K-TEORÍA DE MILNOR

1. Resumen

La K-teoría de Milnor fue un intento temprano de definir los K-grupos de orden superior para un cuerpo F. Inspirado en el cálculo de $K_2(F)$ a partir de símbolos de Steinberg, Milnor define los grupos de orden superior como los grupos que factorizan todos los posibles símbolos que se pueden definir en F. Presentaremos esta construcción, junto con algunos ejemplos de símbolos y enunciaremos la conjetura de Bloch-Kato, uno de los teoremas más fuertes que invoucran los K-grupos de Milnor.

2. Símbolos en álgebra y aritmética

En esta sección estudiaremos dos ejemplos de símbolos asociados a un cuerpo que aparecen en contextos diferentes y llevan a diferentes aplicaciones. Por un lado, aparece el ejemplo de los símbolos de Steinberg. Milnor definió para un anillo R, el grupo $K_2(R)$ como el centro del grupo de Steinberg de R, $St(R)$. Esta definición cumple con las propiedades deseadas para los K-grupos algebraicos y coincide con el correspondiente grupo en la K-teoría de Quillen. En este caso, el Teorema de Matsumoto (ver [3]) prueba que para R un cuerpo, $K_2(R)$ esta generado por los llamados símbolos de Steinberg. Para cada par de elementos $a, b \in R$ se define un elemento $\{a, b\}$ en $K_2(R)$ y se puede probar que dichos elementos generan todo el grupo sujeto a dos relaciones: el ser multiplicativos en cada coordenada y el ser nulos si $a+b=1$. La simpleza de esta descripción permite calcular el K_2 explícitamente en ciertos casos y probar propiedades en otros. Más importante aun, es un acercamiento tratable al problema de calcular K-grupos, que suele ser bastante dificil.

En un mundo diferente, aunque con características similares, aparecen los símbolos de Hilbert. Dado un cuerpo local F, con ideal maximal $\mathfrak{p}$ y caracteristica residual p, se puede definir para cada n el simbolo de Hilbert de potencia n. El mismo, que dados $a, b \in F^\times$ se notará $\left(\frac{a,b}{\mathfrak{p}}\right)$, es una herramienta útil para resolver el problema de identificar potencias n-ésimas en cuerpos locales y finitos. Más aun, la famosa ley de reciprocidad cuadrática de Gauss, es consecuencia directa de una formula del producto para símbolos de Hilbert. Nuevamente, el símbolo de Hilbert comprende una serie de funciones en dos variables, que son multiplicativas en cada argumento y se anulan siempre que $a+b=1$.

Esta sección pretende introducir estos dos ejemplos de símbolos como motivación para el estudio de los K-grupos de Milnor, por lo que nos tomaremos la libertad de omitir varias demostraciones.

2.1. Símbolos de Steinberg. Sea R un anillo. Para cada $n \in \mathbb{N}$ se define el anillo de transvecciones elementales de $n \times n$, $E_n(R)$ como el anillo generado por las matrices

$$e_{ij}(r) = \mathrm{Id} + r\epsilon_{ij}$$

donde $r \in R$ y ϵ_{ij} es la matriz que vale 1 en el lugar (i, j) y 0 en el resto. La unión de todos estos grupos para $n \in \mathbb{N}$ forma el grupo de transvecciones $E(R)$ de tamaño arbitrario. Los elementos de $E(R)$ satisfacen tres relaciones elementales:

ST1: $e_{ij}(r)e_{ij}(s) = e_{ij}(r+s)$.
ST2: $[e_{ij}(r), e_{kl}(s)] = 1$ si $i \neq l$ y $j \neq k$.
ST3: $[e_{ij}(r), e_{jl}(s)] = e_{il}(rs)$ si $i \neq l$.

Según varía el anillo R el grupo $E(R)$ puede tener relaciones extra. Para medir estas relaciones se define el grupo de Steinberg asociado a R, que notaremos $St(R)$, como el generado libremente por los elementos $x_{ij}(r)$ para $i, j \in \mathbb{N}$ y $r \in R$ sujetos a las mismas relaciones

ST1: $x_{ij}(r)x_{ij}(s) = x_{ij}(r+s)$.

ST2: $[x_{ij}(r), x_{kl}(s)] = 1$ si $i \neq l$ y $j \neq k$.
ST3: $[x_{ij}(r), x_{jl}(s)] = x_{il}(rs)$ si $i \neq l$.

Existe un morfismo $St(R) \to E(R)$ definido por enviar $x_{ij}(r) \mapsto e_{ij}(r)$ y se define el grupo $K_2(R)$ como el núcleo de este morfismo. Es posible ver que la imagen de $St(R)$ en $E(R)$ es el subgrupo de conmutadores $[E(R) : E(R)]$ y esto implica que hay una sucesión exacta:

$$1 \to K_2(R) \to St(R) \to E(R) \to K_1(R) \to 1.$$

Para todo anillo R, el grupo $K_2(R)$ posee una serie de elementos distinguidos llamados símbolos de Steinberg. Daremos su definición y enunciaremos sus propiedades principales. Las mismas pueden seguirse en la sección 12.B de [3].

