

**ACERCA DE LAS FORMAS TORCIDAS SOBRE LOS GRUPOS
LINEALES ALGEBRAICOS**

Por

Gabriel Darío Uribe Guerra

Tesis sometida en cumplimiento parcial de los requerimientos para el grado de

MAESTRÍA EN CIENCIAS

en

MATEMÁTICAS PURAS

UNIVERSIDAD DE PUERTO RICO
RECINTO UNIVERSITARIO DE MAYAGÜEZ

Mayo, 2008

Aprobada por:

Uroyoán R. Walker Ramos, Ph.D.
Presidente, Comité Graduado

Fecha

Edgardo Lorenzo González, Ph.D.
Miembro, Comité Graduado

Fecha

Luis Fernando Cáceres Duque, Ph.D.
Miembro, Comité Graduado

Fecha

Pablo Marrero, Ph.D.
Representante de Estudios Graduados

Fecha

Julio C. Quintana Díaz, Ph.D.
Director del Departamento

Fecha

Abstract of Disertation Presented to the Graduate School
of the University of Puerto Rico at Mayagüez in Partial Fulfillment of the
Requirements for the Degree of Master of Science

ON TWISTED FORMS OVER LINEAR ALGEBRAIC GROUP

By

Gabriel Darío Uribe Guerra

May 2008

Chair: Uroyoán R Walker Ramos

Major Department: Mathematical Sciences

Working from the Galois theory, we define linear groups via group schemes. We study different properties of these groups such as connectedness, Lie algebras associated to them, which determine their smoothness. Lastly we use tools from Galois cohomology via Γ -groups to determine the twisted forms associated to a linear algebraic group.

Resumen de Disertación Presentado a Escuela Graduada del Recinto de Mayagüez
de la Universidad de Puerto Rico en Mayagüez como requisito parcial de los
Requerimientos para el grado de Maestría en Ciencias

**ACERCA DE LAS FORMAS TORCIDAS SOBRE LOS GRUPOS
LINEALES ALGEBRAICOS**

Por

Gabriel Darío Uribe Guerra

Mayo 2008

Consejero: Uroyoán R. Walker Ramos
Departamento: Departamento de Ciencias Matemáticas

Centrandonos en la teoría de Galois, definimos los grupos lineales algebraicos
vía los esquemas de grupo, estudiamos las diferentes propiedades de estos como son
la conexidad, las álgebras de Lie las cuales determinan la suavidad, para por último
entrar a las cohomologías vía los Γ - grupos para determinar las formas torcidas de
los grupos lineales algebraicos.

Copyright © 2008

por

Gabriel Darío Uribe Guerra

A mi madre y mi Marcelita.

AGRADECIMIENTOS

A el Dr. Uroyoán R. Walker Ramos por su apoyo, su amistad, su conocimiento y su tiempo para poder culminar este trabajo. Además de haberme encaminado por esta área tan bonita como lo es la geometría algebraica.

Al Dr. Luis Fernando Cáceres que además de darme su apoyo me brindó su amistad, su confianza. A él también le agradezco dejarme participar de sus fantásticos proyectos (AFAMaC y OMPR).

Al Dr. Pedro Vásquez por preocuparse por mi bienestar.

En general, a todas las personas que estuvieron de una manera u otra relacionados con mi enriquecimiento profesional, a Rafael Aparicio y Luis Fuentes por ser mi apoyo incondicional y a las grandes personas que conocí en el proyecto AFAMaC, Carmen Segarra, Roxanna Rodríguez, Keyla Chaves, Dr. Arturo Portnoy y Julián Rodríguez, por que con ellos aprendí a trabajar en grupo.

TABLA DE CONTENIDO

	<u>página</u>
ENGLISH ABSTRACT	ii
SINOPSIS EN ESPAÑOL	iii
AGRADECIMIENTOS	vi
LISTA DE SÍMBOLOS	ix
1 INTRODUCCIÓN	1
2 TEORÍA DE GALOIS	4
2.1 Extensiones de Campo	4
2.2 Campos de Descomposición	7
2.3 Separabilidad	8
2.4 Clausuras Algebraicas	8
2.5 Extensiones Normales	9
2.6 Clausuras Normales	10
2.7 Extensiones de Galois	12
3 ÁLGEBRAS CENTRALES SIMPLES	16
3.1 Preliminares	16
3.2 Álgebras Centrales Simples	18
3.3 Anillos	23
4 GRUPOS ALGEBRAICOS	28
4.1 Álgebras de Hopf	28
4.2 Esquemas de grupo	29
4.3 Componente conexa	33
4.4 Álgebras de Lie y suavidad	35
4.5 Homomorfismos de esquemas de grupo	39
4.6 Automorfismos de grupos de álgebras	41
5 COHOMOLOGÍA DE GALOIS	43
5.1 Conjuntos Cohomólogos	43
5.2 Sucesiones Exactas	46
5.3 Formas Torcidas	47
5.4 Cohomología de Galois de Grupos Algebraicos	48

5.5	Clasificación de Álgebras	54
6	CONCLUSIONES Y TRABAJOS FUTUROS	57
6.1	Conclusiones	57
6.2	Trabajos Futuros	57

LISTA DE SÍMBOLOS

K	Campo.
A	Álgebra.
$A \otimes A$	Producto Vectorial.
L/K	Extensión de Campo.
$Z(A)$	Centro de A .
$a \otimes b$	Producto Tensorial.
$M_n(L)$	Conjunto de matrices $n \times n$.
I_n	Matriz identidad de orden n .
$C_A(B)$	El centralizador de B en A .
I	Ideal.
R	Anillo.
$Char K$	Característica de un campo.
$Aut(K)$	Subgrupo de Automorfismos de K .
L^G	Campo fijo.
$Gal(L/K)$	Grupo de Galois.
G^A	Esquema de Grupo.
Alg_K	Conjunto de álgebras.
$Hom(A, B)$	Homomorfismos de A a B .
G_a	Grupo Aditivo.
G_m	Grupo Multiplicativo.
GL_n	Grupo Lineal General.
SL_n	Grupo Lineal Especial.
μ_n	Grupo de las n -ésimas raíces de la unidad.
$det(A)$	Determinante de A .
O_n	Grupo Ortogonal.
U_n	Grupo Unitario.
Sp_{2n}	Grupo simpléctico.
$S_v(R)$	Subgrupo de estabilizadores de v .
$N_U(R)$	Subgrupo de Normalizadores de U .
$\pi_0(A)$	Conjunto de componentes conexas.
G^0	Componente conexa de G .
$nil(A)$	Conjunto de elementos nilpotentes de A .
A_{red}	Álgebra reducida.
$Der(A, M)$	Conjunto de derivaciones de A a M .
$Lie(G)$	Álgebra de Lie de G .
df	Diferencial de f .
K_{alg}	Clausura algebraica.
K_{sep}	Clausura separable.

PGL_n Grupo lineal proyectivo.
 $H^0(\Gamma, G)$ Campo fijo de G .
 $H^1(\Gamma, G)$ Primera cohomología.
 $Z^1(\Gamma, G)$ Conjunto de 1-cociclos de Γ a G .
 $Z^2(\Gamma, G)$ Conjunto de 2-cociclos de Γ a G .
 $G(K)$ Grupo algebraico de puntos fijos.
 $G_\alpha(K)$ Grupo de formas torcidas de los grupos algebraicos.

Capítulo 1

INTRODUCCIÓN

La homología es tomada como una rama de la topología. El primero en hablar de homología fue el francés Henri Poincaré en *Analysis Situs* en 1895. Él estaba pensando en un espacio topológico complicado y buscaba una manera más fácil de contar los agujeros de cualquier dimensión del espacio, obteniendo ciertos invariantes lineales. Así entonces podemos relacionar la homología como la herramienta que nos ayuda a construir invariantes lineales de una situación no lineal.

También la podemos considerar como una herramienta algebraica fundamental para obtener información sobre los espacios topológicos.

Otro personaje importante que contribuyó con la homología fue el alemán David Hilbert, que consideró ideales, es decir, combinaciones lineales de polinomios con ceros comunes y sus relaciones y después las relaciones entre estas relaciones. Esta es considerada como una jerarquía y es conocida como los *Syzygies de Hilbert*.

En el campo de la geometría algebraica en los años 50 del siglo pasado se desarrolló la teoría de haces, por parte de la escuela francesa de Leray, Cartan, Serre y Grothendieck

Nosotros trabajaremos más sobre la *teoría de Cohomología de Galois*, que es la aplicación del álgebra homológica a los módulos del *grupo de Galois* y en particular sobre las *Formas Torcidas (Twisted Forms)* de los grupos algebraicos lineales.

Daremos a conocer algunos conceptos importantes que han sido estudiados, en nuestro camino hacia el conocimiento de la teoría de cohomologías y que más adelante nos ayudarán a alcanzar nuestro objetivo.

Un *Grupo de Galois* lo definimos de la siguiente manera: Sea L una extensión del campo K , que se denota por L/K . El grupo Galois de L/K de todos los K automorfismos de L ($Aut_K(L)$) equipado con la composición de funciones como operación. Este grupo lo denotamos por $Gal(L/K)$.

También definimos un *Grupo Profinito* el cual es el límite inverso de los sistemas de grupos finitos, o equivalentemente, el grupo topológico compacto en el sentido de Hausdorff y totalmente desconexo. Nosotros tomaremos el grupo profinito Γ como el grupo de Galois absoluto, que denotamos por $\Gamma = Gal(K_{sep}/K)$ donde K_{sep} es una clausura separable fija de K .

Además, definimos los *Conjuntos de Cohomología* $H^i(\Gamma, A)$, con $i = 0, 1, 2$ donde A es un Γ -módulo.

También introducimos el concepto de *Forma Torcida*. Este se basa en los esquemas de grupos algebraicos sobre K . Si consideramos a G como un esquema de grupo y $\rho : G \rightarrow GL(W)$ una representación con W un K -espacio finitamente dimensional. Fijemos $w \in W$, e identifiquemos a W con un F -subespacio de $W_{sep} = W \otimes_K K_{sep}$. Un elemento $w' \in W_{sep}$ lo llamamos ρ -Forma Torcida de w si $w' = \rho_{sep}(g)(w)$ para algún $g \in G(K_{sep})$.

Estos serían nuestros conocimientos básicos para aplicarlos a los grupos algebraicos lineales, que se definen de la siguiente forma:

Grupo Lineal General:

$$GL_n(R) = \{A \in M_n(R) : \det A \neq 0\}$$

Grupo Lineal Especial:

$$SL_n(R) = \{A \in GL_n(R) : \det A = 1\}$$

Grupo Lineal Ortogonal:

$$O_n(R) = \{A \in GL_n(R) : AA^t = I\}$$

Grupo Lineal Simplético:

$$SP_{2n}(R) = \{A \in GL_{2n}(R) : A^t J A = J\}$$

donde J es un elemento de GL_{2n} fijo.

Grupo Lineal Unitario:

$$U_n(C) = \{A \in GL_n(C) : A^* A = I\}$$

donde A^* es la matriz conjugada de A .

Los últimos tres los podríamos definir como especiales al hacer la intersección con el grupo especial lineal.

También utilizaremos conceptos como álgebras de Hopf, álgebras centrales simples, álgebras de Clifford, álgebras de Lie y algunas definiciones y teoremas relacionados.

Capítulo 2

TEORÍA DE GALOIS

2.1 Extensiones de Campo

Definición 2.1.1. Una extensión de campo K está dada por un campo L y un homomorfismo $\theta : K \hookrightarrow L$ tal que θ es una inmersión de K en L . Una extensión de campo la denotamos por L/K .

Decimos que una extensión de campo L/K es finitamente generada si para algún $n \in \mathbb{Z}$ existen $\alpha_1, \alpha_2, \dots, \alpha_n \in L$ tal que $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$. Si $L = K(\alpha)$ para algún $\alpha \in L$, decimos que la extensión es simple.

Definición 2.1.2. Dada una extensión L/K , un elemento $\alpha \in L$ es algebraico sobre K si existe un polinomio $f \in K[X]$ tal que $f(\alpha) = 0$ en L . De otra forma decimos que el elemento α es trascendental sobre K .

Si α es algebraico, el polinomio mónico $f \in K[X]$ de menor grado

$$f = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$$

para el cual $f(\alpha) = 0$, es el polinomio minimal de f . Este polinomio es único e irreducible en K .

Definición 2.1.3. Una extensión de campo L/K es algebraica si cada $\alpha \in L$ es algebraico sobre K y es puramente trascendental si cada $\alpha \in L/K$ es trascendental sobre K .

Recordemos que si K es un campo y $f \in K[X]$ es un polinomio irreducible, el anillo cociente $K[X]/(f)$ es un campo. Podemos notar que es una extensión simple

$K \hookrightarrow K(\alpha) = K[X]/(f)$, donde α denota la imagen de X bajo la aplicación cociente. Así, ésta es una extensión simple algebraica de campo.

Definición 2.1.4. *Si L/K es una extensión de campo, entonces L tiene la estructura de espacio vectorial sobre K . El grado de la extensión, es la dimensión de L sobre K como espacio vectorial. La cual denotamos por $[L : K]$.*

Decimos que L es finito sobre K si $[L : K]$ es finito.

Teorema 2.1.5. *Sea L/K una extensión de campo y $\alpha \in L$, α es algebraico sobre K si y solo si $K[\alpha]/K$ es finita. Cuando α es algebraico, $[K[\alpha] : K]$ es el grado del polinomio mínimo de α .*

Demostración. (\Leftarrow) Si $[K(\alpha) : K] = n$, entonces $1, \alpha, \alpha^2, \dots, \alpha^n$ son linealmente dependientes sobre K , por tanto existe $f \in K[X]$ tal que $f(\alpha) = 0$.

(\Rightarrow) Sea α algebraico sobre K con polinomio minimal f , de esto tenemos que

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0$$

Supongamos que $g \in K[X]$ con $g(\alpha) \neq 0$. Consideremos que f es irreducible y así tenemos que $\text{mcd}(f, g) = 1$. Por el algoritmo de Euclides, esto implica que existen $x, y \in K[X]$ tal que $xf + yg = 1$, pero como $f(\alpha) = 0$, entonces $y(\alpha)g(\alpha) = 1$ en L . Por tanto $g(\alpha)^{-1} \in (1, \alpha, \dots)$ es el subespacio de L generado por las potencias de α . Ahora $K(\alpha)$ consiste de todos los elementos de la forma $h(\alpha)/g(\alpha)$ para $h, g \in K[X]$ polinomios, donde $g(\alpha) \neq 0$. Así $K(\alpha)$ es generado como K -espacio vectorial por $1, \alpha, \dots$ y por tanto de la relación de arriba basta con $1, \alpha, \dots, \alpha^{n-1}$. Por la minimalidad de n , tenemos que el conjunto generado por $1, \alpha, \dots, \alpha^{n-1}$ es una base y así $[K(\alpha) : K] = n$. ■

La siguiente proposición es de las más importantes dentro de la teoría de campos, nosotros la utilizaremos en este capítulo en varias ocasiones para mostrar algunas propiedades.

