UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE CIENCIAS

TESIS

"TEORÍA K DE MILNOR Y APLICACIONES"

PARA OBTENER EL GRADO ACADÉMICO DE MAESTRO EN CIENCIAS CON MENCION EN MATEMÁTICA APLICADA

ELABORADO POR:

GERARDO ZUBIAGA RIVERA

ASESOR:

Dr. JOE ALBINO PALACIOS BALDEÓN

LIMA – PERÚ

2017

A Mi Esposa Yadira Tejada

Agradezco a los Profesores Joe Palacios y Hugo Castillo por la orientación y sus sabios consejos para la culminación del presente trabajo. También deseo agradecer a mi Esposa, a mi Madre y a mi familia, por su apoyo incondicional, y a todas aquellas personas que de una u otra forma me ayudaron a terminar este trabajo.

RESUMEN

En este trabajo de tesis presentamos la prueba del Teorema 90 de Hilbert, en su versión para el grupo K_2 de Milnor. Para ello definimos la teoría K de Milnor, y presentamos sus propiedades principales y algunos resultados interesantes. Previamente, recordamos las principales definiciones acerca de las extensiones de Galois y los grupos de cohomología, definiendo la cohomología de Galois. Finalmente, enunciamos el Teorema de Merkurjev-Suslin, principal aplicación del Teorema 90 de Hilbert.

ÍNDICE

INTRODUCCIÓN

El presente trabajo de tesis tiene como principal objetivo introducir al lector a la teoría K de Milnor, así como a sus principales propiedades y aplicaciones. Entre ellas, mencionamos a la ley de reciprocidad de Weil, el teorema de Milnor y el teorema 90 de Hilbert, que a su vez implica el teorema de Merkurjev-Suslin.

La teoría K de Milnor tuvo su origen en el artículo [8], publicado en 1970. En él, Milnor estudió, entre otras cosas, la relación entre los anillos graduados $K_*^M(k)$, la teoría K de Milnor módulo 2, y la cohomología de Galois $H_*(k)$ con coeficientes en $\mathbb{Z}/2$, donde el cuerpo base k es un cuerpo de característica $\neq 2$. La conjetura de Milnor afirma que dichos anillos son isomorfos, y en dicho artículo se dan algunos ejemplos particulares de este hecho.

Para un cuerpo F arbitrario, existe una aplicación natural del n-ésimo grupo $K_n^M(F)$ de la teoría K de Milnor y el n-ésimo grupo $K_n(F)$ de la teoría K clásica de Quillen. Dicha aplicación es un isomorfismo para $n \leq 2$, pero los grupos son diferentes en general para $n > 2$. El caso $n = 2$ es conocido como el teorema de Matsumoto.

La ley de reciprocidad de Weil es una generalización del siguiente hecho: dados dos polinomios de grados m y n, el producto de los valores del primero en las raíces del segundo es igual al producto de los valores del segundo en las raíces del primero, multiplicado por $(-1)^{mn}$. Más precisamente, sea X una curva algebraica irreducible sobre un cuerpo algebraicamente cerrado K, y sean f, g funciones racionales no nulas. Para cada $a \in X$ se define el *símbolo de Weil* de f y g en a

como el elemento de K dado por

$$[f,g]_a := (-1)^{\mathrm{ord}_a(f)\mathrm{ord}_a(g)} \frac{f^{\mathrm{ord}_a(g)}(a)}{g^{\mathrm{ord}_a(f)}(a)},$$

el cual está bien definido. La ley de reciprocidad de Weil afirma que el producto de los símbolos de Weil $[f,g]_a$ sobre todos los puntos de la curva X es igual a 1. En su versión teoría K de Milnor, este hecho es consecuencia del teorema de Milnor, que incluimos en el capítulo 2.

En 2003, Voevodsky publicó una prueba de la conjetura de Milnor. El resultado era entonces conocido para grado 1, grado 2 (Merkurjev) y grado 3 (Merkurjev-Suslin). La conjetura de Bloch-Kato es una versión más general que se extiende a partir del probado por Voevodsky, que afirma que la teoría K módulo m es isomorfa a la cohomología de Galois con coeficientes en μ_m, para todo primo m y todo cuerpo con característica distinta de m.

En 1982, Merkurjev y Suslin probaron la conjetura de Bloch-Kato para $n = 2$. Esta prueba se basa principalmente en el Teorema 90 de Hilbert, el cual presentamos en la presente tesis, además de un esbozo de la prueba de Merkurjev-Suslin.

En el capítulo 1 revisamos las principales herramientas a usar, como la cohomología de Galois. El capítulo 2 está dedicado a la teoría K de Milnor y sus principales propiedades, además de algunos resultados interesantes, como el Teorema de Milnor y la ley de reciprocidad de Weil. En el capítulo 3 presentamos la prueba del Teorema 90 de Hilbert (en su versión para la teoría K de Milnor), para finalizar en el capítulo 4 con su principal aplicación, el Teorema de Merkurjev-Suslin.

1 PREVIOS

En este capítulo recordamos las herramientas principales que usaremos: las extensiones de Galois y los grupos de cohomología. Recordamos también la noción de norma sobre un cuerpo, y finalmente definimos la cohomología de Galois. Los resultados mencionados en este capítulo se pueden encontrar, por ejemplo, en [2] o [7].

1.1 Grupos de Cohomología

Sea G un grupo.

Definición 1.1.1. Un grupo abeliano A es un G-*módulo* si existe una acción de G sobre A

$$\begin{array}{rcl} G \times A & \to & A \\ (g, a) & \to & ga \end{array}$$

Observación 1.1.2. Un G-módulo A es lo mismo que un $\mathbb{Z}[G]$-módulo. En efecto, si $\sum n_\sigma \sigma \in \mathbb{Z}[G]$ y $a \in A$, entonces $(\sum n_\sigma \sigma)a := \sum n_\sigma \sigma(a)$. Recíprocamente, una estructura de $\mathbb{Z}[G]$-módulo implica una acción de G sobre A.

Definición 1.1.3. Decimos que un G-módulo A es *trivial* si G actúa trivialmente sobre A ($\sigma a = a$, $\forall \sigma \in G, \forall a \in A$). Un G-homomorfismo es un homomorfismo de grupos abelianos $A \xrightarrow{\varphi} B$ compatible con la acción de G (es decir, $\varphi(\sigma a) = \sigma\varphi(a)$).

Denotamos por $\hom_G(A, B)$ al conjunto de G-homomorfismos $A \to B$. Es un grupo abeliano con la suma usual de homomorfismos. Denotamos por A^G al subgrupo de elementos G-invariantes en el G-módulo A:

$$A^G = \{a \in A / \sigma a = a, \forall \sigma \in G\}.$$

Ejemplo 1.1.4. Si V es un espacio vectorial sobre K de dimensión n y $G = GL_n(F)$, entonces V es un G-módulo, con $V^G = \{0\}$.

Ejemplo 1.1.5. Si $K|F$ es Galois con grupo de Galois G, entonces el grupo aditivo K es un G-módulo con $K^G = F$. Similarmente, el grupo multiplicativo $K^\times$ es un G-módulo con $(K^\times)^G = F^\times$.

Buscamos definir, para todo G-módulo A, para todo $i \in \mathbb{Z}_0^+$, grupos abelianos $H^i(G, A)$ tales que:

1. $H^0(G, A) = A^G$.
2. Existe $H^i(G, A) \to H^i(G, B)$ canónico $\forall A \to B$ G-homomorfismo, $\forall i \geq 0$.
3. Dada la sucesión exacta corta (s.e.c.) $0 \to A \to B \to C \to 0$ de G-módulos, existe una sucesión exacta larga

$$\cdots \to H^i(G, A) \longrightarrow H^i(G, B) \longrightarrow H^i(G, C) \to H^{i+1}(G, A) \longrightarrow H^{i+1}(G, B) \longrightarrow H^{i+1}(G, C) \to \cdots$$

de grupos abelianos, empezando en $i = 0$.

Sean entonces G un grupo, A un G-módulo. Tomemos una resolución proyectiva

$$P_\bullet = \cdots \to P_2 \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0$$

del G-módulo trivial $\mathbb{Z}$. Consideremos la sucesión $\hom_G(P_\bullet, A)$ definida por

$$\hom_G(P_0, A) \xrightarrow{d_0} \hom_G(P_1, A) \xrightarrow{d_1} \hom_G(P_2, A) \to \cdots$$

donde $\hom_G(P_i, A) \xrightarrow{d_i} \hom_G(P_{i+1}, A)$ está dado por $\lambda \mapsto \lambda \circ p_{i+1}$. Como $p_{i+1} \circ p_i = 0$, entonces $d_{i+1} \circ d_i = 0$. Definimos

$$H^i(G, A) := H^i(\hom_G(P_i, A)) = \ker(d^i)/\mathrm{Im}(d^{i-1}), \forall i \geq 0.$$

Proposición 1.1.6. *Los grupos $H^i(G, A)$ satisfacen 1, 2 y 3, y sus clases de isomorfismo no dependen de la elección de la resolución $P_\bullet$.*

Observación 1.1.7. De la definición, los grupos de cohomología satisfacen
i) Si

$$\begin{tikzcd} A \arrow[r] \arrow[d] & B \arrow[d] \\ A' \arrow[r] & B' \end{tikzcd}$$

es un diagrama conmutativo de G-módulos, entonces los diagramas asociados

$$\begin{tikzcd} H^i(G, A) \arrow[r] \arrow[d] & H^i(G, B) \arrow[d] \\ H^i(G, A') \arrow[r] & H^i(G, B') \end{tikzcd}$$

conmutan para todo $i \geq 0$.
ii) Dado el diagrama conmutativo de s.e.c.'s

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0 \end{tikzcd}$$

los diagramas

$$\begin{tikzcd} H^i(G, C) \arrow[r] \arrow[d] & H^{i+1}(G, A) \arrow[d] \\ H^i(G, C') \arrow[r] & H^{i+1}(G, A') \end{tikzcd}$$

que vienen de la propiedad funtorial anterior y las sucesiones exactas largas conmutan para todo $i \geq 0$.

Para calcular los grupos $H^i(G, A)$ explícitamente, consideremos el $\mathbb{Z}[G]$-módulo $\mathbb{Z}[G^{i+1}]$, para cada $i \geq 0$, donde la acción de G está dada por $\sigma(\sigma_0, \ldots, \sigma_i) = (\sigma\sigma_0, \ldots, \sigma\sigma_i)$. Éstos son $\mathbb{Z}[G]$-módulos proyectivos (de hecho, libres), pues son isomorfos a $\mathbb{Z}[G]^{i+1}$. Para $i > 0$, definimos G-homomorfismos $\delta^i : \mathbb{Z}[G^{i+1}] \to \mathbb{Z}[G^i]$

por $\delta^i = \sum_j (-1)^j s_j^i$, donde $s_j^i : \mathbb{Z}[G^{i+1}] \to \mathbb{Z}[G^i]$ está dada por $(\sigma_0, \ldots, \sigma_i) \mapsto (\sigma_0, \ldots, \dot{\sigma_j}, \ldots, \sigma_i)$. Así, obtenemos una resolución proyectiva

$$\cdots \to \mathbb{Z}[G^3] \xrightarrow{\delta^2} \mathbb{Z}[G^2] \xrightarrow{\delta^1} \mathbb{Z}[G] \xrightarrow{\delta^0} \mathbb{Z} \to 0,$$

donde δ^0 lleva cada σ_i al 1. Ésta es llamada *la resolución estándar de* $\mathbb{Z}$.
Si definimos, para $\sigma \in G$ fijo, $h^i : \mathbb{Z}[G^{i+1}] \to \mathbb{Z}[G^{i+2}]$ por $(\sigma_0, \ldots, \sigma_i) \mapsto (\sigma, \sigma_0, \ldots, \sigma_i)$, vemos que

$$\delta^{i+1} \circ h^i + h^{i-1} \circ \delta^i = \mathrm{id}_{\mathbb{Z}[G^{i+1}]}.$$

Esto prueba que $\ker(\delta^i) = \mathrm{Im}(\delta^{i+1})$. Para un G-módulo A, los elementos de $\hom_G(\mathbb{Z}[G^{i+1}], A)$ son llamados *i-cocadenas*, los elementos de $Z^{i+1}(\hom_G(\mathbb{Z}[G^\bullet], A))$ son llamados *i-cociclos*, y los elementos de $B^{i+1}(\hom_G(\mathbb{Z}[G^\bullet], A))$ son llamados *i-cobordes*. Denotamos estos grupos por $C^i(G, A)$, $Z^i(G, A)$ y $B^i(G, A)$, respectivamente. Los grupos de cohomología $H^i(G, A)$ son los grupos $H^{i+1}(\hom_G(\mathbb{Z}[G^\bullet], A))$.
Una construcción muy útil es la siguiente: en $\mathbb{Z}[G^{i+1}]$ consideremos los elementos básicos

$$[\sigma_1, \ldots, \sigma_i] := (1, \sigma_1, \sigma_1\sigma_2, \ldots, \sigma_1 \cdots \sigma_i).$$

De la definición de la G-acción en $\mathbb{Z}[G^{i+1}]$, $\mathbb{Z}[G^{i+1}]$ es el $\mathbb{Z}[G]$-módulo libre generado por los elementos $[\sigma_1, \ldots, \sigma_i]$. Vemos que

$$\delta^i([\sigma_1, \ldots, \sigma_i]) = \sigma_1[\sigma_2, \ldots, \sigma_i] + \sum_{j=1}^{i} (-1)^j [\sigma_1, \ldots, \sigma_j\sigma_{j+1}, \ldots, \sigma_i] + (-1)^{j+1}[\sigma_1, \ldots, \sigma_{i-1}]. \tag{1.1}$$

Por lo tanto, podemos identificar i-cocadenas con funciones $[\sigma_1, \ldots, \sigma_i] \mapsto a_{\sigma_1, \ldots, \sigma_i}$ y calcular las aplicaciones $\delta_i : C^{i-1}(G, A) \to C^i(G, A)$ por la fórmula

$$a_{\sigma_1, \ldots, \sigma_i} \mapsto \sigma_1 a_{\sigma_1, \ldots, \sigma_i} + \sum_{j=1}^{i} (-1)^j a_{\sigma_1, \ldots, \sigma_j\sigma_{j+1}, \ldots, \sigma_i} + (-1)^{i+1} a_{\sigma_1, \ldots, \sigma_{i-1}}.$$

Las funciones $a_{\sigma_1,\ldots,\sigma_i}$ son llamadas *cocadenas inhomogéneas.*

Ejemplo 1.1.8. Un 1-cociclo está dado por una función $\sigma \mapsto a_\sigma$ que satisface $a_{\sigma_1\sigma_2} = \sigma a_{\sigma_2} + a_{\sigma_1}$. Es un 1-coborde si, y solo si es de la forma $\sigma \mapsto \sigma a - a$, para algún $a \in A$. En el caso especial en que G actúe trivialmente en A ($\sigma(a) = a$, para todo $a \in A$), entonces $Z^1(G, A) = \hom(G, A)$ y $B^1(G, A) = 0$, luego $H^1(G, A) = \hom(G, A)$.

