Universidad de Cantabria

Facultad de Ciencias

EL TEOREMA DE INMERSIÓN DE HAHN

(Hahn's embedding theorem)

Trabajo de Fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autor: Jorge Martín Álvarez

Director: Jesús Javier Jiménez Garrido

Junio 2023

Agradecimientos

Este trabajo supone la culminación de mis estudios de Matemáticas en la Universidad de Cantabria. Entré en esta facultad con una vaga idea de lo que eran las matemáticas, y cinco años después estoy orgulloso de haber sufrido, pero sobre todo disfrutado, al enfrentarme a las numerosas lecciones, ejercicios y pruebas que han construido el matemático que pronto seré.

En primer lugar, quiero agradecer a mi director, Javier, la ayuda insustituible durante los últimos nueve meses. Sin sus detalladas aportaciones y valiosos consejos, estoy seguro de que el contenido de este texto sería mucho menos completo y organizado de lo que es hoy.

Debo señalar, además, que durante la realización de este trabajo fui beneficiario de una beca de colaboración otorgada por el Ministerio de Educación y Formación Profesional en el Departamento de Matemáticas, Estadística y Computación, al que agradezco su acogida.

Asimismo, doy las gracias a todos los profesores de matemáticas que he tenido durante el grado, tanto en Santander como en Innsbruck, con especial afecto para Fernando, Luis Miguel y Nuria, por haberme convertido en un amante más de esta preciosa disciplina, que como consecuencia seguiré cortejando durante al menos los dos próximos años. También a Bea y Teresa, con las que empecé este camino en el instituto.

A mis padres, por estar siempre ahí y brindarme día a día el mejor ambiente imaginable, y al resto de mi familia, por hacerme sentir que Liendo y Villaprovedo son también mi casa.

A Alejandro y Joseba, por esas charlas interminables en Cañadío, y al resto de doblegradistas, por haberme acompañado en esta loca aventura; también a Pablo, por venirse al lado oscuro a media carrera, a David, por llevarme a le Mans '66, y a Lucho, por comentar conmigo los partidos de Roland Garros. A Blanca y José Ángel por ser mi plan favorito de noche de viernes. A Manu y Pablo por las llamadas eternas y los encuentros olímpicos que siempre acaban con sueño. Y por último, a todas las personas maravillosas que conocí entre Bratislava, París e Innsbruck.

Resumen

Uno de los resultados fundamentales en la teoría de grupos ordenados es el Teorema de Inmersión de Hahn (1907), que proporciona una caracterización sencilla de todo grupo abeliano totalmente ordenado G mediante un isomorfismo con un subgrupo aditivo del producto lexicográfico $\mathbb{R}^\Gamma$, siendo Γ el conjunto de clases de equivalencia arquimedianas no nulas de G. El objetivo fundamental de este trabajo es desarrollar la teoría de grupos ordenados requerida para obtener una demostración autocontenida de este teorema. Para ello, será necesario probar en primer lugar el Teorema de Hölder, que se trata de una particularización del Teorema de Inmersión en grupos arquimedianos, en su caso isomorfos a subgrupos aditivos de $\mathbb{R}$. Posteriormente, para obtener la versión general del resultado necesitaremos tres resultados clave: la biyección entre las clases arquimedianas y los saltos en la cadena de subgrupos convexos de un grupo ordenado, la existencia de envolvente divisible de un grupo abeliano libre de torsión, y la construcción del producto lexicográfico de grupos ordenados. Finalmente, se estudiarán las aplicaciones del teorema, en especial su relación con la búsqueda de soluciones en forma de series de potencias de ecuaciones diferenciales.

Palabras clave: *grupos ordenados, Teorema de Inmersión de Hahn, Teorema de Hölder, clases de equivalencia arquimedianas, producto lexicográfico.*

Abstract

One of the most important results in the theory of ordered groups is Hahn's embedding theorem (1907), which provides a simple characterisation of every linearly ordered abelian group G by means of an isomorphism with an additive subgroup of the lexicographical product $\mathbb{R}^\Gamma$, where Γ is the set of non-zero Archimedean equivalence classes of G. The main goal of this work is to develop the theory of ordered groups needed to obtain a self-contained proof of this theorem. With this aim, it will be necessary to prove Hölder's theorem first, a particular version of Hahn's theorem in Archimedean groups, which are isomorphic to an additive subgroup of $\mathbb{R}$. Obtaining the general statement of the theorem next will require three essential results: the bijection between the set of Archimedean classes and the chain of convex subgroups of an ordered group, the existence of the divisible hull of a torsion-free abelian group, and the construction of the lexicographical product of ordered groups. In the end, applications of the theorem are studied, especially its relation with the search for power series solutions of differential equations.

Key words: *ordered groups, Hahn's embedding theorem, Hölder's Theorem, Archimedean equivalence classes, lexicographical product.*

Índice

1. Introducción **1**

2. Estructuras algebraicas ordenadas **3**
2.1. Bucles ordenados 3
2.2. Homomorfismos de bucles ordenados 9
2.3. Grupos ordenados 11

3. Órdenes arquimedianos **14**
3.1. Propiedad arquimediana 14
3.2. Teorema de Hölder 17

4. Producto lexicográfico **19**
4.1. Producto lexicográfico de grupos 19
4.2. Extensión lexicográfica de un grupo ordenado 22

5. Clases arquimedianas y cadenas de subgrupos **26**
5.1. Clases arquimedianas 26
5.2. Valoraciones de grupos 27
5.3. Familias de subgrupos 29
5.4. Consecuencias de la relación entre clases arquimedianas y subgrupos convexos . . 34

6. El Teorema de Inmersión de Hahn **37**
6.1. Grupo de Hahn y Teorema de Inmersión 37
6.2. Aplicaciones en la resolución de ecuaciones diferenciales 44
6.3. Valoraciones de cuerpos y Teorema de Kaplansky 48

I. Anexo. Relaciones de orden y ordinales **51**

II. Apéndice. Resultados de ordenabilidad en grupos **54**
II.1. Ordenabilidad en términos de semigrupos normales 54
II.2. Ordenabilidad en términos de series centrales de subgrupos 57
II.3. Grupos nilpotentes 60
II.4. Grupos libres 62

Índice alfabético **67**

Bibliografía **68**

1. Introducción

La teoría de estructuras algebraicas ordenadas tiene su origen en las últimas décadas del siglo XIX. La noción de orden es inherente a las matemáticas desde el momento en el que se empezaron a usar los números naturales para contar y *ordenar* colecciones finitas de objetos. No obstante, si bien las relaciones de orden fueron clave en numerosos resultados a lo largo de la historia, por ejemplo al trabajar con sucesiones, su definición formal no llegó hasta el desarrollo de la teoría de conjuntos moderna a finales del siglo XIX. B. Russell se refiere a esta situación y elabora una de los primeros estudios rigurosos sobre conjuntos ordenados [33]. Por su parte, la teoría de estructuras algebraicas, en particular la teoría de grupos, había surgido durante el siglo XIX como una herramienta útil en varios campos de las matemáticas. De la mano de J. L. Lagrange, P. Ruffini y finalmente É. Galois, el estudio de la resolución de ecuaciones polinómicas dio lugar a la teoría de grupos de permutaciones. En teoría de números, la aritmética modular considerada inicialmente por L. Euler y C. F. Gauß y más tarde por N. H. Abel condujo a las definiciones de grupo cíclico y abeliano por L. Kronecker. Asimismo, F. Klein y S. Lie introdujeron la estructura de grupo en la geometría [35].

En este contexto, la primera definición de grupo ordenado (en realidad de semigrupo) fue dada por O. Stolz en 1882, como una lista de siete axiomas que establecían lo que hoy conocemos como condición de compatibilidad entre orden y operación [36]. En los años posteriores siguieron tres trabajos fundamentales que permitieron entender y caracterizar las estructuras ordenadas. En primer lugar, O. Hölder probó en 1901 que todo grupo totalmente ordenado arquimediano es isomorfo a un subgrupo aditivo de los números reales [13]. Seis años más tarde, H. Hahn fue capaz de generalizar el resultado a grupos no necesariamente arquimedianos, al probar que cualquier grupo abeliano totalmente ordenado es isomorfo a un subgrupo del producto lexicográfico de $(\mathbb{R}, +)$ con índices en el conjunto de clases de equivalencia arquimedianas del grupo. Se conoce este resultado como Teorema de Inmersión de Hahn [11]. Finalmente, F. Hausdorff estudió con detalle la estructura de producto lexicográfico construida en el Teorema de Inmersión en 1914, proporcionando una nueva demostración del resultado y facilitando la comprensión y el manejo de los conceptos tratados por Hahn [12]. La vigencia del resultado se ha prolongado hasta la actualidad, en particular dada su aplicación a la búsqueda de soluciones de ecuaciones diferenciales en forma de series de potencias.

El objetivo de este trabajo es desarrollar la teoría de grupos ordenados necesaria para dar una demostración completa y autocontenida del Teorema de Inmersión de Hahn. En su artículo de 1907, Hahn presentó una prueba extensa y farragosa en términos de notación, debido a que la mayoría de las nociones que manejamos en el texto habían apenas sido definidas y no existía un consenso sobre su empleo. Por ejemplo, Hahn trabajó con los axiomas de Stolz en lugar de los conceptos que utilizamos hoy en día, y basó su demostración en construcciones sobre los ordinales, de tal modo que A. H. Clifford se refirió a ella como una "maratón transfinita" [4]. En su trabajo de 1914, Hausdorff dio una prueba notablemente más sencilla. Sin embargo, fue pasada por alto por las reseñas históricas posteriores, que citan las demostraciones surgidas en los años 50 como las primeras en simplificar la prueba de Hahn [7]. El mérito real de éstas fue generalizar el Teorema de Inmersión a diferentes estructuras, siguiendo el resultado de Kaplansky en 1942 que enuncia el equivalente en cuerpos valorados [18].

El texto principal de referencia en la elaboración del trabajo ha sido *Angeordnete Strukturen. Gruppen, Körper, projektive Ebenen*, publicado por la matemática alemana S. Prieß-Crampe en 1983 [30]. De ese modo, hemos seguido la línea de sus demostraciones en los principales resultados enunciados, en general extendiéndolas para lograr un desarrollo lo más completo posible. En particular, nos basamos en el trabajo de B. Banaschewski [1] para probar el Teorema de Inmersión, cuya demostración evita en gran medida el uso de ordinales simplificando considerablemente la notación. Otros textos consultados con frecuencia han sido [6], [17] y [20].

El trabajo consta de cinco capítulos, en el último de los cuales enunciamos y probamos el Teorema de Inmersión. Como hemos anticipado, el Teorema de Inmersión es una generalización a

grupos no necesariamente arquimedianos del Teorema de Hölder. Los Capítulos 2 y 3 establecen las bases de la teoría de estructuras algebraicas ordenadas y culminan con la demostración del Teorema de Hölder. En esta parte, se ha decidido trabajar con bucles en lugar de grupos. Los bucles son estructuras algebraicas que poseen todas las propiedades de grupo salvo la asociativa. En particular, en ellos se satisface la ley de cancelación, suficiente para probar muchos de los resultados sobre estructuras ordenadas. De este modo, realizamos un desarrollo paralelo a la teoría de grupos ordenados que nos permite enunciar resultados más generales, finalizando con el enunciado del Teorema de Hölder en términos de bucles. Adicionalmente, el Capítulo 2 incluye la construcción de la envolvente divisible de un grupo abeliano, que nos permitirá enunciar el Teorema de Hahn para grupos abelianos no necesariamente divisibles.

En los siguientes dos capítulos se introducen las herramientas necesarias para extender el Teorema de Hölder al Teorema de Inmersión de Hahn. De acuerdo con este último, la inmersión de Hahn de un grupo G se realiza sobre el llamado producto lexicográfico de tantas copias de $\mathbb{R}$ como clases de equivalencia arquimedianas no nulas tenga G. Así, el Capítulo 4 está dedicado a construir el producto lexicográfico de una familia de grupos y dotarlo de una estructura de grupo ordenado. En otro orden de ideas, en el Capítulo 5 definimos las clases de equivalencia arquimedianas de un grupo ordenado, y demostramos que existe una biyección entre éstas y los factores de la cadena de subgrupos convexos, de modo que los factores son grupos arquimedianos.

Los argumentos anteriores nos conducen a demostrar el Teorema de Inmersión de Hahn en el Capítulo 6. Dado un grupo abeliano totalmente ordenado G, consideraremos su envolvente divisible $\bar{G}$, y a partir de ella el producto lexicográfico de los factores de la cadena de subgrupos convexos de $\bar{G}$, que son arquimedianos. Aplicando el Teorema de Hölder a cada uno de ellos, habremos encontrado la inmersión buscada. Para terminar, estudiamos las aplicaciones de la construcción de Hahn a la búsqueda de soluciones de ecuaciones diferenciales ordinarias en forma polinómica, e introducimos brevemente el análogo de la teoría en cuerpos valorados.

Asimismo, los conceptos introducidos nos permiten obtener con relativa facilidad resultados que, sin estar relacionados con el Teorema de Inmersión, permitirán al lector interesado profundizar en la teoría de grupos ordenados. De especial interés resulta el estudio de la ordenabilidad de un grupo. Así, incluimos en el texto dos caracterizaciones de grupo ordenable que surgen como el recíproco de sendos resultados sobre grupos ordenados, y dedicamos el Apéndice a buscar condiciones que garantizan la ordenabilidad de un grupo. En particular, probamos que los grupos nilpotentes y los grupos libres son ordenables. Por su parte, el Anexo contiene las nociones y resultados básicos de la teoría de ordinales que empleamos durante el trabajo.

Notación

De forma general, denotaremos a los bucles por $(L, +)$ y a los grupos por $(G, \cdot)$, reservando la notación aditiva en grupos para el caso abeliano. La razón para trabajar con notación aditiva en bucles es que el desarrollo de la teoría de bucles ordenados se dirige hacia el Teorema de Hölder, enunciado para bucles arquimedianos y asociativos para potencias, que son en realidad grupos abelianos.

Siguiendo su definición como ordinal en el Anexo, trabajaremos con el conjunto de los números naturales $\mathbb{N} = \{0, 1, 2, 3, ...\}$, y denotaremos $\mathbb{N}_{\geq k} := \{n \in \mathbb{N} : n \geq k\}$ para $k \in \mathbb{N}$. Extenderemos esta notación a conjuntos totalmente ordenados cualesquiera cuando sea necesario. Del mismo modo, los conjuntos de los números enteros, racionales, reales y complejos se denotan por $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$, respectivamente. Se supondrá en ellos el orden usual si no se indica lo contrario.

Dados dos conjuntos A y B, denotaremos $A \subseteq B$ si A es subconjunto de B y $A \subsetneq B$ si es un subconjunto propio. De igual modo, dado un grupo G y dos subgrupos $A, B \subseteq G$, se denotará $A \triangleleft B$ si A es un subgrupo normal de B. Además, dado un conjunto A, destacamos la distinción entre el subgrupo generado por A dentro de un grupo, que denotamos por $\langle A \rangle$, y el subespacio vectorial generado por A en un $\Bbbk$-espacio vectorial, que denotamos por $\Bbbk\langle A \rangle$.

2. Estructuras algebraicas ordenadas

Los textos elementales sobre estructuras algebraicas suelen excluir la noción de relación de orden, dado que la mayor parte de resultados relevantes sobre grupos o anillos son independientes de la existencia de una ordenación de sus elementos. No obstante, muchas de las estructuras con los que se trabaja normalmente tienen un orden subyacente, o al menos admiten una ordenación que respeta la estructura algebraica, como sucede de forma natural en $\mathbb{Z}$ ó $\mathbb{R}$. En este capítulo introducimos rigurosamente el concepto de orden en estructuras con una operación interna, en particular en bucles y grupos. Recordamos que los bucles satisfacen todas las propiedades de los grupos salvo la asociativa. La mayoría de los resultados fundamentales sobre estructuras ordenadas sólo precisan de la ley de cancelación, que también es válida en bucles. En concreto, como se ha mencionado en la introducción, desarrollamos la teoría de bucles ordenados con el objetivo de obtener una versión para bucles del Teorema de Hölder, que probaremos en el Capítulo 3.

En la misma línea, finalizamos el capítulo introduciendo la noción de grupo abeliano divisible. Probaremos que todo grupo abeliano y libre de torsión tiene una envolvente divisible, que además es totalmente ordenada si lo es el grupo inicial. Más tarde, el concepto de envolvente divisible también será clave en la demostración del Teorema de Inmersión de Hahn, puesto que nos permitirá extender un primer resultado parcial aplicable únicamente a grupos divisibles a grupos abelianos en general.

2.1. Bucles ordenados

Comenzamos recordando las definiciones de las estructuras algebraicas más simples con una operación interna, entre las que se encuentran los bucles.

Definición 2.1. Un conjunto L no vacío dotado de una operación binaria interna $+ : L \times L \to L$ se denomina **magma**. Se consideran en un magma las siguientes propiedades:

(I) Existe un elemento neutro $0 \in L$ tal que $a + 0 = 0 + a = a$ para todo $a \in L$.

(II) Para todos $a, b \in L$, las ecuaciones $x + a = b$ y $a + y = b$ tienen solución única.

Un magma se llama **magma unitario** si satisface la propiedad (I), y **bucle** si satisface (I) y (II) al mismo tiempo.

Observación 2.2. Aclaremos algunos aspectos respecto de la definición previa.

1. Como en el caso de grupos, el elemento neutro es único. En efecto, si suponemos $e_1, e_2 \in L$ neutros, tenemos que $e_1 = e_1 + e_2 = e_2$. De ahí que, en la definición y a lo largo de todo el documento, lo denotemos por 0 en notación aditiva y e en notación multiplicativa.

2. Nótese que la propiedad (II) garantiza la ley de cancelación: si $c + a = x + a$, entonces, por la unicidad de solución, tenemos que $x = c$. De hecho, si L es finito, ambas propiedades son equivalentes, puesto que la ley de cancelación garantiza que la tabla de Cayley de L es un cuadrado latino, es decir, cada elemento aparece exactamente una vez en cada fila o columna. Por este motivo, las ecuaciones de (II) tienen solución única.

   No obstante, la equivalencia no se da en general. Basta considerar $(\mathbb{N}, +)$, que es un magma unitario que verifica la ley de cancelación. Sin embargo, la ecuación $n + 1 = 0$ no tiene solución.

3. Asimismo, la propiedad (II) implica la existencia de inverso por izquierda y derecha, no necesariamente iguales. Sin embargo, el recíproco no es cierto en general. El ejemplo más

sencillo es el conjunto $A = \{0, a, b\}$ con la operación $+$ descrita por la tabla de Cayley:

$+$	0	a	b
0	0	a	b
a	a	a	0
b	b	0	b

con elemento neutro y donde todo elemento tiene inverso único por ambos lados, pero sin la ley de cancelación. En otras palabras, $(A, +)$ es un magma unitario con inverso que no es bucle.

Por otro lado, la existencia de inverso por izquierda y derecha es independiente de la ley de cancelación. Basta observar que los dos ejemplos citados son contraejemplos de las dos implicaciones, respectivamente.

Ejemplos.

1. Todo grupo es a su vez un bucle, que tiene además la propiedad asociativa.
2. Los números enteros con la operación resta $(\mathbb{Z}, -)$ forman un bucle que no es grupo. En efecto, 0 es el elemento neutro, las ecuaciones $x - a = b$ y $a - y = b$ tienen como soluciones únicas $x = a + b$ e $y = a - b$, pero, en general, no se da la igualdad $(a - b) - c = a - (b - c)$.

Como conjuntos, se puede dotar a un bucle o grupo de un orden entre sus elementos. Especialmente interesantes son los casos en los que la relación de orden es compatible con la estructura algebraica, como sucede con el orden usual en $\mathbb{Z}$ ó $\mathbb{R}$. Formalizamos esta idea a continuación.

Definición 2.3. Sean L un bucle y $\leq$ una relación de orden sobre L.

(I) Se dice que $(L, \leq)$ es un **bucle** (parcialmente) **ordenado** si el orden es compatible con la operación en L, esto es, si para todos $a, b, c \in L$,

$$a \leq b \quad \Rightarrow \quad (a + c \leq b + c) \wedge (c + a \leq c + b).$$

Si el orden $\leq$ es total, se dice que el **bucle** es **totalmente ordenado**.

(II) Un elemento $a \in L$ se llama **positivo** o **negativo** si $a > 0$ ó $a < 0$, respectivamente. Se definen así los conjuntos de positivos $P = \{a \in L : a > 0\}$ y negativos $N = \{a \in L : a < 0\}$, también llamados **conos positivo** y **negativo**, respectivamente.

(III) Un **grupo** $(G, \cdot)$ se dice **ordenado** si lo es como bucle.

Recíprocamente, se dice que un bucle o grupo es **ordenable** si admite un orden total compatible con su estructura.

La definición anterior, basada en la compatibilidad entre el orden y la operación, se puede extender de forma análoga a cualquier estructura algebraica con una operación binaria interna. En particular, haremos uso de ella puntualmente en el caso de semigrupos en el Capítulo 6. Por otro lado, nótese que en un grupo, por la propiedad compatibilidad resulta que $a \in P$ si y sólo si $a^{-1} \in N$, y se puede identificar N con $P^{-1} = \{a \in G : a^{-1} \in P\}$.

Ejemplos.

1. Con el orden usual, $(\mathbb{Z}, +)$ es un bucle, y de hecho un grupo, totalmente ordenado.
2. El siguiente es un ejemplo de bucle totalmente ordenado que no es asociativo, y por tanto no es grupo. Consideramos $(\mathbb{R}, \star_p)$ con la operación dada

$$\forall a, b \in \mathbb{R} : a \star_p b = \begin{cases} a + b & \text{si } ab \geq 0, \\ a + pb & \text{si } ab < 0 \wedge |a| \geq p|b|, \\ p^{-1}a + b & \text{si } ab < 0 \wedge |a| < p|b|, \end{cases}$$

donde $p \neq 1$ es un número real positivo. Veamos primero que $(\mathbb{R}, \star_p)$ es un bucle ordenado. Observamos que es magma unitario, con 0 como neutro. Consideremos la ecuación $a = x \star_p b$, y los siguientes casos:

- Si $0 \leq b \leq a$ ó $a \leq b \leq 0$, entonces $x = a - b$ es solución, puesto que se opera con b según el primer caso. En efecto, tenemos que $xb = (a-b)b \geq 0$ para las dos relaciones entre a y b.

Razonando de forma análoga, tenemos que

- Si $b < 0 \leq a$ ó $a \leq 0 < b$, entonces $x = a - pb$ es solución, operando según el segundo caso.
- Si $b < a < 0$ ó $0 < a < b$, entonces $x = p(a - b)$ es solución, ya que se opera con b según el tercer caso.

Así, la ecuación tiene solución única. El desarrollo para la ecuación $a = b \star_P y$ es idéntico, y concluimos que $(\mathbb{R}, \star_p)$ es un bucle.

Por último, comprobemos que el orden usual es compatible con $\star_p$. Empezando por la operación por la derecha, dados $a < b$ y $c \in \mathbb{R}$, se debe comprobar que la compatibilidad se verifica en todos los casos siguientes:

	$bc \geq 0$	$bc < 0 \wedge \lvert b\rvert \geq p\lvert c\rvert$	$bc < 0 \wedge \lvert b\rvert < p\lvert c\rvert$
$ac \geq 0$	(1.1)	(1.2)	(1.3)
$ac < 0 \wedge \lvert a\rvert \geq p\lvert c\rvert$	(2.1)	(2.2)	(2.3)
$ac < 0 \wedge \lvert a\rvert < p\lvert c\rvert$	(3.1)	(3.2)	(3.3)

En los elementos diagonales, a y b se operan con c de la misma manera y se verifica trivialmente la condición de compatibilidad. Demostramos, a modo de ejemplo, el caso (1.2), ya que los razonamientos se repiten en el resto. Suponemos que $ac \geq 0$, $bc < 0$ y $|b| \geq pc$. Dado que $a < b$, debemos tener que $a \leq 0 < b$ con $c < 0$. Tenemos entonces que $a \star_p c = a + c$, $b \star_p c = b + pc$, y por ser $|b| \geq p|c|$,

$$a + c \leq c < 0 \leq b + pc.$$

Las mismas comparaciones, sustituyendo p por su inverso al utilizar la definición de $\star_p$, llevan a probar que el orden es también compatible al operar por la izquierda, y por tanto, concluir que tenemos un bucle ordenado. Sin embargo, no es asociativo, puesto que

$$((-p) \star_p 1) \star_p (-p^{-1}) = 0 \star_p (-p^{-1}) = -p^{-1},$$

mientras que

$$(-p) \star_p (1 \star_p (-p^{-1})) = (-p) \star_p 0 = -p,$$

que son distintos por ser $p \neq 1$ positivo.

Para referirse a la propiedad de compatibilidad, se dice también que el orden es invariante por translaciones, viendo la operación por un elemento fijo como una translación. En ese sentido, tenemos el siguiente resultado.

Lema 2.4. *Sea $(L, +)$ un bucle. Entonces, fijado un elemento $a \in L$, las aplicaciones*

$$\tau_r^a : x \longmapsto x + a, \quad \tau_l^a : x \longmapsto a + x$$

son biyecciones. Además, si L es ordenado, preservan el orden.

Demostración. Por la Definición 2.1 (II), la solución de $y = x + a = \tau_r^a(x)$ existe y es única para todo $y \in L$, y análogamente para τ_l. El orden entre dos elementos se preserva entre sus imágenes por la propiedad de compatibilidad. □

Observación 2.5. La compatibilidad del orden con la operación se puede expresar también con desigualdades estrictas. Como hemos visto en el Lema 2.4, las translaciones son biyecciones, y en consecuencia, dos elementos son iguales si y sólo si lo son sus transladados.

Asimismo, la compatibilidad funciona también en sentido contrario, es decir,

$$a + c \leq b + c \quad \Rightarrow \quad a \leq b.$$

En efecto, dados $a, b, c \in L$ tales que $a+c < b+c$, si fuera $a \geq b$ tendríamos que $a+c \geq b+c$, en contradicción con la hipótesis. La igualdad se preserva por translaciones, de donde deducimos el resultado. Análogamente al operar por la izquierda.

Observemos que ser invariante por translaciones por la derecha (o izquierda respectivamente) no es suficiente para la compatibilidad por ambos lados, como vemos a continuación.

Ejemplo. En $(\mathbb{Z}, -)$ con el orden usual, la operación es compatible al operar por la derecha, pero no al hacerlo por la izquierda. Por ejemplo, dados $0 \leq a < b$, tenemos que $a \leq b$, pero no es cierto que $0 - a \leq 0 - b$.

Consideremos el siguiente ejemplo más elaborado. Tomemos el subgrupo de $GL(2, \mathbb{R})$:

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{R}, b > 0 \right\},$$

junto con la relación de orden dada por

$$\begin{pmatrix} 1 & a_1 \\ 0 & b_1 \end{pmatrix} \leq \begin{pmatrix} 1 & a_2 \\ 0 & b_2 \end{pmatrix} \Leftrightarrow (a_1 \leq a_2) \vee ((a_1 = a_2) \wedge (b_1 \leq b_2)).$$

Tomemos ahora tres matrices

$$A_1 = \begin{pmatrix} 1 & a_1 \\ 0 & b_1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & a_2 \\ 0 & b_2 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & a_3 \\ 0 & b_3 \end{pmatrix}.$$

Operando, se tiene para $i \in \{1, 2\}$:

$$A_i A_3 = \begin{pmatrix} 1 & a_3 + a_i b_3 \\ 0 & b_i b_3 \end{pmatrix}, \quad A_3 A_i = \begin{pmatrix} 1 & a_i + a_3 b_i \\ 0 & b_3 b_i \end{pmatrix}.$$

Por un lado, si $A_1 \leq A_2$:

- Bien $a_1 < a_2$, en cuyo caso $a_3 + a_1 b_3 < a_3 + a_2 b_3$.
- Bien $a_1 = a_2$ y $b_1 \leq b_2$, y entonces $a_3 + a_1 b_3 = a_3 + a_2 b_3$, y $b_1 b_3 \leq b_2 b_3$.

En cualquier caso, resulta $A_1 A_3 \leq A_2 A_3$. Sin embargo, tomando

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},$$

tenemos que $A_1 < A_2$ pero

$$A_3 A_1 = \begin{pmatrix} 1 & 4 \\ 0 & 2 \end{pmatrix} > \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} = A_3 A_2.$$

Definimos a continuación concepto de orden dual en un conjunto, que emplearemos más adelante en el texto.

Definición 2.6. Sea $(A, \leq)$ un **conjunto ordenado**. Se conoce como **dual** al propio conjunto $(A, \leq_D)$ con el orden dado por:

$$x \leq_D y \quad \Leftrightarrow \quad y \leq x.$$

Proposición 2.7. *Dado un bucle (totalmente) ordenado $(L, +, \leq)$, también es (totalmente) ordenada su estructura dual $(L, +, \leq_D)$.*

Demostración. La relación $\leq_D$ es de orden por serlo $\leq$ y es total si y sólo si lo es $\leq$. Por otro lado, es compatible con la operación en L: dados $a, b \in L$, se tiene para todo $c \in L$

$$a \leq_D b \quad \Leftrightarrow \quad b \leq a \quad , \quad c + b \leq c + a \quad \Leftrightarrow \quad c + a \leq_D c + b,$$

luego se cumple la propiedad de compatibilidad por la izquierda. Análogamente podemos razonarlo al operar por la derecha. □

De aquí en adelante, nos centraremos en estructuras con orden total, puesto que el resultado principal del texto se refiere a grupos totalmente ordenados. No obstante, seguiremos hablando de orden en general (no necesariamente total) en los casos en los que las definiciones o resultados coincidan. Veremos que un orden total en un bucle está determinado unívocamente al definir un subconjunto P con ciertas propiedades, que será precisamente el cono positivo del bucle ordenado. En este sentido, nos interesa deducir algún resultado que nos permita trabajar con él fácilmente.

Proposición 2.8. *Sean $a \in L$, P el cono positivo de L, y $a + P = \{a + p : p \in P\}$. Entonces, son equivalentes*

(1) $a < b$.

(2) $b \in a + P$.

(3) $b \in P + a$.

Demostración. Veremos primero que (1) equivale a (2). Supongamos $a < b$. Por la propiedad (II) de la Definición 2.1, existe un único $c \in L$ tal que $b = a + c$. Dado que $b = a + c > a$, tenemos por la Observación 2.5 que $c > 0$, luego $b = a + c \in a + P$. Alternativamente, si $b = a + p$ con $p > 0$, resulta $a = a + 0 < a + p = b$.

La equivalencia entre (1) y (3) es análoga, operando por la izquierda. □

Nos preguntamos a continuación cómo caracterizar el cono positivo P de un bucle totalmente ordenado. Sabemos, por la definición, que $0 \notin P$, y podemos deducir que la intersección con el cono negativo N debe ser vacía. En la Proposición 2.8, hemos visto, además, que se tiene que $a + P = P + a$ para todo elemento $a \in L$, lo que recuerda a la propiedad de normalidad en subgrupos. Veremos, en lo siguiente, si estas condiciones son suficientes, o si debemos considerar alguna más. Extendemos primero la noción de normalidad a subconjuntos cualesquiera de un bucle, con una condición más general debida a la no asociatividad en bucles.

Definición 2.9. Sea $(L, +)$ un bucle. Un **subconjunto** $H \subseteq L$ se dice **normal** si satisface la siguiente propiedad: para todos $a, b \in L$ se satisfacen las igualdades:

$$(a + b) + H = a + (b + H) = (a + H) + b.$$

Observación 2.10. Tomando $a = 0$ en la definición anterior, resulta $b + H = (0 + H) + b = H + b$ para todo $b \in L$. Así, la definición es coherente con la de normalidad en subconjuntos de un grupo.

La propiedad de normalidad en subgrupos es la que permite considerar el grupo cociente. Tenemos la misma propiedad en bucles, donde se define un subbucle del modo siguiente.

Definición 2.11. Sea $(L,+)$ un bucle. Un subconjunto $S \subseteq L$ se denomina **subbucle** si verifica las propiedades:

(I) El elemento neutro $0 \in S$.

(II) Para todos $a, b \in S$, $a+b \in S$.

(III) Las ecuaciones $x+a=b$ y $a+y=b$ tienen solución en S.

La estructura cociente guarda también un paralelismo directo con el caso de los grupos.

Definición 2.12. Dados un bucle L y un subbucle normal H, se define el **bucle cociente** de L sobre H al conjunto de clases $L/H = \{a+H : a \in L\}$ con la operación

$$\begin{array}{rccc} +: & (L/H)\times(L/H) & \longrightarrow & L/H \\ & (a+H, b+H) & \longmapsto & (a+b)+H \end{array} .$$

La operación está bien definida por ser H normal, y por tanto $(L/H,+)$ es un bucle. Esto no tiene por qué ocurrir en general. Con todo ello, estamos en condiciones de enunciar el resultado de caracterización del cono positivo, en cuya prueba nos ayudamos del texto de R. H. Bruck [2].

Teorema 2.13. *Un bucle $(L,+)$ no trivial admite estructura de bucle totalmente ordenado si y sólo si contiene dos subconjuntos no vacíos P, N con las siguientes propiedades:*

(1) $\{0\} \cup P \cup N = L$, $P \cap N = \varnothing$, $0 \notin P \cup N$.

(2) $P + P \subseteq P$.

(3) P *es normal en* L.

Demostración. Consideremos un bucle totalmente ordenado $(L,+)$ no trivial, y sean P y N los conos positivo y negativo de L, respectivamente. Como la relación de orden en L es total, se tiene que $\{0\} \cup P \cup N = L$. Por definición, P y N no contienen a 0, mientras que cualquier elemento $a \in P \cap N$ cumple que $a > 0$ y $a < 0$, lo cual es imposible. Por tanto, se tiene (1).

Dados dos elementos $a, b \in P$, se tiene por ser bucle ordenado que $a+b > 0+b = b > 0$, luego P es cerrado respecto de la operación binaria, lo que prueba (2).

Veamos ahora que P es normal. Tenemos que probar que si tomamos $a, b \in L$, entonces se verifica $(a+b)+P = a+(b+P) = (a+P)+b$. Consideramos $x \in L$, y $c \in L$ el único elemento tal que $a+c=x$. Se verifica la siguiente cadena de equivalencias:

$$x \in a+(b+P) \quad \Leftrightarrow \quad c \in b+P \quad \Leftrightarrow \quad c > b \quad \Leftrightarrow \quad a+c > a+b,$$

lo que equivale a $x \in (a+b)+P$. La otra igualdad se prueba de forma análoga y se concluye que P es normal.

Recíprocamente, sea $(L,+)$ un bucle con las propiedades (1), (2) y (3). Definimos el orden sobre L dado por:

$$a < b \quad \Leftrightarrow \quad b \in a+P.$$

Veamos que se trata de un orden total. En primer lugar, consideramos dos elementos $a, b \in L$. Por el Lema 2.4, la unión $\{a\} \cup (a+P) \cup (a+N)$ está en biyección con $\{0\} \cup P \cup N$, que por (1) es todo el bucle L. Así, b está en alguno de los tres conjuntos, y por tanto está relacionado con a por $\leq$.

