UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

EL ANILLO DE HECKE Y SERIES DE DIRICHLET FORMALES CON UN PRODUCTO DE EULER.

T E S I S

QUE PARA OBTENER EL GRADO DE

M A T E M A T I C O

P R E S E N T A

ROGELIO JIMENEZ FRAGOSO

México, D.F. 1990.

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

I N T R O D U C C I O N

Una de las ideas más fructíferas en la teoría de las formas modulares, la idea de los operadores de Hecke, está basada principalmente en las formas modulares para un grupo G sobre ciertas clases dobles módulo Γ. La mayoría de las relaciones entre operadores de Hecke únicamente refleja relaciones entre las correspondientes clases dobles. El primer capítulo de este trabajo estudia el anillo de Hecke generado por estas clases dobles.

En el capítulo dos se dan propiedades acerca de estas clases dobles y se consideran series formales de Dirichlet con coeficientes en el anillo de Hecke expresadas en términos de productos de Euler.

Aprovecho este espacio para agradecer al Dr. Félix Recillas la dirección de esta tesis, y en general a todos mis maestros que han sabido introducirme en el maravilloso mundo de las Matemáticas.

Mayo 1990.

I N D I C E

CAPITULO 1

1. DEFINICIÓN DEL ANILLO DE HECKE.

Sea G un grupo multiplicativo, Γ y Γ' subgrupos de G. Escribiremos $\Gamma \sim \Gamma'$ si Γ y Γ' son conmensurables, i.e. $\Gamma \cap \Gamma'$ tiene índice finito en Γ y en Γ'; $[\Gamma \cap \Gamma' : \Gamma] < \infty$, $[\Gamma \cap \Gamma' : \Gamma'] < \infty$. Fijemos un subgrupo Γ de G y consideremos el conjunto

$$\tilde{\Gamma} = \{\alpha \in G / \alpha\ \Gamma\alpha^{-1} \sim \Gamma\}$$

Lema 1.1 i) La relación $\sim$ es de equivalencia.

ii) $\tilde{\Gamma}$ es un subgrupo de G que contiene a Γ y al centro de G.

iii) Si $\Gamma \sim \Gamma'$, entonces $\tilde{\Gamma} = \tilde{\Gamma}'$.

Demostración i) Demostraremos únicamente la Transitividad. Sean Γ_1, Γ_2 y Γ_3 subgrupos de G tales que $\Gamma_1 \sim \Gamma_2$ y $\Gamma_2 \sim \Gamma_3$. Entonces la inclusión $\Gamma_1 \cap \Gamma_2 \subset \Gamma_2$ implica la inclusión

$$\Gamma_1 \cap \Gamma_2 / (\Gamma_1 \cap \Gamma_2 \cap \Gamma_3) \subset \Gamma_2 / (\Gamma_2 \cap \Gamma_3)$$

Por lo tanto

$$[\Gamma_1 \cap \Gamma_2 : \Gamma_1 \cap \Gamma_2 \cap \Gamma_3] \leq [\Gamma_2 : \Gamma_2 \cap \Gamma_3] < \infty$$

y

$$[\Gamma_1 : \Gamma_1 \cap \Gamma_3] \leq [\Gamma_1 : \Gamma_1 \cap \Gamma_2 \cap \Gamma_3] = [\Gamma_1 : \Gamma_1 \cap \Gamma_2][\Gamma_1 \cap \Gamma_2 : \Gamma_1 \cap \Gamma_2 \cap \Gamma_3] < \infty$$

de manera semejante se ve que

$$[\Gamma_3 : \Gamma_1 \cap \Gamma_3] < \infty$$

así $\Gamma_1 \sim \Gamma_3$.

ii) Note que si Γ_1 y Γ_2 son dos subgrupos conmensurables de G y $g \in G$, entonces

$$g\Gamma_1 g^{-1} \sim g\Gamma_2 g^{-1}$$

ahora si $\alpha \in \widetilde{\Gamma}$, entonces $\alpha^{-1}\Gamma\alpha \sim \alpha^{-1}(\alpha\,\Gamma\alpha^{-1})\alpha = \Gamma$ lo cual implica que $\alpha^{-1} \in \widetilde{\Gamma}$.

Ahora si $\alpha_1, \alpha_2 \in \widetilde{\Gamma}$, tenemos

$$\alpha_1\,\Gamma\alpha_1^{-1} \sim \Gamma$$

por lo tanto $\alpha_2\,\alpha_1\,\Gamma\alpha_1^{-1}\,\alpha_2^{-1} \sim \alpha_2\Gamma\alpha_2^{-1} \sim \Gamma$

i.e. $$\alpha_2\,\alpha_1\Gamma(\alpha_2\,\alpha_i)^{-1} \sim \Gamma.$$

De esta manera hemos verificado que $\tilde{\Gamma}$ es un subgrupo de G, obviamente $\tilde{\Gamma}$ contiene al centro de G.

iii) Sea $\Gamma \sim \Gamma'$, entonces si $\alpha \in \tilde{\Gamma}$

$$\alpha\Gamma\alpha^{-1} \sim \alpha\Gamma'\alpha^{-1} \sim \Gamma'$$

así $\alpha \in \tilde{\Gamma}'$, i.e. $\tilde{\Gamma} \subset \tilde{\Gamma}'$ de manera semejante se verifica la otra contensión. Por lo tanto $\tilde{\Gamma} = \tilde{\Gamma}'$.

En la discusión siguiente, fijaremos Γ y una familia $\{\Gamma_\lambda\}_{\lambda\in\Lambda}$ de subgrupos de G que son conmensurables con Γ, donde Λ es un conjunto de índices.

Proposición 1.2 Si $\alpha \in \tilde{\Gamma}$, se tienen las siguientes descomposiciones en clases ajenas.

1) $\Gamma_\lambda\alpha\Gamma_\mu = \bigcup_{i=1}^{d} \Gamma_\lambda\alpha_i$ con $d = [\Gamma_\mu : \Gamma_\mu \cap \alpha^{-1}\Gamma_\lambda\alpha]$

2) $\Gamma_\lambda\alpha\Gamma_\mu = \bigcup_{j=1}^{e} \beta_j\Gamma$ con $e = [\Gamma_\lambda : \Gamma_\lambda \cap \alpha\Gamma_\mu\alpha^{-1}]$

Demostración. Sea $\Gamma_\lambda\alpha\Gamma_\mu = \cup_i \Gamma_\lambda\alpha\delta_i$, entonces $\Gamma_\lambda\alpha\delta_i = \Gamma_\lambda\alpha\delta_j \Longrightarrow$ $\delta_j\ \delta_i^{-1} \in \alpha^{-1}\Gamma_\lambda\alpha$ pero $\delta_i, \delta_j \in \Gamma_\mu$ tenemos que $\delta_j\ \delta_i^{-1} \in \Gamma_\mu \cap \alpha^{-1}\Gamma_\lambda\alpha$ esto implica que

$$(\Gamma_\mu \cap \alpha^{-1}\Gamma_\lambda\alpha)\delta_i = (\Gamma_\mu \cap \alpha^{-1}\Gamma_\lambda\alpha)\delta_j$$

observe que todas las implicaciones son reversibles, por lo tanto

$$\Gamma_\lambda \alpha \delta_i = \Gamma_\lambda \alpha \delta_j \iff \delta_j \delta_i^{-1} \in \Gamma_\mu \cap \alpha^{-1} \Gamma_\lambda \alpha$$

como Γ_μ es conmensurable con $\alpha^{-1}\Gamma_\lambda\alpha$, sean

$$d = [\Gamma_\mu : \Gamma_\mu \cap \alpha^{-1}\Gamma_\lambda \alpha] < \infty \quad y$$

$\{\delta_1, \ldots, \delta_d\}$ un conjunto de representantes de $\Gamma_\mu / (\Gamma_\mu \cap \alpha^{-1}\Gamma_\lambda \alpha)$.

Por lo tanto

$$\Gamma_\lambda \alpha \Gamma_\mu = \bigcup_i \Gamma \alpha \delta_i = \bigcup_{i=1}^{d} \Gamma \alpha_i \text{ con } d = [\Gamma_\mu : \Gamma_\mu \cap \alpha^{-1}\Gamma\alpha]$$

Un argumento semejante se aplica al segundo inciso.

Ahora consideremos el $\mathbb{Z}$-módulo $R_{\lambda\mu}$ que consiste de todas las sumas finitas formales de la forma $\Sigma_k C_k (\Gamma_\lambda \alpha_k \Gamma_\mu)$ con $C_k \in \mathbb{Z}$ y $\alpha_k \in \tilde{\Gamma}$.

Para toda $\Gamma_\lambda \alpha \Gamma_\mu$ con $\alpha \in \tilde{\Gamma}$ denotemos por $\operatorname{grad}(\Gamma_\lambda \alpha \Gamma_\mu)$ al número de clases $\Gamma_\lambda \xi$ contenidas en $\Gamma_\lambda \alpha \Gamma_\mu$ y si hacemos $x = \sum_k C_k (\Gamma_\lambda \alpha_k \Gamma_\mu) \in R_{\lambda\mu}$ definimos $\operatorname{grad}(x)$ por

$$\operatorname{grad}(x) = \sum_k C_k \operatorname{grad}(\Gamma_\lambda \alpha_k \Gamma_\mu)$$

y le llamaremos grado de X. (se puede definir otro grado considerando clases laterales izquierdas $\delta\Gamma_\mu$ contenidas en $\Gamma_\lambda\alpha\Gamma_\mu$. Este grado puede no ser igual al anterior, pues en la proposición 1.2 no necesariamente d = e).

Introduzcamos ahora una ley de multiplicación:

$$R_{\lambda\mu} \times R_{\mu\nu} \longrightarrow R_{\lambda\mu}$$

Primero consideremos las siguientes descomposiciones ajenas.

$$\Gamma_\lambda\alpha\Gamma_\mu = \cup_i \Gamma_\lambda\alpha_i, \qquad \Gamma_\mu\beta\Gamma_\nu = \cup_j \Gamma_\mu\beta_j$$

(Evidentemente $\alpha,\beta \in \widetilde{\Gamma}$). Entonces

$$\Gamma_\lambda\alpha\Gamma_\mu\beta\Gamma_\nu = \cup_j \Gamma_\lambda\alpha\Gamma_\mu\beta_j = \cup_{i,j} \Gamma_\lambda\alpha_i\beta_j$$

Por lo tanto $\Gamma_\lambda\alpha\Gamma_\mu\beta\Gamma_\nu$ es unión finita de clases dobles de la forma $\Gamma_\lambda\xi\Gamma_\nu$.

