UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

TEORÍA DE GALOIS Y HACES PRINCIPALES CUÁNTICOS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

P R E S E N T A:

FRANCISCO JAVIER ZÚÑIGA GÓNGORA

DIRECTOR DE TESIS:
DR. MICHO DURDEVICH LUCICH

Ciudad Universitaria, Cd. Mx. **2015**

1. Datos del alumno
Zúñiga
Góngora
Francisco Javier
56883138
Universidad Nacional Autónoma de México
Facultad de Ciencias Carrera
408020521

2. Datos del tutor
Dr
Micho
Durdevich
Lucich

3. Datos del sinodal 1
Dr
Adolfo
Sanchez
Valenzuela

4.Datos del sinodal 2
Dr.
Steven Bruce
Sontz

5. Datos del sinodal 3
Dr.
Carlos
Villegas
Blas

6. Datos del sinodal 4
Dr.
Raymundo
Bautista
Ramos

7. Datos del trabajo escrito
Teoría de Galois y Haces Principales Cuánticos
81 p.
2016

Índice general

Introducción

Es la intención de esta tesis exponer, en primer lugar, cómo 3 teorías que pertenecen a marcos teóricos distintos (la teoría de Galois a la teoría de grupos y campos, los haces principales a la geometría diferencial y la geometría cuántica al análisis funcional) se encuentran en una estructura matemática, el Haz Principal Cuántico. En segundo lugar que este trabajo sirva como una exposición introductoria a estas teorías para otros estudiantes de los últimos semestres de la licenciatura en matemáticas; resaltaremos la parte intuitiva, usando razonamientos analógicos, sobre la parte técnica (que intentaré dejar en lo esencial). Esta tesis es un ejercicio de la madurez matemática que desarrollé durante mis estudios en la facultad de ciencias de la UNAM: familiaridad con la abstracción y la apreciación de su complejidad y propia sustancia, ver la unidad de fenómenos distintos como manifestaciones de un mismo principio, el uso del lenguaje técnico como herramienta del pensamiento nítido y, en particular, un camino a la expansión de la intuición geométrica. A su vez es el testimonio de mis primeras exploraciones en la mayor parte de los temas expuestos y un vistazo a horizontes teóricos de gran interés que me fueron presentados por mi asesor, maestro y amigo Micho Durdevich.

Las discusiones técnicas de este trabajo presuponen conceptos y definiciones elementales del álgebra (números complejos, campo y grado de un campo, polinomios y grado de un polinomio, factorización, operaciones con polinomios, isomorfismos, grupos de matrices, generadores, anillo y módulo), de la topología (compacidad, conexidad, transformaciones continuas, homeomorfismos) y de la geometría diferencial (estructura diferencial en una variedad, difeomorfismos, diferencial y pushforward de un mapeo, campos vectoriales). Hablaremos de *transformaciones* entre *espacios* y de

espacios cociente, que dependiendo del contexto se refieren a las correspondientes estructuras. A este respecto: los conceptos de *categoría* y *funtor* juegan un papel clave, aunque no central, pues permean implícitamente todo el trabajo. A nivel intuitivo una categoría es un espacio discursivo de flechas y puntos (transformaciones continuas y espacios topológicos, variedades suaves y mapeos suaves, $*$-homomorfismos y álgebras C*) y un funtor es un *mecanismo de traducción* de una categoría a otra.

He dividido esta tesis en 4 capítulos relativamente independientes, aunque su composición fue diseñada para leerse de forma lineal. En el primer capítulo elaboramos la Teoría de Galois hasta la demostración de su teorema fundamental. El tema de las simetrías se trata al principio del segundo capítulo, dedicado a los haces. En el tercer capítulo presuponemos los fundamentos formales de la geometría cuántica en el análisis funcional, cuyas herramientas y marco teórico componen la teoría, pues el tema es vasto y resulta excesivo para el enfoque de la tesis. El último capítulo es dependiente de los demás e introduce los haces principales cuánticos con la intención de amalgamar lo expuesto en los capítulos anteriores.

Para dar fluidez al texto, y por preferencia personal, he omitido el esquema de «teorema, demostración y definición». En su lugar los conceptos que aparecen en **negritas** serán definidos o demostrados en el transcurso del párrafo. Los conceptos en *cursivas* son aquellos cuyo significado es contextual e intuitivo, será señalado más adelante en el texto o refiere a una definición estándar en la literatura del tema.

Capítulo 1

Teoría de Galois

Evariste Galois (1811-1832) logró resolver, antes de su trágica muerte a los 20 años, el problema de encontrar una fórmula general, en término de ciertas operaciones aritméticas, que nos permitiera calcular las raíces de polinomios de grado mayor o igual a 5. Sus trabajos en la teoría de ecuaciones resultaron indescifrables para la academia y durante su encarcelamiento por activismo político se dedico a pulir sus ideas; no fue sino hasta años después de su muerte que serían, gracias a amigos que insistieron en su divulgación, cabalmente reconocidas. Para esos tiempos se tenía ya las correspondientes fórmulas para los grados 2, 3 y 4, en las que se usan solamente las operaciones de producto, suma y toma de radicales, que geométricamente corresponden a la *constructibilidad* de la solución. La imposibilidad de este tipo de solución para los polinomios de grado 5 fue probada independientemente por Niels Henrik Abel, y este resultado es conocido como el **teorema de Abel-Ruffini**.

Los profundos resultados de Galois, anteriores a estos últimos, tuvieron a este teorema como consecuencia, además de demostrar lo mismo para grados mayores en un mismo movimiento. Galois fue el primero en utilizar el concepto de *grupo* al referirse a la *estructura algebráica* de las permutaciones de las raíces de un polinomio. En el lenguaje actual hablamos de un *grupo* (de automorfismos) que *actúa* sobre el *campo de descomposición* del polinomio. Su trabajo constituye un antecedente histórico al programa de Erlangen en el que se caracteriza a los grupos cómo conjuntos de *si-*

metrías y a la *simetría* como concepto fundamental de la *geometría*. En este sentido la teoría de Galois, en su forma moderna, constituye la descripción de una *geometría de ecuaciones* desarrollada en el lenguaje de teoría de campos y extensiones. En este capítulo vamos a exponer dicho lenguaje, que nos permitirá expresar las relaciones entre la extensión de un campo y las raíces de un polinomio, sus respectivos *tamaños* y las simetrías que los unifican.

A lo largo del capítulo trabajaremos con un campo abstracto F, que en el marco de esta tesis nos basta pensar como $\mathbb{R}$ o $\mathbb{C}$.

1.1. Extensiones Finitas y Extensiones Algebráicas

Consideremos un campo F y el espacio de polinomios en una variable con coeficientes en este campo, que se denota por $F[x] := \{a_n x^n + a_{n-1}x^{n-1} ... + a_1 x + a_0 \mid n \in \mathbb{N},\ a_i \in F, a_n \neq 0\}$. Para $f(x) = a_n x^n + a_{n-1}x^{n-1} ... + a_1 x + a_0 \in F[x]$ se define $n \in \mathbb{N}$ como el **grado del polinomio** $f(x)$. El problema fundamental al trabajar con polinomios se reduce a la búsqueda de sus raíces, al campo (de *extensión*) donde estas viven y su relación con el campo de coeficientes F que llamamos **campo base**.

Si tenemos un polinomio $f(x) \in F[x]$ de grado n y una raíz $a \in F$ entonces el polinomio puede ser escrito como $f(x) = (x - a)h(x)$ donde $h(x)$ tiene grado $n - 1$. Notamos entonces una relación entre la factorización y las raíces: la existencia de raíces garantiza una factorización en $F[x]$. Por lo anterior, dicho polinomio $f(x)$ puede tener a lo más n raíces distintas. Una noción fundamental es la de **polinomio irreducible**: un polinomio $p(x) \in F[x]$ es irreducible si no se puede factorizar como producto de 2 o más polinomios de grado ≥ 1. Estos son los elementos atómicos de $F[x]$ o en otras palabras los *polinomios primos*, en el sentido de que todo polinomio se puede factorizar en un producto de polinomios irreducibles [10]. Notamos inmediatamente que los polinomios de grado 1 son siempre irreducibles y que un polinomio irreducible de grado ≥ 2 no tiene raíces en F.

Consideremos la factorización del polinomio $(x^2+1) \in \mathbb{R}[x]$: $(x-i)(x+i)$. Esta factorización está realizada en $\mathbb{C}[x]$ donde decimos que el polinomio es **reducible**, pero limitando nuestra atención a $\mathbb{R}[x]$, donde no existe el coeficiente imaginario de los polinomios $x \pm i$, el polinomio es entonces irreducible; fue necesario ir más allá del campo base dado. La noción de irreducibilidad depende íntimamente del campo base. Decimos que un campo E es una **extensión** del campo F si lo contiene como subcampo, simbólicamente $E \geq F$. En el contexto de este trabajo denotamos a una extensión E de F como E/F.

Una primer pieza fundamental de esta teoría es el **teorema de Kroenecker** que nos dice que para todo polinomio $f(x) \in F[x]$ existe una extensión E/F donde este polinomio tiene una raíz. Para encontrarla factorizamos $f(x)$ en irreducibles y construimos una extensión donde alguno de sus factores, digamos $p(x)$, tenga una raíz. La construcción de dicha extensión es muy simple: realizamos el cociente de $F[x]$ por el ideal generado por este polinomio irreducible, que denotamos $< p(x) >$. Resulta que todo polinomio irreducible genera un ideal maximal, cuyos cocientes en anillos conmutativos con unidad resultan en un campo [10]. Definimos entonces la extensión como el cociente $E = F[x]/ < p(x) >$. Nuestro campo base F posee una imagen isomorfa en E bajo la proyección canónica $\pi : F[x] \longrightarrow F[x]/ < p(x) >= E$, viendo a $F \subseteq F[x]$ como el conjunto de polinomios de grado 0. Así tenemos que E es una extensión de F y además

$$p(\xi) = p(x+ < p(x) >) = p(x)+ < p(x) >= 0 \text{ en } E$$

por lo que el elemento $\xi = \pi(x) = x+ < p(x) > \in E$ es una raíz de $p(x)$, entendiendo a x como una variable en E. $\square$

Dada una extensión E/F podemos considerar la dimensión de E como espacio vectorial sobre F, a esta cantidad le llamamos **grado de la extensión** y denotamos por $[E : F]$, en el caso de que la dimensión sea finita (que es el que nos concierne) se dice que se tiene una **extensión finita** E/F. Para la extensión $E = F[x]/ < p(x) >$ que acabamos de construir, el grado de E/F se corresponde con el grado del polinomio $p(x)$. Para verlo supongamos que $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ es irreducible;

podemos interpretar al cociente por $< p(x) >$ como la identificación del polinomio $p(x)$ con el cero, haciendo cero a todo polinomio que lo tenga como factor (es decir a todo $< p(x) >$), esto es $a_0 + a_1x + a_2x^2 + ... + a_nx^n = 0$, que reescribimos como

$$x^n = b_0 + b_1x + b_2x^2 + ... + b_{n-1}x^{n-1}, \text{ donde } b_i = -a_i/a_n$$

La ecuación anterior nos permite reducir cualquier polinomio a un representante de grado $\leq n-1$, visto como elementos de E. En otras palabras: cada clase lateral en E, de la forma, $f(x)+ < p(x) >$, contiene un representante de grado $< n$, pues para cada polinomio $f(x)$ podemos realizar el algoritmo de la división sobre $p(x)$ en $F[x]$ que nos dice que $f(x) = a(x)p(x) + b(x)$ con grado$(b(x)) <$ grado$(p(x))= n$, siendo $b(x)$ el representante en cuestión. Las operaciones en E están dadas por la suma y producto de polinomios *módulo* p(x), lo que permite la existencia de inversos a pesar de su inexistencia en general en $F[x]$. Todo esto implica que la imagen del conjunto $\{1, x, ..., x^{n-1}\}$ bajo la proyección π genera a todo E, de modo que si escribimos $\xi = \pi(x) = x+ < p(x) >$ se tiene que E es generado por $\{1, \xi, ..., \xi^{n-1}\}$. Este conjunto es linealmente independiente, y en consecuencia una base: de otra forma podríamos construir un polinomio en $F[x]$ de grado menor que $n =$grado$(p(x))$, digamos $h(x)$, con ξ como raíz. Esto lo hacemos usando los coeficientes de una combinación lineal que muestre la dependencia lineal. Luego, el algoritmo de la división aplicado a $p(x)$ y $h(x)$ nos dice que $p(x) = a(x)h(x) + b_0(x)$, con grado$(b_0(x))<$grado$(h(x))< n$, expresión que al evaluarse en ξ nos da $b_0(\xi) = 0$. Luego aplicando nuevamente el algoritmo de la división a $p(x)$ y $b_0(x)$ obtenemos $b_1(x)$ con $b_1(\xi) = 0$ y cuyo grado es menor al de $b_0(x)$. Este proceso nos da por inducción una cadena infinita descendente de naturales, dada por los grados de los consecutivos polinomios $b_i(x),\ i \in \mathbb{N}$, y por tanto una contradicción. Esto demuestra que $\{1, \xi, ..., \xi^{n-1}\}$ es una base y que $p(x)$ es el polinomio de menor grado que tiene a ξ como raíz. Esta demostración nos servirá más adelante para definir *el polinomio mínimo asociado a un elemento de la extensión*. A su vez notamos que bajo esta construcción se tiene que

$$[E : F] = n$$

Un resultado importante y sencillo dice que si tenemos extensiones finitas en cadena $E/L/F$ (es decir $E \geq L \geq F$) entonces $[E : F] = [E : L][L : F]$. Decimos

que L es un **campo intermedio** de la extensión finita E/F. La demostración es un simple conteo al expresar los elementos de cada espacio en términos de una base. Por inducción este resultado se extiende a cualquier cadena finita de extensiones finitas $F_n/F_{n-1}, ..., F_2/F_1$ resultando en: $[F_n, F_1] = [F_n, F_{n-1}]...[F_2, F_1]$.

Si tenemos una extensión E/F y un elemento $\alpha \in E$ podemos considerar al campo mínimo que contenga tanto a F como a α, que denotamos por $F(\alpha)$. Esta es una extensión de F contenida en E, lo que es decir que se trata de un campo intermedio de la extensión E/F, y toda extensión de este tipo (obtenida a partir de la *adjunción* de un elemento) es llamada **extensión simple**. Resulta que si $\alpha \in E$ es raíz de un polinomio irreducible sobre F, entonces $F(\alpha)$ es isomorfo a la extensión que encontramos en la prueba del teorema de Kroenecker, es decir

$$F(\alpha) = F[x]/ < p(x) >$$

esto implica en particular que cualquier raíz de $p(x)$ es algebráicamente indistinguible de las demás, en el sentido de que producen extensiones isomorfas. Esto tiene que ver con el hecho más general de que un isomorfismo de campos $\varphi : F \longrightarrow F'$ induce a su vez un isomorfismo $\varphi* : F[x] \longrightarrow F'[x]$ de los correspondientes anillos de polinomios, actuando en cada polinomio coeficiente a coeficiente, que se restringe a un isomorfismo de $< p(x) >$ con el ideal $< \varphi * (p(x)) = p'(x) >$, de modo que los correspondientes espacios cociente son también isomorfos. Entonces para una raíz α de $p(x)$ y una raíz β de $p'(x)$ podemos extender φ a un isomorfismo $\tau : F(\alpha) \longrightarrow F'(\beta)$, incluido el caso en que $F' = F$ y $\varphi = Id_F$, que nos dice ya que las distintas raíces de un mismo polinomio nos dan extensiones isomorfas.

La discusión anterior nos lleva al siguiente concepto: decimos que $\alpha \in E/F$ es un **elemento algebráico** sobre F si existe un polinomio en $F[x]$ que lo tenga como raíz. Una **extensión algebráica** es aquella en que todos sus elementos son algebráicos. En este respecto hay una proposición útil que nos dice que a todo $\alpha \in E$ algebráico sobre F es posible asociarle un único polinomio irreducible **mónico** (es decir, con su coeficiente de mayor grado igual a 1) denotado por $m_{\alpha,F}(x)$ y que llamamos el **polinomio mínimo** de α en $F[x]$ [5]. Esto es intuitivamente claro, pues si α es raíz

de un polinomio en $F[x]$ entonces es raíz de alguno de sus factores irreducibles, el cual queda caracterizado módulo una constante (gracias al algoritmo de la división y el argumento del descenso infinito usado anteriormente). Colapsamos esta última *libertad* al exigir que el polinomio sea mónico. Todo polinomio en $F[x]$ que tenga a α como raíz tendrá a $m_{\alpha,F}(x)$ como factor (irreducible). Entonces tenemos que para todo elemento $\alpha \in E$ algebráico sobre F se cumple

$$F(\alpha) = F[x]/ < m_{\alpha,F}(x) >$$

Aún más, para $\alpha \in E$ con E/F finita, de grado n, el conjunto $\{1, \alpha^1, ..., \alpha^n\}$ es linealmente dependiente sobre F por tener $n+1$ elementos, lo que nos dice que existen coeficientes b_i no todos cero tales que

$$b_0 + b_1\alpha + ... + b_n\alpha^n = 0$$

de modo que $\alpha \in E$ es algebráico. Hemos probado que toda extensión finita es algebráica. A su vez tenemos que para una extensión arbitraria E/F si $\alpha \in E$ es algebráico entonces $F(a)/F$ es una extensión finita cuyo grado es el grado de $m_{\alpha,F}(x)$.

Por otro lado el conjunto de elementos algebráicos de una extensión E/F (arbitraria) forman un campo: para $\alpha, \beta \in E$ elementos algebráicos distintos de cero, los elementos $\alpha\beta, \alpha \pm \beta$ y α/β son algebráicos también pues forman parte de la extension $F(\alpha, \beta) := F(\alpha)(\beta)$ finita, que por lo visto anteriormente es algebráica. Hemos de notar que del grado de la extensión $[F(\alpha, \beta), F]$ está acotado por el producto de los grados de los correspondientes elementos $\alpha, \beta \in E$. En general podemos construir para un conjunto finito $\{\alpha_i\}$ de elementos de E/F la extensión $F(\alpha_0, \alpha_1, ..., \alpha_n)$ que resulta finita por inducción pues la adjunción de cada elemento algebráico nos da una extensión finita acotada por el grado de su polinomio mínimo, se tiene incluso el converso de esta afirmación: Si una extensión es finita entonces es generada por la adjunción de un número finito de elementos algebráicos [5].

1.2. Campo de Descomposición y Extensiones Separables

El teorema de Kroenecker nos permite encontrar para cada polinomio $f(x) \in F[x]$ una extensión de F en la cual podemos expresarlo como producto de polinomios lineales: en la demostración del teorema construimos $E_0 = F(\xi) \geq F$ de modo que $f(x) = (x - \xi)f_1(x)$ donde ξ es una raíz de $f(x)$, luego si $f_1(x)$ se expresa como producto de polinomios lineales entonces hemos acabado, de otra forma factorizamos el polinomio en polinomios irreducibles y realizamos el proceso nuevamente, construyendo una extensión E_1 donde algún factor irreducible no lineal tenga una raíz. Esto nos da un algoritmo en cadena, descendente sobre el grado del polinomio inicial, que después de un número finito de pasos nos lleva a una extensión donde el polinomio se *descompone* en polinomios lineales. A esta extensión se le llama el **campo de descomposición** del polinomio f(x). En este caso el grado de la extensión está acotado por el producto de los grados de los factores irreducibles no lineales, por lo visto en el párrafo anterior.

Podemos extender cualquier isomorfismo entre campos a un isomorfismo entre las correspondientes extensiones de descomposición pues sabemos que la adjunción de cada raíz nos da un isomorfismo entre las correspondientes extensiones simples, así que podemos hablar de EL campo de descomposición (salvo isomorfismo) del polinomio $f(x) \in F[x]$ [5].