Proposición 2.1.6. *Dada una torre de extensiones de campo finitas $K \hookrightarrow L \hookrightarrow M$, entonces $[M : K] = [M : L][L : K]$.*

Demostración. Sea $(u_i)_{i \in I}$, una base para M sobre L y sea $(v_j)_{j \in J}$, una base para L sobre K . Debemos mostrar que $(u_i v_j)_{i \in I, j \in J}$ es una base de M sobre K . Tomemos $x \in M$, recordemos que este elemento de M , lo podemos escribir como combinación lineal de los u_i , es decir,

$$x = \sum_{i \in I} \mu_i u_i$$

para algunos $\mu_i \in L$. Pero recordemos que los v_j generan L sobre K , así podemos escribir a cada μ_i como combinación lineal de los v_j , es decir,

$$\mu_i = \sum_{j \in J} \lambda_{ij} v_j$$

para algunos $\lambda_{ij} \in K$. Por tanto podemos escribir

$$x = \sum_{i \in I, j \in J} \lambda_{ij} u_i v_j$$

lo que significa que $u_i v_j$ genera M sobre K .

Resta probar que los $u_i v_j$ son linealmente independientes sobre K . Supongamos que tenemos

$$\sum_{i \in I, j \in J} \lambda_{ij} u_i v_j = 0$$

para algunos $\lambda_{ij} \in L$. Luego tenemos que

$$\sum_{i \in I} \left(\sum_{j \in J} \lambda_{ij} v_j \right) u_i = 0$$

y considerando que los u_i son linealmente independientes sobre L , tenemos que

$$\sum_{j \in J} \lambda_{ij} v_j = 0$$

para cada $j \in J$. Considerando que los v_j son linealmente independientes sobre K , tenemos que los $\lambda_{ij} = 0$ para cada $i \in I$ y $j \in J$, que era lo que estábamos buscando. ■

2.2 Campos de Descomposición

Sea L/K una extensión de campo y $f \in K[X]$, decimos que f se descompone completamente sobre L , si lo podemos escribir como un producto de factores lineales

$$f = k(X - \alpha_1) \dots (X - \alpha_n) \text{ para } i = 1, 2, \dots, n$$

cuando $k \in K$ y $\alpha_i \in L$. Llamamos a L el campo de descomposición para f .

Notemos que el campo de descomposición siempre existe, ya que si tomamos un factor irreducible g de f , entonces $K[X]/(g) = K(\alpha)$ es una extensión de K para la cual $g(\alpha) = 0$ y por el teorema del residuo tenemos que tanto g como f se descomponen en factores lineales. Por inducción tenemos que existe un campo de descomposición L para f , con $[L : K] \leq n!$ donde n es el grado de f . Por tanto los campos de descomposición son únicos salvo isomorfismos.

Ejemplo.

1. El campo de descomposición para $X^2 - 2$ sobre \mathbb{Q} es $\mathbb{Q}(\sqrt{2})$. Considerando que las raíces $\sqrt{2}$ y $-\sqrt{2}$ pertenecen a $\mathbb{Q}(\sqrt{2})$.
2. El campo de descomposición de $(X^2 - 2)(X^2 - 3)$ sobre \mathbb{Q} , es el campo $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
3. El campo de descomposición de $X^3 - 2$ sobre \mathbb{Q} , no es $\mathbb{Q}(\sqrt[3]{2})$. Ya que las raíces del polinomio son

$$\sqrt[3]{2}, \sqrt[3]{2} \left(\frac{-1 + i\sqrt{3}}{2} \right) \text{ y } \sqrt[3]{2} \left(\frac{-1 - i\sqrt{3}}{2} \right)$$

Por tanto el campo de descomposición de $X^3 - 2$ es $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$.

2.3 Separabilidad

Definición 2.3.1. *Un polinomio f sobre K lo llamamos separable si este no tiene raíces múltiples. Es decir, todas sus raíces son distintas. Un polinomio que no es separable lo llamamos inseparable.*

Así decimos que un campo L es separable sobre K si cada elemento de L es la raíz de un polinomio separable sobre K .

Ejemplo. El polinomio $X^2 - 2$ es separable sobre \mathbb{Q} considerando que $\pm\sqrt{2}$ son raíces distintas. El polinomio $(X^2 - 2)^n$ para $n \geq 2$ es inseparable ya que tiene raíces múltiples.

Un hecho bien importante y que debemos tener en cuenta es que si $\text{char}K = 0$, todos los polinomios son separables. Si $\text{char}K = p > 0$, entonces un polinomio $f \in K[X]$ es inseparable si y solo si $f \in K[X^p]$

De lo anterior, si tomamos una extensión de campo L/K y un elemento $\alpha \in L$, α es separable sobre K si el polinomio minimal $f_\alpha \in K[X]$ es separable. En otras palabras, una extensión se dice separable si α es separable para todo $\alpha \in L$. De otra forma, decimos que la extensión es inseparable.

Ejemplo. Consideremos $L = \mathbb{F}_p(t)$, el campo de funciones racionales sobre el campo finito \mathbb{F}_p con p elementos, y tomemos $K = \mathbb{F}_p(t^p)$. Entonces la extensión L/K es finita pero inseparable, ya que si consideramos el polinomio minimal de t sobre K , $X^p - t^p$, el cual podemos descomponerlo como $(X - t)^p$ sobre L .

2.4 Clausuras Algebraicas

Definición 2.4.1. *Un campo K es algebraicamente cerrado si todo polinomio $f \in K[X]$ se descompone en factores lineales sobre K .*

Ejemplo. El polinomio $X^2 - 5X + 6$ es separable sobre \mathbb{Q} , ya que se descompone en factores lineales $(X - 2)(X - 3)$.

Si pasamos a las extensiones de campo, decimos que una extensión L/K es la clausura algebraica de K si L/K es algebraica y L es algebraicamente cerrado.

Lema 2.4.2. *Si L/K es algebraica y cada polinomio en $K[X]$ se descompone completamente sobre L , entonces L es la clausura algebraica de K .*

Demostración. Debemos probar que L es algebraicamente cerrado. Supongamos que $L(\alpha)/L$ es una extensión finita y que

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

es el polinomio mínimo de α sobre L . Sea $K' = K(a_0, \dots, a_{n-1})$, así $K'(\alpha)/K'$ es una extensión finita y como cada $a_i \in L$ es algebraico sobre K , entonces 2.1.6 nos dice K'/K y $K'(\alpha)/K'$ son extensiones finitas. Entonces α es algebraico sobre K y por lo tanto $\alpha \in L$, lo que significa que L es algebraicamente cerrada. ■

Nota 2.4.3. La clausura algebraica siempre existe y es única.

2.5 Extensiones Normales

Definición 2.5.1. *Sea L una extensión algebraica de K , la cual es el campo de descomposición sobre K para una colección de polinomios $f(X) \in K[X]$. Entonces L se llama una extensión normal sobre K .*

Ejemplo. Si tomamos la extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, notamos que esta no es normal, ya que el polinomio $X^3 - 2$, no se descompone completamente sobre $\mathbb{Q}(\sqrt[3]{2})$.

Teorema 2.5.2. *Una extensión de campo L/K es normal y finita si y solo si L es un campo de descomposición para algún polinomio $f \in K[X]$*

Demostración. (\Rightarrow) Supongamos que L/K es normal y finita. Entonces $L = K(\alpha_1, \dots, \alpha_r)$, donde cada α_i tiene su polinomio minimal $f_i \in K[X]$. Si tenemos que $f = f_1 f_2 \cdots f_r$, es claro que L es el campo de descomposición de f sobre K , pues cada f_i es irreducible con un cero α_i en L . Por tanto, f se descompone completamente sobre L , esto por la normalidad de L .

(\Leftarrow) Supongamos que L es el campo de descomposición de algún $g \in K[X]$. La extensión es claramente finita. Nos resta probar la normalidad.

Supongamos que M/L es el campo de descomposición para un polinomio f y que

α_1 y α_2 son ceros de f en M . Entonces $[L(\alpha_1) : L] = [L(\alpha_2) : L]$. Esto nos lleva al resultado, ya que podemos escoger a $\alpha_1 \in L$ por la suposición y así para alguna raíz α_2 de f en M , tenemos que $[L(\alpha_2) : L] = 1$, es decir, $\alpha_2 \in L$. Por tanto f se descompone completamente sobre L . ■

2.6 Clausuras Normales

Sabemos que alguna extensión finita L/K es finitamente generada si $L = K(\alpha_1, \dots, \alpha_r)$. Sea $f_i \in K[X]$ el polinomio minimal para α_i . Si consideramos el campo de descomposición M/L para $f = f_1 \dots f_r$, entonces sabemos por el teorema anterior que M/L es normal, así definimos a M/K como la clausura normal de L/K .

Nota 2.6.1. La clausura normal de L/K se caracteriza como la extensión minimal M/L tal que M/K es normal, y así es única bajo isomorfismos sobre L .

Definición 2.6.2. Sean L/K y L'/K extensiones de campo. Una K -inmersión de L en L' es una inmersión que deja a K fijo. En el caso que $L = L'$ y L/K es finita, entonces la inmersión es sobreyectiva y por tanto es un automorfismo. En este caso llamamos la K -inmersión un K -automorfismo, denotamos el grupo de K -automorfismos de L/K por $\text{Aut}(L/K)$.

Teorema 2.6.3. Sea L/K una extensión finita y $\theta : L \hookrightarrow M$ una inmersión con M/L normal. Si $L' = L(\theta) \subseteq M$ entonces:

1. El número de K -inmersiones distintas $L \hookrightarrow M$ es a lo más $[L : K]$, la igualdad se da si y solo si L/K es separable.
2. L/K es normal si y solo si cada K -inmersión $\phi : L \hookrightarrow M$ tiene imagen L' si y solo si cada K -inmersión es de la forma $\phi = \theta \circ \alpha$ para algún $\alpha \in \text{Aut}(L/K)$.

Demostración.

1. Esta se da ya que si L/K es una extensión finita, el número de inmersiones $L \hookrightarrow M$ que se extienden a $K \hookrightarrow M$ es a lo más $[L : K]$.
2. Notemos que:
 - (a) L/K es normal si y solo si L'/K es normal.

- (b) Alguna K -inmersión $\phi : L \hookrightarrow M$ nos lleva a una K -inmersión $\psi : L' \hookrightarrow M$, donde $\psi = \phi \circ \theta^{-1}$ y viceversa.
- (c) Alguna K -inmersión $\phi : L \hookrightarrow M$ con imagen L' nos lleva a un automorfismo α de L/K tal que $\psi = \theta \circ \alpha$. Para el otro lado, algún ϕ de esta forma es una K -inmersión con imagen L' .

Por tanto lo único que tendríamos que probar es que L'/K es normal si y solo si alguna K -inmersión $\psi : L' \hookrightarrow M$ tiene imagen L' .

(\Rightarrow) Supongamos que $\alpha \in L'$ con polinomio minimal $f \in K[X]$. Si L'/K es normal entonces f se descompone completamente sobre L' . Ahora si $\psi : L' \hookrightarrow M$ es una K -inmersión, $\psi(\alpha)$ es otra raíz de f . Así $\psi(\alpha) \in L'$. Lo que significa que $\psi(L') \subseteq L'$ y si consideramos que L'/K es finita, entonces $\psi(L') = L'$.

(\Leftarrow) Supongamos que $f \in K[X]$ es un polinomio irreducible con un cero $\alpha \in L'$. Por hipótesis, M contiene una clausura normal M' de L/K y así f se descompone completamente sobre M' . Pero también, si L'/K es finita, $L' \subseteq M'$.

Sea $\beta \in M'$ otra raíz de f , entonces existe un isomorfismo sobre K , tal que $K(\alpha) \simeq K[X]/(f) \simeq K(\beta)$. Considerando que M' es el campo de descomposición para algún polinomio h sobre K , entonces también es el campo de descomposición para h sobre $K(\alpha)$ ó $K(\beta)$. Por tanto, por la unicidad del campo de descomposición $K(\alpha) \simeq K(\beta)$, el cual nos restringe a la K -inmersión $L' \hookrightarrow M$, el cual envía α a β . Por tanto $\beta \in L'$, y considerando que es verdad para todas las raíces β , f se descompone completamente sobre L' , lo que significa que L'/K es normal. ■

Corolario 2.6.4. *Si L/K es finita entonces $|\text{Aut}(L/K)| \leq [L : K]$. La igualdad se da si y solo si L/K es normal y separable.*

Demostración. Si consideramos que M/L es una extensión normal. Entonces por el teorema anterior

$$\begin{aligned} |Aut(L/K)| &= |K\text{-inmersión } L \hookrightarrow M \text{ de la forma } \theta \circ \alpha, \alpha \in Aut(L/K)| \\ &\leq |K\text{-inmersión } L \hookrightarrow M| \\ &\leq [L : K] \end{aligned}$$

es claro que la igualdad se da si y solo si L/K es normal y separable.

2.7 Extensiones de Galois

Definición 2.7.1. Si L es un campo y G es algún grupo finito de automorfismos de L entonces escribimos $L^G \subseteq L$ por el campo fijo

$$L^G = \{x \in L \mid g(x) = x \text{ para todo } g \in G\}$$

Notemos que L^G es un subcampo de L .

Definición 2.7.2. Decimos que una extensión L/K es una extensión Galois si $K = L^G$ para algún grupo finito de automorfismos G , en este caso $G \leq Aut(L/K)$.

Más adelante mostraremos que $G = Aut(L/K)$.

Proposición 2.7.3. Sea G un grupo finito de automorfismos actuando sobre un campo L , con $K = L^G \subseteq L$. Entonces

1. Para cada $\alpha \in L$ tenemos $[K(\alpha) : K] \leq |G|$.
2. L/K es separable.
3. L/K es finita con $[L : K] \leq |G|$.

Demostración. Ver [1]. ■

Teorema 2.7.4. Sea $K \subseteq L$ es una extensión finita de campos. Entonces los siguientes enunciados son equivalentes:

1. L/K es Galois,
2. K es un campo fijo de $Aut(L/K)$,
3. $|Aut(L/K)| = [L : K]$,

4. L/K es normal y separable.

Demostración. $3 \Leftrightarrow 4$: Esto es claro por 2.6.4.

$2 \Rightarrow 1$: Si K es el campo fijo de $\text{Aut}(L/K)$ entonces $K = L^G$ para algún grupo finito G , por tanto L/K es de Galois.

$1 \Rightarrow 2, 3$: Supongamos que $K = L^G$, para algún grupo finito G . De la proposición anterior tenemos que $[L : K] \leq |G|$, Pero $G \leq \text{Aut}(L/K)$ y así $|G| \leq |\text{Aut}(L/K)| \leq [L : K]$, por 2.6.4. Por tanto $|G| = [L : K]$ y $G = \text{Aut}(L/K)$. De aquí K es un campo fijo de $\text{Aut}(L/K)$ y $|\text{Aut}(L/K)| = [L : K]$.

$3 \Rightarrow 1$ Sea $G = \text{Aut}(L/K)$ finito, y consideremos que el conjunto $F = L^G$. Por la definición 2.7.2 tenemos que $F \supseteq K$, además que L/F es una extensión de Galois. Por tanto, $|G| = [L : F]$. Pero por hipótesis $|G| = [L : K]$. Entonces por la proposición 2.1.6, tenemos que $K = F$. ■

Si $K \subseteq L$ es una extensión de Galois, denotamos $\text{Gal}(L/K)$ por $\text{Aut}(L/K)$ y lo llamamos el grupo de Galois de la extensión.