Si $u = \Gamma_\lambda\alpha\Gamma_\mu$, $V = \Gamma_\mu\beta\Gamma_\nu$ y $W = \Gamma_\lambda\xi\Gamma_\nu$ definimos el "producto" U, V siendo este elemento de $R_{\lambda\nu}$ por

$$U\cdot V = \Sigma m(U\cdot V;\ W)W \qquad (1)$$

donde la suma se extiende sobre todos los W, $W = \Gamma_\lambda\xi\Gamma_\nu \subset \Gamma_\lambda\alpha\Gamma_\mu\beta\Gamma_\nu$ y $m(U\cdot V;\ W)$ = número de (i,j) tales que $\Gamma_\lambda\alpha_i\beta_j = \Gamma_\lambda\xi$ (ξ fijo)

Para que nuestra definición tenga sentido debemos demostrar que los lados izquierdo y derecho de (1) dependan de U, V y W y no de la elección de los representantes $\{\alpha_i\}$, $\{\beta_j\}$ y ξ. Para este propósito $\#(S)$ denotará el número de elementos de un conjunto finito S.

Vemos que $\Gamma_\lambda \alpha_i \beta_j = \Gamma_\lambda \xi$ si y solo si $\Gamma_\lambda \alpha_i = \Gamma_\lambda \xi \beta_j^{-1}$.

Notemos que

(i) Para una j dada la última igualdad se cumple exactamente para una i (pues $\Gamma_\lambda \alpha \Gamma_\mu = \cup \Gamma \alpha_i$ es ajena).

(ii) $\xi \beta_j^{-1} \in \Gamma_\lambda \alpha \Gamma_\mu \iff \beta_j \in \Gamma_\mu \alpha^{-1} \Gamma_\lambda \xi$.

(iii) $\beta_j \in \Gamma_\mu \alpha^{-1} \Gamma_\lambda \xi \iff \Gamma_\mu \beta_j \subset \Gamma_\mu \alpha^{-1} \Gamma_\lambda \xi$.

Estas consideraciones nos permiten escribir las siguientes igualdades.

$$\begin{aligned} \#\{(i,j)/\Gamma_\lambda \alpha_i \beta_j = \Gamma \xi\} &= \#\{j/\xi \beta_j^{-1} \in \Gamma_\lambda \alpha \Gamma_\mu\} \\ &= \#\{j/\beta_j \in \Gamma_\mu \alpha^{-1} \Gamma_\lambda \xi\} \\ &= \#\{j/\Gamma_\mu \beta_j \subset \Gamma_\mu \alpha^{-1} \Gamma_\lambda \xi\} \\ &= \text{número de clases de la} \\ &\quad \text{forma } \Gamma_\mu \xi \text{ contenidas en} \\ &\quad \Gamma_\mu \beta \Gamma_\nu \cap \Gamma_\mu \alpha^{-1} \Gamma_\lambda \xi \end{aligned}$$

el último número es obviamente independiente de la elección de $\{\alpha_i\}$ y $\{\beta_j\}$

ahora, si $\Gamma_\lambda \xi \Gamma_\nu = \Gamma_\lambda \eta \Gamma_\nu$, entonces

$$\xi = \delta' \eta \delta \quad \text{con} \quad \delta' \in \Gamma_\lambda \quad \text{y} \quad \delta \in \Gamma_\nu$$

por lo tanto

$$\Gamma_\mu \beta \Gamma_\nu \cap \Gamma_\mu \alpha^{-1} \Gamma_\lambda \xi = \Gamma_\mu \beta \Gamma_\nu \cap \Gamma_\mu \alpha^{-1} \Gamma_\lambda \delta' \eta \delta$$

$$= (\Gamma_\mu \beta \Gamma_\nu \cap \Gamma_\mu \alpha^{-1} \Gamma_\lambda \eta) \delta$$

Por lo tanto el número anterior es independiente de la elección de ξ.

Después de esta verificación, podemos definir la ley de multiplicación $R_{\lambda\mu} \times R_{\mu\nu} \longrightarrow R_{\lambda\nu}$ extendiendo el mapeo $(U, V) \longrightarrow U.V$ linealmente i.e. si $x = \Sigma C_k \Gamma_\lambda \alpha_k \Gamma_\mu \in R_{\lambda\mu}$ y $y = \Sigma b_{k'} \Gamma_\mu \beta_k \Gamma_\nu$ entonces

$$(x,y) \longrightarrow x,y = \sum_{k,k'} C_k b_{k'} (\Gamma_\lambda \alpha_k \Gamma_\mu) \cdot (\Gamma_\mu \rho_{k'} \Gamma_\nu)$$

Proposición 1.3 Sean U, V, W, $\{\alpha_i\}$, $\{\beta_j\}$ y ξ como antes. Entonces

$$\text{grad}(W)\cdot m(u\cdot v,w) = \#\{(i,j)/\Gamma_\lambda\alpha_i\beta_j\Gamma_\nu = \Gamma_\lambda\xi\Gamma_\nu\}$$

Demostración. Sea $\Gamma_\lambda\xi\Gamma_\nu = \overset{f}{\underset{k}{\cup}} \Gamma_\lambda\xi_k$ una descomposición ajena. Entonces

$$\Gamma_\lambda\alpha_i\beta_j\Gamma_\nu = \Gamma_\lambda\xi\Gamma_\nu \text{ si y solo si } \Gamma_\lambda\alpha_i\beta_j = \Gamma_\lambda\xi_k$$

y observando que la última igualdad se cumple para exactamente una k (ya que $\cup\Gamma_\lambda\xi_k$ es ajena) tenemos:

$$\begin{aligned}\#\{(i,j)/\Gamma_\lambda\alpha_i\beta_j\Gamma_\nu = \Gamma_\lambda\xi\Gamma_\nu\} &= \#\{(i,j)/\Gamma_\lambda\alpha_i\beta_j\Gamma_\nu = \cup\Gamma_\lambda\xi_k\} \\ &= \sum_{k=1}^{f} \#\{(i,j)/\Gamma_\lambda\alpha_i\beta_j = \Gamma_\lambda\xi_k\} \\ &= f\cdot m((u\cdot v);w)\end{aligned}$$

Proposición 1.4 Para toda $x \in R_{\lambda\mu}$ y toda $y \in R_{\mu\nu}$ se tiene

$$\text{grad}(x\cdot y) = \text{grad}(x)\cdot\text{grad}(y)$$

Demostración. Consideremos la notación como en la proposición 1.3. Tomando la suma sobre todas las $w = \Gamma_\lambda\xi\Gamma_\nu \subset \Gamma_\lambda\alpha\Gamma_\mu\beta\Gamma_\nu$, tenemos

$$\text{grad}(u\cdot v) = \sum_w \text{grad}(w)\cdot m(u\cdot v;w) =$$

$$= \text{conjunto de todas las parejas } (i,j) \text{ tales que}$$

$$\Gamma_\lambda\alpha_i\beta_j\Gamma_\nu = w$$

pero $\quad i = \#\{\Gamma_\lambda\alpha_k/\Gamma_\lambda\alpha_k \subset \Gamma_\lambda\alpha\Gamma_\mu\} = \text{grad}(U)$

$\quad j = \#\{\Gamma_\mu\beta_\ell/\Gamma_\mu\beta_\ell \subset \Gamma_\mu\beta\Gamma_\nu\} = \text{grad}(V)$

por lo tanto $\text{grad}(U\cdot V) = \text{grad}(U)\cdot\text{grad}(V)$.

ahora bien, si $x = \sum_k a_k\Gamma_\lambda\alpha_k\Gamma_\mu$ y $y = \sum_i b_\ell\Gamma_\mu\beta_\ell\Gamma_\nu$ entonces

$$\text{grad}(x\cdot y) = \sum_{k,\ell} a_k b_\ell \cdot \text{grad}(\Gamma_\lambda\alpha_k\Gamma_\mu\cdot\Gamma_\mu\beta_\ell\Gamma_\nu)$$

$$= \sum_{k,\ell} a_k b_\ell \ \text{grad}(\Gamma_\lambda\alpha_k\Gamma_\mu)\cdot\text{grad}(\Gamma_\mu\beta_\ell\Gamma_\nu)$$

$$= \sum_k a_k \ \text{grad}(\Gamma_\lambda\alpha_k\Gamma_\mu)\cdot\Sigma b \ \text{grad}(\Gamma_\lambda\beta_\ell\Gamma_\nu)$$

$$= \text{grad}(X)\cdot\text{grad}(Y)$$

Proposición 1.5. La multiplicación anterior es asociativa en el sentido de que.

$$(x.y).z = x.(y.z) \text{ con } x\in R_{k\lambda},\ y\in R_{\lambda\mu} \text{ y } z\in R_{\mu\nu}$$

Demostración. Sea M_μ el $\mathbb{Z}$-módulo de todas las sumas finitas formales $\sum_k C_k\cdot\Gamma_\mu\xi_k$ con $C_k\in\mathbb{Z}$ y $\xi_k\in\tilde{\Gamma}$. Sea $U = \Gamma_\lambda\alpha\Gamma_\mu = \cup_i\Gamma_\lambda\alpha_i$ una descomposición ajena. Asignaremos a cada U un mapeo $\mathbb{Z}$ lineal de M_μ en M_λ (el cual denotaremos nuevamente por μ);

$$U : M_\mu \longrightarrow M_\lambda$$

por medio de la acción

$$U : M_\mu \longrightarrow M_\lambda$$

$$\sum_k C_k \Gamma_\mu \xi_k \longmapsto U \cdot \sum C_k \Gamma_\mu \xi_k = \sum_{k,i} C_k \Gamma_\lambda \alpha_i \xi_k$$

Esta definición no depende de los representantes $\{\alpha_i\}, \{\xi_k\}$. En efecto, si

$$U = \Gamma_\lambda \alpha \Gamma_\mu = \bigcup_i \Gamma_\lambda \alpha_i = \bigcup_i \Gamma_\lambda \alpha_i'$$

entonces $\alpha_i = \gamma_\lambda \alpha_i'$ con $\gamma_\lambda \in \Gamma_\lambda$

Por lo tanto

$$\bigcup_i \Gamma_\lambda \alpha_i \cdot \sum C_k \Gamma_\mu \xi_k = \sum_{i,k} C_k \Gamma_\lambda \alpha_i \xi_k$$

$$= \sum_{i,j} C_k \Gamma_\lambda \gamma_\lambda \alpha_i' \xi_k$$

$$= \sum C_k \Gamma_\lambda \alpha_i' \xi_k$$

$$= \bigcup \Gamma_\lambda \alpha_i' \cdot \sum C_k \Gamma_\mu \xi_k$$

también si $\Gamma_\mu \xi_k = \Gamma_\mu \delta_k \Longrightarrow \xi_k = \gamma_\mu \delta_k \quad \gamma_\mu \in \Gamma_\mu$ entonces $u \cdot \sum C_k \Gamma_\mu \xi_k = \sum C_k \Gamma_\lambda \alpha_i \xi_k = \sum C_k \Gamma_\lambda \alpha_i \gamma_\mu \delta_k$ como $\{\alpha_1, \ldots, \alpha_d\}$ es un sistema de representantes de las clases derechas $\Gamma_x \alpha_i$ en $\Gamma_\lambda \alpha \Gamma_\mu$, entonces $\{\alpha_1 \gamma_\mu, \ldots, \alpha_d \gamma_\mu\}$ también es un conjunto de representantes pues

$$\Gamma_\lambda \alpha_i \gamma_\mu = \Gamma_\lambda \alpha_j \gamma_\mu \iff \Gamma_\lambda \alpha_i = \Gamma \alpha_j$$

Es decir la definición no depende de la elección de $\{\alpha_i\}$ y $\{\xi_k\}$.