Un resultado importante dependiente del lema de Zorn es la existencia, para todo campo F, de una **cerradura algebráica** (denotada por $\overline{F}$)[10]. La cerradura algebráica de F es un campo **algebráicamente cerrado**, es decir que contiene todas las raíces de los polinomios con coeficientes en el mismo campo, que contiene a F. Su construcción equivale a la extensión *sucesiva* del campo base al campo de descomposición de cada polinomio en $F[x]$. Es por la imposibilidad de llevar cuenta de todas estas extensiones por las que el lema de Zorn es necesario para garantizar su existencia para cualquier campo. Siempre que trabajamos con raíces de polinomios podemos suponer que estamos manipulando elementos en la cerradura algebráica en

la cual tiene lugar nuestro discurso.

Sea $f(x) \in F[x]$; sobre su campo de descomposición podemos construir una expresión de la forma

$$f(x) = \alpha_0(x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}...(x-\alpha_k)^{n_k}$$

donde $\alpha_0 \in F$ y $\alpha_1, \alpha_2, ..., \alpha_k$ son elementos distintos del campo de descomposición que corresponden a las raíces del polinomio (de modo que el campo de descomposición es justamente $F(\alpha_1, ..., \alpha_k)$). Decimos que α_i es una *raíz múltiple* si $n_i > 1$ y *raíz simple* si $n_i = 1$.

Decimos que tenemos un **polinomio separable** si todas sus raíces son simples. Tenemos un método eficiente para saber si un polinomio es o no separable: $f(x)$ tiene una raíz múltiple α si y sólo si $m_{\alpha,F}(x)$ divide a $f(x)$ y $Df(x)$, donde $Df(x)$ es la derivada de $f(x)$ [5]. La derivada puede ser definida, en este contexto polinomial, en términos puramente algebráicos: para $f(x) = \sum_0^n a_n x^n$ su derivada es $Df(x) = \sum_0^n n a_n x^{n-1}$. En particular, $f(x)$ es separable si y sólo si es primo relativo con su derivada.

Tenemos toda una clase importante de polinomios separables: todo polinomio irreducible sobre un campo de característica cero (como $\mathbb{R}$ o $\mathbb{C}$), pues la derivada de un irreducible $p(x)$ de grado n es un polinomio de grado $n-1$, que es primo relativo a $p(x)$ por su irreducibilidad. Para este tipo de campos tenemos que un polinomio es separable si y sólo si es producto de polinomios irreducibles *distintos módulo factores constantes* [5]; en efecto 2 irreducibles distintos módulo factores constantes no pueden compartir raíz ya que esto implicaría que el polinomio mínimo de esta raíz divide a ambos polinomios y entonces cada uno difiere por una constante del polinomio mínimo por ser irreducibles, contradiciendo el ser distintos módulo constantes.

Una **extensión separable** es aquella donde todos los elementos son raíz de un polinomio separable. Del párrafo anterior deducimos que todas las extensiones

de campos de característica cero son separables pues cada elemento es raíz de su polinomio mínimo, que por ser irreducible es también separable.

Ahora podemos investigar algo más profundo sobre el *tamaño* del grupo de automorfismos de los campos de descomposición. Sea $f(x) \in F[x]$ y E su campo de descomposición. Hemos mencionado como podemos extender un isomorfismo $\varphi : F \longrightarrow F'$ a un isomorfismo entre los correspondientes campos de descomposición $\sigma : E \longrightarrow E'$. Mostraremos por inducción (sobre el grado de la extensión) que el número de tales extensiones de isomorfismos es menor o igual a $[E : F]$, con la igualdad dándose sólo cuando $f(x)$ es separable.

Esta demostración se centra en contar las extensiones al campo de descomposición, primero contando las extensiones del isomorfismo φ a un isomorfismo τ de extensiones simples intermedias y luego las extensiones de estos isomorfismos τ a isomorfismos σ de los campos de descomposición, para los cuales aplicamos una hipótesis de inducción sobre el grado de $f(x)$. Enlistamos las transformaciones pertinentes a este argumento para su referencia rápida:

- $\varphi : F \longrightarrow F'$ induce un isomorfismo $\widehat{\varphi} : F[x] \longrightarrow F'[x]$ donde $\widehat{\varphi} : f(x) \longmapsto f'(x)$ y para un factor irreducible $\widehat{\varphi} : p(x) \longmapsto p'(x)$.
- $\sigma : E \longrightarrow E'$ extensión de φ entre los campos de descomposición.
- $\tau : F(\alpha) \longrightarrow F'(\beta)$ con $\tau : \alpha \longmapsto \beta$. Tomando α y β raíces de $p(x)$ y $p'(x)$ respectivamente y $\tau := \sigma|_{F(\alpha)}$ es un isomorfismo que también extiende a φ.
- $F \leq F(\alpha) \leq E$, $F' \leq F'(\beta) \leq E'$.

En el caso $[E : F] = 1$, se tiene que $E = F$ y $E' = F'$ y por tanto sólo hay una extensión $\sigma = \varphi$. Si $[E : F] > 1$ entonces $f(x)$ tiene por lo menos un factor irreducible $p(x)$ de grado > 1, con su correspondiente $p'(x)$ factor de $f'(x)$. Sea α es una raíz fija de $p(x)$. Si σ es una extensión arbitraria de φ, entonces restringida a $F(\alpha)$ es un isomorfismo τ con algún subcampo de E'. Este isomorfismo está completamente determinado por su efecto en α, es decir por $\tau(\alpha)$, que es necesariamente

una de las raíces de $p'(x)$. De forma inversa para cada raíz β de $p'(x)$ podemos extender φ a un isomorfismo τ que manda α en β. Tenemos entonces tantas posibles extensiones τ como raíces distintas de $p'(x)$ y, como el grado de $p(x)$ y $p'(x)$ es igual a $[F(\alpha) : F]$, esta cantidad esta acotada por $[F(\alpha) : F]$ siendo igual si y sólo si $p(x)$ (o equivalentemente $p'(x)$) es separable.

Como E también es el campo de descomposición de $f(x)$ sobre $F(\alpha)$, y E' de $f'(x)$ sobre $F'(\beta)$, junto con $[E : F(\alpha)] \leq [E : F]$, podemos aplicar la hipótesis de inducción que nos dice que el número de extensiones de τ a σ es menor igual que $[E : F(\alpha)]$ con igualdad si $f(x)$ tiene raíces distintas. Al tener $[E : F] = [E : F(\alpha)][F(\alpha) : F]$, y usando el hecho de que el número total de extensiones de φ a σ se corresponde al producto del número de extensiones de φ a τ multiplicado por el número de τ a φ, se sigue finalmente que el número de extensiones de φ a σ es menor igual que $[E : F]$ con la igualdad si y sólo si $p(x)$ y $f(x)$ tienen raíces distintas, i.e. que $f(x)$ es separable sobre F (pues $p(x)$ es factor suyo). $\square$

Para el caso particular en que $F = F'$ (y por consiguiente $E = E'$) en lugar de isomorfismos hablamos de **automorfismos**, es decir isomorfismos de un espacio en sí mismo, que fijan el campo F. Así el resultado anterior nos dice que si E es el campo de descomposición sobre F del polinomio $f(x) \in F[x]$, entonces

$$|\{\text{automorfismos de } E \text{ que fijan } F\}| \leq [E : F]$$

con igualdad si y sólo si $f(x)$ es separable.

1.3. Automorfismos y Correspondencia de Galois

El conjunto de automorfimos de un campo forman un grupo bajo la composición y en el caso de una extensión E/F nos interesa el subgrupo de automorfismos que dejan fijo el campo base F, que denotamos por $Aut(E/F)$. Inversamente a cada subgrupo de automorfismos $G \leq Aut(E)$ podemos asociarle el conjunto de elementos que permanecen fijos bajo todos elementos del subgrupo, que resulta ser un subcampo $K \leq E$, conocido como el **campo fijo** de G. A esta mutua asignación entre grupos y campos se le llama **correspondencia de Galois**.

Al fijarse los elementos de F bajo la *acción* de $\sigma \in Aut(E/F)$ la transformación inducida $\sigma* : F[x] \longrightarrow F[x]$ por cada automorfismo es la identidad, de modo que si $\alpha \in E$ es raíz de $f(x) \in F[x]$ entonces $\sigma(\alpha)$ es a su vez raíz de $f(x)$. Esto nos dice que los elementos de $Aut(E/F)$ permutan las raíces de cada polinomio $f(x) \in F[x]$. A dos elementos relacionados de esta forma les llamamos **conjugados**.

Claramente la correspondencia de Galois **invierte las inclusiones**, es decir:

- Si $F_1 \leq F_2 \leq E$ entonces $Aut(E/F_2) \leq Aut(E/F_1) \leq Aut(E)$.
- Si $G_1 \leq G_2 \leq Aut(E)$ entonces $K_2 \leq K_1 \leq E$, donde K_i es el campo fijo de G_i.

Veremos el mismo resultado al que llegamos para el campo de descomposición al final de la sección anterior, ahora para una extensión finita arbitraria. Cambiando el énfasis de las extensiones de isomorfismos a la estructura de grupo de los automorfismos demostraremos que el número de automorfismos asociados a una extensión finita arbitraria cumple

$$|Aut(E/F)| \leq [E : F]$$

con igualdad si y sólo si F es el campo fijo de $Aut(E/F)$ (pues en principio este grupo puede fijar un campo más grande que contenga a F), en lugar de la condición sobre la separabilidad de un polinomio.

Suponiendo que $G = Aut(E/F) = \{\sigma_i\}_{i=1}^{i=n}$ y restringiendo cada uno a $E^\times := E \setminus \{0\}$, vemos que estos automorfismos son distintos como **caracteres** del subgrupo multiplicativo $E^\times$ por lo que son linealmente independientes como funciones del grupo [1], este resultado es conocido como el **lemma de Dedekind**. Los caracteres de un grupo son homomorfismos de este en el subgrupo multiplicativo en un campo, en este caso de $E^\times$ en sí mismo. Para un elemento arbitrario $v \in E$ esto significa que una combinación lineal $\sum_{i=1}^{i=n} x^i \sigma_i(v) = 0$ con $x_i \in E$ implica $x^i = 0$ para toda $i \in \{1, 2, .., n\}$. Si $m = [E : F]$ entonces podemos tomar una base $\{\omega_j\}_{j=1}^{j=m} \subset E$, de modo que $v = \sum_{j=1}^{j=m} a^j \omega_j$, con $a^j \in F$. Sustituyendo esto en la anterior expresión de las σ_i llegamos a la expresión $\sum_i x^i \sigma_i(\sum_j a^j \omega_j) = 0$ que, gracias a que las σ_i abren

sumas por ser automorfismos, podemos ver como la suma de m ecuaciones lineales de la forma $\sum_i x^i \sigma_i(a^j \omega_j) = a^j \sum_i x^i \sigma_i(\omega_j) = 0$ con n incógnitas x_i. Así construimos un sistema de m ecuaciones $\sum_i x^i \sigma_i(\omega_j) = 0$. Si, contrario a nuestra afirmación, suponemos que $n = |Aut(E/F)| > [E : F] = m$ entonces existiría una solución no trivial del sistema que resulta a su vez, siguiendo la construcción en reversa, en una combinación no trivial de $\sum_i x^i \sigma_i(v) = 0$, contradiciendo la independencia lineal. □

Más aún, ahora procedemos a demostrar por reducción al absurdo que si F es precisamente el campo fijo de $G = Aut(E/F) = \{\sigma_i\}_{i=1}^{i=n}$ entonces $|G| = [E : F]$. Supongamos pues la negación de esta proposición, que dado el resultado anterior corresponde a $n = |G| < [E : F] = m$. Existen entonces más de n elementos de E linealmente independientes sobre F, de modo que podemos tomar $n + 1$ elementos $\{a_j\}_{j=1}^{j=n+1}$ linealmente independientes sobre F. Supongamos sin perder generalidad que $\sigma_1 = Id$ es el elemento neutro del grupo. El sistema de n ecuaciones (indexadas por i) $\sum_j x_j \sigma_i(a_j)$ tiene $n+1$ incógnitas $\{x_j\}$, por lo que existe una solución no-trivial $\{\beta_j\}$. Por lo menos alguna β_j debe estar fuera de F, ya que de otra manera la primera ecuación $\sum_j \beta_j \sigma_1(a_j) = \sum_j \beta_j a_j$ contradiría la independencia lineal de las a_j. De todas las soluciones β_j de este sistema elijamos una con el menor número de elementos distintos de cero y sea r tal mínimo. Renumerando los índices de dicha solución si es necesario, podemos suponer que $\beta_1, ..., \beta_r$ son distintos de cero. Dividiendo las ecuaciones por β_r podemos suponer además que $\beta_r = 1$. Por lo que hemos ya dicho, algún elemento en $\{\beta_1, ..., \beta_{r-1}, 1\}$ no está en F, supongamos $\beta_1 \notin F$. Entonces el sistema está dado ahora por ecuaciones

$$\sum_{j=1}^{j=r} \beta_j \sigma_i(a_j) = 0 \tag{1.1}$$

Como β_1 no está en F, siendo este el campo fijo bajo el grupo G, existe un elemento $\sigma_0 \in G$ tal que $\sigma_0(\beta_1) \neq \beta_1$. Aplicando σ_0 a las ecuaciones el sistema queda invariante, con coeficientes $\sigma_0(\beta_j)$, pues σ_0 simplemente permuta las σ_i y por ende las ecuaciones. Nos queda

$$\sum_j \sigma_0(\beta_j)\sigma_i(a_j) = 0 \tag{1.2}$$

Sustrayendo (1.2) de (1.1) obtenemos: $\sum_{j=1}^{j=r}[\beta_j - \sigma_0(\beta_j)]\sigma_i(a_j)$. Como $\beta_r = 1$ el término $j = r$ de cada ecuación se cancela, tenemos entonces:

$$\sum_{j=1}^{j=r-1} [\beta_j - \sigma_0(\beta_j)]\sigma_i(a_j) = 0$$

Esto nos da una solución no trivial al sistema original, con $x_1 = \beta_1 - \sigma_0(\beta_1) \neq 0$, con menos que r variables x_i no todas cero, contradiciendo nuestra elección de r. Por tanto $|G| = [E : F]$. $\square$

Así, para un subgrupo $G \leq Aut(E)$ y su campo fijo K, sabemos que $G = Aut(E/K)$, lo que implica a su vez que dos distintos subgrupos de $Aut(E)$ tienen distintos campos fijos. Cuando una extensión E/F cumple $|Aut(E/F)| = [E : F]$, decimos que es una **extensión de Galois** y denotamos al grupo de automorfismos por $Gal(E/F)$, el **grupo de Galois** de la extensión $E \geq F$, para hacer énfasis en el hecho de que se tienen *suficientes* automorfismos.

Existe un teorema importante que nos caracteriza las extensiones de Galois: Una extensión E/F es de Galois si y sólamente si es el campo de descomposición de un polinomio separable. De hecho hemos probado al final de la sección anterior que el campo de descomposición de un polinomio separable es una extensión de Galois, por lo que resta probar el converso de esta afirmación. Además veremos que si una de las raíces α de un polinomio irreducible está en E entonces todas sus raíces están en E (pues *a priori* alguna podría estar en un campo más grande contenido en la cerradura algebráica de F) y el polinomio se descompone.

Sea E/F de Galois, $p(x) \in F[X]$ irreducible y $\alpha \in E$ una raíz. Nuevamente escribimos $G = Aut(E/F) = \{\sigma_i\}_{i=1}^{i=n}$. Tomemos los elementos $\alpha_1 := \sigma_1(\alpha) = \alpha$,$\alpha_2 := \sigma_2(\alpha), ..., \alpha_n := \sigma_n(\alpha)$ (hacemos $\sigma_1 = Id$, sin perder generalidad). Luego supongamos que entre ellos hay $r \leq n$ elementos distintos que volvemos a etiquetar de manera

que sean los primeros, es decir: $\alpha_1 = \alpha, \alpha_2, ..., \alpha_r \in E$. Por composición cada $\tau \in G$ permuta los elementos de G y del campo E dejando fijo al polinomio $p(x)$ (pues fija F), por lo que aplicado al conjunto de las α's simplemente las permuta entre sí. Entonces estos automorfismos permutan los factores del polinomio

$$f(x) = (x - \alpha)(x - \alpha_2)...(x - \alpha_r)$$

de modo que sus coeficientes pertenecen al campo fijo de G, que es precisamente F pues la extensión es de Galois, así que $f(x) \in F[x]$. Como $p(x)$ es irreducible y α es raíz de $f(x)$ entonces $p(x)$ divide a $f(x)$, por otro lado todas las α's son intercambiables (conjugadas) una a otra por la *acción* de los automorfismos, de modo que todas son raíces de $p(x)$ también, lo que implica a su vez que $f(x)$ divide a $p(x)$ y que por tanto $f(x) = p(x)$ es un polinomio separable en E (con todas sus raíces ahí). Además E es una extensión separable de F pues la construcción de este $f(x)$ es válida para cualquier $\alpha \in E$.

Falta ver que E es el campo de descomposición de algún polinomio separable. Consideremos una base $\{\omega_1, \omega_2, ..., \omega_n\}$ de E sobre F y para cada elemento su correspondiente polinomio mínimo $p_i(x)$. Por lo que acabamos de probar cada $p_i(x)$ es separable y tiene todas sus raíces en E. Si tomamos $g(x)$ como el polinomio obtenido de remover raíces repetidas del polinomio $g_0(x) = p_1(x)p_2(x)...p_n(x)$, entonces tanto $g(x)$ como $g_0(x)$ tienen a E como campo de descomposición. Por tanto E es el campo de descomposición del polinomio separable $g(x)$. $\square$

Cabe notar en el argumento anterior que las raíces repetidas que quitamos para que $g(x)$ fuese separable dependen de la existencia de elementos conjugados en la base $\{\omega_1, \omega_2, ..., \omega_n\}$, pues entonces dos o más elementos comparten un mismo polinomio mínimo. Esta demostración nos dice también que para una extensión de Galois E/F las otras raíces del polinomio mínimo de cualquier elemento $\alpha \in E$ son precisamente los conjugados del elemento bajo la acción de $Gal(E/F)$. Ahora, esto nos indica que las permutaciones *válidas* de las raíces del polinomio separable $g(x)$ que genera la extensión son aquellas que permutan sólo entre raíces del mismo factor irreducible. Cada uno de estos factores nos da, como veremos en la siguiente sección, un subgrupo normal del grupo de Galois. Así tenemos un análisis del grupo

de automorfimos $G = Aut(E/F)$ de una extensión de Galois como la suma directa de los grupos de permutaciones de las raíces de los factores irreducibles de nuestro polinomio separable $g(x)$. También vemos directamente que si podemos encontrar un polinomio irreducible con una raíz en E pero con otra raíz *fuera* (aunque siempre dentro de la cerradura algebráica), entonces la extensión no puede ser de Galois.

Antes de continuar resumamos esta discusión en 3 caracterizaciones de las extensiones de Galois $E \geq F$:

- $|Aut(E/F)| = [E : F]$.
- El campo fijo de $Aut(E/F)$ es precisamente F.
- Si es el campo de descomposición de un polinomio separable.

1.4. Teorema Fundamental

El llamado **teorema fundamental de la teoría de Galois** es un compendio de las relaciones entre los subgrupos del grupo de Galois de una extensión y los campos intermedios de la extensión, dadas por la correspondencia de Galois. Para una extensión de Galois E/F y el grupo $G := Gal(E/F)$, $H \leq G$ y $K := K_H$ el campo fijo de H, se cumple lo siguiente:

(1) La correspondencia de Galois establece una relación biyectiva entre los campos intermedios K de la extensión y los subgrupos H del grupo de Galois G.

(2) Esta correspondencia invierte inclusiones.

(3) E/K es una extensión de Galois para todo campo intermedio K, con un grupo de Galois H.

(4) de modo que $[E : K] = |H|$ y $[K : F] = |G : H|$, donde esta última cantidad es el índice de H en G.

(5) K/F es de Galois si y sólo si H es un subgrupo normal de G. En este caso $Gal(K/F) \cong G/H$.

