UNIVERSIDAD DE EL SALVADOR
FACULTAD MULTIDISCIPLINARIA ORIENTAL
DEPARTAMENTO DE CC.NN Y MATEMÁTICA
SECCIÓN DE MATEMÁTICA
LICENCIATURA EN MATEMÁTICA

TEMA DE INVESTIGACIÓN:
INTRODUCCIÓN A LA TEORÍA GEOMÉTRICA DE GRUPO

PRESENTADA POR:
KATERINNE ALEJANDRA MORAGA CHÉVEZ
MARLYN JOANNA OJEDA SALGADO
ELSY NURI ZAVALA BONILLA

INFORME FINAL DE INVESTIGACIÓN PARA OPTAR AL TÍTULO DE:
LICENCIADAS EN MATEMÁTICA

DOCENTE ASESOR:
LICENCIADO MARIO FRANCISCO HERNÁNDEZ HERNÁNDEZ

FECHA DE ENTREGA:
20 DE FEBRERO DE 2023

Ciudad de San Miguel, El Salvador, Centroamérica.

UNIVERSIDAD DE EL SALVADOR
AUTORIDADES

MSC. ROGER ARMANDO ARIAS ALVARADO
RECTOR

DR.RAÚL ERNESTO AZCÚNAGA LÓPEZ
VICE-RECTOR ACADÉMICO

ING.AGRO. JUAN ROSA QUINTANILLLA QUINTANILLA
VICE-RECTOR ADMINISTRATIVO

DR. FRANSISCO ANTONIO ALARCÓN SANDOVAL
SECRETARIO GENERAL

LIC. RAFAEL HUMBERTO PEÑA MARÍN
FISCAL GENERAL

LIC. LUIS ANTONIO MEJÍA LIPE
DEFENSOR DE LOS DERECHOS UNIVERSITARIOS

FACULTAD MULTIDISCIPLINARIA ORIENTAL
AUTORIDADES

LIC. CRISTOBAL HERNÁN RÍOS BENÍTEZ
DECANO

LIC. OSCAR VILLALOBOS
VICE-DECANO

LIC. ISRAEL LÓPEZ MIRANDA
SECRETARIO

MTRO. JORGE PASTOR FUENTES
DIRECTOR GENERAL DE PROCESO DE GRADUACIÓN

DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMÁTICA
SECCIÓN DE MATEMÁTICA
AUTORIDADES

MTRA. KARLA MARÍA MEJÍA ORTÍZ
JEFA DEL DEPARTAMENTO

LICDA. MARIA OLGA QUINTANILLA DE LOVO
COORDINADORA DE LA CARRERA O SECCIÓN

LICDA. SONIA DEL CARMEN MARTÍNEZ DE LÓPEZ
COORDINADOR GENERAL DE PROCESO DE GRADUACIÓN

Agradecimientos

Al finalizar un trabajo arduo como lo es la tesis es imposible no sentirnos agradecidas por el camino recorrido y el bello final al que hemos llegado. Además, no es justo quedarnos con todo el mérito y no pensar en quienes formaron parte de este trayecto, es por ello que queremos utilizar este espacio para agradecerles:

Primeramente a Dios que nos permitió vivir este proceso con sus altos y bajos, con sus momentos de crecimiento en todas su facetas y aprendizajes en esta aventura que comenzamos en el año 2017. A nuestros padres quienes nos apoyaron incanzablemente en todos estos años de formación, por confiar y creer más que nadie en nosotros.

Gracias a cada docente que estuvo presente en estos años de formación, de manera especial al **MSc. Jorge Alberto Martínez Gutiérrez** quien siempre tuvo palabras de ánimo, consejos y corrección en el momento oportuno. Por motivarnos a tomar grandes retos para superarnos a nosotras mismas y tomar este camino que finalmente se termina. De igual manera al **Licenciado Mario Francisco Hernández Hernández** por tomar junto con nosotras este reto y poder realizar esta tesis bajo su dirección, por la confianza en nuestro trabajo y sobre todo por su capacidad de orientarnos de manera rigurosa e invitarnos a seguir aprendiendo constantemente. Y también al **Licenciado Oscar Rutilio Molina Medrano** quién no se negó a orientarnos en esta temática que es su especialidad, infinitas gracias.

Finalmente y no menos importante, agradecemos a la institución que nos formó: Universidad de El Salvador, FMO. Por abrir sus puertas a las generaciones que tienen deseos de superación y darnos un ventanal a las nuevas oportunidades.

Katerinne Alejandra Moraga Chévez.
Marlyn Joanna Ojeda Salgado.
Elsy Nuri Zavala Bonilla.

Índice general

Notación

Símbolos

$\curvearrowright$	actúa sobre
$\lvert\cdot\rvert$	cardinalidad, valor absoluto
$.^*$	conjunto de palabras sobre, o mapeo inducido en palabras
$[a,b[$	conjunto semiabierto
$\circ$	composición de mapeos
$\subset$	contención de conjuntos
$\sim_{QI}$	es cuasi-isométrico a
$\sim$	es equivalente a
$\cong$	es isomorfo a
$\lhd$	es un subgrupo normal a
$\cap$	intersección de conjuntos
$[0,1]$	intervalo unitario en $\mathbb{R}$
$\hat{\cdot}$	inversa formal
$>$	mayor que
$<$	menor que
$\geq$	mayor o igual
$\leq$	menor o igual
$\times$	producto cartesiano
$\cdot$	producto
$\cup$	unión de conjuntos

A

Aut	automorfismo de grupo
A^*	conjunto de palabras finitas

B

$B_r^{X,d}(x)$	bola de radio r alrededor de x en (X,d)

C

$\mathbb{C}$	conjunto de números complejos
$\mathrm{Cay}(G,S)$	grafo de Cayley de G con respecto a S

D

diam B	diámetro de B
dim X	dimensión de X
D_n	grupo diédrico de grado n
d_s	métrica de palabras con respecto a S

E

e	elemento neutral en un grupo
ϵ	palabra vacía

F

F_{red}	conjunto de palabras reducidas
$F(S)$	grupo generado por S
F_n	grupo libre de rango 2
F_2	grupo libre de rango n

G

g^{-1}	elemento del grupo inverso
$G \setminus X$	espacio cociente
G/N	grupo cociente
G_x	grupo estabilizador de x
$G \cdot x$	G-órbita de x
$[G:H]$	índice de H en G

I

id_x	identidad en x
id_y	identidad en y
im	imagen de un mapeo
Isom	grupo de isometrías

K

ker	kernel de un homomorfismo

M

Mor_C	morfismo de C

N

$\mathbb{N}$	conjunto de enteros no negativos

O

Ob	clases de objetos
$\varnothing$	conjunto vacío

P

φ^*	mapeo inducido en palabras

Q

$\mathbb{Q}$	conjunto de números racionales

R

$\mathbb{R}$	conjunto de números reales

S

$\mathbb{S}^1$	círculo unitario
$\widehat{S}$	conjunto de inversas formales de S
$\left(S \cup \widehat{S}\right)^*$	conjunto de palabras sobre $S \cup \widehat{S}$
$\left(S \cup S^{-1}\right)^*$	conjunto de palabras sobre $S \cup S^{-1}$
S_n	grupo simétrico sobre
$\langle S \mid R \rangle$	grupo generado por S con relación a R
$\langle S \rangle_G$	subgrupo de G generado por S
$\langle S \rangle_G^{\triangleleft}$	subgrupo normal generado por S en G

T

T_G	conjunto de todos los subárboles de

X

X^g	conjunto fijo de g

Z

$\mathbb{Z}$	conjunto de números enteros
$\mathbb{Z}/n$	conjunto de enteros módulo n

Resumen

La teoría geométrica de grupos es un área de la matemática que se dedica al estudio de los grupos finitamente generados mediante las exploraciones entre las propiedades de tales grupos y las propiedades geométricas de los espacios donde estos grupos actúan (esto es, cuando los grupos en cuestión son realizados como simetrías geométricas o transformaciones continuas de algunos espacios).

En nuestra investigación bibliográfica estudiamos la teoría geométrica de grupos con la idea de considerar los mismos grupos finitamente generados como objetos geométricos, usamos formas para estudiar grupos, que son los grafos, cada uno de sus vértices son elementos del grupo en cuestión, además, aunque el mismo grupo puede tener grafos moderadamente diferentes, no le impide usar uno para estudiar el grupo. El estudio de ver los grupos como objetos geométricos es usualmente hecho mediante el estudio del grafo de Cayley del grupo, pasando por las acciones de grupo en el cual se puede contemplar una generalización de los grupos como grupos de simetría, hasta llegar a que la estructura del grafo esta adosada a un espacio métrico, mediante una métrica llamada métrica de palabras.

Es importante el estudio de los grupos finitamente generados hasta la cuasi-isometría, para poder llegar a nuestro objetivo, el lema de Švarc-Milnor. En la práctica, este resultado nos indica dos cosas; Si queremos saber más sobre la geometría de un grupo o si queremos saber que un grupo dado está finitamente generado, en este caso, exhibir una buena acción de este grupo en un espacio adecuado es suficiente. Por el contrario, si queremos saber más sobre un espacio métrico, basta con encontrar una buena acción de un grupo conocido adecuado. Por lo tanto, el lema de Švarc-Milnor también se denomina "lema fundamental de la teoría geométrica de grupos".

Palabras claves: Grupos finitamente generados, grafos de Cayley, acciones de grupo, métrica de palabra,cuasi-isometría, lema de Švarc-Milnor.

Abstract

The geometric theory of groups is an area of mathematics that is dedicated to the study of finitely generated groups by explorations between the properties of such groups and the geometric properties of spaces where these groups act (that is, when the groups in question are performed as geometric symmetries or continuous transformations of some spaces).

In our bibliographical research we study the geometric theory of groups with the idea of considering the same finitely generated groups as geometric objects, we use forms to study groups, which are graphs, each of its vertices are elements of the group in question, in addition, although the same group may have moderately different graphs, it does not prevent you from using one to study the group. The study of seeing groups as geometric objects is usually done by studying the group's Cayley graph, passing through group actions in which a generalization of groups as symmetry groups can be contemplated, until the structure of the graph is attached to a metric space, using a metric called word metric.

It is important to study finitely generated groups up to quasi-isometry, to reach our goal, the Švarc-Milnor lemma. In practice, this result tells us two things; if we want to know more about the geometry of a group or if we want to know that a given group is finitely generated, in this case, exhibiting a good action of this group in a suitable space is enough. On the contrary, if we want to know more about a metric space, it is enough to find a good action of a suitable known group. Therefore, the motto Švarc-Milnor is also called "fundamental motto of geometric group theory".

Keywords: Finitely generated groups, Cayley graphs, group actions, word metric, quasi-isometry, Švarc-Milnor lemma.

Introducción

La teoría geométrica de grupo surgió de la teoría combinatoria de grupos que estudiaba en gran medida las propiedades de los grupos discretos mediante el análisis de presentaciones grupales, que describen a los grupos como cocientes de grupos libres. Este campo fue estudiado sistemáticamente por primera vez por Walther Franz Anton von Dyck (1856- 1934).

En la primera mitad del siglo XX, el trabajo pionero de Max Wilhelm Dehn (1878-1952), Jakob Nielsen (1957), Kurt Reidemeister (1893-1971), Otto Sch. (1901-1929), JHC Whitehead (1904-1960), Egbert van Kampen (1908-1942), entre otros, introdujo algunas ideas topológicas y geométricas en el estudio de grupos discretos, además demostraron que cualquier subgrupo de un grupo libre también es libre.

Lo siguiente a destacar son los grafos de Cayley deben su nombre al matemático Arthur Cayley, uno de los fundadores de la escuela británica moderna de matemáticas puras, que trabajó principalmente en teoría de grafos y teoría de grupos. Además, fue miembro de la Royal Society of London for Improving Natural Knowledge y recibió la medalla Copley en 1882, antes de recibir dicha medalla, Arthur Cayley introdujo los grafos que llevan su nombre en el año 1878. La idea fundamental de estos grafos fue el permitir representar la estructura de un grupo de tal manera que fuera visible más allá de una tabla de operaciones, es también un enfoque valioso ya que consigue conectar dos ramas en apariencia distintas y usar la sencillez a la hora de visualizar conceptos de una para aportar claridad a la otra.

La teoría de grupos geométricos, como área diferenciada, es relativamente nueva y se convirtió en una rama claramente identificable de las matemáticas a fines de la década de 1980 y principios de la de 1990.

Por lo tanto, al ser un área relativamente nueva resulta de gran interés para conocer todos aquellos conceptos y propiedades que dan las bases a tal teoría, estudiarla y mostrar

al público lo interesante que es y que probablemente muy poco se sabía de ella. También sentar las bases para futuras investigaciones de áreas que requieren tales conocimientos.

En este trabajo de investigación en primera instancia se hace un breve recordatorio de teoría de grupo muy básica para poder introducir conceptos como Grupo Simétrico, los Grupos Libres y algunas de sus propiedades, Grupos a través de Generadores y relaciones.

Además, como punto central dado que es parte del nombre de dicha investigación es el poder presentar a los grupos finitamente generados de manera que se vean como objetos geométricos lo cual se logra a través de los Grafos de Cayley, esto es asociando una estructura combinatoria con un grupo y un conjunto generador dado.

Por último, dado que la importancia de la Teoría Geométrica de Grupos es estudiar a los grupos como objetos geométricos, después de tener un grupo y asociarle un conjunto generador lo siguiente que sigue es establecer una estructura de espacio métrico, es decir, es necesaria una estructura métrica mediante métrica de palabras, que se induce de los caminos en los grafos de Cayley. Además, con todo ello se abre el paso para tratar la geometría a gran escala ya que se habla de la geometría sobre un grupo.

Por último se tratan las Cuasi-isometrías y las propiedades necesarias para tener espacios que parezcan iguales viéndoles de lejos y cerrar con el Lema de Švarc-Milnor.

Capítulo 1

Preliminares

Como los principales personajes en la teoría geométrica de grupo son **grupos**, comenzamos por repasar algunos conceptos y ejemplos de la teoría de grupos. En particular, se presentarán principios básicos de construcción que nos permitan generar interesantes ejemplos de grupos , esto incluye la descripción de grupos en términos de generadores y relaciones.

1.1. Teoría fundamental de grupo

Comenzaremos con algunas nociones básicas de grupos, varios ejemplos, estudiaremos las construcciones sobre ellos y las propiedades más útiles. Además examinaremos las clases de todos los grupos como objetos y homomorfismos de grupos como morfismos, esto como tal es una categoría de grupos, el estudio de ellos es conocido como: teoría de grupos.

Definición 1.1 (Grupos)

Un **grupo** es un conjunto G junto con una operación binaria $* : G \times G \longrightarrow G$ satisfaciendo los siguientes axiomas:

- Asociativa. Para todo $g_1, g_2, g_3 \in G$ tenemos que

$$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3.$$

- Existencia del elemento neutro. Existe un elemento neutro $e \in G$ para " $*$ ", es

decir,

$$\forall g \in G; \quad e * g = g = g * e.$$

(Esta propiedad determina de forma exclusiva el elemento neutro).

- Existencia del inverso. Para cada $g \in G$ existe un elemento inverso $g^{-1} \in G$ con respecto a " $*$ ", es decir,

$$g * g^{-1} = e = g^{-1} * g.$$

(Esta propiedad determina de forma única el elemento inverso de g).

Recordatorio:

Un grupo G es abeliano si la operación es conmutativa, es decir, si

$$g_1 * g_2 = g_2 * g_1$$

para todo $g_1, g_2 \in G$.

Recordatorio:

En lugar de $a * b$ usaremos simplemente ab o $a \cdot b$.

Definición 1.2 (Subgrupo)

- Sea G un grupo con respecto a "$*$". Un subconjunto $H \subset G$ es un **subgrupo** si H es un grupo con respecto a la restricción de " $*$ " a $H \times H \subset G \times G$.
- Sea H un subgrupo de un grupo G, el **índice** de H en G es el **cardinal** de G/H. Además se define

$$[G : H] = [G/H] = [H/G]$$

Ejemplo 1.1 **(Algunos grupos)**

El conjunto $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ son grupos con respecto a la adición; además, $\mathbb{Z}$ es un subgrupo de $\mathbb{Q}$, y $\mathbb{Q}$ un subgrupo de $\mathbb{R}$.

Definición 1.3 (Homomorfismo/Isomorfismo de grupo)

Sea $G,\ H$ grupos.

- Una función $\varphi : G \longrightarrow H$ es un **homomorfismo** de grupo si φ es compatible con la composición en G y H respectivamente, es decir, si

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$$

  Para todo $g_1,\ g_2 \in G$. (Cada homomorfismo de grupo asigna el elemento neutro al elemento neutro e inverso a inverso).

- Un homomorfismo de grupo $\varphi : G \longrightarrow H$ es un **isomorfismo** de grupo si existe un homomorfismo de grupo $\psi : H \longrightarrow G$ tal que $\varphi \circ \psi = id_H$ y $\psi \circ \varphi = id_G$. Si existe un isomorfismo de grupo entre G y H, entonces G y H son isomorfos, y escribimos $G \cong H$.

Ejemplo 1.2 **(Algunos homomorfismos de grupos)**

- Claramente, todos los grupos triviales son (canónicamente) isomorfos. Por lo tanto, acostumbramos hablar del "grupo trivial".

- Sea $n \in \mathbb{Z}$. Entonces

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto n \cdot x \end{aligned}$$

  Es un homomorfismo de grupo para $n = 0$; sin embargo, la adición de $n \neq 0$ no es un homomorfismo de grupo (por ejemplo, el elemento neutro no se asigna al elemento neutro).

Definición 1.4 (Núcleo / Imagen de homomorfismo)

Sea $\varphi : G \longrightarrow H$ un homomorfismo de grupo entonces el subgrupo

$$\ker \varphi := \left\{ \ g \in G \ \middle| \ \varphi(g) = e \ \right\}$$

de G es el **núcleo** o **kernel** de φ, y el subgrupo

$$\text{im } \varphi := \left\{ \ \varphi(g) \in H \ \middle| \ g \in G \ \right\}$$

de H es la **imagen** de φ.

Sea $X = \{1, 2, \ldots, n\}$ un conjunto, denotamos por S_n al conjunto de todas las funciones biyectivas $\sigma : X \longrightarrow X$; cabe aclarar que este es un grupo con la composición usual de funciones.

Definición 1.5 (Grupo simétrico)

El grupo S_n se llama el **grupo simétrico** sobre X o el grupo de permutaciones de X.

Ejemplo 1.3

Sea $X = \{1, 2, 3\}$, denotamos para $n \geq 3$ el grupo simétrico S_3; encontrar el conjunto de todas las posibles permutaciones.

En la teoría de los espacios vectoriales; el cociente de cualquier espacio vectorial por cualquier subespacio forma naturalmente un espacio vectorial. Sólo los subgrupos especiales dan lugar a grupos cocientes:

Definición 1.6 (Subgrupo normal)

Sea G un grupo y N un subgrupo de G. Se dice que N es un **subgrupo normal** de G si,

$$g^{-1} \cdot N \cdot g \subset N$$

para todo $g \in G$. Si N es un subgrupo normal de G, entonces, lo denotamos como $N \lhd G$.

Ejemplo 1.4 **(Algunos subgrupos (no-)normales)**

- Si G es un grupo abeliano, entonces todo subgrupo de G es normal.
- Sea $\tau \in S_3$ (el grupo simétrico) la biyección dada por el intercambio de 1 a 2 (es decir, $\tau = (1, 2)$). Entonces $\{id, \tau\}$(τ es una permutacion de r-ciclo) es un subgrupo de S_3, pero no es un subgrupo normal. Por otro lado, el subgrupo $\{id, \sigma, \sigma^2\} \subset S_3$ generado por el ciclo $\sigma := (1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1)$ es un subgrupo normal de S_3.

Si bien es cierto todo subgrupo de un grupo abeliano, es normal, el recíproco de esto no es cierto. Existen grupos no abelianos en los cuales lo subgrupos son normales, a dichos grupos se les llama *hamiltonianos*, en honor al matemático irlandés W. R. Hamilton. Por ejemplo grupo no abeliano requerido se puede encontrar en los cuaternios de Hamilton.

El concepto de grupo factor o grupo cociente es muy sútil y de máxima importancia. La formación de un nuevo conjunto a partir de uno anterior utilizando como elementos de dicho conjunto nuevo subconjuntos del anterior.

Proposición 1.1 (Grupo cociente)

Sea G un grupo, y sea N un subgrupo de G.

1. Sea $G/N := \left\{ \; g \cdot N \;\middle|\; g \in G \; \right\}$. Entonces el mapeo

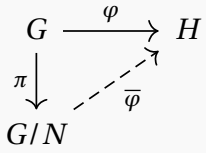
$$G/N \times G/N \longrightarrow G/N$$
$$(g_1 \cdot N, g_2 \cdot N) \longmapsto (g_1 \cdot g_2) \cdot N$$

esta bien definido si y solo si N es normal en G. Si N es normal en G/N, es un grupo con respecto a la composición de aplicaciones, que se denomina **grupo cociente** de G por N.

2. Sea N normal en G. Entonces la proyección canónica

$$\pi : G \longrightarrow G/N$$
$$g \longmapsto g \cdot N$$

es un homomorfismo de grupo, y el grupo cociente G/N junto con π tiene la siguiente propiedad universal: Para todo grupo H y todo homomorfismo de grupo $\varphi : G \longrightarrow H$ con $N \subset \ker \pi$ existe exactamente un homomorfismo de grupo $\overline{\varphi} : G/H \longrightarrow H$ que satisface $\overline{\varphi} \circ \pi = \varphi$



Ejemplo 1.5 **(Grupos cocientes)**

- Sea $n \in \mathbb{Z}$. Entonces la composición en el grupo cociente $\mathbb{Z}/n\mathbb{Z}$ no es más que la adición módulo n. Si $n \neq 0$, entonces $\mathbb{Z}/n\mathbb{Z}$ es un grupo cíclico de orden n: si $n = 0$, entonces $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}$ es un grupo cíclico infinito. También se abrevia $\mathbb{Z}/n := \mathbb{Z}/n\mathbb{Z}$.
- El cociente de S_3 por el subgrupo $\{id, \sigma, \sigma^2\}$ generado por el ciclo

$$\sigma := (1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 1)$$

es isomorfo a $\mathbb{Z}/2$.

Teorema 1.1 (Teorema de Cayley)

Todo grupo es isomorfo a un subgrupo de algún grupo simétrico.

Demostración. Sea G un grupo. Probaremos que si G es un grupo entonces G es isomorfo a un subgrupo de algún grupo simétrico S_G.

1. Probaremos que el mapeo dado es una permutación en G.
   Sea $g \in G$ y definamos f_g de la siguiente forma

   $$f_g : G \longrightarrow G$$

   donde $f_g(h) = gh$, $\forall h \in G$.

   - f_g esta bien definida.
     Sea $h, b \in G$ tal que $h = b$.

     $$\begin{aligned} h = b &\Longrightarrow gh = gb \\ &\Longrightarrow f_g(h) = f_g(b) \qquad \text{; por hipótesis} \end{aligned}$$

     $\therefore f_g$ esta bien definida.
   - f_g es inyectiva.
     Sea $h, b \in G$ tal que $f_g(h) = f_g(b)$.

     $$\begin{aligned} f_g(h) = f_g(b) &\Longrightarrow gh = gb \\ &\Longrightarrow h = b \qquad \text{; por propiedad de cancelación} \end{aligned}$$

     $\therefore f_g$ es inyectiva.
   - f_g es sobreyectiva.
     Para cada $x \in G$ existe $g^{-1}x \in G$ tal que

     $$\begin{aligned} f_g\left(g^{-1}x\right) &= g\left(g^{-1}x\right) \\ &= \left(gg^{-1}\right)x \qquad \text{; por propiedad de grupos (definición 1.1)} \\ &= e \cdot x \\ &= x \end{aligned}$$

     $\therefore f_g$ es sobreyectiva.

   Observamos que f_g es una biyección de G sobre G mismo, por lo que concluimos que f_g es una permutación en el grupo de elementos de G.

2. Sea $G' = \left\{ \; f_g \;\middle|\; g \in G \; \right\}$. Demostraremos que el conjunto G' es un subgrupo del grupo simétrico $S_G = \left\{ \; f : G \to G \;\middle|\; f \text{ es biyección} \; \right\}$.
   Sabemos que la composición de funciones siempre es asociativa entonces demostraremos solamente que G' es cerrado, tiene identidad e inversa.

   - G' es cerrado.
     Para cualquier $f_a, f_b \in G'$ tal que

     $$\begin{aligned} f_a f_b(h) &= f_a\big(f_b(h)\big) \qquad ; f_b \text{ esta definida por lo anterior} \\ &= f_a(bh) \\ &= a(bh) \\ &= (ab)h \\ &= f_{ab}(h) \end{aligned}$$

     Luego $f_a f_b = f_{ab} \in G'$.
     $\therefore G'$ es cerrado.
   - En G' existe el elemento identidad.
     Sea $f_e \in G'$.
     Si $f_e \in G'$ entonces $f_e f_g = f_{eg} = f_g$ y $f_g f_e = f_{ge} = f_g$
     $\therefore$ En G' existe el elemento identidad.
   - En G' existe el inverso.
     Sea $f_a \in G'$. Usaremos el hecho que G' es cerrado, es decir $f_a f_b = f_{ab}$, si $b = a^{-1}$ entonces $f_a f_{a^{-1}} = f_{aa^{-1}} = f_e$ y $f_{a^{-1}} f_a = f_{a^{-1}a} = f_e$
     $\therefore$ En G' existe el inverso.

   $\therefore G'$ es un subgrupo de S_G.

3. Demostraremos que dicho mapeo dado es un isomorfismo.
   Sea ϕ un mapeo

   $$\phi : G \longrightarrow G'$$

   definido por $\phi(g) = f_g$

   - ϕ esta definida.
     Sea $g, b \in G$ tal que $g = b$.

     $$\begin{aligned} g = b &\Longrightarrow f_g = f_b \\ &\Longrightarrow \phi(g) = \phi(b) \qquad ; \text{ por hipótesis} \end{aligned}$$

     $\therefore \phi$ esta definida.

- ϕ es un homomorfismo.
  Sea $x, y \in G$, entonces

$$\begin{aligned}\phi(xy) &= f_{xy} \\ &= f_x f_y \\ &= \phi(x)\phi(y)\end{aligned}$$

  $\therefore \phi$ es un homomorfismo.

- ϕ es inyetiva.
  Sean $a, b \in G$ tal que $\phi(a) = \phi(b)$

$$\begin{aligned}\phi(a) = \phi(b) &\Longrightarrow f_a = f_b \\ &\Longrightarrow f_a(h) = f_b(h) \qquad ; \forall h \in G \\ &\Longrightarrow ah = bh \\ &\Longrightarrow a = b \qquad\qquad ; \text{por propiedad de cancelación}\end{aligned}$$

  $\therefore \phi$ es inyectiva.

- ϕ es sobreyectiva.
  Por hipótesis, sea $f \in G'$.

$$\begin{aligned}f \in G' &\Longrightarrow f = f_g \qquad ; \text{para algún } g \text{ en } G \\ &\Longrightarrow f = \phi(g)\end{aligned}$$

  $\therefore \phi$ es sobreyectiva.
  $\therefore \phi$ es una biyección en G sobre G'.
  $\therefore \phi$ es un isomorfismo.

Observando que G' es un subgrupo del grupo simétrico S_G. Así $G \cong G'$

□

Definición 1.7 (Categoría)

Una **categoría** C consta de los siguientes componentes:

- Una clase $\mathrm{Ob}(C)$; los elementos de $\mathrm{Ob}(C)$ son objetos de C. (Las clases son una generalización de conjuntos, lo que permite, por ejemplo, la definición de la clase de todos los conjuntos).
- Un conjunto $\mathrm{Mor}_C(X, Y)$ para cada elección de objetos $X, Y \in \mathrm{Ob}(C)$; los elemen-

tos de $\mathrm{Mor}_C(X,Y)$ se denominan morfismos de X, Y. (Suponemos implícitamente que los conjuntos de morfismos entre diferentes pares de objetos son disjuntos).

- Para los objetos $X, Y, Z \in \mathrm{Ob}(C)$ una composición

$$\begin{aligned} \circ : \mathrm{Mor}_C(Y,Z) \times \mathrm{Mor}_C(X,Y) &\longrightarrow \mathrm{Mor}_C(X,Z) \\ (g,f) &\longmapsto g \circ f \end{aligned}$$

de morfismos.

Estos datos tienen que cumplir las siguientes condiciones:

- Para cada objeto X en C existe un morfismo $id_X \in \mathrm{Mor}_C(X,X)$ con la siguiente propiedad: Para todo $Y \in \mathrm{Ob}(C)$ y todo $f \in \mathrm{Mor}_C(X,Y)$ y $g \in \mathrm{Mor}_C(Y,X)$ tenemos

$$f \circ id_X = f \text{ y } id_X \circ g = g.$$

(El morfismo id_X está determinado únicamente por esta propiedad; es el morfismo de identidad de X en C).

- La composición del morfismo es asociativa, es decir, para todo $W, X, Y, Z \in \mathrm{Ob}(C)$ y todo $f \in \mathrm{Mor}_C(W,X), g \in \mathrm{Mor}_C(X,Y)$ y $h \in \mathrm{Mor}_C(Y,Z)$ tenemos:

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

El concepto de morfismos y composiciones se basa en el ejemplo de mapeos entre conjuntos y la composición ordinaria de mapeos. Sin embargo, en general, los morfismos en categorías no necesitan darse como conjuntos de mapeos y la composición no necesita ser composición de mapeos.

Ejemplo 1.6 **(Categoría de conjuntos)**

La categoría de conjuntos $C = \mathrm{Set}$ está formada por:

- Objetos: Sea $\mathrm{Ob}(\mathrm{Set})$ la clase de todos los conjuntos.
- Morfismo: Para los conjuntos X y Y, es $\mathrm{Mor}_C(X,Y)$ el conjunto de todos las funciones de conjuntos $X \longrightarrow Y$
- Las composiciones son composiciones ordinarias de funciones: Para conjuntos X, Y, Z definimos la composición

$$\circ : \mathrm{Mor}_C(Y,Z) \times \mathrm{Mor}_C(X,Y) \longrightarrow \mathrm{Mor}_C(X,Z)$$
$$f \times g \longrightarrow f \circ g$$

como la composición usual de funciones.

La noción de categorías contiene todos los ingredientes necesarios para hablar de isomorfismos y automorfismos:

Definición 1.8 (Isomorfismo)

Sea C una categoría y sea X un objeto de C. Los objetos $X, Y \in \mathrm{Ob}(C)$ son **isomorfos** en C si existen $f \in \mathrm{Mor}_C(X,Y)$ y $g \in \mathrm{Mor}_C(Y,X)$ con

$$g \circ f = id_X \text{ y } f \circ g = id_Y$$

En este caso, f y g son isomorfismos en C y escribimos $X \cong_C Y$ (o $X \cong Y$ si la categoría es clara por el contexto).

Definición 1.9 (Grupo de automorfismos)

Sea C una categoría y sea X un objeto de C. Entonces el conjunto $\mathrm{Aut}_C(X)$ de todos los isomorfismos $X \longrightarrow X$ en C es un grupo con respecto a la composición en C (proposición siguiente), el **grupo de automorfismos** de X en C.

Proposición 1.2 (Grupos de automorfismos en Categoría)

- Sea C una categoría y sea $X \in \mathrm{Ob}(C)$. Entonces $\mathrm{Aut}_C(X)$ es un grupo.
- Sea G un grupo. Entonces existe una categoría C y un objeto X en C tal que $G \cong \mathrm{Aut}_C(X)$.

Demostración. Sea C una categoría y sea $X \in \mathrm{Ob}(C)$ entonces probaremos que $\mathrm{Aut}_C(X)$ es un grupo.

1. Para ello, solo probaremos que tiene inverso, ya que la asociatividad y la existencia del elemento id_X está garantizada por la definición de Categoría .

   Sean $\alpha, \beta \in \mathrm{Aut}_C(X)$.

   Como $\alpha, \beta \in \mathrm{Aut}_C(X)$, entonces $\alpha, \beta : X \longrightarrow X$ y $\alpha, \beta \in \mathrm{Mor}_C(X,X)$, así $\alpha \circ \beta : X \longrightarrow X$.

Además, como $\alpha, \beta \in \mathrm{Aut}_C(X)$, entonces existen $\alpha', \beta' \in \mathrm{Mor}_C(X,X)$ tal que:

$$\begin{aligned}\alpha \circ \alpha' &= id_X\\ \alpha' \circ \alpha &= id_X\\ \beta \circ \beta' &= id_X\\ \beta' \circ \beta &= id_X\end{aligned}$$

Ahora bien,

$$\begin{aligned}(\alpha \circ \beta) \circ (\beta' \circ \alpha') &= \alpha \circ (\beta \circ \beta') \circ \alpha' && \text{; por asociatividad}\\ &= \alpha \circ id_X \circ \alpha'\\ &= (\alpha \circ id_X) \circ \alpha'\\ &= \alpha \circ \alpha'\\ &= id_X\end{aligned}$$

Así, $(\alpha \circ \beta) \circ (\beta' \circ \alpha') = id_X$.

De la misma manera,

$$\begin{aligned}(\beta' \circ \alpha') \circ (\alpha \circ \beta) &= \beta' \circ (\alpha' \circ \alpha) \circ \beta && \text{; por asociatividad}\\ &= \beta' \circ id_X \circ \beta\\ &= (\beta' \circ id_X) \circ \beta\\ &= \beta' \circ \beta\\ &= id_X.\end{aligned}$$

Por lo que, $(\beta' \circ \alpha') \circ (\alpha \circ \beta) = id_X$.

Esto significa que $\alpha \circ \beta$ tiene inverso.

Por lo tanto, $\mathrm{Aut}_C(X)$ es un grupo.

2. Ahora debemos probar que dado un grupo G, entonces existe una categoría C y objeto X en C tal que $G \cong \mathrm{Aut}_C(X)$.

   Consideramos la categoría C con un solo objeto X, tomemos $\mathrm{Mor}_C(X,X) = G$ y definamos la composición en G por:

$$\begin{aligned}\circ : \mathrm{Mor}_C(X,X) \times \mathrm{Mor}_C(X,X) &\longrightarrow \mathrm{Mor}_C(X,X)\\ (g,h) &\longmapsto g \circ h = gh\end{aligned}$$

   Probemos que $G \cong \mathrm{Aut}_C(X)$.
   Sea $\psi : G \longrightarrow \mathrm{Aut}_C(X)$ definida como $\psi(f) = f$.

- Probemos que ψ es homorfismo de grupos.
  Sea $f, g \in G$, entonces
  $$\psi(f \circ g) = f \circ g = \psi(f) \circ \psi(g).$$
  Así es morfismo.
- Probemos que ψ es inyectiva.
  Sean $f, g \in G$ tales que $\psi(f) = \psi(g)$. Por como está definida ψ, lo anterior no es más que que
  $$\psi(f) = f,\ \psi(g) = g$$
  Por lo que $f = g$, así es inyectiva.
- Probemos que ψ es sobreyectiva.
  Sea $f \in \mathrm{Aut}_C(X)$. Si $f \in \mathrm{Aut}_C(X)$ implica que $f : X \longrightarrow X$ es biyectiva y morfismo, entonces
  $$f \in \mathrm{Mor}_C(X, X) = G$$
  Luego,
  $$\psi(f) = f$$
  Así, es biyectiva.

Así, si G un grupo entonces existe una categoría C y un objeto X en C tal que $G \cong \mathrm{Aut}_C(X)$. □

1.2. Grupos a través de generadores

En esta sección, se describen las primeras nociones sobre teoría combinatoria de grupos, la idea básica es que se puede saber todo sobre un grupo gracias a un conjunto de generadores.

Comenzamos repasando el concepto de conjunto generador de un grupo; en teoría geométrica de grupo, por lo general solo nos interesan los grupos generados finitamente; además definiremos que son grupos libres en términos de una propiedad muy característica y demostraremos las nociones equivalentes del estudio de grupos libres (unicidad, existencia etc).

Definición 1.10 (Conjunto generador)

- Sea G un grupo y sea un subconjunto $S \subset G$. El subgrupo generado por S en G es el subgrupo más pequeño (con respecto a la inclusión) de G que contiene S; el subgrupo generado por S en G se denota por $\langle S \rangle_G$. El conjunto S genera G si $\langle S \rangle_G = G$.
- Un grupo es finamente generado si contiene un subconjunto finito que genera el grupo en cuestión.

Nota:

Sea G un grupo y sea $S \subset G$. Entonces el subgrupo generado por S en G siempre existe y se puede describir de la siguiente manera:

$$\begin{aligned} \langle S \rangle_G &= \bigcap \left\{ H \;\middle|\; H \subset G \text{ es un subgrupo con } S \subset H \right\} \\ &= \left\{ s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} \;\middle|\; n \in \mathbb{N},\ s_1, \ldots, s_n \in S,\ \varepsilon_1, \ldots, \varepsilon_n \in \{-1, +1\} \right\} \end{aligned} \tag{1.1}$$

Ejemplo 1.7 **(Conjuntos generadores)**

- El grupo trivial es generado por el conjunto $\emptyset$.
- El conjunto generador $\{1\}$ genera el grupo aditivo $\mathbb{Z}$, también por ejemplo, $\{2,3\}$ es un conjunto generador para $\mathbb{Z}$. Pero $\{2\}$ y $\{3\}$ no son conjuntos generadores de $\mathbb{Z}$.

Análisis:

Primero. Por definición 1.10 sea $S \subset G$, el conjunto S que genera a G, es decir, $\langle S \rangle_G$. Entonces $\langle S \rangle_G$ es el subgrupo más pequeño de G que contiene a S, pero el más pequeño de todos los subgrupos de G es $\{e\}$ y si $S = \emptyset$ tenemos que $\emptyset \subset \{e\}$ concluimos que $\langle \emptyset \rangle = \{e\}$.

Segundo. El grupo aditivo se forma por todos los múltiplos de 1, es decir, son de la forma:

$$\begin{aligned} \mathbb{Z} &= \{\ldots -2, -1, 0, 1, 2 \ldots\} \\ &= \left\{ n \cdot 1 \;\middle|\; n \in \mathbb{Z} \right\} \\ &= \langle \{1\} \rangle \end{aligned}$$

Entonces por definición 1.10. Sea $S \subset G$, definimos $S = \{1\}$ el subgrupo generado en G sería $\langle \{1\} \rangle_G = G$ donde G representa al grupo aditivo $\mathbb{Z}$.

Por definición 1.10. Sea $S \subset G$, el conjunto S genera a G, es decir, $\langle S \rangle_G$. Entonces definimos $S = \{2,3\}$ el subgrupo generado en G; en este caso G representa el grupo aditivo $\mathbb{Z}$, es decir, $\langle \{2,3\} \rangle_G = \mathbb{Z}$ verifiquemos que se cumple con la igualdad:

Caso 1: Claramente por simple inspección se cumple la primera inclusión, es decir, $\langle \{2,3\} \rangle_G \subset \mathbb{Z}$.

Caso 2: Para todo $m \in \mathbb{Z}$, donde m es de la forma $m = n_1 \cdot 2 + n_2 \cdot 3$ tal que $n_1, n_2 \in \mathbb{Z}$.
Sea $n_1 = -1$ y $n_2 = 2$.

$$\begin{aligned} n_1 = -1 \text{ y } n_2 = 1 &\Longrightarrow -2 + 3 = 1 \\ &\Longrightarrow -2m + 3m = m \qquad \text{; multiplicamos por } m \\ &\Longrightarrow m \in \langle \{2,3\} \rangle \\ &\Longrightarrow \mathbb{Z} \subset \langle \{2,3\} \rangle \end{aligned}$$

Así $\langle \{2,3\} \rangle_G = \mathbb{Z}$.

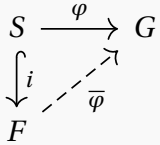
Tomamos un elemento $\{2\}$, este no genera el grupo aditivo $\mathbb{Z}$ por que el subgrupo más pequeño de los números enteros que contiene a $S = \{2\}$ son los números pares, observando que no genera a todo $\mathbb{Z}$.

Luego, de la misma manera tomamos un elemento $\{3\}$, y se nota que este no genera al grupo aditivo $\mathbb{Z}$ ya que el subgrupo más pequeño de los números enteros que contiene $S = \{3\}$ son los múltiplos de tres.

■

Definición 1.11 (Grupos libres, propiedad universal)

Sea S un conjunto. Un grupo F que contiene S es **generado libremente** por S si F tiene la siguiente propiedad universal: Para cada grupo G y cada mapeo $\varphi : S \longrightarrow G$ existe un homomorfismo único $\overline{\varphi} : F \longrightarrow G$ extendiendo φ:



Un grupo es **libre** si contiene un conjunto generador libre.

Ejemplo 1.8 **(Grupos libres)**

- El grupo trivial es generado libremente por el conjunto $\emptyset$.
- El grupo aditivo $\mathbb{Z}$ es generado libremente por $\{1\}$. El grupo aditivo $\mathbb{Z}$ no es generado libremente por $\{2,3\}$ o $\{2\}$ o $\{3\}$; en particular, no todos los grupos generadores de un grupo contienen un grupo generador libre.

Análisis: Desarrollaremos el segundo ejemplo.

Primero. Veamos que en efecto $\mathbb{Z}$ es generado libremente por $\{1\}$, entonces verificamos que se cumple la propiedad universal, es decir, que para todo grupo G y para toda aplicación $\varphi : \{1\} \longrightarrow G$, existe un homomorfismo de grupos, $\overline{\varphi} : \mathbb{Z} \longrightarrow G$, tal que $\overline{\varphi}|_{\{1\}} = \varphi$,

- Probemos que $\overline{\varphi}$ existe. Definamos $\overline{\varphi}$ de la siguiente manera;

$$\begin{aligned} \overline{\varphi} : \mathbb{Z} &\longrightarrow G \\ n &\longmapsto n\varphi(1) \end{aligned}$$

  ahora veamos que $\overline{\varphi}$ esta bien definida, sean $n_1,\ n_2 \in \mathbb{Z}$, tal que $n_1 = n_2$;

$$\begin{aligned} n_1 = n_2 &\Longrightarrow n_1\varphi(1) = n_2\varphi(1) \\ &\Longrightarrow \overline{\varphi}(n_1) = \overline{\varphi}(n_2) \end{aligned}$$

  por lo tanto, $\overline{\varphi}$ esta bien definida.

- Probemos que $\overline{\varphi}$ es un homomorfismo; sean $n_1,\ n_2 \in \mathbb{Z}$,

$$\begin{aligned} \overline{\varphi}(n_1 + n_2) &= (n_1 + n_2)\varphi(1) \\ &= n_1\varphi(1) + n_2\varphi(1) \\ &= \overline{\varphi}(n_1) + \overline{\varphi}(n_2) \end{aligned}$$

  por tanto, $\overline{\varphi}$ es un homomorfismo, así concluimos que $\overline{\varphi}$, existe.

- Demostraremos que se cumple; $\overline{\varphi}|_{\{1\}} = \varphi$.

$$\begin{aligned} \overline{\varphi}(1) &= 1\varphi(1) \\ &= \varphi(1) \end{aligned}$$

  por tanto, $\overline{\varphi}|_{\{1\}} = \varphi$.

- Demostraremos que $\overline{\varphi}$ es único; supongamos que existe otro homomorfismo $\psi : \mathbb{Z} \longrightarrow G$, tal que $\psi|_{\{1\}} = \varphi$,

  Tenemos que $\psi : \mathbb{Z} \longrightarrow G$, así $\psi(n) = \psi(1 + \cdots + 1)$, donde

$$\psi(n) = \begin{cases} \underbrace{1 + \cdots + 1}_{n-veces} & si \quad n \geq 1 \\ 0 & si \quad n = 0 \\ \underbrace{-(1 + \cdots + 1)}_{-n-veces} & si \quad n \leq -1 \end{cases}$$

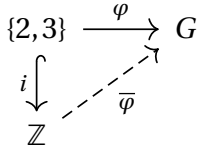
  luego,

$$\begin{aligned} \psi(n) &= \psi(1 + \cdots + 1) \\ &= \psi(1) + \cdots + \psi(1) \\ &= 1\varphi(1) + \cdots + 1\varphi(1) \\ &= n\varphi(1) \\ &= \overline{\varphi}(n) \end{aligned}$$

  por tanto, $\psi = \overline{\varphi}$, así $\overline{\varphi}$ es único. Ya que se cumple la propiedad universal, $\mathbb{Z}$ es generado libremente por $\{1\}$.

Segundo. Verifiquemos que $\mathbb{Z}$ no es libremente generado por $\{2,3\}$, $\{2\}$ ó $\{3\}$

Si $\mathbb{Z}$ no es generado libremente por $\{2,3\}$, significa que no se cumple la propiedad universal, para verificar esto, supongamos lo contrario; $\mathbb{Z}$ es generado libremente por $\{2,3\}$ entonces se cumple que para todo G y para todo $\varphi : \{2,3\} \longrightarrow G$, existe un único homomorfismo, $\overline{\varphi} : \mathbb{Z} \longrightarrow G$, tal que $\overline{\varphi}|_{\{2,3\}} = \varphi$, es decir, que el siguiente diagrama conmute;



$\overline{\varphi} \circ i = \varphi$.

Como se cumple para todo G, definamos un $G = \mathbb{Z}$ y como tenemos que se cumple para todo φ, definámoslo de la siguiente manera;

$$\begin{aligned} \varphi : \{2,3\} &\longrightarrow \mathbb{Z} \\ 2 &\longmapsto \varphi(2) = 1 \\ 3 &\longmapsto \varphi(3) = 1 \end{aligned}$$

existe el homomorfismo $\overline{\varphi}: \mathbb{Z} \longrightarrow \mathbb{Z}$ tal que cumple que;

$$\left(\overline{\varphi} \circ i\right)(2) = \varphi(2) \tag{1.2}$$
$$\left(\overline{\varphi} \circ i\right)(3) = \varphi(3) \tag{1.3}$$

luego,

$$\begin{aligned}\overline{\varphi}(2) &= \overline{\varphi}(1+1)\\ &= \overline{\varphi}(1) + \overline{\varphi}(1) \ \text{; ya que tenemos que } \overline{\varphi} \text{ es un homomorfismo}\\ &= 2\overline{\varphi}(1)\end{aligned}$$

así tenemos que $\overline{\varphi}(2) = 2\overline{\varphi}(1)$ de forma similar, obtenemos que $\overline{\varphi}(3) = 3\overline{\varphi}(1)$. Ahora bien, por la ecuación 1.2;

$$\begin{aligned}\left(\overline{\varphi} \circ i\right)(2) &= \varphi(2)\\ \overline{\varphi}(i(2)) &= 1\\ \overline{\varphi}(2) &= 1\\ 2\overline{\varphi}(1) &= 1 \ \text{; } \overline{\varphi}(1) = n \text{ para algún } n \in \mathbb{Z}\\ 2n &= 1 \quad (\rightarrow\leftarrow)\end{aligned}$$

luego, por la ecuación 1.3;

$$\begin{aligned}\left(\overline{\varphi} \circ i\right)(3) &= \varphi(3)\\ \overline{\varphi}(i(3)) &= 1\\ \overline{\varphi}(3) &= 1\\ 3\overline{\varphi}(1) &= 1\\ 3n &= 1 \quad (\rightarrow\leftarrow)\end{aligned}$$

como notamos no se cumple la propiedad universal para esta caso, y debería cumplir para todo G y para todo φ. Por tanto hemos verificado que no se cumple la propiedad universal, así, $\mathbb{Z}$ no es libremente generado por $\{2,3\}$. De manera análoga se verifica que $\{2\}$, $\{3\}$ no generan libremente a $\mathbb{Z}$.

■

Proposición 1.3 (Grupos libres, unicidad)

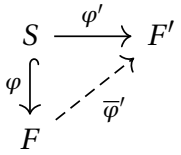
Sea S un conjunto. Entonces, existe como máximo un grupo generado libremente por S, salvo isomorfismos.

Demostración. La prueba consiste en usar la propiedad universal, en donde se consideran dos objetos que tienen la propiedad universal en cuestión. Entonces procedemos de la siguiente manera:

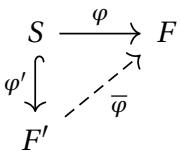
1. Usamos la parte de la existencia de la propiedad universal para obtener interesantes morfismos en ambas direcciones.
2. Usamos la parte de unicidad de la propiedad universal para concluir que ambas composiciones de estos morfismos tienen que ser la identidad (Y por lo tanto que ambos morfismos son isomorfismos).

Sean F y F' dos grupos generados libremente por S.
Sea $\varphi : S \longrightarrow F$ y $\varphi' : S \longrightarrow F'$. Denotamos la inclusión de S en F y F' por φ y φ' respectivamente.

1. Como F es un grupo libre generado por S, por la propiedad universal existe $\overline{\varphi}' : F \longrightarrow F'$ un homomorfismo tal que $\overline{\varphi}' \circ \varphi = \varphi'$.



   Además como F' es un grupo libre generado por S por la propiedad universal existe $\overline{\varphi} : F' \longrightarrow F$ tal que $\overline{\varphi} \circ \varphi' = \varphi$.



2. Ahora probemos que $\overline{\varphi} \circ \overline{\varphi}' = i_F$ y $\overline{\varphi}' \circ \overline{\varphi} = i_{F'}$.

