3-variedades hiperbólicas aritméticas: 1
Álgebras de cuaterniones y sus órdenes

Benjamin Linowitz

Oberlin College

Teorema (Hamilton, 1843)

El $\mathbb{R}$-álgebra $\mathbb{H}$ con base $\{1, i, j, ij\}$ que satisface las relaciones

$$i^2 = -1 \qquad j^2 = -1 \qquad ij = -ji$$

es un álgebra de división de dimensión 4.

Sea k un cuerpo de característica distinta que 2.

Definición

Un **álgebra de cuaterniones** sobre k es un álgebra con base $\{1, i, j, ij\}$ que satisface las relaciones

$$i^2 = a, \qquad j^2 = b, \qquad ij = -ji,$$

para algún $a, b \in k^*$.

Denotaremos esta álgebra de cuaterniones por su *símbolo de Hilbert* $\left(\frac{a,b}{k}\right)$.

Ejemplo: $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$

Sea A un álgebra sobre k.

A es **simple** si no tiene ideales bilaterales no triviales.

A es **central** si un elemento $x \in A$ conmuta con todos los elementos de A si y sólo si $x \in k$.

Ejemplo: El álgebra $\mathrm{M}_2(k)$ siempre es simple central.

Ejemplo: El $\mathbb{R}$-álgebra $\mathbb{C}$ es simple pero no es central.

Dos resultados básicos sobre las álgebras de cuaterniones son los siguientes:

Teorema

El álgebra de cuaterniones $\left(\frac{a,b}{k}\right)$ *es un álgebra simple central de dimensión* 4. *Recíprocamente, si* A *es un álgebra simple central de dimensión* 4 *sobre* k *entonces existen* $a, b \in k^*$ *tales que* $A \cong \left(\frac{a,b}{k}\right)$.

Teorema (Teorema de Estructura de Wedderburn)

Sea A *un álgebra de cuaterniones sobre un cuerpo* k. *Si* A *no es un álgebra de división entonces* $A \cong \mathrm{M}_2(k)$.

Si bien dos elementos $a, b \in k^*$ determinan un álgebra $\left(\frac{a,b}{k}\right)$, un álgebra de cuaterniones A dada no determina unívocamente estos elementos a, b.

Por ejemplo, podemos multiplicar a o b por cuadrados sin cambiar la clase de isomorfismo de $\left(\frac{a,b}{k}\right)$.

Proposición

Si $a, b, x, y \in k^*$ *entonces*

$$\left(\frac{a, b}{k}\right) \cong \left(\frac{ax^2, by^2}{k}\right).$$

Demostración. Sean $\{1, i, j, ij\}$ y $\{1, i', j', i'j'\}$ bases para $\left(\frac{a,b}{k}\right)$ y $\left(\frac{ax^2,by^2}{k}\right)$ respectivamente, y sea

$$\phi : \left(\frac{ax^2, by^2}{k}\right) \to \left(\frac{a, b}{k}\right)$$

el homomorfismo obtenido al definir $\phi(1) = 1$, $\phi(i') = xi$, $\phi(j') = yj$, y $\phi(i'j') = xyij$.

La imagen de ϕ es la k-subálgebra de $\left(\frac{a,b}{k}\right)$ con base $\{1, xi, yj, xyij\}$. Como esta subálgebra tiene dimensión cuatro sobre k, debe coincidir con $\left(\frac{a,b}{k}\right)$. Por eso, ϕ es suryectiva.

Cualquier homomorfismo suryectivo entre k-álgebras de la misma dimensión es un isomorfismo, por lo que la proposición sigue. □

De manera similar, tenemos:

Ejercicio

Las álgebras de cuaterniones $\left(\frac{1,b}{k}\right)$ y $\mathrm{M}_2(k)$ son isomorfas para cualquier $b \in k^*$.

(La prueba está dado en las notas.)

Álgebras de cuaterniones sobre los números complejos

Sólo hay un álgebra de cuaterniones sobre $\mathbb{C}$: $\mathrm{M}_2(\mathbb{C})$.

Teorema

Si A es un álgebra de cuaterniones sobre $\mathbb{C}$ entonces $A \cong \mathrm{M}_2(\mathbb{C})$.

Demostración. El teorema fundamental del álgebra implica que todo elemento de $\mathbb{C}^*$ es un cuadrado, entonces $A \cong \left(\frac{1,1}{\mathbb{C}}\right)$ por la proposición. Esta última álgebra de cuaterniones es isomorfa a $\mathrm{M}_2(\mathbb{C})$ por el ejercicio. □

Demostración 2.