Definición. *Sea R un anillo y $a, b \in R^\times$. Se definen los siguientes elementos de $St(R)$.*

- $w_{ij}(a) = x_{ij}(a)x_{ji}(a^{-1})x_{ij}(a)$
- $h_{ij}(a) = w_{ij}(a)w_{ij}(-1)$
- $\{a, b\}_{ijk} = [h_{ik}(a), h_{ij}(b)]$

Se tiene el siguiente resultado:

Lema 2.1. *Si $ab = ba$ el elemento $\{a, b\}_{ijk}$ no depende de la elección de i, j o k.*

Demostración. Se trata de las Proposiciones 12.21 y 12.22 de [3]. □

Definición. *Dados $a, b \in R^\times$ tales que $ab = ba$ se define el símbolo de Steinberg $\{a, b\}_R := \{a, b\}_{123}$.*

Los símbolos de Steinberg $\{a, b\}$ son elementos de $K_2(R)$ y se tienen los siguientes resultados importantes.

Teorema 2.2. *Si $R = F$ es un cuerpo, entonces los símbolos de Steinberg generan a $K_2(F)$.*

Demostración. Se trata del Teorema 12.30 de [3]. □

Proposición 2.3. *Si a, b y c son unidades que conmutan en un anillo R, se tiene que:*

1. $\{a, b\} = \{b, a\}^{-1}$
2. $\{ab, c\} = \{a, c\}\{b, c\}$
3. $\{a, bc\} = \{a, b\}\{a, c\}$
4. $\{a, b\} = 1$ *si* $a + b = 1$.

Demostración. Es el Teorema 12.31 de [3]. □

El que probablemente sea el resultado más importante respecto a los símbolos de Steinberg es el Teorema de Matsumoto (Teorema 14.69 de [3]). Lo enunciamos a continuación.

Teorema 2.4. *Si F es un cuerpo, el grupo $K_2(F)$ esta generado libremente por los simbolos de Steinberg $\{a, b\}$ para $a, b \in F^\times$ sujeto solo a las relaciones $2, 3$ y 4 de la Proposición 2.3.*

El Teorema de Matsumoto da una descripción bastante sencilla del grupo $K_2(F)$ para F cuerpo. Más aun, la descripción dada de $K_2(F)$ nos dice que es un grupo universal por el que se factorizan todas las funciones $F^\times \times F^\times \to G$ con G un grupo, que son multiplicativas en cada variable y se anulan en los pares que suman 1. En muchos casos los K-grupos algebraicos resultan dificiles de calcular, sin embargo esta descripción permite decir muchas cosas acerca de varios de ellos. Ilustraremos esto con dos ejemplos, para finalizar esta sección el caso de un cuerpo finito, y más adelante, calcularemos $K_2(\mathbb{Q})$.

Ejemplo: Sea F un cuerpo finito. Entonces $K_2(F) = \{1\}$.

Demostración. Sea $v \in F^\times$ un generador. Bastará ver que para todo $n, m \in \mathbb{N}$ el símbolo $\{v^n, v^m\}$ es 1. Se tiene que $\{v^n, v^m\} = \{v, v\}^{nm}$, por lo que sera suficiente ver que $\{v, v\} = 1$. Por otro lado $\{v, v\} = \{v, v\}^{-1}$ por lo que $\{v, v\} = \pm 1$. Para ver que $\{v, v\} = 1$, mostraremos que tiene una potencia impar igual a 1.

Si $|F| = q$ es par, $\{v,v\}^{q-1} = \left\{v^{q-1}, v\right\} = \{1,v\} = 1$ puesto que $\{1,v\}^2 = \{1,v\}$.

Si $|F| = q$ es impar, la mitad de los elementos de $F^\times$ son cuadrados perfectos y la otra mitad no. Por lo tanto la asignación $x \to 1 - x$ que va de $F^\times - \{1\} \to F^\times - \{1\}$ necesariamente envía un no cuadrado en un no cuadrado. En otras palabras, existen dos números impares n y m tales que $v^n + v^m = 1$. Luego $\{v,v\}^{nm} = \{v^n, v^m\} = 1$.

□

2.2. Símbolos de Hilbert. En un mundo diferente aparecen los símbolos de Hilbert. Si bien se trata de símbolos de cuerpos en el mismo sentido que los símbolos de Steinberg (y por lo tanto se factorizan por el respectivo K_2), la teoría desarrollada alrededor de ellos tiene un sabor mucho más aritmético. Comenzamos con una serie de definiciones básicas sobre cuerpos locales. Un desarrollo más profundo de estos temas se puede encontrar en el capítulo 2 de [4].