Vimos en la sección anterior que dos distintos subgrupos de G nos dan distintos campos fijos, lo que nos dice que esta asignación es inyectiva. Como E/F es Galois, entonces E es el campo de descomposición de un polinomio separable $f(x)$: de modo que si K es un campo intermedio arbitrario de la extensión, podemos ver a $f(x)$ como un polinomio separable en $K[x]$, y nuevamente E es el campo de descomposición, por lo que E/K es Galois, lo que implica que K es el campo fijo de $Aut(E/K) \leq G$, de modo que la asignación es suprayectiva, demostrando (1). A su vez queda establecido (3), pues si $K = K_H$ es el campo fijo de H entonces $H = Aut(E/K)$. La inversión de las inclusiones es consecuencia directa de la definición de la correspondencia, cómo se discutió en la sección anterior, estableciendo (2).

Nuevamente tomando $K = K_H$ sabemos que, por ser extensiones de Galois, $[E : K] = |H|$ y $[E : F] = |G|$, lo que nos da $[K : F] = [E : F]/[E : K] = |G|/|H| = |G : H|$, probando (4).

Nos resta probar (5). Sea $K = K_H$. Para cada $\sigma \in Gal(E/F)$, $\sigma|_K$, su restricción a K, es un isomorfismo con $\sigma(K) \leq E$, un *encaje* de K en $E \leq \overline{F}$. Conversamente, sea $\tau : K \longrightarrow \tau(K)$ un isomorfismo de K que fija F, cuya imagen es un campo $\tau(K)$ contenido en la cerradura algebráica $\overline{F}$, a esto llamamos un **encaje** de K (o más bien un encaje de la extensión K/F) en $\overline{F}$. Resulta que de hecho $\tau(K) \leq E$ pues la imagen de cada elemento es raíz del mismo polinomio mínimo, es decir que son elementos conjugados, y E contiene a todas estas raíces por ser una extensión separable. De modo que podemos extender τ a un automorfismo $\sigma \in Gal(E/F)$. Hemos deducido que todos los encajes de K en $\overline{F}$ se obtienen de la restricción de elementos de G.

Por otro lado, dos automorfismos $\sigma, \sigma' \in G$ se restringen al mismo encaje de $K = K_H$ si y sólo si $\sigma^{-1}\sigma'$ es la identidad sobre K, lo que es equivalente a decir que $\sigma^{-1}\sigma' \in H$, pues estos son precisamente los automorfismos que preservan K. Entonces los encajes están en biyección con las clases laterales de H en G:

$$|Encajes(K/F)| = |G : H| = [K : F]$$

donde $Encajes(K/F)$ es el conjunto de encajes de K en la cerradura algebráica $\overline{F}$ que fijan a F. Claramente $Aut(K/F) \subseteq Encajes(K/F)$ de modo que la extensión K/F es de Galois si y sólo si todos los encajes son en realidad automorfismos de K, que es $\sigma(K) = K$ para todo $\sigma \in G$. Para dado $\sigma \in G$ el grupo que deja invariante al campo $\sigma(K)$ es precisamente la clase de conjugación $\sigma H \sigma^{-1}$, pues todos los elementos de este grupo lo fijan y tiene tantos elementos como $[E : \sigma(K)] = [E : K] = |H|$. Por la naturaleza biyectiva de la correspondencia de Galois, sabemos que dos campos intermedios de la extensión E/F son iguales si y sólo si los subgrupos de G que los fijan son el mismo. De modo que $\sigma(K) = K$ para toda $\sigma \in G$, lo que implicaría como mencionamos antes que K/F es de Galois, si y sólo si $\sigma H \sigma^{-1} = H$ para toda $\sigma \in G$, lo que es decir que H es un subgrupo normal en G.

Ya hemos identificado $Encajes(K/F)$ con las clases laterales de H en G, de modo que en este caso el grupo G/H está identificado con el grupo de automorfismos de la extensión de Galois K/F por la definición de la operación del grupo (que es simplemente la composición de automorfismos). De modo que $G/H \cong Aut(K/F)$ completando la prueba de (5). $\square$

Pensemos en lo siguiente: Los subgrupos normales del grupo de Galois $Gal(E/F)$ nos permiten identificar a todos los campos intermedios K que no salen de sí mismos tras la *acción de una simetría*, siendo a su vez simetría de dicho campo intermedio como extensión del campo base F. Si $f(x) \in F[x]$ es el polinomio separable cuyo campo de descomposición podemos identificar con la extensión de Galois E, entonces el polinomio separable que define al campo intermedio K es un factor (no necesariamente irreducible) de $f(x)$ en $F[x]$, siempre y cuando su grupo de automorfismos es normal en $Gal(E/F)$. Esto sucede pues una extensión de Galois es precisamente aquella extensión finita que contiene a todos los posibles conjugados de cada elemento.

La no existencia de grupos normales no triviales define al concepto de **grupo simple**. En términos intuitivos la simplicidad del grupo significa que no se lo puede *colapsar* a un grupo más pequeño. Podemos hablar de un *objeto geométrico* esencial

respecto de sus simetrías, ya que estas no son a su vez simetrías de algún *sub-objeto* similar. Cuando tenemos un subgrupo normal el grupo se colapsa al cociente, en cuyo caso podemos encontrar una extensión de Galois más pequeña. Cuando no es posible hallar dicho subgrupo normal la extensión de Galois está dada por el campo de descomposición de un polinomio irreducible (que siempre es separable en el caso de campos de característica cero), relacionando así la irreducibilidad del polinomio con la simplicidad del grupo.

Capítulo 2

Haces Principales

Los haces principales son estructuras geométricas de una gran riqueza pues encapsulan una idea fundamental: la de *simetría interna*. Un *haz* se puede pensar como un espacio en el que cada punto contiene a su vez un espacio interno de *estados*, que se observan *alineados* localmente (véase más adelante las trivializaciones locales) y en que el paso de un estado a otro, en dicha localidad o punto, está dado por una simetría. Digamos que esta es una perspectiva desde *abajo*. Si por otro lado nuestra perspectiva se ubica desde *arriba*, el haz corresponde a un espacio que se proyecta en otro, como un objeto y su *sombra*. Podemos pensar en una pelota flotando fija en el aire y la sombra producida por un *haz* de luz sobre esta: si rotamos la pelota, sin desplazarla, la sombra es exactamente la misma. Con las simetrías internas de un espacio (la sombra) nos referimos a las simetrías de un espacio superior (la pelota) del que aquel se deriva.

Los haces principales constituyen un foco conceptual de este trabajo, siendo una realización útil del concepto de simetría. En este capítulo construiremos una intuición acerca de su naturaleza, daremos las definiciones pertinentes y expondremos los elementos básicos de su estructura.

2.1. Simetrías

La teoría de grupos es el lenguaje matemático de las *simetrías*. La palabra «simetría» significa etimológicamente «de la misma medida». Esta palabra evoca la noción de armonía estética y equilibrio. En su acepción más general se refiere a la relación de correspondencia característica, de equivalencia o identidad entre los constituyentes de una entidad o entre diferentes entidades. El hablar de simetrías, en el sentido matemático legado por el programa de Erlangen, es hablar de la *acción de un grupo* sobre un espacio u objeto geométrico; una simetría es un elemento del grupo que *actúa* en dicho espacio. En la siguiente sección daremos la definición de *acción*, pero por el momento atendamos a lo que está detrás: nos interesan las transformaciones de una entidad u objeto que se pueden componer entre sí e invertir.

Estudiamos en el capítulo anterior el grupo de automorfismos de una extensión que preserva nuestro campo base: los automorfismos son simetrías de la extensión, en el sentido de que preservan las relaciones algebráicas, formando un grupo que actúa sobre dicha extensión. En este caso nuestro interés está centrado en la propiedad de tener al campo base como *invariante*, de modo que el polinomio que manipulamos también lo sea. Se podrá objetar que un campo no es un objeto geométrico sino un objeto algebráico. Esta distinción depende de lo que entendemos por *geometría*. El programa de Erlangen de Felix Klein es el que da un sentido esclarecedor al uso de la palabra geometría en el ámbito moderno: su propuesta es un programa de investigación que caracteriza la geometría como el estudio de invariantes bajo la acción de un grupo. Sin embargo hay que entender que esta idea tiene limitaciones: existen contra-ejemplos (clásicos y cuánticos) a esta definición de geometría, es decir espacios *distintos* con el mismo grupo de simetrías. Se puede incluso sortear este problema considerando que la diferencia entre espacios con las mismas simetrías difieren a un nivel *más primitivo* que el geométrico, como por ejemplo en su topología. Con todo esta perspectiva resultará iluminadora en varias ocasiones. El grupo puede ser definido a partir de estructuras geométricas conocidas directamente o, a la inversa, definimos las estructuras geométricas como los invariantes de la acción de un grupo. En otras palabras: Los invariantes pueden ser referidos de forma explícita o implícita.

Por ejemplo en el plano euclidiano tenemos definida una métrica dada por el producto interno y a partir de esta podemos considerar el grupo de transformaciones del plano que preservan dicha métrica. Todos las estructuras que podamos definir a partir de esta métrica son entonces invariantes de la acción del grupo; ángulos e incidencias, por ejemplo. Por otro lado, si vamos a retratar un rostro humano imaginario en el plano buscaremos realizar cercanamente una *simetría axial* dada por la reflexión sobre la recta vertical que ha de pasar por el medio de las cejas y la punta de la barbilla. Esta reflexión junto con la identidad forman un grupo, que de manera natural define el espacio en que hallaremos ese rostro imaginario.

Los ejemplos del círculo y la esfera resultan especiales: estos objetos son de gran interés por su naturaleza intuitiva como objetos simétricos y la importancia de sus grupos de simetrías. Estos últimos son conjuntos continuos, con estructura topológica no trivial, representables como grupos de matrices. Para el círculo tenemos el grupo completo de rotaciones alrededor de su centro y las reflexiones por rectas que pasan por este; topológicamente se trata de dos círculos disconexos y es denotado por $O(2)$. Equivalentemente $O(3)$ es el grupo de simetrías de la ésfera, constituidos por las rotaciones sobre los distintos ejes y las reflexiones por planos ecuatoriales; topológicamente se trata de dos copias de la π-esfera (una bola 3-dimensional con los puntos antípodas de su cáscara esférica identificados). Para ver como se llega a esta realización geométrica de $O(3)$, consideramos la componente conexa de la identidad: $SO(3)$. Este es el subgrupo de las rotaciones, o el subgrupo que preserva la orientación del espacio. Lo modelaremos con una bola de radio π centrada en el origen. En esta bola un punto x distinto del origen corresponde a una rotación de la esfera: un eje dado por su dirección desde el origen y una magnitud de rotación en radianes dada por su tamaño en el intervalo $(0, \pi]$. El origen entra en correspondencia con la identidad de la esfera, la simetría que deja todo en su lugar inicial (en la vecindad del origen se encuentran las rotaciones infinitesimales; la continuidad obliga a la identidad a estar ahí). La rotación dada por $-x$ corresponde a una rotación en el mismo eje que x pero con el ángulo de rotación orientado inversamente. Entonces toda la linea de $\pi\frac{x}{|x|}$ a $-\pi\frac{x}{|x|}$ nos da el rango completo de rotación $[-\pi, \pi]$ sobre el

eje definido por x. Sólo nos resta una ambigüedad: los puntos extremos corresponden, respectivamente, a una rotación por π y $-\pi$ sobre el mismo eje. Estas nos dan la misma simetría, por lo cuál realizamos la identificación de puntos antipodales. La π-esfera es el espacio cociente resultante. Este cociente, restringido a la cáscara esférica, produce el plano proyectivo real. Entonces la π-esfera es un plano proyectivo al que le pegamos una bola abierta. La restante componente conexa de $O(3)$ se obtiene componiendo todo $SO(3)$ con alguna reflexión por un plano ecuatorial y es topológicamente una π-esfera también.

Recordemos que $O(n)$ es en general el grupo de transformaciones ortogonales de un espacio vectorial n-dimensional. Su *representación* está dada por matrices cuyos vectores columna forma una base ortonormal del espacio (y cuyo determinante es igual a 1 ó -1). De forma análoga a los casos de bajas dimensiones anteriores, este grupo está dado por rotaciones generalizadas (que forman el subgrupo $SO(n)$), y reflexiones por hiperplanos. Es a su vez el grupo de simetría de la esfera de dimensión $n-1$. Todos los anteriores grupos nombrados son *grupos de Lie*, y en particular ejemplos de los llamados *grupos clásicos (de matrices)* [3] entre los que se incluyen por ejemplo $M_{n\times n}(\mathbb{R})$, $M_{n\times n}(\mathbb{C})$ y subgrupos suyos como $O(n)$, $SO(n)$, $SL(n,\mathbb{C})$, $U(n)$ y $SU(N)$. En un haz principal el grupo de Lie describe los *grados internos de libertad de un espacio base*.

2.2. Acción de Grupo

La **acción** (derecha) de un grupo G sobre un conjunto S se define como una función $S \times G \longrightarrow S$ cuyas imagenes denotamos $(x, g) \longmapsto x * g$ y que cumple

$$(x, e) \longmapsto x, \forall s \in S$$

$$(x * g) * h \longmapsto x * gh$$

donde e es el neutro del grupo y $g, h \in G$. Dejando cada valor de $g \in G$ fijo producimos un mapeo en el grupo de automorfismos de S que, siendo por ahora un conjunto sin más estructura, se trata del grupo de permutaciones de sus elementos. De modo

que la acción se puede definir de manera equivalente a través de un homomorfismo $G \longrightarrow Aut(S)$. Esto es consecuencia directa de las propiedades de la acción. Existe a su vez la noción de acción izquierda, cuyas propiedades son completamente análogas a la acción derecha salvo por cambios en la orientación de la notación.

Un ejemplo es la acción (derecha) $G \times G \longrightarrow G$ dada por la conjugación de elementos del grupo, es decir: $(x, g) \mapsto g^{-1}xg$. A la imagen del homomorfismo inducido por esta acción, $G \longrightarrow Aut(G)$, se le conoce como el grupo de **automorfismos internos** de G. Cada elemento en $g \in G$ se mapea al automorfismo definido como $g^*(x) = g^{-1}xg$, es decir, el que se obtiene de fijar g en la acción de conjugación. Simples cálculos nos muestran que en efecto esto nos da un automorfismo de G:

$$g^*(x) = g^{-1}xg = e \;\Leftrightarrow\; xg = g \;\Leftrightarrow\; x = e$$

$$g^*(x_1x_2) = g^{-1}x_1x_2g = (g^{-1}x_1g)(g^{-1}x_2g) = g^*(x_1)g^*(x_2)$$

Cuando el grupo G es conmutativo entonces el único automorfismo interno es la identidad. Intercambiando los papeles de g y g^{-1} obtenemos la versión izquierda de esta acción.

El conjunto de imágenes de la acción a un punto dado $x \in S$ por todos los elementos del grupo constituyen una clase de equivalencia que llamamos la **órbita** de x, simbólicamente

$$\mathcal{O}_x = \{x * g \mid g \in G\}$$

A su vez definimos el **estabilizador** de un punto como el conjunto de elementos en el grupo cuya acción no lo mueve

$$\mathcal{L}_x = \{g \in G \mid x * g = x\}$$

Se verifica de inmediato que $\mathcal{L}_x$ es un subgrupo de G para cualquier punto x. El estabilizador nos señala la ambigüedad que hay entre cada punto en la órbita y el elemento del grupo que lo produce desde el punto x dado. En efecto, supongamos $x * g = x * g' = y$ para algunos $g, g' \in G$, de modo que en particular $y \in \mathcal{O}_x$, entonces

$$x * g' = x * g \;\Leftrightarrow\; x * g'g^{-1} = x \;\Leftrightarrow\; g'g^{-1} \in \mathcal{L}_x \;\Leftrightarrow\; g' \in \mathcal{L}_x g$$

de modo que tenemos una biyección de conjuntos

$$\mathcal{O}_x \leftrightarrow G/\mathcal{L}_x$$

Introducimos ahora algunos adjetivos que caracterizan a una acción: Cuando la órbita de un punto es todo el conjunto decimos que la acción es **transitiva**. Si el estabilizador de todos los puntos es trivial, $\mathcal{L}_x = \{e\}, \forall x \in S$, decimos que la acción es **libre**. Mientras que si $G \longrightarrow Aut(S)$ es un mapeo inyectivo (sólo e se mapea al automorfismo identidad) la acción es llamada **fiel**.

A manera de ejemplo veamos el grupo $SO(3)$ de rotaciones de la esfera. Vista en representación matricial mediante la elección de una base, la acción está dada simplemente por el producto de un punto de la esfera, representado por un vector (columna), por la matriz que representa la rotación. Considerando 2 puntos arbitrarios en la esfera y el círculo ecuatorial (i.e. aquel obtenido por el corte de un plano que pasa por el centro de la esfera) que los une, podemos encontrar el eje y ángulo de rotación para llevar uno en el otro. De modo que esta acción es transitiva. El estabilizador de un punto es el grupo de rotaciones sobre el eje que define dicho punto. La acción es fiel, pues toda rotación no trivial deja fijo sólo un punto y su antípoda.

En general la acción de G sobre S se denota usando la yuxtaposición, $(x, g) \mapsto xg$, siempre que esto no cause confusión con el producto entre elementos del grupo. La noción de acción izquierda es completamente análoga.

2.3. Grupos de Lie

Los grupos de Lie son la clase de grupos con los que trata la teoría de haces clásicos (en contraposición a los haces cuánticos que veremos posteriormente). Son espacios con una doble estructura: una algebráica y otra geométrica. Por un lado es un grupo y por el otro una variedad suave, donde estas estructuras se encuentran relacionadas por la condición de que las operaciones del grupo sean funciones suaves en el espacio. Una función **suave** es aquella que tiene en su dominio derivadas de todos órdenes; una variedad suave cumple que las funciones de transición de su atlas

son suaves. Si llamamos G a nuestro espacio con sus dos estructuras, será un grupo de Lie si y solamente si la siguiente función es suave:

$$G \times G \longrightarrow G$$

$$(a, b) \longmapsto ab^{-1}$$

La yuxtaposición de elementos de G corresponde a la operación del grupo, que llamamos producto (o multiplicación) del grupo. La suavidad de la función es respecto de la estructura diferenciable de G y la estructura diferenciable del producto cartesiano $G \times G$ (dada por el producto de cartas y funciones de transición del atlas de G). Si fijamos la primera entrada de este mapeo como $a = e$, tenemos que la función $\theta : G \longrightarrow G$ dada por $b \longmapsto b^{-1}$ es también una función suave, que llamamos la **función antípoda (o de inversión) del grupo**, que al ser involutiva es en particular un difeomorfismo de G. En consecuencia la función que describe el **producto del grupo** $(a, b) \longmapsto ab$ es dada también por una función suave $\rho : G \times G \longrightarrow G$.

Del parrafo anterior podemos deducir que el producto de los elementos del grupo por un elemento fijo $a \in G$ define un difeomorfismo del grupo de Lie G visto como variedad suave. Llamamos a este la traslación izquierda (derecha) por a y se denota L_a (R_a):

$$L_a : x \longmapsto ax \ \forall x \in G$$

$$(R_a : x \longmapsto xa)$$

La invertibilidad de las traslaciones es consecuencia de que su inversa es dada por el inverso en el grupo: ${L_a}^{-1} = L_{a^{-1}}$ (${R_a}^{-1} = R_{a^{-1}}$). Tenemos entonces toda una familia de difeomorfismos indexados por los elementos de G: son simetrías de su aspecto de variedad, obtenidas de su estructura algebráica sin ser simetrías en este aspecto. Sin embargo tenemos los automorfismos internos dados por la conjugación $axa^{-1} = L_a R_{a^{-1}}(x)$, que vemos en términos de la composición de las funciones suaves e invertibles que acabamos de ver, por lo que estos automorfismos son además difeomorfismos, siendo entonces simetrías de toda la estructura del grupo de Lie.