La propiedad antisimétrica está garantizada por ser $P \cap N = \varnothing$. Respecto a la transitiva, sean $a, b, c \in L$ con $a < b$ y $b < c$, es decir, $b \in a+P$ y $c \in b+P$. Veamos que $c \in a+P$. Como

L es un bucle y $b \in a + P$, existe un único $p \in P$ tal que $b = a + p$. Por (3), P es normal, y en consecuencia

$$b + P = (a + p) + P = a + (p + P) \subseteq a + P,$$

donde la última inclusión es cierta por (2). Entonces, $c \in a + P$, es decir, $a < c$. Queda por probar la compatibilidad con la estructura de bucle. Si $a < b$, tenemos $b \in a + P$, luego para cualquier $c \in L$, de nuevo por (3):

$$(a + P) + c = (a + c) + P,$$

y así $b + c \in (a + c) + P$, esto es, $a + c < b + c$. El caso de operar por la derecha es análogo. □

Observación 2.14. Notemos que, si se dan las propiedades (1), (2) y (3) del Teorema, se cumplen también (2) y (3) para el cono negativo N. En efecto, N es cerrado análogamente a P, y también es normal en L, usando (1) y las biyecciones del Lema 2.4.

El resultado se puede adaptar a bucles parcialmente ordenados, sin más que retirar la condición $\{0\} \cup P \cup N = L$ de (1).

En el caso de un grupo, recordemos que $N = P^{-1}$. El resultado anterior se puede probar de forma mucho más directa, si bien la prueba anterior es igualmente válida para grupos.

Corolario 2.15. *Un grupo $(G, \cdot)$ no trivial admite estructura de grupo totalmente ordenado si y sólo si contiene un subconjunto no vacío P con las propiedades:*

(1) $\{e\} \cup P \cup P^{-1} = L$, $P \cap P^{-1} = \varnothing$.

(2) $P \cdot P \subseteq P$.

(3) P *es normal en* G.

Para finalizar esta introducción sobre bucles ordenados, introducimos la noción de subconjunto convexo, que utilizaremos a menudo en lo que resta de texto.

Definición 2.16. Dado un conjunto ordenado $(A, \leq)$, se dice que un **subconjunto** C es **convexo** respecto al orden $\leq$ si para todos $a_1, a_2 \in C$, $x \in A$ tales que $a_1 < x < a_2$, entonces también $x \in C$.

Ejemplos.

1. Los intervalos en $\mathbb{R}$ son conjuntos convexos.
2. En $\mathbb{R}^2$ con el orden lexicográfico, el círculo unidad es convexo con la topología usual, pero no respecto del orden. Basta tomar $a_1 = (-1/2, 0), a_2 = (1/2, 0)$ y $x = (0, 2)$.

Observación 2.17. Dado un subconjunto convexo $H \subseteq L$ de un bucle, resulta que para todo $x \in L$, el subconjunto $x + H$ también es convexo. En efecto, tomemos $a, b \in H$ e $y \in L$ tal que $x + a \leq y \leq x + b$. Entonces, podemos escribir $y = x + c$ con $c \in L$ único, y así resulta, por compatibilidad, $a \leq c \leq b$. Por ser H convexo, resulta $c \in H$ y, en consecuencia, $y \in x + H$.

2.2. Homomorfismos de bucles ordenados

Tras definir la noción de bucle ordenado, el paso natural es preguntarse sobre las aplicaciones entre ellos. De la misma forma que en cualquier estructura algebraica, una aplicación entre bucles se llama homomorfismo de bucles si conmuta con la operación interna. En el caso de bucles ordenados, podemos imponer una condición más a los morfismos de forma que se preserve el orden entre elementos.

Definición 2.18. Una aplicación entre dos bucles ordenados $\varphi : (L_1, +, \leq) \to (L_2, \star, \preceq)$ se llama **homomorfismo de bucles ordenados** u ***o*-homomorfismo** si verifica las condiciones siguientes:

(I) φ es homomorfismo de bucles, es decir, para todos $a, b \in L_1$, $\varphi(a+b) = \varphi(a) \star \varphi(b)$.

(II) φ preserva el orden, esto es, si $a, b \in L_1$ con $a \leq b$, entonces $\varphi(a) \preceq \varphi(b)$.

Si φ es además biyectivo, se dice que es un ***o*-isomorfismo**, y se denota $L_1 \cong_o L_2$.

En la Definición 2.18, nótese que en general, un o-homomorfismo no preserva las desigualdades estrictas, y esto será clave para definir una estructura de bucle cociente ordenado. Dado un subbucle $H \subseteq L$ normal y convexo, la normalidad nos permitirá considerar el bucle cociente L/H, y la convexidad, dotarlo de una relación de orden inducida por H a partir del orden en L.

Proposición 2.19. *Sea $(L, \leq)$ un bucle totalmente ordenado.*

(1) El núcleo de cualquier homomorfismo entre L y otro bucle ordenado es un subbucle normal de L. Si, adicionalmente, se trata de un homomorfismo de bucles ordenados, entonces el núcleo es convexo.

(2) Sean H un subbucle normal convexo y P el cono positivo de L. Entonces, el bucle cociente L/H es totalmente ordenado, según la relación de orden dada por

$$a + H \prec b + H \quad \textit{si y sólo si} \quad (a < b) \wedge (a + H \neq b + H),$$

cuyo cono positivo es

$$P(L/H) = \{p + H : p \in P \setminus H\},$$

y el epimorfismo canónico $\pi : L \to L/H$ es o-homomorfismo.

(3) Si $\varphi : L \to L'$, donde L' es otro bucle ordenado, es un o-epimorfismo, entonces $L/\ker\varphi$ y L' son o-isomorfos.

Demostración.

(1) Denotaremos por $0'$ el elemento neutro en un bucle cualquiera L'. Sea $\varphi : L \to L'$ un homomorfismo y $\ker\varphi = \{h \in L : \varphi(h) = 0'\}$ su núcleo.

Veamos, en primer lugar, que $\ker\varphi$ es subbucle. Por ser φ homomorfismo, $\varphi(0) = 0'$, luego $0 \in \ker\varphi$. Dados $a, b \in \ker\varphi$, entonces $\varphi(a+b) = \varphi(a) + \varphi(b) = 0'$, esto es, $a + b \in \ker\varphi$. Además, si $a, b \in \ker\varphi$, y $x, y \in L$ son los únicos elementos tales que $x + a = b$, $a + y = b$, tenemos que

$$0' = \varphi(b) = \varphi(x) + \varphi(a) = \varphi(x),$$

e igualmente $\varphi(y) = 0'$. En consecuencia, $x, y \in \ker\varphi$.

Probemos ahora que es normal. Dados $a, b \in L$, tenemos que ver que $(a+b) + \ker\varphi = a + (b + \ker\varphi) = (a + \ker\varphi) + b$. Consideramos $x = (a+b) + h$, con $\varphi(h) = 0$. Por ser L un bucle, existen $h_1, h_2 \in L$ únicos tales que $x = a + (b + h_1) = (a + h_2) + b$. Vemos entonces que

$$\varphi(x) = \varphi(a) + \varphi(b) = \varphi(a) + (\varphi(b) + \varphi(h_1)),$$

y aplicando dos veces la ley de cancelación, obtenemos $\varphi(h_1) = 0'$. Análogamente, empleando que $x = (a + h_2) + b$, tenemos que $\varphi(h_2) = 0'$. Así, hemos probado que $(a+b) + \ker\varphi$ es subconjunto de $a + (b + \ker\varphi)$ y $(a + \ker\varphi) + b$. Las inclusiones opuestas se prueban del mismo modo, y tenemos que los tres conjuntos son iguales, así que $\ker\varphi$ es un subbucle normal de L.

Por otro lado, veamos que si φ es además o-homomorfismo, entonces es convexo. En efecto, si $h_1, h_2 \in \ker\varphi$, y $h_1 < x < h_2$, entonces $0' = \varphi(h_1) \leq \varphi(x) \leq \varphi(h_2) = 0'$, así que $x \in \ker\varphi$.

(2) Consideramos la relación siguiente sobre L/H:

$$a + H \prec b + H \quad \text{si y sólo si} \quad (a < b) \wedge (a + H \neq b + H).$$

Veamos que no depende de los representantes escogidos. Consideremos $a, a', b, b' \in L$ tales que $a+H = a'+H, b+H = b'+H$, $a < b$ y $a+H \neq b+H$. Tenemos que ver que la relación entre $a' + H$ y $b' + H$ es la misma. De forma automática se tiene $a' + H \neq b' + H$. Veamos que $a' < b'$, suponiendo por reducción al absurdo que $a' \geq b'$. Por ser $a + H = a' + H$, existe $h \in H$ tal que $a' = a + h$, y entonces tenemos

$$b' \leq a' = a + h < b + h,$$

con $b' \in b' + H = b + H$. En consecuencia, por convexidad (Observación 2.17), se tiene que $b + H = b' + H = a' + H = a + H$, en contradicción con la hipótesis.

Una vez probada la buena definición de la relación de orden $\preceq$, están garantizadas las propiedades reflexiva, antisimétrica y transitiva por cumplirse con $\leq$, así como el orden total y la compatibilidad con la operación en el cociente. Por tanto, tenemos una estructura de bucle totalmente ordenado sobre L/H. Estudiemos el cono positivo $P(L/H)$. Dado $a \in L$, se tiene que $0 + H \prec a + H$ si y sólo si $0 < a$ y $a \notin H$. Así, el conjunto $P(L/H)$ resulta de tomar las clases dadas por elementos positivos de L que no estén en H, es decir,

$$P(L/H) = \{p + H : p \in P \setminus H\}.$$

Por último, comprobamos que π es o-epimorfismo. Por la buena definición del bucle cociente con H normal, π es homomorfismo. Además, si $a, b \in L$ con $a \leq b$, se comprueba que $\pi(a) \preceq \pi(b)$, lo que prueba la afirmación.

(3) Por lo probado en (1) y (2), podemos dotar de un orden inducido desde L al bucle $L/\ker\varphi$. De manera análoga al Teorema de Isomorfía en grupos, se define la siguiente aplicación:

$$\begin{array}{rccc} \bar{\varphi}: & L/\ker\varphi & \longrightarrow & L' \\ & a + \ker\varphi & \longmapsto & \varphi(a) \quad . \end{array}$$

En primer lugar, está bien definida ya que $b \in a + \ker\varphi \Leftrightarrow b = a + h$ con $\varphi(h) = 0$, y así $\varphi(b) = \varphi(a)$, y es homomorfismo por serlo φ. También preserva el orden, puesto que lo hace φ. La inyectividad y suprayectividad son directas.

□

2.3. Grupos ordenados

En lo anterior, hemos definido grupo ordenado como aquel que es ordenado como bucle, y hemos deducido algunas propiedades para grupos heredadas de la estructura de bucle. En esta última sección del capítulo, obtenemos resultados referidos exclusivamente a grupos.

Definición 2.20. Sea $(G, \cdot)$ un grupo. Un **elemento** $a \in G$ se dice **de torsión** si existe $n \in \mathbb{N}_{\geq 1}$ tal que $a^n = e$.

Definición 2.21. Un **grupo** G se dice **libre de torsión** si el único elemento de torsión de G es el elemento neutro e.

Proposición 2.22. *Un grupo G totalmente ordenado es libre de torsión.*

Demostración. Sea $a \in G$ no nulo. Podemos suponer sin pérdida de generalidad $a > e$, por ser $N = P^{-1}$. Entonces, razonando por inducción, usando que G es grupo ordenado, vemos que $a^n > e$ para todo $n \in \mathbb{N}_{\geq 1}$. De la misma forma, $(a^{-1})^n < e$, de donde deducimos que no puede haber elementos de torsión en G. □

Más adelante veremos que, en el caso de grupos abelianos, la implicación anterior es de hecho una equivalencia (Proposición 4.8).

Pasamos a la parte final del capítulo, en la que probamos el resultado más importante: la existencia de la envolvente divisible de un grupo abeliano, que usaremos en el Capítulo 6 para demostrar el Teorema de Inmersión de Hahn. Antes de nada, debemos introducir la noción de divisibilidad en un grupo abeliano.

Definición 2.23. Un **grupo abeliano** $(G, +)$ se dice **divisible** si para cada $a \in G$ y $n \in \mathbb{N}_{\geq 1}$ existe $b \in G$ tal que $a = nb$.

El grupo $(\mathbb{Z}, +)$ no es divisible, ya que dados dos números enteros cualesquiera, no es cierto en general que ambos sean divisores del otro. La manera de garantizar la divisibilidad mutua de cualquier par es formar fracciones de enteros, o números racionales. Se extiende así $\mathbb{Z}$ a un grupo divisible como $\mathbb{Q}$, de forma similar al concepto de cuerpo de fracciones sobre anillos. Veamos en primer lugar que la divisibilidad de un grupo se preserva en sus subgrupos convexos.

Proposición 2.24. *Los subgrupos convexos de un grupo abeliano totalmente ordenado y divisible son divisibles.*

Demostración. Dados un subgrupo convexo H de un grupo divisible G y $a \in H$, tenemos que, para todo $n \in \mathbb{N}_{\geq 1}$, existe $b \in G$ tal que $a = nb$. Por las propiedades de los grupos ordenados, debe ser $b > 0$, y además $b \leq a$. Así que $b \in H$, y en consecuencia H es divisible. □

El siguiente teorema es una generalización de la extensión de $\mathbb{Z}$ en $\mathbb{Q}$ a grupos abelianos libres de torsión cualesquiera, usando elementos de $\mathbb{N}_{\geq 1}$ como los denominadores que aportan la divisibilidad.

Teorema 2.25. *Sea $(G, +)$ un grupo abeliano libre de torsión.*

(1) G está contenido, salvo isomorfía, exactamente en un grupo abeliano divisible minimal $(\bar{G}, +)$. Se lo conoce como envolvente divisible de G.

(2) Para cualquier subgrupo $H \subseteq G$, $\bar{G}$ contiene una envolvente divisible $\bar{H}$ de H.

(3) Si además G es totalmente ordenado, existe una única forma de extender el orden sobre G a un orden total sobre $\bar{G}$. En otras palabras, la envolvente divisible ordenada de un grupo abeliano es única salvo o-isomorfía.

Demostración.

(1) Definimos $\bar{G}$ como el cociente del conjunto $\{(a, n) : a \in G, n \in \mathbb{N}_{\geq 1}\}$ por la relación de equivalencia

$$(a, n) \sim (b, m) \text{ si y sólo si } ma = nb \text{ en } G.$$

Para la transitividad de la relación es esencial que G sea libre de torsión. Abusamos de notación y escribimos las clases como elementos, como se hace habitualmente con las fracciones en $\mathbb{Q}$. Definimos con ello la operación

$$\begin{array}{rccc} + : & \bar{G} \times \bar{G} & \longrightarrow & \bar{G} \\ & ((a, n), (b, m)) & \longmapsto & (ma + nb, nm) \end{array},$$

bien definida ya que si $n_2 a_1 = n_1 a_2$ y $m_2 b_1 = m_1 b_2$, entonces

$$\begin{aligned} n_2 m_2 (m_1 a_1 + n_1 b_1) &= n_2 m_2 m_1 a_1 + n_2 m_2 n_1 b_1 = n_1 m_2 m_1 a_2 + n_2 m_1 n_1 b_2 \\ &= n_1 m_1 (m_2 a_2 + n_2 b_2). \end{aligned}$$

El elemento $(0,1)$ es neutro y $(-a,n)$ es inverso de (a,n), y la asociativa y conmutativa se heredan de G, así que $\bar{G}$ es grupo. $\bar{G}$ es divisible, puesto que dado $(a,n) \in \bar{G}$ y $k \in \mathbb{N}$, entonces $(a,n) = k(a,nk)$, y se puede incluir G en $\bar{G}$ mediante $\iota : a \mapsto (a,1)$.

Sea ahora G' un grupo divisible que contiene a G, que podemos suponer libre de torsión. Como G' es divisible, la ecuación $a = nx$ tiene solución para todo $a \in G$, $n \in \mathbb{N}_{\geq 1}$; y como es libre de torsión, la solución es única, y la denotamos por $x = \frac{1}{n}a$. Entonces podemos definir, para todo $q = \frac{r}{s} \in \mathbb{Q}$, el elemento $qa = r\left(\frac{1}{s}a\right) \in G'$, y con ello el subgrupo

$$\mathbb{Q} \cdot G = \{qa : q \in \mathbb{Q}, a \in G\} \subseteq G',$$

que es isomorfo a $\bar{G}$ mediante

$$\begin{array}{rccc} \phi : & \bar{G} & \longrightarrow & G' \\ & (a,n) & \longmapsto & \frac{1}{n}a \end{array} .$$

(2) La construcción de $\bar{H}$ es análoga a la de $\bar{G}$, y de forma natural es un subgrupo de $\bar{G}$. Como H es a su vez grupo, las conclusiones son idénticas.

(3) Definimos el cono positivo $P(\bar{G}) := \{(p,n) : p \in P(G)\}$. Las condiciones del Teorema 2.13 se verifican por construcción, por hacerlo para $P(G)$, y la inmersión ι es un o-homomorfismo. Del mismo modo, al considerar un grupo abeliano, divisble y ordenado G', la aplicación definida en (1) $\phi : \bar{G} \to G'$, como extensión de un o-homomorfismo de G a G', es también o-homomorfismo, y en particular o-isomorfismo sobre su imagen $\mathbb{Q} \cdot G$.

□

Corolario 2.26. *La envolvente divisible de un grupo abeliano libre de torsión es un $\mathbb{Q}$-espacio vectorial.*

Ejemplos.

1. La motivación del concepto de envolvente divisible era generalizar la extensión de $\mathbb{Z}$ a $\mathbb{Q}$, que permite "dividir"por números naturales. Por tanto, como era de esperar, podemos ver con la construcción anterior que $\mathbb{Q}$ es la envolvente divisible de $\mathbb{Z}$.

2. Los grupos $(\mathbb{R},+)$, $(\mathbb{C},+)$ son divisibles, y en consecuencia los espacios vectoriales $\mathbb{R}^n$ y $\mathbb{C}^n$. También es divisible $(\mathbb{C}^*,\cdot)$, pero no su subgrupo $(\mathbb{R}^*,\cdot)$, ya que dado $x < 0$, no existe ningún $y \in \mathbb{R}$ con $x = y^2$. Si bien estos dos grupos no son libres de torsión, por lo que no estamos en las condiciones del Teorema anterior, podemos encontrar un grupo divisible minimal que contiene a $\mathbb{R}^*$. En efecto, consideramos el conjunto de los números complejos no nulos de argumento racional,

$$R^* = \{z = |z|e^{i\varphi} \in \mathbb{C}^* : \varphi \in \mathbb{Q}\} \subseteq C^*.$$

Por un lado, $(R^*,\cdot)$ tiene estructura de grupo, siendo $(\mathbb{R}^*,\cdot)$ un subgrupo. R^* es divisible, ya que podemos tomar raíces n-ésimas dividiendo por n en el argumento, por ser $\mathbb{Q}$ divisible. De hecho, R^* es el subgrupo de $\mathbb{C}$ generado por las raíces de números reales. En particular, contiene las raíces de -1, cuyas potencias generan todas las raíces de la unidad. A su vez, estas permiten, por multiplicación, construir todas las raíces de cualquier número real a partir de la primera. Con todo, R^* es el grupo divisible minimal que contiene a $\mathbb{R}^*$.

3. Órdenes arquimedianos

Recordemos la noción de grupo divisible. De acuerdo con la Definición 2.23, un grupo abeliano G es divisible si para todo $a \in G$ y $n \in \mathbb{N}_{\geq 1}$ existe $b \in G$ de modo que $a = nb$. Supongamos ahora que G es totalmente ordenado. Podemos preguntarnos qué tipo de estructura requiere G para disponer de una versión análoga del concepto de divisibilidad relativa al orden, como sucede en los reales con el orden usual: dados $a, b \in \mathbb{R}$ con $0 < b \leq a$, existe cierto $n \in \mathbb{N}$ de forma que $a \leq nb$. En general, esto no tiene por qué ocurrir en un grupo ordenado: basta considerar $(\mathbb{R}^2, +)$ con el orden lexicográfico.

Este capítulo está dedicado a los bucles o grupos ordenados que poseen esta propiedad, conocida como **propiedad arquimediana**, y las consecuencias que se deducen de ella. Veremos que la estructura de los bucles arquimedianos restringe los posibles o-homomorfismos entre ellos, y probaremos que, bajo ciertas condiciones, los bucles arquimedianos son de hecho grupos abelianos, que de hecho se pueden incluir en $(\mathbb{R}, +)$. Como hemos mencionado en la Introducción, este importante resultado, conocido como Teorema de Hölder, es un caso particular del Teorema de Inmersión de Hahn del que nos ocuparemos en el Capítulo 6.

3.1. Propiedad arquimediana

Definimos la noción de bucle arquimediano generalizando de manera natural la propiedad arquimediana de los números reales.

Definición 3.1. Se dice que un **bucle** totalmente ordenado $(L, +)$ es **arquimediano** si sus elementos verifican la propiedad aquimediana; es decir, si para todos los elementos $a, b, a', b' \in L$ tales que $0 < a < b$ y $b' < a' < 0$, existen números $n, n' \in \mathbb{N}$ de modo que:

$$b < na, \quad n'a' < b'.$$

Recordemos que, en el caso de grupos, se tiene que $N = P^{-1}$. Entonces, podemos prescindir de la relación entre elementos negativos, ya que será consecuencia de la propiedad en los positivos, tomando inversos. Con ello, la definición se reduce a la siguiente.

Definición 3.2. Se dice que un **grupo** totalmente ordenado $(G, \cdot)$ es **arquimediano** si para todos $a, b \in G$ con $e < a < b$, existe $n \in \mathbb{N}$ tal que $b < a^n$.

Ejemplos.

1. Como hemos visto antes, $(\mathbb{R}, +)$, y cualquiera de sus subgrupos, es arquimediano. Así, $(\mathbb{Z}, +)$ y $(\mathbb{Q}, +)$ son también grupos arquimedianos.

2. Al considerar el grupo de polinomios $G[x]$ con coeficientes en un grupo G, entendido como el conjunto de sucesiones con soporte finito en $G^{\mathbb{N}}$ con la operación coordenada a coordenada, tomando los elementos $0 < e < e \cdot x \in G[x]$, resulta $ne < e \cdot x$ para todo $n \in \mathbb{N}$. Se puede razonar de esta forma para el producto lexicográfico de grupos en general, que definiremos en el Capítulo 4.

A continuación buscamos una caracterización de los bucles arquimedianos.

Definición 3.3. Sean $(L, +)$ un bucle totalmente ordenado y $S \subseteq L$ un subbucle no trivial.

- El subbucle S se denomina **cofinal** si para todo $a \in L$, existe $x \in S$ tal que $a \leq x$. De manera análoga se define subbucle **coinicial**.

- Se dice que L es **arquimediano sobre** S si S es cofinal y coinicial.

Definición 3.4. Se dice que un bucle L es **asociativo para potencias** si todo subbucle generado por un único elemento es asociativo, es decir, es un subgrupo de L.

Estamos ahora en condiciones de enunciar un resultado de caracterización de bucles arquimedianos, restringiéndonos a la condición de asociatividad para potencias en primera instancia.

Teorema 3.5. *Sea $(L,+)$ un bucle totalmente ordenado y asociativo para potencias. Entonces las siguientes propiedades son equivalentes:*

(1) L es arquimediano.

(2) L es arquimediano sobre todo subbucle no trivial.

(3) Los únicos subbucles convexos de L son $\{0\}$ y L.

Demostración. Probaremos la cadena de implicaciones.
(1) $\Rightarrow$ (2): Consideramos un subbucle S no trivial de L. Entonces S contiene las potencias de sus elementos. Como L es arquimediano, S es cofinal y coinicial, y así L arquimediano sobre S.
(2) $\Rightarrow$ (3): Consideramos un subbucle S convexo, no trivial. Por hipótesis, L es arquimediano sobre S, y entonces para todo elemento $a \in L$, existen $x, x' \in S$ con $x \leq a \leq x'$. Entonces, por convexidad, $a \in S$ luego $S = L$.
(3) $\Rightarrow$ (1): Para cada $a \in L$ no nulo, consideremos el subconjunto

$$A(a) := \{b \in L : \exists n_b, n_b' \in \mathbb{Z} : n_b' a \leq b \leq n_b a\} \subseteq L.$$

Veamos que la asociatividad en el subbucle generado por a garantiza que $A(a)$ es a su vez subbucle, que además no es trivial porque $a \in A$. En primer lugar, $0 \in A(a)$. Dados $b, c \in A(a)$, tenemos que $n_b' a \leq b \leq n_b a$ y $n_c' a \leq c \leq n_c a$ para $n_b', n_b, n_c', n_c \in \mathbb{Z}$, y como consecuencia $(n_b' + n_c')a \leq b + c \leq (n_b + n_c)a$, luego $b + c \in A(a)$. Por último, sea $x \in L$ es tal que $x + b = c$, con $b, c \in A(a)$ como antes. Tenemos que ver que $x \in A(a)$. Si suponemos que para todo $n \in \mathbb{N}$, se da que $x < na$, entonces tendríamos que $c = x + b < na + n_b a = (n + n_b)a$, lo que equivale a que $c < \tilde{n}a$ para todo $\tilde{n} \in \mathbb{Z}$. Pero esto está en contradicción con que $c \in A(a)$. Entonces debe existir $n_x' \in \mathbb{Z}$ tal que $n_x' a \leq a$. Del mismo modo encontramos n_x con $x \leq n_x a$, así que deducimos que $x \in A(a)$. Un razonamiento análogo sirve para ver que la solución $y \in L$ de la ecuación $b + y = c$ está en $A(a)$, y con esto probamos que $A(a)$ es un subbucle. Por otro lado, dados $b_1, b_2 \in A(a)$ y $c \in L$ tal que $b_1 \leq c \leq b_2$, resulta $n_{b_1}' a \leq c \leq n_{b_2} a$. En consecuencia, $A(a)$ es convexo. Por (3), tenemos $A(a) = L$ para todo $a \in L, a \neq 0$, y así L es arquimediano. □

Tal y como lo hemos probado, podemos aplicar este resultado sólo a bucles asociativos para potencias. Los grupos son bucles asociativos, y en consecuencia este resultado es válido para grupos totalmente ordenados, como usaremos más adelante. Sin embargo, apuntamos por completitud que se puede extender a bucles en general [34].

En el Capítulo 5 generalizaremos el resultado anterior a grupos no necesariamente arquimedianos. Concretamente en el Teorema 5.20, probaremos que las clases arquimedianas no nulas de un grupo totalmente ordenado están en biyección con los saltos entre subgrupos convexos. Así, en grupos arquimedianos, que cuentan con una sola de estas clases, sólo puede haber un salto, y por tanto no existe ningún subgrupo convexo diferente de $\{0\}$ y G.

Por otro lado, la caracterización (3) que acabamos de probar guarda un paralelismo con la no existencia de ideales propios no triviales en un cuerpo. Damos a continuación una propiedad de los morfismos entre bucles arquimedianos que es también familiar en ese sentido.

Proposición 3.6. *Un o-homomorfismo definido en un bucle arquimediano es la aplicación nula o un o-monomorfismo.*

Demostración. Por la Proposición 2.19 (1), tenemos que el núcleo de un o-homomorfismo definido en un bucle totalmente ordenado L es normal y convexo. Por tanto, si L es arquimediano, el núcleo de un o-homomorfismo es $\{0\}$ ó L, de donde se deduce el resultado. □

Pasamos a probar algunas propiedades que se deducen de la propiedad arquimediana en un bucle. En concreto, vemos en el siguiente resultado que los bucles asociativos para potencias que la poseen son en realidad grupos abelianos.

Teorema 3.7 (G. Pickert [29])**.** *Un bucle arquimediano y asociativo para potencias L es un grupo abeliano.*

Demostración. Consideramos el cono positivo $P \subseteq L$. Distinguimos dos casos:

- P posee un elemento mínimo c. Entonces el subgrupo $\langle c\rangle$ es un grupo abeliano por ser asociativo. Dado $b \in P$, como L es arquimediano, existe $n \in \mathbb{N}$ tal que $(n-1)c \leq b < nc$. Recordemos las aplicaciones de translación τ^a definidas en el Lema 2.4, que son de hecho o-isomorfismos, y por tanto su inversa también. Así, escribimos

$$0 = (\tau_l^{(n-1)c})^{-1}((n-1)c) \leq (\tau_l^{(n-1)c})^{-1}(b) < (\tau_l^{(n-1)c})^{-1}(c) = c.$$

  No puede ser $0 < (\tau_l^{(n-1)c})^{-1}(b)$ porque c es el mínimo de P, y deducimos entonces que $b = (n-1)c$, así que $P \subseteq \langle c\rangle$ y entonces $L = \langle c\rangle$.

- P no posee elemento mínimo. Probaremos el resultado por reducción al absurdo. Apuntamos primero que, por no tener P mínimo, para cada $a \in P$ existe $c \in P$ tal que $0 < c < a$. Tenemos así que $a = (\tau_l^c \circ (\tau_l^c)^{-1})(a) = c + (\tau_l^c)^{-1}(a)$, y como $a > c$, es $(\tau_l^c)^{-1}(a) > 0$. Escogiendo $d' = \min\{c, (\tau_l^c)^{-1}(a)\}$, podemos escribir $0 < d' < 2d' \leq c + (\tau_l^c)^{-1}(a) = a$. Repitiendo el proceso encontramos un elemento $d \in L$ tal que $0 < 3d \leq a$.

  Supongamos ahora que L no es asociativo; es decir, que existen $a, b, c \in L$ tales que $(a+b)+c < a+(b+c)$ ó $a+(b+c) < (a+b)+c$. Sin pérdida de generalidad nos restringimos al primer caso. Consideremos ahora el elemento $s \in L$ tal que $s + ((a+b)+c) = 0$, y entonces $s + (a + (b+c)) > 0$. Con lo cual, por lo anterior, encontramos $d \in L$ positivo y con $0 < 3d \leq s + (a + (b+c))$. Utilizamos ahora que L es arquimediano, y consideramos tres naturales $n_1, n_2, n_3 \in \mathbb{Z}$ tales que:

$$n_1 d \leq a < (n_1+1)d, \quad n_2 d \leq b < (n_2+1)d, \quad n_3 d \leq c < (n_3+1)d.$$

  Denotemos $n := n_1 + n_2 + n_3$. Entonces, como además L es asociativo para potencias, se tiene que

$$a + (b+c) < (n+3)d, \quad nd \leq (a+b) + c.$$

  Sumando ahora s por la izquierda en la segunda expresión, vemos que

$$s + nd \leq 0,$$

  y de ahí, empleando la primera de las expresiones anteriores, observamos que

$$s + (a + (b+c)) < 3d,$$

  contradiciendo la relación obtenida antes para d. Un idéntico desarrollo se puede efectuar para la conmutatividad, sin más que sustituir $(a+b)+c$ y $a+(b+c)$ por $a+b$ y $b+a$, respectivamente. Con esto probamos que L es un bucle asociativo y abeliano, es decir, un grupo abeliano.

□

En la Proposición anterior, la propiedad de asociatividad de potencias es determinante: hay bucles arquimedianos que no son grupos. Un ejemplo es tomar el bucle $(\mathbb{R}, \star_p)$ definido en la página 4. Habíamos visto que se trata de bucle totalmente ordenado, considerando el orden usual en $\mathbb{R}$. Además, posee la propiedad arquimediana, ya que la operación $\star_p$ restringida a los elementos con el mismo signo coincide con la suma usual en $\mathbb{R}$. Sin embargo, no es asociativo, y en consecuencia no es un grupo. La condición de asociatividad para potencias no es necesaria, sin embargo, si L tiene elemento mínimo positivo para el orden dado.

Teorema 3.8 (K. Iseki [14])**.** *Si L es un bucle arquimediano cuyo cono positivo $P(L)$ tiene mínimo, entonces L es un grupo abeliano. De hecho, es o-isomorfo a $\mathbb{Z}$.*

Demostración. Sea $c = \min(P(L))$. Veamos que $\langle c\rangle$ es asociativo. Sean $a, b \in L$, y consideremos las biyecciones τ^a como en el Teorema 3.7. Tenemos aquí que, como $c + (a + b) > a + b$:

$$0 < (\tau_l^{a+b})^{-1}(c + (a + b)),$$

y por ser c el mínimo positivo, entonces

$$c \leq (\tau_l^{a+b})^{-1}(c + (a + b)) \quad \Leftrightarrow \quad (a + b) + c \leq c + (a + b).$$

Igualmente, usando σ_r probamos la otra desigualdad, y se deduce que $(a + b) + c = c + (a + b)$. Así, extendiendo por inducción a cualquier $n \in \mathbb{N}$, es $c + nc = nc + c$, y de esta propiedad se deduce la asociatividad en potencias de c, es decir, $\langle c\rangle$ es grupo abeliano. En consecuencia, con el mismo razonamiento que en el Teorema 3.7, L es un grupo cíclico. Como L es totalmente ordenado, por la Proposición 2.22, es libre de torsión, y entonces la aplicación $\varphi : L \to \mathbb{Z}$ tal que $\varphi(c) = 1$ es o-isomorfismo. □

3.2. Teorema de Hölder

En lo anterior nos hemos ocupado de bucles arquimedianos, y hemos visto que la propiedad arquimediana, junto con algún requisito adicional, garantiza de por sí la estructura de grupo abeliano. Veremos ahora que, de hecho, es o-isomorfo a un subgrupo aditivo de $\mathbb{R}$. Este resultado, probado por O. Hölder en 1901 en su trabajo *Die Axiome der Quantität und die Lehre vom Maß* ("Los axiomas de la cantidad y la doctrina de la medida") [13]. La prueba del Teorema de Hölder se basa en el concepto de corte de Dedekind, que definimos a continuación. Richard Dedekind introdujo esta noción para construir formalmente el conjunto $\mathbb{R}$ de los números reales, identificando cada subconjunto de $\mathbb{Q}$ de este tipo con un número real [5]. Usaremos esta misma idea para identificar los elementos de un bucle arquimediano y asociativo para potencias con números reales.

Definición 3.9. Un subconjunto $A \subseteq \mathbb{Q}$ se llama **corte de Dedekind** si verifica las propiedades:

(I) $A \notin \{\varnothing, \mathbb{Q}\}$.

(II) A es una clase inferior, esto es, dados $x, y \in \mathbb{Q}$ tales que $x \in A$ e $y < x$, entonces $y \in A$.

(III) Para todo $x \in A$ existe $y \in A$ con $x < y$.

Con ello, se puede definir $\mathbb{R} = \{A \subseteq \mathbb{Q} : A \text{ es un corte de Dedekind}\} \subseteq \mathcal{P}(\mathbb{Q})$, e incluir $\mathbb{Q}$ en $\mathbb{R}$ relacionando cada $r \in \mathbb{Q}$ con el corte $A_r = \{a \in \mathbb{Q} : a < r\}$. Enunciamos entonces el Teorema de Hölder en su versión para bucles arquimedianos y asociativos para potencias. Notemos que, en particular, el resultado es aplicable a grupos arquimedianos, por el Teorema 3.7.