Sea A un álgebra de división sobre $\mathbb{C}$. Mostraremos que $A = \mathbb{C}$. Sea $x \in A$ y p el polinomio minimal de x. El teorema fundamental del álgebra implica que todos los factores irreducibles de p sobre $\mathbb{C}$ son lineales. Por eso, existe $z \in \mathbb{C}^*$ tal que $z - x = 0$. Entonces $x = z \in \mathbb{C}$ y $A = \mathbb{C}$. El teorema ahora sigue del teorema de estructura de Wedderburn. □

Álgebras de cuaterniones sobre los números reales

La estructura de las álgebras de cuaterniones sobre $\mathbb{R}$ es más complicada que sobre $\mathbb{C}$. Pero sólo un poquito.

Teorema

Si A es un álgebra de cuaterniones sobre $\mathbb{R}$ entonces $A \cong \mathrm{M}_2(\mathbb{R})$ ó $A \cong \mathbb{H}$.

Demostración. La proposición implica que A es isomorfa a una de las siguientes tres álgebras de cuaterniones: $\left(\frac{-1,-1}{\mathbb{R}}\right)$, $\left(\frac{1,-1}{\mathbb{R}}\right)$ o $\left(\frac{1,1}{\mathbb{R}}\right)$. La primera de estas álgebras es isomorfa a $\mathbb{H}$ por definición, mientras que la segunda y la tercera son isomorfas a $\mathrm{M}_2(\mathbb{R})$ por el ejercicio. □

Álgebras de cuaterniones sobre cuerpos p-ádicos

Sea k un cuerpo p-ádico con uniformizador fijo π.

Como ocurrió en el caso sobre $\mathbb{R}$, hay precisamente dos clases de isomorfismos de álgebras de cuaterniones sobre k.

Teorema

La k-álgebra $\left(\frac{u,\pi}{k}\right)$ es la única álgebra de cuaterniones de división sobre k, donde $k(\sqrt{u})$ es la única extensión cuadrática no ramificada de k.

Álgebras de cuaterniones sobre cuerpos de números

Sea k un cuerpo de números y $\left(\frac{a,b}{k}\right)$ un álgebra de cuaterniones.

Si K es un cuerpo que contiene a k entonces podemos obtener una K-álgebra de cuaterniones de $\left(\frac{a,b}{k}\right)$ por extensión de escalares:

$$\left(\frac{a,b}{k}\right) \otimes_k K \cong \left(\frac{a,b}{K}\right).$$

Normalmente se elige como K la completación de k (i.e., $\mathbb{C}, \mathbb{R}$ o un cuerpo p-ádico $k_{\mathfrak{p}}$ para algún primo $\mathfrak{p}$ de k) y se estudia el álgebra sobre K obtenida por extensión de escalares.

Ejemplo

Consideramos el álgebra de cuaterniones $\left(\frac{-1,-1}{\mathbb{Q}}\right)$. Cuando extendemos escalares a $\mathbb{R}$ obtenemos $\mathbb{H}$, que es un álgebra de división. Esto implica que $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ es un álgebra de división también.

Un hecho interesante (¡e importante!) en la teoría de las álgebras de cuaterniones sobre cuerpos de números es que a diferencia de lo que sucede sobre $\mathbb{R}$, no hay una única álgebra de división sobre un cuerpo de números. De hecho, sobre todo cuerpo de números ¡hay infinitas clases de isomorfismos de álgebras de cuaterniones!

Definición

Sea k un cuerpo de números, v un lugar de k y sea k_v la correspondiente completación de k. Decimos que un álgebra de cuaterniones A sobre k es **ramificada en** v si $A \otimes_k k_v$ es un álgebra de división. Si no, decimos que A **se parte en** v.

Notar que si $A = \mathrm{M}_2(k)$ entonces $A \otimes_k k_v \cong \mathrm{M}_2(k_v)$ para todo v. En particular, todo lugar de k se parte en $\mathrm{M}_2(k)$.

Recordar que toda álgebra de cuaterniones sobre k se parte en todos los lugares complejos. Entonces sólo los lugares reales o p-ádicos podrían ramificar.

Supongamos ahora que k tiene r_1 lugares reales y r_2 lugares complejos.

Denotamos por S_∞ el conjunto de lugares arquimedeanos de k.

$$\begin{aligned} A \otimes_{\mathbb{Q}} \mathbb{R} &\cong \bigoplus_{v \in S_\infty} A \otimes_k k_v \\ &\cong \mathrm{M}_2(\mathbb{C})^{r_2} \times \bigoplus_{\sigma : k \hookrightarrow \mathbb{R}} A \otimes_\sigma k_v \\ &\cong \mathrm{M}_2(\mathbb{C})^{r_2} \times \mathrm{M}_2(\mathbb{R})^{s} \times \mathbb{H}^{r_1 - s}, \end{aligned}$$

donde s es el número de lugares reales de k en los que A se parte.