El círculo y la π-esfera son ejemplos que ya hemos mencionado. El círculo es la variedad subyacente al grupo de rotaciones del plano $SO(2)$, o también al grupo de complejos unitarios $U(1)$. Los cuaterniones unitarios hacen de la 3-esfera también un grupo de Lie: $Sp(1)$. El círculo $\mathbb{S}^1$ y la 3-esfera $\mathbb{S}^3$ son los únicos casos entre las esferas $\mathbb{S}^n$ con esta estructura.

2.4. Álgebra de Lie

Por tratarse de un difeomorfismo, la diferencial de L_a nos da un isomorfismo del espacio tangente en la identidad T_e al espacio tangente en a, T_a. Podemos definir entonces los **campos vectoriales invariantes por la izquierda** de la siguiente manera: Sea X un campo vectorial y X_a el vector definido por este sobre el punto $a \in G$. Decimos que X es invariante por la izquierda si $\forall a \in G$ se tiene que $DL_a(X_e) = X_a$, de modo que el campo invariante es en cierto sentido un campo constante, obtenido trasladando el vector X_e a todos los puntos de G. En efecto, inversamente podemos representar cualquier vector X_e en T_e como un campo vectorial invariante, dado por $X_a = DL_a(X_e)\ \forall a \in G$. Todo campo invariante es suave pues la diferencial de la traslación es un operador que varía suavemente sobre los elementos del grupo. De esto resulta que el espacio tangente en la identidad y el conjunto de campos vectoriales invariantes por la izquierda son espacios vectoriales isomorfos.

Propiedades estructurales del grupo de Lie se pueden observar en una vecindad infinitesimal del elemento neutro/identidad, donde encontramos a los elementos infinitesimales del grupo representados geométricamente por los vectores del espacio tangente a G en ese punto. De hecho, todo grupo topológico conexo es generado por una vecindad de la identidad [3]. Esta situación es nueva respecto a la teoría de grupos finitos, donde no hay equivalente natural a los elementos infinitesimales; ahora entra en juego la llamada teoría local de grupos de Lie. El espacio tangente, T_e, es llamado el **álgebra de Lie** $\mathfrak{g}$ del grupo (de Lie) G, que hemos caracterizado como el espacio de campos invariantes por la izquierda. La no-trivialidad de la conjugación en el grupo (consecuencia de su no-conmutatividad) se encuentra representada en el álgebra de Lie por la operación del *corchete de Lie*, que podemos explicar en el caso

de grupos de dimensión finita (como los grupos clásicos de matrices) de la siguiente manera:

Identificando dos elementos, X e Y, del álgebra de Lie como vectores tangentes en la identidad a curvas suaves parametrizadas $A(t) = \{a_{ij}(t)\}$ y $B(s) = \{b_{ij}(s)\}$ en un grupo clásico de matrices G de $n \times n$ (donde $i, j \in \{1, 2, ..., n\}$) que pasan por la identidad, e, en $s = t = 0$. Esto es simbólicamente

$$A'(0) = \frac{\mathrm{d}}{\mathrm{d}t}A(t)\bigg|_{t=0} = \left\{\frac{\mathrm{d}}{\mathrm{d}t}a_{ij}(t)\bigg|_{t=0}\right\}_{i,j\in\{1,2,...,n\}} = X$$

y

$$B'(0) = \frac{\mathrm{d}}{\mathrm{d}s}B(t)\bigg|_{s=0} = \left\{\frac{\mathrm{d}}{\mathrm{d}s}b_{ij}(s)\bigg|_{s=0}\right\}_{i,j\in\{1,2,...,n\}} = Y$$

junto con $A(0) = e$ y $B(0) = e$.

Para cada t consideramos la curva

$$C_t(s) = A(t)B(s)A^{-1}(t)$$

que pasa a su vez por e en $s = 0$ y produce una curva parametrizada de vectores tangentes en el álgebra de Lie dada por

$$D(t) = C_t'(0) = A(t)B'(0)A^{-1}(t) = A(t)YA^{-1}(t)$$

Cuyo tangente en $t = 0$ es a su vez un elemento del álgebra de Lie (un espacio vectorial es cerrado bajo límites en el caso de dimensión finita), que por regla de la cadena es precisamente el *corchete de Lie* de X e Y:

$$D'(0) = A'(0)YA^{-1}(0) + A(0)Y(-A^{-2}(0)A'(0)) = XY - YX = [X, Y]$$

El **corchete de Lie** es una operación que podemos realizar dada una pareja de campos vectoriales para obtener un tercer campo. Todos los campos suaves sobre una variedad suave M forman un álgebra de Lie de forma natural denotada por $\chi(M)$, equivalente al conjunto de derivaciones del álgebra de funciones [14]. Cabe mencionar

que el álgebra de Lie $\mathfrak{g}$ es una subálgebra de $\chi(G)$. En términos de la composición de derivaciones, el corchete de dos campos vectoriales X y Y es

$$[X, Y] = XY - YX$$

En general un álgebra de Lie es un espacio vectorial con una operación binaria bilineal antisimétrica que cumple la identidad de Jacobi, que expresada en corchetes de Lie para campos X,Y y Z es

$$[[X, Y], Z] + [[Z, X], Y] + [[Y, Z], X] = 0$$

Al ser un campo vectorial suave sobre el grupo, todo elemento del álgebra de Lie da lugar una *foliación* unidimensional en la región (abierta) donde este no se anula (conformada por el conjunto de las curvas integrales del campo). Podemos introducir un parámetro t real, que nos permita movernos de forma pareja sobre las *hojas* (curvas integrales), pasando de una a otra por la traslación por un elemento (finito) del grupo. El paso de un elemento infinitesimal a un elemento finito del grupo está dado por una generalización de la función exponencial [14]. Si consideramos el espacio unidimensional generado por un vector tangente X sobre la identidad, la función exponencial se encargará de doblarlo sobre el espacio curvo del grupo exactamente en la hoja de la *foliación* que pasa por la identidad formando un subgrupo uniparamétrico de G (cuyas clases laterales son precisamente el resto de las hojas). El álgebra de Lie de un grupo de Lie nos permite entonces reconstruir la componente conexa de la identidad. Sin embargo sólo determina el grupo módulo cubierta universal [22]. Revisaremos la noción de *foliación* en la sección sobre *conexiones*.

2.5. Definición de Haz

Un **haz principal** es una triada $P(M, G)$ que consta de una variedad suave P, llamada **espacio total**, sobre la que actúa un grupo de Lie G, llamado el **grupo estructural** y una variedad suave M obtenida como el cociente de la acción de G, llamada **espacio base**. Son 3 las propiedades que caracterizan al haz principal:

1. El grupo G actúa libremente por la derecha en P.

2. M es el espacio cociente de P por la relación equivalencia inducida por G, $M = P/G$, y la proyección canónica $\pi : P \longrightarrow M$ es diferenciable.

3. P es localmente trivial, es decir, cada punto $x \in M$ tiene una vecindad abierta U tal que $\pi^{-1}(U)$ es difeomorfa a $U \times G$ en el sentido de que hay un difeomorfismo $\psi : \pi^{-1}(U) \longrightarrow U \times G$ tal que $\psi(u) = (\pi(u), \varphi(u))$ donde φ es una función de $\pi^{-1}(U)$ en G que satisface $\varphi(ua) = (\varphi(u))a$.

Notamos al respecto que:

1. Que la acción de G sea libre implica que la órbita de cualquier elemento del grupo es difeomorfa al grupo G. En el haz tenemos a P *foliado* en copias de G.

2. La preimagen de cada punto x de M es una órbita completa de la acción de G, que llamamos la **fibra** sobre x, lo que es decir $\pi^{-1}(x) \cong G$.

3. La restricción sobre la función ψ nos dice simplemente que las trivializaciones locales respetan la acción del grupo.

Para relacionar nuestra definición intrínseca con la construcción del haz por medio de una cubierta abierta necesitamos las funciones de transición (la construcción a partir de un atlas). El inciso (3) de la definición implica que podemos tomar una cubierta abierta $\{U_\alpha\}$ de M para las que $\pi^{-1}(U_\alpha)$ cuenta con un difeomorfismo $u \mapsto (\pi(u), \varphi_\alpha(u))$ de $\pi^{-1}(U_\alpha)$ en $U_\alpha \times G$ tal que $\varphi_\alpha(ua) = \varphi_\alpha(u)a$. Vemos que $\varphi_\beta(ua)\left(\varphi_\alpha(ua)\right)^{-1} = \varphi_\beta(u)aa^{-1}\left(\varphi_\alpha(u)\right)^{-1} = \varphi_\beta(u)\left(\varphi_\alpha(u)\right)^{-1}$ lo que muestra que este valor depende sólo de $\pi(u)$ y no de u. Así podemos definir las funciones $\psi_{\beta\alpha} : U_\alpha \cap U_\beta \longrightarrow G$ como $\psi_{\beta\alpha}(\pi(u)) = \varphi_\beta(u)\left(\varphi_\alpha(u)\right)^{-1}$. Esta función asigna a cada punto $x \in U_\alpha \cap U_\beta$ un elemento de G que establece la relación entre una trivialización local y otra: $(\pi(u), \varphi_\alpha(u)) \leftrightarrow (\pi(u), \varphi_\beta(u))$. La familia de funciones $\{\psi_{\beta\alpha}\}$ (i.e. para cada par de conjuntos en la cubierta abierta) son llamadas **funciones de transición** del haz $P(M, G)$ correspondientes a la cubierta $\{U_\alpha\}$. Estas funciones cumplen:

$$\psi_{\gamma\alpha}(x) = \psi_{\gamma\beta}(x)\psi_{\beta\alpha}(x) \text{ para } x \in U_\alpha \cap U_\beta \cap U_\gamma$$

Conversamente, si partimos de una variedad M con una cubierta abierta $\{U_\alpha\}$ tal que para cada intersección no vacía $U_\alpha \cap U_\beta$ existen las funciones $\psi_{\beta\alpha} : U_\alpha \cap U_\beta \longrightarrow G$

de modo que se cumpla la relación anterior entre ellas, entonces podemos construir un haz principal $P(M, G)$ con funciones de transición $\{\psi_{\beta\alpha}\}$ [14]. En lo que sigue usaremos la palabra *haz* para referirnos a un haz principal.

Es posible también definir los **homomorfismos de haces** (y hacer de los haces principales una *categoría*). Un homomorfismo entre dos haces $P(M, G)$ y $P'(M', G')$ es una pareja (f', f'') dada por un mapeo $f' : P' \longrightarrow P$ y un homomorfismo $f'' : G' \longrightarrow G$ tal que para $u \in P'$ y $a \in G'$ se cumple $f'(ua) = f'(u)f''(a)$. Estas transformaciones son mapeos entre haces que mandan fibras en fibras y por lo tanto inducen a su vez un mapeo entre las correspondientes bases $f : M' \longrightarrow M$. Por simplicidad se denota a las tres transformaciones por la misma f y escribimos $f : P'(M', G') \longrightarrow P(M, G)$. Un **encaje** de variedades suaves es una inmersión (i.e. un mapeo tal que la diferencial es inyectiva en cada punto) suave, inyectiva y propia (i.e. en que la preimagen de un subconjunto compacto es compacta), lo que se traduce en un difeomorfismo con la imagen y que esta misma es una subvariedad del codominio [12]. Si $f : P' \longrightarrow P$ es un encaje y $f : G' \longrightarrow G$ es un monomorfismo entonces decimos que f es un **encaje de haces** y a su imagen le llamamos un **subhaz** de $P(M, G)$, descrito por $f(P)(f(M), f(G))$.

Un primer ejemplo de haz es el producto $P = M \times G$ de una variedad M con un grupo de Lie G. La acción de G sobre P es simplemente el producto sobre la segunda entrada (para $g \in G$ y $(p, a) \in P$, la acción está dada por $g : (p, a) \mapsto (p, ag)$). Se verifican de inmediato todas las propiedades y M resulta el espacio base. A este haz le llamamos **haz trivial**. No debe sorprendernos que la trivialidad local de un haz corresponde precisamente a que todo haz es localmente como el haz trivial, de hecho es intuitivamente útil pensar a los haces en términos de productos cartesianos *torcidos* o *curvados*.

El ejemplo tradicional es el **haz de marcos** de una variedad suave M de dimensión m, construido de la siguiente manera: sobre cada punto $x \in M$ consideramos el espacio de todas las posibles bases para el espacio tangente a la variedad en ese punto. El paso de una base a otra esta dada por la acción de un operador en $GL(m, \mathbb{R})$. Al

fijar una base arbitraria tenemos una correspondencia biunívoca entre las distintas bases y los elementos de $GL(m,\mathbb{R})$, que naturalmente se trata de un difeomorfismo, siendo así $G = GL(m,\mathbb{R})$ el grupo estructural.

Una manera de obtener nuevos haces resulta de la restricción de un haz inicial: Si tenemos una subvariedad $M' \subseteq M$ podemos restringir el haz $P(M,G)$ al haz $\pi^{-1}(M')(M',G)$, donde las fibras se preservan y restringimos la acción del grupo al espacio $\pi^{-1}(M')(M',G)$, a este haz le llama **porción del haz** $P(M,G)$.

Además podemos introducir toda una clase interesante de haces: partiendo de un grupo de Lie G y un subgrupo cerrado (tambien de Lie) H, podemos construir un haz $G(G/H,H)$. La acción de grupo es el producto en G, y las distintas fibras se corresponden con las clases laterales de H. En el caso de que H sea normal en G tendremos que la base es a su vez un grupo de Lie. Retomamos los círculos y las esferas en la **fibración de Hopf** $\mathbb{S}^3(\mathbb{S}^2,\mathbb{S}^1)$, que es un caso particular de esta construcción. Lo describiremos paso a paso mediante el álgebra de *cuaterniones*:

1. La esfera $\mathbb{S}^3$ se corresponde con el conjunto de *cuaterniones unitarios*. Los **cuaterniones** $\mathbb{H}$ son vectores de $\mathbb{R}^4$ vistos de la forma $\xi = a + bi + cj + dk$, donde $a,b,c,d \in \mathbb{R}$ y los elementos i,j,k son considerados *unidades imaginarias* cuya multiplicación está dada por las relaciones $i^2 = j^2 = k^2 = ijk = -1$. El producto de cuaterniones se sigue de la multiplicación de unidades imaginarias y el producto de números reales. La condición de *unitario* se refiere a su norma como vector de $\mathbb{R}^4$, es decir $|\xi|^2 = a^2 + b^2 + c^2 + d^2 = 1$. Con respecto a esta norma el producto de cuaterniones cumple $|\xi\eta| = |\xi||\eta|$ para $\xi,\eta \in \mathbb{H}$. Esto implica que el producto por cuaterniones unitarios es una simetría de $\mathbb{S}^3$ y en consecuencia la conjugación por un elemento q unitario también lo es: $\xi \mapsto q\xi q^{-1}$. Por cierto, tenemos también la *conjugación* de cuaterniones en el sentido de una involución $\xi = a + bi + cj + dk \mapsto a - bi - cj - dk = \xi^*$ que cumple relaciones análogas al caso complejo: $\xi\xi^* = |\xi|^2$ y $(\xi\eta)^* = \eta^*\xi^*$. Para unitarios $q \in \mathbb{H}$ se cumple que $q^{-1} = q^*$

2. Identificamos $\mathbb{R}^3$ con el conjunto de cuaterniones imaginarios $i\mathbb{R} + j\mathbb{R} + k\mathbb{R}$ y

vemos a la esfera $\mathbb{S}^2$ en este espacio (como el conjunto de cuaterniones imaginarios unitarios). De esta manera los cuaterniones unitarios $\mathbb{S}^3$ pueden actuar en la esfera $\mathbb{S}^2$: simples cálculos nos revelan que la conjugación $\xi \mapsto q\xi q^*$ por cuaterniones unitarios manda cuaterniones imaginarios en cuaterniones imaginarios, dándonos un homomorfismo de grupos $\mathbb{S}^3 \longrightarrow SO(3)$ cuyo kernel es $\{1, -1\}$ (vale la pena mencionar que $\mathbb{S}^3$ es isomorfo a $SU(2)$; el homomorfimo $SU(2) \longrightarrow SO(3)$ es bien conocido en mecánica cuántica).

3. Es fácil ver que se puede parametrizar a los cuaterniones unitarios q, escribiéndolos como $q = Cos(\theta) + uSin(\theta)$ donde u es un cuaternión imaginario unitario, es decir elemento de $\mathbb{S}^2$, y θ es real. Además de que bajo la conjugación por este elemento obtenemos la rotación de $\mathbb{S}^2$ por un ángulo 2θ con centro en u.

4. Entonces definimos la proyección del haz $\pi : \mathbb{S}^3 \longrightarrow \mathbb{S}^2$, tomando un punto arbitrario en $\mathbb{S}^2$, digamos i, de la forma $\pi(q) = qiq^*$. Es decir, la imagen de nuestro cuaternión unitario q bajo la proyección es la imagen de i bajo la isometría inducida en $\mathbb{S}^2$ por q. Todos los elementos qw para $q \in \mathbb{S}^3$ y $w \in \{Cos(\theta) + iSin(\theta) \mid \theta \in \mathbb{R}\} \subset \mathbb{S}^3$ constituyen precisamente la fibra por q de esta proyección: si $\pi(q) = \pi(p)$ tenemos $qiq^* = pip^* \Leftrightarrow p^*qiq^*p = i \Leftrightarrow p^*qi(p^*q)^* = i$, lo que implica que la isometría inducida por p^*q tiene la forma $w = Cos(\theta) + iSin(\theta)$ de modo que $p = wq$ y en efecto $\pi(qw) = (qw)i(qw)^* = qwiw^*q^* = qiq^* = \pi(q)$. Así podemos ver la proyección π como la función cociente definida por la acción derecha de $\mathbb{S}^1 = \{Cos(\theta) + iSin(\theta) \mid \theta \in \mathbb{R}\}$ sobre $\mathbb{S}^3$ dada por el producto cuaterniónico $q \mapsto qw$.

2.6. Haz Asociado

Existe la noción más general de *haz fibrado* [3], donde la fibra puede ser distinta del grupo estructural, y el caso particular de los *haces vectoriales* en donde las fibras son espacios vectoriales. Es posible derivar estas estructuras a partir de la teoría de haces principales mediante la construcción de un **haz asociado** como sigue:

Partimos de un haz principal $P(M, G)$ y una variedad F en que G actúa por la izquierda. La idea es que haremos de F la *fibra estándar* (es decir, la preimagen de cualquier punto en la base bajo la proyección, salvo difeomorfismo) definiendo un nuevo espacio total y una proyección sobre la misma base, construyendo este nuevo haz con las trivializaciones locales del haz principal original. Sobre el producto $P \times F$ definimos la acción de $g \in G$ por $(p, f) \mapsto (pg, g^{-1}f)$. Llamemos $E = P \times_G F$ al espacio cociente que resulta de esta acción y por el momento lo consideramos sólo un conjunto hasta que le demos una estructura diferencial apropiada.

Ahora definimos lo que será nuestra nueva proyección a través de la proyección principal $\pi : P \longrightarrow M$, primero extendiéndola a $P \times F \longrightarrow M$ componiendo la proyección al primer término con π obteniendo $(p, f) \mapsto \pi(p)$ y luego induciendo la correspondiente proyección sobre el cociente $\pi_E : E \longrightarrow M$. Llamamos a $\pi_E^{-1}(x)$ la fibra de E sobre $x \in M$. Para cada $x \in M$ existe una vecindad $U \subseteq M$ en donde el haz principal se trivializa, es decir $\pi^{-1}(U) \simeq U \times G$. Entonces podemos identificar a $\pi_E^{-1}(U)$ con el cociente de $U \times G \times F$ por la acción definida anteriormente, ahora vista localmente en $\pi^{-1}(U) \times F$ como $(x, g, f) \mapsto (x, gh, h^{-1}f)$ para $h \in G$. Así se sigue que el difeomorfismo $\pi^{-1}(U) \simeq U \times G$ induce un difeomorfismo $\pi_E^{-1}(U) \simeq U \times F$ [14]. A través de estas trivializaciones locales podemos inducir una estructura diferenciable para E usando las subvariedades abiertas $\pi_E^{-1}(U)$ para una cubierta abierta apropiada de M. Con esta estructura notamos que la proyección π_E es una función diferenciable.

