Formas Modulares con Aplicaciones a Formas Cuadráticas

Juanita Duque Rosero

Asesor: Guillermo Mantilla-Soler

Una tesis presentada al Departamento de Matemáticas,
para el grado de pregrado en matemáticas

Universidad de los Andes
Bogotá, Colombia
Diciembre, 2016

Introducción

Los polinomios son elementos bastante importantes para el álgebra y para las matemáticas en general. Encontrar raíces de polinomios no es sencillo, por ejemplo, Galois demostró que no existe una solución general en radicales para una ecuación polinomial de grado 5. Por su parte, para la teoría de números solucionar estas ecuaciones también es un tema interesante. Es análisis diofántico el nombre de la teoría de encontrar raíces enteras de polinomios sobre $\mathbb{Z}[\boldsymbol{x}]$ igualados a 0. El nombre es en honor al matemático Diofanto, quien vivió aproximadamente en el siglo III d.c. Gran parte de su producción científica fue acerca del tema. Él no fue el único matemático en trabajar en el tema y por ello la teoría ha tenido un gran desarrollo.

La búsqueda de soluciones ha beneficiado en gran medida a la teoría matemática. Se han logrado muchos avances y nuevas teorías en el proceso. Basta pensar en el popular *último Teorema de Fermat*, una afirmación conjeturada por Fermat en 1637 cuya demostración llegó sólo hasta 1995, a manos del matemático británico Andrew Wiles. Fermat afirmó que la ecuación

$$x^n + y^n = z^n$$

no tiene soluciones enteras no triviales para $n \geq 3$. Como es conocido, él esccribió en el margen de un libro: "*Es imposible descomponer un cubo en dos cubos, un bicuadrado en dos bicuadrados, y en general, una potencia cualquiera, aparte del cuadrado, en dos potencias del mismo exponente. He encontrado una demostración realmente admirable, pero el margen del libro es muy pequeño para ponerla*". Sin embargo, dicha demostración no fue encontrada y durante siglos varios matemáticos intentaron probar el teorema. Con ello, se desarrollaron varios conceptos importantes en la teoría algebraica de números, la geometría aritmética y la teoría de representaciones de Galois. Además, surgió una nueva teoría matemática conocida como la teoría de la modularidad.

Al igual que Fermat, varios matemáticos se ocuparon en algún momento de responder preguntas sobre este tema. Una aproximación inicial fue encontrar todos los puntos enteros en la recta $y = mx + b$ con $m, b \in \mathbb{Z}$. Bézout, un matemático francés que vivió entre 1730 y 1773, probó un lema que solucionó el problema para este tipo de ecuaciones. El lema fue llamado después Lema de Bézout y afirma que si a y b son números enteros diferentes de cero con máximo común divisor d, existen enteros x e y tales que: $ax + by = d$.

Dado que las ecuaciones Diofánticas lineales están completamente resueltas gracias a Bézout, el siguiente caso natural son las de grado dos. El objetivo fue entonces encontrar enteros que son el resultado de evaluar en $\mathbb{Z}$ polinomios sobre los enteros. Por ejemplo, Fermat demostró en 1640 que los primos que se escriben como

$$x^2 + y^2$$

son los congruentes a 1 módulo 4 [Cox13, Teo 1.2, Pg 8]. El análogo para tres variables fue probado por Legendre, quien demostró que todo número entero positivo se puede expresar como la suma de tres cuadrados si y sólo si no es de la forma $4^s(8k + 7)$. Este teorema se demostrará en el capítulo cuatro. Por último, para la suma de cuatro cuadrados, el resultado es mucho más complejo. Lagrange demostró que todo entero positivo se puede escribir como la suma de cuatro cuadrados. Este teorema es conocido como el *Teorema de los Cuatro Cuadrados de Lagrange* y será de espacial interés en este documento. Se demostrará de dos formas distintas, una en el capítulo cuatro y otra en el cinco.

De lo anterior, es posible notar que acercamiento razonable a encontrar soluciones a ecuaciones diofánticas de grado dos es entonces asumir que los polinomios son homogéneos. Esta teoría fue formalizada por Lagrange y Gauss pero incluso antes ya se habían probado cosas al respecto. El mismo Fermat ya había hecho sus aportes respecto a polinomios así. Los polinomios homogéneos de grado 2 son llamados formas cuadráticas, se pueden definir como polinomios sobre cualquier anillo con unidad. Sin embargo, en este documento se estudiará la teoría únicamente para formas sobre los enteros. En el primer capítulo se trataran formas cuadráticas en dos variables, el tema que empezaron estudiando Lagrange y Gauss. Aquí es importante la noción de equivalencia entre formas cuadráticas y de grupos de clases de ideales

introducida por Gauss con resultados realmente impresionantes. Es más, algunas preguntas y generalizaciones que quedaron después de que Gauss expusiera su teoría solo pudieron ser resueltas hasta finales del siglo XX. Posteriormente, se generalizarán los conceptos a formas cuadráticas en más variables.

Para conocer mejor un conjunto, una estrategia puede ser hacer que un grupo actúe sobre él. Para formas cuadráticas binarias se puede definir una acción del grupo $SL_2(\mathbb{Z})$ sobre ellas. Un resultado impresionante que se le debe a Gauss es que las clases de equivalencia dadas por la acción pueden ser dotadas de estructura de grupo Abeliano finito. Es por esto que el segundo capítulo se estudiará mejor al grupo $SL_2(\mathbb{Z})$. Se mostrará una acción del grupo sobre el plano superior complejo. Esto se hará porque esta acción es esencial en la prueba de lo demostrado por Gauss y además será usada en el último capítulo. Aquí también se presentará una demostración geométrica de que $SL_2(\mathbb{Z})$ es finitamente generado. La prueba se basa también en la acción del grupo sobre el plano superior complejo y en algunas propiedades de este último.

Para formas cuadráticas en más variables surge el tema central de este proyecto, un tipo especial de formas cuadráticas. Como en el Teorema de los Cuatro Cuadrados de Lagrange, existen más formas cuadráticas con las que se puede escribir todos los enteros positivos, estas serán llamadas *universales*. Un problema entonces será decidir cuándo una forma cuadrática dada es universal. La solución para un subconjunto de ella (de matriz de Gram entera) fue dada por Conway y Schneeberger en 1993 y resulta ser bastante más sencilla de lo esperado. Este resultado fue denominado el *Teorema de los 15* ya que afirma que una forma cuadrática es universal si y solo si los números del uno al quince pueden ser escritos evaluando dicha forma en tuplas de enteros. La demostración del teorema no fue publicada por sus autores y fue Manjul Bhargava en 2000 quién dio una prueba formal. La demostración se basa en la biyección que existe entre formas cuadráticas enteras y retículos con producto interno entero. Es por esto que en el tercer capítulo se introduce el concepto de retículo con producto interno entero y se explican la biyección y algunas propiedades. Por otra parte, en el capítulo cuatro se presenta la demostración de Bhargava del Teorema de los 15.

Si se considera las formas cuadráticas por fuera del conjunto descrito anteriormente, Conway y Schneeberger también conjeturaron un teorema similar conocido como el *Teorema de los 290*, en el que otra vez su nombre es bastante diciente. La demostración de dicho teorema no ha sido publicada hasta ahora ya que requiere se basa en un algoritmo que aún no se han podido implementar. Además existen otras generalizaciones que se concentran en ver qué condiciones son necesarias para comprobar lo mismo para subconjuntos de los enteros positivos. El resultado más representativo al respecto también está dado por Bhargava quién demostró que para toda forma cuadrática y todo conjunto de enteros existe un subconjunto finito tal que es suficiente demostrar que todo entero de ese subconjunto puede ser escrito evaluando la forma cuadrática en una tupla específica para que todo entero en el conjunto pueda ser escrito de esa forma.

Como ya se explicó antes, un resultado bastante popular relacionado con formas cuadráticas es que la forma

$$x^2 + y^2 + z^2 + w^2$$

es universal (Cuatro Cuadrados de Lagrange). Esto es un corolario del Teorema de los 15. Sin embargo, no sólo interesa probar que todo entero positivo se puede escribir como la suma de cuatro cuadrados sino también contar las formas distintas de hacerlo. Una solución fue dada por Jacobi en 1834. En el presente documento se mostrará una demostración usando técnicas de formas modulares.

La teoría de formas modulares es bastante interesante por sí misma, además del Teorema de Jacobi, es posible demostrar muchos hechos importantes por medio de la misma. Para dar solo una idea, se puede mostrar el *Teorema de Modularidad*, que es el paso que completó la demostración del último teorema de Fermat. Es por eso que en el último capítulo se hará una introducción a la teoría de formas modulares y también se dará la demostración del Teorema de los Cuatro Cuadrados de Jacobi.

Notación y Convenciones

Las letras $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ se reservan únicamente para los naturales, enteros, racionales, reales y complejos.

$GL_2(\mathbb{Z})$ es el conjunto de matrices invertibles 2×2 con entradas en los enteros.

$SL_2(\mathbb{Z})$ es el subconjunto de $GL_2(\mathbb{Z})$ de matrices con determinante 1.

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

p siempre será un número primo.

$\mathcal{H}$ es el plano superior complejo, los números complejos con parte imaginaria positiva.

τ será un elemento en $\mathcal{H}$.

q será $e^{2\pi i \tau}$.

Si R es un anillo, R^* serán sus unidades.

Si G es un grupo y U un subconjunto, $\langle U \rangle$ será el subgrupo generado por U.

$\boldsymbol{x}$ será la tupla $(x_1, \ldots, x_n)$, lo mismo para $\boldsymbol{v}$, $\boldsymbol{m}$ y $\boldsymbol{\alpha}$.

Si M es una matriz, M^t será su transpuesta.

$\ll 0$ significa un entero negativo lo suficientemente pequeño.

Índice

1. Formas cuadráticas sobre los enteros

En este capítulo se presentará una introducción a la teoría de formas cuadráticas sobre los enteros. Una **forma cuadrática** definida sobre $\mathbb{Z}$ es un polinomio $f(x_1, \ldots, x_n) \in \mathbb{Z}[x]$, homogéneo y de grado 2. Diremos que $f(x_1, \ldots, x_n)$ **representa** a un entero m si existe $\boldsymbol{m} \in \mathbb{Z}^n$ tal que $f(\boldsymbol{m}) = m$. Además es **definida positiva** si todos los enteros que representa son positivos. En este documento sólo se estudiarán formas cuadráticas definidas positivas, así que por forma cuadrática se referirá a forma cuadrática definida positiva, a menos que se indique lo contrario.

1.1. Formas cuadráticas binarias

Lagrange y Gauss fueron pioneros en el trabajo con formas cuadráticas. Ambos se concentraron en el estudio de polinomios homogéneos en dos variables, es decir, de la forma $ax^2 + bxy + cy^2$. De dichos polinomios surgen la mayoría de conceptos y preguntas relacionadas con formas cuadráticas en general. Por ello, resulta interesante iniciar entendiendo lo que ocurre con formas cuadráticas binarias. Esta sección se concentrará en ello.

Una forma cuadrática en dos variables es una **forma cuadrática binaria**. Como se dijo, estas son polinomios de la forma

$$f(x, y) = ax^2 + bxy + cy^2.$$

El **discriminante** de $f(x, y)$ se define como $D = b^2 - 4ac$ y $f(x, y)$ será **primitiva** si m.c.d. $(a, b, c) = 1$. Como notación, la forma $f(x, y) = ax^2 + bxy + cy^2$ se representará algunas veces como $f = (a, b, c)$.

Ejemplo 1.1. Un ejemplo bastante común de una forma cuadrática binaria, definida positiva y primitiva es:

$$f(x, y) = x^2 + y^2$$

Uno de los primeros problemas que resulta interesante es dada una forma cuadrática, encontrar qué enteros representa. Esta pregunta se puede reducir a encontrar los primos representados por dicha forma gracias a la composición de formas cuadráticas que se presentará más adelante. Por ejemplo, Fermat estudió la forma presentada en el ejemplo anterior y conjeturó que representa a todos los primos congruentes a uno módulo cuatro. Más adelante, Euler logró realizar una demostración de dicho teorema. La prueba utiliza un argumento que puede demostrarse fácilmente por medio del uso de la teoría de formas cuadráticas. Esto se puede encontrar en [Cox13, Teo. 1.2, Pg. 10].

Por otra parte, es posible definir una acción del grupo $GL_2(\mathbb{Z})$ sobre las formas cuadráticas binarias de la siguiente forma.

Dadas $f(x, y)$ forma cuadrática y $A = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z})$,

$$f^A(x, y) := f(rx + sy, tx + uy). \tag{1.1}$$

$f(x, y)$ y $g(x, y)$ serán **equivalentes** si existe $A \in GL_2(\mathbb{Z})$ tal que $f^A(x, y) = g(x, y)$.

Ejemplo 1.2. Dos formas cuadráticas equivalentes son

$$f = (3, -6, 18) \quad \text{y} \quad g = (2, 2, 3)$$

debido a que

$$g^A(x, y) = g(2x - y, -x + y) = f(x, y) \qquad \text{con } A = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$$

Como se dijo antes, una de las principales preguntas es ver qué enteros representa una forma cuadrática dada. La siguiente proposición está encaminada a demostrar que para responder a dicha pregunta (y a algunas más), es posible considerar formas cuadráticas equivalentes sin cambiar la respuesta.

Proposición 1.3. *Sean $f(x, y)$ y $g(x, y)$ formas cuadráticas binarias equivalentes. Entonces:*

(*i*) *$f(x,y)$ y $g(x,y)$ tienen el mismo discriminante,*

(*ii*) *$f(x,y)$ y $g(x,y)$ representan a los mismos números,*

(*iii*) *$f(x,y)$ es primitiva si y solo si $g(x,y)$ lo es.*

Demostración. Existe una biyección entre formas cuadráticas y matrices enteras con entradas diagonales pares. Es decir, matrices con entradas en $\frac{1}{2}\mathbb{Z}$ Dada $f(x,y) = ax^2 + bxy + cy^2$, la matriz asociada será $B = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ ya que

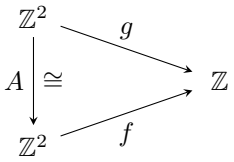
$$f(x,y) = (x,y)\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}.$$

Esto es que $f(x,y) = \boldsymbol{x}B\boldsymbol{x}^t$ en donde $\boldsymbol{x} = (x,y)$. Más adelante, esta matriz será denominada matriz de Gram asociada a la forma $f(x,y)$. Por ahora, lo importante es notar que el determinante de la matriz es $ac - \frac{b^2}{4} = -\frac{D}{4}$. Además, que f y g sean equivalentes es que existe $A \in GL_2(\mathbb{Z})$ tal que

$$g(x,y) = f^A(x,y) = (A\boldsymbol{x}^t)^t B(A\boldsymbol{x}^t) = \boldsymbol{x}(A^tBA)\boldsymbol{x}^t.$$

Pero el determinante de A^tBA es el producto de los determinantes. Además como $A \in GL_2(\mathbb{Z})$, $\det(A^t) = \det(A) = \pm 1$ y por tanto el determinante de A^tBA es el determinante de B. Así el discriminante de g es el mismo de f, de donde se sigue (i).

Por otra parte, toda forma cuadrática define una función de $\mathbb{Z}^2$ en $\mathbb{Z}$ por medio de la evaluación en la forma. De ahí se tiene el siguiente diagrama conmutativo:



Como $A \in SL_2(\mathbb{Z})$, es invertible, entonces existe un automorfismo de $\mathbb{Z}^2$ dado por A. Es así como las imágenes son iguales y las formas representan los mismos números, (ii).

Para la parte (iii) se probará algo mucho más general: si d y d' son el máximo común divisor de los coeficientes de $f(x,y)$ y $g(x,y)$, entonces $d = d'$. Si d es el máximo común divisor de los coeficientes de $f(x,y)$ y m es un entero representado por $f(x,y)$, d divide a m. Igual ocurre con d', el máximo común divisor de los coeficientes de g, que divide a los enteros representados por g. Sin embargo, se mostró que f y g representan a los mismos enteros. Por lo tando $d|d'$ y $d'|d$, necesariamente $d = d'$. □

Proposición 1.4. *La equivalencia en formas binarias es una relación de equivalencia.*

Demostración. La relación es reflexiva porque $f^I = f$, con I la matriz identidad. Si $f^A = g$ con $A \in GL_2(\mathbb{Z})$, entonces A es invertible con inversa también en $GL_2(\mathbb{Z})$. Sea B la matriz asociada a f, se tiene:

$$g^{A^{-1}}(x,y) = \boldsymbol{x}((A^{-1})^tA^tBAA^{-1})\boldsymbol{x}^t = \boldsymbol{x}((AA^{-1})^tB(AA^{-1}))\boldsymbol{x}^t = \boldsymbol{x}B\boldsymbol{x}^t = f(x,y)$$

por ello, la relación es simétrica. En tercer lugar, si $f^A = g$, $g^C = h$ y B sigue siendo la matriz asociada a $f(x,y)$,

$$g(x,y) = \boldsymbol{x}A^tBA\boldsymbol{x}^t$$
$$h(x,y) = g^C(x,y) = \boldsymbol{x}(AC)^tB(AC)\boldsymbol{x}^t = f^{AC}(x,y)$$

por lo que la relación es transitiva. En conclusión la relación es una relación de equivalencia. □

Por lo anterior, para estudiar formas cuadráticas basta trabajar con clases de equivalencia bajo la acción de $GL_2(\mathbb{Z})$. Se dirá que la equivalencia es **propia** cuando la matriz tiene determinante uno, esto es, la misma relación denfinida anteriormente pero restringida al subgrupo $SL_2(\mathbb{Z})$. En general se quiere trabajar con equivalencia propia y más adelante se va a ver por qué.

Definición 1.5. Una forma cuadrática $f = (a, b, c)$ es **reducida** si

$$|b| \leq a \leq c.$$

Un resultado importante es que toda forma definida positiva es propiamente equivalente a una única forma reducida. La demostración se puede ver en [Bue89, Teo 2.3, Pg. 14]. La prueba da un algorítmo para encontrar la forma reducida. Por ello, en lugar de escribir la demostración se expondrá un ejemplo de cómo funciona el algorítmo.

Ejemplo 1.6. Se toma la forma cuadrática $f = (1, 2, 3)$, que no es reducida porque $2 > 1$. El discriminante de f en este caso es -8. En primer lugar se toma un entero δ tal que $|-2 + 2 \cdot 3 \cdot \delta| \leq |3|$. Así $\delta = 0$. Se define

$$A_\delta = \begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix}$$

y de ahí

$$f^{A_0} = f(-y, x + \delta y) = (3, -2 + 6\delta, 1 - 2\delta + 3\delta^2) = (3, -2, 1),$$

una forma propiamente equivalente que aún no es reducida. Se vuelve a hacer lo mismo, δ debe ser tal que $|2 + 2 \cdot 1 \cdot \delta| \leq |1|$ y por tanto $\delta = -1$, entonces

$$(3, -2, 1)^{A_{-1}} = (1, 0, 2),$$

que es una forma de discriminante -8 propiamente equivalente a la primera y reducida.