Por linealidad obtenemos un mapeo de $R_{\lambda\mu}$ en $\mathrm{Hom}(M_\mu \longrightarrow M_\lambda)$;

$$\varphi : R_{\lambda\mu} \longrightarrow \mathrm{Hom}(M_\mu \longrightarrow M_\lambda)$$

$$x \longrightarrow \varphi(x)$$

donde

$$\varphi(x) : M_\mu \longrightarrow M_\lambda$$

está definida por la correspondencia

$$\Sigma\, C_k \Gamma_\mu \xi_k \longrightarrow \varphi(x)(\Sigma\, C_k \Gamma_\mu \xi_k)$$

$$= X \cdot \Sigma C_k\, \Gamma_\mu \xi_k$$

$$= \sum_{i,k} C_k' (\Gamma_\lambda \alpha_i \Gamma_\mu) \Gamma_\mu \xi_k$$

Este mapeo es inyectivo. De hecho, si

$$\sum_\alpha C_\alpha \cdot (\Gamma_\lambda \alpha \Gamma_\mu) \cdot \Sigma d_k \Gamma_\mu \xi_k = 0 \qquad \ldots (*)$$

con $x = \sum_\alpha C_\alpha (\Gamma_\lambda \alpha \Gamma_\mu)$ donde $\Gamma_\lambda \alpha_i \Gamma_\mu \neq \Gamma_\lambda \alpha_j \Gamma_\mu$ $i \neq j$ entonces $\sum_\alpha C_\alpha (\Gamma_\lambda \alpha \Gamma_\mu) d_1 \Gamma_\mu \xi_1 + \ldots + \sum_\alpha C_\alpha (\Gamma_\lambda \alpha \Gamma_\mu) d_\nu \Gamma_\mu \xi_\nu = 0$ por lo tanto

$\sum_{\alpha} C_\alpha (\Gamma_\lambda \alpha \Gamma_\mu)\, d_k \Gamma_\mu \xi_k = 0 \quad k = 1, \ldots, \gamma$ pero $\sum_{\alpha} C_\alpha (\Gamma_\lambda \alpha \Gamma_\mu) d_k \Gamma_\mu \xi_k = \sum_{\alpha,i} C_k d_k \Gamma_\lambda \alpha_i \xi_k$ finalmente

$$\Gamma_\lambda \alpha_i \xi_k = \Gamma_\lambda \alpha_j \xi_k$$

para algunas α_i, α_j pero esto último implicaría que

$$\Gamma_\lambda \alpha_i \Gamma_\mu = \Gamma_\lambda \alpha_j \Gamma_\mu$$

Por lo tanto (*) es imposible. Así φ es inyectiva.

En seguida consideremos las descomposiciones ajenas

$$\Gamma_\lambda \alpha \Gamma_\mu = \cup_i \Gamma_\lambda \alpha_i, \quad \Gamma_\mu \beta \Gamma_\nu = \cup_j \Gamma_\mu \beta_j \quad \text{y} \quad \Gamma_\lambda \xi \Gamma_\nu = \cup_k \Gamma_\lambda \xi_k$$

entonces, tenemos

$$\{\Gamma_\lambda \alpha \Gamma_\mu \cdot \Gamma_\mu \beta \Gamma_\nu\} \cdot \Gamma_\nu \eta = \{\sum_{\xi} m(\Gamma_\lambda \alpha \Gamma_\mu \cdot \Gamma_\mu \beta \Gamma_\nu ; \Gamma_\lambda \xi \Gamma_\nu) \Gamma_\lambda \xi \Gamma_\nu\}\, \Gamma_\nu \eta$$

$$= \sum_{\xi,k} m(\Gamma_\lambda \alpha \Gamma_\mu \cdot \Gamma_\mu \beta \Gamma_\nu ; \Gamma_\lambda \xi \Gamma_\nu) \Gamma_\lambda \xi_k \eta$$

para cada k $m(\Gamma_\lambda \alpha \Gamma_\mu \cdot \Gamma_\mu \beta \Gamma_\nu ; \Gamma_\lambda \xi \Gamma_\nu) \Gamma_\lambda \xi_k = \sum_{i,j} \Gamma_\lambda \alpha_i \beta_j$ para algunas i,j.

Si recurremos todos los ξ obtenemos todos los i,j por lo tanto

$$\{(\Gamma_\lambda \alpha \Gamma_\mu) \cdot (\Gamma_\mu \beta \Gamma_\nu)\}\, \Gamma_\nu \eta = \sum_{ij} \alpha_i \beta_j \eta = \sum_j (\Gamma_\lambda \alpha \Gamma_\mu) \Gamma_\mu \beta_j \eta$$

$$= \Gamma_\lambda \alpha \Gamma_\mu \{(\Gamma_\mu \beta \Gamma_\nu) \cdot \Gamma_\nu \eta\}$$

esto demuestra que $(y.z).a = y(z.a)$ con $y \in R_{\mu\nu}$ $a \in M_\nu$ si además $x \in R_{k\lambda}$, tenemos

$$((x.y)z)a = (x.y)(z.a) = x(y.(z.a)) = (x.(y.z))a$$

por la inyectividad demostrada anteriormente, obtenemos

$$(x.y).z = x.(y.z)$$

Lema 1.6. Sea $a \in \tilde{\Gamma}$. Supongamos que el número de clases de la forma $\Gamma_\lambda \xi$ en $\Gamma_\lambda \alpha \Gamma_\mu$. Entonces existe un conjunto de representantes $\{\alpha_i\}$ tal que

$$\Gamma_\lambda \alpha \Gamma_\mu = \cup_i \Gamma_\lambda \alpha_i = \cup_i \alpha_i \Gamma_\mu$$

Demostración. Sean $\Gamma_\lambda \xi \subset \Gamma_\lambda \alpha \Gamma\mu$ y $\eta\Gamma_\mu \subset \Gamma_\lambda \alpha \Gamma_\mu$ entonces $\xi \in \Gamma_\lambda \alpha \Gamma_\mu = \Gamma_\lambda \eta \Gamma_\mu$ pues $\eta = \gamma_\lambda \alpha \gamma_\mu$ y por lo tanto $\xi = \delta\eta\varepsilon$ con $\delta \in \Gamma_\lambda$ $\varepsilon \in \Gamma_\mu$ sea $\zeta = \delta^{-1}\varepsilon$. Entonces

$$\Gamma_\lambda \xi = \Gamma_\lambda \zeta \quad y \quad \eta\Gamma_\mu = \zeta\Gamma_\mu$$

a decir ζ a un representante común para $\Gamma_\lambda \xi$ y $\eta\Gamma_\mu$. De esta manera si recorremos ξ y η encontramos un ζ representante para $\Gamma_\lambda \xi$ y $\eta\Gamma_\mu$.

Proposición 1.7. Sean $\alpha \in \tilde{\Gamma}$ y $\beta \in \tilde{\Gamma}$. Entonces

(i) $\Gamma_\lambda \alpha\beta\Gamma_\mu = (\Gamma_\lambda \alpha \Gamma_\lambda) \cdot (\Gamma_\lambda \beta \Gamma_\mu)$ si $\Gamma_\lambda \alpha = \alpha\Gamma_\lambda$

(ii) $\Gamma_\lambda \alpha\beta\Gamma_\mu = (\Gamma_\lambda \alpha \Gamma_\mu) \cdot (\Gamma_\mu \beta \Gamma_\mu)$ si $\Gamma_\mu \beta = \beta\Gamma_\mu$

La demostración es inmediata a partir de la definición de producto. De hecho si

$$U = \Gamma_\lambda \alpha \Gamma_\mu \quad y \quad U = \Gamma_\lambda \beta \Gamma_\mu$$

Entonces

$$(\Gamma_\lambda \alpha \Gamma_\lambda) \cdot (\Gamma_\lambda \beta \Gamma_\mu) = \sum_W m(U.V;\ W)W$$

donde $W = \Gamma_\lambda \xi \Gamma_\mu \subset \Gamma_\lambda \alpha \Gamma_\lambda \beta \Gamma_\mu = \Gamma_\lambda \alpha\beta \Gamma_\mu$

así que $m(U.V;\ W) = 1$ y sólo hay una clase $\Gamma_\lambda \xi \Gamma_\mu$ contenida en $\Gamma_\lambda \alpha \Gamma_\lambda \beta \Gamma_\mu$ que es $\Gamma_\lambda \alpha\beta \Gamma_\mu$.

De manera semejante se prueba (ii).

Consideremos un semigrupo Δ fijo tal que $\Gamma \subset \Delta \subset \tilde{\Gamma}$. Sea $R(\Gamma,\Delta)$ el $\mathbf{Z}$ módulo de todas las sumas finitas formales

$$\sum C_k \cdot \Gamma\ \alpha_k \Gamma$$

con $C_k \in \mathbf{Z}$ y $\alpha_k \in \Delta$. Con respecto a la ley de multiplicación introducida anteriormente $R(\Gamma,\Delta)$ es un anillo asociativo el - cual le llamaremos el anillo de Hecke con respecto a Γ y Δ. Obviamente $\Gamma = \Gamma 1 \Gamma$ es el elemento identidad.