Definición. *Un cuerpo local es un cuerpo topológico localmente compacto.*

Todo cuerpo local K admite un valor absoluto $|\cdot|$ que es multiplicativo y satisface la desigualdad triangular. Los cuerpos locales se separan en "arquimedeanos", cuando para todo x existe un n tal que $|nx| > 1$, y "no arquimedeanos" cuando esta propiedad no se cumple. Todo cuerpo arquimedeano es isomorfo a $\mathbb{R}$ o $\mathbb{C}$. Los cuerpos no arquimedeanos aparecen en dos variedades. Los de característica 0 son isomorfos a completaciones de extensiones de $\mathbb{Q}$ respecto a la topología inducida por un ideal primo (son extensiones finitas de $\mathbb{Q}_p$, el cuerpo de numeros p-ádicos) y los de característica positiva son isomorfos al cuerpo de series de Laurent $\mathbb{F}((T))$ para un cuerpo finito $\mathbb{F}$.

Los cuerpos locales no arquimedeanos están equipados con una valuación discreta v que cumple:

- $v(ab) = v(a) + v(b)$.
- $v(a+b) \leq \text{mín}(v(a), v(b))$ con igualdad en caso de que $v(a) \neq v(b)$.

El ejemplo a tener en mente es el de $\mathbb{Q}_p$, en el que $v_p(a)$ es la máxima potencia con la que p divide a a. Para esta valuación se tiene que $|a| = p^{-v_p(a)}$.

Definición. *Un lugar de una extensión $K/\mathbb{Q}$ es o bien una inmersion $K \hookrightarrow \mathbb{C}$ o un ideal primo del anillo de enteros $\mathcal{O}_K$.*

- *Las inmersiones $K \hookrightarrow \mathbb{C}$ se llaman lugares arquimedeanos o infinitos e inducen una topología en K como subespacio de $\mathbb{C}$.*
- *Los ideales primos $\mathfrak{P} \subset \mathcal{O}_K$ se llaman lugares no arquimedeanos o finitos e inducen la topología dada por la valuación $v_{\mathfrak{P}}(a)$ definida como la máxima potencia de $\mathfrak{P}$ que divide al ideal generado por a.*

Dado un lugar v llamamos K_v a la completación de K respecto a la topología correspondiente. Para lugares infinitos, K_v resulta ser un cuerpo local arquimedeano y para los lugares finitos K_v es un cuerpo local no arquimedeano.

Los símbolos de Hilbert son símbolos definidos sobre cuerpos locales K. Sin embargo, la teoría aplica a las extensiones $K/\mathbb{Q}$ finitas, ya que cada una de ellas tiene asociada un cuerpo local por cada primo de su anillo de enteros y cada inmersion en $\mathbb{C}$. Para cada lugar v tenemos la inclusión $K \hookrightarrow K_v$. Es por esto que para cada lugar v y cada par de elementos de un cuerpo global K podemos calcular el simbolo de Hilbert entre a y b relativo a v. Para la definición del símbolo de Hilbert utilizaremos una herramienta importante (y altamente no trivial) de los cuerpos locales. El desarrollo de esta teoría se puede seguir en el capítulo 5 de [4] o en [1] para una versión más constructiva.

Local Class Field Theory: Hay una correspondencia

$$\{\text{Extensiones finitas abelianas de } K\} \longleftrightarrow \left\{\text{Subgrupos cerrados de indice finito de } K^\times\right\}$$

dada por la asignación $L/K \to N_{L/K}(L^\times)$. Más aun, se cumple que si L/K finita entonces $\text{Gal}(L/K)^{ab} \simeq K^\times / N_{L/K}(L^\times)$.

Notación. *Notaremos los morfismos involucrados como:*

- $r_{L/K} : \mathrm{Gal}(L/K)^{ab} \to K^\times / N_{L/K}(L^\times)$.
- $(\quad , L/K) : K^\times \to \mathrm{Gal}(L/K)^{ab}$.

Es decir, dado $a \in K^\times$, notaremos por $(a, L/K)$ al morfismo de $\mathrm{Gal}(L/K)^{ab}$ que le corresponde mediante el isomorfismo $r_{L/K}$.

A partir de ahora, sea $n \in \mathbb{N}$ fijo y K un cuerpo local que contiene a las raices n-esimas de la unidad (que notaremos μ_n). Sea $L = \sqrt[n]{K^\times}$ la máxima extensión abeliana de K de exponente n.

