f : G \to X$ unha bixección, existe unha única operación en X tal que X é grupo e f é un isomorfismo. Con este resultado tense que considerando a xustaposición en f e por definición de $\bar{\chi}$, $\bar{\chi}$ é un isomorfismo. Entón, F é un grupo isomorfo a F_0.

Ademais, F é libre con base X: dado G grupo e $f : X \to G$ aplicación, consideramos $f\chi$ e como F_0 é libre sobre $\{|x| : x \in X\}$, existe un único homomorfismo $h : F_0 \to G$ de xeito que $hi' = f\chi$, sendo i' a inclusión de $\{|x| : x \in X\}$ en F_0. Entón, sexa $h_1 : F \to G$ con $h_1 = h\bar{\chi}^{-1}$. Se i é a inclusión de X en F, tense que $h_1 i = f$, xa que $h_1 i = h\bar{\chi}^{-1} i = hi'\chi^{-1} = f\chi\chi^{-1} = f$. Por outra banda, se $h_2 : F \to G$ é tal que $h_2 i = f$, entón $h_2 i\chi = f\chi$, e así $h_2\bar{\chi}i' = f\chi = hi$. Agora ben, como h é o único homomorfismo que verifica $hi' = f\chi$, entón $h_2\bar{\chi} = h \Rightarrow h_2 = h\bar{\chi}^{-1} = h_1 \Rightarrow h_1 = h_2$, e polo tanto $h_1 : F \to G$ é o único homomorfismo de xeito que $h_1 i = f$, e queda así visto que F é un grupo libre sobre X.

Por último, cabe destacar que X xera F xa que $\{|x| : x \in X\}$ xera F_0. □

Desta proposición, séguese un importante resultado.

Corolario 1.82. *Un grupo G calquera é imaxe homomórfica dun grupo libre. Entón, G é cociente dun grupo libre F, é dicir, $G = F/N$.*

Demostración. Sexa G un grupo, X un conxunto de xeradores de G e F o grupo libre sobre o conxunto X. Dadas as inclusións $j : X \hookrightarrow F$ e $i \hookrightarrow G$, por ser F libre existe un único homomorfismo $h : F \to G$ de xeito que $hj = i$. Agora, como $G = \langle G \rangle$, tense que h é un epimorfismo, xa que para $g \in G$ arbitrario, $g = x_1^{\lambda_1} \cdots x_n^{\lambda_n} = h(x_1^{\lambda_1} \cdots x_n^{\lambda_n})$. Así, polo primeiro teorema de isomorfía, $G \cong F/\ker h$. □

Podemos agora ver dado un grupo arbitrario, que se entende por presentación do grupo.

Definición 1.83. Sexa X un conxunto e Y un conxunto de palabras reducidas en X. Dirase que un grupo G está definido polos **xeradores** X, e as **relacións** Y se $G \cong F/R$, sendo F o grupo libre xerado por X e R o subgrupo normal de F xerado por Y. Unha **presentación** de G é un par da forma $\langle X \mid Y \rangle$.

Coas notacións do corolario anterior (Corolario 1.82), tíñase que $G \cong F/\ker h$, sendo $\ker h = \{(a_1, ..., a_r) \mid a_1 \cdots a_r = 1\}$ con a_i ou $a_i^{-1} \in X$. Así, $\ker h$ é o subgrupo de relacións, e a presentación de G será da forma $G = \langle X \mid \ker h \rangle$.

Vexamos algúns exemplos de presentacións de grupos.

Exemplo 1.84. Sexa a presentación $\langle a, b \mid b^2a = b, ba^2b = a \rangle$ e probemos que é unha presentación do grupo trivial. Como $b^2a = b$, multiplicando por b^{-1} pola esquerda obtense $ba = 1$. Substituíndo na segunda ecuación terase $ba^2b = a \Leftrightarrow (ba)(ab) = a \Rightarrow ab = a$. Se agora se multiplica esta expresión por a^{-1} pola esquerda, obterase $b = 1$, e como se tiña $ba = 1$, entón tamén se deduce que $a = 1$, e así o grupo obtido é, efectivamente, o trivial.

Tense, pois, que un grupo G está determinado, salvo isomorfismos, por un sistema de xeradores e un conxunto de relacións. Inversamente, dado un conxunto X e un conxunto Y de palabras reducidas sobre X, pode construírse un grupo que ten a X como conxunto de xeradores e no que se satisfán tódalas relacións de Y. A construción é a seguinte:

Sexa X o conxunto dado, F o grupo libre sobre X e N o subgrupo normal de F xerado por Y. Tense así $X \hookrightarrow F \to F/N = G$. Identificando X coa imaxe en F/N, G está xerado por X e en G satisfanse tódalas relacións.

Polo visto ata o de agora, o grupo definido por xeradores e relacións dados sempre existe. A continuación verase que é o grupo máis grande posible no seguinte senso.

Teorema 1.85. *(Van Dyck) Sexa G un grupo definido polos xeradores dun conxunto X e as relacións doutro conxunto Y de palabras reducidas de X. É dicir, G está definido polos xeradores*

$x \in X$ e as relacións $u = 1$ para $u \in Y$. Entón, se H é un grupo tal que está xerado por X e verifica as relacións de Y, hai un epimorfismo $G \to H$.

Demostración. Sexa F o grupo libre sobre X. Polo tanto, como $H = \langle X \rangle$, tense a inclusión de X en H. Como F é libre sobre X, pode estenderse cun homomorfismo sobrexectivo $h : F \to H$. Agora ben, tamén se ten que H verifica as relacións de Y, é dicir, se $u \in Y$, tense $u = 1$, e entón $Y \subset \ker h$. Entón, o subgrupo normal N xerado por Y en F está contido en $\ker h$. Como $N \triangleleft F$, $1 \triangleleft H$ e $h : F \to H$ é tal que $h(N) = 1$, existe un homomorfismo sobrexectivo $\bar{h} : F/N \to H$. Así, $G \cong F/N \to H$ é un epimorfismo. □

A continuación, veranse algúns exemplos de grupos definidos por xeradores e relacións que serven para clarificar a clase de razoamentos usados para estudar unha presentación.

Exemplo 1.86. Sexa G o grupo xerado polos elementos s, t verificando as relacións $s^2 = 1$, $t^3 = 1$, e $stst = 1$.

O grupo diédrico D_3 de orde 6, que xa se definiu no Exemplo 1.5, está xerado por dous elementos s, t satisfacendo estas relacións, e polo tanto polo teorema anterior existe un epimorfismo $\phi : G \to D_3$. Así, é claro que $|G| \geq |D_3| = 6$.

Agora sexa F o grupo libre sobre $\{s, t\}$ e N o subgrupo normal xerado por $\{s^2, t^3, stst\}$. Pode verse que todo elemento de F/N é da forma st^jN con $o \leq i \leq 1$, $0 \leq j \leq 2$, polo que como $G \cong F/N$, $|G| = |F/N| \leq 6$. Entón $|G| = 6$ e ϕ é un isomorfismo.

Polo tanto, o grupo definido por eses xeradores e esas relacións é isomorfo a D_3.

En xeral, a presentación por xeradores e relacións do grupo diédrico D_n de orde $2n$ será da forma $\langle s, t \mid t^n = s^2 = (ts)^2 = 1 \rangle$.

Razoemos de xeito análogo para ver cal é a presentación do grupo dos cuaternios de orde 8, do que xa se falou anteriormente (Exemplo 1.9).

Exemplo 1.87. Sexa o grupo G xerado por x e y coas relacións $x^4 = 1$, $x^2y^{-2} = 1$ e $xyxy^{-1} = 1$.

Agora ben, coma os elementos que xeran Q_8 satisfán estas relacións, polo teorema anterior, existe un epimorfismo $\phi : G \to Q_8$, e polo tanto tense que $|G| \geq |Q_8| = 8$.

Sexa F o grupo libre sobre $\{x, y\}$ e N o subgrupo normal xerado por $\{x^4, x^2y^{-2}, xyxy^{-1}\}$. Pode probarse que todo elemento de F/N será da forma a^ib^jN con $0 \leq i \leq 3$ e $0 \leq j \leq 1$. Deste xeito, $|G| = |F/N| \leq 8$. Entón, $|G| = 8$ e ϕ é un isomorfismo.

Polo tanto, o grupo definido por eses xeradores e esas relacións é isomorfo a Q_8.

Entón, o grupo dos cuaternios ten presentación $Q_8 = \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1} \rangle$. Non obstante, pode verse que tamén ten presentación $\langle x, y \mid xyx = y, x^2 = y^2 \rangle$.

Exemplo 1.88. $\mathbb{Z}_6$ ten presentacións $\mathbb{Z}_6 = \langle x \mid x^6 = 1 \rangle = \langle x, y \mid x^2 = y^3 = x^{-1}y^{-1}xy = 1 \rangle$.

Obsérvese que, como se ve nestes exemplos, presentacións distintas poden dar lugar a grupos isomorfos, o que se coñece como **presentacións isomorfas**. Cabe destacar que o problema de decidir cando dúas presentacións son isomorfas pode ser moi complicado, e en xeral non será resoluble.

Capítulo 2

O grupo simétrico

Neste capítulo centrarémonos no grupo simétrico e nas súas características principais, e máis adiante veremos que ten unha gran relación coa teoría musical. Para comezar, estudarase o que é unha permutación, certos tipos de permutacións como son os ciclos e as transposicións e verase o teorema de Cayley. Chegarase a resultados importantes, como que toda permutación se pode factorizar nun produto de transposicións, e que aínda que esta factorización non sexa única, a paridade do número de transposicións non cambia. Así, verase o que son as permutacións pares e impares. Estudaranse as clases de conxugación do grupo simétrico, e finalmente verase unha presentación deste grupo por xeradores e relacións. A bibliografía empregada ao longo deste capítulo volve ser a dos textos de Rotman [12], Cohn [3] e Hungerford [8]. Tamén se empregaron os textos de Dorronsoro [5], de Fraleigh [7], James [9] e Ledermann [10].

2.1. Permutacións

Definición 2.1. Dado un conxunto X, unha **permutación** en X é unha aplicación bixectiva $f : X \to X$.

Con esta información, pode definirse o grupo simétrico sobre un conxunto X como segue.

Definición 2.2. Se X é un conxunto, entón $S_X = \{f : X \to X \mid f \text{ é aplicación bixectiva}\}$ coa composición é un grupo, o **grupo simétrico** $(S_X, \circ)$.

Se na definición anterior se ten $X = \{1, 2, ..., n\}$, entón o grupo simétrico denótase por S_n e chámase **grupo simétrico de** n **elementos**. Ademais se $\sigma \in S_n$ escribirase:

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix} \tag{2.1}$$

O grupo S_n ten orde $n!$.

Os elementos que quedan invariantes non adoitan escribirse. Por exemplo:

Exemplo 2.3. A permutación $\sigma = \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix} \in S_4$ denota á permutación $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$.

Introdúcese a continuación a noción de ciclo, un tipo de permutación.

Definición 2.4. Un **ciclo** ou **permutación circular de orde r** é unha permutación $\sigma \in S_n$ con r elementos $\{a_1, ..., a_r\}$ non invariantes, e tal que $\sigma(a_1) = a_2, \sigma(a_2) = a_3, ..., \sigma(a_r) = a_1$. É dicir, $\sigma(a_i) = a_{i+1}$ para $i = 1, ..., r-1$ e $\sigma(a_r) = a_1$.

Adoitan denotarse estes ciclos como $\sigma = (a_1, ..., a_r)$.

Cando a orde do ciclo é 2, a permutación chámase transposición; que non é máis ca o intercambio de dous elementos. Así,

Definición 2.5. Unha **transposición** é un ciclo de orde 2.

Definición 2.6. Dúas permutacións σ_1, σ_2 dinse **disxuntas** se cada valor que unha deixa non invariante a outra o deixa fixo.

É dicir, dados dous ciclos $\sigma_1 = (a_1, ..., a_n)$ e $\sigma_2 = (b_1, ..., b_m)$ dirase que son disxuntos se se verifica que $\{a_1, ..., a_n\} \cap \{b_1, ..., b_m\} = \emptyset$.

En xeral, o grupo simétrico non é conmutativo, vexámolo nun exemplo.

Exemplo 2.7. Sexan

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 5 & 1 & 4 & 7 & 9 & 12 & 11 & 8 & 2 & 6 & 10 \end{pmatrix} \in S_{12}$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 2 & 1 & 6 & 11 & 9 & 10 & 4 & 5 & 3 & 12 & 8 \end{pmatrix} \in S_{12}$$

Tense que

$$\sigma \circ \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 5 & 3 & 9 & 6 & 8 & 2 & 4 & 7 & 1 & 10 & 11 \end{pmatrix}$$

$$\gamma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 11 & 7 & 6 & 10 & 5 & 8 & 12 & 4 & 2 & 9 & 3 \end{pmatrix}$$

Entón, claramente, $\sigma \circ \gamma \neq \gamma \circ \sigma$, e así vese que S_{12} non é conmutativo. Vexamos agora un resultado xeral para S_n

Proposición 2.8. *S_n non é abeliano para $n \geq 3$.*

Demostración. Precisamos atopar dúas permutacións $\alpha, \beta \in S_n$ tales que $\alpha\beta \neq \beta\alpha$. Consideremos pois:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & ... & n \\ 1 & 3 & 2 & 4 & 5 & ... & n \end{pmatrix} \in S_n \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & ... & n \\ 3 & 2 & 1 & 4 & 5 & ... & n \end{pmatrix} \in S_n$$

Tense entón que

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & ... & n \\ 2 & 3 & 1 & 4 & 5 & ... & n \end{pmatrix} \neq \beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & ... & n \\ 3 & 1 & 2 & 4 & 5 & ... & n \end{pmatrix}$$

□

Non obstante, cando os ciclos son disxuntos pode verse que estes si conmutan.

Proposición 2.9. *Se σ_1 e σ_2 son ciclos disxuntos de S_n, terase que estes conmutan. Isto é, $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.*

Demostración. Denotemos os ciclos por $\sigma_1 = (a_1, ..., a_n)$ e $\sigma_2 = (b_1, ..., b_m)$. Deste xeito, se $1 \leq j < n$, tense que $\sigma_2 \circ \sigma_1(a_j) = \sigma_2(a_{j+1}) = a_{j+1}$ e $\sigma_1 \circ \sigma_2(a_j) = \sigma_1(a_j) = a_{j+1}$, debido a que $a_j, a_{j+1} \notin \{b_1, ..., b_m\}$. Ademais, $\sigma_2 \circ \sigma_1(a_n) = \sigma_2(a_1) = a_1$ e $\sigma_1 \circ \sigma_2(a_n) = \sigma_1(a_n) = a_1$. Razoando de xeito análogo cos b_j, chégase ao mesmo resultado. Agora ben, como σ_1 e σ_2 deixan fixos aos elementos x tales que $x \notin \{a_1, ..., a_n\} \cup \{b_1, ..., b_m\}$ queda probado o resultado. □

A existencia dunha acción dun grupo sobre un conxunto permítenos obter o resultado expresado na proposición seguinte, da que o teorema de Cayley vai ser unha consecuencia importante.