Ejemplo 1.1.9. Un 2-cociclo está dado por una función $(\sigma_1, \sigma_2) \mapsto a_{\sigma_1\sigma_2}$ que satisface

$$\sigma_1 a_{\sigma_2,\sigma_3} - a_{\sigma_1\sigma_2,\sigma_3} + a_{\sigma_1,\sigma_2\sigma_3} - a_{\sigma_1,\sigma_2} = 0.$$

Es un 2-coborde, es decir, un elemento de $\mathrm{Im}(\partial^{1*})$ si es de la forma $\sigma_1 b_{\sigma_2} - b_{\sigma_1\sigma_2} + b_{\sigma_1}$, para alguna 1-cocadena $\sigma \mapsto b_\sigma$.

Ejemplo 1.1.10. Sea G un grupo cíclico finito de orden p generado por un elemento σ. Consideremos las aplicaciones $\mathbb{Z}[G] \to \mathbb{Z}[G]$ dadas por

$$N(a) = \sum_{i=0}^{p-1} \sigma^i a$$

y

$$(\sigma - 1)(a) = \sigma a - a.$$

Se cumple entonces que $\ker(N) = \mathrm{Im}(\sigma - 1)$ y $\mathrm{Im}(N) = \ker(\sigma - 1)$. Así, obtenemos la resolución libre

$$\cdots \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \to \mathbb{Z} \to 0,$$

donde la última aplicación es inducida por $\sigma \mapsto 1$.

Si A es un G-módulo, definimos aplicaciones $N : A \to A$ y $\sigma - 1 : A \to A$ por las mismas fórmulas, y escribimos ${}_NA := \ker(N)$. De la última resolución, obtenemos, para $i > 0$,

$$H^0(G, A) = A^G,\ H^{2i+1}(G, A) =_N A/(\sigma - 1)A,\ H^{2i+2}(G, A) = A^G/NA.$$

Sean H un subgrupo de G, A un H-módulo. Entonces $\mathbb{Z}[G]$ también es un H-módulo, y podemos asociar a A el G-módulo $M_H^G(A) := \hom_H(\mathbb{Z}[G], A)$, donde la acción de G sobre un H-homomorfismo $\phi : \mathbb{Z}[G] \to A$ está dado por $(\sigma\phi)(g) = \phi(g\sigma)$, para cualquier generador $g \in G$. Claramente, $\sigma\phi$ es un H-homomorfismo.

Lema 1.1.11. *Asumamos además un G-módulo M. Se tiene un isomorfismo canónico* $\hom_G(M, \hom_H(\mathbb{Z}[G], A)) \simeq \hom_H(M, A)$, *dado por* $(m \mapsto \phi_m) \mapsto (m \mapsto \phi_m(1))$.

Demostración. Si $\lambda : M \to A$ es un H-homomorfismo, definimos $\lambda_m \in \hom_H(\mathbb{Z}[G], A)$ por $g \mapsto \lambda(gm)$. Esta aplicación es la inversa de la aplicación dada. □

Corolario 1.1.12. *(Lema de Shapiro) Dados un subgrupo H de G y un H-módulo A, se tienen isomorfismos canónicos $H^i(G, M_H^G(A)) \simeq H^i(H, A)$, para todo $i \geq 0$.*

Demostración. Basta aplicar el lema a los términos de una $\mathbb{Z}[G]$-resolución proyectiva $P_\bullet$ de $\mathbb{Z}$. □

Cuando $H = \{1\}$, un H-módulo es simplemente un grupo abeliano. Denotamos $M_H^G(A)$ por $M^G(A)$ en este caso, y lo llamamos el *módulo coinducido* asociado a A.

Corolario 1.1.13. *El grupo $H^i(G, M^G(A))$ es trivial para todo $i > 0$.*

Demostración. En este caso, el lado derecho en el Lema de Shapiro es trivial (podemos tomar, por ejemplo, la resolución $0 \to \mathbb{Z} \to \mathbb{Z} \to 0$ de $\mathbb{Z}$).

Observación 1.1.14. El paso a módulos coinducidos es funtorial: dado un homomorfismo de grupos abelianos $A \to B$, existe un G-homomorfismo asociado $M^G(A) \to M^G(B)$. Lo mismo ocurre para los módulos $M_H^G(A)$.

Dado un G-módulo A, existe una aplicación natural inyectiva $A \to M^G(A)$ que asocia a $a \in A$ el homomorfismo $\mathbb{Z}[G] \to A$ inducido por $\sigma \mapsto \sigma a$.

Cup-product

En esta sección definimos en primer lugar las aplicaciones restricción, para luego definir el *cup-product*, un producto asociativo

$$H^i(G,A) \times H^j(G,B) \to H^{i+j}(G, A \otimes B);\ \cup(a,b) = a \cup b$$

.

Sean G un grupo, A un G-módulo y H un subgrupo de G. Existen aplicaciones naturales de G-módulos

$$A \tilde{\to} \hom_G(\mathbb{Z}[G], A) \to \hom_H(\mathbb{Z}[G], A) = M_H^G(A),$$

el primero que lleva el elemento a al homomorfismo que lleva la identidad en a, y el segundo que considera un G-homomorfismo como H-homomorfismo. Tomando la cohomología, y aplicando el Lema de Shapiro, obtenemos las aplicaciones *restricción*

$$\text{Res} : H^i(G,A) \to H^i(H,A)$$

para todo $i > 0$.

Sean ahora los complejos de grupos abelianos $A^\bullet$ y $B^\bullet$. Definamos el *producto tensorial* $A^\bullet \otimes B^\bullet$. Para ello consideremos el complejo doble

$$
\begin{tikzcd}
 & \vdots & \vdots & \vdots & \\
\cdots \arrow[r] & A^{i-1}\otimes B^{j+1} \arrow[r] \arrow[u] & A^{i}\otimes B^{j+1} \arrow[r] \arrow[u] & A^{i+1}\otimes B^{j+1} \arrow[r] \arrow[u] & \cdots \\
\cdots \arrow[r] & A^{i-1}\otimes B^{j} \arrow[r] \arrow[u] & A^{i}\otimes B^{j} \arrow[r] \arrow[u] & A^{i+1}\otimes B^{j} \arrow[r] \arrow[u] & \cdots \\
\cdots \arrow[r] & A^{i-1}\otimes B^{j-1} \arrow[r] \arrow[u] & A^{i}\otimes B^{j-1} \arrow[r] \arrow[u] & A^{i+1}\otimes B^{j-1} \arrow[r] \arrow[u] & \cdots \\
 & \vdots \arrow[u] & \vdots \arrow[u] & \vdots \arrow[u] &
\end{tikzcd}
$$

donde las aplicaciones horizontales están dadas por $\partial^h_{ij} = \partial^i_A \otimes \mathrm{id}$ y las verticales por $\partial^v_{ij} = \mathrm{id} \otimes (-1)^i \partial^j_B$. Los cuadrados en el diagrama son anticonmutativos:

$$\partial^h_{i,j+1} \circ \partial^v_{ij} = -\partial^v_{i+1,j} \circ \partial^h_{ij}.$$

Tomemos el *complejo total* $T^\bullet$ definido por $T^n = \bigoplus_{i+j=n} A^i \otimes B^j$ y $\partial^n : T^n \to T^{n+1}$ definido por $\partial^h_{ij} + \partial^v_{ij}$ en la componente $A^i \otimes B^j$. Por la anticonmutatividad de arriba, $\partial^{n+1} \circ \partial^n = 0$, y $T^\bullet$ es efectivamente un complejo. Así, definimos $A^\bullet \otimes B^\bullet := T^\bullet$. Consideremos además los grupos abelianos A y B, y los complejos $\hom(A^\bullet, A)$ y $\hom(B^\bullet, B)$, cuyos términos de grado i son $\hom(A^{-i}, A)$ y $\hom(B^{-i}, B)$. Si $\alpha : A^{-i} \to A$ y $\beta : B^{-j} \to B$ son homomorfismos con $i + j = n$, entonces $\alpha \otimes \beta$ es un homomorfismo y define un elemento de grado $i + j$ en $\hom(A^\bullet \otimes B^\bullet, A \otimes B)$ via la inclusión diagonal

$$\hom(A^{-i} \otimes B^{-j}, A \otimes B) \to \hom(\bigoplus_{k+l=i+j} A^{-k} \otimes B^{-l}, A \otimes B).$$

Por construcción, si $\alpha \in Z^i(\hom(A^\bullet, A))$ y $\beta \in Z^j(B^\bullet, B)$, entonces $\alpha \otimes \beta \in Z^{i+j}(\hom(A^\bullet \otimes B^\bullet, A \otimes B))$. Si además $\alpha \in B^i(\hom(A^\bullet, A))$, entonces $\alpha \otimes \beta \in B^{i+j}(\hom(A^\bullet \otimes B^\bullet, A \otimes B))$. Lo mismo ocurre para β. Esto define una aplicación

$$H^i(\hom(A^\bullet, A)) \times H^j(\hom(B^\bullet, B)) \to H^{i+j}(\hom(A^\bullet \otimes B^\bullet, A \otimes B)).$$

Si además todos los grupos abelianos poseen estructura de G-módulos para un grupo G, y α y β son G-homomorfismos, obtenemos

$$H^i(\hom_G(A^\bullet, A)) \times H^j(\hom_G(B^\bullet, B)) \to H^{i+j}(\hom_G(A^\bullet \otimes B^\bullet, A \otimes B)),$$

donde las G-acciones en $A \otimes B$ y $A^\bullet \otimes B^\bullet$ vienen dadas por $\sigma(a \otimes b) = \sigma(a) \otimes \sigma(b)$.

Proposición 1.1.15. *Sean G un grupo y $P_\bullet$ un complejo de G-módulos (donde $P_i := P^{-i}$) que además sea una resolución proyectiva del G-módulo trivial $\mathbb{Z}$. Entonces $P_\bullet \otimes P_\bullet$ es una resolución proyectiva del $\mathbb{Z}[G \times G]$-módulo trivial $\mathbb{Z}$.*

Demostración. [3], Proposición 3.4.3.

En la construcción de arriba, podemos considerar $A^\bullet = B^\bullet = P_\bullet$ y obtenemos aplicaciones

$$H^i(\hom(P_\bullet, A)) \times H^j(\hom(P_\bullet, B)) \to H^{i+j}(\hom(P_\bullet \otimes P_\bullet, A \otimes B)).$$

Por la proposición 1.1.15, $P_\bullet \otimes P_\bullet$ es resolución proyectiva de $\mathbb{Z}$ como $G \times G$-módulo, y por definición de grupos de cohomología, se tiene

$$H^i(G, A) \times H^j(G, B) \to H^{i+j}(G, A \otimes B).$$

A su vez, la inclusión diagonal $G \to G \times G$ induce una aplicación restricción

$$\text{Res} : H^{i+j}(G \times G, A \otimes B) \to H^{i+j}(G, A \otimes B).$$

Componiendo ambas, obtenemos una operación

$$H^i(G, A) \times H^j(G, B) \to H^{i+j}(G, A \otimes B),$$

llamada *cup-product*. Denotamos a la imagen de (a, b) por $a \cup b$.

1.2 Cohomología de Galois

Extensiones de Galois

Definición 1.2.1. La extensión $E|K$ es *normal* si cumple cualquiera de las siguientes condiciones equivalentes:
i) para todo $\alpha \in E$, el polinomio irreducible de α en $K[x]$, denotado por $\text{irr}(\alpha, K, x) \in K[x]$ se descompone completamente en E;
ii) E es cuerpo de descomposición de algún $T \subseteq K[x]$ (es decir, es el menor cuerpo en el que se descomponen todos los polinomios en T);
iii) dado Ω algebraicamente cerrado con $E \subseteq \Omega$, cualquier K-inmersión $\sigma : E \to \Omega$ es un automorfismo de E respecto a K ($\sigma \in \text{Aut}_K(E)$).
La extensión $E|K$ es *separable* si todo elemento de E es la raíz de un polinomio separable sobre K (es decir, $\text{irr}(\alpha, K, x)$ no tiene raíces múltiples, para todo $\alpha \in E$).
La extensión $E|K$ es de *Galois* si es normal y separable.

Sobre la extensión de Galois $E|K$ se define el *grupo de Galois* $\mathrm{Gal}(E|K)$ como el grupo de automorfismos de E sobre K. Como $E|K$ es normal, toda K-inmersión entre E y Ω es un automorfismo, luego $\mathrm{Gal}(E|K) := \mathrm{Aut}_K(E) = \{K-\text{inmersiones } \sigma : E \to \overline{K}\}$. Además, se cumple que $|\mathrm{Gal}(E|K)| = |\mathrm{Aut}_K(E)| = [E : K]$.

Ejemplo 1.2.2. La extensión $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ es Galois con grupo de Galois $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})|\mathbb{Q}) = \{1, \sigma\} \cong \mathbb{Z}_2$, donde $a + b\sqrt{2} \overset{\sigma}{\mapsto} a - b\sqrt{2}$.

Ejemplo 1.2.3. La extensión $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ no es Galois, pues su grupo de automorfismos es de orden 1.

Sea K un cuerpo de característica p, para algún p primo.