Proposición 2.5. $\mathrm{Gal}(L/K) \simeq K^\times/(K^\times)^n$

Demostración. Por Local Class Field Theory, L corresponde a un subgrupo cerrado $H \subseteq K^\times$ y $\mathrm{Gal}(L/K) \simeq K^\times/H$. Por un lado, como $\mathrm{Gal}(L/K)$ tiene exponente n, debe ser que para todo $a \in K^\times$ se tenga que $a^n \in H$. Esto implica que $(K^\times)^n \subseteq H$. Por otro lado, el cociente $K^\times/(K^\times)^n$ tiene exponente n, por lo que la extensión L' correspondiente a $(K^\times)^n$ debe estar contenida en L. Esto implica que $(K^\times)^n \subseteq H$. □

El otro ingrediente necesario para definir el símbolo de Hilbert es la teoría de Kummer. Definimos la aplicación $\psi : K^\times/(K^\times)^n \to \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)$ como

$$\psi(b)(\sigma) = \frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}.$$

Apelamos al siguiente resultado conocido

Proposición 2.6 (Kummer)**.** *ψ es un isomorfismo.*

Con estas dos herramientas estamos en condiciones de definir el símbolo de Hilbert. Sabemos que existe un pairing no degenerado

$$\mathrm{Gal}(L/K) \times \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \to \mu_n$$

y esto induce el símbolo de Hilbert

$$K^\times \times K^\times \to K^\times/(K^\times)^n \times K^\times/(K^\times)^n \simeq \mathrm{Gal}(L/K) \times \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \to \mu_n.$$

Notaremos $\left(\frac{a,b}{K}\right)$ a la imagen del par (a, b) por el simbolo de Hilbert de K.

Observación. $\left(\frac{a,b}{K}\right)$ es la raíz de la unidad $\frac{(a,K(\sqrt[n]{b})/K)\sqrt[n]{b}}{\sqrt[n]{b}}$.

La siguiente proposición muestra que el símbolo de Hilbert es efectivamente un símbolo en el mismo sentido que los símbolos de Steinberg.

Proposición 2.7. *Sea K un cuerpo local y $a, b \in K$. Vale:*

1. $\left(\frac{a,b}{K}\right)$ *es multiplicativo tanto en a como en b.*
2. $\left(\frac{a,b}{K}\right) = 1$ *si y solo si a es la norma de algun elemento de $K(\sqrt[n]{b})$.*
3. $\left(\frac{a,b}{K}\right) = \left(\frac{b,a}{K}\right)^{-1}$.
4. $\left(\frac{a,1-a}{K}\right) = 1$ *y* $\left(\frac{a,-a}{K}\right) = 1$.
5. *Si* $\left(\frac{a,b}{K}\right) = 1$ *para todo $b \in K^\times$ entonces $a \in (K^\times)^n$.*

Demostración. Los ítems 1 y 2 se siguen directamente de la definición. El ítem 5 es consecuencia de que el pairing entre $\mathrm{Gal}(L/K)$ y $\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)$ es no degenerado. Resta probar 2 y 3. Sea $b \in K^\times$ y $x \in K$ tal que $x^n - b \neq 0$. Sea ξ una raiz n-esima de la unidad y $\beta \in \overline{K}$ tal que $\beta^n = b$, se tiene que:

$$x^n - b = \prod_{i=0}^{n-1}(x - \xi^i \beta).$$

Observemos que el lado derecho de la igualdad es una norma de la extensión $K(\sqrt[n]{b})$ y por lo tanto se tiene que

$$\left(\frac{x^n - b, b}{K}\right) = 1.$$

Poniendo $x = 0$ y $x = 1$ se obtiene 4. Finalmente, para conseguir 3 usamos:

$$\left(\frac{a,b}{K}\right)\left(\frac{b,a}{K}\right) = \left(\frac{a,-a}{K}\right)\left(\frac{a,b}{K}\right)\left(\frac{b,a}{K}\right)\left(\frac{b,-b}{K}\right) = \left(\frac{a,-ab}{K}\right)\left(\frac{a,-ab}{K}\right) = \left(\frac{ab,-ab}{K}\right) = 1$$

$\square$

Esto prueba que el símbolo de Hilbert es efectivamente un símbolo. El resto de esta sección estará dedicado a mostrar como el símbolo de Hilbert es una herramienta para resolver el problema aritmético de saber si un elemento es o no una potencia n-esima en un cuerpo finito y mostrar una generalización de la ley de reciprocidad cuadrática de Gauss. De ahora en adelante, sea $K/\mathbb{Q}$ una extensión finita.

Notación. *Dado un primo $\mathfrak{P}$ en $\mathcal{O}_K$ notaremos al símbolo $\left(\frac{a,b}{K_{\mathfrak{P}}}\right)$ como $\left(\frac{a,b}{\mathfrak{P}}\right)$. Por otro lado, $O_{\mathfrak{P}}$ sera el anillo de enteros de $K_{\mathfrak{P}}$ y q sera el orden de $O_{\mathfrak{P}}/\mathfrak{P}$.*

Sea $u \in O_{\mathfrak{P}}^{\times}$. Sabemos que toda tal unidad u es congruente módulo $\mathfrak{P}$ a una única raíz $q-1$-ésima de la unidad que notaremos $w(u)$. El siguiente resultado da una descripción alternativa del símbolo de Hilbert.

