FORMAS MODULARES CUATERNIÓNICAS

GONZALO TORNARÍA

1. Álgebras de cuaterniones

Sea F un cuerpo de característica $\neq 2$. Dados $a, b \in F^\times = F - \{0\}$ construimos un álgebra sobre F con base $\{1, i, j, k\}$, donde la multiplicación está dada por

$$i^2 = a, \quad j^2 = b, \quad \text{y} \quad k = ij = -ji\,.$$

La tabla completa de la multiplicación puede obtenerse a partir de éstas relaciones. Por ejemplo $k^2 = ijij = i(-ij)j = -i^2 j^2 = -ab$. A esta álgebra la denotaremos $(a, b)_F$ y diremos que es un *álgebra de cuaterniones*.

Esta construcción es una generalización del álgebra de *cuaterniones de Hamilton*, que es $\mathbb{H} = (-1, -1)_{\mathbb{R}}$. Para $x = x_0 + x_1\, i + x_2\, j + x_3\, k \in \mathbb{H}$ definimos $x^\star = x_0 - x_1\, i - x_2\, j - x_3\, k$ y la norma $\nu(x) = x\, x^\star = x_0^2 + x_1^2 + x_2^2 + x_3^2$. Como $\nu(x) \in \mathbb{R}^\times$ para $x \neq 0$ deducimos que $\mathbb{H}$ es un álgebra de división.

En general, un álgebra de cuaterniones no necesariamente es un álgebra de división:

Proposición 1.1. *Si a es un cuadrado en $F^\times$, entonces $(a, b)_F \cong M_2(F)$.*

Demostración. Si $a = \alpha^2$ con $\alpha \in F^\times$, podemos definir un homomorfismo de álgebras $\varphi : (a, b)_F \to M_2(F)$ por

$$\varphi(i) = \left(\begin{smallmatrix} \alpha & \\ & -\alpha \end{smallmatrix}\right), \quad \varphi(j) = \left(\begin{smallmatrix} & 1 \\ b & \end{smallmatrix}\right), \quad \varphi(k) = \left(\begin{smallmatrix} & \alpha \\ -b\alpha & \end{smallmatrix}\right).$$

Es fácil verificar que cumple las relaciones, y como $\{\varphi(1), \varphi(i), \varphi(j), \varphi(k)\}$ es linealmente independiente sobre F (pues $\alpha \neq -\alpha$) se sigue que φ es un isomorfismo. □

Cuando a no es un cuadrado en F, podemos considerar el cuerpo $K = F(\sqrt{a})$ y resulta que $(a, b)_F$ es una subálgebra de $(a, b)_K \cong M_2(K)$. Denotemos σ al automorfismo no trivial de K/F, entonces podemos describir explícitamente $(a, b)_F$ como

$$(a, b)_F \cong \left\{ \left(\begin{smallmatrix} u & v \\ bv^\sigma & u^\sigma \end{smallmatrix}\right) \,:\, u, v \in K \right\}.$$

Notemos que $(a, b)_K$ se obtiene por *extensión de escalares* a partir de $(a, b)_F$, es decir que $(a, b)_K = K \otimes (a, b)_F$.

Proposición 1.2. *El álgebra $(a, b)_F$ es un álgebra central simple sobre F.*

Demostración. Si a es un cuadrado, entonces $(a, b)_F \cong M_2(F)$ que se sabe es central y simple. Si a no es un cuadrado, podemos considerar el cuerpo $K = F(\sqrt{a})$ como arriba. Como $(a, b)_F \otimes K \cong M_2(K)$ es un álgebra central y simple sobre K, se sigue fácilmente que $(a, b)_F$ es un álgebra central y simple sobre F. □

Corolario 1.3. *O bien $(a, b)_F$ es un álgebra de división, o bien $(a, b)_F \cong M_2(F)$.*

Demostración. Se sigue de la clasificación de las álgebras centrales simples. □

Se puede probar que si D es un álgebra central simple de dimensión 4 sobre un cuerpo F de característica $\neq 2$ entonces $D \cong (a,b)_F$ para algunos $a, b \in F^\times$. Por eso habitualmente se define un álgebra de cuaterniones como un álgebra central simple de dimensión 4. Esta definición es adecuada incluso en característica 2.

Veremos ahora cómo definir la norma, lo que nos permitirá caracterizar las álgebras de cuaterniones de división. Un álgebra de cuaterniones $D = (a,b)_F$ posee una *involución canónica* $\star : D \to D$ que definimos, para $x = x_0 + x_1\, i + x_2\, j + x_3\, k \in D$, como

$$x^\star = x_0 - x_1\, i - x_2\, j - x_3\, k\,.$$

Notemos que $\star$ es una involución F-lineal que deja fijo F y que $(xy)^\star = y^\star\, x^\star$. Definimos la *traza* y la *norma* (reducidas) de x como

$$\tau(x) = x + x^\star = 2\, x_0\,, \qquad \nu(x) = x\, x^\star = x^\star\, x = x_0^2 - a\, x_1^2 - b\, x_2^2 + ab\, x_3^2\,.$$

Como $x^2 - (x + x^\star)\, x + x^\star\, x = 0$, tenemos que $x \in D$ es raiz de

$$T^2 - \tau(x)\, T + \nu(x) \in F[T]\,,$$

que llamamos *polinomio característico* (reducido) de x.