Proposición 1.8. Si G tiene un antiautomorfimos $\alpha \longmapsto \alpha^*$ tal que $\Gamma^* = \Gamma$ y $(\Gamma \alpha \Gamma)^* = \Gamma \alpha \Gamma$ para todo $\alpha \in \Delta$, entonces $R(\Gamma,\Delta)$ es conmutativo. (Aquí un antiautomorfismo de G significa

un mapeo uno a uno de G sobre si mismo que satisface $(\alpha\beta)^* = \beta^*\alpha^*$,

Demostración

$$\Gamma\ \alpha\ \Gamma = (\Gamma\ \alpha\ \Gamma)^*$$

$$= (\cup\Gamma\alpha_i)^*$$

$$= \cup(\Gamma\alpha_i)^*$$

$$= \cup\alpha_i^*\Gamma$$

por lo tanto $\Gamma\ \alpha\ \Gamma = \cup\Gamma\alpha_i = \cup\alpha_i^*\Gamma$ i.e. hay tantas clases laterales izquierdas como derechas, por el lema 1.5 para cualquiera $\alpha, \beta \in \Delta$ podemos escribir

$$\Gamma\ \alpha\ \Gamma = \underset{i}{\cup}\Gamma\alpha_i = \cup\alpha_i\Gamma \qquad \text{y}$$

$$\Gamma\ \beta\ \Gamma = \underset{j}{\cup}\Gamma\beta_j = \underset{j}{\cup}\beta_j\Gamma$$

(todas las descomposiciones son ajenas). Entonces

$$\Gamma\ \alpha\ \Gamma = \Gamma\ \alpha^*\ \Gamma = \cup\Gamma\alpha_i^* \qquad \text{y}$$

$$\Gamma\ \beta\ \Gamma = \Gamma\ \beta^*\ \Gamma = \cup\Gamma\beta_j^*$$

Si $\Gamma\alpha\Gamma\ \beta\Gamma = \underset{\xi}{\cup}\ \Gamma\ \xi\ \Gamma$, entonces

$$\Gamma\alpha\Gamma\ \beta\Gamma = \Gamma\ \beta^*\ \Gamma\ \alpha^*\ \Gamma = (\Gamma\alpha\Gamma\ \beta\Gamma)^* = \underset{\xi}{\cup}\Gamma\ \xi\Gamma$$

Por lo tanto tenemos

$$(\Gamma\,\alpha\,\Gamma)\ \cdot\ (\Gamma\,\beta\,\Gamma) = \sum_{\xi} C_{\xi}\,(\Gamma\,\xi\,\Gamma)$$

y

$$(\Gamma\,\beta\,\Gamma)\ \cdot\ (\Gamma\,\alpha\,\Gamma) = \Sigma\ C'_{\xi}\,(\Gamma\,\xi\,\Gamma)$$

por la proposición 1.3, tenemos

$$C_{\xi}\ \text{grad}(\Gamma\,\xi\,\Gamma) = \#(\{(i,j)/\Gamma\alpha_i\beta_j\Gamma = \Gamma\,\xi\,\Gamma\})$$

aplicando * $$= \#(\{(i,j)/\Gamma\beta_j^{*}\,\alpha_i^{*}\Gamma = \Gamma\,\xi\Gamma\})$$

$$= C'_{\xi}\ \text{grad}(\Gamma\ \xi\ \Gamma).$$

de modo que

$$C_{\xi} = C'_{\xi}$$

esto completa la demostración.

CAPITULO 2

2. UNA SERIE DE DIRICHLET FORMAL CON UN PRODUCTO DE EULER.

En esta sección nos restringiremos al caso $G = GL_n(\mathbb{Q})$ y $\Gamma = SL_n(\mathbb{Z})$.

Sean $\gamma, \gamma' \in \Gamma$, $\gamma_1 = (\gamma_{ij})$ $\gamma' = (\gamma'_{ij})$ si N es un entero positivo escribiremos

$$\gamma \equiv \gamma' \quad \text{si} \quad \gamma_{ij} \equiv \gamma'_{ij} \bmod(N)$$

lo anterior define una relación de equivalencia con la propiedad de que si

$$\gamma_1 \equiv \gamma_2 \bmod(N) \quad \text{y} \quad \gamma_3 \equiv \gamma_4 \bmod(N)$$

entonces

$$\gamma_1 \gamma_3 \equiv \gamma_2 \gamma_4 \bmod(N)$$

y

$$\gamma_1^{-1} \equiv \gamma_2^{-1} \bmod(N)$$

por lo tanto $A \equiv B \bmod N$ si y solo si

$$AB^{-1} \equiv I_n \bmod(N)$$

---

donde I_n es la matriz identidad y $A,B \in SL_n(\mathbb{Z})$.

Denoraremos por Γ_N al conjunto de todas las matrices en Γ congruentes, módulo N, con la matriz identidad;

$$\Gamma_N = \{\gamma \in \Gamma / \gamma \equiv I \bmod(N)\}$$

Obviamente Γ_N es un subgrupo de Γ.

Si consideramos el mapeo

$$\lambda : SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$$

$$\gamma \longrightarrow \lambda(\gamma) = \gamma \bmod N$$

i.e. Si $\gamma = (\gamma_{ij})$ $\lambda(\gamma) = (\overline{\gamma}_{ij})$

donde

$$\overline{\gamma}_{ij} \equiv \gamma_{ij} \bmod(N)$$

λ así definido es un homomorfismo de $SL_2(\mathbb{Z})$ en $SL_2(\mathbb{Z}/N\mathbb{Z})$. Si logramos ver que λ es sobre, entonces λ nos induce un isomorfismo;

$$\lambda : SL_2(\mathbb{Z})/_{\text{Ker } \lambda} \longrightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$$

Note que $\text{Ker } \lambda = \Gamma_N$.

De esta manera tendríamos que

$$[\Gamma : \Gamma_N] < \infty$$

Antes de probar que λ es sobre, probemos el siguiente lema: Si $(m,n,N) = 1$, entonces existen enteros n', m' tales que $n' \equiv n \mod N$, $m' \equiv \mod N$ y $(n', m') = 1$. Notemos que si $(n, m, N) = 1$, entonces $(n, N) = 1$ o $(m, N) = 1$. Supongamos que $(n, N) = 1$, por el teorema de Dirichlet sobre progresiones aritméticas, ésto implica que la progresión $kN + n$ contiene una una infinidad de números primos. Sea $k_1 \in \mathbb{N}$ tal que $k_1N + n = m'$ es primo y n' un entero con $n' = k_2N + m$ $k_2 \in \mathbb{N}$. Entonces $(n', m') = 1$, $m' \equiv m \mod N$ y $n' \equiv n \mod N$.

Ahora bien si $\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$ es un elemento de $SL_2(\mathbb{Z}/N\mathbb{Z})$ y tomamos enteros a_1, b_1, c_1, d_1 que cumplan con

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \mod N = \begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix}$$

entonces $a_1 d_1 - b_1 c_1 \equiv 1 \mod N$

de modo que $(c_1, d_1, N) = 1$

por el lema anterior podemos suponer que $(c_1, d_1) = 1$. Sea n un entero tal que

$$a_1 d_1 - b_1 c_1 = 1 + nN.$$

como $(c_1, d_1) = 1$ podemos elegir enteros a_2, b_2 tales que

$$a_2 d_1 - b_2 c_1 = -n$$

si hacemos $a = a_1 + a_2N$, $b = b_1 + b_2 N$ $C_1 = C$ $d = d_1$ vemos que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

y

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod N = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$$

por lo tanto hemos demostrado el siguiente.

Lema 2.1. (1) Sea λ el homomorfismo de $SL_2(\mathbb{Z})$ en $SL_2(\mathbb{Z}/N\mathbb{Z})$ definido anteriormente. Entonces.

(1) λ es sobre.

(2) $\ker(\lambda) = \Gamma_N$ en particular Γ_N es subgrupo normal de Γ.

(3) $[\Gamma : N_N] < \infty$.

Lema 2.2. Sea $\beta \in M_n(\mathbb{Z})$, $\det(\beta) = b \neq 0$. Entonces $\Gamma_{Nb} \subset \beta^{-1}\Gamma_N \beta \cap \beta\Gamma_N\beta^{-1}$.

Demostración. Sea $\beta' = b\beta^{-1}$ como $\beta \in M_n(\mathbb{Z})$, si $\gamma \equiv 1_n \bmod(Nb)$, entonces tenemos:

$$\beta'\gamma\beta \equiv \beta'\beta = b.1_N \bmod(Nb)$$

por lo tanto

$$\beta^{-1}\gamma\beta \equiv 1_n \bmod(N)$$

Esto demuestra que

$$\beta^{-1}\gamma\beta \in M_n(\mathbb{Z})$$

Si $\gamma \in \Gamma_{Nb}$, tenemos $\det(\beta^{-1}\gamma\beta) = 1$ de modo que $\beta^{-1}\gamma\beta \in \Gamma_N$, por lo tanto

$$\gamma \in \beta\Gamma_N\beta^{-1}$$

de manera semejante se ve que $\gamma \in \beta^{-1}\Gamma_N\beta$.

Lema 2.3. $\widetilde{\Gamma} = GL_n(\mathbb{Q})$.

Demostración. Si $\alpha \in GL_n(\mathbb{Q})$ entonces $\alpha = C\beta$ con algún $C \in \mathbb{Q}$, $\beta \in M_n(\mathbb{Z})$, tenemos $\alpha\Gamma\alpha^{-1} = \beta\Gamma\beta^{-1}$, por el lema anterior $\Gamma \cap \beta\Gamma\beta^{-1} \supset \Gamma_b$ con $b = \det(\beta)$ como $[\Gamma : \Gamma_b] < \infty$, Tenemos $[\Gamma : \Gamma \cap \alpha\Gamma\alpha^{-1}] < \infty$ transformando por el automorfismo interno $\xi \longrightarrow \alpha^{-1}\xi\alpha$ y sustituyendo α^{-1} por α, obtenemos $[\alpha\Gamma\alpha^{-1} : \alpha\Gamma\alpha^{-1} \cap \Gamma] < \infty$ de modo que $\alpha \in \widetilde{\Gamma}$, la indusión inversa es obvia.