   Consideremos la función identidad $i_F : F \longrightarrow F$ y la composición $\overline{\varphi} \circ \overline{\varphi}' : F \longrightarrow F$ el cual es un homomorfismo ya que $\overline{\varphi}', \overline{\varphi}$ lo son. Además por la parte 1):

$$\begin{aligned}(\overline{\varphi} \circ \overline{\varphi}') \circ \varphi &= \overline{\varphi} \circ (\overline{\varphi}' \circ \varphi) \\ &= \overline{\varphi} \circ \varphi' \\ &= \varphi\end{aligned}$$

   por lo que $(\overline{\varphi} \circ \overline{\varphi}') \circ \varphi = \varphi$.

Y como i_F es la identidad se cumple que $i_F \circ \varphi = \varphi$, así, por la unicidad de la propiedad universal se cumple que $\overline{\varphi} \circ \overline{\varphi}' = i_F$.

$$\begin{array}{ccc} S & \xrightarrow{\varphi} & F \\ {\scriptstyle\varphi}\downarrow & \overset{i_F}{\nearrow} & \\ F & \overset{\overline{\varphi}\circ\overline{\varphi}'}{\nearrow} & \end{array}$$

De manera similar,

$$\begin{aligned} \left(\overline{\varphi}' \circ \overline{\varphi}\right) \circ \varphi' &= \overline{\varphi}' \circ \left(\overline{\varphi} \circ \varphi'\right) \\ &= \overline{\varphi}' \circ \varphi \\ &= \varphi' \end{aligned}$$

Además $i_{F'} \circ \varphi' = \varphi'$, de modo que por la unicidad $\overline{\varphi}' \circ \overline{\varphi} = i_{F'}$, así $\overline{\varphi}$ y $\overline{\varphi}'$ son biyectivos, por tanto son isomorfismos.

Estos isomorfismos son canónicos en el siguiente sentido: inducen el mapeo identidad S y son (por parte de la unicidad de la propiedad universal) los únicos isomorfismos entre F y F' que extienden la identidad en S. □

Teorema 1.2 (Grupos libres, existencia)

Sea S un conjunto. Entonces existe un grupo libremente generado por S. (Por la proposición 1.3, este grupo es único salvo isomorfismo.)

Demostración. La idea de la demostración es construir un grupo formado por "palabras". Utilizaremos el alfabeto, así las palabras estarán compuestas por los elementos de S y los elementos de $\widehat{S}$ (el gorro es una etiqueta y con ese elemento etiquetado con gorro se vuelve un nuevo elemento del alfabeto);

1. Sea $A := S \cup \widehat{S}$, donde $\widehat{S} := \left\{ \widehat{s} \;\middle|\; s \in S \right\}$ es una copia disjunta de S; es decir,

$$\begin{aligned} \widehat{\cdot} : S &\longrightarrow \widehat{S} \\ s &\longmapsto \widehat{s} \end{aligned}$$

   $\widehat{\cdot}$ es una biyección, además se cumple que $S \cap \widehat{S} = \varnothing$. Más adelante, los elementos de $\widehat{S}$ juegan el rol de inverso de los elementos de S en el grupo que vamos a construir. Primero definiremos un conjunto que contenga todas las secuencias finitas de palabras sobre el alfabeto A.

2. Sea
$$A^* \coloneqq \left\{ \; s_1^{\epsilon_1} \cdot s_2^{\epsilon_2} \cdots s_n^{\epsilon_n} \;\middle|\; n \in \mathbb{N},\ \epsilon_i = \{1,-1\} \wedge s_i^{\epsilon_i} = \left\{ \begin{array}{ll} s_i, & \epsilon_i = 1 \\ \widehat{s}_i, & \epsilon_i = -1 \end{array} \right. \right\} \cup \{\epsilon\}$$
(Aquí, ϵ es la palabra vacía), es decir, que A^* es el conjunto de todas las palabras finitas cuyo alfabeto es A. Ahora vamos a definir una composición sobre A^*, dada por concatenación de palabras.

3. Sea
$$\begin{gathered} * : A^* \times A^* \longrightarrow A^* \\ \left(s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}, s_{n+1}^{\epsilon_{n+1}} \cdots s_m^{\epsilon_m}\right) \longmapsto \left(s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} s_{n+1}^{\epsilon_{n+1}} \cdots s_m^{\epsilon_m}\right) \\ \left(\epsilon, s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}\right) \longmapsto \left(s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}\right) \\ \left(s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}, \epsilon\right) \longmapsto \left(s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}\right) \end{gathered}$$
Como logramos ver, por como esta definida esta composición, podemos concluir que cumple ser; cerrada, asociativa, y tiene el elemento identidad que en este caso sería la palabra vacía ϵ.

4. Ahora vamos a definir una relación de equivalencia. Sea $\sim$ que cumple las siguientes condiciones:
$$\begin{aligned} &\forall x, y \in A^*,\ \forall s \in S,\ xs\widehat{s}y \sim xy \\ &\forall x, y \in A^*,\ \forall s \in S,\ x\widehat{s}sy \sim xy \end{aligned} \tag{1.4}$$
Aquí, $\sim$ será la relación de equivalencia en A^* mas pequeña que cumple las condiciones (1.4).

5. Vamos a definir el conjunto de las clases de equivalencia, de la siguiente manera;
$$F(S) \coloneqq \frac{A^*}{\sim} = \left\{ \; [x] \;\middle|\; x \in A^* \; \right\}$$
donde $x = s_1^{\epsilon_1} \cdots s_n^{\epsilon_n},\ n \in \mathbb{N},\ \epsilon_i \coloneqq \{1,-1\}$ y $s_i^{\epsilon_i} = \left\{ \begin{array}{ll} s_i, & \epsilon_i = 1 \\ \widehat{s}_i, & \epsilon_i = -1 \end{array} \right.$. Ya hemos construido el conjunto, vamos a probar que $F(S)$ es un grupo, pero antes definiremos la composición sobre el conjunto.

6. Sea
$$\begin{gathered} \cdot : F(S) \times F(S) \longrightarrow F(S) \\ \big([x], [y]\big) \longmapsto [x] \cdot [y] \coloneqq [x * y] \end{gathered}$$
(por simplicidad en el resto de la prueba escribiremos $[xy]$ en lugar de $[x * y]$) ahora sí, probaremos que $F(S)$ es un grupo:

- **Cerradura**. Para poder demostrar cerradura, probaremos que "$\cdot$" (la composición) esta bien definida. Sea $[x],[y],[x'],[y'] \in F(S)$ tal que $([x],[y]) = ([x'],[y'])$. Si $([\mathbf{x}],[\mathbf{y}]) = ([\mathbf{x}'],[\mathbf{y}'])$, entonces;

$$[x] = [x'] \ \wedge \ [y] = [y'] \implies x \sim x' \ \wedge y \sim y' \tag{1.5}$$

Definiremos x, y, x', y' arbitrarios, les daremos dos formas, para ellos tomaremos dos casos;
i) Sea $x = a\hat{s}sb,\ x' = ab,\ y = a'\hat{s'}s'b',\ y' = a'b'$, donde $a,b,b',a' \in A^*$ y $s,s' \in S$. Ahora bien,

$$\begin{aligned} xy &= x * y \\ &= (a\hat{s}sb) * (a'\hat{s'}s'b') \qquad \text{;por como tenemos definido la composición "}*\text{"} \\ &= a\hat{s}sba'\hat{s'}s'b' \end{aligned}$$

por la relación 1.4 que hemos definido $\sim$, podemos decir que;

$$xy = a\hat{s}sba'\hat{s'}s'b' \sim aba'b' = x'y'$$

por tanto, $xy \sim x'y'$.
Si $xy \sim x'y'$ entonces $[xy] = [x'y']$. En resumen, siguiendo con (1.5);
Si $x \sim x' \wedge y \sim y'$, entonces,

$$\begin{aligned} xy \sim x'y' &\implies [xy] = [x'y'] \\ &\implies [\mathbf{x}] \cdot [\mathbf{y}] = [\mathbf{x}'] \cdot [\mathbf{y}'] \end{aligned}$$

Por lo tanto para este caso $F(S)$, es cerrado.
ii) Sea $x = as\hat{s}b,\ x' = ab,\ y = a's'\hat{s'}b',\ y' = a'b'$, donde $a,b,b',a' \in A^*$ y $s,s' \in S$. Ahora bien,

$$\begin{aligned} xy &= x * y \\ &= (as\hat{s}b) * (a's'\hat{s'}b') \\ &= as\hat{s}ba's'\hat{s'}b' \qquad \text{; por "}*\text{"} \end{aligned}$$

por la relación 1.4 podemos decir que;

$$xy = as\hat{s}ba's'\hat{s'}b' \sim aba'b' = x'y'$$

por tanto, $xy \sim x'y'$.
Si $xy \sim x'y'$ entonces $[xy] = [x'y']$. En resumen, siguiendo con 1.5;

Si $x \sim x' \wedge y \sim y'$, entonces,

$$\begin{aligned} xy \sim x'y' &\Longrightarrow [xy] = \left[x'y'\right] \\ &\Longrightarrow [\mathbf{x}] \cdot [\mathbf{y}] = \left[\mathbf{x}'\right] \cdot \left[\mathbf{y}'\right] \end{aligned}$$

Por lo tanto, $F(S)$ es cerrado.

- **Asociatividad**. Como ya hemos probado que "$\cdot$" esta bien definida, resultara fácil demostrar asociatividad.
  Sea $[x], [y], [z] \in F(S)$

$$\begin{aligned} \big([x] \cdot [y]\big) \cdot [z] &= \big([xy]\big) \cdot [z] \\ &= [xyz] \\ &= [x] \cdot \big([yz]\big) \\ &= [x] \cdot \big([y] \cdot [z]\big) \end{aligned}$$

  Por lo tanto $F(S)$, es asociativo.

- **Identidad**. El elemento identidad existe ya que $F(S) = \frac{A^*}{\sim}$ y $\epsilon \in A^*$ (que es la palabra vacía), así $[\epsilon] \in F(S)$, y lo satisface:
  Sea $x \in A^*$

$$\begin{aligned} [\epsilon] \cdot [x] &= [\epsilon x] \\ &= [x] && \text{; por como se define la composición de palabra "}*\text{"} \\ &= [x\epsilon] \\ &= [x] \cdot [\epsilon] \end{aligned}$$

  Por lo tanto, $[\epsilon]$ es el elemento identidad en $F(S)$.

- **Inverso**. Para poder demostrar que los elementos de $F(S)$ tienen inversos, antes debemos definir una aplicación;
  Sea

$$\begin{aligned} I : A^* &\longrightarrow A^* \\ \epsilon &\longmapsto \epsilon \\ sx &\longmapsto I(x)\widehat{s} \\ \widehat{s}x &\longmapsto I(x)s \end{aligned}$$

  donde $x \in A^*$, tomemos x arbitrario de la forma $x = s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}$.

Probaremos que $I\big(I(x)\big) = x$

$$\begin{aligned} I\big(I(x)\big) &= I\Big(I\big(s_1^{\epsilon_1}\cdots s_n^{\epsilon_n}\big)\Big) \\ &= I\big(s_n^{-\epsilon_n}\cdots s_1^{-\epsilon_1}\big) \qquad \text{; por como se define } I \\ &= s_1^{\epsilon_1}\cdots s_n^{\epsilon_n} \\ &= x \end{aligned}$$

por lo tanto, $I\big(I(x)\big) = x$, $\forall x \in A^*$.
Ahora, probaremos que $\big[I(x)\big](x) = \epsilon$

$$\begin{aligned} I(x)x &= I\big(s_1^{\epsilon_1}\cdots s_n^{\epsilon_n}\big)\big(s_1^{\epsilon_1}\cdots s_n^{\epsilon_n}\big) \\ &= s_n^{-\epsilon_n}\cdots s_1^{-\epsilon_1}s_1^{\epsilon_1}\cdots s_n^{\epsilon_n} \\ &= \epsilon \end{aligned}$$

la última igualdad se cumple por las condiciones 1.4:

$$\begin{aligned} s_n^{-\epsilon_n}\cdots s_1^{-\epsilon_1}s_1^{\epsilon_1}\cdots s_n^{\epsilon_n} &\sim s_n^{-\epsilon_n}\cdots s_n^{\epsilon_n} \\ &\vdots \\ &\sim \epsilon. \end{aligned}$$

Y por último, vamos a probar que se cumple que $(x)\big[I(x)\big] = \epsilon$. Anteriormente, probamos que $[I(x)]\,(x) = \epsilon$ y $I\,(I(x)) = x$.

$$\begin{aligned} I\left(x'\right)x' &= \epsilon \\ I\,(I(x))\,I(x) &= \epsilon \qquad \text{; para } x' = I(x) \\ (I\,(I(x)))\,I(x) &= \epsilon \\ xI(x) &= \epsilon \end{aligned}$$

por tanto, $xI(x) = \epsilon$. Por lo tanto, $\big[I(x)\big] = [x]^{-1}$

Ahora, ya hemos demostrado que las cuatro propiedades de grupo se cumple para $F(S)$.

Por lo tanto, $F(S)$ es un grupo.

7. Ahora que hemos demostrado la existencia del grupo, vamos a demostrar que S genera libremente $F(S)$.

   Primero vamos a definir una aplicación que lleve los elementos de $S \subset A^*$, a su clase de equivalencia en $F(S)$.

Sea

$$\begin{aligned} i : S &\longrightarrow F(S) \\ s &\longmapsto [s] \end{aligned}$$

(mas adelante, demostraremos que i es inyectiva).

Para probar que S genera libremente a $F(S)$, probaremos que para cualquier grupo G y para cualquier función $\varphi : S \longrightarrow G$, existe un único homomorfismo $\overline{\varphi} : F(S) \longrightarrow G$ tal que $\overline{\varphi} \circ i = \varphi$, es decir, que probaremos que $F(S)$ cumple la propiedad universal de un grupo generado libremente por S.

- Primero vamos a probar la existencia de $\overline{\varphi}$, para ello vamos a definir una aplicación φ^*

  Sea

  $$\begin{aligned} \varphi^* : A^* &\longrightarrow G \\ \epsilon &\longmapsto e \\ sx &\longmapsto \varphi(s) \cdot \varphi^*(x) \\ \widehat{s}x &\longmapsto \varphi(s)^{-1} \cdot \varphi^*(x) \end{aligned}$$

  $\forall s \in S$ y $\forall x \in A^*$. En otras palabras φ^* se define de la siguiente forma: para $s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} \in A^*$,

  $$\varphi^*\left(s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}\right) = \varphi(s_1)^{\epsilon_1} \cdots \varphi(s_n)^{\epsilon_n}$$

  donde $\varphi(s_i)^{\epsilon_i} = \begin{cases} \varphi(s_i), & \epsilon_i = 1 \\ \varphi(s_i)^{-1}, & \epsilon_i = -1 \end{cases}$

  Si $s \in S$, $\varphi^*(s) = \varphi(s)$, así $\varphi^*|_S = \varphi$, además;

  $$\varphi^*(x * y) = \varphi^*(x)\ \varphi^*(y).$$

  Ahora, definamos $\overline{\varphi}$:

  Sea

  $$\begin{aligned} \overline{\varphi} : F(S) &\longrightarrow G \\ [x] &\longmapsto \varphi^*(x) \\ \left[s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}\right] &\longmapsto \varphi(s_1)^{\epsilon_1} \cdots \varphi(s_n)^{\epsilon_n} \end{aligned}$$

  i) Demostraremos que $\overline{\varphi}$ es un homomorfismo;

Sea $s_1^{\epsilon_1}\cdots s_n^{\epsilon_n},\ s_{n+1}^{\epsilon_{n+1}}\cdots s_m^{\epsilon_m} \in A^*$

$$\begin{aligned}
\overline{\varphi}\Big(\big[s_1^{\epsilon_1}\cdots s_n^{\epsilon_n}\big] * \big[s_{n+1}^{\epsilon_{n+1}}\cdots s_m^{\epsilon_m}\big]\Big) &= \overline{\varphi}\Big(\big[s_1^{\epsilon_1}\cdots s_n^{\epsilon_n} s_{n+1}^{\epsilon_{n+1}}\cdots s_m^{\epsilon_m}\big]\Big) \\
&= \varphi^*\Big(s_1^{\epsilon_1}\cdots s_n^{\epsilon_n} s_{n+1}^{\epsilon_{n+1}}\cdots s_m^{\epsilon_m}\Big) \\
&= \varphi(s_1)^{\epsilon_1}\cdots\varphi(s_n)^{\epsilon_n}\varphi(s_{n+1})^{\epsilon_{n+1}}\cdots\varphi(s_m)^{\epsilon_m} \\
&= \Big(\varphi(s_1)^{\epsilon_1}\cdots\varphi(s_n)^{\epsilon_n}\Big) * \Big(\varphi(s_{n+1})^{\epsilon_{n+1}}\cdots\varphi(s_m)^{\epsilon_m}\Big) \\
&= \varphi^*\big(s_1^{\epsilon_1}\cdots s_n^{\epsilon_n}\big) * \varphi^*\big(s_{n+1}^{\epsilon_{n+1}}\cdots s_m^{\epsilon_m}\big) \\
&= \overline{\varphi}\Big(\big[s_1^{\epsilon_1}\cdots s_n^{\epsilon_n}\big]\Big) * \overline{\varphi}\Big(\big[s_{n+1}^{\epsilon_{n+1}}\cdots s_m^{\epsilon_m}\big]\Big)
\end{aligned}$$

por lo tanto $\overline{\varphi}$ es homomorfismo.

ii) Ahora probaremos que $\overline{\varphi}$ cumple que $\overline{\varphi}\circ i = \varphi$;

Sea $s \in S$

$$\begin{aligned}
\big(\overline{\varphi}\circ i\big)(s) &= \overline{\varphi}\big(i(s)\big) \\
&= \overline{\varphi}\big([s]\big) \\
&= \varphi^*(s) \\
&= \varphi(s)
\end{aligned}$$

por lo tanto, $\overline{\varphi}\circ i = \varphi$.

Como $F(S) = \big\langle i(s)\big\rangle_{F(S)}$, ya que $\big\langle i(s)\big\rangle_{F(S)} = \big\{[s_1]^{\epsilon_1}\cdots[s_n]^{\epsilon_n}\big\}$, por la ecuación 1.1, entonces podemos decir que $i(s)$ genera a $F(S)$.

- Como segundo paso, demostraremos que $\overline{\varphi}$ es el único homomorfismo que cumple que $\overline{\varphi}\circ i = \varphi$.

  Supongamos que existe otro homomorfismo;

$$\Psi : F(S) \longrightarrow G, \text{ tal que } \Psi\circ i = \varphi, \text{ asi } \Psi\big([s]\big) = \varphi(s),\ \forall s \in S.$$

Sea $x \in F(S)$, donde $x = \big[s_1^{\epsilon_1}\cdots s_n^{\epsilon_n}\big]$. Entonces;

$$\begin{aligned}
\Psi(x) &= \Psi\big(s_1^{\epsilon_1}\cdots s_n^{\epsilon_n}\big) \\
&= \Psi\big([s_1]\big)^{\epsilon_1}\cdots\Psi\big([s_n]\big)^{\epsilon_n} \qquad \text{; por suposición } \Psi \text{ es un homomorfismo} \\
&= \varphi(s_1)^{\epsilon_1}\cdots\varphi(s_n)^{\epsilon_n} \\
&= \varphi^*\big(s_1^{\epsilon_1}\cdots s_n^{\epsilon_n}\big) \\
&= \overline{\varphi}\Big(\big[s_1^{\epsilon_1}\cdots s_n^{\epsilon_n}\big]\Big) \\
&= \overline{\varphi}(x)
\end{aligned}$$

Luego $\Psi = \overline{\varphi}$, así $\overline{\varphi}$ es único.

Por lo tanto, hemos demostrado $F(S)$ es generado libremente por S, ya que, para cualquier grupo G y para cualquier función φ existe un único homomorfismo $\overline{\varphi}$, que cumple que $\overline{\varphi} \circ i = \varphi$

Y por último, demostraremos que i es inyectiva, de esta forma $F(S)$ contiene una copia de S, es decir, que se puede considerar que $S \subset F(S)$.

Sea $s_1, s_2 \in S$, tales que $s_1 \neq s_2$. Ahora, definamos σ.

Sea

$$\begin{aligned} \sigma : S &\longrightarrow \mathbb{Z} \\ s_1 &\longmapsto 1 \\ s_2 &\longmapsto -1 \\ s \neq s_1 \neq s_2 &\longmapsto 0 \end{aligned}$$

Como σ es función, por la propiedad universal para $F(S)$, existe un único homomorfismo $\overline{\varphi}$ tal que $\overline{\varphi} \circ i = \sigma$. Luego,

$$\begin{aligned} \overline{\varphi}\big(i(s_1)\big) &= \big(\sigma \circ i\big)(s_1) \\ &= \sigma(s_1) \\ &= 1 \\ &\neq -1 \\ &= \sigma(s_2) \\ &= \big(\sigma \circ i\big)(s_2) \\ &= \overline{\varphi}\big(i(s_2)\big) \end{aligned}$$

Como σ es función, entonces $i(s_1) \neq i(s_2)$. Por tanto, i es inyectiva.

i, es inyectiva, asi $S \subset F(S)$, ya que $i(S)$ es una copia biyectiva de S y $i(S) \subset F(S)$, entonces podemos asumir $S \subset F(S)$

□

Nota:

De aquí en adelante debemos entender tres cosas:

- $s_1 \cdots s_n \coloneqq s_1 * \cdots * s_n \in S \subset (G, *)$
- En $F(S)$: $s_1 \cdots s_n \coloneqq [s_1 \cdots s_n]$

- En $\left(S \cup \widehat{S}\right)^*$: para $s_1 \cdots s_n$, se cumple que $s_1 \cdots s_n = \epsilon \iff s_1 \cdots s_n \sim \epsilon$

Corolario 1.1
Sea F un grupo libre, y sea S un conjunto generador libre de F. Entonces, S genera a F.

Demostración. Vamos a probar que S genera a F. Tenemos por hipótesis que S es un conjunto generador libre de F.

En la demostración del teorema 1.2, se construyo el conjunto libre, donde a la misma ves, se probó que es un grupo generado libremente por S;

$$F(S) = A^* / \sim$$

el corolario es válido para este grupo. Si probamos que $F(S) \cong F$ entonces la prueba queda concluida.

Por la proposición 1.3, nos garantiza la unicidad del grupo generado libremente por S, entonces;

$$F(S) \cong F$$

es un isomorfismo, que es la identidad sobre S. Como S genera a $F(S)$, y $F(S) \cong F$, entonces S genera F.

□

Proposición 1.4 (Rango de los grupos libres)
Sea F un grupo libre, finitamente generado.

1. Sea $S \subset F$ un conjunto generador libre finito de F y sea S' un conjunto generador finito de F. Entonces $\left|S'\right| \geq |S|$.
2. En particular, todos los conjuntos generadores libres finitos tienen la misma cardinalidad.

Demostración. Iniciaremos probando que $\left|S'\right| \geq |S|$.

1. Consideremos $(\mathbb{Z}/2)^S = \left\{ \; f : S \longrightarrow \mathbb{Z}/2 \;\middle|\; f \text{ es función} \; \right\}$.

   Además, $(\mathbb{Z}/2)^S$ es un espacio vectorial con las operaciones:

i) Si $f, g \in (\mathbb{Z}/2)^S$ entonces $\left(f+g\right)(s) := f(s) + g(s)$.
ii) Si $f \in (\mathbb{Z}/2)^S$ y $m \in \mathbb{Z}/2$ entonces $\left(mf\right)(s) := mf(s)$.

Así, como es un espacio vectorial, tiene una base, la cual es

$$B = \left\{ \ f_s \ \middle| \ s \in S \ \right\}$$

definida como

$$\begin{aligned} f_s : S &\longrightarrow \mathbb{Z}/2 \\ t &\longmapsto f_s(t) \end{aligned}$$

donde $f_s(t) = \begin{cases} \overline{1}, & \text{si } t = s \\ \overline{0}, & \text{si } t \neq s \end{cases}$

Si $s \in S$, tendremos que $f_s \in B$ y si $f_s \in B$, por definición de B , entonces $s \in S$. Así, $|B| = |S|$.

Ahora probemos que B es linealmente independiente como $\mathbb{Z}/2$-módulo.

Sean $\overline{m_1}, \overline{m_2}, ..., \overline{m_k} \in \mathbb{Z}/2$, tales que $\overline{m_1} f_{s_1} + \overline{m_2} f_{s_2} + \cdots + \overline{m_k} f_{s_k} = 0$.

$$\begin{aligned} \overline{m_1} f_{s_1} + \overline{m_2} f_{s_2} + \cdots + \overline{m_k} f_{s_k} = 0 &\Rightarrow \left(\overline{m_1} f_{s_1} + \overline{m_2} f_{s_2} + \cdots + \overline{m_k} f_{s_k}\right)\left(s_j\right) = 0(s_j) \\ &\Rightarrow \overline{m_1} f_{s_1}\left(s_j\right) + \overline{m_2} f_{s_2}\left(s_j\right) + \cdots + \overline{m_k} f_{s_k}\left(s_j\right) = \overline{0}. \end{aligned}$$

Si tomamos $s_j = s_1$ tendremos:

$$\begin{aligned} \overline{m_1} f_{s_1}(s_1) + \overline{m_2} f_{s_2}(s_1) + \cdots + \overline{m_k} f_{s_k}(s_1) = \overline{0} &\Rightarrow \overline{m_1}\left(\overline{1}\right) + \overline{m_2}\left(\overline{0}\right) + \cdots + \overline{m_k}\left(\overline{0}\right) = \overline{0} \\ &\Rightarrow \overline{m_1} = 0 \end{aligned}$$

Si tomamos $s_j = s_2$, tendremos:

$$\begin{aligned} \overline{m_1} f_{s_1}(s_2) + \overline{m_2} f_{s_2}(s_2) + \cdots + \overline{m_k} f_{s_k}(s_2) = \overline{0} &\Rightarrow \overline{m_1}\left(\overline{0}\right) + \overline{m_2}\left(\overline{1}\right) + \cdots + \overline{m_k}\left(\overline{0}\right) = \overline{0} \\ &\Rightarrow \overline{m_2} = 0 \end{aligned}$$

Si continuamos el proceso hasta $s_j = s_k$, obtendremos que $\overline{m_k} = 0$.

Así, $\overline{m_1} = \overline{m_2} = ... = \overline{m_k} = 0$, por lo que B es linealmente independiente en $\mathbb{Z}/2-$módulo.

Ahora probemos que B genera a $(\mathbb{Z}/2)^S$.

Sea $h \in (\mathbb{Z}/2)^S$.

Observamos que $h = \sum_{s \in S} h(s) f_s$ ya que si $t \in S$, entonces:

$$\begin{aligned} h(t) &= h(t)\overline{1} \\ &= h(t) f_t(t) + 0 \\ &= h(t) f_t(t) + \sum_{s \in S - t} h(t) f_s(t) \\ &= \sum_{s \in S} h(s) f_s(t) \end{aligned}$$

Así, $h = \sum_{s\in S} h(s) f_s$.

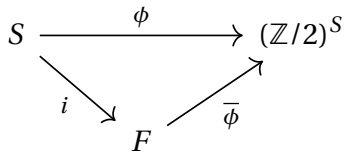
Luego, tomando $\alpha_s = h(s)$ se tiene $h = \sum_{s\in S} \alpha_s f_s$, así B es base de $(\mathbb{Z}/2)^S$.

Como ya vimos $|B| = |S|$, además, como $(\mathbb{Z}/2)^S$ es espacio vectorial tendremos que $|B| = \dim(\mathbb{Z}/2)^S$, lo cual implicaría que $|S| = \dim(\mathbb{Z}/2)^S$.

Ahora definamos

$$\begin{aligned} \phi : S &\longrightarrow (\mathbb{Z}/2)^S \\ s &\longmapsto \phi(s) = f_s \end{aligned}$$

Como F es libremente generado por S, así existe $\overline{\phi} : F \longrightarrow (\mathbb{Z}/2)^S$ homomorfismo tal que $\overline{\phi}|_S = \phi$ y el siguiente diagrama conmuta:



Por hipótesis, tenemos que S' genera a F, en otras palabras, $F = \langle S' \rangle_F$. Verifiquemos que $\overline{\phi}$ es sobreyectiva.

Sea $h \in (\mathbb{Z}/2)^S$.

Como B es base, podemos escribir h como

$$\begin{aligned} h \in (\mathbb{Z}/2)^S \Rightarrow h &= \sum_{s\in S} h(s) f_s \\ \Rightarrow h &= \sum_{s\in S} h(s)\overline{\phi}(s) \end{aligned}$$

Y como F es libremente generado, entonces $\overline{\phi}(s) = f_s$ y si $h(s) \in \mathbb{Z}/2$, entonces $h(s) = \overline{0}$ ó $h(s) = \overline{1}$.

Ahora definamos $\widehat{h} : S \to F$ como $\widehat{h} = \begin{cases} 0, & \text{si } h(s) = \overline{0} \\ 1, & \text{si } h(s) = \overline{1} \end{cases}$

Dado que $\overline{\phi}$ es homomorfismo tendremos:

$$\begin{aligned} h = \sum_{s\in S} h(s)\overline{\phi}(s) \Rightarrow h &= \sum_{s\in S} \overline{\phi}\left(\widehat{h}(s)s\right) \\ \Rightarrow h &= \overline{\phi}\left(\prod_{s\in S} \widehat{h}(s)s\right) \end{aligned}$$

Por lo tanto, $\overline{\phi}$ es sobreyectiva.

Ahora bien, como S' genera a F y $\phi : F \longrightarrow (\mathbb{Z}/2)^S$ es un homomorfismo sobreyectivo, tendremos que $\overline{\phi}(S')$ genera a $(\mathbb{Z}/2)^S$ de modo que:

$$|S| = \dim(Z/2)^S \leq \left|\overline{\phi}(S')\right|$$

Como $\overline{\phi}|_{S'} : S' \to \overline{\phi}(S')$ es sobreyectiva, así $|S'| \geq \left|\left(\overline{\phi}(S')\right)\right|$. Por lo que: $\left|\overline{\phi}(S')\right| \geq |S|$ y $|S'| \geq \left|\overline{\phi}(S')\right|$, así, $|S'| \geq \left|\overline{\phi}(S')\right| \geq |S|$, de donde se obtiene el resultado deseado.

Por lo tanto, $|S'| \geq |S|$.

2. Ahora probaremos que todos los conjuntos generadores libres tienen la misma cardinalidad.

   Sean S', S dos conjuntos finitos que son generadores libres de F.

   Como S es generador libre y S' es un generador de F, así por la primera parte de esta proposición $|S'| \geq |S|$. Además, S' también es generador libre, y S es generador entonces $|S| \geq |S'|$.

   Por lo tanto, $|S| = |S'|$.

   $\therefore$ Todos los conjuntos generadores libres finitos tienen la misma cardinalidad.

□

Definición 1.12 (Grupo libre F_n)

Sean $n \in \mathbb{N}$ y $S = \{x_1, \ldots, x_n\}$, donde $x_1, \ldots, x_1$ son n elementos distintos. Entonces escribimos F_n para "el" grupo generado libremente por S, y llamamos F_n, el **grupo libre** de rango n.

Ahora dedicaremos un momento para demostrar un resultado bastante útil, el cual se enuncia de la siguiente manera:

Proposición 1.5

Si $f : G \longrightarrow H$ es homomorfismo de grupo y $\langle S \rangle_G = G$, entonces $\langle f(S) \rangle_{\text{im}\,(f)} = \text{im}\,(f)$.

Demostración. Se demostrará que $\langle f(S) \rangle_{\text{im}\,(f)} \subset \text{im}\,(f)$ y $\text{im}\,(f) \subset \langle f(S) \rangle_{\text{im}\,(f)}$ para obtener la igualdad deseada.

"$\langle f(S) \rangle_{\text{im}\,(f)} \subset \text{im}\,(f)$"

Como la imagen de f es el grupo, la primera inclusión $\langle f(S)\rangle_{\text{im}\,(f)} \subset \text{im}\,(f)$ es evidente, porque se considera el generador en la imagen de f, (aquí el universo es la imagen de F).

"im $(f) \subset \langle f(S)\rangle_{\text{im}\,(f)}$"

Sea $h \in \text{im}\,(f)$.

$$h \in \text{im}\,(f) \Longrightarrow h = f(x), x \in G.$$

Ahora bien

$$x \in G \Longrightarrow x \in G = \langle S\rangle_G = \left\{ s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} \;\middle|\; s_i \in S, \epsilon_i \in \{-1,1\}, i = 1,\ldots,n \in \mathbb{N} \right\}$$

$$\begin{aligned}
&\Longrightarrow f(x) = f\left(s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}\right) \\
&\Longrightarrow f(x) = f(s_1)^{\epsilon_1} \cdots f(s_n)^{\epsilon_n} && \text{; ya que } f \text{ es homomorfismo} \\
&\Longrightarrow h = f(s_1)^{\epsilon_1} \cdots f(s_n)^{\epsilon_n} && \text{; } h = f(x) \\
&\Longrightarrow h = f(s_1)^{\epsilon_1} \cdots f(s_n)^{\epsilon_n} \in \langle f(S)\rangle_{\text{im}\,(f)}
\end{aligned}$$

Como $h \in \text{im}\,(f)$ y hemos llegado a que $h \in \langle f(S)\rangle_{\text{im}\,(f)}$, así , im $(f) \subset \langle f(S)\rangle_{\text{im}\,(f)}$.

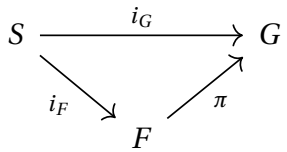
Por lo tanto, im $(f) = \langle f(S)\rangle_{\text{im}\,(f)}$. □

Corolario 1.2
Un grupo se genera finitamente si y solo si es el cociente de un grupo libre finitamente generado, es decir, un grupo G es finitamente generado si y solo si existe un grupo libre F finitamente generado y un homomorfismo de un grupo sobreyectivo $F \longrightarrow G$.

Demostración. Vamos a demostrar la primera implicación.
"$\Longrightarrow$" Si un grupo se genera finitamente, entonces es el cociente de un grupo libre finitamente generado.

Sea G un grupo generado finitamente, supongamos que es generado por el conjunto finito S, tal que $S \subset G$ y sea F un grupo libre generado por S, por el corolario 1.1, como F es generado por S, el cual es finito, entonces tendremos que F es un grupo libre finitamente generado.

Ahora, por la propiedad universal de grupos libres tendremos:



es decir, existe la extensión π que cumple que: $\pi \circ i_F = i_G = id|_S$, es decir, la función identidad en S.

Ahora probemos que π es sobreyectiva.

Como S genera a G y además $S \subseteq \text{im } (\pi)$, así $G = \langle S \rangle_G \subset \langle \text{im } (\pi) \rangle_G = \text{im } (\pi)$, luego $\text{im } (\pi) = G$, así π es sobreyectiva.

Por lo que $G \cong F/\ker \pi$ (Por el Primer Teorema de Isomorfismo), es decir, G es el cociente de un grupo libre finitamente generado.

"$\Longleftarrow$" Si G es el cociente de un grupo libre finitamente generado, entonces G se genera finitamente.

Supongamos que G es el cociente de un grupo libre finitamente generado, así existe un isomorfismo $\psi : F/N \to G$ (N no necesariamente el ker).

Definamos

$$\begin{aligned} \pi : F &\longrightarrow G \\ x &\longmapsto \pi(x) = \psi(xN) \end{aligned}$$

- Probemos que π es función.

  Sean $x, y \in F$, tal que $x = y$

  $$\begin{aligned} x = y \in F &\Longrightarrow xN = yN \\ &\Longrightarrow \psi(xN) = \psi\left(yN\right) \\ &\Longrightarrow \pi(x) = \pi\left(y\right) \end{aligned}$$

  Por lo tanto, π es función.

- Probemos que π es homomorfismo.

  Sean $x, y \in F$.

  $$\begin{aligned} \pi\left(xy\right) &= \psi\left(xyN\right) \\ &= \psi\left((xN)\left(yN\right)\right) \\ &= \psi(xN)\,\psi\left(yN\right)) \\ &= \pi(x)\,\pi\left(y\right) \end{aligned}$$

  Así, π es homomorfismo.

- Ahora, veremos que π es sobreyectivo.

  Sea $g \in G$. Como ψ es isomorfismo, entonces existe xN en F/N tal que $\psi(xN) = g$.

  Pero, $\psi(xN) = \pi(x)$, así, $\pi(x) = \psi(xN) = g$.

  Por lo que, π es sobreyectivo.

Así, existe $\pi : F \longrightarrow G$ homomorfismo sobreyectivo, como F es finitamente generado como grupo, digamos que el conjunto finito que lo genera es S, esto es, $\langle S \rangle_F = F$ con S finito; entonces $\pi(S)$ genera a im $(\pi) = G$, pero sabemos que S es finito, por lo que $\pi(S)$ también es finito.

Por lo tanto, $G = \langle \pi(S) \rangle_G$, es decir, G es finitamente generado.

□

1.3. Generadores y relaciones

Los grupos libres nos permiten generar grupos genéricos sobre un conjunto dado; para obligar a los generadores a satisfacer una lista dada de ecuaciones de teoría de grupos, dividimos un subgrupo normal adecuado.

Definición 1.13 (Generador normal)

Sea G un grupo y sea un subconjunto $S \subset G$. El subgrupo normal de G generado por S es el subgrupo normal más pequeño (con respecto a la inclusión) de G que contiene S; se denota por $\langle S \rangle_G^{\triangleleft}$.

Nota:

Sea G un grupo y sea $S \subset G$. Entonces el subgrupo normal generado por S en G siempre existe y se puede describir de la siguiente manera:

$$\begin{aligned} \langle S \rangle_G^{\triangleleft} &= \bigcap \left\{ H \;\middle|\; H \subset G \text{ es un subgrupo con } S \subset H \right\} \\ &= \left\{ g_1 \cdot s_1^{\varepsilon_1} \cdot g_1^{-1} \cdots g_n \cdot s_n^{\varepsilon_n} \cdot g_n^{-1} \;\middle|\; n \in \mathbb{N},\ s_1, \ldots, s_n \in S,\ \varepsilon_1, \ldots, \varepsilon_n \in \{-1, +1\},\ g_1, \ldots, g_n \in G. \right\} \end{aligned} \tag{1.6}$$

Si G es un grupo, y $N \triangleleft G$, entonces, en general, es bien difícil determinar cuál es el número mínimo de elementos de un subconjunto $S \subset G$ este satisface $\langle S \rangle_G^{\triangleleft} = N$.

A continuación, usamos la notación A^* para el conjunto de palabras (posiblemente vacío) en un conjunto A; además, abusamos de la notación y denotamos elementos del grupo libre $F(S)$ sobre un conjunto S por palabras en $\left(S \cup S^{-1}\right)^*$ (aunque, estrictamente hablando, los elementos de $F(S)$ son clases de equivalencia de palabras en $\left(S \cup S^{-1}\right)^*$). Si queremos enfatizar la formalidad de los inversos, a veces también usaremos palabras en $\left(S \cup \widehat{S}\right)^*$ en lugar de $\left(S \cup S^{-1}\right)^*$. En otras palabras estaremos trabajando como si $F(S) = \left(S \cup S^{-1}\right)^*$, donde $x = y$ si y sólo sí $x \sim y$.

Definición 1.14

Sea S un conjunto, sea $R \subset F(S)$ un subconjunto; sea $F(S)$ el grupo libre generado por S entonces el grupo

$$\langle S \mid R \rangle := F(S) \,/\, \langle R \rangle^{\triangleleft}_{F(S)}$$

se dice que es **generado por S con las relaciones R.**
Si G es un grupo con $G \cong \langle S \mid R \rangle$, entonces el par (S, R) **es una presentación de** G ; también usamos el símbolo $\langle S \mid R \rangle$ para denotar esta presentación.

Las relaciones de la forma "$w \cdot w'^{-1}$" también se denotan a veces como "$w = w'$", porque en el grupo generado, las palabras w y w' representan el mismo elemento del grupo.

La siguiente proposición es una manera formal de decir que $\langle S \mid R \rangle$ es un grupo en el que las relaciones R se cumplen de la forma más no trivial posible:

Proposición 1.6 (Propiedad universal de generadores y relaciones)

Sea S un conjunto y sea $R \subset \left(S \cup S^{-1}\right)^*$. El grupo $\langle S \mid R \rangle$ generado por S con relaciones R junto con el mapeo canónico $\pi : S \longrightarrow F(S) \,/\, \langle R \rangle^{\triangleleft}_{F(S)} = \langle S \mid R \rangle$ tiene la siguiente propiedad universal: Para todo grupo G y cada mapeo $\varphi : S \longrightarrow G$ con la propiedad que

$$\varphi^*(r) = e \in G$$

se cumple para todas las palabras $r \in R$, que existe precisamente un homomorfismo de grupo $\overline{\varphi} : \langle S \mid R \rangle \longrightarrow G$ tal que $\overline{\varphi} \circ \pi = \varphi$; aquí, $\varphi^* : \left(S \cup S^{-1}\right)^* \longrightarrow G$ es la extensión canónica de φ a palabras sobre $S \cup S^{-1}$ (Como se describe en la prueba del teorema 1.2). Además $\langle S \mid R \rangle$ (junto con π) se determina de forma única (hasta el isomorfismo canónico) por esta propiedad universal.

Demostración. Queremos demostrar que para todo grupo G y cada mapeo $\varphi : S \longrightarrow G$ (con la propiedad que $\varphi^*(r) = e \in G$ se cumple para todo las palabras) existe precisamente un homomorfismo de grupo $\overline{\varphi} : \langle S \mid R \rangle \longrightarrow G$ tal que $\overline{\varphi} \circ \pi = \varphi$.

Sea G un grupo y sea $\varphi : S \longrightarrow G$ una función tal que $\varphi^*(r) = e, \forall r \in \mathbb{R}$.

Y tomemos $H = \langle R \rangle^{\triangleleft}_{F(S)}$, como $F(S)$ es el grupo libre generado por S, para φ se tendría que por la propiedad universal existe un único homomorfismo $\varphi^* : F(S) \longrightarrow G$ (este es el mismo homomorfismo que aparece en el enunciado) tal que $\varphi^*|_S = \varphi$. Y el siguiente diagrama conmuta:

$$\begin{array}{ccc} S & \xrightarrow{\varphi} & G \\ \downarrow{\scriptstyle i} & \nearrow_{\varphi^*} & \\ F(S) & & \end{array}$$

Sea $x \in H = \langle R \rangle^{\triangleleft}_{F(S)}$.

$$x \in H \Longrightarrow x = y_1 r_1^{\epsilon_1} y_1^{-1} \cdots y_n r_n^{\epsilon_n} y_n^{-1}; \text{ donde } y_i \in F(S), \epsilon_i \in \{-1, 1\}, n \in \mathbb{N}$$

Ahora, aplicando φ^*, tenemos:

$$\begin{aligned} \varphi^*(x) &= \varphi^*\left(y_1 r_1^{\epsilon_1} y_1^{-1} \cdots y_n r_n^{\epsilon_n} y_n^{-1}\right) \\ &= \varphi^*\left(y_1\right)\varphi^*(r_1)^{\epsilon_1}\varphi^*\left(y_1\right)^{-1} \cdots \varphi^*\left(y_n\right)\varphi^*(r_n)^{\epsilon_n}\varphi^*\left(y_n\right)^{-1}; \end{aligned}$$

Pero como $\varphi^*(r) = e, \forall r \in \mathbb{R}$, así:

$$\begin{aligned} \varphi^*(x) &= \varphi^*\left(y_1\right)\varphi^*\left(y_1\right)^{-1} \cdots \varphi^*\left(y_n\right)\varphi^*\left(y_n\right)^{-1} \\ &= e \cdots e = e \end{aligned}$$

Así, $x \in \ker\varphi^*$.

Por lo tanto, $H \subset \ker\varphi^*$.

Ahora, por la propiedad universal de la proyección (proposición 1.5-ítem 2), tendremos que existe un único homomorfismo $\overline{\varphi} : \langle S \mid R \rangle \longrightarrow G$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} F(S) & \xrightarrow{\varphi^*} & G \\ \downarrow{\scriptstyle \pi'} & \nearrow_{\overline{\varphi}} & \\ \langle S \mid R \rangle & & \end{array}$$

es decir, $\overline{\varphi} \circ \pi' = \varphi^*$, aquí $\pi'(x) = xH$.

Como $\pi = \pi'|_S = \pi' \circ i$, tenemos que:

$$\begin{aligned} \overline{\varphi} \circ \pi &= \overline{\varphi} \circ \pi' \circ i \\ &= \varphi^* \circ i \qquad \text{; ya que } \overline{\varphi} \circ \pi' = \varphi^* \end{aligned}$$

Pero $\varphi^*|_S$ es φ, así

$$\begin{aligned}\overline{\varphi}\circ\pi &= \varphi^*\circ i\\ &= \varphi^*|_S = \varphi\end{aligned}$$

Por lo tanto, $\overline{\varphi}\circ\pi = \varphi$.

Ahora probaremos la unicidad.

Suponga que existe un homomorfismo $\overline{\overline{\varphi}}:\langle S\mid R\rangle \longrightarrow G$ tal que $\overline{\overline{\varphi}}\circ\pi = \varphi$.

Sea $x\in F(S)$.

$x\in F(S)\Longrightarrow x = s_1^{\epsilon_1}\cdots s_n^{\epsilon_n};\ \ i=1,...,n\in\mathbb{N}, s_i\in S$ y $\epsilon_i\in\{-1,1\}$

Ahora bien,

$$\begin{aligned}\left(\overline{\overline{\varphi}}\circ\pi'\right)(x) &= \left(\overline{\overline{\varphi}}\circ\pi\right)\left(s_1^{\epsilon_1}\cdots s_n^{\epsilon_n}\right)\\ &= \left(\overline{\overline{\varphi}}\circ\pi'\right)(s_1)^{\epsilon_1}\cdots\left(\overline{\overline{\varphi}}\circ\pi'\right)(s_n)^{\epsilon_n}.\end{aligned}$$

Y como $\pi'|_S = \pi$, entonces de lo anterior tenemos:

$$\begin{aligned}\left(\overline{\overline{\varphi}}\circ\pi'\right)(x) &= \left(\overline{\overline{\varphi}}\circ\pi\right)(s_1)^{\epsilon_1}\cdots\left(\overline{\overline{\varphi}}\circ\pi\right)(s_n)^{\epsilon_n}\\ &= \varphi(s_1)^{\epsilon_1}\cdots\varphi(s_n)^{\epsilon_n}\\ &= \varphi^*\left(s_1^{\epsilon_1}\cdots s_n^{\epsilon_n}\right)\\ &= \varphi^*(x)\end{aligned}$$

Con lo que llegamos a que $\overline{\overline{\varphi}}\circ\pi' = \varphi^*$. Pero $\overline{\varphi}$ es el único homomorfismo que cumple $\overline{\varphi}\circ\pi' = \varphi^*$, por ende obtenemos que $\overline{\overline{\varphi}} = \overline{\varphi}$.

Ahora probaremos que $\langle S\mid R\rangle$ se determina de manera única.

Sea H un grupo que cumpla la propiedad universal descrita en el enunciado. Probemos que si existe tal grupo H que cumpla la propiedad universal, entonces se debe cumplir que $\langle S\mid R\rangle$ y H son isomorfos.

Como $\langle S\mid R\rangle$ es generado libremente por S, por la propiedad universal existe un único homomorfismo

$$j:\langle S\mid R\rangle\longrightarrow H$$

tal que $j\circ\theta = \theta'$, donde θ,θ' son las funciones proyección.

De forma similar como H es generado libremente por S por la propiedad universal existe un único homomorfismo

$$k : H \longrightarrow \langle S \mid R \rangle$$

tal que $k \circ \theta' = \theta$.

Ahora, consideremos el producto $h = k \circ j$ y el homomorfismo identidad i, así tendremos:

$$\begin{aligned} h \circ \theta &= k \circ j \circ \theta \\ &= k \circ \big(j \circ \theta\big) \\ &= k \circ \theta' \qquad ; \text{ ya que } j \circ \theta = \theta' \\ &= \theta \qquad\quad ; \text{ ya que } k \circ \theta' = \theta \end{aligned}$$

Pero como k y j son únicos, entonces:

$$h = k \circ j = i \Longrightarrow k \circ j = i$$

De la misma manera, consideremos el producto $h = j \circ k$ y el homomorfismo identidad i.

Bajo esas consideraciones, tendremos que:

$$\begin{aligned} h \circ \theta' &= j \circ k \circ \theta' \\ &= j \circ \big(k \circ \theta'\big) \end{aligned}$$

$$\begin{aligned} h \circ \theta' &= j \circ \theta \qquad ; \text{ya que } k \circ \theta' = \theta \\ &= \theta' \qquad\quad ; \text{ya que } j \circ \theta = \theta' \end{aligned}$$

Pero como k y j son homomorfismos únicos, entonces:

$$h = j \circ k = i \Longrightarrow j \circ k = i$$

Por lo que, k y j son isomorfos.

Por lo tanto, H y $\langle S \mid R \rangle$ son isomorfos y son determinados únicamente por θ' y θ.

□

Ejemplo 1.9

Para todo $n \in \mathbb{N}$, tenemos $\langle x \mid x^n \rangle \cong \mathbb{Z}/n$. Esto se puede ver a través de la propiedad universal.

Análisis: Probaremos que $\mathbb{Z}/n$ cumple la propiedad universal.