Proposición 2.10. *Sexa G un grupo que actúa sobre un conxunto X. Existe un homomorfismo de grupos de G en S_X.*

Demostración. Para cada elemento de G, defínese $\theta(g)$ como a aplicación que a un x de X lle fai corresponder $\theta(g)(x) = gx$. Como $x = g(g^{-1}x)$ para todo $x \in X$, $\theta(g)$ é sobrexectiva. $\theta(g)$ tamén é inxectiva: para $x, y \in X$, terase que $gx = gy$, e polo tanto, $x = g^{-1}(gx) = g^{-1}(gy) = y$. Entón, $\theta(g)$ é unha bixección, ou o que é o mesmo, unha permutación de X. Finalmente, a aplicación $G \to S_X$ que a cada $g \in G$ lle fai corresponder $\theta(g)$ é un homomorfismo de grupos debido a que $\theta(g_1 g_2) = \theta(g_1)\theta(g_2)$ para todos $g_1, g_2 \in G$. □

Como consecuencia:

Corolario 2.11. *(de Cayley) Todo grupo G é isomorfo a un subgrupo dun grupo simétrico. En particular, se G é finito, G é isomorfo a un subgrupo dun grupo simétrico de n elementos.*

Agora, estudarase que toda permutación pode escribirse como produto de ciclos.

Proposición 2.12. *Toda permutación σ de S_n é ou ben un ciclo, ou ben pode descompoñerse en produto de ciclos disxuntos (de orde polo menos 2). Esta descomposición é única, salvo a orde dos ciclos e o seu primeiro elemento.*

Demostración. Vexamos en primeiro lugar que pode descompoñerse σ en produto de ciclos. Tomando de xeito recursivo $1 = \sigma^0(1)$, $\sigma(1)$, $\sigma^2(1) = \sigma(\sigma(1)), ..., \sigma^n(1) = \sigma(\sigma^{n-1}(1))$, téñense $n+1$ elementos, e como $\sigma \in S_n$, só hai n imaxes posibles. Entón, terase que hai polo menos unha repetición, é dicir $\exists j, k \in \{0, ..., n\}$, $j \neq k$ (tomemos sen perda de xeneralidade $k > j$) de xeito que $\sigma^j(1) = \sigma^k(1)$. Así, $\sigma^{k-j}(1) = 1$, onde $0 < k - j \leq n$, e entón tomando m_1 coma o menor enteiro positivo verificando que $\sigma^{m_1}(1) = 1$, defínese $\sigma_1 = (1, \sigma(1), ..., \sigma^{m_1-1}(1))$.

Tomemos agora un elemento $x \in \{1, ..., n\}$ de xeito que $x \notin \{1, \sigma(1), ..., \sigma^{m_1-1}\}$. Repítese o procedemento anterior, atopando o menor enteiro positivo m_2 verificando que $\sigma^{m_2}(x) = x$. Terase entón $\sigma_2 = (x, \sigma(x), ..., \sigma^{m_2-1}(x))$.

Repetindo o procedemento ata rematar cos n elementos de $\{1, ..., n\}$, obtense unha cantidade finita, r, de ciclos $\sigma_1, ..., \sigma_r$ de xeito que $\sigma = \sigma_r \circ ... \circ \sigma_1 = \sigma_r \cdots \sigma_1$.

Os ciclos obtidos seguindo este procedemento son disxuntos, como se ve a continuación. Probemos que, por exemplo, σ_1 e σ_2 son disxuntos. Se $\sigma^j(1) = \sigma^s(x)$, terase que $\sigma^{j-s}(1) = x$, e polo tanto $x \in \{1, \sigma(1), ..., \sigma^{m_1-1}(1)\}$, o que é unha contradición coa elección feita anteriormente. Entón, os ciclos son disxuntos, e pola Proposición 2.9, conmutan. Deste xeito, a descomposición de σ non se ve afectada pola orde dos ciclos.

Por último, vexamos que a elección do primeiro elemento é arbitraria, ou o que é o mesmo, non inflúe na descomposición en ciclos. É dicir, se $y = \sigma^j(x)$ con $0 < j < m_2$, hai que ver que $\sigma_2 = (x, \sigma(x), ..., \sigma^{m_2-1}(x))$ é igual a $\tilde{\sigma_2} = (y, \sigma(y), ..., \sigma^{m_2-1}(y))$.

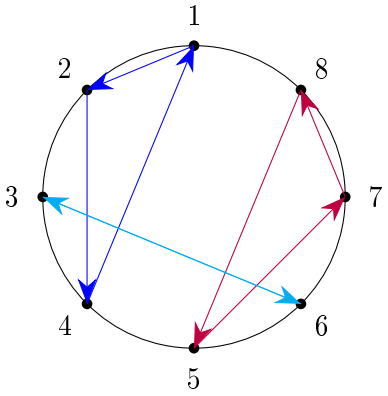
Agora ben, $\tilde{\sigma_2}(y) = \sigma(y) = \sigma^{j+1}(x) = \sigma_2(\sigma^j(x)) = \sigma_2(y)$. En xeral $\forall s, 1 \leq s \leq m_2 - 1$, $\tilde{\sigma_2}(\sigma^s(y)) = \sigma^{s+1}(y) = \sigma^{s+1+j}(x) = \sigma_2(\sigma^{s+j}(x)) = \sigma_2(\sigma^s(y))$. □

Unha forma moi sinxela de visualizar este resultado é representar nun círculo os n elementos $\{1, ..., n\}$ e ver como actúa unha permutación neste conxunto. Vexámolo nun exemplo.

Exemplo 2.13. Sexa a permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 1 & 7 & 3 & 8 & 5 \end{pmatrix}$$

É claro que $\sigma = (1,2,4)(3,6)(5,7,8)$, o que se representa do seguinte xeito:



Como resultado da proposición anterior tense o seguinte corolario.

Corolario 2.14. *A orde dunha permutación $\sigma \in S_n$ é o mínimo común múltiplo das ordes dos seus ciclos disxuntos.*

Demostración. Sexa $\sigma = \sigma_1 \cdots \sigma_r$ a descomposición de σ en ciclos disxuntos. Agora ben, os ciclos disxuntos conmutan, e polo tanto terase que $\sigma^s = \sigma_1^s \cdots \sigma_r^s \ \forall s \in \mathbb{Z}$. Ademais, $\sigma^s = (1) \Leftrightarrow \sigma_i^s = (1)$ $\forall i \in \{1, ..., r\}$. Deste xeito, $\sigma^s = (1) \Leftrightarrow |\sigma_i|$ divide a s para cada i. Finalmente, como $|\sigma|$ é o mínimo de xeito que $\sigma^{|\sigma|} = (1)$ obtense o resultado. □

Xa se viu que toda permutación se pode descompoñer en produto de ciclos disxuntos (Proposición 2.12). Non obstante, pode irse máis lonxe e probar que toda permutación se pode escribir coma produto de transposicións. Para iso, só compre ver que todo ciclo se pode descompoñer en produto de transposicións.

Proposición 2.15. *Todo ciclo pode descompoñerse nun produto de transposicións. En conclusión, toda permutación pode escribirse como produto de transposicións.*

Demostración. É sinxelo ver que $(x_1) = (x_1, x_2)(x_1, x_2)$, e deste xeito para $r > 1$ tense

$$(x_1, x_2, ..., x_r) = (x_1, x_r)(x_1, x_{r-1}) \cdots (x_1, x_3)(x_1, x_2).$$ □

Outra posible descomposición é $(x_1, x_2, x_3, ..., x_{n-1}, x_n) = (x_1, x_2)(x_2, x_3) \cdots (x_{n-1}, x_n)$. Vexamos un exemplo dunha permutación con máis dunha factorización.

Exemplo 2.16. $(1,2,3) = (1,3)(1,2) = (2,3)(1,3) = (1,3)(4,2)(1,2)(1,4)$.

Entón, como acaba de verse, a factorización non é única. Non obstante, o número de transposicións que aparece na factorización dunha permutación é sempre o mesmo módulo 2. É dicir, dito número é sempre par ou impar.

Ademais, as transposicións nas que se factoriza unha permutación non teñen por que conmutar. Vexamos un exemplo:

Exemplo 2.17. $(1,2,3) = (1,3)(1,2) \neq (1,2)(1,3)$.

2.2. Permutacións pares e impares

Analizarase que a paridade dunha permutación é sempre a mesma. Cabe destacar que a proba deste resultado atopada en bastantes libros fai uso dunha construción artificiosa, polo que resulta bastante complicada. A demostración que se verá será a que segue o libro de Fraleigh [7]. Para iso, deben primeiro introducirse algunhas nocións.

Sexa $\sigma \in S_n$. Entón, para cada $i, j \in \{1, ..., n\}$ pode definirse unha relación de equivalencia: $i \sim j \Leftrightarrow \exists s \in \mathbb{Z}$ tal que $j = \sigma^s(i)$.

Efectivamente, vexamos que a relación que acaba de definirse é de equivalencia. É reflexiva, xa que $i = id(i) = \sigma^0(i)$, e polo tanto $i \sim i$. Tamén se verifica que é simétrica, pois se $i \sim j$, entón tense que $\exists s \in \mathbb{Z}$ tal que $j = \sigma^s(i)$, e polo tanto $\exists -s \in \mathbb{Z}$ tal que $i = \sigma^{-s}(j)$, e entón $j \sim i$. Finalmente, a relación tamén é transitiva, pois se $i \sim j$ e $j \sim k$, entón $\exists s, r \in \mathbb{Z}$ tal que $j = \sigma^s(i)$ e $k = \sigma^r(j)$. Deste xeito, $k = \sigma^r(j) = \sigma^r(\sigma^s(i)) = \sigma^{r+s}(i)$, ou o que é o mesmo, $\exists r + s \in \mathbb{Z}$ tal que $k = \sigma^{r+s}(i)$, e polo tanto, $i \sim k$.

Defínense nesta relación de equivalencia as súas clases.

Definición 2.18. Sexa $\sigma \in S_n$. Denominamos **órbitas** de σ ás clases de equivalencia en $\{1, ..., n\}$ coa relación que acaba de verse.

Cabe destacar que este concepto de órbita coincide co que xa se mencionou en accións de grupos (Definición 1.63). As órbitas de σ son as clases coa relación $i \sim j \Leftrightarrow \exists m \in \mathbb{Z}$ tal que $\sigma^m(i) = j$. É dicir, $[i] = \{\sigma^r(i) \mid r \in \mathbb{Z}\}$. Entón, considerando a acción do grupo cíclico xerado pola permutación σ, $\langle\sigma\rangle$ sobre o conxunto $\{1, ..., n\}$, que a un par (σ^r, i) lle fai corresponder $\sigma^r(i)$, terase que as órbita de σ que se acaban de definir coinciden coas órbitas desta acción.

Observemos un exemplo de órbitas dunha permutación particular.

Exemplo 2.19. A permutación identidade en S_n é aquela que deixa fixos os n elementos, e polo tanto terá n órbitas que consisten nos subconxuntos unitarios de $\{1, ..., n\}$.

Despois desta definición, pode facerse unha revisión do visto anteriormente. Deste xeito, pode darse unha definición alternativa de ciclo, que é unha permutación que ten ao sumo unha órbita con máis dun elemento. A orde dun ciclo é o máximo dos números de elementos das súas órbitas. Con respecto á factorización dunha permutación en ciclos disxuntos, xa se viu que era única salvo a orde dos ciclos e o seu primeiro elemento. Isto ten sentido debido a que as órbitas dunha permutación son únicas.

Vexamos agora un lema útil para posteriormente ver que a paridade do número de transposicións dunha permutación é sempre a mesma.

Lema 2.20. *Sexan $\sigma \in S_n$ e $\tau \in S_n$ unha transposición. O número de órbitas de σ difire do de $\tau\sigma$ nunha unidade.*

Demostración. Denotemos $\tau = (i, j)$. Esencialmente hai dous casos. Por unha banda, se i, j pertencen a órbitas distintas de σ, τ crea unha especie de unión entre elas, de xeito que $\tau\sigma$ terá unha órbita menos ca σ. Por outra banda, se i, j pertencen á mesma órbita de σ, τ vai separala en dúas órbitas en $\tau\sigma$, de xeito que terá unha órbita máis ca σ. Ademais, a multiplicación de σ por τ deixará fixas ás órbitas que non conteñen nin a i nin a j.

Sexa en primeiro lugar σ de xeito que i e j están en órbitas distintas. Factorízase σ nun produto de r ciclos disxuntos:

$$\sigma = (u, ..., a, i, ..., v)(x, ..., b, j, ..., y)\sigma_3 \cdots \sigma_r,$$

onde $\sigma_1 = (u, ..., a, i, ..., v)$ e $\sigma_2 = (x, ..., b, j, ..., y)$ son os ciclos contendo i e j. Tense entón $\tau\sigma_1\sigma_2 = (i, j)(u, ..., a, i, ..., v)(x, ..., b, j, ..., y) = (u, ..., a, j, ..., y, x, ..., b, i)$, e así a órbita de i e a de j únense nunha soa.

Por outra banda, se i e j están na mesma órbita de σ, terase outra vez a factorización de σ en produto de ciclos disxuntos:

$$\sigma = (x, ..., a, i, ..., b, j, ..., y)\sigma_2 \cdots \sigma_r,$$

onde $\sigma_1 = (x, ..., a, i, ..., b, j, ..., y)$ é o ciclo que contén a i e a j. Neste caso tense polo tanto que $\tau\sigma_1 = (i, j)(x, ..., a, i, ..., b, j, ..., y) = (x, ..., a, j, ..., y)(i, ..., b)$, e como consecuencia σ_1 queda dividido en dous ciclos disxuntos, é dicir, en dúas órbitas.