Veremos que las 3-variedades hiperbólicas aritméticas se construyen a partir de las álgebras de cuaterniones en que $r_2 = 1$ y $s = 0$.

Sea $\mathrm{Ram}(A)$ el conjunto de lugares de k (pueden ser finitos o infinitos) en que A es ramificado.

Teorema (Clasificación de Álgebras de Cuaterniones sobre cuerpos de números)

Sea k un cuerpo de números. Si A es un álgebra de cuaterniones sobre k entonces $\mathrm{Ram}(A)$ es finito y de cardinalidad par. Recíprocamente, dado cualquier conjunto finito S de lugares (finitos o infinitos) de k con cardinalidad par, existe una única álgebra de cuaterniones A sobre k tal que $\mathrm{Ram}(A) = S$.

Corolario

Si k es un cuerpo de números y A, A' son álgebras de cuaterniones sobre k entonces $A \cong A'$ si y sólo si $\mathrm{Ram}(A) = \mathrm{Ram}(A')$.

Notar que el teorema implica que hay infinitas clases de isomorfismos de álgebras de cuaterniones de división sobre todo cuerpo de números.

Además, el teorema implica que podemos contarlos de acuerdo con su discriminante

$$\prod_{\mathfrak{p} \in \mathrm{Ram}(A)} N(\mathfrak{p}).$$

Por ejemplo, sobre $\mathbb{Q}$, esto es equivalente a contar enteros libres de cuadrados con un número par (o impar) de factores primos.

(Se puede contar estos números usando el teorema de los números primos.)

Órdenes en álgebras de cuaterniones

Sea R un dominio de Dedekind con cuerpo cociente K, y A un álgebra de cuaterniones sobre K.

Definición

Un elemento $\alpha \in A$ es **integral** con respecto a R si su polinomio característico (reducido) $x^2 - \mathrm{tr}(\alpha)x + n(\alpha)$ tiene coeficientes en R. Llamamos a $\mathrm{tr}(\alpha)$ la **traza** (reducida) de α y a $n(\alpha)$ la **norma** (reducida) de α.

Recordar que el conjunto de todos los elementos integrales de un cuerpo de números forman un anillo (y muy importante para lo que sigue, un $\mathbb{Z}$-módulo finitamente generado). Sin embargo, esto no es cierto en el caso de álgebra de cuaterniones. Considerar los siguientes dos elementos de $\mathrm{M}_2(\mathbb{Q})$:

$$A = \begin{pmatrix} \frac{5}{4} & -\frac{1}{8} \\ \frac{1}{2} & \frac{3}{4} \end{pmatrix}, \qquad B = \begin{pmatrix} \frac{11}{6} & \frac{1}{2} \\ \frac{5}{18} & \frac{7}{6} \end{pmatrix}.$$

Los polinomios característicos de A y B son $p_A(x) = x^2 - 2x + 1$ y $p_B(x) = x^2 - 3x + 2$. Entonces A y B son integrales (con respecto a $\mathbb{Z}$). Sin embargo, ni $A + B$ ni AB son integrales; sus polinomios característicos son $p_{A+B}(x) = x^2 - 5x + \frac{809}{144}$ y $p_{AB}(x) = x^2 - \frac{487}{144}x + 2$.

Definición

Sea V un espacio vectorial sobre K. Un R-**retículo** en V es un R-módulo finitamente generado contenido en V. Un R-retículo L se dice **completo** si $L \otimes_R K \cong V$.

Definición

Un **orden** $\mathcal{O}$ en A es un R-retículo completo en A que es también un subanillo de A. Un **orden maximal** es un orden en A que es maximal con respecto a la inclusión.

Ejemplos:

- El anillo $\mathrm{M}_2(R)$ es siempre un orden de $\mathrm{M}_2(K)$.
- Supongamos que $A = \left(\frac{a,b}{K}\right)$, donde a, b son elementos integrales de K. Entonces $R[1, i, j, ij]$ es un orden de A.

Una caracterización importante de los órdenes es la siguiente.

Proposición

$\mathcal{O}$ es un orden en A si y sólo si $\mathcal{O}$ es un anillo de elementos integrales en A que contiene a R y satisface $\mathcal{O} \otimes_R K = A$.

Lema

El orden $\mathrm{M}_2(R)$ *es un orden maximal de* $\mathrm{M}_2(K)$.