Para cada elemento $(p, f) \in P \times F$ denotamos por pf a su clase de equivalencia en el cociente $P \times_G F$ y por su definición se cumple que

$$(pg)f = p(gf)$$

Así podemos ver a cada $p \in P$ como un mapeo que manda a cada $f \in F$ en $pf \in E$ y en consecuencia de F en $F_x = \pi_E^{-1}(x)$, donde $x = \pi(p)$. Un **isomorfismo** entre dos fibras $F_x = \pi_E^{-1}(x)$ y $F_y = \pi_E^{-1}(y)$ es un mapeo que se pude representar como $q \circ p^{-1}$, donde $p \in \pi^{-1}(x)$ y $q \in \pi^{-1}(y)$ son vistos mapeos de F en F_x y F_y respectivamente. Entonces cada **automorfismo** de la fibra F_x (isomorfismo de la fibra en sí misma) se puede ver como $q \circ p^{-1}$, donde los elementos pertenecen a la

misma fibra ($p, q \in \pi^{-1}(x)$) lo que nos dice que $q = pg$ para una única $g \in G$ y el automorfismo se expresa como $p \circ g \circ p^{-1}$ para un elemento fijo arbitrario $p \in \pi^{-1}(x)$, de modo que el grupo de automorfismos de la fibra está dado por G como grupo estructural.

Hemos construido entonces el haz fibrado asociado con fibra F al haz principal $P(M, G)$, que se denota por $E(M, F, G, P)$. Se tiene a $E = P \times_G F$ como espacio total, π_E la proyección sobre la base M y G el grupo estructural.

El ejemplo paradigmático es el *haz tangente* a una variedad M de dimensión n (donde M es la base y las fibras son el espacio tangente a esta sobre cada punto) como haz asociado al haz de marcos sobre M tomando por fibra a $F = \mathbb{R}^n$ con la acción izquierda de $G = GL(m, \mathbb{R})$ dada naturalmente, pues este es el grupo de sus simetrías lineales como espacio vectorial. Ver [14].

2.7. Conexión

Dado un haz principal $P(M, G)$ se tiene una distribución intrínseca dada por los espacios tangentes a las fibras $\{V_p\}_{p \in P}$. Una **distribución** es una asignación (suave) de subespacios vectoriales al espacio tangente sobre los puntos de una variedad; se trata de un arreglo de *direccionamientos* de cualquier dimensión. La dimensión es una invariante topológica así que esta no cambia para una distribución sobre las componentes conexas de la variedad, por lo que podemos definir la dimensión de una distribución sobre una componente como la dimensión de los subespacios que la definen en esta. Una **conexión** en un haz principal es una distribución suave $\{H_p\}_{p \in P}$ *complementaria* a esta distribución intrínseca, en el sentido de que $T_pP = V_p \oplus H_p$. Además esta distribución debe portarse bien bajo la acción del grupo, es decir

$$H_{pg} = R_{g^*} H_p$$

donde R_{g^*} es la diferencial de la acción derecha de $g \in G$. En otras palabras: se requiere que la conexión sea invariante bajo la acción del grupo. Pensando en las fibras como espacios *verticales* del haz (pues se encuentran *sobre* cada punto de la

base) la conexión nos permite movernos de una forma determinada de una fibra a otra de forma *horizontal*. Una forma de caracterizar a los espacios verticales $\{V_p\}_{p\in P}$ es como el núcleo de la diferencial de la proyección vista como función entre los correspondientes haces tangentes, $d\pi : TP \longrightarrow TM$. Los espacios horizontales son entonces isomorfos bajo esta proyección a los espacios tangentes de la base, de modo que para cada vector tangente a un punto en la base podemos asignarle un único vector tangente horizontal a cada punto de la fibra. A su vez cada campo vectorial (y vector) en TP se puede descomponer en sus componentes vertical y horizontal. Para tener la noción de *movimiento horizontal* en el haz, una noción geométrica primitiva, basta explicar el procedimiento del **levantamiento de curvas** por la conexión:

Dada una curva γ con extremos en $\{x, y\}$ y la porción del haz sobre ella podemos levantar los vectores tangentes a una distribución 1-dimensional, que siempre es integrable en dicha porción (por el teorema de existencia y unicidad de soluciones para ecuaciones diferenciales). Partiendo de un punto arbitrario en la fibra $\pi^{-1}(x)$ seguimos la curva integral hasta llegar a un punto determinado en la fibra $\pi^{-1}(y)$. Es claro que cada una de estas curvas (una por cada elemento en la fibra) se proyecta bajo π a la curva original γ. Así estas curvas unen a las fibras de forma horizontal por las cuales podemos realizar el **transporte paralelo** de vectores de la fibra $\pi^{-1}(x)$ a la fibra $\pi^{-1}(y)$, lo que antes mencionamos intuitivamente como *movimiento horizontal*. Así pues una conexión en efecto *conecta* las distintas fibras en forma específica a lo largo de una curva en el espacio base.

En esta discusión está implícito un concepto que mencionamos al final de la sección sobre álgebras de Lie, hablamos entonces de **foliaciones**. Estas son esencialmente particiones de una variedad suave en variedades disjuntas de dimensión constante localmente: en el caso 1-dimensional hablamos del conjunto de curvas integrales de un campo suave que no se anule en ningún punto. La **integrabilidad** de una distribución se refiere a la existencia de una foliación (*maximal*) de la variedad tal que los espacios tangentes a las **hojas** (estas son las distintas componentes conexas de la foliación) son precisamente los subespacios de la distribución, de la misma forma en que las curvas integrales tienen como tangentes al campo que las

define [16].

La integrabilidad de una distribución suave está caracterizada por el **teorema de Frobenius**. Sabemos que sobre una variedad M el espacio de todas los campos vectoriales $\chi(M)$ forma un álgebra de Lie. La condición de integrabilidad dada por este teorema es que el subespacio de campos vectoriales restringidos a la distribución en cuestión sea además una subálgebra de Lie. Esto es decir que el corchete de Lie de dos campos vectoriales contenidos en la distribución sea un campo también contenido en ella. No siempre es posible integrar la distribución de la conexión (de espacios horizontales) a diferencia de lo que pasa con los verticales donde las fibras mismas constituyen la foliación integral. De hecho una condición necesaria y suficiente para que esto suceda es que el haz tenga curvatura cero [14]. En el caso antes mencionado de una distribución 1-dimensional arbitraria resulta fácil comprobar la condición del teorema de Frobenius: dos campos vectoriales en esta distribución se pueden describir como múltiplos escalares de un mismo campo vectorial ξ, que determina una base local de los direccionamientos 1-dimensionales. Si los campos en cuestión son $f\xi$ y $g\xi$, donde f y g son campos escalares, se tiene que su corchete es

$$[f\xi, g\xi] = (f(\xi g) + g(\xi f))\xi$$

el cual es nuevamente un múltiplo escalar de ξ, por lo que la distribución es integrable.

Para un tratamiento más detallado sobre los haces principales, conexión, curvatura y el teorema de Froebenius refiero al libro *Principal Bundles The Classical Case* por Stephen Sontz [20] publicado recientemente en compañia de un tomo en el que trata también el caso cuántico de los haces principales [21], mismo que expondremos en una primera aproximación en esta tesis.

Capítulo 3

Geometría Cuántica

La geometría cuántica es un entorno en que se extiende la noción clásica de espacio. Cuando hablamos de un **espacio**, en sentido clásico, queremos decir un conjunto de *puntos* dotados de cierta *estructura*. Por ejemplo, un espacio topológico es un conjunto de puntos con una topología dada por una familia de subconjuntos que llamamos *abiertos*. En el caso de un espacio métrico se tiene una función (valuada en números reales) con parejas de puntos como argumentos, llamada la *métrica*. Un espacio de medida toma ciertos subconjuntos como elementos de una *sigma-álgebra* para los que tenemos una *función de medida* valuada en los reales (o a veces en los complejos). En el caso de una variedad suave; un atlas y funciones de transición. Esta formalización se llevó a cabo entre los siglos XIX y XX; estos conceptos han demostrado ser precisas y elegantes formulaciones de propiedades geométricas de las que están dotados los modelos y las teorías científicas, que son a su vez abstracciones de los *sistemas* observables en la naturaleza, permitiéndonos un análisis profundo que ha dado lugar, por un lado, a grandes avances científico-tecnológicos y, por otro, al estudio de espacios abstractos alejados de nuestra intuición directa pero que están al alcance de dichos formalismos, dando lugar a una ampliación de los horizontes de la intuición. Trabajar en cierto entorno geométrico limitado permite identificar relaciones no evidentes a un nivel profundo, fundamentado en el lenguaje desarrollado. La Geometría Cuántica propone un paso en esta dirección: reubica las estructuras geométricas bajo otro marco conceptual, del álgebra y el

análisis funcional, y abre una brecha hacia el mundo de los espacios cuánticos, antes desconocidos, en los cuales, a pesar de su rareza (en contraste con los espacios antes mencionados, en general un espacio cuántico no tiene *puntos*), persiste la geometría.

Como concepto la geometría cuántica surge de la necesidad construir un formalismo coherente para la física cuántica. Desde sus inicios hasta su formulación moderna (por Schrödinger y Heisenberg) se han reconocido inconsistencias en los fundamentos de la teoría, que fueron siempre solventados por sus resultados experimentales, particularmente en la epistemología de la *realidad física* y la *medición* [18]. Einstein era consciente de incompatibilidades teóricas entre las variedades suaves usadas en relatividad y la cualidad discreta del mundo cuántico. Una idea para solucionar estas complicaciones consiste en introducir en la geometría las nociones cuánticas de *indeterminación* y *estocasticidad*. La geometría cuántica se propone como dicho formalismo para la introducción de estas *fluctuaciones cuánticas* negligibles a escala macroscópica, pero esenciales en longitudes cercanas a la longitud de Plank [6]. Es notable el hecho de que ejemplos de espacio cuántico surgen en situaciones de contexto clásico, en los cuales no es posible dar un estructura geométrica coherente al espacio, como es el caso del espacio cociente de un foliación ergódica o el de las teselaciones de Penrose [4].

Un primer paso conceptual que da lugar a la geometría cuántica está en la *representación algebráica* de las estructuras geométricas clásicas. Sobre un espacio dado podemos considerar el conjunto de funciones complejo-valuadas definidas sobre este espacio restringiéndonos al subconjunto de estas funciones que soportan la estructura geométrica en cuestión: en el caso de la topología nos interesan las funciones continuas complejo-valuadas; sobre la estructura diferencial, las funciones suaves complejo-valuadas (que forman un subconjunto de las continuas); para una medida sobre el espacio, las funciones medibles. Gracias a la estructura algebráica de los números complejos estos conjuntos de funciones, equipados con la norma apropiada, adquieren una estructura de álgebra C^* (pronunciado c-estrella) en el caso topológico, y de álgebra de Von Neumann para las medibles. Resulta que esta álgebra determina de forma biunívoca el espacio al que está asociado, siendo un *invariante algebráico*

perfecto: Para todo espacio de Hausdorff localmente compacto el álgebra de funciones forma un álgebra C* conmutativa y toda álgebra C^* conmutativa es el álgebra de funciones de algún espacio, dándonos una equivalencia de categorías. La relación es análoga entre álgebras de Von Neumann conmutativas y espacios de medida [4]. En este capítulo discutiremos principalmente aspectos topológico-diferenciales (la topología es considerada tradicionalmente la estructura geométrica más primitiva) de los espacios y su traducción en álgebras conmutativas, por lo que nuestros espacios clásicos modelo serán las variedades topológicas y las variedades suaves (dependiendo del contexto). Los espacios cuánticos resultan de la generalización a álgebras no-conmutativas, en las cuales los conceptos geométricos siguen teniendo sentido y donde los elementos del álgebra se interpretan como funciones continuas/suaves complejo-valuadas sobre el espacio cuántico (el cual no conocemos directamente sino a través de su álgebra). Se extiende la equivalencia a la más amplia categoría de espacios cuánticos [23] y álgebras no-conmutativas. Así vemos a la geometría clásica como un caso particular de la cuántica (el caso conmutativo). Es por eso que la geometría cuántica es llamada, de forma más precisa pero menos sugerente, geometría no-conmutativa. Al tratar directamente con el álgebra de funciones nos vemos obligados a manipular elementos geométricos globales en lugar del enfoque clásico de coordenadas, conjuntos abiertos y puntos.

3.1. Álgebras C*

Un álgebra C* es un álgebra normada completa sobre $\mathbb{C}$, A, con un operador $*$ (estrella)

$$* : A \longrightarrow A$$

$$* : a \longmapsto a^*$$

que cumple $(a^*)^* = a$ (involutividad), $(a+b)^* = a^* + b^*$ (aditividad), $(ab)^* = b^*a^*$ (anti-multiplicatividad) y $(\lambda a)^* = \overline{\lambda}a^*$ (anti-linealidad sobre los complejos) donde $a, b \in A$, además de la **condición C***:

$$||aa^*|| = ||a||^2$$

En particular la condición C* implica que $||a^*|| = ||a||$. El álgebra C* es entonces una $*$-álgebra normada completa sobre los complejos que cumple la condición C*. Notamos como el operador $*$ es análogo a la conjugación compleja y que sus propiedades son condiciones de compatibilidad con el resto de la estructura del álgebra. De hecho se verifica inmediatamente que los complejos $\mathbb{C}$ son un álgebra C*.

Resulta que para estos espacios los *morfismos* relevantes son los **$*$-homomorfismos (unitales)**, es decir funciones $\Phi : A \longrightarrow B$ entre álgebras C* que son lineales, multiplicativas y hermitianas (y que, en el caso de álgebras con unidad, que preservan dicha unidad), que para $z \in \mathbb{C}$ y $f, g \in A$ significa respectivamente que

$$\Phi(zf + g) = z\Phi(f) + \Phi(g)$$

$$\Phi(fg) = \Phi(f)\Phi(g)$$

$$\Phi(f^{*_A}) = \Phi(f)^{*_B}$$

$$(\Phi(1_A) = 1_B)$$

Un $*$-homomorfismo unital de un álgebra A en los complejos es llamado **caracter** de A.

Un hecho interesante es que en un álgebra C* la estructura métrica está completamente determinada por la estructura algebráica: para cada $*$-álgebra existe a lo más una única norma que la hace un álgebra C*. Se puede demostrar que todo $*$-homomorfismo de álgebras C* es una contracción (y en particular es continua respecto a las correspondientes métricas), es decir que para toda $f \in A$

$$||\Phi(f)||_B \leq ||f||_A$$

Esto implica como afirmamos antes que la métrica de un álgebra C* es única dada su estructura de $*$-álgebra y además que todo isomorfismo de álgebras C* es *isométrico* [13].

A continuación daremos unos ejemplos de álgebras C*. Trataremos las álgebras $C(X)$, $C_0(X)$ y $B(H)$ que son las relevantes al teorema de Gelfand-Naimark que expondremos más adelante.

Para un espacio topológico X compacto y de Hausdorff consideremos el conjunto de funciones continuas complejo valuadas $C(X) = \{f : X \longrightarrow \mathbb{C}\}$. Este espacio se enviste de forma natural con la suma, producto y producto por escalares dadas puntualmente por las operaciones en $\mathbb{C}$

$$(f+g)(x) = f(x) + g(x)$$

$$(fg)(x) = f(x)g(x)$$

$$(\alpha f)(x) = \alpha f(x)$$

con $f, g \in C(X)$, $x \in X$ y $\alpha \in \mathbb{C}$. Y junto con un operador $*$ inducido puntualmente por la conjugación compleja

$$f^*(x) = \overline{f(x)}$$

hace de $C(X)$ una $*$-álgebra conmutativa con la función constante 1 como unidad. Luego, si envestimos a este espacio con la norma del supremo

$$||f|| = \sup_{x \in X}\{|f(x)|\}$$

verificamos que $C(X)$ es un álgebra C* conmutativa con unidad. Sabemos además que esta norma está dada por el máximo en algún punto, ya que toda función sobre un compacto de Hausdorff está acotada y alcanza dicho máximo. En efecto la norma del supremo hace de C(X) un espacio completo [19].

De forma análoga el espacio $C_0(X)$ de las funciones continuas sobre un espacio de Hausdorff localmente compacto que decaen hacia el infinito (i.e. para las que $\forall \varepsilon > 0\ \exists K \subseteq X$ conjunto compacto tal que $|f(x)| \leq \varepsilon\ \forall x \in X - K$) es un álgebra C* conmutativa sin unidad (la función constante 1, la única alternativa de unidad para un espacio de funciones con operaciones puntuales, no es parte de este espacio pues no decrece al infinito salvo en el caso de que X sea compacto, en cuyo caso $C_0(X) \cong C(X)$).

El otro ejemplo importante, y del que podremos representar a todas las álgebras C*, es el espacio de operadores acotados $B(H)$ de un espacio de Hilbert complejo H. Recordamos que un espacio de Hilbert es un espacio vectorial con producto interno, completo bajo la correspondiente norma inducida. $B(H)$ está dado por las transformaciones lineales $T : H \longrightarrow H$ para los que se existe una constante que limita la expansión de los vectores, es decir que existe $M \in \mathbb{R}$ tal que para toda $v \in H$

$$||T(v)|| \leq M||v||$$

Estos son los operadores para los que se define la **norma de operadores**, que está definida como la mínima M que cumple dicha propiedad. El operador $*$ es la adjunción de operadores dada por el producto interno, es decir, que T^* es el único operador tal que para todo $v, w \in H$

$$< T(v), w >=< v, T^*(w) >$$

Así, junto con la suma de operadores y composición de estos como producto se verifica que $B(H)$ es precisamente un álgebra C*.

Como caso particular tenemos el caso en que H es de dimensión finita: el álgebra de matrices cuadradas complejas $M_n(\mathbb{C})$. Con la suma y producto tradicionales de matrices, el operador $*$ dado por la adjunción (transposición y conjugación de la matriz) y la norma de operadores esta es también un álgebra C* no conmutativa (para $n \geq 2$).

Hemos de mencionar que la noción de **C*-subálgebra** para álgebras C* es directa. Una **$*$-subálgebra** es un subespacio vectorial del álgebra, cerrado bajo el producto y el operador $*$. Claramente una $*$-subálgebra de un álgebra C* es a su vez C* si y solamente si es un subespacio cerrado (i.e. están contenidos todos los límites de sucesiones de Cauchy).

3.2. Teorema de Gelfand y Naimark

El **teorema de Gelfand-Naimark** nos dice que toda álgebra C* conmutativa es precisamente el álgebra de funciones continuas sobre un espacio localmente compacto (X) que decaen hacia el infinito $(C_0(X))$ o el álgebra de las funciones continuas $(C(X))$ en un espacio (X) compacto en el caso de tener unidad. El artículo que contiene la demostración de este resultado fue publicado en 1943 y en general se considera el lugar de nacimiento de la teoría de álgebras C* [11].

Si $F : X \longrightarrow Y$ es una transformación continua entre espacios topológicos compactos, entonces podemos definir un morfismo $\widehat{F} : C(Y) \longmapsto C(X)$ dado por el *pullback*:

$$\widehat{F}(f) = f \circ F \text{ , para } f \in C(Y)$$

Claramente $\widehat{F}$ es un $*$-homomorfismo. Las asignaciones $X \mapsto C(X)$ y $F \mapsto \widehat{F}$ definen un *funtor contravariante* de la *categoría* de espacios de Hausdorff compactos y las funciones continuas en la *categoría* de álgebras C* conmutativas con unidad y los $*$-homomorfismos unitales. Definiremos ahora un funtor en sentido opuesto: Dado un $*$-homomorfismo unital $F : A \longrightarrow B$ obtendremos de este funtor la expresión $\Omega(F) : \Omega(B) \longrightarrow \Omega(A)$. $\Omega(B)$ y $\Omega(A)$ son los correspondientes espacios de caracteres con la topología $*$-débil (definida en los espacios duales de estas álgebras como veremos en la siguiente sección) y $\Omega(F)$ está definida por $\Omega(F)(\kappa) = \kappa^*$, con $\kappa^* \in \Omega(A)$ el pullback de $\kappa \in \Omega(B)$

$$\kappa^*(a) = \kappa \circ F(a) \text{ para } a \in A$$

Israel Gelfand y Mark Naimark probaron que estos dos funtores son *cuasi-inversos* uno del otro, siendo cada uno una equivalencia de categorías [13]. Esto es equivalente a la existencia, para todo espacio de Hausdorff compacto X y toda álgebra C* conmutativa con unidad A, de los *isomorfismos naturales*

$$X \longrightarrow \Omega(C(X))$$

$$A \longrightarrow C(\Omega(A))$$

dados por $x \mapsto \kappa_x$ y $a \mapsto \hat{a}$ respectivamente (en cada caso estos homomorfismos llevan a un elemento en la correspondiente función de evaluación).