Chégase así ao resultado do lema. □

Teorema 2.21. *As permutacións en S_n non poden expresarse simultaneamente coma o produto dun número par de transposicións e dun número impar delas.*

Demostración. Supoñamos que $\sigma \in S_n$ pode expresarse simultaneamente coma o produto dun número impar de permutacións e coma o produto dun número par delas, para así tratar de chegar a

unha contradición. Deste xeito, como $(a,b)^{-1} = (a,b)$, terase que o inverso dun produto de transposicións é o produto das mesmas transposicións na orde inversa, é dicir, $[(a,b)(c,d)\cdots(x,y)]^{-1} = (x,y)\cdots(c,d)(a,b)$. Entón, como σ pode expresarse coma o produto dun número par e dun número impar de transposicións, o mesmo ocorrerá con σ^{-1}.

Tomemos o produto $\sigma\sigma^{-1} = id$, onde se expresou σ cun número par de transposicións, σ^{-1} cun número impar delas, e id representa a permutación identidade. Deste xeito, tense que $\sigma_{2r+1}\sigma_{2r}\cdots\sigma_2\sigma_1 = id$, onde observamos que temos á permutación identidade id expresada coma o produto dun número impar de transposicións. Multiplicando a parte da esquerda pola identidade, terase que $\sigma_{2r+1}\sigma_{2r}\cdots\sigma_2\sigma_1 id = id$, onde como xa se dixo, as σ_i son transposicións. Estamos agora en condicións de utilizar o lema anterior. Entón, aplicando o lema varias veces, obtense que o número de órbitas de id difire nun número impar co número de órbitas de id. Como o número de órbitas de id é n, chégase entón a unha contradición, que xorde ao supoñer que se pode expresar σ coma o produto dun número par e dun número impar de transposicións. □

A partir deste resultado, pode introducirse unha definición dependendo da descomposición en transposicións dunha permutación.

Definición 2.22. Dada unha permutación σ, o seu **signo** ou **signatura** é $sig(\sigma) := (-1)^n$, (sendo n o número de transposicións na factorización de σ) e deste xeito, $sig(\sigma) \in \{\pm 1\}$. Ademais, cando $sig(\sigma) = 1$, dise que σ é **par** (ten un número par de transposicións); mentres que cando $sig(\sigma) = -1$, σ é **impar** (ten un número impar de transposicións).

Á súa vez, a partir desta definición pódese introducir un subgrupo particular de S_n.

Definición 2.23. O **subgrupo alternado**, que se denota por A_n, é o subgrupo de S_n definido por $A_n := \{\sigma \in S_n \mid sig(\sigma) = 1\}$.

Teorema 2.24. *Para cada $n \geq 2$, o subgrupo alternado A_n é un subgrupo normal de S_n de índice 2 e orde $|S_n|/2 = n!/2$.*

Demostración. Denótese por C o grupo multiplicativo $C = \{1, -1\}$. Sexa $f : S_n \longrightarrow C$ a aplicación dada por $f(\sigma) = sig(\sigma)$. Claramente f é un homomorfismo sobrexectivo de grupos cuxo núcleo é A_n. Deste xeito, A_n é normal en S_n, e ademais polo primeiro teorema de isomorfía, $S_n/A_n \cong C$. Así, $(S_n : A_n) = 2$ e $|A_n| = |S_n|/2 = n!/2$. □

Agora xa estamos en condicións de aclarar o comentario feito no capítulo anterior sobre o recíproco do teorema de Lagrange. O grupo A_4 ten orde 12 pero non ten ningún subgrupo de orde 6. Se existise un subgrupo $S < A_4$ de orde 6, o índice de S en A_4 sería $(A_4 : S) = 2$, e entón para todo $s \in A_4$ teríase que $s^2 \in S$. Agora ben, como A_4 contén 8 ciclos de orde 3, teríase que

se s é un deses ciclos, $s = s^4 = (s^2)^2$ está en S, e polo tanto S tería 8 elementos, o cal é unha contradición.

2.3. Clases de conxugación de S_n

Previamente xa se falou da conxugación nun grupo e da clase de conxugación dun elemento do grupo (Definición 1.33). Analizarase agora o caso particular de que o grupo sexa S_n. Entón, a clase de conxugación dun elemento $\sigma \in S_n$ estará formada por elementos da forma $\tau^{-1}\sigma\tau$, onde $\tau \in S_n$. Vexamos primeiro que se temos un ciclo $\sigma \in S_n$, entón para $\tau \in S_n$, o conxugado $\tau^{-1}\sigma\tau$ continúa a ser un ciclo.

Proposición 2.25. *Sexa $\sigma \in S_n$ un ciclo de orde k con $\sigma = (i_1, i_2, ..., i_k)$ e $\tau \in S_n$. Entón, $\tau^{-1}\sigma\tau$ é tamén un ciclo de orde k e ademais $\tau^{-1}\sigma\tau = (\tau^{-1}i_1, \tau^{-1}i_2, ..., \tau^{-1}i_k)$.*

Demostración. Sexa $A = \{i_1, ..., i_k\}$ e tomemos $i_r \in A$. Tense entón que $(\tau^{-1}\sigma\tau)\tau^{-1}i_r = \tau^{-1}\sigma i_r = \tau^{-1}i_{r+1}$, ou $\tau^{-1}i_1$ no caso de que $r = k$.

Agora, para $1 \leq i \leq n$, con $i \notin A$, terase $(\tau^{-1}\sigma\tau)\tau^{-1}i = \tau^{-1}\sigma i = \tau^{-1}i$.

Chégase así ao resultado $\tau^{-1}(i_1, ..., i_k)\tau = (\tau^{-1}i_1, ..., \tau^{-1}i_k)$. □

Xa se viu que toda permutación σ se pode descompoñer nun produto de ciclos disxuntos $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$, de xeito que os ciclos teñen ordes $m_1, m_2, ..., m_r$ respectivamente (Proposición 2.12). Para o estudo que se vai realizar, é conveniente considerar tamén os ciclos de lonxitude 1, e así os n elementos de σ estarán na descomposición en ciclos.

Deste xeito, os enteiros $m_1, m_2, ..., m_r$ denomínanse **estrutura en ciclos** de σ. Entón, tódalas estruturas en ciclos de S_n están nunha correspondencia un a un cos conxuntos de enteiros $m_1, m_2, ..., m_r$ verificando $1 \leq m_1 \leq m_2 \leq ... \leq m_r$, $m_1 + m_2 + ... + m_r = n$.

Alternativamente, se σ ten e_1 ciclos de orde 1, e_2 de orde 2,..., e_n de orde n, a estrutura en ciclos de σ vén dada polos enteiros non negativos $e_1, e_2, ..., e_n$, de xeito que $e_1 + 2e_2 + ... + ne_n = n$.

O seguinte resultado relaciona as clases de conxugación de S_n coa estrutura en ciclos.

Proposición 2.26. *Se $\sigma \in S_n$, a clase de conxugación de σ en S_n está formada por tódalas permutacións de S_n que teñen a mesma estrutura en ciclos ca σ.*

Demostración. Consideremos unha permutación $\sigma \in S_n$ e a súa descomposición en ciclos disxuntos $\sigma = \sigma_1\sigma_2 \cdots \sigma_r = (x_1, x_2, ...x_{m_1})(y_1, y_2, ..., y_{m_2}) \cdots (w_1, w_2, ..., w_{m_r})$. Cada σ_i é de orde m_i,

verificando $m_1 + m_2 + ... + m_r = n$ e $m_1 \leq m_2 \leq ... \leq m_r$. Sexa $\tau \in S_n$:

$$\tau^{-1}\sigma\tau = \tau^{-1}(x_1, x_2, ...x_{m_1})\tau\tau^{-1}(y_1, y_2, ..., y_{m_2})\tau \cdots \tau^{-1}(w_1, w_2, ..., w_{m_r})\tau =$$
$$= (\tau^{-1}x_1, \tau^{-1}x_2, ...\tau^{-1}x_{m_1})(\tau^{-1}y_1, \tau^{-1}y_2, ..., \tau^{-1}y_{m_2}) \cdots (\tau^{-1}w_1, \tau^{-1}w_2, ..., \tau^{-1}w_{m_r})$$

Entón é claro que σ e $\tau^{-1}\sigma\tau$ teñen a mesma estrutura en ciclos.

Reciprocamente, sexan $\alpha, \beta \in S_n$ dúas permutacións coa mesma estrutura en ciclos:

$\alpha = (x_1, ...x_{m_1})(y_1, ..., y_{m_2}) \cdots (w_1, ..., w_{m_r})$ e $\beta = (x'_1, ...x'_{m_1})(y'_1, ..., y'_{m_2}) \cdots (w'_1, ..., w'_{m_r})$.

Como son produto de ciclos disxuntos, existe un $\tau \in S_n$ de xeito que $\tau(x_1) = x'_1, ..., \tau(x_{m_1}) = x'_{m_1}, ..., \tau(w_1) = w'_1, ..., \tau(w_{m_r}) = w'_{m_r}$. Así, polo visto antes, chégase a que $\tau^{-1}\beta\tau = \alpha$, ou o que é o mesmo, α e β son conxugadas. □

Vexamos un exemplo disto.

Exemplo 2.27. As permutacións $(2, 3, 1)(4, 5)(6)$ e $(5, 6, 2)(3, 1)(4)$ son permutacións de S_6 que son conxugadas.

Entón, hai tantas clases de conxugación en S_n coma posibles estruturas en ciclos. É dicir, o número de clases de conxugación en S_n é igual ao número de particións de n en sumandos non negativos. Máis adiante denotaremos a partición por $1^{e_1}2^{e_2}...n^{e_n}$ (onde, lembremos, e_i denota o número de ciclos de orde i). Aínda que non hai ningunha fórmula que exprese o número de clases de conxugación de S_n coma unha función de n, o que si pode verse é cantos elementos hai en cada clase.

Proposición 2.28. *Sexa $\sigma \in S_n$ con estrutura en ciclos dada pola partición $1^{e_1}2^{e_2}...n^{e_n}$. Entón o número de permutacións que son conxugadas con σ en S_n é igual a*

$$h_\sigma = \frac{n!}{1^{e_1}e_1!2^{e_2}e_2!...n^{e_n}e_n!}.$$

Demostración. A estrutura en ciclos de σ, denotada por $1^{e_1}2^{e_2}...n^{e_n}$ como xa se viu, pode verse do seguinte xeito:

$$\underbrace{(.)(.)...(.)}_{e_1}\underbrace{(..)(..)...(..)}_{e_2}...$$

Téñense exactamente n espazos, que completados con n obxectos de calquera xeito, dan un elemento de S_n, que por construción terá a mesma estrutura en ciclos ca σ. Sábese que hai $n!$ formas de ordenar os n elementos. Non obstante, haberá ordenacións que proporcionen o mesmo elemento de S_n.

Centrémonos nos e_i ciclos de orde i $(1 \leq i \leq n)$. Estes ciclos, poden permutarse de $e_i!$ formas, de xeito que o resultado segue a ser o mesmo elemento de S_n. Ademais, cada ciclo $(a_1, a_2, ..., a_i)$ pode escribirse de i formas distintas $((a_1, a_2, ..., a_i) = (a_2, a_3, ..., a_i, a_1) = ... = (a_i, a_1, ..., a_{i-1}))$.

Entón, cada elemento de S_n foi contado $e_i! i^{e_i}$ veces por cada ciclo de orde i. Polo tanto, cada elemento da clase de conxugación de σ repítese $1^{e_1} e_1! 2^{e_2} e_2! ... n^{e_n} e_n!$ veces, e así chégase á fórmula dada pola proposición. □

No primeiro capítulo falouse de xeradores, relacións e presentacións de grupos. No seguinte epígrafe identificaranse estes conceptos no caso particular do grupo simétrico de n elementos. Para iso, utilizarase o texto de Dummit e Foote [6].

2.4. Presentación de S_n

En primeiro lugar estudaranse subconxuntos de S_n que xeran a S_n. Os máis sinxelos son as transposicións da forma $(i, i+1) = t_i$ para $1 \leq i \leq n$. Aos $n-1$ elementos t_i chamarémolos transposicións simples de S_n.

Teorema 2.29. I. *O grupo simétrico S_n está xerado polas $n-1$ transposicións simples.*

II. *S_n está xerado polas transposicións $(1, i)$, con $2 \leq i \leq n$.*

III. *Para $n \geq 3$, S_n está xerado pola transposición $(1, 2)$ e o $n-$ciclo $(1, 2, ..., n)$.*

IV. *Para $n \geq 3$, S_n está xerado pola transposición $(1, 2)$ e o $(n-1)-$ciclo $(2, 3, ..., n)$.*

Demostración. I. Unha inclusión dase trivialmente, é dicir, $\langle t_1, ..., t_{n-1} \rangle < S_n$. En primeiro lugar, $(i, n) = t_i t_{i+1} \cdots t_{n-1}$ para todo $1 \leq i \leq n-1$. Procedemos a probar o enunciado por indución en n. Para $n = 1, 2$ non hai nada que probar.

Agora, supoñamos que o resultado se cumpre para $n-1$, é dicir, S_{n-1} está xerado polas $n-2$ transposicións simples e vexamos que se cumpre para S_n. Consideremos a acción de S_n sobre o conxunto $\{1, ..., n\}$ e E o seu estabilizador. Tense que $E \cong S_{n-1}$, que por hipótese de indución está xerado polas transposicións simples $t_1, ..., t_{n-2}$ de S_n. Sexa $\sigma \in S_n$. Por unha banda, se $\sigma \in E$, entón $\sigma \in \langle t_1, ..., t_{n-2} \rangle \subset \langle t_1, ..., t_{n-2}, t_{n-1} \rangle$. Por outra banda, se $\sigma \notin E$, terase que $\sigma(n) = k \neq n$. Consideremos agora $\tau = (k, n) = t_k t_{k+1} \cdots t_{n-1}$. Así, $\tau \in \langle t_1, ..., t_{n-1} \rangle$, e entón $\tau\sigma(n) = \tau(k) = n$. Deste xeito, $\tau\sigma \in E$, e polo tanto $\tau\sigma \in \langle t_1, ..., t_{n-1} \rangle$. Finalmente, que $\sigma = \tau(\tau\sigma) \in \langle t_1, ..., t_{n-1} \rangle$ proba a outra inclusión $S_n \subset \langle t_1, ..., t_{n-1} \rangle$.

II. Denotemos por $S = \langle (1,2),(1,3),...,(1,n)\rangle$. Entón, $t_i = (i,i+1) = (1,i)(1,i+1)(1,i) \in S$ con $1 \leq i \leq n$. Non obstante, S_n é o menor subgrupo contendo ás transposicións t_i, e polo tanto $S_n < S$. Non obstante, pola definición de S terase que $S \subset S_n$, e así $S = S_n$.