Sea L/K una extensión finita de campos. El grupo $G = \text{Aut}(L/K)$ tiene $|G| \leq [L : K]$ por 2.7.3. Además, si $F = L^G \supseteq K$. Entonces por 2.7.4 llegamos a que $|G| = [L : F]$.

1. Si H es un subgrupo of G , entonces el campo fijo $M = L^H$ es un campo intermedio, es decir, $F \subseteq M \subseteq L$ con L/M Galois, así por 2.7.4 tenemos que $\text{Aut}(L/M) = H$.
2. Para algún campo intermedio $F \subseteq M \subseteq L$, es $H = \text{Aut}(L/M)$ un subgrupo de G .

De lo anterior concluimos que las operaciones

$$H \leq G \rightarrow F \subseteq L^H \subseteq L$$

$$\text{Aut}(L/M) \leq G \leftarrow F \subseteq M \subseteq L$$

Son mutuamente inversas.

Teorema 2.7.5 (Teorema Fundamental de la Teoría de Galois). *Con la notación de arriba,*

1. Existe una biyección de orden inverso entre los subgrupos H de G y el campo intermedio $F \subseteq M \subseteq L$, donde a H le corresponde al campo fijo L^H y a M le corresponde $\text{Aut}(L/M)$.
2. Un subgrupo H de G es normal si y solo si L^H/F es normal si y solo si L^H/F es Galois.
3. Si $H \triangleleft G$, entonces la aplicación $\alpha \in G \mapsto \alpha|_{L^H}$ determina un homomorfismo de grupos de G sobre $\text{Gal}(L^H/F)$ con núcleo H , y por tanto $\text{Gal}(L^H/F) \cong G/H$.

Demostración.

1. Esto fue lo que demostramos arriba.
2. Sea $M = L^H$, es fácil probar que el campo fijo para el subgrupo conjugado $\sigma H \sigma^{-1}$ con $\sigma \in G$ es σM . Entonces por la biyección probada en la parte 1, deducimos que $H \triangleleft G$ si y solo si $\sigma M = M$ para todo $\sigma \in G$. Veamos ahora que L es normal sobre F . Sabemos que L es el campo de descomposición para algún polinomio $f \in F[X]$ y por tanto L contiene una clausura normal N de M/F . Si algún $\sigma \in G$ determina una F -inmersión $M \hookrightarrow N$, y para el otro lado si cada F -inmersión $M \hookrightarrow N$ se extiende a un F -automorfismo σ de el campo de descomposición L de f . Por tanto M/F es normal si y solo si $\sigma M = M$ para todo $\sigma \in G$. Por último, M/F siempre es separable y así M/F es normal si y solo si M/F es Galois.
3. Sea $M = L^H$ y $H \triangleleft G$. Entonces tenemos que $\sigma(M) = M$ para todo $\sigma \in G$ y por tanto $\sigma|_M$ es un F -automorfismo de M . Por tanto existe un homomorfismo de grupos $\theta : G \rightarrow \text{Gal}(M/F)$ con $\ker \theta = \text{Gal}(L/M)$. Pero $\text{Gal}(L/M) = H$ por 2.7.4, y así $\theta(G) \cong G/H$. De aquí $|\theta(G)| = [G : H] = |G|/|H| = [L : F]/[L : M] = [M : F]$. Pero $|\text{Gal}(M/F)| = [M : F]$, entonces M/F es Galois y así θ es sobreyectiva e induce un isomorfismo $G/H \cong \text{Gal}(M/F)$.

Sea $f \in K[X]$ un polinomio separable y L/K una extensión de campos para f . Definimos el grupo de Galois de f por $\text{Gal}(f) = \text{Gal}(L/K)$.

Como f tiene todas sus raíces distintas en L por ser separable, entonces $L = K(\alpha_1, \dots, \alpha_d)$. Sabemos que un K -automorfismo de L es determinado por las acciones sobre las raíces α_i , así tenemos un homomorfismo inyectivo $\theta : G \hookrightarrow S_d$.

Lema 2.7.6. *Con las hipótesis consideradas arriba, $f \in K[X]$ es irreducible si y solo si G actúa transitivamente sobre las raíces de f , es decir, $\theta(G)$ es un subgrupo transitivo de S_d .*

Demostración. (\Leftarrow) Supongamos por reducción al absurdo que f es reducible. Por tanto $f = gh$ con $g, h \in K[X]$ y grado mayor que 0. Supongamos que α_1 es una raíz de g , Entonces para algún $\sigma \in G$, tenemos que $\sigma(\alpha_1)$ también es una raíz de g . Así G solo permuta raíces dentro de los factores irreducibles, lo que nos hace concluir que la acción no es transitiva.

(\Rightarrow) Supongamos que f es irreducible, entonces para i, j existe un K -isomorfismo $K(\alpha_i) \rightarrow K(\alpha_j)$, el cual podemos extender a K -automorfismos σ en L , así podemos hacer $\sigma(\alpha_i) = \alpha_j$, lo que significa que G actúa transitivamente sobre las raíces.

Definición 2.7.7. *Sea $f \in K[X]$ un polinomio con raíces distintas $\alpha_1, \dots, \alpha_d$ en el campo de descomposición L . El conjunto $\Delta = \prod_{i < j} (\alpha_i - \alpha_j)$. Entonces el discriminante D de f es*

$$D = \Delta^2 = (-1)^{d(d-1)/2} \prod_{i \neq j} (\alpha_i - \alpha_j)$$

Notemos que D es un elemento fijo de $G = \text{Gal}(L/K)$ y por tanto es un elemento de K .

También es importante notar que si $\text{char}K \neq 2$ y $f \in K[X]$ es un polinomio irreducible y separable de grado d , entonces $\Delta \neq 0$ y $\theta(G) \subseteq A_d$ si y solo si Δ es fijo bajo G .

Capítulo 3

ÁLGEBRAS CENTRALES SIMPLES

3.1 Preliminares

En este capítulo definiremos lo que es un álgebra central simple y discutiremos algunos teoremas importantes sobre estas álgebras que nos serán útiles más adelante. Comencemos por definir lo que es un álgebra, definida sobre un campo arbitrario K .

Definición 3.1.1. *Un K -álgebra es un par (A, μ) , donde A es un K -espacio vectorial y $\mu : A \times A \rightarrow A$ es una aplicación k -bilineal, la cual llamamos ley del producto de A .*

Un K -álgebra A se llama asociativa (conmutativa, unitaria) si la ley del producto es asociativa (conmutativa, unitaria).

Ejemplo. *El anillo de polinomios $K[X]$ es un K -álgebra conmutativa unitaria.*

Ejemplo. *Si L/K es una extensión de campo, entonces L es un K -álgebra conmutativa unitaria.*

Definición 3.1.2. *Un homomorfismo de K -álgebras es una aplicación K -lineal $f : A \rightarrow B$ que satisface*

$$f(aa') = f(a)f(a') \text{ para todo } a, a' \in A$$

Si consideramos a A y B como álgebras unitarias, tenemos la condición que $f(1_A) = 1_B$. También definimos un isomorfismo de K -álgebras como un homomorfismo de K -álgebras biyectivo.

Definición 3.1.3. *Un subálgebra de un K -álgebra A es un subespacio lineal de A el cual es cerrado bajo el producto.*

Decimos que un subálgebra es unitaria (asociativa, conmutativa) si el álgebra también lo es.

Ejemplo. La imagen de un homomorfismo de K -álgebras $f : A \rightarrow B$ es un subálgebra de B .

Ejemplo. El centro de un K -álgebra A la cual definimos por

$$Z(A) = \{z \in A \mid az = za \text{ para todo } a \in A\}$$

es un subálgebra conmutativa de A .

Continuamos con estos preliminares definiendo lo que es un K -álgebra de división y el producto tensorial.

Definición 3.1.4. *Un K -álgebra de división es un K -álgebra que también es un anillo de división, es decir, cada elemento distinto de cero es inversible.*

Si A y B son K -álgebras, llamamos el *producto tensorial* $A \otimes_K B$ al K -espacio vectorial generado por elementos de la forma $a \otimes b$, donde $a \in A$ y $b \in B$, que además satisfaga:

$$(a + a') \otimes b = a \otimes b + a' \otimes b$$

$$a \otimes (b + b') = a \otimes b + a \otimes b'$$

$$(\lambda a) \otimes b = a \otimes (\lambda b) = \lambda(a \otimes b)$$

para todo $a, a' \in A$, $b, b' \in B$ y $\lambda \in K$.

El producto sobre $A \otimes_K B$ es la única ley distributiva que cumple

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb' \text{ para todo } a, a' \in A, b, b' \in B$$

De lo anterior tenemos que la K -álgebra $A \otimes_K B$ es unitario (asociativa, conmutativa) cuando A y B lo son.

3.2 Álgebras Centrales Simples

Ahora consideramos todas las K -álgebras unitaria, asociativas y finito dimensionales sobre K , así podemos identificar a K con $K \cdot 1_A$, y por tanto tenemos que $K \subseteq Z(A)$.

Tomemos un K -álgebra A tal que tenemos el isomorfismo de L -álgebras

$$A \otimes_K L \simeq M_n(L)$$

para alguna extensión de L/K .

Necesitamos encontrar condiciones necesarias para la existencia de tal isomorfismo.

Esto lo hacemos con la siguiente proposición.

Proposición 3.2.1. *Si $A \otimes_K L \simeq M_n(L)$, entonces $Z(A) = K$.*

Demostración. Veamos primero cuál es el centro de A . Supongamos que

$f : A \otimes_K L \xrightarrow{\sim} M_n(L)$ es un isomorfismo de L -álgebras, que además es L -lineal, así

$$f(1 \otimes \lambda) = f(\lambda \cdot 1 \otimes 1) = \lambda \cdot f(1 \otimes 1) = \lambda I_n \text{ para todo } \lambda \in L.$$

Por definición tenemos que $K \subseteq Z(A)$. Resta mostrar que $Z(A) \subseteq K$. Para esto tomemos $a \in Z(A)$. Esto implica que $f(a \otimes 1) \in Z(M_n(L)) = LI_n$. Por tanto, $f(a \otimes 1) = \lambda I_n$ para algún $\lambda \in L$. Así obtenemos que $f(a \otimes 1) = f(1 \otimes \lambda)$ y además que $a \otimes 1 = 1 \otimes \lambda$.

Sea $e_1 = 1, e_2, \dots, e_m$ una K -base de A , escribimos a $a = \lambda_1 1 + \lambda_2 e_2 + \dots + \lambda_m e_m$ para algunos $\lambda_i \in K$, así podemos escribir

$$\begin{aligned} a \otimes 1 &= 1 \otimes \lambda_1 + e_2 \otimes \lambda_2 + \dots + e_m \otimes \lambda_m \\ &= \lambda_1 \cdot (1 \otimes 1) + \lambda_2 \cdot (e_2 \otimes 1) + \dots + \lambda_m \cdot (e_m \otimes 1). \end{aligned}$$

Entonces, como $a \otimes 1 = 1 \otimes \lambda$,

$$\lambda_1 \cdot (1 \otimes 1) + \lambda_2 \cdot (e_2 \otimes 1) + \dots + \lambda_m \cdot (e_m \otimes 1) = \lambda \cdot (1 \otimes 1).$$

Así llegamos a que $1 \otimes 1, e_2 \otimes 1, \dots, e_m \otimes 1$ es una L -base de $A \otimes_K L$. Además tenemos que $\lambda = \lambda_1 \in K$ y $\lambda_2 = \lambda_3 = \dots = \lambda_m = 0$, lo que significa que $a = \lambda e_1 = \lambda 1 \in K$. Por tanto $Z(A) \subseteq K$. En conclusión $Z(A) = K$. ■

De lo anterior podemos dar la siguiente definición.

Definición 3.2.2. *Un K -álgebra A la llamamos central si $Z(A) = K$.*

Los siguientes ejemplos nos ilustran este tipo de álgebras.

Ejemplo. La K -álgebra $M_n(L)$ es central.

Ejemplo. Si D es un anillo de división, entonces $Z(D)$ es un campo y D es un $Z(D)$ -álgebra central.

Ejemplo. Si L/K es una extensión de campo, entonces L no es un K -álgebra central.

Definamos ahora lo que es un álgebra simple:

Definición 3.2.3. *Un K -álgebra A se llama simple si sus únicos ideales a ambos lados son (0) y A .*

Ejemplo. Si K es un campo arbitrario, entonces $M_n(K)$ es un K -álgebra central simple para todo $n \geq 1$.

Ejemplo. Si D es un anillo de división, entonces D es un $Z(D)$ -álgebra central simple.

Definición 3.2.4. *Un K -álgebra central simple decimos que es desplegada si es isomorfa a un álgebra de matrices.*

Lo que veremos ahora son algunas propiedades importantes de las álgebras centrales simples, en sí es verificación de las operaciones clásicas. Comenzamos con un lema sobre productos tensoriales.

Lema 3.2.5. *Sean A y B dos K -álgebras. Si $b_1, b_2, \dots, b_m \in B$ son linealmente independientes sobre K , entonces para todo $x_1, x_2, \dots, x_m \in A$, tenemos*

$$x_1 \otimes b_1 + x_2 \otimes b_2 + \dots + x_m \otimes b_m = 0 \Rightarrow x_1 = x_2 = \dots = x_m = 0$$

De la misma manera, si $a_1, \dots, a_n \in A$ son linealmente independientes sobre K , entonces para todo $y_1, y_2, \dots, y_n \in B$, tenemos

$$a_1 \otimes y_1 + a_2 \otimes y_2 + \dots + a_n \otimes y_n = 0 \Rightarrow y_1 = y_2 = \dots = y_n = 0$$

Demostración. Haremos solamente la primera parte. La otra parte se hace de manera similar. Empecemos completando b_1, b_2, \dots, b_m , en una K -base b_1, b_2, \dots, b_s de B . Sea a_1, a_2, \dots, a_r una K -base de A , por tanto podemos escribir $x_j = \sum_i x_{ij} a_i$, para $x_{ij} \in K$. Tenemos que

$$\sum_{i,j} x_{ij} a_i \otimes b_j = 0$$

Así $(a_i \otimes b_j)_{i,j}$ es una K -base de $A \otimes_K B$, por tanto $x_{ij} = 0$ para todo i, j . En conclusión $x_1 = \dots = x_m = 0$. ■

Este lema también es cierto para K -espacios vectoriales no necesariamente finito dimensionales.

Definición 3.2.6. Sea A un K -álgebra, y sea $B \subseteq A$ un subconjunto de A . El centralizador de B en A es el conjunto $C_A(B)$ que definimos por

$$C_A(B) = \{a \in A \mid ab = ba \text{ para todo } b \in B\}$$

Notemos que el centralizador de B en A es un subálgebra de A y que $C_A(A) = Z(A)$.