Definición 1.2.4. Una extensión algebraica $L|K$ es *puramente inseparable* si, para cualquier $\alpha \in L$, el polinomio minimal de α sobre K tiene solo una raíz distinta. La extensión es *separable* si, para cualquier elemento $\alpha \in L$, el polinomio minimal de α sobre K tiene todas sus raíces distintas (es decir, es *separable*).

Proposición 1.2.5. *Sean L_1, L_2 extensiones puramente inseparables (separables) de K. Entonces L_1L_2 es una extensión puramente inseparable (separable) de K.*

Proposición 1.2.6. *Sea $L|K$ una extensión algebraica. Entonces existe un único cuerpo L_{sep} con $L \supseteq L_{sep} \supseteq K$ tal que $L|L_{sep}$ es puramente inseparable y $L_{sep}|K$ es separable. El cuerpo L_{sep} es el conjunto de elementos de L separables sobre K.*

El grado de $L|L_{\mathrm{sep}}$ es llamado *grado inseparable* de $L|K$, y el grado de $L_{\mathrm{sep}}|K$ es llamado *grado separable* de $L|K$. Estos se denotan por $[L : K]_i$ y $[L : K]_s$ respectivamente. Además se cumple que

$$[L : K] = [L : K]_i[L : K]_s.$$

Sea E una extensión finita de k, $\mathrm{char}(k) = p$. Sean $r = [E : k]_s$ y $p^\mu = [E : k]_i$. Sean $\sigma_1, \ldots, \sigma_r$ los distintos monomorfismos de E en $\overline{k}$. Si $\alpha \in E$, definimos su *norma* como

$$N_{E|k}(\alpha) = \prod_{i=1}^{r} \sigma_i \alpha^{p^\mu} = (\prod_{i=1}^{r} \sigma_i \alpha)^{[E:k]_i}.$$

Si la extensión es puramente inseparable, entonces $r = 1$ y

$$N_{E|k}(\alpha) = \alpha^{[E:k]}.$$

Si $E|K$ es Galois, entonces

$$N_{E|K}(\alpha) = \prod_{g \in \mathrm{Gal}(E|K)} g(\alpha).$$

Ejemplo 1.2.7. Como $\mathrm{Gal}(\mathbb{C}|\mathbb{R})$ consiste de la identidad y de la conjugación, se tiene

$$N_{\mathbb{C}|\mathbb{R}}(x + iy) = (x + iy)(x - iy) = x^2 + y^2.$$

Ejemplo 1.2.8. La norma no tiene porqué ser positiva. Si consideramos la extensión $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$, vemos por ejemplo que

$$N_{\mathbb{Q}(\sqrt{2})|\mathbb{Q}}(1 + \sqrt{2}) = (1 + \sqrt{2})(1 - \sqrt{2}) = -1.$$

Proposición 1.2.9. *Se tienen las siguientes propiedades:*

1. $N_{E|K} : E^\times \to K^\times$ *es un homomorfismo de grupos, es decir*

   $$N_{E|K}(\alpha\beta) = N_{E|K}(\alpha) N_{E|K}(\beta),$$

   para todo $\alpha, \beta \in E^\times$.

2. $N_{E|K}(a\alpha) = a^{[E:K]} N_{E|K}(\alpha)$, *para todo* $a \in K^\times$, $\alpha \in E^\times$.

3. $N_{E|K}(a) = a^{[E:K]}$, *para todo* $a \in K^\times$.

4. *Si* $L|E$ *es finita,* $N_{L|K} = N_{E|K} \circ N_{L|E}$.

Cohomología de Galois

Una aplicación importante de los grupos de cohomología ocurre cuando el grupo G es el grupo de Galois de una extensión $K|F$. El grupo de Galois $\mathrm{Gal}(K|F)$ es el límite inverso $\varprojlim \mathrm{Gal}(L|F)$ de los grupos de Galois de las extensiones finitas L de F contenidas en K, y es un grupo topológico compacto con respecto a su *topología de Krull*, es decir, la única topología tal que para todo $\sigma \in G$, la familia de subconjuntos

$$\{\sigma \mathrm{Gal}(K|L)/\sigma \in G, L|F \text{ extensión finita de Galois}\}$$

es una base de vecindades abiertas para σ. Para definir los grupos de cohomología en este contexto definimos los grupos *profinitos* como límites inversos arbitrarios de grupos finitos. Si G es profinito, entonces $G = \varprojlim G/N$, donde el límite inverso se toma sobre los subgrupos normales N de G.

Definición 1.2.10. Si G es un grupo profinito, un *G-módulo discreto* es un G-módulo A con la topología discreta tal que la acción de G sobre A es continua

Como en A se define la topología discreta todo elemento $a \in A$ es abierto, y la continuidad de la acción de G sobre A es equivalente a que el estabilizador G_a de a en G sea un subgrupo abierto de G, y por lo tanto de índice finito (por ser G compacto). A su vez, esto es equivalente a que $A = \bigcup A^H$, donde la unión se toma sobre los subgrupos abiertos H de G.
Para definir los grupos de cohomología $H^n(G, A)$ de un grupo profinito G que actúa sobre un G-módulo discreto A, basta requerir que las cocadenas $C^n(G, A)$ sean aplicaciones continuas. Las definiciones de las aplicaciones coborde (1.1) y de los grupos de cociclos, cobordes y los correspondientes grupos de cohomología permanecen igual.

Definición 1.2.11. Si G es un grupo profinito y A es un G-módulo discreto, los grupos de cohomología calculados usando complejos continuos son llamados *grupos* *de cohomología discretos o continuos.* Cuando $G = \mathrm{Gal}(K|F)$ es el grupo de Galois de una extensión $K|F$ Galois, los *grupos de cohomología de Galois* son los grupos de cohomología calculados usando complejos continuos.

Podemos escribir $G = \varprojlim(G/N)$ y $A = \bigcup A^N$, donde N recorre los subgrupos normales abiertos de G (que son de índice finito por ser G compacto). Luego A^N es un G/N-módulo y se cumple que

$$H^n(G, A) = \varinjlim_N H^n(G/N, A^N),$$

donde los grupos de cohomología son continuos y el límite directo se toma sobre la colección de todos los subgrupos normales abiertos N de G.

1.3 Álgebras Simples Centrales

Sea k un cuerpo. Recordemos que un k-álgebra A es un anillo que contiene a k en su centro, y cuya identidad coincide con la de k.

Definición 1.3.1. Decimos que el k-álgebra A es *simple* si A no contiene ideales bilaterales propios no triviales. Un *k-álgebra simple central* es un k-álgebra simple cuyo centro coincide con k.

Entre los ejemplos más sencillos de k-álgebra simple central encontramos a $M_n(k)$, el álgebra de matrices $n \times n$ con coeficientes en k, y a los cuaterniones, para $k = \mathbb{R}$

Teorema 1.3.2. *Sean k un cuerpo y A un k-álgebra de dimensión finita. Entonces A es un algebra simple central si, y solo si existe una extensión finita $K|k$ tal que $A \otimes_k K$ es isomorfo al anillo de matrices $M_n(K)$, para algún $n > 0$.*

En este caso decimos que K es *cuerpo de descomposición de A* o simplemente que K *descompone* a A. Este resultado se puede encontrar en [6], página

81. De él podemos concluir que la dimensión de A sobre k es un cuadrado perfecto. El entero $\sqrt{\dim_k(A)}$ se conoce como *grado* de A.
Si $K|k$ es una extensión Galois finita, denotamos por $\mathrm{ASC}_K(n)$ al conjunto de clases de k-isomorfismo de k-álgebras simples centrales de grado n descompuestas por K.

Definición 1.3.3. Dadas las k-álgebras centrales simples A y A', decimos que son *similares* o *Brauer equivalentes* si existen $m, m' > 0$ tales que $A \otimes_k M_m(k) \cong A' \otimes_k M_{m'}(k)$. La relación recién descrita define una relación de equivalencia en la unión de los conjuntos $\mathrm{ASC}_K(n)$. Denotamos al conjunto de clases de equivalencia por $\mathrm{Br}(K|k)$, y a la unión de los conjuntos $\mathrm{Br}(K|k)$ para todas las extensiones Galois finitas por $\mathrm{Br}(k)$.

Consideremos una extensión cíclica $K|k$, es decir, una extensión Galois con grupo Galois cíclico $G = \mathrm{Gal}(K|k)$. Sea $n = |G| = [K : k]$. Un elemento $\chi \in \hom(G, \mathbb{Z}/n)$ es llamado un *caracter*. Presentar un caracter sobreyectivo es equivalente a presentar un isomorfismo $\chi : G \xrightarrow{\cong} \mathbb{Z}/n$, o elegir un generador $\sigma \in G$ tal que $\chi(\sigma) = \overline{1}$.
Sean entonces χ un caracter sobreyectivo y $a \in k^\times$. Denotemos por σ a la preimagen de $\overline{1}$ via χ. Definimos el k-álgebra (χ, a) como el K-espacio vectorial generado por $\{1, e, e^2, \ldots, e^{n-1}\}$, con la multiplicación dada por $e\lambda = \sigma(\lambda)e$ para $\lambda \in K$, y $e^n = a$. Vemos además que $\dim_k(\chi, a) = n^2$, pues $\dim_K(\chi, a) = n = [K : k]$.

Ejemplo 1.3.4. Consideremos la extensión cíclica $\mathbb{C}|\mathbb{R}$. En este caso, $n = 2$ y $G = \{\mathrm{id}, \sigma\}$, donde σ es la conjugación compleja. Sea $\chi : G \to \mathbb{Z}/2$ el caracter definido por $\chi(\sigma) = \overline{1}$. Entonces, si $a \in \mathbb{R}^\times$,

$$(\chi, a) = \{z + we/z, w \in \mathbb{C}\},$$

donde $e^2 = a$ y $ez = \overline{z}e$. Si $a > 0$, consideremos

$$\phi : (\chi, a) \to M_2(\mathbb{R})$$

dado por

$$\phi(\alpha + i\beta + \gamma e + i\delta e) = \begin{bmatrix} \alpha + \gamma\sqrt{a} & \beta - \delta\sqrt{a} \\ -\beta - \delta\sqrt{a} & \alpha - \gamma\sqrt{a} \end{bmatrix}.$$

ϕ es inyectiva, y como (χ, a) y $M_2(\mathbb{R})$ tienen dimensión 4 sobre $\mathbb{R}$, debe ser un isomorfismo.

1.4 Variedades Algebraicas

Recordemos que, así como las variedades topológicas o diferenciables se construyen pegando bolas abiertas de un espacio euclidiano, un *esquema* resulta de pegar conjuntos abiertos llamados *esquemas afines.* Un esquema afín es un espacio localmente anillado isomorfo al espectro de un anillo. Un *morfismo* de esquemas es un morfismo de espacios localmente anillados. Un *isomorfismo* es un morfismo que posee inversa. Así, los esquemas junto con los morfismos de esquemas forman una categoría. Un *punto genérico* es aquel cuya clausura es igual al cerrado irreducible que lo contiene.

Un esquema X es *integral* si el anillo asociado a cada abierto $U \subset X$ es un dominio de integridad.

Un morfismo de esquemas $f : X \to Y$ es *de tipo finito* si existe un cubrimiento de Y por abiertos afines $Y_i = \mathrm{Spec}(B_i)$ tal que para cada i, $f^{-1}(V_i)$ puede ser cubierto por una cantidad finita de afines abiertos $U_{ij} = \mathrm{Spec}(A_{ij})$, donde A_{ij} es un B_i-álgebra finitamente generado.

Dados los esquemas X y S, decimos que X es un *esquema sobre* S si existe un morfismo $X \to S$. Si X, Y son esquemas sobre S, definimos el producto fibrado $X \times_S Y$ sobre S, junto con *proyecciones* $p_1 : X \times_S Y \to X$ y $p_2 : X \times_S Y \to Y$ que hacen conmutar un diagrama con los morfismos $X \to S$ y $Y \to S$, de la siguiente manera: dados el esquema Z sobre S y morfismos $f : Z \to X$ y $g : Z \to Y$ que hacen conmutar un diagrama con $X \to S$ y $Y \to S$, entonces existe un único morfismo $\theta : Z \to X \times_S Y$ tal que $f = p_1 \circ \theta$ y $g = p_2 \circ \theta$.

$$\begin{tikzcd}
Z \arrow[dr, dashed] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\
& X \times_S Y \arrow[r] \arrow[d] & X \arrow[d] \\
& Y \arrow[r] & S
\end{tikzcd}$$

Una *inmersión cerrada* es un morfismo de esquemas $f : Y \to X$ tal que f induce un homeomorfismo de Y sobre un subconjunto cerrado de X (Y y X vistos como espacios topológicos), y la aplicación inducida de haces $f^\sharp$ es sobreyectiva. Si X es un esquema sobre Y, definimos el morfismo *diagonal* como el único morfismo $\Delta : X \to X \times_Y X$ cuya composición con ambas proyecciones $p_1, p_2 : X \times_Y X \to X$ es la identidad. Si dicho morfismo es una inmersión cerrada, decimos que X es *separado* sobre Y.

Definimos una *variedad algebraica*, o simplemente *variedad*, como un esquema separado integral de tipo finito sobre un cuerpo algebraicamente cerrado k.

2 TEORÍA K DE MILNOR

El presente capítulo está dedicado por completo a la teoría K de Milnor. Vemos además el símbolo *tame* y la aplicación norma, que generaliza aquella vista en el capítulo anterior. También mencionamos resultados interesantes, como la Ley de Reciprocidad de Weil y el Teorema de Milnor.

2.1 Los K-grupos de Milnor

Sea k un cuerpo.

Definición 2.1.1. Definimos los *K-grupos de Milnor* $K_n^M(k)$ asociados a k como los cocientes de $(k^\times)^{\otimes n}$ por el subgrupo generado por los elementos de la forma $a_1 \otimes \cdots \otimes a_n$ con $a_i + a_j = 1$, para $1 \leq i < j \leq n$ (relación de Steinberg).