III. Denotando $\sigma = (1,2,...,n)$, tense que $\sigma^i(1) = i+1$ para $1 \leq i \leq n-1$. Agora, aplicando a Proposición 2.25, $\sigma^{i-1}(1,2)\sigma^{-(i-1)} = (\sigma^{i-1}(1), \sigma^{i-1}(2)) = (i,i+1) = t_i$.

Así, para todo $1 \leq i \leq n-1$, $t_i \in \langle (1,2),\sigma\rangle$. Polo tanto, como S_n está xerado polas $n-1$ transposicións simples t_i, $S_n < \langle (1,2),\sigma\rangle$. Non obstante, tamén se ten que $(1,2),\sigma \in S_n$ e polo tanto $S_n = \langle (1,2),(1,2,...,n)\rangle$.

IV. $(1,2)(2,3,...,n) = (1,2,...,n)$, o que significa que $(1,2,...,n) \in \langle (1,2),(2,3,...,n)\rangle$. Ademais, $(1,2) \in \langle (1,2),(2,3,...,n)\rangle$. Agora ben, polo punto anterior, $S_n = \langle (1,2),(1,2,...,n)\rangle$, e polo tanto $S_n < \langle (1,2),(2,3,...,n)\rangle$. Como $\langle (1,2),(2,3,...,n)\rangle < S_n$ trivialmente, entón $S_n = \langle (1,2),(2,3,...,n)\rangle$.

□

As transposicións simples de S_n, que como se acaba de probar é un conxunto de xeradores de S_n, verifican unhas relacións que se probarán a continuación e con todo darase unha presentación de S_n.

Proposición 2.30. *As transposicións simples de S_n, sempre que $n \geq 2$, verifican as relacións: $t_i^2 = 1$, con $1 \leq i \leq n-1$, $t_it_j = t_jt_i$, para $|i-j| > 1$ e $t_it_{i+1}t_i = t_{i+1}t_it_{i+1}$.*

Demostración. Como as t_i son transposicións, a relación $t_i^2 = 1$ con $1 \leq i \leq n-1$ é inmediata. Por outra banda, cando $|i-j| > 1$ tense que $|i-j| \geq 2$, e polo tanto t_i e t_j son disxuntos. Deste xeito, pola Proposición 2.9 conmutan, e así $t_it_j = t_jt_i$. Finalmente, se se ten que $1 \leq i \leq n-2$ verifícase que $t_it_{i+1}t_i = (i,i+1)(i+1,i+2)(i,i+1) = (i,i+2) = (i+1,i+2)(i,i+1)(i+1,i+2) = t_{i+1}t_it_{i+1}$. □

A última destas relacións equivale a que $(t_it_{i+1})^3 = 1$ para $1 \leq i \leq n-2$.

A continuación defínese unha matriz simétrica $M = (m_{ij})$ de orde $n-1 \times n-1$ con entradas en $\mathbb{Z}$:

$$m_{ij} = \begin{cases} 1, \text{ se } i = j \text{ e } 1 \leq i \leq n-1 \\ 2, \text{ se } |i-j| > 1 \\ 3, \text{ se } j = i+1 \text{ e } 1 \leq i \leq n-2 \end{cases}$$

Agora podemos reescribir as relacións da anterior proposición do seguinte xeito: $(t_it_j)^{m_{ij}} = 1$.

Consideremos agora dous conxuntos. Un de xeradores $X = \{x_1, ..., x_{n-1}\}$ e outro de relacións $R = \langle (x_i x_j)^{m_{ij}} \mid 1 \leq i, j \leq n-1 \rangle$. Entón, tense que se F é o grupo libre xerado por X e R, $W_n = \langle x_1, ..., x_{n-1} \mid (x_i x_j)^{m_{ij}} \text{ con } 1 \leq i, j \leq n-1 \rangle$ será da forma $W_n = F/R$. Ademais, como $x_i^{-1} = x_i$, os elementos $\omega \in W_n$ poden expresarse do seguinte xeito: $\omega = x_{i_1} x_{i_2} \cdots x_{i_k}$, para todo $1 \leq i \leq n-1$ con $1 \leq i_1, i_2, ..., i_k \leq n$.

Lema 2.31. $|W_n| \leq n!$ *cando* $n \geq 2$.

Demostración. Verase esta demostración por indución en n. Para o primeiro caso, $n = 2$, tense que $W_2 = \{1, t_1\}$, polo que $|W_2| = 2 \leq 2!$.

Agora supóñase o resultado certo para n, é dicir, $|W_n| \leq n!$, e vexamos que se cumpre para $n+1$. Sexa V o subgrupo de W_{n+1} xerado por $x_1, ..., x_{n-1}$, $V = \langle x_1, ..., x_{n-1} \rangle < W_{n+1}$. Entón, como V é subgrupo de W_{n+1}, os x_i cumpren as relacións $(x_i x_j)^{m_{ij}} = 1$, con $1 \leq i, j \leq n-1$. Deste xeito, polo Teorema de van Dyck 1.85, existe un epimorfismo $W_n \to V$. Unindo isto coa hipótese de indución, terase que $|V| \leq |W_n| \leq n!$.

Defínense a continuación os conxuntos $V_0 = x_1 x_2 \cdots x_n V$, $V_1 = x_2 \cdots x_n V$,..., $V_{n-1} = x_n V$, $V_n = V$. Probemos que, para $1 \leq i, j \leq n$,

$$x_i V_j = \begin{cases} V_{i-1}, \text{ se } i = j \\ V_i, \text{ se } j = i-1 \\ V_j, \text{ se } i \neq j, i-1 \end{cases}$$

En primeiro lugar, se $i = j$, $x_i V_j = x_i V_i = x_i x_{i+1} \cdots x_n V = V_{i-1}$.

En segundo lugar, sexa $j = i - 1$. Así, $x_i V_j = x_i V_{i-1} = x_i x_i x_{i+1} \cdots x_n V = x_{i+1} \cdots x_n V = V_i$.

Finalmente, consideremos o caso $j \neq i, i-1$, que separaremos noutros dous: que $j \geq i+1$ ou que $j \leq i-2$.

En primeiro lugar, estudaremos o caso $j \geq i+1$. Nese caso, $\forall j+1 \leq k \leq n$, $|k-i| > 1$, e entón $x_i x_k = x_k x_i$. Ademais, como $j \geq i+1$, tense que $i < n$, o que implica que $x_i \in V$, e polo tanto $x_i V = V$. Deste xeito, $x_i V_j = x_i x_{j+1} x_{j+2} \cdots x_n V = x_{j+1} \cdots x_n x_i V = x_{j+1} \cdots x_n V = V_j$.

Consideremos agora o caso $j \leq i-2$. Neste outro caso, $\forall 1 \leq k \leq i-2$, $x_i x_k = x_k x_i$ e ademais verifícase a terceira relación da Proposición 2.30, é dicir, $x_i x_{i-1} x_i = x_{i-1} x_i x_{i-1}$. Así, $x_i V_j = x_i x_{j+1} x_{j+2} \cdots x_n V = x_{j+1} \cdots x_{i-2} x_i x_{i-1} x_i x_{i+1} \cdots x_n V = x_{j+1} \cdots x_{i-2} x_{i-1} x_i x_{i-1} x_{i+1} \cdots x_n V$. Para todo $i+1 \leq k \leq n$, $x_{i-1} x_k = x_k x_{i-1}$, e ademais como $i - 1 \leq n$, $x_{i-1} x_k = x_k x_{i-1}$ e entón $x_i V_j = x_{j+1} \cdots x_n x_{i-1} V = x_{j+1} \cdots x_n V = V_j$.

Así probouse que $\forall 1 \leq i, j \leq n$, $\exists 1 \leq k \leq n$ de xeito que $x_i V_j = V_k$. Por outra banda, xa se dixera que para $\omega \in W_n$ se ten que $\omega = x_{i_1} \cdots x_{i_m}$. Entón, para algún j, $\omega V = \omega V_n = V_j$, e

polo tanto, $W_{n+1}/V = \{V_0, V_1, ..., V_n\}$. En principio, os V_i non teñen por que ser disxuntos dous a dous, polo que $(W_{n+1} : V) \leq n+1$. Así, $|W_{n+1}| = (W_{n+1} : V)|V| \leq (n+1)n! = (n+1)!$, co que queda probada a proposición. □

Deste xeito, estamos en condicións de ver cal é a presentación de S_n.

Teorema 2.32. *O grupo simétrico S_n ten presentación $S_n \cong \langle t_1, t_2, ..., t_{n-1} \mid (t_i t_j)^{m_{ij}} = 1$ con $1 \leq i, j \leq n-1\rangle$, sendo $n \geq 2$.*

Demostración. Pola Proposición 2.29, as $n-1$ transposicións simples xeran S_n, e ademais verifican as relacións da Proposición 2.30, que xa se dixo que se traducen en $(t_i t_j)^{m_{ij}} = 1$ para todo $1 \leq i, j \leq n-1$. Deste xeito, pode aplicarse o Teorema de van Dyck 1.85, e así hai un epimorfismo $W_n \to S_n$, levando x_i en t_i para $1 \leq i \leq n-1$. Denotemos dito epimorfismo por f.

Entón, tense trivialmente que $|W_n| \geq |S_n| = n!$ Ademais, acaba de verse no lema anterior a desigualdade oposta, é dicir, $|W_n| \leq n!$ para $n \geq 2$. Así, terase que $|W_n| = n!$, e polo tanto como f é sobrexectiva, tamén e inxectiva, chegando así ao resultado do teorema. □

Capítulo 3

As matemáticas e os acordes

Neste capítulo relacionarase o visto ata agora de teoría de grupos coa teoría musical. En concreto, estudaranse os acordes de tres notas. Con este propósito, definiranse algunhas transformacións de acordes, para posteriormente ver que estas transformación forman un grupo. Para iso, utilizaranse os textos de Agustín-Aquino, du Plessis, Lluis-Puebla e Montiel [1] e o de du Plessis [11].

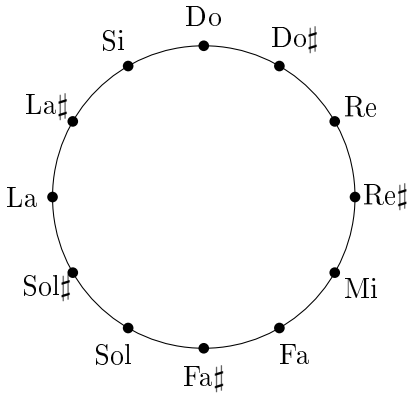
3.1. Nocións musicais

Como sabemos, na escala diatónica hai exactamente sete notas musicais: Do, Re, Mi, Fa, Sol, La e Si. Despois do Si volve repetirse o Do. O intervalo que hai entre dous Dos consecutivos, e en xeral entre dúas notas co mesmo nome consecutivas, denomínase oitava. Outra forma de definir unha oitava é coma o intervalo que hai entre dúas notas que teñen a metade ou o dobre de frecuencia unha da outra. A afinación equitemperada consiste en dividir unha oitava en 12 intervalos iguais, de xeito que a frecuencia de cada ton resulta de multiplicar por $\sqrt[12]{2}$ a do anterior. Tense entón que nunha oitava hai exactamente 12 notas, de maneira que a diferenza de frecuencia que hai entre dúas notas consecutivas se denomina semitón. A escala cromática é entón o conxunto das seguintes doce notas separadas por un semitón entre elas:

Do, Do♯, Re, Re♯, Mi, Fa, Fa♯, Sol, Sol♯, La, La♯, Si.

Denotaranse as notas con inicial maiúscula. O símbolo díese ♯ nunha nota enténdese como subir esa mesma nota un semitón. Igualmente, o símbolo bemol ♭ nunha nota enténdese como esa mesma nota un semitón por debaixo. Así, hai veces que dúas notas distintas representan un mesmo son, feito que se coñece coma equivalencia enharmónica. Por exemplo o Do♯ é a mesma nota ca Re♭.

Como xa se dixo, a seguinte nota ao Si é de novo o Do, e polo tanto volve repetirse esta secuencia. Isto pode lembrarnos a un grupo cíclico. Pola definición de oitava, os múltiplos dunha certa frecuencia represéntanse coa mesma nota. É por isto que podemos asociar o noso conxunto de doce notas co grupo cíclico de doce elementos $\mathbb{Z}_{12}$. Deste xeito, adoitamos asociar a nota Do co primeiro elemento de $\mathbb{Z}_{12}$, o 0, Do♯ co 1 e así sucesivamente. Esta correspondencia é a máis usual, aínda que podería ser calquera outra mentres conserve a orde pola disposición cíclica das notas. Por outra banda, en realidade o que estamos é a asociar clases de equivalencia, mais por abuso de notación cando se di que o Do é o 0, o que se quere dicir é que é o $\bar{0}$. Pode representarse o conxunto das notas coma o grupo cíclico de 12 elementos do seguinte xeito.



Cabe destacar que unicamente estaremos interesados nos acordes, que son conxuntos de notas que se tocan de forma simultánea. De xeito máis específico, a nosa análise xirará en torno aos acordes de tres notas, denominados tríades. Porén, non estudaremos todos os tipos de tríades, se non que nos centraremos nos acordes de tres notas maiores e menores, que se definen a continuación. Este estudo non é arbitrario, se non que se debe a que a harmonía básica de moitas cancións e pezas musicais se basea neste tipo de tríades. Como se dixo, cando falamos dunha nota estamos a falar dunha clase de equivalencia, e polo tanto, cando falemos dun acorde pasará o mesmo. Así, cando nos refiramos a unha tríade $\{x, y, x\}$, estaremos a referirnos á clase da tríade, $\{\bar{x}, \bar{y}, \bar{z}\}$.

Definición 3.1. Un acorde $\{x, y, z\} \in \mathcal{P}(\mathbb{Z}_{12})$ dise maior se é da forma $y = x + 4$ e $z = x + 7$.

A primeira nota do acorde, x na definición, é a raíz do acorde. Denotaranse os acordes maiores coa nota da raíz en maiúsculas, para diferencialos das notas. Por exemplo, o acorde de Do maior, $\mathbf{DO} = \{0, 4, 7\}$, vén dado na posición fundamental. Non obstante, a orde dos elementos non inflúe no conxunto debido a que os acordes son conxuntos de notas que soan simultaneamente. É dicir, para denotar este mesmo acorde podemos utilizar indistintamente o conxunto deses mesmos tres números en calquera orde.

Analogamente, defínense os acordes menores:

Definición 3.2. Un acorde $\{x, y, z\} \in \mathcal{P}(\mathbb{Z}_{12})$ dise menor cando $y = x + 3$ e $z = x + 7$.