La equivalencia de categorías expresada anteriormente aplica también en el caso (no necesariamente compacto) de los espacios de Hausdorff localmente compactos y las álgebras conmutativas. Sin embargo, para que se dé dicha equivalencia, debemos restringir los morfismos permitidos a las **transformaciones propias** (aquellas transformaciones continuas para las que la imagen inversa de un compacto es compacta) y **$*$-homomorfismos propios**, que son los que mandan *unidades aproximativas* en unidades aproximativas [13]. Una **unidad aproximativa** en un álgebra A es una *red* $\{e_i\}_{i\in I}$ tal que para cada elemento $a \in A$ $e_i a \longrightarrow a$ y equivalentemente $ae_i \longrightarrow a$.

Otro de los resultados importantes en este artículo tiene que ver con la *representación* de las álgebras C*. El enunciado dice lo siguiente: Toda álgebra C* es isomorfa a una C*-subálgebra del álgebra $B(H)$ de operadores acotados sobre un espacio de Hilbert H. En particular toda álgebra C* A de dimensión finita es isomorfa a la suma directa de una cantidad finita de espacios de matrices sobre $\mathbb{C}$

$$A \cong M_{n_1}(\mathbb{C}) \oplus M_{n_2}(\mathbb{C}) \oplus ... \oplus M_{n_m}(\mathbb{C})$$

3.3. Conceptos Geométricos Fundamentales

En lo que sigue de esta exposición consideraremos en general a X como una variedad suave, salvo que se diga otra cosa, a razón de que en estos espacios es donde se desarrolla de manera más natural la intuición física del espacio y donde es posible definir la mayoría de los conceptos geométrico-diferenciales. Debemos mencionar que es en la reconciliación de las *fluctuaciones cuánticas* con la estructura suave del espacio-tiempo en relatividad general donde esta teoría matemática puede resultar de especial interés [6]. También tenemos la razón secundaria de que no perdemos nada esencial en el contexto de esta tesis al reducir la generalidad de esta discusión. De hecho, para nuestras intensiones, resulta indiferente si tomamos el álgebra de funciones continuas $C(X)$ o el álgebra de funciones suaves $C^\infty(X)$ de la variedad suave X pues nuestro interés está en generalizar las estructuras a álgebras arbitrarias (estas álgebras pueden a su vez pensarse como funciones continuas o suaves sobre el

espacio cuántico dependiendo de otras consideraciones).

Punto y Parte

Para un espacio compacto X es posible ver a cada punto $x \in X$ como un elemento del espacio dual de $C(X)$, es decir una función

$$\kappa_x : C(X) \longmapsto \mathbb{C}$$

dada por

$$\kappa_x(f) = f(x)$$

Estamos viendo entonces a cada punto como una *función de evaluación* de los elementos de $C(X)$ sobre sí mismo. Se verifica fácilmente que esta función de evaluación es un $*$-homomorfismo unital de álgebras, es decir que κ_x es un caracter. Para $x \neq y$ se tiene que $\kappa_x \neq \kappa_y$, por lo que la asociación $x \mapsto \kappa_x$ es inyectiva.

Ya hemos definido a las funciones $\kappa : A \longrightarrow \mathbb{C}$ que son $*$-homomorfismos (unitales) de álgebras como **caracteres** del álgebra A. El resultado concreto que nos da el teorema de Gelfand-Naimark es el siguiente: dada un álgebra conmutativa con unidad arbitraria A, el conjunto de caracteres $\Omega(A)$ en el espacio dual, A^* con la topología $*$-débil, es un subespacio $X := \Omega(A) \subseteq A^*$ tal que $C(X) \cong A$. La **topología $*$-débil** es la topología más gruesa (es decir, con la menor cantidad de conjuntos abiertos) en A^* que hace a las funciones evaluación inducidas por los elementos de A continuas: para $f \in A$, la función evaluación es $T_f : A^* \longrightarrow \mathbb{C}$, donde $T_f(\phi) = \phi(f)$ para $\phi \in A^*$. De esta forma tenemos una generalización del concepto geométrico de **punto** a la noción algebráica de caracter.

Con un conjunto cerrado Λ en un espacio X podemos construir el ideal $J_\Lambda = \{f \in A \mid f|_\Lambda = 0\}$, donde $A = C(X)$, de aquellas funciones que se anulan en dicho conjunto cerrado. De forma inversa podemos pensar que un ideal del álgebra es equivalente a un conjunto cerrado, es decir, a una *parte* de X. Fijémonos en lo siguiente sobre el cociente de álgebras: Si A y B son álgebras C* y tenemos un $*$-homomorfismo

suprayectivo $F : A \longrightarrow B$, podemos construir un isomorfismo de álgebras $\widetilde{F} : A/J \longrightarrow B$, donde $J = Ker(F)$, que cumple $\widetilde{F} \circ p = F$ donde $p : A \longrightarrow A/J$ es la proyección canónica. Con las operaciones por representantes y la norma dada por $||a|| = \text{ínf}_{b \in J}\{||a + b||\}$, se tiene que A/J es a su vez un álgebra C*. En particular, si F corresponde a la restricción a Λ de las funciones en $C(X)$ tenemos que

$$C(X)/J_\Lambda = C(\Lambda)$$

Sin embargo resulta que casi todas las álgebras no-conmutativas son simples, por lo que no podemos distinguir *partes* en los espacios cuánticos. A su vez estas álgebras C* no-conmutativas no tienen caracteres, por lo que se trata de espacios sin puntos [6].

Si bien podría considerarse escandaloso hablar de espacios sin partes o puntos, los espacios cuánticos presentan estructuras y conceptos a su vez fundamentales en geometría.

Transformaciones y Simetrías

Las funciones suaves entre espacios inducen a su vez homomorfismos de las álgebras correspondientes. Si $F : X \longrightarrow Y$ es una transformación entre espacios tenemos el correspondiente homomorfismo $\widehat{F} : C(Y) \longmapsto C(X)$ dado por el *pullback*:

$$\widehat{F}(f) = f \circ F$$

Resulta entonces que $\widehat{F}$ es inyectiva si y sólo si F es suprayectiva, e inversamente $\widehat{F}$ es suprayectiva si F es inyectiva. Como consecuencias un homeomorfismo (difeomorfismo) entre espacios induce un isomorfismo de las correspondientes álgebras. Así tenemos que las simetrías de los espacios están dados por simetrías de las álgebras. Los automorfismos de un álgebra C* no-conmutativa son entonces simetrías de un espacio cuántico. Existe también la simetría de un espacio dada por la acción de un grupo, como vimos en el capítulo anterior, pero abordaremos esta posibilidad cuando tratemos con los grupos cuánticos.

Campo Vectorial

Los campos vectoriales también tienen equivalentes cuánticos. Un campo vectorial suave en una variedad X nos permite *derivar* los elementos del álgebra $A = C^\infty(X)$ de funciones suaves sobre la variedad (tomando en cada punto la derivada direccional inducida por el vector en ese punto). En efecto el campo vectorial induce una **derivación**. Una derivación en un álgebra es una función $\varphi : A \longrightarrow A$ lineal no trivial que cumple la **regla de Leibniz**:

$$\varphi(fg) = \varphi(f)g + f\varphi(g)$$

Se puede demostrar que el conjunto de derivaciones del álgebra de funciones suaves sobre una variedad suave es isomorfo al conjunto de campos vectoriales [14], tratándose en ambos casos de un álgebra de Lie. Partiendo de un álgebra no-conmutativa arbitraria podemos entonces definir los **campos vectoriales** como **derivaciones** del álgebra.

Producto Cartesiano y Unión Disjunta

Intuitivamente es claro que el álgebra de funciones de la unión disjunta de dos espacios está dada por parejas de funciones de cada uno

$$C(X \sqcup Y) \cong C(X) \oplus C(Y)$$

pues de la misma forma en que cada espacio mantiene una topología propia en la unión, cada funcional está descrita completamente por su restricción a cada uno de los componentes de esta. Así, la suma directa de álgebras C* es geométricamente la unión disjunta de espacios cuánticos (es un álgebra C* con las operaciones por componentes). La situación es distinta con el producto cartesiano, en el cual ambos espacios se combinan en un objeto con una topología no trivial. En este caso el álgebra correspondiente está dada a través del producto tensorial

$$C(X \times Y) \cong C(X) \otimes C(Y)$$

Sin embargo en el caso no-conmutativo el producto tensorial algebráico de dos álgebras C* puede no ser completo, la identidad anterior se refiere al *producto tensorial C**. Sean A y B dos álgebras C*, entonces necesitamos que la norma de $A \otimes_{alg} B$ cumpla

$$||a \otimes b|| = ||a||||b||$$

y definimos el **producto tensorial C*** por la cerradura del espacio bajo dicha norma:

$$A \otimes B = \overline{A \otimes_{alg} B}$$

En general es difícil describir explícitamente el álgebra C(X) para un espacio compacto de Hausdorff arbitrario X pero esto es posible para espacios suficientemente sencillos:

Sea $X = \{\cdot\}$ el espacio singular de un punto, entonces es evidente que $C(X) = \mathbb{C}$. Se sigue entonces que el espacio $X = \{P_1, P_2, ..., P_n\}$ que consta de n puntos nos da $C(X) = \mathbb{C}^n$.

En el caso del círculo unitario tenemos que $C(\mathbb{S}^1) \cong < U >= \{\sum_{i=1}^{i=n} c_i U^i \mid n \in \mathbb{Z}, c_i \in \mathbb{C}\}$ donde U es un elemento unitario, es decir $UU^* = 1$ o equivalentemente $U : \mathbb{S}^1 \longrightarrow \mathbb{C}$ es tal que su imagen es precisamente $\mathbb{S}^1 \subset \mathbb{C}$ (esta álgebra se puede describir como el álgebra libre sobre el generador U introduciendo la operación $*$ y la relación $UU^* = 1$). Para verlo evaluamos un caracter en el generador U del álgebra lo que nos indica que $\kappa(U^*) = \kappa(U^{-1})$ o equivalentemente $\overline{\kappa(U)} = \frac{1}{\kappa(U)}$, de modo que $|\kappa(U)|^2 = 1$. Es así que cada caracter está determinado por un complejo de módulo 1, es decir que esta álgebra corresponde precisamente a $\mathbb{S}^1$.

Así podemos calcular el álgebra de funciones del toro $\mathbb{S}^1 \times \mathbb{S}^1$, que es $< U > \otimes < V >$ con U y V elementos unitarios.

Compactificaciones

Dos compactificaciones fundamentales en topología son la de Alexandrov y la de

Stone-Cech. Una compactificación corresponde a la construcción de un espacio compacto a partir de un espacio topológico. En términos más precisos, se trata de un espacio compacto en el que podemos *encajar* de forma densa un espacio topológico inicial. Como lo sugiere el teorema de Gelfand-Naimark, podemos asociar la compacidad de un espacio con la existencia de un neutro/unidad en su álgebra de funciones:

A nivel de las álgebras C* la *compactificación de Alexandrov* corresponde a la unitalización del álgebra (siendo el álgebra C* unital más pequeña que contiene al álgebra inicial como un ideal). La compactificación de Alexandrov consiste en añadir el infinito al espacio para compactarlo, como es fácil visualizar en la proyección estereográfica (compactificación de $\mathbb{R}^2$ en $\mathbb{S}^1$). Por otro lado tenemos que la *compactificación de Stone-Cech*, que es la compactificación más grande en el sentido de que cualquier función continua del espacio en un compacto se *factoriza* de forma única por esta (su propiedad universal), se realiza al nivel de las álgebras C* como el espacio asociado al **álgebra de multiplicadores**, definida como el álgebra C* $M(A)$ más grande que contiene al álgebra inicial A como un ideal *esencial* o más precisamente por una propiedad universal dual a la de la compactificación: para cualquier álgebra B que contenga al álgebra A como ideal esencial existe un único $*$-homomorfismo $B \longrightarrow M(A)$ que se restringe a la identidad en A.

3.4. El Toro Cuántico

Consideremos un álgebra C* generada por dos elementos *unitarios* U y V, simbólicamente $B =< U, V >$. Esto es el álgebra libre en dos generadores (que consta de todos los productos entre ambos y sus $*$, y todas las combinaciones lineales finitas de estos productos) módulo las relaciones $UU^* = VV^* = 1$, junto con una condición especial de no-conmutatividad: $UV = zVU$ donde $z \in \mathbb{C} \setminus \{0\}$. El caso $z = 1$ corresponde al del álgebra conmutativa en estos dos generadores, y si κ es un caracter de esta álgebra tenemos que:

$$\kappa(UU^*) = \kappa(VV^*) = \kappa(1) \Rightarrow \kappa(U)\overline{\kappa(U)} = \kappa(V)\overline{\kappa(V)} = 1$$

$$\Rightarrow |\kappa(U)| = 1 = |\kappa(V)|$$

Como cada caracter de esta álgebra está determinado por sus valores en los generadores, esta última ecuación nos dice que cada caracter es descrito por una pareja de complejos unitarios. Inversamente, dada una pareja de complejos unitarios podemos definir un caracter definiendo su valor en los generadores como dicha pareja. De este modo los caracteres entran en correspondencia biunívoca con $\mathbb{S}^1 \times \mathbb{S}^1$: esta álgebra es el álgebra de funciones complejas sobre el **toro** y de acuerdo a lo que vimos antes del álgebra del toro tenemos $< U, V > \cong < U > \otimes < V >$. Resulta inmediato descubrir que la definición de estos caracteres sólo es válida para el caso conmutativo:

$$\kappa(UV) = \kappa(zVU) \Rightarrow \kappa(U)\kappa(V) = z\kappa(V)\kappa(U) = z\kappa(U)\kappa(V) \Rightarrow z = 1$$

Tenemos entonces para $z \neq 1$ un álgebra no conmutativa B con unidad representando a un espacio cuántico compacto (por tratarse de un álgebra con unidad) cuyo *límite conmutativo* es el toro, llamamos a este espacio el **toro cuántico**. La idea aquí nos puede recordar a la ruptura de simetrías en teoría cuántica: Woronowicz expone que la existencia de los grupos cuánticos permite deformaciones continuas no triviales de grupos de simetría, que describen *observables* físicas, que de otra forma sólo admiten deformaciones triviales [25]. El toro cuántico es un bonito ejemplo de espacio cuántico pues tenemos el caso del toro clásico *a un parámetro de distancia*, describiendo una *cuantización* del toro.

3.5. Grupo Cuántico y Álgebra de Hopf

Supongamos que G es un grupo de Lie compacto. Hemos visto como traducir al lenguaje de álgebras C* ciertas estructuras y construcciones algebráicas. Entre estas la más relevante para nosotros será la de grupo cuántico como generalización de grupo de Lie. Como vimos en el capítulo anterior, el grupo está determinado por una operación binaria dada por una función suave

$$\rho : G \times G \longrightarrow G$$

asociativa, con la existencia de un neutro $e \in G$ y una *función de inversión*. Podemos enunciar estas propiedades en términos de funciones suaves que realizan la conmutatividad de ciertos diagramas, en el caso de la asociatividad tenemos

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\rho \times Id} & G \times G \\ \downarrow{\scriptstyle Id \times \rho} & & \downarrow{\scriptstyle \rho} \\ G \times G & \xrightarrow{\rho} & G \end{array}$$

El neutro se puede definir como una función

$$e : \{\cdot\} \longrightarrow G$$

que hace conmutar los siguientes diagramas, donde p_i es la proyección en el i-ésimo término del producto cartesiano

$$\begin{array}{ccc} \{\cdot\} \times G & \xrightarrow{e \times Id} & G \times G \\ & \searrow^{p_2} & \downarrow{\scriptstyle \rho} \\ & & G \end{array}$$

$$\begin{array}{ccc} G \times \{\cdot\} & \xrightarrow{Id \times e} & G \times G \\ & \searrow^{p_1} & \downarrow{\scriptstyle \rho} \\ & & G \end{array}$$

que corresponden al neutro por la izquierda y por la derecha respectivamente. Análogamente expresamos la existencia de inversos por una función

$$\theta : G \longrightarrow G$$

llamada **función de inversión**, que hace conmutar los siguientes diagramas (nuevamente, representando la propiedad izquierda y derecha, de los inversos, respectivamente) donde *diag* es el mapeo diagonal $g \mapsto (g, g)$:

$$\begin{array}{ccccc} G & \xrightarrow{diag} & G \times G & \xrightarrow{\theta \times id} & G \times G \\ \downarrow & & & & \downarrow{\scriptstyle \rho} \\ \{\cdot\} & & \xrightarrow{\quad e \quad} & & G \end{array}$$

$$\begin{array}{ccccc} G & \xrightarrow{diag} & G \times G & \xrightarrow{id\times\theta} & G \times G \\ \downarrow & & & & \downarrow \rho \\ \{\cdot\} & & \xrightarrow{\qquad e \qquad} & & G \end{array}$$

Ahora, elaborando sobre la teoría expuesta en lo que va de este capítulo, *dualizamos* esta estructura al mundo algebráico reemplazando cada espacio en estos diagramas (por ejemplo G) por su correspondiente álgebra de funciones ($A = C(G)$) y cada transformación por el correspondiente morfismo, que recordamos está dado por el pullback. La orientación de los diagramas quedará invertida por la contravarianza de este funtor. Entonces tenemos para $A = C(G)$ morfismos de álgebras

$$\phi := \hat{\rho} : A \longrightarrow A \otimes A \ , \ \epsilon := \hat{e} : A \longrightarrow \mathbb{C} \text{ y } \zeta := \hat{\theta} : A \longrightarrow A$$

que hacen conmutar los siguientes diagramas

$$\begin{array}{ccc} A & \xrightarrow{\phi} & A \otimes A \\ \downarrow \phi & & \downarrow \phi\otimes Id_A \\ A \otimes A & \xrightarrow{Id_A\otimes\phi} & A \otimes A \otimes A \end{array}$$

$$\begin{array}{ccc} A & \xrightarrow{\phi} & A \otimes A \\ & \searrow^{\hat{p_2}} & \downarrow \epsilon\otimes Id_A \\ & & \mathbb{C} \otimes A \end{array}$$

$$\begin{array}{ccc} A & \xrightarrow{\phi} & A \otimes A \\ & & \downarrow \zeta\otimes Id_A \\ \downarrow \epsilon & & A \otimes A \\ & & \downarrow \widehat{diag} \\ \mathbb{C} & \xhookrightarrow{\iota} & A \end{array}$$

Hemos utilizado que el pullback del producto cartesiano de mapeos se traduce al producto tensorial del pullback de los mismos, de donde obtuvimos los homomorfismos

$$\widehat{\rho \times Id_G} = \hat{\rho} \otimes \widehat{Id_G},\ \widehat{Id_G \times \rho} = \widehat{Id_G} \otimes \hat{\rho},\ \widehat{e \times Id} = \hat{e} \otimes \widehat{Id_G} \text{ y } \ \widehat{\theta \times Id_G} = \hat{\theta} \otimes \widehat{Id_G}$$

en los que hicimos el cambio de notación por ϕ, ϵ y ζ. Además usamos que naturalmente $\widehat{Id_G} = Id_A$ (esta es una de las propiedades de un *funtor*).