Observación. Por lo anterior, si $x \notin F$ entonces $F[x]$ es un álgebra de dimensión 2 con base $\{1, x\}$. Se sigue que la traza y la norma quedan determinadas por la relación $x^2 = \tau(x)\, x - \nu(x)$ y la involución canónica por $x^\star = \tau(x) - x$.

Ejemplo 1. En el álgebra de matrices $M_2(F)$ la involución canónica está dada por

$$\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right)^\star = \left(\begin{smallmatrix} t & -v \\ -w & u \end{smallmatrix}\right),$$

mientras que la traza y norma reducidas estarán dadas por la traza y el determinante de la matriz, respectivamente:

$$\tau\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) = u + t, \qquad \nu\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) = ut - vw.$$

La norma nos permite caracterizar los elementos invertibles en un álgebra de cuaterniones D. En efecto, $x \in D$ es invertible si y solamente si $\nu(x) \in F^\times$, y en tal caso el inverso de x está dado por $x^{-1} = \nu(x)^{-1}\, x^\star$.

Proposición 1.4. *Sea $D = (a,b)_F$ un álgebra de cuaterniones sobre F. Son equivalentes*

(1) *$D \cong M_2(F)$.*
(2) *D no es un álgebra de división.*
(3) *La forma cuadrática ν es isotrópica en D (tiene ceros no triviales).*
(4) *La forma cuadrática $a\, x^2 + b\, y^2$ representa 1.*

Demostración. El Corolario 1.3 prueba (1) $\Leftrightarrow$ (2). La equivalencia (2) $\Leftrightarrow$ (3) sigue de la caracterización de los elementos invertibles en D. La implicación (4) $\Rightarrow$ (3) es clara. Falta probar (3) $\Rightarrow$ (4). Sea $x \in D$, $x \neq 0$ tal que $\nu(x) = 0$. El ideal Dx, como espacio vectorial sobre F, tiene dimensión 2, entonces existe un $y \in Dx$, $y \neq 0$ tal que $y = y_0 + y_1\, i + y_2\, j$, es decir $\nu(y) = y_0^2 - a\, y_1^2 - b\, y_2^2 = 0$. Para concluir, si $y_0 \neq 0$ se sigue que $a\, x^2 + b\, y^2$ representa 1, mientras que si $y_0 = 0$ se sigue que $a\, x^2 + b\, y^2$ es isotrópica, pero una forma cuadrática isotrópica es universal y por lo tanto representa 1. $\square$

1.1. **Clasificación de álgebras de cuaterniones.** En esta sección vamos a mencionar resultados de clasificación de álgebras de cuaterniones sobre algunos cuerpos, particularmente sobre $\mathbb{Q}$.

Proposición 1.5. *Toda álgebra de cuaterniones sobre $\mathbb{C}$ es isomorfa a $M_2(\mathbb{C})$.*

Demostración. Todo $a \in \mathbb{C}^\times$ es un cuadrado, entonces $(a,b)_{\mathbb{C}} \cong M_2(\mathbb{C})$. □

Proposición 1.6. *Un álgebra de cuaterniones sobre $\mathbb{R}$ es isomorfa a $M_2(\mathbb{R})$ o a $\mathbb{H}$.*

Demostración. Si $a > 0$ o si $b > 0$ entonces $(a,b)_{\mathbb{R}} \cong M_2(\mathbb{R})$. Por otra parte si $a = -x^2$ y $b = -y^2$ entonces es claro que $(-x^2,-y^2)_{\mathbb{R}} \cong (-1,-1)_{\mathbb{R}} \cong \mathbb{H}$. □

Proposición 1.7. *Toda álgebra de cuaterniones sobre un cuerpo finito $\mathbb{F}_q$ es isomorfa a $M_2(\mathbb{F}_q)$.*

Demostración. Vamos a probar que $a\,x^2 + b\,y^2 = 1$ tiene solución en $\mathbb{F}_q$. En efecto, la imágen de $a\,x^2$ tiene $(q+1)/2$ elementos y la imágen de $1 - b\,y^2$ también tiene $(q+1)/2$ elementos. Por el principio del palomar, tienen un valor en común, es decir una solución de $a\,x^2 = 1 - b\,y^2$ como afirmamos. □

Sea D un álgebra de cuaterniones sobre $\mathbb{Q}$. Consideramos $D_\infty = D \otimes \mathbb{R}$, que es un álgebra de cuaterniones sobre $\mathbb{R}$. Decimos que D es *definida* cuando $D_\infty \cong \mathbb{H}$ y que D es *indefinida* cuando $D_\infty \cong M_2(\mathbb{R})$ (esto corresponde a que la forma norma ν sea definida o indefinida, respectivamente). Es claro que la clase de isomorfismo de D_∞ es un invariante de D; por ejemplo, $(-1,-1)_{\mathbb{Q}} \ncong (-1,3)_{\mathbb{Q}}$