Teorema 3.10 (**Teorema de Hölder** [13])**.** *Todo bucle arquimediano y asociativo para potencias L es o-isomorfo a un subgrupo de $(\mathbb{R}, +)$.*

Demostración. Por el Teorema 3.7, L es un grupo abeliano. Fijamos $x \in P(L)$ y consideramos para cada $a \in L$ el conjunto:

$$S(a) = \left\{ \frac{m}{n} : mx < na, \text{ con } m \in \mathbb{Z}, n \in \mathbb{N}_{\geq 1} \right\}.$$

Veamos que se trata de un corte de Dedekind. La propiedad arquimediana en L garantiza que se cumple (I). Para ver (II), tomamos ahora

$$r_1 := \frac{m_1}{n_1}, \quad r_2 := \frac{m_2}{n_2}$$

racionales tales que $r_1 \in S(a)$ y $r_2 < r_1$, esto es, $m_1 x < n_1 a$ y $m_2 n_1 < m_1 n_2$. Entonces, con ambas desigualdades, se tiene que $m_2 n_1 x < m_1 n_2 x < n_2 n_1 a$, luego

$$\frac{m_2 n_1}{n_2 n_1} = \frac{m_2}{n_2} \in S(a).$$

Por último, veamos (III). Dado $r = m/n \in S(a)$, tenemos que $mx < na$, es decir, existe $p \in P(L)$ con $na = mx + p$. Por ser L arquimediano, existe $k \in \mathbb{N}$ tal que $kp > x$, y de ese modo resulta, usando que L es grupo abeliano,

$$kna = k(mx + p) = kmx + kp > (km + 1)x \quad \Rightarrow \quad \frac{m}{n} < \frac{km+1}{kn} \in S(a).$$

Así, cada $a \in L$ determina un número real $S(a)$. Definimos con ello la aplicación

$$\begin{array}{rccc} \sigma: & L & \longrightarrow & \mathbb{R} \\ & a & \longmapsto & S(a) \end{array} .$$

Veamos que σ es un o-homomorfismo sobre L. Dados $a, b \in L$, se tiene para todo $m/n \in \mathbb{Q}$,

$$m/n < \sigma(a+b) \quad \Leftrightarrow \quad mx < n(a+b) \quad \Leftrightarrow \quad mx < na + nb \quad \Leftrightarrow \quad m/n < \sigma(a) + \sigma(b),$$

y por tanto $\sigma(a+b) = \sigma(a)+\sigma(b)$. Por otro lado, si $a \leq b$, entonces por la definición del conjunto S se tiene que $S(a) \subseteq S(b)$, y en consecuencia $\sigma(a) \leq \sigma(b)$. Además se tiene que $\sigma(x) = 1$, luego $\sigma(L) \neq \{0\}$, y por la Proposición 3.6, es un o-monomorfismo. □

Para terminar estudiaremos los o-homomorfismos entre grupos arquimedianos. Por el Teorema 3.10, los tratamos a partir de ahora como subgrupos de $(\mathbb{R}, +)$.

Teorema 3.11. *Sean A y B dos subgrupos de $(\mathbb{R}, +)$ con el orden usual, y $\varphi : A \to B$ un o-homomorfismo. Entonces existe un número real $r \geq 0$ tal que $\varphi(a) = ra$ para todo $a \in A$, entendido como el producto usual en el cuerpo $\mathbb{R}$.*

Demostración. Por la Proposición 3.6, φ es la aplicación nula o un o-monomorfismo. En el primer caso, tomando $r = 0$ se tiene el resultado. Supongamos entonces que φ es inyectiva, y sean a_1, a_2 positivos, y por tanto también sus imágenes. Supongamos por reducción al absurdo que

$$\frac{\varphi(a_1)}{\varphi(a_2)} \neq \frac{a_1}{a_2}.$$

Entonces existe $m/n \in \mathbb{Q}$, con $m, n \in \mathbb{N}$, entre ambos cocientes, lo que implica que la desigualdad entre ma_2 y na_1 se invierte para $\varphi(ma_2)$ y $\varphi(na_1)$, en contradicción con que φ es o-homomorfismo. Con lo cual, la anterior es una igualdad para cualquier par $a_1, a_2 > 0$, y podemos escribir, para todo $a \in A$, incluyendo los negativos por ser φ homomorfismo,

$$r := \frac{\varphi(a)}{a} = \frac{\varphi(a_1)}{a_1},$$

lo que prueba el resultado. □

Como consecuencia, se deduce también lo siguiente.

Corolario 3.12. *El grupo de o-automorfismos de un grupo arquimediano es isomorfo a un subgrupo de $(\mathbb{R}_{>0}, \cdot)$.*

Demostración. Podemos identificar cada φ con su respectivo factor $r \in \mathbb{R}_{>0}$ (ya que φ no puede ser la aplicación neutra) dado en el Teorema 3.11, de forma que dos automorfismos tienen el mismo factor si y sólo si son iguales. Asimismo, es claro que la composición de dos homomorfismos tiene como factor el producto de ambos factores. □

4. Producto lexicográfico

En el capítulo anterior hemos demostrado el Teorema de Hölder, según el cual todo grupo arquimediano totalmente ordenado es o-isomorfo a un subgrupo aditivo de los reales. Nos interesa ahora avanzar hacia el Teorema de Inmersión de Hahn, que generaliza este resultado a grupos no necesariamente arquimedianos. Recordamos que para su demostración, nos basaremos en la construcción de un grupo producto, cuyas componentes serán grupos arquimedianos sobre los que aplicar el Teorema de Hölder.

En este capítulo formalizamos la construcción del producto de grupos totalmente ordenados. Estudiaremos cómo definir un orden en el grupo producto, para lo que necesitaremos restringirnos a un subgrupo del producto directo de grupos, al que denominaremos producto lexicográfico. Algunos de los argumentos empleados requieren el uso de la propiedad asociativa; es por ello que nos centramos en los resultados relativos a grupos, y abandonamos la estructura de bucle.

En la parte final enunciaremos algunos resultados colaterales que se deducen de la estructura del producto lexicográfico: daremos una caracterización de la ordenabilidad de un grupo abeliano, y desarrollaremos la teoría de la extensión lexicográfica de un grupo totalmente ordenado.

4.1. Producto lexicográfico de grupos

Recordemos primero cómo se extiende el orden al producto cartesiano en el caso de conjuntos. Tomando una familia de conjuntos totalmente ordenados, dotada de una indexación ordinal (Axioma de Elección), podemos considerar el orden lexicográfico en el producto cartesiano. Así, para relacionar dos elementos, se comparan en primer lugar los índices de sus conjuntos correspondientes y, si estos coinciden, se comparan entre sí dentro del mismo conjunto.

El desarrollo con grupos es parecido, pero hay que verificar, además, que el orden que se define en el grupo producto es compatible con la operación definida sobre él. Comencemos con la definición de grupo producto de una familia (no necesariamente finita) de grupos ordenados.

Definición 4.1. Sea Γ un conjunto no vacío de índices, y para cada $\gamma \in \Gamma$ sea $(G_\gamma, \cdot_\gamma)$ un grupo. El **producto cartesiano** o **producto directo** de la familia $\{G_\gamma\}_{\gamma\in\Gamma}$ se define como el conjunto

$$\prod_{\gamma\in\Gamma} G_\gamma = \left\{ x : \Gamma \to \bigcup_{\gamma\in\Gamma} G_\gamma, \text{ tal que } x(\gamma) \in G_\gamma \text{ para todo } \gamma \in \Gamma \right\}.$$

Probamos a continuación que el producto definido admite una estructura de grupo, con la operación coordenada a coordenada.

Proposición 4.2. *El producto cartesiano de grupos definido es un grupo.*

Demostración. Consideramos el producto cartesiano $\Lambda := \prod_{\gamma\in\Gamma} G_\gamma$ de una familia $\{G_\gamma\}_{\gamma\in\Gamma}$ de grupos ordenados. Admitiendo el axioma de elección, y dado que los G_γ son grupos y, por tanto, no vacíos, el producto Λ es no vacío. Definamos en él la operación binaria $\cdot : \Lambda \times \Lambda \to \Lambda$, de forma que para todo par $x, y \in \Lambda$,

$$\begin{array}{rccc} x \cdot y : & \Gamma & \longrightarrow & \bigcup_{\gamma\in\Gamma} G_\gamma \\ & \gamma & \longmapsto & x(\gamma) \cdot_\gamma y(\gamma) \end{array} .$$

Veamos que $(\Lambda, \cdot)$ es un grupo, es decir, que la operación está bien definida, es asociativa, existe un elemento neutro y todo elemento tiene inverso.

La buena definición de la operación en Λ se debe a que dados $x, y \in \Lambda$, ambos $x(\gamma), y(\gamma) \in G_\gamma$, y por ser G_γ un grupo, su producto $x(\gamma)\cdot_\gamma y(\gamma) \in G_\gamma \subseteq \bigcup_{\gamma\in\Gamma} G_\gamma$. Con esto tenemos que el producto es magma.

La asociatividad es también consecuencia de la de cada operación $\cdot_\gamma$ en su respectivo grupo. Con la misma idea, vemos que la aplicación dada por $e(\gamma) = e_\gamma$ para cada $\gamma \in \Gamma$, que denota el elemento neutro en G_γ, para todo $\gamma \in \Gamma$, es elemento neutro en Λ. Por último, dado $x \in \Lambda$, su inverso $\bar{x} \in \Lambda$ está dado por $\bar{x}(\gamma) = x(\gamma)^{-1}$ para cada $\gamma \in \Gamma$. □

Supondremos de ahora en adelante que Γ es un conjunto totalmente ordenado. Tenemos así un producto Λ de los grupos G_γ sobre el conjunto de índices Γ. Sin embargo, Γ no tiene por qué tener elemento máximo, con lo que no podemos definir directamente un orden lexicográfico análogo al caso de un producto finito. Elegiremos un subgrupo de Λ en el que sí podamos hacerlo. Para ello, definamos primero el concepto de soporte, y a continuación, el de producto lexicográfico.

Definición 4.3. Se llama **soporte** de $x \in \Lambda$ al conjunto $s(x) := \{\gamma \in \Gamma : x(\gamma) \neq e_\gamma\}$.

Definición 4.4. Denotamos por Λ_{lex} el conjunto de los elementos de Λ tales que su soporte está bien ordenado respecto del orden dual en Γ, es decir, de modo que todo subconjunto no vacío del soporte tiene máximo. Se conoce este conjunto como **producto lexicográfico** de la familia de grupos $\{G_\gamma\}_{\gamma\in\Gamma}$.

La condición anterior guarda relación con la cuestión de cómo determinar si un elemento $x \in \Lambda$ del grupo producto es positivo o negativo. Así, si su soporte tiene un elemento máximo $\beta \in \Gamma$, podremos asociar a cada elemento del producto el signo del elemento $x(\beta)$ en G_β, y veremos que esta construcción dota de un orden total al producto lexicográfico.

Por el Teorema del Buen Orden, el conjunto Γ siempre se puede dotar de un orden total de manera que el orden dual sea un buen orden. Para dicha ordenación, se tiene que $\Lambda_{lex} = \Lambda$. Sin embargo, en construcciones concretas el conjunto Γ tiene un orden prefijado que nos interesa respetar, dado que conlleva también relaciones entre los grupos que forman el producto de manera que Λ_{lex} tiene una estructura más conveniente. En particular, esto ocurre en la construcción que conduce al Teorema de Inmersión de Hahn en el Capítulo 6. Tendremos que Γ es el conjunto de clases arquimedianas de un grupo G, que se puede dotar de un orden total que tiene elemento mínimo y está ligado al orden entre los subgrupos convexos, con los que se construye el producto. Además, trabajar con el orden prefijado de Γ nos será especialmente útil si Γ tiene estructura de semigrupo o grupo totalmente ordenado, ya que en ese caso se podrá definir un producto de Cauchy en el producto lexicográfico y dotarlo así de una estructura de anillo o cuerpo, respectivamente, como probamos en la Proposición 6.2.

Por otro lado, se podría definir de forma equivalente el producto lexicográfico empleando soportes bien ordenados respecto del orden en Γ, y no del dual. En nuestro caso, de cara a probar el Teorema de Inmersión, resulta más natural considerar el orden dual de forma que trabajemos con el orden dado por la inclusión en la cadena de subgrupos convexos. Sin embargo, los ejemplos más comunes de productos lexicográficos, como las series formales de potencias o las series de Puiseux, tienen elementos con soporte bien ordenado.

Veamos que esta restricción no plantea ningún problema adicional, puesto que Λ_{lex} también tiene estructura de grupo.

Proposición 4.5. *Λ_{lex} es un subgrupo de Λ. Además, si G_γ es totalmente ordenado para todo $\gamma \in \Gamma$, entonces se puede dotar a Λ_{lex} de un orden total mediante el conjunto de positivos*

$$P_{lex} := \left\{x \in \Lambda_{lex} : x(\text{máx}(s(x))) > e_{\text{máx}(s(x))}\right\}.$$

Demostración. Veamos primero que Λ_{lex} es un subgrupo. Tenemos que no es vacío porque el elemento neutro de Λ pertenece a Λ_{lex}. Dados $x, y \in \Lambda_{lex}$, entonces $s(xy^{-1}) \subseteq s(x) \cup s(y)$. Veamos que todo subconjunto no vacío $C \subseteq s(xy^{-1}) \subseteq s(x) \cup s(y)$ tiene máximo. Podemos escribir $C = A \cup B$ tales que $A \subseteq s(x), B \subseteq s(y)$. Si uno de ellos es vacío, el resultado es

directo; en caso contrario, el orden total en Γ y la propiedad transitiva aseguran que entonces $\text{máx}(C) = \text{máx}\{\text{máx}(A), \text{máx}(B)\}$.

Supongamos ahora que los grupos G_γ son totalmente ordenados. Para cada $x \in P_{lex}$, si denotamos $\alpha = \text{máx}(s(x))$, entonces $x(\alpha)$ es un elemento positivo en G_α. Con ello, se puede comprobar que P_{lex} verifica las propiedades del Corolario 2.15, teniendo en cuenta para la normalidad que para todos $x \in \Lambda_{lex}$ y $p \in P_{lex}$,

$$\text{máx}(s(p)) = \text{máx}(s(x^{-1}px)).$$

□

De ese modo, el conjunto Λ_{lex} definido previamente es un grupo totalmente ordenado. Al hablar de **producto lexicográfico de grupos**, asumiremos que nos referimos a esta estructura.

Ejemplos.

1. El producto finito de grupos totalmente ordenados es un producto lexicográfico, ya que todo subconjunto finito de $\mathbb{N}$ tiene máximo.

2. El conjunto $\Lambda = G^{\mathbb{N}}$ de sucesiones sobre un grupo totalmente ordenado G, junto con la operación coordenada a coordenada, no es un producto lexicográfico tal y como lo hemos definidol, pero sí considerando la definición equivalente que emplea soportes bien ordenados, según lo explicado en la página anterior. También lo es el subgrupo $(G^{\mathbb{N}})_{\text{fin}}$ formado por las sucesiones de soporte finito sí. En el trabajo terminaremos considerando la inmersión de un grupo ordenado en el producto lexicográfico de copias de $\mathbb{R}$. En esas condiciones, el conjunto de sucesiones $\mathbb{R}^{\mathbb{N}}$ admite estructura de anillo, y se conoce normalmente como el anillo de series de potencias con coeficientes reales, $\mathbb{R}[[x]]$. El correspondiente subgrupo de series con soporte finito es el anillo de polinomios $\mathbb{R}[x]$. Con ello en mente, hablamos en el texto de *grupos* de series de potencias y de polinomios al considerar los grupos $G^{\mathbb{N}}$ y $G^{\mathbb{N}}_{\text{fin}}$ con la operación coordenada a coordenada.

Veamos que podemos generalizar la idea de sucesiones con soporte acotado. Empezamos definiendo, para cada $\Omega \subseteq \Gamma$, el subconjunto

$$\Lambda(\Omega) := \{x \in \Lambda : s(x) \subseteq \Omega\},$$

y a partir de él $\Lambda_{lex}(\Omega) := (\Lambda(\Omega))_{lex}$. Se puede comprobar que $\Lambda(\Omega)$ es subgrupo de Λ, y en consecuencia también $\Lambda_{lex}(\Omega)$. De acuerdo con la Proposición 2.19, para considerar el cociente necesitamos trabajar con subgrupos convexos. En ese sentido, introducimos la siguiente noción, que ya hemos empleado al considerar cortes de Dedekind en el capítulo anterior.

Definición 4.6. Se dice que un subconjunto $\Delta \subseteq \Gamma$ es una **clase inferior** si para cada $\gamma \in \Delta$, se tiene que

$$\alpha \leq \gamma \quad \Rightarrow \quad \alpha \in \Delta.$$

Proposición 4.7. *Sea $\Delta \subseteq \Gamma$ una clase inferior, y considérese el conjunto $\Lambda_{lex}(\Delta)$. Entonces:*

(1) $\Lambda_{lex}(\Delta)$ es un subgrupo convexo y normal de Λ_{lex}.

(2) El grupo cociente totalmente ordenado $\Lambda_{lex}/\Lambda_{lex}(\Delta)$ es o-isomorfo a $\Lambda_{lex}(\Gamma \setminus \Delta)$.

Demostración.

(1) La elección de elementos con soporte bien ordenado supone que al operar en $\Lambda_{lex}(\Delta)$ el buen orden se preserva. Por otro lado, $s(x) \cap (\Gamma \setminus \Delta) = \varnothing$ para todo $x \in \Lambda_{lex}(\Delta)$. Con lo cual, como $s(xy^{-1}) \subseteq s(x) \cup s(y)$, se tiene que $s(xy^{-1}) \cap (\Gamma \setminus \Delta) = \varnothing$ para todo $x, y \in \Lambda_{lex}(\Delta)$, y así $xy^{-1} \in \Lambda_{lex}(\Delta)$. Con lo cual, $\Lambda_{lex}(\Delta)$ es subgrupo de Λ_{lex}.

La convexidad se deduce a partir de la propiedad de clase inferior impuesta a Δ.

En cuanto a la normalidad, tomando $x \in \Lambda_{lex}(\Delta)$, $y \in \Lambda_{lex}$ y $\gamma \in \Gamma \setminus \Delta$, tenemos que $(yxy^{-1})(\gamma) = y(\gamma) \cdot_\gamma x(\gamma) \cdot_\gamma y(\gamma)^{-1} = e_\gamma$ por ser $x(\gamma) = e_\gamma$, luego $yxy^{-1} \in \Lambda_{lex}(\Delta)$.

(2) Por la Proposición 2.19 (2), el grupo cociente es totalmente ordenado, y la o-isomorfía viene dada al aplicar el Teorema de Isomorfía al o-homomorfismo:

$$\varphi : \begin{array}{ccc} \Lambda_{lex} & \longrightarrow & \Lambda_{lex}(\Gamma \setminus \Delta) \\ x & \longmapsto & \varphi(x) \end{array}, \text{ donde } \varphi(x)(\gamma) = \begin{cases} e_\gamma & \text{si } \gamma \in \Delta \\ x(\gamma) & \text{si } \gamma \in \Gamma \setminus \Delta \end{cases}.$$

□

El desarrollo de la idea de producto lexicográfico de grupos, junto con el concepto de envolvente divisible introducido en la sección 2.3, nos permiten probar ya el recíproco de la Proposición 2.22, y obtener así una primera caracterización de los grupos ordenables, en el caso abeliano.

Proposición 4.8 (F.W. Levi [22])**.** *Un grupo abeliano es ordenable si y sólo si es libre de torsión.*

Demostración. Por lo probado en la Proposición 2.22, sólo queda por demostrar que un grupo G abeliano y libre de torsión es ordenable. Consideramos la envolvente divisible $\bar{G}$ de G definida en el Teorema 2.25, que es un espacio vectorial sobre $\mathbb{Q}$ de acuerdo con el Corolario 2.26. Sea entonces $\mathcal{B}$ una base de $\bar{G}$. Por el Teorema del Buen Orden [17], se puede dotar a $\mathcal{B}$ de un orden total, luego $\bar{G}$ es isomorfo al subgrupo de los elementos con soporte finito del producto lexicográfico $\left(\prod_{b \in \mathcal{B}} \mathbb{Q}\right)_{lex}$. En consecuencia es un grupo ordenable, y $G \subseteq \bar{G}$ también. □

Enunciaremos una segunda caracterización, esta vez para grupos no necesariamente abelianos, en el Teorema 5.24, a partir de los conceptos introducidos en el Capítulo 5. Asimismo, incluimos algunos resultados notables sobre ordenabilidad en el Apéndice.

4.2. Extensión lexicográfica de un grupo ordenado

Se considera a continuación la definición de extensión de grupos según la teoría de Schreier [20], y su análogo en grupos ordenados. Si bien no emplearemos el concepto de extensión lexicográfica en el desarrollo de la teoría de grupos ordenados necesaria para probar el Teorema de Inmersión de Hahn, incluimos esta sección dada la relevancia de la teoría de extensiones lexicográficas en muchas construcciones relacionadas con productos de grupos ordenados. En particular, se emplea para probar algunos resultados que recogemos en el Apéndice.

Definición 4.9. Sean G y B dos grupos y A un subgrupo normal de G.

(I) Se dice que G es una **extensión** de B por A si $G/A \cong B$.

(II) Si además G y B son grupos totalmente ordenados y el subgrupo A es convexo, se dice que G es una **extensión lexicográfica** de B por A si $G/A \cong_o B$.

Con la notación anterior, por el punto (2) de la Proposición 4.7, el grupo ordenado Λ_{lex} es una extensión lexicográfica de $\Lambda_{lex}(\Gamma \setminus \Delta)$ por $\Lambda_{lex}(\Delta)$.

Antes de seguir, recordaremos un concepto que nos será útil en los próximos resultados.

Definición 4.10. Dado un grupo $(G, \cdot)$, se dice que un endomorfismo $\varphi : G \longrightarrow G$ es un **automorfismo interno** si corresponde a la acción de conjugación de un elemento fijo de G; esto es, si existe $x \in G$ tal que $\varphi(a) \equiv \varphi_x(a) = x^{-1}ax$ para todo $a \in G$.

La denominación anterior es consistente, porque ciertamente φ_x es un automorfismo, cuyo inverso es $\varphi_{x^{-1}}$.

El resultado siguiente nos dice cuándo, dada una extensión de grupos G de un grupo B por otro A, ambos totalmente ordenados, se puede dotar a G de un orden de forma que la extensión sea también lexicográfica.

Lema 4.11 (F.W. Levi [23], K. Iwasawa [15])**.** *Sean G un grupo y A un subgrupo normal totalmente ordenado de G, tal que el cociente G/A es también totalmente ordenado. Si el conjunto de positivos $P(A)$ es invariante respecto de automorfismos internos en G, se puede extender el orden en A a un orden en todo G, de modo que el orden inducido en el cociente G/A coincide con el dado. Además, el orden en G está unívocamente determinado por los de A y G/A.*

Demostración. Consideramos el conjunto de positivos $P(G/A)$ del grupo cociente y definimos $P := P(A) \cup \{x \in G : xA \in P(G/A)\}$. Probemos que P es un conjunto de positivos en G.

El conjunto P es cerrado para la operación: los dos conjuntos considerados en su definición lo son, y si tomamos $y \in P(A)$ y $z \in \{x \in G : xA \in P(G/A)\}$, entonces $yA + zA = zA \in P$. Además, P es normal. Tomemos $g \in G$ y $x \in P$. Si $x \in P(A)$, entonces $g^{-1}xg$ es su imagen por un automorfismo interno en G, y en consecuencia pertenece a $P(A)$ por la hipótesis de ser invariante; si no, tenemos que $xA \in P(G/A)$, y entonces $g^{-1}xgA \in P(G/A)$ por la normalidad de $P(G/A)$. Consideremos ahora $x \in G$ no neutro y $x \notin P$, es decir, $x \notin P(A)$ y $xA \notin P(G/A)$. Si $x \notin A$, entonces $xA \neq A$, y así $xA \in P(G/A)^{-1}$, luego $x \in P^{-1}$. Alternativamente, si $x \in A$, se tiene que $x \in P(A)^{-1} \subseteq P^{-1}$. Tenemos entonces que $\{e\} \cup P \cup P^{-1} = G$. Por último, si suponemos $x \in P \cap P^{-1}$, debe ocurrir que $x \notin A$, y por tanto $xA \in P(G/A) \cap P(G/A)^{-1} = \varnothing$, lo cual es imposible, así que la intersección es vacía. Así, hemos dotado a G de estructura de grupo totalmente ordenado, que preserva la de A ya que $P(A) \subseteq P$.

Queda por probar que P induce en G/A el mismo orden que $P(G/A)$. Consideremos así el epimorfismo canónico $\pi : G \to G/A$. Los elementos $x \in P$ tienen imagen por π neutra o en $P(G/A)$, así que π es o-homomorfismo. Además, se sigue entonces que $A = \ker \pi$ es convexo, y por la Proposición 2.19, tenemos un o-isomorfismo, y el orden inducido en el cociente G/A coincide con el considerado al principio. La definición por construcción de P para que se preserve el orden en A y G/A asegura la unicidad. □

En los conceptos y resultados anteriores, nos hemos referido únicamente a grupos, ya que los aplicaremos a ellos más adelante. No obstante, se pueden extender de forma análoga para bucles, como prueba P. I. Sklifos [34].

Estudiaremos a continuación el análogo para grupos ordenados del método de Schreier para extensiones de grupos, consistente en construir una extensión G de un grupo X por otro A, a partir de ciertas hipótesis sobre las estructuras de A y X. En este caso, vemos que si A y X son totalmente ordenados, entonces se puede definir un orden total en el mismo G construido. Nótese la diferencia con el resultado anterior, en el que se suponía la existencia de un grupo G, de forma que uno de sus subgrupos normales y el correspondiente cociente eran grupos totalmente ordenados, y se dotaba con ello de un orden a G.

Por simplicidad de notación, dados dos grupos $(A, \cdot_A)$ y $(X, \cdot_X)$, denotaremos con un punto las operaciones en A, y lo omitiremos en las de X. Además, denotaremos los elementos neutros como $1 \in A$ y $e \in X$.

Teorema 4.12. *Sean $(A, \cdot_A)$ y $(X, \cdot_X)$ dos grupos totalmente ordenados. Considérese para cada $x \in X$ un o-automorfismo $\phi_x : A \longrightarrow A$, y adicionalmente una aplicación $f : X \times X \longrightarrow A$. Por brevedad, para cada $x \in X$ y cada $a \in A$ se denota $a^x = \phi_x(a)$; y para cada $(x, y) \in X \times X$, $f_{x,y} := f(x, y)$. En estas condiciones, supóngase que se verifican:*

(I) $f_{e,x} = f_{x,e} = 1 \in A$, donde e denota el neutro en X.

(II) $a^e = a$.

(III) $(a^x)^y = f_{x,y}^{-1} \cdot a^{xy} \cdot f_{x,y}$.

(IV) $f_{xy,z} \cdot (f_{x,y})^z = f_{x,yz} \cdot f_{y,z}$.

Entonces, existe una extensión lexicográfica $(G, \cdot_G)$ *de* X *por* A *y un sistema de representantes completo* $\{g_x : x \in X\} \subseteq G$ *del grupo* G/A*, tales que se verifican:*

(1) La imagen de g_x *por el o-isomorfismo de* G/A *en* X *es* x*, y en consecuencia* $g_e = 1 \cdot_G A$.

(2) Los automorfismos ϕ_x *sobre* A *y los elementos* $f_{x,y} \in A$ *se relacionan con los elementos* $g_x \in G$ *según*

$$a^x = g_x^{-1} \cdot_G a \cdot_G g_x, \quad f_{x,y} = g_{xy}^{-1} \cdot_G g_x \cdot_G g_y.$$

Demostración. Definimos el magma $G = X \times A = \{(x, a) : x \in X, a \in A\}$, con la operación $\cdot_G$ descrita por

$$(x, a) \cdot_G (y, b) := (xy, f_{x,y} \cdot a^y \cdot b).$$

Nótese que para elementos $(e, a), (e, b)$ con $a, b \in A$, resulta $(e, a) \cdot_G (e, b) = (e, a \cdot_A b)$. Por ello, denotaremos ambas con un punto a partir de ahora. Veamos primero que G es grupo. Tomemos $(x, a), (y, b), (z, c) \in G$ y comprobemos que la operación en G es asociativa:

$$\begin{aligned}
[(x, a) \cdot (y, b)] \cdot (z, c) &= (xy, f_{x,y} \cdot a^y \cdot b) \cdot (z, c) \\
&= (xyz, f_{xy,z} \cdot (f_{x,y} \cdot a^y \cdot b)^z \cdot c) = (xyz, f_{xy,z} \cdot (f_{x,y})^z \cdot (a^y)^z \cdot b^z \cdot c) \\
&= (xyz, f_{x,yz} \cdot f_{y,z} \cdot f_{y,z}^{-1} \cdot a^{yz} \cdot f_{y,z} \cdot b^z \cdot c) = (xyz, f_{x,yz} \cdot a^{yz} \cdot f_{y,z} \cdot b^z \cdot c) \\
&= (x, a) \cdot (yz, f_{y,z} \cdot b^z \cdot c) = (x, a) \cdot [(y, b) \cdot (z, c)].
\end{aligned}$$

Resulta por otro lado que $(e, 1) \cdot (x, a) = (x, a) = (x, a) \cdot (e, 1)$, así que también tenemos elemento neutro. Queda por probar la existencia de inverso. Consideramos las operaciones entre (x, a) y $(x^{-1}, (a^{x^{-1}})^{-1} \cdot f_{x,x^{-1}}^{-1})$:

$$\begin{aligned}
(x, a) \cdot (x^{-1}, (a^{x^{-1}})^{-1} \cdot f_{x,x^{-1}}^{-1}) &= (e, f_{x,x^{-1}} \cdot a^{x^{-1}} \cdot (a^{x^{-1}})^{-1} \cdot f_{x,x^{-1}}^{-1}) = (e, 1). \\
(x^{-1}, (a^{x^{-1}})^{-1} \cdot f_{x,x^{-1}}^{-1}) \cdot (x, a) &= (e, f_{x^{-1},x} \cdot ((a^{x^{-1}})^{-1})^x \cdot (f_{x,x^{-1}}^{-1})^x \cdot a) \\
&= (e, f_{x^{-1},x} \cdot f_{x^{-1},x}^{-1} \cdot a^{-1} \cdot f_{x^{-1},x} \cdot (f_{x,x^{-1}}^{-1})^x \cdot a) = (e, 1),
\end{aligned}$$

donde hemos usado que ϕ_x conmuta con la inversión por ser automorfismo y, operando en (IV) con $(x, y, z) = (x, x^{-1}, x)$, que $(f_{x,x^{-1}})^x = f_{x^{-1},x}$. Concluimos así que G es un grupo.

El siguiente paso es ver que G es una extensión de grupos de X por A tal que existe un sistema de representantes $\{g_x : x \in X\} \subseteq G$ del grupo G/A con las propiedades (1) y (2). La proyección canónica $\pi : G \to X$ es un homomorfismo de grupos suprayectivo, con $\ker \pi = \{e\} \times A \cong A$. Por tanto, por el Teorema de Isomorfía, se tiene que $G/A \cong X$. Podemos definir $g_x := (x, 1)$ para $x \in X$, y así tenemos una representación del grupo cociente isomorfo a X. Comprobemos las propiedades (1) y (2):

(1) Tenemos que para todo $x \in X$, $\pi(g_x) = \pi((x, 1)) = x$, y así, g_e se corresponde con $1 \cdot A$.

(2) En el primer caso, comprobamos que

$$g_x \cdot a^x = (x, 1) \cdot (e, a^x) = (x, a^x) = (e, a) \cdot (x, 1) = a \cdot g_x.$$

En el segundo, de forma similar:

$$g_{xy} \cdot f_{x,y} = (xy, 1) \cdot (e, f_{x,y}) = (xy, f_{x,y}) = (x, 1) \cdot (y, 1) = g_x \cdot g_y,$$

lo que concluye esta parte de la prueba.

Queda por probar que la extensión G es, además, una extensión lexicográfica. Para que se cumplan las hipótesis del Lema 4.11, falta verificar que el conjunto de positivos $P(A)$ es invariante respecto de automorfismos internos en G, y entonces tendremos un orden definido sobre G y la o-isomorfía entre X y G/A. Dado entonces $(e,p) \in P(A)$, consideramos su imagen por el automorfismo en G:

$$\begin{array}{rccc} \zeta_{(x,a)}: & G & \longrightarrow & G \\ & g & \longmapsto & (x,a)^{-1} \cdot g \cdot (x,a) \end{array} .$$

Observamos que:

$$(e,p) \cdot (x,a) = (x, p^x \cdot a) = (x,a) \cdot (e, a^{-1} \cdot p^x \cdot a),$$

y en consecuencia, $\zeta_{(x,a)}((e,p)) = (e, a^{-1} \cdot p^x \cdot a)$. Por lo tanto, $\zeta_{(x,a)}|_A$ es composición de la aplicación ϕ_x con un automorfismo interno sobre A. Por hipótesis, la primera es o-automorfismo en A, mientras que, por ser A ordenado, los automorfismos internos preservan el orden. Así, la composición $\zeta_{(x,a)}|_A$ también es o-automorfismo en A, de donde deducimos que $P(A)$ es cerrado respecto de automorfismos internos de G, lo que finaliza la prueba. □

5. Clases arquimedianas y cadenas de subgrupos

Hemos visto que la propiedad arquimediana permite obtener numerosas propiedades sobre los grupos que la poseen, en especial el Teorema de Hölder. Como hemos apuntado, éste se extiende al Teorema de Inmersión de Hahn en el caso general, y del mismo modo algunos de los resultados obtenidos para grupos arquimedianos. Sin embargo, necesitamos un formalismo que nos permita emplear argumentos paralelos en grupos no arquimedianos. Para ello consideraremos primero las clases arquimedianas de un grupo totalmente ordenado, es decir, clasificaremos sus elementos en componentes que sí tienen la propiedad arquimediana. A continuación, estudiaremos las propiedades de la cadena de subgrupos convexos, con especial interés en el concepto de salto entre subgrupos, avanzando hacia el resultado clave del capítulo: el Teorema 5.20, que nos permitirá identificar los saltos en la cadena de subgrupos convexos de un grupo totalmente ordenado con sus clases arquimedianas. Como consecuencia, dispondremos de una cadena de subgrupos con factores arquimedianos, sobre los que podremos utilizar los resultados del Capítulo 3.

5.1. Clases arquimedianas

La noción valor absoluto nos permite introducir las clases arquimedianas.

Definición 5.1. Sean $(G, \cdot)$ un grupo y $a \in G$. Se conoce como **valor absoluto** de a a la cantidad

$$|a| := \text{máx}\{a, a^{-1}\}.$$

Usando el concepto de valor absoluto, la caracterización de subgrupos convexos se puede reformular de manera más sencilla. Si H es un subgrupo, entonces $e \in H$, y es fácil ver que la condición de convexidad es equivalente a que, para todos $h \in H$ y $x \in G$, $|x| \leq |h|$ implica $x \in H$. Emplearemos en general esta caracterización en este capítulo.

Vamos a trabajar en un grupo no necesariamente arquimediano, agrupando entre sí los elementos que verifiquen la propiedad arquimediana.

Definición 5.2. Dados un grupo $(G, \cdot)$ y dos elementos $a, b \in G$, se dice que a y b son **arquimedianamente equivalentes** si existen $n, m \in \mathbb{N}$ tales que $|b| \leq |a|^n$ y $|a| \leq |b|^m$.

Obsérvese que la equivalencia arquimediana define una relación de equivalencia. Consideramos así la siguiente definición.

Definición 5.3. En un grupo G, las clases del conjunto cociente de la relación de equivalencia anterior se conocen como **clases arquimedianas**. Se denota por por $[G]$ el conjunto cociente y por $[x]$ la clase arquimediana de un elemento $x \in G$.