Se verá más adelante que algo importante de este concepto es que con la excepción de $(a, b, a) \sim (a, -b, a)$ y $(a, a, c) \sim (a, -a, c)$, ningún par de formas reducidas es equivalente [Bue89, Teo 2.4, Pg. 15].

Con esto en mente, dado $D < 0$ se define $h(D)$ como el **número de clases**, ésto es, el número de formas reducidas de discriminante D. Si se tiene una forma $f = (a, b, c)$ reducida, entonces

$$4b^2 \leq 4ac = b^2 - D \quad \text{y de ahí} \quad |b| \leq \sqrt{\frac{-D}{3}}.$$

Teorema 1.7. *Para todo $D < 0$, $h(D)$ es finito.*

Demostración. Se realizarán dos demostraciones, la primera es algorítmica, la segunda es más algebraica y se puede generalizar a formas de n variables. En primer lugar se vio que toda forma de discriminante D debe cumplir que $|b| \leq \sqrt{-D/3}$. Como b además es entero, existen finitos b que satisfacen la desigualdad. Además $4ac = b^2 - D$, pero otra vez a y c deben ser enteros y así dado b, existen finitas posibilidades de parejas a, c. En conclusión $h(D)$ debe ser finito. □

Ejemplo 1.8. Para $h(-3)$, se tiene que $D = -3$ y toda forma reducida $f = (a, b, c)$ de ese discriminante debe cumplir que $|b| \leq 1$. Entonces existen tan solo tres posibilidades para b: 0 y ± 1. Si $b = 0$, $D \equiv 0$ (mód 4) y por tanto no puede ser -3, entonces esto no puede ocurrir. Si $b = 1$, $1 - 4ac = -3$, de donde se sigue que $a = c = \pm 1$. Sin embargo, a no puede ser negativo porque $1 = |b| \leq a$, entonces se descarta el caso $a = c = -1$. Es así como el único caso posible en el que $a = c = 1$ y se tiene la forma reducida:

$$x^2 + xy + y^2.$$

En conclusión, $h(-3) = 1$.

Existe una demostración que involucra métodos geométricos y se puede generalizar a más variables. Dicha demostración será presentada en el capítulo dos.

Observación 1.9. Una forma cuadrática (a, b, c) es definida positiva si y solo si $a > 0$ y $D < 0$.
Esto ocurre porque mediante el criterio de Sylvester (se explica en la próxima sección), la matriz asociada a una forma es definida positiva si y solo si $a > 0$ y su determinante también es positivo. El determinante es $ac - \frac{b^2}{4} = -\frac{D}{4}$ y que sea mayor que 0 implica que $D < 0$.
Por esta razón es que en los teoremas sólo era necesario considerar el caso de $D < 0$ ya que, como se dijo al principio, sólo se trabaja con formas definidas positivas.

Si se tienen dos formas del mismo discriminante, tales que una representa a un entero m y otra a un entero n, es una pregunta válida la de si se puede encontrar una forma cuadrática que represente al producto. De ésto se encargaron Gauss y Dirichlet.

Definición 1.10. Si $f(x, y)$ y $g(x, y)$ son formas primitivas de discriminante D, entonces su **composición** será una forma cuadrática $F(x, y)$ con las mismas características de las anteriores tal que

$$f(x, y)g(z, w) = F(B_1(x, y; z, w), B_2(x, y; z, w))$$

en donde

$$B_i(x, y; z, w) = a_i xz + b_i xw + c_i yz + d_i yw, \qquad i = 1, 2$$

Gauss y Dirichlet presentaron distintas maneras de componer formas cuadráticas. Los resultados pueden no ser propiamente equivalentes.
Ejemplo 1.11. Uno de los ejemplos más simples es tomar las formas:

$$f(x, y) = x^2 + y^2 \quad \text{y} \quad g(z, w) = z^2 + w^2,$$

$$f(x, y)g(z, w) = (xz + yw)^2 + (xw - yz)^2$$

y por tanto la composición se puede definir como

$$F(s, t) = s^2 + t^2$$

Ejemplo 1.12. Se consideran las formas

$$f(x, y) = 2x^2 + 2xy + 3y^2 = g(x, y).$$

Su discriminante es $D = -20$ y además

$$f(x, y)g(z, w) = (2xz + xw + yz + 3yw)^2 + 5(xw - yz)^2.$$

Entonces se define la composición como

$$F(s, t) = s^2 + 5t^2,$$

que también se puede comprobar, tiene discriminante $D = -20$.
Por otra parte, $f(x, y)$ representa al 10 porque $f(-1, 2) = 10$ y $g(x, y)$ hace lo mismo con el 7, $g(1, 1) = 7$. Entonces $F(s, t)$ debería representar al 70 y en efecto lo hace:

$$F(2 \cdot (-1) \cdot 1 - 1 \cdot 1 + 2 \cdot 1 + 3 \cdot 2 \cdot 1, -1 \cdot 1 - 2 \cdot 1) = F(5, -3) = 5^2 + 5 \cdot (-3)^2 = 70$$

El resultado esencial de esta teoría fue que, por ambos caminos, el conjunto de clases propiamente equivalentes de formas cuadráticas junto con la operación de componer resulta ser un grupo abeliano finito. Esto es, si las formas cuadráticas de discriminante D se denotan por Q_D, entonces

$$\#Q_D/SL_2(\mathbb{Z}) < \infty.$$

El índice de $SL_2(\mathbb{Z})$ sobre $GL_2(\mathbb{Z})$ es dos y por lo tanto $\#Q_D/GL_2(\mathbb{Z})$ también es finito, sin embargo no se tiene una estructura de grupo. Por esta razón principalmente es que se consideran sólo equivalencias propias de formas cuadráticas.

Gauss escribió estos resultados en su libro *Disquisitiones Arithmeticae* hacia 1798 y Dirichlet aproximadamente en 1850. El siguiente avance importante hecho en el tema se le debe a Bhargava, quien recientemente encontró nuevas reglas de composición. Empezó a trabajar y publicar en el tema en 2001 en su tesis doctoral y presentó cuatro escritos importantes desde ese año hasta 2008.

El conjunto de clases en la relación de equivalencia se escribe como $C(D)$, el resultado dice que es un grupo y por tanto se lo denomina el **grupo de clases**. El número $h(D)$ mostrado anteriormente es por tanto la cardinalidad de dicho grupo. Es claro que la propiedad de ser un grupo abeliano finito facilita mucho el estudio de $C(D)$ y es por sí misma una teoría bastante interesante. Para encontrar más al respecto se puede ver [Cox13, Cap. 3, Pg. 42-46] o [Bou05, Pg. 14-39].

1.2. Generalización a más variables

Como se dijo anteriormente, la teoría de las formas cuadráticas empezó con formas cuadráticas binarias y se extendió a formas en más variables. Sin embargo, surgen nuevos conceptos interesantes. Uno de ellos, el que más interesa estudiar en este documento, es el de univesalidad. Esta sección se encarga de explicar las generalizaciones y el nuevo concepto.

Definición 1.13. La **matriz de Gram** asociada a una forma cuadrática $f(\boldsymbol{x})$ será la matriz simétrica A tal que

$$f(\boldsymbol{x}) = \boldsymbol{x}B\boldsymbol{x}^t \tag{1.2}$$

Es importante resaltar que las formas cuadráticas están unívocamente determinadas por su matriz de Gram. El **determinante** de una forma cuadrática será el determinante de su matriz de Gram. Una forma cuadrática será **no degenerada** si el determinante de su matriz de Gram es distinto de 0. Esto es, si no existe una tupla de enteros no trivial que al ser evaluada en la forma sea igual a 0. Otra vez, interesará trabajar únicamente con formas no degeneradas.

Definición 1.14. Una forma cuadrática es **entera** si su matriz de Gram tiene únicamente valores enteros.

Estas formas cuadráticas serán de gran interés posteriormente. En el caso de formas cuadráticas binarias, la condición es únicamente que el coeficiente del término xy sea par. En n variables es que todos los coeficientes de los términos cruzados lo sean.

Un recurso importante para revisar si una forma cuadrática es definida positiva es el siguiente

Hecho 1.15. ***(Criterio de Sylvester)*** *Una forma cuadrática con matriz de Gram B es definida positiva si y solo si las siguientes matrices tienen determinante positivo:*

$$\{[B_{ij}] \mid 1 \leq i \leq k,\ 1 \leq j \leq k\}, \qquad \text{para todo } m \in \{1, \ldots, n\}.$$

Demostración. Ver [Mey00, Sec 7.6, Pg. 558]. □

Al igual que con formas cuadráticas binarias, se puede definir la acción de $GL_n(\mathbb{Z})$ sobre las formas cuadráticas como: dadas $A \in GL_n(\mathbb{Z})$ y $f(\boldsymbol{x})$ forma cuadrática con matriz de Gram B,

$$f^A(\boldsymbol{x}) := \boldsymbol{x}A^tBA\boldsymbol{x}^t.$$

Definición 1.16. Dos formas cuadráticas f y g son **equivalentes** si existe una matriz A con entradas enteras y determinante ± 1 tal que $f^A = g$.

Esta es la misma noción de equivalencia que se tenía con las formas cuadráticas binarias. Igualmente se puede decir que dos formas son **propiamente equivalentes** si la matriz que las relaciona tiene determinante uno y por razones parecidas a las expuestas para formas binarias, interesará más tratar únicamente con la relación de equivalencia propia. Al igual que con formas binarias, se tendrá una relación de equivalencia y finitas clases de equivalencia como se ve en lo que sigue.

Hecho 1.17. *La relación definida anteriormente es una relación de equivalencia.*

La demostración es igual a la mostrada para formas binarias, por lo tanto no se repitirá.

Hecho 1.18. *Existen finitas clases de equivalencia de formas cuadráticas del mismo determinante*

Este teorema se demostrará en el segundo capítulo.

La relación que se probó en la sección anterior que afirma que si dos formas son equivalentes estas tienen el mismo discriminante, representan los mismos números y son primitivas si y solo si la otra lo es también se sigue en este contexto. La demostración, otra vez, es la misma que se hizo antes.

Definición 1.19. Una forma cuadrática es **universal** si representa a todos los enteros positivos.

Observación 1.20. En las formas cuadráticas binarias no se definió forma cuadrática universal dado que no existen formas binarias universales. De hecho, tampoco existen formas universales en tres variables. Se dará una demostración de este hecho en el cuarto capítulo. Es por ello que uno de los ejemplos más populares de una forma cuadrática universal es el siguiente.

Ejemplo 1.21. El polinomio

$$x^2 + y^2 + z^2 + w^2$$

es una forma cuadrática universal. Este es el Teorema de los Cuatro Cuadrados de Lagrange, que también se estudiará más adelante.

Por otra parte, recordando el Ejemplo 1.1, se vio que la forma cuadrática $x^2 + y^2$ es definida positiva porque todo número real elevado al cuadrado lo es y los enteros son subconjunto de los reales. De ahí, se puede pensar que revisar propiedades de formas cuadráticas sobre anillos relacionados con los enteros puede llegar a ser útil en algunas ocasiones. En este orden de ideas se introducirá el concepto de enteros p-ádicos para corroborar dicha idea.

Así como los números reales son la completación de los racionales con la norma $d(x, y) = |x - y|$ (que aquí será llamada la norma infinito), **el cuerpo *p*-ádico** será la completación de $\mathbb{Q}$ con la norma

$$d_p(x, y) = \frac{1}{p^k},$$

en donde k es la potencia exacta de p que aparece en la descomposición en primos de $x - y$. Este cuerpo será $\mathbb{Q}_p$ para todo p primo. Además, cuando $p = \infty$, $\mathbb{Q}_\infty$ será el cuerpo de los números reales, la completación de $\mathbb{Q}$ con la norma infinito. Como los cuerpos $p-$ádicos son el análogo a los racionales, es interesante definir subconjuntos de $\mathbb{Q}_p$ análogos a los números enteros. Los **enteros *p*-ádicos** serán los elementos en $\mathbb{Q}_p$ de norma menor o igual a uno.

La anterior no es la única forma de definir al conjunto de los enteros p-ádicos, aunque naturalmente todas son equivalentes. Una manera algebraica es definirlos como el límite inverso de $\mathbb{Z}/p^n\mathbb{Z}$ ordenados bajo proyección. Los enteros $p-$ádicos se denotan como $\mathbb{Z}_p$ para todo p primo.

Aunque usar números p-ádicos suele facilitar algunos argumentos, es mucho más sencillo trabajar con congruencias módulo un primo, es decir, en el cuerpo $\mathbb{Z}/p\mathbb{Z}$. Para ello es necesario el siguiente resultado y sus generalizaciones .

Hecho 1.22. ***(Lema de Hensel).*** *Si $f(x) \in \mathbb{Z}_p[x]$ y si existe $a \in \mathbb{Z}_p$ tal que*

$$f(a) \equiv 0 \pmod{p} \qquad \text{y} \qquad f'(a) \not\equiv 0 \pmod{p},$$

entonces existe un único $\alpha \in \mathbb{Z}_p$ tal que

$$f(\alpha) = 0 \qquad \text{y} \qquad \alpha \equiv a \pmod{p}.$$

Demostración. Ver [Cas78, Lema 4.1, Pg. 47]. Posteriormente se demostrará una versión más general del Lema. □

Observación 1.23. En términos de la métrica de $\mathbb{Z}_p$, este resultado es equivalente a que si

$$|f(a)|_p < 1 \quad \text{y} \quad |f'(a)|_p = 1,$$

entonces existe un único $\alpha \in \mathbb{Z}_p$ tal que $f(\alpha) = 0$ y $|\alpha - a|_p < 1$

Un resultado importante es que si p es un primo impar y $u \in \mathbb{Z}_p^*$, u es un cuadrado en $\mathbb{Z}_p$ si y solo si su reducción módulo p es un cuadrado en $(\mathbb{Z}/p\mathbb{Z})^*$. Esto se hace tomando el polinomio $p(x) = x^2 - u$ con u un entero no divisible por p. El polinomio cumple las hipótesis del lema y por lo tanto se sigue el resultado.

Ejemplo 1.24. Usando lo anterior, 3 es un cuadrado en $\mathbb{Z}_7$ porque $(\mathbb{Z}/7\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z}$ y $3^2 \equiv 3 \pmod 6$.

El problema está cuando el primo es 2. Para ello se debe hacer una versión más fuerte del lema.

Teorema 1.25. ***(Lema de Hensel fuerte).*** *Si $f(x) \in \mathbb{Z}_p[x]$ y $a \in \mathbb{Z}_p$ es tal que*

$$|f(a)|_p < |f'(a)|_p^2,$$

entonces existe un único $\alpha \in \mathbb{Z}_p$ tal que $f(\alpha) = 0$ y $|\alpha - a|_p < |f'(a)|_p \leq 1$

Demostración. Si $|f'(a)|_p = 0$, $|f(a)|_p = 0$ y se sigue el resultado. Entonces se puede suponer que $|f'(a)|_p \neq 0$, lo que implica que $|f'(a)|_p \leq 1$. El Teorema del Punto Fijo de Banach afirma que si (X, d) es un espacio métrico, no vacío y completo y $T : X \to X$ es una contracción, entonces T tiene un único punto fijo [AMO01, Teo. 1.1, pg. 1]. Se toma $X = B_{|f'(a)|_p}(a)$, por hipótesis $|f'(a)|_p \neq 0$ y así X es no vacío. Es completo porque $\mathbb{Z}_p$ es la completación de $\mathbb{Q}$. Ahora se define la contracción $T : X \to X$ como

$$T(x) = x - \frac{f(x)}{f'(a)}.$$

Usando el Teorema de Banach, T tiene un único punto fijo $\alpha \in X$. Esto implica que $f(\alpha) = 0$ y además $|\alpha - a|_p < |f'(a)|_p \leq 1$. □

De ahí se puede concluir que u es un cuadrado en $\mathbb{Z}_2$ si y solo si su reducción módulo 8 es un cuadrado en $(\mathbb{Z}/8\mathbb{Z})^*$ (que es equivalente a que su reducción módulo 8 sea 1 ya que el único cuadrado en $(\mathbb{Z}/8\mathbb{Z})^*$ es 1).

Para polinomios en varias variables se puede hacer algo similar. Uno de los resultados más representativos es el siguiente teorema.

Hecho 1.26. *Si $F(\boldsymbol{x}) \in \mathbb{Z}_p[x]$ y existen $a_1, \ldots, a_n$ enteros p-ádicos tales que para algún $i \in \{0, \ldots, n\}$ y para k entero no negativo,*

$$F(\boldsymbol{a}) \equiv 0 \pmod{p^{2k+1}}$$
$$\frac{\partial F}{\partial x_i}(\boldsymbol{a}) \equiv 0 \pmod{p^k}$$
$$\frac{\partial F}{\partial x_i}(\boldsymbol{a}) \not\equiv 0 \pmod{p^{k+1}},$$

entonces existen números p-ádicos $\alpha_1, \ldots, \alpha_n$ tales que

$$F(\boldsymbol{\alpha}) = 0$$
$$\alpha_1 \equiv a_1 \pmod{p^{k+1}}, \quad \ldots, \quad \alpha_n \equiv a_n \pmod{p^{k+1}}.$$

Demostración. Ver [BS66, Teo. 3, pg. 42]. □

En este contexto se puede generalizar la definición de equivalencia a la siguiente.

Definición 1.27. Dos formas cuadráticas f y g son **equivalentes sobre** $\mathbb{Z}_p$ si existe una matriz A con entradas en $\mathbb{Z}_p$ tal que su determinante sea una unidad en $\mathbb{Z}_p$ y $f^A = g$. Es decir, f y g son equivalentes sobre $\mathbb{Z}_p$ si existe A_p con coeficientes en $\mathbb{Z}_p$ y $\det(A_p) \in \mathbb{Z}_p^*$ tal que

$$f(\boldsymbol{x}) = g(A_p \boldsymbol{x}) \tag{1.3}$$

Además es posible definir un elemento que ayuda a demostrar propiedades localmente (sobre $\mathbb{Z}_p$) para después volverlas propiedades locales.

Definición 1.28. Dos formas cuadráticas pertenecen al mismo **género** si y solo si son equivalentes sobre $\mathbb{Z}_p$ para todo p (incluyendo infinito).

Ejemplo 1.29. Las formas cuadráticas

$$x^2 + 55y^2 \qquad \text{y} \qquad 5x^2 + 11y^2$$

están en el mismo género pero no son equivalentes.
Las formas no son equivalentes dado que no representan los mismos números (la segunda representa al 11 pero la primera no). Sin embargo, las formas son iguales tomando módulo p para todo $p \neq 5, 11$ ya que 5 y 11 son unidades en $\mathbb{Z}/p\mathbb{Z}$. Para $p = 5$ se tiene:

$$x^2 + 55y^2 \equiv x^2 \equiv 11y^2 \equiv 5x^2 + 11y^2 \qquad (\text{mód } 5).$$

Igualmente, para $p = 11$:

$$x^2 + 55y^2 \equiv x^2 \equiv 5y^2 \equiv 5x^2 + 11y^2 \qquad (\text{mód } 11).$$

Entonces las formas pertenecen al mismo género.