Así, $K_0^M(k) = \mathbb{Z}$ y $K_1^M(k) = k^\times$. La imagen de $a_1 \otimes \cdots \otimes a_n$ en el cociente se denota por $\{a_1, \ldots, a_n\}$, y se le conoce como *símbolo*.
En $K_n^M \times K_m^M$, definimos la multiplicación $(\alpha, \beta) \mapsto \{\alpha, \beta\}$. Esta operación está bien definida, pues si $a_1 \otimes \cdots \otimes a_n$ es cero en K_n^M o $b_1 \otimes \cdots \otimes b_m$ es cero en K_m^M, entonces es claro que $a_1 \otimes \cdots \otimes b_m$ debe ser cero en K_{n+m}^M. Esta multiplicación permite definir, como veremos a continuación, el anillo graduado anticonmutativo

$$K_*^M(k) = \bigoplus_{n \geq 0} K_n^M(k).$$

Veamos algunas propiedades de los símbolos que nos resultarán útiles.

Proposición 2.1.2. *Se cumplen las siguientes propiedades:*

1. *En $K_2^M(k)$ se cumple $\{x, -x\} = 0$ y $\{x, x\} = \{x, -1\}$.*

2. $\{\alpha, \beta\} = (-1)^{nm}\{\beta, \alpha\}$*, para todo* $\alpha \in K_n^M$ *y todo* $\beta \in K_m^M$*.*

3. Si $a_1 + \cdots + a_n$*, la suma de elementos no nulos de* K*, es 0 ó 1, entonces* $\{a_1, \ldots, a_n\} = 0$*.*

4. $\{a_1, \ldots, 1, \ldots, a_n\} = 0$

Demostración.

1. Se cumple que $\{x, -x\} + \{x, -(1-x)x^{-1}\} = \{x, 1-x\} = 0$, luego

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

lo cual prueba la primera propiedad. En cuanto a la segunda,

$$\{x, x\} - \{x, -1\} = \{x, x\} + \{x, -1\} = \{x, -x\} = 0.$$

2. Basta ver el caso $n = m = 1$.

$$0 = \{xy, -xy\} = \{x, -x\} + \{x, y\} + \{y, x\} + \{y, -y\} = \{x, y\} + \{y, x\}.$$

Aplicando inducción se obtiene el resultado.

3. Aplicando inducción sobre n, sabemos que el resultado es cierto para $n = 1, 2$. Supongamos que $n \geq 3$. Si $a_1 + a_2 = 0$, entonces sabemos que $\{a_1, a_2, \ldots, a_n\} = 0$. Si $a_1 + a_2 \neq 0$, entonces tendremos que

$$\frac{a_1}{a_1 + a_2} + \frac{a_2}{a_1 + a_2} = 1,$$

y por lo tanto,

$$\left\{\frac{a_1}{a_1 + a_2}, \frac{a_2}{a_1 + a_2}\right\} = 0.$$

Multiplicando por $\{a_3, \ldots, a_n\}$, obtenemos

$$\begin{aligned} 0 &= \left\{\frac{a_1}{a_1+a_2}, \frac{a_2}{a_1+a_2}, a_3, \ldots, a_n\right\} \\ &= \{a_1, a_2, a_3, \ldots, a_n\} - \{a_1+a_2, a_2, a_3, \ldots, a_n\} - \\ &\quad (\{a_1+a_2, a_2, a_3, \ldots, a_n\} - \{a_1+a_2, a_1+a_2, a_3, \ldots, a_n\}), \end{aligned}$$

donde los tres últimos sumandos son 0, por la propiedad anterior y la hipótesis inductiva $\{a_1+a_2, a_3, \ldots, a_n\} = 0$.

4. $\{a_1, \ldots, 1, \ldots, a_n\} = \{a_1, \ldots, 1^2, \ldots, a_n\} = 2\{a_1, \ldots, 1, \ldots, a_n\}$, de donde $\{a_1, \ldots, 1, \ldots, a_n\} = 0$. $\square$

Ejemplo 2.1.3. Para todo cuerpo finito F_q, el grupo $K_2^M(F_q)$ es trivial. En efecto, si $x \in F_q^\times$ es un generador, basta ver que $x \otimes x$ es cero en $K_2^M(F_q)$. Si q es par, es decir, si la característica del cuerpo es 2, entonces $x = -x$ y $\{x, x\} = \{x, -x\} = 0$. Supongamos que q es impar. Es claro que $0 = \{u, 1-u\} = \{x^n, x^m\} = nm\{x, x\}$, pero si n o m fuera par, la igualdad es trivial. En efecto, basta notar que $2\{x, x\} = \{x, x\} + \{x, -1\} = \{x, -x\} = 0$. Basta encontrar entonces un elemento u no cuadrado tal que $1-u$ también sea no cuadrado. Considerando la función $u \mapsto 1-u$ en $F_q - \{0, 1\}$, vemos que es una biyección (es una involución), y como este conjunto tiene $(q-1)/2$ cuadrados $(x^2, x^4, \ldots, x^{q-1})$, tendrá $(q-3)/2$ no cuadrados, por lo que tal u debe existir.

2.2 El Símbolo *Tame*

Sea K un cuerpo con valuación discreta $v : K^\times \to \mathbb{Z}$. Denotemos por A al respectivo anillo de valuación discreta, por M a su ideal maximal y por κ a su cuerpo residual. Fijemos un parámetro local π, de tal manera que todo elemento de $K^\times$ se escribe de manera única como $x = \pi^i u$, para alguna unidad u de A y para algún entero i. Veamos que los símbolos de la forma $\{\pi, u_2, \ldots, u_n\}, \{u_1, \ldots, u_n\}$, con $u_i \in A^\times$, generan $K_n^M(K)$. Basta hacerlo para $n = 2$:

$$\begin{aligned}\{x, y\} &= \{\pi^i u, \pi^j w\} \\ &= ij\{\pi, \pi\} + i\{\pi, w\} + j\{u, \pi\} + \{u, w\} \\ &= ij\{\pi, -1\} + i\{\pi, w\} - j\{\pi, u\} + \{u, w\}.\end{aligned}$$

Proposición 2.2.1. *Para cada $n \geq 1$, existe un único homomorfismo*

$$\begin{aligned}\partial^M : K_n^M(K) &\to K_{n-1}^M(\kappa) \\ \{\pi, u_2, \ldots, u_n\} &\mapsto \{\overline{u}_2, \ldots, \overline{u}_n\}\end{aligned}$$

para todo parámetro local π y toda unidad $u_j \in A^\times$. Además, fijando un parámetro local $\pi \in A$, existe un único homomorfismo

$$\begin{aligned}s_\pi^M : K_n^M(K) &\to K_n^M(\kappa) \\ \{\pi^{i_1} u_1, \ldots, \pi^{i_n} u_n\} &\mapsto \{\overline{u}_1, \ldots, \overline{u}_n\}\end{aligned}$$

para todo entero i_j y toda unidad u_j de A.

Demostración. Vemos que $\{u_1, u_2 \ldots, u_n\} + \{\pi, u_2, \ldots, u_n\} = \{\pi u_1, u_2, \ldots, u_n\}$, donde πu_1 es un parámetro local, por lo que $\{u_1, \ldots, u_n\}$ debe ser anulado por ∂^M. Esto asegura la unicidad de ∂^M. La unicidad de s_π^M sigue de la unicidad de la escritura de un elemento de K en la forma $\pi^i u$, para algún entero i y alguna unidad u.

En cuanto a la existencia, consideremos el $K_*^M(\kappa)$-álgebra $K_*^M(\kappa)[\xi]$ donde se cumple

$$\xi^2 = \{-1\}\xi$$

Esta álgebra tiene graduación natural

$$K_*^M(\kappa)[\xi] = \bigoplus_{n\geq 0} L_n,$$

donde ξ tiene grado 1 y

$$L_n = K_n^M(\kappa) \oplus K_{n-1}^M(\kappa)\xi$$

para $n > 0$, $L_0 = \mathbb{Z}$.

Consideremos también, para un parámetro π fijo, el homomorfismo de grupos

$$\begin{aligned} d_\pi : K^\times &\to L_1 = \kappa^\times \oplus \mathbb{Z}\xi \\ \pi^i u &\mapsto (\overline{u}, i\xi). \end{aligned}$$

Tomando potencia tensorial y usando la estructura de producto en $K_*^M(\kappa)[\xi]$, obtenemos

$$d_\pi^{\otimes n} : (K^\times)^{\otimes n} \to L_n$$

Denotemos las proyecciones $L_n \to K_n^M(\kappa)$ y $L_n \to K_{n-1}^M(\kappa)$ por π_1 y π_2 respectivamente. Considerando las composiciones

$$\pi_2 \circ d_\pi^{\otimes n} : K^{\otimes n} \to K_{n-1}^M(\kappa)$$

y

$$\pi_1 \circ d_\pi^{\otimes n} : K^{\otimes n} \to K_n^M(\kappa),$$

la construcción estará completa si establecemos la relación de Steinberg

$$d_\pi^{\otimes 2}(\{x, 1-x\}) = d_\pi(x)d_\pi(1-x) = 0$$

en L_2.

Sea $x = \pi^i u \in \kappa^\times$. Si $i > 0$, entonces $x \in M$ y $\overline{1-x} = \overline{1} \in \kappa$. Luego $d_\pi(1-x) = (\overline{1}, 0\xi)$ y $d_\pi(x)d_\pi(1-x) = 0$.

Si $i < 0$, $1 - x = (-u + \pi^i)\pi^i$ y $d_\pi(1-x) = (-\overline{u}, i\xi)$. Luego

$$\begin{aligned} d_\pi(x)d_\pi(1-x) &= (\overline{u}, i\xi)(-\overline{u}, i\xi) = (\{\overline{u}, -\overline{u}\}, (-1)^{-i^2}\overline{u}^i(-\overline{u})^{-i}\xi) \\ &= (0, \{(-1)^{-i^2-i}\}\xi) = 0. \end{aligned}$$

Si $i = 0$ y $v(1-x) \neq 0$, reemplazando x por $1-x$ llegamos a los casos anteriores. Si $i = 0$ y $v(1-x) = 0$, es decir, si x y $1-x$ son unidades, entonces $d_\pi(x)d_\pi(1-x) = (\{\overline{u}, 1-\overline{u}\}, 0\xi) = 0$. □

Ejemplo 2.2.2. Cuando $n = 1$, el símbolo *tame* $\partial^M : K_1^M(K) \to K_0^M(\kappa)$ es la valuación discreta $v : K^\times \to \mathbb{Z}$.
Cuando $n = 2$, tendremos que $\partial^M : K_2^M(K) \to K_1^M(\kappa)$ está dado por

$$\begin{aligned} \partial^M(\{a,b\}) &= \partial^M(\{\pi^i u, \pi^j w\}) = \partial^M(ij\{\pi,-1\} - j\{\pi,u\} + i\{\pi,w\} + \{u,w\}) \\ &= (-1)^{ij}\overline{u^{-j}w^i} = (-1)^{ij}\overline{(\pi^{-ij}u^{-j})(\pi^{ij}w^i)} \\ &= (-1)^{ij}\overline{a^{-j}b^i} = (-1)^{v(a)v(b)}\overline{a^{-v(b)}b^{v(a)}}, \end{aligned}$$

para $a = \pi^i u, b = \pi^j w \in K^\times$.

Observación 2.2.3. La manera en que se relacionan los símbolos *tame* y las aplicaciones especialización es la siguiente: para todo parámetro local π,

$$s_\pi^M(\{a_1, \ldots, a_n\}) = \partial^M(\{-\pi, a_1, \ldots, a_n\}),$$

para cualquier $\{a_1, \ldots, a_n\} \in K_n^M(K)$. En efecto, si $a_1 = \pi^i u_1$, entonces

$$\{-\pi, a_1, \ldots, a_n\} = i\{-\pi, \pi, \ldots, a_n\} + \{-\pi, u_1, \ldots, a_n\},$$

donde el primer sumando de la parte derecha de la igualdad es igual a cero. Continuando este proceso, podemos suponer que los a_i son unidades, y la afirmación sigue de la definición.

Definición 2.2.4. Definimos U_n como el subgrupo de $K_n^M(K)$ generado por los símbolos $\{u_1, \ldots, u_n\}$ con $u_i \in A^\times$, y $U_n^1 \subset K_n^M(K)$ como el subgrupo generado por los símbolos $\{x_1, \ldots, x_n\}$ con $x_1 \in A^\times$ tal que $\overline{x}_1 = 1$.

Observación 2.2.5. Veamos que U_n^1 es un subgrupo de U_n. Escribiendo $x = \pi^i u \in A^\times$ para alguna unidad u, basta ver el caso $n = 2$. Veamos que los símbolos de la forma $\{1 + a\pi, \pi\}$, con $a \in A$, pertenecen a U_2. Si $a \in A^\times$, entonces

$$\begin{aligned} \{1 + a\pi, \pi\} &= \{1 + a\pi, -a\pi\} + \{1 + a\pi, -a^{-1}\} \\ &= \{1 + a\pi, -a^{-1}\} \in U_2. \end{aligned}$$

Si $a \in M$, entonces

$$\begin{aligned} \{1 + a\pi, \pi\} &= \{1 + (\frac{1+a}{1-\pi})\pi, \pi\} + \{1 - \pi, \pi\} \\ &= \{1 + (\frac{1+a}{1-\pi})\pi, \pi\} \in U_2 \end{aligned}$$

por el caso anterior, pues $\frac{1+a}{1-\pi} \in A^\times$.

Proposición 2.2.6. *Se tienen sucesiones exactas*

$$0 \to U_n \to K_n^M(K) \stackrel{\partial^M}{\to} K_{n-1}^M(\kappa) \to 0$$

y

$$0 \to U_n^1 \to K_n^M(K) \stackrel{(s_\pi, \partial^M)}{\longrightarrow} K_n^M(\kappa) \oplus K_{n-1}^M(\kappa) \to 0.$$

Demostración. De la definición, sabemos que ∂^M y s_π^M son sobreyectivas. Para que la primera sucesión sea exacta, debemos mostrar que $U_n = \ker(\partial^M)$. Es claro de la definición que $U_n \subseteq \ker(\partial^M)$. Veamos lo que pasa con los símbolos de la forma $\beta = \{\pi, u_2, \ldots, u_n\}$, $u_i \in A^\times$.

