Teoría de cuerpos de clase y aplicaciones.

Alberto Daza Garcia

Tutorizado por Antonio Rojas León

Abstract

One problems which has lead the advance of number theory since the 20th century until now, is Hilbert's twelfth problem, a problem which aims to find explicit generators for the maximal abelian extension of each number field. This problem has been solved in the case of quadratic imaginary number fields and has been extended to fields with complex multiplication.

The objective of this thesis is to give the proof of the quadratic imaginary case. In order to do that, the tools needed will be studied. Those tools are: class field theory, modular forms and elliptic curves.

Resumen

Uno de los problemas abierto que ha guiado el avance de la teoría de números desde el siglo XX hasta ahora, es el problema duodécimo de Hilbert, un problema que pretende encontrar generadores expícitos para la extensión abeliana maximal de cada cuerpo de números. Este problema se ha resuelto en el caso de los cuerpos de números cuadráticos imaginarios y se ha extendido a los cuerpos con multiplicación compleja.

El objetivo de esta memoria será llegar a la prueba del caso cuadrático y para ello, se estudiarán las herramientas necesarias que son: la teoría de cuerpos de clase, las funciones modulares y las curvas elípticas.

Índice general

Capítulo 0

Introducción

Tal y como comenta Robert Langland en [RL] el problema duodécimo de Hilbert nos recuerda, la gran relación que hay entre la teoría de cuerpos de clase, la teoría de multiplicación compleja y la teoría de funciones automorfas.

Fue en el año 1853 cuando Kronecker enuncia el siguiente teorema:

Teorema 1 (Teorema de Kronecker-Weber.)**.** *Toda extensión abeliana finita de $\mathbb{Q}$ está contenida en una extensión ciclotómica.*

Cuando enunció el teorema dio una prueba pero esta estaba incompleta. En 1886 Weber completó la prueba faltandole aún algún detalle por rellenar que completaron Hilbert y Speiser.

Kronecker, sigue interesado en este resultado y en 1880 le escribe una carta a Dedekind en la que le comenta la relación que encuentra entre las extensiones abelianas de cuerpos cuadráticos imaginarios y la teoría de curvas elípticas. Será en 1900 cuando Hilbert publicó el problema de encontrar generadores de la extensión abeliana maximal de los cuerpos cuadráticos imaginarios en su lista de 23 problemas.

La teoría de cuerpos de clase nace como un intento para caracterizar las extensiones abelianas en términos de datos analíticos del cuerpo. Se obtienen resultados muy interesantes como por ejemplo, una biyección entre ciertos subgrupos abiertos del grupo de idèles de un cuerpo de números K y sus extensiones abelianas finitas (que se llamarán cuerpos de clase). El enfoque que se toma es el de encontrar los generadores de algunos de estos cuerpos relacionandolos con el grupo.

El cuerpo de clases de Hilbert, es uno de los cuerpos de los que se encuentran los generadores. Tiene la particularidad de que es una extensión que cuya dimensión como espacio vectorial sobre el cuerpo de números es el número de clases del anillo de enteros. De hecho, el grupo de Galois es isomorfo al grupo de clases de ideales.

Si se toma como cuerpo base un cuerpo cuadrático imaginario, el interes de encontrar generadores se puede poner de manifiesto dado que de acuerdo con el siguiente teorema que aparece en [COX]:

Proposición 1. *Sea $n > 0$ un entero libre de cuadrados tal que $n \not\equiv 3 \ mod\ 4$, entonces existe un polinomio mónico irreducible $f(x) \in \mathbb{Z}[x]$ cuyo grado el el número de clases de $K = \mathbb{Q}(\sqrt{-n})$ tal que dado un primo p impar que no divide ni a n ni al discriminante de $f(x)$, se tiene que $p = a^2 + nb^2$ tiene solución si y sólo si $\left(\frac{-n}{p}\right) = 1$ y $f(x) \equiv 0 \ mod\ p$ tiene una solución entera.*

Se puede elegir f como el polinómio mínimo de un α tal que $L = K(\alpha)$ es el cuerpo de clase de Hilbert de K.