Sin embargo, esto no alcanza para tener una clasificación sobre $\mathbb{Q}$. Por ejemplo las álgebras $D = (-1,-1)_{\mathbb{Q}}$ y $D' = (-1,-3)_{\mathbb{Q}}$ son ambas definidas pero no son isomorfas. Consideremos las respectivas formas normas:

$$\nu(x) = x_0^2 + x_1^2 + x_2^2 + x_3^2\,, \qquad \nu'(y) = y_0^2 + y_1^2 + 3\,y_2^2 + 3\,y_3^2\,.$$

Es fácil ver que la segunda no tiene ceros no triviales módulo 9, mientras que la primera los tiene ($1^2 + 2^2 + 2^2 = 9$). ¿Es posible usar esto para probar que $(-1,-1)_{\mathbb{Q}} \ncong (-1,-3)_{\mathbb{Q}}$? Esto presenta algunas dificultades. En primer lugar los enteros módulo 9 no son un cuerpo. Si trabajamos módulo 3, para tener un cuerpo, entonces ambas formas tienen ceros no triviales módulo 3, y de todas maneras ya vimos que hay una única clase de isomorfismo de álgebras de cuaterniones sobre $\mathbb{F}_3$. Por otra parte $\mathbb{Q}$ no está contenido en los enteros módulo 9 o módulo 3, por lo que no es tan claro el cambio de base.

Para resolver estas dificultades, debemos emplear el cuerpo de los números 3-ádicos $\mathbb{Q}_3$. En primer lugar $\mathbb{Q} \subset \mathbb{Q}_3$ por lo cual podemos considerar el cambio de base $D \otimes \mathbb{Q}_3$. Por otra parte, las afirmaciones hechas arriba acerca de los ceros módulo 9 de las formas normas se traducen en: ν es isotrópica en $D \otimes \mathbb{Q}_3$ (tiene ceros no triviales), y ν' es anisotrópica en $D' \otimes \mathbb{Q}_3$ (no tiene ceros excepto el trivial $\nu'(0) = 0$). Entonces $D \otimes \mathbb{Q}_3 \cong M_2(\mathbb{Q}_3)$ mientras que $D' \otimes \mathbb{Q}_3$ es un álgebra de división.

> **Interludio: los números p-ádicos.** Si consideramos el valor absoluto usual en $\mathbb{Q}$ obtenemos una métrica en $\mathbb{Q}$ cuya completación son los números reales. De la misma manera podemos construir, para cada primo p, los números p-ádicos como la completación de $\mathbb{Q}$ con respecto al valor absoluto p-ádico.

Al cuerpo de los números p-ádicos lo denotaremos $\mathbb{Q}_p$, y en ocasiones denotaremos $\mathbb{Q}_\infty$ al cuerpo de los números reales; estos son ejemplos de *cuerpos locales*. Usaremos la letra v para referirnos a un primo p o al *primo arquimediano* ∞.

Para construir el valor absoluto p-ádico definimos la *valuación p-ádica* $v_p : \mathbb{Q}^\times \to \mathbb{Z}$ dada por $v_p(p^r \frac{a}{b}) = r$ siempre que $p \nmid a, b$. Finalmente definimos $|x|_p = p^{-v_p(x)}$ para $x \in \mathbb{Q}^\times$, y $|0|_p = 0$. Es un ejercicio verificar que $|x|_p$ es un valor absoluto.

Como $\mathbb{Q}_p$ es la completación de $\mathbb{Q}$, todo $x \in \mathbb{Q}_p$ puede ser escrito como límite de una sucesión de números racionales. Observar que $|p^r|_p \to 0$ cuando $r \to \infty$, y podemos escribir x como una serie $\sum_{n \geqslant N_0} a_n p^n$. Las sumas parciales corresponden a considerar x módulo p^r.

Por más detalles consultar la sección 2.1 de las notas de Pacetti.

En nuestro ejemplo, la forma cuadrática $y_0^2 + y_1^2 + 3\,y_2^2 + 3\,y_3^2$ no tiene ceros no triviales en $\mathbb{Q}_3$, pues no los tiene módulo 9. Por otra parte, la forma cuadrática $x_0^2 + x_1^2 + x_2^2 + x_3^2$ tiene ceros módulo 9, e.g. $1^2 + 2^2 + 2^2 \equiv 0 \pmod 9$. A partir de este cero es posible construir ceros en $\mathbb{Q}_3$ mediante una construcción conocida como *Lema de Hensel*. Una solución es $1^2 + 2^2 + x^2 = 0$ con $x = 2 + 2 \cdot 3^2 + 3^4 + 3^6 + 3^9 + \cdots \in \mathbb{Q}_3$.

Proposición 1.8 (Clasificación local)**.** *Hay exactamente dos clases de isomorfismo de álgebras de cuaterniones sobre $\mathbb{Q}_v$.*

En otras palabras, además del álgebra de matrices $M_2(\mathbb{Q}_v)$, existe un álgebra de cuaterniones de división sobre $\mathbb{Q}_v$, única a menos de isomorfismo.