Consideremos la aplicación

$$\begin{aligned}\psi : K^M_{n-1}(\kappa) &\rightarrow K^M_n(K)/U^1_n \\ \{\overline{u}_1, \ldots, \overline{u}_{n-1}\} &\mapsto \{\pi, u_1, \ldots, u_{n-1}\} \bmod U^1_n.\end{aligned}$$

Esta aplicación está bien definida. En efecto, basta ver el caso $n = 2$. Si $\overline{u'} = \overline{u}$, es decir, $u' = u + a\pi$, entonces

$$\begin{aligned}\{\pi, u'\} &= \{\pi, u + a\pi\} = \{\pi, u(1 + au^{-1}\pi)\} \\ &= \{\pi, u\} + \{\pi, 1 + au^{-1}\pi\}.\end{aligned}$$

Como $\{\pi, 1+au^{-1}\pi\} = -\{1+au^{-1}\pi, \pi\} \in U^1_2$, se tiene que $\{\pi, u'\} = \{\pi, u\} \bmod U^1_2$.
Si $\beta \in \ker(\partial^M)$, entonces

$$0 = (\psi \circ \partial^M)(\beta) = \beta \bmod U^1_n,$$

es decir, $\beta \in U^1_n \subset U_n$. Como todo símbolo se escribe como combinación de elementos de U_n y del tipo β, tendremos que $\ker(\partial^M) = U_n$.
Para la segunda sucesión, definimos

$$\begin{aligned}K^M_n(\kappa) &\rightarrow U_n/U^1_n \\ \{\overline{u}_1, \ldots, \overline{u}_n\} &\mapsto \{u_1, \ldots, u_n\} \bmod U^1_n\end{aligned}$$

Nuevamente, dicha aplicación está bien definida, y como s^M_π es trivial en U^1_n (propiedad 4 de los símbolos), es la inversa de la aplicación inducida por la restricción $s^M_\pi\big|_{U_n}$. $\square$

2.3 El Teorema de Milnor

Sea k un cuerpo algebraicamente cerrado. Recordemos que existe una biyección entre los anillos de valuación discreta de $k(t)$ triviales en k y los puntos cerrados P del espacio proyectivo $\mathbb{P}^1_k$. Para tal P, denotamos por A_P, $\kappa(P)$ y v_P a los correspondientes anillo de valuación discreta, cuerpo residual y valuación, respectivamente.

Si $P \neq \infty$, denotamos al respectivo parámetro local por π_P. El grado de π_P es llamado simplemente grado de P (lo cual denotamos por $\mathrm{grad}(P)$) y coincide con $[\kappa(P) : k]$, la dimensión de $\kappa(P)$ como k-espacio vectorial. En efecto, basta ver que si $\mathrm{grad}(P) = d$, entonces $\{\bar{1}, \bar{t}, \bar{t}^2, \cdots, \bar{t}^{d-1}\}$ es una base de $\kappa(P)$ como k-espacio vectorial.

Si $P = \infty$, consideramos $\pi_P = t^{-1}$. Así, tendremos símbolos *tame*

$$\partial_P^M : K_n^M(k(t)) \to K_{n-1}^M(\kappa(P))$$

y especializaciones

$$s_{\pi_P}^M : K_n^M(k(t)) \to K_n^M(\kappa(P)).$$

Si definimos

$$\partial^M := (\partial_P^M) : K_n^M(k(t)) \to \prod_{P \in \mathbb{P}_0^1} K_n^M(\kappa(P)),$$

vemos que la imagen está en la suma directa. En efecto, $f = g/h \in k(t)$ es unidad en A_P si, y solamente si $f^{-1} = h/g \in A_P$. Esto ocurre cuando P no es raíz de g, lo cual no ocurre solo en una cantidad finita de puntos. Por lo tanto, la imagen de $\{f_1, f_2, \ldots, f_n\}$ es nula en todo $K_{n-1}^M(\kappa(P))$, excepto para una cantidad finita de puntos cerrados.

Teorema 2.3.1. *(Milnor) La sucesión*

$$0 \to K_n^M(k) \to K_n^M(k(t)) \to \bigoplus_{P \in \mathbb{P}_0^1} K_{n-1}^M(\kappa(P)) \to 0$$

es exacta y split por la especialización $s_{t^{-1}}$ en ∞.

Demostración. Es claro que $K_n^M(k(t))$ tiene una filtración

$$K_n^M(k) = L_0 \subset L_1 \subset \cdots \subset L_d \subset \cdots$$

donde L_d es el subgrupo generado por los símbolos $\{f_1, \ldots, f_n\}$, con f_i polinomio de grado $\leq d$ para todo $i = 1, \ldots, n$. Para cada $d > 0$, consideremos

$$\partial_d^M : K_n^M(k(t)) \to \bigoplus_{\mathrm{grad}(P)=d} K_{n-1}^M(\kappa(P)),$$

la suma directa de las aplicaciones ∂_P^M para los puntos cerrados de grado d. La restricción de esta aplicación a L_d induce un isomorfismo

$$\overline{\partial}_d^M : L_d/L_{d-1} \simeq \bigoplus_{\mathrm{grad}(P)=d} K_{n-1}^M(\kappa(P))$$

Esta aplicación existe, pues si P es un punto cerrado de grado d y $\{f_1, \ldots, f_n\}$ es un generador de L_{d-1}, cada f_i tiene grado a lo más $d-1$, y será combinación de elementos $\{u_1, \ldots, u_n\}$ (pues $\mathrm{grad}(\pi_P) = d$). Luego ∂_P^M es trivial en L_{d-1}. Veamos que $\overline{\partial}_d^M$ posee inversa.

Sea P un punto cerrado de grado d. Para todo $\overline{a} \in \kappa(P)$ existe un único polinomio $a \in k[t]$ de grado $\leq d-1$ con imagen $\overline{a}$ en $\kappa(P)$. Así, podemos definir

$$\begin{aligned} h_P : K_{n-1}^M(\kappa(P)) &\to L_d/L_{d-1} \\ \{\overline{a}_2, \ldots, \overline{a}_n\} &\mapsto \{\pi_P, a_2, \ldots, a_n\} \bmod L_{d-1} \end{aligned}$$

Veamos que h_P es un homomorfismo. Basta ver el caso $n = 2$. Supongamos que $\overline{a}_2 = \overline{b}_2\overline{c}_2$. Si $a_2 = b_2c_2$, no hay nada que probar. Supongamos entonces que $a_2 \neq b_2c_2$. Dividiendo por π_P obtenemos $b_2c_2 = a_2 - \pi_P f$, para algún $f \in k[t]$ con grado $< d-1$. Luego

$$\frac{\pi_P f}{a_2} = 1 - \frac{b_2 c_2}{a_2}$$

y

$$\begin{aligned}
\{\pi_P, b_2c_2\} - \{\pi_P, a_2\} &= \{\pi_P, b_2c_2/a_2\} \\
&= -\{f/a_2, b_2c_2/a_2\} + \{\pi_P f/a_2, b_2c_2/a_2\} \\
&= -\{f/a_2, b_2c_2/a_2\} \in L_{d-1}
\end{aligned}$$

Aplicando inducción, obtenemos sucesiones exactas

$$0 \to L_0 \to L_d \to \bigoplus_{\mathrm{grad}(P)\leq d} K^M_{n-1}(\kappa(P) \to 0 \tag{2.1}$$

para todo $d > 0$. En efecto, por lo anterior tenemos sucesiones exactas

$$0 \to L_{d-1} \to L_d \xrightarrow{\alpha} \bigoplus_{\mathrm{grad}(P)=d} K^M_{n-1}(\kappa(P) \to 0$$

para todo $d > 0$. Si suponemos la afirmación verdadera para $d-1$, tendremos

$$0 \to L_0 \to L_{d-1} \xrightarrow{\beta} \bigoplus_{\mathrm{grad}(P)\leq d-1} K^M_{n-1}(\kappa(P) \to 0.$$

Considerando la aplicación $(\alpha,\beta) : L_d \to \bigoplus_{\mathrm{grad}(P)\leq d} K^M_{n-1}(\kappa(P))$ obtenemos la fórmula 2.1, teniendo en cuenta que

$$\ker(\alpha,\beta) = L_0 \cap L_d = L_0.$$

Dichas sucesiones exactas forman un sistema natural directo respecto a las inclusiones que vienen de la filtración. Como $L_0 = K^M_n(k)$ y $\bigcup_{d>0} L_d = K^M_n(k(t))$, la sucesión exacta del teorema se obtiene pasando al límite directo, que respeta sucesiones exactas. Además, es claro que la sucesión es split, pues para $P = \infty$, se tiene $\kappa(P) = k$. $\square$

Como la sucesión del teorema es split, podemos definir aplicaciones coresiduales $\psi : K_{n-1}^M(\kappa(P)) \to K_n^M(k(t))$ para todo punto cerrado $P \neq \infty$, tales que $\partial_P^M \circ \psi_P^M = \mathrm{id}_{\kappa(P)}$ y $\partial_P^M \circ \psi_Q^M = 0$ para $Q \neq P$.

Corolario 2.3.2. *Para todo $\alpha \in K_n^M(k(t))$, para todo $n > 0$, se cumple que*

$$\alpha = s_{t^{-1}}(\alpha)_{k(t)} + \sum_{P \in \mathbb{A}_0^1} (\psi_P^M \circ \partial_P)(\alpha).$$

Demostración. Para todo $P \neq \infty$, tenemos de la definición de ψ_P que

$$\partial_P \left(\alpha - \sum_{P \neq \infty} (\psi_P \circ \partial_P)(\alpha) \right) = \partial_P(\alpha) - \partial_P(\alpha) = 0,$$

luego

$$\alpha - \sum_{P \neq \infty} (\psi_P \circ \partial_P)(\alpha) \in \ker(\partial_P)$$

y, por la sucesión exacta de Milnor,

$$\alpha - \sum_{P \neq \infty} (\psi_P \circ \partial_P)(\alpha) = \beta$$

para algún β que viene de $K_n^M(k)$; es decir, $\beta = s_{t^{-1}}(\alpha)_{k(t)}$. □

Para todo $P \neq \infty$ definimos normas $N_P : K_n^M(\kappa(P)) \to K_n^M(k)$ mediante $N_P := -\partial_\infty^M \circ \psi_P^M$, para todo $n \geq 0$. Si $P = \infty$, definimos N_P como la identidad en $K_n^M(k)$.

Corolario 2.3.3. *(Ley de reciprocidad de Weil) Para todo $\alpha \in K_n^M(k(t))$, se cumple que*

$$\sum_{P \in \mathbb{P}_0^1} (N_P \circ \partial_P^M)(\alpha) = 0.$$

Demostración. Usando la notación del corolario anterior, $\partial_\infty(\beta) = 0$, luego

$$\begin{aligned} -\partial_\infty(\alpha - \sum_{P\neq\infty}(\psi_P \circ \partial_P)(\alpha)) &= -\partial_\infty(\alpha) + \sum_{P\neq\infty}(N_P \circ \partial_P)(\alpha) \\ &= \sum_{P\in\mathbb{P}^1_0}(N_P \circ \partial_P^M)(\alpha) = 0 \end{aligned}$$

□

Observación 2.3.4. Si $L|K$ es una extensión finita y la valuación discreta w extiende a v, entonces $v(K^\times)$ es un subgrupo de índice finito en $w(K^\times)$. Este índice es llamado *índice de ramificación* y se denota por $e(w|v)$, o simplemente por e. Denotando al símbolo *tame* asociado por ∂_L^M, tendremos que

$$\partial_L^M(\alpha_L) = e\partial^M(\alpha),$$

para todo $\alpha \in K_n^M(K)$. En efecto, basta escribir un parámetro local π para v como $\pi = \pi_L^e u_L$ para algún parámetro local π_L y una unidad u_L para w. Entonces para cualquier $(n-1)$-upla $(u_2, \ldots, u_n)$ de unidades para v se obtiene

$$\{\pi, u_2, \ldots, u_n\}_L = e\{\pi_L, u_2, \ldots, u_n\} + \{u_L, u_2, \ldots, u_n\},$$

donde el segundo término de la suma es eliminado por ∂_L^M.

La proposición que sigue a continuación es consecuencia de los siguientes lemas:

Lema 2.3.5. *Sea $L|K$ una extensión de cuerpos, $P \in \mathbb{P}^1_K$ un punto cerrado. Entonces*

$$\begin{tikzcd} K_n^M(\kappa(P)) \arrow[r, "N_P"] \arrow[d, "\bigoplus i_{\kappa(Q)|\kappa(P)}"'] & K_n^M(K) \arrow[d, "i_{L|K}"] \\ \bigoplus_{Q\mapsto P} K_n^M(\kappa(Q)) \arrow[r, "\sum e_Q N_Q"] & K_n^M(L) \end{tikzcd}$$

conmuta, donde e_Q es el índice de ramificación de la valuación v_Q que extiende v_P a $L(t)$.

Demostración. Por la observación anterior, el diagrama

$$\begin{tikzcd}
K_{n+1}^M(K(t)) \arrow[r, "\partial_P^M"] \arrow[d, "i_{L(t)|K(t)}"'] & K_n^M(K) \arrow[d, "\bigoplus i_{\kappa(Q)|\kappa(P)}"] \\
K_{n+1}^M(L(t)) \arrow[r, "\sum e_Q \partial_Q^M"] & \bigoplus_{Q\mapsto P} K_n^M(\kappa(Q))
\end{tikzcd}$$

es conmutativo. Luego, también lo es el diagrama

$$\begin{tikzcd}
K_n^M(\kappa(P)) \arrow[r, "\psi_P^M"] \arrow[d, "\bigoplus i_{\kappa(Q)|\kappa(P)}"'] & K_{n+1}^M(K(t)) \arrow[d, "i_{L(t)|K(t)}"] \\
\bigoplus_{Q\mapsto P} K_n^M(\kappa(Q)) \arrow[r, "\sum e_Q \psi_Q^M"] & K_{n+1}^M(L(t))
\end{tikzcd}$$

De la definición de las normas N_P, se obtiene la compatibilidad del lema. □

Lema 2.3.6. *Sea $L|K$ una extensión de cuerpos finita. Asumamos que la clausura integral del anillo de valuación A_v (v valuación discreta en K) de v en L es un A_v-módulo finitamente generado. Entonces*

$$\sum_{w|v} e(w|v)[\kappa(w)|\kappa(v)] = [L : K],$$

donde los w extienden a v sobre L.