Ejemplos.

1. Si $(G, \cdot)$ es un grupo arquimediano no trivial, el conjunto cociente tiene dos elementos: la clase del neutro $[e]$ y la del resto de elementos $[x] = \{x \in G : x \neq e\}$.

2. En el caso del producto lexicográfico definido en la Sección 4, consideremos $x, y \in \Lambda_{lex}$. Por la definición de la operación en Λ_{lex}, si $[x] = [y]$, tenemos que $\text{máx}(s(x)) = \text{máx}(s(y)) =: \gamma$. Además, los elementos $x(\gamma), y(\gamma)$ deben ser equivalentes en G_γ. El recíproco también es cierto, luego deducimos que las clases de dos elementos coinciden si y sólo si se verifican ambas condiciones.

3. En particular, si consideramos un producto lexicográfico cuyos grupos son arquimedianos, la condición anterior se reduce a la primera cláusula, esto es, a la igualdad del índice máximo del soporte. Por ejemplo, en $\mathbb{R}[x]$, el conjunto cociente es

$$[\mathbb{R}[x]] = \{[0]\} \cup \{[x^n] : n \in \mathbb{N}\}.$$

De manera natural, podemos definir un orden total en $[G]$ mediante la relación

$$[a] < [b] \quad \Leftrightarrow \quad \forall n \in \mathbb{N}, |a|^n < |b|,$$

Asumiremos entonces a partir de ahora que $[G]$ es totalmente ordenado.

Definición 5.4. Dados un grupo G y $a, b \in G$ tales que $[a] < [b]$ en $[G]$, se dice que a es **infinitamente menor** que b y b es **infinitamente mayor** que a.

El lema que enunciamos a continuación aporta algunas propiedades correspondientes a operaciones con valores absolutos y clases arquimedianas, que serán de utilidad a lo largo del capítulo.

Lema 5.5. *Sea $(G, \cdot)$ un grupo totalmente ordenado y $a, b \in G$. Entonces*

(1) $|ab| \leq \text{máx}\{|a||b|, |b||a|\} \leq |a||b||a|$.

(2) G es abeliano si y sólo si $|ab| \leq |a||b|$ para todos $a, b \in G$.

(3) $[ab] \leq \text{máx}\{[a], [b]\}$.

Demostración.

(1) Tenemos que $|ab| = \text{máx}\{ab, b^{-1}a^{-1}\} \leq \text{máx}\{|a||b|, |b||a|\}$, y como a ó a^{-1} es positivo, lo anterior no es mayor que $|a||b||a|$.

(2) Si G es abeliano, la desigualdad es clara. Si no, existen $a, b \in G \setminus \{e\}$ tales que $ab \neq ba$. Si ambos son positivos o negativos, respectivamente, entonces su producto también; en consecuencia, $|a||b| \neq |b||a|$, y así $|ab| = |ba| = \text{máx}\{|a||b|, |b||a|\} > \text{mín}\{|a||b|, |b||a|\}$, luego en uno de los casos no se da la desigualdad. Supongamos ahora que uno es positivo y otro negativo. Por la ley de cancelación, tenemos que $b^{-1}a = b^{-1}abb^{-1} \neq b^{-1}bab^{-1} = ab^{-1}$, y la desigualdad no se cumple para a y b^{-1} por el caso anterior.

(3) Supongamos sin pérdida de generalidad que $[a] \leq [b]$, es decir, existe $n \in \mathbb{N}$ tal que $|a| \leq |b|^n$. Por (1), resulta entonces $|ab| \leq |b|^{n+1}$, y por lo tanto $[ab] \leq [b] = \text{máx}\{[a], [b]\}$.

□

5.2. Valoraciones de grupos

La aplicación canónica $\pi : G \to [G]$ nos conduce al concepto de valoración. La noción habitual en este sentido es la de valoración de un cuerpo mediante un grupo, de la que hablaremos en el Capítulo 6. Sin embargo, su definición no es aplicable como tal a grupos. Por ello, consideramos la siguiente variación que nos permite estudiar un concepto similar para un grupo.

Definición 5.6. Sea Γ un conjunto totalmente ordenado con $e_0 := \text{mín}(\Gamma)$ y $(G, \cdot)$ un grupo. Se dice que una aplicación suprayectiva $\nu : G \to \Gamma$ es una **valoración de grupo** de G por el conjunto Γ si verifica, para todos $x, y \in G$:

(I) $\nu(x) = e_0$ si y sólo si $x = e$.

(II) $\nu(x) = \nu(x^{-1})$.

(III) $\nu(xy) \leq \text{máx}\{\nu(x), \nu(y)\}$.

Definición 5.7. Dadas dos **valoraciones** ν_1, ν_2 de un grupo $(G, \cdot)$ por conjuntos Γ_1, Γ_2, respectivamente, se dice que son **equivalentes** si existe una biyección $\sigma : \Gamma_1 \to \Gamma_2$ que preserve el orden y de forma que $\nu_2 = \sigma \circ \nu_1$.

Ejemplos.

1. Dado un grupo totalmente ordenado $(G, \cdot)$, la aplicación canónica $\pi : G \to [G]$ es una valoración, llamada **valoración natural**. En efecto, con la relación de orden natural en $[G]$, tenemos (I) ya que $[e] = \text{mín}([G])$, y además $[x] = [e] = \{e\}$ si y sólo si $x = e$. Por otro lado, $[x] = [x^{-1}]$ por coincidir sus valores absolutos, así que se da (II); mientras que (III) es consecuencia del Lema 5.5.

2. En el caso particular del producto lexicográfico de grupos $\Lambda_{lex} = \Pi_{\gamma\in\Gamma} G_\gamma$, la aplicación canónica
$$\begin{array}{rccc} \pi: & \Lambda_{lex} & \longrightarrow & \Gamma \cup \{e\} \\ & x & \longmapsto & \left\{ \begin{array}{cc} e, & \text{si } x = e, \\ \text{máx}(s(x)), & \text{en otro caso,} \end{array} \right. \end{array}$$
donde $s(x)$ denota el soporte de $x \in \Lambda_{lex}$, es una valoración de grupos. Si, adicionalmente, todos los grupos son arquimedianos, entonces dos elementos son arquimedianamente equivalentes si y sólo si sus soportes tienen el mismo máximo, y por tanto la aplicación anterior es la valoración natural de Λ_{lex} en $[\Lambda_{lex}]$.

3. Una posible valoración de $\mathbb{Z}$ es la valoración p-ádica. Dado $m \in \mathbb{Z}$, existe una factorización única (salvo unidades) en números primos,
$$m = \prod_{i=1}^{n} p_i^{r_i}.$$
Dado un primo $p \in \mathbb{N}$, podemos escribir entonces $m = \hat{m}p^r$, con $\hat{m}$ coprimo con p, y $r \in \mathbb{N}$. Con ello, definimos la aplicación
$$\begin{array}{rccc} \tilde{\nu}_p: & \mathbb{Z} & \longrightarrow & \{0\} \cup \mathbb{N}_{\geq 1}^{-1} \cup \{\infty\} \\ & m & \longmapsto & \left\{ \begin{array}{cc} 0, & \text{si } m = 0. \\ 1/r, & \text{en otro caso.} \end{array} \right. \end{array}$$
Se puede comprobar que satisface las tres propiedades de la definición de valoración. Este ejemplo es la adaptación de la valoración p-ádica clásica sobre $\mathbb{Q}$ a la definición de valoración de grupos, y su definición como valoración de cuerpos, que introducimos en la Sección 6.3, resulta mucho más natural. Se puede probar que las valoraciones p-ádicas son las únicas posibles no triviales en $\mathbb{Z}$ salvo equivalencia [32].

Enunciamos a continuación propiedades características de las valoraciones.

Lema 5.8. *Sea $(G, \cdot)$ un grupo y $\nu : G \to \Gamma$ una valoración. Entonces:*

(1) Si $\nu(a) \neq \nu(b)$, entonces $\nu(ab) = \text{máx}\{\nu(a), \nu(b)\}$.

(2) Dado un subconjunto finito $\{a_i : 1 \leq i \leq n\} \subseteq G$, se tiene que
$$\nu\left(\prod_{i=1}^{n} a_i\right) \leq \text{máx}\{\nu(a_i) : 1 \leq i \leq n\},$$
y la igualdad está garantizada si se verifica $\nu(a_k) = \text{máx}\{\nu(a_i) : 1 \leq i \leq n\}$ para exactamente un índice k.

Demostración.

(1) Supongamos sin pérdida de generalidad $\nu(a) < \nu(b)$. Siguiendo la definición tenemos que $\nu(ab) \leq \text{máx}\{\nu(a), \nu(b)\}$. Si la desigualdad fuera estricta, tendríamos
$$\nu(b) = \nu(a^{-1}ab) \leq \text{máx}\{\nu(a), \nu(ab)\} < \nu(b),$$
lo cual es imposible, de donde deducimos que se trata de una igualdad.

(2) Usando que máx{máx{x, y}, z} = máx{x, y, z}, observamos por inducción que podemos extender la propiedad (III) de la Definición 5.6 a un conjunto finito de elementos. En el caso de la igualdad, tengamos en cuenta que (1) prueba el resultado para $n = 2$, y supongamos que existe exactamente un índice k tal que $\nu(a_k) = \text{máx}\{\nu(a_i) : 1 \leq i \leq n\}$. Entonces, separando el producto en tres factores, y usando la propiedad de dos en dos:

$$\begin{aligned}\nu\left(\prod_{i=1}^{n} a_i\right) &= \nu\left(\left[\prod_{i=1}^{k-1} a_i\right] a_k \left[\prod_{i=k+1}^{n+1} a_i\right]\right) \\ &= \text{máx}\left\{\text{máx}\left\{\nu\left(\prod_{i=1}^{k-1} a_i\right), \nu(a_k)\right\}, \nu\left(\prod_{i=k+1}^{n+1} a_i\right)\right\} \\ &= \text{máx}\left\{\nu(a_k), \nu\left(\prod_{i=k+1}^{n+1} a_i\right)\right\} = \nu(a_k) = \text{máx}\{\nu(a_i) : 1 \leq i \leq n\},\end{aligned}$$

donde alguno de los productos considerados puede ser vacío, y por tanto igual al neutro.

□

5.3. Familias de subgrupos

En lo que resta de capítulo, emplearemos las propiedades especiales de ciertas familias de subgrupos para estudiar la estructura de grupo totalmente ordenado. El desarrollo se basará en el concepto de salto entre dos subgrupos, definido en las denominadas familias completas, y que nos permitirá relacionar en un grupo ordenado las clases arquimedianas con los subgrupos convexos en el Teorema 5.20. En particular, veremos en el Teorema 5.22 que los factores entre subgrupos convexos son grupos arquimedianos.

Definición 5.9. Dados un subgrupo H de un grupo $(G, \cdot)$ y un elemento $g \in G$, se define el **subgrupo conjugado** de H, y se denota por H^g, como la imagen de H por el automorfismo interno $\varphi_g : G \to G$ tal que $\varphi_g(x) = g^{-1}xg$ para $x \in G$.

Obsérvese que H^g es un subgrupo por ser la imagen por un homomorfismo del subgrupo H.

Definición 5.10. Sea G un grupo. Se dice que una **familia** $\mathcal{G}$ de subgrupos de G, parcialmente ordenada por la inclusión, es **completa**, si la unión e intersección arbitrarias de elementos de $\mathcal{G}$ pertenece a $\mathcal{G}$.

Proposición 5.11. *Una familia completa de subgrupos está totalmente ordenada por la inclusión.*

Demostración. Dados un grupo G, una familia completa $\mathcal{G}$ de subgrupos de G y $H, K \in \mathcal{G}$, tenemos que $H \cup K$ es subgrupo si y sólo si $H \subseteq K$ ó $K \subseteq H$, así que la relación de inclusión define un orden total. □

Dado este resultado, también emplearemos con frecuencia el término **cadena** para referirnos a una familia completa, en especial cuando más adelante hablemos de la familia de subgrupos convexos. Observamos que toda cadena posee elemento máximo y mínimo, coincidentes con la unión e intersección de todos sus elementos, respectivamente.

Definición 5.12. Sea G un grupo. Se dice que una familia completa $\mathcal{G}$ es **subinvariante** si posee, además, las propiedades:

(I) $\{e\}, G \in \mathcal{G}$.

(II) Para todo $H \in \mathcal{G}$ y todo $g \in G$, $H^g \in \mathcal{G}$.

Ejemplos.

1. En $\mathbb{Z}$, las familias de subgrupos $\mathcal{Z}(n) = \{n^k\mathbb{Z} : k \in \mathbb{N}\} \cup \{\{0\}\}$ con n fijo son subinvariantes: su unión e intersección son, respectivamente, el subgrupo generado por la potencia menor y mayor de n, y para $k = 0$ se tiene todo $\mathbb{Z}$; las otras dos propiedades se verifican trivialmente.

2. Dado un grupo $(G, \cdot)$ y el grupo de polinomios con coeficientes en él, $G[x]$, cada una de las familias $\mathcal{G}(\Gamma) = \{G_n[x] : n \in \Gamma\}$, donde $\Gamma \subseteq \mathbb{N}$, es completa. Si además se le añaden los subgrupos $\{e\}$ y $G[x]$, entonces es subinvariante. En efecto, la segunda propiedad se verifica porque el grado de $q^{-1}pq$ coincide con el de q para cualquier par de polinomios $p, q \in G[x]$, por ser la conjugación, aplicada a cada coeficiente, un isomorfismo en G.

En los dos ejemplos propuestos, podemos ver que hay pares de subgrupos consecutivos respecto de la inclusión; es decir, que no hay ningún elemento en la familia entre ellos. Podemos definir con rigor esta propiedad.

Definición 5.13. Sean $\mathcal{G}$ una familia completa de subgrupos y $A \subsetneq B \in \mathcal{G}$. Se dice que entre A y B hay un **salto**, y se denota $A \sqsubset B$, si no hay ningún elemento de $\mathcal{G}$ entre A y B. Se dice que A y B son, respectivamente, los subgrupos inferior y superior del salto.

Definición 5.14. Dada una familia completa de subgrupos $\mathcal{G}$, la familia de pares de subgrupos $\mathcal{S}(\mathcal{G}) = \{(A, B) \in \mathcal{G} \times \mathcal{G} : A \sqsubset B \text{ es un salto}\}$ se llama **conjunto de saltos** de la familia $\mathcal{G}$.

Emplearemos indistintamente las notaciones $A \sqsubset B$ y (A, B) para referirnos a un salto en una familia $\mathcal{G}$, según la conveniencia. Asimismo, denotaremos el conjunto de saltos simplemente por $\mathcal{S}$ cuando no haya ambigüedad sobre la familia de subgrupos considerada.

Observación 5.15. Podemos extraer las siguientes propiedades de la definición de salto.

1. Consideramos dos saltos $A \sqsubset B$ y $A \sqsubset C$ en una familia $\mathcal{G}$. Entonces, como consecuencia de la Proposición 5.11, se tiene que $B \subseteq C$ por el primer salto y $C \subseteq B$ por el segundo, y así $B = C$. El mismo razonamiento se puede realizar en el sentido opuesto. Es decir, un subgrupo posee a lo sumo un único sucesor y antecesor en $\mathcal{G}$.

2. Sea $\mathcal{G}$ es una familia completa de subgrupos de un grupo G. Entonces, cada elemento no neutro $x \in G$ determina un salto en $\mathcal{G}$, es decir, existe una aplicación

$$\begin{array}{rccc} h_{\mathcal{G}}: & G & \longrightarrow & \mathcal{S}(\mathcal{G}) \\ & x & \longmapsto & (A(x), B(x)) \end{array},$$

donde

$$A(x) := \bigcup_{x \notin H, H \in \mathcal{G}} H, \quad B(x) := \bigcap_{x \in H, H \in \mathcal{G}} H.$$

Comprobamos que está bien definida. Por la Proposición 5.11, se tiene que $A(x) \subsetneq B(x)$. Para cualquier otro subgrupo $C \in \mathcal{G}$, si $x \in C$ entonces $B(x) \subseteq C$, y si no $C \subseteq A(x)$. Así que no hay subgrupos de $\mathcal{G}$ entre ambos, de donde deducimos $A(x) \sqsubset B(x)$.

En general, no todo subgrupo de una familia completa tiene por qué corresponder a un salto. Por ejemplo, podemos considerar, fijado $n \in \mathbb{Z}_{\geq 2}$, la familia

$$\mathcal{Z}_n = \{\{0\}\} \cup \left\{n^k\mathbb{Z} : k \in \mathbb{N}\right\}.$$

Observamos que para todo $k \in \mathbb{N}$, la inclusión $n^{k+1}\mathbb{Z} \subseteq n^k\mathbb{Z}$ es un salto, pero sin embargo no existe ningún $k \in \mathbb{N}$ tal que $\{0\} \sqsubset n^k\mathbb{Z}$. No obstante, probamos a continuación que si la cantidad de saltos es finita, podemos identificar cada subgrupo de la cadena, a excepción del máximo, con el subgrupo inferior de un salto.

Proposición 5.16. *Sea $\mathcal{G}$ una familia completa de subgrupos. Si el número de saltos en $\mathcal{G}$ es finito, entonces todo elemento de $\mathcal{G}$ es el subgrupo inferior de un salto, excepto el máximo M. En consecuencia, existe una biyección entre $\mathcal{G} \setminus \{M\}$ y el conjunto de saltos $\mathcal{S}(\mathcal{G})$, y por tanto la familia $\mathcal{G}$ es finita.*

Demostración. Consideramos un subgrupo $H \in \mathcal{G}$ distinto de M, y para cada $x \in M \setminus H$, el salto $h_{\mathcal{G}}(x) = (A(x), B(x))$ que determina. Dado que la familia de saltos es finita, la intersección $\bigcap_{x \in M \setminus H} A(x)$ es finita, y por tanto igual a $A(x_0)$ para cierto $x_0 \in M \setminus H$. Como entre $A(x)$ y $B(x)$ no hay subgrupos de $\mathcal{G}$ y $x \in B(x)$, se tiene que $H \subseteq A(x)$ para todo $x \in M \setminus H$, y en particular $H \subseteq A(x_0)$. Por otro lado, para todo $x \in M \setminus H$, $x \notin A(x_0)$, luego $A(x_0) \subseteq H$. Tenemos así que $H = A(x_0)$ es el subgrupo inferior del salto $h_{\mathcal{G}}(x_0)$.

Con ello, queda definida automáticamente la biyección entre $\mathcal{G} \setminus \{M\}$ y $\mathcal{S}(\mathcal{G})$. □

Esta biyección nos será de gran utilidad cuando trabajemos con la cadena de subgrupos convexos de un grupo G, que como veremos es subinvariante. En ese caso, tendremos $M = G$, y en consecuencia, en el caso finito podremos extender las propiedades de los subgrupos que forman un salto a todos los subgrupos propios de la familia.

Antes de seguir enunciando resultados sobre saltos, recordamos el concepto de normalizador de un subconjunto de un grupo.

Definición 5.17. Sea A un subconjunto de un grupo $(G, \cdot)$. Se define el **normalizador** de A, y se denota por $N(A)$, como el conjunto de elementos $g \in G$ tales que $gA = Ag$.

Un resultado conocido es que $N(A)$ es un subgrupo de G, y en consecuencia $A \cap N(A)$ es un subconjunto normal de $N(A)$.

Lema 5.18. *Sea $\mathcal{G}$ una familia completa de subgrupos y $A \sqsubset B$ un salto. Entonces:*

(1) A es normal en B.

(2) $N(A) = N(B)$.

Demostración.

(1) Dado $b \in B$, A^b es un subgrupo de $\mathcal{G}$ contenido en B. Si fuera $A^b = B$, entonces, como la conjugación es biyectiva, se tendría $B^{b^{-1}} = B$, y al mismo tiempo $B^{b^{-1}} = (A^b)^{b^{-1}} = A$, así que $B = A$, en contradicción con $A \sqsubset B$. Entonces debe ser $A^b \subseteq A$, y en consecuencia A es normal en B.

(2) Dado $g \in G$, resulta $A^g \subseteq B^g$, y por la relación de inclusión es de hecho un salto $A^g \sqsubset B^g$. Entonces, si $g \in N(A)$, tenemos $A = A^g$, y así, dos saltos a B y B^g. En consecuencia, son iguales, por la Observación 5.15 (1). Luego $g \in N(B)$. El mismo razonamiento sirve para probar la otra inclusión, y concluimos la igualdad.

□

Se pueden emplear las nociones anteriores para estudiar la estructura ordenada de un grupo, a través de los subgrupos convexos, como ya hemos avanzado al presentar algunas de ellas. Empezamos viendo que la cadena de subgrupos convexos de un grupo totalmente ordenado verifica las definiciones anteriores.

Lema 5.19. *La familia $\mathcal{G}$ de los subgrupos convexos de un grupo totalmente ordenado $(G, \cdot)$ es subinvariante.*

Demostración. Veamos que la inclusión define un orden total en $\mathcal{G}$. Consideramos dos conjuntos convexos distintos $A, B \in \mathcal{G}$. Supongamos sin pérdida de generalidad $A \not\subseteq B$. Veamos que entonces se tiene $B \subseteq A$. Sean $b \in B$ y $a \in A \setminus B$, supuestos positivos. Entonces, como $a \notin B$, debe ser $e < b < a$, y por convexidad de A, resulta $b \in A$. En consecuencia, $B \subseteq A$. Por ello, la unión e intersección de subgrupos convexos forma también parte de la familia.

Por otro lado, $\{e\}$ y G son subgrupos convexos. Queda por ver que dado un subgrupo convexo H, su conjugado H^g es convexo para todo $g \in G$. Sean así $g, x \in G$ y $a \in H$, tales que

$$e \leq x \leq g^{-1}ag.$$

Entonces, por la compatibilidad del orden con la operación, resulta

$$e = geg^{-1} \leq gxg^{-1} \leq a.$$

Por tanto $gxg^{-1} \in H$, y así $x = g^{-1}(gxg^{-1})g \in H^g$, con lo que H^g es también convexo. □

En este punto estamos en condiciones de probar el resultado central del capítulo, en el que relacionamos los subgrupos convexos de un grupo totalmente ordenado con sus clases arquimedianas. Éste será otro de los argumentos esenciales a la hora de demostrar el Teorema de Inmersión de Hahn, puesto que nos permitirá generalizar el resultado de Hölder a grupos con más de una clase arquimediana.

Teorema 5.20. *Sean $(G, \cdot)$ un grupo totalmente ordenado y $x \in G$ un elemento distinto del neutro. Entonces:*

(1) Los conjuntos

$$G_{[x]} = \{g \in G : [g] < [x]\}, \ y \quad G^{[x]} = \{g \in G : [g] \leq [x]\}$$

son, a su vez, subgrupos convexos.

(2) Si $h(x) = (A, B)$ es el salto determinado por x en la familia de subgrupos convexos, se tiene que $G_{[x]} = A$ y $G^{[x]} = B$.

(3) Dotando al conjunto $\mathcal{S}$ de saltos entre subgrupos convexos de G, con el orden dado por

$$(A, B) \prec (A', B') \quad \Leftrightarrow \quad A \subsetneq A',$$

la siguiente es una o-biyección entre $\mathcal{S} \cup \{e_0\}$ y el conjunto de clases arquimedianas de G:

$$\eta : \begin{array}{ccc} [G] & \longrightarrow & \mathcal{S} \cup \{e_0\} \\ [x] & \longmapsto & \begin{cases} e_0, & \text{si } x = e, \\ h(x), & \text{en otro caso.} \end{cases} \end{array}$$

(4) La aplicación $\nu = \eta \circ \pi$, donde $\pi : G \mapsto [G]$ denota la valoración natural, es una valoración sobre G equivalente a π.

Demostración.

(1) Los conjuntos definidos no son vacíos porque ambos contienen al neutro. Además, por ser $|a^{-1}| = |a|$, y usando la propiedad (3) del Lema 5.5, las desigualdades se mantienen al operar ab^{-1} para todo par a, b en cualquiera de los dos conjuntos, luego son subgrupos.

En cuanto a la convexidad, dados $a \in G$ y $b \in G^{[x]}$ con $|a| \leq |b|$, se tiene que $[a] \leq [b] \leq [x]$, luego $a \in G^{[x]}$. El mismo razonamiento es válido empleando desigualdades estrictas, lo que prueba que ambos subgrupos son convexos.

(2) Notamos primero que $G_{[x]} \neq G^{[x]}$, dado que $x \in G^{[x]} \setminus G_{[x]}$. Con ello, veamos que $A \subseteq G_{[x]}$ y $G^{[x]} \subseteq B$, lo que garantiza $A = G_{[x]}$ y $G^{[x]} = B$, por la propiedad de salto. En efecto, dado $a \in A$, como A es subgrupo convexo y $x \notin A$, debe ser $|a^n| < |x|$ para todo $n \in \mathbb{N}$. Por lo tanto, tenemos $[a] < [x]$, y con ello $A \subseteq G_{[x]}$. Asimismo, si $g \in G^{[x]}$, entonces existe $n \in \mathbb{N}$ tal que $|g| < |x^n| \in B$, y por convexidad tenemos $g \in B$.

(3) Observamos primero que, dados $x, y \in G$, tenemos que $[x] = [y]$ si y sólo si $G_{[x]} = G_{[y]}$ y $G^{[x]} = G^{[y]}$, y esto a su vez equivale a que $h(x) = \left(G_{[x]}, G^{[x]}\right) = h(y)$. Con ello tenemos que η está bien definida y es inyectiva. La suprayectividad sigue de que la diferencia $B \setminus A$ nunca es vacía para un salto $(A, B) \in \mathcal{S}$.

Vemos también que η transforma el orden en $[G]$ en el orden definido en $\mathcal{S} \cup \{e_0\}$ a partir de la definición de $G_{[x]}$ y $G^{[x]}$ y lo visto en (2).

(4) Considerando la valoración natural $\pi : G \longmapsto [G]$, observamos que $\nu = \eta \circ \pi$. Por lo tanto, la aplicación ν es una valoración equivalente a la valoración natural.

□

En otras palabras, acabamos de probar que los saltos entre subgrupos convexos de G se corresponden uno a uno con las clases arquimedianas del grupo. En particular, todos los elementos que se encuentran entre dos subgrupos convexos pertenecen a la misma clase arquimediana, lo que significa que el grupo cociente entre dos subgrupos que forman un salto es arquimediano, y en consecuencia o-isomorfo a un subgrupo aditivo de los reales, como consecuencia del Teorema de Hölder. Recogemos este razonamiento a continuación, definiendo primero el concepto de factor en una familia subinvariante, que nos facilitará la redacción al estudiar cocientes entre sus elementos.

Definición 5.21. Dada una familia subinvariante de subgrupos $\mathcal{G}$, los grupos cociente entre los subgrupos superior e inferior de cada uno de sus saltos se denominan **factores**.

Teorema 5.22 (K. Iwasawa [15])**.** *Sea $\mathcal{G}$ la familia de subgrupos convexos de un grupo totalmente ordenado $(G, \cdot)$. Dado un salto $(A, B) \in \mathcal{S}(\mathcal{G})$, el grupo cociente B/A es o-isomorfo a un subgrupo de $(\mathbb{R}, +)$. Además, el subgrupo de automorfismos de B/A generado por automorfismos internos de $N(A)/A$ es isomorfo a un subgrupo de $(\mathbb{R}_{>0}, \cdot)$.*

Demostración. Como $A \sqsubset B$ es un salto en la familia de subgrupos convexos, los únicos subgrupos convexos de B/A son $\{e\}$ y el total, y por el Teorema 3.5, B/A es arquimediano. En consecuencia, por el Teorema 3.10, es o-isomorfo a un subgrupo de $(\mathbb{R}, +)$.

Dado $g \in N(A)$, consideramos $gA \in N(A)/A$, y definimos el homomorfismo de grupos:

$$\begin{array}{rccc} \varphi_g : & B/A & \longrightarrow & B/A \\ & bA & \longmapsto & (gA)^{-1} \cdot bA \cdot gA \end{array} ,$$

bien definido porque $g \in N(A) = N(B)$, y que preserva el orden inducido en B/A, por la compatibilidad al operar con $g \in N(A) \subseteq G$. El resultado se sigue del Corolario 3.12. □

Corolario 5.23. *La cadena de subgrupos convexos de un grupo G totalmente ordenado es una familia subinvariante con factores abelianos. En otras palabras, G es un AN-grupo*[1]*.*

[1] En el sentido de Kurosch [21], p. 20-22, 28.

5.4. Consecuencias de la relación entre clases arquimedianas y subgrupos convexos

Para completar esta sección, veremos que el recíproco del Teorema 5.22 también es cierto, si bien no se trata de un resultado necesario para lo que sigue. En otras palabras, la ordenabilidad de un grupo está garantizada si posee una familia subinvariante con las propiedades deducidas para la cadena de subgrupos convexos, y dicha familia será precisamente la de los subgrupos convexos. En primer lugar, damos una segunda caracterización de grupo ordenable que se suma a la del Teorema 4.8, esta vez extendida a grupos no necesariamente abelianos. Como se ha indicado, el Apéndice incluye algunos resultados más acerca de la caracterización de los grupos ordenables.

Teorema 5.24 (A. I. Kokorin [19])**.** *Un grupo $(G,\cdot)$ es ordenable si y sólo si posee una familia subinvariante de subgrupos $\mathcal{G}$, de forma que para todo salto $A \sqsubset B$ en $\mathcal{G}$, el grupo cociente $N(A)/A$ es ordenable. Además, se puede elegir el orden en G de forma que los elementos de $\mathcal{G}$ sean subgrupos convexos.*

Demostración. Hemos probado que la condición es necesaria en el Teorema 5.22. En efecto, si el subgrupo de automorfismos de B/A generado por automorfismos internos de $N(A)/A$ es isomorfo a un subgrupo de $(\mathbb{R}_{>0},\cdot)$, que es un grupo totalmente ordenado, podemos dotar a $N(A)/A$ del orden total inducido por este isomorfismo.

Recíprocamente, suponemos que G posee una familia subinvariante de subgrupos $\mathcal{G}$ con la propiedad enunciada. Sea $\mathcal{S}$ el conjunto de saltos de $\mathcal{G}$. Para cada salto $(A,B) \in \mathcal{S}$ consideramos la familia $\{(A^g, B^g) : g \in G\} \subseteq \mathcal{S}$ dada por los conjugados del salto por elementos de G, y con ella la correspondiente partición de $\mathcal{S}$. Elegimos un representante de cada clase, que denotamos por (A^*, B^*). Por hipótesis, para cada una de ellas existe una ordenación total de $N(A^*)/A^*$, caracterizada por el conjunto de positivos $\bar{P}_A^*$. Denotamos por P_A^* la intersección con B^* de los elementos de $N(A^*)$ cuya clase es positiva en el cociente, y a partir de ello:

$$P_A := \bigcup_{g\in G} g^{-1}P_A^* g, \quad P := \bigcup_{(A,B)\in\mathcal{S}} P_A.$$

Probaremos que P es un conjunto de positivos de G, según la caracterización del Corolario 2.15.

Primero, veamos que $\{e\} \cup P \cup P^{-1} = G$. Sea $x \in G \setminus P$ no neutro, y sea $g \in G$ tal que x determina el salto $g^{-1}A^*g \sqsubset g^{-1}B^*g$ de $\mathcal{S}$, de acuerdo con la Observación 5.15. Entonces se tiene que $gxg^{-1} \in B^* \setminus P_A^*$, y equivalentemente, dado que $x \neq e$, su clase en $N(A^*)/A^*$ verifica

$$gxg^{-1}A^* \in N(A^*)/A^* \setminus \left(\{e_0\} \cup \bar{P}_A^*\right),$$

donde e_0 es el neutro en $N(A^*)/A^*$. Como $\bar{P}_A^*$ es conjunto de positivos, debe ser $g^{-1}x^{-1}g \in P_A^*$, y así $x \in P^{-1}$. Un razonamiento similar prueba que $P \cap P^{-1} = \varnothing$: si suponemos $x \in P \cap P^{-1}$, y consideramos el salto $g^{-1}A^*g \sqsubset g^{-1}B^*g$ determinado por x, tenemos que ambos elementos $x, x^{-1} \in (g^{-1}B^*g) \setminus (g^{-1}A^*g)$. Por definición de los P_H^* con $(H,K) \in \mathcal{S}$, dado que $x \notin (g^{-1}A^*g)$, x no puede pertenecer a ningún P_H^* con $H \subsetneq A$. Por otra parte, las clases definidas por x son nulas, y por tanto no positivas, para los saltos (H,K) con $A \subsetneq H$. Razonando análogamente para x^{-1}, llegamos a que $gxg^{-1}, gx^{-1}g^{-1} \in P_A^*$. Sin embargo, esto no es posible por ser $N(A^*)/A^*$ totalmente ordenado, y se concluye que la intersección es vacía.

Lo siguiente es ver que P es cerrado respecto de la operación en G. Sean entonces $x, y \in P$ y denotemos los saltos que determinan x e y por, respectivamente

$$g^{-1}A^*g \sqsubset g^{-1}B^*g, \quad h^{-1}H^*h \sqsubset h^{-1}K^*h.$$

Supongamos sin pérdida de generalidad que $g^{-1}B^*g \subseteq h^{-1}K^*h$. Si de hecho son iguales, tenemos también $A = H$, y con ello $x \in g^{-1}P_A^*g$, e $y \in h^{-1}P_A^*h$. Deducimos que $B^* \subseteq hg^{-1}B^*gh^{-1} \subseteq B^*$,

es decir, $(gh^{-1})^{-1}B^*(gh^{-1}) = B^*$. En consecuencia, $gh^{-1} \in N(B^*) = N(A^*)$, donde la igualdad sigue del Lema 5.18, y entonces $gxg^{-1} \in P_A^*$, es decir, $gxg^{-1}A^* \in \bar{P}_A^*$ en el grupo cociente $N(A^*)/A^*$. Operando con $gh^{-1}A^*$, tenemos $(gh^{-1}A^*)^{-1}(gxg^{-1}A^*)(gh^{-1}A^*) = hxh^{-1}A^* \in \bar{P}_A^*$. Además $hyh^{-1} \in P_A^*$, es decir, $hyh^{-1}A^* \in \bar{P}_A^*$. Ahora, sin más que operar ambas expresiones, obtenemos $h(xy)h^{-1}A^* \in \bar{P}_A^*$, por tanto $h(xy)h^{-1} \in P_A^*$, y entonces $xy \in P$. Falta por considerar el caso en el que $g^{-1}B^*g \subsetneq h^{-1}K^*h$. Por tratarse de un salto, resulta $g^{-1}B^*g \subseteq h^{-1}H^*h$. Entonces $hxh^{-1}H^*$ es la clase nula en $N(H^*)/H^*$, con lo que $h(xy)h^{-1}H^* = hyh^{-1}H^*$, que es positivo. Luego $h(xy)h^{-1} \in P_H^*$, y entonces de nuevo $xy \in P$.

Por último, probamos que P es un subconjunto normal de G. Si $x \in P$, entonces $x = g^{-1}ag$ para algún $g \in G$, $a \in P_A^*$. Ahora, dado $h \in G$, se tiene que $h^{-1}g^{-1}agh = (gh)^{-1}a(gh) \in P_A \subseteq P$, luego P es normal.