Lema 1.30. *Dos formas en el mismo género tienen el mismo determinante*

Demostración. Si f y g están en el mismo género, la Igualdad 1.3 implica que para todo primo p existe A_p tal que:

$$\det(f) = (\det(A_p))^2 \det(g).$$

Por lo tanto $\dfrac{\det(f)}{\det(g)}$ es una unidad en $\mathbb{Z}_p$ para todo primo p, pero los únicos números que cumplen eso son ± 1. Entonces $\det(f) = \pm \det(g)$

Si en particular se toma $p = \infty$, $\dfrac{\det(f)}{\det(g)} = 1$, lo que implica que el signo de los determinantes es el mismo. □

Corolario 1.31. *Existen finitas clases de equivalencia de formas cuadráticas en el mismo género*

Demostración. Por el Hecho 1.18 existen finitas clases de equivalencia de formas cuadráticas con el mismo determinante, de lo cual se sigue inmediatamente el resultado. □

Ejemplo 1.32. Se puede probar que el género de las formas presentadas en el Ejemplo 1.29 son las únicas formas no equivalentes en ese género. Se puede revisar cuántos elementos tiene el género de una forma por medio del programa Magma usando el código:

```
M:=Matrix(IntegerRing(),2,2, [1,0,0,55]);
L:=LatticeWithGram(M);
G:=Genus(L);
#G;
```

El resultado es 2. Como se probó que las formas no son equivalentes, deben ser las únicas no equivalentes en su género.

Ahora se enunciará uno de los teoremas más importantes que conciernen a este documento. Lo esencial es el corolario que se presenta después.

Hecho 1.33. *Si f es una forma cuadrática de determinante distinto de 0 y m un entero representado por f sobre $\mathbb{R}$ y todo $\mathbb{Z}_p$ para $p|2d$ si $n \neq 2$ o $p|2md$ si $p = 2$, entonces existe f^* en el mismo género de f tal que f^* representa a m sobre $\mathbb{Z}$*

Demostración. Ver [Cas78, Teo 5.1, Pg. 129]. □

Ejemplo 1.34. Si se toman otra vez las dos formas del Ejemplo 1.29, se mostró ya que el número de clases en su género es 2. Una forma elaborada de demostrar que 11 debe ser representado por la forma $5x^2 + 11y^2$ es notar que $x^2 + 55y^2$ representa a 11 localmente para todo $p|2 \cdot 5 \cdot 11$. Por Lema de Hensel, para $p = 2$, se debe revisar módulo 8

$$x^2 + 55y^2 - 11 \equiv x^2 + 7y^2 + 5 \qquad (\text{mód } 8).$$

Una solución es $x = 2$, $y = 1$.

Para $p = 5$,

$$x^2 + 55y^2 - 11 \equiv x^2 + 4 \qquad (\text{mód } 5).$$

Pero 1 es solución de dicha ecuación y por lo tanto existen x, y tales que $x^2 + 55y^2 = 11 \pmod 5$, lo que implica que 11 es representado por la forma en $\mathbb{Z}_5$. Por otra parte, si se toma $p = 11$, se hace lo mismo que antes:

$$x^2 + 55y^2 - 11 \equiv x^2 \qquad (\text{mód } 11)$$

cuya solución es $x = 0$. Entonces $x^2 + 55y^2$ representa a 11 en $\mathbb{Z}_{11}$.

Además $(\sqrt{11})^2 + 55 \cdot 0^2 = 11$, entonces la forma representa a 11 en $\mathbb{R}$. Sin embargo, $x^2 + 55y^2$ no puede representar a 11 ya que 11 no es un entero cuadrado y $55 > 11$. Por lo tanto, otra forma no equivalente en el mismo género debe representar a 11, como sólo hay una única forma no equivalente, $5x^2 + 11y^2$ debe representar a 11 sobre $\mathbb{Z}$.

Corolario 1.35. *Si f es una forma cuadrática única en su género y m es un entero representado por f en todo $\mathbb{Z}_p$ para $p|2d$ con d el determinante de f, entonces f representa a m sobre $\mathbb{Z}$.*

Demostración. Se sigue inmediatamente del teorema anterior. □

Una de las consecuencias más importantes es que si una forma es única en su género que representa localmente a un entero para todo p, entonces lo representa globalmente. Es una propiedad bastante fuerte ya que muchas veces es más sencillo trabajar localmente para obtener propiedades globales gracias al Lema de Hensel.

2. La acción del grupo modular

El plano superior complejo será una parte básica de este documento debido a que se definirá la acción de $SL_2(\mathbb{Z})$ en este conjunto y esta acción será esencial para trabajar con algunos conceptos posteriormente. Uno de sus primeros usos será la demostración que quedó abierta del capítulo anterior de que el número de clases es finito.

Definición 2.1. El **plano superior complejo** es el conjunto $\mathcal{H} \subseteq \mathbb{C}$ definido por

$$\mathcal{H} = \{z \in \mathbb{C} | \text{Im}(z) > 0\}.$$

Definición 2.2. El **grupo modular** es

$$SL_2(\mathbb{Z}) = \{\gamma \in M_2(\mathbb{Z}) | \det(\gamma) = 1\}.$$

Dos propiedades esenciales para el desarrollo de los temas presentados en este documento son que el grupo modular actúa sobre el plano superior complejo y que es finitamente generado. Seguidamente se presentarán las demostraciones de dichos hechos.

Se define la función que va de $SL_2(\mathbb{Z}) \times \mathbb{C}$ a $\mathbb{C} \cup \{\infty\}$ y está dada por:

$$\gamma(\tau) = \frac{a\tau + b}{c\tau + d}, \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \ \ \tau \in \mathbb{C}.$$

Dicha función toma el valor de infinito cuando $\tau = -\dfrac{d}{c}$. Entonces, lo que en realidad se está definiendo es una función $SL_2(\mathbb{Z}) \times \mathbb{CP}^1 \to \mathbb{CP}^1$ tal que $\gamma[\tau : 1] = \gamma(\tau)$ si $\tau \neq -\frac{d}{c}$ y $[1 : 0]$ si lo es.

Se quiere probar que la anterior función restringida a $\mathcal{H}$ define una acción del grupo modilar. Para ello, es necesaria la siguiente propiedad, que también se usará varias veces más adelante.

Proposición 2.3.

(i) Dados $\tau \in \mathcal{H}$ y $\gamma \in SL_2(\mathbb{Z})$,

$$\text{Im}(\gamma(\tau)) = \frac{\text{Im}(\tau)}{|c\tau + d|^2}.$$

(ii) La función $SL_2(\mathbb{Z}) \times \mathcal{H} \to \mathcal{H}$ definida anteriormente es una acción de $SL_2(\mathbb{Z})$ en $\mathcal{H}$.

Demostración. Sean $\tau \in \mathcal{H}$ y $\gamma \in SL_2(\mathbb{Z})$, entonces

$$\begin{aligned} 2\text{Im}(\gamma(\tau)) &= \frac{a\tau + b}{c\tau + d} - \overline{\left(\frac{a\tau + b}{c\tau + d}\right)} = \frac{a\tau + b}{c\tau + d} - \frac{a\overline{\tau} + b}{c\overline{\tau} + d} \\ &= \frac{ac|\tau|^2 + bc\overline{\tau} + ad\tau + bd - ac|\tau|^2 - ad\overline{\tau} - bc\tau - bd}{|c\tau + d|^2} \\ &= \frac{bc(\overline{\tau} - \tau) + ad(\tau - \overline{\tau})}{|c\tau + d|^2} = \frac{2\text{Im}(\tau)(ad - bc)}{|c\tau + d|^2} \\ &= \frac{2\text{Im}(\tau)}{|c\tau + d|^2}. \end{aligned}$$

Como $\tau \in \mathcal{H}$, Im $\tau > 0$, entonces $\text{Im}(\gamma(\tau)) > 0$ y así $\gamma(\tau) \in \mathcal{H}$.

Por otra parte, $I(\tau) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tau = \frac{\tau}{1} = \tau$. Para terminar,

$$\begin{aligned}(\gamma\gamma')(\tau) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}(\tau) \\ &= \frac{(aa'+bc')\tau + ab' + bd'}{(ca'+dc')\tau + cb' + dd'} = \frac{\frac{aa'\tau+ab'}{c'\tau+d'} + b}{\frac{ca'\tau+cb'}{c'\tau+d'} + d} \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\frac{a'\tau+b'}{c'\tau+d'}\right) = \gamma(\gamma'(\tau)).\end{aligned}$$

Entonces se puede concluir que la función define una acción del grupo $SL_2(\mathbb{Z})$ sobre el conjunto $\mathcal{H}$. □

Es importante ver que el grupo modular es finitamente generado. Para probarlo se emplea el concepto de dominio fundamental. Si Γ acúa sobre $\mathcal{H}$, un cerrado F de $\mathcal{H}$, es un **dominio fundamental** para Γ si para todo $\tau \in \mathcal{H}$ existen $z \in \mathcal{H}$ y $\gamma \in \Gamma$ tales que $\tau = \gamma z$ y no existen τ_1, τ_2 distintos en el interior de F tales que $\tau_1 = \gamma\tau_2$ para alguna matriz $\gamma \in \Gamma$.

Lema 2.4. *Sea F el sub-conjunto de $\mathcal{H}$ dado por*

$$F := \left\{\tau \in H : \ |Re\ \tau| \leq \frac{1}{2}, |\tau| \geq 1\right\}.$$

Entonces F es dominio fundamental para $\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$, el subrupo de $SL_2(\mathbb{Z})$ generado por esos dos elementos.

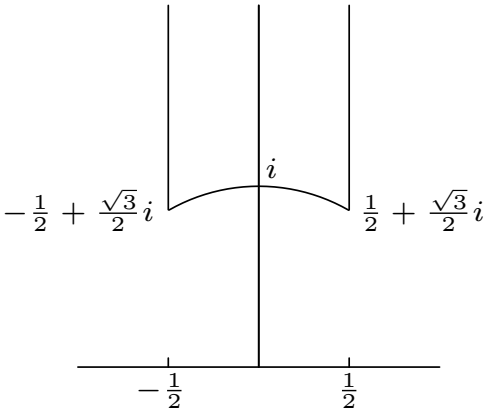


Figura 1: Dominio fundamental F

Demostración. Se encuentra en [Kob93]. La región que define F es la presentada en la figura anterior. Defina

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Sea Γ el subgrupo de $SL_2(\mathbb{Z})$generado por S y T. Fije $\tau \in \mathcal{H}$. Suponga que no existe $\gamma \in \Gamma$ tal que $\gamma\tau \in F$. Se vio en la Proposición 2.3 del Capítulo 1 que, dado $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ en $\Gamma \subseteq SL_2(\mathbb{Z})$, $\text{Im}\ \gamma\tau = \text{Im}\ \tau/|c\tau + d|^2$. Sin embargo, $|c\tau + d|$ está acotado por abajo por 0. Además los números $|c\tau + d|$ con c y d variando están ubicados sobre el retículo generado por 1 y τ. Entonces existe una

bola alrededor de 0 que contiene a al menos un punto de esa forma en el retículo y por tanto un mínimo para $|c\tau + d|$. Así existe una matriz $\gamma \in \Gamma$ tal que Im $\gamma\tau$ es maximal. Por otra parte Re $T\tau =$ Re $\tau + 1$ y Re $T^{-1}\tau =$ Re $\tau - 1$, por lo tanto existe j tal que si se toma $\gamma' = T^j\gamma$, $|\text{Re } \gamma'\tau| \leq 1/2$. Además, Im $T\tau =$ Im τ, entonces Im $\gamma\tau =$ Im $\gamma'\tau$. Así es posible asumir que $-\frac{1}{2} \leq$ Im $(\gamma\tau) \leq \frac{1}{2}$

Si $\gamma\tau \notin F$ (por hipótesis), necesariamente $|\gamma\tau| < 1$. Otra vez usando la Proposición 2.3 del Capítulo 1, se tiene

$$\text{Im } S\gamma\tau = \frac{\text{Im } \gamma\tau}{|\gamma\tau|^2} > \text{Im } \gamma\tau.$$

Esto contradice la maximalidad Im $\gamma\tau$ y por tanto, debe existir $\gamma \in \Gamma$ tal que $\gamma\tau \in F$.

Ahora considere τ_1 y τ_2 en F tales que existe $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ con $\tau_2 = \gamma\tau_1$. Suponga sin pérdida de generalidad que Im $\tau_1 \leq$ Im τ_2. Por la Proposición 2.3 del Capítulo 1, Im $\tau_2 = \dfrac{\text{Im } \tau_1}{|c\tau_1 + d|} \leq$ Im τ_1, entonces $|c\tau_1 + d| \geq 1$. Pero $\tau_1 \in F$ y d es un entero, así que la desigualdad no se cumple si $|c| \geq 2$. Este resultado y el hecho de que $\gamma \in SL_2(\mathbb{Z})$ lleva a cuatro casos:

(*i*) $c = 0$ y $d = \pm 1$ (ya que $ad = 1$). Esto implica que $\gamma = \pm \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ y por tanto $\pm\gamma = T^j$ para algún j. Sin embargo, $\gamma\tau_1 \in F$ y por lo tanto $j = \pm 1$ y τ_1 está en alguna de las rectas Re $\tau = -1/2$ o Re $\tau = 1/2$. En ese caso ambos puntos están en la frontera de F.

(*ii*) $c = \pm 1$, $d = 0$ y τ_1 pertenezca al círculo unitario. Aquí $\gamma = \pm \begin{pmatrix} * & -1 \\ 1 & 0 \end{pmatrix} = \pm T^a S$ con $a = 0$ o $a = \pm 1$. Si $a = 0$, $|\tau_2| = |-1/\tau_1| = |\tau_1| = 1$, entonces τ_1 y τ_2 están sobre el círculo unitario, la frontera de F. Si en cambio $a = \pm 1$, $\tau_1 = \tau_2 = \pm\frac{1}{2} + \frac{\sqrt{3}}{2}i$.

(*iii*) $c = d = \pm 1$ y $\tau_1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Entonces $\gamma = \pm \begin{pmatrix} x & x-1 \\ 1 & 1 \end{pmatrix} = \pm T^a \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \pm T^a S$. Si $a = 0$, $\tau_2 = \tau_1$. Si $a = 1$, $\tau_2 = \tau_1 + 1 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ y ambos puntos están en la frontera de F.

(*iv*) $c = -d = \pm 1$ y $\tau_1 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$, que es un caso análogo al anterior y también se llega a que ambos puntos pertenecen a la frontera de F.

Por lo tanto, si existen $\gamma \in \Gamma$ y $\tau \in F$ tales que $\gamma\tau \in F$, necesariamente $\gamma = I$ o τ y $\gamma\tau$ pertenecen a la frontera de F. Ésto concluye la prueba de que F es el dominio fundamental de Γ. □

Proposición 2.5. *El grupo modular está generado por las matrices*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad y \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Demostración. Sean Γ como en el lema anterior, τ en el interior de F y $g \in SL_2(\mathbb{Z})$. Como el dominio fundamental de Γ es F, existe $\gamma \in \Gamma$ tal que $\gamma g\tau \in F$, pero por hipótesis τ está en el interior de F, entonces $\gamma g = I$, es decir, $g = \gamma^{-1}$ y por lo tanto $g \in \Gamma$. □

2.1. Finitud del número de clases

Anteriormente se probó para formas binarias que el número de clases es finito. La demostración fue usando la desigualdad que caracteriza una forma reducida. Sin embargo, existe una forma mucho más geométrica de demostrarlo que además se puede generalizar a más variables. Esta prueba usa la acción de $SL_2(\mathbb{Z})$ sobre el plano superior complejo y por eso sólo se puede realizar hasta este momento.

Lema 2.6. *Si α es una raíz compleja del polinomio $ax^2 + bx + c$ y si el discriminante se define como $D = b^2 - 4ac$, entonces $D = a^2(\alpha - \overline{\alpha})^2$. Si en particular el polinomio es mónico, $D = (\alpha - \overline{\alpha})^2$.*

Demostración. Si α es una raíz compleja del polinomio $f(x) = ax^2 + bx + c$, $\overline{\alpha}$ también lo es porque $f(x) \in \mathbb{Z}[x] \subseteq \mathbb{R}[x]$. Se tiene que $a \neq 0$ porque α tiene parte imaginaria positiva. Por las fórmulas de polinomios simétricos, $\dfrac{b}{a} = \alpha + \overline{\alpha}$ y $\dfrac{c}{a} = \alpha\overline{\alpha}$. Así

$$D = b^2 - 4ac = a^2(\alpha + \overline{\alpha})^2 - 4a^2\alpha\overline{\alpha} = a^2(\alpha^2 + 2\alpha\overline{\alpha} + \overline{\alpha}^2 - 4\alpha\overline{\alpha}) = a^2(\alpha - \overline{\alpha})^2.$$

□

Teorema 2.7. *Para todo $D < 0$, $h(D)$ es finito.*

Demostración. Para la segunda demostración se define $Q_D(x, y)$ como el conjunto de formas cuadráticas de discriminante D. En el capítulo primero se vio que $SL_2(\mathbb{Z})$ actúa sobre el plano superior complejo así:

$$\gamma(\alpha) = \frac{r\alpha + s}{t\alpha + u}, \qquad \gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z}), \ \ \tau \in \mathbb{C}.$$

Sea α en $\mathcal{H}$ un elemento algebraico, es decir, α es raíz de un polinomio con coeficientes en $\mathbb{Z}$. Suponga que el polinomio minimal sobre $\mathbb{Z}$ del cual α es raíz es de grado dos, entonces α será un **número cuadrático**. Sea $ax^2 + bx + c \in \mathbb{Z}[x]$ dicho polinomio. Se puede suponer que $(a, b, c) = 1$ y que $a > 0$, de lo contrario divida entre el máximo común divisor y multiplique por -1. Análogamente a lo que se hizo con formas cuadráticas, se define el discriminante del polinomio como $D = b^2 - 4ac$. Ahora se toma el conjunto $\mathcal{H}(D)$ de todos los números cuadráticos con polinomio minimal de discriminante D.

El primer hecho a notar es que $\mathcal{H}(D)$ es invariante bajo la acción de $SL_2(\mathbb{Z})$. Si $\gamma \in SL_2(\mathbb{Z})$ y α es un número cuadrático, la extensión $\mathbb{Q}(\alpha)/\mathbb{Q}$ tiene grado 2. Como $\mathbb{Q}(\alpha)$ es un cuerpo, $\gamma(\alpha) \in \mathbb{Q}(\alpha)$. Además $\gamma(\alpha) \notin \mathbb{Q}$ porque Im $\gamma(\alpha) > 0$. Además, 2 es primo, por lo cual no pueden existir cuerpos intermedios entre $\mathbb{Q}$ y $\mathbb{Q}(\alpha)$. Por lo tanto $\mathbb{Q}(\alpha) = \mathbb{Q}(\gamma(\alpha))$ y así $\mathbb{Q}(\gamma(\alpha))/\mathbb{Q}$ tiene grado 2, lo que implica que el polinomio minimal sobre $\mathbb{Q}$ de $\gamma(\alpha)$ es de grado 2. Se puede suponer que el polinomio está sobre $\mathbb{Z}$ multiplicando por el mínimo común múltiplo de los denominadores de los coeficientes. Entonces $\gamma(\alpha)$ es también número cuadrático.