El primer diagrama corresponde con la asociatividad de la multiplicación ρ (describe la propiedad de **co-asociatividad**), mientras el segundo y tercero corresponden a las propiedades izquierdas del neutro y de la función de inversión (las derechas se tienen análogamente).

Mediante un salto (no trivial como veremos al final de esta sección) generalizamos directamente esta estructura pensando en A como un álgebra C* arbitraria, no necesariamente conmutativa, dotada de funciones ϕ, ϵ y ζ (jugando los papeles de $\hat{\rho}$, $\hat{e}$ y $\hat{\theta}$), que hacen conmutar estos diagramas; llamamos a estos morfismos la **co-multiplicación**, el **co-neutro** y la **antípoda**. Un espacio cuántico dado por un álgebra C* junto con una co-multiplicación co-asociativa con co-neutro y antípoda es la noción de **grupo cuántico** que usaremos en el siguiente capítulo para las simetrías del haz principal cuántico. Hay que notar, consecuencia directa de la actual presentación, que el grupo de Lie resulta un caso particular de grupo cuántico (cuando A es conmutativa).

Hay que comentar unos detalles importantes de los grupos cuánticos así definidos. Al dualizar la estructura como hemos hecho resulta que:

- El co-neutro ϵ es un caracter por lo que cada grupo cuántico tiene por lo menos un punto.
- El pullback del mapeo diagonal falla en ser un homomorfismo continuo en general. En ciertos casos podemos representar a este mapeo como el producto del álgebra: $x \otimes y \mapsto xy$.
- La antípoda es un anti-homomorfismo, queriendo decir que ζ^2 es un homomorfismo (de hecho, por corresponder a la función de inversión, en el caso clásico $\zeta^2 = \hat{\theta}^2$ es la identidad). La antípoda para el grupo cuántico cumple

$$\zeta(ab) = \zeta(b)\zeta(a)$$

$$\zeta(a^*) = (\zeta^{-1}(a))^* \Leftrightarrow \zeta(\zeta(a^*)^*) = a \tag{3.1}$$

por lo que es un homomorfismo continuo sólo en el caso en que el álgebra es conmutativa.

La ecuación (3.1) es llamada **condición de Woronowicz**; se refiere al hecho de que el grupo cuántico es un **álgebra de Hopf involutiva** o **$*$-álgebra de Hopf**. Un álgebra de Hopf es al mismo tiempo *álgebra* y *co-álgebra* asociativa, provista de un mapeo antípoda [17]. En el caso conmutativo la antípoda es involutiva pues la definimos a partir de la función de inversión del grupo, pero en general la antípoda puede ser un anti-homomorfismo no involutivo. La *estructura* representa la geometría del espacio (cuántico), mientras la *co-estructura* su aspecto algebráico como grupo de simetrías.

Podemos ver una asimetría conceptual del caso conmutativo y el caso no-conmutativo: En el segundo nuestros morfismos dejan la categoría correspondiente (ζ no es homomorfismo). Además, la existencia de un punto clásico en cada grupo cuántico (dado por el co-neutro) *deshomogeiniza* la teoría. El trabajo reciente de Durdevich resuelve esta situación mediante la *categoría trenzada* como un modelo general de simetría que incluye en un mismo marco conceptual a grupos clásicos y cuánticos [9].

3.6. $SU(2)$ Cuántico

Para cerrar el capítulo presentaremos un ejemplo de grupo cuántico desarrollado por Woronowicz [24]. Este es un caso particular de su teoría sobre *grupo cuánticos compactos* cuya construcción consiste en un álgebra C* generada por las entradas de una matriz cuadrada [25].

El grupo $SU(2)$ clásico consiste en los operadores unitarios con determinante igual a 1, que podemos representar como un conjunto de matrices de la forma

$$U = \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \mid a, b \in \mathbb{C} \text{ y } |a|^2 + |b|^2 = 1$$

donde la última ecuación se deriva de la restricción sobre el determinante de U.

Con esto en mente consideremos la matriz

$$U = \{u_{ij}\}_{i,j\in\{1,2\}} = \begin{pmatrix} \alpha & -\mu\gamma^* \\ \gamma & \alpha^* \end{pmatrix}$$

cuya forma es análoga a las matrices de $SU(2)$ salvo un parámetro $\mu \in [-1,1] \setminus \{0\}$ de *no-conmutatividad* o *deformación*. La entradas de esta matriz son elementos abstractos, con los que construiremos el grupo cuántico, a los que aplicamos una operación $*$ en lugar de la conjugación compleja. Suponer que esta matriz es unitaria en el sentido usual quiere decir que bajo el producto de matrices cumple $UU^* = 1$ y $U^*U = 1$, de donde obtenemos (respectivamente por columna) las siguientes relaciones

- $\alpha\alpha^* + \mu^2\gamma^*\gamma = 1$
- $\alpha\gamma^* = \mu\gamma^*\alpha$
- $\gamma\alpha^* = \mu\alpha^*\gamma$
- $\gamma\gamma^* + \alpha^*\alpha = 1$
- $\alpha^*\alpha + \gamma^*\gamma = 1$
- $\gamma^*\alpha^* = \mu\alpha^*\gamma^*$
- $\alpha\gamma = \mu\gamma\alpha$
- $\mu^2\gamma\gamma^* + \alpha\alpha^* = 1$

que podemos reducir, sin redundancias, al siguiente conjunto ($\diamond$)

- $\diamond$ $\alpha\alpha^* + \mu^2\gamma^*\gamma = 1$
- $\diamond$ $\alpha^*\alpha + \gamma^*\gamma = 1$
- $\diamond$ $\alpha\gamma^* = \mu\gamma^*\alpha$
- $\diamond$ $\alpha\gamma = \mu\gamma\alpha$
- $\diamond$ $\gamma\gamma^* = \gamma^*\gamma$

La forma de la matriz U no es arbitraria, se deriva de consideraciones concernientes al determinante de la matriz: en lugar de solicitar la **unimodularidad** de U (es decir $det(U) = 1$) se requiere de U una condición de unimodularidad *torcida* [24] que se define para operadores en $M_2(B)$, el espacio de matrices con entradas en un

álgebra no-conmutativa B. Esta condición nos da tanto la forma de la matriz como el conjunto de relaciones $\diamond$.

Ahora necesitamos de unas construcciones algebráicas que nos serán de utilidad en el resto de este trabajo: el *álgebra de grupo* y el *álgebra libre*. Estos objetos, junto con el *grupo libre* y *espacio vectorial libre*, resultan de una operación a nivel conceptual: el uso de reglas de sintaxis algebráicas sobre un conjunto de elementos para construir un objeto con los mínimos requerimientos para ser compatible con la estructura en cuestión (grupo, espacio vectorial, álgebra). Partiendo de un grupo $G = \{g_\alpha\}_{\alpha\in\Lambda}$ (indexado por un conjunto de índices Λ) cuyos elementos llamamos generadores y un campo de K, denotamos por $K(G)$ al espacio vectorial libre generado por los elementos de G sobre el campo dado K. A este espacio le damos estructura de álgebra extendiendo linealmente el producto del grupo. Llamamos a $K(G)$ el **álgebra de grupo** de G sobre K. Partiendo de menos estructura, con un conjunto D, podemos realizar la construcción anterior usando el grupo libre generado por este conjunto, $G =< D >$ (recordamos que el **grupo libre** es el grupo de *palabras* utilizando a D como *abecedario*). Llamamos a esta estructura el **álgebra libre** sobre K generada por D, la denotamos $K[D]$. El espacio de polinomios $F[x]$ que vimos en el primer capítulo se puede pensar como el álgebra libre generada por el conjunto $\{x\}$ sobre un campo F; de hecho podemos pensar al álgebra libre como un equivalente no conmutativo de los espacios de polinomios (en n variables).

Nuestro interés está en el álgebra C* generada por los elementos α y γ (de las entradas de la matriz U) junto con las relaciones $\diamond$, que denotamos A. Esta se construye como la $*$-álgebra libre sobre $\mathbb{C}$ generada por las entradas de U, esto es el álgebra libre $\mathbb{C}[\alpha, \gamma, \alpha^*, \gamma^*]$ junto al operador $*$ (definido como el homomorfismo anti-multiplicativo que manda $\alpha \mapsto \alpha^*$, $\gamma \mapsto \gamma^*$ y viceversa) y las relaciones $\diamond$. Introducir relaciones en un álgebra (y en otras estructuras algebráicas) corresponde usualmente a tomar el cociente por el ideal N generado por dichas relaciones. Sin embargo en este caso haremos algo muy parecido a nivel de las *representaciones* del álgebra. Sobre la $*$-álgebra $\mathbb{C}[\alpha, \gamma, \alpha^*, \gamma^*]$ definimos una métrica dada por

$$||a|| = sup_\pi ||\pi(a)||$$

donde el supremo se toma sobre las *representaciones* π para las cuales $\pi(\alpha)$ y $\pi(\gamma)$ cumplen las relaciones $\diamond$. Esta métrica nos da una C*-*seminorma* en $\mathbb{C}[\alpha, \gamma, \alpha^*, \gamma^*]$. Con esto obtenemos un ideal (*bilateral*)

$$N = \{a \in \mathbb{C}[\alpha, \gamma, \alpha^*, \gamma^*] \mid ||a|| = 0\}$$

y llegamos a una $*$-álgebra normada

$$\mathcal{A} = \mathbb{C}[\alpha, \gamma, \alpha^*, \gamma^*]/N$$

de la que, completando, obtenemos nuestra álgebra A.

Woronowicz piensa $\mathcal{A}$ como el álgebra funciones polinomiales sobre un *pseudo-espacio* (espacio cuántico), y A como el álgebra de funciones continuas sobre dicho espacio. Para nosotros A *es* nuestro $SU(2)$ cuántico, que Woronowicz identifica con los elementos de una familia *uniparamétrica* $S_\mu U(2)$, donde $\mu \in [-1, 1] \setminus \{0\}$ es el parámetro de no-conmutatividad.

La co-estructura de A puede ser descrita por el producto (de matrices) de U consigo misma, salvo que el producto de las entradas es sustituido por el producto tensorial. Es decir, definimos la co-multiplicación sobre las entradas de U (generadores de A) como

$$\phi(u_{ij}) = \sum_k u_{ik} \otimes u_{kj}$$

junto a un co-neutro dado por

$$\epsilon(u_{ij}) = \delta_{ij}$$

y un operador antípoda (que es como la conjugación y transposición de matrices)

$$\kappa(u_{ij}) = u_{ij}^*$$

Ahora demostraremos que A es un grupo cuántico como lo definimos en la sección anterior. Calcularemos explícitamente para las propiedades izquierdas, nuevamente a razón de que para las derechas todo es análogo:

El diagrama de co-asociatividad corresponde a la ecuación

$$(\phi \otimes Id)(\phi) = (Id \otimes \phi)(\phi)$$

Para un generador evaluamos cada lado de la ecuación

$$(\phi \otimes Id)(\phi)(u_{ij}) = (\phi \otimes Id) \sum_k u_{ik} \otimes u_{kj} = \sum_k (\sum_l u_{il} \otimes u_{lk}) \otimes u_{kj} = \sum_{k,l} u_{il} \otimes u_{lk} \otimes u_{kj}$$

$$(Id \otimes \phi)(\phi)(u_{ij}) = (Id \otimes \phi) \sum_k u_{ik} \otimes u_{kj} = \sum_k u_{ik} \otimes (\sum_l u_{kl} \otimes u_{lj}) = \sum_{k,l} u_{ik} \otimes u_{kl} \otimes u_{lj}$$

notando que los últimos términos son iguales pues difieren sólo en la posición relativa de los índices k y l. Luego tratamos con el co-neutro, cuya propiedad izquierda se traduce en

$$(\epsilon \otimes Id)(\phi) = \hat{p_2}$$

Recordemos que p_2 corresponde a la proyección $\{\cdot\} \times G \longrightarrow G$, que es claramente un difeomorfismo. A nivel de las álgebras $\hat{p_2}$ es el *isomorfismo natural* $A \longrightarrow \mathbb{C} \otimes A$ dado por $a \mapsto 1 \otimes a$. Dadas estas consideraciones calculamos

$$(\epsilon \otimes Id)(\phi)(u_{ij}) = (\epsilon \otimes Id)(\sum_k u_{ik} \otimes u_{kj}) = \sum_k \delta_{ik} \otimes u_{kj} = 1 \otimes u_{ij} = \hat{p_2}(u_{ij})$$

Por último veremos la propiedad izquierda de la antípoda siguiendo el mismo esquema. Esta propiedad se expresa por la ecuación

$$\widehat{diag}(\zeta \otimes Id)(\phi) = \iota(\epsilon)$$

Recordando la relación del mapeo diagonal con el producto del álgebra, evaluamos en un generador para confirmar nuestra afirmación

$$\widehat{diag}(\zeta \otimes Id)(\phi)(u_{ij}) = \widehat{diag}(\zeta \otimes Id)(\sum_k u_{ik} \otimes u_{kj}) = \widehat{diag}(\sum_k u_{ki}^* \otimes u_{kj})$$

$$= \sum_k u_{ki}^* u_{kj} = \delta_{ij} = \iota(\epsilon)(u_{ij})$$

obteniendo la penúltima igualdad de las relaciones $\diamond$ al calcular directamente los sumandos usando las entradas de U (tomando las 4 posibilidades para $i, j \in \{1, 2\}$). $\square$

Capítulo 4

Haces Principales Cuánticos

En este último capítulo hemos de conectar las teorías antes expuestas en una generalización cuántica de los haces principales. El haz principal cuántico está conformado por un espacio cuántico sobre el que actúa un grupo cuántico como grupo estructural, siendo entonces el grupo de simetrías internas de un espacio cuántico base. Procederemos paso a paso guiados intuitivamente por la traducción algebráica del caso clásico: pensando inicialmente a los morfismos de álgebras como imágenes *funtoriales* de transformaciones entre espacios clásicos, las consideramos de inmediato como morfismos generales entre álgebras no necesariamente conmutativas y por ende correspondientes a transformaciones entre espacios cuánticos. Hallamos la conexión entre la teoría de Galois y los haces principales cuánticos representando al haz principal por una *extensión de Hopf-Galois* de álgebras C*. Exploramos la definición general de una extensión de Hopf-Galois en la que álgebras y álgebras de Hopf juegan un papel análogo a los campos y sus grupos de automorfismos, como vimos al estudiar las extensiones de campo, descubriendo a las extensiones de Galois como un caso particular.

4.1. Acción de Grupo Cuántico

Podemos definir al haz principal en primer lugar, a través de la acción del grupo cuántico. La acción de grupo clásica está dada por una función

$$\phi : P \times G \longrightarrow P$$

que cumple una condición de asociatividad, que nos dice que la composición de la acción de dos elementos está dada por su producto, que podemos describir como la conmutatividad del siguiente diagrama

$$\begin{array}{ccc} P \times G \times G & \xrightarrow{\phi \times Id_G} & P \times G \\ \downarrow{\scriptstyle Id_P \times \rho} & & \downarrow{\scriptstyle \phi} \\ P \times G & \xrightarrow{\phi} & P \end{array}$$

donde ρ es el producto del grupo. Representando a G por su $*$-álgebra de Hopf $A = C^\infty(G)$, a P por su álgebra C*, $B = C^\infty(P)$ y a las transformaciones por sus respectivos pullbacks *dualizamos* el diagrama anterior para obtener

$$\begin{array}{ccc} B & \xrightarrow{\hat{\phi}} & B \otimes A \\ \downarrow{\scriptstyle \hat{\phi}} & & \downarrow{\scriptstyle \widehat{Id_P} \otimes \hat{\rho}} \\ B \otimes A & \xrightarrow{\hat{\phi} \otimes \widehat{Id_G}} & B \otimes A \otimes A \end{array}$$

donde llamamos a $\hat{\phi}$ la **co-acción** (derecha) de A sobre B, siempre que sea tal que haga conmutar este diagrama. Notando que $\widehat{Id_G} = Id_A$ y $\widehat{Id_P} = Id_B$. Tomamos las álgebras C^∞ simplemente por tomar en cuenta la estructura diferencial del haz y el grupo de Lie. En el caso del haz principal se requiere que la acción sea libre. En términos clásicos la libertad nos permite establecer un difeomorfismo del grupo con la fibra (i.e. la órbita de la acción): Fijando un elemento de P, la acción $\phi : P \times G \longrightarrow P$ induce un difeomorfismo con la imagen, es decir un *encaje*, de los que se tienen tantos como fibras en el haz (i.e. puntos en la base). La condición de libertad se traduce de la siguiente forma [7], para toda $a \in A$ existen elementos $q_k, b_k \in B$ tales que

$$\sum_k q_k \hat{\phi}(b_k) = 1 \otimes a$$

lo que en palabras significa que podemos recuperar al grupo, representado por el álgebra A, como una subálgebra en $B \otimes A$ a partir de la co-acción y el álgebra B.

Así como representamos al espacio total P por el álgebra C* de funciones complejas B, podemos representar al espacio base por la subálgebra C de B dada por las funciones *constantes sobre las fibras*. Entonces el espacio base puede ser caracterizado como la subálgebra $C \leq B$ fija bajo la co-acción [7], es decir:

$$C = \{b \in B \mid \hat{\phi}(b) = b \otimes 1\}$$

mientras que la proyección (función suprayectiva) del espacio total en la base está ahora dada por un $*$-homomorfismo inyectivo de álgebras

$$C \hookrightarrow B$$

Así hemos definido el **haz principal cuántico** de forma completamente análoga a los haces estudiados en el capítulo 3. Ahora la triada característica $B(C, A)$ es un álgebra C*, B, en la que co-actúa (por la derecha) un álgebra de Hopf, A, y con base en un espacio representado por un álgebra C*, C.

4.2. Otro Acercamiento al Haz

Otro acercamiento a la definición del haz principal resulta reveladora. Consideramos ahora la acción libre de forma implícita, requiriendo la existencia de un difeomorfismo

$$\Psi : P \times G \longrightarrow P \times_M P$$

$$\Psi : (p, g) \longmapsto (p, p * g)$$

$P \times_M P$ es el *producto fibrado* de P consigo mismo dado por la proyección $\pi : P \longrightarrow M$ del haz. El *producto fibrado* es una construcción categórica, es decir aquella descrita por una *propiedad universal*, que depende de dos transformaciones con el mismo codominio. Por ahora sólo nos interesa este caso particular, que podemos describir como sigue: Son las parejas $(x, y) \in P \times P$ tales que tienen la misma proyección, es decir $\pi(x) = \pi(y)$, lo que equivale a decir que difieren sólo por la

acción de un elemento del grupo estructural, digamos $g \in G$, de modo que $x = y * g$. Este espacio es entonces un producto cartesiano $P \times P$ con estructura extra, su topología es la **topología débil** inducida por $\{\pi \circ p_i\}_{i=1,2}$, donde las p_i son las proyecciones canónicas, esto es la topología más gruesa que hace continua a esta pareja de funciones.

Notamos de inmediato lo siguiente:

- Ψ es suave en efecto, pues es la composición de funciones suaves (la acción de grupo está dada por un mapeo suave).
- La suprayectividad Ψ nos dice que cada fibra de P es en efecto una órbita de la acción de G. Corresponderá, al dualizar al caso general de las álgebras, a una condición de regularidad que codifica la trivialidad local del haz [8].
- La inyectividad de Ψ es equivalente a la libertad de la acción y en consecuencia a la identidad entre el grupo y la fibra.
- El difeomorfismo Ψ de estas características describe a un haz principal, pues codifica la acción de G como grupo estructural.

Llevando estas condiciones al nivel de las álgebras podemos describir el haz por un espacio cuántico representado por un álgebra C* arbitraria, B, una $*$-subálgebra $C \leq B$, y un grupo cuántico representado por una $*$-álgebra de Hopf, A, junto con un isomorfismo

$$B \otimes_C B \longrightarrow B \otimes A$$

donde $\otimes_C$ se refiere al producto tensorial C* factorizado de manera dual al producto fibrado que vimos antes: ahora factorizamos por el ideal generado por el conjunto $\{ac \otimes b - a \otimes cb \mid a, b \in B \ c \in C\}$. Esta construcción es un ejemplo de una extensión de Hopf-Galois de álgebras C*.