Cuando D es un álgebra de cuaterniones sobre $\mathbb{Q}$, podemos considerar $D_v = D \otimes \mathbb{Q}_v$ para todo v (primo o ∞). Decimos que D ramifica en v cuando D_v es un álgebra de división. La ramificación de D, definida como el conjunto de los v en los que D ramifica, es un invariante de D.

Teorema 1.9 (Clasificación global)**.** *Sean D y D' dos álgebras de cuaterniones sobre $\mathbb{Q}$.*

(1) *$D \cong D' \iff D_v \cong D'_v$ para todo $v \iff D$ y D' tienen igual ramificación.*
(2) *La ramificación de D es un conjunto finito de cardinal par.*
(3) *Dado un conjunto de lugares que sea finito y de cardinal par, existe un álgebra de cuaterniones sobre $\mathbb{Q}$ con esa ramificación.*

Es un ejercicio probar que si $a, b \in \mathbb{Z}$ y $p \nmid 2ab$ entonces $(a, b)_{\mathbb{Q}_p} \cong M_2(\mathbb{Q}_p)$. Es decir que $(a, b)_{\mathbb{Q}}$ solo puede ramificar en los divisores de $2ab$ o en ∞.

Ejemplo 2. Sea N un primo (finito). De acuerdo al teorema existe un álgebra de cuaterniones ramificada en $\{N, \infty\}$. Por ejemplo:

(1) El álgebra $(-1, -1)_{\mathbb{Q}}$ ramifica en $\{2, \infty\}$.
(2) Si $N \equiv 3 \pmod 4$, el álgebra $(-1, -N)_{\mathbb{Q}}$ ramifica en $\{N, \infty\}$.
(3) Si $N \equiv 5 \pmod 8$, el álgebra $(-2, -N)_{\mathbb{Q}}$ ramifica en $\{N, \infty\}$.

Cuando F es un cuerpo de números, los lugares de F corresponden a las inmersiones de F en $\mathbb{R}$ o en $\mathbb{C}$ (lugares arquimedianos) y a los ideales primos en su anillo de enteros (lugares no arquimedianos). Las completaciones de F con respecto a los lugares arquimedianos son $\mathbb{R}$ o $\mathbb{C}$, y las completaciones con respecto a los lugares no arquimedianos son extensiones finitas de los $\mathbb{Q}_p$.

Los resultados mencionados se generalizan para F. En otras palabras, si D es un álgebra de cuaterniones sobre F, la ramificación de D (el conjunto de lugares de F donde D es de división) es un conjunto finito de cardinal par que deterimina la clase de isomorfismo de D. Además, dado un conjunto de lugares de F que sea finito y de cardinal par, y que no contenga ningún lugar complejo, existe un álgebra de cuaterniones sobre F con esa ramificación.

1.2. **Órdenes de cuaterniones.** Sea D un álgebra de cuaterniones sobre $\mathbb{Q}$. Un *retículo* en D es un subgrupo $M \subset D$ tal que M es finitamente generado y tal que $\mathbb{Q}M = D$. Equivalentemente M es un $\mathbb{Z}$-módulo libre de rango 4; en otras palabras existe una base $\{d_1, d_2, d_3, d_4\}$ de D que genera M como $\mathbb{Z}$-módulo. Recíprocamente, cualquier base de D genera un retículo en D. Usaremos la notación $[d_1, d_2, d_3, d_4]$ para referirnos al retículo generado por esos elementos. La *norma de un retículo* M se define como $\nu(M) = \operatorname{mcd}\{\nu(d) : d \in M\}$, que existe pues M es finitamente generado. En efecto $\nu([d_1, d_2, d_3, d_4]) = \operatorname{mcd}\{d_1, d_2, d_3, d_4\}$.

Un elemento $x \in D$ es *integral* si $\tau(x), \nu(x) \in \mathbb{Z}$. Equivalentemente $\mathbb{Z}[x]$ es finitamente generado como $\mathbb{Z}$-módulo. Un *orden* en D es un retículo $R \subset D$ que es un subanillo, esto es tal que $1 \in R$ y R es cerrado por el producto. Los elementos de R deben ser integrales, pues si $x \in R$ entonces $\mathbb{Z}[x] \subset R$ debe ser finitamente generado; sin embargo *el conjunto de los elementos de D integrales no forma un anillo!*

Por ejemplo, tanto $x = \left(\begin{smallmatrix} 1 & 1/2 \\ 0 & 1 \end{smallmatrix}\right)$ como $y = \left(\begin{smallmatrix} 1 & 0 \\ 1/2 & 1 \end{smallmatrix}\right)$ son elementos integrales en $M_2(\mathbb{Q})$, pero $x + y$ no lo es. En efecto, tanto $\mathbb{Z}[x]$ como $\mathbb{Z}[y]$ son finitamente generados como $\mathbb{Z}$-módulos, pero no así $\mathbb{Z}[x + y]$.