Demostración. La prueba se puede encontrar en [9], Sección I.4, Proposición 10. □

Proposición 2.3.7. *Para $n = 0$, $N_P : K_0^M(\kappa(P)) \to K_0^M(k)$ está dada por la multiplicación por $[\kappa(P) : k]$, y para $n = 1$, coincide con la norma del cuerpo $N_{\kappa(P)|k} : \kappa(P)^\times \to k^\times$.*

Demostración. Aplicamos el primer lema con $K = \overline{k}$, la clausura algebraica de k. En este caso, los puntos Q tienen grado 1 sobre K, y las aplicaciones N_Q son la identidad. Además, las aplicaciones verticales son inyectivas para $n = 0, 1$. La afirmación para $n = 0$ sigue del segundo lema, pues tendremos que $\sum e_Q = [\kappa(P) : k]$, mientras que para $n = 1$, la afirimación sigue de la definición de la norma del cuerpo $N_{\kappa(P)|k}(\alpha)$ como el producto de las raíces en K (con multiplicidad) del polinomio minimal de α. □

Observación 2.3.8. Las aplicaciones N_P satisfacen la *fórmula de proyección*

$$N_P(\{\alpha_{\kappa(P)}, \beta\}) = \{\alpha, N_P(\beta)\},$$

para todo $\alpha \in K_n^M(k)$, para todo $\beta \in K_m^M(\kappa(P))$.

Lema 2.3.9. *El subgrupo $L_d \subset K_n^M(k(t))$ está generado por símbolos de la forma*

$$\{a_1, \dots, a_m, \pi_{m+1}, \dots, \pi_n\},$$

con $a_i \in k^\times$ y $\pi_i \in k[t]$ polinomios mónicos irreducibles tales que

$$grad(\pi_{m+1}) < \cdots < grad(\pi_n) \leq d.$$

Demostración. L_d está generado por símbolos $\{f_1, \dots, f_n\}$ con $\mathrm{grad}(f_i) \leq d$. Factorizando estos polinomios, y aplicando bilinealidad y anticonmutatividad, podemos considerar los generadores del lema, pero con $\mathrm{grad}(\pi_{m+1}) \leq \cdots \leq \mathrm{grad}(\pi_n) \leq d$. Si $n = 2$, supongamos que $\mathrm{grad}(\pi_1) = \mathrm{grad}(\pi_2) \leq d$. Aplicando inducción sobre d, si $d = 0$, $\pi_1 = a_1$, $\pi_2 = a_2$. Supongamos que $d > 0$. Si $\mathrm{grad}(\pi_1) = \mathrm{grad}(\pi_2) < d$, la hipótesis inductiva nos da el resultado. Si $\mathrm{grad}(\pi_1) = \mathrm{grad}(\pi_2) = d$, dividimos π_2 por π_1 para obtener $\pi_2 = \pi_1 + f$ con $\mathrm{grad}(f) < d$. Entonces $1 = \frac{\pi_1}{\pi_2} + \frac{f}{\pi_2}$ y $\{\frac{\pi_1}{\pi_2}, \frac{f}{\pi_2}\} = 0$ en $K_2^M(k(t))$. Escribimos

$$\begin{aligned} \{\pi_1, \pi_2\} &= \{\frac{\pi_1}{\pi_2}, \pi_2\} + \{\pi_2, -1\} = -\{\frac{\pi_1}{\pi_2}, \frac{f}{\pi_2}\} + \{\frac{\pi_1}{\pi_2}, f\} + \{\pi_2, -1\} \\ &= \{\pi_1, f\} + \{\pi_2, \frac{1}{f}\} + \{\pi_2, -1\} = \{\pi_1, f\} + \{\pi_2, -\frac{1}{f}\} \\ &= -\{f, \pi_1\} + \{-f, \pi_2\}. \end{aligned}$$

Factorizando f y aplicando la hipótesis inductiva, obtenemos el resultado. El caso general es similar. □

Proposición 2.3.10. *(Lema de Bass-Tate) Sea $K = k(a)$ con a de grado d. Entonces $K_*^M(K)$ es generado como $K_*^M(k)$-módulo a izquierda por elementos de la forma $\{\pi_1(a), \ldots, \pi_m(a)\}$, donde los π_i son polinomios mónicos irreducibles en $k[t]$ que satisfacen*

$$\mathit{grad}(\pi_1) < \cdots < \mathit{grad}(\pi_m) \leq d - 1.$$

Demostración. Sea π_P el polinomio minimal de a sobre k, el cual define un punto cerrado P de grado d en $\mathbb{P}_k^1$. Se sigue de la demostración del Teorema de Milnor que el símbolo *tame* ∂_P^M induce una suryección de L_d sobre $K_n^M(\kappa(P))$. Del lema anterior concluimos que $K_n^M(\kappa(P))$ está generado por símbolos de la forma

$$\partial_P^M(\{a_1, \ldots, a_m, \pi_{m+1}, \ldots, \pi_n\}),$$

con $a_i \in k^\times$ y π_i polinomios mónicos irreducibles tales que $\mathrm{grad}(\pi_{m+1}) < \cdots < \mathrm{grad}(\pi_n) \leq d$. Si $\pi_n \neq \pi_P$, los π_i satisfacen $v_\pi(\pi_i) = 0$ (pues $\pi_i = \pi_P^0 u_i$), y los símbolos son cero. Si $\pi_n = \pi_P$, los símbolos son

$$\partial_P(\{\ldots, \pi_P\}) = \pm\partial_P(\{\pi_P, \ldots\}) = \pm\{a_1, \ldots, a_m, \pi_{m+1}(a), \ldots, \pi_{n-1}(a)\}.$$

□

Corolario 2.3.11. *Sea $K|k$ una extensión finita. Supongamos que se cumple que dicha extensión es cuadrática o de grado primo p y k no admite extensiones finitas no triviales de grado primo con p. Entonces $K_*^M(K)$ está generado como $K_*^M(k)$-módulo a izquierda por $K_1^M(K) = K^\times$. Es decir, las aplicaciones producto*

$$K_{n-1}^M(k) \otimes K^\times \to K_n^M(K)$$

son sobreyectivas.

Demostración. En ambos casos, K se obtiene adjuntando un solo elemento a a k, y los únicos polinomios mónicos irreducibles en $k[t]$ de grado $< [K : k]$ son los polinomios lineales $x - a$. Se concluye el resultado aplicando la proposición. □

Observación 2.3.12. Un caso típico en el que se satisface la segunda condición es cuando k es una *extensión maximal prima con p* de algún cuerpo $k_0 \subset k$. Esto es, una extensión algebraica $k|k_0$ tal que todas sus subextensiones finitas tienen grado primo con p, y la cual es maximal con respecto a esta propiedad. Para un cuerpo k_0 de característica p, tal extensión k se puede construir tomando el subcuerpo de una extensión separable $k_s|k_0$ fijada por un pro-p subgrupo de Sylow de $\mathrm{Gal}(k_s|k_0)$.

2.4 La Aplicación Norma

Sea $K|k$ una extensión finita. Deseamos extender la noción de norma (de una extensión Galois) $N_{K|k} : K^\times \to k^\times$ vista en el capítulo anterior a aplicaciones $N_{K|k} : K_n^M(K) \to K_n^M(k)$, para todo $n \geq 0$. Si $K = k(a)$, el polinomio minimal de a define un punto cerrado $P \in \mathbb{P}_k^1$ para el cual $K \simeq \kappa(P)$. La aplicación N_P definida en la sección anterior satisface, como ya hemos visto, las siguientes propiedades:

1. $N_P : K_0^M(K) \to K_0^M(k)$ es la multiplicación por $[K : k]$.

2. $N_P : K_1^M(K) \to K_1^M(k)$ es la norma usual $N_{K|k} : K^\times \to k^\times$.

3. (Fórmula de proyección) $N_P(\{\alpha_K, \beta\}) = \{\alpha, N_P(\beta)\}$, para todo $\alpha \in K_n^M(k)$, para todo $\beta \in K_m^M(K)$

Observación 2.4.1. Si una norma $N_{K|k}$ satisface las propiedades 1-3 de arriba, tendremos que $N_{K|k} \circ i_{K|k} : K_n^M(k) \to K_n^M(k)$ está dada por la multiplicación por $[K : k]$, para todo n. En efecto, esto es obvio para $n = 0$ (propiedad 1) y $n = 1$ (prop. 1.2.1). Usando inducción y la fórmula de proyección, obtenemos el resultado en general.

Definimos entonces, para una extensión simple $K = k(a)$, (cambiando la notación dada al principio) $N_{a|k} : K_n^M(k(a)) \to K_n^M(k)$ por $N_{a|k} := N_P$, donde P es el punto cerrado considerado anteriormente. Si consideramos una extensión finita arbitraria $K|k$, podemos escribir $K = k(a_1, \dots, a_r)$ para algunos generadores $a_1, \dots, a_r \in K$, y

$$k \subset k(a_1) \subset k(a_2) \subset \cdots \subset k(a_1, \dots, a_r) = K.$$

Haciendo

$$N_{a_1,\dots,a_r|k} := N_{a_r|k(a_1,\dots,a_{r-1})} \circ \cdots \circ N_{a_2|k(a_1)} \circ N_{a_1|k},$$

obtenemos una aplicación que satisface las propiedades 1-3 de arriba y que además satisface

4. (Composición) Dada la torre $K'|K|k$, se tiene

$$N_{K'|k} = N_{K|k} \circ N_{K'|K}.$$

Por la observación anterior, también se tiene que $N_{a_1,\dots,a_r|k} \circ i_{K|k}$ es la multiplicación por $[K : k]$. Finalmente, mencionamos un teorema debido a Kato y una ley de reciprocidad que será usada más adelante:

Teorema 2.4.2. *Las aplicaciones $N_{a_1,\ldots,a_r|k} : K_n^M(K) \to K_n^M(k)$ no dependen de la elección de los generadores $a_1, \ldots, a_r$.*

Un esbozo de la prueba se puede encontrar en *Kato : A generalization of local class field theory by using K-groups, II.*
Así, podemos definir

$$N_{K|k} := N_{a_1,\ldots,a_r|k} : K_n^M(K) \to K_n^M(k),$$

para todo $n \geq 0$.

Corolario 2.4.3. *Si $\sigma : K \to K$ es un k-automorfismo, entonces se cumple $N_{K|k} \circ \sigma = N_{K|k}$.*

Demostración. En efecto, por el teorema se tiene $N_{a_1,\ldots,a_r|k} = N_{\sigma(a_1),\ldots,\sigma(a_r)|k}$. □

Proposición 2.4.4. *Sea K un cuerpo completo con respecto a la valuación discreta v con cuerpo residual κ. Sea $K'|K$ una extensión finita y denotemos por κ' al cuerpo residual de la única extensión v' de v a K. Entonces, para todo $n > 0$, el diagrama*

$$\begin{tikzcd}
K_n^M(K') \arrow[r, "\partial_{K'}^M"] \arrow[d, "N_{K'|K}"'] & K_{n-1}^M(\kappa') \arrow[d, "N_{\kappa'|\kappa}"] \\
K_n^M(K) \arrow[r, "\partial_K^M"] & K_{n-1}^M(\kappa)
\end{tikzcd}$$

conmuta.

3 TEOREMA 90 DE HILBERT

En este capítulo incluimos el resultado principal de nuestro trabajo, el Teorema 90 de Hilbert para K_2. Previamente definimos las variedades de Severi-Brauer, así como algunos resultados necesarios en la prueba de dicho teorema.

3.1 Variedades de Severi-Brauer

Definición 3.1.1. Una *variedad de Severi-Brauer* sobre un cuerpo k es una variedad algebraica proyectiva sobre k tal que la extensión de base $X_K := X \times_k K$ es isomorfa a $\mathbb{P}_K^{n-1}$, para alguna extensión finita $K|k$. El cuerpo K es llamado *cuerpo de descomposición* para X.

Para una variedad X sobre k de dimensión d, denotemos por X_i al conjunto de sus puntos de dimensión i (viendo a X como k-esquema). Para todo entero n, tenemos complejos de grupos abelianos

$$S_n(X) : \bigoplus_{P \in X_d} K_{n+d}^M(\kappa(P)) \xrightarrow{\partial} \bigoplus_{P \in X_{d-1}} K_{n+d-1}^M(\kappa(P)) \xrightarrow{\partial} \cdots \xrightarrow{\partial} \bigoplus_{P \in X_0} K_n^M(\kappa(P)),$$

llamados *complejos de Gersten en K-teoría de Milnor.*

Definición 3.1.2. Para $0 \leq i \leq d$, denotemos al i-ésimo grupo de homología del complejo $S_n(X)$ (es decir, la homología en el término indexado por los puntos en X_i) por $A_i(X, K_n^M)$. Este es llamado *i-ésimo grupo de homología de X con valores en K_n^M.*

Proposición 3.1.3. *Para todo entero $n, d \geq 0$, se cumple que*

$$A_i(\mathbb{P}^d, K_n^M) \cong \begin{cases} K_{n+i}^M(k) & \text{si } 0 \leq i \leq d \\ 0 & \text{en cualquier otro caso.} \end{cases}$$

Demostración. La prueba se puede encontrar en [3], Proposición 8.2.6.

Ejemplo 3.1.4. El caso que nos interesa es el de $n = 2 - d$. En tal caso, tenemos

$$A_d(\mathbb{P}^d, K^M_{2-d}) \cong K^M_2(k),$$

$$A_{d-1}(\mathbb{P}^d, K^M_{2-d}) \cong k^{\times},$$

$$A_{d-2}(\mathbb{P}^d, K^M_{2-d}) \cong \mathbb{Z}$$

y 0 en los demás casos.