Sea $S = \{x\}$, $R = \{x^n\}$.
Definimos la proyección π, como:

$$\begin{aligned} \pi : S &\longrightarrow \mathbb{Z}/n \\ x &\longmapsto \overline{1} \end{aligned}$$

Ahora, sea G un grupo y sea un mapeo $\varphi : S \longrightarrow G$ con la propiedad que $\varphi^*(x^n) = e$. Consideramos al mapeo $\overline{\varphi}$, definido como:

$$\begin{aligned} \overline{\varphi} : \mathbb{Z}/n &\longrightarrow G \\ \overline{m} &\longmapsto \overline{\varphi}(\overline{m}) = \varphi(x)^m \end{aligned}$$

- $\overline{\varphi}$ esta bien definida.
  Sea $\overline{m}, \overline{t} \in \mathbb{Z}/n$ tal que $\overline{m} = \overline{t}$.

  $$\begin{aligned} \overline{m} = \overline{t} &\Longrightarrow \overline{\varphi}(\overline{m}) = \overline{\varphi}(\overline{t}) \\ &\Longrightarrow \varphi(x)^m = \varphi(x)^t \end{aligned}$$

  $\therefore$ $\overline{\varphi}$ esta bien definida.

- $\overline{\varphi}$ es homomorfismo.
  Sea $\overline{m}, \overline{t} \in \mathbb{Z}/n$ entonces

  $$\begin{aligned} \overline{\varphi}(\overline{m} + \overline{t}) &= \overline{\varphi}(\overline{m+t}) \\ &= \varphi(x)^{m+t} && \text{; por propiedad de exponentes} \\ &= \varphi(x)^m + \varphi(x)^t \end{aligned}$$

  $\therefore$ $\overline{\varphi}$ es homomorfismo.

- $\overline{\varphi}$ es único.
  Supongamos que existe otro homomorfismo $\phi : \mathbb{Z}/n \longrightarrow G$ tal que $\phi \circ \pi = \varphi$.

Como $\phi \circ \pi = \varphi$, definimos lo siguiente: $\phi\left(\overline{1}\right) = \phi\left(\pi\left(s\right)\right) = \varphi\left(x\right)$. Luego;

$$\begin{aligned}
\phi\left(\overline{m}\right) &= \phi\left(m \cdot \overline{1}\right) && ;\phi \text{ es homomorfismo} \\
&= \phi\left(\overline{1}\right)^{m} \\
&= \varphi\left(x\right)^{m} && ; \text{por definición} \\
&= \overline{\varphi}\left(\overline{m}\right)
\end{aligned}$$

$\therefore \overline{\varphi}$ es único.

- $\overline{\varphi}$ cumple la propiedad universal.
  Por hipótesis, sabemos que $\overline{\varphi} : \mathbb{Z}/n \longrightarrow G$ y $\pi : S \longrightarrow \mathbb{Z}/n$ entonces

$$\begin{aligned}
\left(\overline{\varphi} \circ \pi\right)\left(x\right) &= \overline{\varphi}\left(\overline{1}\right) \\
&= \varphi\left(x\right)^{1} \\
&= \varphi\left(x\right)
\end{aligned}$$

  $\therefore \overline{\varphi} \circ \pi = \varphi$, se cumple la propiedad universal.

Por la proposición anterior se comprueba que $\mathbb{Z}/n$ al cumplir con la propiedad universal es isomorfo a $\langle x \mid x^{n} \rangle$.

■

Capítulo 2

Grafos de Cayley y Grupos libres

Una cuestión fundamental en la teoría geométrica de grupo es cómo los grupos pueden ser vistos como objetos geométricos. Una forma de ver un grupo (finitamente generado) como objeto geométrico es a través de los grafos de Cayley:

- Como primer paso, se asocia una estructura combinatoria con un grupo y un conjunto generador dado: el correspondiente grafo de Cayley. Este paso ya tiene un sabor geométrico rudimentario y se discute en este capítulo.
- Como segundo paso, se añade una estructura métrica a los grafos de Cayley mediante métrica de palabras. Estudiaremos este paso en el capítulo 3.

En este capítulo iniciaremos introduciendo los grafos de Cayley y discutimos ejemplos básicos de grafos de Cayley en la sección 2.1; en particular, mostraremos que los grupos libres pueden caracterizarse combinatoriamente mediante árboles: El grafo de Cayley de un grupo libre con respecto a un conjunto generador libre es un árbol; por el contrario, si un grupo admite un grafo de Cayley que es un árbol, entonces el conjunto generador correspondiente es libre (sección 2.2).

2.1. Grafos de Cayley

Comenzamos revisando alguna terminología básica de la teoría de grafos. En lo siguiente, siempre consideraremos grafos simples, sin dirección y sin bucles:

Definición 2.1 (Grafos)

Un **grafo** es un par $X = (V, E)$ de conjuntos disjuntos donde E es un conjunto de subconjuntos de V que contienen exactamente dos elementos, es decir,

$$E \subset V^{[2]} := \left\{ \; e \;\middle|\; e \subset V,\ |e| = 2 \; \right\}.$$

Los elementos de V son los vértices, los elementos de E son las aristas de X.

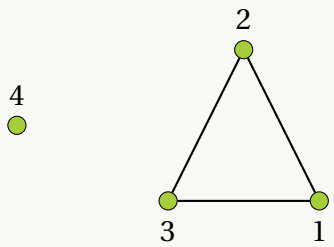
Definición 2.2 (Adyacente, vecino, grado)

- Decimos que dos vértices $v, v' \in V$ son **vecinos** o **adyacentes** si están unidos por una arista, es decir, si $\{v, v'\} \in E$.
- El número de vecinos de un vértice es el **grado** de este vértice.

Dicho de otra manera, los grafos son un punto de vista diferente en las relaciones (simétricas) y normalmente se utilizan grafos para modelar relaciones; la forma usual de trazar un grafo es dibujando un punto por cada vértice y unir dos de estos puntos con una línea si los dos vértices correspondientes forman una arista. Cómo se dibujan estos puntos y líneas es irrelevante, todo lo que importa es la información sobre los pares de vértices que forman aristas y los que no.

Ejemplo **2.1**

El grafo X_1



tiene vértices $V := \{1, 2, 3, 4\}$ y aristas $E := \{\{1, 2\}, \{2, 3\}, \{3, 1\}\}$.

Análisis:

Construimos lo siguiente: $X_1 := (V, E)$ donde V representa los vértices y E las aristas. Dibujamos los puntos del conjunto V, entonces:

- Para el punto 1 trazamos la recta hacia el punto 2, a esa recta le llamamos: arista, observando que 1 y 2 son vecinos.
- Para el punto 2 trazamos la recta hacia el punto 3, a esa recta le llamamos: arista, observando que 2 y 3 son vecinos.
- Para el punto 3 trazamos la recta hacia el punto 1, a esa recta le llamamos: arista, observando que 3 y 1 son vecinos.
- Para el punto 4 no se define arista por lo tanto no se considera vecino de ninguno de los puntos del conjunto V.

■

Uno de los problemas en teoría de grafos es ver si entre dos vértices hay un camino, además de poder empezar y terminar en el mismo vértice al recorrer un grafo o una parte de él llamada ciclo:

Definición 2.3 (Camino, Ciclo)

Sea $X := (V, E)$ un grafo,

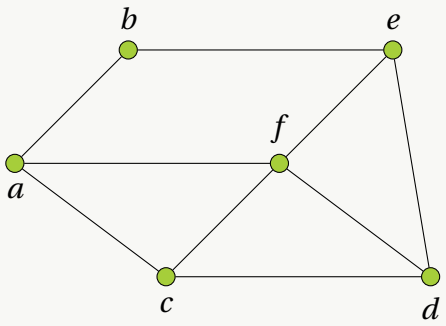
- Sea $n \in \mathbb{N} \cup \{\infty\}$. Un **camino** en X de longitud n es una secuencia $v_0, \ldots, v_n$ de vértices $v_0, \ldots, v_n \in V$ diferentes con la propiedad que $\{v_j, v_{j+1}\} \in E$ tiene para todos los $j \in \{0, \ldots, n-1\}$; si $n < \infty$, entonces decimos que este camino conecta los vértices v_0 y v_n
- Sea $n \in \mathbb{N}_{>2}$. Un **ciclo** en X de longitud n es un camino $v_0, \ldots, v_{n-1}$ en X con $\{v_{n-1}, v_0\} \in E$

Nota:

- Un **camino cerrado** en el grafo es un camino cuyos vértices origen y final son el mismo.
- Un ciclo, también puede ser interpretado como un camino cerrado.
- La **longitud** de un camino se mide por la cantidad de aristas que componen el grafo.

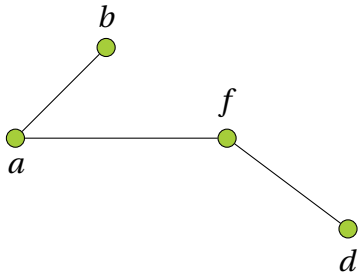
Ejemplo **2.2**

Dado el siguiente grafo, este posee caminos y ciclos:



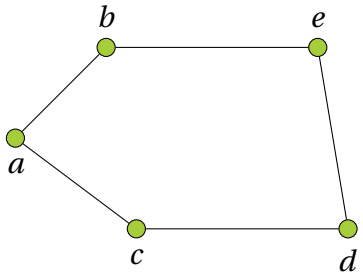
Análisis: La idea de camino y ciclo es la siguiente.

El **camino** posible del grafo de "b" a "d" es:



Este grafo se representa por: $\{b,a\},\{a,f\},\{f,d\}$, ya que entre los vértices de "b" y "d" recorre una sucesión de aristas, con longitud 3.

El **ciclo** del grafo dado es:

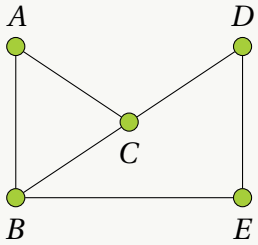


Este grafo se representa por: $\{b,a\},\{a,c\},\{c,d\},\{d,e\},\{e,b\}$, como se logra observar se forma un camino cerrado, con longitud 5. ■

El grafo X se llama **conexo** si cada par de sus vértices puede ser conectado por al menos un camino en X. Un grafo que no es conexo se denomina grafo **disconexo** o **inconexo**.

Ejemplo **2.3**

El presente grafo es conexo:



Análisis:

Se observa que en el grafo los vértices "AB", "AC", "CB", "CD", "EB", "ED" son vecinos simplemente por sus aristas, pero si se observa nuevamente el vértice "E" simplemente no puede ser vecino con el vértice "A" pero puede hacerlo a través de un camino:

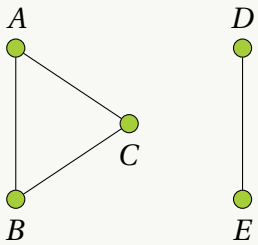
$$A \rightarrow B \rightarrow E$$

Entonces, sabemos que un grafo es conexo si para cualquier par de vértices es posible determinar un camino entre ellos, en otras palabras cualquier vértice que tomemos se puede llegar a otro exactamente por un camino.

■

Ejemplo **2.4**

El presente grafo es disconexo:



Es decir, este grafo representa un caso particular cuando un grafo no es conexo.

Análisis:

Se observa que en el grafo los vértices "AB", "AC", "CB", son vecinos simplemente por sus aristas; además el vértice "D" es vecino del vértice "E".

Ahora si observamos nuevamente el vértice "E" no puede ser vecino del vértice "A" debido a que no existe por lo menos un camino entre esos vértices que los una, por lo cual el grafo dado es disconexo.

■

Hay muchas maneras de extraer las partes de un grafo, hacer combinaciones, o hacer otras operaciones en los grafos a fin de obtener nuevos grafos, una de las formas es extrayendo el subgrafo del grafo dado:

Definición 2.4 (Subgrafo)

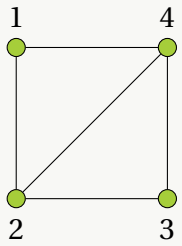
Un **subgrafo** de un grafo (V,E) es un grafo $\left(V',E'\right)$ con $V' \subset V$ y $E' \subset E$.

Es decir, un subgrafo es: Un grafo cuyos conjuntos de vértices y aristas son subconjuntos del grafo dado.

Ejemplo **2.5**

Del siguiente grafo G definimos los vértices y aristas respectivas, notando que este posee subgrafos:

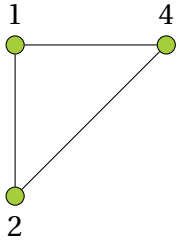
$$V := \{1,2,3,4\}$$
$$E := \{\{1,2\},\{2,3\},\{3,4\},\{4,1\},\{2,4\}\}$$



Análisis:

Sea un grafo G definido por $G := (V,E)$ usando la definición 2.4 tenemos las siguientes coordenadas:

$$V' := \{1,2,4\}$$
$$E' := \{\{2,1\},\{1,4\},\{2,4\}\}$$



Construyendo el subgrafo $G' := (V', E')$. De igual manera podemos formar otro subgrafo del grafo G con los vértices $V'' := \{2, 3, 4\}$.

■

Nota:

Cabe aclarar que un grafo que no es conexo tambien se le define como la unión de dos o más subgrafos conexos que dos a dos no tienen vértices en común. A esos subgrafos conexos se les llama componentes conexas.

El mismo grafo puede representarse de muchas formas. Por tanto, es natural preguntarse cuando dos representaciones corresponden al mismo grafo, o más concretamente, cuando se trata del mismo grafo:

Definición 2.5 (Grafo isomorfo)

Sea $X = (V, E)$ y $X' = (V', E')$ grafos. Los grafos X y X' son isomorfos si existe un **isomorfismo de grafo** entre X y X', es decir, una biyección

$$f : V \longrightarrow V'$$

Tal que para todos los $v, w \in V$ tenemos $\{v, w\} \in E$ si y solo si $\{f(v), f(w)\} \in E'$. Por lo tanto, los grafos isomorfos sólo difieren en las etiquetas de sus vértices.

Los isomorfismos de un grafo a sí mismo se llaman **Automorfismos**. En las operaciones de composición, la familia de todo los automorfismo de un grafo forma a un grupo, llamado **"El grupo de automorfismos del grafo"**.

Nota:

En general dos grafos son isomorfos si tienen exactamente las mismas propiedades, es decir:

1. Deben tener la misma cantidad de vértices.
2. Deben tener la misma cantidad de aristas.
3. Deben tener los mismos grados de los vértices.
4. Deben tener caminos de la misma longitud.

Luego si encontramos un par de grafos que no comparten las mismas propiedades, entonces no son isomorfos.

Ejemplo 2.6

Se presentan los siguientes grafos:

Figura 2.1. Grafos G y G'

Estos grafos son isomorfos.

Análisis:

Para garantizar que dos grafos son isomorfos podemos mostrar que cumplen exactamente las mismas propiedades. A partir de ello tenemos lo siguiente:

- Los vértices del grafo G son $\{a, b, c, d\}$ y los vértices del grafo G' son $\{x, y, z, u\}$, de manera que ambos grafos poseen 4 vértices.
- El número de aristas en el grafo G estan representadas por $\{e_1, e_2, e_3, e_4\}$ y las aristas del grafo G' están representadas por $\{e'_1, e'_2, e'_3, e'_4\}$, de manera que ambos grafos poseen 4 aristas.
- Los grados de los vértices son:

Grafo G	Grafo G'
$a \longrightarrow 2$	$x \longrightarrow 2$
$b \longrightarrow 2$	$y \longrightarrow 2$
$c \longrightarrow 2$	$z \longrightarrow 2$
$d \longrightarrow 2$	$u \longrightarrow 2$

  Observando que los grados de los vértices de ambos grafos son de 2 grados.

- Ambos grafos poseen caminos de longitud 4.
  Concluimos que los grafos dados son isomorfos.

Ahora, la condición suficiente para que los grafos dados sean isomorfos es usando la definición 2.5.

Sean los grafos G y G' isomorfos, existe una biyección $f : V \longrightarrow V'$ tal que la asígnación de cada vértice del grafo G y cada vértice del grafo G' hace que las aristas del grafo G se preserven en el grafo G'. Es decir,
asígnamos $f(a) = x, f(b) = y, f(c) = z, f(d) = u$, para verificar si se preservan f en E' hacemos lo siguiente:

$a, b \in V$, tenemos $\{a, b\} \in E \Longleftrightarrow \{x, y\} \in E'$, donde $\{x, y\}$ representa la arista e'_1.
$b, c \in V$, tenemos $\{b, c\} \in E \Longleftrightarrow \{y, z\} \in E'$, donde $\{y, z\}$ representa la arista e'_2.
$c, d \in V$, tenemos $\{c, d\} \in E \Longleftrightarrow \{z, u\} \in E'$, donde $\{z, u\}$ representa la arista e'_3.
$d, a \in V$, tenemos $\{d, a\} \in E \Longleftrightarrow \{u, x\} \in E'$, donde $\{u, x\}$ representa la arista e'_4.

Observan que las aristas del grafo G se preservan en el grafo G', así los grafos G y G' (ver figura 2.1) son isomorfos.

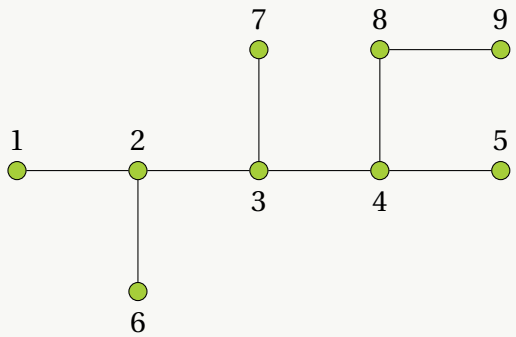
■

Definición 2.6 (Árbol)
Un **árbol** es un grafo conexo, que no contiene ningún ciclo.

Ejemplo **2.7**

El grafo con vértices V y aristas E es un árbol.

$$V := \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$
$$E := \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{2, 6\}, \{3, 7\}, \{4, 8\}, \{8, 9\}\}$$



Análisis:

La forma usual de trazar el grafo es dibujando los puntos por cada vértice y unir dos de estos puntos con una línea (si estos vértices son correspondientes forman una arista). Analicemos que este grafo, en efecto es un árbol;

Notemos que el grafo dado es conexo, ya que los vértices $\{1,2,3,4,5,6,7,8,9\}$ respectivos comparten su arista correspondiente para formar por lo menos un camino, es decir, observemos el vértice 1 simplemente este no puede ser vecino del vértice 9 pero puede hacerlo a través de un camino:

$$1 \to 2 \to 3 \to 4 \to 8 \to 9$$

Además, de este grafo no podemos formar un camino del cual podamos empezar y terminar en el mismo vértice, es decir, si consideramos el vértice origen 1 y el vértice final 9 observamos que no existe un camino donde el vértice de origen y el vértice final sean el mismo por lo que el grafo no produce ningún ciclo. Así, el grafo en efecto es un árbol.

■

Definición 2.7 (Bosque)

Un bosque es un grafo que no contiene ningún ciclo (puede o no ser conexo). Si tenemos un bosque no conexo, entonces se sigue que sus componentes conexas son árboles.

Nota:

Un árbol es lo mismo que un bosque conexo.

Ejemplo **2.8**

El presente grafo G es un bosque:

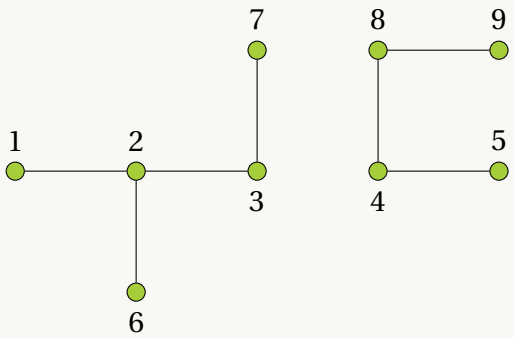


Figura 2.2. Grafos G' (izquierda) y G'' (derecha)

Análisis:
Sea el grafo G definido por:
G' (izquierda): $V := \{1,2,3,6,7\}$, $E := \{\{1,2\},\{2,3\},\{2,6\},\{3,7\}\}$; y G'' (derecha): $V := \{4,5,8,9\}$, $E := \{\{4,5\},\{4,8\},\{8,9\}\}$.

Observemos que el grafo G' es conexo, ya que los vértices $\{1,2,3,6,7\}$ comparten su arista correspondiente para formar por lo menos un camino, es decir, si tomamos el vértice 1; este no es vecino del vértice 7 pero podemos hacer que sean vecinos a través de un camino:

$$1 \to 2 \to 3 \to 7$$

Luego, si consideramos el vértice origen 1 y el vértice final 7 observamos que no existe un camino donde el vértice de origen y el vértice final sean el mismo por lo que el grafo no produce ningún ciclo. De manera análoga se realiza el caso para el grafo G''; como resultado ambos grafos G' y G'' son árboles.

Ahora, el grafo G en general no es conexo, dicho de otra manera; si tomamos el vértice 3 no puede ser vecino del vértice 4 debido a que no existe un camino entre estos vértices que los una por lo que el grafo en general no es conexo. Además, se tiene el grafo en general esta formado por subgrafos que son árboles por lo cual se considera que es un bosque ya que si el grafo G no es conexo entonces esta formado por componentes conexas que son árboles, también estos árboles no contienen ningún ciclo por lo que el grafo G tampoco posee ciclo.
Así, G es un bosque.

■

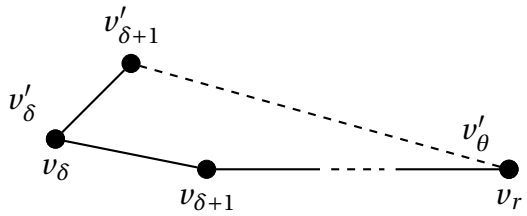
Proposición 2.1 (Caracterización de árboles)
Un grafo es un árbol si y solo si para cada par de vértices existe exactamente un camino que conecta estos vértices.

Demostración. "$\Longrightarrow$" Un grafo es un árbol entonces para cada par de vértices existe exactamente un camino que conecta estos vértices.

Sea G un árbol, por definición 2.6 G es conexo, entonces existe por lo menos un camino que conecta a este par de vértices de G. Ahora bien, verifiquemos que este camino es único, supongamos v y v' dos vértices cualesquiera de G unidos por al menos dos caminos distintos:

$$P : v = v_0, v_1, \ldots, v_{n-1} = v'$$
$$P' : v = v'_0, v'_1, \ldots, v'_{k-1} = v'$$

Sea $\delta = \text{mín}\left\{ \; i \;\middle|\; v_i \neq v'_i \; \right\} - 1$.
Ahora, sea $r = \text{mín}\left\{ \; t \;\middle|\; t > \delta \text{ y } \exists\theta : v_t = v'_\theta \; \right\} \neq \emptyset$, entonces $v_r = v'_\theta$, así tenemos:



Consideramos el camino: $v_\delta = v'_\delta, v'_{\delta+1}, \ldots, v'_\theta = v_r, v_{r-1}, \ldots, v_{\delta+1}$ pero $\{v_{\delta+1}, v_\delta\} \in E$, así el camino que recorre $v_\delta = v'_\delta, v'_{\delta+1}, \ldots, v'_\theta = v_r, v_{r-1}, \ldots, v_{\delta+1}, v_\delta$ genera un ciclo en G. Esto nos lleva a una contradicción de que G es un árbol.

"$\Longleftarrow$" Para cada par de vértices existe exactamente un camino que conecta estos vértices entonces el grafo dado es un árbol.

Sea G un grafo tal que para cada par de vértices puede estar conectado por exactamente un camino en G lo cual implica que G es conexo. Supongamos que G contiene un ciclo $v_0, v_1, \ldots, v_{n-1}$, esto implica que existen al menos tres vértices en G, es decir, $n > 2$. Como $v_0, \ldots, v_{n-1}$ es un ciclo, entonces $\{v_0, v_{n-1}\}$ es arista, así v_0, v_{n-1} es un camino que conecta v_0 con v_{n-1} distinto del camino $v_0, v_1, \ldots, v_{n-1}$ y esto contradice la hipótesis.

Así, un grafo es un árbol si y solo si para cada par de vértices existe exactamente un camino que conecta estos vértices.

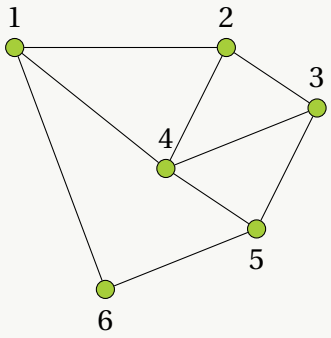
□

Al crear el árbol es muy importante que no existan ciclos, además debe existir un camino entre cada par de vértices. Un grafo puede tener muchos árboles de expansión:

Definición 2.8 (Árbol de expansión)
Un **árbol de expansión** de un grafo X es un subgrafo de X que es un árbol y contiene todos los vértices de X.

Ejemplo **2.9**

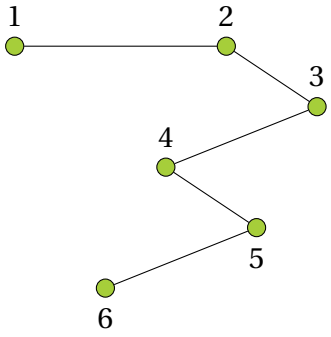
Dado el siguiente grafo G:



Este grafo tiene un árbol de expansión.

Análisis:

El grafo dado esta compuesto por los vértices $V := \{1,2,3,4,5,6\}$ conectados con sus aristas $E := \{\{1,2\},\{2,3\},\{3,4\},\{4,5\},\{5,6\},\{1,4\},\{1,6\},\{2,4\},\{3,5\}\}$. Entonces para que sea un árbol de expansión tomamos un subgrafo del grafo G sin ciclos ya que por definición 2.8 este subgrafo debe ser un árbol y debe contener todos los vértices del grafo G. Así, el subgrafo de G que representaría un árbol de expansión es:



Con vértices y aristas conectadas a estos vértices:

$$V := \{1,2,3,4,5,6\} \text{ y } E := \{\{1,2\},\{2,3\},\{3,4\},\{4,5\},\{5,6\}\}$$

■

Dado un conjunto generador de un grupo, podemos organizar la estructura combinatoria dada por el grupo generador como un grafo:

Definición 2.9 (Grafos de Cayley)

Sea G un grupo y sea $S \subset G$ un conjunto generador de G. Entonces el **grafo de Cayley** de G con respecto al conjunto generador S es el grafo $\mathrm{Cay}(G,S)$ cuyo

- Conjunto de vértices es G, y cuyo
- Conjunto de aristas es: $\left\{ \{g, g*s\} \;\middle|\; g \in G, s \in \left(S \cup S^{-1}\right) \setminus \{e\} \right\}$

Es decir, dos vértices en un grafo de Cayley son adyacentes si y solo si difieren en la multiplicación derecha por un (inverso de un) elemento del conjunto generador en cuestión. Por definición, el grafo de Cayley con respecto a un conjunto generador S coincide con los grafos de Cayley para S^{-1} y $S \cup S^{-1}$.

Ejemplo **2.10**

Los grafos de Cayley del grupo aditivo $\mathbb{Z}$ con respecto a los conjuntos de generadores $\{1\}$ y $\{2,3\}$, respectivamente, se muestran las siguientes figuras en el análisis. Al mirar estos dos gráficos "desde lejos", parecen tener la misma estructura global, es decir, parecen la línea real.

Análisis:

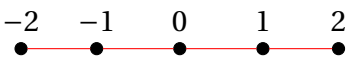
Por definición 2.9 tenemos que $\mathrm{Cay}(\mathbb{Z},\{1\})$ y $\mathrm{Cay}(\mathbb{Z},\{2,3\})$ son grafos de Cayley donde $\mathbb{Z}$ es el conjunto de vértices y las aristas son las siguientes:

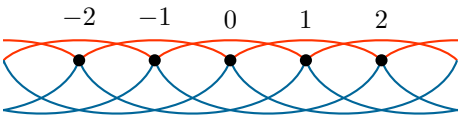
Caso 1: Para $S = \{1\}$.

$$\{0, 0+1\} = \{0,1\}$$
$$\{1, 1+1\} = \{1,2\}$$
$$\{2, 2+1\} = \{2,3\}$$
$$\{1, 1+(-1)\} = \{1,0\}$$
$$\{2, 2+(-1)\} = \{2,1\}$$

Caso 2: Para $S = \{2,3\}$.

$$\{0, 0+2\} = \{0,2\} \qquad \{0, 0+3\} = \{0,3\}$$
$$\{1, 1+2\} = \{1,3\} \qquad \{1, 1+3\} = \{1,4\}$$
$$\{2, 2+2\} = \{2,3\} \qquad \{2, 2+3\} = \{2,5\}$$
$$\{1, 1+(-2)\} = \{1,-1\} \qquad \{1, 1+(-3)\} = \{1,-2\}$$
$$\{2, 2+(-2)\} = \{2,0\} \qquad \{2, 2+(-3)\} = \{2,-1\}$$

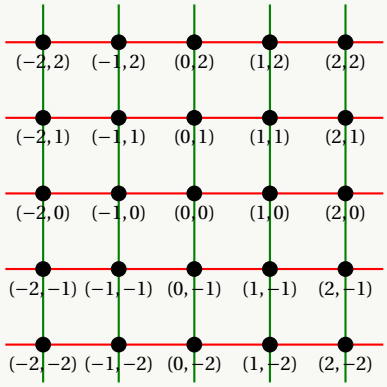




■

Ejemplo 2.11

El grafo Cayley del grupo aditivo $\mathbb{Z}^2$ con respecto al conjunto generador $\{(1,0),(0,1)\}$ se parece al entramado de enteros en $\mathbb{R}^2$.



.

Figura 2.3. Grafo de Cayley de $\mathbb{Z}^2$

Ejemplo 2.12

El grafo Cayley del grupo cíclico $\mathbb{Z}/6$ con respecto al conjunto generador $\{[1]\}$.

Análisis:

Por definición 2.9 tenemos que el conjunto de vértices es el grupo de los enteros módulo 6, es decir:

$$\mathbb{Z}/6 = \{[0],[1],[2],[3],[4],[5]\}$$

Y las aristas están dadas de la siguiente manera:

Caso 1: Para $S = [1]$.

$$\{[0],[0]+[1]\} = \{[0],[1]\}$$
$$\{[1],[1]+[1]\} = \{[1],[2]\}$$
$$\{[2],[2]+[1]\} = \{[2],[3]\}$$
$$\{[3],[3]+[1]\} = \{[3],[4]\}$$
$$\{[4],[4]+[1]\} = \{[4],[5]\}$$
$$\{[5],[5]+[1]\} = \{[5],[0]\}$$

Caso 2: Para $S = [-1]$.

$$\{[1],[1]+[-1]\} = \{[1],[0]\}$$
$$\{[2],[2]+[-1]\} = \{[2],[1]\}$$
$$\{[3],[3]+[-1]\} = \{[3],[2]\}$$
$$\{[4],[4]+[-1]\} = \{[4],[3]\}$$
$$\{[5],[5]+[-1]\} = \{[5],[4]\}$$

Teniendo los vértices y las aristas respectivas, se forma el siguiente grafo:

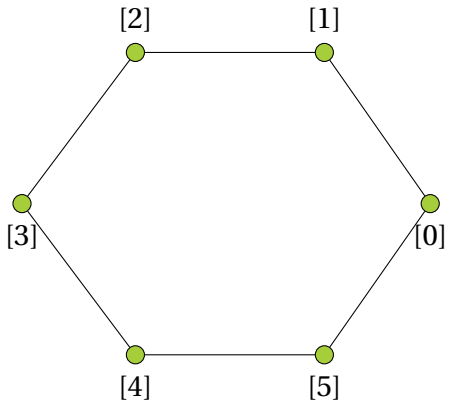


Figura 2.4. Grafo de cayley en forma de hexágono regular

■

2.2. Grafos de Cayley de grupos libres

Puede resultar intuitivo que los conjuntos generadores libres no conducen a ningún ciclo en los correspondientes grafos de Cayley y viceversa pero enunciaremos este resultado de manera formal y una prueba formal de ello requiere la descripción de los grupos libres en términos de palabras reducidas. En general, cualquier descripción explícita y completa del grafo de Cayley de un grupo G con respecto a un conjunto generador S requiere esencialmente resolver el problema de palabras de G con respecto a S.

La construcción $F(S)$ de grupo libre generado por S consiste en tomar el conjunto de todas las palabras de los elementos de S y sus inversos formales, y tomar el cociente por la relación de cancelación (prueba del teorema 1.2). Aunque esta construcción es técnicamente limpia y sencilla, tiene el inconveniente de que conseguir la naturaleza precisa de dicha relación de equivalencia es tedioso. A continuación, discutimos una construcción alternativa de un grupo libremente generado por S mediante palabras reducidas; es técnicamente un poco más engorroso, pero tiene la ventaja de que cada elemento del grupo está representado por una palabra canónica:

Definición 2.10 (Palabra reducida)

Sea S un conjunto, y sea $\left(S\cup\widehat{S}\right)^*$ un conjunto de palabras sobre S y los inversos formales de los elementos de S.

- Sea $n\in\mathbb{N}$ y sea $s_1\cdots s_n\in\left(S\cup\widehat{S}\right)^*$. La palabra $s_1\cdots s_n$ es reducida si,

$$\widehat{s_{j+1}}\neq s_j \text{ y } s_{j+1}\neq\widehat{s_j}$$

sostiene que para todo $j\subset\{1,\ldots,n-1\}$. Por tanto para toda palabra reducida $s_1\cdots s_n$, tenemos que $s_1\cdots s_n\nsim\epsilon$ (en $F(S)$ significa $s_1\cdots s_n\neq\epsilon$). Por convenio vamos a suponer que ϵ será una palabra reducida.

- Escribimos $F_{red}(S)$ por el **conjunto de palabras reducidas** sobre $\left(S\cup\widehat{S}\right)^*$.

Nota:

La operación de grupo que tendrá F_{red} es la siguiente: red$\circ$concatenación$|_{F_{red}}$, que primero concatena dos palabras reducidas y luego reduce la palabra concatenada.

Ejemplo **2.13**

Para $S=\{a\}$, el conjunto de palabras reducidas estará dado por:

$$F_{red}(S)=\{\epsilon,\ a,\ aa,\ aaa,\ \ldots,\ \widehat{a},\ \widehat{a}\widehat{a},\ \widehat{a}\widehat{a}\widehat{a},\ldots\}$$

el cual es un grupo con la operación que concatena y luego reduce la palabra.

Lema 2.1

Sea G un grupo y S un conjunto generador $S\subset G$. Si el grafo $\mathrm{Cay}(G,S)$ contiene un camino $g_0,\ldots,g_n$, entonces $g_0^{-1}g_n\in F_{red}(S)-\{\epsilon\}$.

Demostración. Tenemos por hipótesis que el grafo contiene un ciclo, $g_0,\ g_1,\ldots,g_n$, definámoslo de la siguiente manera;

$$g_0,\ g_1:=g_0s_1,\ldots,g_n:=g_0s_1s_2\cdots s_n$$

vamos a probar que $s_1\cdots s_n$ es reducida. Por contradicción, supongamos que $s_1\cdots s_n$ no es reducida.

Si $s_1\cdots s_n$ no es reducida, entonces,

$$\exists j \text{ tal que } s_j=\widehat{s_{j+1}} \text{ ó } \widehat{s_j}=s_{j+1}$$

En este caso $S \subset G$ tiene el producto del grupo G, así $s_j = s_{j+1}^{-1}$ o $s_j^{-1} = s_{j+1}$. Ahora, tomemos tres elementos consecutivos distintos del camino, es decir, tres vértices; $g_{j-1},\ g_j,\ g_{j+1}$. Luego, por como tenemos definidos los vértices, tendremos que;

$$\begin{aligned} g_j = g_{j-1} \cdot s_j &\Longrightarrow g_{j+1} = g_j \cdot s_{j+1} \\ &\Longrightarrow g_{j+1} = g_{j-1} \cdot s_j \cdot s_{j+1} \\ &\Longrightarrow g_{j+1} = g_{j-1} e = g_{j-1} \quad ; \text{ como tenemos que } s_j = {s_{j+1}}^{-1} \text{ ó } {s_j}^{-1} = s_{j+1} \end{aligned}$$

pero esto es una contradicción ya que teníamos que $g_{j-1},\ g_j,\ g_{j+1}$ son distintos, así, $s_1 \cdots s_n$ es reducida. □

Proposición 2.2 (Grupos libres a través de palabras reducidas)

Sea S un conjunto.

1. El conjunto $F_{red}(S)$ de palabras reducidas sobre $S \cup \widehat{S}$ forma un grupo con respecto a la composición $*_{red} = \text{red} \circ \text{concatenación}|_{red} = F_{red}(S) \times F_{red}(S) \longrightarrow F_{red}(S)$ dada por

$$(s_1 \cdots s_n, s_{n+1} \cdots s_m) \longmapsto (s_1 \cdots s_{n-r} s_{n+1+r} \cdots s_{n+m}),$$

donde $s_1 \cdots s_n$ y $s_{n+1} \cdots s_m$ están en $F_{red}(S)$ (con $s_1, \ldots, s_m \in S \cup \widehat{S}$), y

$$r := \max\left\{k \in \{0, \ldots, \min(n, m-1)\} \mid \forall\, j \in \{0, \ldots, k-1\},\ s_{n-j} = \widehat{s_{n+1+j}} \vee \widehat{s_{n-j}} = s_{n+1+j}\right\}$$

En otras palabras, la composición de las palabras reducidas se da concatenando primero las palabras y luego reduciendo al máximo en la concatenación posición.

2. El grupo $F_{red}(S)$ es generado libremente por S.

Demostración. Primero se demostrará que el conjunto $F_{red}(S)$ de palabras reducidas sobre $S \cup \widehat{S}$ forma un grupo con respecto a la composición y por último se probará que tal grupo es generado libremente por S.

1. Como sabemos un grupo es una estructura algebraica que consta de un conjunto con una operación binaria, tal operación combina parejas de elementos para formar un tercer elemento.

Sin embargo, para garantizar que es un grupo se deben verificar los axiomas de grupo: Asociatividad, existencia del elemento inverso y tener un elemento neutro.

Primero verifiquemos que la composición está bien definida.

Tenemos $F_{red}(S) \times F_{red}(S) \longrightarrow F_{red}(S)$ dada por

$$(s_1 \cdots s_n, s_{n+1} \cdots s_m) \longmapsto (s_1 \cdots s_{n-r} s_{n+1+r} \cdots s_{n+m}),$$

como sabemos $s_1 \cdots s_n, s_{n+1} \cdots s_m \in F_{red}(S)$.

Ahora, si $(s_1 \cdots s_n, s_{n+1} \cdots s_m), \left(t_1 \cdots t_p, t_{p+1} \cdots t_k\right) \in F_{red}(S) \times F_{red}(S)$ tal que

$$(s_1 \cdots s_n, s_{n+1} \cdots s_m) = \left(t_1 \cdots t_p, t_{p+1} \cdots t_k\right),$$

entonces,

$$s_1 \cdots s_n = t_1 \cdots t_p \text{ y } s_{n+1} \cdots s_m = t_{p+1} \cdots t_k$$

Por lo que, $n = p$, $s_i = t_i$, $m = k$ y $s_{n+j} = t_{p+j}$ (puesto que son palabras iguales). Ahora, sea

$$r := \text{máx}\left\{i \in \{0, \ldots, \text{mín}(n, m-1)\} \mid \forall\, j \in \{0, \ldots, i-1\} \ , s_{n-j} = \widehat{s_{n+1+j}} \vee \widehat{s_{n-j}} = s_{n+1+j}\right\},$$

luego

$$(s_1 \cdots s_{n-r} s_{n+1+r} \cdots s_{n+m}) = \left(t_1 \cdots t_{p-r} t_{p+1+r} \cdots t_{p+k}\right),$$

por lo tanto, está bien definido.

Elemento neutro.

Si componemos dos palabras reducidas, la palabra compuesta se reduce. Además, la concatenación tiene la palabra vacía como elemento neutro. Por lo tanto, si se concatena una palabra reducida con la palabra vacía da como resultado la palabra reducida, así que la palabra vacía es el elemento neutro. Es decir,

$$(s_1 \cdots s_n, \epsilon) = s_1 \cdots s_n$$

Por lo tanto, el elemento neutro es la palabra vacía ϵ

Elemento inverso.

No es difícil demostrar que toda palabra reducida admite un inverso con respecto a esta composición.

Tomando la palabra $(s_1 \cdots s_n) \in F_{red}(S)$. Al invertirla tenemos la palabra $(\widehat{s_n} \cdots \widehat{s_1})$ donde $\widehat{\widehat{s}} = s$ si $s \in S$ y esta palabra también sería reducida.

Por lo que, toda palabra reducida admite un inverso.

Asociatividad.

Ahora solo resta probar que esta composición es asociativa. Este es el caso más tedioso, sin embargo, en lugar de dar una demostración que involucre muchos índices explicaremos el argumento gráficamente.

Sean $x, y, z \in F_{red}(S)$.

Queremos mostrar que $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

Por definición sabemos que al componer dos palabras reducidas, tenemos que eliminar el área de reducción máxima donde se encuentran las dos palabras.

Nótese:

i) Si las áreas de reducción de x, y y y, z no tienen intersección en y, entonces claramente:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

Como se muestra en la siguiente figura.

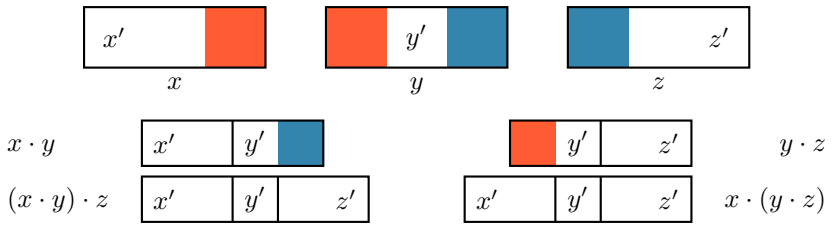


Figura 2.5. Si las áreas de reducción de los elementos exteriores no interfieren.

ii) Si las áreas de reducción de x, y y y, z tienen una intersección no trivial y'' en y, entonces la igualdad

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

Se sigue al inspeccionar las áreas de reducción en x y z y las regiones vecinas, como se indica en la figura 2.6, debido a la superposición en y'', sabemos que x'' y z'' coinciden (ambos son el inverso de y'').

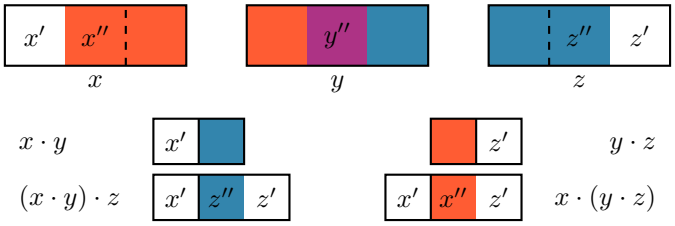


Figura 2.6. Si las áreas de los elementos exteriores interfieren.

2. Ahora veremos si S es un conjunto generador libre de $F_{red}(S)$, lo haremos verificando la propiedad universal:

   Sea H un grupo y sea $\varphi : S \longrightarrow H$ un mapeo.

   Por cálculo directo se muestra que $\overline{\varphi} := \varphi^*|_{F_{red}(S)} : F_{red}(S) \longrightarrow H$ es un homomorfismo de grupo. Veamos:

   Sea $\overline{\varphi} := \varphi^*|_{F_{red}(S)} : F_{red}(S) \longrightarrow H$ definida como

   $$\overline{\varphi}(s_1 s_2 \cdots s_n) = \varphi(s_1)\varphi(s_2)\cdots\varphi(s_n).$$

   - Probemos que $\overline{\varphi}$ está bien definida.
     Sean $(s_1 s_2 \cdots s_n), \left(s_1' \cdots s_n'\right) \in F_{red}(S)$ tal que $s_1 s_2 \cdots s_n = s_1' s_2' \cdots s_n'$.
     Si $s_1 s_2 \cdots s_n = s_1' s_2' \cdots s_n'$, entonces

     $$\begin{aligned} s_1 = s_1', \ldots, s_n = s_n' & \\ \varphi(s_1) = \varphi\left(s_1'\right), \ldots, \varphi(s_n) = \varphi\left(s_n'\right) & \quad \text{; ya que } \varphi \text{ es mapeo} \\ \varphi(s_1)\cdots\varphi(s_n) = \varphi\left(s_1'\right)\cdots\varphi\left(s_n'\right) & \\ \overline{\varphi}(s_1 \cdots s_n) = \overline{\varphi}\left(s_1' \cdots s_n'\right). & \end{aligned}$$

     Por lo tanto, $\overline{\varphi}$ está bien definida.

   - Ahora probemos que $\overline{\varphi}$ es homomorfismo.
     Sean $s_1 s_2 \cdots s_n, s_{n+1} \cdots s_m \in F_{red}(S)$.

     $$\begin{aligned} \overline{\varphi}((s_1 s_2 \cdots s_n)\cdot(s_{n+1}\cdots s_m)) &= \overline{\varphi}(s_1 \cdots s_{n-r} s_{n+1+r} \cdots s_{n+m}) \\ &= \varphi(s_1)\cdots\varphi(s_{n-r})\varphi(s_{n+1+r})\cdots\varphi(s_{n+m}) \\ &= \left(\varphi(s_1)\cdots\varphi(s_n)\right)\cdot\left(\varphi(s_{n+1})\cdots\varphi(s_m)\right); \text{ se agregan los} \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{elementos superfluos} \\ &= \overline{\varphi}(s_1 \cdots s_n)\cdot\overline{\varphi}(s_{n+1}\cdots s_m) \end{aligned}$$

     Por lo tanto, $\overline{\varphi}$ es homomorfismo.

Claramente $\overline{\varphi}|_S = \varphi$. Además S genera $F_{red}(S)$, así, se deduce que $\overline{\varphi}$ es el único homomorfismo de este tipo.

Por lo tanto, $F_{red}(S)$ es generado libremente por S.

□

Resulta de particular interés la segunda parte de la demostración anterior, por ello como corolario a la segunda parte de la prueba anterior tenemos:

Corolario 2.1 (Forma Normal para grupos libres)
Sea S un conjunto. Cada elemento del grupo libre $F(S) = \left(S \cup \widehat{S}\right)^* / \sim$ se puede representar exactamente con una palabra reducida sobre $S \cup \widehat{S}$.

Demostración. Sean $F(S)$ un grupo libre y $i : S \longrightarrow F(S)$ el mapeo inclusión.

Ahora bien, como $F_{red}(S)$ es generado libremente por S, existe un único homomorfismo

$$\overline{i} : F_{red}(S) \longrightarrow F(S)$$

el cual está dado por

$$s_1 \cdots s_n \longmapsto s_1 \cdots s_n$$

Además, dado que S genera libremente a $F_{red}(S)$, eso significa que

$$F(S) \cong F_{red}(S)$$

Entonces existe un isomorfismo entre $F_{red}(S)$ y $F(S)$, el cual es

$$\theta : F_{red}(S) \longrightarrow F(S)$$

dado por

$$s_1 \cdots s_n \longmapsto s_1 \cdots s_n$$

Ahora, sea $y \in F(S)$. Como $\theta : F_{red}(S) \longrightarrow F(S)$ es isomorfismo, es sobreyectiva, por lo que existe $x \in F_{red}(S)$ tal que $\theta(x) = y$.

Como $x \in F_{red}(S)$ se debe cumplir que

$$\begin{aligned} x = s_1 \cdots s_n &\Longrightarrow \theta(x) = \theta(s_1 \cdots s_n) \\ &\Longrightarrow \quad y = \theta(s_1 \cdots s_n) \\ &\Longrightarrow \quad y = s_1 \cdots s_n \end{aligned}$$

Es decir, cualquier elemento del grupo libre $F(S)$ se puede representar por una palabra reducida. Con lo que se concluye la demostración. □

Una caracterización combinatoria de grupos libres puede ser dada en términos de árboles:

Teorema 2.1 (Grafos de Cayley de grupos libres)
Sea F un grupo libre, libremente generado por $S \subset F$. Entonces el correspondiente grafo de Cayley $\mathrm{Cay}(F,S)$ es un árbol.

Demostración. Tenemos por hipótesis que;

$$F \text{ es libremente generado por } S \ldots (*)$$

Además, por la proposición 2.2-ítem 2, tenemos que;

$$F_{red}(S) \text{ es libremente generado por } S \ldots (**)$$

por $(*)$ y $(**)$, dos grupos son libremente generados por S, entonces podemos decir que;

$$F \cong F_{red}(S)$$

mediante isomorfismo canónico, ya que la proposición 1.3 nos garantiza la unicidad del grupo que es generado libremente por S. Ahora sí, vamos a probar que $\mathrm{Cay}(F,S)$, es un árbol, para ello demostraremos que $\mathrm{Cay}(F,S)$ es un grafo conexo que no contiene ningún ciclo (según la definición 2.6).

- Primero probaremos que $\mathrm{Cay}(F,S)$ es un grafo conexo.

  Debemos probar que cada par de vértices de F puede ser conectado por un camino en $\mathrm{Cay}(F,S)$. Sea $x,\ y \in F_{red}(S)$ arbitrarios, donde $x = s_1 \cdots s_n,\ y = t_1 \cdots t_m$.

  Tenemos por definición de grafo de Cayley que las aristas son de la forma:

  $$\{x,\ x\widehat{s}\} = \{s_1 \cdots s_n,\ s_1 \cdots s_n \widehat{s_n}\} = \{s_1 \cdots s_n,\ s_1 \cdots s_{n-1}\}$$

  como notamos, $x,\ x\widehat{s}$ son elementos consecutivos, entonces podemos formar un camino;

  $$x,\ x\widehat{s_n},\ x\widehat{s_n}\widehat{s_{n-1}}, \ldots,\ xx^{-1} = \epsilon,\ \epsilon t_1,\ t_1 t_2, \ldots, t_1 \cdots t_m = y$$

  entonces tenemos un camino que conecta x a y, así el grafo es conexo.