Si R es un orden en D su determinante se define $\det R = \det(\tau(d_i^\star\, d_j)) \in \mathbb{Z}$ donde $\{d_1, d_2, d_3, d_4\}$ es una base de R. Es fácil ver que no depende de la elección de la base. Además $\det R$ es un cuadrado, y definimos el discriminante de R como $\operatorname{disc} R = \sqrt{\det R}$. Cuando $R' \subset R$ tenemos que $\operatorname{disc} R' = [R' : R] \operatorname{disc} R$ y deducimos que existen ordenes maximales (aquellos con discriminante minimal).

Proposición 1.10. *Si R es un orden maximal en D entonces* $\operatorname{disc} R$ *es el producto de todos los primos donde D ramifica. En particular todos los ordenes maximales tienen igual discriminante, que es libre de cuadrados; a este número lo denotamos* $\operatorname{disc} D$.

Ejemplo 3. Sea $D = (-1, -1)_{\mathbb{Q}}$. Tenemos un orden $R = [1, i, j, k]$ (cuaterniones de Lipschitz) pero su discriminante es 4, entonces R no es maximal. Sea $\rho = \frac{1+i+j+k}{2}$, que es integral, entonces $R + \mathbb{Z}\,\rho$ es un orden y es maximal (cuaterniones de Hurwitz).

Ejemplo 4. Sea $D = (-1, -N)_{\mathbb{Q}}$ donde $N \equiv 3 \pmod 4$ es primo. Entonces el retículo $[1, i, \frac{1+j}{2}, \frac{i+k}{2}]$ es un anillo y tiene discriminante N, por lo tanto es maximal.

Fijemos un orden R en un álgebra de cuaterniones D. Un *ideal a derecha para R* es un retículo $I \subset D$ tal que $IR = I$. Decimos que I es *propio* si es localmente principal (cuando R es maximal todos los ideales son propios). Denotaremos $\mathcal{I}(R)$ al conjunto de ideales a derecha para R propios. El grupo multiplicativo $D^\times$ actúa en $\mathcal{I}(R)$ por multiplicación a la izquierda. Las órbitas de $\mathcal{I}(R)$ por esta acción se llaman *clases de ideales*. Llamaremos $h(R)$ al número de clases de ideales de R.

Teorema 1.11. *El número de clases de ideales $h(R)$ es finito.*

2. Formas modulares cuaterniónicas

En esta sección haremos una introducción a las formas modulares cuaterniónicas en un caso particular. En las notas de Harris se verá una definición más general.

Sea D un álgebra de cuaterniones sobre $\mathbb{Q}$; suponemos que D es definida (es decir, $D_\infty = D \otimes \mathbb{R}$ es un álgebra de división).

Definición 2.1. Dado un orden $R \subset D$, una *forma modular cuaterniónica* para R es una función $f : \mathcal{I}(R) \to \mathbb{C}$ tal que $f(d\,I) = f(I)$ para todo $d \in D^\times$.

Denotaremos $\mathcal{M}(R)$ al espacio de formas modulares cuaterniónicas para R. Dado un ideal I, la función característica de la clase de I es una forma modular cuaterniónica que denotaremos $[I]$. A efectos computacionales es conveniente fijar un conjunto de representantes de las clases de ideales $\{I_1, \dots, I_h\}$, de modo que $\{[I_1], \dots, [I_h]\}$ es una base de $\mathcal{M}(R)$.

Para cada ideal $I \in \mathcal{I}(R)$ el grupo $\Gamma_I = \{d \in D^\times \,:\, d\,I = I\}/\mathbb{Z}^\times$ es finito, ya que es discreto dentro de $D_\infty^\times/\mathbb{R}^\times \cong SO_3(\mathbb{R})$ que es compacto. Denotamos $w_I = \#\Gamma_I$, que depende solamente de la clase de I.

Definimos un producto interno en $\mathcal{M}(R)$ que está dado en la base por

$$\langle [I], [J] \rangle := \tfrac{1}{2}\,\#\big\{d \in D^\times \,:\, I = d\,J\big\} = \begin{cases} w_I & \text{si } [I] = [J], \\ 0 & \text{si } [I] \neq [J]. \end{cases}$$

Notar que $\{[I_1], \dots, [I_h]\}$ es una base ortogonal de $\mathcal{M}(R)$.

El *grado* de una forma modular se define como un funcional lineal tal que $\mathrm{gr}([I]) = 1$. Alternativamente sea $e_0 = \sum_{i=1}^h \frac{1}{w_{I_i}}[I_i]$, entonces $\mathrm{gr}(f) = \langle f, e_0 \rangle$. Decimos que f es *cuspidal* si es ortogonal a e_0, equivalentemente si $\mathrm{gr}(f) = 0$.