Ahora se verá que el discriminante de $\gamma(\alpha)$ también es D. Basta demostrarlo para los generadores de $SL_2(\mathbb{Z})$. Se define

$$p(x) = ax^2 + bx + c$$

el polinomio para el cual $p(\alpha) = 0$. El primer generador del grupo es la transformación $\alpha \mapsto \alpha + 1$, este último es raíz del polinomio $p(x - 1) \in \mathbb{Z}[x]$. El coeficiente que acompaña a x^2 es a y por el Lema 2.6, el discriminante del polinomio cuadrático minimal de $\alpha+1$ sobre $\mathbb{Z}$ es: $a^2((\alpha+1)-(\overline{\alpha+1}))^2 = a^2(\alpha-\overline{\alpha} = D$. El otro generador del grupo es la transformación $\alpha \mapsto -1/\alpha$. Por el mismo procedimiento, $-1/\alpha$ es raíz de $p(-1/x)$ y por tanto, también es raíz de $x^2p(-1/x)$ (x nunca es 0). El término que acompaña a x^2 en dicho polinomio es c y también por el Lema 2.6, el discriminante del polinomio es

$$c^2\left(-\frac{1}{\alpha} + \frac{1}{\overline{\alpha}}\right)^2 = c^2\left(\frac{\alpha - \overline{\alpha}}{\alpha\overline{\alpha}}\right)^2.$$

Pero se sabe que $\alpha\overline{\alpha} = c/a$, de donde se obtiene que:

$$c^2\left(-\frac{1}{\alpha} + \frac{1}{\overline{\alpha}}\right)^2 = a^2\left(\alpha - \overline{\alpha}\right)^2 = D.$$

Ahora se define la función $\phi : Q_D(x, y) \to \mathcal{H}(D)$ dada por $\phi(ax^2 + bxy + cy^2) = (-b + \sqrt{D})/2a$. Por la construcción $\phi(f) \in \mathcal{H}(D)$ para toda forma cuadrática f de discriminante D. Además es posible definir ψ como: dado un número cuadrático α en $\mathcal{H}(D)$ raíz del polinomio $ax^2 + bx + c$, $\psi(\alpha) = ax^2 + bxy + cy^2$. Es claro que ψ es la inversa de ϕ y por tanto definen un isomorfismo. Además ϕ respeta la acción de $SL_2(\mathbb{Z})$. Si $A \in SL_2(\mathbb{Z})$ y $f \in Q_D(x, y)$, $\phi(f^A) = A\phi(f)$.

Al final se puede concluir que ϕ induce una biyección entre $Q_D(x, y)/SL_2(\mathbb{Z})$ y $\mathcal{H}(D)/SL_2(\mathbb{Z})$. Además, $\phi(f)$ está acotado en la parte imaginaria por $\sqrt{D}/2$. Entonces se tiene que el dominio fundamental es un cerrado discreto contenido en la siguiente región

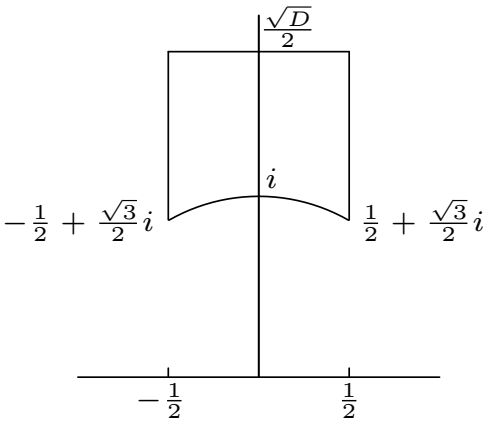


Figura 2: Dominio fundamental de $SL_2(\mathbb{Z})$ en $\mathcal{H}(D)$

Como es cerrado en $\mathbb{R}^2$, es compacto, pero es un discreto y por tanto debe contener finitos puntos. Entonces $\mathcal{H}(D)/SL_2(\mathbb{Z})$ es finito, de donde se llega a que $h(D) = \#Q_D/SL_2(\mathbb{Z})$ también lo es. □

Teorema 2.8. *Existen finitas clases de equivalencia de formas cuadráticas del mismo determinante.*

Idea de la demostración. Se hace una generalización de la demostración anterior para el caso de dos variables. También se basa en demostrar que en un subconjunto compacto de $\mathcal{H}$ se puede encontrar un representante de cada clase de equivalencia. Además esos puntos deben ser abiertos y forman un subconjunto cerrado. Entonces se tiene un subconjunto cerrado, acotado y discreto de $\mathbb{R}^n$, lo que implica que debe ser finito.

Una prueba algebraica se puede encontrar en [Cas78, Teo 1., Pg. 128].

3. Retículos

Existe una biyección entre una clase especial de retículos y formas cuadáticas enteras. En algunos casos es más sencillo estudiar estos retículos. De hecho, más adelante será de gran utilidad conocer dicha biyección.

Definición 3.1. Un **retículo** es un subrupo de $\mathbb{R}^n$ que es un $\mathbb{Z}-$módulo finitamente generado por un conjunto linealmente independiente.

En la definición no se pide que se tengan n vectores linealmente independientes pero muchas veces esa condición es necesaria. Un retículo que cumpla eso se denomina **retículo completo** y para este documento sólo se trabajará con retículos de este tipo.

Ejemplo 3.2. Un retículo Λ puede ser el generado por $(0,1)$ y $(1,0)$ en $\mathbb{R}^2$ y se ve geométricamente así:

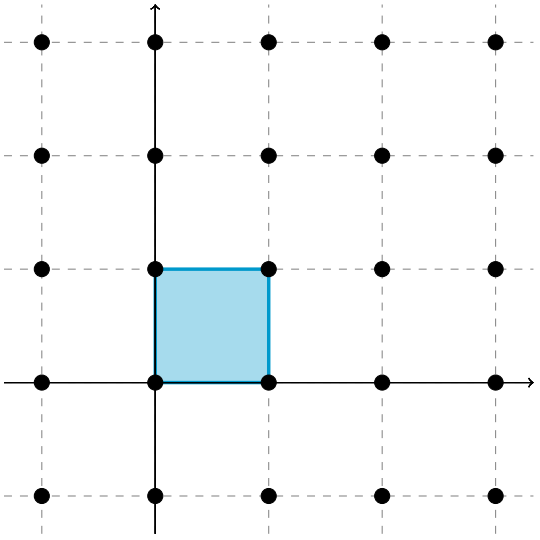


Figura 3: Retículo generado por $(0,1)$ y $(1,0)$

Definición 3.3. La **región fundamental** para un retículo Λ en $\mathbb{R}^n$ generado por $v_1, \ldots, v_n$ será:

$$D(\Lambda) = \left\{ \sum_{i=1}^{n} \lambda_i v_i \;\middle|\; 0 \leq \lambda_i \leq 1 \right\}$$

Dos retículos son iguales si tienen la misma región fundamental. Sin embargo, comparar dos regiones fundamentales dadas presenta dificultades en dimensiones grandes y por lo tanto se debe introducir la definición que se da a continuación.

Definición 3.4. El **volumen** de un retículo es el volumen de la región fundamental. Se denota por $d(\Lambda)$.

En el Ejemplo 3.2 está sombreada la región fundamental, es fácil ver que su volumen es 1.

Si bien el volumen ayuda a comprobar si dos retículos son distintos, no es siempre cierto que si dos retículos tienen el mismo volumen, entonces son iguales. Por ejemplo, el retículo generado por $(1, \frac{1}{2})$ y $(\frac{1}{2}, \frac{3}{2})$ también tiene volumen uno, pero no es el mismo retículo generado por $(1,0)$ y $(0,1)$ ya que las regiones fundamentales son distintas.

Como los retículos son subconjuntos de $\mathbb{R}^n$ heredan la métrica de este espacio. Por tanto para cualquier retículo $\Lambda \subseteq R^n$ y cualquier $\boldsymbol{x} \in \Lambda$ se definir la **norma** de $\boldsymbol{x}$ como $\langle \boldsymbol{x}, \boldsymbol{x} \rangle$. En $\mathbb{R}^n$ esta definición es equivalente al cuadrado de la norma, pero en este contexto será más sencillo trabajar con la primera.

Al igual que con las formas cuadráticas se define la **matriz de Gram** de un retículo Λ como la matriz

$$\begin{pmatrix} v_1 \cdot v_1 & v_1 \cdot v_2 & \dots & v_1 \cdot v_n \\ v_1 \cdot v_2 & v_2 \cdot v_2 & \dots & v_2 \cdot v_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1 \cdot v_n & v_2 \cdot v_n & \dots & v_n \cdot v_n \end{pmatrix}.$$

En donde $v_1, \dots, v_n$ son una base de Λ.

Resulta útil tener una noción geométrica de lo que representa el determinante de la matriz de Gram.

Definición 3.5. El **covolumen** de un retículo es el cuadrado de su volumen.

Observación 3.6. El covolumen resulta ser el determinante de la matriz de Gram de un retículo.

Definición 3.7. Dos retículos son **equivalentes** si sus matrices de Gram B y B' estan relacionadas por:

$$B' = A\,{}^{\mathrm{t}}BA \tag{3.1}$$

con B una matriz entera con determinante ± 1.

Las formas serán **propiamente equivalentes** si el determinante de B es 1.

Las definiciones resultan bastante similares con lo hecho con formas cuadráticas. La relación de la Definición 3.1 resulta ser una relación de equivalencia. De la misma forma, para retículos se tendrá un análogo a forma cuadrática entera, como se puede ver en la siguiente definición.

Definición 3.8. Un **retículo con producto interno entero** es un retículo con matriz de Gram entera.

Que un retículo tenga producto interno entero es equivalente a que para cada par de vectores en el retículo, su producto interno resulta ser un número entero.

3.1. Retículos y formas cuadráticas

Es sabido que existe una biyección entre clases de equivalencia de formas cuadráticas enteras y retículos con producto interno entero.

$$\left\{ \begin{array}{c} \text{Formas cuadráticas} \\ \text{enteras} \end{array} \right\} \quad \begin{array}{c} \xrightarrow{\varphi} \\ \xleftarrow{\psi} \end{array} \quad \left\{ \begin{array}{c} \text{Retículos con producto} \\ \text{interno entero} \end{array} \right\}. \tag{3.2}$$

El objetivo es hacer explícita dicha biyección.

Sean $f(\boldsymbol{x})$ una forma cuadrática entera y B su matriz de Gram. Como B es simétrica, es diagonalizable y por lo tanto

$$B = Q^{-1}DQ$$

con Q matriz ortogonal. Se define $\sqrt{D}$ como la matriz diagonal con entradas las raíces de los elementos de la diagonal de D. Así

$$B = Q^{-1}DQ = Q\,{}^{\mathrm{t}}DQ = Q\,{}^{\mathrm{t}}\sqrt{D}\sqrt{D}Q = (\sqrt{D}Q)^t(\sqrt{D}Q).$$

Se toma $A = \sqrt{D}Q$. Debido a que $\sqrt{D}$ es diagonal, $\sqrt{D}^t = \sqrt{D}$. De lo anterior se concluye que $B = A\,{}^{\mathrm{t}}A$.

Es así como cualquier matriz de Gram de una forma cuadrática se puede escribir como el producto de una matriz transpuesta y la misma matriz sin transponer. Entonces se define

$$\varphi(f) = L_A := \{A\boldsymbol{x} \ : \ \boldsymbol{x} \in \mathbb{Z}^n\},$$

el retículo generado por los vectores columna de la matriz A.

Ahora, dado un retículo Λ con producto interno entero y base $v_1, \ldots, v_n$, se considera B la matriz de Gram de Λ y se define

$$\psi(L) = \boldsymbol{x}B\boldsymbol{x}^t,$$

que es una forma cuadrática entera porque B es su matriz de Gram.

Hecho 3.9. *Las funciones definidas anteriormente definen una biyección entre clases de equivalencia.*

Demostración. Ver [CS99, Sec. 2.2, Pg. 42] □

Observación 3.10. Con lo anterior, si f y Λ están en biyección, es posible suponer que ambos tienen la misma matriz de Gram.

Proposición 3.11. *Dados f forma cuadrática y Λ retículo correspondiente a f, f representa a $m \in \mathbb{Z}$ si y solo si existe $\boldsymbol{v} \in \Lambda$ tal que $\boldsymbol{v} \cdot \boldsymbol{v} = m$*

Demostración. Sean B la matriz de Gram de f y $m \in \mathbb{Z}$ representado por $f(\boldsymbol{x})$, entonces existen $v_1, \ldots, v_n \in \mathbb{Z}$ tales que $f(\boldsymbol{v}) = m$, esto es:

$$\boldsymbol{v}B\boldsymbol{v}^t = m.$$

Sin embargo, como Λ está asociado a f, B es la matriz de Gram de B y por tanto la anterior igualdad es la norma de $\boldsymbol{v}$ en el retículo Λ.

En segundo lugar, suponga que existe $\boldsymbol{v} \in L$ tal que $\boldsymbol{v} \cdot \boldsymbol{v} = m$, esto es,

$$\boldsymbol{v}B\boldsymbol{v}^t = m.$$

Entonces la forma f evaluada en $\boldsymbol{v}$ es igual a m. □

Por la biyección, todos los conceptos de formas cuadráticas se generalizan a retículos con producto interno entero.

En el primer capítulo, Definición 1.5 se vio que es posible definir una noción de reducibilidad en formas cuadráticas binarias. Usando retículos con producto interno entero, es posible generalizar dicha noción.

Definición 3.12. f forma cuadrática es **Minkowski reducida** si se expresa en términos de una base integral $e_1, \ldots, e_n$ tales que para todo t, $1 \leq t \leq n$

$$f(e_t) \leq f(v) \tag{3.3}$$

para todo vector v tal que $e_1, \ldots, e_{t-1}, v$ se puede extender a una base integral.

Entre otras condiciones, para que una forma cuadrática sea Minkowski reducida, su matriz de Gram B debe cumplir:

$$0 \leq b_{11} \leq \ldots \leq b_{nn}. \tag{3.4}$$

Si ahora se define $v = e_t + \sum_{s \in S} \epsilon_s e_s$ para algún conjunto de índices S con $s < t$ para todo $s \in S$ y $\epsilon_s = \pm 1$ arbitrarios. Ya que v es una combinación lineal de elementos de la base y los índices son menores que t, se puede reemplazar e_t por v y sigue siendo posible tener una base integral, es decir, $e_1, \ldots, e_{t-1}, v$ se puede extender a una base integral. Por lo tanto, para que la forma sea Minkowski $f(e_t)$ puede ser extendido a una base integral. Por ende se debe cumplir 3.3 y así:

$$2\left|\sum_{s \in S} \epsilon_s b_{st} - \sum_{\substack{r,s \in S \\ r<s}} \epsilon_r \epsilon_s b_{rs}\right| \leq \sum_{s \in S} b_{ss}.$$

Para el caso particular en el que $S = \{s\}$, la desigualdad anterior se escribe como:

$$2|b_{st}| \leq b_{ss}. \tag{3.5}$$

Si en cambio $S = \{r, s\}$ con $r < s < t$, se tiene

$$2|b_{rs} \pm b_{rt} \pm b_{st}| \leq b_{rr} + b_{ss}. \tag{3.6}$$

Igualmente si $S = \{q, r, s\}$ con $q < r < s < t$ y $\{\alpha, \beta, \gamma\} \subseteq \{\pm 1\}$,

$$2|\alpha b_{qt} + \beta b_{rt} + \gamma b_{st} - \alpha\beta b_{qr} - \alpha\gamma b_{qs} - \beta\gamma b_{rs}| \leq b_{qq} + b_{rr} + b_{ss}. \tag{3.7}$$

Se contínua así para cada conjunto posible y se dan condiciones necesarias sobre la matriz de Gram para que la forma sea Minkowski reducida. En el caso de $n \leq 4$ se puede hacer una afirmación mucho más fuerte.

Hecho 3.13. *Si se tiene una forma cuadrática en dos y tres variables, las desigualdades 3.4, 3.5, 3.6 y 3.7 dan condiciones suficientes para que una forma sea Minkowski reducida.*

La demostración se puede encontrar en [Cas78, Lema 1.2, Pg. 257].

Observación 3.14. Para formas binarias, que una forma sea Minkowski reducida es equivalente a que sea reducida.

Esto es, porque en el lema anterior se asegura que las desigualdades son condiciones suficientes para que las formas sean Minkowski reducidas. Si se tiene $f = (a, b, c)$ forma binaria definida positiva y reducida, entonces $|b| \leq a \leq c$ y su matriz de Gram es

$$B = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

La Desigualdad 3.4 pide que $a \leq c$, que se cumple porque f es reducida. Por su parte, 3.5 se cumple si

$$2\left|\frac{b}{2}\right| \leq a, \text{ equivalente a que } |b| \leq a.$$

De la misma forma, es fácil demostrar que si una forma binaria es Minkowski reducida entonces es reducida. Así, ambas definiciones coinciden en formas cuadráticas binarias.

Para reducir una matriz de Gram, esta se debe mantener simétrica, por lo tanto lo que se hace es un análogo al algorítmo de Gauss - Jordan de multiplicar por matrices elementales. Dada una matriz elemental E, una matriz de Gram equivalente a la matriz de Gram B será:

$$EBE^t.$$

Ejemplo 3.15. La forma cuadrática $x^2 + y^2 + 3z^2 + 4yz$ no es Minkowski reducida ya que su matriz de Gram es

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 3 \\ 0 & 3 & 5 \end{pmatrix}$$

pero $2|b_{23}| > b_{22}$ ya que $2 \cdot 3 > 2$. Sin embargo, la matriz se puede reducir por el método explicado anteriormente así:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 3 \\ 0 & 3 & 5 \end{pmatrix} \xrightarrow[c_2 = c_2 - c_3]{f_2 = f_2 - f_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & -2 & 5 \end{pmatrix} \xrightarrow[c_3 = c_3 + 2c_2]{f_3 = f_3 + 2f_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

La matriz obtenida es Minkowski reducida porque $1 \leq 1 \leq 1$ y $0 \leq 1$.

4. Formas cuadráticas universales

Cuando se habló de formas cuadráticas se dijo que una forma cuadrática es **universal** si representa a todos los enteros positivos. Una pregunta bastante interesante será cuándo una forma cuadrática es universal. En principio el problema parece bastante complicado porque se puede creer que hace falta revisar que la forma representa a todos los enteros positivos. Sin embargo, en el año 1993 John Conway y William Schneeberger se acercaron a resolver el problema planteando un teorema y una conjetura. El teorema, que se explicará a continuación, da una condición necesaria y suficiente para que una forma cuadrática entera sea universal y la conjetura, para que cualquier forma cuadrática lo sea.