Sea $\Delta = \{\alpha \in M_n(\mathbb{Z})/\det(\alpha) > 0\}$ obviamente Δ es un semigrupo y $\Gamma \subset \Delta \subset \widetilde{\Gamma}$. Ahora determinaremos la estructura de $R(\Gamma,\Delta)$. Para n enteros $a_1,\ldots,a_n$ sea $\mathrm{diag}[a_1,\ldots,a_n]$ la matriz diagonal con elementos diagonales $a_1,\ldots,a_n$. En virtud de la teoría de los divisores elementales (lema siguiente) sabemos que los representantes para $\Gamma\backslash\Delta/\Gamma$ estan dados por $\mathrm{diag}[a_1,\ldots,a_n]$ con enteros positivos $a_1,\ldots,a_n$ tales que $a_i | a_{i+1}$. Entonces sabemos que la transposición $\xi \longrightarrow \xi^T$ es un antiautomorfismo de G y $(\Gamma\alpha\Gamma)^T = \Gamma\alpha\Gamma$ para toda clase doble $\Gamma\alpha\Gamma$. Por la proposición 1.8 esto demuestra que $R(\Gamma,\Delta)$ es conmutativo.

Nuestra próxima tarea es obtener una pequeña tabla de multiplicar de $R(\Gamma,\Delta)$.

La idea principal es asignar un retículo a cada clase Γ_α y contar el número de retículos en lugar de contar el número de clases. Para este propósito, sea.

$$V = Q^n = \text{Espacio Vectorial de todos los vectores renglón con componentes en } Q,$$

y sea $G = GL_n(Q)$ que actúa a la derecha de V. Llamaremos a un submódulo L de V, un retículo (más especificamente un $\mathbb{Z}$-retículo en V; si L es finitamente generado sobre $\mathbb{Z}$, y V es generado por L sobre Q. Los siguientes resultados son fáciles de deducir:

1) L es retículo en V $\Longleftrightarrow$ L es un $\mathbb{Z}$-módulo libre de rango n.

2) Si $\alpha \in G$ y L es retículo en V, entonces $L\alpha$ es un retículo en V.

3) Si W es un subespacio de V y L es un retículo en V entonces $L \cap W$ es un retículo en W.

4) Si L y M son retículos en V entonces:

   (i) $L+M$ y $L \cap M$ son retículos en V.

   (ii) existe un entero positivo C tal que CLCM.

Lema 2.4*. Sea L y M retículos en V. Entonces existen n elementos $u_1,\ldots,u_n$ de V y números racionales positivos $b_1,\ldots b_n$ tales que

$$L = \sum_{i=1}^{n} \mathbb{Z}u_i \quad M = \sum_{i=1}^{n} \mathbb{Z}b_i u_i \quad b_{i+1} \in b_i\mathbb{Z}.$$

Este es precisamente el teorema fundamental de los divisores elementales de M relativos a L, y escribiremos

$$\{L : M\} = \{b_1,\ldots,b_n\} = \{b_1\mathbb{Z},\ldots,b_n\mathbb{Z}\}$$

Si $M \subset L$ se tiene $[L : M] = b_1 \ldots b_n$.

En efecto si $M \subset L$, entonces $b_1,\ldots,b_n$ son enteros. Sea $u_1,\ldots,u_n$ una base de L y $b_1u_1,\ldots,b_nu_n$ una base de M, de modo que L/M es el producto directo de grupos cíclicos finitos de orden $b_1,\ldots,b_n$ por lo tanto $[L/M] = b_1 \ldots b_n$.

En particular si $\alpha = \text{diag}[b_1,\ldots,b_n]$, entonces $\{L : L\alpha\} = \{b_1,\ldots,b_n\}$.

De aquí en adelante denotaremos exclusivamente por L al retículo $\mathbb{Z}^n$.

Sean $\alpha \in \Gamma \subset G$ y $\ell \in L$, entonces

* Van der Waerden, B.L. Algebra (traducción 5a. edición), Ungar, 1970.

$$\ell\alpha = (\ell_1,\ldots,\ell_n) \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{bmatrix}$$

$$= \sum_{i=1}^{n} \ell_i\alpha_{i1},\ldots,\sum_{i=1}^{n} \ell_i\alpha_{in}$$

Este último vector pertenece a L pues $\ell_i\ \alpha_{ij}$ son enteros para todos i,j. Lo anterior nos permite afirmar que

$$\Gamma \subset \{\alpha \in G/L\alpha = L,\ \det \alpha > 0\}$$

De hecho la igualdad se satisface, para probarlo tomemos $\alpha' \in \{\alpha \in G/L\alpha = L \det\alpha > 0\}$ como $L\alpha' = L$ y $\det(\alpha') > 0$ existen $z_1,\ldots,z_n \in \mathbb{Z}^n$ con $z_i\alpha' = e_i = (0,\ldots,1,0,\ldots,0)$, 0

$$z\alpha' = I_n\ z = \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix},\ I_n = \begin{bmatrix} 1 & 0 & . & . & 0 \\ 0 & 1 & & & . \\ . & & . & & . \\ . & & & . & \\ 0 & . & . & & 1 \end{bmatrix}$$

y $\det(z.\alpha') = \det z.\det\alpha' = \det I_n = 1$. Obviamente $\det z \in \mathbb{Z}$ y $\det \alpha' \in \mathbb{Z}$ pues $e_i\alpha' = (\alpha_i,\ldots,\alpha_{in}) \in \mathbb{Z}^n$ por lo tanto $\det z = \det \alpha = 1$. En consecuencia

$$\Gamma = SL_n(\mathbb{Z}) = \{\alpha \in G/L\alpha = L \det \alpha > 0\}$$

———

Por otro lado $\Gamma_\alpha = \Gamma_\beta \iff L\alpha = L\beta$. Ya que si $\Gamma\alpha = \Gamma_\beta$ entonces $\Gamma\alpha\beta^{-1} = \Gamma$ y $\alpha\beta^{-1} \in \Gamma$ por lo anterior $L\alpha\beta^{-1} = L$ finalmente $L\alpha = L\beta$.

Lema 2.5. Sean M y N reticulos en V. Entonces $\{L : M\} = \{L : N\}$ si y solo si existe un elemento $\alpha \in \Gamma$, tal que $M\alpha = N$.

Demostración. Supongamos que existe $\alpha \in \Gamma$ tal que $M\alpha = N$. Entonces $L\alpha = L$ y

$$\{L : M\} = \{L\alpha : M\alpha\} = \{L : M_\alpha\} = \{L : N\}$$

inversamente si

$$\{L : M\} = \{L : N\} = \{a_1, \ldots, a_n\}$$

Entonces existen elementos u_i y v_i, $i = 1, 2, \ldots, n$, de v tales que

$$L = \sum_{i=1}^{n} \mathbb{Z}\, u_i = \sum_{i=1}^{n} \mathbb{Z}\, v_i$$

y

$$M = \sum_{i=1}^{n} \mathbb{Z}\, a_i u_i \qquad N = \sum_{i=1}^{n} \mathbb{Z}\, a_i v_i$$

Sea $\alpha \in G$ que satisfaga $u_i\alpha = v_i$. como $\{u_i\}$, $\{v_i\}$ son bases $\det\alpha = \pm 1$ si $\det\alpha = -1$ tomamos $-v_i$ en lugar de v_i de esta manera $\alpha \in \Gamma$, por lo tanto $L\alpha = L$ y $M\alpha = N$.

Sean $a_i (i = 1,2,\ldots,n)$ enteros positivos tales que a_{i+1} es divisible por a_i. Definimos

$T(a_1,\ldots,a_n) \in R(\Delta,\Gamma)$ como

$$T(a_1,\ldots,a_n) = \Gamma \alpha \Gamma \qquad \alpha = \mathrm{diag}[a_1,\ldots,a_n]$$

Como se observó antes, el anillo $R(\Delta,\Gamma)$ es generado por los $T(a_1,\ldots,a_n)$ sobre $\mathbb{Z}$.

En seguida se da la correspondencia entre las clases de $\Gamma\alpha\Gamma$ y ciertos retículos, mas precisamente tenemos el siguiente.

Lema 2.6. Sea $\Gamma\alpha\Gamma = T(a_1,\ldots,a_n)$ entonces $\Gamma\xi \longrightarrow L\xi$ da una correspondencia uno a uno entre las clases $\Gamma\xi$ de $\Gamma\alpha\Gamma$ y los retículos M tales que $\{L : M\} = \{a_1,\ldots,a_n\}$.

Demostración. Podemos asumir que $\alpha = \mathrm{diag}[a_1,\ldots,a_n]$ si $\Gamma\xi = \Gamma\alpha\delta$ con $\delta \in \Gamma$, tenemos

$$\{L : L\xi\} = \{L : L\alpha\delta\} = \{L : L\alpha\} = \{a_1,\ldots,a_n\}$$

Inversamente, si $\{L : M\} = \{a_1,\ldots,a_n\}$ entonces por el lema 2.5 existe $\gamma \in \Gamma$ tal que $M = L\alpha\gamma$. Obviamente $\Gamma\alpha\gamma \subset \Gamma\alpha\Gamma$, esta correspondencia; $\Gamma\xi \longrightarrow L\xi$ es uno a uno, puesto que $\Gamma\xi = \Gamma\eta$ si y solo si $L\xi = L\eta$.

Proposición 2.7. El grado de $T(a_1,\ldots,a_n)$ coincide con el número de retículos M tales que $\{L : M\} = \{a_1,\ldots,a_n\}$.

Demostración. Como el grado de $T(a_1,\ldots,a_n)$ es el número de clases $\Gamma\xi$ contenidas en T la proposición es consecuencia inmediata del lema anterior.

Proposición 2.8. Si $(\Gamma\alpha\Gamma).(\Gamma\beta\Gamma) = \sum_{\xi} C_\xi \Gamma\xi\Gamma$ con $C_\xi \in \mathbb{Z}$. Entonces C_ξ es el número de retículos M tales que $\{L : M\} = \{L : L\beta\}$ y $\{M : L\xi\} = \{L : L\alpha\}$.

Demostración. Sean $\Gamma\alpha\Gamma = \bigcup_i \Gamma\alpha_i$ y $\Gamma\beta\Gamma = \bigcup_j \Gamma\beta_j$ (ambas descomposiciones ajenas). Entonces

$$C_\xi = \#\{(i,j)/\Gamma\alpha_i\beta_j = \Gamma_\xi\} = \#\{(i,j)/L\alpha_i\beta_j = L\xi\}$$

Note que i está univocamente determinado por ξ y j. Supongamos que $L\alpha_i\beta_j = L\xi$ y sea $M = L\beta_j$. Entonces, dado que $L\beta_j = L\beta\gamma_i$ $\gamma_i \in \Gamma$, se tiene

$$\{L : M\} = \{L : L\beta\} \quad \text{por lema}$$

y $$\{M : L\xi\} = \{L\beta_j : L\alpha_i\beta_j\} = \{L : L\alpha_i\} = \{L : L\alpha\}$$

Inversamente, sea M un retículo tal que

$$\{L : M\} = \{L : L\beta\} \text{ y } \{M : L\xi\} = \{L : L\alpha\}$$

Por lema 2.5 $M = L\beta\gamma_i = L\beta_i$, $\gamma_i \in \Gamma$ para alguna i. Entonces $\{L : L\xi\beta_j^{-1}\} = \{L\beta_j : L\xi\} = \{L : L\alpha\}$. Nuevamente por lema $L\xi\beta_j^{-} = L\alpha_i$ para alguna i y $L\xi = L\alpha_i\beta_j$. Así cada M determina un par (i,j) e inversamente. Esto demuestra la proposición.