- Segundo, probaremos que $\mathrm{Cay}(F,S)$ no contiene ningún ciclo.

  Por contradicción. Supongamos que $\mathrm{Cay}(F,S)$ es un grafo conexo que contiene un ciclo.

  Sea $g_0,\ldots,g_n$ un ciclo, así $g_n = g_0$, luego $g_0^{-1}g_n = \epsilon$ pero esto es absurdo porque el lema 2.1 afirma que $g_0^{-1}g_n \in F_{red}(S) - \{\epsilon\}$.

□

El inverso de este teorema no es cierto en general;

Ejemplo 2.14

El grafo de Cayley $\mathrm{Cay}(\mathbb{Z}/2,\{[1]\})$, consiste en dos vértices unidos por una arista; claramente, este grafo es un árbol, pero el grupo $\mathbb{Z}/2$ no es libre.

Análisis:

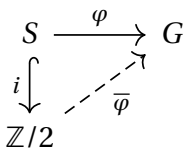
Por definición 2.9 el grafo de Cayley de $\mathbb{Z}/2$ con respecto al conjunto generador $[1]$ es el grafo $\mathrm{Cay}(\mathbb{Z}/2,[1])$ cuyo conjunto de vértices es $\mathbb{Z}/2 = \{[0],[1]\}$ y cuyo conjunto de aristas es

$$\{[0],[0]+[1]\} = \{[0],[1]\} \qquad \{[1],[1]+[1]\} = \{[0],[2]\}$$
$$\{[0],[0]+[-1]\} = \{[0],[-1]\} \qquad \{[1],[1]+[-1]\} = \{[1],[0]\}$$

En efecto $\mathrm{Cay}(\mathbb{Z}/2,[1])$ es un árbol, ya que no contiene ningún ciclo, es decir, no cumple que para los vértices $\{[0],[1]\}$ exista un camino cerrado ya que es una linea.

Ahora verifiquemos que el grupo $\mathbb{Z}/2$ no es libre. Por contradicción, supongamos que $\mathbb{Z}/2$ es libre, entonces contiene un conjunto generador libre.

Sea S subconjunto generador libre (arbitrario) de $\mathbb{Z}/2$, entonces $\mathbb{Z}/2$ es un grupo libremente generado por S, por la propiedad universal tenemos que para todo grupo G y para todo $\varphi : S \longrightarrow G$, existe un único homomorfismo $\overline{\varphi} : \mathbb{Z}/2 \longrightarrow G$ tal que $\overline{\varphi} \circ i = \varphi$:



Como es para todo G y para todo φ supongamos que $G = \mathbb{Z}$ y definamos φ de la siguiente manera;

$$\begin{aligned} \varphi : S &\longrightarrow \mathbb{Z} \\ s &\longmapsto \varphi(s) = 1 \end{aligned}$$

existe el homomorfismo:

$$\begin{aligned} \overline{\varphi} : \mathbb{Z}/2 &\longrightarrow \mathbb{Z} \\ [0] &\longmapsto \overline{\varphi}([0]) = 0 \\ [1] &\longmapsto \overline{\varphi}([1]) = 0 \end{aligned}$$

cumple que:

$$\left(\overline{\varphi} \circ i\right)(s) = \varphi(s) \Longrightarrow \overline{\varphi}(s) = \varphi(s) \tag{2.1}$$

Para $[0] \in \mathbb{Z}/2$:

$$\begin{aligned} \overline{\varphi}([0]) = 0 \Longrightarrow \overline{\varphi}(2s) = 0 \quad & ; \text{ya que en } \mathbb{Z}/2 : [0] = [2s] \\ \overline{\varphi}(s+s) = 0 \quad & \\ \overline{\varphi}(s) + \overline{\varphi}(s) = 0 \quad & ; \overline{\varphi} \text{ es homomorfismo} \\ \varphi(s) + \varphi(s) = 0 \quad & ; \text{por la ecuación 2.1} \\ 1 + 1 = 0 \quad & \\ 2 = 0 \quad & (\rightarrow\leftarrow) \end{aligned}$$

por tanto no es cierto que $\mathbb{Z}/2$ contiene un conjunto generador libre.

■

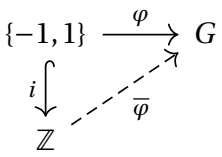
Hay que aclarar que en cualquier grafo de Cayley $\mathrm{Cay}(G, S)$, S no necesariamente es el subconjunto libre de G, es decir, G puede ser libre pero S no lo genera libremente, sino, otro subconjunto de G diferente de S, como se ilustra en el siguiente ejemplo:

Ejemplo 2.15

El grafo de Cayley $\mathrm{Cay}(\mathbb{Z}, \{-1, 1\})$ coincide con $\mathrm{Cay}(\mathbb{Z}, \{1\})$, que es un árbol (que parece una línea). Pero $\{-1, 1\}$ no es un conjunto generador libre de $\mathbb{Z}$ (a pesar que $\mathbb{Z}$ es libre).

Análisis:

Vamos a demostrar que el conjunto $\{-1,1\}$, no necesariamente genera a $\mathbb{Z}$. Supongamos por contradicción que $\{-1,1\}$ genera a $\mathbb{Z}$, es decir, se cumple la propiedad universal; para todo G, y para todo φ, existe un único homomorfismo, tal que $\overline{\varphi}\,|_{\{-1,1\}} = \varphi$



Como es para todo G, definimos para $G = \mathbb{Z}$

$$\begin{aligned} \varphi : \{-1,1\} &\longrightarrow \mathbb{Z} \\ -1 &\longmapsto \overline{\varphi}(-1) = 1 \\ 1 &\longmapsto \overline{\varphi}(1) = 0 \end{aligned}$$

y sea

$$\begin{aligned} \overline{\varphi} : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ n &\longmapsto n\varphi(1) \end{aligned}$$

tal que $\left(\overline{\varphi} \circ i\right)(-1) = \varphi(-1)$.

$$\begin{aligned} \left(\overline{\varphi} \circ i\right)(-1) = \varphi(-1) &\Longrightarrow \overline{\varphi}(i(-1)) = \varphi(-1) \\ &\Longrightarrow \overline{\varphi}(-1) = \varphi(-1) \\ &\Longrightarrow -1\varphi(1) = 1 \\ &\Longrightarrow -1\varphi(1) = 1 \\ &\Longrightarrow -1(1) = 1 \\ &\Longrightarrow -1 = 1 \quad (\rightarrow\leftarrow) \end{aligned}$$

llegamos a una contradicción, por tanto, $\{-1,1\}$, no genera a $\mathbb{Z}$.

■

Teorema 2.2 (Arboles de Cayley y grupos libres)

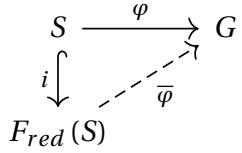
Sea G un grupo, sea $S \subset G$ conjunto generador que satisface $s \cdot t \neq e$ para todo $s, t \in S$. Si el grafo de Cayley $\mathrm{Cay}(G,S)$ es un árbol, entonces S es un conjunto generador libre de G.

Demostración. Tenemos por hipótesis que el grafo de Cayley es un árbol, es decir, es un grafo conexo que no contiene ningún ciclo, debemos probar que S genera libremente a G, probando que se cumple la propiedad universal.

La proposición 2.2-ítem 2 nos dice que $F_{red}(S)$ es libremente generado por S, si demostramos que $G \cong F_{red}(S)$, nos ayudará a demostrar la propiedad universal para G.

Ahora bien, teníamos que $F_{red}(S)$ es libremente generado por S, por la propiedad universal, enunciada en el definición 1.11 decimos que para todo G y para todo $\varphi : S \longrightarrow G$, existe un único homomorfismo de grupo;

$$\overline{\varphi} : F_{red}(S) \longrightarrow G$$



demostraremos que $\overline{\varphi}$ es un isomorfismo tal que $\overline{\varphi}|_S$ es la identidad, y así podemos concluir la prueba. Definamos

$$\begin{aligned} \varphi : S &\longrightarrow G \\ s &\longmapsto s \end{aligned}$$

para el homomorfismo $\overline{\varphi}$ se cumple que $\overline{\varphi} \circ i = \varphi$, así

$$\begin{aligned} \left(\overline{\varphi} \circ i\right)(s) &= \varphi(s) \\ \overline{\varphi}(i(s)) &= s \\ \overline{\varphi}|_S &= id_S(s) \end{aligned}$$

demostremos que $\overline{\varphi}$ es un isomorfismo:

- **Sobreyectividad**. Probaremos que para $g \in G$, existe $x \in F_{red}(S)$, tal que $\overline{\varphi}(x) = g$. Sea $g \in G$, donde $g = s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}$.

  Sea $x = s_{n_1}^{\epsilon_{n_1}} \cdots s_{n_r}^{\epsilon_{n_r}}$ la palabra que resulta al eliminar los elementos superfluos de $s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}$, es decir, al reducir $s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}$, aquí $s_i^{\epsilon_i} = \begin{cases} s_i, & \epsilon_i = 1 \\ \widehat{s}_i, & \epsilon_i = -1 \end{cases}$, y $\widehat{\widehat{s}} = s$, $\forall s \in S$;

  $$\begin{aligned} \overline{\varphi}(x) &= \overline{\varphi}\left(s_{n_1}^{\epsilon_{n_1}} \cdots s_{n_r}^{\epsilon_{n_r}}\right) \\ &= s_{n_1}^{\epsilon_{n_1}} \cdots s_{n_r}^{\epsilon_{n_r}} && \text{; ya que } \overline{\varphi} \text{ es la identidad en } S \\ &= s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} && \text{; agregamos los elementos superfluos} \end{aligned}$$

  así para todo $g \in G$, existe $x \in F_{red}(S)$, tal que $\overline{\varphi}(x) = g$.

- **Inyectividad**. Por contradicción, supongamos que $\overline{\varphi}$ no es inyectiva.

Entonces existe $s_1 \cdots s_n \in F_{red}(S) \setminus \{\epsilon\}$, donde $s_1, \ldots, s_n \in S \cup \widehat{S}$, con longitud mínima tal que;

$$\overline{\varphi}(s_1 \cdots s_n) = e \tag{2.2}$$

consideremos los siguientes casos:

Caso 1: Para $n = 1$, sea $s_1 \in F_{red}(S) \setminus \{\epsilon\}$.

Si $s_1 \in F_{red}(S) \setminus \{\epsilon\}$, entonces

$$\overline{\varphi}(s_1) = e$$

esto es una contradicción ya que teníamos que $\overline{\varphi}$ es el mapeo identidad en S, es decir, $\overline{\varphi}(s_1) = s_1$ y $s_1 \neq e$ (porque $e \notin S$, de lo contrario tendríamos $e \cdot e = e$ en S y esto no es posible por hipótesis).

Caso 2: Para $n = 2$, sea $s_1 s_2 \in F_{red}(S) \setminus \{\epsilon\}$.

Si $s_1 s_2 \in F_{red}(S) \setminus \{\epsilon\}$, entonces,

$$\begin{aligned} \overline{\varphi}(s_1 \cdot s_2) = e &\Longrightarrow \overline{\varphi}(s_1) \cdot \overline{\varphi}(s_2) = e \ \text{; ya que } \overline{\varphi} \text{ es homomorfismo} \\ &\Longrightarrow s_1 \cdot s_2 = e \ (\rightarrow\leftarrow) \end{aligned}$$

esto es una contradicción ya que tenemos en el enunciado del teorema que para $s_1,\ s_2 \in S$ se satisface que $s_1 \cdot s_2 \neq e$.

Caso 3: Para $n \geq 3$.

Consideremos los siguientes elementos de G: $g_0,\ g_1, \ldots, g_n$.

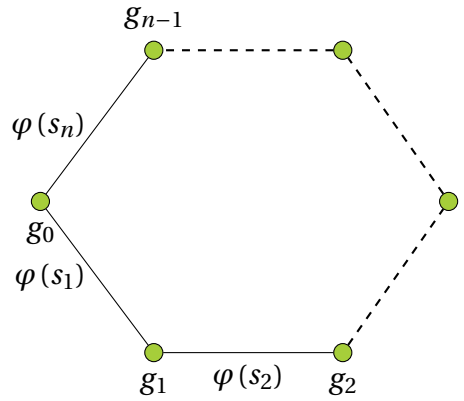


Figura 2.7. Los ciclos conducen a palabras reducidas, y viceversa

Definamos;

$$g_0 := e,\ g_1 := g_0\ \overline{\varphi}(s_1), \ldots, g_n := g_0\ \overline{\varphi}(s_1) \cdots \overline{\varphi}(s_n) \quad \text{ver figura 2.7}$$

como $\overline{\varphi}$ es el mapeo identidad en S, tenemos que;

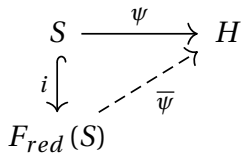
$$\begin{aligned} g_n &= g_0\ \overline{\varphi}(s_1)\cdots\overline{\varphi}(s_n) \\ &= g_0\overline{\varphi}(s_1\cdots s_n) && \text{; ya que } \overline{\varphi} \text{ es homomorfismo} \\ &= g_0 e && \text{; hemos definido a } \overline{\varphi} \text{ en 2.2} \\ &= g_0 \end{aligned}$$

entonces tenemos un ciclo; $g_0 = e,\ g_1,\ldots,g_n = g_0$ pero esto es una contradicción porque tenemos por hipótesis que $\mathrm{Cay}(G,S)$, es un árbol. Por tanto, $\overline{\varphi}$ es inyectiva.

Por lo tanto, $\overline{\varphi}$ es biyectiva y así, $F_{red}(S) \cong G$.

Ahora bien, tenemos que $\overline{\varphi}$ es un isomorfismo, así $G \cong F_{red}(S)$. Ahora probaremos que G es libre, probemos que se cumple la propiedad universal, vamos a probar que para todo H y para todo $\psi : S \longrightarrow H$ existe un único homomorfismo ϕ.

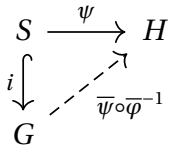
Debemos de tomar en cuenta que $F_{red}(S)$ es libre, entonces se cumple que para todo H y para todo $\psi : S \longrightarrow H$, existe un único homomorfismo, $\overline{\psi} : F_{red}(S) \longrightarrow H$ tal que, $\overline{\psi}|_S = \psi$



Ya probamos que $\overline{\varphi}|_S = id_S$, y además como $\overline{\varphi}$ es isomorfismo, sabemos que $\overline{\varphi}^{-1}$ existe,

$$\overline{\varphi}(s) = s \Longrightarrow \overline{\varphi}^{-1}(s) = s$$

Consideremos $\overline{\psi} \circ \overline{\varphi}^{-1} : G \longrightarrow H$, así el diagrama conmuta:



$\overline{\psi} \circ \overline{\varphi}^{-1}$ es un homomorfismo, ya que es composición de dos homomorfismos, entonces existe el homomorfismo que necesitamos, $\phi = \overline{\psi} \circ \overline{\varphi}^{-1}$.

- Probemos que se cumple que $\phi \circ i = \psi$

$$\begin{aligned}(\phi \circ i)(s) &= \phi(s) \\ &= \left(\overline{\psi} \circ \overline{\varphi}^{-1}\right)(s) \\ &= \overline{\psi}\left(\overline{\varphi}^{-1}(s)\right) \\ &= \overline{\psi}(s) \\ &= \psi(s)\end{aligned}$$

  por tanto, cumple que $\phi \circ i = \psi$.

- Ahora, probaremos que ϕ, es único.

  Supongamos que existe otro homomorfismo $\overline{\overline{\psi}} : G \longrightarrow H$, tal que $\overline{\overline{\psi}} \circ i = \psi$. Si notamos, $\overline{\overline{\psi}} \circ \overline{\varphi} : F_{red}(S) \longrightarrow H$

$$\begin{aligned}\left(\overline{\overline{\psi}} \circ \overline{\varphi}\right)(s) &= \overline{\psi}(s) \\ &= \overline{\psi}(i(s)) \\ &= \left(\overline{\psi} \circ i\right)(s) \\ &= \psi(s)\end{aligned}$$

  así, $\left(\overline{\overline{\psi}} \circ \overline{\varphi}\right)(s) = \psi(s)$, pero por unicidad de $\overline{\psi}$ se tiene que $\overline{\overline{\psi}} \circ \overline{\varphi} = \overline{\psi}$, entonces $\overline{\overline{\psi}} = \overline{\psi} \circ \overline{\varphi}^{-1}$, así $\phi = \overline{\psi} \circ \overline{\varphi}^{-1}$, es decir, ϕ es único.

Por tanto, S genera libremente a G. □

2.3. Grupos libres y acción sobre los árboles

En las secciones anteriores de este capítulo estudiamos el primer paso de los grupos a la geometría como tal, considerando los grafos de Cayley y algunas propiedades sobre ellos. Entonces en esta presente sección estudiaremos otro aspecto geométrico de los grupos que son: las acciones de grupo, en esto se puede contemplar una generalización de los grupos como grupos de simetría.
Comenzamos con algunos conceptos básicos sobre las acciones de grupo, se muestra que los grupos libres pueden caracterizarse geométricamente a través de acciones libres en los árboles y además la caracterización de los grupos libres en términos de acciones libres sobre los árboles nos permite comprobar la parte libre de ciertos subgrupos de grupos.

Definición 2.11 (Grupo acción)

Sea G un grupo, sea C una categoría, y sea X un objeto en C. Una acción de G en X en la categoría C es un homomorfismo de grupo $G \longrightarrow \mathrm{Aut}_C(X)$. En otras palabras, un **grupo acción** de G en X consiste de una familia $\left(f_g\right)_{g\in G}$ de automorfismos de X tal que

$$f_g \circ f_h = f_{g\cdot h}$$

para todo $g, h \in G$.

Normalmente los grupos surgen junto con su acción sobre algún conjunto, generalmente lo definimos como acción a la izquierda y acción a la derecha.

Definición 2.12 (Acción a la izquierda)

Una **acción a la izquierda** de un grupo G sobre un conjunto X es una función $\varphi : G \times X \longrightarrow X$ tal que:

- $\varphi\left(g, \varphi(h,x)\right) = \varphi\left(gh, x\right) \quad \forall g, h \in G,\ x \in X$;
- $\varphi(e,x) = x \quad \forall x \in x,\ e \in G$.

Definición 2.13 (Acción a la derecha)

Una **acción a la derecha** de un grupo G sobre un conjunto X es una función $\phi : X \times G \longrightarrow X$ tal que:

- $\phi\left(\phi(x,h), g\right) = \phi\left(x, hg\right) \quad \forall g, h \in G,\ x \in X$;
- $\phi(x,e) = x \quad \forall x \in x,\ e \in G$.

Recordatorio:

Sin embargo, se acostumbra a escribir $g \cdot x$ en lugar de $\varphi\left(g, x\right)$, con esta notación las propiedades de una acción a la izquierda son:

- $g \cdot (h \cdot x) = \left(gh\right) \cdot x \quad \forall g, h \in G,\ x \in X$;
- $e \cdot x = x \quad \forall x \in x,\ e \in G$.

(De igual manera para las propiedades de acción a la derecha).

La relación entre grupos y objetos geométricos sobre los que se actúa es particularmente fuerte si la acción del grupo es llamada **acción libre**. De una manera más formal se

define lo siguiente:

Definición 2.14 (Acción libre en un conjunto)

Sea un grupo G, sea X un conjunto y sea $\cdot : G \times X \longrightarrow X$ una acción de G en X. Esta acción es **libre** si

$$g \cdot x \neq x$$

para todo $g \in G \setminus \{e\}$ y todo $x \in X$. En otras palabras, una acción es libre si y solo si todo elemento de grupo no trivial actúa sin puntos fijos.

Nota:

Contra reciproco de la definición de acción libre en un conjunto es: Sea G un grupo, sea X un conjunto y sea $\cdot : G \times X \longrightarrow X$ una acción de G en X. Esta acción es **libre** si

$$g \cdot x = x$$

para algún $g \in G$ y algún $x \in X$ entonces $g = e$.

Ejemplo 2.16 **(Acción de traslación por la izquierda)**

Si G es un grupo entonces la acción de traslación por la izquierda

$$\begin{aligned} G &\longrightarrow S_G = \mathrm{Aut}_{set}(G) \\ g &\longmapsto (h \mapsto g \cdot h) \end{aligned}$$

Es una acción libre de G sobre si mismo por biyecciones.

Análisis:

Queremos probar que la acción de traslación por la izquierda es una acción libre de G. Sea

$$\begin{aligned} \varphi : G &\longrightarrow S_G = \mathrm{Aut}_{set}(G) \\ g &\longmapsto \varphi(g) : G \longrightarrow G \\ & \qquad\quad h \longmapsto g * h \end{aligned}$$

Definimos la acción de traslación por la izquierda:

$$\begin{aligned} \cdot : G \times G &\longrightarrow G \\ (g, h) &\longmapsto g \cdot h = g * h \end{aligned}$$

Sea G un grupo.
Sea $h \in G$ tal que $g \cdot h = h$.

$$\begin{aligned} g \cdot h = h &\Longrightarrow g \cdot h\left(h^{-1}\right) = h\left(h^{-1}\right) && \text{; inverso multiplicativo de } h \\ &\Longrightarrow g \cdot \left(hh^{-1}\right) = hh^{-1} && \text{; por propiedad de grupos (definición 1.1)} \\ &\Longrightarrow g = e \end{aligned}$$

Por tanto la acción de traslación por la izquierda es una acción libre de G.

■

Ejemplo 2.17 **(Rotación en $\mathbb{C}$)**

Sea $\mathbb{S}^1 := \left\{ z \in \mathbb{C} \;\middle|\; |z| = 1 \right\}$ el círculo unitario en $\mathbb{C}$, y sea $\alpha \in \mathbb{R}$. Entonces la acción de rotación

$$\begin{aligned} \mathbb{Z} \times \mathbb{S}^1 &\longrightarrow \mathbb{S}^1 \\ (n, z) &\longmapsto e^{2\pi i \cdot \alpha \cdot n} \cdot z \end{aligned}$$

de $\mathbb{Z}$ en $\mathbb{S}^1$ es libre si y solo si α es irracional.

Análisis:

"$\Longrightarrow$" La acción de rotación de $\mathbb{Z}$ en $\mathbb{S}^1$ es libre entonces α es irracional.

Por hipótesis la acción de traslación por la izquierda de $\mathbb{Z}$ en $\mathbb{S}^1$ es libre, es decir, que si $n \neq 0$, y $\forall z \in \mathbb{S}^1$ entonces $n \cdot z \neq z$.
Además, supongamos que $\alpha \in \mathbb{Q}$, así existen l, s en $\mathbb{Z}$ tal que $\alpha = \frac{l}{s}$ para $s \neq 0$.

$$\begin{aligned} &\Longrightarrow \alpha = \frac{l}{s} \\ &\Longrightarrow e^{2\pi i \cdot \alpha \cdot s} = e^{2\pi i \cdot l} = 1 && \text{; el ángulo es múltiplo de } 2\pi \\ &\Longrightarrow e^{2\pi i \cdot \alpha \cdot s} \cdot z = z && \text{; multiplicamos por un número complejo} \\ &\Longrightarrow s \cdot z = z && \text{; } \forall z \in \mathbb{S}^1 \end{aligned}$$

Pero contradice nuestra hipótesis de que: si $n \neq 0$, y $\forall z \in \mathbb{S}^1$, entonces $n \cdot z \neq z$.
$\therefore$ Si la acción de rotación de $\mathbb{Z}$ en $\mathbb{S}^1$ es libre entonces α es irracional.

"$\Longleftarrow$" α es irracional entonces la acción de rotación de $\mathbb{Z}$ en $\mathbb{S}^1$ es libre.

Supongamos que $\alpha \notin \mathbb{Q}$.
Sabemos que $e^{\theta i} = 1$ cuando $\theta = 2\pi \cdot k$, para $k \in \mathbb{Z}$. Tomamos $\theta = 2\pi \cdot n \cdot \alpha$ pero por hipótesis α

es irracional por lo que θ no será un múltiplo de 2π entonces $e^{2\pi i\cdot\alpha\cdot n}=1$ solamente cuando $n=0$.
Ahora, sea $n\cdot z=z$, para algún $z\in\mathbb{S}^1$,

$$\begin{aligned} n\cdot z=z &\Longrightarrow e^{2\pi i\cdot\alpha\cdot n}\cdot z=z \\ &\Longrightarrow e^{2\pi i\cdot\alpha\cdot n}=1 \\ &\Longrightarrow n=0 \end{aligned}$$

$\therefore$ Si $\exists z: n\cdot z=z$ entonces $n=0$, en otras palabras la acción es libre.
$\therefore$ Si α es irracional entonces la acción de rotación de $\mathbb{Z}$ en $\mathbb{S}^1$ es libre.

Así, esto demuestra que $\mathbb{Z}$ en $\mathbb{S}^1$ es libre si y solo si α es irracional.

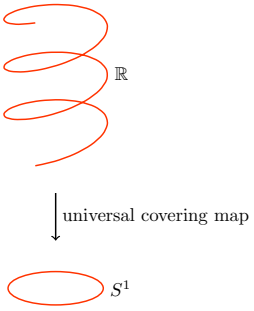


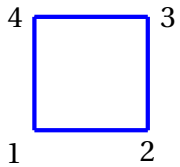
Figura 2.8. Recubrimiento universal de $\mathbb{S}^1$.

■

Ejemplo **2.18**

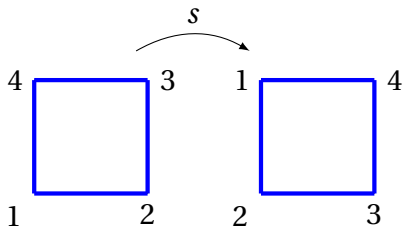
Las isometrías del cuadrado unitario están formadas por el grupo diédrico D_4.

Análisis: Sea un cuadrado unitario.

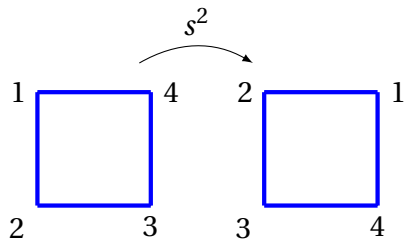


Definiremos las rotaciones y reflexiones presentes: Sea s la rotación y t la reflexión del cuadrado unitario.

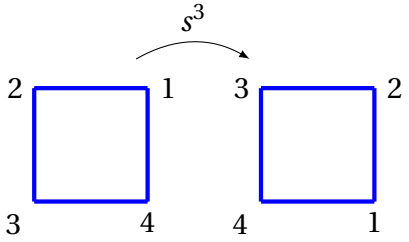
Rotación de $90° \Longrightarrow s = (1\ 2\ 3\ 4)$:



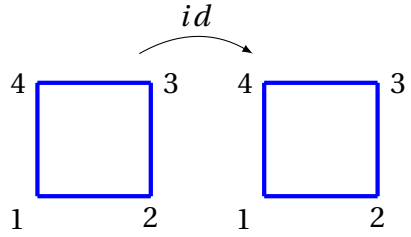
Rotación de $180° \Longrightarrow s^2 = (2\ 4)\,(1\ 3)$:



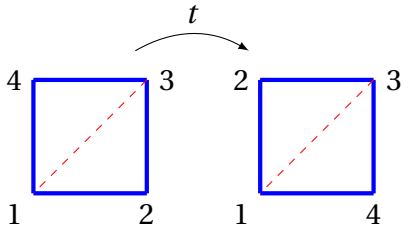
Rotación de $270° \Longrightarrow s^3 = (1\ 4\ 3\ 2)$:



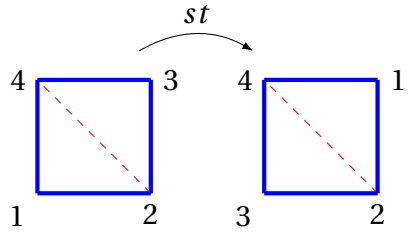
Rotación de $360° \Longrightarrow s^4 = id$:



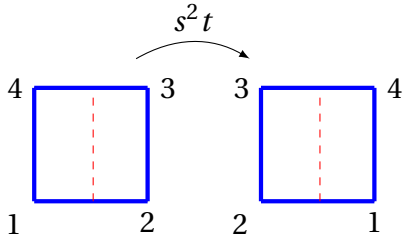
Reflexión a través de la diagonal $\Longrightarrow t = (2\ 4)$:



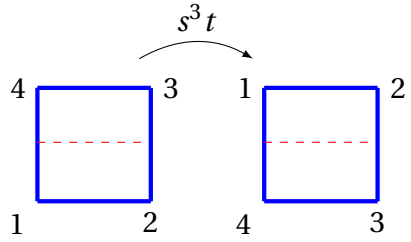
Reflexión a través de la diagonal $\Longrightarrow st = (1\ 3)$:



Reflexión a través del eje vertical $\Longrightarrow s^2t = (1\ 4)\,(2\ 3)$:



Reflexión a través del eje horizontal $\Longrightarrow s^3t = (1\ 2)\,(3\ 4)$:



Por lo tanto D_4 se define como:
$D_4 = \{id, s, s^2, s^3, t, st, s^2t, s^3t\}$.
Así D_4 representa las isometrías del cuadrado unitario.

■

Ejemplo 2.19 **(Isometría de grupos)**

En general, la acción de un grupo de isometría sobre un objeto geométrico subyacente no es necesariamente libre, por ejemplo, el grupo de isometrías del cuadrado unitario no actúa libremente sobre el cuadrado unitario; por ejemplo, los vértices del cuadrado unitario están fijos por reflexión a lo largo de la diagonal que pasa por el vértice en cuestión. Además, el centro del cuadrado está fijado por todas las isometrías del cuadrado.

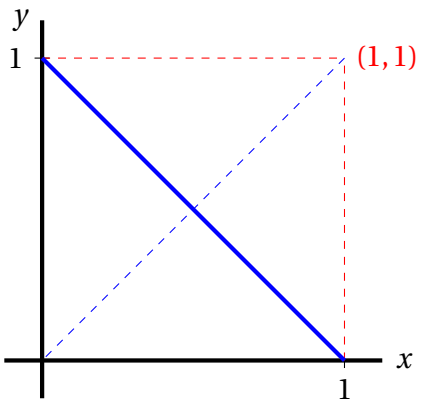
Análisis:

Sea $X = [0,1]^2$ con la métrica usual $d = \tau_{us}$ y sea G el grupo de isometrías del cuadrado unitario $G = \text{Isom}(X) := \left\{ f : X \longrightarrow X \;\middle|\; f \text{ es isometría} \right\}$, donde f es sobreyectiva y $1-1$, además, G un grupo bajo la composición. Definamos la acción como:

$$\begin{aligned} G \times X &\longrightarrow X \\ (h,(x,y)) &\longmapsto h \bullet (x,y) = h(x,y) \end{aligned}$$

consideremos $h \in G$ definida como

$$\begin{aligned} h : X \times X &\longrightarrow X \\ (x,y) &\longmapsto h(x,y) = (1-y, 1-x) \end{aligned}$$



Que es la reflexión con respecto a la diagonal. Luego, como $h(x,y) = (1-y, 1-x)$, así se garantiza que $h \neq e = id_X$.

Ahora veremos que h es isometría, para ello se verificará inyectividad y sobreyectividad.

- Probemos que h es inyectiva.

  Sea $h(x,y) = h(m,n)$.

$$\begin{aligned} h(x,y) = h(m,n) &\Longrightarrow (1-y, 1-x) = (1-n, 1-m) \\ &\Longrightarrow 1-y = 1-n \ \text{ y } \ 1-x = 1-m \\ &\Longrightarrow -y = -n \ , \ -x = -m \\ &\Longrightarrow y = n \ , \ x = m \\ &\Longrightarrow (x,y) = (m,n) \end{aligned}$$

  por lo tanto, es inyectiva.

- Probemos que h es sobreyectiva.

  Sea $(x,y) \in X$.

$$(x,y) \in X \Longrightarrow (1-y, 1-x) \in X$$

  también,

$$\begin{aligned} h(1-y, 1-x) &= \left(1-(1-y), 1-(1-x)\right) \\ &= (x,y) \end{aligned}$$

  por lo cual es sobreyectiva.

Así, al comprobar inyectividad y sobreyectividad tenemos que h es isometría y $h \in G$. Luego, consideremos la acción definida como

$$h \bullet (x,y) = h(x,y)$$

donde $h \in G, (x,y) \in X$. Ahora, tomemos el elemento $(x, 1-x)$ que está en la diagonal del cuadrado, entonces:

$$\begin{aligned} h \bullet (x, 1-x) &= h(x, 1-x) \\ &= (1-(1-x), 1-x) \\ &= (x, 1-x) \end{aligned}$$

pero como sabemos $h \neq e$ y hemos llegado a que $h \bullet (x, 1-x) = (x, 1-x)$ notamos que la acción no es libre, entonces tenemos que no es cierto que si existe $(x,y) \in X$ tal que $h \cdot (x,y) = (x,y)$ eso implique que $h = e$.
Por lo tanto, la acción no es libre.

■

Hay dos definiciones naturales de acciones libres sobre grafos: una requiere que ningún elemento del grupo no trivial fije ningún vértice, ni ningún borde y otra que solo requiere que no se fije ningún vértice, usaremos lo primero más fuerte:

Definición 2.15 (Acción libre sobre un grafo)

Sea un grupo G que actúa sobre un grafo (V,E) por isomorfismos de grafo mediante el mapeo

$$\rho : G \longrightarrow \mathrm{Aut}\,(V,E)$$

la acción ρ es libre si para todo $g \in G/\{e\}$ tenemos:

$$\forall v \in V \ \ \left(\rho\left(g\right)\right)(v) \neq v, \quad \text{y}$$
$$\forall_{\{v,v'\}\in E} \left\{\left(\rho\left(g\right)\right)(v) \ \ , \left(\rho\left(g\right)\right)\left(v'\right)\right\} \neq \left\{v, v'\right\}.$$

Ejemplo **2.20**

Sea G un grupo y sea S un conjunto generador de G. Entonces el grupo G actúa mediante isomorfismos de grafos en el grafo de Cayley $\mathrm{Cay}\,(G,S)$ mediante la traslación a la izquierda:

$$G \longrightarrow \mathrm{Aut}\left(\mathrm{Cay}\,(G,S)\right)$$
$$g \longrightarrow \left(h \mapsto g \cdot h\right)$$

Observe que este mapeo está bien definido y es un homomorfismo de grupo.

Análisis:

Sea

$$\rho : G \longrightarrow \mathrm{Aut}\left(\mathrm{Cay}\,(G,S)\right)$$
$$g \longrightarrow \rho\left(g\right) : \mathrm{Cay}\,(G,S) \longrightarrow \mathrm{Cay}\,(G,S)$$
$$h \mapsto g \cdot h$$

Verifiquemos que ρ es función.

Sean $g_1, g_2 \in G$ tales que $g_1 = g_2$ y sea $h \in \mathrm{Cay}\,(G,S)$.

Como $g_1 = g_2$ y como la operación del grupo está bien definida, entonces

$$\begin{aligned} g_1 = g_2 &\Longrightarrow g_1 * h = g_2 * h && ;\forall h \\ &\Longrightarrow \left(\rho\left(g_1\right)\right)(h) = \left(\rho\left(g_2\right)\right)(h) \\ &\Longrightarrow \rho\left(g_1\right) = \rho\left(g_2\right). \end{aligned}$$

Así, ρ es función.

Ahora probaremos que ρ es homomorfismo.

Sean $g_1, g_2 \in G$ y $h \in \mathrm{Cay}(G, S)$.

$$\begin{aligned} \left(\rho\left(g_1 * g_2\right)\right)(h) &= \left(g_1 * g_2\right) * (h) \\ &= g_1 * \left(g_2 * h\right) \\ &= \left(\rho\left(g_1\right)\right)\left(g_2 * h\right) \\ &= \left(\rho\left(g_1\right)\right)\left(\rho\left(g_2\right)\right)(h) \\ &= \left(\rho\left(g_1\right) \circ \rho\left(g_2\right)\right)(h) \end{aligned}$$

así, $\rho\left(g_1 * g_2\right) = \rho\left(g_1\right) \circ \rho\left(g_2\right)$. Por lo tanto, ρ es homomorfismo.

Ahora verificaremos las dos condiciones de la definición de acción a la izquierda.

Sean $g, g' \in G$ y $h \in \mathrm{Cay}(G, S)$.

- Verificaremos que $\rho\left(g, \rho\left(g', h\right)\right) = \rho\left(gg', h\right)$.
  Partiendo del lado izquierdo notamos que:

  $$\begin{aligned} \rho\left(g, \rho\left(g', h\right)\right) &= g * \left(g' * h\right) && ;\text{ por nota dada anteriormente} \\ &= \left(g * g'\right) * h && ;\text{ dado que la operación del grupo es asociativa} \\ &= \rho\left(gg', h\right) \end{aligned}$$

  $\therefore \rho\left(g, \rho\left(g', h\right)\right) = \rho\left(gg', h\right).$

- $\rho(e, h) = h$.

  $$\begin{aligned} \rho(e, h) &= e * h && ;\text{ por nota dada anteriormente} \\ &= h \end{aligned}$$

  $\therefore \rho(e, h) = h.$

Por lo tanto, el grupo G actúa mediante isomorfismos.

■

Recordatorio:

El orden de un elemento g de un grupo G es el mínimo de todos los $n \in \mathbb{N}_{>0}$ con $g^n = e$.

Proposición 2.3 . (Acciones libres sobre grafos de Cayley)

Sea G un grupo, y sea S un conjunto generador libre de G. Entonces, la acción traslación a la izquierda sobre el grafo de Cayley $\mathrm{Cay}(G,S)$ es libre si y solo si S no contiene ningún elemento de orden 2.

Demostración. La acción traslación izquierda sobre el grafo de Cayley $\mathrm{Cay}(G,S)$ es libre, cuando hablamos de la acción traslación izquierda, hablamos de acción sobre los vértices.

"$\Leftarrow$" Vamos a probar que si S no contiene ningún elemento de orden 2, entonces la acción traslación izquierda sobre el grafo de Cayley $\mathrm{Cay}(G,S)$ es libre. Probemos por contrareciproco, reescribamos el enunciado: supongamos que la acción traslación izquierda sobre el grafo de Cayley no es libre, entonces S contiene un elemento de orden 2.

Tenemos por hipótesis que la acción traslación izquierda sobre el grafo de Cayley no es libre, entonces no se cumple la definición 2.15, es decir, tendremos que se cumple las siguientes dos condiciones:

$$1.\ \left(\exists g \in \{G - \{e\}\},\ \exists g' : g \cdot g' = g'\right) \vee\ 2.\ \left(\exists g_1, g_2 \in G : \{g g_1, g g_2\} = \{g_1, g_2\}\right)$$

De 1 tenemos: si $g \cdot g' = g'$, entonces $g' = e$, pero esto es absurdo ya que $g \in \{G - \{e\}\}$.

De 2. tenemos que $\{g_1, g_2\}$ es una arista de $\mathrm{Cay}(G,S)$, como tenemos una traslación por la izquierda, tenemos;

$$\{g_1, g_2\} = g \cdot \{g_1, g_2\} = \{g \cdot g_1, g \cdot g_2\}$$

por definición escribimos el vértice $g_2 = g_1 \cdot s$ con $s \in S \cup S^{-1} / \{e\}$. Entonces se da uno de los siguientes casos:

1. Tenemos por hipótesis que la acción traslación izquierda sobre el grafo de Cayley no es libre, entonces no se cumple la definición 2.15, así, tendremos que;

   $$g \cdot g_1 = g_1 \ \wedge\ g \cdot g_2 = g_2$$

   y esto nos dice que $g = e$ y esto es absurdo.

2. Tenemos que $g \cdot g_1 = g_2$ y $g \cdot g_2 = g_1$, entonces en G, tendremos;

$$\begin{aligned} g_1 &= g \cdot g_2 \\ &= g \cdot (g_1 \cdot s) \qquad \text{; por lo que hemos definido antes de los items} \\ &= (g \cdot g_1) \cdot s \\ &= g_2 \cdot s \\ &= (g_1 \cdot s) \cdot s \\ &= g_1 \cdot s^2 \end{aligned}$$

si $g_1 = g_1 \cdot s^2$, entonces $s^2 = e$. Teníamos que $s \in S \cup S^{-1} \setminus \{e\}$, así $s \neq e$. Ya que $s^2 = e$, S contiene un elemento de orden 2.

por tanto hemos probado la afirmación.

"⇒" Ahora vamos a demostrar que si la acción traslación izquierda sobre el grafo de Cayley es libre, entonces S no contiene un elemento de orden 2

Probemos por contra-recíproco, reescribamos el enunciado: si S contiene un elemento de orden 2, entonces la acción traslación izquierda sobre el grafo de Cayley no es libre.

Sea $s \in S$, tal que $s^2 = e$ con $s \neq e$, ya que tenemos por hipótesis que S contiene un elemento de orden 2. Sea $g = s$ donde g es un vértice, así $\{e, g\}$ es una arista;

$$\begin{aligned} g \cdot \{e, s\} &= \{g \cdot e, g \cdot s\} \\ &= \{g, g \cdot s\} \\ &= \{s, s \cdot s\} \\ &= \{s, s^2\} \\ &= \{s, e\} \\ &= \{e, s\} \end{aligned}$$

por tanto, tenemos que $g \cdot \{e, s\} = \{e, s\}$, así la acción traslación izquierda sobre el grafo de Cayley no es libre. □

Una acción de grupo puede dividirse en **órbitas**, lo que lleva al espacio de órbitas de la acción. Por el contrario, se puede tratar de entender el objeto completo mirando el espacio orbital y las órbitas/estabilizadores.

Definición 2.16 (Orbitas)

Sea G un grupo que actúa sobre un conjunto X.

- La **órbita** de un elemento $x \in X$ con respecto a esta acción es el conjunto;

$$G \cdot x := \left\{ \; g \cdot x \;\middle|\; g \in G \; \right\} = \mathrm{Orb}\,(x)$$

- El cociente de X dado por la acción G (o espacio de órbitas) es el conjunto;

$$G \setminus X := \left\{ \; G \cdot x \;\middle|\; x \in X \; \right\}$$

de órbitas, escribimos "$G \setminus X$", porque G actúa "a la izquierda".

Proposición 2.4

$G \setminus X$ es partición de X.

Demostración. Probemos que, $G \setminus X$ es partición de X, en otras palabras debemos probar tres cosas:

1. $\forall E \in G \setminus X,\ E \neq \varnothing$.
2. $E,\ F \in G \setminus X$, entonces $E = F$ ó $E \cap F = \varnothing$.
3. $X = \bigcup_{E \in G \setminus X} E$

Primero. Sea $E \in G \setminus X$. Si $E \in G \setminus X$ así $E = G \cdot x$, donde $x \in X$.

Como $x \in G \cdot x$, entonces $G \cdot x \neq \varnothing$, por lo que $E \neq \varnothing$.

Segundo. Sea $E,\ F \in G \setminus X$ donde $E = G \cdot x_1$ y $F = G \cdot x_2$ tal que $E \cap F \neq \varnothing$. Si $G \cdot x_1 \cap G \cdot x_2 \neq \varnothing$, entonces existe $z \in G \cdot x_1 \cap G \cdot x_2$ tal que $z = g_1 \cdot x_1$ y $z = g_2 \cdot x_2$

- $G \cdot x_1 \subset G \cdot x_2$.

  Sea $w \in G \cdot x_1$, así $w = g_3 \cdot x_1$,

$$\begin{aligned} w = g_3 \cdot x_1 &\Longrightarrow w = g_3 \left(g_1^{-1} \cdot z \right) \\ &\Longrightarrow w = g_3 \left(g_1^{-1} \cdot g_2 \cdot x_2 \right) \\ &\Longrightarrow w = \left(g_3 g_1^{-1} g_2 \right) \cdot x_2 \\ &\Longrightarrow w \in G \cdot x_2. \end{aligned}$$

  así, $G \cdot x_1 \subset G \cdot x_2$.

- $G \cdot x_2 \subset G \cdot x_1$.

  Sea $w \in G \cdot x_2$, así $w = g_3 \cdot x_2$,

$$\begin{aligned} w = g_3 \cdot x_2 &\Longrightarrow w = g_3 \left(g_2^{-1} \cdot z\right) \\ &\Longrightarrow w = g_3 \left(g_2^{-1} \cdot g_1 \cdot x_1\right) \\ &\Longrightarrow w = \left(g_3 g_2^{-1} g_1\right) \cdot x_1 \\ &\Longrightarrow w \in G \cdot x_1. \end{aligned}$$

  así, $G \cdot x_2 \subset G \cdot x_1$.

Hemos demostrado que $E = G \cdot x_1 = G \cdot x_2 = F$.

Tercero. Probaremos que $X = \bigcup_{E \in G \setminus X} E$

- $X \subset \bigcup_{E \in G \setminus X} E$.

  Para todo $x \in X$, se cumple que $x \in E = G \cdot x$, entonces $x \in \bigcup_{y \in X} G \cdot y$. Así $X \subset \bigcup_{E \in G \setminus X} E$.

- $\bigcup_{E \in G \setminus X} E \subset X$.

  Tenemos que para todo $x \in X$ se cumple que $G \cdot x \subset X$, entonces, $\cup_{x \in X} G \cdot x \subset X$ así, $\cup_{E \in G \setminus X} E \subset X$.

por tanto, $X = \bigcup_{E \in G \setminus X} E$.

Hemos demostrado que se cumplen las tres condiciones, por lo tanto, $G \setminus X$ es partición de X. □

Ejemplo 2.21 **(Rotación en $\mathbb{C}$)**

Consideramos la acción del círculo unitario $\mathbb{S}^1$ (que es un grupo con respecto a la multiplicación) en los números complejos $\mathbb{C}$ dada por la multiplicación de números complejos. La órbita del origen 0 es solo $\{0\}$; la órbita de un elemento $z \in \mathbb{C} \setminus \{0\}$ es el círculo alrededor de 0 que pasa a través de z. El cociente de $\mathbb{C}$ por esta acción puede ser identificado con $\mathbb{R}_{\geq 0}$ (a través del valor absoluto).

Análisis:

Los números complejos en el círculo unitario se pueden escribir como $z = \cos(\theta) + i \cdot \operatorname{sen}(\theta)$, de manera más abreviada $z = \cos(\theta) + i \cdot \operatorname{sen}(\theta) = e^{i\theta}$. (Ver figura 2.9)

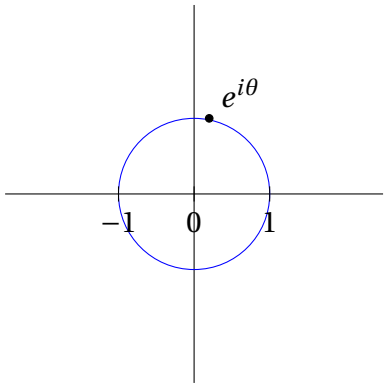


Figura 2.9. Representación del círculo unitario.

Además, sabemos que el círculo unitario esta representado como:

$$\mathbb{S}^1 := \left\{ \; z \in \mathbb{C} \;\middle|\; |z| = 1 \; \right\}.$$

Ahora bien, consideramos la acción del círculo unitario $\mathbb{S}^1$ con la multiplicación de números complejos. Tomamos la órbita en el origen 0, ya que estamos hablando de la multiplicación de números complejos, $z = 1$ en esta órbita no posee un inverso multiplicativo por lo que simplemente es $\{0\}$ o la órbita en el origen 0.

Entonces por lo mencionado anteriormente, al tomar un elemento $z \in \mathbb{C} \setminus \{0\}$ de la órbita, este es el circulo alrededor de cero; notemos que a través de esa acción (multiplicación de números complejos) se generan las siguientes órbitas con $\mathbb{S}^1 \cdot z = \left\{ \; w \cdot z \;\middle|\; w \in \mathbb{S}^1 \; \right\}$ pero sabemos que $w \in \mathbb{S}^1$ tiene norma 1 así $|w \cdot z| = |z|$ entonces en el conjunto $\mathbb{S}^1 \cdot z$ todos sus elementos tienen $|z|$, es decir:

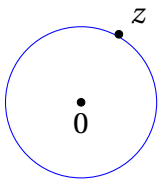


Figura 2.10. Representación de $\mathbb{S}^1 \cdot z$.

El cociente $\mathbb{C}$ por esta acción puede ser identificado por $\mathbb{R}_{\geq 0}$.
Sea $\mathbb{C}/\mathbb{S}^1 = \left\{ \; \mathbb{S}^1 \cdot z \;\middle|\; z \in \mathbb{C} \; \right\}$. Definimos el mapeo ϕ:

$$\begin{aligned} \phi : \mathbb{C}/\mathbb{S}^1 &\longrightarrow \mathbb{R}_{\geq 0} \\ \mathbb{S}^1 \cdot z &\longmapsto \phi\left(\mathbb{S}^1 \cdot z\right) = |z| \end{aligned}$$

Probaremos que $\mathbb{C}/\mathbb{S}^1$ identificado por $\mathbb{R}_{\geq 0}$.

- ϕ esta bien definida.
  Sea $\mathbb{S}^1 \cdot z, \mathbb{S}^1 \cdot w \in \mathbb{C}/\mathbb{S}^1$ tal que $\mathbb{S}^1 \cdot z = \mathbb{S}^1 \cdot w$.

$$\begin{aligned} \mathbb{S}^1 \cdot z = \mathbb{S}^1 \cdot w &\Longrightarrow |z| = |w| \\ &\Longrightarrow \phi\left(\mathbb{S}^1 \cdot z\right) = \phi\left(\mathbb{S}^1 \cdot w\right) \end{aligned}$$

  $\therefore \phi$ esta bien definida.