4.1. Teorema de los 15

Teorema 4.1. ***(Teorema de los 15, Conway–Schneeberger)*** *Una forma cuadrática entera es universal si y solo si representa a los enteros: 1,2,3,5,6,7,10,14,15*

Antes de pasar a la demostración del teorema, se presentará un resultado interesante.

Corolario 4.2. ***(Cuatro Cuadrados de Lagrange).*** *La forma cuadrática*

$$x^2 + y^2 + z^2 + w^2$$

es universal.

Demostración. Esta es una forma cuadrática definida positiva y entera. Es fácil ver que

$$\begin{array}{rcccccccc}
1 &=& 1^2 &+& 0^2 &+& 0^2 &+& 0^2 \\
2 &=& 1^2 &+& 1^2 &+& 0^2 &+& 0^2 \\
3 &=& 1^2 &+& 1^2 &+& 1^2 &+& 0^2 \\
5 &=& 2^2 &+& 1^2 &+& 0^2 &+& 0^2 \\
6 &=& 2^2 &+& 1^2 &+& 1^2 &+& 0^2 \\
7 &=& 2^2 &+& 1^2 &+& 1^2 &+& 1^2 \\
10 &=& 3^2 &+& 1^2 &+& 0^2 &+& 0^2 \\
14 &=& 3^2 &+& 2^2 &+& 1^2 &+& 0^2 \\
15 &=& 3^2 &+& 2^2 &+& 1^2 &+& 1^2.
\end{array}$$

Por el teorema anterior, la forma es universal. □

Como se puede notar, el teorema simplifica mucho los cálculos y por eso hace relativamente fácil comprobar si una forma cuadrática entera es universal o no. A continuación se explicará una prueba del teorema. La demostración usa elementos computacionales y la teoría que fue expuesta en capítulos anteriores. Se inicia con la biyección entre formas cuadráticas enteras y retículos con producto interno. Por lo tanto es importante notar que el teorema de los 15 se puede reescribir para retículos como se sigue.

Teorema 4.3. ***Teorema de los 15 (versión geométrica)*** *Un retículo con producto interno entero es universal si y solo si tiene vectores de norma 1,2,3,5,6,7,10,14,15*

En esta sección se trabajará únicamente con formas cuadrátias enteras y retículos con producto interno entero. A continuación se darán algunas definiciones necesarias para desarrollar la demostración.

Definición 4.4. Si f es una forma no universal, el **ausente** de f será el mínimo entero positivo que f no representa.

Ejemplo 4.5. El ausente de x^2 es 2 y el de $x^2 + 4xy + 2y^2$ es 3.

Definición 4.6. Una **escalada** de un retículo no universal Λ es un retículo generado por Λ y un vector de norma el ausente de Λ.

Ejemplo 4.7. El ausente de $2x^2 + 3y^2$ es 1, entonces la matriz de Gram de una escalada puede ser:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Definición 4.8. Un **retículo escalado** es el que se obtiene mediante una sucesión de escaladas del retículo cero dimensional.

Ahora el objetivo será encontrar todos los posibles retículos escalados. Aunque parece que pueden existir infinitos, se verá que existe únicamente una cantidad finita de ellos. Para la demostración se usará varias veces la biyección entre formas cuadráticas y retículos. Además, se puede suponer que los retículos escalados están Minkowski reducidos (tome el representante de la clase que lo esté).

Se toma el retículo cero dimensional, [0], que corresponde a la forma cuadrática 0. Su ausente es el 1, por lo tanto su única escalada es [1], que corresponde a la forma cuadrática x^2. Es fácil ver que el ausente de esta forma es el 2. Su escalada debe ser un retículo generado por un vector de norma uno y otro independiente de norma 2. Por lo tanto la matriz de Gram se verá así:

$$\begin{pmatrix} 1 & a \\ a & 2 \end{pmatrix}. \tag{4.1}$$

Si v_1 y v_2 son los generadores, la desigualdad de Cauchy-Schwarz asegura:

$$a^2 = (v_1 \cdot v_2)^2 \leq (v_1 \cdot v_1)(v_2 \cdot v_2) = 2. \tag{4.2}$$

Por lo tanto, los únicos valores que puede tomar a son $1, 0$ y -1.

A continuación se analizará uno de los casos detalladamente.

Si $a = 1$ de la matriz (4.1) se obtiene:

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}. \tag{4.3}$$

Como interesan los retículos equivalentes basta con encontrar dos vectores en $\mathbb{Z}^2$ que cumplan dicha relación. Se toma

$$v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad v_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}. \tag{4.4}$$

Entonces la región fundamental de dicho retículo es:

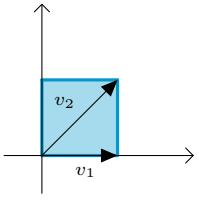


Figura 4: Región fundamental generada por por $(1, 0)$ y $(1, 1)$

A partir de la gráfica es claro que el látice generado por v_1 y v_2 es el generado por e_1 y e_2 ya que las regiones fundamentales son iguales. La región fundamental del segundo se muestra a continuación:

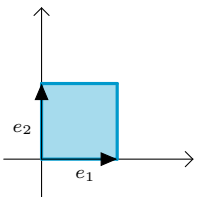


Figura 5: Región fundamental generada por por $(1, 0)$ y $(0, 1)$

La igualdad se da porque

$$e_1 = v_1 \qquad \text{y} \qquad e_2 = v_2 - v_1$$

Por otra parte, si se realiza la reducción de la matriz de Gram (4.3), se obtiene:

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \xrightarrow[c_2=c_2-c_1]{f_2=f_2-f_1} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Es así como por los dos procedimientos se concluye que el retículo con matriz de Gram 4.3 es el retículo con matriz de Gram igual a la identidad.

La identidad es Minkowski reducida porque una base de su forma cuadrática correspondiente $f(x, y) = x^2 + y^2$ es $B = \{e_1, e_2\}$ con $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ y $e_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ que cumplen:

$$f(e_1) = 1 \qquad y \qquad f(e_2) = 1$$

Por lo que para todo vector no trivial $v \in \mathbb{Z}^2$, $f(e_1) = f(e_2) \leq f(v)$, en cuyo caso se obtiene el resultado.

Si $a = -1$:

$$\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \xrightarrow[c_2=c_2+c_1]{f_2=f_2+f_1} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Si $a = 0$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix},$$

una matriz que ya es Minkowski reducida.

Es así como después de la tercera escalada, se obtienen dos matrices Minkowski reducidas:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{y} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}.$$

Es importante aclarar que los retículos correspondientes a ambas matrices no son equivalentes porque su covolumen es distinto (1 y 2). Las matrices de Gram corresponden a las formas cuadráticas:

$$x^2 + y^2 \qquad \text{y} \qquad x^2 + 2y^2,$$

que tienen por ausentes a:

$$3 \qquad \text{y} \qquad 5.$$

Se deben estudiar ahora los dos casos por separado. La escalada de la forma $x^2 + y^2$, será:

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ a & b & 3 \end{pmatrix}. \tag{4.5}$$

Otra vez por Cauchy-Schwarz, $\{a, b\} \subseteq \{-1, 0, 1\}$. Además, si se reduce la matriz de Gram, se obtiene:

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ a & b & 3 \end{pmatrix} \xrightarrow[c_3=c_3-ac_1]{f_3=f_3-af_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & b & 3-a^2 \end{pmatrix} \xrightarrow[c_3=c_3-bc_2]{f_3=f_3-bf_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3-a^2-b^2 \end{pmatrix}.$$

Entonces se tienen varios casos: el primero, $a = \pm 1$ y $b = \pm 1$, en cuyo caso se obtienen la matriz

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Si $a = \pm 1$ y $b = 0$ o si $a = 0$ y $b = \pm 1$ la escalada es:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Y por último, si $a = b = 0$, la matriz queda de la forma

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Los tres retículos asociados no son iguales ya que tienen covolumenes distintos (1,2,3). En conclusión, para la escalada de la forma $x^2 + y^2$, se tienen tres opciones.

Por otro lado, se debe realizar el mismo análisis para la forma $x^2 + 2y^2$. La escalada debe tener la forma:

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 2 & b \\ a & b & 5 \end{pmatrix}. \tag{4.6}$$

con $a \in \{0, \pm 1, \pm 2\}$ y $b \in \{0, \pm 1, \pm 2, \pm 3\}$ (por Cauchy-Schwarz). Si se hace la reducción de Minkowski de la matriz se llega a:

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 2 & b \\ a & b & 5 \end{pmatrix} \xrightarrow[c_3 = c_3 - ac_1]{f_3 = f_3 - af_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & b \\ 0 & b & 5 - a^2 \end{pmatrix}.$$

De donde se siguen los casos:

$a = 0$, $b = 0$ $\quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}$

$a = 0$, $b = 1$ $\quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 5 \end{pmatrix}$

$a = 0$, $b = -1$ $\quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -1 \\ 0 & -1 & 5 \end{pmatrix} \xrightarrow[c_3 = c_3 + c_2]{f_3 = f_3 + f_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 4 \end{pmatrix}$

$a = 0$, $b = 2$ $\quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 2 & 5 \end{pmatrix} \xrightarrow[c_3 = c_3 - c_2]{f_3 = f_3 - f_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$

$a = 0$, $b = -2$ $\quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -2 \\ 0 & -2 & 5 \end{pmatrix} \xrightarrow[c_3 = c_3 + c_2]{f_3 = f_3 + f_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$

$a = 0$, $b = 3$ $\quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 3 \\ 0 & 3 & 5 \end{pmatrix} \xrightarrow[c_2 = c_2 - c_3]{f_2 = f_2 - f_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & -2 & 5 \end{pmatrix} \xrightarrow[c_3 = c_3 + 2c_2]{f_3 = f_3 + 2f_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$a = 0$, $b = -3$ $\quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -3 \\ 0 & -3 & 5 \end{pmatrix} \xrightarrow[c_3 = c_3 + 2c_2]{f_3 = f_3 + 2f_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 5 \end{pmatrix} \xrightarrow[c_3 = c_3 - 2c_2]{f_3 = f_3 - 2f_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$$
\begin{array}{ll}
a=\pm 1 \\ b=0 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix} \\[2ex]
a=\pm 1 \\ b=1 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 4 \end{pmatrix} \\[2ex]
a=\pm 1 \\ b=-1 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -1 \\ 0 & -1 & 4 \end{pmatrix} \xrightarrow[c_3=c_3+c_2]{f_3=f_3+f_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 4 \end{pmatrix} \\[2ex]
a=\pm 1 \\ b=2 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 2 & 4 \end{pmatrix} \xrightarrow[c_3=c_3-c_2]{f_3=f_3-f_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \\[2ex]
a=\pm 1 \\ b=-2 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -2 \\ 0 & -2 & 4 \end{pmatrix} \xrightarrow[c_3=c_3+c_2]{f_3=f_3+f_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}
\end{array}
$$

Hacen falta en la lista los últimos dos casos que se dan cuando $a = \pm 1$ y $b = \pm 3$. En ambos casos el determinante de la matriz es -1 y por el Criterio de Sylvester (Capítulo 2) las matrices no son definidas positivas, así que el caso no se puede dar. En conclusión se obtienen en total nueve retículos escalados de dimensión tres con matrices de Gram Minkowski reducidas:

$$
\begin{gathered}
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \\
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 5 \end{pmatrix} \ y \ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}
\end{gathered} \tag{4.7}
$$

Ninguna igual a otra porque tienen covolumen distinto: 1, 2, 3, 4, 6, 7, 8, 9 y 10 respectivamente.
En la tabla anexa se presentan los retículos escalados de dimensión tres con sus respectivos covolumenes y ausentes.

El algorítmo para encontrar las escaladas se vuelve más largo a medida que la dimensión crece. Por lo tanto, el procedimiento para las escaladas de dimensión cuatro debe hacerse computacionalmente. No se presentará el código pero se obtienen en total 207 retículos no equivalentes como se encuentra en [BFLR00, Pg. 37].

Como se explicó cuando se presentaron las formas cuadráticas universales (Obs. 1.20), no existen formas universales en tres o menos variables; por tanto, los retículos de dimensión cuatro son los primeros retículos que pueden llegar a ser universales. La forma de comprobar cuál es el ausente se basa en estudiar los retículos en dimensión tres y usar la teoría del género de formas cuadráticas para ver qué enteros representan. Al final se llega a que 201 retículos de la lista son universales.

Para probar que son universales se realiza el mismo procedimiento con todos ellos. Para cada retículo de dimensión cuatro L se encuentra un retículo Λ de dimensión tres que sea único en su género. Mediante un análisis local se encuentran los enteros representados por Λ, que también son representados por L. La idea será ver que L como antes representa a todos los enteros lo suficientemente grandes y por lo tanto sólo hace falta comprobar que L representa a finitos enteros, operación que también se hace computacionalmente.

A continuación se mostrará el procedimiento descrito antes para un retículo de la lista 4.7. Como se dijo, el análisis para los otros es similar.

Sea Λ el retículo con matriz de Gram

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Su forma cuadrática asociada es

$$f(x, y, z) = x^2 + y^2 + z^2$$

Como se explicó en el capítulo 2, $h(1)$ es finito y los representantes de las clases se pueden tomar Minkowski reducidos. Por lo tanto, es posible generar mediante un algoritmo un representante de cada clase de equivalencia Minkowski reducido. Además como las matrices en el mismo género tienen igual determinante, para ver que A es única en su género basta comprobar que los otros representantes no pertenecen al mismo género de A. El código en Magma necesario para ejecutar en anterior procedimiento es:

```
M:=Matrix(IntegerRing(),3,3, [1,0,0,0,1,0,0,0,1]);
L:=LatticeWithGram(M);
G:=Genus(L);
#G;
```

En donde el resultado es 1. Así A es única en su género. Otra demostración usa el siguiente teorema.

Hecho 4.9. *Toda forma cuadrática de determinante 1 en n variables con $n \leq 5$ es propiamente equivalente a*

$$x_1^2 + \cdots + x_n^2$$

Demostración. Ver [Cas78, Cor. 2, Pg. 138]. □

Entonces la forma $f(x, y, z)$ no solo es única en su género sino que es la única clase de equivalencia de formas de determinante 1. Ahora se deben encontrar los enteros que no son representados por $f(x, y, z)$. Para ello, se trabajará localmente.

Se toma $r = 2^a b$ un entero 2-ádico, donde a es un entero no negativo y b es una unidad 2-ádica. Se busca encontrar condiciones necesarias y suficientes para comprobar si r es representado por $f(x, y, z)$. Se puede asumir que a es 0 o 1 cambiando las variables por 2 veces ellas si es necesario. Si $a = 1$, $r \equiv 2, 6$ (mód 8) y ambas posibilidades son representadas tomando módulo 8, entonces por la versión de Hensel de varias variables con $k = 1$ (Hecho. 1.26), los dos casos son representados por $f(x, y, z)$. Si en cambio $a = 0$, $r \equiv 1$, 3, 5 o 7 (mód 8). Por la misma versión del Lema de Hensel, tomando módulo 8, los casos 1, 3, 5 son representados por $f(x, y, z,)$ pero el caso 7 no. En conclusión, $r = 2^a b$ es representado por $f(x, y, z)$ a menos que a sea par y $b \equiv 7$ mód 8.

Por lo tanto, $f(x, y, z)$ representa a todos los enteros positivos excepto a los de la forma $4^s(7k + 8)$ para $s, k \in \mathbb{Z}_{\geq 0}$.

Observación 4.10. Si un entero x no es representado por Λ, $x = 2^{2s}(8k + 7)$. Tomando congruencia módulo 8 se tiene $x \equiv 2^{2s} \cdot 7$ (mód 8). Si $s = 0$, $x \equiv 7$ (mód 8). En caso de que s sea 1, $x \equiv 4$ (mód 8). Si $s \geq 2$, $x \equiv 0$ (mód 8) porque $8 \mid 2^3 2^l$ para todo $l \geq 0$. En conclusión, si x no es representado por Λ, puede ser congruente a 0, 4 o 7 módulo 8.

Ahora se considerará el complemento ortogonal de Λ en L. Se denota a su matriz de Gram como $[\mu]$. Como el retículo es un grupo libre sobre $\mathbb{Z}$, se tiene únicamente la contenencia $\Lambda \oplus [\mu] \subseteq L$. El objetivo será mostrar que dicha suma directa representa a todos los enteros lo suficientemente grandes.

Se toma L como antes y $g(x, y, z, w)$ su forma cuadrática asociada. Si g no es universal, existe $u \in \mathbb{Z}$, su ausente. Es necesario notar que u es libre de cuadrados porque si $u = t^2 r$ con $t > 1$, $r = u/t^2$ tampoco

puede ser representado por g y se contradice la minimalidad de u. Además, Λ tampoco representa a u (porque si eso pasa, L lo haría) y por lo visto anteriormente, u debe escribirse de la forma $u = 4^s(8k+7)$ para s, $k \in \mathbb{Z}$. Como u es libre de cuadrados, $s = 0$ y así $u \equiv 7 \pmod 8$.

Ahora la idea será ver que Λ representa a $u - \mu$ o a $u - 4\mu$ para $u \not\equiv 0 \pmod 8$. Para $\mu \equiv 1, 2, 4, 5$ o $6 \pmod 8$ se tiene que $u - \mu \equiv 6, 5, 3, 2$ o $1 \pmod 8$ y por la observación 4.10, $u - \mu$ es representado por Λ. Por otra parte, cuando $\mu \equiv 3$ o $7 \pmod 8$, $u - 4\mu \equiv 3$ o $4 \pmod 8$ y por la misma observación anterior, $u - 4\mu$ es representado por Λ. Si $u \geq 4\mu$ con $\mu \not\equiv 0 \pmod 8$, o $u - \mu$ o $u - 4\mu$ son representados por Λ. Esto implica que $\Lambda \oplus [\mu]$ representa a u porque $[\mu]$ representa a μ y a 4μ, una contradicción porque se supuso que u es el ausente de L pero $\Lambda \oplus [\mu] \subseteq L$. Entonces necesariamente $u \leq 4\mu$.

Para continuar, el ausente de la forma $f(x, y, z) = x^2 + y^2 + z^2$ es 7. Entonces L debe tener por matriz de Gram a:

$$\begin{pmatrix} 1 & 0 & 0 & a \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & c \\ a & b & c & 7 \end{pmatrix}$$

Por Cauchy-Schwartz, a, b y c pertenecen al conjunto $\{0, \pm 1, \pm 2\}$. Es posible reducir la matriz y se obtiene que es equivalente a:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 7 - a^2 - b^2 - c^2 \end{pmatrix}$$

Pero la forma es definida positiva, por criterio de Sylvester (1.15, cap. 2), necesariamente $7 \geq a^2 + b^2 + c^2$. Es importante notar que si el retículo es generado por los vectores v_1, v_2, v_3 y v_4, este último es ya el complemento ortogonal de los tres anteriores y así $\mu = v_4 \cdot v_4$ es la entrada 4,4 de la matriz. Las diferentes opciones que se tienen para μ son: 7, 6, 5 y 4. Entonces μ nunca es múltiplo de 8. El máximo valor que puede tomar μ es 7. Se puede revisar que la escalada representa a todos los enteros hasta 4μ para cualquiera de los posibles valores de μ (esto se hace computacionalmente). Entonces si L no es universal, su ausente debe ser mayor a 4μ. Sin embargo, μ nunca es múltiplo de 8 y por lo tanto es posible utilizar lo probado anteriormente: todo entero mayor que 4μ es representado por L. Entonces no puede existir un ausente de L, lo que implica que es universal.