Veamos que, además, el orden así definido hace que los elementos de $\mathcal{G}$ sean subgrupos convexos. Sea $(A, B) \in \mathcal{S}$ un salto. Probamos primero que, en ese caso, A es un subgrupo convexo, y posteriormente que lo es cualquier elemento de $\mathcal{G}$. El epimorfismo canónico $\pi_A : B^* \to B^*/A^*$ es, por la definición de P en función de P_A^*, un o-homomorfismo, cuyo núcleo es A^*, que por tanto es convexo en B^*. Con ello, debido a la propiedad de compatibilidad, A es convexo en B. Queda por probar que lo es en G. Consideramos $g \in G$ tal que $e < g < h \in A \sqsubset B$, y sea $H \sqsubset K$ el salto determinado por g. Si fuera $A \subseteq H$, resultaría $h \in H$ con $g \in K \setminus H$, lo que es imposible por ser H convexo en K. Como la familia $\mathcal{G}$ es subinvariante, debe ser $H \subsetneq A$, y entonces $g \in A$, así que A es convexo. Consideramos ahora un subgrupo cualquiera $H \in \mathcal{G}$. Dado $x \in G$, recordamos la caracterización del subgrupo inferior $A(x)$ del salto que determina como el subgrupo maximal de $\mathcal{G}$ que no contiene a x. Por lo probado antes, el subgrupo $A(x)$ es convexo. Con ello, podemos describir H según

$$H = \bigcap_{x \in G \setminus H} A(x),$$

y por ser la intersección de subgrupos un subgrupo convexo, hemos probado el resultado. □

Este resultado nos permite extender también el Teorema 5.22 y formularlo como una equivalencia. Deduciremos además que no sólo los subgrupos de la familia subinvariante $\mathcal{G}$ son convexos, sino que esta contiene todos los subgrupos convexos de G.

Corolario 5.25 (K. Iwasawa [15])**.** *Un grupo $(G, \cdot)$ es ordenable si y sólo si posee una familia subinvariante de subgrupos $\mathcal{G}$ con las propiedades:*

(1) Para todo salto $A \sqsubset B$ en $\mathcal{G}$, el grupo cociente B/A es isomorfo a un subgrupo de $(\mathbb{R}, +)$.

(2) El grupo de automorfismos de B/A generado por los automorfismos internos de $N(A)/A$ es isomorfo a un subgrupo de $(\mathbb{R}, \cdot)$.

Además, existe una ordenación de G de forma que $\mathcal{G}$ es la cadena de subgrupos convexos de G.

Demostración. La implicación directa ya se ha probado en el Teorema 5.22, mientras que empleando el Teorema 5.24 junto con las hipótesis enunciadas, se obtiene la ordenabilidad en $\mathcal{G}$.

Probamos que con el orden definido en el Teorema 5.24, todo subgrupo convexo de G está en $\mathcal{G}$. Sea $H \neq \{e\}$ un subgrupo convexo de G. Sean A el subgrupo maximal de $\mathcal{G}$ contenido en H y B el subrupo minimal de $\mathcal{G}$ que contiene a H. Supongamos que ninguna de las contenciones es una igualdad. Entonces existen elementos $h, b \in G$ de modo que $h \in H \setminus A$ y $b \in B \setminus H$, y en consecuencia no pueden determinar el mismo salto en la cadena de subgrupos convexos. Por el Teorema 5.20, esto implica que las clases arquimedianas de h y b en G son diferentes, y así, para todo $n \in \mathbb{N}$, resulta también

$$(hA)^n < bA.$$

Sin embargo, esto no es posible por ser B/A isomorfo a un subgrupo de $\mathbb{R}$ y, en consecuencia, arquimediano. □

Para cerrar el capítulo, mostramos algunos resultados que se deducen de la relación entre subgrupos convexos y clases arquimedianas. Consideremos un automorfismo interno σ en un grupo totalmente ordenado G, y la correspondencia inducida en $[G]$ según $\hat{\sigma} : [g] \mapsto [\sigma(g)]$. Se trata, de hecho, de una aplicación, porque σ preserva el orden debido a la propiedad de compatibilidad en la estructura ordenada. Además, $\hat{\sigma}$ es biyectiva y preserva el orden en $[G]$. Suponiendo sin pérdida de generalidad $[g] \leq [\sigma(g)]$, tenemos la cadena

$$... \leq [\sigma^{-2}(g)] \leq [\sigma^{-1}(g)] \leq g \leq [\sigma(g)] \leq [\sigma^2(g)] \leq ...$$

En relación con ello, enunciamos el siguiente resultado. Recordamos que una sucesión de conjuntos totalmente ordenada por la inclusión satisface la condición de cadena ascendente o descendente si uno de los conjuntos que la forma es cota superior o inferior, respectivamente.

Proposición 5.26. *Sea G un grupo totalmente ordenado. Si la familia $[G]$ de sus clases arquimedianas satisface la condición de cadena ascendente o descendente, entonces todos los subgrupos convexos de G son normales. Se dice entonces que la cadena es invariante y, así, G es un AI-grupo*[2]*.*

Demostración. Supongamos que $[G]$ satisface la condición de cadena ascendente o descendente. Entonces existe $n \in \mathbb{Z}$ tal que $[\sigma^n(g)] = [\sigma^{n+1}(g)]$, y así, aplicando $\hat{\sigma}^{-n}$, resulta $[g] = [\sigma(g)]$ para cada $g \in G$. En consecuencia, las clases arquimedianas son invariantes frente a conjugación. Adicionalmente, se trata de una familia finita.

Considerando la o-biyección entre $[G]$ y el conjunto de saltos $\mathcal{S}$ definida en el Teorema 5.20, tenemos que los saltos definidos por los conjugados por σ de elementos de G coinciden con los definidos por elementos de G, y entonces los subgrupos convexos que forman un salto son invariantes. Además, $\mathcal{S}$ es finito por serlo $[G]$. Así, empelando la Proposición 5.16, concluimos que todo subgrupo convexo es invariante frente a conjugación, y por tanto normal. □

Como acabamos de ver, la Proposición 5.16 hace que el caso en que $[G]$ es finito tenga gran interés. Lo ilustramos con un último resultado. Para ello, recordamos primero la noción de grupo resoluble, de importancia conocida en la Teoría de Galois [6].

Definición 5.27. Dado un grupo G y $n \in \mathbb{N}$, se dice que una sucesión finita de subgrupos $\{e\} = A_0 \subseteq A_1 \subseteq ... \subseteq A_n = G$ es una **torre normal** si cada subgrupo A_{i-1} es normal en A_i para todo $i \in \{1, ..., n\}$. Se dice que es una **serie normal** si todos los subgrupos son además normales en G.

Definición 5.28. Se dice que un un **grupo** G es **resoluble** si posee una torre normal con factores abelianos, es decir, si existe $n \in \mathbb{N}$ y una sucesión finita de subgrupos de G

$$\{e\} = A_0 \triangleleft A_1 \triangleleft ... \triangleleft A_n = G,$$

con A_i/A_{i-1} abeliano para todo $i \in \{1, ..., n\}$.

Observamos que, si la cadena de subgrupos convexos es finita, entonces se trata de una torre normal. Sin embargo, no necesariamente es una serie normal. Extendemos este razonamiento a continuación, probando que un grupo totalmente ordenado en esas condiciones es resoluble.

Corolario 5.29. *Un grupo totalmente ordenado con un número finito de clases arquimedianas es resoluble.*

Demostración. Basta observar que la familia de saltos es finita, por serlo el número de clases arquimedianas, como consecuencia de la Proposición 5.16. Así, también es finita la cadena de subgrupos convexos. Dado que ésta es subinvariante, y por tanto completa, el Lema 5.18 asegura que cada subgrupo es normal en el siguiente. El Teorema 5.22 garantiza que los factores son abelianos, y con ello, que el grupo es resoluble. □

[2]Según el sentido de Kurosch [21], p. 20-22, 28.

6. El Teorema de Inmersión de Hahn

Iniciamos el capítulo en el que probamos el resultado central de este trabajo, el Teorema de Inmersión de Hahn, enunciado por H. Hahn en su trabajo de 1907 *Über die nichtarchimedischen Größensysteme* ("Sobre los sistemas de magnitudes no arquimedianos") [11]. En el Capítulo 3, hemos visto que todo grupo arquimediano es abeliano, y que su estructura como grupo ordenado coincide con la de un subgrupo aditivo de los números reales, de acuerdo con el Teorema de Hölder. Buscamos ahora caracterizar los grupos totalmente ordenados en general, es decir, sin asumir la propiedad arquimediana. Observaremos que el caso de grupos arquimedianos se puede entender como una particularización del caso general, descrito por el Teorema de Inmersión, según el cual todo grupo totalmente ordenado se puede incluir en el grupo producto formado por tantas copias de $\mathbb{R}$ como clases arquimedianas distintas de la del neutro tenga.

6.1. Grupo de Hahn y Teorema de Inmersión

Como hemos apuntado en la introducción, probaremos el resultado siguiendo el texto de S. Prieß-Crampe [30], basado en la idea de B. Banaschewski [1]. EL primer paso es presentar la noción de grupo de Hahn.

Definición 6.1. Sean Γ un conjunto totalmente ordenado y $\mathcal{F}_\Gamma = \{G_\gamma\}_{\gamma\in\Gamma}$ una familia de grupos abelianos. Se define el **grupo de Hahn** $H(\Gamma, \mathcal{F}_\Gamma)$ como el producto lexicográfico de grupos de la familia $\mathcal{F}_\Gamma$.

En el caso de que para todo $\gamma \in \Gamma$, G_γ sea mismo grupo G, denotamos el grupo de Hahn por $H(\Gamma, G)$. En particular, si los grupos G_γ son subgrupos de un mismo grupo G, tenemos que el grupo de Hahn $H(\Gamma, \mathcal{F}_\Gamma)$ es un subgrupo de $H(\Gamma, G)$. Como anticipamos al motivar el producto lexicográfico de grupos en el Capítulo 4, la estructura ordenada del conjunto Γ determina las propiedades algebraicas del grupo de Hahn $H(\Gamma, \mathcal{F}_\Gamma)$. Para demostrarlo, nos basamos en la detallada prueba de F. Hausdorff [12]. Este resultado no es necesario para demostrar el Teorema de Hahn, pero nos proporciona una mejor comprensión del contexto.

Proposición 6.2. *Sean Γ un conjunto totalmente ordenado, $\Bbbk$ un cuerpo y $H(\Gamma, \Bbbk)$ el grupo de Hahn asociado. En estas condiciones:*

(1) Si $(\Gamma, *)$ es un semigrupo abeliano totalmente ordenado, entonces $H(\Gamma, \Bbbk)$ es un anillo conmutativo y unitario, con la multiplicación definida por el producto de Cauchy

$$(g \cdot_H h)(\gamma) = \sum_{\alpha * \beta = \gamma} g(\alpha) \cdot h(\beta),$$

para todos $g, h \in H(\Gamma, \Bbbk)$ y $\gamma \in \Gamma$.

(2) Si $(\Gamma, *)$ es un grupo abeliano totalmente ordenado, entonces $H(\Gamma, \Bbbk)$ es un cuerpo.

Demostración. (1) Supongamos primero que $(\Gamma, *, \leq)$ es un semigrupo abeliano totalmente ordenado. De acuerdo con la definición de producto lexicográfico de grupos, $H(\Gamma, \Bbbk)$ es un grupo para la operación (suma) coordenada a coordenada, que además es abeliano por serlo $\Bbbk$. Tenemos que probar que se trata, además, de un monoide conmutativo para el producto de Cauchy definido, y que el producto es distributivo respecto de la suma.

Para empezar, probemos que el producto está bien definido. En primer lugar, debemos ver que la suma que define cada componente es finita para todo $\gamma \in \Gamma$. Como $g, h \in H(\Gamma, \Bbbk)$, los duales en el sentido del orden de sus soportes $s(g)$ y $s(h)$ son conjuntos bien ordenados. Consideramos el conjunto $\Delta := \{\alpha * \beta : \alpha \in s(g), \beta \in s(h)\} \subseteq \Gamma$. Por un lado, tenemos que si $\gamma \notin \Delta$, entonces $(g \cdot_H h)(\gamma) = 0$. Alternativamente, dado $\gamma \in \Delta$, observamos que si $\alpha_1 * \beta_1 = \alpha_2 * \beta_2$ con $\alpha_1 > \alpha_2$, entonces $\beta_1 < \beta_2$, por la compatibilidad en la estructura de semigrupo totalmente ordenado. Así,

como el conjunto $\{\alpha \in s(g) : \alpha * \beta \text{ para algún } \beta \in s(h)\} \subseteq s(g)$ está dualmente bien ordenado, entonces el correspondiente $\{\beta \in s(h) : \alpha * \beta \text{ para algún } \alpha \in s(g)\} \subseteq s(h)$ está bien ordenado, y viceversa, puesto que están en biyección. En consecuencia, por el Corolario I.10 del Anexo, son conjuntos finitos, y por lo tanto también lo es el conjunto de pares $(\alpha, \beta) \in s(g) \times s(h)$ tales que $\alpha * \beta = \gamma$. Con ello, tenemos que el producto de Cauchy definido es un elemento del producto directo $\Bbbk^\Gamma$. Nos queda por ver que $s(g \cdot_H h)$ está dualmente bien ordenado. Por reducción al absurdo, supongamos que existe una sucesión creciente en $s(g \cdot_H h)$

$$\alpha_0 * \beta_0 < \alpha_1 * \beta_1 < \alpha_2 * \beta_2 < ...$$

Entonces, como el dual de $s(g)$ está bien ordenado, podemos definir recursivamente

$$\alpha_{i_0} = \text{máx}\{\alpha_i : i \in \mathbb{N}\}; \quad \alpha_{i_k} = \text{máx}\{\alpha_i : i \in \mathbb{N}_{\geq i_{k-1}}\} \text{ para } k \geq 1,$$

y obtener con ello la sucesión

$$\alpha_{i_0} * \beta_{i_0} < \alpha_{i_1} * \beta_{i_1} < \alpha_{i_2} * \beta_{i_2} < ...$$

Como $\alpha_{i_k} > \alpha_{i_{k+1}}$ para todo $k \in \mathbb{N}$, debe existir en $s(h)$ la sucesión creciente

$$\beta_{i_0} < \beta_{i_1} < \beta_{i_2} < ...$$

lo que contradice el hecho de que $s(h)$ está dualmente bien ordenado.

En conclusión, el producto de cualesquiera dos elementos $g, h \in H(\Gamma, \Bbbk)$ está en el producto lexicográfico, así que la operación $\cdot_H$ está bien definida en $H(\Gamma, \Bbbk)$. En estas condiciones, la operación entre dos elementos de $H(\Gamma, \Bbbk)$ tiene las mismas propiedades que el producto usual entre polinomios o series de potencias. Así, denotaremos cuando sea conveniente cada elemento $g \in H(\Gamma, \Bbbk)$ por

$$g = \sum_{\gamma \in \Gamma} g_\gamma t^\gamma,$$

donde $g_\gamma = g(\gamma)$ y los monomios t^γ son simplemente indicadores de posición para $\gamma \in \Gamma$. Adicionalmente, si sólo se indican los términos correspondientes a un subconjunto $\Delta \subseteq \Gamma$, se supone que el resto de los coeficientes son nulos. Por simplicidad de notación, denotaremos la operación $\cdot_H$ como el producto usual en $\Bbbk$ cuando no haya lugar a confusión.

Continuamos con la prueba de que $H(\Gamma, \Bbbk)$ tiene estructura de anillo. Como $(\Gamma, *)$ es un semigrupo y $(\Bbbk, \cdot)$ es un grupo, ambos verifican la propiedad asociativa, y de ello podemos deducir que también la posee el producto en $H(\Gamma, \Bbbk)$. En efecto, dados $f, g, h \in H(\Gamma, \Bbbk)$ y $\gamma \in \Gamma$, se tiene que

$$\begin{aligned}
[(f \cdot g) \cdot h](\gamma) &= \sum_{\alpha * \beta = \gamma} (f \cdot g)(\alpha) \cdot h(\beta) = \sum_{\alpha * \beta = \gamma} \left(\sum_{\mu * \nu = \alpha} f(\mu) \cdot g(\nu) \right) \cdot h(\beta) \\
&= \sum_{\mu * \nu * \beta = \gamma} f(\mu) \cdot g(\nu) \cdot h(\beta) = \sum_{\mu * \eta = \gamma} f(\mu) \cdot \left(\sum_{\nu * \beta = \eta} g(\nu) \cdot h(\beta) \right) \\
&= \sum_{\mu * \eta = \gamma} f(\mu) \cdot (g \cdot h)(\eta) = [f \cdot (g \cdot h)](\gamma).
\end{aligned}$$

Se comprueba de forma directa que $1_H = 1 \cdot t^{e_\Gamma}$ es el elemento neutro para el producto, donde 1 es el neutro del producto en $\Bbbk$ y e_Γ es el elemento neutro en Γ. Finalmente, observamos que la operación $\cdot_H$ es distributiva respecto de la suma como consecuencia de la propiedad distributiva en el anillo $(\Bbbk, +, \cdot)$. Hemos probado que $H(\Gamma, \Bbbk)$ es un anillo con unidad, y la conmutatividad es directa a partir de las de Γ y $\Bbbk$. Concluimos con ello la demostración de (1).

(2) Ahora, supongamos que $(\Gamma, *, \leq)$ es un grupo abeliano totalmente ordenado, y tenemos que probar adicionalmente la existencia de elemento inverso respecto del producto para todo $g \in H(\Gamma, \Bbbk)$ no nulo. Sea $\alpha = \text{máx}(s(g)) \in \Gamma$. Consideramos los conjuntos $M = \{h \in H(\Gamma, \Bbbk) : 1 - hg \neq 0\}$ y $S(M) = \{\text{máx}(s(1 - hg)) : h \in M\}$, y distinguimos los siguientes casos:

- Si existe $\beta = \text{mín}(S(M))$, sea $h \in M$ con $\beta = \text{máx}(s(1-hg))$, es decir, de forma que

$$c := 1 - hg = c_\beta t^\beta + \sum_{\gamma<\beta} c_\gamma t^\gamma.$$

Por otro lado, por ser Γ un grupo, el elemento α tiene un inverso $\tilde{\alpha}$, y entonces tenemos

$$\left(\frac{c_\beta}{g_\alpha} t^{\beta * \tilde{\alpha}}\right) \cdot g = c_\beta t^\beta + \sum_{\gamma<\beta} d_\gamma t^\gamma.$$

Con ello, definiendo

$$f := h - \frac{c_\beta}{g_\alpha} t^{\beta*\tilde{\alpha}} \in H(\Gamma, \Bbbk),$$

tenemos que $\text{máx}(s(1-fg)) < \beta$. Como $\beta = \text{mín}(S(M))$, deducimos que $f \notin M$ y por lo tanto $1 - fg = 0$, así que f es el inverso de g respecto de producto.

- Si el conjunto $S(M)$ no tiene mínimo, tomamos $\tau \in S(M)$ y consideramos dos elementos $h, h' \in M$ tales que $\text{máx}(s(1-hg)) < \tau$ y $\text{máx}(s(1-h'g)) < \tau$, cuya existencia está garantizada porque $S(M)$ no tiene mínimo. Denotando $\delta := \tilde{\alpha} * \tau$, donde $\tilde{\alpha}$ es el inverso de α, vamos a ver que $h(\delta) = h'(\delta) =: f_\delta$ para cualesquiera dos elementos así. Supuesto $h \neq h'$, deducimos por cómo hemos elegido h y h' que

$$\text{máx}(s(h'-h)) * \text{máx}(s(g)) = \text{máx}(s((h-h')g)) < \tau,$$

donde la desigualdad se deduce de que $(h-h')g = (1-h'g) - (1-hg)$. En consecuencia, $\text{máx}(s(h'-h)) < \tilde{\alpha} * \tau = \delta$, y así $h(\delta) = h'(\delta)$, como queríamos probar. Construimos así

$$f := \sum_{\delta \in \tilde{\alpha} * S(M)} f_\delta t^\delta.$$

Veamos que su soporte es un subconjunto dualmente bien ordenado de Γ. De nuevo, supongamos por reducción al absurdo que existe una sucesión creciente en $s(f)$ sin elemento máximo,

$$\delta_0 < \delta_1 < \delta_2 < ...$$

En particular, $\delta_0 = \tilde{\alpha} * \tau_0$ para cierto $\tau_0 \in S(M)$, y podemos encontrar $h \in M$ de forma que $\text{máx}(s(1-hg)) < \tau_0 < \tau_i$ para todo $i \in \mathbb{N}$, con $\tau_i = \alpha * \delta_i$. Por lo razonado anteriormente, entonces $h(\delta_i) = f_{\delta_i} \neq 0$ para todo $i \in \mathbb{N}$, luego la sucesión es un subconjunto de $s(h)$ sin elemento máximo, en contradicción con que $h \in H(\Gamma, \Bbbk)$. En consecuencia, $f \in H(\Gamma, \Bbbk)$.

Para terminar, veamos que f es el inverso de g. Suponiendo lo contrario, resulta $f \in M$, y por tanto existe $\beta_m = \text{máx}(s(1-fg)) \in S(M)$. Así, podemos encontrar un elemento $h \in M$ de modo que $\text{máx}(s(1-hg)) < \beta_m$, y de esa forma tendremos, repitiendo un razonamiento anterior, que $\text{máx}(s(h-f)) = \tilde{\alpha} * \beta_m =: \delta_m$, y por lo tanto $f(\delta_m) \neq h(\delta_m)$. Sin embargo, según lo que habíamos visto, en estas condiciones se tiene que $h(\delta_m) = f_{\delta_m} = f(\delta_m)$, así que la suposición $f \in M$ conduce a contradicción y concluimos que $fg = 1$.

□

El resultado anterior no es cierto si relajamos la hipótesis y suponemos que alguno de los subgrupos de la familia $\mathcal{F}_\Gamma$ no son todos iguales, aunque sean subcuerpos de un mismo cuerpo $\Bbbk$. Por ejemplo, se puede comprobar que el producto no está bien definido tomando $\Gamma = \mathbb{N}$ y

$$G_\gamma = \begin{cases} \mathbb{Q} & \text{, si } \gamma = 1; \\ \mathbb{R} & \text{, en otro caso.} \end{cases}$$

Ejemplos.

1. Si Γ es un conjunto finito de cardinal $n \in \mathbb{N}_{\geq 1}$, el grupo de Hahn $H(\Gamma, \mathbb{R})$ coincide con $(\mathbb{R}^n, +)$. En este caso el producto lexicográfico coincide con el producto directo, por ser Γ finito y por tanto bien ordenado. Más en general, dada una familia $\mathcal{F}_\Gamma$, se tiene que $H(\Gamma, \mathcal{F}_\Gamma)$ es un subgrupo de $(\mathbb{R}^n, +)$.

2. Como anticipamos en el Capítulo 4, en los ejemplos habituales el orden natural en el conjunto Γ es el que va a proporcionarnos el buen orden del soporte de los elementos del grupo de Hahn. Así, para respetar la construcción realizada en la que requerimos que el soporte esté bien ordenado respecto del orden dual, debemos trabajar con el dual del orden natural en Γ. Omitiremos este matiz cuando no haya lugar a la confusión. En ese sentido, los siguientes tres casos son de especial relevancia:

   - El anillo de *series formales de potencias* con coeficientes reales es el grupo de Hahn asociado al semigrupo $\Gamma = (\mathbb{N}, +, \leq_D)$. Como $\mathbb{N}$ es un conjunto bien ordenado, toda serie $\sum_{i \in \mathbb{N}} a_i t^i$ es un elemento del anillo. Habitualmente se denota por $\mathbb{R}[[x]]$.
   - El cuerpo de *series de Laurent* con coeficientes reales es el grupo de Hahn asociado al grupo $\Gamma = (\mathbb{Z}, +, \leq_D)$. Sus elementos son series de la forma $\sum_{i \in \mathbb{Z}_{\geq k_0}} a_i t^i$ para cierto $k_0 \in \mathbb{Z}$, ya que un subconjunto de $\mathbb{Z}$ está bien ordenado si y sólo si tiene mínimo. El cuerpo de series de Laurent coincide con el cuerpo de fracciones del anillo $\mathbb{R}[[x]]$, ya que toda serie formal de potencias tiene su inverso en $H(\mathbb{Z}, \mathbb{R})$ y toda serie de Laurent se puede construir como suma finita de series formales de potencias y sus inversos. En consecuencia, se denota también como $\mathbb{R}((x))$.
   - El cuerpo de *series de Puiseux* con coeficientes reales es el subcuerpo del grupo de Hahn $H(\mathbb{Q}, \mathbb{R})$ que contiene los elementos con soporte de la forma $\left\{ \frac{i}{q} : i \in \mathbb{Z}_{\geq k_0} \right\}$ para cierto $q \in \mathbb{N}$ fijo y $k_0 \in \mathbb{Z}$. En otras palabras, los soportes de las series de Puiseux son subconjuntos bien ordenados de $\mathbb{Q}$ cuyos elementos tienen denominadores acotados. Así, podemos escribir cualquier serie de Puiseux como $\sum_{i \in \mathbb{Z}_{\geq k_0}} a_i t^{\frac{i}{q}}$. Se puede comprobar que la suma y producto de dos series de Puiseux también lo es, y en el caso del inverso, basta observar que multiplicando por t^q obtenemos una serie de Laurent, cuyo inverso es de nuevo una serie de Laurent, así que los denominadores del inverso en $H(\mathbb{Q}, \mathbb{R})$ están de nuevo acotados por q. Con ello, las series de Puiseux forman un subcuerpo de $H(\mathbb{Q}, \mathbb{R})$. Al final del capítulo, veremos que $H(\mathbb{Q}, \mathbb{R})$ es el grupo de Hahn más pequeño que contiene a las series de Puiseux, salvo isomorfía. En otras palabras, el cuerpo de series de Puiseux no es isomorfo como grupo a ningún grupo de Hahn, lo que pone de manifiesto que la inmersión del Teorema de Hahn no tiene por qué ser un isomorfismo.

El interés de estas series está ligado a la resolución de ecuaciones diferenciales polinómicas, como detallamos en la Sección 6.2. En concreto, dada una ecuación algebraica o diferencial de forma polinómica y con coeficientes en un cuerpo algebraicamente cerrado, las soluciones obtenidas mediante el método de Newton-Puiseux son precisamente series de exponentes racionales con denominadores acotados, de acuerdo con el Teorema de Puiseux [31].

Extendiendo la notación anterior en términos de series de potencias, la expresión $\Bbbk[[x^\Gamma]]$ es habitual en muchos textos para referirse al grupo de Hahn $H(\Gamma, \Bbbk)$, si bien en esta parte nos ceñiremos a la empleada en la definición. Sí que la emplearemos cuando hablemos de cuerpos valorados. De igual forma, cuando Γ es un grupo abeliano totalmente ordenado se suele hablar de **cuerpos de Hahn**.

Volvemos ahora al caso en el que Γ es simplemente un conjunto totalmente ordenado. El siguiente lema auxiliar recoge un resultado básico sobre espacios vectoriales. En él probamos que en cualquier espacio vectorial existe una aplicación que lleva cada subespacio en su suplementario, invirtiendo las contenciones. Se trata de un resultado muy útil de cara a la demostración del Teorema de Inmersión, puesto que nos permitirá evitar en ella el tecnicismo asociado a trabajar con ordinales, a diferencia de lo que sucede en la prueba original de Hahn.

Lema 6.3. *Sean V un espacio vectorial sobre un cuerpo $\Bbbk$, y $S(V)$ el conjunto de subespacios vectoriales de V. Entonces existe una aplicación $\sigma : S(V) \to S(V)$ con las siguientes propiedades, para todos $U, W \in S(V)$:*

(1) Si $U \subseteq W$, entonces $\sigma(W) \subseteq \sigma(U)$.

(2) $V = W \oplus \sigma(W)$.

Demostración. Sean $\{e_i\}_{i\in I}$ una base de V con I un ordinal, cuya existencia justificamos en la Observación I.9 del Anexo, y $W \in S(V)$. Definimos

$$T_W := \{e_j : e_j \notin \Bbbk\langle W \cup \{e_i : i < j\}\rangle\},$$

donde $\Bbbk\langle M\rangle$ denota el subespacio vectorial generado por un subconjunto $M \subseteq V$. Construimos así la aplicación $\sigma : S(V) \to S(V)$ tal que $\sigma(W) = \Bbbk\langle T_W\rangle$. Veamos primero que $W \cap \Bbbk\langle T_W\rangle = \{0\}$. Si no, existiría $0 \neq w \in W$ tal que

$$w = \sum_{i=1}^{n} \alpha_i e_{k_i},$$

de modo que $e_{k_i} \in T_W$ y $0 \neq \alpha_i \in \Bbbk$ para $1 \leq i \leq n$. Tomando $\ell = \text{máx}\{k_i : 1 \leq i \leq n\}$, tendríamos entonces $e_\ell \in \Bbbk\langle W \cup \{e_k : k < \ell\}\rangle$, en contradicción con la definición de T_W. Veamos que $W + \Bbbk\langle T_W\rangle = V$ empleando el Principio de Inducción Transfinita, probado en el Anexo. Sea e_{j_0} el primer elemento de la base que no está en W. Tenemos así que $\Bbbk\langle W \cup \{e_i : i < j_0\}\rangle = W$, y en consecuencia $e_{j_0} \in T_W \subseteq \Bbbk\langle T_W\rangle \subseteq W + \Bbbk\langle T_W\rangle$. Ahora, dado $j \in I$, supongamos que para todo $i < j$ se tiene que $e_i \in W + T_W$. Entonces, o bien $e_j \in \Bbbk\langle W \cup \{e_i : i < j\}\rangle$, contenido en $W + \Bbbk\langle T_W\rangle$ por hipótesis de inducción, o bien $e_j \in T_W \subseteq \Bbbk\langle T_W\rangle$. En ambos casos tenemos $e_j \in W + \Bbbk\langle T_W\rangle$. Deducimos que la suma es directa, lo que prueba (2).

Para probar la propiedad (1), sean $U \subseteq W$ y $e_j \in \sigma(W) = \Bbbk\langle T_W\rangle$, es decir, se tiene que $e_j \notin \Bbbk\langle W \cup \{e_i : i < j\}\rangle$. Entonces, $e_j \notin \Bbbk\langle U \cup \{e_i : i < j\}\rangle$, y por tanto $e_j \in \Bbbk\langle T_U\rangle = \sigma(U)$. □

Pasamos ahora a demostrar el Teorema de Inmersión, cuya prueba dividimos en dos etapas. En primer lugar, obtendremos el resultado para grupos divisibles, y después lo extenderemos a la versión general usando la noción de envolvente divisible definida en el Capítulo 2. Recordemos que en el Capítulo 5, concretamente en el Teorema 5.20, hemos probado que dados un grupo totalmente ordenado G y un elemento $x \in G$, los subgrupos convexos $G_{[x]} = \{g \in G : [g] < [x]\}$ y $G^{[x]} = \{g \in G : [g] \leq [x]\}$ forman un salto $G_{[x]} \sqsubset G^{[x]}$ en la cadena de subgrupos convexos de G, siendo $[x]$ denota la clase arquimediana de x en G. Si denotamos por $\Gamma = [G] \setminus \{[0]\}$ el conjunto de clases arquimedianas no neutras de G, podemos denotar estos subgrupos por G_γ y G^γ, respectivamente, donde $\gamma = [x]$, dado que $G_{[x]}$ es independiente del representante escogido.

Teorema 6.4. *Sean $(G, +)$ un grupo abeliano divisible totalmente ordenado, y $\Gamma = [G] \setminus \{[0]\}$ el conjunto de sus clases arquimedianas no nulas. Entonces, existe un o-monomorfismo*

$$\varphi : G \longrightarrow \left(\prod_{\gamma\in\Gamma} G^\gamma/G_\gamma\right)_{lex}$$

de modo que $g \in G^\beta \setminus G_\beta$, es decir, $[g] = \beta$, si y sólo si $\beta = \text{máx}(s(\varphi(g)))$. En ese caso, se tiene que $\varphi(g)(\beta) = g + G_\beta$.

Demostración. Como G es un grupo abeliano divisible, y es libre de torsión por ser totalmente ordenado, se trata de un $\mathbb{Q}$-espacio vectorial, por el Corolario 2.26. Además, cualquier subgrupo convexo de G es divisible, por la Proposición 2.24, y con ello un subespacio vectorial de G.

Sean $S(G)$ el conjunto de subespacios vectoriales de G y $\sigma : S(G) \to S(G)$ una aplicación que verifica las propiedades del Lema 6.3. Entonces, para cada $\gamma \in \Gamma$, tenemos la suma directa $G = G^\gamma \oplus \sigma(G^\gamma)$, de forma que cada $g \in G$ se descompone según $g = g_\gamma + \hat{g}_\gamma$, con $g_\gamma \in G^\gamma$ y $\hat{g}_\gamma \in \sigma(G^\gamma)$. Definimos la aplicación

$$\begin{array}{rccc} \varphi : & G & \longrightarrow & \prod\limits_{\gamma\in\Gamma} G^\gamma/G_\gamma \\ & g & \longmapsto & \varphi(g) \end{array} \quad \text{, con } \varphi(g)(\gamma) = g_\gamma + G_\gamma \text{ para todo } \gamma \in \Gamma.$$

En primer lugar, veamos que la imagen de φ está en el producto lexicográfico $\left(\prod_{\gamma\in\Gamma} G^\gamma/G_\gamma\right)_{lex}$, esto es, que todo subconjunto no vacío del soporte $s(\varphi(g))$ tiene máximo para cualquier $g \in G$. Consideremos un elemento $g \in G$ y un subconjunto no vacío $T \subseteq s(\varphi(g)) = \{\gamma \in \Gamma : g_\gamma \notin G_\gamma\}$. Definimos el subgrupo

$$G^T := \bigcup_{\gamma\in T} G^\gamma,$$

que es convexo por ser la familia de subgrupos convexos de G una cadena, por el Lema 5.19, y, por lo tanto, es un subespacio vectorial de G.

Usando el Lema 6.3 sobre G^T, tenemos la descomposición $g = x+y$ con $x \in G^T$ e $y \in \sigma(G^T)$. Entonces, existe $\beta \in T$ tal que $x \in G^\beta$. Veamos que $\beta = \max(T)$. Dado que $G^\gamma \subseteq G^T$, se tiene que $\sigma(G^T) \subseteq \sigma(G^\gamma)$, y así, para todo $\gamma \in T$ resulta que $y_\gamma = 0$. En consecuencia, para todo $\gamma \in T$ se tiene que $g_\gamma = (x + y)_\gamma = x_\gamma$, y en particular $g_\beta = x_\beta$. Como $x \in G^\beta$, tenemos que $g_\beta = x$, y como $\beta \in s(\varphi(g))$, $x \notin G_\beta$. Por tanto, $x \in G^\beta \setminus G_\beta$, es decir, $[x] = \beta$ y $x = x_\beta$. Con ello, para todo $\gamma > \beta$ se tiene que $x \in G^\gamma$, luego $x = x_\gamma$, es decir,

$$\varphi(g)(\gamma) = g_\gamma + G_\gamma = x + G_\gamma = g_\beta + G_\gamma = 0 + G_\gamma,$$

dado que $G^\beta \subseteq G_\gamma$. En consecuencia, $\gamma \notin T$, y así $\beta = \max(T)$.