Proposición 3.2.7. Sean A y B dos K -álgebras. Asumamos que A' y B' son subálgebras de A y B respectivamente, entonces tenemos

$$C_{A \otimes_K B}(A' \otimes_K B') = C_A(A') \otimes_K C_B(B')$$

Demostración. Es claro de la definición que $C_{A \otimes_K B}(A' \otimes_K B') \supseteq C_A(A') \otimes_K C_B(B')$. Por otro lado, sea b_1, b_2, \dots, b_m una K -base de B , y sea $x \in C_{A \otimes_K B}(A' \otimes_K B')$. Podemos escribir los elementos de B como combinaciones lineales de b_j donde $j = 1, \dots, m$, así vemos que $x = x_1 \otimes b_1 + \dots + x_m \otimes b_m$, donde los $x_i \in A$, y como

$x \in C_{A \otimes_K B}(A' \otimes_K B')$ entonces para todo $a' \in A'$, tenemos que $(a' \otimes 1)x = x(a' \otimes 1)$, de esto obtenemos que

$$(a'x_1 - x_1a') \otimes b_1 + \cdots + (a'x_m - x_ma') \otimes b_m = 0 \text{ para todo } a' \in A'$$

y por el lema anterior tenemos que

$$a'x_j = x_ja' \text{ para todo } a' \in A'.$$

Así $x_1, x_2, \dots, x_m \in C_A(A')$. También si consideramos una K -base a_1, \dots, a_n de $C_A(A')$, entonces podemos escribir a x como

$$x = a_1 \otimes y_1 + \cdots + a_n \otimes y_n$$

para $y_i \in B$. De igual manera llegamos a que $y_1, y_2, \dots, y_n \in C_B(B')$. Por tanto, $x \in C_A(A') \otimes_K C_B(B')$ que era lo que queríamos probar. ■

Corolario 3.2.8. Sean A y B dos K -álgebras, y sea L/K una extensión de campo.

Lo siguiente se cumple:

1. $A \otimes_K B$ es central sobre K si y solo si A y B son centrales sobre K .
2. $A \otimes_K L$ es central sobre L si y solo si A es central sobre K .

Demostración.

1. Por la proposición anterior tenemos que $Z(A \otimes_K B) = Z(A) \otimes_K Z(B)$, además, $\dim_K(Z(A \otimes_K B)) = \dim_K(Z(A))\dim_K(Z(B))$. Como $A \otimes_K B$ es central sobre K si y solo si $\dim_K(Z(A \otimes_K B)) = 1$, tenemos $\dim_K(Z(A)) = \dim_K(Z(B)) = 1$, lo que significa que A y B son centrales sobre K .
2. De nuevo por la proposición anterior, tenemos $Z(A \otimes_K L) = Z(A) \otimes_K L$, así $\dim_L(Z(A \otimes_K L)) = \dim_K(Z(A))$, lo que concluye la prueba. ■

Proposición 3.2.9. Si A y B son K -álgebras simples, entonces $A \otimes_K B$ es simple.

Demostración. Sea I un ideal a ambos lados no trivial de $A \otimes_K B$, y sea

$x = a_1 \otimes b_1 + \cdots + a_m \otimes b_m \in I, x \neq 0$ tal que $m \geq 1$ es minimal. En particular,

b_1, \dots, b_m son K -linealmente independientes. Probémoslo primero para $m = 1$. Consideremos que $a_m \neq 0$. Por la minimalidad de m , el ideal a dos lados de A generado por a_m es A , así existen $x_i, x'_i \in A$ tal que $\sum_i x_i a_m x'_i = 1$. Entonces tenemos

$$\sum_i (x_i \otimes 1)x(x'_i \otimes 1) = \left(\sum_i x_i a_1 x'_i\right) \otimes b_1 + \dots + \left(\sum_i x_i a_m x'_i\right) \otimes b_m \in I.$$

Así podemos asumir, sin pérdida de generalización, que $a_m = 1$.

Ahora asumamos que $m > 1$. Por la minimalidad de m , a_{m-1} y $a_m = 1$ son K -linealmente independientes, así $a_{m-1} \notin K$. Sea A central, pero $a_{m-1} \notin Z(A)$, luego existe $a \in A$ tal que $aa_{m-1} - a_{m-1}a \neq 0$. Como $a_m = 1$, tenemos

$$(a \otimes 1)x - x(a \otimes 1) = (aa_1 - a_1a) \otimes b_1 + \dots + (aa_{m-1} - a_{m-1}a) \otimes b_{m-1}.$$

Así este elemento es un elemento no cero de I , pues $aa_{m-1} - a_{m-1}a \neq 0$ y b_1, b_2, \dots, b_{m-1} son linealmente independientes, lo que contradice la minimalidad de m . Por tanto $m = 1$, e I contiene un elemento de la forma $1 \otimes b$. Considerando que B es simple, entonces tenemos que I contiene a $1 \otimes 1$ y así $I = A \otimes_K B$, lo que concluye la prueba. ■

Corolario 3.2.10. Sean A y B dos K -álgebras y sea L/K una extensión de campo.

Lo siguiente se cumple:

1. Si A y B son centrales simples, entonces también lo es $A \otimes_K B$.
2. Si A es central simple sobre K , entonces $A \otimes_K L$ es central simple sobre L .

La demostración de este corolario es inmediata del corolario anterior y de la proposición que acabamos de demostrar.

Lema 3.2.11. (Schur) Sea M un módulo simple sobre una K -álgebra A , Entonces los $\text{End}_A(M)$ es una álgebra de división.

3.3 Anillos

Si R es un anillo y $e \in R$ es un elemento idempotente diferente de cero, entonces eRe es un anillo para la suma y la multiplicación de R , con unidad e . Con esta pequeña introducción podemos enunciar los siguientes dos lemas:

Lema 3.3.1. *Si R es un anillo, y e es un elemento idempotente diferente de cero en R , entonces tenemos un isomorfismo de anillos*

$$eRe \simeq \text{End}_R(eR)$$

donde eR es considerado un R -módulo a la derecha.

Demostración. Ver [1].■

Lema 3.3.2. *Sea R un anillo, y sea M un R -módulo a la derecha para todo $n \geq 1$, tenemos un isomorfismo de anillos*

$$\text{End}_R(M^n) \simeq M_n(\text{End}_R(M))$$

Demostración. ver [1].■

Ahora sea A un K -álgebra central simple, entonces decimos que A tiene un ideal a derecha (izquierda), si el ideal I a derecha (izquierda) de A es en particular un subespacio lineal y así finito dimensional sobre K . Por tanto un ideal diferente de cero de la menor dimensión posible es minimal.

Proposición 3.3.3. *Sea A un K -álgebra central simple, y sea I un ideal minimal a izquierda (derecha). Entonces para cada A -módulo a izquierda (derecha) finitamente generado $M \neq 0$, tenemos*

$$M \simeq I^n \text{ para algún } n \geq 1$$

En particular, todos los ideales a izquierda (derecha) son isomorfos.

Demostración. Probaremos la proposición solo para ideales a izquierda, la demostración para ideales a derecha se hace similarmente. Un ideal a derecha generado por los

elementos de I es un ideal diferente de cero a ambos lados de A , y por tanto iguales a A , por la hipótesis. En particular, podemos escribir

$$1 = \alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_m a_m \text{ para algunos } a_i \in A \text{ y } \alpha_i \in I$$

Así para todo $a \in A$,

$$a = a(\alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_m a_m) = (a\alpha_1)a_1 + (a\alpha_2)a_2 + \cdots + (a\alpha_m)a_m$$

de lo anterior decimos que I es un ideal a izquierda, pues nosotros tenemos $a\alpha_i \in I$ para todo i , y además $A = Ia_1 + Ia_2 + \dots + Ia_m$. Sea M un A -módulo a izquierda. Por la hipótesis,

$$M = A \cdot x_1 + A \cdot x_2 + \cdots + A \cdot x_r$$

para algunos $x_1, x_2, \dots, x_r \in A$. Como $A = 1 \cdot a_1 + 1 \cdot a_2 + \cdots + 1 \cdot a_m$

$$M = \sum_{i,j} (a_j I) \cdot x_i = \sum_{i,j} I \cdot (a_j \cdot x_i)$$

Debemos probar que existen elementos $m_1, m_2, \dots, m_n \in M$ tal que $M = I \cdot m_1 + \cdots + m_n \cdot I$. Escojamos un n que sea minimal para esta propiedad. Sabemos que $n \geq 1$ si $M \neq 0$, entonces $M = I \cdot m_1 \oplus I \cdot m_2 \oplus \cdots \oplus I \cdot m_n$. Asumamos que $\beta_1 \cdot m_1 + \cdots + \beta_n \cdot m_n = 0$ para algunos $\beta_i \in I$. Si uno de estos es diferente de cero, supongamos β_n , entonces $A\beta_n$ es un ideal a izquierda de A diferente de cero que está contenido en I , ya que $\beta_n \in I$. Así I es minimal y $A\beta_n = I$. Por tanto

$$I \cdot m_n = A \cdot (\beta_n \cdot m_n) = A \cdot (-\beta_1 \cdot m_1 - \cdots - \beta_{n-1} \cdot m_{n-1})$$

para cada i , por tanto tenemos que $A \cdot (\beta_i \cdot m_i) = (A\beta_i) \cdot m_i \subset I \cdot m_i$, lo que nos lleva finalmente a que

$$M = I \cdot m_1 + \cdots + I \cdot m_{n-1}$$

Esto contradice la minimalidad de n . Ahora la aplicación A -lineal

$$f : I^n \rightarrow M$$

$$(\beta_1, \dots, \beta_n) \mapsto \sum_{i=1}^n \beta_i \cdot m_i$$

es un isomorfismo de A -módulos a izquierda, considerando a $M = I \cdot m_1 \oplus I \cdot m_2 \oplus \dots \oplus I \cdot m_n$. Si J es un ideal a izquierda minimal, entonces este es finitamente generado sobre K , así por lo que acabamos de probar $J \simeq I^n$ para algún $n \geq 1$. Pero un ideal minimal a izquierda es un A -módulo a izquierda simple, lo que nos dice que $n = 1$, y esto concluye nuestra prueba. ■

Con lo anterior tenemos las bases suficientes para probar el teorema de Wedderburn, que es de los más importantes en la teoría de las álgebras centrales simples.

Teorema 3.3.4. (Wedderburn) *Sea K un campo.*

1. *Para todo par de enteros $r, s \geq 1$ y todo par de K -álgebras de división D y D' , tenemos que*

$$M_r(D) \simeq M_s(D') \Rightarrow D \simeq D'$$

2. *Para cada K -álgebra central simple A , existe un entero $r \geq 1$ y una K -álgebra de división D tal que $A \simeq M_r(D)$. El entero r y la clase de isomorfismos de D son únicamente determinadas por la clase de isomorfismos de A .*

Demostración. Sea que K un campo.

1. Veamos primero que si $T = (d_{ij}) \in M_r(D)$, entonces

$$E_{11}TE_{11} = d_{11}E_{11} = E_{11}d_{11}$$

esto lo notamos fácilmente, pues si consideramos la aplicación

$$E_{11}DE_{11} \rightarrow D$$

$$d_{11}E_{11} \mapsto d_{11}$$

podemos ver que este es un isomorfismo.

Ahora probemos que $M = E_{11}D$ es un ideal minimal a derecha de D . Empecemos asumiendo que

$$M = \begin{pmatrix} * & \dots & * \\ 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix} = \{d_{11}E_{11} + \dots + d_{1r}E_{1r} \in D\}$$

Consideremos que I es un ideal a derecha no cero que está contenido en M . Sea $T = d_{11}E_{11} + \dots + d_{1r}E_{1r}$, con $d_{1j} \in I$. Así $E_{1s} = E_{1j}E_{js} \in I$ para $1 \leq s \leq r$, lo que nos lleva a que $M \subset I$, por tanto $M = I$ y M es minimal y usando el lema [3.3.1](#) tenemos que

$$D \simeq E_{11}M_r(D)E_{11} \simeq \text{End}_{M_r(D)}(M)$$

De una manera similar llegamos a que $D' \simeq \text{End}_{M_s(D)}(M')$, donde M' es un ideal minimal a derecha de $M_s(D)$. Supongamos $\phi : M_r(D) \simeq M_s(D')$ es un isomorfismo de k -álgebras, entonces $\phi(M)$ es un ideal a derecha minimal de M' y como por la proposición anterior tenemos que todos los ideales minimales a derecha son isomorfos, entonces tenemos que $M' \simeq \phi(M)$, además que

$$D \simeq \text{End}_{M_r(D)}(M) \simeq \text{End}_{M_s(D')}(\phi(M)) \simeq \text{End}_{M_s(D')}(M') \simeq D'$$

Concluimos que D está determinado de forma única por A isomorfismos.

2. Sea M un ideal minimal a derecha de A . Consideremos que M es un A -módulo simple. Sabemos que $D = \text{End}_A(M)$ es un anillo de división por el lema de Schur. Más aún, si A es un A -módulo a derecha, tenemos que $A \simeq M^r$ para algún $r \geq 1$. Por la proposición, por el primer lema con $e = 1$ y por el segundo tenemos que

$$A \simeq \text{End}_A(A) \simeq \text{End}_A(M^r) \simeq M_r(\text{End}_A(M)) = M_r(D)$$

Dos resultados inmediatos del teorema son:

Corolario 3.3.5. *Sean A y B dos k -álgebras centrales simples. Para cada entero $n \geq 1$, tenemos que*

$$M_n(A) \simeq M_n(B) \Leftrightarrow A \simeq B$$

Demostración. *Supongamos que $M_n(A) \simeq M_n(B)$. Por el teorema de Wedderburn, podemos escribir $A \simeq M_r(D)$ y $B \simeq M_s(D')$, donde D, D' son K -álgebras centrales simples. Por lo tanto*

$$M_{nr}(D) \simeq M_{ns}(D')$$

Por la unicidad del teorema de Wedderburn, tenemos que $nr = ns$ y $D = D'$, lo cual implica que $A \simeq B$.

Corolario 3.3.6. *Si k es algebraicamente cerrado, cada k -álgebra central simple es isomorfa a un álgebra de matrices.*

Para concluir este capítulo, enunciaremos un teorema que más adelante nos será muy útil.

Teorema 3.3.7. *(Skolem-Noether) Sea A un álgebra central simple sobre K y sea $B \subset A$ una subálgebra simple. Cada homomorfismo de K -álgebras $\rho : B \rightarrow A$ se extiende a un automorfismo interno, es decir, existe un $a \in A^\times$ tal que $\rho(b) = aba^{-1}$ para todo $b \in B$.*

Capítulo 4

GRUPOS ALGEBRAICOS

En este capítulo definiremos lo que es un grupo lineal algebraico, empezamos definiendo lo que es un esquema de grupo y vemos algunas propiedades de estos, como lo son la componente conexa y las álgebras de Lie.

4.1 Álgebras de Hopf

Sea K un campo y A una K -álgebra conmutativa con multiplicación $m : A \otimes_K A \rightarrow A$. Asumamos los siguientes homomorfismos de K -álgebras

$$c : A \rightarrow A \otimes_K A \text{ (co-multiplicación)}$$

$$i : A \rightarrow A \text{ (co-inversa)}$$

$$u : A \rightarrow K \text{ (co-unidad)}$$

los cuales satisfacen:

a. El diagrama

$$\begin{array}{ccc}
 A & \xrightarrow{c} & A \otimes_K A \\
 \downarrow c & & \downarrow c \otimes id \\
 A \otimes_K A & \xrightarrow{id \otimes c} & A \otimes_K A \otimes_K A
 \end{array}$$

conmuta.

b. La aplicación

$$A \xrightarrow{c} A \otimes_K A \xrightarrow{u \otimes id} K \otimes_k A = A$$

es igual a la aplicación $id : A \rightarrow A$.

c. Las dos aplicaciones

$$A \xrightarrow{c} A \otimes_K A \xrightarrow{i \otimes id} A \otimes_K A \xrightarrow{m} A$$

$$A \xrightarrow{u} K \xrightarrow{\cdot 1} A$$

coinciden.