Teorema 3.1.5. *Sea k un cuerpo, p un primo invertible en k, y X una variedad de Severi-Brauer de dimensión $d = p - 1$ sobre k. Si $K|k$ es una extensión finita de grado p que descompone a X, las aplicaciones naturales*

$$A_{d-i}(X, K^M_{i+1-d}) \to A_{d-i}(X_K, K^M_i + 1 - d)$$

son inyectivas para todo $0 \leq i \leq p - 1$.

Demostración. Teorema 8.3.1, [3].

3.2 Teorema 90 de Hilbert para K_2

Empecemos enunciando el Teorema 90 de Hilbert en su forma original y un par de resultados que usaremos en la prueba de su versión para K_2:

Teorema 3.2.1. *(90 de Hilbert) En una extensión cíclica $K|k$ con $G = Gal(K|k) = \langle\sigma\rangle$, todo elemento de norma 1 es de la forma $\sigma(e)e^{-1}$, para algún $e \in K$.*

El nombre del teorema es debido a que fue el 90o teorema de su obra Zahlbericht (informe de los números, 1897), aunque se debe originalmente a Kummer (1855). Noether probó un teorema más general (1933) que recibe el mismo nombre. Este dice que si $K|k$ es Galois finita, entonces $H^1(G, K^\times)$ es trivial.

Proposición 3.2.2. *Sean k un cuerpo y $m > 0$ un entero. Dada la extensión cíclica Galois $K|k$ de grado m y con grupo G, sea $\chi : G \xrightarrow{\sim} \mathbb{Z}/m$ un isomorfismo. Entonces el isomorfismo*

$$Br(K|k) \simeq k^\times / N_{K|k}(K^\times)$$

lleva un elemento $b \in k^\times$ a la clase del álgebra cíclica (χ, b).

Demostración. Corolario 4.7.4 [3].

Proposición 3.2.3. *La clase del álgebra cíclica (χ, b) en $Br(K|k)$ es trivial si, y solamente si b es una norma para la extensión $K|k$.*

Demostración. Corolario 4.7.5 [3].

Lema 3.2.4. *Sean G un grupo profinito y $(A_\alpha, \phi_{\alpha\beta})$ un sistema directo de G-módulos continuos. Entonces el G-módulo $\varinjlim A_\alpha$ también es continuo, los grupos $H^i(G, A_\alpha)$ con las aplicaciones inducidas forman un sistema directo y existen isomorfismos canónicos*

$$\varinjlim H^i(G, A_\alpha) \xrightarrow{\sim} H^i(G, \varinjlim A_\alpha)$$

para todo $i > 0$.

Demostración. Lema 4.3.3 [3].

Sea $K|k$ una extensión cíclica Galois de grado primo p, σ un generador de $\mathrm{Gal}(K|k)$. Consideremos la sucesión

$$K_2^M(K) \xrightarrow{\sigma - 1} K_2^M(K) \xrightarrow{N_{K|k}} K_2^M(k),$$

donde $\sigma : K_2^M(K) \to K_2^M(K)$ es inducida por $\sigma(a \otimes b) = \sigma(a) \otimes \sigma(b)$ en $K^\times \otimes K^\times$. La sucesión es un complejo, pues $N_{K|k}(\sigma(\alpha)) = N_{K|k}(\alpha)$, para todo $\alpha \in K_2^M(K)$

(Corolario 2.4.3). Luego $N_{K|k} \circ (\sigma - 1)(\alpha) = N_{K|k}(\alpha) - N_{K|k}(\alpha) = 0$. El Teorema 90 de Hilbert para K_2, clave para la prueba del Teorema de Merkurjev-Suslin, se presenta a continuación:

Teorema 3.2.5. *(90 de Hilbert para K_2) Sea $K|k$ una extensión cíclica Galois de grado primo p, y sea σ un generador de Gal$(K|k)$. Entonces el complejo*

$$K_2^M(K) \xrightarrow{\sigma-1} K_2^M(K) \xrightarrow{N_{K|k}} K_2^M(k) \tag{3.1}$$

es exacto.

Demostración. Dividiremos la prueba en partes. Establecemos primero algunas notaciones: si $F|k$ es una extensión y $K \otimes_k F$ no es un cuerpo, entonces es la suma directa de p copias de F (es decir, $K \otimes_k F \cong F^{\oplus p}$). En este último caso, denotaremos por $N_{K\otimes_k F|F} : K_2^M(K \otimes_k F) \to K_2^M(F)$ a la aplicación $K_2^M(F)^{\oplus p} \to K_2^M(F)$ dada por la suma de las aplicaciones identidad.
Para cualquier extensión $F|k$, denotemos por $V(F)$ a la homología del complejo

$$K_2^M(K \otimes_k F) \xrightarrow{\sigma-1} K_2^M(K \otimes_k F) \xrightarrow{N_{K\otimes_k F|F}} K_2^M(F),$$

donde el automorfismo σ actúa sobre $K \otimes_k F$ via el primer factor y $K_2^M(K \otimes_k F)$ está equipado con la acción inducida. Para una torre $E|F|k$ se tienen homomorfismos naturales $V(k) \to V(F) \to V(E)$.

Parte 1

Supongamos primero que k no posee extensiones finitas de grado primo con p y que $N_{K|k} : K^\times \to k^\times$ es sobreyectivo. Consideremos la aplicación

$$\overline{N}_{K|k} : K_2^M(K)/(\sigma - 1)K_2^M(K) \to K_2^M(k)$$

inducida por la norma $N_{K|k}$. Veamos que dicha aplicación posee inversa. Sea

$$\widetilde{\psi} : k^\times \times k^\times \to K_2^M(K)/(\sigma - 1)K_2^M(K)$$

la aplicación definida por $\widetilde{\psi}(a, b) := \{c, b\}$, donde $c \in K^\times$ es un elemento tal que $N_{K|k}(c) = a$; $a, b \in k^\times$. Para ver que está bien definida, sea $c' \in K^\times$ tal que $N_{K|k}(c') = a$. Como

$$N_{K|k}(c'c^{-1}) = N_{K|k}(c')N_{K|k}(c)^{-1} = 1,$$

por el Teorema 90 de Hilbert, $c'c^{-1}$ es de la forma $\sigma(e)e^{-1}$, para algún $e \in K$. Además, $\sigma(b) = b$, luego

$$\{c', b\} - \{c, b\} = \{c'c^{-1}, b\} = \{\sigma(e)e^{-1}, b\} = (\sigma - 1)\{e, b\} \in (\sigma - 1)K_2^M(K).$$

Como $\widetilde{\psi}$ es bilineal, podemos extenderla a $k^\times \otimes_{\mathbb{Z}} k^\times$. Para inducir una aplicación en $K_2^M(k)$, veamos que respeta la relación de Steinberg. Sea $a \in k^\times$ con $a \neq 0, 1$. Si $a \notin k^{\times p}$, definimos $L = k(\alpha)$, para algún $\alpha \in \overline{k}$ tal que $\alpha^p = a$. De otro modo, definimos $L = K$. Consideremos el k-álgebra $M = K \otimes_k L$. Sabemos que

$$\dim_k(M) = [K : k][L : k] = p^2,$$

y la aplicación

$$\begin{aligned} \varphi : M &\to KL \\ a \otimes b &\mapsto ab \end{aligned}$$

es sobreyectiva (los elementos de la forma ab, con $a \in K, b \in L$ generan KL). Si $L \neq K$, entonces $[KL : k] = p^2 = \dim_k(M)$, φ es un isomorfismo y M es un cuerpo (pues KL lo es). Si $L = K$, entonces $M \cong K^p$. De cualquier forma, tendremos que

$H^1(G, M^\times) = 0$, en el primer caso por el Teorema 90 de Hilbert y en el segundo porque $M^\times$ es un G-módulo coinducido.

En seguida, veamos que

$$1 - a_K = N_{M|K}(1 - \alpha_M). \tag{3.2}$$

Si $L = k(\alpha)|k$ es puramente inseparable, entonces $M = K(\alpha)|K$ también lo es, y de la definición de norma tendremos

$$N_{M|K}(1 - \alpha_M) = (1 - \alpha_M)^p = 1 - a_K$$

De lo contrario, $L|k$ es Galois cíclica, y $\mathrm{Gal}(L|k)$ está generado por un automorfismo τ (recordemos que k contiene a las p-ésimas raíces de la unidad). Por lo tanto, en L, se tiene la descomposición

$$x^p - a = \prod_{i=0}^{p-1}(x - \tau^i(\alpha)).$$

Haciendo $x = 1$ obtenemos

$$1 - a = \prod(1 - \tau^i(\alpha)) = N_{L|k}(1 - \alpha).$$

Como M es una extensión cíclica Galois de grado p de K o una suma directa de p copias de K, esto implica 3.2. Usando la fórmula de proyección, obtenemos

$$\{c, 1 - a\} = N_{M|K}(\{c_M, 1 - \alpha_M\}) = N_{M|K}(\{c_M\alpha_M^{-1}, 1 - \alpha_M\} + \{\alpha_M, 1 - \alpha_M\}).$$

Como $N_{M|K}(c_M\alpha_M^{-1}) = N_{M|K}(c_M)N_{M|K}(\alpha_M)^{-1} = a(\alpha^p)^{-1} = 1$, existe $d \in M$ tal que $c_M\alpha_M^{-1} = \sigma(d)d^{-1}$ (si $L \neq K$, por el teorema 90 clásico; si $L = K$, porque

$H^1(G, M^\times) = 0$, y todo cociclo es un coborde - ejemplo 1.1.10), luego

$$\{c, 1-a\} = N_{M|K}(\{\sigma(d)d^{-1}, 1-\alpha_M\}) = (\sigma - 1)N_{M|K}(\{d, 1-\alpha_M\})$$

y $\tilde{\psi}(a \otimes (1-a)) = \{c, 1-a\} \in (\sigma - 1)K_2^M(K)$, por lo que la aplicación está bien definida.
Tendremos entonces una aplicación

$$\psi : K_2^M(K) \to K_2^M(K)/(\sigma - 1)K_2^M(K)$$

que cumple

$$N_{K|k}(\psi(\{a, b\})) = N_{K|k}(\{c, b\}) = \{N_{K|k}(c), b\} = \{a, b\},$$

por lo que ψ debe ser inyectiva. La sobreyectividad se debe al corolario 2.3.3, teniendo en cuenta que k no admite extensiones finitas no triviales de grado primo con p. Este asegura que la aplicación $K^\times \otimes_{\mathbb{Z}} K^\times \to K_2^M(K)$ es sobreyectiva, por lo que ψ también lo es.

Parte 2

Veamos a continuación que si $k'|k$ es una extensión algebraica de grado primo con p o, si la extensión es infinita, con todas las subextensiones finitas de grado primo con p, entonces $V(k) \to V(k')$ es inyectivo.

Supongamos una extensión finita $L|k$. A partir del diagrama

$$\begin{tikzcd}
K_2^M(K \otimes_k L) \arrow[r, "\sigma-1"] \arrow[d, "N_{K\otimes_k L|K}"] & K_2^M(K \otimes_k L) \arrow[r, "N_{K\otimes_k L|L}"] \arrow[d, "N_{K\otimes_k L|K}"] & K_2^M(L) \arrow[d, "N_{L|k}"] \\
K_2^M(K) \arrow[r, "\sigma-1"] & K_2^M(K) \arrow[r, "N_{K|k}"] & K_2^M(k)
\end{tikzcd}$$

obtenemos una aplicación norma $N_{L|k} : V(L) \to V(k)$. De la Observación 2.4.1, sabemos que la composición $V(k) \to V(L) \to V(k)$ es la multiplicación por $[L : k]$. En particular, si $L = K$, dicha composición es la multiplicación por p. Por otro lado, $K \otimes_k K$ se descompone como una suma directa de p copias de K, y σ actúa trivialmente en cada componente pues hemos definido su acción en $K \otimes_k K$ via el primer factor. De ahí que $V(K) = 0$.
Así, obtenemos que $pV(K) = 0$. Además, si $L = k'$ es una extensión finita de grado primo con p, la composición $V(k) \to V(k') \to V(k)$ es la multiplicación por $[k' : k]$, y por lo tanto $V(k) \to V(k')$ debe ser inyectiva. Para pasar al caso general de una extensión algebraica $k'|k$ de grado primo con p, basta considerar k' como el límite directo de sus subextensiones finitas, y notar que el funtor $L \to V(L)$ conmuta con productos tensoriales y sucesiones exactas, luego con límites directos.

Parte 3

Sea X una variedad de Severi-Brauer con cuerpo de descomposición la extensión $K|k$ cíclica de grado p. Entonces la aplicación $V(k) \to V(k(X))$ es inyectiva.

Consideremos el diagrama

$$\begin{tikzcd}
K_2^M(K) \arrow[r, "\sigma-1"] \arrow[d] & K_2^M(K) \arrow[r, "N_{K|k}"] \arrow[d] & K_2^M(k) \arrow[d] \\
K_2^M(K(X)) \arrow[r, "\sigma-1"] \arrow[d, "\partial^M"'] & K_2^M(K(X)) \arrow[r, "N_{K|k}"] \arrow[d, "\partial^M"'] & K_2^M(k(X)) \arrow[d, "\partial^M"'] \\
\bigoplus_{P\in X_K^1} \kappa(P)^\times \arrow[r, "\sigma-1"] & \bigoplus_{P\in X_K^1} \kappa(P)^\times \arrow[r, "N_{K|k}"] & \bigoplus_{P\in X^1} \kappa(P)^\times
\end{tikzcd}$$

cuyas filas y columnas son complejos. Tomemos un elemento de $\mathrm{Ker}(V(k) \to V(k(X)))$. Es decir, la clase de un elemento $\alpha \in \mathrm{Ker}(N_{K|k})$ en $K_2^M(K)$ cuya imagen en $K_2^M(K(X))$ sea de la forma $\alpha_{K(X)} = (\sigma-1)(\beta)$, para algún $\beta \in K_2^M(K(X))$. Veamos que $\beta \in K_2^M(K)$, es decir, que la clase de α es 0.