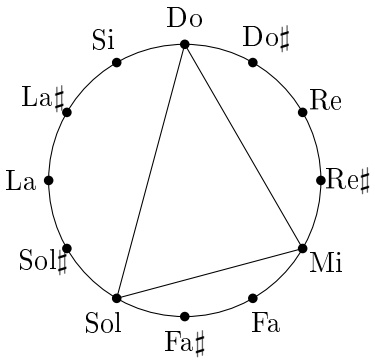
Denotaranse os acordes menores coa raíz en minúsculas e cun m minúsculo ao lado, diferenciándoos así dos maiores e das notas. Por exemplo, o acorde de Do menor será $\mathbf{do}\mathrm{m} = \{0, 3, 7\}$. Analogamente ao que ocorre cos acordes maiores, cambiar a orde das notas no conxunto non altera o acorde.

Téñense entón 12 acordes maiores e outros tantos menores. Defínese o conxunto dos 24 acordes maiores e menores.

Definición 3.3. $\mathcal{M} = \{\{x, x+3, x+7\}, \{X, X+4, X+7\} \mid x, X \in \mathbb{Z}_{12}\}$ é o conxunto de tódolos acordes maiores e menores.

Como se viu, as tríades son en realidade clases de tríades, e polo tanto os elementos de $\mathcal{M}$ serán tamén clases. Por exemplo, tomando $\mathbf{do}\mathrm{m} = \{0, 3, 7\}$, en realidade estamos a falar do conxunto $\{..., \{-12, -9, -5\}, \{0, 3, 7\}, \{12, 15, 19\}, ...\}$. Nótese que o conxunto $\mathcal{M}$ posúe 24 elementos.

Pode representarse un acorde coma un triángulo cuxos vértices representan as tres notas que o forman. Por exemplo, para representar o acorde de Do maior, **DO**, terase:



Nas próximas seccións relacionaranse os coñecementos dos capítulos anteriores sobre accións de grupos, grupos libres, xeradores, relacións e grupo simétrico coa teoría musical.

3.2. Transformacións de acordes

Para levar a cabo o noso estudo, comezaranse introducindo unha serie de transformacións sobre o conxunto dos acordes maiores e menores $\mathcal{M}$.

3.2.1. Transposicións e inversións

Definiranse a continuación dúas transformacións sobre o conxunto dos acordes maiores e menores. Consideraranse subgrupos do grupo de permutacións de $\mathcal{M}$, $S_{\mathcal{M}}$.

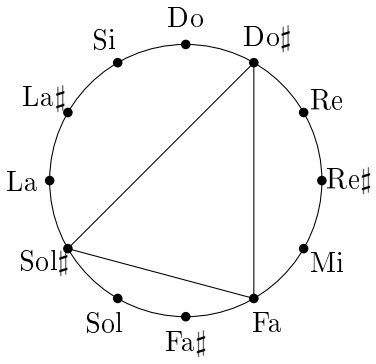
Definición 3.4. Dado $x \in \mathcal{M}$, con $x = \{x_1, x_2, x_3\}$, defínese unha **transposición** como unha función $T_n : \mathcal{M} \to \mathcal{M}$ con $T_n(x) = x + n = \{x_1 + n, x_2 + n, x_3 + n\}$, e $n \in \mathbb{Z}$.

Musicalmente, pode interpretarse este concepto de transposición que se acaba de definir como a translación dun acorde por un intervalo constante.

Cabe destacar que en realidade definindo T_1 pode obterse $T_n = (T_1)^n$. Ademais, observamos que se pode aplicar T_n aos 24 elementos de $\mathcal{M}$ unha cantidade, en principio infinita, de veces, xa que $n \in \mathbb{Z}$. Porén, é fácil darse conta de que despois de aplicar T_1 12 veces se obtén a tríade inicial. Deste xeito, é suficiente con definir T_n para $n \in \mathbb{Z}_{12}$. Así, T_n é un subgrupo cíclico de $S_{\mathcal{M}}$, un ciclo, que está xerado por T_1, un ciclo de orde 12. Isto é debido a que é unha transformación bixectiva dentro do conxunto dos acordes maiores e menores. Por outra banda, observamos que T_0 actúa coma a función identidade en $\mathcal{M}$.

Esta operación está ben definida, é dicir, tomando dúas tríades da mesma clase $\{\bar{x}, \bar{y}, \bar{z}\}$ con $\bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_{12}$, terase que a súa imaxe por T_n é a mesma. Efectivamente, sexan $\{x_1, y_1, z_1\}$ e $\{x_2, y_2, z_2\} \in \mathcal{M}$ dous representantes de dita clase. Así, $T_n(\{x_1, y_1, z_1\}) = \{x_1+n, y_1+n, z_1+n\} = \{x_2 + n, y_2 + n, z_2 + n\} = T_n(\{x_2, y_2, z_2\})$, debido a que $a \in \bar{b} \Rightarrow a + n \in \overline{b + n}$.

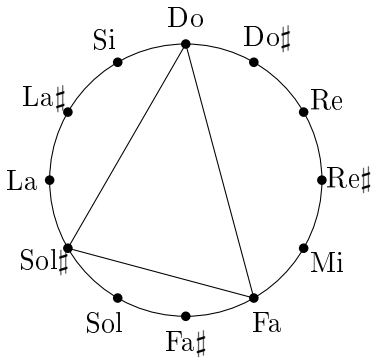
Pode observarse que aplicando sucesivamente T_1 a un dos acordes maiores se obteñen os 12 que hai, e analogamente cos menores. Xa se dixo que se pode pensar un acorde coma un triángulo, con cada un dos vértices representando unha nota. Polo tanto, as transposicións non serán máis ca rotacións do triángulo no sentido das agullas do reloxo de $2\pi n/12 = n\pi/6$ radiáns. Entón, partindo por exemplo do acorde **DO** $= \{0, 4, 7\}$, represéntase $T_1(\{0, 4, 7\}) = \{1, 5, 8\} =$ **DO♯** como



Definición 3.5. Defínese unha inversión dun acorde $x \in \mathcal{M}$, con $x = \{x_1, x_2, x_3\}$ como unha

función $I_n : \mathcal{M} \to \mathcal{M}$ definida como $I_n(x) = -x + n = \{-x_1 + n, -x_2 + n, -x_3 + n\}$ e con $n \in \mathbb{Z}$.

Mentres que as transposicións converten acordes maiores en maiores e o mesmo cos menores, as inversións transforman acordes maiores en menores e viceversa. De novo, observamos que se se lle aplica a unha tríade I_n con $n \in \mathbb{Z}$, non se teñen máis ca 12 inversións distintas. Se ademais se lle aplica a mesma inversión I_n a unha tríade dúas veces consecutivas, obtense a tríade incial. Así, unha inversión non é máis ca unha transposición dentro de $S_{\mathcal{M}}$. Deste xeito, xeometricamente vemos que aplicar a inversión I_0 a unha tríade, que como xa se dixo se representa coma un triángulo nun círculo, dá como resultado a reflexión do triángulo respecto ao eixo que pasa polo 0 e o 6 no círculo. Partindo de novo do acorde de **DO** $= \{0, 4, 7\}$, vemos que $I_0(\{0, 4, 7\}) = \{0, -4, -7\} = \{0, 5, 8\} = \{5, 8, 0\} =$ **fa**m, que se representa por



Ademais, o resto de inversións T_n obtéñense aplicando primeiro a inversión I_0 e posteriormente a transposición T_n.

Esta operación está ben definida, é dicir, tomando dúas tríades da mesma clase $\{\bar{x}, \bar{y}, \bar{z}\}$ con $\bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_{12}$, terase que a súa imaxe por I_n é a mesma. Efectivamente, sexan $\{x_1, y_1, z_1\}$ e $\{x_2, y_2, z_2\} \in \mathcal{M}$ dous representantes de dita clase. Deste xeito, terase que $I_n(\{x_1, y_1, z_1\}) = \{-x_1 + n, -y_1 + n, -z_1 + n\} = \{-x_2 + n, -y_2 + n, -z_2 + n\} = I_n(\{x_2, y_2, z_2\})$, debido a que $-a \in \bar{b} \Rightarrow -a + n \in \overline{b + n}$.

Xa se dixo que basta definir tanto as transposicións T_n coma as inversións I_n para $n \in \mathbb{Z}_{12}$. Vexamos que isto efectivamente é certo.

Proposición 3.6. *Sexan $n, m \in \mathbb{Z}$ de xeito que $n \equiv m$(mód 12). Entón verifícase que $T_n = T_m$ e $I_n = I_m$.*

Demostración. Que $n \equiv m$(mód 12) implica que $\exists k \in \mathbb{Z}$ de xeito que $n = m + 12k$. Entón:

Por unha banda, $T_n = T_{m+12k} = T_m \circ T_{12k} = T_m \circ (T_0)^k = T_m \circ (id)^k = T_m$, onde id é a transformación identidade.

Por outra banda sexa $\{x, y, z\} \in \mathcal{M}$. Entón,
$I_n(\{x, y, z\}) = I_{m+12k}(\{x, y, z\}) = \{-x + m + 12k, -y + m + 12k, -z + m + 12k\} =$
$T_{12k}(\{-x + m, -y + m, -z + m\}) = T_{12k}(I_m(\{x, y, z\})) = T_{12k} \circ I_m(\{x, y, z\}) \Rightarrow I_n = I_{m+12k} =$
$T_{12k} \circ I_m$. Así, $I_n = I_{m+12k} = T_{12k} \circ I_m = (t_0)^k \circ I_m = (id)^k \circ I_m = I_m$, onde de novo id é a transformación identidade. □

Pode entón definirse o conxunto formado por tódalas transposicións e inversións.

Definición 3.7. Defínese TI o conxunto de tódalas transposicións e inversións como $TI := \{T_n, I_n \mid n = 0, ..., 11\}$.

Vexamos algunhas propiedades que se verifican entre os elementos do conxunto TI.

Lema 3.8. *Os elementos do conxunto TI cumpren as seguintes propiedades:*

$$T_l \circ T_n = T_{l+n\,(mód\,12)}.$$

$$T_l \circ I_n = I_{l+n\,(mód\,12)}.$$

$$I_l \circ T_n = I_{l-n\,(mód\,12)}.$$

$$I_l \circ I_n = T_{l-n\,(mód\,12)}.$$

Demostración. Probaranse as igualdades unha a unha. Para iso, sexa $\{x, y, z\} \in \mathcal{M}$: Primeiro, $T_l \circ T_n(\{x, y, z\}) = T_l(T_n(\{x, y, z\})) = T_l(\{x+n, y+n, z+n\}) = \{x+n+l, y+n+l, z+n+l\} = \{x + (l + n), y + (l + n), z + (l + n)\} = T_{l+n\,(\text{mód } 12)}(\{x, y, z\})$.

En segundo lugar, $T_l \circ I_n(\{x, y, z\}) = T_l(I_n(\{x, y, z\})) = T_l(\{-x + n, -y + n, -z + n\}) = \{-x+n+l, -y+n+l, -z+n+l\} = \{-x+(l+n), -y+(l+n), -z+(l+n)\} = T_{l+n\,(\text{mód } 12)}(\{x, y, z\})$.

En terceiro lugar, tense $I_l \circ T_n(\{x, y, z\}) = I_l(T_n(\{x, y, z\})) = I_l(\{x + n, y + n, z + n\}) = \{-x-n+l, -y-n+l, -z-n+l\} = \{-x+(l-n), -y+(l-n), -z+(l-n)\} = I_{l-n\,(\text{mód } 12)}(\{x, y, z\})$.

Finalmente, terase $I_l \circ I_n(\{x, y, z\}) = I_l(I_n(\{x, y, z\})) = I_l(\{-x + n, -y + n, -z + n\}) = \{-(-x + n) + l, -(-y + n) + l, -(-z + n) + l\} = \{x + (l - n), y + (l - n), z + (l - n)\} = T_{l-n\,(\text{mód } 12)}(\{x, y, z\})$. □

Tomando calquera tríade de $\mathcal{M}$, e aplicándolle as funcións do conxunto TI de xeito sucesivo, obtense todo o conxunto $\mathcal{M}$. Estamos agora en condicións de ver que o conxunto TI ten estrutura de grupo.

Teorema 3.9. *O conxunto TI ten estrutura de grupo coa composición.*

Demostración. O conxunto TI é pechado baixo a composición, pois tomando dúas funcións calquera $\phi, \psi \in \mathcal{M}$, polo Lema 3.8, a súa composición $\phi \circ \psi$ está en TI.

O elemento T_0 é o elemento neutro para a composición en TI. Efectivamente, de novo polo Lema 3.8, $T_0 \circ T_n = T_{0+n} = T_n$, $T_0 \circ I_n = I_{0+n} = I_n$, $T_n \circ T_0 = T_{n+0} = T_n$ e $I_n \circ T_0 = I_{n-0} = I_n$.

Vexamos agora que todo elemento no conxunto TI ten inverso para a composición. Observamos en primeiro lugar que $I_n \circ I_n = T_{n-n} = T_0$, e entón $I_n^{-1} = I_n$. En segundo lugar, para un elemento T_n tense que $T_n \circ T_{12-n} = T_{n+12-n} = T_{12} = T_0$ e analogamente $T_{12-n} \circ T_n = T_{12-n+n} = T_{12} = T_0$, e entón $T_n^{-1} = T_{12-n}$. Así chégase a que $I_n^{-1} = I_n$ e $T_n^{-1} = T_{12-n}$, e polo tanto todo elemento de TI ten inverso.

Finalmente, a composición de funcións é asociativa, e polo tanto a composición restrinxida ao conxunto TI é asociativa.

Queda así probado que TI é un grupo coa composición. □

Recapitulando, TI é un grupo xerado por unha transposición (I_0) e un ciclo de orde 12 (T_1), ambos permutacións do grupo $S_{\mathcal{M}}$.

3.2.2. Tríades paralelas e relativas. O intercambio de sétima

Vexamos outras tres transformacións do conxunto dos acordes maiores e menores $\mathcal{M}$: a paralela (P), o intercambio de sétima ou leittonwechsel (L) e a relativa (R). Para as tres definicións denótanse $x = \{x_1, x_2, x_3\}$ e $X = \{X_1, X_2, X_3\}$ dúas tríades unha menor e outra maior respectivamente.

Definición 3.10. Defínense as tríades **paralelas** como unha parella de tríades de paridade oposta. É dicir, ámbalas dúas tríades teñen a mesma nota no nome, pero unha é menor e outra maior. Entón, terase $P(x) = P(x_1, x_2, x_3) = \{x_1, x_2 + 1, x_3\}$ e $P(X) = P(\{X_1, X_2, X_3\}) = \{X_1, X_2 - 1, X_3\}$.