Es así como todas las escaladas de A son universales. Sin embargo, este resultado no siempre es cierto. Van a existir escaladas de dimensión 4 no universales como se podrá observar a continuación.

Se toma ahora

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

con su forma cuadrática asociada

$$f(x, y, z) = x^2 + 2(y^2 + z^2).$$

Sea Λ el retículo con matriz de Gram A y L una escalada de Λ. En primer lugar, aplicando otra vez el algorítmo en Magma se obtiene que $f(x, y, z)$ es única en su género. Por un argumento similar al que se usó antes (Lema de Hensel localmente), los enteros que no son representados por Λ son también de la forma $4^s(8k + 7)$. Otra vez se toma u el ausente de L y $[\mu]$ el complemento ortogonal de Λ en L. El mimo análisis que se hizo antes se puede usar para ver que $\Lambda \oplus [\mu]$ representa a todos los enteros mayores o iguales a 4μ si $\mu \not\equiv 0 \pmod 8$. Además para esos retículos se puede demostrar analizando cómo se ve la escalada que μ nunca es mayor que 28. Otra vez, mediante un algorítmo se puede verificar que L representa a todos los enteros positivos hasta $4 \cdot 28$. Su μ no es múltiplo de 8, esto muestra que las escaladas son universales.

El caso de $\mu = 8s$ es un poco más problemático, para ello es necesario reconocer cómo se ve la matriz de Gram de L:

$$\begin{pmatrix} 1 & 0 & 0 & a \\ 0 & 2 & 0 & b \\ 0 & 0 & 2 & c \\ a & b & c & 2 \end{pmatrix}$$

con $a \in \{0, \pm 1\}$ y $b, c \in \{0, \pm 1, \pm 2\}$. Un cálculo explícito de las posibilidades muestra que únicamente dos escaladas tienen a μ como múltiplo de 8. Para estas escaladas se encuentra un sub retículo único en su género y se vuelve a realizar el mismo procedimiento. Siempre se podrá encontrar que representan a los enteros lo suficientemente grandes. Sin embargo, un caso particular de esas escaladas resulta ser no universal porque no representa a un único número.

Así se aplica el mismo argumento para cada matriz de la lista 4.7. Al final se obtienen sólo seis retículos que no son universales por la misma razón que en el ejemplo anterior, no representan a un único entero. Estos casos se pueden ver en la tabla 2 anexa. Es así como si se escalan los retículos no universales de dimensión cuatro, se obtendrán retículos universales ya que se les agregará el único entero positivo que no representan. Por lo tanto todos los retículos escalados de dimensión 5 son universales.

Observación 4.11. Todos los posibles ausentes de un retículo escalado son: 1, 2, 3, 5, 6, 7, 10, 14 y 15 (se ve en los análisis que se hicieron antes y en las tablas anexas 1 y 2).

Del análisis anterior se siguen inmediatamente los lemas:

Lema 4.12. *Todo retículo universal contiene a un sub retículo escalado de dimensión a lo sumo 5.*

Demostración. Se construye una sucesión de retículos escalados $0 \subseteq [1] \subseteq L_2 \subseteq \ldots \subseteq L$. Entonces o L_4 o L_5 son universales. □

Corolario 4.13. *Toda forma cuadrática universal tiene a lo menos dimensión cuatro.*

Teorema 4.14. ***Teorema de los 15***

Demostración. Todo retículo universal contiene al menos a un retículo escalado. Si no es universal, es porque no contiene a un retículo escalado universal, esto es, el retículo escalado maximal que contenga tendrá un ausente. Sin embargo, las posibilidades para los ausentes, como se ve en la observación 4.11, son únicamente 1, 2, 3, 5, 6, 7, 10, 14 y 15, de donde se sigue el teorema. □

5. Formas modulares

Como se explicó en la introducción, el Teorema de los Cuatro Cuadrados de Lagrange es de bastante interés ya que es una de las formas cuadráticas univerdales más populares. Con el fin de probar que la forma

$$x^2 + y^2 + z^2 + w^2$$

es universal se puede contar de cuántas formas se puede representar un entero positivo arbitrario. Si se muestra de alguna forma que el número de maneras posibles es distinto de 0, se tiene el Teorema de los Cuatro Cuadrados de Lagrange. En el capítulo anterior se vio que en efecto este número es distinto de 0 para todos los enteros positivos ya que se probó el teorema usando el Teorema de los 15. En este capítulo se buscará el número exacto de representaciones. Para ello se usará una técnica bastante común, definir una función generatriz. Se define

$$r(n) = \#\{(v_1, v_2, v_3, v_4) \in \mathbb{Z}^4 \mid v_1^2 + v_2^2 + v_3^2 + v_4^2 = n\}$$

y de ahí la función con valores en los complejos

$$F(\tau) = \sum_{n \geq 0} r(n) q^n, \qquad q = e^{2\pi i}.$$

Se quieren calcular los coeficientes de la función y para ello es importante conocer ciertas propiedades de la misma. Esto motiva el estudio de formas modulares ya que dicha función es un tipo de forma modular.

La teoría de formas modulares involucra elementos de análisis complejo y de grupos de matrices, entonces son necesarias las siguientes definiciones para construir la noción de forma modular.

Definición 5.1. Una función $f : \mathbb{C} \to \mathbb{C}$ se dice **holomorfa** si es diferenciable en todo punto $z \in \mathbb{C}$. Además si $f : R \cup \{\infty\}$, se dice **meromorfa** si es holomorfa en todos sus puntos excepto en un conjunto discreto de puntos S tal que para todo $\alpha \in S$ existe $n \in \mathbb{Z}^+$ que cumple que $(z - \alpha)^n f(z)$ es holomorfa en α.

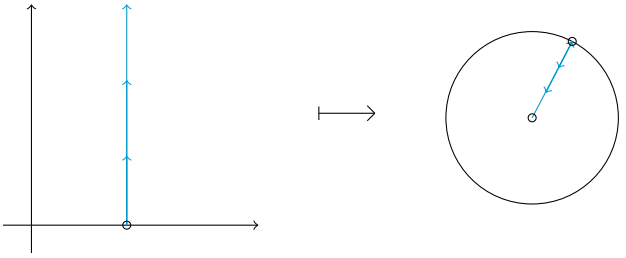
Ejemplo 5.2. $1/(z - i)$ es meromorfa en $\mathbb{C}$ pero no holomorfa ya que tiene un polo en i.

Como se definió en el primer capítulo, el conjunto $\mathcal{H}$ denota el plano superior complejo. Es claro que este conjunto no es compacto, así que interesa trabajar con el conjunto $\mathcal{H} \cup \{\infty\}$, en donde el punto ∞ puede imaginarse arriba del eje imaginario positivo (por lo tanto el punto se piensa muchas veces como $i\infty$). Como también se mencionó en el mismo capítulo, los elementos se pueden ver en $\mathbb{CP}^1$.

Con el fin de estudiar mejor las propiedades de $\mathcal{H} \cup \{\infty\}$, se define una aplicación de $\mathcal{H}$ al círculo unitario de la siguiente forma:

$$\tau \mapsto q := e^{2\pi i \tau}, \qquad \tau \in \mathcal{H}.$$

Para ver a qué punto debe ser enviado ∞ considere una línea $a + ti$ en donde t varía sobre los reales positivos. Cada punto en la línea es enviado a $e^{2\pi i(a+it)} = e^{2\pi i a} e^{-2\pi t}$. Entonces el ángulo para todos los elementos de la recta es el mismo y la norma se hace más pequeña a medida que t crece. Esto se puede apreciar en la siguiente figura:



Lo anterior ocurre para toda recta que se tome en $\mathcal{H}$ y eso implica que el punto $i\infty$ debe ser enviado a $(0,0)$.

Con esto en mente, dada una función f en $\mathcal{H}$ con periodo 1, diremos que es **meromorfa en ∞** si se puede escribir como una serie de potencias en la variable q con a lo sumo finitos terminos a_n distintos de 0 para los n negativos. Es decir,

$$f(\tau) = \sum_{n\in\mathbb{Z}} a_n q^n$$

con $a_n = 0$ para $n \ll 0$. Además, f es **holomorfa en ∞** si $a_n = 0$ para todo $n < 0$.

Recuerde que el **grupo modular** es $SL_2(\mathbb{Z})$, las matrices cuadradas de tamaño 2 con determinante uno. Éste es uno de los elementos más importantes de la teoría de formas modulares. Algunos subrupos especiales también jugarán un papel, serán llamados sub-grupos de congruencias. Entonces tiene sentido tomar $f : \mathcal{H} \to \mathbb{C}$ y evaluar f en $\gamma(\tau)$ para todo $\gamma \in SL_2(\mathbb{Z})$ y $\tau \in \mathcal{H}$. Es así como es posible realizar la siguiente definición.

Definición 5.3. Sea k un entero no negativo, una función meromorfa $f : \mathcal{H} \to \mathbb{C}$ es **modular de peso k** si:

(i) f es holomorfa en $\mathcal{H}$,

(ii) para todo $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \quad f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$,

(iii) f es holomorfa en ∞.

Ahora el objetivo será estudiar ciertas formas modulares. Para ello es necesario notar que las formas modulares cumplen algunas propiedades enunciadas a continuación:

Observación 5.4. La única forma modular de peso k para k impar es la función 0.

Demostración. Si f es modular de peso impar, se puede tomar $\gamma = -I \in SL_2(\mathbb{Z})$ y para todo $\tau \in \mathcal{H}$,

$$f(\tau) = f(-I\tau) = (-1)^k f(\tau) = -f(\tau).$$

Por lo tanto $f(\tau) = 0$ y para que ocurra para todo τ, f debe ser la función constante cero. □

Observación 5.5. Si f es una forma modular de cualquier peso, entonces tiene periodo 1.

Demostración. Para todo $\tau \in \mathcal{H}$, $f(\tau + 1) = f\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tau\right) = (1)^1 f(\tau) = f(\tau)$. □

Observación 5.6. Si $\mathcal{M}_k(SL_2(\mathbb{Z}))$ es el conjunto de formas modulares de peso k, entonces $\mathcal{M}_k(SL_2(\mathbb{Z}))$ es un espacio vectorial sobre $\mathbb{C}$.

5.1. Formas modulares para sub-grupos de congruencia

Existen funciones holomorfa en $\mathcal{H}$ y en ∞ que no cumplen que $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ para todo $\gamma \in SL_2(\mathbb{Z})$, pero sí para un subgrupo especial. También se busca estudiar dichas formas y por lo tanto se requiere conocer cuáles son los subgrupos y cuál es el análogo de una forma modular restringida a ellos.

Definición 5.7. Si $N \in \mathbb{N}$, el **subgrupo principal de congruencia de nivel N** es:

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

en donde la congruencia de matrices se da entrada a entrada.

A partir de estos grupos se tienen los subgrupos de congruencia Γ, que son aquellos tales que $\Gamma(N) \subseteq \Gamma$ para algún $N \in \mathbb{N}$. Ahí decimos que Γ es un **subgrupo de congruencia de nivel N**. Ejemplos importantes de subrupos de congruencia de nivel N son los definidos por:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

donde $*$ representa que la entrada puede ser cualquiera.

Estos subgrupos vienen de una definición mucho más natural que la anterior. Si se toma el homomorfismo

$$\mathrm{red}_N : SL_2(\mathbb{Z}) \to SL_2\left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)$$

dado por reducir cada coeficiente de la matriz módulo N, $\Gamma(N)$ es el núcleo de dicho homomorfismo. Además $\Gamma_0(N)$ corresponde al subgrupo de $SL_2(\mathbb{Z}/N\mathbb{Z})$ de matrices triangulares superiores. Por otra parte $\Gamma_1(N)$ es el subgrupo de matrices unipotentes de $SL_2(\mathbb{Z}/N\mathbb{Z})$ y $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^*$, las unidades de $(\mathbb{Z}/N\mathbb{Z})$.

Ejemplo 5.8. $\Gamma_0(4) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \right\rangle$.

Para demostrar la igualdad se puede usar la misma idea con la que se probó que $SL_2(\mathbb{Z})$ es finitamente generado. Se encuentra una región fundamental para el subgrupo generado por los dos elementos y posteriormente se muestra que esa también es la región fundamental de $\Gamma_0(4)$. También se puede hacer una demostración más algorítmica y para ello se puede ver [DS05, Ej. 1.2.4, Pg. 21].

Para hacer más fácil la notación se define

$$j(\gamma, \tau) = c\tau + d. \tag{5.1}$$

De ahí, una forma modular de peso k cumple que $f(\gamma\tau) = j(\gamma, \tau)^k f(\tau)$. Éste será el **factor de automorfismo**. Nunca será 0 porque para ello necesariamente $\mathrm{Im}\ \tau = 0$ pero $\tau \in \mathcal{H}$. Igualmente no puede ser infinito porque τ debería serlo.

Definición 5.9. Dados $\gamma \in SL_2(\mathbb{Z})$ y k entero, el **operador de peso k**, $[\gamma]_k$, está definido sobre funciones $f : \mathcal{H} \to \mathbb{C}$ como:

$$(f[\gamma]_k)(\tau) = j(\gamma, \tau)^{-k} f(\gamma(\tau)), \qquad \tau \in \mathcal{H}.$$

Como el factor de automorfismo no es 0 o infinito, si f es meromorfa, $f[\gamma]_k$ también lo será.

Definición 5.10. Dado Γ un subgrupo de congruencia, una **forma modular de peso k con respecto a** Γ es una función $f : \mathcal{H} \to \mathbb{C}$ tal que:

(i) f es holomorfa,

(ii) $f[\gamma]_k = f$ para todo $\gamma \in \Gamma$ (f es invariante de peso k bajo Γ),

(iii) $f[\alpha]_k$ es holomorfa en ∞ para todo $\alpha \in SL_2(\mathbb{Z})$.

El conjunto de formas modulares de peso k sobre Γ se denotará como $\mathcal{M}_k(\Gamma)$. Es claro que, al igual que en el caso de $\mathcal{M}_k(SL_2(\mathbb{Z}))$, cada conjunto forma un espacio vectorial sobre $\mathbb{C}$. Una observación importante es que la condición *(iii)* se puede reemplazar por la condición:
Si la serie de fourier de f es

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n,$$

entonces los coeficientes para $n > 0$ sarisfacen:

$$|a_n| \leq Cn^r, \qquad C \text{ y } r \text{ constantes.}$$

La demostración de dicha equivalencia requiere métodos mucho más avanzados que no se usarán dentro del documento, se puede encontrar en [DS05, Prop. 5.9.1]. Sin embargo, esta observación será útil posteriormente con el fin de probar que algunas funciones son modulares con respecto a un subgrupo de congruencia.

Lema 5.11. *Dados $\alpha, \beta \in SL_2(\mathbb{Z})$ y $\tau \in \mathcal{H}$, se tiene:*

(i) $j(\alpha\beta, \tau) = j(\alpha, \beta\tau)j(\beta, \tau)$,

(ii) $[\alpha\beta]_k = [\alpha]_k[\beta]_k$

Demostración. Los elementos en $SL_2(\mathbb{Z})$ actúan sobre los vectores columna con entradas complejas de tamaño 2 por medio de la multiplicación por izquierda. Esta acción se relaciona a la de $SL_2(\mathbb{Z})$ por:

$$\gamma \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \begin{pmatrix} \gamma\tau \\ 1 \end{pmatrix} j(\gamma, \tau).$$

Si la propiedad se aplica al producto de matrices $\alpha\beta$, ambas en $SL_2(\mathbb{Z})$ se tiene:

$$\alpha\beta \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \begin{pmatrix} (\alpha\beta)\tau \\ 1 \end{pmatrix} j(\alpha\beta, \tau)$$

Pero por otro lado, el producto de matrices es asociativo, entonces:

$$\alpha\beta \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \alpha \begin{pmatrix} \beta\tau \\ 1 \end{pmatrix} j(\beta, \tau) = \begin{pmatrix} (\alpha\beta)\tau \\ 1 \end{pmatrix} j(\alpha, \beta\tau)j(\beta, \tau)$$

En conlusión, $j(\alpha\beta, \tau) = j(\alpha, \beta\tau)j(\beta, \tau)$, de donde se sigue (i).

Ahora, si $f : \mathcal{H} \to \mathbb{C}$ y $\tau \in \mathcal{H}$

$$\begin{aligned} (f[\alpha\beta]_k)(\tau) &= j(\alpha\beta, \tau)^{-k} f(\alpha\beta\tau) \\ ((f[\alpha]_k)[\beta]_k)(\tau) &= j(\beta, \tau)^{-k}(f[\alpha]_k)(\beta\tau) \\ &= j(\beta, \tau)^{-k} j(\alpha, \beta\tau)^{-k} f(\alpha\beta\tau) \\ &= j(\alpha\beta, \tau)^{-k} f(\alpha\beta\tau) \qquad \text{por } (i). \end{aligned}$$

Como ocurre para todo f, τ, se tiene la igualdad de los operadores: $[\alpha\beta]_k = [\alpha]_k[\beta]_k$ y (ii) se tiene. □

Corolario 5.12. *Si Γ es un subrgrupo de congruencia finitamente generado, para que se cumpla (ii) en la Definición 5.10, basta con probar que es cierto para sus generadores.*

Demostración. Sea $G = \{\gamma_1, \ldots, \gamma_n\}$ el conjunto de los generadores de Γ. Tome $f : \mathcal{H} \to \mathbb{C}$ tal que (ii) se cumple para todos los elementos de G y sean α, β en ese conjunto (no necesariamente $\alpha \neq \beta$). Entonces,

$$\begin{aligned} (f[\alpha\beta]_k)(\tau) &= j(\beta, \tau)^{-k}(f[\alpha]_k)(\beta\tau) && \text{por Lema 5.11, } (ii) \\ &= j(\beta, \tau)^{-k} f(\beta\tau) && f[\alpha]_k = f \\ &= (f[\beta]_k)(\tau) \\ &= f(\tau) && f[\beta]_k = f \end{aligned}$$

Análogamente se prueba para cualquier producto de elementos en G y como todo elemento de Γ se escribe así, (ii) vale para todo $\gamma \in \Gamma$ □

Esta es una de las observaciones más relevantes para demostrar que una función es una forma modular sobre algún Γ particular. En el caso del Ejemplo 5.8, se enunció que $\Gamma_0(4)$ es generado por dos elementos, entonces para ver que una función es forma modular de peso k con respecto a $\Gamma_0(4)$, basta ver que la segunda condición se cumple para los dos generadores del subgrupo, entonces la demostración se simplifica.