A continuación vamos a definir una familia de operadores en $\mathcal{M}(R)$ que llamaremos *operadores de Hecke*. Dado un ideal $I \in \mathcal{I}(R)$ y $m \geqslant 1$ un entero definimos

$$\mathcal{T}_m(I) = \big\{I' \in \mathcal{I}(R) \,:\, I' \subset I, \quad \nu(I') = m\,\nu(I)\big\}.$$

Entonces el operador de Hecke $t_m : \mathcal{M}(R) \to \mathcal{M}(R)$ se define, en la base, como

$$t_m[I] = \sum_{I' \in \mathcal{T}_m(I)} [I'].$$

Lema 2.2. *Sean $I, J \in \mathcal{I}(R)$ y $m \geqslant 1$. Entonces $J \in \mathcal{T}_m(I) \Leftrightarrow m\,I \in \mathcal{T}_m(J)$.*

Demostración. Supongamos que $J = d\,I$ con $d \in D^\times$. Si $d\,I \in \mathcal{T}_m(I)$ entonces $\nu(d) = m$ y $d\,I \subset I$. Entonces también $d^\star I \subset I$ y concluimos que $m\,I = d\,d^\star I \subset d\,I$, y comparando normas concluimos que $m\,I \in \mathcal{T}_m(d\,I)$. Cuando I y J no son equivalentes se prueba del mismo modo pero localmente. □

Proposición 2.3. *Los operadores de Hecke en $\mathcal{M}(R)$ satisfacen*

1. *t_m es autoadjunto.*
2. *Si $(m, m') = 1$ entonces $t_m\,t_{m'} = t_{m'}\,t_m = t_{m\,m'}$.*
3. *Si $p \nmid \mathrm{disc}\,R$ es primo entonces $t_{p^{k+2}} = t_{p^{k+1}}\,t_p - p\,t_{p^k}$.*
4. *Si $(m\,m', \mathrm{disc}\,R) = 1$ entonces $t_m\,t_{m'} = \sum_{d \mid (m,m')} d\,t_{m\,m'/d^2}$*

En particular los operadores t_p con $p \nmid \operatorname{disc} R$ primo generan un álgebra conmutativa $\mathbb{T}_R$ que contiene todos los operadores t_m con $(m, \operatorname{disc} R) = 1$. Además éstos últimos generan $\mathbb{T}_R$ como $\mathbb{Z}$-módulo.

Demostración. Calculamos

$$\begin{aligned}\langle t_m[I], [J]\rangle &= \sum_{I' \in \mathcal{T}_m(I)} \langle [I'], [J]\rangle \\ &= \sum_{I' \in \mathcal{T}_m(I)} \tfrac{1}{2} \#\{d \in D^\times \ : \ I' = d\,J\} \\ &= \tfrac{1}{2} \#\{d \in D^\times \ : \ d\,J \in \mathcal{T}_m(I)\}\end{aligned}$$

Se prueba que $d\,J \in \mathcal{T}_m(I) \Leftrightarrow m\,I \in \mathcal{T}_m(d\,J)$ entonces la última expresión es

$$\begin{aligned}&= \tfrac{1}{2} \#\{d \in D^\times \ : \ m\,I \in \mathcal{T}_m(d\,J)\} \\ &= \tfrac{1}{2} \#\{d \in D^\times \ : \ m\,d^{-1}\,I \in \mathcal{T}_m(J)\} \\ &= \tfrac{1}{2} \#\{d' \in D^\times \ : \ d'\,I \in \mathcal{T}_m(J)\} \\ &= \langle [I], t_m[J]\rangle\end{aligned}$$

Las afirmaciones (2) y (3) se prueban localmente. La afirmación (4) es un ejercicio a partir de (2) y (3). □

Corolario 2.4. *El espacio $\mathcal{M}(R)$ tiene una base ortogonal de vectores propios para $\mathbb{T}_R$.*

Para $p \nmid \operatorname{disc} R$ primo se prueba que $\#\mathcal{T}_p(I) = p + 1$. Entonces t_p es homogéneo de grado $p+1$ en el sentido de que $\operatorname{gr}(t_p f) = (p+1)\operatorname{gr}(f)$, y se deduce que e_0 es un vector propio para $\mathbb{T}_R$ con $t_p\, e_0 = (p+1)\, e_0$. Cualquier otro vector propio será ortogonal a e_0, es decir cuspidal.

Ejemplo 5. Consideramos el álgebra $D = (-1,-11)_{\mathbb{Q}}$ ramificada en $\{11, \infty\}$ y el orden maximal $R = [1, i, \frac{1+j}{2}, \frac{i+k}{2}]$ de discriminante 11. El número de clases es 2, y un conjunto de representantes es

$$\begin{aligned}I_1 &= [1, i, \tfrac{1+j}{2}, \tfrac{i+k}{2}] \\ I_2 &= [2, 2i, i + \tfrac{1+j}{2}, 1 + i + \tfrac{i+k}{2}]\end{aligned}$$