- ϕ es inyectivo.
  Sea $\mathbb{S}^1 \cdot z, \mathbb{S}^1 \cdot w \in \mathbb{C}/\mathbb{S}^1$ tal que $\phi\left(\mathbb{S}^1 \cdot z\right) = \phi\left(\mathbb{S}^1 \cdot w\right)$.

$$\begin{aligned} \phi\left(\mathbb{S}^1 \cdot z\right) = \phi\left(\mathbb{S}^1 \cdot w\right) &\Longrightarrow |z| = |w| \\ &\Longrightarrow \mathbb{S}^1 \cdot z = \mathbb{S}^1 \cdot w \end{aligned}$$

  $\therefore \phi$ es inyectivo.

- ϕ es sobreyectivo.
  Sea $r \in \mathbb{R}_{\geq 0}$.
  $r \in \mathbb{R}_{\geq 0} \Longrightarrow \mathbb{S}^1 \cdot r = |r| = r$.
  $\therefore \phi$ es sobreyectivo.
  $\therefore \phi$ es biyectivo.

Por tanto ϕ es isomorfismo. Así $\mathbb{C}/\mathbb{S}^1$ identificado por $\mathbb{R}_{\geq 0}$.

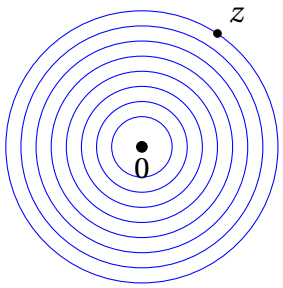


Figura 2.11. Órbitas de acción de rotación de $\mathbb{S}^1$ sobre $\mathbb{C}$.

■

Definición 2.17 (Estabilizador, conjunto fijo)

Sea G un grupo que actúa sobre un conjunto X.

- El grupo **estabilizador** de un elemento $x \in X$ con respecto a esta acción es dada por

$$G_x := \left\{ \; g \in G \;\middle|\; g \cdot x = x \; \right\} \subset G;$$

observe que G_x es de hecho un grupo (un subgrupo de G).

- El **conjunto fijo** de un elemento $g \in G$ está dado por

$$X^g := \left\{ \; x \in X \;\middle|\; g \cdot x = x \; \right\} \subset X;$$

más generalmente, si $H \subset G$ es un subconjunto, entonces escribimos $X^H := \bigcap_{h \in H} X^h$.

- Decimos que la acción de G sobre X tiene un **punto fijo global**, si $X^G \neq \emptyset$.

Ejemplo 2.22 **(Isometrías del cuadrado unitario)**

Sea $Q = [0,1] \times [0,1]$ el cuadrado unitario en $\mathbb{R}^2$, y sea G el grupo de isometría de Q con respecto a la métrica euclidiana en $\mathbb{R}^2$. Entonces G actúa naturalmente sobre Q por isometrías.

- Sea $t \in G$ la reflexión a lo largo de la diagonal que pasa por $(0,0)$ y $(1,1)$. Entonces

$$Q^t = \left\{ \; (x,x) \;\middle|\; x \in [0,1] \; \right\}.$$

- Sea $s \in G$ la rotación por $\pi/2$. Entonces

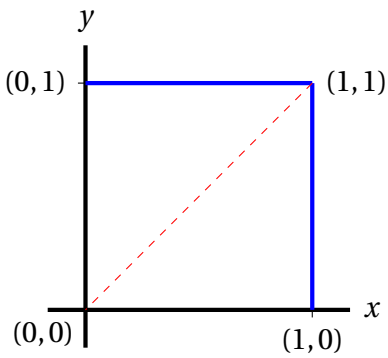
$$Q^s = \{(1/2, 1/2)\}.$$

- La órbita de $(0,0)$ son los cuatro vértices de Q, y el estabilizador de $(0,0)$ es $G_{(0,0)} = \left(id_Q, t\right)$.
- El estabilizador de $(1/3,0)$ es el grupo trivial.
- El estabilizador de $(1/2,1/2)$ es $G_{(1/2,1/2)} = G$, entonces $(1/2,1/2)$ es un punto fijo global de esta acción.

Análisis:

Con respecto al ejemplo 2.18 se comprueba que el cuadrado unitario actúa naturalmente por isometrías Q, entonces probaremos que se cumplen los siguientes ítems.
Primero. Sea $t \in G$ la reflexión de la diagonal del cuadrado unitario. Definimos la iso-

metría $t : Q \longrightarrow Q$ entonces:
La reflexión con respecto a la diagonal que pasa por $(0,0)$ a $(1,1)$ es:



$$\begin{aligned} t : Q &\longrightarrow Q \\ (x,y) &\longmapsto t(x,y) = (y,x) \end{aligned}$$

Ahora bien, la acción generada por isometrías en Q esta dada por:

$$\begin{aligned} \rho : G := \mathrm{Isom}(Q) &\longrightarrow \mathrm{Aut}(G) \\ t &\longmapsto \rho(t) : Q \longrightarrow Q \\ &\qquad (x,y) \longmapsto (\rho(t))(x,y) = t(x,y) \end{aligned}$$

Aplicando, acción por la izquierda:

$$\begin{aligned} G \times Q &\longrightarrow Q \\ (t,(x,y)) &\longmapsto t \cdot (x,y) = (y,x) \end{aligned}$$

Entonces por definición 2.17-ítem 2, $Q^t \subset Q$, así

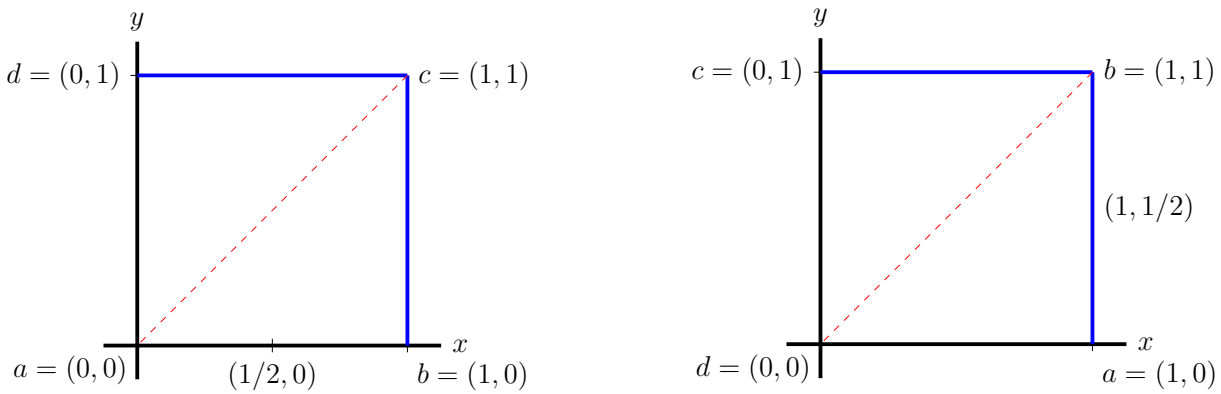
$$\begin{aligned} Q^t &= \left\{ (x,y) \;\middle|\; t \cdot (x,y) = (x,y) \right\} \\ &= \left\{ (x,y) \;\middle|\; (y,x) = (x,y) \right\} \\ &= \left\{ (x,y) \;\middle|\; y = x \right\} \\ &= \left\{ (x,x) \;\middle|\; x \in [0,1] \right\} \end{aligned}$$

Así concluimos que, si $t \in G$ es la reflexión a lo largo de la diagonal que pasa por $(0,0)$ y $(1,1)$ entonces $Q^t = \left\{ (x,x) \;\middle|\; x \in [0,1] \right\}$ con $Q^t \neq \emptyset$.

Segundo. Sea $s \in G$ una rotación por $\pi/2$. Aplicamos la matriz generadora de rotación:

$$\begin{aligned} s(x,y) &= \begin{pmatrix} \cos(\theta) & \text{-sen}(\theta) \\ \text{sen}(\theta) & \cos(\theta) \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \\ s(x,y) &= \begin{pmatrix} \cos(\pi/2)\cdot x + (\text{-sen}(\pi/2)\cdot y) \\ (\text{sen}(\pi/2)\cdot x) + \cos(\pi/2)\cdot y \end{pmatrix} = \begin{pmatrix} 0\cdot x - 1\cdot y \\ 1\cdot x + 0\cdot y \end{pmatrix} \\ s(x,y) &= \begin{pmatrix} -y \\ x \end{pmatrix} \end{aligned}$$

Así, $s(x,y) = (-y,x)$. Por definición 2.17 si el conjunto se mantiene fijo tenemos:



(a) Sin rotación (b) Con rotación

Figura 2.12. Representación del cuadrado unitario con rotación y sin rotación.

la regla de correspondencia esta dada por: $s(x,y) = (-y,x)$. Entonces

$$\begin{aligned} Q^s &= \left\{ (x,y) \;\middle|\; (-y,x) = (x,y) \right\} \\ &= \left\{ (x,x) \;\middle|\; x = 1 - x \right\} \\ &= \left\{ (x,x) \;\middle|\; x = 1/2 \right\} \\ &= \{(1/2,1/2)\} \end{aligned}$$

Así se concluye que, si $s \in G$ la rotación por $\pi/2$ entonces $Q^s = \{(1/2,1/2)\}$ con $Q^s \neq \emptyset$.

Tercero. Sea la órbita de $(0,0)$.
Aplicamos definición 2.16-ítem 1 entonces $\text{Orb}((0,0)) = \{(0,0)\}$. Notemos que la órbita del origen solo se contiene a si misma, por lo que $(0,0)$ es un punto fijo de esta acción, mostrando que cada elemento del conjunto (del cuadrado unitario) lo deja fijo.

Ahora, verificamos el estabilizador de $(0,0)$ por ejemplo 2.18 se tiene que:

$$\begin{aligned} G_{(0,0)} &= \left\{ \ f \ \middle| \ f(0,0) = (0,0) \ \right\} \\ &= \{id_Q, t\} \end{aligned}$$

Así la órbita de $(0,0)$ son los 4 vértices de Q y el estabilizador de $(0,0)$ es $G_{(0,0)} = \{id_Q, t\}$.

Cuarto. Consideramos el punto $(1/3,0)$.
Si hacemos las rotaciones y reflexiones dadas por el ejemplo 2.18 observamos que los puntos en la misma órbita son diferentes entonces poseen diferentes estabilizadores, además notamos que en la rotación; que se cumple al tener el punto fijo y no cambia es $G_{(1/3,0)} = \{id_Q\}$.
Así se concluye que el estabilizador de $(1/3,0)$ es el grupo trivial.

Quinto. Consideramos el punto $(1/2,1/2)$.
Hacemos las respectivas rotaciones y reflexiones dadas por el ejemplo 2.18 observamos que el punto se mantiene fijo, por lo que $G_{(1/2,1/2)} = G$, además el punto $(1/2,1/2)$ cumple ser un punto fijo global de esta acción.
Así se concluye que el estabilizador de $(1/2,1/2)$ es G y además se considera como punto fijo global de esta acción.

■

Lema 2.2
Sea (V,E) un árbol finito, es decir, $|V| = n$ y sea G el grupo que actúa sobre el árbol, entonces $\exists v \in V^G$ ó $\exists \{v, v'\} \in E : \{gv, gv'\} = \{v, v'\}$, $\forall g \in G$. (En otras palabras, existe un vértice o una arista estable con respecto a la acción).

Demostración. Procederemos por inducción.

- Para $n = 1$.

  Si $V = \{v\}$ y $G \curvearrowright V$ lo cual significa que hay una isometría

  $$\begin{aligned} \rho : G &\longrightarrow \mathrm{Aut}(V,E) \\ g &\longrightarrow \rho(g) : (V,E) \longrightarrow (V,E) \\ & \qquad v \longmapsto g \cdot v := \rho(g)(v) \end{aligned}$$

  donde $\rho(g)$ es un isomorfismo de grafos $\forall g \in G$, es decir, que es una función biyectiva tal que $\{v, v'\} \in E \Leftrightarrow \{gv, gv'\} \in E$.

Como $V = \{v\}$, entonces

$$\begin{aligned}\left(\rho\left(g\right)\right)(v) = v, \forall g \in G &\Longrightarrow gv = v, \forall g \in G \\ &\Longrightarrow v \in V^G \\ &\Longrightarrow V^G \neq \emptyset \\ &\Longrightarrow \exists v \in V^G \ \forall g \in G\end{aligned}$$

Por lo tanto, se cumple que: $\exists v \in V^G$ ó $\exists \left\{v, v'\right\} \in E : \left\{gv, gv'\right\} = \left\{v, v'\right\}, \ \forall g \in G$.

- Para $n = 2$.

  Sea $V = \{v_1, v_2\}$ y como $G \curvearrowright V$, entonces $\rho\left(g\right)$ es una isometría de grafos para todo $g \in G$, así:

$$\begin{aligned}\left(\rho\left(g\right)\right)(v_1) \neq \left(\rho\left(g\right)\right)(v_2) & \\ \left(\rho\left(g\right)\right)(v_1) = v_1 \ \text{ ó } \ v_2, & \\ \left(\rho\left(g\right)\right)(v_2) = v_1 \ \text{ ó } \ v_2 &\end{aligned}$$

  pero como $\rho(g)$ es biyección, es decir que es inyectiva y sobreyectiva, así sucederá uno de los siguientes casos:

  Caso 1: $\left(\rho\left(g\right)\right)(v_1) = v_1$ y $\left(\rho\left(g\right)\right)(v_2) = v_2$.

  Caso 2: $\left(\rho\left(g\right)\right)(v_1) = v_2$ y $\left(\rho\left(g\right)\right)(v_2) = v_1$.

  En ambos casos se ve que existe una arista en E, tal que $\left\{gv_1, gv_2\right\} = \{v_1, v_2\}, \forall g \in G$.

  $\therefore \exists v \in V^G$ ó $\exists \{v_1, v_2\} \in E : \left\{gv_1, gv_2\right\} = \{v_1, v_2\}, \forall g \in G$.

- Ahora probaremos para los mayores que n.

  Sea $|V| = n$.

  Si $n = 1$ ó $n = 2$ entonces la afirmación es verdadera.

  Supongamos $n \geq 3$ y además que el lema es verdadero para todo árbol finito con $k < n$ vértices. Como (V, E) es un árbol finito, donde $V = \{v_1, v_2, \ldots, v_m\}$, es decir que existirán vértices $(m \geq 2)$ de grado igual a 1.

  Dado que $n \geq 3$ y (V, E) es un árbol, existirá al menos un vértice de grado estrictamente mayor a 1, considérese V' como el conjunto de vértices que tienen más de un vecino, entonces tendremos un subgrafo $\left(V', E'\right)$ el cual es un subárbol propio de (V, E). Además, $\left(V', E'\right)$ es un árbol pues lo que se ha hecho es quitar de (V, E) todos aquellos vértices que tienen exactamente un vecino, es decir, que se han quitado aquellos vértices que están en los extremos.

Luego, como (V', E') es un subárbol propio de (V, E), entonces para todo $\varphi \in \mathrm{Aut}(V, E)$ se cumplirá que

$$\varphi|_{(V',E')} \in \mathrm{Aut}(V', E').$$

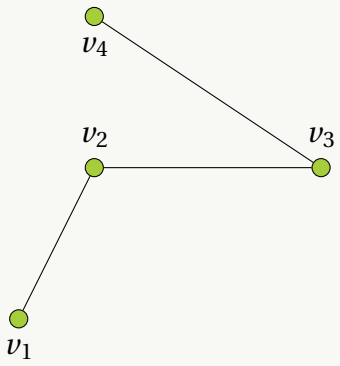
como $|V'| < |V|$, entonces por hipótesis de inducción $\forall g \in G$, $(V')^G \neq \emptyset$ ó $\exists \{v, v'\} \in E'$ tal que $\{gv, gv'\} = \{v, v'\}$ y como $(V')^G \subset V^G$ y $E' \subset E$, entonces (V, E) tiene un vértice o una arista estable con respecto a la acción.

□

Una manera de obtener un vértice o una arista estable con respecto a la acción consiste en eliminar todos aquellos vértices que tienen exactamente un vecino y seguir de esta manera hasta obtener un vértice o una arista, y estos últimos serían estables con respecto a la acción:

Ejemplo 2.23

Consideremos el siguiente árbol (V, E) de 4 vértices:



y sea G cualquier grupo que actúa sobre el árbol. En este árbol al eliminar los vértices que tienen exactamente un vecino estaríamos quitando los vértices v_1, v_4 y nos quedaría el subgrafo $(V' = \{v_2, v_3\}, E' = \{\{v_2, v_3\}\})$ y esta arista resultante sería estable con respecto a la acción.

Análisis: Como el árbol tiene 4 vértices, entonces $V = \{v_1, v_2, v_3, v_4\}$, dado de la manera anterior y como el grupo G actúa sobre el árbol, entonces existe una isometría

$$\begin{aligned} \rho : G &\longrightarrow \mathrm{Aut}(V, E) \\ g &\longrightarrow \rho(g) : (V, E) \longrightarrow (V, E) \\ & \qquad v \longmapsto (\rho(g))(v) = g \cdot v \end{aligned}$$

tal que preserva la estructura del grafo, es decir, $\{(\rho(g))(v),(\rho(g))(v')\} \in E \iff \{v,v'\} \in E$.

Se debe verificar que $(\rho(g))(\{v_1,v_4\}) = \{v_1,v_4\}$ es decir, que la acción sobre un vértices con un sólo vecino resulta ser un vértice con un sólo vecino.

- $(\rho(g))(v_1,v_4) = \{v_1,v_4\}$.

  i) Primero se demostrará que $(\rho(g))(\{v_1,v_4\}) \subset \{v_1,v_4\}$.

  Por contradicción suponga que $(\rho(g))(v_1) \in \{v_2,v_3\}$, se tendrían dos casos:

  Caso 1: $(\rho(g))(v_1) = v_2$.

  Del grafo sabemos que $\{v_1,v_2\},\{v_2,v_3\} \in E$, pero como $(\rho(g))(v_1) = v_2$, entonces:

  $$\{v_1,(\rho(g))(v_1)\},\{(\rho(g))(v_1),v_3\} \in E$$

  pero $\rho(g)$ es una biyección, entonces es sobreyectiva, es decir que v_1 y v_3 tendrían una preimagen v_1' y v_3' respectivamente, así, de lo anterior se tiene que:

  $$\{(\rho(g))(v_1'),(\rho(g))(v_1)\},\{(\rho(g))(v_1),(\rho(g))(v_3')\} \in E$$

  y como ρ es automorfismo de grafo, se cumple que:

  $$\begin{aligned}\{(\rho(g))(v_1'),(\rho(g))(v_1)\},\{(\rho(g))(v_1),(\rho(g))(v_3')\} \in E &\Longrightarrow \{v_1',v_1\},\{v_1,v_3'\} \in E \\ &\Longrightarrow v_1' = v_3' \quad ;\ v_1 \text{ tiene solo un vecino} \\ &\Longrightarrow v_1 = v_3\end{aligned}$$

  pero es una contradicción ya que v_1 y v_3 son dos vértices diferentes en el grafo.

  Caso 2: $(\rho(g))(v_1) = v_3$.

  Del grafo sabemos que $\{v_2,v_3\},\{v_3,v_4\} \in E$, pero como $(\rho(g))(v_1) = v_3$, entonces:

  $$\{v_2,(\rho(g))(v_1)\},\{(\rho(g))(v_1),v_4\} \in E$$

  pero $\rho(g)$ es una biyección, entonces es sobreyectiva, es decir que v_2 y v_4 tendrían una preimagen, v_2' y v_4' respectivamente, entonces se tiene que:

  $$\{(\rho(g))(v_2'),(\rho(g))(v_1)\},\{(\rho(g))(v_1),(\rho(g))(v_4')\} \in E$$

  Ahora bien, como ρ es automorfismo de grafo, se cumple que:

  $$\begin{aligned}\{(\rho(g))(v_2'),(\rho(g))(v_1)\},\{(\rho(g))(v_1),(\rho(g))(v_4')\} \in E &\Longrightarrow \{v_2',v_1\},\{v_1,v_4'\} \in E \\ &\Longrightarrow v_2' = v_4' \quad ;\ v_1 \text{ tiene solo un vecino} \\ &\Longrightarrow v_2 = v_4\end{aligned}$$

pero es una contradicción ya que v_2 y v_4 son dos vértices diferentes en el grafo.

Así, en ambos casos se tiene que $\left(\rho\left(g\right)\right)\left(v_1\right) \in \{v_1, v_4\}$.

ii) Análogamente se demuestra que $\left(\rho\left(g\right)\right)\left(v_4\right) \in \{v_1, v_4\}$.

Por contradicción suponga que $\left(\rho\left(g\right)\right)\left(v_4\right) \in \{v_2, v_3\}$, se tendrían dos casos:

Caso 1: $\left(\rho\left(g\right)\right)\left(v_4\right) = v_2$.

Del grafo sabemos que $\{v_1, v_2\}, \{v_2, v_3\} \in E$, pero como $\left(\rho\left(g\right)\right)\left(v_4\right) = v_2$, entonces:

$$\left\{v_1, \left(\rho\left(g\right)\right)\left(v_4\right)\right\}, \left\{\left(\rho\left(g\right)\right)\left(v_4\right), v_3\right\} \in E$$

pero $\rho\left(g\right)$ es una biyección, entonces es sobreyectiva, es decir que v_1 y v_3 tendrían una preimagen v_1' y v_3' respectivamente, así, de lo anterior se tiene que:

$$\left\{\left(\rho\left(g\right)\right)\left(v_1'\right), \left(\rho\left(g\right)\right)\left(v_4\right)\right\}, \left\{\left(\rho\left(g\right)\right)\left(v_4\right), \left(\rho\left(g\right)\right)\left(v_3'\right)\right\} \in E$$

y como ρ es automorfismo de grafo, se cumple que:

$$\begin{aligned}\left\{\left(\rho\left(g\right)\right)\left(v_1'\right), \left(\rho\left(g\right)\right)\left(v_4\right)\right\}, \left\{\left(\rho\left(g\right)\right)\left(v_4\right), \left(\rho\left(g\right)\right)\left(v_3'\right)\right\} \in E &\Longrightarrow \{v_1', v_4\}, \{v_4, v_3'\} \in E \\ &\Longrightarrow v_1' = v_3' \qquad ; v_4 \text{ tiene solo un vecino} \\ &\Longrightarrow v_1 = v_3\end{aligned}$$

pero es una contradicción ya que v_1 y v_3 son dos vértices diferentes en el grafo.

Caso 2: $\left(\rho\left(g\right)\right)\left(v_4\right) = v_3$.

Del grafo sabemos que $\{v_2, v_3\}, \{v_3, v_4\} \in E$, pero como $\left(\rho\left(g\right)\right)\left(v_4\right) = v_3$, entonces:

$$\left\{v_2, \left(\rho\left(g\right)\right)\left(v_4\right)\right\}, \left\{\left(\rho\left(g\right)\right)\left(v_4\right), v_4\right\} \in E$$

pero $\rho\left(g\right)$ es una biyección, entonces es sobreyectiva, es decir que v_2 y v_4 tendrían una preimagen, v_2' y v_4' respectivamente, entonces se tiene que:

$$\left\{\left(\rho\left(g\right)\right)\left(v_2'\right), \left(\rho\left(g\right)\right)\left(v_4\right)\right\}, \left\{\left(\rho\left(g\right)\right)\left(v_4\right), \left(\rho\left(g\right)\right)\left(v_4'\right)\right\} \in E$$

Ahora bien, como ρ es automorfismo de grafo, se cumple que:

$$\begin{aligned}\left\{\left(\rho\left(g\right)\right)\left(v_2'\right), \left(\rho\left(g\right)\right)\left(v_4\right)\right\}, \left\{\left(\rho\left(g\right)\right)\left(v_4\right), \left(\rho\left(g\right)\right)\left(v_4'\right)\right\} \in E &\Longrightarrow \{v_2', v_4\}, \{v_4, v_4'\} \in E \\ &\Longrightarrow v_2' = v_4' \quad ; v_4 \text{ tiene solo un vecino} \\ &\Longrightarrow v_2 = v_4\end{aligned}$$

pero esto es una contradicción ya que v_2 y v_4 son dos vértices diferentes en el grafo.

Así, en ambos casos se tiene que $\left(\rho\left(g\right)\right)\left(v_4\right) \in \{v_1, v_4\}$.

Por lo tanto, $\left(\rho\left(g\right)\right)\left(\{v_1, v_4\}\right) \subset \{v_1, v_4\}$.

iii) Por otro lado, como tenemos el conjunto finito $\{v_1, v_4\}$ y como $\left(\rho\left(g\right)\right)\left(\{v_1, v_4\}\right)$ es inyectiva y sabemos que si tenemos una función inyectiva de un conjunto finito al mismo conjunto finito tal función inyectiva es también biyectiva, por lo tanto $\{v_1, v_4\} = \left(\rho\left(g\right)\right)\left(\{v_1, v_4\}\right)$.

Por lo tanto, $\left(\rho\left(g\right)\right)\left(\{v_1, v_4\}\right) = \{v_1, v_4\}$.

- $\left\{g v_2, g v_3\right\} = \{v_2, v_3\}$.

  Por lo anteriormente demostrado $g v_2 \neq v_1$ y $g v_2 \neq v_4$, de la misma manera $g v_3 \neq v_1$ y $g v_3 \neq v_4$, porque si alguno de ellos es v_1 ó v_4 tendrían una preimagen y ya sabemos que v_1 y v_4 tienen una preimagen (justamente v_1 ó v_4). Por lo que se tendría:

$$g v_2 = v_2 \text{ y } g v_3 = v_3$$
$$\text{ó}$$
$$g v_2 = v_3 \text{ y } g v_3 = v_2$$

  En ambos casos tenemos que $\left\{g v_2, g v_3\right\} = \{v_2, v_3\}$ por lo que se preserva la arista.

Se concluye que en este árbol al eliminar los vértices que tienen exactamente un vecino estaríamos quitando los vértices v_1, v_4 y nos quedaría el subgrafo $\left(V' = \{v_2, v_3\}, E' = \{\{v_2, v_3\}\}\right)$ y esta arista resultante sería estable con respecto a la acción.

Por lo tanto, para $|V| = 4$ existe una arista que se mantiene fija.

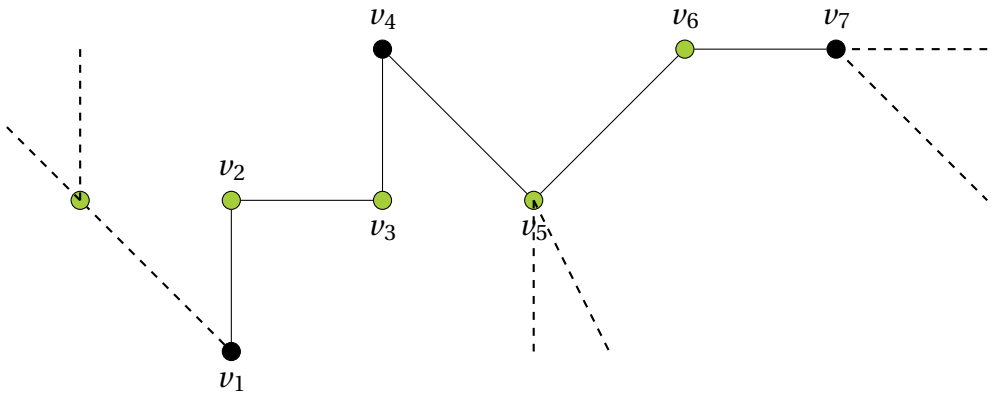
■

Ejemplo **2.24**

Cada subconjunto finito A de vértices de un árbol V se puede extender a un subárbol finito, esto se consigue al considerar todos los vértices de V que están en los caminos que unen dos vértices arbitrarios de A.

Análisis:

Sea V un árbol de un grupo finito G de la siguiente manera:



Tomemos el conjunto de vértices $\{v_1, v_4, v_7\}$.

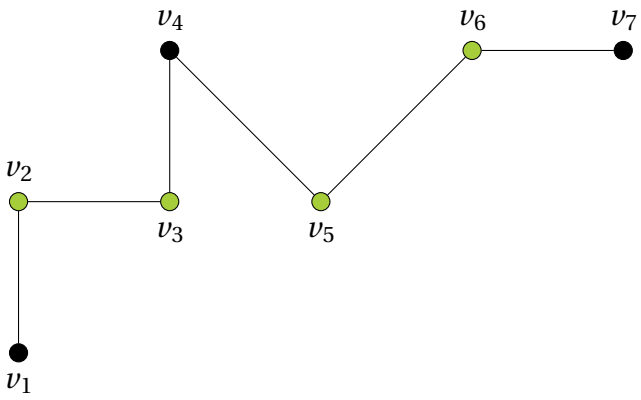
Al tomar solo los vértices aún no es un árbol porque necesitamos conectar los vértices por las aristas y formar el camino.

Ahora bien del árbol V sabemos que hay un camino entre v_1 y v_4 y lo mismo entre v_4 y v_7, así el conjunto de vértices $\{v_1, v_4, v_7\}$ lo extendemos a un árbol agregando todos los vértices que están en los caminos que conectan los vértices v_4, v_1 y v_4, v_7, es decir:

$$Ext(\{v_1, v_4, v_7\}) = (\{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}, \{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_4, v_5\}, \{v_5, v_6\}, \{v_6, v_7\})$$

donde, $\{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$ es el conjunto de vértices y también se tiene que el conjunto de aristas es: $\{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_4, v_5\}, \{v_5, v_6\}, \{v_6, v_7\}\}$.

A continuación se muestra el subárbol que hemos construido:



Así, $Ext\{v_1, v_4, v_7\}$ es un subárbol y es finito.

Luego, si a este subgrafo se le quitasen los vértices que solo tienen un vecino, los primeros candidatos son v_1 y v_7 tal que al quitarlos se obtiene un nuevo subgrafo al que se le puede

seguir quitando los vértices que solo tienen un vecino y así sucesivamente hasta obtener que v_4 es el vértice fijo.

■

Proposición 2.5 (Acciones de grupos finitos sobre árboles)

Si $|G| = n$ y $G \curvearrowright (V,E)$, entonces $V^G \neq \emptyset$ ó $\exists \{v,v'\} \in E : \{gv, gv'\} = \{v,v'\},\ \forall g \in G$. En otras palabras cada acción de un grupo finito en un árbol no vacío tiene un punto fijo global (es decir, un vértice o una arista en la que todos los elementos del grupo actúan trivialmente).

Demostración. Sea G un grupo finito y sea (V,E).

Como G es finito, entonces $G = \{g_1, g_2, \ldots, g_n\}$ (se puede enumerar). Entonces, por definición de órbita, la órbita de $v \in V$ está dada por:

$$G \cdot v = \{g_1 v, g_2 v, \ldots, g_n v\}$$

donde $\{g_1 v, g_2 v, \ldots, g_n v\}$ también es finito y $\{g_1 v, g_2 v, \ldots, g_n v\} \subset V$.

Sea $Ext(G \cdot v)$ el conjunto de todos los vértices de V que están en los caminos que unen dos vértices de $G \cdot v$, como se observa en el ejemplo anterior $Ext(G \cdot v)$ es un árbol.

Sea la acción

$$\begin{aligned} \rho : G &\longrightarrow \mathrm{Aut}(V,E) \\ g &\longmapsto \rho(g) : (V,E) \longrightarrow (V,E) \\ & \qquad\qquad v \longmapsto g \cdot v := (\rho(g))(v). \end{aligned}$$

Como $\rho(g)$ es un isomorfismo de grafos lo único que le hace al grafo es intercambiar los vértices preservando la estructura del grafo.

Ahora bien, el automorfismo que se considera es una biyección, por lo que $\rho(g)$ es una biyección, en donde se toma un vértice del árbol y lo lleva a otro elemento del mismo árbol, además, toma una arista $\{v,v'\}$ de E y lo lleva a $\{gv, gv'\}$ que es también una arista.

Ahora vamos a restringir $\rho(g)$ al subgrafo $Ext(G \cdot v)$ y vamos a determinar que es un automorfimso del grafo $Ext(G \cdot v)$. Debemos verificar que

$$\rho(g)|_{Ext(G \cdot v)} : Ext(Gv) \longrightarrow Ext(Gv).$$

sea una función biyectiva.

En primer lugar notemos que $\rho(g)$ es una isometría, entonces $\rho(g)$ es inyectiva, así que cualquier restricción es también inyectiva. Verifiquemos entonces si cumple la sobreyectividad: Probaremos primero que $(\rho(g))(Gv) = Gv$.

- $(\rho(g))(Gv) \subset Gv$.

  Partiendo del lado izquierdo tenemos:

  $$\begin{aligned}(\rho(g))(Gv) &= g \cdot Gv \\ &= \{gg_1v, gg_2v, \ldots, gg_nv\}\end{aligned}$$

  pero, $\{gg_1v, gg_2v, \ldots, gg_nv\} \subset \{g_1v, g_2v, \ldots, g_nv\} = Gv$, ya que $G = \{g_1, \ldots, g_n\}$.

  Por lo tanto, $(\rho(g))(Gv) \subset Gv$.

- $Gv \subset g \cdot Gv$.

  Sea $g_j \cdot v \in G \cdot v$.

  $$\begin{aligned}g^{-1}g_j \in G &\Longrightarrow g^{-1}g_j = g_k \text{ para algún } k = 1, \ldots, k \\ &\Longrightarrow gg^{-1}g_j = gg_k \\ &\Longrightarrow g_j = gg_k \\ &\Longrightarrow g_jv = gg_kv \in g \cdot G \cdot v\end{aligned}$$

  Por lo tanto, $Gv \subset g \cdot Gv$.

  Así, $(\rho(g))(Gv) = g \cdot Gv = Gv$. Esto último significa que $\rho(g)$ preserva Gv, y como $\rho(g)$ preserva subárboles, se tiene que: $(\rho(g))(Ext(Gv)) = Ext(Gv)$.

  Por lo tanto G actúa en el grupo finito $Ext(Gv)$.

  Ahora, por Lema 2.2, existe $v \in Ext(Gv)$ y como $Ext(Gv) \subset V$, así $v \in V$, además $(Ext(Gv))^G \subset V^G$, por lo que $v \in V^G$, así, $V^G \neq \emptyset$ ó $\exists \{v, v'\} \in E_v \subset E$ (donde E_v son aristas de $Ext(Gv)$) tal que $\{gv, gv'\} = \{v, v'\}, \forall g \in G$.

  Por lo tanto $V^G \neq \emptyset$ ó $\exists \{v, v'\} \in E : \{gv, gv'\} = \{v, v'\},\ \forall g \in G$

□

Proposición 2.6 (Contando órbitas)

Sea G un grupo que actúa sobre un conjunto X.

1. Si $x \in X$, entonces el mapeo,

$$\begin{aligned} A_x : G/G_x &\longrightarrow G \cdot x \\ g \cdot G_x &\longmapsto g \cdot x \end{aligned}$$

esta bien definida y es biyectiva. Aquí, G/G_x denota el grupo cociente de todas las clase laterales derecha de G_x en G, es decir, $G/G_x = \left\{ \; g \cdot G_x \;\middle|\; g \in G \; \right\}$

2. Además, el número de órbitas distintas es igual al promedio de la cantidad de puntos fijados por un elemento del grupo: es decir, si G y X son finitos, entonces,

$$|G \setminus X| = \frac{1}{|G|} \cdot \sum_{g \in G} \left| X^g \right|$$

Demostración. Sea $g_1, g_2 \in G$ distintos.

1. **i)** Demostraremos que A_x esta bien definida, es decir, que los valores en los subconjuntos no dependen de los representantes elegidos en G/G_x.

   Sea $g_1 \cdot G_x,\ g_2 \cdot G_x \in G/G_x$ tal que $g_1 \cdot G_x = g_2 \cdot G_x$.

   Si $g_1 \cdot G_x = g_2 \cdot G_x$, entonces existe un $h \in G_x$ con $g_1 = g_2 \cdot h$. Recordando, tenemos por la definición 2.17-ítem 1, que el grupo de estabilizadores de un elemento $x \in X$ con respecto a la acción esta dado por; $G_x := \left\{ \; g \in G \;\middle|\; g \cdot x = x \; \right\}$, entonces como $h \in G_x$, se cumple que $h \cdot x = x$.

$$\begin{aligned} h \cdot x = x &\Longrightarrow g_2 \cdot (h \cdot x) = g_2 \cdot x \\ &\Longrightarrow \left(g_2 \cdot h\right) \cdot x = g_2 \cdot x \\ &\Longrightarrow g_1 \cdot x = g_2 \cdot x \end{aligned}$$

   así, hemos probado que si $g_1 \cdot G_x = g_2 \cdot G_x$, entonces $g_1 \cdot x = g_2 \cdot x$ donde $g_1 \cdot x,\ g_2 \cdot x \in G \cdot x$, A_x esta bien definida.

   ii) Demostraremos que A_x es biyección.

   - **Inyectividad**. Sea $g_1 \cdot x,\ g_2 \cdot x \in G \cdot x$ tal que $g_1 \cdot x = g_2 \cdot x$,

$$\begin{aligned} g_1 \cdot x = g_2 \cdot x &\Longrightarrow x = g_1^{-1} \cdot g_2 \cdot x \\ &\Longrightarrow g_1^{-1} \cdot g_2 \in G_x \end{aligned}$$

luego, como $g_1^{-1} \cdot g_2 \in G_x$ obtenemos que, $g_2 \cdot G_x = g_1 \cdot G_x$. Hemos probado que sí $g_1 \cdot x = g_2 \cdot x$, entonces, $g_2 \cdot G_x = g_1 \cdot G_x$ donde $g_2 \cdot G_x,\ g_1 \cdot G_x \in G/G_x$, A_x es inyectiva.

- **Sobreyectividad**. Sea $g_1 \cdot x \in G \cdot x$.
  Para $g_1 \cdot x \in G \cdot x$, existe $g_1 \cdot G_x \in G/G_x$, tal que $A_x\left(g_1 \cdot G_x\right) = g_1 \cdot x$, así A_x es sobreyectiva.

Por lo tanto, A_x es biyectiva.

2. Consideremos el siguiente conjunto;

$$F := \left\{ \ (g,x) \ \middle| \ g \in G,\ x \in X,\ g \cdot x = x \ \right\} \subset G \times X$$

Ahora, probaremos que $|F| = \sum_{x \in X} |G_x|$ (a la izquierda) y que $|F| = \sum_{g \in G} \left|X^g\right|$ (a la derecha);

$$\begin{aligned} F &= \left\{ \ (g,x) \ \middle| \ g \in G,\ x \in X,\ g \cdot x = x \ \right\} \\ &= \bigcup_{x \in X} \left\{ \ (g,x) \ \middle| \ g \in G_x \ \right\} \\ &= \bigsqcup_{x \in X} G_x \times \{x\} \\ |F| &= \left| \bigsqcup_{x \in X} G_x \times \{x\} \right| \\ &= \sum_{x \in X} |G_x \times \{x\}| \\ &= \sum_{x \in X} |G_x| \times |\{x\}| \\ &= \sum_{x \in X} |G_x| \end{aligned}$$

$$\begin{aligned} F &= \left\{ \ (g,x) \ \middle| \ g \in G,\ x \in X,\ g \cdot x = x \ \right\} \\ &= \left\{ \ (g,x) \ \middle| \ g \in G,\ x \in X^g \ \right\} \\ &= \bigcup_{g \in G} \left\{ \ (g,x) \ \middle| \ x \in X^g \ \right\} \\ &= \bigsqcup_{g \in G} \{g\} \times X^g \\ |F| &= \left| \bigsqcup_{g \in G} X^g \right| \\ &= \sum_{g \in G} \left|X^g\right| \end{aligned}$$

así, hemos obtenido la siguiente igualdad:

$$\sum_{x \in X} |G_x| = |F| = \sum_{g \in G} \left|X^g\right|. \tag{2.3}$$

Por el teorema de Lagrange tenemos que se cumple; $|G/G_x| \cdot |G_x| = |G|$. Como $G \setminus X$ es finito, supongamos que, $|G \setminus X| = m$, entonces a $G \setminus X$ lo podemos enumerar. Digamos que $G \setminus X$ es de la forma;

$$G \setminus X = \{G \cdot x_1, \ldots, G \cdot x_m\}$$

pero G es finito así $|G \cdot x_i| = m_i$ (es finito), por ende $G \cdot x_i = \left\{x_1^{(1)}, \ldots, x_{m_i}^i\right\}$. Como $G \setminus X$ es partición de X, tendríamos que,

$$\begin{aligned} X = \bigcup_{i=1}^{m} G \cdot x_i \Longrightarrow X &= \bigcup_{i=1}^{m} \left\{x_j^{(i)}; j = 1, \ldots, m_i\right\} \\ \Longrightarrow X &= \left\{x_j^{(i)}; j = 1, \ldots, m_i; i = 1, \ldots, m\right\} \end{aligned}$$

Luego,

$$\sum_{x\in X}|G_x| = \sum_{x\in X}\frac{|G|}{|G/G_x|} \Longrightarrow \sum_{x\in X}|G_x| = \sum_{x\in X}\frac{|G|}{|G\cdot x|} \quad ; \text{ya que } |G/G_x| = |G\cdot x|$$

$$\Longrightarrow \sum_{x\in X}|G_x| = \sum_{i=1}^{m}\left(\sum_{j=1}^{m_i}\frac{|G|}{\left|G\cdot x_i^j\right|}\right)$$

$$\Longrightarrow \sum_{x\in X}|G_x| = \sum_{i=1}^{m}\left(\sum_{j=1}^{m_i}\frac{|G|}{|G\cdot x_i|}\right)$$

$$\Longrightarrow \sum_{x\in X}|G_x| = \sum_{i=1}^{m} m_i\frac{|G|}{|G\cdot x_i|}$$

$$\Longrightarrow \sum_{x\in X}|G_x| = \sum_{i=1}^{m}|G| \quad ; \text{ya que } |G\cdot x_i| = m_i$$

$$\Longrightarrow \sum_{x\in X}|G_x| = m|G| \quad ; \text{tenemos que } |G\setminus X| = m$$

$$\Longrightarrow \sum_{x\in X}|G_x| = |G\setminus X|\cdot|G|$$

entonces obtuvimos que $\sum_{x\in X}|G_x| = |G\setminus X|\cdot|G|$, pero por la igualdad 2.3, tenemos que;

$$\sum_{x\in X}|G_x| = \sum_{g\in G}\left|X^g\right| \Longrightarrow \sum_{g\in G}\left|X^g\right| = |G\setminus X|\cdot|G|$$

$$\Longrightarrow |G\setminus X| = \frac{1}{|G|}\sum_{g\in G}\left|X^g\right|$$

□

Las **acciones transitivas** sobre "espacios conexos" producen conjuntos generadores a través de "vecinos cercanos". Un primer ejemplo de este principio general es la Proposición 2.7, una versión métrica de este principio es el lema de Švarc-Milnor.

Definición 2.18 (Acción transitiva sobre un conjunto)
Una acción de grupo sobre un conjunto es transitiva si $|G\setminus X| = 1$.

Recordatorio:

Otra manera de definir que una acción es transitiva:
Si para todo $x, y \in X$ existe $g \in G$ tal que $y = g\cdot x$.
Además es equivalente decir que $X = G\cdot x, \forall x \in X$.

Vamos a caracterizar los grafos de Cayley en términos de acciones sobre grafos:

Proposición 2.7 (Las acciones en los grafos producen grafos de Cayley)

Sea G un grupo y sea G actúa sobre un grafo conexo $X = (V, E)$ por automorfismos de grafo. Si esta acción es libre y transitiva sobre el conjunto V de vértices de X y si $x \in V$, entonces el conjunto

$$S := \left\{ \; s \in G \;\middle|\; \{x, s \cdot x\} \in E \; \right\}$$

genera G y el grafo de Cayley $\mathrm{Cay}(G, S)$ es isomorfo a X.

Demostración. Definimos el mapeo de G en V, por la nota anterior podemos definir a V como $V = G \cdot x$ entonces:

$$\begin{aligned} \varphi : G &\longrightarrow V = G \cdot x \\ g &\longmapsto \varphi(g) = g \cdot x \end{aligned}$$

Probaremos que:

1. La acción en los vértices es biyectiva.

   - La acción G en V esta definida.
     Sea $g, h \in G$, tal que $g = b$. Tenemos:

     $$\begin{aligned} g = b &\Longrightarrow \rho(g) = \rho(h) \\ &\Longrightarrow \rho(g)(x) = \rho(h)(x) \qquad ; \text{para } x \in V \\ &\Longrightarrow g \cdot x = h \cdot x \end{aligned}$$

     Así, la acción G en V esta definida.
   - La acción G en V es inyectiva.
     Sea $g, h \in G$ tal que $g \cdot x = h \cdot x$.

     $$\begin{aligned} g \cdot x = h \cdot x &\Longrightarrow x = h^{-1} \cdot g \cdot x \\ &\Longrightarrow h^{-1} \cdot g \in G_x \\ &\Longrightarrow h^{-1} \cdot g = e \qquad ; \text{la acción es libre y } G_x \text{ es trivial} \\ &\Longrightarrow h = g \end{aligned}$$

     Así, la acción G en V es inyectiva.
   - La acción G en V es sobreyectiva.
     Sea $y \in V$, como la acción es transitiva existe $g \in G$ tal que $y = \varphi(g)$.
     Así, la acción G en V es sobreyectiva.

Por lo tanto la acción en los vértices es biyectiva.

2. El conjunto S genera a G.
   Tomemos $g \in G$.
   Como $X = (V, E)$ es conexo por definición existe por lo menos un camino $x = x_0, x_1, \ldots, x_n = g \cdot x$. Ahora, sea $g_j, s_j \in G$, $\forall\ 0 \leq j \leq n-1$ definido por:

$$g_j := \varphi^{-1}(x_j) \ \ y \ \ s_j := {g_j}^{-1} \cdot g_{j+1}; \text{ con } g_n := g. \tag{2.4}$$

   Como $x = x_0, x_1, \ldots, x_n = g \cdot x$ es un camino, entonces $\{x_j, x_{j+1}\}$ es una arista en X y como G actúa por automorfismos tenemos que ${g_j}^{-1} \cdot \{x_j, x_{j+1}\}$ es una arista en X (Ver figura 2.13), así usando ecuación 2.4:

$$\begin{aligned}
{g_j}^{-1} \cdot \{x_j, x_{j+1}\} &= \{{g_j}^{-1} \cdot x_j, {g_j}^{-1} \cdot x_{j+1}\} \\
&= \left\{\left(\varphi^{-1}(x_j)\right)^{-1} \cdot x_j, {g_j}^{-1} \cdot (g_{j+1} \cdot x)\right\} \\
&= \left\{\left(\varphi^{-1}(x_j)\right)^{-1} \cdot (g_j \cdot x), {g_j}^{-1} \cdot (g_{j+1} \cdot x)\right\} \\
&= \left\{\left(\varphi^{-1}(x_j)\right)^{-1} \cdot (\varphi^{-1}(x_j) \cdot x), ({g_j}^{-1} \cdot g_{j+1}) \cdot x\right\} \\
&= \left\{\left[\left(\varphi^{-1}(x_j)\right)^{-1} \cdot \varphi^{-1}(x_j)\right] \cdot x, s_j \cdot x\right\} \\
&= \{x, s_j \cdot x\}
\end{aligned}$$

   Así $\{x, s_j \cdot x\}$ es una arista en X entonces $s_j \in S$, por consiguiente:

$$\begin{aligned}
g = g_n &= g_0 \cdot g_0^{-1} \cdot g_1 \cdots g_{n-1} \cdot g_{n-1}^{-1} \cdot g_n \\
&= e \cdot s_0 \cdot s_1 \cdots s_{n-1}
\end{aligned}$$

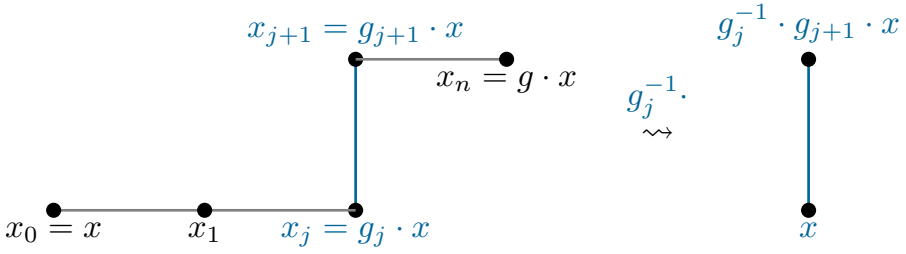


Figura 2.13. De caminos a palabras, usando una acción transitiva.

Por lo tanto S es un conjunto generador de G.

3. $\mathrm{Cay}(G,S)$ es isomorfo a X.
   Por ítem 1 se probó que φ es biyectiva en los vértices. Ahora probaremos que φ es biyectiva en las aristas, además que φ es isomorfismo en $\mathrm{Cay}(G,S)$ sobre X.

   Sea $g,h \in G$. usando la definición 2.5 tenemos que φ es una biyección tal que:

$$\begin{aligned}
\{g,h\} \in E_G &\iff \{\varphi(g),\varphi(h)\} \\
&\iff \{g\cdot x, h\cdot x\} \\
&\iff g^{-1}\cdot\{g\cdot x, h\cdot x\} && ;\ G \text{ actúa por automorfismos en } X \\
&\iff \{g^{-1}\cdot(g\cdot x), g^{-1}\cdot(h\cdot x)\} \\
&\iff \{(g^{-1}\cdot g)\cdot x, (g^{-1}\cdot h)\cdot x\} \\
&\iff \{e\cdot x, (g^{-1}\cdot h)\cdot x\} \\
&\iff \{x, (g^{-1}\cdot h)\cdot x\} \in E
\end{aligned}$$

   Así, por construcción de S tenemos que $g^{-1}\cdot h \in S$ y también que φ es biyectiva en las aristas.
   Por lo tanto $\mathrm{Cay}(G,S)$ es isomorfo a X.