Proposición 2.8. *Si $(n,p) = 1$ y $a, b \in K_{\mathfrak{P}}^{\times}$ se tiene que*

$$\left(\frac{a,b}{\mathfrak{P}}\right) = w((-1)^{\alpha\beta}\frac{b^{\alpha}}{a^{\beta}})^{\frac{q-1}{n}}$$

donde $\alpha = v_{\mathfrak{P}}(a)$ y $\beta = v_{\mathfrak{P}}(b)$.

Demostración. Proposición 3.4 del capítulo 5 de [4]. $\square$

Podemos sacar dos conclusiones simples de la Proposición anterior. Por un lado, si $u_1, u_2 \in O_{\mathfrak{P}}^{\times}$ entonces $\left(\frac{u_1,u_2}{\mathfrak{P}}\right) = 1$. Por otro lado, si $a \in O_{\mathfrak{P}}^{\times}$ y $\pi \in O_{\mathfrak{P}}$ es un elemento de valuación 1 el símbolo:

$$\left(\frac{\pi,a}{\mathfrak{P}}\right) = w(a)^{\frac{q-1}{n}}$$

no depende de π.

Definición. *Sea $a \in O_{\mathfrak{P}}^{\times}$. Definimos el símbolo de Legendre, o símbolo residual de la n-ésima potencia como*

$$\left(\frac{a}{\mathfrak{P}}\right) = \left(\frac{\pi,a}{\mathfrak{P}}\right).$$

Con esta definición, $\left(\frac{a}{\mathfrak{P}}\right)$ es la raiz de la unidad que cumple

$$\left(\frac{a}{\mathfrak{P}}\right) = a^{\frac{q-1}{n}} \pmod{\mathfrak{P}}.$$

Proposición 2.9. *Sea $(n,p) = 1$ y $u \in O_{\mathfrak{P}}^{\times}$. Se tiene que*

$$\left(\frac{a}{\mathfrak{P}}\right) = 1 \Leftrightarrow a \text{ es una potencia } n\text{-ésima en } O_{\mathfrak{P}}/\mathfrak{P}$$

Demostración. Se sigue sencillamente de la definición de $\left(\frac{a}{\mathfrak{P}}\right)$. $\square$

Finalmente, enunciamos la formula del producto para símbolos de Hilbert y la ley de reciprocidad para potencias n-ésimas que se obtiene al pensar los símbolos de Legendre como casos particulares de símbolos de Hilbert.

Teorema 2.10. *Sean $a, b \in K^\times$. Se tiene que:*

$$\prod_{\mathfrak{P}} \left(\frac{a,b}{\mathfrak{P}}\right) = 1$$

Demostración. Se trata del Teorema 8.1 del capítulo 7 de [4]. No daremos una demostración para no desviarnos tanto del tema que estamos tratando. Sin embargo, cabe decir que una vez definidos los śimbolos de Hilbert como en nuestro caso, el resultado es una consecuencia simple de la Teoría de Cuerpos de Clase para el cuerpo K (Class Field Theory). Una demostración en para el caso de $\mathbb{Q}$, que no apela a esta tecnología e involucra el cálculo del $K_2(\mathbb{Q})$ por medio de símbolos de Steinberg se encuentra en la discusión que procede al Corolario 2.31 de [2]. □

Definición. *Dados $a, b \in K^\times$, coprimos entre si y con n, definimos, si $(b) = \prod_{\mathfrak{P}_i} \mathfrak{P}_i^{v_i(b)}$, al símbolo de Jacobi:*

$$\left(\frac{a}{b}\right) = \prod_i \left(\frac{a}{\mathfrak{P}_i}\right)^{v_i(b)}.$$

Con esta ultima definición, vale la siguiente Ley de Reciprocidad.

Teorema 2.11. *Sean a, b coprimos entre si y con n. Entonces se tiene que*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{\mathfrak{P} \mid n\infty} \left(\frac{a,b}{\mathfrak{P}}\right).$$

Demostración. Si $\mathfrak{P} \nmid bn\infty$ se tiene que

$$\left(\frac{b}{\mathfrak{P}}\right)^{v_{\mathfrak{P}}(a)} = \left(\frac{\pi, b}{\mathfrak{P}}\right)^{v_{\mathfrak{P}}(a)} = \left(\frac{\pi^{v_{\mathfrak{P}}(a)}, b}{\mathfrak{P}}\right) = \left(\frac{a,b}{\mathfrak{P}}\right).$$

Puesto que $a = u\pi^{v_{\mathfrak{P}}(a)}$ y u y b son unidades en $K_{\mathfrak{P}}$. Siguiendo esta igualdad se tiene que:

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{\mathfrak{P} \mid b} \left(\frac{a}{\mathfrak{P}}\right)^{v_{\mathfrak{P}}(b)} \prod_{\mathfrak{P} \mid a} \left(\frac{b}{\mathfrak{P}}\right)^{-v_{\mathfrak{P}}(a)} = \prod_{\mathfrak{P} \mid b} \left(\frac{b,a}{\mathfrak{P}}\right) \prod_{\mathfrak{P} \mid a} \left(\frac{a,b}{\mathfrak{P}}\right)^{-1} =$$

$$= \prod_{\mathfrak{P} \mid ab} \left(\frac{b,a}{\mathfrak{P}}\right) = \prod_{\mathfrak{P} \nmid n\infty} \left(\frac{b,a}{\mathfrak{P}}\right) = \prod_{\mathfrak{P} \mid n\infty} \left(\frac{a,b}{\mathfrak{P}}\right).$$

□

Observemos que para $K = \mathbb{Q}$ y $n = 2$ (que es el único n posible, ya que es el único n tal que $\mathbb{Q}$ contiene las raíces n-ésimas de la unidad) se obtiene la formula

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \left(\frac{a,b}{2}\right)\left(\frac{a,b}{\infty}\right).$$

Es posible calcular el símbolo de Hilbert en 2 y en ∞ y comprobar que esta es otra forma de enunciar la ley de reciprocidad cuadrática de Gauss.

3. K-teoría de Milnor

En esta sección definiremos los K-grupos de Milnor y explicaremos su conexión con los ejemplos presentados. En la segunda parte construiremos el símbolo de Galois y enunciaremos la famosa conjetura de Bloch-Kato.

3.1. Los K-grupos de Milnor. Los K-grupos de Milnor fueron un intento temprano de definir la K-teoría de orden superior para un cuerpo F. Inspirado en el calculo de $K_2(F)$ por medio de símbolos de Steinberg, Milnor definio en 1970:

$$K_*^M(F^\times) = T*(F^\times)/(a \otimes (1-a)).$$

Donde $T^*(F^\times)$ es el álgebra tensorial asociada a grupo multiplicativo $F^\times$. Asi definido, cada grupo $K_n^M = (F^\times)^{\otimes n}/I_n$ donde I_n es el ideal generado por los tensores $a_1 \otimes \ldots \otimes a_n$ para los que existen indices $i \neq j$ tales que $a_i + a_j = 1$. En este sentido, $K_n^M(F^\times)$ es el grupo universal que factoriza todos los posibles símbolos de F en n variables. Bajo esta nueva definición, el Teorema de Matsumoto se puede interpretar como la simple igualdad

$$K_2(F) = K_2^M(F).$$

Ya equipados con esta definición, ilustraremos la definición con el ejemplo prometido en la sección 2.1.

Ejemplo (Tate):

$$K_2(\mathbb{Q}) = \{\pm 1\} \oplus \mathbb{F}_3^\times \oplus \mathbb{F}_5^\times \oplus \mathbb{F}_7^\times \oplus \mathbb{F}_{11}^\times \oplus \mathbb{F}_{13}^\times \oplus \mathbb{F}_{17}^\times \oplus \ldots$$

Consideremos los siguientes símbolos en $\mathbb{Q}$:

- Para cada $p \geq 3$ primo definimos

$$\lambda_p(a,b) = (-1)^{v_p(a)v_p(b)} \frac{a^{v_p(b)}}{b^{v_p(a)}}$$

- Para $p = 2$ definimos

$$\lambda_2(a,b) = \left(\frac{a,b}{\mathbb{Q}_2}\right)$$

Se puede chequear que todos estos son símbolos y por lo tanto cada uno de ellos induce un morfismo $\overline{\lambda_p} : K_2^M(\mathbb{Q}) \to R_p$ donde $R_p = \mathbb{F}_p^\times$ si $p \geq 3$ y $R_2 = \{\pm 1\}$. Afirmamos que el $\prod_p \overline{\lambda_p}$ es un isomorfismo.

Para probar esto construiremos los siguientes subgrupos de $K_2(\mathbb{Q})$, para cada $n \in \mathbb{N}$ definimos Λ_n como el grupo generado por todos los símbolos $\{a,b\}$ con a y b unidades o primos menores o iguales que n. Notemos que los grupos Λ_n solo pueden cambiar en los subíndices n primos y que $K_2(\mathbb{Q}) = \cup_n \Lambda_n$.

Probaremos por inducción que $\Lambda_p \simeq \prod_{q<p} R_q$ para todo $p \geq 2$:

El caso base, para $p = 1$ y $p = 2$, consiste en ver que $\Lambda_1 = \Lambda_2 \simeq \{\pm 1\}$. Para Λ_1, el único posible elemento no trivial es $\{-1,-1\}$ ya que $\{a,1\} = \{a,1\}^2$, implicando que $\{a,1\} = 1$ para todo $a \in \mathbb{Q}$. Efectivamente $\{-1,-1\}$ es no trivial, ya que $\lambda_2(-1,-1) = \left(\frac{-1,-1}{2}\right) = -1$ (se puede probar que -1 no es una norma de $\mathbb{Q}_2(i)$) y es claro que tiene orden 2.