El problema se resolvió para el caso de cuerpos de números cuadráticos en 1927 por Hasse. También estuvo tras la solución Weber pero se vio envuelto en argumentos complicados. La solución se extendió al resto de los cuerpos cuadráticos gracias a Shimura en 1967.

En esta memoria sólo se explorará la solución parcial dada por Shimura para cuerpos cuadráticos imaginarios. Para ello, se darán herramientas que serán necesarias para la comprensión de la prueba.

En el capítulo 1, se desarrollará la teoría de cuerpos de clase. Se introducirán los idèles, se explicará la reciprocidad de Artin, se explicará qué son los cuerpos de clase y se dará la correspondencia entre las extensiones abelianas finitas de un cuerpo y los subgrupos abiertos del grupo de idèles. En este capítulo, la fuente principal ha sido [NC].

En el capítulo 2, se introducirán las funciones modulares. Se definirá el dominio fundamental de un subgrupo discreto de $SL_2(\mathbb{R})$ y se encontrará un dominio fundamental de $SL_2(\mathbb{Z})$. Acto seguido se introducirán algunas funciones modulares que serán útiles más tarde, entre ellas la más importante: $J(z)$. Todo lo que sale en este capítulo, se puede encontrar en [SH], pero muchas veces se ha tomado el enfoque de [SE], que puede resultar algo más sencillo.

El capítulo 3 será donde se introduzcan las curvas elípticas. Se comenzará hablando de los divisores para explicar el teorema de Riemman-Roch que sirve por ejemplo para reducir el estudio de las curvas a aquellas que están en forma de Weierstrass. Se verá que cuando se trabaja sobre $\mathbb{C}$, se puede parametrizar la curva a partir del toro complejo y se usará esto para estudiar los morfismos entre curvas. Finalmente veremos las propiedades de $J(z)$ que la empiezan a relacionar claramente con la teoría de números. El principio de este capítulo tiene como referencia principal [SIL], y al final, cuando habla de órdenes y de las propiedades de $J(z)$, se basa en [SH].

Finalmente, el capítulo 4 se basa completamente en el capítulo 5 de [SH]. Allí, se dará la solución del problema de Hilbert en el caso particular de los cuerpos cuadráticos imaginarios.

Capítulo 1

Teoría de cuerpos de clase

1.1. Primeras definiciones.

Esta sección servirá para introducir algunas definiciones sin entrar en demasiada profundidad en ellas. Estas definiciones serán el punto de partida para marcar el objetivo de esta memoria.

Sea K/F una extensión finita de cuerpos de números algebraicos y sean $\mathcal{O}_K$ y $\mathcal{O}_F$ sus respectivos anillos de enteros, se elegirá un ideal primo $\mathfrak{p} \subseteq \mathcal{O}_F$. Como $\mathcal{O}_K$ es un dominio de Dedekid [IR, Cap 12], el ideal extendido $\mathfrak{p}\mathcal{O}_K$ se factoriza únicamente como:

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

Para ciertos ideales primos $\mathfrak{P}_i$ de $\mathcal{O}_k$. Con esta notación se pueden dar las siguientes definiciones:

Definición 1. *Se dice que* $\mathfrak{p}$*:*

- ***No ramifica*** *en* K/F *si* $e_j = 1$ *para todo* $j = 1, ..., g$
- ***Ramifica totalmente*** *en* K/F *si* $g = 1$ *y* $e_1 = [K : F]$
- ***Permanece inerte*** *en* K/F *si el ideal extendido* $\mathfrak{p}\mathcal{O}_K$ *es primo.*
- ***Se descompone totalmente*** *en* K/F *si* $g = [K : F]$.

Para trabajar de forma más natural se introduce el concepto de ideales fraccionarios.