Es claro que el diagrama es conmutativo (prop. 2.4.1). Como $(\sigma-1)\partial^M(\beta) = 0$, entonces $\sigma(\partial^M(\beta)) = \partial^M(\beta)$, y $\partial^M(\beta)$ debe provenir de un elemento de $\bigoplus_{X^1} \kappa(P)^\times$. Además, las valuaciones de este elemento que provienen de puntos de X^2 deben ser triviales, tal como aquellas de $\partial^M(\beta)$. Esto es, debe existir un elemento

$$\gamma_0 \in Z(X) := \mathrm{Ker}(\bigoplus_{P\in X^1} \kappa(P)^\times \to \bigoplus_{P\in X^2} \mathbb{Z})$$

tal que $\partial^M(\beta) = \gamma_{0,K}$. Consideremos ahora el diagrama conmutativo

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & \\
K_2^M(k(X))/K_2^M(k) \arrow[r, "\partial^M"] \arrow[d] & Z(X) \arrow[r] \arrow[d] & A_{d-1}(X, K_{2-d}^M) \arrow[r] \arrow[d] & 0 \\
K_2^M(K(X))/K_2^M(K) \arrow[r, "\partial^M"] & Z(X_K) \arrow[r] & A_{d-1}(X_K, K_{2-d}^M) \arrow[r] & 0
\end{tikzcd}$$

Las filas son exactas por la definición de los grupos $A_{d-1}(X, K_{2-d}^M)$, y la inyectividad de la tercera columna viene del Teorema 3.1.5. Del diagrama vemos que existe $\beta_0 \in K_2^M(k(X))$ tal que $\partial^M(\beta_0) = \gamma_0$. Podemos entonces reemplazar β por $\beta - \beta_{0,K}$ sin que la relación $\alpha = (\sigma - 1)\beta$ se vea afectada, pero ahora $\partial^M(\beta) = 0$. Es decir, $\beta \in A_d(X_K, K_{2-d}^M) \subset K_2^M(K(X))$. Como X_K es un espacio proyectivo sobre K, del ejemplo 3.1.2 se tiene que $\beta \in K_2^M(K)$.

Parte 4

Finalmente, definamos una torre de cuerpos

$$k = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_\infty = \bigcup_n F_n$$

de manera inductiva, como sigue:

1. El cuerpo F_{2n+1} es una extensión maximal prima con p de F_{2n} (Observación 2.3.12).

2. El cuerpo F_{2n+2} es la composición de todos los cuerpos de funciones de las variedades de Severi-Brauer asociadas a álgebras cíclicas de la forma (χ, b), donde χ es un elemento fijo de $\mathrm{Gal}(F_{2n+1}K|F_{2n+1}) \cong \mathrm{Gal}(K|k)$, y $b \in F_{2n+1}^\times$.

La composición de todos los cuerpos de funciones de una familia de variedades $\{X_i/i \in I\}$ se refiere al límite directo del sistema directo de cuerpos de funciones de todas las variedades $X_{i_1} \times \cdots \times X_{i_r}$ para subconjuntos finitos $\{i_1, \ldots, i_r\} \subset I$, parcialmente ordenados por las inclusiones naturales.

Además, las extensiones $KF_j|F_j$ son todas cíclicas de grado p. En efecto, esta propiedad se preserva cuando se pasa a una extensión de grado primo con p y cuando se toma el cuerpo de funciones de un producto de variedades de Severi-Brauer, pues estas variedades son geométricamente integrales, y por lo tanto el cuerpo base es algebraicamente cerrado en su cuerpo de funciones.

La parte 2 arriba muestra que $V(F_{2n})$ se encaja en $V(F_{2n+1})$ para $n \geq 0$, y una aplicación iterada de la parte 3 muestra que $V(F_{2n+1})$ se encaja en $V(F_{2n+2})$. Así, $V(k) = V(F_0)$ encaja en $V(F_\infty)$. Veamos ahora que el cuerpo F_∞ satisface las condiciones de la parte 1, lo cual concluye la prueba. Por construcción, no admite extensiones algebraicas de grado primo con p. La sobreyectividad de la norma $N_{KF_\infty|F_\infty}$ viene de la proposición previa a este teorema, que dice que bajo el isomorfismo $F_\infty^\times/N_{KF_\infty|F_\infty}((KF_\infty)^\times) \cong \mathrm{Br}(KF_\infty|F_\infty)$, las clases de todos los elementos $b \in F_\infty^\times$ son llevadas a las clases de las álgebras (χ, b). Pero cada b proviene de algún F_{2n+1}, y por lo tanto la clase del álgebra (χ, b) en $\mathrm{Br}(KF_{2n+2}|F_{2n+2})$ es trivial por la Proposición 3.2.3. Como $\mathrm{Br}(KF_\infty|F_\infty)$ es el límite directo de los $\mathrm{Br}(KF_j|F_j)$ (lemma 3.2.1), esto concluye la prueba del teorema. $\square$

4 EL TEOREMA DE MERKURJEV-SUSLIN

En este capítulo final mencionamos la principal aplicación del Teorema 90, el Teorema de Merkurjev-Suslin, que dio pie para el resultado general conocido como conjetura de Bloch-Kato, probado más adelante por Voevodsky.

4.1 El Símbolo de Galois

Sean k un cuerpo, $m > 0$ un entero primo con la característica de k, y denotemos por μ_m al grupo de raíces m-ésimas de la unidad en una clausura separable fija k_s de k, equipado con su acción por $G = Gal(k_s|k)$.

Proposición 4.1.1. *Existe un isomorfismo canónico*

$$k^\times / k^{\times m} \xrightarrow{\sim} H^1(k, \mu_m),$$

inducido por enviar $a \in k^\times$ a la clase del 1-cociclo $\sigma \mapsto \sigma(\alpha)\alpha^{-1}$, donde α es una m-ésima raíz de a.

Esta proposición (teoría de Kummer) nos asegura la existencia de una aplicación

$$\partial : k^\times \to H^1(k, \mu_m)$$

sobreyectiva, con núcleo $k^{\times m}$. Tomando producto tensorial n veces, obtenemos la aplicación

$$k^{\times \otimes n} \to H^1(k, \mu_m) \otimes \cdots \otimes H^1(k, \mu_m).$$

A su vez, considerando el *cup-product* obtenemos

$$\partial^n : H^1(k, \mu_m) \otimes \cdots \otimes H^1(k, \mu_m) \to H^n(k, \mu_m^{\otimes n}).$$

Debido a la siguiente proposición, esta aplicación induce otra definida en los K-grupos de Milnor.

Proposición 4.1.2. *Si $a_1, \ldots, a_n \in k^{\times}$ son tales que $a_i + a_j = 1$ para algunos $1 \leq i < j \leq n$, entonces*

$$\partial^n(a_1 \otimes \cdots \otimes a_n) = 0.$$

Definición 4.1.3. La aplicación inducida se denota por

$$h^n_{k,m} : K^M_n(k) \to H^n(k, \mu_m^{\otimes n})$$

y es llamada *símbolo de Galois.*

4.2 El Teorema de Merkurjev-Suslin

La conjetura de Bloch-Kato dice que el símbolo de Galois induce un isomorfismo $K^M_n(k)/m \xrightarrow{\sim} H^n(k, \mu_m^{\otimes n})$, para todo $n \geq 0$, todo cuerpo k y todo m primo con la característica de k. Para $n = 0$, el resultado es trivial. Para $n = 1$, la teoría de Kummer nos da la respuesta. El caso en que m es una potencia de 2 (conocido como conjetura de Milnor) fue probado por Voevodsky en 1996. El caso general fue probado por Rost y Voevodsky en 2008. Un avance importante había sido alcanzado por Merkurjev y Suslin en 1982, el cual enunciamos en esta sección. Previamente mencionaremos algunos resultados necesarios para la prueba del mismo.

Proposición 4.2.1. *Sean $m, n > 0$ enteros con m invertible en k. Asumamos que el símbolo de Galois $h^{n-1}_{k,m}$ es sobreyectivo, y que $k^n_{k,p}$ es biyectivo para todo divisor primo p de m. Entonces el símbolo de Galois $h^n_{k,m}$ es biyectivo.*

Demostración. Proposición 7.5.9, [3].

Proposición 4.2.2. *Asumamos que k es un cuerpo tal que el símbolo de Galois $h^2_{L,p}$ es inyectivo para toda extensión finita $L|k$. Entonces $h^2_{k,p}$ es sobreyectivo.*

Demostración. Proposición 8.5.7, [3].

Proposición 4.2.3. *Sea k un cuerpo que contenga las p-ésimas raíces de la unidad para algún primo p invertible en k, y sean $a, b \in k^\times$. Si $h^2_{k,p}(\{a, b\}) = 0$, entonces $\{a, b\} \in pK^M_2(k)$.*

Demostración. Lema 7.6.3, [3].

Proposición 4.2.4. *Sea k un cuerpo que contenga una p-ésima raíz primitiva de la unidad ω, y sea $K = k(\sqrt[p]{a})$ una extensión de Galois de grado p. El núcleo de la aplicación natural*

$$K^M_2(k)/pK^M_2(k) \to K^M_2(K)/pK^M_2(k)$$

consiste de imágenes de símbolos de la forma $\{a, b\}$ con $b \in k^\times$.

Demostración. Teorema 8.6.1, [3].

Teorema 4.2.5. *(Merkurjev-Suslin) Sean k un cuerpo y $m > 0$ un entero invertible en k. Entonces el símbolo de Galois*

$$h^2_{k,m} : K^M_2(k)/m \to H^2(k, \mu_m^{\otimes 2})$$

es un isomorfismo.

La prueba completa se puede encontrar en [3]. Aquí presentamos un resumen de dicha prueba, citando los resultados del texto mencionado.
En virtud de la Proposición 4.2.1, basta tratar el caso en que $m = p$ es un número primo: si $h^n_{k,p}$ es biyectivo para todo divisor primo p de m, y si $h^{n-1}_{k,m}$ es sobreyectivo, entonces $h^n_{k,m}$ es biyectivo. Como mencionamos anteriormente, es sabido el caso $n = 1$ y por lo tanto la sobreyectividad de $h^1_{k,m}$. Luego, basta probar que $h^2_{k,p}$ es biyectivo para p primo.
Para la sobreyectividad usamos la Proposición 4.2.2: si $h^2_{L,p}$ es inyectiva para toda extensión finita $L|k$, entonces $h^2_{k,p}$ es sobreyectiva. Como k es arbitrario, basta

probar la inyectividad de $h^2_{k,p}$. Este resultado es consecuencia de algunos argumentos presentados en la Sección 8.5, que a su vez se apoyan de manera directa en el Teorema 90 de Hilbert.

Se puede asumir que k posee una raíz p-ésima primitiva de la unidad. Si $L|k$ es una extensión finita de grado primo con p, existe una aplicación inyectiva $\ker(h^2_{k,p}) \hookrightarrow \ker(h^2_{L,p})$. En particular, si $L = k(w)$ con w una raíz p-ésima primitiva de la unidad y $h^2_{L,p}$ es inyectiva, entonces $h^2_{k,p}$ es inyectiva.

Se toma entonces $\alpha = \{a_1, b_1\} + \cdots + \{a_n, b_n\} \in K_2^M(k)$ tal que $\alpha \mod p \in \ker(h^2_{k,p})$. Se demuestra que $\alpha \in pK_2^M(k)$ por inducción sobre n, aplicando la proposición 4.2.3 para el caso $n = 1$ y la proposición 4.2.4 para el caso general. Este último teorema es también consecuencia indirecta del Teorema 90 de Hilbert.

5 CONCLUSIONES

Los principales resultados expuestos en esta tesis, el Teorema 90 de Hilbert para K_2 y el Teorema de Merkurjev-Suslin, fueron publicados en el mismo artículo de 1982, *K-cohomology of Severi-Brauer Varieties and the Norm Residue Homomorphism* (en ruso). Este teorema, como nos cuentan Gille y Szamuely en el prefacio de [3], significó la culminación de la teoría de grupos de Brauer de cuerpos, iniciada en los años 30 por Brauer, Noether, Hasse y Albert, y a la vez el inicio de la teoría de la cohomología motívica, campo a la vanguardia de las investigaciones en geometría algebraica y K-teoría.

A su vez, dicho teorema representó un paso importante en la prueba del teorema más general, el Teorema del Isomorfismo (*Norm Residue Isomorphism Theorem*), conocido también como Conjetura de Bloch-Kato Motívica. Este dice que, para un cuerpo k y un entero m invertible en k, la aplicación

$$\partial^n : K_n^M(k)/m \to H^n(k, \mu_m^{\otimes n})$$

es un isomorfismo. El teorema de Merkurjev-Suslin es el caso $n = 2$ y m arbitrario. Rost en 1986, e independientemente los mismos Merkurjev y Suslin en 1991, probaron el caso $n = 3$, $m = 2$. La conjetura de Milnor se trataba del caso $m = 2$ y n arbitrario, y fue probada por Vladimir Voevodsky en 2000, y fue él mismo quien probó el resultado general en 2008.

BIBLIOGRAFÍA

[1] G. Berhuy, An Introduction to Galois Cohomology and its Applications, Cambridge University Press, 2010.

[2] D. Dummit, R. Foote, Abstract Algebra, John Wiley and Sons, 2004.

[3] P. Gille y T. Szamuely, Central Simple Algebras and Galois Cohomology, Cambridge University Press 2006.

[4] D. R. Grayson, On the K-Theory of Fields, http://www.math.uiuc.edu/ dan/Papers/KTheoryOfFields.pdf

[5] R. Hartshorne, Algebraic Geometry, Springer-Verlag New York, 1977.

[6] T. Y. Lam, Introduction to Quadratic Forms over Fields, American Mathematical Society, 2005.

[7] S. Lang, Algebra, Springer-Verlag New York, 2002.

[8] J. Milnor, Algebraic K-Theory and Quadratic Forms, Invent. Math. 9 (1969/1970), 318-44.

[9] J.P. Serre, Local Fields, Springer-Verlag New York, 1979.

[10] E. Tengan, Central Simple Algebras and the Brauer Group, XVIII Latin American Algebra Colloquium, 2009.

[11] Ch. Weibel, The K-Book, An Introduction to Algebraic K-theory, American Mathematical Society, 2013.