Proposición 2.9. Sean α y β elementos de $\Delta = \{\alpha \in M_n(\mathbb{Z}) / \det\alpha > 0\}$ tal que $(\det(\alpha), \det(\beta)) = 1$. Entonces $(\Gamma\alpha\Gamma).(\Gamma\beta\Gamma) = \Gamma\alpha\beta\Gamma$. En otras palabras, $T(a_1,\ldots,a_n).T(b_1,\ldots,b_n) = T(a_1b_1,\ldots,a_nb_n)$ si $(a_n,b_n) = 1$.

Demostración. Sea $\xi \in \Gamma\alpha\Gamma\beta\Gamma$. Sean M y M' tales que $\{L : M\} = \{L : M'\} = \{L : L\beta\}$ y $\{M : L\xi\} = \{M' : L\xi\} = \{L : L\alpha\}$.

Por lo tanto como

$$[M + M' : M] = [M' : M \cap M'] \qquad (*)$$

y dado que $M + M' \subset L$ y $L\xi \subset M \cap M'$ se tiene

$$[L : M] = [L : M + M'][M + M' : M] \qquad (**)$$

y

$$[M' : L\xi] = [M' : M \cap M'] \; [M \cap M' : L\xi] \qquad (***)$$

i.e. El lado izquierdo de (*) es un divisor de $[L : M]=\det(\beta)$, y el lado derecho es un divisor de $[M' : L\xi] = \det(\alpha)$. Pero $(\det\alpha, \det\beta) = 1$ por lo tanto

$$M' = M \cap M' \quad y \quad M = M \cap M'$$

Esto implica que $M' \subset M$ y que $M \subset M'$ por lo tanto $M = M'$. Si tomamos en cuenta la proposición 2.8 lo anterior significa que la multiplicidad de $\Gamma\xi\Gamma$ en $\Gamma\alpha\Gamma \cdot \Gamma\beta\Gamma$ es uno. Ahora si $\xi \in \Gamma\alpha\Gamma\beta\Gamma$, podemos determinar al menos una M como antes. Dado que $L\xi \subset M \subset L$ consideremos el homomorfismo

$$f' : L/L\xi \longrightarrow L/M$$

$$\ell + L\xi \longmapsto \ell + M$$

el núcleo de f' es $M/L\xi$; Ker $f' = M/L\xi$ por lo tanto f' nos induce un isomorfismo

$$f : (L/L\xi)/(M/L\xi) \longrightarrow L/M$$

De aquí que $L/L\xi = (L/M) \oplus (M/L\xi)$ pero $M/L\xi \simeq L/L\alpha$ y $L/M \simeq L/L\beta$ además $(\det\alpha, \det\beta) = 1$ por lo tanto

$$L/L\xi \simeq (L/L\alpha) \oplus (L/L\beta)$$

por lo tanto los divisores elementales de $L\xi$ relativos a L están completamente determinados por α y β. Esto demuestra que $\Gamma\alpha\Gamma\beta\Gamma$ consiste de una sola clase doble, la cual es obviamente $\Gamma\alpha\beta\Gamma$.

De la proposición anterior, se sigue que todo $T(a_1,\ldots,a_n)$ es un producto de elementos de la forma $T(p^{e_1},\ldots,p^{e_n})$ con p primo y exponentes $0 \leq e_1, <\ldots< e_n$, y tal expresión es única. Para cada primo p, sea $R_p^{(n)}$ el subanillo de $R(\Gamma,\Delta)$ generado por los elementos $T(p^{e_1},\ldots,p^{e_n})$. Entonces nos restringiremos al estudio de la estructura de $R_p^{(n)}$. Antes de iniciar esta tarea, notemos el siguiente hecho.

Proposición 2.9. $T(c,\ldots,c).T(b_1,\ldots,b_n) = Y(cb_1,\ldots,cb_n)$

Demostración. Como $\Gamma c\Gamma\beta\Gamma = \Gamma c\beta\Gamma$, donde $C = \text{diag}[c,\ldots,c]$, sólo hay una clase $\Gamma\xi\Gamma$ contenida en $\Gamma c\Gamma\beta\Gamma$, y esta es de multiplicidad uno pues $\#\{(i,j)/\Gamma c\beta_j = \Gamma_\xi\}$ es uno.

Ahora fijemos un primo p estudiaremos la estructura de $R_p^{(n)}$. Consideremos a $(\mathbf{Z}/p\mathbf{Z})^n = L/pL$ como un espacio vectorial de dimensión n sobre el campo primo $\mathbf{Z}/p\mathbf{Z}$.

Proposición 2.10. Sea $C_k^{(n)}$ el número de subespacios de dimensión k de $(\mathbf{Z}/p\mathbf{Z})^n$. Entonces

$$C_k^{(n)} = C_{(n-k)}^n = \text{grad}(T(\underbrace{1,\ldots,1}_{n-k}, \underbrace{p,\ldots,f}_{k}))$$

La idea de la demostración es sencilla, sabemos por la Proposición 2.7 que $\text{grad}(T(a_1,\ldots,a_n))$ coincide con el número de retículos M tales que

$$\{L : M\} = \{a_1,\ldots,a_n\}.$$

Entonces a cada retículo M con $\{L : M\} = \{1,\ldots,1.p,\ldots,p\}$ le asociaremos un subespacio vectorial de L/pL de dimensión $n-k$ y recíprocamente a cada subespacio de dimensión $n-k$ le asociaremos un retículo M tal que $M/pL = K$ y

$$\{L : M\} = \{1,\ldots,1,p,\ldots,p\} \text{ con } n-k \text{ unos}$$

Demostración. La igualdad $C_k^{(n)} = C_{n-k}^{(n)}$ es bien conocida. Para conectarla con el grado de T, usaremos la proposición 2.7. Sean $\mathbb{Z}^n = \mathbb{Z}u_1+\ldots+\mathbb{Z}u_n$ y $M = \mathbb{Z}u_1+\ldots+\mathbb{Z}u_{n-k}+\mathbb{Z}u_{n-k+1}p+\ldots+\mathbb{Z}u_np$.

Entonces

$$\{L : M\} = \{1,\ldots,1,p,\ldots,p\}$$

Con $n-k$ unos y k p's. Entonces

$$PL \subset M \subset L$$

pero $[L : M] = p^k$ entonces $[M : PL] = p^{n-k}$ i.e. M/PL tiene dimensión $n-k$.

Inversamente, para todo subespacio k, de dimensión n-k, de L/pL si $K = \mathbb{Z}_p u_{i_1} + \mathbb{Z}_p u_{i_2} + \ldots + \mathbb{Z}_p u_{i_{(n-k)}}$ sea

$M = \mathbb{Z}u_{i_1} + \mathbb{Z}u_{i_2} + \ldots + \mathbb{Z}u_{i_{(n-k)}} + \mathbb{Z}u_{i_{(n-k+1)}}\, p + \ldots + \mathbb{Z}u_n\, p$

vamos a probar que $K = M/PL$. Es claro de $K \subset M/PL$. Entonces

$$z_1 u_{i_1} + \ldots + z_{n-k} u_{i_{(n-k)}} + z_{n-k+1} u_{i_{(n-k+1)}} p + \ldots + z_n u_n p + \mathbb{Z}pu_{i_1} + \ldots + \mathbb{Z}pu_n$$

$$= (z_1 + \mathbb{Z}p)u_{i_1} + (z_{n-k} + \mathbb{Z}_p)u_{i_{(n-k)}} + \mathbb{Z}pu_{i_{(n-k+1)}} + \ldots + \mathbb{Z}pu_n$$

$$\in \mathbb{Z}_p u_{i_1} + \mathbb{Z}_p u_{i_1} + \ldots + \mathbb{Z}_p u_{i_{(n-k)}} + 0 + \ldots + 0 = K$$

Esto último prueba que $M/PL \subset K$. Veamos ahora que dimensión tiene $K.[L : M] = p^k$ por lo tanto $[M : PL] = p^{n-k}$ i.e. $M/PL = K$ tiene dimensión n-k.

L ó anterior junto con la proposición 2.7 muestran la igualdad.

Definamos un mapeo $\mathbb{Z}$-lineal $\psi : R_p^{(n+1)} \longrightarrow R_p^{(n)}$

como $$\psi(T(1, p^{a_1}, \ldots, p^{a_n})) = T(p^{a_1}, \ldots, p^{a_n})$$

y $$\psi(T(p^{a_0}, p^{a_1}, \ldots, p^{a_n})) = 0 \quad \text{si } a_0 > 0.$$

Entonces

Lema 2.11. ψ es un homomorfismo suprayectivo, y Ker (ψ) coincide con $T(p_1, \ldots, p).R_p^{(n+1)}$.

Demostración. La suprayectividad es obvia, la igualdad $\mathrm{Ker}(\psi) = T(p,\ldots,p)R_p^{(n+1)}$ se sigue de la proposición 2.9 y la definición de ψ. Para simplificar el resto de la demostración pondremos

$$e' = \{1,p^{a_1},\ldots,p^{a_n}\} \qquad c = \{p^{a_1},\ldots,p^{a_n}\}$$

$$f' = \{1,p^{b_1},\ldots,p^{b_n}\} \qquad f = \{p^{b_1},\ldots,p^{b_n}\}$$

$$g' = \{1,p^{c_1},\ldots,p^{c_n}\} \qquad g = \{p^{c_1},\ldots,p^{c_n}\}$$

$$\mu g = m(T(e).T(f);\ T(g)) \qquad \mu g' = m(T(e).T(f');\ T(g'))$$

Entonces tenemos

$$T(e').T(f') = \Sigma\ g''T(g'')$$

Agrupemos aquellos sumandos de la forma $\mu g'T(g')$ por un lado y el resto en $T(p,\ldots,p).X$, $X \subset R_p^{(n+1)}$ por lo tanto

$$T(e').T(f') = \sum_{T(g')} \mu g'T(g') + T(p,\ldots,p).X$$

aplicando ψ obtenemos

$$\psi(T(e').T(f')) = \Sigma \mu g'\psi(T(g')) = \Sigma \mu g'T(g)$$

además $T(e).T(f) = \Sigma \mu g\ T(g)$. Por lo tanto si probamos que $\mu g = \mu g'$ habremos terminado.