Un K -álgebra A junto con las aplicaciones c , i y u , la llamamos un *álgebra de Hopf sobre K* . Un homomorfismo de tales K -álgebras preserva c , i y u , es decir, si $f : A \rightarrow B$ es un homomorfismo de K -álgebras, entonces $(f \otimes f) \circ c_A = c_B \circ f$, $f \circ i_A = i_B \circ f$ y $u_A = u_B \circ f$.

Nota 4.1.1. Las álgebras de Hopf y los homomorfismos de álgebras de Hopf forman una categoría.

Si consideramos A una K -álgebra de Hopf y L/K una extensión de campo, entonces A_L junto con c_L , i_L y u_L , forman un una álgebra de Hopf sobre L . También si J es un ideal de A tal que $c(J) \subset J \otimes_K A + A \otimes_K J$, $i(J) \subset J$ y $u(J) = 0$ lo llamamos el *ideal de Hopf*.

4.2 Esquemas de grupo

Sea A un álgebra de Hopf sobre K , para alguna K -álgebra asociativa conmutativa unital R , definimos el producto

$$G^A = \text{Hom}_{\text{Alg}_K}(A, R)$$

por la fórmula $fg = m_R \circ (f \otimes_R g) \circ c_R$ donde m_R es la multiplicación en R . Notemos que por las propiedades de álgebras de Hopf este producto es asociativo. Además, tiene una identidad por izquierda dada por $A \xrightarrow{u} K \rightarrow R$ y una inversa dada por $f^{-1} = f \circ i$, por tanto G^A cumple las condiciones para ser un grupo.

Siguiendo con esto para un homomorfismo de K -álgebras $f : R \rightarrow S$, existe un homomorfismo de grupos

$$G^A(f) : G^A(R) \rightarrow G^A(S), g \mapsto f \circ g$$

Por tanto podemos definir el functor¹

$$G^A : \text{Alg}_K \rightarrow \text{Grupos}$$

Dado todo lo de arriba definimos un *esquema de grupo (afín)* G sobre K por el functor $G : \text{Alg}_K \rightarrow \text{Grupos}$, que es isomorfo a G^A , para alguna álgebra de Hopf A sobre K . Por el lema de Yoneda² podemos representar a $A = k[G]$.

Nota 4.2.1. Un esquema de grupo G es conmutativo si y solo si $G(R)$ es conmutativo.

Definición 4.2.2. Un esquema de grupo G lo llamamos *algebraico* si la K -álgebra $K[G]$ es *finitamente generada*.

También podemos mirar a $G(R)$ como el conjunto de soluciones de las ecuaciones sobre R , esto lo vemos mejor en los siguientes ejemplos de esquemas de grupo.

Ejemplo.

1. Definimos $G_a = \text{Hom}_{\text{Alg}_K}(K[X], R)$, considerando

$$c(X) = X \otimes 1 + 1 \otimes X$$

$$i(X) = -X$$

$$u(X) = 0$$

El cual llamamos *el grupo aditivo* y lo denotamos por $G_a(R) = (R, +)$.

¹ Un functor es un morfismo entre categorías

² El lema de Yoneda nos dice que cualquier álgebra A está únicamente representada por G

2. Definimos por $G_m = \text{Hom}_{\text{alg}_K}(K[X, X^{-1}], R)$, considerando

$$c(X) = X \otimes X$$

$$i(X) = X^{-1}$$

$$u(X) = 1$$

el cual llamamos *el grupo multiplicativo* y lo denotamos por $G_m(R) = (R^\times, \times)$.

3. Definimos por $SL_n(R) = \text{Hom}_{\text{Alg}_K}\left(\frac{K[X_{11}, X_{22}, \dots, X_{nn}]}{\det(X_{ij}) - 1}, R\right)$. Considerando

$$c(X_{ij}) = X_{ij} \otimes X_{ij}$$

$$i(X_{ij}) = X_{ij}^{-1} \qquad \det(X_{ij}) = 1$$

$$u(X_{ij}) = Id_n$$

A este esquema grupo lo llamamos el *grupo lineal especial*.

4. Del ejemplo anterior, tenemos que las matrices $n \times n$ con entradas en R con determinante igual a la unidad nos genera el esquema de grupo

$$GL_n(R) = \left(\frac{K[X_{11}, X_{22}, \dots, X_{nn}, Y]}{\det(X_{ij}Y - 1)}, R\right)$$

El cual tiene la misma estructura para c , i y u . Este lo llamamos el *grupo lineal general*.

5. Definimos por $\mu_n = \text{Hom}_{\text{Alg}_K}(K[X]/(X^n - 1), R)$, considerando

$$c(X) = X \otimes X$$

$$i(X) = X^{n-1}$$

$$u(X) = 1$$

Este lo llamamos el esquema de grupo de las n -ésimas raíces de unidad.

6. Sea V un espacio vectorial finito dimensional sobre K definimos el esquema de grupo $\mathbf{GL}(V) = \{\text{automorfismos de } R \otimes_K V \text{ con determinante } 1\}$

7. Definimos por $O_n(R) = \{X \in GL_n(R) \mid XX^t = I\}$ y lo llamamos *grupo ortogonal*.
8. Definimos por $U_n(R) = \{X \in GL_n(R) \mid X\overline{X^t} = I\}$, este lo llamamos *grupo unitario*.
9. Definimos por $Sp_n(R) = \{J \in GL_n(R) \mid B^tJB = J \text{ para todo } B \in GL_n\}$, este lo llamamos *grupo simpléctico*. En este caso $n = 2k$

Los últimos tres ejemplos son subgrupos de GL_n , como también lo es SL_n . Decimos que el esquema de grupo H representado por A/J donde J es un ideal de Hopf y el homomorfismo de esquemas de grupo $\rho : H \rightarrow G$ inducidos por la aplicación natural $A \rightarrow A/J$, nos llevan a decir que el homomorfismo $\rho_R : H(R) \rightarrow G(R)$ es inyectivo, y así, podemos identificar a $H(R)$ como un subgrupo de $G(R)$, donde H lo llamamos *el subgrupo (cerrado) de G* y a ρ la llamamos la *inmersión cerrada*.

Nota 4.2.3. H es un subgrupo normal de G , siempre y cuando $H(R)$ sea normal a $G(R)$, con $R \in Alg_K$.

Además de los subgrupos ya mostrados podemos definir otros más que nos serán muy útiles:

Ejemplo.

1. Para algún esquema de grupo G , definimos el *ideal de aumento* por $I = \ker(u) \subset K[G]$ correspondiente a los subgrupos triviales $\mathbf{1}$ considerando $K[G]/I \simeq K$.
2. Sea V un espacio vectorial finito dimensional sobre K . Para $v \in V$, con $v \neq 0$, consideramos

$$S_v(R) = \{\alpha \in \mathbf{GL}(\mathbf{V}_R) \mid \alpha(v) = v\} \subset \mathbf{GL}(\mathbf{V})(R)$$

Este lo llamamos *estabilizador de v* .

3. Sea $U \subset V$ un subespacio, consideremos

$$N_U(R) = \{\alpha \in \mathbf{GL}(\mathbf{V}_R) \mid \alpha(U_R) = U_R\} \subset \mathbf{GL}(\mathbf{V})(R)$$

Este lo llamamos *normalizador de U* .

4. Sea $\rho : G \rightarrow \mathbf{GL}$ un homomorfismo de esquemas de grupo y sea $0 \neq v \in V$. La imagen inversa del estabilizador $\rho^{-1}(S_v)$ la denotamos por $\mathbf{Aut}_G(v)$,

$$\mathbf{Aut}_G(v)(R) = \{g \in G(R) \mid \rho_R(g)(v) = v\}$$

5. Sea A una K -álgebra de dimensión finita, $V = \text{Hom}(A \otimes_K A, A)$ y $v \in V$ la aplicación multiplicación en A . Consideramos el homomorfismo de esquema de grupo

$$\rho : \mathbf{GL}(A) \rightarrow \mathbf{GL}(V)$$

dado por

$$\rho_R(\alpha)(f)(a \otimes a') = \alpha(f(\alpha^{-1}(a) \otimes \alpha^{-1}(a')))$$

Este esquema de grupo en especial lo denotamos por $\mathbf{Aut}_{\text{Alg}}(A)$.

4.3 Componente conexa

Este es un concepto topológico muy importante que estaremos implementando mucho a lo largo de este capítulo. Empecemos recordando que un espacio topológico no vacío es irreducible si no lo podemos escribir como la unión de dos subconjuntos cerrados propios. Sea K -álgebra finitamente generada y sea $B \subset A$ una subálgebra étale [2] sobre K . Consideremos la K_{sep} -álgebra $B \otimes_K K_{\text{sep}}$ que es generada por idempotentes. Notemos que la $\dim_K B$ es acotada por un número finito de idempotentes primitivos de $A \otimes_K K_{\text{sep}}$. Así existe una única K -álgebra étale grande en A , la cual denotamos por $\pi_0(A)$. En el caso topológico $\pi_0(A)$ sería el conjunto de todas las componentes conexas, que es el subespacio conexo maximal. Nosotros lo miramos como K -álgebras separables y $\pi_0(A)$ será el álgebra separable maximal.

Proposición 4.3.1. *Sea A una K -álgebra finitamente generada*

1. *A es conexa si y solo si $\pi_0(A)$ es un campo.*
2. *Si L/K es una extensión de campo, entonces*

$$\pi_0(A_L) = \pi_0(A)_L$$

3. Si B es una K -álgebra finitamente generada

$$\pi_0(A \otimes_K B) = \pi_0(A) \otimes_K \pi_0(B)$$

Demostración. Ver [7, 6.5]. ■

Proposición 4.3.2. *Sea A un álgebra de Hopf finitamente generada sobre K . Entonces A es conexa si y solo si $\pi_0(A) = K$.*

Demostración. \Leftarrow) Supongamos que $\pi_0(A) = K$, por tanto por la primera parte de 4.3.1 tenemos que A es conexa.

\Rightarrow) Si suponemos que A es conexa, y como $u : \pi_0 \rightarrow A$, entonces $\pi_0(A) = K$ ■

Notemos que si tomamos

$$c : \pi_0(A \otimes_K A) = \pi_0(A) \otimes_K \pi_0(A) \rightarrow \pi_0(A)$$

$$i : \pi_0(A) \rightarrow \pi_0(A)$$

$$u : \pi_0(A) \rightarrow A$$

Tenemos que $\pi_0(A)$ es un K -álgebra de Hopf. El respectivo esquema de grupo lo denotamos $\pi_0(G)$ y existe la sobreyección $G \rightarrow \pi_0(G)$. Por las proposiciones 4.3.1 y 4.3.2 llegamos a que G es conexo si y solo si $\pi_0(G) = \mathbf{1}$.

Al núcleo de la sobreyección lo denotamos por G^0 , este es un subgrupo cerrado normal, representado por $A/A \cdot I_0 = A/A(1 - e) = Ae$, donde I_0 es el ideal de aumento en $\pi_0(A)$. Así Ae es conexa y por tanto G^0 . Llamamos a G^0 la *componente conexa de G* .

Con la siguiente proposición caracterizaremos las componentes conexas. Para hacer esto, definimos por $nil(A)$ el conjunto de todos los elementos nilpotentes de A . Este es un ideal y es la intersección de todos los ideales primos de A . Denotamos el álgebra $A/nil(A)$ por A_{red} .

Proposición 4.3.3. *Sea G un esquema de grupo algebraico sobre K y sea $A = K[G]$. Entonces las siguientes condiciones son equivalentes:*

1. G es conexo
2. A es conexa
3. A_{red} es conexa
4. A_{red} es un dominio entero.

Demostración. Ver [2, 20.15]. ■

Veamos algunos ejemplos:

Ejemplo.

1. GL_n y SL_n son conexos.
2. Sp_{2n} es conexa.
3. μ_n no es conexa.

4.4 Álgebras de Lie y suavidad

Sea M un A -módulo. Una *derivación* D de A en M es una aplicación K -lineal $D : A \rightarrow M$ tal que

$$D(ab) = a \cdot D(b) + b \cdot D(a)$$

Denotamos por $Der(A, M)$ al conjunto de todas las derivaciones de A en M .

Sea G un esquema de grupo algebraico sobre K y sea $A = K[G]$. Decimos que una derivación $D \in Der(A, A)$ es *invariante por izquierda* si $c \circ D = (Id \otimes D) \circ c$, donde c es la co-multiplicación. El espacio vectorial sobre K de derivaciones a izquierda lo denotamos por $Lie(G)$ y lo llamamos *álgebra de Lie* de G .

Denotemos por $K[\varepsilon]$ el álgebra de números duales, es decir, $K[\varepsilon] = K \cdot 1 \otimes K \cdot \varepsilon$ con multiplicación $\varepsilon^2 = 0$. Así podemos decir que existe un único homomorfismo de K -álgebras $\kappa : K[\varepsilon] \rightarrow K$ con $\kappa(\varepsilon) = 0$. Por tanto, el núcleo de $G(K[\varepsilon]) \xrightarrow{G(\kappa)} G(K)$ tiene estructura natural de espacio vectorial sobre K .

La siguiente proposición nos da una manera de calcular las álgebras de Lie de los esquemas de grupo.

Proposición 4.4.1. *Existe un isomorfismo natural entre los siguientes espacios vectoriales sobre K :*

1. $Lie(G)$
2. $Der(A, K)$ donde K es considerado un A -módulo vía la aplicación co-unidad $u : A \rightarrow K$
3. $ker(G(K[\varepsilon]) \xrightarrow{G(\kappa)} G(K))$

Demostración. $1 \Leftrightarrow 2$ Supongamos que $D \in Lie(G)$. Por definición tenemos que $u \circ D \in D(A, K)$, lo cual prueba la primera implicación. Ahora supongamos que $d \in D(A, K)$, lo que nos lleva a que $D = (id \otimes d) \circ c \in Lie(G)$.

$2 \Leftrightarrow 3$ Un elemento $f \in ker(G(\kappa))$, es un homomorfismo de K -álgebras $f : A \rightarrow K[\varepsilon]$, de tal forma que $f(a) = u(a) + d(a) \cdot \varepsilon$, por tanto $d \in D(A, K)$

Antes de los ejemplos debemos notar que si tenemos un homomorfismo de esquemas de grupo $f : G \rightarrow H$, este induce el diagrama conmutativo

$$\begin{array}{ccc}
 G(K[\varepsilon]) & \xrightarrow{f_{K[\varepsilon]}} & H(K[\varepsilon]) \\
 \downarrow G(\kappa) & & \downarrow H(\kappa) \\
 G(K) & \xrightarrow{f_K} & H(K)
 \end{array}$$

Así definimos la aplicación K -lineal $df : Lie(G) \rightarrow Lie(H)$, el cual es un homomorfismo de álgebras de Lie y lo llamamos el *diferencial* de f . Si f es una inmersión cerrada, entonces df es inyectiva e identifica a $Lie(G)$ con la subálgebra de Lie $Lie(H)$.