Demostración.
Si $\mathrm{M}_2(R)$ no es maximal, entonces sea $\mathcal{O}$ un orden maximal que contiene a $\mathrm{M}_2(R)$ y algún elemento $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ con al menos uno de los x, y, z, w que no pertenezca a R. Sumando y multiplicando elementos de $\mathrm{M}_2(R)$ podemos conseguir un elemento $\alpha \in \mathcal{O}$ de la forma $\alpha = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ con $a \notin R$. Tal elemento claramente no es integral, lo cual es una contradicción. □

Proposición

Si $\alpha \in A$ es integral entonces α está contenido en un orden maximal de A.

Demostración. Si $\alpha \in R$ entonces α está en *todo* orden de A. Podemos asumir entonces que $\alpha \notin R$. En tal caso, $K(\alpha)$ es una extensión cuadrática de K que está contenida en A. Sea $\beta \in A^*$ tal que $\beta\alpha\beta^{-1} = \overline{\alpha}$. La existencia de tal elemento es debida al Teorema de Skolem–Noether y podemos tomar β integral simplemente limpiando denominadores. El R-módulo generado por α y β es $R + R\alpha + R\beta + R\alpha\beta$ y es claramente un orden de A. Este orden podría no ser maximal, pero todo orden está contenido en un orden maximal (por el Lema de Zorn). □

Números de tipo

Hemos visto que el conjunto de todos los elementos integrales en un álgebra de cuaterniones no es un orden.

Debido a esto, debemos estudiar *tipos* de órdenes.

Supongamos que $\mathcal{O}_1$ y $\mathcal{O}_2$ son órdenes en A que son isomorfos via algún isomorfismo $f : \mathcal{O}_1 \to \mathcal{O}_2$.

Por extensión de escalares, la función f induce un isomorfismo $F : \mathcal{O}_1 \otimes_R K \to \mathcal{O}_2 \otimes_R K$.

$\mathcal{O}_1$ y $\mathcal{O}_2$ son órdenes, entonces $\mathcal{O}_1 \otimes_R K \cong A \cong \mathcal{O}_2 \otimes_R K$, y F es un automorfismo de A que está dado por conjugación por el Teorema de Skolem–Noether.

En particular, $\mathcal{O}_2 = a\mathcal{O}_1 a^{-1}$ por algún $a \in A^*$.

Concluimos que en un álgebra de cuaterniones, dos órdenes son isomorfos si y sólo si son conjugados.

Definición

El **número de tipo** de un álgebra de cuaterniones es el número de clases de conjugación de órdenes maximales.

El número de tipo de un álgebra de cuaterniones sobre un cuerpo de números es de algún modo una reminiscencia del número de clases de un cuerpo de números:

- es siempre finito (lo cual a priori no es obvio), y
- puede ser arbitrariamente grande.

Además, cuando A es no ramificado en un primo arquimedeano de K, el número de tipo es siempre una potencia de 2.

Sea k un cuerpo de números y A/k un álgebra de cuaterniones que cumple que $A \otimes_{\mathbb{Q}} \mathbb{R} \ncong \mathbb{H}^{[k:\mathbb{Q}]}$.

Sea k_A la extensión abeliana maximal de k que tiene exponente 2, es no ramificada fuera de los lugares reales en $\mathrm{Ram}(A)$, y en la que todo primo finito de $\mathrm{Ram}(A)$ se parte completamente.

Teorema (L., 2012)

Las clases de conjugación de órdenes maximales en A están en correspondencia uno a uno con los elementos de $\mathrm{Gal}(k_A/k)$.

Corolario

Sea h el número de clases de ideales en el sentido de equivalencia estricto. Si h es impar entonces todos los órdenes maximales de A son conjugados (i.e., el número de tipo de A es 1).

Ejemplo

Sea $k = \mathbb{Q}(\sqrt{-10})$. Consideramos el álgebra de cuaterniones $A = \left(\frac{-1,-3}{k}\right)$. Veremos que el número de tipo de A es 2 y calcularemos (usando MAGMA) los conjuntos generadores para los representantes de las dos clases de conjugación de órdenes maximales de A (considerados como módulos sobre $\mathcal{O}_k$).

```
> k<t>:=QuadraticField(-10);
> t^2;
-10
> A<i,j,ij>:=QuaternionAlgebra<k|-1,-3>;
> C:=ConjugacyClasses(MaximalOrder(A));
> #C;
2
IsConjugate(C[1],C[2]);
false
> Generators(C[1]);
[ 1, i, 1/2*i + 1/2*j, 1/2 + 1/2*t*i + 1/6*t*j +
1/6*ij ]
> Generators(C[2]);
[ 1, 2*i, 3*t*i, 1 + 1/2*i + 1/2*j, 1/2*(t + 2) +
1/4*(t + 2)*i + 1/4*(t + 2)*j, 1/2*(t + 1) + 1/4*(t +
4)*i - 1/12*t*j + 1/6*ij ]
```