Para Λ_2, se tiene que $\{2,-2\} = 1$ (en virtud de que $1 = \{1/a, 1-1/a\} = \left\{a, \frac{1-a}{-a}\right\}^{-1} = \{a, 1-a\}^{-1}\{a,-a\}$) y luego

$$\{2,2\} = \{2,-1\}\{2,-2\} = \{2,-1\} = 1.$$

Esto prueba el caso inicial. Para el paso inductivo, probaremos que para todo p primo se tiene un isomorfismo $\phi_p : \mathbb{F}_p^\times \to \Lambda_p/\Lambda_{p-1}$ inverso a $\overline{\lambda_p}$.

Definimos $\phi_p(x) = \{x,p\}$. Debemos probar que ϕ_p esta bien definido y es morfismo. Para eso, sean $0 < x,y,z < p$, debemos probar que siempre que $xy = z \pmod{p}$ se tiene que

$$\{x,p\}\{y,p\} = \{z,p\} \pmod{\Lambda_{p-1}}.$$

Sea $xy = z + pk$, claramente $0 \leq k < p$ y si $k = 0$ el resultado es automático. Caso contrario se tiene que

$$1 = \left\{\frac{kp}{xy}, 1 - \frac{kp}{xy}\right\} = \left\{\frac{kp}{xy}, \frac{z}{xy}\right\} = \{p,z\}\{p,xy\}^{-1}\{k,z\}\{k,xy\}^{-1}\{xy,z\}^{-1}\{xy,xy\}.$$

Observemos que los últimos 4 símbolos del último término de la igualdad pertenecen a Λ_{p-1}, puesto que sus entradas son producto de numeros menores a p. Esto prueba que ϕ_p es morfismo.

Para ver que es isomorfismo, observemos que $\overline{\lambda_p}$ se anula en Λ_{p-1} y $\overline{\lambda_p}(\phi_p(x)) = \overline{\lambda_p}(x,p) = x$, por lo que ϕ_p es monomorfismo. Por otro lado, en virtud de que $\{p,p\} = \{-1,p\}$, se tiene que los símbolos $\{a,p\}$ para a coprimo con p general Λ_p/Λ_{p-1}, por lo que ϕ_p es sobreyectiva. Esto prueba que ϕ_p es isomorfismo y concluye el cálculo de $K_2(\mathbb{Q})$.

3.2. El símbolo de Galois. En esta sección construiremos el último símbolo de este trabajo. Se trata de el símbolo de Galois, que da una conexión entre la K-teoría de Milnor y ciertos grupos de cohomología de Galois.

Notación. *Para un cuerpo F, notamos por G_F a su grupo de Galois absoluto* $\mathrm{Gal}(\overline{F}/F)$.

Sea F un cuerpo y $N \in \mathbb{N}$ coprimo con la característica de F. Consideremos la sucesión exacta corta dada por elevar a la N

$$1 \longrightarrow \mu_n \longrightarrow \overline{F}^\times \xrightarrow{N} \overline{F}^\times \longrightarrow 1.$$

Observemos que todos los terminos de la sucesión son G_F-módulos, por lo que podemos tomar cohomología y obtenemos la sucesión exacta larga

$$\ldots \longrightarrow \mathrm{H}^0(G_F, \overline{F}^\times) \longrightarrow \mathrm{H}^0(G_F, \overline{F}^\times) \xrightarrow{\delta_F} \mathrm{H}^1(G_F, \mu_n) \longrightarrow \mathrm{H}^1(G_F, \overline{F}^\times) \longrightarrow \ldots$$

Sabemos que $\mathrm{H}^0(G_F, \overline{F}^\times) = F^\times$ y el Teorema 90 de Hilbert nos dice que $\mathrm{H}^1(G_F, \overline{F}^\times) = 0$. Por lo tanto, sabemos que el morfismo $\delta_F : F^\times \to \mathrm{H}^1(G_F, \mu_N)$ es sobreyectivo y tiene núcleo igual a $(F^\times)^N$.

Por otro lado, el cup product nos da un morfismo

$$\mathrm{H}^1(G_F, \mu_N) \times \ldots \times \mathrm{H}^1(G_F, \mu_N) \longrightarrow \mathrm{H}^n(G_F, \mu_N^{\otimes n}).$$

Componiendo ambos morfismos obtenemos el símbolo de Galois.

Definición. *Se define el simbolo de Galois*

$$F^\times \times \ldots \times F^\times \to \mathrm{H}^n(G_F, \mu_N^{\otimes n})$$

como $(a_1, \ldots, a_n)_F = \delta_F(a_1) \cup \ldots \cup \delta_F(a_n)$.