La definición de φ asegura que se trata de un homomorfismo de grupos, por serlo en cada componente. De hecho, es un monomorfismo: si $g \in G$ tiene imagen neutra por φ, entonces $g_\gamma \in G_\gamma$ para todo $\gamma \in \Gamma$, y por tanto $[g] < [x]$ para todo $x \in G$ no nulo, con lo cual $g = 0$.

Probemos ahora la propiedad enunciada. Si $g \in G^\beta \setminus G_\beta$, entonces $\varphi(g)(\beta) \neq 0 + G_\beta$. Razonando como antes, para todo $\gamma > \beta$ tenemos que $\varphi(g)(\gamma) = 0+G_\gamma$, luego $\beta = \max(s(\varphi(g)))$. Recíprocamente, si $\beta = \max(s(\varphi(g)))$, se tiene que $g_\gamma \in G_\gamma$ para todo $\gamma > \beta$, y $g_\beta \notin G_\beta$. Por tanto, resulta $[g] = \beta$. En este caso, para todo $\gamma \geq \beta$ se cumple que $g \in G^\gamma$, luego $g = g_\beta$, y concluimos que $\varphi(g)(\beta) = g + G_\beta$.

Finalmente, comprobemos que φ preserva el orden. Si $g \in P(G)$ y $g \in G^\beta \setminus G_\beta$, entonces $0 + G_\beta < g + G_\beta = \varphi(g)(\beta)$, siendo $\beta = \max(s(\varphi(g)))$, así que $\varphi(g)$ es un elemento positivo en el producto lexicográfico, como consecuencia de la Proposición 4.5. □

Con el Teorema de Inmersión extendemos este resultado a grupos no necesariamente divisibles, empleando para ello la noción de envolvente divisible desarrollada en la Sección 2.3.

Teorema 6.5 (**Teorema de Inmersión de Hahn** [11])**.** *Todo grupo abeliano totalmente ordenado G admite una inmersión en el grupo de Hahn $H(\Gamma, \mathbb{R})$ que preserva el orden, donde $\Gamma = [G] \setminus \{[0]\}$ es el conjunto de clases arquimedianas no nulas de G.*

Demostración. Sea G un grupo abeliano totalmente ordenado y por tanto libre de torsión, de acuerdo con la Proposición 2.22. Consideramos la envolvente divisible $\bar{G}$, construida en el Teorema 2.25, que es también un grupo abeliano totalmente ordenado, mediante una extensión del orden de G. Las clases arquimedianas de $\bar{G}$ están en biyección con las de G, puesto que

cualquier elemento del tipo $\frac{a}{n}$ con $a \in G$ y $n \in \mathbb{N}_{\geq 1}$ es arquimedianamente equivalente a a. Además, la biyección preserva el orden en $\Gamma = [G] \setminus \{[0]\}$.

Por otro lado, observamos que el monomorfismo φ del Teorema 6.4 preserva la valoración de un elemento g de acuerdo con las valoraciones naturales en G y $\left(\prod_{\gamma\in\Gamma} \bar{G}^\gamma/\bar{G}_\gamma\right)_{lex}$. En efecto, dado $g \in G$ con clase arquimediana $\gamma = [g]$, se tiene que

$$[g] = \gamma = \text{máx}(s(\varphi(g))) = [\varphi(g)],$$

donde la última igualdad se debe a que, por ser los grupos $\bar{G}^\gamma/\bar{G}_\gamma$ arquimedianos, el conjunto de clases arquimedianas no neutras del producto es el mismo Γ. Usando de nuevo este argumento, podemos aplicar el Teorema 5.22 y ver que cada grupo $\bar{G}^\gamma/\bar{G}_\gamma$ es o-isomorfo a un subgrupo de $(\mathbb{R}, +)$, y en consecuencia existe una o-inmersión $\tau : \left(\prod_{\gamma\in\Gamma} \bar{G}^\gamma/\bar{G}_\gamma\right)_{lex} \hookrightarrow H(\Gamma, \mathbb{R})$.

Con todo, tenemos la siguiente cadena de o-monomorfismos,

$$G \overset{\iota}{\hookrightarrow} \bar{G} \overset{\varphi}{\hookrightarrow} \left(\prod_{\gamma\in\Gamma} \bar{G}^\gamma/\bar{G}_\gamma\right)_{lex} \overset{\tau}{\hookrightarrow} H(\Gamma, \mathbb{R}),$$

que definen una o-inmersión de G en el grupo de Hahn $H(\Gamma, \mathbb{R})$. □

Notemos que, con el Teorema de Inmersión, hemos logrado incluir grupos abelianos totalmente ordenados no necesariamente divisibles en el grupo de Hahn $H(\Gamma, \mathbb{R})$. De hecho, quedándonos con los dos primeros monomorfismos, tenemos una o-inmersión del grupo G en el produco lexicográfico de los grupos $\bar{G}^\gamma/\bar{G}_\gamma$. Sin embargo, es importante reiterar que los subgrupos $\bar{G}_\gamma$ y $\bar{G}^\gamma$ no son, en general, subgrupos de G, sino de su envolvente divisible. En otras palabras, el Teorema 6.4 no es cierto para grupos no divisibles, y A. H. Clifford muestra un ejemplo considerando el siguiente subgrupo de $\mathbb{Q}^2$ [4]:

$$G = \langle\{(p_n^{-1}, np_n^{-1}) : p_n \text{ es el } n\text{-ésimo primo}\}\rangle,$$

con el orden lexicográfico, es decir, $(x, y) < (0, 0)$ si $x < 0 \vee (x = 0 \wedge y < 0)$. Observamos que, para cada par $(n, m) \in \mathbb{Z}^2$, tenemos que

$$p_n(p_n^{-1}, np_n^{-1}) - p_m(p_m^{-1}, mp_m^{-1}) = (0, n - m),$$

luego $\{0\} \times \mathbb{Z} \subseteq G$. Por otro lado, veamos que estos son los únicos elementos con primera coordenada nula. Si suponemos que $x = \sum_{i\in S} k_i(p_i^{-1}, ip_i^{-1}) \in \{0\} \times \mathbb{Q}$, con $S \subseteq \mathbb{N}_{\geq 1}$ finito y $k_i \in \mathbb{Z}$ para $i \in S$, entonces tenemos que

$$\sum_{i\in S} k_i p_i^{-1} = \prod_{i\in S} p_i^{-1} \left(\sum_{i\in S} k_i \prod_{j\neq i} p_j\right) = 0.$$

Por un argumento de divisibilidad, como los p_i son primos, tenemos que $p_i \mid k_i$ para todo $i \in S$, y con ello $x \in \{0\} \times \mathbb{Z}$. Por lo tanto, se tiene que $\{0\} \times \mathbb{Z} = \{(0, r) \in G : r \in \mathbb{Q}\}$, y en particular es un subgrupo convexo. Esto prueba también que G no es divisible, puesto que $(0, 1) \in G$ pero $(0, 1/2)$ no. Cualquier otro subgrupo convexo distinto del anterior debe contener a todos los elementos (p_n^{-1}, np_n^{-1}) y por tanto es igual a G, luego la cadena de subgrupos convexos de G es

$$\{0\} \subseteq \{0\} \times \mathbb{Z} \cong \mathbb{Z} \subseteq G.$$

Sin embargo, si fuera $G = \mathbb{Z} \times H$ para cierto subgrupo $H \subseteq G$, tendríamos que $(p_n^{-1}, np_n^{-1}) \in H$, pero hemos visto que combinaciones de elementos de esta forma generan todo G. Concluimos que la construcción del o-homomorfismo del Teorema 6.4 no es posible en este caso.

Por último, veamos que $H(\mathbb{Q},\mathbb{R})$ es el grupo de Hahn más pequeño que contiene al cuerpo de las series de Puiseux, como mencionamos en la página 40. Para cada $r \in \mathbb{Q}$, el monomio t^r es una serie de Puiseux. Con el orden lexicográfico, dos monomios t^r y t^s pertenecen a la misma clase arquimediana si y sólo si $r = s$, luego el conjunto de clases arquimedianas no nulas del cuerpo de series de Puiseux está contenido en $\mathbb{Q}$. De hecho coincide con $\mathbb{Q}$, ya que todo elemento no nulo es equivalente arquimediano del monomio de menor grado. Como el conjunto de clases arquimedianas del grupo de Hahn $H(\Gamma,\mathbb{R})$ es el propio Γ, tenemos que si $H(\Gamma,\mathbb{R})$ contiene a las series de Puiseux, entonces $\mathbb{Q} \subseteq \Gamma$ y en consecuencia $H(\mathbb{Q},\mathbb{R}) \subseteq H(\Gamma,\mathbb{R})$. Sin embargo, la serie

$$\sum_{n\in\mathbb{N}_{\geq 1}} t^{1-1/n} \in H(\mathbb{Q},\mathbb{R})$$

no es una serie de Puiseux. Con ello concluimos que, si bien podemos incluir todo grupo abeliano totalmente ordenado G en un grupo de Hahn, no es cierto en general que exista un conjunto Γ de forma que G sea isomorfo a $H(\Gamma,\mathbb{R})$. Un ejemplo más sencillo es considerar $(\mathbb{Q},+)$ con el orden usual, que es arquimediano pero no es isomorfo a $\mathbb{R}$.

6.2. Aplicaciones en la resolución de ecuaciones diferenciales

La principal motivación para hallar un resultado como el Teorema de Inmersión de Hahn tuvo su origen en la resolución de ecuaciones diferenciales. Más concretamente, los grupos de Hahn y el Teorema de Inmersión permitieron obtener y describir espacios que contienen las soluciones, en forma de series de potencias con exponentes reales, de ecuaciones diferenciales ordinarias con coeficientes polinómicos. Dedicamos esta última sección a detallar esta relación, describiendo el método de resolución de ecuaciones que dio lugar a la idea de series con exponentes reales y enunciando algunos resultados relacionados con este problema. Se trata de una sección descriptiva, en la que por lo general omitiremos los detalles de los desarrollos o demostraciones.

El punto de partida es la resolución de ecuaciones algebraicas con coeficientes polinómicos. Las soluciones se pueden determinar, como series con exponentes racionales, a través del método de Newton-Puiseux. Este tiene su origen en el algoritmo de Newton, basado en la construcción del polígono homónimo, y que fue estudiado más tarde por V. A. Puiseux. Mostramos a continuación sus fundamentos.

Consideremos una ecuación algebraica

$$F(x,y) = 0,$$

donde $F \in \Bbbk[x,y]$, siendo $\Bbbk$ un cuerpo algebraicamente cerrado. Suponemos que $F(0,0) = 0$. En caso contrario, podemos lograr esta condición mediante un cambio de variables. Adicionalmente, suponemos que $\hat{F}(y) = F(x,y) \in \Bbbk[x][y]$ no es un polinomio constante en la variable y. La idea de Newton era encontrar, de forma recursiva, una serie

$$y = \sum_{q\in\mathbb{Q}} \gamma_q x^q$$

que describiera una rama de la curva alrededor del origen; o, equivalentemente, encontrar localmente una raíz de $\hat{F}(y)$. Para ello definiremos el polígono de Newton. Denotamos

$$F(x,y) = \sum_{i,j} \alpha_{i,j} x^i y^j. \tag{1}$$

Tenemos que $\alpha_{0,0} = 0$, ya que F se anula en el origen. Si $\alpha_{i,0} = 0$ para todo $i \in \mathbb{N}$, tenemos la solución trivial $y \equiv 0$. Suponemos entonces que no todos se anulan a la vez. Consideramos el siguiente subconjunto de $\mathbb{N}^2$:

$$A = \{(i,j) \in \mathbb{N}^2 : \alpha_{i,j} \neq 0\},$$

Su envolvente convexa H, formada por un número finito de segmentos que unen puntos de A, se conoce como *polígono de Newton*. Por hipótesis, existe $c = \min\{i \in \mathbb{N}_{\geq 1} : \alpha_{i,0} \neq 0\}$. Además, H tiene al menos un lado porque $\hat{F}$ no es constante. Sea (i_1, j_1) el punto final del segmento con origen en $(i_0, 0)$, que está contenido en la recta $a + \mu b = c$, con $\mu, c \in \mathbb{Q}$, y que contiene los puntos

$$(c, 0) = (a_1, b_1), (a_2, b_2), ..., (a_r, b_r) = (i_1, j_1) \in A,$$

Entonces, resulta $i + \mu j \geq c$ para todo $(i, j) \in A$. Introducimos ahora la variable $y_{(1)} = y - \beta x^{\mu}$, con β por determinar de forma que $y_{(1)}$ no tenga término en x^{μ}. Tenemos entonces que

$$\begin{aligned} F(x, y_{(1)}) &= \sum_{i,j} \alpha_{i,j} x^i (y_{(1)} + \beta x^{\mu})^j = \sum_{i,j} \alpha_{i,j} \sum_{k=0}^{j} \binom{j}{k} y_{(1)}^{j-k} \beta^k x^{i+\mu k} \\ &= \sum_{i,j} \alpha_{i,j} \beta^j x^{i+\mu j} + y_{(1)} \sum_{i,j} \alpha_{i,j} \sum_{k=0}^{j-1} \binom{j}{k} y_{(1)}^{j-k-1} \beta^k x^{i+\mu k} \\ &= x^c \sum_{\ell=1}^{r} \alpha_{a_\ell, b_\ell} \beta^{b_\ell} + \sum_{i+\mu j > c} \alpha_{i,j} \beta_j x^{i+\mu j} + y_{(1)} \sum_{i,j} \alpha_{i,j} \sum_{k=0}^{j-1} \binom{j}{k} y_{(1)}^{j-k-1} \beta^k x^{i+\mu k}. \end{aligned}$$

De este modo, obtenemos como coeficiente del término x^c un polinomio en β sobre un cuerpo algebraicamente cerrado. Entonces, escogiendo β como una de sus raíces, anulamos el coeficiente y así eliminamos el punto $(c, 0)$ del polígono de Newton del polinomio $F(x, y_{(1)})$. De hecho, cada solución nos dará a posteriori una rama de la curva. La transformación realizada garantiza que el primer punto $(i, 0)$ sobre el eje X del nuevo polígono, si es que hay alguno, satisface $i > c$, puesto que es uno de los términos del segundo sumando. Por su parte, el resto de puntos del segmento seguirá formando parte del polígono, de forma que al repetir el proceso obtendremos un segmento de inclinación mayor, y con ello un segundo exponente $\mu^{(1)} > \mu^{(0)} := \mu$. Ilustraremos este procedimiento con un ejemplo concreto.

En consecuencia, el método da lugar a una serie con una sucesión creciente de exponentes racionales $\{\mu^{(n)}\}_{n \in \mathbb{N}}$, y el Teorema de Puiseux garantiza que los denominadores están acotados [31]. Expresado de otro modo, existen $m \in \mathbb{N}$ y $n_0 \in \mathbb{Z}$ de forma que

$$y = \sum_{n=n_0}^{\infty} \beta_n x^{n/m},$$

y por tanto y es una serie de Puiseux. Mostramos a continuación un ejemplo de la aplicación del método a una ecuación algebraica.

Ejemplo. Consideramos la curva algebraica $F(x, y) = 0$ con $F(x, y) := y^2 - x^2 + x^3$, similar a la conocida como cúbica de Tschirnhaus. El segmento inicial del algoritmo de Newton-Puiseux es el que contiene los puntos $(2, 0)$ y $(0, 2)$, de inclinación $\mu^{(0)} = 1$. Así, tomamos $y_{(1)} = y - \beta_1 x$, y obtenemos la ecuación

$$(\beta_1^2 - 1)x^2 + x^3 + 2\beta_1 x y_{(1)} + y_{(1)}^2 = 0,$$

con lo que tenemos dos soluciones $\beta_1 = 1$ y $\beta_1 = -1$. Eligiendo la primera, se tiene que $F(x, y_{(1)}) = x^3 + 2xy_{(1)} + y_{(1)}^2$, y repitiendo el proceso elegimos el segmento que contiene los puntos $(1, 1)$ y $(3, 0)$, de inclinación $\mu^{(1)} = 2$. Los tres primeros pasos conducen a la siguiente aproximación de la rama que cruza al origen con pendiente positiva

$$y(x) \simeq x - \frac{1}{2}x^2 - \frac{1}{8}x^3$$

Tomando $\beta_1 = -1$ obtendríamos la rama simétrica $-y(x)$.

En 1856, C. Briot y T. Bouquet trataron de extender en primera instancia el método de Newton-Puiseux a la resolución de ecuaciones diferenciales ordinarias, del tipo

$$f(x, \mathbf{y}) = 0,$$

con $f \in \Bbbk[x, \mathbf{y}] = \Bbbk[x, y_0, y_1, ..., y_n]$, e $y_k = \partial^k y_0$, donde se define el operador $\partial g = x\frac{dg}{dx}$ para cualquier función g. La elección de esta derivada en lugar de la usual se debe a que simplifica la notación al derivar monomios, ya que con ella resulta $\partial^k(x^n) = n^k x^n$ en lugar de $\prod_{\ell=0}^{k} n(n-\ell)x^{n-k}$. Podemos escribir entonces

$$f(x, \mathbf{y}) = \sum_{i,J} \alpha_{i,J} x^i \mathbf{y}^J,$$

donde $J = (j_0, ..., j_n) \in \mathbb{N}^{n+1}$, y representar el conjunto

$$A = \{(i, j) : \alpha_{i,J} \neq 0 \text{ para algún } J \text{ con } \sum_{i=0}^{n} j_i = j\} \subseteq \mathbb{Z}^2,$$

cuya envolvente convexa H es el polígono de Newton de la ecuación. Notemos que, ahora, cabe la posibilidad de que varios monomios $x^i\mathbf{y}^J$ correspondan al mismo punto. Así, existen dos posibilidades de proceder con el método: anular la suma de términos correspondientes a un segmento o a un vértice. En el primer caso, obtendríamos en la solución un término cuyo exponente μ es su inclinación, mientras que en el segundo, puede ser válido cualquier exponente real con valor entre las inclinaciones de lados contiguos. Por otro lado, al realizar el cambio de variable y por $y_{(1)}$, debemos considerar sus derivadas, y con ellas, las ecuaciones imponen condiciones también sobre el exponente μ, de forma que la existencia de solución no está asegurada. Vemos a continuación tres casos ilustrativos.

Ejemplos.

1. Consideramos el polinomio $f(x, y_0, y_1, y_2) = y_0y_2 - y_1^2$. El polígono de Newton asociado a la ecuación $f = 0$ tiene sólo un vértice, el punto $(0, 2)$, al que corresponden los dos monomios. Observamos que toda función del tipo $y_0(x) = \beta x^\mu$ con $\beta \in \mathbb{R}$ e inclinación $\mu \in \mathbb{R}_{>0}$ satisface la ecuación, y por lo tanto cualquier elección de los parámetros conduce a una solución válida.

2. Alternativamente, la ecuación $f = 0$ con $f(x, y_0, y_1) = y_1^3 + x^3y_1^2 - 7x^3y_0y_1 + 12x^3y_0^2 - x^{11}$ no tiene ninguna solución en forma de serie con exponentes reales. El polígono de Newton asociado consta de dos lados con el vértice múltiple común $(3, 2)$. Al tratar de anular los términos correspondientes se obtienen condiciones imposibles sobre β y μ, de modo que no podemos construir ninguna solución con el método anterior. Se pueden consultar los detalles en [3].

3. En los casos anteriores, hemos obtenido soluciones series de potencias con exponentes en un grupo arquimediano como $\mathbb{R}$. Sin embargo, la ecuación $x^2y_1 - 2y_0 - x^3 + 2x = 0$ posee, además de la solución $y(x) = x$ que proporciona el método de Newton-Puiseux, la solución $y(x) = x+e^{-1/x^2}$. Dado que la función $y = e^{-1/x^2}$ es plana en $x = 0$ y no es comparable con $y = x$, para describirla como serie de potencias surge la necesidad de considerar cuerpos de series con exponentes en grupos no arquimedianos, dotados de una regla de derivación compatible con la derivada usual. Ésta es una de las motivaciones para el desarrollo de la teoría de cuerpos valorados y cuerpos diferenciales que introducimos en la Sección 6.3.

Dilucidar en cuál de los anteriores casos nos encontramos no es sencillo: D. Grigoriev y M. F. Singer probaron que el problema de decidir si una ecuación diferencial tiene soluciones en forma de series con exponentes reales es indecidible [10]. Por otro lado, antes del desarrollo de

la teoría de estructuras ordenadas y sin un resultado como el Teorema de Inmersión de Hahn, la búsqueda de soluciones de ecuaciones diferenciales en forma de series carecía de un marco teórico que proporcionara espacios donde encontrar dichas soluciones. Veremos que precisamente el trabajo de Grigoriev y Singer fue relevante, además, en la determinación de subgrupos de series con exponentes reales soluciones de ecuaciones diferenciales.

El trabajo de H. Hahn en 1907 generalizó las series formales de potencias con exponentes enteros, que era el único ejemplo grupo de Hahn que había sido usado con anterioridad, y las construcciones de cuerpos ordenados no arquimedianos que habían dado en los años anteriores G. Veronese y T. Levi-Civita [7].

Gracias al Teorema de Puiseux, el espacio de soluciones en forma de series de potencias de ecuaciones algebraicas polinómicas con coeficientes en un cuerpo algebraicamente cerrado queda completamente determinado con un caso particular de grupo de Hahn, las series de Puiseux. En cambio, en el caso de las ecuaciones diferenciales, como hemos razonado previamente, pueden existir soluciones en forma de series de potencias con exponentes reales. En este sentido, el aspecto relevante de la construcción de Hahn es la generalización del cuerpo $H(\mathbb{Q},\mathbb{R})$, que contiene al cuerpo de las series de Puiseux, para un conjunto cualquiera de clases arquimedianas Γ. Así, de manera análoga al caso algebraico, se han encontrado diferentes ejemplos de grupos de Hahn que contienen las soluciones en forma de series de potencias de ecuaciones diferenciales cuyos coeficientes cumplen ciertas propiedades. A modo ilustrativo, mostramos a continuación dos ejemplos concretos, acompañados de los resultados que describen el espacio de soluciones en cada caso.

En primer lugar, observamos que la construcción del polígono de Newton conduce a series de potencias cuyos exponentes son una sucesión creciente de números reales. En el trabajo citado previamente, Grigoriev y Singer buscaron soluciones de ecuaciones diferenciales polinómicas con coeficientes en $H(\mathbb{Z},\mathbb{C})$, es decir, series de Laurent sobre los complejos. En particular, consideraron el conjunto

$$\Omega = \left\{ \sum_{i\in\mathbb{N}} \beta_i x^{\mu_i} \in H(\mathbb{R},\mathbb{C}) : \mu_{i+1} > \mu_i \text{ para todo } i \in \mathbb{N} \right\}.$$

En la primera parte de su trabajo, Grigoriev y Singer muestran que las únicas series de potencias de la forma anterior que pueden ser solución de una ecuación diferencial polinómica con coeficientes series de Laurent son aquellas para las que la sucesión de exponentes no está acotada, como recoge el siguiente enunciado.

Proposición 6.6 (D. Grigoriev, M. F. Singer [10])**.** *Si, dada una serie* $g = \sum_{i\in\mathbb{N}} \beta_i x^{\mu_i} \in H(\mathbb{R},\mathbb{C})$ *con* $\mu_{i+1} > \mu_i$ *para todo* $i \in \mathbb{N}$*, existe* $\mu \in \mathbb{R}$ *tal que* $\mu = \lim_{i\to\infty} \mu_i$*, entonces* g *no satisface ninguna ecuación diferencial polinómica con coeficientes en* $H(\mathbb{Z},\mathbb{C})$*.*

A continuación, desarrollan con detalle el método de Newton-Puiseux y describen un procedimiento para enumerar el conjunto de series de potencias que son solución de una ecuación diferencial. Finalmente demuestran que no existe un algoritmo que decida si una ecuación diferencial admite una solución en forma de series de este tipo, al contrario de lo que sucede en el caso algebraico.

En segundo lugar consideramos, en el caso en que Γ sea un monoide, en particular un semigrupo, las ecuaciones cuyos coeficientes son series reticuladas en la variable x. La definición de las series reticuladas se basa en el concepto de conjunto reticulado en un semigrupo totalmente ordenado, construido como una red sobre un origen y un número finito de direcciones, como formalizamos a continuación.

Definición 6.7. Sea $(\Gamma,+,\leq)$ un monoide totalmente ordenado. Se dice que un subconjunto $\Delta \subseteq \Gamma$ es un **subconjunto reticulado** si existen $\eta \in \Delta$ y $\{\gamma_i : 1 \leq i \leq r\} \subseteq \Delta$ un subconjunto

finito de forma que todo $\delta \in \Delta$ se puede escribir como

$$\delta = \eta + \sum_{i=1}^{r} n_i \gamma_i,$$

donde $n_i \in \mathbb{N}$ para todo $i \in \{1, ..., r\}$.

La definición general para monoides parcialmente ordenados considera un número finito de orígenes η_j; sin embargo, se puede probar que la definición dada es equivalente si Γ es totalmente ordenado [37]. El interés de los conjuntos reticulados al trabajar con elementos de un producto lexicográfico se debe al siguiente resultado.

Proposición 6.8. *Todo conjunto reticulado está bien ordenado.*

Con ello, podemos tomar subconjuntos reticulados de Γ con el orden dual como soportes de elementos de $H(\Gamma, \mathbb{R})$, o en general del grupo $H(\Gamma, \Bbbk)$ para un cuerpo cualquiera $\Bbbk$.

Definición 6.9. Dados un cuerpo $\Bbbk$ y un monoide totalmente ordenado Γ, se dice que un elemento de $H(\Gamma, \Bbbk)$ es una **serie reticulada** si su soporte es un subconjunto reticulado de Γ.

Se verifica a partir de la definición que el conjunto de series reticuladas es un subgrupo de $H(\Gamma, \Bbbk)$, que denotaremos por $H_R(\Gamma, \Bbbk)$. Por otro lado, el siguiente resultado garantiza que se trata de un espacio de soluciones de ecuaciones diferenciales en forma de series de potencias.

Teorema 6.10 (J. van der Hoeven [37])**.** *Sea $\Bbbk$ un cuerpo algebraicamente cerrado, y considérese la ecuación diferencial*

$$f(x, \mathbf{y}) = \sum_{J} f_J(x) \mathbf{y}^J = 0,$$

donde $J \in \mathbb{N}^r$ para cierto $r \in \mathbb{N}$ y $f_J \in H_R(\mathbb{R}, \Bbbk)$ para todo $J \in \mathbb{N}^r$. Entonces, si $g \in H(\mathbb{R}, \Bbbk)$ es solución de la ecuación, se tiene que $g \in H_R(\mathbb{R}, \Bbbk)$.

En otras palabras, las soluciones en forma de serie de potencias de ecuaciones diferenciales cuyos coeficientes son series reticuladas son necesariamente series reticuladas. Así, tenemos una primera descripción de un subgrupo de soluciones de ecuaciones diferenciales en forma series de potencias en los términos introducidos por Hahn.

6.3. Valoraciones de cuerpos y Teorema de Kaplansky

Por último, dedicamos unos párrafos a las ideas con las que continuaría esta línea de trabajo. En primer lugar, realizamos una breve introducción a la teoría de cuerpos valorados, que sigue un desarrollo paralelo a la teoría de grupos ordenados que hemos estudiado en este trabajo, culminando con el Teorema de Kaplansky como equivalente del Teorema del Inmersión de Hahn. Como indicamos en el Capítulo 5, un concepto más habitual que el de valoración de un grupo por un conjunto es el de valoración de un cuerpo por un grupo totalmente ordenado. Seguimos en esta parte el texto de L. Fuchs y L. Salce [9].

Consideramos un grupo abeliano totalmente ordenado Γ, y añadimos a Γ un elemento denotado por ∞, de forma que para todo $\gamma \in \Gamma$ resulta $\gamma < \infty$ y la operación en Γ se extiende a $\Gamma \cup \{\infty\}$ según $\gamma + \infty = \infty$. De ese modo, $\Gamma \cup \{\infty\}$ es un magma unitario totalmente ordenado, y lo denotaremos por Γ_∞.

Definición 6.11. Sean K un cuerpo, Γ un grupo abeliano totalmente ordenado y Γ_∞ su extensión por ∞. Se dice que una aplicación $\nu : K \to \Gamma_\infty$ es una **valoración de cuerpos** de K por el grupo Γ si satisface, para todos $x, y \in K$:

(I) $\nu(x) = \infty$ si y sólo si $x = 0$.

(II) $\nu(xy) = \nu(x) + \nu(y)$.

(III) $\nu(x+y) \geq \text{mín}(\nu(x), \nu(y))$.

En estas condiciones, se dice que (K, ν, Γ) es un **cuerpo valorado**.

Podemos observar que la definición es similar a la de valoración de grupos (Definición 5.6), considerando el orden dual en Γ y cambiando $e_0 = \text{mín}(\Gamma)$ por ∞. De hecho, como habíamos anticipado, el Ejemplo 3 de la página 28, la valoración de grupos p-ádica $\tilde{\nu}$, se entiende de forma natural como una valoración de cuerpos de $\mathbb{Q}$ en $\mathbb{Z} \cup \{\infty\}$, asociando a cada $m/n \in \mathbb{Q}$ el valor $\nu_p(m) - \nu_p(n)$, siendo $\nu_p(a) := \tilde{\nu}_p(a)^{-1}$ y $\{0\} = \nu_p(\tilde{\nu}_p^{-1}(\infty))$. Igualmente, podemos aplicar esta definición a cualquier cuerpo de Hahn, con coeficientes en $\mathbb{R}$ u otro cuerpo cualquiera, obteniendo la valoración natural. Además, podemos suponer sin pérdida de generalidad que las valoraciones de cuerpos son aplicaciones suprayectivas, como las valoraciones de grupos, ya que $\nu(K \setminus \{0\})$ es siempre un subgrupo de Γ.

La noción de valoración nos permite considerar el cuerpo residual de un cuerpo valorado, que tiene en el Teorema de Kaplansky un papel análogo al de $\mathbb{R}$ en el Teorema de Hahn.

Definición 6.12. Se dice que un anillo conmutativo R es un **anillo de valoración** si la familia de sus ideales está totalmente ordenada por la inclusión. Se dice que es un **dominio de valoración** si R es además un dominio de integridad.

Como consecuencia de la definición, si un anillo de valoración no es un cuerpo posee un único ideal maximal, que contiene todos los elementos no invertibles de R. En particular, un anillo de valoración es un anillo local.

Definición 6.13. Dados un anillo de valoración R y su ideal maximal $\mathfrak{m}$, se dice que el cuerpo cociente $R/\mathfrak{m}$ es el **cuerpo residual** de R.

El siguiente resultado permite conciliar estas definiciones con las valoraciones de cuerpos.

Proposición 6.14. *Dado un cuerpo valorado (K, ν, Γ), el subconjunto*

$$R_\nu = \{x \in K : \nu(x) \geq 0\}$$

es un dominio de valoración, cuyo único ideal maximal es

$$\mathfrak{m}_\nu = \{x \in K : \nu(x) > 0\}.$$

En estas condiciones, se dice que R_ν es el **anillo de valoración** de ν, y $k_\nu = R_\nu/\mathfrak{m}_\nu$ su cuerpo residual. Alternativamente, se puede probar que todo dominio de valoración es el anillo de valoración de una valoración sobre su cuerpo de fracciones [9].

Además, dados un cuerpo k y un grupo abeliano totalmente ordenado Γ, podemos considerar el equivalente del grupo de Hahn, que denotamos en esta parte por $k[[x^\Gamma]]$. En este caso, no impondremos que k sea un cuerpo ordenado, como sí lo es $\mathbb{R}$. No obstante, nótese que en la Proposición 6.2 no usamos que $\mathbb{R}$ es ordenado, y por lo tanto podemos asegurar que $k[[x^\Gamma]]$ tiene estructura de cuerpo. De ese modo, podemos considerar la valoración natural $\nu_\Gamma : k[[x^\Gamma]] \to \Gamma$. Con todo lo anterior, estamos en condiciones de enunciar el Teorema de Kaplansky.

Teorema 6.15 (**Teorema de Kaplansky** [18])**.** *Si (K, ν, Γ) es un cuerpo valorado de característica cero tal que el cuerpo residual k de la valoración es un subcuerpo de K, entonces (K, ν, Γ) es isomorfo a un subcuerpo valorado de $(k[[x^\Gamma]], \nu_\Gamma, \Gamma)$.*

La similitud con el Teorema de Inmersión de Hahn se hace evidente si consideramos cuerpos ordenados.

Definición 6.16. Sean $(K, +, \cdot)$ un cuerpo y $\leq$ una relación de orden sobre K. Se dice que K es un **cuerpo totalmente ordenado** si $(K, +, \leq)$ es un grupo totalmente ordenado y, adicionalmente, se verifica que para todos $a, b \in K$ tales que $a > 0$ y $b > 0$, entonces $a \cdot b > 0$.

Así, el grupo de valoración correspondiente a la valoración natural sobre K es el grupo de las clases arquimedianas de K, y el resultado proporciona una generalización directa del Teorema de Hahn para cuerpos.

Finalizamos el texto enunciando uno de los problemas abiertos con más interés en esta área: la búsqueda de una versión diferencial del Teorema de Kaplansky [27]. Para su formulación, debemos considerar primero la noción de cuerpo diferencial, con el cual se extiende el concepto de derivada de una serie de potencias con exponentes reales a cuerpos de series generalizadas.

Definición 6.17. Dado un cuerpo K, se dice que una aplicación $d : K \to K$ es una **ley de derivación** si satisface, para todos $a, b \in K$:

(I) $d(a + b) = d(a) + d(b)$.

(II) $d(ab) = d(a)b + ad(b)$ (Regla de Leibniz).

Se dice que un cuerpo K dotado de una ley de derivación d es un **cuerpo diferencial** (K, d).

Observación 6.18. Se puede comprobar el conjunto $\Bbbk := \ker d = \{c \in K : d(c) = 0\}$ es un subcuerpo de K, conocido como **cuerpo de constantes** de K respecto de d. Entonces, dados $a \in K$ y $c \in \Bbbk$, se tiene que $d(ca) = d(c)a + cd(a) = cd(a)$. Combinando esta propiedad con (I), se puede caracterizar una ley de derivación como una aplicación $\Bbbk$-lineal que satisface la regla de Leibniz.

El siguiente paso es conciliar los conceptos de valoración y ley de derivación.

Definición 6.19. Sean (K, d) un cuerpo diferencial y $\Bbbk$ su cuerpo de constantes. Sean ν una valoración definida en K, R_ν su anillo de valoración y $\mathfrak{m}_\nu$ el ideal maximal de R_ν. Se dice la valoración ν es una **valoración diferencial** si satisface

(I) $R_\nu = \Bbbk + \mathfrak{m}_\nu$.

(II) Para todos $a, b \in \mathfrak{m}_\nu$ con $b \neq 0$, se tiene que $\frac{d(a)b}{d(b)} \in \mathfrak{m}_\nu$.

Dados un cuerpo diferencial (K, d) y una valoración diferencial ν sobre él, se dice que (K, d, ν) es un **cuerpo valorado diferencial**.

Dados dos cuerpos valorados diferenciales y un isomorfismo entre ellos, se dice que son isomorfos *analíticamente* si el isomorfismo conmuta con la valoración, y que son isomorfos *diferencialmente* si conmuta con la ley de derivación. Por otro lado, existen particularizaciones de la definición de ley de derivación en cuerpos valorados diferenciales que imponen condiciones adicionales sobre la aplicación d. Un ejemplo es la derivación de tipo Hardy, que permite extender a las series generalizadas algunas reglas que verifican las series formales. La definición formal se pueden consultar en [27].