Según lo anterior las siguientes propiedades se cumplen:

Proposición 4.4.2.

1. Para alguna extensión L/K , $Lie(G_L) = Lie(G) \otimes_K L$.
2. Sean $f_i : G_i \rightarrow H$ un homomorfismo de esquemas de grupo, $i = 1, 2$, entonces

$$Lie(G_1 \times_H Lie(G_2)) = Lie(G_1 \times_{Lie(H)} Lie(G_2))$$

en particular:

(a) Para un homomorfismo $f : G \rightarrow H$ y un subgrupo $H' \subset H$

$$\text{Lie}(f^{-1}(H')) = df^{-1}(\text{Lie}H')$$

(b) $\text{Lie}(\ker(f)) = \ker(df)$

(c) $\text{Lie}(G_1 \times G_2) = \text{Lie}(G_1) \times \text{Lie}(G_2)$

3. $\text{Lie}(G) = \text{Lie}(G^0)$

Demostración. Ver [7, 12]. ■

Ejemplo.

1. Sea $G = \mathbf{V}$, donde V es un espacio vectorial sobre K . Notemos que los elementos de $\ker G(\kappa)$, son de la forma $v \cdot \varepsilon$ con $v \in V$ arbitrario. Por tanto, $\text{Lie}(G) = V$. En particular, $\text{Lie}(G_a) = K$.
2. Sea $G = GL_1(A) = G_m$, donde A es una álgebra finita dimensional asociativa sobre K . Notemos que los elementos del $\ker G(\kappa)$ son de la forma $1 + a \cdot \varepsilon$, con $a \in A$. Por tanto $\text{Lie}(GL_1(A)) = A$. En particular, $\text{Lie}(G_m) = K$.
3. Si $G = GL_n(R)$, entonces los elementos de $\ker G(\kappa)$ son las matrices inversibles de la forma $I + M \cdot \varepsilon$. Por tanto $\text{Lie}(GL_n)$ es el espacio de matrices $n \times n$.
4. Sea $G = SL_n(R)$. Como este es un subgrupo de $GL_n(R)$, tenemos $\text{Nrd}(I + M \cdot \varepsilon) = 1 + \text{Trd}(M) \cdot \varepsilon$. Para que esta norma sea 1, la traza reducida debe de ser igual a 0, es decir,

$$\text{Lie}(SL_n) = \{M \in GL_n(R) \mid \text{Trd}(M) = 0\} \subset R$$

5. Sea $G = O_n$, Veamos cómo son los elementos de $\ker G(\kappa)$. Sea M una matriz $n \times n$, tal que $MM^t = I$, entonces

$$\begin{aligned} (1 + M \cdot \varepsilon)(1 + M \cdot \varepsilon)^t &= (1 + M \cdot \varepsilon)(1 + M^t \cdot \varepsilon) \\ &= 1 + M^t \cdot \varepsilon + M \cdot \varepsilon \\ &= 1 + (M + M^t) \cdot \varepsilon \end{aligned}$$

Por tanto $Lie(O_n(R)) = \{M \in GL_n(R) \mid M + M^t = 0\}$

6. Si $G = Sp_{2n}$, Sea M una matriz $n \times n$ tal que existe $J \in GL_n(R)$ tal que $M^t J M = J$, Entonces

$$Lie(Sp_{2n}(R)) = \{M \in GL_{2n}(R) \mid JM + M^t J = 0\}$$

La siguiente proposición nos ayuda a definir la suavidad de los esquemas de grupo.

Proposición 4.4.3. *Sea G un esquema de grupo algebraico sobre K y sea $A = K[G]$.*

Las siguientes condiciones son equivalentes:

1. A_L es reducida para alguna extensión L/K .
2. $A_{K_{alg}}$ es reducida.
3. $\dim_K(Lie(G)) = \dim(G)$

Demostración. Ver [2, 21.9]

Un esquema de grupo algebraico G se sabe que es *suave* si G satisface las condiciones de la proposición 4.4.3. Los esquemas de grupo algebraicos suaves lo llamamos *grupos algebraicos*.

Las siguientes propiedades se cumplen

Proposición 4.4.4.

1. *Sea G un esquema de grupo algebraico sobre K y sea L/K un extensión de campo. Entonces G_L es suave si y solo si G es suave.*
2. *Si G_1 y G_2 son suaves, entonces $G_1 \times G_2$ es suave.*
3. *Un esquema de grupo algebraico G es suave si y solo si la componente conexa de G^0 es suave.*

Demostración. Estos son consecuencias inmediatas de la proposición 4.4.3. ■

Ejemplo.

1. Como la $\dim(Lie(GL_n)) = n^2 = \dim(GL_n)$, entonces GL_n es suave.
2. Lo mismo pasa SL_n , es decir, también es suave.

4.5 Homomorfismos de esquemas de grupo

Un homomorfismo de esquemas de grupo $f : G \rightarrow H$ es inyectivo si $\ker(f) = 1$ o equivalentemente, si $f_R : G(R) \rightarrow H(R)$ es inyectiva para algún $R \in \text{Alg}_K$.

Proposición 4.5.1. *Sea $f : G \rightarrow H$ un homomorfismo de esquemas de grupo algebraicos. Las siguientes condiciones son equivalentes:*

1. f es inyectiva.
2. f es una inmersión cerrada.
3. $f_{\text{alg}} : G(K_{\text{alg}}) \rightarrow H(K_{\text{alg}})$ es inyectiva y df es inyectiva. Denotamos por K_{alg} a la clausura algebraica de K .

Demostración. Ver [2, 22.2]. ■

Una proposición similar enunciamos para homomorfismos sobreyectivos.

Proposición 4.5.2. *Sea $f : G \rightarrow H$ un homomorfismo de esquemas de grupo algebraicos. Si H es suave, entonces las siguientes condiciones son equivalentes:*

1. f es sobreyectiva
2. $f_{\text{alg}} : G(K_{\text{alg}}) \rightarrow H(K_{\text{alg}})$ es sobreyectiva.

Demostración. Ver [2, 22.3]. ■

El siguiente resultado es debido a la sobreyectividad de los esquemas de grupos algebraicos:

Proposición 4.5.3. *Sea $f : G \rightarrow H$ un homomorfismo de esquemas de grupo algebraicos.*

1. Si G es conexo (resp. suave), entonces H es conexa (resp. suave).
2. Sea H' un subgrupo de H . Entonces la restricción de f a $f^{-1}(H')$ es un homomorfismo sobreyectivo $f^{-1}(H') \rightarrow H'$.

Demostración. Ver [2, 22.4]. ■

Por último enunciemos la proposición para los isomorfismos entre esquemas de grupos algebraicos:

Proposición 4.5.4. *Sea $f : G \rightarrow H$ un homomorfismo de esquemas de grupo algebraicos con H suave. Entonces las siguientes condiciones son equivalentes:*

1. f es un isomorfismo.
2. f es inyectivo y sobreyectivo.
3. $f_{alg} : G(K_{alg}) \rightarrow H(K_{alg})$ es un isomorfismo y df es inyectivo.

Una sucesión de esquemas de grupo

$$1 \rightarrow N \xrightarrow{f} G \xrightarrow{g} H \rightarrow 1$$

la llamamos *exacta*, si f induce un isomorfismo de N con el $\ker(g)$ y g es sobreyectiva, o equivalentemente si f es inyectiva y $H \simeq G/\text{im}(f)$. Para algún homomorfismo de esquemas de grupo $g : G \rightarrow H$ podemos formar la sucesión exacta

$$1 \rightarrow \ker(g) \rightarrow G \rightarrow \text{im}(g) \rightarrow 1$$

, Es decir, $\text{im}(g) \simeq G/\ker(g)$.

Proposición 4.5.5. *Una sucesión de esquemas de grupo*

$$1 \rightarrow N \xrightarrow{f} G \xrightarrow{g} H \rightarrow 1$$

con H suave es exacta si y solo si

1. $1 \rightarrow N(R) \xrightarrow{f_R} G(R) \xrightarrow{g_R} H(R)$ es exacta para cada $R \in \text{Alg}_K$ y
2. $g_{alg} : G(K_{alg}) \rightarrow H(K_{alg})$ es sobreyectiva.

Demostración. De la primera parte tenemos que $N = \ker(g)$ y de la proposición 4.5.2, que g es sobreyectiva, por tanto la sucesión es exacta. La otra dirección es inmediata. ■

Proposición 4.5.6. *Supongamos que*

$$1 \rightarrow N \xrightarrow{f} G \xrightarrow{g} H \rightarrow 1$$

es exacta, entonces

$$\dim G = \dim N + \dim H$$

Un homomorfismo sobreyectivo $f : G \rightarrow H$ lo llamamos separable si el diferencial $df : Lie(G) \rightarrow Lie(H)$ es sobreyectivo.

Proposición 4.5.7. *Un homomorfismo sobreyectivo $f : G \rightarrow H$ de grupos algebraicos es separable si y solo si $\ker(f)$ es suave.*

Demostración. Supongamos que $N = \ker(f)$, por las proposiciones 4.4.3 y 4.5.6

$$\begin{aligned} \dim Lie(N) &= \dim \ker(df) = \dim Lie(G) - \dim im(df) \\ &= \dim G - \dim im(df) = \dim N + \dim H - \dim im(df) \\ &= \dim N + \dim Lie(H) - \dim im(df) \end{aligned}$$

Así, N es suave si y solo si $\dim N = \dim Lie(N)$ si y solo si $\dim Lie(H) - \dim im(df) = 0$ si y solo si df es sobreyectiva. ■

4.6 Automorfismos de grupos de álgebras

Ahora hablaremos sobre los automorfismos de grupos sobre álgebras, para ello consideramos esquemas de grupos relacionados con álgebras.

Sea L el centro de A que es un álgebra asociativa unital separable sobre K . Denotemos el núcleo del homomorfismo $Aut_{alg}(A) \rightarrow Aut_{alg}(L)$ por $Aut_L(A)$. Podemos notar que $Lie(Aut_L(A)) = Der(A, A) = A/L$, esto considerando que las L -derivaciones de A son internas, las cuales denotaremos por $ad(a)(x) = [a, x] = ax - xa$.

Por la proposición 4.5.6 podemos notar que el esquema de grupo $Aut_L(A)$ es suave y es conexa por la proposición 4.5.3. Así tenemos la sucesión exacta de grupos algebraicos conexos

$$1 \rightarrow GL_1(L) \rightarrow GL_1(A) \rightarrow Aut_L(A) \rightarrow 1.$$

Si tenemos que A es un álgebra central simple sobre K , entonces $L = K$ y escribimos $PGL_1(A)$ por el grupo $Aut_{alg}(A)$, y cumple

$$PGL_1(A) \simeq GL_1/G_m \quad Lie(PGL_1(A)) = A/K$$

y

$$PGL_1(A)(R) = Aut_R(A_R); \quad R \in Alg_K.$$

Decimos que una K -álgebra R satisface la condición SN ³ si para alguna álgebra central simple A sobre K todos los automorfismos de R -álgebras son internos. Por tanto si, R satisface la condición SN entonces $PGL_1(A)(R) = A_R^\times/R^\times$.

El conjunto $PGL(V) = PGL_1(End(V)) = GL(V)/G_m$ y llamamos a $PGL(V)$ el *grupo lineal general proyectivo*, el cual escribimos $PGL(V) = PGL_n$ si $V = K^n$.

³ La condición SN se refiere al teorema de Skolem-Noether, donde todos los automorfismos son internos.

Capítulo 5

COHOMOLOGÍA DE GALOIS

En este Capítulo describiremos las cohomologías y algunas de sus propiedades. Primero lo haremos sobre Γ -grupos partiendo del conjunto fijo $H^0(\Gamma, G)$ y extendiéndola a conjuntos punteados y a sus respectivos homomorfismos. Luego describiremos cómo ayudan las sucesiones exactas en la búsqueda de cohomologías. Por último, describiremos las cohomologías de los grupos algebraicos y encontraremos las formas torcidas de algunos de ellos.

Un grupo A el cual también es un Γ -conjunto se llama un Γ -grupo si Γ actúa por homomorfismos de grupo, es decir, $\sigma(a_1.a_2) = \sigma a_1.\sigma a_2$ para $\sigma \in \Gamma$, $a_1, a_2 \in A$. Cuando el Γ -grupo es conmutativo se llama un Γ -módulo.

5.1 Conjuntos Cohomólogos

Dado un Γ -conjunto A , definimos

$$H^0(\Gamma, A) = \{a \in A \mid \sigma a = a \text{ para todo } \sigma \in \Gamma\}$$

Si A es un Γ -grupo, entonces $H^0(\Gamma, A)$ es un subgrupo de A .

Sea A un Γ -grupo definimos por 1-cociclo de Γ sobre A a la aplicación

$$\begin{aligned} \alpha : \Gamma &\rightarrow A \\ \sigma &\mapsto \alpha_\sigma \end{aligned}$$

con la propiedad que $\alpha_{\sigma\tau} = \alpha_\sigma \sigma \alpha_\tau$ para todo $\sigma, \tau \in \Gamma$.

Denotemos por $Z^1(\Gamma, A)$ al conjunto de todos los 1-cociclos de Γ en A . La aplicación constante $\mathbf{1} : \sigma \rightarrow 1$ la conocemos como un *elemento distinguido* de $Z^1(\Gamma, A)$ y lo llamamos el 1-cociclo trivial.

Ahora observemos que si tenemos un 1-cociclo $\alpha \in Z^1(\Gamma, A)$ y un elemento $a \in A$, entonces la aplicación

$$\begin{aligned}\beta : \Gamma &\rightarrow A \\ \sigma &\mapsto \beta_\sigma = a\alpha_\sigma\sigma a^{-1}\end{aligned}$$

también está en $Z^1(\Gamma, A)$ ya que

$$\begin{aligned}\beta_{\sigma\tau} &= a\alpha_{\sigma\tau}\sigma\tau a^{-1} \\ &= a\alpha_\sigma\sigma\alpha_\tau\sigma\tau a^{-1} \\ &= a\alpha_\sigma\sigma\alpha_\tau\tau a^{-1} \\ &= a\alpha_\sigma\sigma a^{-1}a\alpha_\tau\tau a^{-1} \\ &= a\alpha_\sigma\sigma a^{-1}\sigma a\alpha_\tau\tau a^{-1} \\ &= \beta_\sigma\sigma\beta_\tau\end{aligned}$$

Podemos decir entonces que si $a \in A$ y $\beta_\sigma = a\alpha_\sigma\sigma a^{-1}$ para todo $\sigma \in \Gamma$ que $\beta \sim \alpha$ y lo leemos como β es cohomólogo con α o β es equivalente a α . Notemos que \sim es una relación de equivalencia y denotamos la clase de equivalencia de α por $[\alpha]$ y el conjunto de clases de equivalencia de 1-cociclos por $H^1(\Gamma, A)$, que es un conjunto punteado, es decir, un conjunto con elementos distinguidos.

También notemos que $Z^1(\Gamma, A)$ y $H^1(\Gamma, A)$ son conjuntos punteados con elementos distinguidos. Si A es abeliano, entonces $Z^1(\Gamma, A)$ y $H^1(\Gamma, A)$ son grupos y se identifican por la definición de grupos cohomológicos.