Los estabilizadores son $\Gamma_{I_1} = \{\pm 1, \pm i\}$ y $\Gamma_{I_2} = \{\pm 1, \pm \frac{2-i+k}{4}, \pm \frac{-2-i+k}{4}\}$, de modo que $w_{I_1} = 2$ y $w_{I_2} = 3$. Se puede calcular

$$\begin{aligned}\mathcal{T}_2(I_1) &= \{(1+i)\,I_1,\ I_2,\ \tfrac{2-i-k}{4}\,I_2\}, \\ \mathcal{T}_2(I_2) &= \{2\,I_1,\ \tfrac{2+i-k}{2}\,I_1,\ \tfrac{2-i+k}{2}\,I_1\}.\end{aligned}$$

Entonces el operador de Hecke t_2 está dado por

$$t_2[I_1] = [I_1] + 2[I_2], \qquad t_2[I_2] = 3[I_1],$$

y tiene vectores propios $e_0 = \frac{1}{2}[I_1] + \frac{1}{3}[I_2]$ con valor propio 3, y $f_1 = [I_1] - [I_2]$ con valor propio -2. Podemos calcular otros operadores de Hecke, que en la base $\{[I_1], [I_2]\}$

resultan:

$$t_2 = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 0 \end{smallmatrix}\right), \quad t_3 = \left(\begin{smallmatrix} 2 & 2 \\ 3 & 1 \end{smallmatrix}\right), \quad t_5 = \left(\begin{smallmatrix} 4 & 2 \\ 3 & 3 \end{smallmatrix}\right), \quad t_7 = \left(\begin{smallmatrix} 4 & 4 \\ 6 & 2 \end{smallmatrix}\right), \quad \dots \quad .$$

El vector propio e_0 tiene valores propios 3, 4, 6, 8, ..., como ya habíamos observado, mientras que f_1 tiene valores propios -2, -1, 1, -2, ...

2.1. **Correspondencia de Eichler.** Para evitar dificultades técnicas nos limitaremos al caso de un orden R de discriminante N primo en un álgebra definida. Necesariamente R es un orden maximal en un álgebra de cuaterniones D ramificada en $\{N, \infty\}$.

Hemos visto que el espacio $\mathcal{M}(R)$ tiene una acción por operadores autoadjuntos del álgebra conmutativa $\mathbb{T} = \mathbb{T}_R$, que es similar a la acción de Hecke en espacios de formas modulares. Observemos que las relaciones de la Proposición 2.3 son las mismas que para los operadores de Hecke en formas modulares de peso 2 para $\Gamma_0(N)$.

Eichler calcula la traza de t_m actuando en $\mathcal{M}(R)$ y por otra parte calcula la traza de T_m actuando en $\mathfrak{M}_2(\Gamma_0(N))$. Comparando ambas obtiene el siguiente resultado.

Teorema 2.5. *Para todo $m \geqslant 1$ tenemos*

$$\mathrm{Tr}(t_m \circlearrowright \mathcal{M}(R)) = \mathrm{Tr}(T_m \circlearrowright \mathfrak{M}_2(\Gamma_0(N)))$$

Como consecuencia de este resultado, y puesto que ambas álgebras de Hecke son semisimples y están generadas como $\mathbb{Z}$-módulo por los operadores de Hecke, se deduce que son isomorfas y que hay una correspondencia

$$\{\text{vectores propios en } \mathcal{M}(R)\}/\mathbb{C}^\times \longleftrightarrow \{\text{vectores propios en } \mathfrak{M}_2(\Gamma_0(N))\}/\mathbb{C}^\times$$

donde formas correspondientes tienen los mismos valores propios. Otra forma de enunciar lo mismo es decir que existe un isomorfismo $\mathcal{M}(R) \cong \mathfrak{M}_2(\Gamma_0(N))$ que preserva la acción de Hecke. Sin embargo este isomorfismo no es canónico.

Sabemos que en $\mathfrak{M}_2(\Gamma_0(N))$ los espacios propios tienen dimensión 1 (no hay formas viejas porque N es primo y $\mathfrak{M}_2(\Gamma_0(1)) = \{0\}$), y lo mismo vale entonces para $\mathcal{M}(R)$.

Definición 2.6. Sean $f, g \in \mathcal{M}(R)$. Definimos

$$\phi(f,g) = \frac{\mathrm{gr}(f) \cdot \mathrm{gr}(g)}{2} + \sum_{m \geqslant 1} \langle t_m f, g \rangle \, q^m$$

Proposición 2.7. *$\phi(f,g)$ es una forma modular de peso 2 para $\Gamma_0(N)$ y*

$$\phi(t_m\, f, g) = \phi(f, t_m\, g) = T_m\, \phi(f,g)\,.$$

En otras palabras

$$\phi : \mathcal{M}(R) \underset{\mathbb{T}}{\otimes} \mathcal{M}(R) \to \mathfrak{M}_2(\Gamma_0(N))$$

es $\mathbb{T}$-equivariante, y como $\mathcal{M}(R)$ es un $\mathbb{T}$-módulo libre de rango 1 se sigue que ϕ es un isomorfismo de $\mathbb{T}$-módulos.