En algunas ocasiones se desea definir una forma modular como serie de potencias en la variable q. Para ver que la función definida es holomorfa, será útil considerar el lema que se enuncia a continuación.

Lema 5.13. *Si $\{a_n\}_{n=0}^{\infty}$ es una sucesión de números complejos tal que $a_n = \mathcal{O}(n^\nu)$ para algún $\nu > 0$, entonces*

$$f(\tau) := \sum_{n=0}^{\infty} a_n q^n$$

converge absolutamente y uniformemente en subconjuntos compactos de $\mathcal{H}$. Además, $f(\tau)$ es holomorfa en $\mathcal{H}$.

Demostración. Para todo $s \in \mathbb{C}$ con Re $s > 0$ se define la función Γ como

$$\Gamma(s) = \int_0^{\infty} e^{-t} t^{s-1} dt.$$

Esta es una función más usada en la teoría de la probabilidad dado que a partir de ella es posible definir una función de densidad de una variable aleatoria. Euler demostró que para todo $s \in \mathbb{R}$ positivo

$$\Gamma(s) = \lim_{n\to\infty} \frac{n! n^s}{s(s+1)\cdots(s+n)}.$$

Entonces si $\nu > 0$,

$$\begin{aligned} \Gamma(\nu+1) &= \lim_{n\to\infty} n^\nu (-1)^n \frac{n!}{(-\nu-1)(-\nu-2)\cdots(-\nu-1-n+1)} \\ &= \lim_{n\to\infty} \frac{n^\nu}{(-1)^n \begin{pmatrix} -\nu-1 \\ n \end{pmatrix}}. \end{aligned}$$

Por hipótesis $a_n = \mathcal{O}(n^\nu)$, es decir, existen M constante y $N \in \mathbb{N}$ tales que $|a_n| \leq M n^\nu$ para todo $n \geq N$. Despejando n^ν de la igualdad anterior y teniendo en cuenta que $\Gamma(\nu+1)$ es constante, se llega a que existe L tal que

$$|a_n| \leq L(-1)^n \begin{pmatrix} -\nu-1 \\ n \end{pmatrix}$$

para todo $n \geq N$. Si ahora se toma $\tau = x + iy$,

$$\sum_{n=0}^{\infty} |a_n|\, |e^{2\pi i n \tau}| \leq L \left(\sum_{n=0}^{\infty} (-1)^n \begin{pmatrix} -\nu-1 \\ n \end{pmatrix} e^{-2\pi n y} \right) = L(1 - e^{-2\pi y})^{-\nu-1}.$$

Entonces $f(\tau)$ converge absolutamente y uniformemente en subconjuntos compactos de $\mathcal{H}$. Entonces $f(\tau)$ es holomorfa.

□

5.2. Series de Eisenstein

El primer ejemplo que se dará de una forma modular son las series de Eisenstein. Es uno de los ejemplos más importantes en la teoría y se construye como un análogo dos dimensional de la función ζ de Riemann. Interesa verlo aquí ya que será una de las bases de la prueba del Teorema de Lagrange.

Definición 5.14. Dado k un entero mayor o igual a 2, la **serie de Eisenstein de peso k** será:

$$G_k(\tau) = \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ (c,d)\neq(0,0)}} \frac{1}{(c\tau+d)^k}, \qquad \tau \in \mathcal{H}, \tag{5.2}$$

Para $k > 2$ la serie es absolutamente convergente. Además será una forma modular. En cambio, para $k = 2$ converge condicionalmente. Si se quiere una forma modular de peso 2, se debe definir una función distinta. Para probar ambas afirmaciones, es necesario encontrar antes la expansión en series de Fourier de los $G_k(\tau)$.

Lema 5.15. *Si $\tau \in \mathcal{H}$,*

$$\frac{1}{\tau} + \sum_{d=1}^{\infty}\left(\frac{1}{\tau-d}+\frac{1}{\tau+d}\right) = \pi\cot(\pi\tau) = \pi i - 2\pi i\sum_{m=0}^{\infty} q^m. \tag{5.3}$$

Demostración. Utilizando la expresión producto de $\operatorname{sen} z$, ver por ejemplo [AS92],

$$\operatorname{sen} z = z\prod_{d=1}^{\infty}\left(1-\frac{z^2}{\pi^2 d^2}\right).$$

Si se sustituye z por $\pi\tau$, y se toma la derivada logarítmica (la derivada del logarítmo de la función) con respecto a τ, se obtiene:

$$\frac{\pi\cos\pi\tau}{\operatorname{sen}\pi\tau} = \frac{1}{\tau} + \sum_{d=1}^{\infty}\left(\ln\left(1-\frac{\tau^2}{d^2}\right)\right)'. \tag{5.4}$$

Pero

$$\left(\ln\left(1-\frac{\tau^2}{d^2}\right)\right)' = -\frac{d^2}{d^2-\tau^2}\cdot\frac{2\tau}{d^2} = -\frac{2\tau}{d^2-\tau^2} = -\frac{1}{d-\tau}+\frac{1}{d+\tau} = \frac{1}{\tau-d}+\frac{1}{\tau+d}$$

y así 5.4 se conviente en

$$\frac{1}{\tau} + \sum_{d=1}^{\infty}\left(\frac{1}{\tau-d}+\frac{1}{\tau+d}\right) = \pi\cot(\pi\tau).$$

Por otra parte,

$$\pi\cot\pi\tau := \pi i\frac{e^{\pi i\tau}+e^{-\pi i\tau}}{e^{\pi i\tau}-e^{-\pi i\tau}} = \pi i\frac{e^{2\pi i\tau}+1}{e^{2\pi i\tau}-1} = \pi i + \frac{2\pi i}{e^{2\pi i\tau}-1}.$$

Si se toma la serie del segundo término,

$$\pi\cot\pi\tau = \pi i + 2\pi i\sum_{m=0}^{\infty} q^m.$$

□

Proposición 5.16. *Para $k \geq 2$ y par*

$$G_k(\tau) = 2\zeta(k) + 2\frac{(-2\pi i)^k}{(k-1)!}\sum_{c=1}^{\infty}\left(\sum_{m|n} m^{k-1}\right)q^n. \tag{5.5}$$

Demostración. Para empezar, $G_k(\tau)$ se puede reescribir como:

$$\sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ (c,d)\neq(0,0)}} \frac{1}{(c\tau+d)^k} = \sum_{d\neq 0}\frac{1}{d^k} + 2\sum_{c=1}^{\infty}\left(\sum_{d\in\mathbb{Z}}\frac{1}{(c\tau+d)^k}\right).$$

Pero $\sum_{d\neq 0}\frac{1}{d^k}=2\zeta(k)$, entonces sólo hace falta encontrar la expresión para $\sum_{d\in\mathbb{Z}}\frac{1}{(c\tau+d)^k}$.

El primer término de la Igualdad 5.3 se puede representar así:

$$\frac{1}{\tau}+\sum_{d=1}^{\infty}\left(\frac{1}{\tau-d}+\frac{1}{\tau+d}\right)=\frac{1}{\tau}+\sum_{d\in\mathbb{Z}_{>0}}\frac{1}{\tau+d}+\sum_{d\in\mathbb{Z}_{<0}}\frac{1}{\tau+d}=\sum_{d\in\mathbb{Z}}\frac{1}{\tau+d}.$$

Ahora se deriva $k-1$ veces la igualdad 5.3 con respecto a τ

$$\sum_{d\in\mathbb{Z}}\frac{1}{(\tau+d)^k}=\frac{(-2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty}m^{k-1}q^m.$$

Si se reemplaza τ por $c\tau$ se tiene

$$\sum_{d\in\mathbb{Z}}\frac{1}{(c\tau+d)^k}=\frac{(-2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty}m^{k-1}q^{cm}$$

y si se factoriza q^n,

$$\sum_{d\in\mathbb{Z}}\frac{1}{(c\tau+d)^k}=\frac{(-2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty}\left(\sum_{m|n}m^{k-1}\right)q^n.$$

Por último, la expresión deseada es:

$$\sum_{\substack{(c,d)\in\mathbb{Z}^2\\(c,d)\neq(0,0)}}\frac{1}{(c\tau+d)^k}=2\zeta(k)+2\frac{(-2\pi i)^k}{(k-1)!}\sum_{c=1}^{\infty}\left(\sum_{m|n}m^{k-1}\right)q^n.$$

□

Hecho 5.17. *$G_k(\tau)$ es absolutamente convergente para todo $k>2$.*

Demostración. Se puede encontrar en [Ser73, Lema 1, Pg. 82]. No se probará en este texto porque no será usado posteriormente. □

Proposición 5.18. *$G_k(\tau)$ es una forma modular de peso k para todo $k>2$.*

Demostración. Como $k>2$, se tiene por el lema anterior que G_k es holomorfa. Además ya que en la expresión en serie de potencias sobre la variable q aparecen sólo índices positivos, G_k es holomorfa en infinito. Por otra parte es claro que $G_k(\tau+1)=G_k(\tau)$ y

$$G_k\left(-\frac{1}{\tau}\right)=\sum_{\substack{(c,d)\in\mathbb{Z}^2\\(c,d)\neq(0,0)}}\frac{1}{\left(-c\frac{1}{\tau}+d\right)^k}=\sum_{\substack{(c,d)\in\mathbb{Z}^2\\(c,d)\neq(0,0)}}\frac{\tau^k}{(-c+d\tau)^k}=\tau^k\sum_{\substack{(c,d)\in\mathbb{Z}^2\\(c,d)\neq(0,0)}}\frac{1}{(c\tau+d)^k}=\tau^kG_k(\tau).$$

Pero estas dos transformaciones son las generadoras de $SL_2(\mathbb{Z})$ y por el Corolario 5.12, G_k es una forma modular de peso k. □

Para encontrar la expresión en series de potencias de $G_k(\tau)$ no se usó la convergencia absoluta de $G_k(\tau)$, entonces también es válido para $k=2$. Sin embargo, $G_2(\tau)$ no es una forma modular ya que no converge absolutamente. Por esto es que se debe tomar una expresión relacionada para obtener una forma modular con respecto a un subgrupo de congruencia. Esta expresión será para todo entero positivo N,

$$G_{2,N}(\tau)=G_2(\tau)-NG_2(N\tau) \tag{5.6}$$

Se sabe que $G_{2,N}\in\mathcal{M}_2(\Gamma_0(N))$, pero el interés principal para la demostración del Teorema de Lagrange será ver que $G_{2,2}(\tau)$ y $G_{2,4}(\tau)$ pertenecen a $\mathcal{M}_2(\Gamma_0(4))$, entonces la atención se centrará en dichas funciones.

Proposición 5.19. *Las representaciones en series de potencias en la variable q de $G_{2,2}$ y $G_{2,4}$ son:*

$$G_{2,2}(\tau) = -\frac{\pi^2}{3}\left(1 + 24\sum_{n=1}^{\infty}\sum_{\substack{0<d|n\\ 2\nmid n}} d\, q^n\right) \tag{5.7}$$

$$G_{2,4}(\tau) = -\pi^2\left(1 + 8\sum_{n=1}^{\infty}\sum_{\substack{0<d|n\\ 4\nmid n}} d\, q^n\right) \tag{5.8}$$

Demostración. En el caso de $G_{2,2}$:

$$\begin{aligned}
G_{2,2}(\tau) &= -2\zeta(2) + 8\left(2\sum_{n=1}^{\infty}\sum_{m|n} m\, q^{2n} - \sum_{n=1}^{\infty}\sum_{m|n} m\, q^n\right)\\
&= -\frac{\pi^2}{3}\left(1 - 24\left(\sum_{n=1}^{\infty}\sum_{m|n}(2m)\, q^{2n} - \sum_{n=1}^{\infty}\sum_{m|n} m\, q^n\right)\right) \qquad \zeta(2) = \frac{\pi^2}{6}\\
&= -\frac{\pi^2}{3}\left(1 - 24\left(\sum_{n=1}^{\infty}\sum_{\substack{m|n\\ 2|m}} m\, q^n - \sum_{n=1}^{\infty}\sum_{m|n} m\, q^n\right)\right)\\
&= -\frac{\pi^2}{3}\left(1 + 24\sum_{n=1}^{\infty}\sum_{\substack{m|n\\ 2\nmid m}} m\, q^n\right)
\end{aligned}$$

Usando casi el mismo argumento para $G_{2,4}$,

$$\begin{aligned}
G_{2,4}(\tau) &= -6\zeta(2) + 8\left(4\sum_{n=1}^{\infty}\sum_{m|n} m\, q^{4n} - \sum_{n=1}^{\infty}\sum_{m|n} m\, q^n\right)\\
&= -\pi^2\left(1 - 8\left(\sum_{n=1}^{\infty}\sum_{m|n}(2m)\, q^{4n} - \sum_{n=1}^{\infty}\sum_{m|n} m\, q^n\right)\right) \qquad \zeta(2) = \frac{\pi^2}{6}\\
&= -\pi^2\left(1 - 8\left(\sum_{n=1}^{\infty}\sum_{\substack{m|n\\ 4|m}} m\, q^n - \sum_{n=1}^{\infty}\sum_{m|n} m\, q^n\right)\right)\\
&= -\pi^2\left(1 + 8\sum_{n=1}^{\infty}\sum_{\substack{m|n\\ 4\nmid m}} m\, q^n\right)
\end{aligned}$$

□

Por la proposición es claro que $G_{2,2}$ y $G_{2,4}$ son holomorfa en ∞. Además, el número de divisores positivos de n está acotado por n y por tanto los términos de ambas series están acotados por una constante por

n. Entonces $a_n = \mathcal{O}(n)$ y por el Lema 5.13 las funciones son holomorfa.

Ahora se verá que $G_{2,2}$ es modular de peso dos sobre $\Gamma_0(4)$. Como se vio en el Lema 5.12, basta con probar que es invariante bajo los generadores de $\Gamma_0(4)$. Es claro que $G_2(\tau+2) = G_2(\tau+1) = G_2(\tau)$, de donde se sigue que $G_{2,2}(\tau+1) = G_{2,2}(\tau)$. Para ver qué ocurre con el otro generador es importante que ya se tenga que $G_{2,2}$ converge absolutamente para reordenar la serie.

$$\begin{aligned} G_{2,2}\left(\frac{1}{4\tau+1}\right) &= \sum_{c,d}{}' \frac{1}{\left(\frac{c}{4\tau+1}+d\right)^2} - \sum_{e,f}{}' \frac{2}{\left(\frac{2e}{4\tau+1}+f\right)^2} \\ &= \sum_{c,d}{}' \frac{(4\tau+1)^2}{(c+4d\tau+d)^2} - \sum_{e,f}{}' \frac{2(4\tau+1)^2}{(2e+4f\tau+f)^2} \\ &= (4\tau+1)^2 \left(\sum_{c,d}{}' \frac{1}{(c+4d\tau+d)^2} - \sum_{e,f}{}' \frac{2}{(2e+4f\tau+f)^2} \right) \\ &= (4\tau+1)^2\, G_{2,2}(\tau). \end{aligned}$$

El mismo procedimiento se hace para $G_{2,4}$ y por lo tanto es posible concluir que ambas funciones pertenecen al espacio vectorial $\mathcal{M}_2(\Gamma_0(4))$

5.3. Funciones Teta

Como se explicó antes, el estudio de formas modulares dentro de este documento se realiza con el objetivo de probar el Teorema de los Cuatro Cuadrados de Lagrange. El teorema es equivalente a ver:

$$\#\{\boldsymbol{v} \in \mathbb{Z}^4 \ : \ n = v_1^2 + v_2^2 + v_3^3 + v_4^2\} \neq 0 \qquad \forall n \in \mathbb{Z}_{\geq 0} \tag{5.9}$$

Una expresión un poco más general es:

$$r(n,k) = \#\{\boldsymbol{v} \in \mathbb{Z}^k \ : \ n = v_1^2 + \ldots + v_k^2\}, \qquad k \geq 0. \tag{5.10}$$

Para estudiar estos valores se definirá la función generadora **(función teta)**:

$$\theta(\tau, k) := \sum_{n=0}^{\infty} r(n,k) q^n, \qquad \tau \in \mathcal{H}. \tag{5.11}$$

Proposición 5.20. *$\theta(\tau, k)$ es absolutamente convergente para todo $\tau \in \mathcal{H}$ y $k \in \mathbb{Z}$*

Demostración. En primer lugar, $r(n,k) \leq 2^k n^k$. Además recuerde que $q = e^{2\pi i \tau}$, entonces si $\tau = x + iy$,

$$|r(n,k)q^n| = \left|r(n,k)e^{2\pi i x}e^{-2\pi y}\right| \leq 2^k n^k |e^{-2\pi n y}|.$$

Usando criterio de la razón para la serie definida por $2^k n^k |e^{-2\pi n y}|$,

$$\lim_{n\to\infty} \frac{2^k(n+1)^k|e^{-2\pi(n+1)y}|}{2^k n^k |e^{-2\pi n y}|} = \lim_{n\to\infty} \left(\frac{n+1}{n}\right)^k e^{-2\pi y} = e^{-2\pi y}.$$

Pero $y > 0$ ya que $\tau \in \mathcal{H}$. Entonces $e^{-2\pi y} < 1$ y la serie converge. Por criterio de comparación, $\theta(\tau, k)$ converge absolutamente. □

Note que el resultado implica que $\theta(\tau, k)$ es holomorfa ya que su serie de Laurent converge absolutamente y uniformemente en subconjuntos compactos de $\mathcal{H}$.

En general, la función teta no es una forma modular, pero sí será una forma modular de peso 2 con respecto a un subgrupo de $SL_2(\mathbb{Z})$. La siguiente teoría será desarrollada para probar dicha afirmación.

Proposición 5.21. *La función θ cumple:*

(i) $\theta(\tau+1,k)=\theta(\tau,k)$

(ii) $\theta(\tau,k_1)\theta(\tau,k_2)=\theta(\tau,k_1+k_2)$

Demostración. En primer lugar,

$$\theta(\tau+1,k)=\sum_{n=0}^{\infty}r(n,k)e^{2\pi i(\tau+1)}=\sum_{n=0}^{\infty}r(n,k)e^{2\pi i\tau}e^{2\pi i}=\sum_{n=0}^{\infty}r(n,k)e^{2\pi i\tau}=\theta(\tau,k)$$

Por otra parte, si $i+j=k$, por definición de $r(n,k)$,

$$r(n,k)=\sum_{l+m=n}r(l,i)r(m,j).$$

Entonces:

$$\theta(\tau,k_1)\theta(\tau,k_2)=\sum_{n=0}^{\infty}\sum_{l+m=n}r(l,k_1)r(m,k_2)q^n=\sum_{n=0}^{\infty}r(n,k_1+k_2)q^n=\theta(\tau,k_1+k_2)$$

□

Para simplificar la notación, se define $\theta(\tau)=\theta(\tau,1)$. Para estudiar dicha función es necesario conocer:

$$r(n,1)=\begin{cases}0 & \text{si } \sqrt{n}\notin\mathbb{Z}\\ 1 & \text{si } n=0\\ 2 & \text{en otro caso}\end{cases}\tag{5.12}$$

Así, se concluye:

$$\theta(\tau)=\sum_{n=0}^{\infty}r(n,1)e^{2\pi in\tau}=\sum_{d\in\mathbb{Z}}e^{2\pi id^2\tau}\tag{5.13}$$

Una propiedad importante será la igualdad:

$$\theta\left(-\frac{1}{4\tau}\right)=\sqrt{-2i\tau}\,\theta(\tau).$$

Para demostrarla se necesita antes un resultado técnico de análisis de Fourier que es la fórmula de sumatoria de Poisson.