Exemplo 3.11. Un exemplo disto serían os acordes **do**m e **DO**.

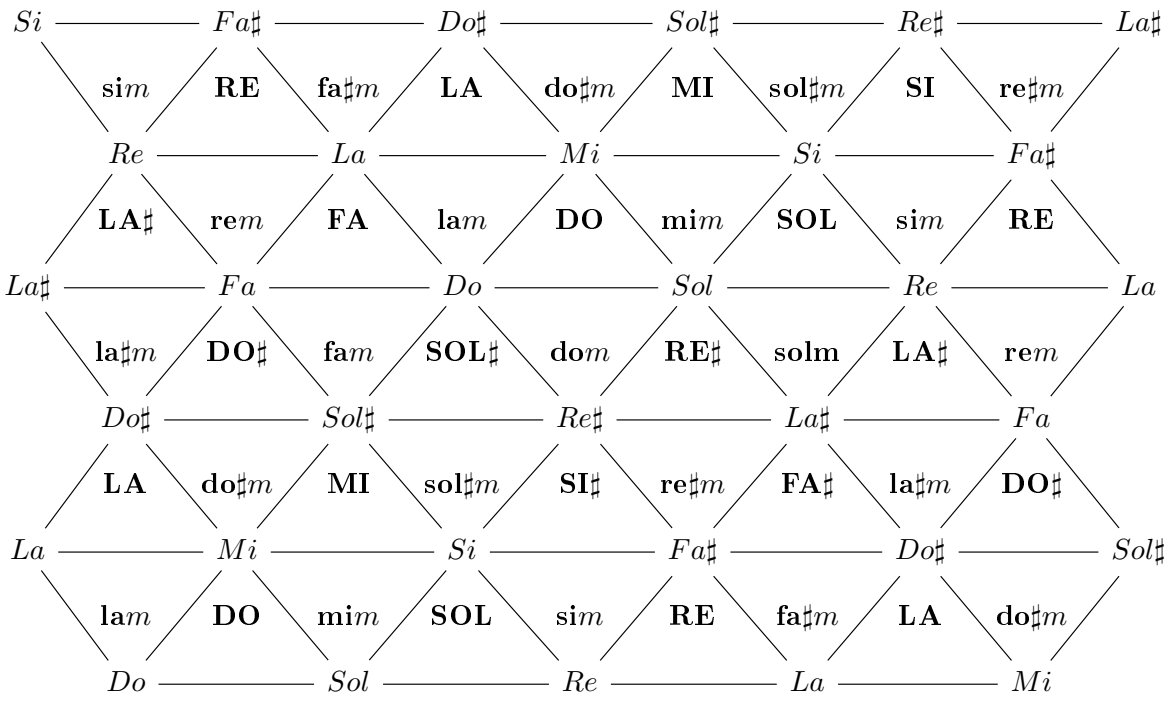
Definición 3.12. Defínense as tríades **relativas** como as parellas de tríades que son de paridade oposta e a raíz da que é menor está tres semitóns por baixo da raíz da maior. Deste xeito, $R(x) = R(\{x_1, x_2, x_3\}) = \{x_2, x_3, x_1 - 2\}$ e $R(X) = R(\{X_1, X_2, X_3\}) = \{X_3 + 2, X_1, X_2\}$.

Exemplo 3.13. Por exemplo, partindo do acorde de **DO** $= \{0, 4, 7\}$, a súa tríade relativa será $\{9, 0, 4\}$, que se corresponde con **la**m.

Definición 3.14. Defínese o **intercambio de sétima** como a tríade resultante ao intercambiar a raíz da tríade orixinal pola súa sétima. Así, $L(x) = L(\{x_1, x_2, x_3\}) = \{x_3 + 1, x_1, x_2\}$ e $L(X) = L(\{X_1, X_2, X_3\}) = \{X_2, X_3, X_1 - 1\}$.

Exemplo 3.15. Partindo de novo do acorde de **DO** $= \{0, 4, 7\}$, o intercambio de sétima correspóndese co acorde $\{4, 7, 11\}$, que é **mi**m.

Pode facerse unha representación gráfica conxunta destas tres transformación nunha rede de triángulos denominada **Tonnetz** ou **rede de tonos**.



Os triángulos representan acordes maiores e menores. Os nomes destes aparecen no centro e as notas que os forman nos vértices. A reflexión do triángulo con respecto a cada unha das tres arestas corresponde con unha das transformacións P, L e R, de xeito que todas estas transformacións conservan dúas das notas da tríade orixinal. Tomando un triángulo cuxa base estea cara abaixo (por exemplo **DO**), a reflexión con respecto á base corresponde coas tríades paralelas. Así, o triángulo superior será o maior e o de abaixo o correspondente menor, correspondéndose esta operación con P. A reflexión respecto ao lado esquerdo representa as tríades relativas, operación que se corresponde con R. Por último, a reflexión respecto ao lado dereito representa o intercambio de sétima, correspondéndose esta transformación con L. Así, vese que, como xa se dixo, a paralela a **DO** é **do**m, a súa relativa é **la**m, e o seu intercambio de sétima é **mi**m.

Cabe destacar que as tres transformacións P, L, e R están ben definidas, é dicir, a imaxe de dúas tríades da mesma clase coincide. Vexámolo para tríades menores, sendo análogo para as maiores. Sexa pois $\{\bar{x}, \bar{y}, \bar{z}\} \in \mathcal{M}$, con $\bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_{12}$, unha clase de tríades e $\{x_1, y_1, z_1\}$ e $\{x_2, y_2, z_2\}$ dous representantes de dita clase. Entón, tense $P(\{x_1, y_1, z_1\}) = \{x_1, y_1 + 1, z_1\} = \{x_2, y_2 + 1, z_2\} = P(\{x_2, y_2, z_2\})$, debido a que $y_1, y_2 \in \bar{y} \Rightarrow y_1 + 1, y_2 + 1 \in \overline{y + 1}$. Deste xeito, P está ben definida. Cun razoamento equivalente, chégase a que tamén L e R están ben definidas.

Probemos que estas tres transformacións son involutivas.

Lema 3.16. *Verifícase que $P^2 = L^2 = R^2 = id$, sendo id a transformación identidade.*

Demostración. Demóstrase para tríades maiores, sendo a proba para tríades menores totalmente análoga. Sexa pois unha tríade maior $\{X, Y, Z\} \in \mathcal{M}$. Entón:

$$P^2(\{X,Y,Z\}) = P(P(\{X,Y,Z\})) = P(\{X,Y-1,Z\}) = \{X,Y-1+1,Z\} = id(\{X,Y,Z\})$$

$$L^2(\{X,Y,Z\}) = L(L(\{X,Y,Z\})) = L(\{Y,Z,X-1\}) = \{X-1+1,Y,Z\} = id(\{X,Y,Z\})$$

$$R^2(\{X,Y,Z\}) = R(R(\{X,Y,Z\})) = R(\{Z{+}2,X,Y\}) = \{X,Y,Z{+}2{-}2\} = id(\{X,Y,Z\}) \quad \square$$

Cabe destacar que, como ocorría coas transformacións T e I, P, L, e R son transformacións bixectivas de $\mathcal{M}$ en $\mathcal{M}$. Así, son permutacións de $S_{\mathcal{M}}$, e como se acaba de ver que son involutivas, serán transposicións.

A continuación, verase que relacións hai entre as funcións P, L, e R para tratar de ver que estas tres transformacións forman tamén un grupo baixo a composición.

Comézase observando que aplicándolle sucesivamente primeiro R a unha tríade de $\mathcal{M}$ e logo L ao resultado, obtense unha sucesión cíclica de tríades na que aparecen listados tódolos elementos de $\mathcal{M}$. Isto é fácil de observar no Tonnetz. Tomando por exemplo **DO**, aplicar R é, como xa se dixo, a reflexión do triángulo á esquerda, **la**m, e aplicarlle a este L correspóndese tamén coa reflexión cara a esquerda, que será **FA** (por estar este triángulo invertido). Se continuamos movéndonos cara a esquerda sucesivamente, chégase de novo a **DO**. Vexámolo para unha tríade menor $\{x, y, z\} \in \mathcal{M}$, sendo a proba análoga para tríades maiores.

Proposición 3.17. *Verifícase que $(L \circ R)^{12} = (L \circ R)^0 = id$. Ademais, se $n, k \in \mathbb{Z}$ de xeito que $n \equiv m$(mód 12), entón $(L \circ R)^n = (L \circ R)^m$ e $R \circ (L \circ R)^n = R \circ (L \circ R)^m$.*

Demostración. Sexa unha tríade menor $\{x, y, z\} \in \mathcal{M}$. Entón, tense que $(L \circ R)(\{x,y,z\}) = L(R(\{x,y,z\})) = L(\{y,z,x-2\}) = \{z,x-2,y-1\}$. Aplicando isto tres veces:

$$\begin{aligned}(L \circ R)^3(\{x,y,z\}) &= (L \circ R)^2((L \circ R)(\{x,y,z\}))) = (L \circ R)^2(\{z,x-2,y-1\}) = \\ &= (L \circ R)(\{y-1,z-2,x-3\}) = \{x-3,y-3,z-3\}.\end{aligned}$$

Utilizando esta igualdade catro veces, obtense

$$\begin{aligned}(L \circ R)^{12}(\{x,y,z\}) &= (L \circ R)^9((L \circ R)^3(\{x,y,z\})) = (L \circ R)^9(\{x-3,y-3,z-3\}) = \\ &= (L{\circ}R)^6((L{\circ}R)^3(\{x{-}3,y{-}3,z{-}3\})) = (L{\circ}R)^6(\{x{-}6,y{-}6,z{-}6\}) = \\ &= (L{\circ}R)^3((L{\circ}R)^3(\{x{-}6,y{-}6,z{-}6\})) = (L{\circ}R)^3(\{x{-}9,y{-}9,z{-}9\}) = \\ &= \{x-12,y-12,z-12\} = \{x,y,z\} = id(\{x,y,z\}).\end{aligned}$$

Queda así probado que $(L \circ R)^{12} = (L \circ R)^0 = id$.

Por outra banda, $(L \circ R)^n = (L \circ R)^{12k+m} = (L \circ R)^{12k}(L \circ R)^m = ((L \circ R)^0)^k (L \circ R)^m = id^k (L \circ R)^m = (L \circ R)^m$, do que se deduce que $R \circ (L \circ R)^n = R \circ (L \circ R)^m$. □

Téñense así os 24 elementos de $\mathcal{M}$, que se obteñen partindo dunha tríade calquera e aplicando $(L \circ R)^n$ e $R \circ (L \circ R)^n$, para $n = 0, ..., 11$.

Vexamos que a partir destas dúas funcións $(L \circ R)^n$ e $R \circ (L \circ R)^n$, se poden obter as funcións L e P.

Lema 3.18. *Cúmprese que* $P = R \circ (L \circ R)^3$ *e* $L = R \circ (L \circ R)^{11}$.

Demostración. Vexamos que se verifica para unha tríade menor $\{x, y, z\} \in \mathcal{M}$, sendo a proba para unha tríade maior análoga.

$$\begin{aligned} R \circ (L \circ R)^3(\{x, y, z\}) &= R((L \circ R)^3(\{x, y, z\})) = R(\{x - 3, y - 3, z - 3\}) = \\ &= \{y - 3, z - 3, x - 3 - 2\} = \{y - 3, z - 3, x - 5\}. \end{aligned}$$

Agora ben, como a tríade é menor, $y = x + 3$, $z = a + 7$ e $z = y + 4$, e deste xeito, $R \circ (L \circ R)^3(\{x, y, z\}) = \{y - 3, z - 3, x - 5\} = \{y - 3, z - 3, z + 7\} = \{x, y + 1, z\} = P(\{x, y, z\})$.

Por outra banda,

$$\begin{aligned} R \circ (L \circ R)^{11}(\{x, y, z\}) &= R \circ (L \circ R)^2 \circ (L \circ R)^9(\{x, y, z\}) = R \circ (L \circ R)^2(\{x - 9, y - 9, z - 9\}) = \\ &= R \circ L \circ R \circ L \circ R(\{x - 9, y - 9, z - 9\}) = R \circ L \circ R \circ L(\{y - 9, z - 9, x - 11\}) = \\ &= R \circ L \circ R(\{z - 9, x - 11, y - 10\}) = R \circ L(\{x - 11, y - 10, z - 11\}) = \\ &= R(\{y - 10, z - 11, x - 12\}) = R(\{y - 10, z - 11, x\}) = \{z - 11, x, y - 12\} = \\ &= \{z + 1, x, y\} = L(\{x, y, z\}). \end{aligned}$$

□

Defínese a continuación o conxunto das funcións paralela, relativa e intercambio de sétima.

Definición 3.19. O conxunto PLR é o conxunto das transformacións paralela, relativa e intercambio de sétima. Defínese como $PLR := \{(L \circ R)^n, R \circ (L \circ R)^n \mid n \in \{0, 1, ..., 11\}\}$.

Observamos que na definición do conxunto non aparecen de xeito explícito as transformación P e L. Non obstante, poden obterse en función das transformacións $(L \circ R)^n$ e $R \circ (L \circ R)^n$, como se viu no Lema 3.18.

Ademais, se en lugar de aplicar primeiro R e logo L se fai ao revés, obtense a mesma sucesión que antes se mencionou pero na orde inversa. De feito, as funcións $R \circ L$ e $L \circ R$, que de agora en diante se denotarán por RL e LR respectivamente, relaciónanse do xeito seguinte: $(LR)^n = (RL)^{12-n}$, con $n \in \mathbb{Z}_{12}$ e $R \circ (LR)^m = L \circ (RL)^{11-m}$, con $m \in \mathbb{Z}_{12}$

Deste xeito, observamos que o conxunto PLR contén ás funcións P, L, R, e ás composicións RL e LR.

Vexamos agora que PLR é un grupo.

Teorema 3.20. *O conxunto PLR é un grupo coa composición. Ademais, $(R(LR)^i)^{-1} = R(LR)^i$ e $((LR)^i)^{-1} = (LR)^j$, sendo $j \equiv -i (\text{mód } 12)$.*

Demostración. Comezarase vendo que o conxunto PLR é pechado baixo a composición. Como se definiu o conxunto $PLR = \{(L \circ R)^n, R \circ (L \circ R)^n \mid n \in \{0, 1, ..., 11\}\}$, as posibles composicións dentro del serán da forma $(LR)^i \circ (LR)^j$, $R \circ (LR)^i \circ R \circ (LR)^j$, $(LR)^i \circ R \circ (LR)^j$ e $R \circ (LR)^i \circ (LR)^j$. Comprobemos que todas estas composicións están no conxunto PLR.