En estas condiciones, se enuncia el **problema de inmersión de Kaplansky diferencial**, que consiste en estudiar qué cuerpos valorados diferenciales son isomorfos analíticamente y diferencialmente a un subcuerpo del cuerpo de series generalizadas correspondiente dotado de una derivación de Hardy. Una instancia particular del problema anterior es la **conjetura de inmersión de Kaplansky diferencial**, según la cual el enunciado anterior es cierto en los cuerpos de Hardy de gérmenes de funciones en el infinito, extendiendo el resultado demostrado para la versión axiomática de los cuerpos de Hardy, los llamados H-cuerpos [26].

I. Anexo. Relaciones de orden y ordinales

En el texto, asumimos la axiomática de Zermelo-Fraenkel junto con el Axioma de Elección. La lista de axiomas de esta teoría se puede consultar en [17].

Recordamos que una **relación** sobre un conjunto M se dice **de orden** si verifica las propiedades reflexiva, antisimétrica y transtitiva. Si para cada par $x, y \in M$, resulta $x \leq y$ ó $y \leq x$, se dice que el orden es **total**. Por otro lado, si cada subconjunto no vacío de M posee mínimo, se dice que $\leq$ es un **buen orden**, o que $(M, \leq)$ está bien ordenado.

Se emplea habitualmente la notación $x < y$ cuando $(x \leq y) \wedge (x \neq y)$. En el texto, al dotar de orden a un conjunto lo especificamos con uno u otro símbolo indistintamente, siendo evidente el significado del otro, en cada caso. Adicionalmente, se dice que una aplicación biyectiva, inyectiva o suprayectiva entre dos conjuntos ordenados es, respectivamente, un **isomorfismo**, **monomorfismo** o **epimorfismo de orden** si preserva el orden entre cada par de elementos. Se emplean equivalentemente el término *o*-**isomorfismo** y sus análogos. Así, si M y N son conjuntos o-isomorfos, lo denotamos por $M \approx N$.

Desarrollamos a continuación una breve introducción a la teoría de los ordinales. Los ordinales son conjuntos que nos permiten extender la noción de enumeración a conjuntos infinitos.

Definición I.1. Se dice que un **conjunto** T es **transitivo** si todo elemento de T es un subconjunto de T o, equivalentemente, si $T \subseteq \mathcal{P}(T)$.

Definición I.2. Se dice que un conjunto es un **ordinal** si es transitivo y está bien ordenado respecto de la relación de pertenencia $\in$.

Se deduce de la definición que un ordinal está, de hecho, totalmente ordenado, defininiendo $\alpha < \beta$ si $\alpha \in \beta$. Así, notamos que todo elemento de un ordinal es a su vez un ordinal, que contiene los elementos menores que él. Por definición, el conjunto vacío es un ordinal, contenido en todos los demás, que denotamos por $0 := \varnothing$. Para cualquier ordinal α, observamos que $\alpha \cup \{\alpha\}$ también es un ordinal.

Definición I.3. Dado un ordinal α, se dice que $\alpha + 1 := \alpha \cup \{\alpha\}$ es su **sucesor**.

Definición I.4. Sea α un ordinal.

(I) Se dice que α es un **ordinal sucesor** si existe un ordinal β tal que $\alpha = \beta + 1$.

(II) Se dice que α es un **ordinal límite** si no es un sucesor.

Podemos construir los ordinales finitos sin más que considerar los ordinales sucesores del primer ordinal, el conjunto vacío:

$$0 := \varnothing, \quad 1 := 0 + 1 = \{\varnothing\}, \quad 2 := 1 + 1 = \{\varnothing, \{\varnothing\}\},$$

y así sucesivamente. En estos términos, por el Axioma de Infinitud sabemos que existe un conjunto x tal que $0 \in x$ y para todo $y \in x$, entonces $y + 1 \in x$. Los conjuntos con esta propiedad se denominan **conjuntos sucesores**. Empleando axiomas de la teoría de conjuntos, se puede probar que existe un conjunto sucesor contenido en cualquier conjunto sucesor, que conocemos como conjunto de los números naturales y denotamos por ω ó $\mathbb{N}$. Adicionalmente, resulta que ω es el conjunto de todos los ordinales finitos y satisface los axiomas de Peano. Empleando estas propiedades se demuestra, además, que ω es un ordinal, en particular el primer ordinal infinito.

El conjunto de los números naturales ω es un conjunto bien ordenado en el que se verifica el Principio de Inducción, lo que nos permite obtener el Teorema de Recurrencia y definir con él la aritmética sobre ω. A continuación vamos a ver, por un lado, que todo conjunto bien ordenado está en biyección con un ordinal; y por otro, que podemos extender el Principio de Inducción a

cualquier ordinal. Algunas de las demostraciones que siguen se basan en conceptos de la teoría de conjuntos que exceden el interés de este trabajo, por lo que las omitimos o no detallamos completamente en algunos casos.

Comencemos introduciendo el concepto de intervalo inicial.

Definición I.5. Sean $(M, \leq)$ un conjunto totalmente ordenado y $x \in M$. Se llama **intervalo inicial en M dado por** x al subconjunto

$$M_x = \{y \in M : y < x\}.$$

Pasamos a enunciar uno de los resultados que nos conducirán a probar que todo conjunto bien ordenado está en biyección con un ordinal.

Proposición I.6 (**Ley de tricotomía**)**.** *Dados dos conjuntos bien ordenados M, N, se cumple exactamente una de las siguientes afirmaciones:*

- *M es o-isomorfo a N.*
- *Existe $x \in M$ tal que M_x es o-isomorfo a N.*
- *Existe $y \in N$ tal que N_y es o-isomorfo a M.*

Por otro lado, emplearemos también la siguiente propiedad, conocida como paradoja de Burali-Forti.

Teorema I.7. *No existe el conjunto de todos los ordinales.*

Demostración. Supongamos por reducción al absurdo que existe el conjunto Ω de todos los ordinales. Vamos a ver que, entonces, Ω es transitivo y está bien ordenado.

En el caso de la transitividad, observamos que si $\alpha \in \Omega$ y $\beta \in \alpha$, entonces α es un ordinal y por tanto β también, luego $\beta \in \Omega$. Para ver la buena ordenación, supongamos por contradicción que existe $M \subseteq \Omega$ no vacío sin primer elemento. Entonces, dado $\alpha \in M$ existe $\beta \in M$ tal que $\beta \in \alpha$, así que $\beta \in \alpha \cap M$. Como α es un ordinal y $\alpha \cap M \subseteq \alpha$ un subconjunto no vacío, tiene un primer elemento $\alpha_0 = \text{mín}(\alpha \cap M)$. Veamos que este elemento debe ser el primero de M. Dado cualquier $\gamma \in M$, utilizamos la ley de tricotomía entre α y γ para ver que $\alpha_0 \in \gamma$:

- Si $\gamma \in \alpha$, entonces $\gamma \in \alpha \cap M$, y por tanto $\alpha_0 \in \gamma$.
- Si $\alpha \in \gamma$ ó $\alpha \approx \gamma$, entonces $\alpha \subseteq \gamma$ y así $\alpha_0 \in \gamma$.

En consecuencia, M debe tener mínimo y por tanto Ω está bien ordenado.

Hemos probado que Ω es un ordinal, así que $\Omega \in \Omega$, lo que implica $\Omega < \Omega$. Sin embargo esto es imposible en un ordinal, ya que se trata de un conjunto totalmente ordenado.

□

Como consecuencia, se dice que los ordinales forman una clase. En este punto estamos en condiciones de probar el resultado que buscábamos.

Teorema I.8. *Sea $(x, \leq)$ un conjunto bien ordenado. Entonces existe un único ordinal α, salvo isomorfismo, tal que α es o-isomorfo a x.*

Demostración. Dado cualquier ordinal α, consideramos la ley de tricotomía entre x y α. En los casos $x \approx \alpha$ y $x \approx \alpha_\gamma$ con $\gamma \in \alpha$, tenemos el o-isomorfismo. Por otro lado, el tercer caso, $x_a \approx \alpha$ con $a \in x_a$, no se puede dar en todos los ordinales. En efecto, usando argumentos propios de la teoría de conjuntos se puede probar que, si ese fuera el caso, existiría el conjunto de todos los ordinales, en contradicción con el Teorema I.7. En consecuencia, tenemos asegurada la existencia de un ordinal que cumple una de las dos primeras afirmaciones de la ley de tricotomía y por tanto es o-isomorfo a x. □

Observación I.9. A partir del teorema anterior, veamos que en todo espacio vectorial podemos encontrar una base indexada por un ordinal, como usamos en el Lema 6.3. Por el Axioma de Elección, todo espacio vectorial tiene una base y todo conjunto se puede dotar de un buen orden. Por tanto, podemos asumir que todo espacio vectorial tiene una base bien ordenada. Por el Teorema I.8, dicha base es o-isomorfa a un ordinal. Este hecho nos permite realizar razonamientos inductivos transfinitos sobre los elementos de una base de un espacio vectorial.

Una consecuencia directa del teorema anterior es el siguiente resultado que empleamos en el trabajo.

Corolario I.10. *Si un conjunto totalmente ordenado $(A, \leq)$ está bien ordenado respecto del orden $\leq$ y del orden dual $\leq_D$, entonces es finito.*

Demostración. Como A está bien ordenado, está en o-biyección con un ordinal α. Si α no fuera finito, entonces $\omega \subseteq \alpha$, y en consecuencia existiría un subconjunto $B \subseteq A$ en o-biyección con ω. Sin embargo, esto no es posible porque ω no tiene elemento máximo, mientras que B debe tenerlo por estar A bien ordenado respecto del orden dual. □

Para terminar, consideramos el concepto de transfinito. Al igual que hablamos de sucesiones finitas o infinitas, cuando su dominio es, respectivamente, un conjunto finito ó $\mathbb{N}$, se emplea el concepto de sucesión **transfinita** para referirnos a sucesiones definidas sobre un ordinal. El argumento de inducción también tiene su equivalente en el caso transfinito.

Proposición I.11 (**Inducción transfinita**). *Sea β un ordinal y γ un subconjunto de β con las propiedades:*

(1) $\varnothing \in \gamma$.

(2) Si $\alpha \in \beta$ *y* $\alpha \subseteq \gamma$, *entonces* $\alpha \in \gamma$.

Entonces $\gamma = \beta$.

Demostración. Supongamos que $\gamma \subsetneq \beta$, con lo que $\beta \setminus \gamma$ es un subconjunto no vacío de β, y por tanto existe $\alpha_0 = \text{mín}(\beta \setminus \gamma)$. Por (1), $\alpha_0 \neq \varnothing$. Por ser el mínimo, se tiene que $\alpha_0 \subseteq \gamma$, y entonces satisface (2), luego $\alpha_0 \in \gamma$, en contradicción con su definición. Así que debe ser $\gamma = \beta$. □

Del mismo modo que para los números naturales, se pueden definir con algo de precaución la suma y producto de ordinales, y con ello los ordinales sucesores de ω: $\omega+1, \omega+2, ...$, hasta llegar al siguiente ordinal límite, $\omega + \omega =: \omega \cdot 2$, y más tarde $\omega \cdot 3, ..., \omega \cdot \omega =: \omega^2, ...$ Análogamente al caso de ω, podemos obtener la caracterización $\alpha = \{\beta : \beta < \alpha\}$ para cualquier ordinal. Omitimos el formalismo porque excede el interés de este trabajo.

II. Apéndice. Resultados de ordenabilidad en grupos

Dedicamos este apéndice a probar algunos resultados más relativos al concepto de ordenabilidad en un grupo, que acompañarán a las caracterizaciones de grupo ordenable enunciadas en la Proposición 4.8 y el Teorema 5.24. Si bien los resultados de esta sección no guardan relación con el Teorema de Inmersión de Hahn, a diferencia de los recogidos en el resto del trabajo, su inclusión completa la teoría de grupos ordenados desarrollada a lo largo del texto, sin necesidad de introducir una gran cantidad de nociones nuevas. En particular, caracterizaremos en primer lugar la ordenabilidad en términos de semigrupos normales, y posteriormente probaremos que los grupos nilpotentes y los grupos libres son grupos ordenables. Hemos usado el texto de D.S. Dummit y R.M. Foote [6] como referencia principal en esta parte.

II.1. Ordenabilidad en términos de semigrupos normales

Comenzamos por considerar el cono positivo P de un orden parcial sobre un grupo G, y nos preguntamos bajo qué condiciones se puede extender éste a un conjunto $\bar{P}$ que defina un orden total, de forma que G tenga estructura de grupo totalmente ordenado. Denotaremos por $P_0 = P \cup \{e\}$ el conjunto de elementos no negativos, que tiene estructura de monoide. En efecto, se trata de un conjunto no vacío con la operación (asociativa) heredada de G, que es cerrada en P por la propiedad de compatibilidad, y por tanto en P_0, y posee un elemento neutro e. Dado un subconjunto $A \subseteq G$, denotamos por $S(A)$ el semigrupo generado por A, que se puede caracterizar como el conjunto de combinaciones finitas de elementos de A cuando este no es vacío. De forma similar, consideremos el siguiente concepto.

Definición II.1. Sea A un subconjunto de un grupo G. Se define el **semigrupo normal generado por** A como

$$S_N(A) = \bigcap_{N \in \mathcal{N}_A} N,$$

donde $\mathcal{N}_A$ es la familia de semigrupos normales de G que contienen a A.

El conjunto $S_N(A)$ definido es semigrupo normal por ser intersección de semigrupos normales. Presentamos ahora una caracterización del mismo.

Proposición II.2. *Sea A un subconjunto no vacío de G. Entonces, el semigrupo normal $S_N(A)$ generado por A es el semigrupo generado por la unión $\bigcup_{g \in G} A^g$, es decir, por los conjugados de elementos de A por elementos de G.*

Demostración. Denotando la unión considerada por A_N, tenemos que ver que $S(A_N) = S_N(A)$, de acuerdo con la Definición II.1. Veamos primero que $S(A_N)$ es un semigrupo normal, que contiene a A, y así tendremos que $S_N(A) \subseteq S(A_N)$. Tomamos un elemento

$$x = \prod_{i=1}^{n} g_i^{-1} x_i g_i \in S(A_N),$$

con $x_i \in A$ y $g_i \in G$ para todo $1 \leq i \leq n$. Dado $g \in G$, tenemos que

$$g^{-1} x g = g^{-1} \left(\prod_{i=1}^{n} g_i^{-1} x_i g_i \right) g = \prod_{i=1}^{n} g^{-1} g_i^{-1} x_i g_i g = \prod_{i=1}^{n} (g_i g)^{-1} x_i (g_i g) \in S(A_N),$$

luego $g^{-1} S(A_N) g \subseteq S(A_N)$, y así $S(A_N)$ es normal. Además, como $A^e = A$, tenemos que $A \subseteq S(A_N)$, y por tanto la primera contención.

En sentido opuesto, veamos que $S(A_N) \subseteq S_N(A)$. Dado un semigrupo normal que contiene a A, por normalidad contiene también al conjunto conjugado de A por cualquier elemento $g \in G$, y en consecuencia a la unión A_N de estos conjuntos. Por lo tanto, por ser semigrupo, contiene al semigrupo generado $S(A_N)$ generado por A_N. □

En el caso de tener un conjunto finito $A = \{a_i : i \in \{1, ..., n\}\} \subseteq G$, denotaremos por $S_N(A)$ el semigrupo normal generado por A, y por $S_N(A^\epsilon)$ el generado por $A^\epsilon = \{a_i^{\epsilon_i} : i \in \{1, ..., n\}\}$, donde $\epsilon = (\epsilon_1, ..., \epsilon_n) \in \{-1, 1\}^n$. Además, emplearemos la notación $S_N(a_1) := S_N(\{a_1\})$ si $A = \{a_1\}$, y $S_N(A, B) := S_N(A \cup B)$ para dos subconjuntos $A, B \subseteq G$.

Con todo ello, podemos enunciar un resultado que da una condición necesaria y suficiente para que un orden parcial se pueda extender a un orden total. La idea es poder construir un conjunto normal, disjunto de los positivos del orden parcial y cerrado respecto de la operación en G, de modo que cada elemento o su inverso estén en él. Este será a posteriori el conjunto de negativos, que definirá el orden total buscado.

Teorema II.3 (L. Fuchs [8])**.** *Sean G un grupo parcialmente ordenado y $P \subseteq G$ el cono positivo. Entonces, son equivalentes:*

(1) El orden definido por P se puede extender a un orden total.

(2) Para cualquier conjunto finito $A \subseteq G$ con $e \notin A$, existe $\epsilon \in \{-1, 1\}^{\sharp A}$ de forma que $P_0 \cap S_N(A^\epsilon) = \varnothing$.

Demostración. Supongamos que un orden parcial dado por P sobre un grupo G se puede extender a un orden total $\bar{P}$. En ese caso, dado un conjunto finito $A = \{a_i : i \in \{1, ..., n\}\} \subseteq G$ con $e \notin A$, exactamente un elemento de $\{a_i, a_i^{-1}\}$ pertenece a $\bar{P}^{-1}$, de acuerdo con la caracterización del Corolario 2.15. Por la propiedad de compatibilidad, como $\bar{P}^{-1}$ es normal y cerrado para la operación en G, se puede escoger ϵ de modo que $A^\epsilon \subseteq \bar{P}^{-1}$ y $S_N(A^\epsilon) \subseteq \bar{P}^{-1}$. Así, se tiene que

$$(P_0 \cap S_N(A^\epsilon)) \subseteq \left(\bar{P}_0 \cap S_N(A^\epsilon)\right) \subseteq \left(\bar{P}_0 \cap \bar{P}^{-1}\right) = \varnothing.$$

Recíprocamente, consideremos un orden parcial dado por $P \subseteq G$ que verifica (2). Debemos encontrar un orden total cuyo conjunto de positivos contenga a P. Dado $x \in G$, probaremos que, si P' define un orden parcial que satisface (2), entonces al menos uno de $P'S_N(x)$ ó $P'S_N(x^{-1})$ también define un orden parcial con la propiedad (2). Supongamos que existen subconjuntos finitos $A, B \subseteq G$ que no contienen al neutro, y tales que para toda elección de ϵ, η, es

$$P'_0 \cap S_N(x, A^\epsilon) \neq \varnothing, \quad P'_0 \cap S_N(x^{-1}, B^\eta) \neq \varnothing.$$

Entonces, tendríamos que $P'_0 \cap S_N(x^{\epsilon_0}, A^\epsilon, B^\eta) \neq \varnothing$, donde $\epsilon_0 \in \{-1, 1\}$, en contradicción con que P' cumple (2). Así, notamos que para algún $\epsilon_0 \in \{-1, 1\}$, se cumple que para todo subconjunto A existe una sucesión ϵ tal que $P'_0 \cap S_N(x^{\epsilon_0}, A^\epsilon) = \varnothing$. Supongamos que $\epsilon_0 = 1$. Tomando así el conjunto $P'S_N(x^{-1})$, se puede comprobar que es normal y cerrado para la operación de G, ya que lo son P' y $S_N(x^{-1})$. Veamos que además satisface (2). Por normalidad podemos escribir todo elemento de $P'S_N(x^{-1})$ como px^{-k} con $p \in P'$ y $k \in \mathbb{N}_{\geq 1}$. Entonces, dado un subconjunto finito $A \subseteq G$ con $e \notin A$,

$$px^{-k} \in S_N(A^\epsilon) \quad \Rightarrow \quad p \in S_N(x^k, A^\epsilon) \subseteq S_N(x, A^\epsilon),$$

lo cual es imposible por lo razonado para x. Por otro lado, $e \notin S_N(A^\epsilon) \subseteq S_N(x, A^\epsilon)$, con lo que concluimos que $(P'S_N(x^{-1}))_0 \cap S_N(A^\epsilon) = \varnothing$. Finalmente, observamos que dado cualquier $y \in G$ no neutro, la propiedad (2) implica que $P'S_N(x^{-1}) \cap S_N(y^\eta) = \varnothing$ para algún $\eta \in \{-1, 1\}$, y en consecuencia tenemos que $(P'S_N(x^{-1})) \cap (P'S_N(x^{-1}))^{-1} = \varnothing$. Con ello concluimos que $P'S_N(x^{-1})$ define un orden parcial con la propiedad (2). Si fuera $\epsilon_0 = -1$, obtendríamos el resultado para $P'S_N(x)$.

Podemos ahora considerar la cadena de subconjuntos de G formada al añadir sucesivamente un elemento de cada par $\{x, x^{-1}\}$, según el desarrollo previo, al orden parcial P. Dicha cadena está totalmente ordenada por la inclusión y acotada superiormente por el grupo G. Usando el Lema de Kuratowski-Zorn, posee un elemento maximal $\bar{P}$, que satisface (2) y define un orden sobre G que extiende el definido por P. Además, el orden es total, puesto que si no podríamos repetir la construcción anterior y extenderlo a un orden estrictamente mayor. Así, queda probado que G es ordenable. □

Podemos aplicar el Teorema en el caso particular de que no tengamos un orden parcial en G, es decir, $P = \varnothing$, y con ello, establecer otra caracterización de un grupo ordenable, que se añade a las obtenidas en el trabajo.

Corolario II.4. *Un grupo G es ordenable si y sólo si para cualquier conjunto finito $A \subseteq G$ que no contenga al elemento neutro, existe $\epsilon \in \{-1,1\}^{\sharp A}$ de tal forma que $e \notin S_N(A^\epsilon)$.*

Ejemplo. Con este resultado podemos probar que el grupo $(\mathbb{C}, \cdot)$ no es ordenable, ya que tomando $A = \{i\}$, se tiene que $1 \in S_N(A) = \{i, -i, 1, -1\}$.

Consideramos ahora la intersección de los $2^{\sharp A}$ semigrupos $S_N(A^\epsilon)$ para diferentes posibilidades de elección de la sucesión $\epsilon \in \{-1,1\}^{\sharp A}$. Tenemos la siguiente caracterización.

Lema II.5. *Para cualquier conjunto finito $A \subseteq G$, el conjunto*

$$\bigcap_{\epsilon \in \{-1,1\}^{\sharp A}} S_N(A^\epsilon)$$

es un subgrupo de G o el conjunto vacío.

Demostración. Sea $A = \{a_i : i \in \{1, ..., n\}\}$. Supongamos que la intersección no es vacía y sean $x, y \in \bigcap_{\epsilon \in \{-1,1\}^n} S_N(A^\epsilon)$. Así, ambos se pueden escribir de al menos 2^n formas como producto finito de potencias de conjugados de elementos de cada A^ϵ, respectivamente, que denotaremos por $x(\epsilon)$, $y(\epsilon)$. Dado $\epsilon \in \{-1,1\}^n$, sean

$$x(\epsilon) = \prod_{j=1}^{k} (g_j^{-1} a_j^{\epsilon_j} g_j)^{r_j}, \quad y(\epsilon) = \prod_{j=1}^{l} (h_j^{-1} b_j^{\epsilon_j} h_j)^{s_j},$$

donde $a_j, b_j \in A$, $g_j, h_j \in G$ y $r_j, s_j \in \mathbb{N}_{\geq 1}$ para todo $j \in \{1, ..., \text{máx}\{k, l\}\}$. Entonces, para cualquier $\epsilon \in \{-1,1\}^n$, observamos que xy^{-1} se puede escribir como elemento de $S_N(A^\epsilon)$ según

$$\begin{aligned} x(\epsilon)y(-\epsilon)^{-1} &= \left(\prod_{j=1}^{k} (g_j^{-1} a_j^{\epsilon_j} g_j)^{r_j} \right) \left(\prod_{j=1}^{m} (h_j^{-1} b_j^{-\epsilon_j} h_j)^{s_j} \right)^{-1} \\ &= \left(\prod_{j=1}^{k} (g_j^{-1} a_j^{\epsilon_j} g_j)^{r_j} \right) \left(\prod_{j=m}^{1} (h_j^{-1} b_j^{\epsilon_j} h_j)^{s_j} \right), \end{aligned}$$

y concluimos que xy^{-1} es también elemento de la intersección. □

Con ello enunciamos otra consecuencia del Teorema II.3.

Corolario II.6. *Un grupo G es ordenable si y sólo si para cualquier conjunto finito $A \subseteq G$ que no contenga al elemento neutro,*

$$\bigcap_{\epsilon \in \{-1,1\}^{\sharp A}} S_N(A^\epsilon) = \varnothing.$$

Demostración. Basta ver que, si la intersección no es vacía, entonces es un subgrupo y e es un elemento de ella. En caso contrario, e no está en alguno de los $S_N(A^\epsilon)$. □

Como consecuencia del Corolario anterior, enunciamos una caracterización más de los grupos ordenables, en términos de los subgrupos de generación finita.

Teorema II.7 (**Teorema local de ordenabilidad**). *Un grupo G es ordenable si y sólo si lo es cada uno de sus subgrupos finitamente generados.*

Demostración. Si G es ordenable, lo son todos sus subgrupos, en particular los de generación finita. Recíprocamente, tomando un conjunto finito $A \subseteq G$ que no contenga al elemento neutro, A es subconjunto del subgrupo (finitamente) generado por A. Por ser este ordenable, la intersección de los $S_N(A^\epsilon)$ debe ser vacía, así que por el Corolario II.6, el propio G es ordenable. □

II.2. Ordenabilidad en términos de series centrales de subgrupos

En esta sección introducimos un tipo particular de familias subinvariantes de subgrupos en un grupo: las series centrales. En particular, trabajaremos con las denominadas series central inferior y superior de un grupo, y deduciremos un resultado de ordenabilidad basado en condiciones sobre estas series. Además, las series centrales nos permitirán definir el concepto de grupo nilpotente en la siguiente sección, y probar que tanto los grupos nilpotentes como los grupos libres son ordenables.

Definición II.8. Sean $(G, \cdot)$ un grupo y $\mathcal{G}$ una familia subinvariante de subgrupos normales de G. Se dice que la familia $\mathcal{G}$ es una **serie central** si para todo salto $A \sqsubset B$ de $\mathcal{G}$, el grupo cociente B/A está contenido en el centro del grupo G/A.

De forma habitual, las series centrales vienen definidas en términos de conmutadores de subgrupos.

Definición II.9. Sea G un grupo, y $g, h \in G$. Se define el **conmutador** de g y h como el elemento de G dado por $[g, h] := g^{-1}h^{-1}gh$.

Definición II.10. Sean G un grupo y H y K dos subgrupos de G. Se define el **conmutador** de H y K, denotado por $[H, K]$, como el subgrupo generado por el conjunto

$$\{[h, k] : h \in H, k \in K\}.$$

El interés del conmutador de subgrupos está relacionado con la búsqueda de grupos cociente abelianos. Por ejemplo, $[G, G]$ es el subgrupo normal de G más pequeño de forma que el cociente es abeliano. En general, tenemos la siguiente propiedad.

Proposición II.11. *Dados un grupo G y dos subgrupos normales H y K, el conmutador $[H, K]$ es un subgrupo normal.*

Demostración. Consideramos tres elementos $g \in G$, $h \in H$ y $k \in K$. Si demostramos que $g^{-1}[h, k]g \in [H, K]$, tendremos el resultado también para todo elemento generado por elementos del tipo $[h, k]$, y concluiremos que $[H, K]$ es normal. Entonces,

$$g^{-1}[h, k]g = g^{-1}h^{-1}k^{-1}hkg = (g^{-1}h^{-1}g)(g^{-1}k^{-1}g)(g^{-1}hg)(g^{-1}kg) = [g^{-1}hg, g^{-1}kg].$$

Dado que H y K son normales, $g^1hg \in H$ y $g^{-1}kg \in K$, por lo tanto $g^{-1}[h, k]g \in [H, K]$, como queríamos probar. □

Pasamos ahora a considerar las series centrales inferior y superior transfinitas de un grupo, que emplearemos en la caracterización de grupo ordenable. El adjetivo transfinito hace referencia a la necesidad de definir estas series en términos de ordinales cuando el grupo es infinito. Una breve teoría de ordinales ha sido desarrollada en el Anexo.

Definición II.12. Sean $(G, \cdot)$ un grupo y α un ordinal.

(I) Se llama **serie central inferior transfinita** de G a la cadena de subgrupos normales en G con índices en α,

$$... \subseteq G_\tau \subseteq G_{\tau-1} \subseteq ... \subseteq G_1 \subseteq G_0 = G,$$

definida según:

- $G_\tau = [G_{\tau-1}, G]$ si τ es un ordinal sucesor.
- $G_\tau = \bigcap_{\sigma<\tau} G_\sigma$ si τ es un ordinal límite.

(II) Se llama **serie central superior transfinita** de G a la cadena de subgrupos normales en G con índices en α,

$$\{e\} = Z_0(G) \subseteq Z_1(G) \subseteq ... \subseteq Z_\tau(G) \subseteq Z_{\tau+1}(G) \subseteq ...$$

definida según:

- $Z_\tau(G) = \{h \in G : [h, g] \in Z_{\tau-1}(G) \text{ para todo } g \in G\}$ si τ es un ordinal sucesor.
- $Z_\tau(G) = \bigcup_{\sigma<\tau} Z_\sigma(G)$ si τ es un ordinal límite.

Comprobemos que las series están bien definidas. Por la Proposición II.11, los subgrupos G_τ son normales para todo $\tau \in \alpha$. Asimismo, $Z_\tau(G) \triangleleft Z_{\tau+1}(G)$ por definición. Las siguientes propisiciones prueban que las dos cadenas de subgrupos definidas son, en efecto, series centrales, de acuerdo con la Definición II.8. En el segundo caso deducimos, además, que los subgrupos $Z_\tau(G)$ también son normales en G.

Proposición II.13. *Sean G un grupo y $\{G_\tau\}_{\tau\in\alpha}$ la serie central inferior transfinita de G. Entonces, para todo ordinal $\tau \in \alpha$ se verifica que*

$$G_\tau/G_{\tau+1} \subseteq Z(G/G_{\tau+1}).$$

En particular, los factores son abelianos.

Demostración. Consideramos $\tau \in \alpha$ y un elemento $h \in G_\tau$. Queremos ver que la operación entre $hG_{\tau+1} \in G_\tau/G_{\tau+1}$ y cualquier elemento $gG_{\tau+1} \in G/G_{\tau+1}$ es conmutativa. Tenemos la siguiente cadena de equivalencias:

$$(hG_{\tau+1})(gG_{\tau+1}) = (gG_{\tau+1})(hG_{\tau+1}) \quad \Leftrightarrow \quad (hg)G_{\tau+1} = (gh)G_{\tau+1} \quad \Leftrightarrow \quad (gh)^{-1}(hg) \in G_{\tau+1}.$$

Observamos que $(gh)^{-1}(hg) = h^{-1}g^{-1}hg = [h, g]$, y éste, usando la definición, es un elemento de $G_{\tau+1} = [G_\tau, G]$. □

Proposición II.14. *Sean G y $\{Z_\tau(G)\}_{\tau\in\alpha}$ la serie central superior transfinita de G. Entonces, para todo ordinal $\tau \in \alpha$ se verifica que*

$$Z_{\tau+1}(G)/Z_\tau(G) = Z(G/Z_\tau(G)).$$

En particular, los factores son abelianos. Además, $Z_{\tau+1}(G)$ es un subgrupo normal en G.

Demostración. La prueba del primer enunciado es una mera comprobación a partir de la definición. Dado $h \in G$, tenemos que

$$\begin{aligned} hZ_\tau(G) \in Z_{\tau+1}(G)/Z_\tau(G) \quad &\Leftrightarrow \quad [hZ_\tau(G), gZ_\tau(G)] = Z_\tau(G) \quad \forall g \in G \\ &\Leftrightarrow \quad hZ_\tau(G) \in Z(G/Z_\tau(G)). \end{aligned}$$

Con ello, veamos que $Z_{\tau+1}(G)$ es normal en G. Sean $h \in Z_{\tau+1}(G)$ y $g \in G$. Por la igualdad anterior, $Z_{\tau+1}(G)/Z_\tau(G) \triangleleft G/Z_\tau(G)$. Así, existe $\bar{h} \in Z_{\tau+1}(G)$ tal que $g^{-1}hgZ_\tau(G) = \bar{h}Z_\tau(G)$, y en consecuencia $g^{-1}hg = \bar{h}z$ para cierto $z \in Z_\tau(G)$. Como $Z_\tau(G) \subseteq Z_{\tau+1}(G)$, tenemos que $g^{-1}hg \in Z_{\tau+1}(G)$, lo que prueba la normalidad. □

El hecho de que las series definidas sean cadenas asegura la normalidad en el caso de los subgrupos correspondientes a ordinales límite.

Observación II.15.

1. Si G es abeliano, tenemos las relaciones $[G, G] = \{e\}$ y $Z(G) = G$, y en consecuencia las series centrales inferior y superior son triviales. Veremos que una generalización consiste en estudiar los grupos para las que son finitas, conocidos como grupos nilpotentes.

2. La igualdad en la Proposición II.14 implica que la serie central superior es la cadena ascendente de subgrupos de G que crece más rápido. En otras palabras, dada cualquier serie central $\{H_\tau\}_{\tau\in\alpha}$ con $H_0 = \{e\}$, se tiene que $H_\tau \subseteq Z_\tau(G)$ para todo $\tau \in \alpha$, por la definición de serie central. Adicionalmente, observamos que el subgrupo $Z_1(G)$ coincide con el centro de G, y siguiendo esa denominación, se dice que $Z_\tau(G)$ es el τ-ésimo centro de G.

Mostramos a continuación un ejemplo de series centrales inferior y superior de un grupo.

Ejemplo. Consideramos el grupo $G = D_4 \times (\mathbb{Z}/2\mathbb{Z})$, donde D_4 denota el grupo diédrico de las simetrías del cuadrado, de orden 8. Calculemos sus series centrales inferior y superior de acuerdo con la Definición II.12. Se puede comprobar que tanto el conmutador como el centro conmutan con el producto de grupos, así que podemos trabajar independientemente con ambos grupos.

Como $K := \mathbb{Z}/2\mathbb{Z}$ es abeliano, ambas series son triviales, es decir, $K_1 = \{e\}$ y $Z_1(K) = K$. En el caso de $H := D_4$, observamos primero que $H_1 = [H, H]$ es el subgrupo normal más pequeño de forma que H/H_1 es un grupo abeliano. Como H tiene orden 8 y al menos dos subgrupos de orden 4, el conmutador, que es único, debe tener orden 2. Encontramos que $\{1, a^2\}$ es normal y el cociente es abeliano, luego $H_1 = \{1, a^2\}$. Este es a su vez es abeliano, así que $H_2 = \{e\}$. Con todo, la serie inferior viene dada por

$$\{e\} \subseteq \{1, a^2\} \times \{e\} \subseteq D_4 \times (\mathbb{Z}/2\mathbb{Z}).$$

Alternativamente, tenemos también que $Z_1(D_4) = \{1, a^2\}$, y por ser el cociente abeliano, usando la Proposición II.14 obtenemos $Z_2(D_4) = D_4$. Por lo tanto, la serie superior es

$$\{e\} \subseteq \{1, a^2\} \times (\mathbb{Z}/2\mathbb{Z}) \subseteq D_4 \times (\mathbb{Z}/2\mathbb{Z}).$$

Este ejemplo pone de manifiesto que las series inferior y superior no tienen por qué coincidir.