Sean $L' = \mathbb{Z}^{n+1} = \sum_{i=0}^{n} \mathbb{Z}u_i$, $L = \sum_{i=1}^{n} \mathbb{Z}u_i$

$N' = \mathbb{Z}_0 + \sum_{i=1}^{n} \mathbb{Z}p^{ci}u_i$, $N = \sum_{i=1}^{n} \mathbb{Z}p^{ci}u_i$

Note que $N' = \mathbb{Z}u_0 + N$ y $L' = \mathbb{Z}u_0 + L$

Entonces

$$\{L : N\} = \{p^{c1}, \ldots, p^{cn}\} = g$$

y

$$\{L' : N'\} = \{1, p^{c1}, \ldots, p^{cn}\} = g'$$

A hora por proposición 2.8.

$$\mu g = \#\{M / \{L : M\} = f, \ \{M : N\} = e\}$$

$$\mu g' = \#\{M' / \{L' : M'\} = f', \{M', N'\} = e'\}$$

Probaremos que dado M' con $\{L' : M'\} = f'$ y $\{M' : N'\} = e'$ este nos determina de manera única un M que satisface $\{L : M\} = f$ y $\{M : N\} = e$ y viceversa.

Sea M' que satisface $\{L' : M'\} = f'$ y $\{M' : N'\} = e'$ de la primera igualdad vemos que $M' = \mathbb{Z}u_0 + \sum_i \mathbb{Z}p^{bi}u_i = \mathbb{Z}u_0 + \Sigma\mathbb{Z}u_i$ y de la segunda deducimos que $N' = \mathbb{Z}u_0 + \Sigma\mathbb{Z}p^{ai}v_i$. Entonces $u_0 \in N' \subset M'$ sea $M = M \cap L$ i.e. $M = \Sigma\mathbb{Z}p^{bi}u_i = \mathbb{Z}v_i$ entonces $M' = \mathbb{Z}u_0 + M$. Ahora bien $\{L : M\} = f$ y $\{M : N\} = e$ nuestra primera igualdad se obtiene de las expresiones $L = \Sigma\mathbb{Z}u_i$ y $M = \Sigma\mathbb{Z}p^{bi}u_i$, y la segunda de $M = \Sigma\mathbb{Z}v_i$ y $N = \Sigma\mathbb{Z}p^{ai}v_i$. El inver

so se hace de manera semejante. Esto completa la demostración.

Teorema 2.12. El anillo $R_p^{(n)}$ es el anillo de polinomios sobre $\mathbb{Z}$ en n elementos

$$T(1,\ldots,1,p),T(1,\ldots,1,p,p),\ldots,T(p,p,\ldots,p)$$

los cuales son algebraicamente independientes. En especial $R_p^{(n)}$ no tiene divisores de cero (diferentes del cero).

Demostración. Usaremos inducción sobre n. Para $n=1$, la proposición es clara puesto que $T(p^a) = T(p)^a$ por proposición 2.9. Por lo tanto supondremos que $n > 1$, y que la proposición es verdadera para $n-1$. Para toda $\Gamma\alpha\Gamma$ con $\det(\alpha) = p^\nu$, pongamos $\omega(\Gamma\alpha\Gamma) = \nu$, y para $X = \sum_k c_k.\Gamma\alpha_k\Gamma \in R_p^{(n)}$, definimos $\omega(X)$ como el máximo de los $\omega(\Gamma\alpha_k\Gamma)$ con $c_k \neq 0$. Llamaremos a X homogéneo si los $\omega(\Gamma\alpha_k\Gamma)$ son los mismos para toda $c_k \neq 0$. En particular $T(p^{a_1},\ldots,p^{a_n})$ es homogéneo, y $\omega(T(p^{a_1},\ldots,p^{a_n})) = a_1+a_2+\ldots+a_n$. Sea $T_k^{(n)} = T(1,1,\ldots,1,p,\ldots,p)$ con $n-k$ 1's y k p's. Utilizaremos inducción sobre ω para probar que todo elemento X de $R_p^{(n)}$ es un polinomio en $T_1^{(n)},\ldots,T_n^{(n)}$. Consideraremos únicamente los generadores, es decir elementos de la forma $X = T(p^{a_1},\ldots,p^{a_n})$, si $a_1 > 0$, tenemos por el lema 2.9.

$$T(p^{a_1},\ldots,p^{a_n}) = T(p,\ldots,p)T(p^{a_1-a},\ldots,p^{a_{n-1}}),$$

de modo que nuestro problema se reduce a un elemento con ω menor. (Note que $\omega(X) = 0$ si y solo si X es constante i.e. un elemento de $\mathbb{Z}$). Por lo tanto supondremos que $a_1 = 0$. Consideremos el homomorfismo $\psi : R_p^{(n+1)} \longrightarrow R_p^{(n)}$ obtenido en el lema 2.11. Por hipótesis de inducción, tenemos

$$\psi(X) = T(P^{a_2},\ldots,p^{a_n}) = \sum_k u_k . M_k(T_i^{(n-1)}),$$

donde $u_k \in \mathbb{Z}$, y los $M_k(T_i^{(n-1)}$ son monomios en $T_1^{(n-1)},\ldots,T_{n-1}^{(n-1)}$. Note que cada $M_k(T_i^{(n-1)})$ es homogéneo. Por lo tanto supondremos que $\omega(M_k(T_i^{(n-1)})) = \omega(X)$ $\forall_k$, puesto que no hay cancelación entre elementos homogéneos con ω's distintos. Si sustituimos $T_i^{(n)}$ por $T_i^{(n-1)}$ y hacemos

$$Y = \sum_k u_k . M_k(T_1^{(n)},\ldots,T_{n-1}^{(n)})$$

Como $\omega(T_i^{(n)}) = i$ entonces $\omega(M_k(T_1^{(n)})) = \omega(X)$. Ahora como $\psi(X - Y) = 0$ existe un elemento Z de $R_p^{(n)}$ tal que $X - Y = T(p,\ldots,p).Z$ como $\omega(X) = N_k\, \omega(M_k(T_1^{(n-1)})$ entonces $\omega(Z) < \omega(X)$. Nuestra hipótesis de inducción no dice que Z es un polinomio en $T_i^{(n)}$ por lo tanto $X \in \mathbb{Z}[T_1^{(n)},\ldots,T_n^{(n)}]$.

Para demostrar la independencia algebraica de los $T_i^{(n)}$. Supondremos que ellos son algebraicamente dependientes. Sea

$P(T_1^{(n)},\ldots,T_n^{(n)}) = 0$ una relación polinomial en $T_1^{(n)},\ldots,T_n^{(n)}$ $P \neq 0$. Expresamos P en la forma

$$P(T_1^{(n)},\ldots,T_n^{(n)}) = \sum_{i=k}^{i} (T_n^{(n)})^i P_i(T_1^{(n)},\ldots,T_{n-1}^{(n)})$$

donde $P_k \neq 0$. Como $T_k^{(n)}$ no es un divisor de cero, tenemos

$$0 = \sum_{i=k}^{i} (T_n^{(n)})^{i-k} P_i(T_1^{(n)},\ldots,T_{n-1}^{(n)})$$

Aplicando ψ, obtenemos $P_k(T_1^{(n-1)},\ldots,T_{n-1}^{(n-1)}) = 0$ inductivamente tenemos $P_k = 0$. Contradicción. Esto completa la demostración.

Del teorema 2.12 se sigue que todo el anillo $R(\Gamma,\Delta)$ es un anillo de polinomios sobre $\mathbb{Z}$ con una infinidad de indeterminadas de la forma $T(1,\ldots 1,p,\ldots,p)$ donde p es un primo. En particular $R(\Gamma,\Delta)$ es un dominio entero.

Para todo entero positivo m, $T(m)$ denotará la suma de todos los $\Gamma\alpha\Gamma$ con $\alpha \in \Delta$ y $\det(\alpha) = m$. Ahora consideraremos una serie de Dirichlet formal (con coeficientes en $R(\Gamma,\Delta)$)

$$D(S) = \sum_{m=1}^{\infty} T(m) m^{-s} = \sum_{\Gamma\backslash\Delta/\Gamma} (\Gamma\alpha\Gamma).\det(\alpha)^{-s},$$

Donde la última suma se toma sobre todas las clases dobles distintas $\Gamma\alpha\Gamma$ con α en Δ. De la proposición 2.9 sabemos que $\Gamma\alpha\Gamma \cdot \Gamma\beta\Gamma = \Gamma\alpha\beta\Gamma$ donde $\alpha = \mathrm{diag}[a_1,\ldots,a_1]$ $\beta = \mathrm{diag}[b_1,\ldots,b_n]$

y $(a_n, b_n) = 1$ por lo tanto $T(m).T(m') = \Sigma\Gamma\alpha\Gamma \,.\, \Sigma\Gamma\beta\Gamma$ con $\det\alpha = m$ $\det(\beta) = m'$, i.e. $T(m).T(m') = \sum_{\alpha,\beta} \Gamma\alpha\beta\Gamma = T(m'm')$ esto sucede si $(\det(\beta), \det(\alpha)) = 1$. Resumiendo $T(m).T(m') = T(m.m')$ si $(m, m') = 1$. Por lo tanto $D(s)$ se puede escribir (formalmente) como un producto infinito

$$D(S) = \prod_p \left[\sum_{k=0}^{\infty} T(p^k) p^{-ks} \right],$$

donde p corre sobre todos los primos. Por nuestra definición de $T(m)$ tenemos

$$\sum_{k=0}^{\infty} T(p^k) X^k = \sum_{0 \leq e_1 \leq \ldots \leq e_n} T(p^{e_1}, \ldots, p^{e_n}) X^{e_1 + \ldots + e_n}$$

donde X es una indeterminada. Ahora demostraremos que esta serie formal de potencias es en realidad una expresión racional en X:

Teorema 2.13. Sea $T_i^{(n)} = T(1, \ldots, 1, p, \ldots, p)$ con $n - i$ 1's e i p's, y sea X una indeterminada entonces

$$\sum_{k=0}^{\infty} T(p^k) X^k = \left[\sum_{i=1}^{n} (-1)^i p^{i(i-1)/2} T_i^{(n)} X^i \right]^{-1},$$

y por lo tanto

$$\sum_{n=1}^{\infty} T(m) m^{-s} = \prod_p \left[\sum_{i=0}^{n} (-1)^i p^{i(i-1)/2} T_i^{(n)} p^{-is} \right]^{-1}$$

donde el producto se extiende sobre todos los primos p. Primero demostraremos dos lemas.