- Comecemos vendo que ocorre con $R \circ (LR)^i \circ R \circ (LR)^j$. É claro que se $i = j = 0$, tense que $R \circ (LR)^0 \circ R \circ (LR)^0 = R \circ id \circ R \circ id = R^2 = id = (LR)^0$. Agora vexamos que se cumpre o caso xeral polo método de indución. Supoñamos, polo tanto, que se cumpre que $R \circ (LR)^i \circ R \circ (LR)^i = id$ e vexamos que se verifica que $R \circ (LR)^{i+1} \circ R \circ (LR)^{i+1} = id$, e entón tamén estará en PLR.

  $R \circ (LR)^{i+1} \circ R \circ (LR)^{i+1} = R \circ (LR)^i \circ L \circ R \circ R \circ (LR)^{i+1} = R \circ (LR)^i \circ L \circ (LR)^{i+1} = R \circ (LR)^i \circ L \circ L \circ R \circ (LR)^i = R \circ (LR)^i \circ R \circ (LR)^i$, que é a identidade por hipótese de indución. Agora imos estudar que ocorre cando $i \neq j$

  Se $j > i$, entón $R \circ (LR)^i \circ R \circ (LR)^j = (R \circ (LR) \circ R \circ (LR)^i) \circ (LR)^{j-i} = id \circ (LR)^{j-i} = (LR)^{j-i}$ pertence a PLR.

  Se $j < i$, entón
  $$\begin{aligned} R \circ (LR)^i \circ R \circ (LR)^j &= R \circ (LR)^{i-j} \circ (LR)^j \circ R \circ (LR)^j = \\ &= R \circ (LR)^{i-j-1} \circ L \circ (R \circ (LR)^j \circ R \circ (LR)^j) = R \circ (LR)^{i-j-1} \circ L \circ id = \\ &= R \circ (LR)^{i-j-1} \circ L = (RL)^{i-j} = (LR)^{11(i-j)}, \text{ que pertence a } PLR. \end{aligned}$$
  A última igualdade débese a que $(RL) = (LR)^{11}$.

- Analiceemos o caso $(LR)^i \circ (LR)^j$. Pola Proposición 3.17, cúmprese que $(LR)^i \circ (LR)^j = (LR)^{i+j} = (LR)^{i+j(\text{mód } 12)}$, que está en PLR.

- Como consecuencia do caso $(LR)^i \circ (LR)^j$, a composición $R \circ (LR)^i \circ (LR)^j$ está en PLR.

- Finalmente, estudemos que ocorre con $(LR)^i \circ R \circ (LR)^j$. Utilizando o primeiro caso e que $L = R \circ (LR)^{11}$, conclúese que $(LR)^i \circ R \circ (LR)^j = L \circ (R \circ (LR)^{i-1} \circ R \circ (LR)^j) = R \circ (LR)^{11} \circ (R \circ (LR)^{i-1} \circ R \circ (LR)^j)$ tamén pertence a PLR.

Visto que o conxunto é pechado para a composición, comprobemos que efectivamente é un grupo. A composición de funcións é asociativa, e polo tanto cúmprese a asociatividade. Con respecto

aos inversos, acábase de ver que $R \circ (LR)^i \circ R \circ (LR)^i = id$, e así $(R(LR)^i)^{-1} = R(LR)^i$. Por outra banda, $((LR)^i)^{-1} = (LR)^{-i} = (LR)^{-i(\text{mód } 12)} = (LR)^j$, sendo $j \equiv -i(\text{mód } 12)$. □

3.2.3. O isomorfismo entre TI e PLR

A continuación estudarase a relación que hai entre os grupos TI e PLR. Probarase que hai un isomorfismo entre ámbolos dous grupos, e que os dous serán tamén isomorfos ao grupo diédrico de orde 24. Polo tanto, o grupo simétrico do polígono regular de 12 lados é isomorfo a dous subgrupos de $S_{\mathcal{M}}$, un formado a partir dun ciclo de orde 12 e unha transposición, e outro formado a partir de tres transposicións. Ademais, polo visto no Exemplo 1.86, D_{12} ten presentación libre da forma $D_{12} = \langle x, y \mid x^{12} = 1,\ y^2 = 1,\ xyxy = 1 \rangle$.

Teorema 3.21. *O grupo TI é isomorfo ao grupo diédrico de orde 24.*

Demostración. Tense que o grupo TI está xerado polos elementos T_1 e I_0. Ademais, verifícase que $(T_1)^{12} = (I_0)^2 = id$. Vexamos que $(T_1 \circ I_0)^2 = id$. Sexa $\{x, y, z\} \in \mathcal{M}$. Entón, $(T_1 \circ I_0)^2(\{x, y, z\}) = T_1(I_0(T_1(I_0(\{x, y, z\})))) = T_1(I_0(T_1(\{-x, -y, -z\}))) = T_1(I_0(\{-x + 1, -y + 1, -z + 1\})) = T_1(\{x - 1, y - 1, z - 1\}) = \{x, y, z\} = id(\{x, y, z\})$.

Entón, polo Teorema de van Dyck 1.85, existe un epimorfismo $D_{12} \to TI$. Polo tanto, é claro que $|D_{12}| \geq |TI| = 24$, dado que en TI hai exactamente 24 funcións distintas. Non obstante, sábese que D_{12} ten orde 24 e deste xeito o epimorfismo é en realidade un isomorfismo, e así TI é isomorfo a D_{12}. □

É sinxelo visualizar este resultado, debido a que D_{12} se corresponde co grupo simétrico do dodecágono, e xa se dixo que T_n se corresponden con rotacións, I_0 coa reflexión con respecto ao eixo vertical e o resto de reflexións I_n obtéñense facendo primeiro I_0 e a continuación T_n. O grupo TI está xerado entón por T_1 e I_0, verificando estes as relacións $(T_1)^{12} = id$, $(I_0)^2 = id$ e $(T_1 \circ I_0)^2$.

Vexamos que o grupo PLR ten a mesma presentación libre.

Teorema 3.22. *O grupo PLR é isomorfo ao grupo diédrico D_{12} de orde 24.*

Demostración. O grupo PLR está xerado polos elementos LR e R. Ademais, verifícase que $(LR)^{12} = (R)^2 = id$. Vexamos que $(LR \circ R)^2 = id$. Así, $(TLR \circ R)^2 = (L \circ R^2)^2 = (L)^2 = id$.

Polo Teorema de van Dyck 1.85, existe un epimorfismo $D_{12} \to PLR$. Polo tanto, como en PLR hai exactamente 24 funcións distintas, é claro que $|D_{12}| \geq |PLR| = 24$. Non obstante, sábese que D_{12} ten orde 24, e deste xeito o epimorfismo é en realidade un isomorfismo, e así PLR é isomorfo a D_{12}. □

Así, tense inmediatamente que os grupos TI e PLR son isomorfos por ser ambos isomorfos ao grupo diédrico D_{12} de orde 24. Deste xeito, o isomorfismo que se constrúe será o que leve os xeradores dun grupo nos xeradores do outro respectando que se cumpran as relacións, ademais de levar o elemento neutro dun grupo no do outro. Entón, o isomorfismo buscado será $\psi : PLR \to TI$ tal que $\psi(LR) = T_1$, $\psi(R) = I_0$ e $\psi((LR)^0) = T_0$. Ademais, o resto das correspondencias mostran unha especie de patrón entre os subíndices das funcións T_n e I_n e as potencias de RL. É dicir, $\psi((LR)^n) = T_n$ e $\psi(R \circ (LR)^n) = I_{12-n}$, sendo $n \in \mathbb{Z}_{12}$.

Vexamos que, efectivamente, ψ é un isomorfismo.

Teorema 3.23. *Existe un isomorfismo $\psi : PLR \to TI$, cumprindo que $\psi((LR)^n) = T_n$ e $\psi(R \circ (LR)^n) = I_m$, sendo $m \equiv -n$(mód 12).*

Demostración. A función definida así é claramente bixectiva, xa que todo elemento do dominio se leva a exactamente un elemento do codominio, e que tódolos elementos do codominio teñen unha preimaxe. Entón agora hai que ver que para calquera par de elementos $f, g \in PLR$ e $x \in \mathcal{M}$ se ten que $\psi(f \circ g)(x) = \psi(f)(\psi(g)(x))$.

- Sexa $x \in \mathcal{M}$, $f = LR$ e $G = R$.

  Tense que $\psi(f \circ g)(x) = \psi((LR) \circ R)(x) = \psi(L \circ R^2)(x) = \psi(L)(x) = \psi(R \circ (LR)^{11})(x) = I_1(x)$.

  Por outra banda, $\psi(f)(\psi(g)(x)) = \psi(LR)(\psi(R)(x)) = T_1(I_0(x)) = I_{1+0}(x) = I_1(x)$.

  Así, chégase á igualdade.

- Sexan agora $f = R$ e $g = LR$.

  En primeiro lugar, $\psi(f \circ g)(x) = \psi(R \circ LR)(x) = I_{11}(x)$.

  Ademais, $\psi(f)(\psi(g)(x)) = \psi(R)(\psi(LR)(x)) = I_0(T_1(x)) = I_{0-1}(x) = I_{-1}(x) = I_{11}(x)$, chegando de novo á igualdade.

- Tomemos agora $f = LR$ e $g = LR$.

  Por un lado, $\psi(f \circ g)(x) = \psi((LR) \circ (LR))(x) = \psi((LR)^2)(x) = T_2(x)$.

  Polo outro lado, $\psi(f)(\psi(g)(x)) = \psi(LR)(\psi(LR)(x)) = T_1(T_1(x)) = T_{1+1}(x) = T_2(x)$.

- Por último, consideremos $f = R$ e $g = R$.

  Por unha banda, $\psi(g \circ g)(x) = \psi(R \circ R)(x) = \psi(id)(x) = \psi((LR)^0)(x) = T_0(x)$.

  Polo outro lado, $\psi(f)(\psi(g)(x)) = \psi(R)(\psi(R)(x)) = I_0(I_0(x)) = T_{0+0}(x) = T_(x)$.

Queda entón probado que $\psi(f \circ g)(x) = \psi(f)(\psi(g)(x))$ para $x \in \mathcal{M}$ e $f, g \in PLR$, o que implica que ψ é un homomorfismo. Como xa se dixo, ψ é bixectivo, e polo tanto é un isomorfismo. □

3.3. Accións dos grupos TI e PLR sobre $\mathcal{M}$

Nesta sección verase que $\mathcal{M}$ é tanto un TI-conxunto coma un PLR-conxunto. Así, estudaranse os conceptos de accións de grupos nos casos particulares dos grupos TI e PLR actuando sobre $\mathcal{M}$.

3.3.1. O grupo TI

Comézase observando que o grupo TI é un subgrupo do grupo simétrico xerado por $\mathcal{M}$, $S_{\mathcal{M}}$, xa que os seus elementos son funcións bixectivas de $\mathcal{M}$ en $\mathcal{M}$. Ademais, como xa se dixo, o grupo TI está xerado por unha transposición e un ciclo de orde 12 en $\mathcal{M}$. Entón, tense unha acción de TI actuando sobre $\mathcal{M}$, $TI \times \mathcal{M} \to \mathcal{M}$. Vexámolo.

Proposición 3.24. *O grupo TI actúa sobre o conxunto $\mathcal{M}$, é dicir, $\mathcal{M}$ é un TI-conxunto.*

Demostración. Defínese a acción $\alpha : TI \times \mathcal{M} \to \mathcal{M}$ coma a avaliación dunha función de TI sobre un elemento $x \in \mathcal{M}$. Entón, $\alpha(g, x) = gx = g(x)$.

En primeiro lugar, tense trivialmente que $T_0 x = T_0(x) = x$ para todo $x \in \mathcal{M}$.

En segundo lugar, hai que probar que $g(hx) = (gh)x$ para todos $g, h \in TI$ e $x \in \mathcal{M}$. Vexamos os distintos casos.

- Se $g = T_n$ e $h = T_l$, entón $T_n(T_l x) = T_n(T_l(x)) = (T_n \circ T_l)(x) = (T_n T_l)(x)$.
- Se $g = T_n$ e $h = I_l$, entón $T_n(I_l x) = T_n(I_l(x)) = (T_n \circ I_l)(x) = (T_n I_l)(x)$.
- Se $g = I_n$ e $h = T_l$, entón $I_n(T_l x) = I_n(T_l(x)) = (I_n \circ T_l)(x) = (I_n T_l)(x)$.
- Se $g = I_n$ e $h = I_l$, entón $I_n(I_l x) = I_n(I_l(x)) = (I_n \circ I_l)(x) = (I_n I_l)(x)$.

Queda así probado que o grupo TI actúa sobre $\mathcal{M}$. □

Dado $x \in \mathcal{M}$ pode agora calcularse a súa órbita de x e o seu subgrupo de isotropía.

Proposición 3.25. *Se $x \in \mathcal{M}$, verifícase que $TIx = \mathcal{M}$ e $TI_x = T_0$.*

Demostración. En primeiro lugar sexa $x \in \mathcal{M}$ unha tríade maior ou menor. Se é maior, aplicando T_1 12 veces obtéñense o resto de tríades maiores. Por outra banda, aplicando I_0 obtense unha tríade menor, á que se se lle aplica T_1 12 veces dá como resultado o resto de tríades menores. Pode razoarse dun xeito análogo se a tríade inicial é menor. Así, partindo dunha tríade calquera

de $\mathcal{M}$, aplicando as funcións de TI obtéñense os 24 elementos de $\mathcal{M}$. Deste xeito, a órbita de x é $TIx = \{\psi x \mid \psi \in TI\} = \mathcal{M}$.

Por outra banda, utilizando a Proposición 1.66, tense que $|TIx| = (TI : TI_x) = |TI|/|TI_x| \Rightarrow |TI_x| = |TI|/|TIx|$. Agora ben, como en TI hai 24 funcións e $TIx = \mathcal{M}$, entón $|TI| = |TIx| = 24$, o que implica que $|TI_x| = 1$. Entón, $idx = x$, e polo tanto o único elemento de TI_x é a identidade, é dicir, $TI_x = \{\psi \in TI | \psi x = x\} = id = T_0$. □

A continuación, probarase que esta acción é fiel e transitiva.

Proposición 3.26. *A acción do grupo TI en $\mathcal{M}$ é regular.*

Demostración. En primeiro lugar, como se acaba de ver na proposición anterior, $TI_x = T_0$, para $x \in \mathcal{M}$, e polo tanto a acción é fiel.