En relación con las definiciones anteriores, enunciamos el siguiente resultado. En él se recogen dos condiciones suficientes para la ordenabilidad de un grupo, que se demuestran de forma paralela.

Teorema II.16 (B. H. Neumann [28])**.** *Sea $(G, \cdot)$ un grupo.*

(1) Si G posee una serie central con factores libres de torsión, entonces G es ordenable.

(2) Si G posee una serie central inferior dada por un conjunto ordinal de índices α, cuyos factores $G_\tau/G_{\tau+1}$ son libres de torsión, y tal que $G_\alpha = \{e\}$, entonces G es ordenable.

Demostración. En ambos casos tenemos que para todo salto $A \sqsubset B$ de la serie normal correspondiente, B/A es abeliano y libre de torsión, y por tanto, de acuerdo con la Proposición 4.8, ordenable. Además, en los dos casos resulta $B/A \subseteq Z(G/A)$. Empleando un argumento de inducción, suponemos que G/B es ordenable, y estamos en condiciones de aplicar el Lema 4.11: tenemos que B/A y el cociente $(G/A)/(B/A) \cong G/B$ son grupos ordenables. Como consecuencia, deducimos que una ordenación de B/A lo es a su vez de G/A, y por tanto de $N(A)/A$, dado que $G = N(A)$ para todo A por ser las series normales. Para el caso (1), tenemos que toda serie central es subinvariante. En (2), la única propiedad que debemos confirmar es el punto (I) de la Definición 5.12, y se verifica por ser $G_\alpha = \{e\}$, así que la familia también es subinvariante. En ambos casos estamos en condiciones de aplicar el Teorema 5.24, y concluimos que G es ordenable. □

II.3. Grupos nilpotentes

En la Proposición 4.8, hemos probado que un grupo abeliano libre de torsión admite un orden compatible con la operación de grupo. Vemos ahora que, en realidad, podemos relajar la hipótesis de ser abeliano por la de ser nilpotente, más débil. Empezamos con la definición de grupo nilpotente.

Definición II.17. Un grupo $(G, \cdot)$ se dice **nilpotente** si posee una serie central de longitud finita.

Una serie central es, en particular, una familia completa. En ese caso, de acuerdo con la Proposición 5.16, los subgrupos de las series centrales de longitud finita están en biyección con los saltos. Esta propiedad es fundamental para poder deducir que los grupos nilpotentes y libres de torsión son ordenables.

La denominación de grupo nilpotente se debe a que, dada esa propiedad, se puede comprobar que la aplicación

$$\begin{array}{rccc} \mathrm{ad}_g: & G & \longrightarrow & G \\ & x & \longmapsto & [g,x] \end{array}$$

es nilpotente, es decir, que existe $n \in \mathbb{N}$ tal que $(\mathrm{ad}_g)^n$ es la aplicación neutra, para todo $g \in G$.

Definición II.18. Dado un grupo nilpotente G, se denomina **clase de nilpotencia** al mínimo de las longitudes de las series centrales.

Los grupos abelianos son grupos nilpotentes de clase de nilpotencia 1, ya que el centro coincide con el propio grupo, y entonces la serie central superior es trivial. El grupo $D_4 \times (\mathbb{Z}/2\mathbb{Z})$, cuyas series centrales han sido calculadas en la página 59, es un ejemplo de grupo nilpotente no abeliano, de clase 2.

Definición II.19. Se dice que un grupo G es **localmente nilpotente** si todo subgrupo de G finitamente generado es nilpotente.

Para la siguiente propiedad sobre los grupos nilpotentes, seguiremos la demostración de A. G. Kurosch [21]. En ella se emplea el siguiente concepto.

Definición II.20. Se dice que un grupo es un **r-grupo** si para todo $a \in G$ y $n \in \mathbb{N}$, la ecuación $x^n = a$ tiene a lo sumo una solución.

La r en la denominación proviene de que, si existe, la raíz n-ésima de un elemento es única. Observamos que esta condición es equivalente a que dados $x, y \in G$ tales que $x^n = y^n$ con $n > 0$, entonces $x = y$. Basta tomar $a = y^n$ en la definición y observar que y es solución. A continuación enunciamos un resultado que nos llevará a probar la ordenabilidad de los grupos nilpotentes y libres de torsión.

Lema II.21 (A. G. Kurosch [21])**.** *Todo grupo nilpotente y libre de torsión posee una serie central de longitud finita con factores libres de torsión.*

Demostración. Consideramos un grupo G nilpotente y libre de torsión. Dividiremos la demostración en dos partes. En primer lugar, veremos que G es un r-grupo, y a continuación veremos que, en consecuencia, existe una serie central superior en G con factores abelianos y libres de torsión.

Probamos el primer resultado por inducción en la clase de nilpotencia k de G. El caso $k = 1$ se corresponde con el de un grupo abeliano. Con ello, dados $x, y \in G$ con $x^n = y^n$, resulta $1 = x^n y^{-n} = (xy^{-1})^n$, y como G es libre de torsión, $x = y$, así que G es r-grupo. En el caso general, consideramos la serie central superior de longitud k

$$\{e\} = Z_0(G) \subseteq Z_1(G) \subseteq \ldots \subseteq Z_{k-1}(G) \subseteq Z_k(G) = G.$$

Sean $x, y \in G$ dos elementos tales que $x^n = y^n$ con $n \in \mathbb{N}_{\geq 1}$, y consideramos el subgrupo $H = \langle Z_{k-1}(G), x\rangle$. Por la Proposición II.14, el factor $G/Z_{k-1}(G)$ es abeliano. En consecuencia, dados $z \in G$ y $h \in H$ existe $m \in \mathbb{Z}$ tal que

$$(z^{-1}hz)Z_{k-1}(G) = (z^{-1}x^m z)Z_{k-1}(G) = x^m Z_{k-1}(G).$$

Así $z^{-1}hz \in x^m Z_{k-1}(G)$, y en consecuencia $z^{-1}hz \in H$. Por tanto, H es normal en G. Veamos que, además, H es nilpotente de clase a lo sumo $k-1$, es decir, que el $(k-1)$-ésimo término $Z_{k-1}(H)$ de la serie central superior de H coincide con H.

Demostramos primero por inducción que $Z_{k-1}(G)$ es un subgrupo de $Z_{k-1}(H)$, para lo que basta comprobar que es un subconjunto. Dado que $\{e\} = Z_0(G) = Z_0(H)$, el primer caso es una igualdad. Supongamos entonces que $a \in Z_i(G) = \{a \in G : \forall y \in G, [a, b] \in Z_{i-1}(G)\}$ para $i \leq k-1$, y veamos que $a \in Z_i(H)$. Por un lado, como $a \in Z_i(G)$, tenemos que $[a, b] \in Z_{i-1}(G)$ para todo $b \in G$. Dado $b \in H$, como además $a \in Z_i(G) \subseteq Z_{k-1}(G) \subseteq H$, el conmutador $[a, b] \in H$. Por hipótesis de inducción, $Z_{i-1}(G) \subseteq Z_{i-1}(H)$, así que entonces $[a, b] \in Z_{i-1}(H)$, y en consecuencia $a \in Z_i(H)$.

Ahora, usando el Teorema de Isomorfía, tenemos que

$$H/Z_{k-1}(H) \subseteq H/Z_{k-1}(G) \cong \langle xZ_{k-1}(G)\rangle,$$

y con ello $H/Z_{k-1}(H)$ es un grupo cíclico. Sin embargo, se puede comprobar que esto sólo es posible si $H = Z_{k-1}(H)$, por lo tanto H es nilpotente de grado a lo sumo $k-1$. Aplicando la hipótesis de inducción, H es un r-grupo. Tenemos ahora que

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

Por ser H normal, x e $y^{-1}xy$ son elementos de H. Como H es r-grupo, entonces son iguales, así que x e y conmutan. Usando el mismo argumento que si G es abeliano, concluimos que $x = y$.

Veamos ahora la segunda parte. Por ser G nilpotente, podemos tomar la serie central de longitud k anterior, si bien el resultado es cierto aunque la serie no sea finita. Probaremos que los factores G_i/G_{i-1} son abelianos y libres de torsión, y los cocientes G/G_i son r- grupos, para todo $1 \leq i \leq k$. Podemos asumir que el grupo $G_1 \cong G_1/G_0$ es el centro de G, y en consecuencia es un grupo abeliano y libre de torsión. Tenemos además que G/G_1 es r-grupo. En efecto, dados $x, y \in G$,

$$x^n G_1 = y^n G_1 \quad \Leftrightarrow \quad x^n y^{-n} \in G_1 \quad \Leftrightarrow \quad x^n y^{-n} = g = y^{-n}x^n$$

para cierto $g \in G_1 = Z(G)$. Tenemos así que

$$x^n = y^{-n}x^n y^n = (y^{-n}xy^n)^n,$$

luego, como G es r-grupo, $x = y^{-n}xy^n$. Repitiendo el proceso llegamos a $x = y^{-1}xy$, y entonces $(xy^{-1})^n \in G_1$. Así, dado $g \in G$, resulta $(xy^{-1})^n = g^{-1}(xy^{-1})^n g = (g^{-1}xy^{-1}g)^n$, y en consecuencia $xy^{-1} = g^{-1}xy^{-1}g$, luego $xy^{-1} \in G_1$. Con esto, probamos G/G_1 es r-grupo.

Empleando de nuevo inducción, sea $2 \leq j \leq k$ supongamos que G_{j-1}/G_{j-2} es también abeliano y libre de torsión, y que G/G_{j-1} es r-grupo. Asumimos de nuevo que G_j/G_{j-1} es el centro de G/G_{j-1}, que como consecuencia es abeliano, como centro, y libre de torsión, por la propiedad de r-grupo. Con un razonamiento análogo al caso $j = 1$, vemos que el cociente G/G_j es también r-grupo, con lo que queda finalizada la demostración. □

Concluimos la sección con el resultado principal de ordenabilidad.

Teorema II.22. *Un grupo G libre de torsión y localmente nilpotente es ordenable.*

Demostración. Consideramos un subgrupo H de G finitamente generado. Por hipótesis, es nilpotente y libre de torsión. En consecuencia, de acuerdo con el Lema II.21, posee una serie central superior de longitud finita, cuyos factores son libres de torsión. Aplicando el Teorema II.16 (1), H es ordenable. Así, todos los subgrupos finitamente generados de G son ordenables, y usando el el Teorema II.7, tenemos entonces que G es ordenable. □

II.4. Grupos libres

Pasamos a hablar ahora de otra familia de grupos en los que está garantizada la ordenabilidad: los grupos libres. La idea de grupo libre es la de un grupo generado por un conjunto A en cuya presentación no hay relaciones entre los elementos de A, más allá de las dadas por los axiomas de grupo. En otras palabras, dada una concatenación de elementos de A, $a = \prod a_i^{\epsilon_i}$ con $a_i \in A$, $\epsilon_i \in \{-1, 1\}$, las únicas simplificaciones posibles en la expresión de a serán omitir el elemento neutro, los pares consecutivos $a_i a_i^{-1}$ (y viceversa), y agrupar un mismo elemento repetido en potencias, usando la propiedad asociativa. Tratamos de plasmar esta idea con rigor a continuación.

Definición II.23. Sea A un conjunto, y denotemos por A^{-1} un conjunto disjunto y biyectable con A, de forma que para cada $x \in A$, denotamos por x^{-1} su correspondiente en A^{-1}, y análogamente, para cada $y \in A^{-1}$, denotamos por $y^{-1} \in A$ el elemento tal que su correspondiente es y. Sea $\{e\}$ un conjunto de un elemento disjunto de A y A^{-1}. Se define una **palabra** sobre A como una secuencia finita

$$a = \prod_{i=1}^{n} a_i,$$

donde el producto indica concatenación de elementos y $a_i \in A \cup A^{-1} \cup \{e\}$ para todo $1 \leq i \leq n$.

Nos interesa ahora reducir palabras en las que un elemento y su inverso aparezcan de forma consecutiva. Por ejemplo, de forma que la secuencia aa^{-1} coincida con e. Asumiremos que e coincide con todas sus potencias, y que la operación de e con cualquier otro elemento $a \in A \cup A^{-1}$ es a, por izquierda o derecha. Entonces, dada una palabra sobre A podemos realizar cancelaciones hasta obtener lo que llamamos forma reducida.

Definición II.24. Se dice que una palabra $a = \prod_{i=1}^{n} a_i$ sobre un conjunto A, de longitud n y distinta de la palabra vacía e, está en **forma reducida**, si se verifican las condiciones

(I) $a_i \neq e$ para todo $1 \leq i \leq n$.

(II) $a_{i+1} \neq a_i^{-1}$ para todo $1 \leq i \leq n-1$.

Con ello, se puede definir la operación $\star$ entre dos palabras en forma reducida como la forma reducida de su concatenación, cancelando los términos finales de la primera con los iniciales de la segunda, para obtener otra palabra en forma reducida sobre A. Por definición, la operación de concatenación es asociativa, y por tanto $\star$ también, y tiene a e como elemento neutro. Por otro lado, dado $a = \prod_{i=1}^{n} a_i$, encontramos que $a^{-1} := \prod_{i=n}^{1} a_i^{-1}$ es su un elemento inverso. En consecuencia, tenemos una estructura de grupo sobre la unión del conjunto de palabras en forma reducida y el elemento neutro. Esta estructura es única por construcción.

Definición II.25. Sea A un conjunto. Se dice que el conjunto de palabras en forma reducida sobre A, junto con la palabra vacía, dotado de la operación $\star$, es el **grupo libre** generado por A, y se denota $F(A)$.

Dado un homomorfismo de grupos de un grupo libre F en un grupo G, nos fijamos en que basta conocer la imagen de los elementos del conjunto generador de F para, por las propiedades de los homomorfismos de grupos, determinar la imagen de cualquier elemento de F. En otras palabras, cualquier aplicación de un conjunto A en un grupo G se extiende de manera única a un homomorfismo de grupos de $F(A)$ en G. Se conoce esta propiedad como la **propiedad universal** de los grupos libres, y es análoga a propiedades similares en otras ramas del álgebra, como el caso de una base de un espacio vectorial y una aplicación lineal definida sobre él.

Ejemplos.

1. El grupo libre F_0 generado por el conjunto vacío es el grupo trivial, ya que la única palabra posible es e.

2. El grupo libre F_1 generado por un elemento es el grupo cíclico infinito, y por tanto isomorfo a $(\mathbb{Z}, +)$. En efecto, por cancelación de a con a^{-1}, todas palabras en forma reducida son del tipo a^n con $n \in \mathbb{Z}$, tomando $a^0 := e$ y $a^n := (a^{-1})^{-n}$ cuando $n < 0$. Las potencias son todas diferentes por definición de grupo libre.

3. Los grupos libres generados por conjuntos de 2 o más elementos son grupos infinitos no abelianos. Por ejemplo, F_2 tiene dos generadores a, b, y por definición tenemos que $ab \neq ba$. No obstante, apreciamos que el cociente $F_2/\langle a\rangle_N$ sí es abeliano, ya que es isomorfo a $\langle b\rangle \cong \mathbb{Z}$, donde $\langle a\rangle_N$ es el subgrupo normal generado por a. En efecto, consideremos la aplicación dada por
$$\begin{array}{rccc} \pi_a : & F_2 & \longrightarrow & F_1 = \langle b\rangle \\ & a & \longmapsto & e \\ & b & \longmapsto & b \end{array} .$$
π_a es homomorfismo de grupos suprayectivo. Observamos que si consideramos un elemento $x = \prod_{i=1}^n x_i \in \ker \pi_a$, donde $x_i \in \{a, b, a^{-1}, b^{-1}\}$, su imagen es, por un lado, un elemento de $F_1 = \langle b\rangle$, y por tanto de la forma $\prod_{i=1}^k b^{\epsilon_i}$ con $\epsilon_i \in \{-1, 1\}$, y por otro igual al elemento neutro en F_1. Así, tiene que haber tantos factores b como b^{-1} en la expresión de x, y en consecuencia podemos escribir x como un elemento generado por potencias de a y sus conjugados por b. Usando un razonamiento similar al empleado para caracterizar un semigrupo normal en la Proposición II.2, se puede probar que $\langle a\rangle_N$ está generado por estos mismos elementos, y además $\langle a\rangle_N \subseteq \ker \pi_a$, de donde deducimos que son iguales. Concluimos el resultado aplicando el Teorema de Isomorfía.

Mostramos a continuación una idea análoga a la del punto 3 del ejemplo anterior se puede aplicar a un grupo libre cualquiera, incluso infinito, de forma que construimos una serie central inferior con factores abelianos y libres de torsión. Hemos seguido para ello el desarrollo de Jacobson [16], apoyándonos también en la prueba original de Magnus, dividida en [24] y [25]

Lema II.26 (W. Magnus [24, 25])**.** *Todo grupo libre posee una serie central inferior con factores libres de torsión*
$$F = F_1 \supseteq F_2 \supseteq ... \supseteq F_n \supseteq F_{n+1} \supseteq ... \supseteq F_\omega = \{e\},$$
siendo ω el primer ordinal infinito.

Demostración. Partimos de un grupo libre F, generado por el conjunto $\{a_i : i \in I\}$. Para cada a_i definimos la variable x_i, y consideramos el anillo $R = \mathbb{Z}\{\{x_1, x_2, ...\}\}$ de series formales dotado de la suma usual y un producto de convolución asociativo pero no conmutativo. Veamos que F es isomorfo al subgrupo de $(R \setminus \{0\}, \cdot)$ generado por los elementos $\alpha_i = 1 + x_i$, si se identifica cada generador a_i con α_i. Para ello, probemos que si $\prod_j \alpha_{i_j}^{k_j}$ es una palabra sobre el conjunto de generadores con $i_j \neq i_{j+1}$, entonces no es igual a 1. En otras palabras, ninguna expresión de ese tipo puede ser reducida. Para $k \in \mathbb{N}_{\geq 1}$, tenemos que
$$\alpha_i^k = (1 + x_i)^k = 1 + kx_i + \sum_{l=2}^{k} \binom{k}{l} x_i^l; \quad \alpha_i^{-k} = \Big((1 + x_i)^k\Big)^{-1} = 1 - kx_i + \binom{k}{2} x_i^2 + ...,$$
y en consecuencia, dado que R no es conmutativo y que índices consecutivos son diferentes, el término $\left(\prod_j k_j\right)\left(\prod_j x_{i_j}\right)$ no se cancela con ningún otro, y el producto nunca es igual a 1.

Consideramos ahora el ideal $\mathfrak{a}$ de las series de potencias sin término constante,

$$\mathfrak{a} = \bigcup_{i \in I} x_i R,$$

y para cada $n \in \mathbb{N}_{\geq 1}$, definimos el siguiente subconjunto de F:

$$F^{[n]} := \{\alpha \in F : \alpha - 1 \in \mathfrak{a}^n\}.$$

Observamos que, si $n = 1$, entonces $\alpha_i \in F^{[n]}$ para $i \in I$, y de hecho cualquier producto de los generadores α_i, por las características del grupo libre. Tenemos entonces que $F^{[1]} = F$. En general, notemos que los elementos de $F^{[n]}$ son de la forma $\alpha = 1 + \mu$, con $\mu \in \mathfrak{a}^n$. Dado un segundo $\nu \in \mathfrak{a}^n$, resulta

$$(1+\mu)(1+\nu)^{-1} = (1+\mu)\left(\sum_{i \in \mathbb{N}} (-1)^i \nu^i\right) = 1 + \mu - \nu \sum_{i \in \mathbb{N}} (-1)^i (\nu^i + \mu\nu^i) \in 1 + \mathfrak{a}^n,$$

así que $F^{[n]}$ es un subgrupo de F, que se conoce como subgrupo de F de dimensión n.

De modo similar, vemos que si $\alpha = 1 + \mu \in F^{[n]}$ y $\beta = 1 + \nu \in F^{[m]}$, entonces tenemos la siguiente expresión para su conmutador:

$$[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta = \sum_{i \in \mathbb{N}} \sum_{j \in \mathbb{N}} (-1)^{i+j} \mu^i \nu^j (1 + \mu + \nu + \mu\nu).$$

Se puede comprobar que los términos univariados se cancelan, y en consecuencia, se tiene que $[\alpha, \beta] - 1 \in (\mu\nu) \subseteq \mathfrak{a}^{n+m}$, es decir, $(\alpha, \beta) \in F^{[n+m]}$. Por lo tanto,

$$\left[F^{[n]}, F^{[m]}\right] \subseteq F^{[n+m]}$$

para todos $n, m \in \mathbb{N}_{\geq 1}$. Como consecuencia, y por ser $F^{[1]} = F$, todos los subgrupos $F^{[n]}$ son normales en F, por la Proposición II.11. Con ello, podemos definir $F_1 := F^{[1]} = F$ y recursivamente $F_n := [F_{n-1}, F]$ para cada $n \in \mathbb{N}_{\geq 2}$, y tenemos así una cadena $F = F_1 \supseteq F_2 \supseteq ...$, que es de hecho una serie central inferior transfinita, de acuerdo con la Definición II.12. Además, se sigue que $F_n \subseteq F^{[n]}$ para todo $n \in \mathbb{N}_{\geq 1}$, y dado que

$$\bigcap_{n \in \mathbb{N}_{\geq 1}} F^{[n]} = \{1\},$$

resulta $F_\omega = \{e\}$.

Para terminar, queda por probar que los factores F_n/F_{n+1} son libres de torsión para todo $n \in \mathbb{N}_{\geq 1}$. Junto con lo anterior, se puede probar que, de hecho, se tiene la igualdad $F_n = F^{[n]}$. Omitimos la prueba completa porque es bastante técnica, y se apoya en resultados previos que extenderían más de lo deseado esta demostración. De forma similar a la idea anterior, en este caso se basa en la construcción de un pseudo-anillo en el que el producto no es asociativo, y el uso de argumentos de pertenencia a ideales para ver que el homomorfismo de paso al cociente $F^{[n]} \to F^{[n]}/F_n$ es la aplicación nula [25].

Con ello, basta comprobar que los factores $F^{[n]}/F^{[n+1]}$ son libres de torsión. Sea así $\alpha \in F^{[n]} \setminus F^{[n+1]}$, es decir, distinto del neutro en el grupo cociente, y $k \in \mathbb{N}_{\geq 1}$. Veremos que $\alpha^k \notin F^{[n+1]}$. Por definición de $F^{[n]}$, podemos escribir $\alpha = 1 + \mu = 1 + \mu_n + \hat{\mu}$, donde $\mu \in \mathfrak{a}^n$ se puede descomponer en $\mu_n \in \mathfrak{a}^n \setminus \mathfrak{a}^{n+1}$ y $\hat{\mu} \in \mathfrak{a}^{n+1}$, con $\mu_n \neq 0$ por ser $a \notin F^{[n+1]}$. Expresado de otro modo, μ_n acumula los términos de grado n en las variables x_i, y $\hat{\mu}$ los de grado $n+1$ o mayor. Con ello, se expresa

$$\begin{aligned}\alpha^k = (1 + \mu_n + \hat{\mu})^k &= (1+\mu_n)^k + \hat{\mu} \sum_{j=1}^{k} \binom{k}{j} (1+\mu_n)^{k-j} \hat{\mu}^{j-1} \\ &= 1 + k\mu_n + \mu_n^2 \sum_{j=2}^{k} \binom{k}{j} \mu_n^{j-2} + \hat{\mu} \sum_{j=1}^{k} \binom{k}{j} (1+\mu_n)^{k-j} \hat{\mu}^{j-1} \in (1 + k\mu_n) + \mathfrak{a}^{n+1},\end{aligned}$$

de donde se deduce que $(\alpha^k - 1) + \mathfrak{a}^{n+1} = k\mu_n + \mathfrak{a}^{n+1}$, que es distinto de 0 por ser $\mu_n \neq 0$ una serie formal de grado n con coeficientes en $\mathbb{Z}$. En consecuencia, $\alpha^k - 1 \notin \mathfrak{a}^{n+1}$, y tenemos el resultado. □

Con ello, tenemos el siguiente enunciado.

Teorema II.27. *Un grupo libre es ordenable.*

Demostración. Dado un grupo libre F, por el Lema II.26, tenemos que F tiene una serie central inferior $\{C_\tau\}_{\tau\in\Omega}$ con factores libres de torsión y de forma que $C_\omega = \{e\}$ para un $\omega \in \Omega$. Entonces, aplicando el Teorema II.16 (2), resulta que F es ordenable. □

El último resultado de esta sección proporciona una descripción de cualquier grupo totalmente ordenado mediante como la imagen de un grupo libre por un o-epimorfismo. Para probarlo, necesitamos introducir antes el concepto de presentación de un grupo.

Las presentaciones suponen una forma útil e intuituiva de describir un grupo [6]. En general, dado un grupo $(G, \cdot)$, podemos escoger un subconjunto $A \subseteq G$ de forma que cualquier $g \in G$ se puede escribir como producto finito de elementos de A y sus inversos. Se dice entonces que los elementos de A son generadores. Alternativamente, podemos encontrar ecuaciones que verifican todos los generadores de G, llamadas relaciones. Por ejemplo, si $G = (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, +)$, tenemos que $a = (1, 0)$ y $b = (0, 1)$ son generadores, y se dan las relaciones $a^3 = e$, $b^3 = e$, $ab = ba$. En este caso, todas las relaciones entre elementos de G se derivan de estas tres, y se escribe

$$G = \langle a, b \mid a^3, b^3, aba^{-1}b^{-1}\rangle,$$

donde se omite la igualdad con el neutro en las relaciones.

La descripción formal de la presentación de un grupo se basa en los grupos libres. De acuerdo con la propiedad universal, toda aplicación de un conjunto A en un grupo G se extiende de manera única a un homomorfismo de grupos de $F(A)$ en G. Si A es un conjunto de generadores de G, entonces la aplicación $\iota : A \hookrightarrow G$ determina un epimorfismo de $F(A)$ en G.

Definición II.28. Sean G un grupo y A un subconjunto de G tal que $G = \langle A\rangle$.

(I) Una **presentación** de G es un par (A, R), de modo que R es un conjunto de palabras de $F(A)$ tal que el subgrupo normal $\langle R\rangle_N$ que genera es el núcleo del homomorfismo $\pi : F(A) \to G$ que extiende la inclusión $\iota : A \hookrightarrow G$. Se conocen los elementos de A como **generadores** y los de R como **relaciones**.

(II) Se dice que G es de **generación finita** si admite una presentación (A, R) con A finito, y de **presentación finita** si admite una presentación (A, R) con A y R finitos.

Se denota en general $G = \langle A \mid R\rangle$.

Por el Teorema de Isomorfía, observamos que

$$G = \operatorname{Im}\, \pi \cong F(A)/\ker \pi.$$

Así, tenemos que $\langle A \mid R\rangle = F(A)/\langle R\rangle_N$ para cualquier presentación. Deducimos que todo grupo G admite una presentación: basta tomar G como conjunto generador y las relaciones dadas por $\ker \pi \subseteq F(G)$, y tenemos entonces $G = \langle G \mid \ker \pi\rangle$.

Tras este desarrollo, estamos en condiciones de enunciar el resultado mencionado respecto de los grupos ordenados.

Teorema II.29 (K. Iwasawa [15])**.** *Todo grupo totalmente ordenado es la imagen por un o-epimorfismo de un grupo libre.*

Demostración. Consideramos un grupo ordenado G, y la presentación $G = \langle A, R\rangle \cong F(A)/N$, donde $N := \langle R\rangle_N$ es el subgrupo normal generado por R. Así, podemos considerar el cociente $F(A)/N$ con el orden de G.

Por el Teorema II.27, $F(A)$ es ordenable y, entonces, podemos dotar a N de un orden cuyo cono positivo sea invariante por automorfismos internos de $F(A)$. Estamos con ello en condiciones de aplicar el Lema 4.11, y concluir que el orden sobre N se extiende al orden sobre $F(A)$ de tal forma que el orden inducido en el cociente $F(A)/N$ coincide con el dado por el isomorfismo con G. En consecuencia, $\pi : F(A) \to F(A)/N \cong_o G$ es un o-epimorfismo. □

Índice alfabético

anillo
  de valoración, 49
  local, 49
arquimediana
  clase, 26, 32, 42
  equivalencia, 26
  propiedad, 14, 26
automorfismo interno, 22, 29

bucle, 3
  arquimediano, 14, 15, 17
  asociativo para potencias, 14, 17
  cociente, 8, 10
  ordenable, 4
  ordenado, 4, 8, 14

cadena (de subgrupos), 29
conmutador, 57
  de subgrupos, 57
cuerpo
  de Hahn, 40
  diferencial, 50
  ordenado, 50
  residual, 49
  valorado, 49

Dedekind, corte de, 17
derivación, ley de, 50

envolvente divisible, 12, 42
extensión lexicográfica, 22

factor, 33
familia (de subgrupos)
  completa, 29
  subinvariante, 29, 34

grupo
  arquimediano, 14, 17
  de Hahn, 37, 42
  divisible, 12, 41
  libre, 62, 65
  libre de torsión, 11, 12, 22, 61
  localmente nilpotente, 60
  nilpotente, 60
  ordenable, 4, 22, 34, 56, 59, 65
  ordenado, 4, 9, 11, 36, 42
  resoluble, 36

homomorfismo de bucles ordenados, 10

magma, 3
  unitario, 3

nilpotencia, clase de, 60

orden, 7, 51
  arquimediano, 14
  buen, 51
  dual, 7
  parcial, 54
  total, 51, 54, 55
ordinal, 51

palabra (grupo libre), 62
  forma reducida, 62
positivo
  cono, 4, 7, 8
  elemento, 4
presentación de grupos, 65
producto
  directo de grupos, 19
  lexicográfico de grupos, 21, 26

salto (de subgrupos), 30, 35
semigrupo normal, 54
serie
  central, 57, 60
    inferior, 57, 63
    superior, 58
  normal, 36
series
  de Laurent, 40, 47
  de Puiseux, 40, 45
  formales de potencias, 40
  reticuladas, 48
soporte, 20
subbucle, 8
  convexo, 10, 15
  normal, 8, 10
subconjunto
  convexo, 9
  normal, 7
  reticulado, 47
subgrupo
  conjugado, 29
  convexo, 26, 32, 35, 36
  finitamente generado, 56, 60

torre
  normal, 36

valor absoluto, 26
valoración, 32
  de cuerpos, 48
  de grupos, 27
  diferencial, 50
  natural, 28, 49

Bibliografía

[1] Banaschewski B. (1957), "Total geordnete Moduln", *Arch. Math.* **7**, 430-440.

[2] Bruck R. H. (1971), *A Survey of Binary Systems*, Springer Verlag.

[3] Cano J. (1995), "The Puiseux theorem for differential equations", *Singularity theory (Trieste, 1991)*, 128-152, *World Sci. Publ., River Edge.*

[4] Clifford A. H. (1954), "Note on Hahn's theorem on ordered abelian groups", *Proc. Amer. Math. Soc.* **5**, 499-504.

[5] Dedekind R. (1901), *Essays on the Theory of Numbers*, The Open Court Publishing Company, 12-15.

[6] Dummit D. S., Foote R. M. (2003), *Abstract Algebra*, John Wiley & Sons.

[7] Ehrlich P. (1995), "Hahn's *Über die nichtarchimedischen Größensysteme* and the development of the modern theory of magnitudes and numbers to measure them", *From Dedekind to Gödel: essays on the development of the foundations of mathematics*, Springer Verlag, 165-213.

[8] Fuchs L. (1959), "Note on ordered groups and rings", *Fund. Math.* **46**, 167-174.

[9] Fuchs L., Salce L. (2001), *Modules over Non-Noetherian Domains*, Mathematical Surveys and Monographs, 84. Americal Mathematical Society.

[10] Grigoriev D., Singer M. F. (1991), "Solving ordinary differential equations in terms of series with real exponents", *Tran. Amer. Math. Soc.* **327** (1), 329-351.

[11] Hahn H. (1907), "Über die nichtarchimedischen Größensysteme", *S.-B. Akad. Wiss. Wien, math.-naturw. Kl.* **116** (Abt. IIa), 601-655.

[12] Hausdorff F. (1914), *Grundzüge der Mengenlehre*, Veit and Comp. Leipzig, 194-209.

[13] Hölder O. (1901), "Die Axiome der Quantität und die Lehre vom Maß", *Ber. Verh. Kgl. sachs. Ges. Wiss. Leipzig, math.-phys. Kl* **53**, 1-64.

[14] Iseki K. (1951), "Structure of special ordered loops", *Portugal. Math.*, **10** (2), 81-83.

[15] Iwasawa K. (1948), "On linearly ordered groups", *J. Math. Soc. Japan* **1**, 1-9.

[16] Jacobson N. (1992), "Magnus' method in theory of free groups", *Ulam Quart.*, **1** (1), 1-3.

[17] Jech T. (1978), *Set Theory. Pure and Applied Mathematics*, Academic Press, 19-20, 39.

[18] Kaplansky I. (1942), "Maximal fields with valuations", *Duke Math. J.* **9**, 303-321.

[19] Kokorin A. I. (1966), "Γ-fully orderable and relatively convex subgroups of orderable groups", *Sibirsk. Math. Ž* **7**, 713-717.

[20] Kurosch A. G. (1970), *Gruppentheorie I*, Akademie Verlag.

[21] Kurosch A. G. (1972), *Gruppentheorie II*, Akademie Verlag.

[22] Levi F. W. (1913), "Arithmetische Gesetze im Gebiete diskreter Gruppen", *Rend. Circ. Math. Palermo* **35**, 225-236.

[23] Levi F. W. (1943), "Contributions to the theory of ordered groups", *Proc. Indian Acad. Sci. Sect. A* **17**, 199-201.

[24] Magnus W. (1935) “Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring”, *Math. Ann.* **111** (1), 259-280.

[25] Magnus W. (1937), “Über Beziehungen zwischen höheren Kommutatoren”, *J. Reine Angew. Math.* **177**, 105-115.

[26] Matusinski M. (2014) “On generalized series fields and exponential-logarithmic series fields with derivations”, Valuation theory in interaction, 350–372. EMS Ser. Congr. Rep., Eur. Math. Soc., Zürich.

[27] Matusinski M. (2020), Séries formelles et méthodes trasncendantes en géométrie modérée, thèse d’habilitation, Université de Bordeaux.

[28] Neumann B. H. (1949), “On ordered groups”, *Amer. J. Math.* **71**, 1-18.

[29] Pickert G. (1955), *Projektive Ebenen*, Springer Verlag.

[30] Prieß-Crampe S. (1983), *Angeordnete Strukturen. Gruppen, Körper, projektive Ebenen*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 98. Springer Verlag.

[31] Puiseux V. A. (1850), “Recherches sur les fonctions algébriques”, *J. Math. Pures Appl.*, **15**, 365-480.

[32] Ribenboim P. (1999), *The Theory of Classical Valuations*, Springer Monographs in Mathematics. Springer Verlag, 3, 13-16.

[33] Russell B. (1903), *The Principles of Mathematics*, Cambridge University Press, 199-226.

[34] Sklifos P. I. (1970), “Ordered loops”, *Algebra i Logika*, **9**, 714-730.

[35] Smith D. E. (2006), *History of Modern Mathematics*, Mathematical Monographs No. I. Leopold Classic Library.

[36] Stolz O. (1883), ”Zur Geometrie der Alten, insbesondere über ein Axiom des Archimedes”, *Math. Ann.* **22** (4), 504-519.

[37] van der Hoeven J. (1997), Asymptotique automatique, Ph.D. Thesis, Université Paris VII, Paris.