Lema 2.14. Sean los enteros $C_i^{(k)}$ como en la proposición 2.10. Entonces

$$T_i^{(n)}X^i \cdot (\sum_{m=0}^{\infty} T(p^m)X^m)$$

$$= \sum_{k=0}^{n} C_i^{(k)} \cdot \{ \sum_{1 \leq d_1 \leq \ldots \leq d_k} T(1,\ldots,1,p^{d_1},\ldots,p^{dk})X^{d_1+\ldots+d_k} \}$$

se entiende que $C_i^{(k)} = 0$ si $i > k$, y $C_0^{(n)} = 1$.

Demostración. Fijemos un conjunto de exponentes $\{d_1,\ldots,d_k\}$, y denotemos con $\mu(d)$ el coeficiente de $T(1,\ldots 1,p^{d_1},\ldots,p^{dk})X^{d_1+\ldots+dk}$ en el producto $T_i^{(n)}X^i \cdot (\sum_{m=0}^{\infty} T(p^m)X^m)$. Observese que dicho término aparece en $T_i^{(n)} X^i T(p^n)X^m$ solo si $i+m = d_1+\ldots+d_k$. Fijemos un retículo N que satisfaga $\{L : N\} = \{1,\ldots,1,1,p^{d_1},\ldots,p^{dk}\}$ por la proposición 2.8.

$$\mu(d) = \sum_{\alpha} \#\{M/\{L : M\} = \{1,..1,p,\ldots,p\},\ \{M : N\} = \{L : L\alpha\}$$

donde la suma se extiende sobre todas las $\Gamma\alpha\Gamma$ con $\det(\alpha) = p^m$ y $\alpha \in \Delta$. (aquí y en lo que sigue el número de repeticiones de p es siempre i). Si $\{L : M\} = \{1,\ldots,1,p,\ldots,p\}$ y $N \subset M$, podemos encontrar α de Δ que satisfaga $\{M : N\} = \{L : L\alpha\}$, y obviamente $\det(\alpha) = p^m$. Por lo tanto $\mu(d)$ es el número de retículos M que satisfacen

(*) $\qquad N \subset M, \quad \{L : M\} = \{1,..,1,p,\ldots,p\}$

---

tomemos una base $\{u_i\}$ de modo que $L = \sum_{\nu=1}^{n} \mathbf{Z}u_\nu$, y

$$N = \sum_{\nu=1}^{n-k} \mathbf{Z}u_\nu + \sum_{\nu=1}^{k} \mathbf{Z}p^{d\nu}u_{n-k+\nu} .$$

Entonces $PL + N = \sum_{\nu=1}^{n-k} \mathbf{Z}u_\nu + \Sigma \mathbf{Z}pu_{n-k+\nu}$, por lo tanto $L/(pL + N)$ es isomorfo a $(\mathbf{Z}/p\mathbf{Z})^n$. Si M satisface (*), tenemos $PL + N \subset M$, y L/M es isomorfo a $(\mathbf{Z}/p\mathbf{Z})^i$. Por lo tanto $\mu(d) \neq 0$ solo si $i \leq k$. Supongamos que $i \leq k$ vemos que $M/(PL + N)$ es un subespacio de $L/(PL + N)$ de dimensión $k-i$. Inversamente, cualquier subespacio de dimensión $(k-i)$ de $L/(PL + N)$ puede escribirse en la forma $M/(PL + N)$ con M única que satisfaga (*).

Así tenemos $\mu(d) = C_i^{(k)}$ con esto completamos la demostración.

Lema 2.15. $\sum_{i=0}^{k-1} (-1)^i p^{i(i-1)/2} C_i^{(k)} = 0$ si $k > 0$.

Demostración. Sea $f(X) = \prod_{i=0}^{k} (X - p^i)$. Entonces

$$1 = \sum_{i=0}^{k-1} f(X)/[f'(p^i)(X - p^i)],$$

puesto que el lado derecho es un polinomio de grado $< k$ el cual toma el valor 1 en k puntos $p^0, p^1, \ldots, p^{k-1}$. (Sustituyendo p^k por X). Entonces.

$$1 = \sum_{i=0}^{k-1} C_i^{(k)} (-1)^{k-i-1} p^{(k-1)(k-i-1)/2}$$

$$= \sum_{j=1}^{k} C_j^{(k)} (-1)^{j-1} p^{j(j-1)/2}$$

que es lo que se quería demostrar.

Demostración del Teorema 2.13.

Consideremos el producto

$$[\sum_{i=0}^{n} (-1)^i p^{i(i-1)/2} T_i(n) X^i] \; [\sum_{n=0}^{\infty} T(p^m) X^m]$$

por el lema 2.14, esto es igual a

$$\sum_{i=0}^{n} (-1)^i p^{i(1-1)/2} \sum_{k=1}^{n} C_i^{(k)} \{\Sigma\, T(1,\ldots,1,p^{d_1},\ldots,p^{dk}) X^{d_1+\ldots+dk}\}$$

por el lema 2.15, únicamente el término con $k = 0$ es no nulo y este término es precisamente 1, con esto concluimos la demostración.

Si $n = 1$ el Teorema 2.13 nos dice que

$$\sum_{m=1}^{\infty} T(m) m^{-s} = \prod_p [1 - T(p) p^{-s}]^{-1}$$

y si $n = 2$ podemos escribir el Teorema 2.13 como

$$(**) \qquad \sum_{m=1}^{\infty} T(m) m^{-s} = \prod_p [1 - T(1,p) p^{-s} + T(p,p) p^{1-2s}]^{-1}$$

(Nótese que $T(1,p) = T(p)$).

Teorema 2.16. Si $n=2$, y p denota un primo, entonces las siguientes fórmulas se cumplen.

(1) $$T(m) = \sum_{ad/m} T(a,d)$$

(2) $$T(1,p^k) = T(p^k) - T(p,p)T(p^{k-2}) \qquad (k \geq 2)$$

(3) $$T(m)T(n) = \sum_{d(m,n)} d.T(d,d)T(m.n/d^2)$$

(4) $$T(p^r)T(p^s) = \sum_{\ell=0}^{r} p^{\ell}T(p^{\ell},p^{\ell})T(p^{r+s-2\ell}) \qquad (r \leq s)$$

(5) $$T(p)T(1,p^k) = T(1,p^{k+1}) + \begin{cases} (p+1)T(p,p) & (k=1) \\ pT(p,p^k) & (k>1) \end{cases}$$

(6) $$\text{grad}(T(1,p^k) = \text{grad}(T(p^i,p^{i+k})) = p^{k-1}(p+1), \quad (k>0)$$

(7) $$\text{grad}(T(m)) = \text{la suma de los divisores positivos de } m.$$

Demostración. Las primeras dos relaciones son obvias. Como $R_p^{(2)}$ es un anillo de polinomios $\mathbb{Z}[T(p), T(p,p)]$, podemos sumergir $R_p^{(2)}$ es un anillo de polinomios $Q[A,B]$ con dos indeterminadas A,B de modo que

$$1 - T(p)X + pT(p,p)X^2 = (1-AX)(1-BX)$$

Entonces

$$\sum_{m=0}^{\infty} T(p^m)X^{m+1} = [(1-AX)^{-1} - (1-BX)^{-1}]/(A-B)$$

$$= \sum_{m=0}^{\infty} (A^m - B^m)X^m/A - B$$

de modo que $T(p^m) = (A^{m+1} - B^{m+1})/A - B = \sum_{t=0}^{m} A^{m-\tau} B^{\tau}$ por lo tanto

$$\Delta T(p^r).T(p^s) = [A^{s+1}T(p^r) - B^{s+1}T(p^r)] / (A-B)$$

$$= (A^{s+1} \sum_{\ell=0}^{r} A^{r-\tau}B^{\tau} - B^{s+1} \sum_{\ell=r}^{r} A^{\tau}B^{r-\tau}) / (A-B$$

$$= \sum_{\ell=0}^{r} A^{\tau}B^{\tau}(A^{r+s-2\tau+1} - B^{r+s-2\tau+1}) / (A-B)$$

$$= \sum_{\ell=0}^{r} p^{\tau}T(p^{\tau}, p^{\tau})T(p^{r+s-2\tau}).$$

con esto demostramos (4). Observese que (4) es un caso especial de (3). Por lo tanto (3) se sigue de (4) y (**). Si $k = 1$, (5) es un caso especial de (4). Si $k > 1$, obtenemos de (2) y (4)

$$T(p)T(1,p^k) = T(p^{k+1}) + T(p,p)[pT(p^{k-1}) - T(p)T(p^{k-2})]$$

$$= T(1,p^{k+1}) + T(p,p)[(p+1)T(p^{k-1}) - T(p)T(p^{k-1})]$$

El término $T(p)T(p^{k-2})$ está dado por (3) de modo que al sustituir obtenemos (5). Por la proposición 2.10, tenemos $grad(T(p)) = C_1^{(2)} = P + 1$ y $grad(T(p,p) = 1$ Aplicando la proposición 1.4 a (4) obtenemos:

$$(p+1).grad(T(p^k)) = grad(T(p^{k+1})) + p.grad(T(p^{k-1})).$$

aplicando inducción sobre k, vemos que

$$(***) \qquad \text{grad}(T(p^k)) = 1 + p + \ldots + p^k$$

De esta relación y la proposición 1.4 y de la relación $T(m.m') = T(m).T(m')$ obtenemos (7). Finalmente (6) se sigue de (***) y (2).

B I B L I O G R A F I A

1. Adrianov A.N. Quadratic forms and Hecke operators, Springer - Verlag, 1987.

2. Koblitz N. Introduction to Elliptic Curves and Modular Forms, Springer-Verlag, 1984.

3. Miyake T. Modular forms, Springer-Verlag, 1989.

4. Shimura G. Introduction to the Arithmetic Theory of Automorphic Functions, Princeton Univ. Press, 1971.

5. Shimura G. Sur les Intégrales Attachées aux Formes Automorphes, J. Math. Soc., Japan, 11 (1959), 291-311.

6. Tamagawa T. On the ζ-functions of a División Algebra. Ann, Math., Vol. 77, 387-405 (1963).