Por outra banda, dado $x \in \mathcal{M}$, $TIx = \mathcal{M}$. Entón, para todos $y, z \in \mathcal{M}$, existen $\phi, \psi \in TI$ tales que $y = \phi x$ e $z = \psi x$. Así, $(\phi)^{-1}(y) = x$ e $(\psi \circ \phi^{-1})y = \psi(\phi^{-1}(y)) = \psi x = z$, o que implica que existe $\psi \circ \phi^{-1} \in TI$ de xeito que leva y en z. Finalmente, se existen $\phi, \psi \in TI$ de xeito que $\phi x = \psi x$, tense que $(\psi^{-1} \circ \phi)x = x$. Non obstante, coma $TI_x = T_0$ terase que $\psi^{-1} \circ \phi = id$, o que implica que $\psi = \phi$. Así, a acción é transitiva.

Deste xeito, pola Definición 1.73, a acción é regular. □

3.3.2. O grupo PLR

Analogamente ao feito co grupo TI, é fácil darse conta de que o grupo PLR é un subgrupo do grupo simétrico xerado por $\mathcal{M}$, $S_{\mathcal{M}}$, cuxos elementos P, L e R son transposicións.

Proposición 3.27. *O grupo PLR actúa sobre o conxunto $\mathcal{M}$, ou o que é o mesmo, o conxunto $\mathcal{M}$ é un PLR-conxunto.*

Demostración. Defínese a acción $\alpha : PLR \times \mathcal{M} \to \mathcal{M}$ coa avaliación dunha función de PLR nun elemento $x \in \mathcal{M}$. É dicir, para $g \in PLR$, terase que $\alpha(g, x) = gx = g(x)$.

En primeiro lugar, tense trivialmente que $(LR)^0 x = (LR)^0(x) = x$ para todo $x \in \mathcal{M}$.

En segundo lugar, hai que probar que $g(hx) = (gh)x$ para todos $g, h \in TI$ e $x \in \mathcal{M}$. Vexamos os distintos casos.

- Se $g = (LR)^n$ e $h = (LR)^l$, entón $(LR)^n((LR)^l x) = (LR)^n((LR)^l(x)) = ((LR)^n \circ (LR)^l)(x)$.
- Se $g = R \circ (LR)^n$ e $h = (LR)^l$, entón $R \circ (LR)^n((LR)^l x) = R \circ (LR)^n((LR)^l(x)) = (R \circ (LR)^n \circ (LR)^l)(x)$.

- Se $g = (LR)^n$ e $h = R \circ (LR)^l$, entón $(LR)^n(R \circ (LR)^l x) = (LR)^n(R \circ (LR)^l(x)) = ((LR)^n \circ R \circ (LR)^l)(x)$.
- Se $g = R \circ (LR)^n$ e $h = R \circ (LR)^l$, entón $R \circ (LR)^n(R \circ (LR)^l x) = R \circ (LR)^n(R \circ (LR)^l(x)) = (R \circ (LR)^n \circ R \circ (LR)^l)(x)$.

Queda así probada a proposición. □

Pódense entón identificar as órbitas e os subgrupos de isotropía dun elemento $x \in \mathcal{M}$ asociados a esta acción.

Proposición 3.28. *Se $x \in \mathcal{M}$, entón $PLRx = \mathcal{M}$ e $PLR_x = (LR)^0$.*

Demostración. Xa se dixo anteriormente que partindo dunha tríade $x \in \mathcal{M}$ se obteñen os 24 elementos de $\mathcal{M}$ aplicando $(LR)^n$ e $R \circ (LR)^n$ con $n = 0, ..., 11$. Deste xeito, a órbita de x é $PLRx = \{\psi x \mid \psi \in PLR\} = \mathcal{M}$. Isto implica que $|PLRx| = 24$

Agora ben, utilizando a Proposición 1.66, tense $|PLRx| = (PLR : PLR_x) = |PLR|/|PLR_x|$, o que implica que $|PLR_x| = |PLR|/|PLRx|$. Deste xeito, como en PLR se teñen 24 funcións, e $|PLRx| = 24$, terase que $|PLR_x| = 1$. Unindo isto con que $idx = x = (LR)^0 x$, o único elemento de PLR_x é a identidade, é dicir, $PLR_x = \{\psi \in PLR | \psi x = x\} = id = (LR)^0$. □

A continuación verase que propiedades verifica esta acción.

Proposición 3.29. *A acción do grupo PLR en $\mathcal{M}$ é regular.*

Demostración. En primeiro lugar, como se acaba de ver na proposición anterior tense que, para $x \in \mathcal{M}$, $TI_x = (LR)^0$, e polo tanto a acción é fiel.

Por outra banda, dado $x \in \mathcal{M}$, $PLRx = \mathcal{M}$. Entón, para todos $y, z \in \mathcal{M}$ tense que existen $\phi, \psi \in PLR$ tales que $y = \phi x$ e $z = \psi x$. Así, $(\phi)^{-1}(y) = x$ e $(\psi \circ \phi^{-1})y = \psi(\phi^{-1}(y)) = \psi x = z$, o que implica que existe $\psi \circ \phi^{-1} \in PLR$ de xeito que leva y en z. Finalmente, se existen $\phi, \psi \in PLR$ de xeito que $\phi x = \psi x$, tense que $(\psi^{-1} \circ \phi)x = x$. Non obstante, como $PLR_x = (LR)^0$ terase que $\psi^{-1} \circ \phi = id$, o que implica que $\psi = \phi$. Así, a acción é transitiva.

Logo, pola Definición 1.73, tense que a acción é regular. □

3.4. Conmutatividade e dualidade

Dada unha acción dun grupo nun conxunto, xa se viu no primeiro capítulo o que é o centralizador dun subgrupo dun grupo. A continuación estudaranse os centralizadores de TI e PLR en

$S_{\mathcal{M}}$. Verase que son subgrupos do grupo simétrico $S_{\mathcal{M}}$ isomorfos tales que un é o centralizador do outro. Unindo isto ao estudado ata agora, veremos que os grupos son duais.

Lema 3.30. *O elementos dos grupos TI e PLR conmutan entre eles.*

Demostración. Bastará probar a conmutatividade entre os xeradores de cada grupo, polo que se terán catro casos. Farase a proba para unha tríade menor $\{x, y, z\} \in \mathcal{M}$, sendo análoga para tríades maiores.

- $T_1 \circ (LR) = (LR) \circ T_1$:

  $T_1(LR(\{x, y, z\})) = T_1(L(R(\{x, y, z\}))) = T_1(L(\{y, z, x-2\})) = T_1(\{z, x-2, y-1\}) = \{z+1, x-1, y\}$.

  E por outra parte, $LR(T_1(\{x, y, z\})) = L(R(T_1(\{x, y, z\}))) = L(R(\{x+1, y+1, z+1\})) = L(\{y+1, z+1, x-1\}) = \{z+1, x-1, y\}$.

- $T_1 \circ R = R \circ T_1$:

  Por un lado da igualdade, $T_1(R(\{x, y, z\})) = T_1(\{y, z, x-2\}) = \{y+1, z+1, x-1\}$.

  Por outro lado, $R(T_1(\{x, y, z\})) = R(\{x+1, y+1, z+1\}) = \{y+1, z+1, x-1\}$.

- $I_0 \circ (LR) = (LR) \circ I_0$:

  Por unha banda, tense $I_0(LR(\{x, y, z\})) = I_0(L(R(\{x, y, z\}))) = I_0(L(\{y, z, x-2\})) = I_0(\{z, x-2, y-1\}) = \{-z, -x+2, -y+1\}$.

  Pola outra banda terase $(LR(I_0(\{x, y, z\}))) = L(R(I_0(\{x, y, z\}))) = L(R(\{-x, -y, -z\})) = L(R(\{-x, -x-3, -x-7\})) = L(R(\{-x, -x+9, -x+5\})) = L(R(\{-x+5, -x+9, -x\})) = L(R(\{-z, -y, -x\})) = L(\{-x+2, -z, -y\}) = \{-y+1, -x+2, -z\}$. Como xa se dixo, os acordes son conxuntos non ordenados, entón chégase á igualdade.

- $I_0 \circ R = R \circ I_0$:

  Por un lado, $I_0(R(\{x, y, z\})) = I_0(\{y, z, x-2\}) = \{-y, -z, -x+2\}$.

  Polo outro, $R(I_0(\{x, y, z\})) = R(\{-x, -y, -z\}) = I_0(\{-z, -y, -x\}) = \{-x+2, -z, -y\}$. De novo, chegamos a que os conxuntos teñen os mesmos elementos, polo que son o mesmo.

□

A continuación, visto este lema, veremos unha definición que caracterizará posteriormente aos grupos TI e PLR.

Definición 3.31. Sexa X un conxunto e S_X o grupo simétrico sobre X. Se H e K son dous subgrupos de S_X tales que cada un define unha acción regular sobre X, e un é o centralizador do outro en S_X, entón dise que H e K son **duais**.

A continuación, verase que TI e PLR verifican as condicións da definición anterior.

Teorema 3.32. *Os grupos TI e PLR son duais.*

Demostración. Xa se dixo anteriormente que TI e PLR son subgrupos do grupo simétrico de $\mathcal{M}$, xa que son transformacións de $\mathcal{M}$ en si mesmo. Ademais, xa se probou na Proposición 3.26 e na Proposición 3.29 que as accións dos grupos TI e PLR sobre $\mathcal{M}$ son regulares. Entón o que falta por ver é que un é o centralizador do outro.

Consideremos o centralizador do grupo TI, $C_{\mathcal{M}}(TI) = \{g \in S_{\mathcal{M}} \mid g\varphi = \varphi g \ \forall \varphi \in TI\}$. Polo Lema 3.30 tense que $g\varphi = \varphi g$ para todo $g \in PLR$ e $\varphi \in TI$, polo que $PLR \subset C_{\mathcal{M}}(TI)$.

Como se ten que $C_{\mathcal{M}}(TI) \in S_{\mathcal{M}}$, o que hai que ver é que en $C_{\mathcal{M}}(TI)$ só hai as funcións de PLR. Estudemos o subgrupo de isotropía de x en $C_{\mathcal{M}}(TI)$, é dicir, $(C_{\mathcal{M}}(TI))_x = \{g \in C_{\mathcal{M}}(TI) \mid gx = x\}$. Entón, tómase $f \in C_{\mathcal{M}}(TI)$ de xeito que $f(x) = x$ e sexa $g \in TI$. Así, $g(f(x)) = g(x)$, e como $f \in C_{\mathcal{M}}(TI)$, terase que $f(g(x)) = g(x)$.

Pola Proposición 3.26 sábese que a acción de TI sobre $\mathcal{M}$ é regular, e entón para todo elemento $y \in \mathcal{M}$ tense que existe $g \in TI$ tal que $y = g(x)$.

Entón, $f(g(x)) = f(y) = g(x) = y$ para todos $x, y \in \mathcal{M}$, e entón $f(y) = y$.

Como f é o único elemento en $C_{\mathcal{M}}(TI)$ que deixa fixo calquera elemento en $C_{\mathcal{M}}(TI)$, debe ser a identidade (único elemento que deixa fixas tódalas tríades de $\mathcal{M}$). Así, $(C_{\mathcal{M}}(TI))_x = \{id\}$ é o grupo trivial.

Agora ben, a órbita de calquera elemento $x \in \mathcal{M}$ é $\mathcal{M}$, polo que $|(C_{\mathcal{M}}(TI))x| = 24$. Ademais, como se acaba de ver que $(C_{\mathcal{M}}(TI))_x = \{id\}$, tense que $|(C_{\mathcal{M}}(TI))_x| = 1$. Utilizando a Proposición 1.66, $|(C_{\mathcal{M}}(TI))x| = |(C_{\mathcal{M}}(TI))|/|(C_{\mathcal{M}}(TI))_x|$. Polo tanto, $|C_{\mathcal{M}}(TI)| = 24$.

Como $PLR \subset C_{\mathcal{M}}(TI)$ e teñen o mesmo número de elementos, son iguais, é dicir, $C_{\mathcal{M}}(TI)$ é exactamente o grupo PLR.

Cun razoamento totalmente análogo, chégase ao resultado de que o centralizador de PLR, $C_{\mathcal{M}}(PLR)$ é TI. □

Deste xeito, queda visto que os dous grupos de transformacións sobre o conxunto das tríades maiores e menores vistos, TI e PLR, son duais. É dicir, téñense dous grupos isomorfos non coincidentes de xeito que un é o centralizador do outro. Así, ambos grupos expoñen de formas matemáticas distintas a mesma simetría subxacente no conxunto das tríades maiores e menores

Bibliografía

[1] Agustín-Aquino, O. A., du Plessis, J., Lluis-Puebla, E. e Montiel, M. (2009). *Una introducción a la Teoría de Grupos con aplicaciones en la Teoría Matemática de la Música*, Publicaciones Electrónicas Sociedad Matemática Mexicana Serie: Textos. Vol. 10.

[2] Carstensen, C., Fine, B. e Rosenberger, G. (2011). *Abstract Algebra: Applications to Galois Theory, Algebraic Geometry and Cryptography*, De Gruyter.

[3] Cohn, P. M. (1974). *Algebra*, 2nd ed., Volume 1, John Wiley & Sons.

[4] Crans, A. S., Fiore, T. M. e Satyendra, R. (2009). Musical Actions of Dihedral Groups. *The American Mathematical Monthly*, 116(6), 479-495.

[5] Dorronsoro, J. e Hernández E. (1996). *Números, grupos y anillos*, Addison-Wesley Iberoamericana España S.A.

[6] Dummit, D. S. e Foote R. M. (2004), *Abstract Algebra*, 3rd ed, John Wiley & Sons.

[7] Fraileigh, J. B.(1993) *A first course in Abstract Algebra*, 5th ed., Addison-Wesley.

[8] Hungerford, T. W. (1974). *Algebra*, Graduate Texts in Mathematics, 73, Springer-Verlag.

[9] James, G. e Liebeck, M. (1993). *Representations and Characters of Groups*, Cambridge Mathematical Textbooks, Cambridge University Press.

[10] Ledermann, W. (1976). *Introduction to group theory*, Longman Group Limited.

[11] Du Plessis, J. (2008). *Transformation Groups and Duality in the Analysis of Musical Structure*. Tesis de maestría, Universidad Estatal de Georgia.

[12] Rotman, J. J. (1995). *An Introduction to the Theory of Groups*, 4th ed., Graduate Texts in Mathematics, 148, Springer-Verlag.