Definición 2. *Sean* R *un dominio de integridad,* K *su cuerpo de fracciones e* I *un* R*-submódulo de* K*. Se dice que* I *es un* ***ideal fraccionario*** *de* R *si existe un elemento* $a \in K$ *tal que* aI *es un ideal de* R*. Si* aI *es principal se dice que* I *es un* ***ideal principal fraccionario****.*

Ahora bien, sea K un cuerpo de números, la ventaja de trabajar con este tipo de ideales es que el conjunto $\mathcal{I}_K$ de ideales fraccionarios de $\mathcal{O}_K$ con la multiplicación habitual es un grupo abeliano. Si I es un ideal fraccionario de $\mathcal{O}_K$, su inverso es $I^{-1} = \{x \in K \mid xI \subset \mathcal{O}_K\}$. Se puede definir $\mathcal{P}_K$ como el subgrupo de ideales principales fraccionarios. De esta forma, el grupo de clases de ideales (del que se habló en [AD, Capítulo 2]) se puede definir como $\mathcal{C}_K = \frac{\mathcal{I}_K}{\mathcal{P}_K}$.

Si I es un ideal fraccionario de $\mathcal{O}_K$ tiene una factorización de la forma:

$$I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$$

Con $\mathfrak{p}_1, ..., \mathfrak{p}_r$ ideales primos de $\mathcal{O}_K$ y $a_1, ..., a_r \in \mathbb{Z} \setminus \{0\}$.

Definición 3. *Con la notación anterior, si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_k$, se define el **orden de $\mathfrak{p}$ en** I como:*

$$ord_{\mathfrak{p}}(I) = \begin{cases} a_i & \text{si existe } i = 1, ..., r \text{ tal que } \mathfrak{p} = \mathfrak{p}_i \\ 0 & \text{en otro caso} \end{cases}$$

Si $a \in K$ se define el orden de $\mathfrak{p}$ en a como $ord_{\mathfrak{p}}(a) \coloneqq ord_{\mathfrak{p}}\langle a \rangle$

Ahora bien, usando esta función, se puede definir un valor absoluto para cada $\mathfrak{p}$:

$$\begin{array}{rccc} |\cdot|_{\mathfrak{p}}\colon & K & \to & \mathbb{R} \\ & \alpha & \mapsto & \mathcal{N}_K(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(\alpha)} \end{array}$$

Siendo $\mathcal{N}_K(\mathfrak{p}) = \#\left(\frac{\mathcal{O}_K}{\mathfrak{p}}\right)$.

Este valor absoluto cumple que $|\alpha + \beta|_{\mathfrak{p}} \leq \text{máx}(|\alpha|_{\mathfrak{p}}, |\beta|_{\mathfrak{p}})$ para todo $\alpha, \beta \in K$.

Se denota a la completación respecto a esta norma como $K_{\mathfrak{p}}$. Se tiene una inclusión de K en $K_{\mathfrak{p}}$ si se envía $\alpha \in K$ a la sucesión constante $\overline{\{\alpha\}_n}$

Se define el anillo de enteros $\mathfrak{p}-$ádicos como $\mathcal{O}_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}} \mid |x|_{\mathfrak{p}} \leq 1\}$. Este es un anillo local cuyo ideal maximal es $\mathfrak{m}_{\mathfrak{p}} = \{x \in \mathcal{O}_{\mathfrak{p}} \mid |x|_{\mathfrak{p}} < 1\}$. [CF, Cap 1.1]

Dado $\alpha \in K$ se dirá que es totalmente positivo si para todo monomorfismo $\sigma\colon K \to \mathbb{R}$ se tiene $\sigma(\alpha) > 0$. Se denotará como $\alpha \gg 0$. También se notará $\alpha \overset{\times}{\equiv} 1 \bmod \mathfrak{m}$ si para cada $\mathfrak{p}$ tal que $\mathfrak{p} \mid \mathfrak{m}$ se tiene que en el anillo de enteros de $K_{\mathfrak{p}}$, $\alpha \equiv 1 \bmod \mathfrak{m}_{\mathfrak{p}}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})}$

Teniendo estas definiciones, dado un ideal $\mathfrak{m}$ de $\mathcal{O}_K$ se pueden definir los siguientes subgrupos de $\mathcal{I}_K$:

- $\mathcal{P}_{K,\mathfrak{m}}^{+} = \{\langle \alpha \rangle \mid \alpha \in K \ \alpha \gg 0, \text{ y } \alpha \overset{\times}{\equiv} 1 \bmod \mathfrak{m}\}$

- $\mathcal{I}_K(\mathfrak{m}) = \{\mathfrak{a} \mid \mathfrak{a} \in \mathcal{I}_K \text{ y } \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = 0 \text{ para cada } \mathfrak{p} \text{ tal que } \mathfrak{p} \mid \mathfrak{m}\}$
- $\mathcal{P}_{K,\mathfrak{m}} = \{\langle\alpha\rangle \mid \alpha \in K \text{ y } \alpha \overset{\times}{\equiv} 1 \bmod \mathfrak{m}\}$

Finalmente, a partir de estos subgrupos se se puede acabar dando las definiciones siguientes:

Definición 4. *Se define el* ***grupo de clases de ray estricto*** *de K para $\mathfrak{m}$ como $\mathcal{R}^+_{K,\mathfrak{m}} = \frac{\mathcal{I}_K(\mathfrak{m})}{\mathcal{P}^+_{K,\mathfrak{m}}}$*

De la misma manera se define el ***grupo de clases de ray*** *de K para $\mathfrak{m}$ como $\mathcal{R}_{K,\mathfrak{m}} = \frac{\mathcal{I}_K(\mathfrak{m})}{\mathcal{P}_{K,\mathfrak{m}}}$*

En este caso, hay que notar que los grupos de clases de ray juegan un papel similar al grupo de clases de ideales. De hecho, si $\mathfrak{m} = \mathcal{O}_K$, entonces $\mathcal{R}_{K,\mathfrak{m}} = \frac{\mathcal{I}_K}{\mathcal{P}_K}$ que es el grupo de clases de ideales.

Ahora bien, dado un conjunto de primos $\mathcal{S}$ de $\mathcal{O}_K$, es interesante ser capaz de definir qué proporción del total significa este conjunto. Para ello, se define la densidad de Dirichlet:

Definición 5. *Con la notación anterior, si*

$$\delta_K(\mathcal{S}) = \lim_{s\to 1} \frac{\sum_{\mathfrak{p}\in\mathcal{S}} \mathcal{N}_K(\mathfrak{p})^{-s}}{\log\left(\frac{1}{s-1}\right)}$$

.

existe, se dice que $\mathcal{S}$ tiene ***Densidad de Dirichlet*** *$\delta_K(\mathcal{S})$*

Si $\mathcal{T}$ y $\mathcal{S}$ son conjuntos de ideales primos de $\mathcal{O}_K$, se denota $\mathcal{S} \approx \mathcal{T}$ si $\delta_K(\mathcal{S} \setminus \mathcal{T}) = \delta_K(\mathcal{T} \setminus \mathcal{S}) = 0$.

Para terminar esta sección de definiciones se definirán los cuerpos de clase:

Definición 6. *Sea K/F una extensión de cuerpos de números, se define $\mathcal{S}_{K/F} = \{\mathfrak{p} \mid \mathfrak{p}$ ideal primo de $\mathcal{O}_F$ tal que descompone totalmente en $K/F\}$. Dado un ideal $\mathfrak{m}$ de $\mathcal{O}_F$ y un grupo $\mathcal{H}$ que cumple $\mathcal{P}^+_{F,\mathfrak{m}} < \mathcal{H} < \mathcal{I}_F(\mathfrak{m})$ se dice que K es* ***el cuerpo de clases sobre*** *F* ***respecto de*** *$\mathcal{H}$ si K/F es Galois y $\mathcal{S}_{K/F} \approx \{\mathfrak{p} \mid \mathfrak{p}$ es primo y $\mathfrak{p} \in \mathcal{H}\}$*

Si existe el cuerpo de clases es único. [NC, Prop 2.2, cap 3]

1.2. Idèles

En esta sección, el objetivo será reformular algunas definiciones dadas en la sección anterior. Durante esta sección K será un cuerpo de números algebraicos.