En general, no es fácil encontrar el $a \in A$ tal que $\beta_\sigma = a\alpha_\sigma\sigma a^{-1}$. En particular, si $\alpha = \mathbf{1}$, entonces $\beta_\sigma = a\mathbf{1}_\sigma\sigma a^{-1} = a\sigma a^{-1}$ para algún $a \in A$. Más adelante veremos que hay teoremas que nos ayudan con esto como lo es el teorema de Lang.

Para calcular la primera cohomología de una manera más eficiente podemos usar la segunda cohomología de grupos abelianos, la cual definimos de la siguiente forma. Sea A un Γ -grupo abeliano con la aplicación $\alpha : \Gamma \times \Gamma \rightarrow A$ que satisface que

$$\sigma\alpha_{\tau,\rho} \cdot \alpha_{\sigma,\tau\rho} = \alpha_{\sigma\tau,\rho}\alpha_{\sigma,\tau} \text{ Para } \sigma, \tau, \rho \in \Gamma$$

la cual llamamos un 2-cociclo. De manera similar que los 1-cociclos, definimos el conjunto de 2-cociclos por $Z^2(\Gamma, A)$ y decimos que $\alpha, \beta \in Z^2(\Gamma, A)$ son cohomólogos si existe una aplicación $\phi : \Gamma \rightarrow A$ que satisface

$$\beta_{\sigma,\tau} = \sigma\phi_\tau \cdot \phi_{\sigma\tau}^{-1} \cdot \phi_\sigma \cdot \alpha_{\sigma,\tau}$$

para todo $\sigma, \tau \in \Gamma$. En este caso también podemos notar que esta es una clase de equivalencia, la cual denotamos por $H^2(\Gamma, A)$.

Hablemos un poco de de las aplicaciones y homomorfismos entre estas calses de conjuntos y de grupos. Si tenemos M y N dos conjuntos punteados la aplicación $\phi : M \rightarrow N$ es un morfismo de conjuntos punteados, si este envía los elementos distinguidos de M en los elementos distinguidos de N . Ahora si tenemos los Γ -grupos A y B , junto con el homomorfismo de grupos $f : A \rightarrow B$, este lo llamamos un Γ -homomorfismo de grupos si respeta la acción, es decir

$$f(\sigma a) = \sigma f(a) \text{ para todo } \alpha \in \Gamma \text{ y } a \in A$$

Si $f : A \rightarrow B$ es un Γ -homomorfismo, de inmediato este induce las aplicaciones

$$f^i : H^i(\Gamma, A) \rightarrow H^i(\Gamma, B) \text{ para } i = 0, 1$$

Notemos que f^0 es un homomorfismo de grupos y que f^1 es un morfismo de conjuntos punteados.

5.2 Sucesiones Exactas

Este tipo de sucesiones son importantes dentro de nuestro trabajo y son fundamentales en el estudio de las cohomologías.

Definamos el núcleo $\ker(\mu)$ como el conjunto de todos los elementos de M enviados a los elementos distinguidos de N por el morfismo de conjuntos punteados $\mu : M \rightarrow N$. Entonces podemos decir que la sucesión de morfismos de conjuntos punteados

$$M \xrightarrow{\rho} N \xrightarrow{\mu} P$$

es exacta si $\text{im}(\rho) = \ker(\mu)$. Así la sucesión $N \xrightarrow{\mu} P \rightarrow 1$ es exacta, si y solo si μ es sobreyectiva, También podemos decir que la sucesión $1 \rightarrow M \xrightarrow{\rho} N$ es exacta si y solo si $\ker(\rho)$ contiene solo los elementos distinguidos de M . Notemos que no es necesario que μ sea inyectiva.

Proposición 5.2.1. *Sea A un Γ -grupo y B un Γ -subgrupo de A . Si $i : B \rightarrow A$ es la aplicación inclusión. Entonces A/B es un Γ -conjunto con acción natural Γ sobre la coclase, esto lo vemos si B es normal. Si $\pi : A \rightarrow A/B$ es la proyección canónica*

i. Definimos

$$\delta^0 : H^0(\Gamma, A/B) \rightarrow H^1(\Gamma, B)$$

$$aB \mapsto [\alpha]$$

donde α es el cociclo definido por $\alpha_\sigma = a^{-1} \cdot \sigma a$. Entonces δ^0 es la aplicación de conjuntos punteados y la sucesión

$$1 \rightarrow H^0(\Gamma, B) \xrightarrow{i^0} H^0(\Gamma, A) \xrightarrow{\pi^0} H^0(\Gamma, A/B) \xrightarrow{\delta^0} H^1(\Gamma, B) \rightarrow H^1(\Gamma, A)$$

es exacta.

ii. Si B es normal, la sucesión obtenida en la parte i añadiéndole

$$\dots \xrightarrow{\pi^1} H^1(\Gamma, A/B)$$

es exacta.

iii. Supongamos que B es un subgrupo del centro de A . Dado $\gamma \in Z^1(\Gamma, A/B)$ escojemos un $\beta : \Gamma \rightarrow A$ con $\beta_\sigma \in \gamma_\sigma$ para cada $\sigma \in \Gamma$, con $\alpha_{\sigma,\tau} = \beta_\sigma \cdot \sigma\beta_\tau \cdot \beta_{\sigma\tau}^{-1}$, entonces

$$\delta^1 : H^1(\Gamma, A/B) \rightarrow H^2(\Gamma, B)$$

$$[\gamma] \mapsto [\alpha]$$

Así la sucesión en ii añadiéndole

$$\dots \xrightarrow{\delta^1} H^2(\Gamma, B)$$

es exacta.

Demostración. Ver [5, 2.4]

5.3 Formas Torcidas

En esta sección discutimos lo que son los torcimientos y las formas torcidas. Consideremos un Γ -conjunto B , y sea A un Γ -grupo con una acción sobre B que conmuta con la acción de Γ , es decir

$$\sigma(a \cdot b) = \sigma a \cdot \sigma b \text{ para todo } b \in B, a \in A, \sigma \in \Gamma$$

Si fijamos un 1-cociclo arbitrario $\alpha \in Z^1(\Gamma, A)$ y definimos la acción

$$\sigma * b = \alpha_\sigma(\sigma b) \text{ para } \sigma \in \Gamma \text{ y } b \in B$$

Esta nueva acción la denotamos por B_α y la llamamos la *forma torcida* de B . Decimos que B_α se obtiene por el *torcimiento* B por el 1-cociclo α .

El ejemplo más sencillo es cuando B es un Γ -grupo y $A = \text{Aut}(B)$ es el conjunto de automorfismos de B , entonces exista una acción de Γ sobre A dada por $\sigma a =$

$\sigma^{-1} \circ a \circ \sigma$ para $\sigma \in \Gamma$ y $a \in A$. Donde \circ es la composición de aplicaciones sobre B . Notemos que $H^0(\Gamma, \text{Aut}(B))$ es exactamente el conjunto de Γ -automorfismos de B .

Proposición 5.3.1. *Sea A un Γ -grupo y $\alpha \in Z^1(\Gamma, A)$. Entonces la aplicación*

$$\theta_\alpha : H^1(\Gamma, A_\alpha) \rightarrow H^1(\Gamma, A), \quad [\gamma] \mapsto [\alpha\gamma]$$

donde $\alpha\gamma$ lo denotamos por $\sigma \mapsto \alpha_\sigma \gamma_\sigma$, es una biyección bien definida, la cual envía la clase trivial de $H^1(\Gamma, A_\alpha)$ a la clase de α en $H^1(\Gamma, A)$.

Demostración. Sea γ un cociclo con valores en A_α . Tenemos que $\gamma_{\sigma\tau} = \gamma_\sigma \alpha_\sigma \sigma(\gamma_\tau) \alpha_\sigma^{-1}$, así

$$\begin{aligned} \gamma_{\sigma\tau} \cdot \alpha_{\sigma\tau} &= \gamma_\sigma \cdot \alpha_\sigma \cdot \sigma(\gamma_\tau) \cdot \alpha_\sigma^{-1} \cdot \alpha_\sigma \sigma(\alpha_\tau) \\ &= \gamma_\sigma \cdot \alpha_\sigma \cdot \sigma(\gamma_\tau) \cdot \sigma(\alpha_\tau) \\ &= \gamma_\sigma \cdot \alpha_\sigma \cdot \sigma(\gamma_\tau \alpha_\tau) \end{aligned}$$

Lo que significa que $\gamma\alpha \in Z^1(\Gamma, A)$. Si $\gamma' \in Z^1(\Gamma, A_\alpha)$ es cohomólogo con γ y $a \in A$ tal que $\gamma'_\sigma = a \cdot \gamma_\sigma \cdot (\sigma * a^{-1})$, entonces

$$\begin{aligned} \gamma'_\sigma \alpha_\sigma &= a \gamma_\sigma \cdot (\sigma * a^{-1}) \cdot \alpha_\sigma \\ &= a \gamma_\sigma \cdot \alpha_\sigma \cdot \sigma a^{-1} \alpha_\sigma^{-1} \alpha_\sigma \\ &= a \gamma_\sigma \cdot \alpha_\sigma \cdot \sigma a^{-1} \end{aligned}$$

Por tanto $\gamma'\alpha$ es cohomóloga a $\gamma\alpha$. Lo que demuestra que θ_α está bien definida. Resta demostrar que es una biyección. Para esto notemos que la aplicación $\sigma \mapsto \alpha_\sigma^{-1}$ es un 1-cociclo en $Z^1(\Gamma, A_\alpha)$. Por tanto la aplicación inducida $\theta_{\alpha^{-1}} : H^1(\Gamma, A) \rightarrow H^1(\Gamma, A_\alpha)$ es la inversa de θ_α . Por lo tanto, θ_α es una biyección. ■

5.4 Cohomología de Galois de Grupos Algebraicos

Sea G un grupo algebraico definido sobre K y sea k una extensión de Galois de K contenida en la clausura \overline{K} . Si consideramos que k es separable, entonces está contenido en K_{sep} . Entonces definimos

$\Gamma_{sep} = Gal(K_{sep}/K)$ y $\Gamma = Gal(k/K)$, Entonces Γ_{sep} actúa continuamente⁴ sobre G , y por tanto actúa continuamente sobre $Aut(G)$.

Si definimos a

$$G(K) = \{g \in G \mid \gamma g = g \text{ para todo } \gamma \in \Gamma_{sep}\}$$

el cual contiene los puntos fijos de G , Entonces las acciones de Γ sobre $G(K)$ y sobre $Aut_K(G)$ son inducidos por las acciones de Γ_{sep} sobre G y $Aut(G)$. Así la primera cohomología $H^1(\Gamma_{sep}, Aut(G))$ la llamamos *cohomología de Galois* de G . Denotaremos $H^1(\Gamma_{sep}, G)$ y $H^1(\Gamma_{sep}, Aut(G))$ por $H^1(K, G)$ y $H^1(K, Aut(G))$ respectivamente.

Dado $\alpha \in Z^1(\Gamma_{sep}, Aut(G))$, definimos la nueva acción $*$ de Γ_{sep} sobre G con respecto a α como lo hicimos en la sección 4.3 por

$$\gamma * g = \alpha_\gamma \gamma g \text{ para } \gamma \in \Gamma \text{ y } g \in G$$

y definimos a G_α como el grupo G junto con la acción $*$ en vez de la acción natural de Γ_{sep} sobre G . Al grupo G_α lo llamamos la *forma torcida* de G inducida por α .

Podemos resaltar que si k es una extensión de K , contenida en \overline{K} , entonces

$$\begin{aligned} G_\alpha(K) &= \{g \in G \mid \gamma * g = g \text{ para todo } \gamma \in Gal(K_{sep}/K)\} \\ &= \{g \in G \mid \alpha_\gamma \gamma g = g \text{ para todo } \gamma \in Gal(K_{sep}/K)\} \end{aligned}$$

⁴ esto significa que actúa continuamente dentro de la topología profinita y también dentro de la topología de Zariski (topología que consiste de los ceros de un conjunto de polinomios)

y que si $\alpha = \mathbf{1}$, entonces

$$\begin{aligned} G_1(K) &= \{g \in G \mid \mathbf{1}_\gamma \gamma g = g \text{ para todo } \gamma \in \text{Gal}(K_{sep}/K)\} \\ &= \{g \in G \mid \gamma g = g \text{ para todo } \gamma \in \text{Gal}(K_{sep}/K)\} = G(K) \end{aligned}$$

La siguiente proposición nos da propiedades de cuándo dos formas torcidas son conjugadas en $\text{Aut}(G)$, es decir, nos dice cómo las formas torcidas son clasificadas por $H^1(\Gamma_{sep}, \text{Aut}(G))$.

Proposición 5.4.1. *Sea G un grupo lineal algebraico definido sobre K . Sea L una extensión de Galois de K , la cual está contenida en \overline{K} y sea k una extensión de Galois K contenida en L . Sea $\Gamma = \text{Gal}(L/K)$. Si α y β están en $Z^1(\Gamma, \text{Aut}_L(G))$, entonces ellos son cohomólogos con respecto a $f \in \text{Aut}_L(G)$ (que es, $f(\alpha) = \beta$) si y solo si $f(G_\alpha(K)) = G_\beta(K)$*

Demostración. Supongamos que $f \in \text{Aut}_L(G)$ es tal que $\beta_\gamma = f\alpha_\gamma\gamma f^{-1}$ para todo $\gamma \in \Gamma$. Si $g \in G_\beta(K)$

$$\begin{aligned} f^{-1}(g) &= f^{-1}(\beta_\gamma \gamma g) \\ &= f^{-1}(f\alpha_\gamma\gamma f^{-1}\gamma g) \\ &= \alpha_\gamma\gamma f^{-1}g \end{aligned}$$

lo que significa que $f^{-1}g \in G_\alpha(K)$ para todo $\gamma \in \Gamma$. Por tanto $f(G_\alpha(K)) = G_\beta(K)$.

Ahora supongamos que $f(G_\alpha(K)) = G_\beta(K)$. Esto significa que para cada $g \in G_\beta(K)$ existe un $h \in G_\alpha(K)$ tal que $f(h) = g$ y

$$\beta_\gamma \gamma g = g = f(h) = f(\alpha_\gamma \gamma h) = f(\alpha_\gamma \gamma f^{-1} f(h)) = f(\alpha_\gamma \gamma f^{-1} \gamma g)$$

para todo $\gamma \in \Gamma$. Así para todo $g \in G_\beta(K)$, tenemos que $\beta_\gamma = f\alpha_\gamma\gamma f^{-1}$, lo que nos dice que α y β son cohomólogos. ■

Notemos que para los grupos algebraicos también se cumple la proposición 5.2.1, visto en la sección de sucesiones exactas.

La siguiente proposición nos relaciona la cohomología de Galois con los isomorfismos entre espacios vectoriales.