□

Ahora nos encargaremos de mostrar que los grupos libres pueden caracterizarse geométricamente mediante acciones libres sobre árboles; recordemos que para una acción libre de un grupo sobre un grafo no se permite que ningún elemento de grupo no trivial fije ningún vértice o arista (Definición 2.15).

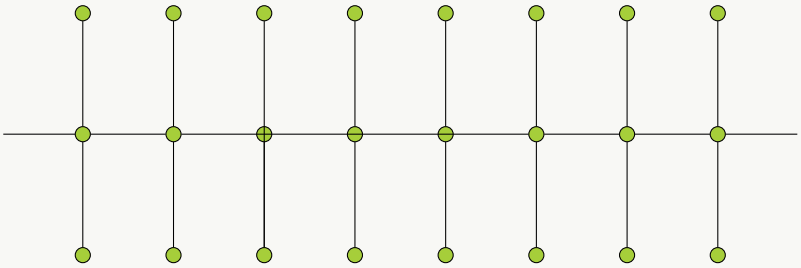
Los **Árboles de expansión para acciones grupales** son una generalización natural de los árboles de expansión de grafos.

Definición 2.19

Sea G un grupo que actúa sobre un grafo conexo X mediante automorfismos de grafo. Un **árbol de expansión** de esta acción es un subgrafo de X que es un árbol y que contiene exactamente un vértice de cada órbita de la acción G inducida en los vértices de X.

Ejemplo 2.25 **(Árboles de expansión)**

Consideremos la acción de $\mathbb{Z}$ "horizontal" en el árbol (infinito), representado en la figura. Entonces, el subgrafo red, es un árbol de expansión para esta acción.



Análisis: Tenemos que la acción de $\mathbb{Z}$ horizontal, esta dada como;

$$\begin{aligned}\rho : \mathbb{Z} &\longrightarrow \mathrm{Aut}\,(V,E)\\ n &\longrightarrow \rho\,(n) : (V,E) \longrightarrow (V,E)\\ &\qquad n \longmapsto \big(\rho\,(n)\big)\,(v) = n \cdot v\end{aligned}$$

es traslación horizontal de v n-veces hacia la izquierda si n es negativo y a la derecha si n es positivo . Para detallar más como funciona esta acción analicemos para $n = -1, 0, 1, 2 \in \mathbb{Z}$.

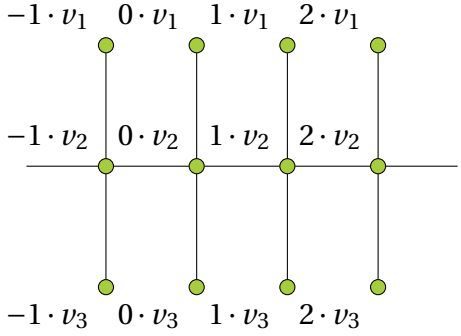
$$\begin{aligned}\rho\,(-1) : V &\longrightarrow V\\ v_1 &\longmapsto -1 \cdot v_1\\ v_2 &\longmapsto -1 \cdot v_2\\ v_3 &\longmapsto -1 \cdot v_3\end{aligned}$$

$$\begin{aligned}\rho\,(0) : V &\longrightarrow V\\ v_1 &\longmapsto 0 \cdot v_1\\ v_2 &\longmapsto 0 \cdot v_2\\ v_3 &\longmapsto 0 \cdot v_3\end{aligned}$$

$$\begin{aligned}\rho\,(1) : V &\longrightarrow V\\ v_1 &\longmapsto 1 \cdot v_1\\ v_2 &\longmapsto 1 \cdot v_2\\ v_3 &\longmapsto 1 \cdot v_3\end{aligned}$$

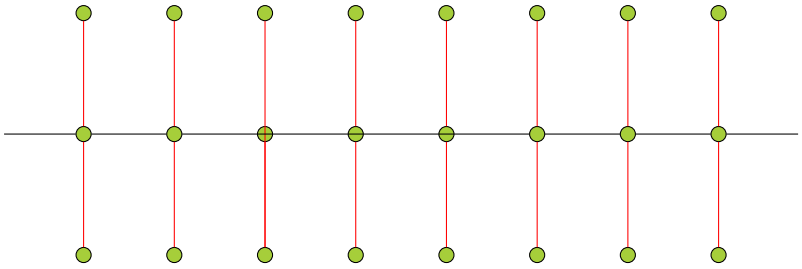
$$\begin{aligned}\rho\,(2) : V &\longrightarrow V\\ v_1 &\longmapsto 2 \cdot v_1\\ v_2 &\longmapsto 2 \cdot v_2\\ v_3 &\longmapsto 2 \cdot v_3\end{aligned}$$

tenemos tres órbitas en este grafo:



$$\begin{aligned}\mathbb{Z} \cdot v_1 &= \left\{ \; z \cdot v_1 \;\middle|\; z \in \mathbb{Z} \; \right\}\\ \mathbb{Z} \cdot v_2 &= \left\{ \; z \cdot v_2 \;\middle|\; z \in \mathbb{Z} \; \right\}\\ \mathbb{Z} \cdot v_3 &= \left\{ \; z \cdot v_3 \;\middle|\; z \in \mathbb{Z} \; \right\}\end{aligned}$$

por la definición 2.19, un árbol de expansión tiene que poseer exactamente un vértice de cada órbita, si observamos en la siguiente figura las líneas verticales de color rojo son los árboles de expansión en este grafo.



■

Teorema 2.3 (Existencia del árbol de expansión)

Toda acción de un grupo que actúa por automorfismo sobre un grafo conexo $X \neq \varnothing$ admite un árbol de expansión.

Demostración. Sea T_G el conjunto de todos los subárboles de X, donde cada subárbol de T_G contiene a lo sumo un vértice de cada órbita. Ahora, vamos a demostrar que T_G contiene un elemento maximal.

Tenemos que $\varnothing \in T_G$, entonces $\{\varnothing\} \subset T_G$, así $T_G \neq \varnothing$. En T_G, vamos a definir un orden parcial "$\leq$" donde $X' \leq X''$ si y solo si X' es un subárbol de X'' para $X', X'' \in T_G$.

Sea ζ una cadena de subárboles en T_G. Sea $Y = \bigcup_{X' \in \zeta} X'$, ahora vamos a demostrar que $Y \in T_G$, primero probaremos que Y es un árbol, es decir demostraremos que para cada par de vértices en Y existe exactamente un camino que conecta estos vértices para utilizar la proposición 2.1.

Sean $x_1,\ x_2 \in V_Y$ donde $V_Y = \bigcup_{X' \in \zeta} V_{X'}$.

Si $x_1,\ x_2 \in V_Y$ entonces existen $X',\ X'' \in T_G$ tal que $x_1 \in V_{X'}$ y $x_2 \in V_{X''}$ ($V_{X'}, V_{X''}$ son los vértices en $X',\ X''$ respectivamente). Como hemos definido el orden parcial "$\leq$", podríamos tener dos casos:

- $X' \leq X''$.

  $$x_1 \in V_{X'} \Longrightarrow x_1 \in V_{X''}$$
  $$\Longrightarrow x_1,\ x_2 \in V_{X''},\ \exists\ p \text{ un único camino de } x_1 \text{ a } x_2 \text{ ya que } X'' \text{ es un árbol}$$

  Como X'' es arbitrario, entonces $x_1,\ x_2 \in V_Y$, existe un único camino de x_1 a x_2, Y es un árbol.

- $X'' \leq X'$. La prueba es análoga al caso anterior.

por la proposición 2.1, Y es un árbol. Ahora, solo falta demostrar que Y contiene a lo sumo un vértice de cada órbita, pero esto es intuitivo ya que Y es la unión de subárboles que contienen a lo sumo un vértice de cada órbita y tomando en cuenta el orden parcial que se cumple $X' \leq X''$, decimos que Y es un árbol que contiene a lo sumo un vértice de cada órbita, $Y \in T_G$.

Y es una cota superior, por tanto, toda cadena de subárboles en T_G tiene una cota superior, que es; la unión de todos los subárboles en dicha cadena. Luego, por el lema de Zorn, decimos que T_G contiene un elemento maximal $T = (V_T, E)$, donde T es no vacío.

Vamos a demostrar que T es un árbol de expansión (por contradicción). Supongamos que T no es un árbol de expansión. Como T no es un árbol de expansión entonces no cumplen la definición 2.19, entonces, decimos que existe un vértice v tal que ningún elemento de la órbita $G \cdot v$ es un vértice de T , de otra forma ;

$$G \cdot v \cap V_T = \varnothing$$

Ahora vamos a demostrar que existe un vértice v_0 tal que $G \cdot v_0 \cap V_T = \varnothing$ y además, que existe $v_0' \in T_G$ tal que $\{v_0, v_0'\} \in E$.

Como X es conexo, entonces existe un camino p que conecta algún vértice u de T con v :

$$p : u, v_1, v_2, \ldots, v_n, v$$

Sea $v' = v_j$ donde $j = 1, \ldots, n$ el primer vértice que se encuentra en p que no esta en T, tenemos dos casos:

- Supongamos que ninguno de los vértices de $G \cdot v'$ está en T es decir, $G \cdot v' \cap V_T = \varnothing$. Como v' es el primer vértice en p que no esta en T, obtenemos que $v_{j-1} \in V_T$, así,

  $$\exists v_{j-1} \in V_T \text{ tal que } \{v_{j-1}, v_j\} \in E$$

  tomemos $v_0 = v_j \wedge v_0' = v_{j-1}$. Por tanto, hemos probado que el vértice v_0, cumple con la propiedad deseada.

- Ahora supongamos que $G \cdot v' \cap V_T \neq \varnothing$. Existe un $g \in G$ tal que $g \cdot v' \in G \cdot v'$, $g \cdot v' \in V_T$. Si p' denota el subcamino de p, $|p'| \leq |p|$, que inicia en $v' = v_j$ y termina en v;

  $$p' : v_j, \ldots, v_n, v$$

entonces, $g\cdot p' : g\cdot v_j,\ldots,g\cdot v_n, g\cdot v$; un camino que inicia en $g\cdot v' \in V_T$ y termina en $g\cdot v$, tal que $g\cdot v \notin V_T$ por lo que tenemos al inicio .

Sea $v'' = g\cdot v_i,\ i\in\{j,\ldots,n\}$ el primer vértice en $g\cdot p'$, tal que no esta en T; tendremos dos casos, así como hicimos para v'

- Supongamos que $G\cdot v''\cap V_T = \varnothing$.

  Como $v'' = g\cdot v_i$ es el primer vértice que no esta en $g\cdot p'$, obtenemos que $g\cdot v_{i-1}\in V_T$, así,

  $$\exists g\cdot v_{i-1}\in V_T \text{ tal que } \{g\cdot v_{i-1}, g\cdot v_j\}\in E$$

  tomemos $v_0 = g\cdot v_i \wedge v_0' = g\cdot v_{i-1}$. Por tanto, hemos probado que el vértice v_0, cumple con la propiedad deseada.

- Ahora supongamos que $G\cdot v''\cap V_T \neq \varnothing$

  Como el camino p' es más corto que p, si seguimos el proceso, eventualmente se encontrara un vértice con la propiedad deseada.

Sea $v_0\in G\cdot v_0$ tal que $G\cdot v_0\cap V_T\neq\varnothing$ y $\exists v_0'\in V_T/\{v_0', v_0\}\in E$. Como $v_0'\in V_T$ podemos crear un nuevo grafo, agregando la arista $\{v_0', v_0\}$;

$$T' = \left(V_{T'}, E'\right) \text{ donde } V_{T'} = V_T\cup\{v_0\} \text{ y } E' = E\cup\left\{v_0', v_0\right\}$$

como logramos notar T' se forma agregando el v_0 de la órbita $G\cdot v_0$, entonces T' sigue cumpliendo ser un árbol y además contiene a lo sumo un vértice de cada órbita, así $T'\in T_G$ y $T\leq T'$, esto contradice el hecho que T es maximal, por tanto, lo supuesto no es cierto. T es un árbol de expansión. □

Teorema 2.4 (Grupos libres y acciones sobre árboles)

Un grupo es libre si y solo si admite una acción libre en un árbol (no vacío).

Demostración. Iniciaremos la demostración de izquierda a derecha.

"$\Longrightarrow$" Si un grupo es libre, entonces admite una acción libre en un árbol (no vacío).

Sea F un grupo libre, generado libremente por S, $S\subset F$.

Por Teorema 2.1 sabemos que: si tenemos un grupo libre F finitamente generado por $S\subset F$, entonces el correspondiente grafo de Cayley $\mathrm{Cay}(F,S)$ es un árbol. Así, $\mathrm{Cay}(F,S)$ es un árbol.

Ahora consideremos la acción de traslación a la izquierda de F sobre $\mathrm{Cay}(F,S)$, debemos verificar que S no contiene elementos de orden 2. Por contradicción supongamos que si tiene elemento de orden 2, es decir, $\exists s \in S$ tal que $s \neq \epsilon$ y $ss = \epsilon$.

Considérese la función

$$\begin{aligned} f : S &\longrightarrow \mathbb{Z} \\ x &\longmapsto f(x) = 1 \end{aligned}$$

ahora bien, por la propiedad universal tendremos que:

$$\begin{array}{ccc} S & \xrightarrow{\quad f \quad} & \mathbb{Z} \\ \downarrow{\scriptstyle i} & \nearrow_{\overline{f}} & \\ F(S) & & \end{array}$$

como $ss = \epsilon$ y $\overline{f}$ es homomorfismo, pero todo homomorfismo manda la identidad hacia la identidad, entonces:

$$\begin{aligned} \overline{f}(ss) = \overline{f}(\epsilon) &\Longrightarrow \overline{f}(s) + \overline{f}(s) = 0 \\ &\Longrightarrow 2 = 0 \end{aligned}$$

lo cual es una contradicción. Por lo tanto, S no contiene elementos de orden 2.

Así, por la proposición 2.3 que nos dice que si tenemos un grupo y un conjunto generador libre de tal grupo, entonces la acción traslación a la izquierda sobre el grafo de Cayley de tal grupo y su generador, es libre si y solo si el conjunto generador no contiene elementos de orden 2. Entonces, bajo esta consideración la acción traslación a la izquierda es una acción libre en $\mathrm{Cay}(F,S)$.

Por lo tanto, si un grupo es libre, entonces admite una acción libre en un árbol (no vacío).

"$\Longleftarrow$"

Sea G un grupo que actúa libremente sobre un árbol T por automorfismos de grafos.

Por Teorema anterior que nos dice que cada acción de un grupo en un grafo conexo por automorfismos de grafo admite un árbol de expansión, entonces por dicho teorema existe un árbol de expansión T' para esta acción. Decimos que una arista de T se llama **esencial** si uno de sus vértices no pertenece a T', pero el otro vértice de la arista en cuestión pertenece a T'.

Como primer paso construimos un $S \subset G$ candidato para un conjunto generador libre de G: Sea e una arista esencial de T, la cual definimos como $e = \{u, v\}$, es decir que son vértices tales que u es vértice de T', pero v no es vértice de T'.

Como T' es un árbol de expansión sabemos que $\left|G_v \cap T'\right| = 1$, es decir que existe un elemento el cual es de la forma $gv \in T'$. Ahora bien, definamos $g_e = g^{-1}$. Sabemos que $g = \left(g^{-1}\right)^{-1}$, por lo tanto, existe $g_e \in G$ tal que $g_e^{-1} \cdot v$ es un vértice de T'.

Análogamente, como ya sabemos T' es un árbol y $g_e^{-1} v$ es un vértice de T', entonces al aplicar el isomorfismo g_e el cual es una acción de automorfismos tendremos que:

$$\begin{aligned} g_e^{-1} v \in T' &\Longrightarrow \left(\rho\left(g_e\left(g_e^{-1}\right)\right)\right)(v) \in g_e T' \\ &\Longrightarrow v \in g_e T' \end{aligned}$$

por lo tanto, se observa que $g_e \in G$ tal que v es un vértice de $g_e \cdot T'$.

El elemento g_e está determinado únicamente: supongamos que existen dos elementos g_e y g_e' tal que $v \in g_e T'$ y $v \in g_e' T'$. Entonces, se tendría que

$$g_e^{-1} v \in T' \quad \text{y} \quad \left(g_e'\right)^{-1} v \in T'$$

pero tales elementos estarían en la misma órbita y como la órbita Gv comparte un solo vértice con T' (y como G actúa libremente sobre T), entonces:

$$\begin{aligned} g_e^{-1} v = \left(g_e'\right)^{-1} v &\Longrightarrow g_e g_e^{-1} v = g_e \left(g_e'\right)^{-1} v \\ &\Longrightarrow v = g_e \left(g_e'\right)^{-1} v \\ &\Longrightarrow g_e \left(g_e'\right)^{-1} \in G_v \\ &\Longrightarrow g_e \left(g_e'\right)^{-1} = e_G \qquad ; G_v = \{e_G\} \text{ el estabilizador} \\ &\Longrightarrow g_e = g_e' \end{aligned}$$

Por lo tanto, g_e es el único que cumple la propiedad que: $\forall e = \{u, v\}$ donde $u \in T'$, $v \notin T'$, $\exists g_e$: $v \in g_e T'$.

Ahora, definamos el conjunto

$$\widetilde{S} = \left\{ \; g_e \in G \;\middle|\; e \text{ es una arista esencial de } T \; \right\}.$$

$\widetilde{S}$ cumple las siguientes propiedades:

1. Por definición $e_G \notin \widetilde{S}$: porque si estuviera el elemento neutro, entonces $e_G = g_e$ donde $e = \{u, v\}$ es una arista esencial de T ($u \in T'$, $v \notin T'$). Por tanto, $v \in g_e T' = e_G T' = T'$, y entonces se tendría que $v \in T'$ lo cual es una contradicción.

2. El conjunto $\widetilde{S}$ no contiene elementos de orden 2 : Razonando por contradicción supongamos que existe $g_e \neq e_G$ tal que $g_e^2 = e_G$. Entonces, como $g_e \neq e_G$ consideramos H definido como $H = \{e_G, g_e\}$ el cual es subgrupo de e_G.

   Ahora bien, la inclusión $i : H \longrightarrow G$ es homomorfismo. Consideremos

   $$\begin{aligned} \rho : G &\longrightarrow \mathrm{Aut}(T) \\ g &\longmapsto \rho(g) : T \longrightarrow T \\ & \qquad v \longmapsto (\rho(g))(v) = gv \end{aligned}$$

   y como tenemos la inclusión i al componerla con ρ tenemos que:

   $$\rho|_H : H \longrightarrow \mathrm{Aut}(T)$$

   es una acción de un grupo finito ya que H tiene 2 elementos.

   Ahora, como H es finito, por proposición 2.5 existe un punto fijo global, es decir, $\exists v_0 \in T : g_e v_0 = v_0$ ó $\exists \{v_1, v_2\} \in E : g_e \{v_1, v_2\} \in E$. Pero como la acción es libre (G actúa libremente en un árbol no vacío), entonces $g_e = e_G$, lo cual es absurdo.

   De modo que $\widetilde{S}$ no contiene elementos de orden 2.

3. Si e y e' son aristas esenciales tales que $g_e = g_{e'}$, entonces $e = e'$, (por que si $e \neq e'$ y dado que T es un árbol no pueden haber dos aristas diferentes que conecten el mismo subgrafo conexo T', y que se dé que $g_e T' = g_{e'} T'$).

4. Si $g \in \widetilde{S}$, así $g = g_e$ para alguna arista esencial $e = \{u, v\}$ tal que $u \in T', v \notin T'$, se tendría que hay un único g_e para el que $v \in g_e T'$ y como $g = g_e$, $g_e T' = g T'$ entonces $g^{-1} v \in T'$.

   Ahora bien, $g \neq e_G$, así:

   $$g^{-1} e = \{g^{-1} u, g^{-1} v\} \Longrightarrow g^{-1} e = \{g^{-1} v, g^{-1} u\}$$

   la cual es una arista esencial porque el primer elemento $g^{-1} v \in T'$ y $g^{-1} u$ no está en T' ya que T' es un árbol de expansión solo tiene un elemento de cada órbita.

   Además, $u \in T'$ y $g^{-1} u$ es otro elemento que está en la misma órbita que u, pero como la acción es libre dos elementos en la órbita son diferentes, así $g^{-1} u \notin T'$. Como $g^{-1} e$ es arista esencial de T, existe un único $g_{g^{-1} e}$ tal que $g^{-1} u \in g_{g^{-1} e} T'$, pero ya sabíamos

que $u \in T'$, entonces $g^{-1}u \in g^{-1}T'$ y por unicidad se tendría que $g^{-1} = g_{g^{-1}e}$, es decir, $g^{-1} \in \widetilde{S}$ ya que $g^{-1}e$ es arista esencial de T.

En particular, existe $S \subset \widetilde{S}$ tal que:

$$S \cap S^{-1} = \emptyset \text{ y también } 2|S| = \left|\widetilde{S}\right|$$

así, $|S| = \frac{|\widetilde{S}|}{2}$, ya que del ítem 3 sabemos que

$$\varphi : \{\text{Aristas esenciales de } T\} \longrightarrow \widetilde{S}$$
$$e \longmapsto \varphi(e) = g_e$$

es inyectiva y también sobreyectiva por definición de $\widetilde{S}$, así φ es biyección. Por ende,

$$\left|\widetilde{S}\right| = \text{ N° de aristas esenciales de } T.$$

Por lo tanto,

$$|S| = \tfrac{1}{2} \cdot (\text{N° de aristas esenciales de } T).$$

El conjunto $\widetilde{S}$ (y también S) genera al grupo G: Sea $g \in G$ y v un vértice de T'.

Como T es conexo, existe un camino p en T que une a v con $g \cdot v$, pues $v \in T'$ y $g \cdot v \notin T'$. El camino p pasa por diferentes copias de T':

Sea p el camino en T tal que $p : v_0, v_1, v_2, \ldots, v_{n-1}, v_n = gv$.

Entre los primeros vértices pueden haber muchos otros vértices que están en T' pero no en gT'; sea v_{j_1} el primer vértice en p tal que $v_{j_1} \notin T'$.

Si $v_{j_1} \in gT'$, entonces $v_{j_1}, v_{j_1+1}, v_{j_1+2}, \ldots, v_n = gv$ es un camino y como gT' es un árbol que contiene a v_{j_1} y gv, entonces existirá un camino en T' que conecta a v_{j_1} con gv y tal camino tendría que ser $v_{j_1}, v_{j_1+1}, v_{j_1+2}, \ldots, v_n = gv$, por la unicidad de caminos en un árbol, entonces $\forall\, j_1 \leq j \leq j_n\ , v_j \in gT'$.

Por lo tanto, $v_0, v_1, \ldots, v_{j_1-1} \in T'$ y $v_{j_1}, \ldots, v_n = gv \in gT'$. Es decir que p pasa por T' y gT'.

En caso contrario $v_{j_1} \notin gT'$. Como T' es un árbol de expansión contiene exactamente un elemento de cada órbita, así, la órbita del elemento v_{j_1} tiene uno en T', entonces $\exists g_1 \in G$: $v_{j_1} \in g_1 T'$, $g_1 \neq g$.

Sea el subcamino $p_1 : v_{j_1}, v_{j_1+1}, \ldots, v_{n-1}, v_n = gv$ de p tal que $v_{j_1} \in g_1 T'$ y sea v_{j_2} el primer vértice en p_1 tal que $v_{j_2} \notin g_1 T'$.

Si $v_{j_2} \in gT'$, entonces se tendría que el subcamino $p_2 : v_{j_2}, v_{j_2+1}, \ldots, v_n = gv$ es un camino en gT'. Así $v_0, v_1, \ldots, v_{j_1-1} \in T'$, $v_{j_1}, v_{j_1+1}, \ldots, v_{j_2-1} \in g_1T'$ y $v_{j_2}, \ldots, gv \in gT'$.

Por lo tanto, el camino p pasa por T', g_1T y gT'.

Caso contrario, si $v_{j_2} \notin gT'$, entonces $\exists g_2 \in G : v_{j_2} \in g_2T'$ donde $g_2 \neq g_1$.

Así, consideramos el camino $p_2 : v_{j_2}, v_{j_2+1}, \ldots, v_{n-1}, v_n = gv$ y si sigue el mismo proceso anteriormente descrito: Obtendremos que p pasa a través de algunas copias de T', digamos $g_0T', g_1T', \ldots, g_nT'$, donde $g_0 = e_G, g_i \neq g_{i+1},\ i = 0, \ldots, n-1$ y $g_n = g$.

Ahora, tomemos $j \in \{0, 1, \ldots, n-1\}$, como T' es un árbol de expansión y $g_j \neq g_{j+1}$ las copias $g_j \cdot T'$ y $g_{j+1} \cdot T'$ son unidas por una arista e_j. Por construcción sabemos que $v_{j_1} \in g_1T'$, entonces $v_{j_j} \in g_jT'$ y $v_{j_{j+1}} \in g_{j+1}T'$, a la arista formada por esos elementos la llamamos e_j, es decir, $e_j = \left\{v_{j_j}, v_{j_{j+1}}\right\}$. Luego

$$g_j^{-1}e_j = \left\{g_j^{-1}v_{j_j}, g_j^{-1}v_{j_{j+1}}\right\}$$

y como $v_{j_j} \in g_jT'$, entonces $g_j^{-1}v_{j_j} \in T'$ y $g_j^{-1}v_{j_{j+1}} \notin T'$.

Verificaremos que $g_j^{-1}v_{j_{j+1}} \notin T'$**:** Por contradicción supongamos que $g_j^{-1}v_{j_{j+1}} \in T'$.

Si $g_j^{-1}v_{j_{j+1}} \in T'$, entonces $g_j^{-1} = g_{j+1}^{-1}$. Por otro lado sabemos que $v_{j_{j+1}} \in g_{j+1}T'$, entonces $g_{j+1}^{-1}v_{j_{j+1}} \in T'$, lo cual implicaría que $g_j = g_{j+1}$, de ambas situaciones tenemos que:

$$g_j^{-1} = g_{j+1}^{-1} \quad \text{y} \quad g_j = g_{j+1}$$

lo cual es una contradicción. Por lo tanto, $g_j^{-1}v_{j_{j+1}} \notin T'$, es decir, $g_j^{-1}e_j$ es esencial.

Ahora bien, ya sabemos que $v_{j_{j+1}} \in g_{j+1}T'$, entonces $g_j^{-1}v_{j_{j+1}} \in g_j^{-1}g_{j+1}T'$, pero por definición de $\widetilde{S}$ el elemento $g_j^{-1}g_{j+1}$ es elemento de $\widetilde{S}$.

Por lo tanto, $g_j^{-1} \cdot e_j$ es una arista esencial y el elemento $g_j^{-1}g_{j+1}$ del grupo correspondiente se encuentra en $\widetilde{S}$.

Luego, definamos $s_j := g_j^{-1} \cdot g_{j+1}$, entonces:

$$g_j^{-1} \cdot g_{j+1} \in \widetilde{S} \Longrightarrow s_j \in \widetilde{S}.$$

Ahora partimos de que $g = g_n$, entonces:

$$\begin{aligned} g = g_n &= e \cdot g_n \\ &= e^{-1} \cdot g_n \end{aligned}$$

teníamos que

$$\begin{aligned} g = e^{-1} \cdot g_n \Longrightarrow g &= g_0^{-1} \cdot g_n \\ &= g_0^{-1} \cdot e \cdot e \cdots e \cdot g_n \\ &= g_0^{-1} \cdot g_1 \cdot g_1^{-1} \cdot g_2 \cdot g_2^{-1} \cdots g_{n-1} \cdot g_{n-1}^{-1} \cdot g_n \\ &= s_0 \cdot s_1 \cdots s_{n-1} \end{aligned}$$

Así, $\widetilde{S}$ es generador de G. Por lo que S es generador de G.

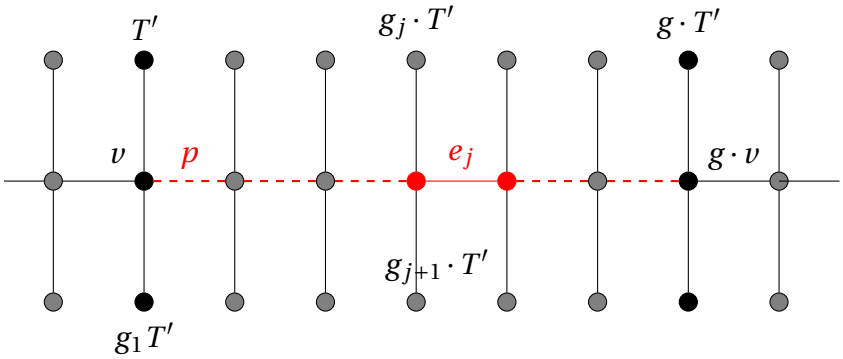


Figura 2.14. El conjunto $\widetilde{S}$ genera a G

El conjunto S es un conjunto generador libre de G: Utilizando el teorema 2.2 debemos probar que $\mathrm{Cay}(G,S)$ no contiene ciclos.

Por contradicción supongamos que contiene un ciclo, así existe $n \in \mathbb{N}$ tal que $n \geq 3$ y $g_0, \ldots, g_{n-1}$ es un ciclo en $\mathrm{Cay}(G,S) = \mathrm{Cay}\left(G, \widetilde{S}\right)$.

Por definición de grafos de Cayley los elementos

$$s_j = g_j^{-1} \cdot g_{j+1}, \ \forall\, j \in \{0, 1, \ldots, n-2\}$$

y

$$s_{n-1} = g_{n-1}^{-1} \cdot g_0.$$

están en $\widetilde{S}$.

Ahora, para cada $j = 1, \ldots, n$ sea e_j una arista esencial que conecta las copias T' y $s_j \cdot T'$.

Supongamos que e_j es de la forma $e_j = \{w_j, z_j\}$, en donde $w_j \in T'$ y $z_j \in s_j T'$. Y definamos $w_n = w_0, z_n = z_0$ y $g_n = g_0$.

Luego, si multiplicamos e_j por g_j, tenemos:

$$g_j e_j = \{g_j w_j, g_j z_j\}$$

la cual es una arista porque e_j es una arista y $g_j w_j \in g_j T'$, $g_j z_j \in g_{j+1} T'$. Además, $g_{j+1} e_{j+1}$ es de la forma $g_{j+1} e_{j+1} = \{g_{j+1} w_{j+1}, g_{j+1} z_{j+1}\}$, en donde

$$g_{j+1} w_{j+1} \in g_{j+1} T' \ , g_{j+1} z_{j+1} \in g_{j+2} T'$$

Ahora bien, se puede observar que $g_j z_j$ y $g_{j+1} w_{j+1}$ están en $g_{j+1} T'$ y ya que cada copia de T' es un subgrafo conexo, podemos conectar las aristas utilizando los vértices, es decir, conectar las aristas

$$g_j \cdot e_j \text{ y } g_j \cdot s_j \cdot e_{j+1} = g_{j+1} \cdot e_{j+1}$$

donde $g_j \cdot s_j \cdot e_{j+1} \in g_{j+1} \cdot T'$, por un camino en $g_{j+1} T'$. Ya que $g_{j+1} T'$ es árbol existe un camino, llamemosle q_j que conecta los vértices $g_j z_j$ y $g_{j+1} w_{j+1}$. Entonces, se tendrá el camino $r_j : g_j w_j,\ q_j,\ g_{j+1} w_{j+1}$ que va de $g_j T'$ hacia $g_{j+1} T'$.

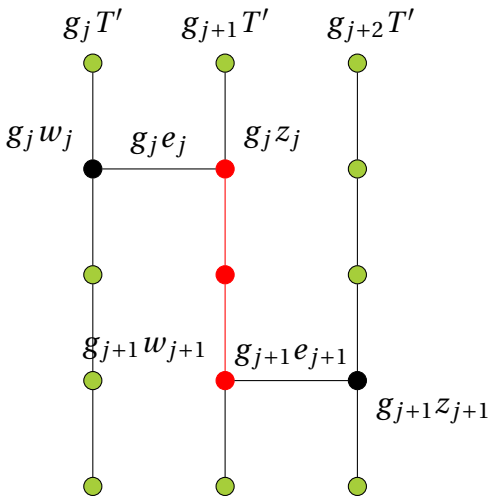


Figura 2.15. Ciclos en $\mathrm{Cay}(G, \widetilde{S})$ conducen a ciclos en T.

Al concatenar los caminos $r_0, r_1, \ldots, r_{n-1}$ se obtiene un camino r que conecta $g_0 w_0$ con $g_n w_n$,

es decir, tendremos un ciclo porque r comienza en $g_0 w_0$ y termina en $g_n w_n$ y sabemos que $g_n = g_0$, entonces terminaría en el mismo vértice completando un ciclo.

Por lo tanto, r es ciclo en T, pero esto es una contradicción ya que T es un árbol.

Así, el conjunto S es un conjunto generador libre de G.

□

Proposición 2.8 (Caracterización de árboles finitos)

Sea $X = (V, E)$ un grafo conexo finito con $V \neq \emptyset$. Demostrar que X es un árbol si y solo si

$$|E| = |V| - 1.$$

Demostración. "$\Longrightarrow$" Si X es un árbol finito, entonces $|E| = |V| - 1$.

Sea X el árbol con n vértices, probaremos que X tiene $n-1$ aristas. Procedemos por inducción:

- Para $n = 1$.

$$\begin{aligned} n = 1 &\Longrightarrow |E| = |V| - 1 \\ &\Longrightarrow |E| = 1 - 1 \\ &\Longrightarrow |E| = 0 \end{aligned}$$

  Por lo tanto, se cumple para $n = 1$.

- Se quiere demostrar que se cumple para los $n > 1$.

  Suponga que se cumple para todos los árboles con $k < n$ vértices, es decir,

$$|V| = k < n.$$

  Ahora se demostrará que se cumple para $|V| = n$. Pero antes se verificará que se puede quitar una arista de un árbol de manera que queden dos grafos separados.

  Tómese el árbol $X = (V, E)$ y suponga que no existe un vértice que forme parte de una única arista, es decir,

$$\forall\, v \in V, v \in \{w, v\} \in E \text{ y } v \in \{t, v\} \in E.$$

Considérese el vértice $v_0 \in V$. Si $v_0 \in V$ entonces $v_0 \in \{v_0, s\} \in E$ para algún $s \in V$.

Ahora, sea $v_1 \in V$ tal que $v_1 = s$, entonces $v_0 \in \{v_0, v_1\}$. Por hipótesis v_1 estará en al menos dos aristas, entonces considérese la arista $\{v_1, v_2\}$ tal que $v_1 \in \{v_1, v_2\}$, donde $\{v_1, v_2\} \neq \{v_0, v_1\}$. Luego, por hipótesis v_2 estará en al menos dos aristas, así podemos considerar la arista $\{v_2, v_3\}$ tal que $v_2 \in \{v_2, v_3\}$, es decir, $v_2 \in \{v_1, v_2\}$ y $v_2 \in \{v_2, v_3\}$ donde $\{v_1, v_2\} \neq \{v_2, v_3\}$.

De la misma manera se puede seguir construyendo hasta v_k tal que $v_k \in \{v_j, v_k\}$ y $v_k \in \{v_k, v_n\}$, donde $\{v_j, v_k\} \neq \{v_k, v_n\}$ y $j < k < n$, tal que se construya un camino de vértices.

Ahora bien, como el grado del árbol es finito por el principio del palomar en algún momento se pasará por un vértice por el que se haya pasado antes y así tener un ciclo, pero eso no puede pasar en un árbol, por lo que habría una contradicción. Por lo que en un árbol siempre existirá un vértice con una única arista.

Por lo tanto, al quitar una arista de un árbol finito resultan dos árboles separados.

Ahora, ya sabemos que existe el vértice v tal que existe una única arista A en E donde $v \in A$, es decir, $A = \{v, v'\} \in E$. Si quitamos tal vértice del grafo (V, E), por lo demostrado anteriormente tenemos dos grafos separados.

Sean (V', E') y (V'', E'') tales grafos conexos separados, donde

$$|V'| = \{v\} \text{ y } |V''| = V - \{v\}$$

para los cuales se cumple la hipótesis de inducción. Así,

$$|V''| = n - 1 < n$$

y como se ha quitado un vértice, entonces:

$$|E'| = \emptyset \text{ y } |E''| = E - \{A\}$$

Luego, por hipótesis de inducción se tiene que:

$$|V''| = n - 1 < n \Longrightarrow |E''| = n - 2$$

entonces, para E tendremos que:

$$\begin{aligned} E = |E''| + 1 &\Longrightarrow E = n - 2 + 1 \\ &\Longrightarrow E = n - 1 \end{aligned}$$

y se tiene lo que se requería demostrar.

Por lo tanto, si X es un árbol finito, entonces $|E| = |V| - 1$.

"$\Longleftarrow$" Si un grafo conexo tiene n vértices y $n-1$ aristas, entonces es un árbol.

Sea $X=(V,E)$ el grafo conexo de n vértices y $n-1$ aristas. Por contradicción suponga que X no es un árbol, es decir, que si X no es un árbol entonces existirá un ciclo.

Ahora bien, si tomamos una arista tal que se quita del grafo puede ocurrir que, resulte un grafo que contenga ciclos o un nuevo grafo el cual sea conexo para el que cada par de vértices puede ser conectado por un camino. Así que si surge un grafo que contenga ciclo quitamos otra arista y obtenemos un nuevo grafo con los mismos casos anteriores.

Se puede seguir el mismo proceso de tomar aristas y quitarlas del grafo de tal manera que se obtiene un grafo conexo de n vértices y aristas $n-k$ con $k>1$, el cuál será un árbol por construcción ya que en dicho proceso se va eliminando la posibilidad de que tenga un ciclo, es decir, se ha ido "rompiendo" el grafo para que no tenga ciclo, de tal manera que hay exactamente un camino entre dos vértices cualesquiera.

Ahora bien, se ha llegado a tener un árbol con n vértices y $n-k$ aristas (con $k>1$), pero tal cosa genera una contradicción a lo que se demostró en la implicación anterior de que todo árbol con n vértices tiene $n-1$ aristas.

Por lo tanto si $X=(V,E)$ es un grafo conexo con n vértices y $n-1$ aristas, entonces X es un árbol.

Así, X es un árbol finito si y solo si $|E|=|V|-1$.

□

Corolario 2.2 (Teorema de Nielsen- Schreier)
Los subgrupos de grupos libres son libres.

Demostración. Sea F un grupo libre, existe T un árbol no vacío tal que $F \curvearrowright T \neq 0$ que actúa libremente, es decir, sea φ un mapeo definido por:

$$\begin{aligned} \varphi : F \times T &\longrightarrow T \\ (f, v) &\longmapsto f \cdot v \end{aligned}$$

Ahora, sea G un subgrupo de F.
Definimos el mapeo $\varphi|_{G\times T}$ como:

$$\begin{aligned} \varphi|_{G\times T} : G \times T &\longrightarrow T \\ (g, v) &\longmapsto \varphi(g, v) = g \cdot v \end{aligned}$$

Por teorema 2.4 G actúa libremente sobre un árbol no vacío.
Por tanto G es un grupo libre.
Así, los subgrupos de grupos libres son libres.

□

Corolario 2.3 (Teorema de Nielsen-Schreir, versión cuantitativa)
Sea F un grupo libre de rango $n \in \mathbb{N}$ y sea $G \subset F$ un subgrupo de índice $k \in \mathbb{N}$. Entonces G es un grupo libre de rango $k(n-1)+1$. En particular, los subgrupos de índice finito de grupos libres de rango finito son finitamente generados.

Demostración. Sea S un conjunto generador libre de F y sea $T := \mathrm{Cay}(F,S)$.

Si $T := \mathrm{Cay}(F,S)$ entonces es un árbol ya que S es el generador y F es un grupo libre. Además, la acción de traslación a la izquierda de F sobre T es también libre.

Ahora, la acción de traslación a la izquierda del subgrupo $G \subset T$ es libre y como $G \subset T$, entonces G es también libre. Por la demostración del Teorema 2.4 tenemos que

$$\text{rank } (G) = |E|/2$$

donde $|E| = N$ř de aristas esenciales de la acción G en T.

Ahora, se calculará $|E|$:

Sea T' un árbol de extensión de la acción de G sobre T; como $G \subset F$ es un subgrupo de índice $k \in \mathbb{N}$, entonces $[F:G] = k$.

Ahora,

$$\begin{aligned} |G \setminus T| &= \frac{1}{|G|} \sum_{g \in G} \left| T^G \right| \\ &= \frac{1}{|G|} \sum_{g \in G} \left| \mathrm{Cay}(F,S) \right| \qquad \text{; ya que } T := \mathrm{Cay}(F,S) \end{aligned}$$

Pero sabemos que $X^g = \left\{ \; x \in X \;\middle|\; g \cdot x = x \; \right\}$, entonces en nuestro caso

$$\mathrm{Cay}(F,S)^g = \left\{ \; x \in F \;\middle|\; g \cdot x = x \; \right\}$$

y como G es subgrupo de F la operación en $g \cdot x$ es la multiplicación de grupo; así, para que $g \cdot x = x$ suceda es necesario que $g = e_F$.

Entonces:

$$\mathrm{Cay}(F,S)^g = \left\{ \; x \in F \;\middle|\; g \cdot x = x \; \right\} = \begin{cases} \emptyset, & \text{si } g \neq e_F \\ F, & \text{si } g = e_F \end{cases}$$

Luego, por proposición 2.6 sabemos que $|G \setminus X| = \frac{1}{|G|} \sum_{g \in G} \left| X^g \right|$, en nuestro caso tenemos:

$$\left| G \setminus \mathrm{Cay}(F,S) \right| = \frac{1}{|G|} \sum_{g \in G} \left| \mathrm{Cay}(F,S)^g \right|$$

Ahora, dado que G es subgrupo de F, el neutro de G es el mismo neutro de F, entonces $e_G = e_F$, así:

$$\left| G \setminus \mathrm{Cay}(F,S) \right| = \tfrac{1}{|G|} \left| \mathrm{Cay}(F,S)^{e_F} \right|$$

y como $\mathrm{Cay}(F,S) = F$ si $g = e_F$, entonces

$$\tfrac{1}{|G|} \left| \mathrm{Cay}(F,S)^{e_F} \right| = \tfrac{|F|}{|G|}$$

pero $\frac{|F|}{|G|} = [F : G] = k$, entonces $\frac{|F|}{|G|} = k$.

Por lo tanto, $\left| G \setminus \mathrm{Cay}(F,S) \right| = \frac{|F|}{|G|} = k$, es decir, el conjunto de órbitas.

Luego, por definición sabemos que la cardinalidad de T' es igual al número de órbitas y el número de órbitas es $\left| G \setminus \mathrm{Cay}(F,S) \right|$ pero hemos llegado a $\left| G \setminus \mathrm{Cay}(F,S) \right| = \frac{|F|}{|G|} = k$, así, se deduce que T' tiene exactamente k vértices.

Para un vértice v en T denotamos por $d_T(v)$ el grado de v en T, es decir, el número de vecinos de v en T.

Como T es regular, todos los vértices tienen el mismo grado $2 \cdot |S| = 2 \cdot n$ y obtenemos (donde $V(T')$ denota el conjunto de vértices de T').

Así,

$$\begin{aligned} \sum_{v \in V(T')} d_T(v) &= \sum_{v \in V(T')} 2 \cdot |S| \\ &= \sum_{v \in V(T')} 2 \cdot n \end{aligned}$$

seguimos

$$\begin{aligned}\sum_{v\in V(T')} 2\cdot n &= 2\cdot n\cdot \sum_{v\in V(T')} 1\\ &= 2\cdot n\cdot \underbrace{(1+1+1+\cdots+1)}_{k-\text{ veces}}\\ &= 2\cdot n\cdot k\end{aligned}$$

Luego, como T' es un árbol finito con k vértices sabemos que T' tiene entonces $k-1$ aristas.

Por otro lado, ya que las aristas de T' son contadas dos veces cuando sumamos los grados de los vértices de T', obtenemos:

$$2\cdot n\cdot k = \sum_{v\in V(T')} d_T(v) = 2(k-1)+E$$

donde E es el número de aristas esenciales, así por lo anterior:

$$\begin{aligned}\sum_{v\in V(T')} d_T(v) = 2\cdot n\cdot k &\Longrightarrow 2\cdot n\cdot k = 2(k-1)+E\\ &\Longrightarrow 2\cdot n\cdot k - 2(k-1) = E\\ &\Longrightarrow E = 2\cdot n\cdot k - 2k + 2\\ &\Longrightarrow E = 2(k(n-1)+1)\end{aligned}$$

y como rank $G = |E|/2$, se tiene que:

$$\begin{aligned}\text{rank } G &= \frac{2(k(n-1)+1)}{2}\\ &= k(n-1)+1\end{aligned}$$

Es decir, que el rango de G es $k(n-1)+1$.

Por lo tanto, G es un grupo libre de rango $k(n-1)+1$.

En particular, si tenemos H un subgrupo de índice finito de un grupo libre, dicho subgrupo H también será libre y de rango $k(n-1)+1$. Entonces, H tendrá $k(n-1)+1$ generadores libres, es decir, es finitamente generado. □

Corolario 2.4

Si F es un grupo libre de rango al menos 2 y $n\in\mathbb{N}$, entonces existe un subgrupo de F que es libre de rango finito al menos n.

Demostración. Por hipótesis se tiene que F es un grupo libre de rango al menos 2, es decir que $|S| \geq 2$, entonces existe s en S y podemos definir la función

$$\begin{aligned} f : S &\longrightarrow \mathbb{Z}_k = \left\{\overline{0}, \ldots, \overline{k-1}\right\} \\ x &\longmapsto \overline{1} \end{aligned}$$

Además, como F es libremente generado por S existe $\overline{f}$, el único homomorfismo de F hacia $\mathbb{Z}_k$ tal que

$$\begin{aligned} \varphi = \overline{f} : F &\longrightarrow \mathbb{Z}_k \\ s^j &\longmapsto \varphi\left(s^j\right) = \underbrace{\varphi(s) + \cdots + \varphi(s)}_{j-\text{veces}} = \overline{j} \end{aligned}$$

que es sobreyectiva porque si se toma la clase de $\overline{j}$ como ya sabemos que existen al menos 2 elementos en S, entonces se da que $\varphi(s) + \cdots + \varphi(s)$. Y como es sobreyectiva por el primer teorema de Isomorfismo tendremos que

$$F \setminus \ker\ \varphi \cong \mathbb{Z}_k \Longrightarrow \left|F \setminus \ker\ \varphi\right| \cong |\mathbb{Z}_k|$$

donde $|\mathbb{Z}_k| = k$.

Luego, como G es de índice finito consideremos $G = \ker\ \varphi$, entonces $[F : G] = k$. Así, por Teorema de Nielsen versión cuantitativa tendremos que

$$\begin{aligned} \text{rank } G &= k(n-1) + 1 \geq n \\ &= k(n-1) \geq n - 1 \\ k &\geq 1 \end{aligned}$$

Por lo tanto, el subgrupo G de F es libre de rango finito al menos n.

□

Corolario 2.5

Los subgrupos de índice finito de grupos generados finitamente, son generados finitamente.

Demostración. Sea G un grupo generado finitamente y sea H un subgrupo de G de índice finito. Probaremos que H es generado finitamente.

Como G es un grupo generado finitamente, por el corolario 1.2, existe $\pi : F(S) \longrightarrow G$ sobreyectivo, donde $F(S)$ es el grupo libre generado por S, con $S < \infty$.

Sea H' una preimagen de H bajo π. Si H' una preimagen de H bajo π entonces H' es un subgrupo de $F(S)$. Ahora vamos a probar que el índice de H' en $F(S)$ es igual al índice de H en G:

$$\left[F(S) : H'\right] = [G : H] \tag{2.5}$$

para concluir que el índice de H' es finito. Definamos $\psi : F(S)/H' \to G/H$, como tenemos que $H' = \pi^{-1}(H)$, ψ queda de la siguiente manera

$$\begin{aligned} \psi : F(S)/\pi^{-1}(H) &\longrightarrow G/H \\ xH' &\longmapsto \pi(x)H. \end{aligned}$$

La idea es demostrar que ψ es un isomorfismo, para que sea inmediato probar la igualdad 2.5.

Probemos que ψ esta bien definida.

Sean $x_1H',\ x_2H' \in F(S)/\pi^{-1}(H)$, tal que $x_1H' = x_2H'$.

$$\begin{aligned} x_1H' = x_2H' &\Longrightarrow x_2^{-1}x_1 \in H' \\ &\Longrightarrow x_2^{-1}x_1 \in \pi^{-1}(H) \\ &\Longrightarrow \pi\left(x_2^{-1}x_1\right) \in H \\ &\Longrightarrow \pi(x_1)H = \pi(x_2)H \\ &\Longrightarrow \psi\left(x_1H'\right) = \psi\left(x_2H'\right) \end{aligned}$$

por tanto, ψ esta bien definida.

Probaremos que ψ es un homomorfimos. Sean $x_1H',\ x_2H' \in F(S)/\pi^{-1}(H)$

$$\begin{aligned} \psi\left(x_1H'x_2H'\right) &= \psi\left(x_1x_2H'\right) \\ &= \pi(x_1x_2)H \\ &= \pi(x_1)\pi(x_2)H \qquad ;\ \pi \text{ es homomorfismo} \\ &= \pi(x_1)H\pi(x_2)H \\ &= \psi\left(x_1H'\right)\psi\left(x_2H'\right) \end{aligned}$$

por tanto, ψ es un homomorfismo.