Demostración. Sean $I, J \in \mathcal{I}(R)$. Consideramos el retículo $M = \{d \in D \ : \ d\,J \subset I\}$. En la demostración de la Proposición 2.3 calculamos

$$\langle t_m[I], [J] \rangle = \tfrac{1}{2} \# \left\{ d \in D^\times \ : \ d\,J \in \mathcal{T}_m(I) \right\}.$$

Ahora $d\,J \in \mathcal{T}_m(I)$ es equivalente a $d \in M$ con $\nu(d) = m\,\nu(M)$, es decir que

$$\langle t_m[I], [J] \rangle = \tfrac{1}{2} \# \left\{ d \in M \ : \ \nu(d) = m\,\nu(M) \right\}.$$

Luego

$$\phi([I],[J]) = \tfrac{1}{2}\sum_{d\in M} q^{Q(d)}$$

es la serie theta asociada a la forma cuadrática $Q(d) = \nu(d)/\nu(M)$, que es una forma modular en $\mathfrak{M}_2(\Gamma_0(N))$. En general $\phi(f,g)$ es combinación lineal de estas series theta.

La igualdad $\phi(t_m\, f, g) = \phi(f, t_m\, g)$ se deduce fácilmente pues t_m es autoadjunto y es homogéneo respecto al grado. La última igualdad basta probarla con $m = p$ primo. Usando la fórmula de T_p en términos de coeficientes de Fourier calculamos

$$T_p\,\phi(f,g) = (p+1)\,\frac{\mathrm{gr}(f)\cdot\mathrm{gr}(g)}{2} + \sum_{m\geqslant 1}\left(\langle t_{mp}\, f, g\rangle + p\,\left\langle t_{m/p}\, f, g\right\rangle\right) q^m$$

bajo la convención que $t_{m/p} = 0$ si $p \nmid m$. Por otra parte

$$\phi(t_p\, f, g) = \frac{\mathrm{gr}(t_p\, f)\cdot\mathrm{gr}(g)}{2} + \sum_{m\geqslant 1}\langle t_m\, t_p\, f, g\rangle\, q^m\,.$$

El resultado se sigue pues por la Proposición 2.3 tenemos $t_m\, t_p = t_{mp} + p\, t_{m/p}$. □

Ejemplo 6. Continuando con el ejemplo 5, las series theta asociadas a la base de $\mathcal{M}(R)$ son $\theta_{ij} = \phi([I_i],[I_j])$:

$$\begin{aligned}
\theta_{11} &= \tfrac{1}{2} + 2q + 2q^2 + 4q^3 + 10q^4 + 8q^5 + 16q^6 + 8q^7 + 18q^8 + 14q^9 + O(q^{10})\\
\theta_{12} &= \tfrac{1}{2} + 6q^2 + 6q^3 + 6q^4 + 6q^5 + 12q^6 + 12q^7 + 18q^8 + 18q^9 + O(q^{10})\\
\theta_{22} &= \tfrac{1}{2} + 3q + 3q^3 + 12q^4 + 9q^5 + 18q^6 + 6q^7 + 18q^8 + 12q^9 + O(q^{10})
\end{aligned}$$

Con estas series theta podemos calcular

$$\begin{aligned}
E_0 &= \phi(e_0,[I_1]) = \tfrac{1}{2}\,\theta_{11} + \tfrac{1}{3}\,\theta_{12} = \phi(e_0,[I_2]) = \tfrac{1}{2}\,\theta_{12} + \tfrac{1}{3}\,\theta_{22}\\
&= \tfrac{5}{12} + q + 3q^2 + 4q^3 + 7q^4 + 6q^5 + 12q^6 + 8q^7 + 15q^8 + 13q^9 + O(q^{10})\\
F_1 &= \phi(f_1, \tfrac{1}{2}[I_1]) = \tfrac{1}{2}\,(\theta_{11} - \theta_{12}) = \phi(f_1, -\tfrac{1}{3}[I_2]) = \tfrac{1}{3}\,(\theta_{22} - \theta_{12})\\
&= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 + O(q^{10})\\
0 &= \phi(f_1, e_0) = \tfrac{1}{2}\,\theta_{11} - \tfrac{1}{6}\,\theta_{12} - \tfrac{1}{3}\,\theta_{22}
\end{aligned}$$

Las dos primeras son las dos autoformas modulares normalizadas de peso 2 para $\Gamma_0(11)$. La forma E_0 es una serie de Eisenstein, y F_1 es una autoforma cuspidal que corresponde a la curva elíptica $y^2 + y = x^3 - x^2 - 10x - 20$.

Observación. Notamos que $e_0 = \frac{1}{2}\,[I_1] + \frac{1}{3}\,[I_2] \equiv \frac{1}{2}\,[I_1] - \frac{1}{2}\,[I_2] = \frac{1}{2} f_1 \pmod 5$. Se deduce que $E_0 = \phi(e_0,[I_1]) \equiv \phi(\frac{1}{2}\,f_1,[I_1]) = F_1 \pmod 5$. En efecto, $E_0 - F_1 = \frac{5}{6}\,\theta_{12}$. Esta congruencia está relacionada con el hecho que la curva elíptica $y^2 + y = x^3 - x^2 - 10x - 20$ tiene torsión de orden 5.