Para una extensión de Galois finita $G = Gal(L/K)$ denotamos por V_L al L -espacio vectorial $V \otimes_K L$ y por Φ_L a el tensor inducido por V_L sobre Φ . De esta forma asociamos a la pareja (V, Φ) con el L -objeto (V_L, Φ_L) . Sabemos que (V, ϕ) y (W, Ψ) son isomorfos sobre L , si existe un L -isomorfismo de (V, Φ) en (W, Ψ) . A este isomorfismo es el que nos representa la (L/K) -forma torcida de (V, ϕ) . Estas formas torcidas las clasificamos de la siguiente manera:

Dado un K -automorfismo $\sigma : L \rightarrow L$, el cual se extiende al K -automorfismo $V_L \rightarrow V_L$, el cual denotamos también por σ . Así cada aplicación lineal $f : V_L \rightarrow W_L$ que induce la aplicación $\sigma(f) : V_L \rightarrow W_L$, la cual definimos por $\sigma(f) = \sigma \circ f \circ \sigma^{-1}$. Entonces si f es un L -isomorfismo de (V_L, Φ_L) a (W_L, Ψ_L) , así también lo es $\sigma(f)$. La aplicación $f \rightarrow \sigma(f)$ preserva la composición de automorfismos y también la acción a izquierda de $G = Gal(L/K)$ sobre $Aut(\Phi)$.

El hecho es que podemos relacionar la clase $[\alpha_\sigma]$ en $H^1(G, Aut_K(\Phi))$ del cociclo α_σ con los L -isomorfismos $g : (V_L, \Phi_L) \rightarrow (W_L, \Psi_L)$ y que esto depende (W, Ψ) y no de g . Esto lo representamos en la siguiente proposición.

Proposición 5.4.2. *Para un K -objeto (V, Φ) consideramos el conjunto punteado $(\bar{V}, \bar{\Phi})$ de (L/K) -formas torcidas de (V, Φ) , entonces los puntos base o puntos distinguidos están dados por (V, Φ) , la aplicación $(W, \Psi) \rightarrow [\alpha_\sigma]$ definida arriba induce la biyección*

$$(\bar{V}, \bar{\Phi}) \rightarrow H^1(G, Aut_L(\Phi))$$

Demostración. Tomemos un 1-cociclo α_σ , recordemos que este nos representa la clase cohomológica de $H^1(G, Aut_L(\Phi))$ y si consideramos a $W = H^0(G, V_L)$, entonces tenemos que $\sigma(\Phi_L) = \Phi_L$ para todo $\sigma \in G$ y también que $\alpha_\sigma(\Phi_L) = \Phi_L$ para todo $\sigma \in G$. Estos nos deja decir que $\alpha_\sigma \sigma(\Phi_L) = \Phi_L$ para todo $\sigma \in G$. Esto nos dice que Φ_L es un tensor de W , el cual definimos por Ψ y así conseguimos el K -objeto

(W, Ψ) . Pero sabemos que $W \otimes_K L \simeq V_L$. Por la construcción del isomorfismo identificamos a Φ_L con Ψ_L . Así (W, Ψ) identifica la forma torcida de (V, Φ) ya que si $\alpha_\sigma = c^{-1}\beta_\sigma\sigma c$ con algún 1-cociclo $\sigma \mapsto \beta_\sigma$ y $c \in \text{Aut}_L(\Phi)$. Por tanto llegamos a que $H^0(G, V_L) = c(W)$. Lo que implica que W y $c(W)$ son isomorfos y nos da que

$$H^1(G, \text{Aut}_L(\Phi)) \rightarrow (\overline{V}, \overline{\Phi})$$

Ejemplo. Consideremos $V = K^n$ y Φ es el tensor trivial. Entonces $\text{Aut}_k(\Phi)$ es GL_n . Sabemos que dos K -espacios vectoriales n -dimensionales son isomorfos sobre L , también son isomorfos sobre K , por tanto

$$H(G, GL_n) = 1$$

Para $n = 1$, es la prueba que se hace en [2] y se conoce como el teorema de Hilbert 90, se cumple que $H^1(G, GL_1) = 1$ y en particular, como $GL_1 \simeq G_m$, entonces $H^1(G, G_m) = 1$.

Ejemplo. Considerando que $\text{Nrd} : GL_n \rightarrow G_m$ es una aplicación sobreyectiva, la sucesión

$$1 \rightarrow SL_n \rightarrow GL_n \xrightarrow{\text{Nrd}} G_m \rightarrow 1$$

es exacta e induce la sucesión exacta

$$\cdots \rightarrow H^0(G, GL_n) \rightarrow H^0(G, G_m) \rightarrow H^1(G, SL_n) \rightarrow H^1(G, GL_n)$$

que es lo mismo que tener a $\cdots \rightarrow GL_n \rightarrow G_m \rightarrow H^1(G, SL_n) \rightarrow 1$, lo que nos hace concluir que $H^1(G, SL_n) = 1$.

Ejemplo. Otro ejemplo importante, es si asumimos que la característica de K es diferente de 2, que V es un espacio vectorial n -dimensional, y que Φ es una forma bilineal simétrica no degenerada sobre V . Entonces los $\text{Aut}_K(\Phi)$ es el grupo O_n de matrices ortogonales con respecto a la forma bilineal y por tanto de 5.4.2 tenemos

que

$$(\overline{V}, \overline{\Phi}) \leftrightarrow H^1(G, O_n)$$

Notemos que esta diferencia de las otras, no es igual a 1. Pero es bien importante para la clasificación de formas cuadráticas.

Ejemplo. Tomemos ahora el grupo simpléctico Sp_{2n} . Como dos formas bilineales alternantes no degeneradas sobre K^{2n} son isomorfas, entonces tenemos que $H^1(F, Sp_{2n}) = 1$.

Ahora construiremos algunos ejemplos para grupos lineales algebraicos de orden pequeño.

Empecemos con $GL_1(K)$. Para ello vamos a definir el grupo de la siguiente forma

$$GL_1(K) = \{(x, y) \in K^2 \mid xy = 1\}$$

es decir, es el grupo lineal con norma igual a 1. Si queremos calcular la forma torcida de este grupo, debemos considerar sus automorfismos y ellos son $\mathbf{1} : (x, y) \mapsto (x, y)$ y el otro es $\tau : (x, y) \mapsto (y, x)$. Notemos que este último cumple que $\tau^2 = \mathbf{1}$

Si consideramos el primero, es decir, si tomamos el 1-cociclo $\alpha = \mathbf{1}$, como sabemos, $(GL_1)_\alpha(K) = GL_1(K)$. Si tomamos $\alpha = [\tau]$, entonces

$$\begin{aligned} (GL_1)_\alpha(K) &= \{(x, y) \in K^2 \mid xy = 1, \alpha_\sigma(x, y) = (x, y)\} \\ &= \{(x, y) \in K^2 \mid xy = 1, \tau\sigma(x, y) = (x, y)\} \\ &= \{(x, y) \in K^2 \mid xy = 1, \tau(\sigma(x), \sigma(y)) = (x, y)\} \\ &= \{(x, y) \in K^2 \mid xy = 1, (\sigma(y), \sigma(x)) = (x, y)\} \\ &= \{(x, y) \in K^2 \mid xy = 1, \sigma(x) = y\} \\ &= \{(x, y) \in K^2 \mid x\sigma(x) = 1\} \end{aligned}$$

Es decir que este se asemeja al grupo lineal unitario, es decir, $(GL_1)_\alpha(K) = U_1(K)$.

Ahora consideremos a $SL_2(K) = \{x \in GL_2(K) \mid Nrd(x) = 1\}$. De nuevo, si consideramos el 1-cociclo α , tenemos varias opciones ya que para este no es fácil encontrar los automorfismos. En [5, 51] se calculan las cohomologías de Galois y las relacionan con norma reducida. Calculemos entonces, a partir de su resultado la forma torcida de $SL_2(K)$.

Sea $\pi = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$ y $M = h\pi^{-1}$ donde $\pi = \begin{pmatrix} & 1 \\ c & \end{pmatrix}$ esto sale de la prueba de la proposición [5], además, $\alpha_\sigma = [c_h]^5$. Entonces la aplicación $f_M : K^2 \times K^2 \rightarrow K$ la cual definimos por $f_M : (v, w) \mapsto vM\bar{w}^t$ es una forma hermitiana, así

$$\begin{aligned}
g \in (SL_2)_\alpha(K) &\Leftrightarrow \alpha_\sigma \sigma g = g \\
&\Leftrightarrow h\bar{g}h^{-1} = g \\
&\Leftrightarrow h\pi^{-1}\pi\bar{g}\pi^{-1}\pi h^{-1} = g \\
&\Leftrightarrow M\bar{g}^{-t}M^{-1} = g \\
&\Leftrightarrow gM\bar{g}^t = M \\
&\Leftrightarrow f_M(vg, wg) = vgM\bar{g}^t\bar{w}^t = vM\bar{w}^t = f_M(v, w) \\
&\Leftrightarrow g \in SU_2(K, f_M)
\end{aligned}$$

Así tenemos que $(SL_2)_\alpha(K) = SU_2(K, f_M)$. Todas estas operaciones las comprobamos.

5.5 Clasificación de Álgebras

En esta sección queremos dar a conocer cómo funcionan las cohomologías y las formas torcidas sobre los grupos algebraicos definidos sobre álgebras centrales simples.

Sea A un álgebra finito dimensional sobre K . La multiplicación en A nos lleva a una aplicación lineal $w : A \otimes_K A \rightarrow A$. Sea $W = Hom_K(A \otimes_K A, A)$ y $G = GL(A)$

⁵ Esta es una acción por conjugación

el grupo lineal de A , donde A es visto como un K -espacio vectorial. Consideremos la representación

$$\rho : G \rightarrow GL(w)$$

dada por la fórmula

$$\rho(g)(\phi)(x \otimes y) = g \circ \phi(g^{-1}(x) \otimes g^{-1}(y))$$

para $g \in G$, $\phi \in W$ y $x, y \in A$. Una aplicación lineal $g \in G$ es un automorfismo de álgebras de A si y solo si $\rho(g)(w) = w$. Así el esquema de grupos $Aut_G(w)$ coincide con el esquema de grupo $Aut_{alg}(A)$ para todos los automorfismos de álgebras de A .

Una ρ -forma torcida de w es una estructura de álgebra A' sobre el K -espacio vectorial A tal que la F_{sep} -álgebras A'_{sep} y A_{sep} son isomorfas. Así por 5.4.2 existe la biyección

$$\boxed{\begin{array}{l} \text{Clases de } K\text{-isomorfismos de } K\text{-} \\ \text{álgebras } A' \text{ tal que las } K_{sep}\text{-} \\ \text{álgebras } A'_{sep} \text{ y } A \text{ son isomorfas} \end{array}} \longleftrightarrow H^1(F, Aut_{alg}(A))$$

La biyección está dada explícitamente como sigue: Si $\beta : A_{sep} \rightarrow A'_{sep}$ es un K_{sep} -isomorfismo, entonces el 1-cociclo correspondiente es

$$\alpha_\gamma = \beta^{-1} \circ (Id \otimes \gamma) \circ \beta \circ (Id \otimes \gamma^{-1})$$

Por el otro lado, dado el 1-cociclo $\alpha \in Z^1(K, Aut_{alg}(A))$, tenemos que

$$A' = \{x \in A_{sep} \mid \alpha_\gamma \circ (Id \otimes \gamma)(x) = (x) \text{ para todo } \gamma \in F\}$$

Ahora aplicaremos este principio general a las álgebras centrales simples.

Trabajemos con las álgebras centrales simples. Sea $A = M_n(A)$, un álgebra de matrices de grado n . Consideremos que cada K -álgebra central simple se descompone en K_{sep} , así cada K -álgebra A' tal que $A'_{sep} \simeq M_n(K_{sep})$ es central simple. Las formas torcidas de A son exactamente las K -álgebras centrales simples de grado n . Por el

teorema de Skloem-Noether vemos que cada automorfismo de A es interno y por tanto que $\mathbf{Aut}_{alg}(A) = \mathbf{PGL}_n$. Por lo tanto obtenemos la siguiente biyección

$$\boxed{\begin{array}{l} \text{Clases de } K\text{-isomorfismos de} \\ K\text{-álgebras centrales simples de} \\ \text{grado } n \end{array}} \longleftrightarrow H^1(F, \mathbf{PGL}_n)$$

Consideremos la sucesión exacta

$$1 \rightarrow G_m \rightarrow GL_n \rightarrow PGL_n \rightarrow 1$$

Los torcimientos son todos los grupos para un cociclo en $H^1(F, PGL_n)$, correspondientes a las K -álgebras centrales simples B de grado n .

Capítulo 6

CONCLUSIONES Y TRABAJOS FUTUROS

6.1 Conclusiones

1. Conocimos la teoría de álgebras centrales simples y la aplicamos en las cohomologías de Galois y en las formas torcidas.
2. Identificamos los grupos algebraicos como un esquema de grupo algebraico suave, para ello, estudiamos las álgebras de Hopf, álgebras de Lie y teoría relacionada. Se calculó el grupo Lie de algunos grupos lineales algebraicos.
3. Logramos identificar las cohomologías de Galois de algunos grupos lineales algebraicos y dar a conocer unos ejemplos particulares de las formas torcidas.
4. Identificamos que no es fácil encontrar las formas torcidas, de los esquemas de grupo.

6.2 Trabajos Futuros

1. Estudiar más a fondo la teoría de variedades y cómo se definen los grupos algebraicos a partir de este.
2. Profundizar y entender los sistemas de raíces y su relación con los toros maximales, para determinar las formas torcidas vía álgebras de Lie.
3. Especializarnos más en el área de geometría algebraica, para ver cómo funcionan las formas torcidas de los grupos cohomológicos sobre las curvas elípticas.

REFERENCIAS BIBLIOGRÁFICAS

- [1] Dummit-Foote, Abstract Algebra, Wiley International Edition. 2004.
- [2] Knus-Merkurjev-Rost-Tignol, The Book of Involutions, American Mathematical Society, 1998.
- [3] Serre, JP, Local Fields, Springer-Verlag, 1968.
- [4] Serre, JP, Galois Cohomology, Springer-Verlag, 2002
- [5] Haller, S, Computing Galois Cohomology And Forms of Linear Algebraic Groups, Technische Universiteit Eindhoven, 2005
- [6] Springer, T.A, Linear Algebraic Groups, Birkhauser, 1998
- [7] Waterhouse, Introduction to Affine Group Schemes, Springer-Verlag, New York, 1979

ACERCA DE LAS FORMAS TORCIDAS SOBRE LOS GRUPOS LINEALES ALGEBRAICOS

Gabriel Darío Uribe Guerra

(787) 464-2723

Departamento de Departamento de Ciencias Matemáticas

Consejero: Uroyoán R. Walker Ramos

Grado: Maestría en Ciencias

Fecha de Graduacion: Mayo 2008

La Homología y los conjuntos cohomológicos son una teoría que viene desarrollandose con fuerza desde principios de los años 50 del siglo XX. Nosotros estudiamos un poco de la teoría de álgebras centrales simples y esquemas de grupos definidos sobre álgebras centrales simples, las álgebras de Lie, para introducirnos en el campo de los conjuntos cohomológicos $H^i(\Gamma, G)$ para $i = 0, 1$ y estudiar sus propiedades. Luego aplicamos esto en las cohomologías de Galois $H^1(\Gamma = Gal(K_{sep}/K), Aut_K(G))$, donde K es un campo y G es un grupo algebraico. Esto se resuelve buscando las formas torcidas (los isomorfismos entre álgebras) que se relacionan con la primera cohomología de Galois.