Hecho 5.22. *Si $f\in L^2$ y es periódica, se define*

$$\overline{f}(x)=\sum_{d\in\mathbb{Z}}f(x+d).$$

Entonces:

$$\overline{f}(x)=\sum_{n\in\mathbb{Z}}\left(\int_0^1\overline{f}(t)e^{-2\pi int}dt\right)e^{2\pi inx}.$$

Demostración. Ver [Dei05, Lema 1.4.3, Pg. 14]. □

Teorema 5.23. ***Fórmula de sumatoria de Poisson*** *Sea $f:\mathbb{R}\to\mathbb{C}$ con $f\in L^2$ tal que $\sum_{d\in\mathbb{Z}}f(x+d)$ converge absolutamente y uniformemente en $[0,1]$. Entonces*

$$\sum_{d\in\mathbb{Z}}f(x+d)=\sum_{m\in\mathbb{Z}}\hat{f}(m)e^{2\pi imx}.\tag{5.14}$$

En donde $\hat{f}$ es la transformada de Fourier de f:

$$\hat{f}(m)=\int_{-\infty}^{\infty}f(t)e^{-2\pi imt}dt.\tag{5.15}$$

Demostración. En primer lugar,

$$\int_0^1 \left(\sum_{n\in\mathbb{Z}} |f(x+n)| \right) dx = \sum_{n\in\mathbb{Z}} \left(\int_0^1 |f(x+n)|dx \right) = \sum_{n\in\mathbb{Z}} \int_n^{n+1} |f(y)|dy = \int_{-\infty}^{\infty} |f(y)|dy < \infty$$

ya que f converge uniformemente en subconjuntos compactos, posteriormente se realiza el cambio de variable $y = x + n$ y $f \in L^1$. Ahora se define Por el razonamiento anterior, $\overline{f}(x)$ es integrable sobre 0,1. Además

$$\overline{f}(x+1) = \sum_{d\in\mathbb{Z}} f(x+d+1) = \sum_{d\in\mathbb{Z}} f(x+d) = \overline{f}(x),$$

entonces la función es periódica con periodo 1.

$$\begin{aligned} \int_0^1 \overline{f}(x)e^{-2\pi imx}dx &= \int_0^1 \left(\sum_{n\in\mathbb{Z}} f(x+n) \right) e^{-2\pi imx}dx \\ &= \sum_{n\in\mathbb{Z}} \int_0^1 f(x+n)e^{-2\pi imx}dx \\ &= \sum_{n\in\mathbb{Z}} \int_n^{n+1} f(y)e^{-2\pi im(y-n)}dy \\ &= \int_{-\infty}^{\infty} f(y)e^{-2\pi imy}dy \\ &= \hat{f}(m). \end{aligned} \tag{5.16}$$

Como $f \in L^2$, el Hecho 5.22 implica que $\overline{f}(x) = \sum_{m\in\mathbb{Z}} \left(\int_0^1 \overline{f}(t)e^{-2\pi imt}dt \right) e^{2\pi imx}$. Pero 5.16 implica que

$$\begin{aligned} \overline{f}(x) &= \sum_{m\in\mathbb{Z}} \hat{f}(m)e^{2\pi imx} \\ \sum_{d\in\mathbb{Z}} f(x+d) &= \sum_{m\in\mathbb{Z}} \hat{f}(m)e^{2\pi imx}. \end{aligned} \tag{5.17}$$

□

Se quiere usar la fórmula anterior para $f(x) = e^{-\frac{\pi ix^2}{2\tau}}$ con $\tau \in \mathcal{H}$. Para ello basta ver que $f(x)$ cumple con las hipótesis. Se tiene que $\forall\tau \in \mathcal{H}$ y $\forall x \in \mathbb{R}$, si $\tau = a + ib$,

$$|f(x+d)| = \left| e^{-\frac{a\pi i(x+d)^2}{2\|\tau\|^2} - \frac{b\pi(x+d)^2}{2\|\tau\|^2}} \right|.$$

Como $e^{-\frac{a\pi i(x+d)^2}{2\|\tau\|^2}}$ tiene norma 1,

$$|f(x+d)| = \left| e^{-\frac{b\pi(x+d)^2}{2\|\tau\|^2}} \right|.$$

Además $b > 0$ y por lo tanto $\dfrac{b\pi(x+d)^2}{2\|\tau\|^2} > 0$ casi siempre. Entonces $\sum_{d\in\mathbb{Z}} \left| e^{-\frac{b\pi(x+d)^2}{2\|\tau\|^2}} \right|$ converge y $\sum_{d\in\mathbb{Z}} e^{-\frac{\pi ix^2}{2\tau}}$ converge absolutamente.

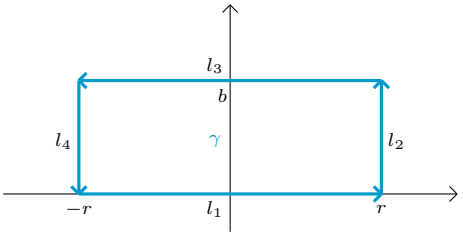
Por lo tanto, se aplica la sumatoria de Poisson a $f(x)$. Si se toma $x = 0$ en la ecuación 5.14 y se reemplaza $f(d)$, se obtiene:

$$\sum_{d\in\mathbb{Z}} e^{-\frac{\pi id^2}{2\tau}} = \sum_{m\in\mathbb{Z}} \hat{f}(m). \tag{5.18}$$

Para hallar una ecuación más precisa hace falta encontrar $\hat{f}(m)$.

$$\begin{aligned}
\hat{f}(m) &= \int_{-\infty}^{\infty} e^{-\frac{\pi i t^2}{2\tau}} e^{-2\pi i m t} dt && u = \tfrac{\sqrt{i}t}{\sqrt{2\tau}} = \tfrac{t}{\sqrt{-2i\tau}},\ du = \tfrac{1}{\sqrt{-2i\tau}}dt \\
&= \sqrt{-2i\tau} \int_{-\infty}^{\infty} e^{-\pi u^2} e^{-2\pi i m\sqrt{-2i\tau}u} du \\
&= \sqrt{-2i\tau} \int_{-\infty}^{\infty} e^{-\pi(u+im\sqrt{-2i\tau})^2 + 2\pi i m^2\tau} du \\
&= \sqrt{-2i\tau} e^{2\pi i m^2\tau} \int_{-\infty}^{\infty} e^{-\pi(u+im\sqrt{-2i\tau})^2} du && (*) \\
&= \sqrt{-2i\tau} e^{2\pi i m^2\tau} \int_{-\infty}^{\infty} e^{-\pi v^2} dv && (5.19) \\
&= \sqrt{-2i\tau} e^{2\pi i m^2\tau} 2\int_{0}^{\infty} e^{-\pi v^2} dv && s = \pi v^2,\ ds = 2\pi v dv \\
&= \sqrt{-2i\tau} e^{2\pi i m^2\tau} \frac{1}{\pi} \int_{0}^{\infty} e^{-s} s^{-1/2} ds \\
&= \sqrt{-2i\tau} e^{2\pi i m^2\tau} \frac{1}{\pi} \Gamma\left(\frac{1}{2}\right) && \Gamma\left(\tfrac{1}{2}\right) = \sqrt{\pi} \\
&= \sqrt{-2i\tau} e^{2\pi i m^2\tau}.
\end{aligned}$$

$(*)$ se sigue de:



$$\begin{aligned}
0 = \int_{\gamma} e^{-\pi z^2} d\gamma &= \int_{l_1} e^{-\pi z^2} dl_1 + \int_{l_2} e^{-\pi z^2} dl_2 + \int_{l_3} e^{-\pi z^2} dl_3 + \int_{l_4} e^{-\pi z^2} dl_4 \\
&= \int_{-r}^{r} e^{-\pi t^2} dt - \int_{-r}^{r} e^{-\pi(t+ib)^2} dt + \int_{l_2} e^{-\pi z^2} dl_2 - \int_{l_2} e^{-\pi z^2} dl_2
\end{aligned}$$

ya que la trayectoria l_4 es menos la trayectoria l_2 para una función par como lo es $e^{-\pi z^2}$. Si se toma $r \to \infty$, es posible hacer la sustitución:

$$\int_{-\infty}^{\infty} e^{-\pi t^2} dt = \int_{-\infty}^{\infty} e^{-\pi(t+u)^2} dt.$$

De 5.18 y 5.19 se concluye que:

$$\sum_{d\in\mathbb{Z}} e^{-\frac{\pi i d^2}{2\tau}} = \sqrt{-2i\tau} \sum_{m\in\mathbb{Z}} e^{2\pi i m^2\tau}.$$

Pero por 5.13 y la anterior igualdad,

$$\theta\left(-\frac{1}{4\tau}\right) = \sqrt{-2i\tau}\ \theta(\tau). \tag{5.20}$$

Todo lo anterior se hizo para ver:

$$\begin{aligned}
\theta\left(\frac{\tau}{4\tau+1}\right) &= \theta\left(-\frac{1}{4(-1/(4\tau)-1)}\right) \\
&= \sqrt{2i\left(\frac{1}{4\tau}+1\right)}\ \theta\left(-\frac{1}{4\tau}-1\right) \quad \text{por 5.20} \\
&= \sqrt{2i\left(\frac{1}{4\tau}+1\right)}\ \theta\left(-\frac{1}{4\tau}-1\right) \quad \text{por 5.21} \\
&= \sqrt{2i\left(\frac{1}{4\tau}+1\right)}\ \theta\left(-\frac{1}{4\tau}\right) \quad \text{por 5.21} \\
&= \sqrt{2i\left(\frac{1}{4\tau}+1\right)}\ \sqrt{-2i\tau}\ \theta(\tau) \quad \text{por 5.20} \\
&= \sqrt{4\tau+1}\ \theta(\tau).
\end{aligned}$$

Si se usa la propiedad de que $\theta(\tau,k_1)\theta(\tau,k_1)=\theta(\tau,k_1+k_2)$ (Proposición 5.21), $\theta(\tau,4)=\theta(\tau)^4$ y así:

$$\theta\left(\frac{\tau}{4\tau+1},4\right)=(4\tau+1)^2\ \theta(\tau,4). \tag{5.21}$$

En este caso se tiene que si θ es una forma modular sobre $\Gamma_0(4)$, entonces es de peso 2.

Teorema 5.24. *La función $\theta(\tau,4)$ pertenece a $\mathcal{M}_2(\Gamma_0(4))$.*

Demostración. Ya se vió que $\theta(\tau,k)$ es holomorfa para todo k entero positivo (Proposición 5.20). Recuerde que $\Gamma_0(4)$ está generado por las matrices $T=\begin{pmatrix}1&1\\0&1\end{pmatrix}$ y $\gamma=\begin{pmatrix}1&0\\4&1\end{pmatrix}$. Por la Proposición 5.21, $\theta(\tau,4)[T]_2=\theta(\tau,4)$ y por la ecuación 5.21 $\theta(\tau,4)[\gamma]_2=\theta(\tau,4)$. Entonces por el Corolario 5.12, $\theta(\tau,4)[\beta]_2=\theta(\tau,4)$ para todo $\beta\in\Gamma_0(4)$. Por último, θ está definida como su serie de Fourier y que para todo $n>0$

$$r(n,4)<2^4n^4$$

ya que si n es la suma de cuatro cuadrados, el valor absoluto de estos números es menor que n, entonces existen a lo sumo n^4 posibilidades para el valor absoluto. El 2^4 se obtiene porque para cada una de estas posibilidades el entero puede ser positivo o negativo. Es así como se tienen las tres condiciones y por tanto $\theta(\tau,4)$ pertenece a $\mathcal{M}_2(\Gamma_0(4))$. □

5.4. Formas modulares de peso 2 sobre $\Gamma_0(4)$

En las secciones anteriores se encontraron tres formas modulares en $\mathcal{M}_2(\Gamma_0(4))$, una de ellas es la función $\theta(\tau,4)$ y si se logra probar que ninguno de los coeficientes de su expansión en serie de Fourier es 0, se consigue una prueba del Teorema de los cuatro cuadrados de Lagrange.

Hecho 5.25. *$\mathcal{M}_2(\Gamma_0(4))$ tiene dimensión 2 como espacio vectorial sobre $\mathbb{C}$.*

Demostración. La prueba de este teorema se puede encontrar en [DS05, Pg. 108]. La demostración usa métodos de geometría algebraica, específicamente los teoremas de Riemann-Roch y Riemann-Hurwitz. □

Por las Ecuaciones 5.7 y 5.8,

$$G_{2,2}(\tau) = -\frac{\pi^2}{3}\left(1 + 24\sum_{n=1}^{\infty}\sum_{\substack{0<d|n\\ 2\nmid n}} d\, q^n\right) \quad \text{y} \quad G_{2,4}(\tau) = -\pi^2\left(1 + 8\sum_{n=1}^{\infty}\sum_{\substack{0<d|n\\ 4\nmid n}} d\, q^n\right)$$

y ambas formas son de peso 2 sobre $\Gamma_0(4)$. Un lema importante es el que se tiene a continuación.

Lema 5.26. *Las formas $G_{2,2}$ y $G_{2,4}$ son linealmente independientes sobre $\mathbb{C}$*

Demostración. Ningún coeficiente de q^n en ambas series es 1 ya que todos son sumatorias de términos positivos y al menos uno siempre divide a cualquier entero. Suponga que $G_{2,2} = zG_{2,4}$, para que esto ocurra se debe tener igualdad término a término de la serie de potencias. Es decir,

$$-\frac{\pi^2}{3} = -z\pi^2 \quad \text{y} \quad -24\frac{\pi^2}{3}\sum_{\substack{0<d|n\\ 2\nmid n}} d = -8z\pi^2\sum_{\substack{0<d|n\\ 4\nmid n}} d, \quad \forall n > 0.$$

De la primera igualdad se obtiene que $z = \frac{1}{3}$, si se calcula la segunda igualdad para $n = 1$ se debe cumplir

$$-\frac{24}{3}\pi^2 = -\frac{8}{3}\pi^2,$$

una igualdad falsa. Por lo tanto $G_{2,2}$ y $G_{2,4}$ son linealmente independientes sobre $\mathbb{C}$. □

Ahora se tienen dos elementos linealmente independientes en $\mathcal{M}_2(\Gamma_0(4))$, un espacio vectorial de dimensión dos. Por ello deben formar una base del espacio y $\theta(\tau, 4)$ debe escribirse como combinación lineal de ambas funciones. Esto es, $\theta(\tau, 4) = z_1G_{2,2}(\tau) + z_2G_{2,4}(\tau)$. Sin embargo, $r(0, 4) = 1$ porque la única forma de escribir 0 como la suma de cuatro cuadrados es $0^2 + 0^2 + 0^2 + 0^2$ y $r(1, 4) = 8$ debido a que 1 se puede escribir como:

$$(\pm1)^2 + 0^2 + 0^2 + 0^2, \quad 0^2 + (\pm1)^2 + 0^2 + 0^2, \quad 0^2 + 0^2 + (\pm1)^1 + 0^2 \quad \text{o} \quad 0^2 + 0^2 + 0^2 + (\pm1)^2.$$

Es así como necesariamente

$$\theta(\tau, 4) = -\frac{1}{\pi^2}G_{2,4}(\tau) = 1 + 8\sum_{n=1}^{\infty}\sum_{\substack{0<d|n\\ 4\nmid n}} d\, q^n.$$

Esto implica que $r(n, 4) > 0$ para todo entero positivo n ya que 1 siempre divide a n. Además implica el teorema:

Teorema 5.27. ***Teorema de Jacobi de los Cuatro Cuadrados*** *Dado un entero positivo n, existen exactamente*

$$8\sum_{\substack{0<d|n\\ 4\nmid n}} d$$

formas de escribir n como la suma de cuatro cuadrados

Corolario 5.28. ***Teorema de los cuatro cuadrados de Lagrange*** *Todo entero positivo se puede escribir como la suma de cuatro cuadrados.*

6. Anexos

Matriz de Gram	**Covolumen**	**Ausente**
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	1	7
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$	2	14
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$	3	6
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$	4	7
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$	6	10
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 4 \end{pmatrix}$	7	7
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}$	8	14
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 5 \end{pmatrix}$	9	7
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}$	10	10

Tabla 1: retículos escalados de dimensión 3

Matriz de Gram	**Único ausente**
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 4 \end{pmatrix}$	10
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 4 & 1 \\ 0 & 0 & 1 & 5 \end{pmatrix}$	10
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 5 & 1 \\ 0 & 0 & 1 & 5 \end{pmatrix}$	15
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix}$	15
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 \\ 0 & 0 & 5 & 2 \\ 0 & 1 & 2 & 8 \end{pmatrix}$	15
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 \\ 0 & 0 & 5 & 1 \\ 0 & 1 & 1 & 9 \end{pmatrix}$	15

Tabla 1: retículos escalados de dimensión 3

Referencias

[Ahl78] Lars V. Ahlfors. *Complex analysis*. McGraw-Hill Book Co., New York, third edition, 1978. An introduction to the theory of analytic functions of one complex variable, International Series in Pure and Applied Mathematics.

[AMO01] Ravi P. Agarwal, Maria Meehan, and Donal O'Regan. *Fixed point theory and applications*, volume 141 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2001.

[AS92] Milton Abramowitz and Irene A. Stegun, editors. *Handbook of mathematical functions with formulas, graphs, and mathematical tables*. Dover Publications, Inc., New York, 1992. Reprint of the 1972 edition.

[BFLR00] Eva Bayer-Fluckiger, David Lewis, and Andrew Ranicki, editors. *Quadratic forms and their applications*, volume 272 of *Contemporary Mathematics*. American Mathematical Society, Providence, RI, 2000.

[Bou05] Florian Bouyer. Composition and bahargava's cubes. *Amer. Math. Monthly*, 105(10):907–922, 2005.

[BS66] A. I. Borevich and I. R. Shafarevich. *Number theory*. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York-London, 1966.

[Bue89] Duncan A. Buell. *Binary quadratic forms*. Springer-Verlag, New York, 1989. Classical theory and modern computations.

[Cas78] J. W. S. Cassels. *Rational quadratic forms*, volume 13 of *London Mathematical Society Monographs*. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978.

[Cox13] David A. Cox. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[CS99] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, third edition, 1999. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

[Dei05] Anton Deitmar. *A first course in harmonic analysis*. Universitext. Springer-Verlag, New York, second edition, 2005.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[Kob93] Neal Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1993.

[Mey00] C. D. Meyer. *Matrix analysis and applied linear algebra*. Siam, Philadelphia, 2000.

[Ser73] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.