4.3. Extensión de Hopf-Galois

Una **extensión de Hopf-Galois** parte de un álgebra A, sobre un campo K, que es un H-comódulo *derecho* para un álgebra de Hopf H. La estructura de *comódulo* se puede pensar como una co-acción de H sobre A, de la misma manera que podemos ver a un módulo como la acción de un anillo sobre un espacio vectorial (recordando que el álgebra es un caso particular de ambas estructuras), pues el comódulo está dado por un mapeo $\rho : A \longrightarrow A \otimes_K H$. Si consideramos $B \subset A$ como la subálgebra fija bajo esta co-acción, es decir la *subálgebra co-invariante* de los elementos tales que $\rho(b) = b \otimes 1$, decimos que A es una H**-extensión** derecha de B.

En general denotamos la co-acción sobre un elemento del álgebra por

$$\rho(a) = \sum_a a_0 \otimes a_1$$

usando la **notación de Sweedler** en la cual la suma sobre $a \in A$ se refiere a sumar una cantidad de términos dependiente de a y donde $a_0 \in A$ y $a_1 \in H$ representan los componentes izquierdo y derecho de cada término.

Decimos que dicha extensión es **H-Galois** (Hopf-Galois) derecha si el **mapeo de Galois**

$$\beta : A \otimes_B A \longrightarrow A \otimes_K H$$

dado por

$$r \otimes s \mapsto (r \otimes 1)\rho(s)$$

es biyectivo.

La forma de este mapeo es precisamente la que obtenemos al dualizar la construcción del haz que vimos en la sección anterior. Esto es evidente tomando $K = \mathbb{C}$, A como el álgebra C* del haz, B el álgebra C* asociada a la base y H el grupo cuántico (esto es un simple cambio de notación respecto de la sección anterior). El primer factor del mapeo de Galois corresponde a la entrada fija del caso clásico, $(p, g) \mapsto (p, p * g)$, mientras que el segundo a la acción del grupo estructural del haz,

que está dada ahora por la co-acción del álgebra de Hopf. Se verifica entonces que el Haz Principal Cuántico es, como lo definimos en este trabajo, una extensión de Hopf-Galois. La diferencia radica en que en el haz principal cuántico tenemos además la estructura C* en las álgebras que, podemos decir, es la que codifica la geometría de los espacios cuánticos.

Para establecer la conexión entre la extensión de Galois (de campos) y la extensión de Hopf-Galois mostraremos como esta se reduce a aquella y viceversa, para ello debemos enunciar algunos detalles y resultados sobre álgebras y módulos que nos permitirán esta labor [17]:

(1) Se puede demostrar que en el caso del álgebra de grupo para un campo y grupo arbitrarios K y G, se tiene que un álgebra A sobre K es $K(G)$-módulo si y sólo si G es un subgrupo de automorfismos de A; la acción que define al módulo se deriva de manera directa de la acción de G como dicho subgrupo de automorfismos.

(2) Sea el álgebra A un H-comódulo derecho y supongamos que H de dimensión finita, entonces H^* (el espacio dual de H) es un álgebra de Hopf y A es a su vez un H^*-módulo izquierdo. Además se tiene que los elementos co-invariantes bajo la co-acción de H son exactamente los elementos invariantes bajo la acción de H^*. Naturalmente tenemos proposiciones duales intercambiando *derechas* por *izquierdas* y/o los roles de H y H^*.

Para demostrarlo tomamos la co-acción derecha $\rho : A \longrightarrow A \otimes_K H$ dada por $\rho(a) = \sum_a a_0 \otimes a_1$ y definimos una acción izquierda de H^* para $f \in H^*$ arbitrario como

$$f \cdot a = \sum_a f(a_1)a_0$$

Por otro lado una acción izquierda de H, $(h, a) \mapsto h \cdot a$, determina una co-acción derecha de H^* vía

$$a \mapsto \sum_i (h_i \cdot a) \otimes f_i$$

donde $\{h_i\}_{i=1}^{i=n}$ es una base de H y $\{f_i\}_{i=1}^{i=n}$ la base dual. Se verifica que con esta acción y esta co-acción obtenemos en efecto un módulo y un comódulo respectivamente.

Entonces se ha demostrado que para H de dimensión finita: H actúa sobre A si y sólo si H^* co-actúa sobre A (usamos el hecho de que se tiene un *isomorfismo natural* entre $(H^*)^*$ y H). Considerando lo anterior supongamos que $a \in A$ es co-invariante bajo una co-acción derecha de H, esto es $\rho(a) = \sum_a a_0 \otimes a_1 = a \otimes 1$. Entonces bajo la acción izquierda inducida de $f \in H^*$ obtenemos

$$f \cdot a = \sum_a f(a_1)a_0 = f(1)a = 1a = a$$

dualmente supongamos que $a \in A$ es un elemento invariante bajo una acción izquierda de H, esto es $h \cdot a = a \; \forall h \in H$, de modo que bajo la co-acción derecha de H^* sobre este mismo elemento obtenemos

$$a \mapsto \sum_i (h_i \cdot a) \otimes f_i = a \otimes \sum_i f_i = a \otimes 1$$

Esto de muestra que los elementos invariantes de la acción izquierda de H (respectivamente H^*) y los co-invariantes de la co-acción derecha de H^* (resp. H) son iguales.

(3) El espacio dual de $K(G)$ es K^G, el álgebra de funciones $G \longrightarrow K$. La estructura de álgebra de Hopf de este espacio es la *dual formal* de la de $K(G)$:

Para $f, g \in K^G$ el producto $\bigtriangledown : K^G \otimes K^G \longrightarrow K^G$ está dado por

$$(f \bigtriangledown g)(x) := f(x)g(x)$$

y el co-producto $\bigtriangleup : K^G \longrightarrow K^G \otimes K^G$ es

$$\bigtriangleup(f)(x \otimes y) = f(xy)$$

mientras que su antípoda $\zeta : K^G \longrightarrow K^G$ esta dada por la antípoda $\theta : g \mapsto g^{-1}$ del grupo

$$\zeta(f)(x) = f(\theta(x))$$

4.4. Extensiones Geométricas

Cerraremos el círculo de esta tesis recuperando a continuación las extensiones de Galois (finitas) que presentamos en el primer capítulo como extensiones de Hopf-Galois.

A grandes rasgos la situación es la siguiente. Consideremos el mapeo de Galois ahora aplicado a una extensión de campo E/F con $G = Aut(E/F)$. Todo campo puede ser visto como álgebra sobre algún subcampo $K \leq E$, de modo que E toma el lugar de A; el espacio co-invariante C por el campo base F; el grupo G toma *indirectamente* el papel del álgebra de Hopf A mediante el álgebra de grupo sobre K, $K(G)$. En efecto podemos darle a $K(G)$ una estructura de álgebra de Hopf de manera natural, definiendo la co-multiplicación por $\phi(g) = g \otimes g$, el co-neutro por $\epsilon(g) = 1$ y la antípoda $\theta(g) = g^{-1}$, para luego extender linealmente estas funciones al resto de los elementos de $K(G)$ (usaremos de hecho el álgebra de Hopf dual a esta). Así tendremos al campo base, su extensión y el grupo asociado a la extensión en los lugares respectivos del espacio base, el haz y el grupo estructural.

Empecemos por suponer que la extensión E/F es de Galois para luego demostrar que es H-Galois. Basta demostrar que con esta extensión podemos construir un mapeo de Galois biyectivo. Primero vemos a E como un álgebra sobre el campo base F de modo que el grupo de Galois G, que actúa sobre E por la izquierda como subgrupo de automorfismos, lo preserva. Entonces E es un $F(G)$-módulo izquierdo, por (1), y como G es una base finita para $F(G)$ sabemos que F^G es un álgebra de Hopf, de acuerdo a (3), que co-actúa sobre E por la derecha debido a (2). Siendo F el campo fijo bajo la acción de G, resulta el álgebra (sobre sí mismo) invariante bajo la acción de $F(G)$. Por (2), F es a su vez el espacio co-invariante de la co-acción de F^G.

Sea $n = [E : F] = |G|$, recordando que podemos caracterizar a E/F como una extensión de Galois como aquella que cumple $[E : F] = |G|$. Entonces podemos escribir $G = \{x_1, x_2..., x_n\}$ (como base de $F(G)$), $\{p_1, p_2, ..., p_n\}$ la base dual en F^G

y tomar $\{b_1, b_2, ..., b_n\}$ una base de E sobre F. Como ya mencionamos la acción de G en E determina una acción de $F(G)$ en E, que a su vez nos da una co-acción $\rho : E \longrightarrow E \otimes_F F^G$ del espacio dual dada por

$$\rho(a) = \sum_{i=1}^{n} (x_i \cdot a) \otimes p_i$$

de modo que el mapeo de Galois $\beta : E \otimes_F E \longrightarrow E \otimes_F F^G$ sobre un elemento simple del álgebra nos da

$$\beta(a \otimes b) = (a \otimes 1)\rho(b) = (a \otimes 1) \sum_{i=1}^{n} (x_i \cdot b) \otimes p_i = \sum_{i=1}^{n} a(x_i \cdot b) \otimes p_i$$

Notemos que $dim(F^G) = |G| = dim(E)$, de modo que β es un mapeo entre espacios de la misma dimensión y por ello nos bastará con demostrar que β es inyectivo. Un elemento arbitrario de $E \otimes_F E$ se escribe como $w = \sum_{j=1}^{j=m} \gamma_j \otimes \delta_j$ para $m \in \mathbb{N}$. Usando la base $\{b_i\}$ descomponemos las δ_j y escribimos $w = \sum_j \gamma_j \otimes (\sum_i f_{ij} b_i) = \sum_i (\sum_j \gamma_j f_{ij}) \otimes b_i$, sustituyendo $a_i = \sum_j \gamma_j f_{ij}$, podemos escribir a w de la forma $w = \sum_{j=1}^{j=n} a_j \otimes b_j$. Supongamos que w está en el núcleo del mapeo de Galois, es decir

$$\beta(w) = \sum_{i,j} a_j (x_i \cdot b_j) \otimes p_i = 0$$

con ambos índices corriendo hasta n. Pensando el factor izquierdo de cada término como un coeficiente en el campo, esta expresión corresponde a una combinación lineal de $\{p_i\}_{i=1}^{i=n}$, que siendo linealmente independiente implica que para cada i

$$\sum_j a_j (x_i \cdot b_j) = 0$$

ecuación que podemos reescribir en forma matricial

$$B \overrightarrow{a} = \overrightarrow{0}$$

donde $[B]_{ij} = x_i \cdot b_j$, $\overrightarrow{a} = (a_1, ..., a_n)$ y $\overrightarrow{0} = (0, ..., 0)$. Como la acción de G es fiel el lemma de Dedekind sobre la independencia de automorfismos (que vimos en la sección 3 de capítulo 1), en este caso de las x_i, implica que las columnas de B son

linealmente independientes y así que B es invertible. Entonces tenemos que $\overrightarrow{a} = \overrightarrow{0}$ lo que significa que $a_j = 0$ para todo j y a su vez que $w = 0$, probando la inyectividad de β.

Ahora tratamos el converso suponiendo que la definición de la extensión de Hopf-Galois aplica para una extensión E/F, esto es, el álgebra E es un F^G-comódulo con una co-acción que escribimos como $\rho(a) = \sum_{h\in G} a_h \otimes p_h$ (indexando los términos por los elementos del grupo) donde $\{p_h\}_{h\in G}$ es nuevamente la base dual a $F(G)$, tal que $F \leq E$ es el espacio co-invariante y el mapeo de Galois $\beta : E \otimes_F E \longrightarrow E \otimes_F F^G$ es biyectivo. La acción dual de G a esta co-acción es de la forma $g \cdot a = \sum_{h\in G} < g, p_h > a_h = a_g$. Así $a \in E$ es un elemento fijo de la acción de G si y sólo si $g \cdot a = a$ si y sólo si $a_g = a$ para toda $g \in G$ o equivalentemente $\rho(a) = a \otimes \sum_{h\in G} p_h = a \otimes 1$. Esto de muestra que el espacio invariante bajo la acción de G es el espacio co-invariante de la co-acción de F^G, es decir F. Por otro lado la biyectividad del mapeo de Galois y la finitud en la dimensión de los espacio nos dicen que $[E : F]^2 = [E : F]dim(F^G)$, y como $dim(F^G) = dim(F(G)) = |G|$ concluimos que $|G| = [E : F]$, por lo que E/F es de Galois. $\square$

Conlusiones

Hemos visto conceptos y resultados básicos de las tres teorías expuestas y usado dicho aparato para presentar las extensiones de Hopf-Galois como un modelo no-conmutativo del haz principal. Al delinear los principios de la teoría de Galois elaboramos un lenguaje alrededor del cual se desarrolla un formalismo adecuado para ciertos problemas, es decir, la teoría de grupos como herramienta para la teoría de ecuaciones. Podemos pensar en los grupos de automorfismos como simetrías de ecuaciones y en este sentido la teoría de Galois describe una geometría de ecuaciones. Los haces principales nacen propiamente de la acción de un grupo, es decir, del estudio mismo de las simetrías y permiten introducir la noción de simetría interna importantísima para la geometría diferencial y para la física moderna. Hemos introducido la teoría cuántica a través de la traducción de conceptos geométrico-topológico-diferenciales a lenguaje algebráico y extrapolando la categoría de espacios (de Hausdorff localmente compactos) a los espacios cuánticos gracias al teorema de Gelfand-Naimark. Ello nos permitió introducir una definición intuitiva de grupo cuántico que nos llevo de forma natural al haz principal cuántico y a un modelo de este como extensión de Hopf-Galois. Finalmente recuperamos a las extensiones de Galois (de campos) como caso particular de extensión de Hopf-Galois, cerrando circularmente la tesis.

En más detalle, resulta que cuando el grupo estructural de un haz principal cuántico es un *grupo cuántico compacto de matrices*, entonces el haz es descrito por una extensión de Hopf-Galois [8]. A grandes rasgos los **grupos cuánticos compactos de matrices** se definen como matrices con entradas en un álgebra C* unital A, cuyas entradas generan una subálgebra densa $\mathcal{A}$, con un co-producto emparentado

al producto de matrices [25].

La teoría de Galois tiene hoy en día formas más abstractas que encontramos en la teoría de conexiones de Galois y la teoría de Hopf-Galois. Las extensiones de Hopf-Galois fueron introducidas por Chanse y Sweedler [2] en el caso conmutativo y por Kreimer y Takeuchi [15] el caso de álgebras de Hopf de dimensión finita, introduciendo generalizaciones directas de los axiomas que definen a una extensión de Galois, reemplazando la acción de grupo por la co-acción de un álgebra de Hopf H, del que recuperamos el caso de la extensión de Galois ordinaria tomando el dual del álgebra de grupo.

Después de este trabajo he descubierto lo profundo que son aún estas teorías para mí. Me queda adentrarme en las increíbles aplicaciones de la teoría de haces en la física, en particular a las *teorías de campos gauge* en las que las teorías físicas se describen como haces con base en el espacio-tiempo con específicos grupos estructurales que llevan a modelos geométricos de las partículas elementales (el modelo estándar) o de más fundamentales fluctuaciones energéticas (teorías de cuerdas). Es de hecho de la física y el mundo observable de donde muchas de las definiciones de la teoría de haces se han inspirado. La simetría parece ser como un código fundamental de las fuerzas físicas y formas materiales, como de la geometría misma. Los haces principales cuánticos señalan un posible camino hacia la unificación de la mecánica cuántica con la relatividad general [6], pero su interés como objeto matemático es intrínseco.

La geometría cuántica es un entorno muy interesante que pone al límite las nociones de geometría. Resulta increíble pensar en su sencillez conceptual contrapuesta a todo el trabajo y la evolución de las ideas que están detrás y hacen posible la presentación que hago en esta tesis de los mismos: desde los trabajos de Riemann en geometría diferencial y el programa de Erlangen de Feliz Klein que dan lugar a la geometría de principios del siglo XX como importante factor en el nacimiento de la relatividad y la mecánica cuántica, la axiomatización impulsada por Hilbert y la formalización de Bourbaki, hasta los trabajos de Alain Connes, Woronowicz y las

investigaciones más recientes en geometría cuántica como las de mi asesor Micho Durdevich que ha sido de gran ayuda e inspiración en la elaboración de esta tesis y de mi interés en futuras investigaciones. Invito al lector a referirse al recien publicado *Principal Bundles The Quantum Case* escrito por mi sinodal de tesis Stephen Sontz [21], en el que recaba y elabora elementos de la geometría cuántica de los haces principales de manera autocontenida junto con algunos de los desarrollos recientes y horizontes. Es increíble pensar en toda esta comunidad espacio-temporal, que resulta imposible citar en su totalidad, que invita a que nuevas generaciones podamos expandir nuestra visión del mundo.

Bibliografía

[1] Emil Artin, *Galois Theory*, Dover Publications Inc. (1998)

[2] S.U. Chanse & M.E. Sweedler *Hopf algebras and Galois theory*, vol. 97 of Lecture Notes in Math. Springer, (1969)

[3] Claude Chevalley, *Theory of Lie Groups*, Princeton University Press (1946)

[4] Alain Connes *Noncommutative Geometry*, Academic Press (1994)

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

[6] Micho Durdevich, *Quantum principal bundles and corresponding gauge theories*, J. Physics A: Math. Gen. 30 (1997) 2027–2054

[7] Micho Durdevich, *Geometry of quantum principal bundles II*, extended version, Rev. Math. Phys. 9, No. 5 (1997) 531–607

[8] Micho Durdevich, *Quantum principal bundles as Hopf–Galois extensions*, Acad. Res. 23 (2009) 41–49

[9] Micho Durdevich, *Quantum gauge transformations and braided structure on quantum principal bundles*, Misc. Alg. 5 (2001) 5–30

[10] J.B. Fraleigh *A First Course in Abstract Algebra*, Addison Wesley, 7ed. (2002)

[11] I. Gelfand & M. Naimark *On the imbedding of normed rings into the ring of operators in Hilbert space*, Rec. Math. [Mat. Sbornik] N.S., (1943) Volume 12(54), Number 2, 197–217

[12] V. Guillemin Pollack & A. Pollack *Differential Topology*, American Mathematical Soc., 2010 (1974)

[13] M. Khalkhali, *Very Basic Noncommutative Geometry*, Vanderbilt University, Department of Mathematics, arXiv preprint math/0408416

[14] S. Kobayashi & K. Nomizu, *Foundations of Differential Geometry vol. 1*, Wiley Classics Library (1996)

[15] H.F. Kreimer & M. Takeuchi *Hopf Algebras and Galois Extensions of an Algebra*, Indiana Univ. Math. J. 30 (1981)

[16] John M. Lee *Introduction to Smooth Manifolds*, Graduate Texts in Mathematics, Springer (2002)

[17] Susan Montgomery, *Hopf Galois Theory: A Survey*, Geometry and Topology Monographs 16 (2009) 367-400

[18] Eduard Prugovečki, *Quantum Geometry - A Framework for Quantum General Relativity*, Kluwer Academic Publishers (1992)

[19] Walter Rudin, *Functional Analysis*, McGraw-Hill (1973)

[20] Stephen Bruce Sontz, *Principal Bundles. The Classical Case*, Universitext, Springer (2015)

[21] Stephen Bruce Sontz, *Principal Bundles. The Quantum Case*, Universitext, Springer (2015)

[22] John Stillwell, *Naive Lie Theory*, Springer (2008)

[23] S.L Woronowicz, *Pseudospaces, Pseudogroups & Pontriagin Duality*, Proceedings of the International Conference of Mathematical Physics, Lausanne: Lecture Notes in Physics **116**, 407-412 (1979).

[24] S.L. Woronowicz, *Twisted SU(2) Group. An Example of a Non-Commutative Differential Calculus*, PubL RIMS, Kyoto Univ. 23 (1987), 117-181

[25] S.L. Woronowicz, *Compact Matrix Pseudogroups*, Communications in Mathematical Physics, 613-665, Springer-Verlag (1987)