Ahora demostraremos que ψ es biyección.

- **Inyectividad.** Probaremos que el $K(\psi) = e$ en este caso $K(\psi) = \{H'\}$, sea $xH' \in F(S)/\pi^{-1}(H)$

$$\begin{aligned}\psi\left(xH'\right) = H &\Longrightarrow \pi(x)\, H = H \\ &\Longrightarrow \pi(x) \in H \\ &\Longrightarrow x \in \pi^{-1}(H) \\ &\Longrightarrow x \in H' \\ &\Longrightarrow xH' = H'\end{aligned}$$

  por tanto $K(\psi) = \{H\}$, ψ es inyectiva.

- **Sobreyectividad.** Sea $yH \in G/H$.

  Como $y \in G$, entonces $y = \pi(x)$

$$\begin{aligned}yH \in G/H &\Longrightarrow \pi(x)H \in G/H \\ &\Longrightarrow \pi(x)H = \psi(xH')\end{aligned}$$

  así, para todo $yH \in G/H$, $\exists xH' \in F(S)/\pi^{-1}(H)$, tal que $\psi\left(xH'\right) = yH$, ψ es sobreyectiva.

Por lo tanto, ψ es biyección. Tenemos que la función ψ es un homomorfismo isomorfo, entonces obtenemos que;

$$\left[F(S) : \pi^{-1}(H)\right] = [G : H] \Longrightarrow \left[F(S) : H'\right] = [G : H]$$

Como hipótesis tenemos que el índice de H en G es finito $[G : H]$, entonces por la igualdad 2.5 que hemos demostrado podemos concluir que el índice de H' en $F(S)$ es finito, $\left[F(S) : H'\right] = k < \infty$

$$\begin{aligned}\left|\frac{F(S)}{H'}\right| < \infty &\Longrightarrow \text{rank } H' = k\,(|S| - 1) + 1, \infty \qquad \text{; por el corolario 2.3} \\ &\Longrightarrow H' \text{ es finitamente generado}\end{aligned}$$

H' es finitamente generado ya que rank H' es finito asi existe un S_H finito que genera a H', asi, $|S_H| = \text{rank } H'$. Luego, tenemos que $\pi(S_H)$ genera a H, $\langle \pi(S_H) \rangle_G = H$, entonces H es generado finitamente.

□

Capítulo 3

Cuasi-isometría

La importancia de la teoría geométrica de grupo es estudiar a los grupos como objetos geométricos por ende en el capítulo 2 se introduce un grupo G y se asocia un conjunto generador S esto forma lo que son los grafos de Cayley; entonces el principal objetivo de este presente capítulo es poder introducir ese grupo G y asociarlo al conjunto generador S estableciendo una estructura de espacio métrico, es decir:
Si G es un grupo y S un conjunto generador de G, entonces los caminos en el grafo de Cayley asociado, induce una métrica en G, esta métrica es llamada: métrica de la palabra con respecto al conjunto generador S (se hace unas respectivas restricciones en G del grafo de Cayley). Esta métrica mide la longitud más corta posible de un camino entre dos elementos de G en el grafo de Cayley, desafortunadamente, en general la métrica depende del conjunto generador seleccionado.

Para obtener una noción de geometría sobre un grupo, independientemente de la elección de conjuntos generadores, pasamos a la geometría a gran escala; por consecuencia, llegamos a tal noción para grupos finitos de tipo cuasi-isométrico, que es fundamental para la teoría geométrica de grupo.

En este apartado, se presentan algunas generalidades de isometrías y cuasi-isometrías, además, se aplican estos conceptos a los grupos finitamente generados y finalmente se demuestra el lema de Švarc-Milnor, el cual es la clave para unir a la teoría geométrica de grupo con la geometría usual.

3.1. Tipos de cuasi-isometría de espacios métricos

A continuación, consideramos diferentes niveles de similitud entre espacios métricos, definiremos: isometrías, equivalencias bilipschitz y cuasi-isometrías. Intuitivamente, queremos una noción geométrica de similitud a gran escala, es decir, espacios para ser equivalentes si parecen ser iguales cuando se miran desde lejos.

Evidentemente, definimos el concepto más importante de la matemática moderna:

Definición 3.1 (Espacio métrico)

Un **espacio métrico** (X, d) está formado por un conjunto X y un mapeo d que esta definido como $d : X \times X \longrightarrow \mathbb{R}_{\geq 0}$ satisfaciendo las siguientes condiciones:

- $d(x, y) \geq 0$ para todo $x, y \in X$, con $d(x, x) = 0$ y $d(x, y) > 0$ si $x \neq y$.
- Para todo $x, y \in X$ tenemos $d(x, y) = 0$ si y solo si $x = y$.
- Para todo $x, y \in X$ tenemos $d(x, y) = d(y, x)$.
- Para todo $x, y, z \in X$ la desigualdad triangular cumple que:

$$d(x, z) \leq d(x, y) + d(y, z).$$

Recordatorio:

En algunas ocasiones hablaremos simplemente de un espacio métrico X, sin hacer referencia a la función distancia, la que genéricamente es denotada con d.

Empezamos con el tipo más fuerte de similitud entre espacios métricos:

Definición 3.2 (Isometría)

Sea $f : X \longrightarrow Y$ un mapeo entre los espacios métricos (X, d_X) y (Y, d_Y).

- Decimos que f es un **embebimiento isométrico** si

$$\forall x, x' \in X \quad d_Y(f(x), f(x')) = d_X(x, x')$$

- El mapeo f es una **isometría** si es un embebimiento isométrico y si existe un embebimiento isométrico $g : Y \longrightarrow X$ tal que

$$f \circ g = id_Y \quad \text{y} \quad g \circ f = id_X$$

En otras palabras, una isometría no es más que un embebimiento isométrico biyectivo.

- Dos espacios métricos son **isométricos** si existe una isometría entre ellos.

Recordemos la definición de homeomorfismo y continuidad dada en espacios métricos:

Definición 3.3 (Homeomorfismo)

Sea $f : X \longrightarrow Y$ es un homeomorfismo si f es biyectiva, continua y su inversa f^{-1} tambien es continua.

Definición 3.4 (Continuidad)

Sean $(X, d_X), (Y, d_Y)$ espacios métricos. Una función $f : X \longrightarrow Y$ es continua en un punto $a \in X$ si para cada $\epsilon > 0$ existe $\delta > 0$ tal que si $d_X(a, x) < \delta$ entonces $d_Y\left(f(a), f(x)\right) < \epsilon$.

Ejemplo **3.1**

- Cada embebimiento isométrico es inyectivo.
- Cada isometría es un homeomorfismo.

Análisis:

Primero. Sea un mapeo f, entre espacios métricos X e Y, definimos:

$$\begin{aligned} f &: X \longrightarrow Y \\ x, y &\longmapsto d_Y\left(f(x), f\left(y\right)\right) = d_X\left(x, y\right) \end{aligned}$$

Entonces probaremos que f es inyectiva.

Sea $x, y \in X$ tal que $f(x) = f\left(y\right)$.

$$\begin{aligned} f(x) = f\left(y\right) &\Longrightarrow d_Y\left(f(x), f\left(y\right)\right) = 0 \\ &\Longrightarrow d_X\left(x, y\right) = 0 \\ &\Longrightarrow x = y \end{aligned}$$

$\therefore$ f es inyectiva
Así, cada embebimiento isométrico es inyectivo.

Segundo. Probaremos que si $f : X \longrightarrow Y$ es una isometría entre los espacios X e Y entonces f es homeomorfismo. Usamos definición 3.3 tenemos:
i) Probaremos que f es biyectivo.

- f es inyectiva.
  Por ítem anterior se probó que f es inyectiva.
  $\therefore$ f es inyectiva.

- f es sobreyectiva.
  Sea $y \in Y$, usando definición 3.2-ítem 2 tenemos que $g(y) \in X$ así
  $f \circ g = id_Y$.

$$\begin{aligned} f \circ g = id_Y &\Longrightarrow (f \circ g)(y) = id_Y(y) \\ &\Longrightarrow f(g(y)) = y \\ &\Longrightarrow f(x) = y \qquad ; \text{tomamos } x = g(y) \end{aligned}$$

  $\therefore$ f es sobreyectiva.

Así, f es biyectiva.

ii) Probaremos que f es continua.
Sea $\epsilon > 0$, probemos que $\exists\, \delta > 0$ tal que $d_X(x,y) < \delta$ entonces $d_Y(f(x), f(y)) < \epsilon$ (definición 3.4).
Tomemos $\delta = \epsilon$ así $d_Y(f(x), f(y)) = d_X(x,y) < \delta$ entonces $d_Y(f(x), f(y)) < \epsilon$, así f es continua.

iii) Probaremos que f^{-1} es continua.
Sea $\epsilon > 0$, probemos que $\exists\, \delta > 0$ tal que si $d_Y(x,y) < \delta$ entonces $d_X(f^{-1}(x), f^{-1}(y)) < \epsilon$.
Como f es isometría por definición 3.2, así:

$$\begin{aligned} d_X(f^{-1}(x), f^{-1}(y)) &= d_Y(f(f^{-1}(x)), f(f^{-1}(y))) \\ &= d_Y(x,y) \end{aligned}$$

tomamos $\delta = \epsilon$. Si $d_X(f^{-1}(x), f^{-1}(y)) = d_Y(x,y) < \delta$ entonces $d_X(f^{-1}(x), f^{-1}(y)) < \epsilon$. Por lo que, f^{-1} es continua.

Así, cada isometría f es un homeomorfismo.

■

La noción de isometría es muy rígida (demasiado rígida para nuestros propósitos), es por esta razón que queremos una noción de "similitud" para espacios métricos que solo

refleja la forma a gran escala del espacio, pero no los detalles locales. Un primer paso es debilitar la condición de isometría permitiendo un error multiplicativo uniforme, se presenta la siguiente definición:

Definición 3.5 (Equivalencia Bilipschitz).

Sea $f : X \longrightarrow Y$ un mapeo entre espacios métricos (X, d_X) y (Y, d_Y).

- Decimos que f es un **embebimiento bilipschitz** si existe una constante $c \in \mathbb{R}_{>0}$ tal que
$$\forall x, x' \in X \quad \frac{1}{c} \cdot d_X(x, x') \leq d_Y(f(x), f(x')) \leq c \cdot d_X(x, x')$$
- El mapeo f es una **equivalencia bilipschitz** si es un embebimiento de bilipschitz y si existe un embebimiento bilipschitz $g : Y \longrightarrow X$ tal que
$$f \circ g = id_Y \quad \text{y} \quad g \circ f = id_X$$
- Dos espacios métricos se denominan **equivalente bilipschitz** si existe una equivalencia bilipschitz entre ellos.

Ejemplo **3.2**

- Cada embebimiento bilipschitz es inyectiva.
- Y cada equivalencia bilipschitz es un homeomorfismo.
- Además, un embebimiento bilipschitz es una equivalencia bilipschitz si y solo si es biyectiva.

Análisis: Sea $f : X \longrightarrow Y$ un mapeo entre espacios métricos (X, d_X) y (Y, d_Y).

Primero. Verificamos que cada embebimiento bilipschitz es inyectivo: Sean $x, x' \in X$ tales que $f(x) = f(x')$.

Si $f(x) = f(x')$, entonces $d_Y(f(x), f(x')) = 0$. Ahora, de la definición de equivalencia bilipschitz sabemos que existe una constante $c \in \mathbb{R}_{>0}$ tal que se cumple lo siguiente:

$$\forall x, x' \in X \quad \frac{1}{c} \cdot d_X(x, x') \leq d_Y(f(x), f(x')) \leq c \cdot d_X(x, x')$$

pero $d_Y(f(x), f(x')) = 0$, así se tiene que:

$$\forall x, x' \in X \;\; \frac{1}{c} \cdot d_X\left(x, x'\right) \leq 0 \leq c \cdot d_X\left(x, x'\right)$$

es decir, que $\frac{1}{c} \cdot d_X\left(x, x'\right) \leq 0$, pero por definición $c > 0$ y sabemos que la distancia siempre es mayor que 0, así resulta que:

$$d_X\left(x, x'\right) = 0 \implies x = x'$$

Por lo tanto, la función es inyectiva.

Segundo. Ahora probaremos que un embebimiento de bilipschitz es continuo.

Considerando la desigualdad de la definición 3.5-ítem 1 en donde sabemos que existe una constante $c \in \mathbb{R}_{>0}$ tal que

$$\forall x, x' \in X \;\; \frac{1}{c} \cdot d_X\left(x, x'\right) \leq d_Y\left(f(x), f\left(x'\right)\right) \leq c \cdot d_X\left(x, x'\right)$$

Por otra parte, usaremos un teorema que nos dice: Sea $f : X \longrightarrow Y$ y sea X e Y metrizables con distancias d_X y d_Y, respectivamente. Entonces la continuidad de f es equivalente a exigir que dados $x \in X$ y $\epsilon > 0$, existe $\delta > 0$ tal que : $d_X\left(x, y\right) < \delta \Longrightarrow d_Y\left(f(x), f\left(y\right)\right) < \epsilon$.

Tomemos $\delta = \frac{\epsilon}{c}$, de la desigualdad de la definición 3.5-ítem 1 tenemos que:
$d_Y\left(f(x), f\left(x'\right)\right) \leq c \cdot d_X\left(x, x'\right)$, entonces $d_X\left(x, x'\right) < \delta$.

Ahora bien,

$$\begin{aligned} d_X\left(x, x'\right) < \delta &\Longrightarrow \frac{1}{c} \cdot d_Y\left(f(x), f\left(x'\right)\right) \leq d_X\left(x, x'\right) < \delta \\ &\Longrightarrow c \cdot \frac{1}{c} \cdot d_Y\left(f(x), f\left(x'\right)\right) \leq c \cdot d_X\left(x, x'\right) < c \cdot \delta \\ &\Longrightarrow d_Y\left(f(x), f\left(x'\right)\right) \leq c \cdot d_X\left(x, x'\right) < \epsilon \\ &\Longrightarrow d_Y\left(f(x), f\left(x'\right)\right) < \epsilon \end{aligned}$$

así se cumple el enunciado del teorema . Por lo tanto, f es continua.

Luego, por definición sabemos que en este caso existe una inversa que es bilipschitz, es decir, una inversa que es inyectiva y que es continua, así f será biyectiva, continua y con inversa continua, por lo tanto es un homeomorfismo.

Tercero. Con lo anterior también se tiene que si un embebimiento bilipschitz es una equivalencia bilipschitz entonces es biyectiva, solo resta probar que si es biyectiva enton-

ces es equivalencia. Como f es biyectiva tiene inversa g, debemos verificar que $g : Y \longrightarrow X$ también es bilipschitz.

Sean $y, y' \in Y$.
Si $y, y' \in Y$, entonces $g(y), g(y') \in X$; como f es embebimiento bilipschitz existe $c > 0$ tal que

$$\frac{1}{c} \cdot d_X(g(y), g(y')) \leq d_Y(f(g(y)), f(g(y'))) \leq c \cdot d_X(g(y), g(y'))$$

y dado que g es la inversa de f tenemos:

$$f(g(y)) = y \quad \text{y} \quad f(g(y')) = y'$$

así,

$$\frac{1}{c} \cdot d_X(g(y), g(y')) \leq d_Y(y, y') \leq c \cdot d_X(g(y), g(y'))$$

luego:

$$\begin{aligned} \frac{1}{c} \cdot d_Y(y, y') &\leq \frac{1}{c} \cdot (c \cdot d_X(g(y), g(y'))) \\ &= d_X(g(y), g(y')) \end{aligned}$$

y por lo anterior tenemos que:

$$\frac{1}{c} \cdot d_X(g(y), g(y')) \leq d_Y(y, y') \Longrightarrow d_X(g(y), g(y')) \leq c \cdot d_Y(y, y')$$

así,

$$\frac{1}{c} \cdot d_Y(y, y') \leq d_X(g(y), g(y')) \leq c \cdot d_Y(y, y')$$

y de acuerdo con la definición se cumple que g es bilipschitz.

■

Las equivalencias bilipschitz también preservan todos los detalles que estamos buscando para que represente las propiedades a gran escala. Como paso siguiente y final, permitimos un error aditivo uniforme:

Definición 3.6 (Cuasi-isometría)

Sea $f : X \longrightarrow Y$ un mapeo entre espacios métricos (X, d_X) y (Y, d_Y).

- El mapeo f es un **embebimiento cuasi-isométrico** si existen constantes

$c \in \mathbb{R}_{>0}$ y $b \in \mathbb{R}_{>0}$ tal que f es un embebimiento (c,b)-cuasi-isométrico, es decir,

$$\forall x, x' \in X \ \ \frac{1}{c} \cdot d_X\left(x, x'\right) - b \leq \ d_Y\left(f\left(x\right), f\left(x'\right)\right) \leq c \cdot d_X\left(x, x'\right) + b$$

- Un mapeo $f' : X \longrightarrow Y$ tiene una **distancia finita** de f si existe un $c \in \mathbb{R}_{>0}$ con

$$\forall x \in X \ d_Y\left(f\left(x\right), f'\left(x\right)\right) \leq c.$$

- Sea $f : X \longrightarrow Y$ un mapeo entre espacios métricos. Decimos que $g : Y \longrightarrow X$ es **cuasi-inverso** de f si existe c tal que para todo $y \in Y$ tenemos

$$d_Y\left(f \circ g\left(y\right), y\right) \leq c$$

De manera similar, para todo $x \in X$ tenemos que

$$d_X\left(g \circ f\left(x\right), x\right) \leq c$$

- El mapeo f es una **cuasi-isometría** si f es un embebimiento cuasi-isométrico para el cual existe un embebimiento cuasi-isométrico cuasi-inverso, es decir, si existe un embebimiento cuasi-isométrico $g : Y \longrightarrow X$ tal que $g \circ f$ tiene una distancia finita de id_X y $f \circ g$ tiene una distancia finita de id_Y.
- Los espacios métricos X e Y son **cuasi-isométricos** si existe una cuasi-isometría $X \longrightarrow Y$; en este caso escribimos $X \sim_{Qi} Y$.

Ejemplo **3.3**

Cada isometría es una equivalencia bilipschitz, y cada equivalencia bilipschitz es una cuasi-isometría.

Análisis: De la definición de cuasi-isometría tenemos la siguiente desigualdad:

$$\forall x, x' \in X, \ \ \frac{1}{c} \cdot d_X\left(x, x'\right) - b \leq d_Y\left(f\left(x\right), f\left(x'\right)\right) \leq c \cdot d_X\left(x, x'\right) + b$$

Si consideramos $b = 0$ en tal desigualdad, tenemos que:

$$\forall x, x' \in X, \ \ \frac{1}{c} \cdot d_X\left(x, x'\right) - 0 \leq d_Y\left(f\left(x\right), f\left(x'\right)\right) \leq c \cdot d_X\left(x, x'\right) + 0$$

Es decir,

$$\forall x, x' \in X, \quad \frac{1}{c} \cdot d_X(x, x') \leq d_Y(f(x), f(x')) \leq c \cdot d_X(x, x')$$

un embebimiento bilipschitz. Además si $b = 0$ y $c = 1$ tenemos que:

$$\forall x, x' \in X, \quad \frac{1}{1} \cdot d_X(x, x') \leq d_Y(f(x), f(x')) \leq 1 \cdot d_X(x, x') \Longrightarrow d_X(x, x') \leq d_Y(f(x), f(x')) \leq d_X(x, x')$$
$$\Longrightarrow d_X(x, x') = d_Y(f(x), f(x'))$$

$\forall x, x' \in X$, f es una isometría.

Se puede notar que todo embebimiento isométrico es un embebimiento bilipschitz y todo embebimiento bilipschitz es un embebimiento cuasi-isométrico.

■

Ejemplo 3.4

- Todos los espacios métricos no vacíos de diámetro finito son cuasi-isométricos: el diámetro de un espacio métrico (X, d) es

$$\operatorname{diam} X := \sup_{x,y \in X} (x, y).$$

- Por otro lado, si un espacio es cuasi-isométrico a un espacio de diámetro finito, entonces también tiene diámetro finito. Entonces, el espacio métrico $\mathbb{Z}$ (con la métrica inducida sobre $\mathbb{R}$) es no cuasi-isométrico a un espacio métrico de diámetro finito.

Análisis:

Primero. Sea X e Y espacios métricos no vacíos con diámetro finito, es decir, diam X y diam Y finitos.

Consideramos f un mapeo cualquiera:

$$f : X \longrightarrow Y$$
$$x \longmapsto y_0$$

demostraremos que f es cuasi-isométrico.
Usamos la definición 3.6-ítem 4, tomemos cualquier mapeo

$$g : Y \longrightarrow X$$
$$y \longmapsto x_0$$

un embebimiento cuasi-isométrico.
Existen c y b en $\mathbb{R}_{>0}$, definimos $c=1$ y $b=\text{diam } X+\text{diam } Y$ tal que $\forall x,x'\in X$, entonces

$$\begin{aligned}\frac{1}{c}\cdot d_X\left(x,x'\right)-b &= 1\cdot d_X\left(x,x'\right)-\left(\text{diam } X+\text{diam } Y\right)\\ &= \left(d_X\left(x,x'\right)-\text{diam } X\right)-\text{diam } Y\\ &\leq d_Y\left(f\left(x\right),f\left(x'\right)\right)\\ &\leq \text{diam } Y\\ &\leq d_X\left(x,x'\right)+\text{diam } X+\text{diam } Y\\ &= c\cdot d_X\left(x,x'\right)+b\end{aligned}$$

De modo que, f es un embebimiento cuasi-isométrico.
Luego, por definición 3.6-ítem 2; $f\circ g: Y\longrightarrow Y$ a una distancia finita de $id_Y: Y\longrightarrow Y$ es

$$d_Y\left(\left(f\circ g\right)\left(y\right),id_Y\left(y\right)\right)\leq \text{diam } Y=c'.$$

De igual manera, $g\circ f: X\longrightarrow X$ a una distancia finita de $id_X: X\longrightarrow X$ es

$$d_X\left(\left(g\circ f\right)\left(x\right),id_X\left(x\right)\right)\leq \text{diam } X=c'.$$

Entonces, por la definición 3.6-ítem 4 se cumple que f es cuasi-isométrico.
Así, todos los espacios métricos no vacíos de diámetro finito son cuasi-isométricos.

Segundo. Sea X un espacio cuasi-isométrico a un espacio Y de diámetro finito.
Si X es un espacio cuasi-isométrico a Y, entonces existe f una cuasi-isometría, es decir, para $x,x'\in X$,

$$\forall x,x'\in X\ \ \frac{1}{c}\cdot d_X\left(x,x'\right)-b\leq\ d_Y\left(f\left(x\right),f\left(x'\right)\right)\leq c\cdot d_X\left(x,x'\right)+b$$

analicemos por separado la siguiente desigualdad (la otra es de manera análoga)

$$\frac{1}{c}\cdot d_X\left(x,x'\right)-b\leq\ d_Y\left(f\left(x\right),f\left(x'\right)\right)\Longrightarrow d_X\left(x,x'\right)\leq c\cdot d_Y\left(f\left(x\right),f\left(x'\right)\right)+c\cdot b$$

Si Y es finito, entonces $d_Y\left(f\left(x\right),f\left(x'\right)\right)$ es finito así $c\cdot d_Y\left(f\left(x\right),f\left(x'\right)\right)+c\cdot b$ es finita; por lo que $d_X\left(x,x'\right)$ es finito, lo que nos lleva a que X es finito y posee diámetro finito.

■

Podemos dar una caracterización alternativa de las cuasi-isometrías; para esto, considere la siguiente definición:

Definición 3.7 (Imagen cuasi-densa)

Un mapeo $f : X \longrightarrow Y$ tiene una **imagen cuasi-densa** si existe una constante $c \in \mathbb{R}_{>0}$ tal que

$$\forall y \in Y, \exists x \in X \; d_Y(f(x), y) \leq c.$$

Proposición 3.1 (Caracterización alternativa de cuasi-isometría)

Un mapeo $f : X \longrightarrow Y$ entre espacios métricos (X, d_X) y (Y, d_Y) es una cuasi-isometría si y solo si es un embebimiento cuasi-isométrico con imagen cuasi-densa.

Demostración. "$\Longleftarrow$" Si f es un embebimiento cuasi-isométrico con imagen cuasi-densa entonces f es una cuasi-isometría.

Sea f un embebimiento cuasi-isométrico con imagen cuasi-densa, existe una constante $c \in \mathbb{R}_{>0}$ tal que

$$\forall x, x' \in X \quad \frac{1}{c} \cdot d_X(x, x') - c \leq d_Y(f(x), f(x')) \leq c \cdot d_X(x, x') + c \tag{3.1}$$

y

$$\forall y \in Y, \exists x \in X \quad d_Y(f(x), y) \leq c.$$

Ahora, por el axioma de elección, existe un mapeo g definido por:

$$\begin{aligned} g : Y &\longrightarrow X \\ y &\longmapsto g(y) = x_y \end{aligned}$$

tal que para cada $y \in Y$, tomamos un elemento x_y con $d_Y(f(x_y), y) \leq c$.
Luego, probemos que el mapeo g es cuasi-inverso de f, entonces por construcción: $\forall y \in Y$ tenemos

$$d_Y(f \circ g(y), y) = d_Y(f(x_y), y) \leq c \tag{3.2}$$

Notemos que $f \circ g$ tiene una distancia finita con respecto al mapeo identidad id_Y, esto por definición 3.6-ítem 4.
Por otra parte, $\forall x \in X$ como f es un embebimiento cuasi-isométrico, tenemos

$$\begin{aligned} d_X(g \circ f(x), x) &= c \cdot d_Y(f(g(f(x))), f(x)) + c^2 \\ &= c \cdot d_Y(f(x_{f(x)}), f(x)) + c^2 \\ &\leq 2 \cdot c^2 \end{aligned}$$

Así, $g \circ f$ tiene una distancia finita con respecto al mapeo identidad id_X, esto por definición 3.6-ítem 4.

Ahora, probaremos que g es un embebimiento cuasi-isométrico.
Sabemos que existe una constante c, además sean $y, y' \in Y$. Entonces:

$$\begin{aligned} d_X\left(g\left(y\right), g\left(y'\right)\right) &= d_X\left(x_y, x_{y'}\right) \\ &\leq c \cdot d_Y\left(f\left(x_y\right), f\left(x_{y'}\right)\right) + c^2 \\ &\leq c \cdot \left[d_Y\left(f\left(x_y\right), y\right) + d_Y\left(y, y'\right) + d_Y\left(f\left(x_{y'}\right), y'\right)\right] + c^2 \\ &= c \cdot \left[d_Y\left(y, y'\right) + 2 \cdot c\right] + c^2 && \text{; por ecuación 3.2} \\ &\leq c \cdot d_Y\left(y, y'\right) + 2 \cdot c^2 + c^2 \\ &= c \cdot d_Y\left(y, y'\right) + 3 \cdot c^2 \end{aligned}$$

Dados $y, y' \in Y$ tales que $g\left(y\right) = x$ y $g\left(y'\right) = x'$ tenemos que $d_Y\left(f\left(x\right), y\right) \leq c$ y $d_Y\left(f\left(x'\right), y'\right) \leq c$, por lo que:

$$\begin{aligned} d_Y\left(y, y'\right) &\geq d_Y\left(f\left(x\right), y\right) + d_Y\left(f\left(x\right), f\left(x'\right)\right) + d_Y\left(f\left(x'\right), y'\right) \\ &= c + d_Y\left(f\left(x\right), f\left(x'\right)\right) + c \\ &\geq 2 \cdot c + c \cdot d_X\left(x, x'\right) + c && \text{; por ecuación 3.1} \\ &\geq c \cdot d_X\left(x, x'\right) + 3 \cdot c \end{aligned}$$

Entonces, multiplicamos la desigualdad anterior por -1:

$$\begin{aligned} -d_Y\left(y, y'\right) &\geq -c \cdot d_X\left(x, x'\right) - 3 \cdot c \\ -d_Y\left(y, y'\right) + 3 \cdot c &\geq -c \cdot d_X\left(x, x'\right) \\ \frac{1}{c} \cdot d_Y\left(y, y'\right) - \frac{3 \cdot c}{c} &\leq d_X\left(g\left(y\right), g\left(y'\right)\right) \\ \frac{1}{c} \cdot d_Y\left(y, y'\right) - 3 &= d_X\left(g\left(y\right), g\left(y'\right)\right) \end{aligned}$$

Tomando ambas desigualdades $\nu = \max\left\{3 \cdot c^2, 3\right\}$ y usando 3.1 obtenemos:

$$\frac{1}{c} \cdot d_Y\left(y, y'\right) - \nu \leq d_X\left(g\left(y\right), g\left(y'\right)\right) \leq c \cdot d_Y\left(y, y'\right) + \nu$$

Así, g es un embebimiento cuasi-isométrico, se cumplen las condiciones dadas en la definición 3.6-ítem 4 y efectivamente f es una cuasi-isometría.

"$\Longrightarrow$" Si f es una cuasi-isometría entonces f es un embebimiento cuasi-isométrico con imagen cuasi-densa.

Supongamos que g es cuasi-inversa de f, donde f es una cuasi-isometría, entonces existe una constante $c \in \mathbb{R}_{>0}$ tal que $\forall y \in Y$ con $g(y) := x$ definimos:

$$d_Y(f \circ g(y), y) \leq c$$

Así, por definición 3.6 f es un embebimiento cuasi-isométrico y además posee una imagen cuasi-densa. □

Cuando se trabaja con cuasi-isometrías, las siguientes propiedades de herencia puede ser útil:

Proposición 3.2 (Propiedades de Herencia de embebimientos cuasi-isométricos)

1. Cada mapeo a una distancia finita de un embebimiento cuasi-isométrico es un embebimiento cuasi-isométrico.
2. Todo mapeo a una distancia finita de una cuasi-isometría es una cuasi-isometría.
3. Sean X, Y, Z espacios métricos y sean $f, f' : X \longrightarrow Y$ mapeos que tienen distancia finita entre si:
   i) Si $g : Z \longrightarrow X$ es un mapeo, entonces $f \circ g$ y $f' \circ g$ tienen una distancia finita entre sí.
   ii) Si $g : Y \longrightarrow Z$ es un embebimiento cuasi-isométrico, entonces $g \circ f$ y $g \circ f'$ también tienen una distancia finita entre sí.
4. Composiciones de embebimientos cuasi-isométricos [bilipschitz] son embebimientos cuasi-isométricos [bilipschitz].
5. Las composiciones de cuasi-isometrías [equivalencia bilipschitz] son cuasi-isometrías [equivalencia bilipschitz].

Demostración. Iniciaremos demostrando el ítem 1.

1. Sea f un mapeo con distancia finita de una cuasi-isometría embebida g.

   Como f es un mapeo con distancia finita existe $c \geq 0$ tal que

   $$d_Y(f(x), g(x)) \leq c, \quad \forall x \in X$$

   y como g es un embebimiento cuasi-isométrico existe $c', b > 0$ tal que $\forall x, x' \in X$

luego,

$$\frac{1}{c'}\cdot d_X\left(x,x'\right)-b\leq d_Y\left(g\left(x\right),g\left(x'\right)\right)\leq c'\cdot d_X\left(x,x'\right)+b.$$

Probaremos que f también es un embebimiento cuasi-isométrico.

Ahora bien,

$$\begin{aligned}
d_Y\left(f\left(x\right),f\left(x'\right)\right) &\leq d_Y\left(f\left(x\right),g\left(x\right)\right)+d_Y\left(g\left(x\right),f\left(x'\right)\right)\\
&\leq d_Y\left(f\left(x\right),g\left(x\right)\right)+d_Y\left(f\left(x'\right),g\left(x'\right)\right)+d_Y\left(g\left(x\right),g\left(x'\right)\right)\\
&\leq c+c+d_Y\left(g\left(x\right),g\left(x'\right)\right)\\
&= 2\cdot c+d_Y\left(g\left(x\right),g\left(x'\right)\right)\\
&\leq 2\cdot c+c'\cdot d_X\left(x,x'\right)+b\\
&= 2\cdot c+b+c'\cdot d_X\left(x,x'\right)
\end{aligned}$$

Además,

$$\begin{aligned}
\frac{1}{c'}\cdot d_X\left(x,x'\right)-\left(2\cdot c+b\right) &\leq d_Y\left(g\left(x\right),g\left(x'\right)\right)-2\cdot c-b+b\\
&\leq d_Y\left(f\left(x\right),g\left(x\right)\right)+d_Y\left(f\left(x\right),g\left(x'\right)\right)-2\cdot c-b+b\\
&\leq d_Y\left(f\left(x\right),g\left(x\right)\right)+d_Y\left(f\left(x'\right),g\left(x'\right)\right)+d_Y\left(f\left(x\right),f\left(x'\right)\right)-2\cdot c-b+b\\
&\leq c+c+d_Y\left(f\left(x\right),f\left(x'\right)\right)-2\cdot c-b+b\\
&= d_Y\left(f\left(x\right),f\left(x'\right)\right)-b+b\\
&\leq d_Y\left(f\left(x\right),f\left(x'\right)\right)
\end{aligned}$$

Por lo tanto, f es un embebimiento cuasi-isométrico.

2. Sea f un mapeo con distancia finita de una cuasi-isometría. Probemos que f es cuasi-isometría.

   Como f es un mapeo con distancia finita existe $c\geq 0$ tal que

   $$d_Y\left(f\left(x\right),g\left(x\right)\right)\leq c,\quad \forall x\in X$$

   y como g es una cuasi-isometría existe $h:Y\longrightarrow X$ tal que h es un embebimiento cuasi-isométrico. Además, $h\circ g$ tiene distancia finita con id_X y $g\circ h$ tiene distancia finita con id_Y.

   Ahora bien, como $h\circ g$ tiene distancia finita con id_X, existe $c_1\geq 0$ tal que

   $$d_X\left(\left(h\circ g\right)\left(x\right),id_X\left(x\right)\right)\leq c_1$$

   también existe $c_2\geq 0$ tal que

$$d_Y\left(\left(g\circ h\right)(y), id_Y(y)\right) \leq c_2$$

Probemos entonces que $h\circ f$ tiene distancia finita con id_X y $f\circ h$ tiene distancia finita con id_Y.

$$\begin{aligned} d_X\left(\left(h\circ f\right)(x), id_X(x)\right) &\leq d_X\left(\left(h\circ f\right)(x), \left(h\circ g\right)(x)\right) + d_X\left(\left(h\circ g\right)(x), id_X(x)\right) \\ &\leq d_X\left(\left(h\circ f\right)(x), \left(h\circ g\right)(x)\right) + c_1 \\ &= d_X\left(h\left(f(x)\right), h\left(g(x)\right)\right) + c_1 \\ &\leq c'\cdot d_Y\left(f(x), g(x)\right) + b + c_1 \\ &\leq c'\cdot c + b + c_1 \end{aligned}$$

Así, $h\circ f$ tiene distancia finita con id_X.

Luego,

$$\begin{aligned} d_Y\left(\left(f\circ h\right)(y), id_Y(y)\right) &\leq d_Y\left(\left(f\circ h\right)(y), \left(g\circ h\right)(y)\right) + d_Y\left(\left(g\circ h\right)(y), id_Y(y)\right) \\ &\leq d_Y\left(\left(f\circ h\right)(y), \left(g\circ h\right)(y)\right) + c_2 \\ &= d_Y\left(f\left(h(y)\right), g\left(h(y)\right)\right) + c_2 \\ &\leq c + c_2 \end{aligned}$$

así, $f\circ h$ tiene distancia finita con id_Y

3. Por hipótesis $f, f' : X \longrightarrow Y$ tienen distancia finita entre ellos.

i) Como f, f' tienen distancia finita entre ellos existe $c>0$ tal que $d_Y\left(f(x), f'(x)\right) \leq c$.

Supongamos que $g : Z \longrightarrow X$ es un mapeo. Ahora,

$$\begin{aligned} d_Y\left(\left(f\circ g\right)(z), \left(f'\circ g\right)(z)\right) &\leq d_Y\left(f\left(g(z)\right), f'\left(g(z)\right)\right) \\ &\leq c \end{aligned}$$

Así, $f\circ g$ y $f'\circ g$ tienen distancia finita entre ellos.

ii) Supongamos que $g : Y \longrightarrow Z$ es un embebimiento cuasi-isométrico.

Si g es un embebimiento cuasi-isométrico existen $c_1, b>0$ tales que

$$\frac{1}{c_1}\cdot d_Y\left(x, x'\right) - b \leq d_Z\left(g(x), g\left(x'\right)\right) \leq c_1\cdot d_Y\left(x, x'\right) + b$$

Luego,

$$\begin{aligned} d_Z\left(\left(g\circ f\right)(x), \left(g\circ f'\right)(x)\right) &= d_Z\left(g\left(f(x)\right), g\left(f'(x)\right)\right) \\ &\leq c_1\cdot d_Y\left(f(x), f'(x)\right) + b \\ &\leq c_1\cdot c + b \end{aligned}$$

Así, $d_Z\left(\left(g\circ f\right)(x), \left(g\circ f'\right)(x)\right) \leq c_1\cdot c + b$ y $g\circ f$, $g\circ f'$ tienen distancia finita.

4. Sean $g : X \longrightarrow Y$ y $f : Y \longrightarrow Z$.

   Supongamos que f y g son cuasi-isometrías, probemos que $f \circ g$ también es cuasi-isometría.

   Si f y g son cuasi-isometrías existen $c_1, c_2, b_1, b_2 > 0$ tal que

$$\frac{1}{c_1} \cdot d_X\left(x, x'\right) - b_1 \leq d_Y\left(g\left(x\right), g\left(x'\right)\right) \leq c_1 \cdot d_X\left(x, x'\right) + b_1$$

   y

$$\frac{1}{c_2} \cdot d_Y\left(y, y'\right) - b_2 \leq d_Z\left(f\left(y\right), f\left(y'\right)\right) \leq c_2 \cdot d_Y\left(y, y'\right) + b_2$$

   Ahora bien,

$$\begin{aligned} d_Z\left(\left(f \circ g\right)(x), \left(f \circ g\right)\left(x'\right)\right) &= d_Z\left(f\left(g\left(x\right)\right), f\left(g\left(x'\right)\right)\right) \\ &\leq c_2 \cdot d_Y\left(g\left(x\right), g\left(x'\right)\right) + b_2 \\ &\leq c_2 \cdot \left(c_1 \cdot d_X\left(x, x'\right) + b_1\right) + b_2 \\ &= c_1 \cdot c_2 \cdot d_X\left(x, x'\right) + c_2 \cdot b_1 + b_2 \end{aligned}$$

   Además,

$$\begin{aligned} \frac{1}{c_1 \cdot c_2} d_X\left(x, x'\right) - c_2 \cdot b_1 - b_2 &= \frac{1}{c_2} \cdot \left(\frac{1}{c_1} \cdot d_X\left(x, x'\right)\right) - c_2 \cdot b_1 - b_2 \\ &\leq \frac{1}{c_2} \cdot \left(d_Y\left(g\left(x\right), g\left(x'\right)\right) + b_1\right) - c_2 \cdot b_1 - b_2 \\ &= \frac{1}{c_2} \cdot d_Y\left(g\left(x\right), g\left(x'\right)\right) + \frac{b_1}{c_2} - c_2 \cdot b_1 - b_2 \\ &\leq d_Z\left(\left(f \circ g\right)(x), \left(f \circ g\right)\left(x'\right)\right) + b_2 + \frac{b_1}{c_2} - c_2 \cdot b_1 - b_2 \\ &= d_Z\left(\left(f \circ g\right)(x), \left(f \circ g\right)\left(x'\right)\right) + \frac{b_1}{c_2} - c_2 \cdot b_1 \\ &\leq d_Z\left(\left(f \circ g\right)(x), \left(f \circ g\right)\left(x'\right)\right) \end{aligned}$$

   Así, $f \circ g$ es un embebimiento cuasi-isométrico.

   Ahora probemos que si f y g es un embebimiento bilipschitz entonces también lo es $f \circ g$.

   Por definición existen $c_1, c_2 > 0$ tal que

$$\frac{1}{c_1} \cdot d_X\left(x, x'\right) \leq d_Y\left(g\left(x\right), g\left(x'\right)\right) \leq c_1 \cdot d_X\left(x, x'\right)$$

$$\frac{1}{c_2} \cdot d_Y(y, y') \leq d_Z(f(y), f(y')) \leq c_2 \cdot d_Y(y, y')$$

Luego,

$$\begin{aligned} d_Z((f \circ g)(x), f \circ g(x')) &= d_Z(f(g(x)), f(g(x'))) \\ &\leq c_2 \cdot d_Y(g(x), g(x')) \\ &\leq c_1 \cdot c_2 \cdot d_X(x, x') \end{aligned}$$

Por otro lado,

$$\begin{aligned} \frac{1}{c_1 \cdot c_2} \cdot d_X(x, x') &\leq \frac{1}{c_2} \cdot (d_Y(g(x), g(x'))) \\ &\leq d_Z(f(g(x)), f(g(x'))) \end{aligned}$$

Así,

$$\begin{aligned} \frac{1}{c_1 \cdot c_2} \cdot d_X(x, x') &\leq d_Z((f \circ g)(x), f \circ g(x')) \\ &\leq c_1 \cdot c_2 \cdot d_X(x, x') \end{aligned}$$

Así, $f \circ g$ es un embebimiento bilipschitz.

5. Sean $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ cuasi-isometrías.

   Probemos que $g \circ f$ es una cuasi-isometría.

   Si f y g son cuasi-isometrías por definición son embebimientos cuasi-isométricos para los cuales existe $f' : Y \longrightarrow g$ y $g' : Z \longrightarrow Y$ tal que $f' \circ f$ tiene distancia finita con id_X y $f \circ f'$ tienen distancia finita con id_Y.

   También $g' \circ g$ tiene distancia finita con id_Y y $g \circ g'$ tiene distancia finita con id_Z.

   Luego por ítem 4 $f' \circ g'$ es un embebimiento cuasi-isométrico y por ítem 3-**i)** $(f' \circ g') \circ (g \circ f)$ tiene distancia finita con id_Z y $(g \circ f) \circ (f' \circ g')$ tiene distancia finita con id_X.

   Por lo tanto, $g \circ f$ es una cuasi-isometría.

   Ahora probemos que si f y g son equivalencias bilipschitz entonces $g \circ f$ también lo es.

   Si f y g son equivalencias bilipschitz entonces por definición f y g son embebimientos bilipschitz para los cuales existe $f' : Y \longrightarrow X$ y $g : Z \longrightarrow Y$ tal que

$$\begin{aligned} f \circ f' &= i_y \\ f' \circ f &= i_x \\ g \circ g' &= i_z \\ g' \circ g &= i_y \end{aligned}$$

Por ítem 4 tendremos que $f' \circ g'$ es un embebimiento bilipschitz y además

$$\begin{aligned}(f' \circ g') \circ (g \circ f) &= f' \circ (g' \circ g) \circ f \\ &= f' \circ i_y \circ f \\ &= f' \circ f \\ &= i_x \\ (g \circ f) \circ (f' \circ g') &= g \circ (f \circ f') \circ g' \\ &= g \circ i_x \circ g' \\ &= g \circ g' \\ &= i_z\end{aligned}$$

Así, $g \circ f$ también es una equivalencia bilipschitz.

□

3.2. Tipos de cuasi-isometría de grupo

Cada conjunto generador de un grupo produce una métrica en el grupo en cuestión por las longitudes de los caminos en el grafo de Cayley correspondiente. La noción geométrica de gran escala de cuasi-isometría nos permite asociar tipos a grupos generados finitamente que no dependen de la elección finita de conjuntos generadores.

Definición 3.8 (Métrica en un grafo)

Sea $X = (V,\ E)$ un grafo conexo.
Entonces el mapeo,

$$\omega : V \times V \longrightarrow \mathbb{R}_{\geq 0}$$
$$(v,\ w) \longmapsto \text{mín}\left\{\ n \in \mathbb{N} \;\middle|\; \text{existe un camino de longitud } n \text{ que conecta a } v \text{ con } w \text{ en } X\ \right\}$$

es una métrica en V, **la métrica en** V **asociada a** X.

Definición 3.9 (Métrica de palabra, longitud de palabra)

Sea G un grupo y $S \subset G$ un conjunto generador. **La métrica de palabra** d_S en G con respecto a S es la métrica en G asociado al grafo de Cayley $\text{Cay}(G, S)$. En otras

palabras,

$$d_S(g,h) = \min\left\{ \; n \in \mathbb{N} \;\middle|\; \exists s_1,\ldots,s_n \in S \cup S^{-1},\; g^{-1}\cdot h = s_1 \cdots s_n \; \right\}$$

para todo $h, g \in G$. La distancia $d_S(e,g)$ es también llamada la **longitud de palabra** de g con respecto a S.

Ejemplo 3.5 **(Métrica de palabra en $\mathbb{Z}$)**

La métrica de palabra sobre $\mathbb{Z}$ correspondiente al conjunto generado $\{1\}$ coinciden con la métrica sobre $\mathbb{Z}$ inducida a partir de la métrica estándar sobre $\mathbb{R}$. Por otra parte, en la métrica denominativa sobre $\mathbb{Z}$ correspondiente al conjunto generador $\mathbb{Z}$, todos los elementos del grupo tienen distancia 1 de cualquier otro elemento del grupo.

Análisis: Analicemos de un caso específico al general para mayor comprensión.

i) La métrica de palabra sobre $\mathbb{Z}$ correspondiente al conjunto generador $\{1\}$ coincide con la métrica sobre $\mathbb{Z}$ inducida a partir de la métrica estándar sobre $\mathbb{R}$.
Tomemos en cuenta que la operación del grupo es la suma. Sea $5 \in \mathbb{Z}$ y $s_1,\ldots,s_n \in \{1\}\cup\{-1\}$.

Observamos que a 5 lo podemos reescribir como $5 = -1_1+1_2+1_3+1_4+1_5+1_6+1_7$ una palabra de longitud $n=7$, pero también podemos reescribirlo como $5 = 1_1+1_2+1_3+1_4+1_5$, una palabra de longitud $n=5$, y es la palabra con longitud mínima con la que podemos reescribir a 5. Entonces, según la definición de métrica de palabra, para la distancia entre $5,3 \in \mathbb{Z}$

$$d_{\{1\}}(3,5) = \left\{ \; n \in \mathbb{N} \;\middle|\; \exists s_1,\ldots,s_n \in \{1\}\cup\{-1\} \;\; -3+5 = s_1+\cdots+s_n = 1_1+1_2 \; \right\} = 2 = |-3+5|.$$

En general, para $m, n \in \mathbb{Z}$ la palabra más corta que representa la diferencia $m-n$, tiene longitud $|m-n|$. Entonces,

$$d_{\{1\}}(m,n) = |m-n|$$

como notamos realmente si coincide con la métrica sobre $\mathbb{Z}$ inducida a partir de la métrica estándar en $\mathbb{R}$ (la métrica usual).

ii) La métrica sobre el grupo $\mathbb{Z}$ correspondiente al conjunto generador $\mathbb{Z}$, todos los elementos del grupo tienen distancia 1 de cualquier otro elemento del grupo. Sea $7,1 \in \mathbb{Z}$

$$d_{\mathbb{Z}}(7,1) = \left\{ \; n \in \mathbb{N} \;\middle|\; \exists s_1,\ldots,s_n \in \{\mathbb{Z}\} \;\; -7+1 = s_1 = -6_1 \; \right\} = 1$$

Entonces en caso general para $m, n \in \mathbb{Z}$ tendremos que

$$d_{\mathbb{Z}}(m,n) = \left\{ \ n \in \mathbb{N} \ \middle| \ \exists s_1, \ldots, s_n \in \{\mathbb{Z}\} \ -m+n = s_1 \ \right\} = 1$$

en efecto todos los elementos del grupo $\mathbb{Z}$ correspondientes al conjunto generador $\mathbb{Z}$ tienen distancia 1 de cualquier otro elemento del grupo.

■

En general, las métricas de palabras de un grupo determinado dependen del conjunto de generadores elegido. Sin embargo, la diferencia es insignificante cuando se observa el grupo desde lejos:

Proposición 3.3

Sea G un grupo finitamente generado, sean S y S' conjuntos generadores finitos de G.

1. Entonces el mapeo identidad id_G es una equivalencia bilipschitz entre (G, d_S) y $(G, d_{S'})$.
2. En particular, todo espacio métrico (X, d) que sea equivalente bilipschitz [o cuasi-isométrico] a (G, d_S) también es equivalente bilipschitz [o cuasi-isométrico, respectivamente] a $(G, d_{S'})$ (a través de los mismos mapas).

Demostración. Probaremos el ítem 1, vamos a demostrar que $id_G : (G, d_S) \longrightarrow (G, d_{S'})$ es una equivalencia bilipschitz, para ello debemos probar que cumple dos condiciones:

i) Si existe un embebimiento bilipschitz, en otras palabras según la definición 3.5, debemos probar que existe una constante $c \in \mathbb{R}_{>0}$, tal que

$$\forall x, x' \in G, \frac{1}{c} \cdot d_S\left(x, x'\right) \leq d_{S'}\left(id_G(x), id_G\left(x'\right)\right) \leq c \cdot d_S\left(x, x'\right)$$

ii) Si existe un embebimiento bilipschitz $g : (G, d_{S'}) \longrightarrow (G, d_S)$, tal que $id_G \circ g = id_G$ y $g \circ id_G = id_G$.

Primera condición. Sabemos que S es finito, entonces el máximo,

$$c = \max_{S \cup S^{-1}} d_{S'}(e, s)$$

es finito.