Observación. Observemos que como grupos abelianos μ_N y $\mu_N^{\otimes n}$ son isomorfos, pero la acción de G_F es diferente. Si χ es el caracter por el que G_F actúa en μ_N entonces la accion en $\mu_N^{\otimes n}$ esta dada por χ^n.

Debemos probar que el símbolo de Galois es efectivamente un símbolo, y por lo tanto se tiene la siguiente proposición.

Proposición 3.1. *El símbolo de Galois induce un morfismo*

$$K_n^M(F) \to \mathrm{H}^n(G_F, \mu_N^{\otimes n})$$

Demostración. Para probar que hay un morfismo debemos probar que el símbolo de Galois es multiplicativo en cada coordenada y se anula siempre que haya dos coordenadas que sumen 1. La multiplicatividad es inmediata de la definición. Para probar que se anula siempre que haya coordenadas $i \neq j$ con $a_i + a_j = 1$, podemos asumir que $i = 1$, $j = 2$ y $n = 2$, en virtud de que $(a_1, a_2, a_3, \ldots, a_n)_F = (a_1, a_2)_F \cup (a_3, \ldots, a_n)_F$.

Sea $n = 2$ y $a \in F^\times$, $a \neq 1$. Queremos probar que $(a, 1-a)_F = 1$.

Consideremos la factorización $X^n - a = \prod_i f_i(x)$ con f_i mónicos e irreducibles en $F[X]$. Para cada i, sea a_i una raíz de f_i y $F_i = F(a_i)$. Se tiene que

$$1 - a = \prod_i f_i(1) = \prod_i N_{F_i/F}(1 - a_i).$$

Luego, obtenemos que $(1-a, a)_F = \prod_i (N_{F_i/F}(1-a_i), a)_F$.

Por otro lado, tenemos para cada F_i tenemos que $G_{F_i} \subseteq G_F$ y morfismos de restricción y correstricción entre los grupos de cohomología para G_F y G_{F_i}. Se tienen las siguientes dos propiedades:

- El morfismo $F_i^\times \simeq \mathrm{H}^0(G_{F_i}, \overline{F}^\times) \xrightarrow{cor} \mathrm{H}^0(G_F, \bar{(}F)^\times) \simeq F^\times$ es la norma $N_{F_i/F}$. Y el morfismo correspondiente a la restricción es la inclusión $F^\times \subseteq F_i^\times$
- Restricción y correstricción conmutan con los morfismos de las sucesiones exactas largas de cohomología y son compatibles con el cup product del siguiente modo:
$$cor(a \cup res(b)) = cor(a) \cup b.$$

Usando ambas propiedades se tiene que:

$$\begin{gathered}(N_{F_i/F}(1-a_i), a)_F = \delta_F(cor(1-a_i)) \cup \delta_F(a) = cor(\delta_{F_i}(1-a_i)) \cup \delta_F(a) = \\ = cor(\delta_{F_i}(1-a_i) \cup res(\delta_F(a))) = cor(\delta_{F_i}(1-a_i) \cup \delta_{F_i}(res(a))) = cor((1-a_i, a)_{F_i}) = \\ = cor((1-a_i, a_i^N)_{F_i}) = cor((1-a_i, a_i)_{F_i}^N) = cor(1) = 1.\end{gathered}$$

Esto prueba que el símbolo de Galois es efectivamente un símbolo y por lo tanto se factoriza por $K_n^M(F)$. □

3.3. La conjetura de Bloch-Kato. Terminamos este trabajo enunciando la conjetura de Bloch-Kato.

Teorema 3.2 (Conjetura de Bloch-Kato)**.** *Si $N \in \mathbb{N}$ es coprimo con la característica de F, el morfismo*
$$h_F : K_n^M(F)/NK_n^M(F) \longrightarrow \mathrm{H}^n(G_F, \mu_N^{\otimes n})$$
inducido por el símbolo de Galois, es un isomorfismo.

Demostración. La conjetura fue probada para $N = 2$ por Voevodsky en 1995 (conocida como conjetura de Milnor en ese caso particular). En el 2003, Voevodsky publicó un trabajo en el que presentaba una prueba para la conjetura en total generalidad, pero omitía la prueba de tres resultados. Dos de esos tres resultados fueron probados en los años siguientes, pero el primero de ellos fue probado falso. Años más tarde, Weibel dio con un argumento para solucionar el problema de la prueba de Voevodsky y en 2009 publicó un trabajo que contiene un resumen de las ideas de Voevodsky junto con la demostración completa de las conjeturas. □

Bibliografía

[1] M. Hazewinkel, *Local Class Field Theory is easy*, Advances in Mathematics, Vol. 18, pp. 148-181. 1975.
[2] F. Lemmermeyer, *Reciprocity Laws, From Euler to Eisenstein*, Springer, 2000.
[3] B.A. Magurn, *An algebraic introduction to K-theory*, Cambridge University Press, 2002.
[4] J. Neukirch, *Algebraic Number Theory.* Springer, 1999.