Sean $x, x' \in G$ y $n := d_S(x, x')$. Como $n = d_S(x, x')$, por definición de métrica de palabra se cumple que $x^{-1} \cdot x' = s_1 \cdots s_n$ con $s_1, \ldots, s_n \in S \cup S^{-1}$, entonces $x' = x \cdot s_1 \cdots s_n$ luego,

$$\begin{aligned} d_{S'}(x, x') &= d_{S'}(x, x \cdot s_1 \cdots s_n) \\ &\leq d_{S'}(x, x \cdot s_1) + d_{S'}(x \cdot s_1, x \cdot s_1 \cdot s_2) + \cdots + d_{S'}(x \cdot s_1 \cdots s_{n-1}, x \cdot s_1 \cdots s_n) \end{aligned}$$

por definición de métrica de palabra, tenemos que $d_{S'}(x, x \cdot s_1) = 1$ ya que $x^{-1} \cdot x \cdot s_1 = s_1$, así $n = 1$. También $d_{S'}(e, s_1) = 1$ ya que $e^{-1} \cdot s_1 = s_1$, ahora con esto retomamos que

$$\begin{aligned} d_{S'}(x, x') &\leq d_{S'}(x, x \cdot s_1) + d_{S'}(x \cdot s_1, x \cdot s_1 \cdot s_2) + \cdots + d_{S'}(x \cdot s_1 \cdots s_{n-1}, x \cdot s_1 \cdots s_n) \\ &= d_{S'}(e, s_1) + d_{S'}(e, s_2) + \cdots + d_{S'}(e, s_n) \\ &\leq c + c + \cdots + c \\ &= c \cdot n \\ &= c \cdot d_S(x, x') \end{aligned}$$

entonces tenemos que

$$\frac{1}{c} \cdot d_{S'}(x, x') \leq d_S(x, x'). \tag{3.3}$$

Ahora, para obtener la otra desigualdad, vamos a tomar a $n := d_{S'}(id_G(x), id_G(x'))$ como es la identidad en G, podemos reescribir a $n := d_{S'}(x, x')$ y sea $c = \max_{S \cup S^{-1}} d_S(e, s)$

$$\begin{aligned} d_S(x, x') &= d_S(x, x \cdot s_1 \cdots s_n) \\ &\leq d_S(x, x \cdot s_1) + d_S(x \cdot s_1, x \cdot s_1 \cdot s_2) + \cdots + d_S(x \cdot s_1 \cdots s_{n-1}, x \cdot s_1 \cdots s_n) \\ &= d_S(e, s_1) + d_S(e, s_2) + \cdots + d_S(e, s_n) \\ &\leq c + c + \cdots + c \\ &= c \cdot n \\ &= c \cdot d_{S'}(x, x') \end{aligned}$$

entonces tenemos que

$$d_S(x, x') \leq c \cdot d_{S'}(x, x'). \tag{3.4}$$

Ahora uniendo la desigualdad 3.3 y la 3.4,

$$\frac{1}{c} \cdot d_{S'}(x, x') \leq d_S(x, x') \leq c \cdot d_{S'}(x, x')$$

por tanto existe un embebimiento bilipschitz.

Segunda condición. Ya que estamos trabajando con $id_G : (G, d_S) \longrightarrow (G, d_{S'})$ se ve que se cumple que existe un embebimiento bilipschitz $g : (G, d_{S'}) \longrightarrow (G, d_S)$, tal que $id_G \circ g = id_G$ y $g \circ id_G = id_G$.

Ahora, que hemos probado las dos condiciones tenemos que $id_G : (G, d_S) \longrightarrow (G, d_{S'})$ es una equivalencia bilipschitz.

Probaremos el ítem 2. **Sea** (X, d) **un espacio métrico equivalente bilipschitz** (G, d_S)**, vamos a demostrar que** (X, d) **es equivalente bilipschitz a** $(G, d_{S'})$**.**

Como (X, d) un espacio métrico equivalente bilipschitz (G, d_S) por definición 3.5 tenemos que existe una equivalencia bilipschitz entre ellos,

$$\Phi : (X, d) \longrightarrow (G, d_S)$$

tenemos también por el ítem anterior que $id_G : (G, d_S) \longrightarrow (G, d_{S'})$ es una equivalencia bilipschitz. Entonces, tenemos dos equivalencias bilipschitz

$$\Phi : (X, d) \longrightarrow (G, d_S) \text{ y } id_G : (G, d_S) \longrightarrow (G, d_{S'})$$

por la proposición 3.2-ítem 5, obtenemos que

$$\Phi \circ id_G : (X, d) \longrightarrow (G, d_{S'})$$

es una equivalente bilipschitz, por lo tanto (X, d) es equivalencia bilipschitz a $(G, d_{S'})$.

Sea (X, d) **un espacio métrico cuasi-isométrico** (G, d_S)**, vamos a demostrar que** (X, d) **es cuasi-isométrico a** $(G, d_{S'})$**.** De forma análoga si (X, d) un espacio métrico cuasi-isométrico (G, d_S), entonces existe una cuasi-isometría

$$\Phi : (X, d) \longrightarrow (G, d_S) \text{ y } id_G : (G, d_S) \longrightarrow (G, d_{S'})$$

luego, por la proposición 3.2-ítem 4

$$\Phi \circ id_G : (X, d) \longrightarrow (G, d_{S'})$$

es una cuasi-isometría. Por lo tanto, (X, d) es cuasi-isométrico a $(G, d_{S'})$ □

Ejemplo 3.6 **(Grafos de Cayley de $\mathbb{Z}$)**

Para conjuntos generadores infinitos, la proposición anterior no se sostiene en general; por ejemplo, tomando $\mathbb{Z}$ como un conjunto generado para $\mathbb{Z}$ lleva al espacio $(\mathbb{Z}, d_{\mathbb{Z}})$ de diámetro finito, mientras que $\left(\mathbb{Z}, d_{\{1\}}\right)$ no tiene diámetro finito.

Análisis: Se procede hacer el análisis respectivo:
i) Sea $S = \{\mathbb{Z}\}$ y $G = \mathbb{Z}$ con la métrica inducida por las palabras, usando el ejemplo 3.5. Para cualesquiera $m, n \in \mathbb{Z}$.

$$d_{\mathbb{Z}}(m, n) = \left\{ \ n \in \mathbb{N} \ \middle| \ \exists s_1, \ldots, s_n \in \{\mathbb{Z}\} \ \ -m + n = s_1 \ \right\} = 1$$

Entonces todos los elementos del grupo $\mathbb{Z}$ con respecto al conjunto generador $\{\mathbb{Z}\}$ tienen distancia 1.
Así, $\mathbb{Z}$ generado por $\{\mathbb{Z}\}$ tiene diámetro finito.

ii) Ahora, si tomamos $S = \{1\}$.
Para cualesquiera $m, n \in \mathbb{Z}$ por el ejemplo 3.5 tenemos que es básicamente $\mathbb{Z}$ inducida por la métrica usual en $\mathbb{R}$, por lo que la distancia estará dada como:

$$d_{\{1\}}(m,n) = |m-n|$$

Así, la longitud dada será positiva y sabemos que se encuentran en $\mathbb{Z}$; donde $\mathbb{Z}$ esta formado como un conjunto infinito. Lo que concluye es que $\mathbb{Z}$ generado por $\{1\}$ tiene diámetro infinito.

Con respecto a la proposición anterior no se sostiene para conjuntos generadores infinitos: Si consideramos al espacio $(\mathbb{Z}, d_{\mathbb{Z}})$ con el conjunto generador $S = \mathbb{Z}$ notemos que el primer caso, la familia generadora no es finita y al aplicar la definición de métrica de palabra nos da como resultado que el espacio $(\mathbb{Z}, d_{\mathbb{Z}})$ posee diámetro finito, ya que todos los elementos están a distancia 1 de los demás. Al contrario si observamos el otro caso considerando al espacio $\left(\mathbb{Z}, d_{\{1\}}\right)$ con el conjunto generador $S = \{1\}$, la familia generadora es finita pero al aplicar la definición de métrica de palabra observamos que el espacio $\left(\mathbb{Z}, d_{\{1\}}\right)$ posee diámetro infinito. Por lo tanto no podemos aplicar las condiciones de la proposición anterior por que no encontraremos constantes que nos cumplan las desigualdades de las definiciones de cuasi-isometría y equivalencia bilipschitz.

■

Definición 3.10 (Tipo de cuasi-isometría de grupos generados finitamente)
Sea G un grupo finitamente generado.

- El grupo G es **equivalente bilipschitz** a un espacio métrico X si para algunos (y por lo tanto cada) conjunto generador finito S de G los espacios métricos (G, d_s) y X son equivalentes bilipschitz.
- El grupo G es **cuasi-isométrico** a un espacio métrico X si para algunos (y por lo tanto cada) conjunto generador finito S de G los espacios métricos (G, d_S) y X son cuasi-isométricos.

Análogamente, definimos cuando dos grupos generados finitamente se denominan equivalente bilipschitz o cuasi-isométrico.

Nota:

- Dos grupos G, H son equivalente bilipschitz a un espacio métrico X si para algún conjunto generador finito S de G y para algún conjunto generador finito T de H, los espacios métricos (G, d_S) y (H, d_T) son equivalentes bilipschitz al espacio métrico X.
- Dos grupos G, H son cuasi-isométricos a un espacio métrico X, si para algún conjunto generador finito S de G y para algún conjunto generador finito T de H, los espacios métricos (G, d_S) y (H, d_T) son cuasi-isométricos al espacio métrico X.

La cuestión de cómo se relacionan la cuasi-isometría y la equivalencia bilipschitz para grupos generados finitamente conduce a problemas interesantes y aplicaciones útiles. Un primer paso hacia una respuesta es el siguiente:

Proposición 3.4

Las cuasi-isometrías biyectivas entre grupos generados finitamente (con respecto a la métrica de palabra de ciertos conjuntos generados finitamente) son equivalencias bilipschitz.

Demostración. Sean G y H dos grupos finitamente generados por S y T respectivamente y

$$f : (G, d_S) \longrightarrow (H, d_T)$$

una (λ, c)-cuasi-isometría biyectiva y a, b dos elementos diferentes de G, entonces $d_S(a, b) \geq 1$ y

$$\frac{1}{\lambda} \cdot d_S(a, b) - c \leq d_T\left(f(a), f(b)\right) \leq \lambda \cdot d_S(a, b) + c$$

Queremos encontrar $k \in \mathbb{R}^+$ tal que

$$\frac{1}{k} \cdot d_S(a, b) \leq \frac{1}{2} \cdot d_S(a, b) - c \tag{3.5}$$

$$\lambda \cdot d_S(a, b) + c \leq k \cdot d_S(a, b) \tag{3.6}$$

De la ecuación 3.5 obtenemos

$$\left(\frac{1}{2} - \frac{1}{k}\right) \cdot d_S(a, b) \geq c$$

De la ecuación 3.6 se tiene

$$(k - 2) \cdot d_S(a, b) \geq c$$

De estas dos últimas ecuaciones tenemos

$$\left[\left(\frac{k^2-1}{k}\right)-\left(\frac{\lambda^2-1}{\lambda}\right)\right]\cdot d_S(a,b)\geq 2\cdot c$$

Como $d_S(a,b)\geq 1$ solo habrá que encontrar k tal que

$$\left[\left(\frac{k^2-1}{k}\right)-\left(\frac{\lambda^2-1}{\lambda}\right)\right]\geq 2\cdot c \Longrightarrow \frac{k^2-1}{k}\geq 2\cdot c+\frac{\lambda^2-1}{\lambda}$$

dado que la función $f(x)=\frac{x^2-1}{x}$ es biyectiva y además creciente en $(0,\infty)$ podemos encontrar un $k\in\mathbb{R}^+$ que satisface la desigualdad. □

Iniciamos con clasificación de cuasi-isometría de grupos finitos.

Proposición 3.5 (Propiedades de la métrica de palabra)

Sea G un grupo y sea $S\subset G$ un conjunto generador. Entonces, S es finito si y solo si la métrica de palabra d_S sobre G es propia, en el sentido que todas las bolas de radio finito en (G,d_S) son finitas.

Demostración. "$\Longleftarrow$" La métrica de palabra d_S sobre G es propia, entonces S es finito.

(Por contra-reciproco) Si S es infinito, entonces la métrica de palabra d_S sobre G no es propia en el sentido que todas las bolas de radio finito, son infinitas. Sea $B(e,1)$ en (G,d_S)

$$\begin{aligned} x\in B(e,1) &\Longrightarrow d(x,e)=1 \\ &\Longrightarrow \exists s_1\in S\cup S^{-1} \text{ tal que } x^{-1}\cdot e=s_1 \qquad \text{; por definición 3.9} \\ &\Longrightarrow |B(e,1)|=|S| \end{aligned}$$

$B(e,1)$ contiene $|S|$ elementos, y como S es infinito entonces la bola $B(e,1)$ de radio finito es infinita en (G,d_S). Entonces la métrica d_S sobre G no es propia.

"$\Longrightarrow$" Si S es finito, entonces la métrica de palabra d_S sobre G es propia, en el sentido que todas las bolas de radio finito en (G,d_S) son finitas. Sea $B(e,n)$ (de radio finito) en (G,d_S).

Tenemos que el conjunto S es finito entonces $\left(S\cup S^{-1}\right)^n$ es finito, donde $\left(S\cup S^{-1}\right)^n$ es el conjunto de todas las palabras sobre $S\cup S^{-1}$ de longitud n.

Sea

$$\begin{aligned} \sigma:\left(S\cup S^{-1}\right)^n &\longrightarrow B(e,n) \\ s_1\cdots s_n &\longmapsto (s_1\cdots s_n)^{-1} \end{aligned}$$

probemos que σ es sobreyectiva. Sea $x \in B(e,n)$

$$\begin{aligned} x \in B(e,n) &\Longrightarrow d(x,e) = n \\ &\Longrightarrow \exists s_1,\ldots,s_n \in S \cup S^{-1} \text{ tal que } x^{-1}\cdot e = s_1 \cdots s_n \\ &\Longrightarrow x^{-1} = s_1 \cdots s_n \in \left(S \cup S^{-1}\right)^n \\ &\Longrightarrow \left(x^{-1}\right)^{-1} = \sigma(s_1 \cdots s_n) \\ &\Longrightarrow x = \sigma(s_1 \cdots s_n) \end{aligned}$$

así, σ es sobreyectiva, entonces se cumple que

$$|B(e,n)| \leq \left|\left(S \cup S^{-1}\right)^n\right|$$

como $\left(S \cup S^{-1}\right)^n$ es finito, entonces $B(e,n)$ es finita, por lo tanto, la métrica d_S es propia en G. □

Ejemplo 3.7 **(Clasificación de cuasi-isometría de grupos finitos)**

Un grupo finitamente generado es cuasi-isométrico a un grupo finito si y solo si este es finito.

Análisis: "$\Longrightarrow$" Si un grupo G finitamente generado es cuasi-isométrico a un grupo finito X, entonces este es finito. Si G es finitamente generado por un conjunto S, el grupo G nos conduce a un espacio métrico (G, d_S).

Por hipótesis tenemos que G es cuasi-isométrico a X, entonces por la definición 3.10-ítem 2 tenemos que (G, d_S) y X son cuasi-isométricos.

Ahora bien, como por hipótesis X es finito, entonces es de diámetro finito, por el ejemplo 3.4-ítem 2 tenemos que si (G, d_S) es cuasi-isométrico a X de diámetro finito, entonces (G, d_S) es de diámetro finito.

Si (G, d_S) es de diámetro finito, entonces las bolas en (G, d_S) de radio finito, son finitas por la proposición 3.5, sabemos que S es finito, del cual se deduce que G es finito.

"$\Longleftarrow$" Si G es un grupo finitamente generado y es finito, entonces es cuasi-isométrico a un conjunto X. Sabemos que si G es finito y finitamente generado, entonces nos conduce a espacio métrico (G, d_S) de diámetro finito, y por lo tanto, todos son cuasi-isométricos por el ejemplo 3.4-ítem 1.

■

3.3. El lema de Švarc-Milnor

En la geometría de espacios métricos, a menudo resulta útil que el espacio en cuestión sea geodésico, es decir, que su métrica pueda ser realizada por caminos. Sin embargo, no siempre se tiene un espacio geodésico, es por esta razón que se introduce un concepto más general: el de un espacio cuasi-geodésico. Un espacio cuasi-geodésico es un espacio métrico que salvo un error uniforme, su métrica puede ser realizada por caminos. Por ejemplo, esta será una hipótesis importante en el lema Švarc-Milnor.

Antes de abordar los conceptos de cuasi-geodésico y espacio cuasi-geodésico, es conveniente definir lo siguiente:

Definición 3.11 (Espacio Geodésico)

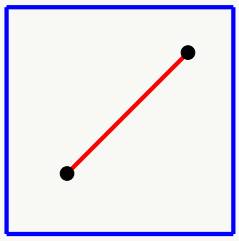
Sea el espacio métrico (X, d).

- Sea $L \in \mathbb{R}_{\geq 0}$. Una **geodésica** de longitud L en X es un embebimiento isométrico $\gamma : [0, L] \longrightarrow X$, donde el intervalo $[0, L]$ lleva la métrica inducida de la métrica estándar en $\mathbb{R}$; el punto $\gamma(0)$ es el punto de inicio de γ y $\gamma(L)$ es el punto final de γ.
- El espacio métrico X se llama **geodésico** si para todo $x, x' \in X$ existe un geodésico en X con punto inicial x y punto final x'.

Ejemplo **3.8** **(Espacios Geodésicos)**

1. Sea $n \in \mathbb{N}$. Las geodésicas en el espacio euclidiano $\mathbb{R}^n$ son precisamente los segmentos de línea euclidiana (parametrizados mediante un vector de longitud unitaria). Como dos puntos cualesquiera de $\mathbb{R}^n$ pueden unirse mediante un segmento de línea, el espacio euclidiano $\mathbb{R}^n$ es geodésico.
2. El espacio $\mathbb{R}^2 \setminus \{0\}$ dotado de la métrica inducida de la métrica euclidiana sobre $\mathbb{R}^2$ no es geodésico.

Estas afirmaciones se ilustran en la figura dada a continuación.


Espacio de $\mathbb{R}^2$

Análisis:

1. Sean $x, y \in \mathbb{R}^n$, entonces

$$x = \{x_1, x_2, \ldots, x_n\}$$
$$y = \{y_1, y_2, \ldots, y_n\}$$

donde su vector unitario es

$$u = \frac{y-x}{\| y-x \|} = \frac{(y_1, y_2, \ldots, y_n) - (x_1, x_2, \ldots, x_n)}{\| (y_1, y_2, \ldots, y_n) - (x_1, x_2, \ldots, x_n) \|}$$
$$= \frac{(y_1 - x_1, y_2 - x_2, \ldots, y_n - x_n)}{\| (y_1, y_2, \ldots, y_n) - (x_1, x_2, \ldots, x_n) \|}$$

Sea $L : [0,1] \longrightarrow \mathbb{R}^n$ definida como

$$L(t) = x + t(y - x)$$

entonces

$$L(t) = (x_1, \ldots, x_n) + t(y_1 - x_1, \ldots, y_n - x_n)$$

Observamos que L es un segmento que une x con y, ya que

$$\begin{aligned} L(0) &= (x_1, \ldots, x_n) + 0(y_1 - x_1, \ldots, y_n - x_n) \\ &= (x_1, \ldots, x_n) + 0 \\ &= (x_1, \ldots, x_n) \\ &= x \end{aligned}$$

y

$$\begin{aligned} L(1) &= (x_1, \ldots, x_n) + 1(y_1 - x_1, \ldots, y_n - x_n) \\ &= (x_1 + y_1 - x_1, \ldots, x_n + y_n - x_n) \\ &= (y_1, \ldots, y_n) \\ &= y \end{aligned}$$

y como L es una geodésica, entonces $X = \mathbb{R}^n$ es un espacio geodésico.

2. Probemos que $X = \mathbb{R}^2 - \{0\}$ es conexo por caminos pero no geodésico.

   Sean $x, y \in X$.

$$x, y \in X \Longrightarrow x = (a,b) \text{ y } y = (c,d)$$

   como $X = \mathbb{R}^2 - \{0\}$, entonces $a \neq 0, b \neq 0, c \neq 0, d \neq 0$.

   Definamos el camino $L(t) = x + t\left(y - x\right)$. Observamos que

$$\begin{aligned} L(0) &= x + 0\left(y - x\right) = x = (a,b) \neq (0,0) \\ L(1) &= x + 1\left(y - x\right) = x + y - x = y = (c,d) \neq (0,0) \end{aligned}$$

   Notemos que, L está contenido en $\mathbb{R}^2 - \{0\}$.

   Así, X es conexo por caminos.

   Ahora veremos que X no es geodésico.

   Si tomamos $x = (a,b)$, $y = (-a,-b)$ y construimos el camino

$$\begin{aligned} L(t) &= (-a,-b) + t\left(x - y\right) \\ &= (-a,-b) + t\left((a,b) - (-a,-b)\right) \\ &= (-a,-b) + t\left(2 \cdot a, 2 \cdot b\right) \\ &= (-a + 2 \cdot a \cdot t, -b + 2 \cdot b \cdot t) \end{aligned}$$

   donde $a, b \neq 0$ y tomamos $t = \frac{1}{2}$, notamos que

$$\begin{aligned} L\left(\frac{1}{2}\right) &= \left(-a + 2 \cdot a \cdot \left(\frac{1}{2}\right), -b + 2 \cdot b \cdot \left(\frac{1}{2}\right)\right) \\ &= (-a + a, -b + b) \\ &= (0,0) \notin X \end{aligned}$$

   Así, X no es geodésico.

■

Definición 3.12 (Espacio Cuasi-geodésico)

Sea (X,d) un espacio métrico, sean $c \in \mathbb{R}_{>0}$ y $b \in \mathbb{R}_{\geq 0}$.

- Entonces un (c,b)-**cuasi-geodésico** en X, es un embebimiento cuasi-isométrico $\gamma : I \longrightarrow X$, donde $I = \left[t, t'\right] \subset \mathbb{R}$ es algún intervalo cerrado; el punto $\gamma(t)$ es el punto inicial de γ, y el punto $\gamma\left(t'\right)$ es el punto final de γ.

- El espacio X es (c,b)-**cuasi-geodésico** si para todo $x, x' \in X$ existe un (c,b)-cuasi-geodésico en X con punto inicial x y punto final x'.

Ejemplo 3.9

Todo espacio geodésico es también cuasi-geodésico (es decir, $(1,0)$-cuasi-geodésico).

Análisis. Sea X un espacio geodésico, vamos a comprobar que X es $(1,0)$-cuasi-geodésico.

Si X es un espacio geodésico, definimos $\gamma : [t, t'] \longrightarrow X$ es un embebimiento isométrico, entonces para $s, s' \in [t, t']$

$$|s - s'| = d(\gamma(s), \gamma(s')) \Longrightarrow \text{ para } c = 1, b = 0 : \frac{1}{c} \cdot |s - s'| - b \leq d(\gamma(s), \gamma(s')) \leq c \cdot |s - s'| + b$$
$$\Longrightarrow \gamma \text{ es } (1,0)\text{-cuasi-geodésico}$$

■

Ejemplo 3.10 **(Espacios cuasi-geodésico)**

- Si $X = (V, E)$ es un grafo conexo, entonces la métrica asociada sobre V convierte a V en un $(1,1)$-espacio geodésico.
- En particular, si G es un grupo y S es un conjunto generador de G, entonces (G, d_S) es un espacio $(1,1)$-cuasi-geodésico.
- Para cada $\epsilon \in \mathbb{R}_{>0}$ el espacio $\mathbb{R}^2 - \{0\}$ es $(1,\epsilon)$-cuasi-geodésico con respecto a la métrica inducida de la métrica euclidiana sobre $\mathbb{R}^2$.

Análisis.

Primero. Tenemos que X es un grafo conexo, entonces para cualesquiera dos vértices en V hay al menos un camino que los conecta, esto nos ayudara a poder definir γ. Sea

$$\gamma : [0, n] \longrightarrow X$$
$$[i, i+1[\longmapsto v_i$$

Probemos que γ es una $(1,1)$-cuasi-isometría.

$$t, t' \in [0, n] \Longrightarrow t, t' \in [i, i+1[$$

seguimos

$$\begin{aligned} \text{si } t, t' \in [i, i+1[&\Longrightarrow \left|t - t'\right| < 1 \\ &\Longrightarrow 1 \cdot \left|t - t'\right| - 1 \leq 0 \end{aligned}$$

luego, como $t, t' \in [i, i+1[$ y sabemos que γ es $[i, i+1[\longmapsto v_i$, entonces $t \longmapsto v_i$ y $t' \longmapsto v_i$, por lo que $d\left(\gamma(t), \gamma\left(t'\right)\right) = 0$. Entonces, hasta el momento tenemos que

$$1 \cdot \left|t - t'\right| - 1 \leq d\left(\gamma(t), \gamma\left(t'\right)\right)$$

luego, como $0 \leq \left|t - t'\right|$, entonces $0 \leq 1 \cdot \left|t - t'\right| + 1$. Podemos concluir que

$$\frac{1}{1} \cdot \left|t - t'\right| - 1 \leq d\left(\gamma(t), \gamma\left(t'\right)\right) \leq 1 \cdot \left|t - t'\right| + 1$$

así, cada camino en el grafo X que realiza la distancia entre dos vértices es un $(1,1)$-cuasi-geodésico, entonces la métrica asociada sobre V convierte a V en un $(1,1)$-espacio geodésico.

Segundo. Tratamos con un grafo de Cayley, entonces es un caso particular del primer ítem.

Tercero. Probemos que $X = \mathbb{R}^2 - \{0\}$ es un espacio $(1,\epsilon)$-cuasi-geodésico.

Sean $x, x' \in X$, entonces $x = (a, b)$ y $x' = \left(a', b'\right)$.

Sea $\gamma : [0,1] \longrightarrow X$ definida como

$$\gamma(t) = \left(\left(a' - a\right)t + a, \left(b' - b\right)t + b\right)$$

Así,

$$\begin{aligned} \gamma(0) &= \left(\left(a' - a\right)(0) + a, \left(b' - b\right)(0) + b\right) \\ &= (a, b) \\ &= x \end{aligned}$$

$$\begin{aligned} \gamma(1) &= \left(\left(a' - a\right)(1) + a, \left(b' - b\right)(1) + b\right) \\ &= \left(a' - a + a, b' - b + b\right) \\ &= \left(a', b'\right) \\ &= x' \end{aligned}$$

así, x es el punto inicial y x' es el punto final.

Ahora probemos que γ es un $(1,\epsilon)$-cuasi-geodésico. Es decir, probemos que

$$1 \cdot d\left(t, t'\right) - \epsilon \leq d\left(\gamma\left(t\right), \gamma\left(t'\right)\right) \leq 1 \cdot d\left(t, t'\right) + \epsilon$$

Partimos de

$$\begin{aligned} 1 \cdot d(t, t') - \epsilon &= d\left(t, t'\right) - \epsilon \\ &= \left|t, t'\right| - \epsilon \\ &< 1 - \epsilon \qquad \text{; pues } t, t' \in [0,1] \end{aligned}$$

Luego,

$$\begin{aligned} d\left(\gamma\left(t\right), \gamma\left(t'\right)\right) &= d\left(\left(\left(a'-a\right)t + a, \left(b'-b\right)t + b\right), \left(\left(a'-a\right)t' + a, \left(b'-b\right)t' + b\right)\right) \\ &= \sqrt{\left[\left(a'-a\right)t + a - \left(a'-a\right)t' - a\right]^2 + \left[\left(b'-b\right)t + b - \left(b'-b\right)t - b\right]^2} \end{aligned}$$

Por lo que

$$\begin{aligned} d\left(\gamma\left(t\right), \gamma\left(t'\right)\right) &= \sqrt{\left(a'-a\right)^2\left(t-t'\right)^2 + \left(b'-b\right)^2\left(t-t'\right)^2} \\ &\leq \sqrt{\left(a'-a\right)^2 + \left(b'-b\right)^2} \end{aligned}$$

y como $d\left(\gamma\left(t\right), \gamma\left(t'\right)\right) > 0$ y $\epsilon > 0$, entonces

$$\begin{aligned} 1 \cdot d\left(t, t'\right) - \epsilon &< \sqrt{\left(a'-a\right)^2 + \left(b'-b\right)^2} \\ &\leq d\left(\gamma\left(t\right), \gamma\left(t'\right)\right) \end{aligned}$$

y dado que $d\left(t, t'\right) = \left|t, t'\right|$, así

$$\begin{aligned} d\left(\gamma\left(t\right), \gamma\left(t'\right)\right) &\leq \left|t - t'\right| + \epsilon \\ &= d\left(t, t'\right) + \epsilon \end{aligned}$$

Por lo que, γ es un $(1, \epsilon)$-cuasi-geodésico.

Por lo tanto, X es un espacio $(1, \epsilon)$-cuasi-geodésico.

■

Cuando surge un grupo G, puede no ser evidente que G se genera de forma finita. Además si se conoce un conjunto generador finito S todavía se tiene poca idea de como se ve el grafo de Cayley correspondiente, entonces es de vital importancia que tengamos herramientas de como mostrar que el grupo dado se genera finitamente y determinar la estructura métrica del grafo hasta obtener una cuasi-isometría, por ende el Lema Švarc-Milnor es fundamental para este tipo de situaciones; comenzamos con la formulación métrica del Lema de Švarc-Milnor para espacios cuasi-geodésicos:

Proposición 3.6 (Lema de Švarc-Milnor)

Sea G un grupo que actúa por isometrías sobre un espacio métrico (X,d). Supongamos que existen constantes $c,b\in\mathbb{R}_{>0}$ tales que X es (c,b)-cuasi-geodésico y que existe un conjunto $B\subset X$ con las siguientes propiedades:

1. El diámetro de B es finito.
2. Las G-traslaciones de B cubren todo X, i.e
$$\bigcup_{g\in G} g\cdot B = X.$$
3. El conjunto $S:=\left\{\ g\in G\ \middle|\ g\cdot B'\cap B'\neq\emptyset\ \right\}$ es finito, donde
$$B'=B^{X,d}_{2\cdot b}(B)=\left\{\ x\in X\ \middle|\ \exists y\in B\ \ d(x,y)\leq 2\cdot b\ \right\}.$$

Entonces:

i) El grupo G es generado por S; en particular G es finitamente generado.

ii) Para todo $x\in X$, el mapeo:
$$\begin{aligned} G &\longrightarrow X\\ g &\longmapsto g\cdot x\end{aligned}$$
es una cuasi-isometría (respecto a la métrica de palabra d_s en G).

Demostración. **i)** Sea $g\in G$, probaremos que el conjunto S genera G, es decir, $g\in\langle S\rangle_G$.
Sea $x\in B$.
Dado que X es (c,b)-cuasi-geodésico, existe una (c,b)-cuasi-geodésico $\gamma:[0,L]\longrightarrow X$ con punto inicial x y punto final $g\cdot x$ (Ver figura 3.1). Lo siguiente es buscar puntos suficientemente cercanos sobre este cuasi-geodésico γ, para esto tomamos una partición del intervalo $[0,L]$.

Sea $n:=\left[L\cdot\frac{c}{b}\right]=\min\left\{\ k\in\mathbb{N}\ \middle|\ L\cdot\frac{c}{b}\leq k\ \right\}$, luego para cada $j\in\{0,\dots,n-1\}$ definimos:

$$t_j:=j\cdot\frac{b}{c} \tag{3.7}$$

y

$$t_n:=L$$

de modo que $t_j \in [0, L]$ y además denotamos que

$$x_j := \gamma(t_j) \qquad ; j \in \{0, \ldots, n\} \tag{3.8}$$

Notemos que con las condiciones anteriores

$$x_0 = \gamma(0) = x$$

y

$$x_n = \gamma(L) = g \cdot x$$

entonces se cumple que $x_j \in \gamma([0, L])$, para cada $j \in \{0, \ldots, n-1\}$. Por otro lado, como las G-traslaciones de B cubren a X (ítem 2), existen elementos $g_j \in G$ tales que $x_j \in g_j \cdot B$, tomamos $g_0 = e$ y $g_n = g$ (Ver figura 3.1).

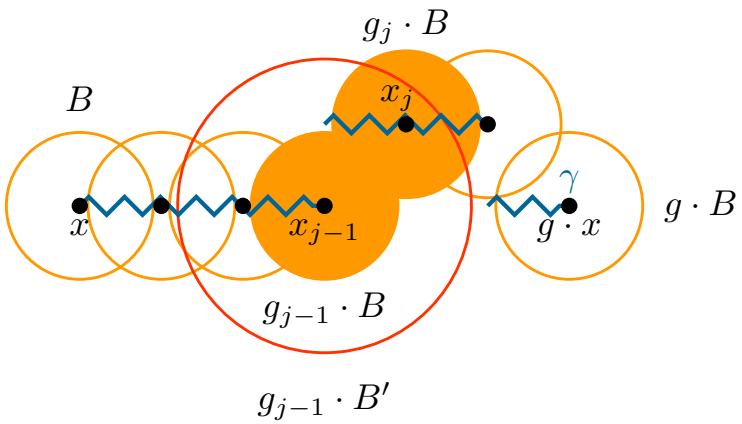


Figura 3.1. Cubierta de un cuasi-geodésico por traslaciones de B

Ahora, probemos que $\forall\, j \in \{0, \ldots, n\}$ el elemento del grupo $s_j := g_{j-1}^{-1} \cdot g_j \in S$.
Por la construcción 3.8 para toda $j \in \{0, \ldots, n\}$ se tiene que:

$$x_j := \gamma(t_j) \in \gamma([0, L])$$

como γ es una (c, b)-cuasi-geodésico:

$$\begin{aligned} d(\gamma(t_{j-1}), \gamma(t_j)) &\leq |t_{j-1} - t_j| \cdot c + b \\ &= \left| (j-1) \cdot \frac{b}{c} - j \cdot \frac{b}{c} \right| \cdot c + b \qquad \text{; por ecuación 3.7} \\ &= \left| j \cdot \frac{b}{c} - \frac{b}{c} - j \cdot \frac{b}{c} \right| \cdot c + b \\ &= \left| -\frac{b}{c} \right| \cdot c + b \end{aligned}$$

seguimos

$$\begin{aligned}\left|-\frac{b}{c}\right|\cdot c+b &= \frac{b}{c}\cdot c+b\\ &\leq 2\cdot b\end{aligned}$$

Dado que $x_{j-1}=\gamma\left(t_{j-1}\right)\in g_{j-1}\cdot B$ se sigue

$$x_{j-1}\in B_{2\cdot b}^{X,d}\left(g_{j-1}\cdot B\right)=\left\{\ x\in X\ \middle|\ \exists y\in g_{j-1}\cdot B,\text{tal que } d\left(x,y\right)\leq 2\cdot b\ \right\}.$$

Pero como G actúa por isometrías en X se tiene que

$$x_{j-1}\in B_{2\cdot b}^{X,d}\left(g_{j-1}\cdot B\right)=g_{j-1}\cdot B_{2\cdot b}^{X,d}\left(B\right)=g_{j-1}\cdot B'.$$

Por otra parte $x_j\in g_j\cdot B\subset g_j\cdot B'$ así

$$g_{j-1}\cdot B'\cap g_j\cdot B'\neq\emptyset.$$

Aplicando g_{j-1}^{-1} se obtiene que

$$\begin{aligned}g_{j-1}^{-1}\cdot g_{j-1}\cdot B'\cap g_{j-1}^{-1}\cdot g_j\cdot B'&\neq\emptyset\\ B'\cap g_{j-1}^{-1}\cdot g_j\cdot B'&\neq\emptyset\end{aligned}$$

Por hipótesis ítem 3 se deduce que $g_{j-1}^{-1}\cdot g_j=s_j\in S$. Por lo tanto

$$g=g_n=g_{n-1}\cdot g_{n-1}^{-1}\cdot g_n=g_{n-2}\cdot g_{n-2}^{-1}\cdot s_n=\cdots=g_0\cdot s_1\cdots s_n=s_1\cdots s_n$$

es un elemento del subgrupo generado por S. Como g es un elemento arbitrario se sigue que S es un conjunto generador de G; en particular G es finitamente generado, puesto que S es finito.

ii) Sea $x\in X$.
Definimos el mapeo φ:

$$\begin{aligned}\varphi: G &\longrightarrow X\\ g &\longmapsto g\cdot x\end{aligned}$$

es una cuasi-isometría, demostraremos que φ es un embebimiento cuasi-isométrico con imagen cuasi-densa.

- Probaremos que φ tiene imagen cuasi-densa.
  Sea $x'\in X$.

Dado que las G-traslaciones de B cubren a X, existe un $g \in G$ tal que $x' \in g \cdot B$, como $x \in B$ cumple que $g \cdot x \in g \cdot B$, lo cual implica

$$\begin{aligned} d\left(x', \varphi\left(g\right)\right) &= d\left(x', g \cdot x\right) \\ &\leq \operatorname{diam}\, g \cdot B \\ &\leq \operatorname{diam}\, B \end{aligned}$$

Puesto que G actúa por isometrías en X, el diámetro de $g \cdot B$ es el diámetro de B, entonces por hipótesis ítem 1, B es finito.
Por lo tanto φ tiene imagen cuasi-densa.

- Probaremos que φ es un embebimiento cuasi-isométrico.
  Existen $c_1, c_2 \in \mathbb{R}_{>0}$ tal que para cualesquiera $g, h \in G$ se cumple que

$$\frac{1}{c_1} \cdot d_S\left(g, h\right) - c_2 \leq d\left(\varphi\left(g\right), \varphi\left(h\right)\right) \leq c_1 \cdot d_S\left(g, h\right) + c_2$$

  pero como G está denotado con la métrica de las palabras y este actúa por isometrías en X, para cualesquiera $g, h \in G$ tenemos que $d_S\left(g, h\right) = d_S\left(e, g^{-1} \cdot h\right)$ y además

$$\begin{aligned} d\left(\varphi\left(e\right), \varphi\left(g^{-1} \cdot h\right)\right) &= d\left(e \cdot x, g^{-1} \cdot h \cdot x\right) \\ &= d\left(g \cdot x, g \cdot g^{-1} \cdot h \cdot x\right) \\ &= d\left(g \cdot x, h \cdot x\right) \\ &= \left(\varphi\left(g\right), \varphi\left(h\right)\right) \end{aligned}$$

  de modo que es suficiente verificar que existen $c_1, c_2 \in \mathbb{R}_{>0}$ tal que para todo $g \in G$ sucede que:

$$\frac{1}{c_1} \cdot d_S\left(e, g\right) - c_2 \leq d\left(\varphi\left(e\right), \varphi\left(g\right)\right) \leq c_1 \cdot d_S\left(e, g\right) + c_2$$

  Sea $g \in G$, encontraremos una cota inferior de $d\left(\varphi\left(e\right), \varphi\left(g\right)\right)$ en términos de $d_S\left(e, g\right)$.
  Suponemos $x \in B$, puesto que G actúa por isometrías en X y las G-traslaciones de B cubren a X (ítem 2), tenemos:
  Sea $\gamma : [0, L] \longrightarrow X$ un (c, b)-cuasi-geodésico de x a $g \cdot x$ entonces el argumento de la primera parte muestra que

$$\begin{aligned} d\left(\varphi\left(e\right), \varphi\left(g\right)\right) &= d\left(x, g \cdot x\right) \\ &= d\left(\gamma\left(0\right), \gamma\left(L\right)\right) \end{aligned}$$

  Como γ es un embebimiento (c, b)-cuasi-isométrico tenemos:

$$\begin{aligned} d\left(\gamma\left(0\right), \gamma\left(L\right)\right) &\geq \frac{1}{c} \cdot d\left(0, L\right) - b \\ &= \frac{1}{c} \cdot L - b \end{aligned}$$

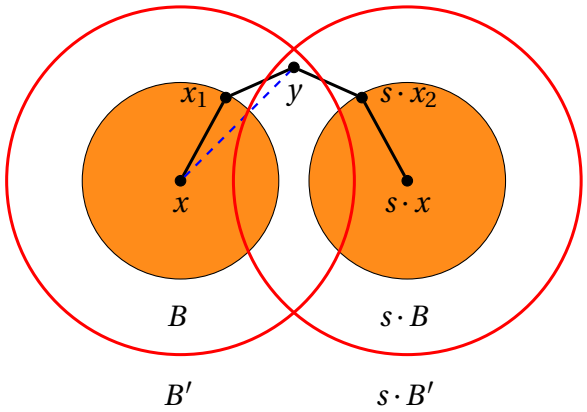
Tomando a $n \coloneqq \min\left\{ k \in \mathbb{N} \;\middle|\; L \cdot \frac{c}{b} \leq k \right\}$ escribimos a L como: $t_n \coloneqq L \geq \frac{b\cdot(n-1)}{c} = t_{n-1}$ lo cual implica que

$$\begin{aligned} d\left(\varphi(e), \varphi(g)\right) &\geq \frac{1}{c} \cdot L - b \\ &\geq \frac{1}{c} \cdot \left[\frac{b \cdot (n-1)}{c} \right] - b \\ &= \frac{b \cdot (n-1)}{c^2} - b \\ &= \frac{b}{c^2} \cdot n - \frac{b}{c^2} - b \\ &\geq \frac{b}{c^2} \cdot d_S(e, g) - \frac{b}{c^2} - b \end{aligned}$$

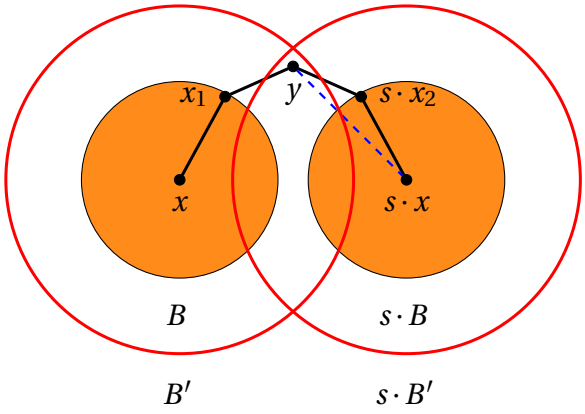
Esto sucede ya que g se puede escribir con n elementos de S lo cual implica que $d_S(e,g) = n$, existen $s_1, \ldots, s_n \in S$ tal que $g = s_1 \cdots s_n$ para S conjunto generador de G.
Ahora, encontraremos una cota superior de $d\left(\varphi(e), \varphi(g)\right)$ en términos de $d_S(e,g)$.
Pero antes de encontrar la cota superior requerida, verificamos que si $s \in S$ entonces $d(x, s\cdot x) \leq 2 \cdot (\text{diam } B + 2 \cdot b)$.
Sea $y \in B'$, existe $x_1 \in B$ tal que $d(x_1, y) \leq 2 \cdot b$, entonces:

$$\begin{aligned} d(x,y) &\leq d(x, x_1) + d(x_1, y) \qquad \text{; por desigualdad triangular} \\ &\leq \text{diam } B + 2 \cdot b \end{aligned}$$

Gráficamente es:



De manera similar para $y \in s \cdot B'$, se cumple que $d(y, s\cdot x) \leq \text{diam } B + 2\cdot b$, este resultado se muestra gráficamente:



Por otra parte, si $s \cdot B' \cap B' \neq \emptyset$ entonces $y \in B' \cap s \cdot B'$, existe algún $x_1 \in B'$ tal que $d(x_1, y) < 2 \cdot b$ y $s \cdot x_2 \in s \cdot B'$ tal que $d(s \cdot x_2, y) < 2 \cdot b$ por ende

$$\begin{aligned} d(x, s \cdot x) &\leq d(x, x_1) + d(x_1, y) + d(y, s \cdot x_2) + d(s \cdot x_2, s \cdot x) \\ &\leq \text{diam } B + 2 \cdot b + 2 \cdot b + \text{diam } B \\ &\leq 2 \cdot (\text{diam } B + 2 \cdot b) \end{aligned}$$

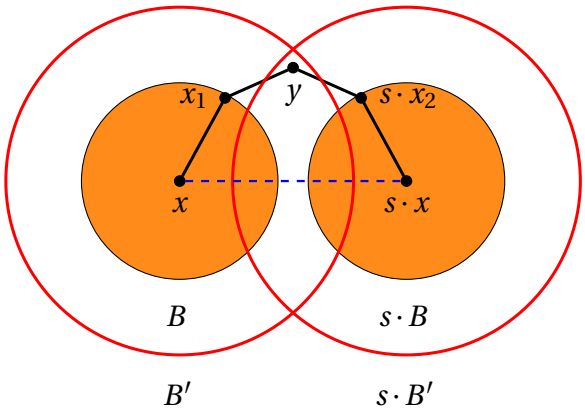


Figura 3.2. Si $s \in S$ entonces $d(x, y) \leq 2 \cdot (\text{diam } B + 2 \cdot b)$

Procedemos a encontrar la cota superior de $d(\varphi(e), \varphi(g))$ en términos de $d_S(e, g)$.
Sea $n = d_S(e, g)$, existen $s_1, \ldots, s_n \in S$ tal que $g = s_1 \cdots s_n$.
Aplicamos desigualdad triangular y por consiguiente $s_j \cdot B' \cap B' \neq \emptyset$, para todo

$j \in \{1, \ldots, n-1\}$ implica que

$$\begin{aligned} d\left(\varphi(e), \varphi(g)\right) &= d\left(x, g \cdot x\right) \\ &= d\left(x, s_1 \cdots s_n \cdot x\right) \\ &\leq d\left(x, s_1 \cdot x\right) + d\left(x, s_1 \cdots s_n \cdot x\right) \\ &\leq d\left(x, s_1 \cdot x\right) + d\left(s_1 \cdot x, s_1 \cdot s_2 \cdot x\right) + d\left(s_1 \cdot s_2 \cdot x, s_1 \cdots s_n \cdot x\right) \\ &= d\left(x, s_1 \cdot x\right) + d\left(s_1 \cdot x, s_1 \cdot s_2 \cdot x\right) + \ldots + d\left(s_1 \cdots s_{n-1} \cdot x, s_1 \cdots s_n \cdot x\right) \\ &= d\left(x, s_1 \cdot x\right) + d\left(x, s_2 \cdot x\right) + \ldots + d\left(x, s_n \cdot x\right) \\ &\leq 2 \cdot \left(\text{diam } B + 2 \cdot b\right) \cdot n \\ &= 2 \cdot \left(\text{diam } B + 2 \cdot b\right) \cdot d_S\left(e, g\right) \end{aligned}$$

Por hipótesis ítem 1 el diámetro de B es finito y las cotas encontradas tanto superior como inferior son:

$$c_1 = \text{máx}\left\{2 \cdot \left(\text{diam } B + 2 \cdot b\right), \frac{b}{c^2}\right\}$$

y

$$c_2 = -b - \frac{b}{c^2}$$

Por lo tanto, las cotas encontradas muestran que φ es un embebimiento cuasi-isométrico.

Así, el mapeo con respecto a la métrica de palabra es una cuasi-isometría.

□

El lema de Švarc-Milnor se puede formular desde un punto de vista topológico en el cual toman mayor importancia las propiedades de la acción del grupo sobre el espacio métrico. Antes de proporcionar la formulación topológica de Švarc-Milnor definimos lo siguiente:

Definición 3.13

Sea G un grupo y X un espacio topológico. Una acción de G en X es propia si para todo $K \subset X$ compacto, el conjunto $\left\{ \; g \in G \;\middle|\; g \cdot K \cap K \neq \emptyset \; \right\}$ es finito.

Definición 3.14

Sea G un grupo y X un espacio topológico. Una acción de G en X es co-compacta, si existe un $k \subset X$ compacto tal que

$$G \cdot K := \bigcup_{g \in G} g \cdot K = X$$

Corolario 3.1 (Formulación topológica de Švarc-Milnor)
Sea G un grupo que actúa por isometrías sobre un espacio métrico (X,d) propio y geodésico (no vacío). Además, supongamos que esta acción es propia y co-compacta. Entonces G se genera finitamente, y para todo $x \in X$ el mapeo

$$\begin{aligned} G &\longrightarrow X \\ g &\longmapsto g \cdot x \end{aligned}$$

es una cuasi-isometría.

Demostración. Notemos que como X es geodésico, en particular es un espacio $(1,\epsilon)$-cuasi-geodésico para cualquier $\epsilon \in \mathbb{R}_{>0}$. Necesitamos encontrar un $B \subset X$, por lo que aplicaremos las hipótesis de la proposición 3.6.

Dado que la acción de G sobre X es co-compacta, existe un subconjunto compacto $B \subset X$ tal que

$$\bigcup_{g \in G} g \cdot B = X.$$

es decir, las G-traslaciones de B cubren a X, puesto que X es un espacio métrico, B es acotado y por tanto B posee diámetro finito y además

$$B' := B_{2\cdot\epsilon}^{X,d}(B)$$

es de diámetro finito.
Ahora como X es propio, toda bola cerrada es compacta; en particular B' es compacto, luego como la acción de G sobre X es propio implica que el conjunto $\left\{ \; g \in G \;\middle|\; g \cdot B' \cap B' \neq \emptyset \; \right\}$ es finito.
Así se satisfacen todas las hipótesis de la primera versión del Lema de Švarc-Milnor. Por tanto G se genera finitamente por S y para todo $x \in X$ el mapeo

$$\begin{aligned} G &\longrightarrow X \\ g &\longmapsto g \cdot x \end{aligned}$$

es una cuasi-isometría. □

Bibliografía

[1] Löh, C. (2018). Geometric Group Theory: An Introduction (2017 ed.). Springer.

[2] I.N. Herstein. Abstract algebra - 3rd ed. (1995).

[3] Ma. Ángeles Moreno Frías , Enrique Pardo Espino. (2003). Teoría de Grupos.