Dados dos valores absolutos $\|\cdot\|_1$ y $\|\cdot\|_2$ en K, se define la relación de equivalencia $\|\cdot\|_1 \sim \|\cdot\|_2$ si y sólo si generan el mismo espacio topológico.

Definición 7. *Cada clase de equivalencia por la relación anterior se llamará* ***lugar*** *y el conjunto de lugares se denotará* V_K.

Cada lugar está tiene un representante que será una norma de uno de los siguientes tipos [BS, Cap 4, Thm 1]:

1. $|\cdot|_{\mathfrak{p}}$ para algún ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$.
2. Una norma definida como $\|\alpha\|_\sigma = |\sigma(\alpha)|$ para cada monomorfismo $\sigma\colon K \to \mathbb{R}$.
3. Una norma definida como $\|\alpha\|_\sigma = |\sigma(\alpha)|^2 = \left|\overline{\sigma(\alpha)}\right|^2$ para cada par monomorfismos conjugados $\overline{\sigma}, \sigma\colon K \to \mathbb{C}$.

Además los valores absolutos anteriores no son equivalentes entre sí. Para agilizar la notación, si $v \in V_K$, se denotará como $\|\cdot\|_v$ al representante mencionado anteriormente y se denotará K_v a la completación de K respecto al representante mencionado antes.

Definición 8. *Si* $v \in V_K$*, se dirá que* v *es un lugar* ***finito*** *si* $\|\cdot\|_v = |\cdot|_{\mathfrak{p}}$ *para algún ideal primo* $\mathfrak{p}$*. En otro caso se dirá que* v *es un lugar* ***infinito****. Si* v *es infinito, se dirá que* v *es* ***real*** *si* v *es del segundo tipo mencionado antes y* ***complejo*** *si es del tercer tipo.*

Si v es un lugar se llamará K_v a la completación de K respecto del valor absoluto $\|\cdot\|_v$. Si v es finito, como se vio antes, $K_v \cong K_{\mathfrak{p}}$ para el primo $\mathfrak{p}$ tal que $|\cdot|_{\mathfrak{p}}$ es un representante de v, si v es infinito y real, entonces $K_v \cong \mathbb{R}$ y si es complejo $K_v \cong \mathbb{C}$. Se denotará $i_v\colon K \to K_v$ a la inyección natural y se denotará $U_v = \mathcal{O}_v^\times$ si v es finito y $U_v = K_v^\times$ si v es infinito.

Ahora se tiene suficiente notación como para definir los idèles.

Definición 9. *Un* ***idèle*** *de un cuerpo de números* K *es un vector* $\boldsymbol{a} = (a_v)_{v \in V_K}$ *donde cada* $a_v \in K_v^\times$ *y* $a_v \in U_v$ *excepto para una cantidad finita de lugares.*

El conjunto de idèles de K, que denotaremos como J_K forma un grupo con el producto $(a_v)(b_v) = (a_v b_v)$. Existe una forma canónica de ver $K^\times$ como subgrupo de J_K, via el homomorfismo:

$$\begin{aligned} i\colon K^\times &\to J_K \\ a &\mapsto (i_v(a)) \end{aligned}$$

Se puede dotar a este grupo de una topología definiendo como base de abiertos el siguiente conjunto:

$$\{\prod_{v\in V_K} C_v \mid C_v \subseteq K_v^\times \text{es abierto y } C_v = U_v \text{ exepto para una cantidad finita de lugares}\}$$

Con esta topología J_K es un grupo topológico. Es decir, las funciones

$$\begin{aligned}\tau\colon J_K \times J_K &\to J_K\\ (a,b) &\mapsto ab\end{aligned}$$

$$\begin{aligned}\gamma\colon J_K &\to J_K\\ a &\mapsto a^{-1}\end{aligned}$$

son contínuas. Además esta topología lo hace localmente compacto. Para entender la relación de este grupo con las clases de ideales, se define primero el subgrupo $\mathcal{E}_K = \prod_{v\in V_K} U_v$. Con esta notación se tiene el sigiente resultado:

Proposición 2. $\frac{J_K}{\mathcal{E}_K} \cong \mathcal{I}_K$

Demostración. Se define el siguiente homomorfismo:

$$\begin{aligned}\eta\colon J_K &\to \mathcal{I}_K\\ (a_v)_{v\in V_K} &\mapsto \prod_{v \text{ finito}} \mathfrak{p}_v^{\mathrm{ord}_v(a_v)}\end{aligned}$$

Donde $\mathfrak{p}_v$ es el primo tal que $\|\cdot\|_v = |\cdot|_{p_v}$. Con esta notación se tiene:

$$\begin{aligned}\ker\eta = \{(a_v)\colon \mathrm{ord}_v(a_v) = 0 \ \forall\ v \in V_K \text{ y } v \text{ finito}\} =\\ \{(a_v)\colon a_v \in U_v \ \forall\ v \in V_K \text{ y } v \text{ finito}\} = \mathcal{E}_K\end{aligned}$$

.

Para probar el resultado sólo habría que probar que η es sobreyectiva. Para ello, si $I \in \mathcal{I}_K$ se factoriza como $I = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_k^{e_k}$, entoces se elige a_v de forma que $\mathrm{ord}_v(a_v) = e_i$ si v tiene como representante $|\cdot|_{\mathfrak{p}_i}$ y $a_v = 1$ en otro caso. Entonces, $\eta((a_v)) = I$ □

El siguiente resultado de esta sección se enuncia tras definir dos subgrupos dado un ideal no nulo $\mathfrak{m} \subseteq \mathcal{O}_K$:

- $J^+_{K,\mathfrak{m}} = \{(a_v) \in J_K \mid a_v > 0 \ \forall\ v \text{ real, y } a_v \equiv 1 \bmod \mathfrak{p}_v^{\mathrm{ord}_v(\mathfrak{m})} \ \forall\ \mathfrak{p}_v \mid \mathfrak{m}\}$
- $\mathcal{E}^+_{K,\mathfrak{m}} = \mathcal{E}_K \cap J^+_{K,\mathfrak{m}}$

Proposición 3. *Dado un ideal no nulo $\mathfrak{m} \subseteq \mathcal{O}_K$, se tiene el siguiente isomorfismo:*

$$\frac{J_K}{K^\times \mathcal{E}^+_{K,\mathfrak{m}}} \cong \frac{\mathcal{I}_K(\mathfrak{m})}{\mathcal{P}^+_{F,\mathfrak{m}}}$$

Para probar esta proposición se usará el teorema de aproximación que se enuncia de la siguiente forma:

Teorema 2. *(Teorema de aproximación) Sean $\|\cdot\|_1, ..., \|\cdot\|_n$ valores absolutos no equivalentes dos a dos sobre un cuerpo de números K y sean $\beta_1, ..., \beta_b$ elementos no nulos de K. Para todo $\epsilon > 0$, existe un $\alpha \in K$ tal que $\|\alpha - \beta_i\|_i < \epsilon$.*

Demostración. [NC, Thm 1.1, Cap 3] □

La prueba de la proposición 2 es como sigue:

Demostración. Para comenzar se define como antes el homomorfismo:

$$\begin{aligned} \eta_{\mathfrak{m}} \colon J^+_{K,\mathfrak{m}} &\to \mathcal{I}_K(\mathfrak{m}) \\ (a_v)_{v \in V_K} &\mapsto \prod_{v \text{ finito}} \mathfrak{p}_v^{\mathrm{ord}_v(a_v)} \end{aligned}$$

Análogamente a la prueba de la proposición anterior $\eta_{\mathfrak{m}}$ es sobreyectiva y $\ker \eta_{\mathfrak{m}} = \mathcal{E}_K \cap J^+_{K,\mathfrak{m}} = \mathcal{E}^+_{K,\mathfrak{m}}$. Además $\eta_{\mathfrak{m}}(K^\times \cap J^+_{K,\mathfrak{m}}) = \mathcal{P}(\mathfrak{m})$. Por tanto:

$$\frac{\mathcal{I}(\mathfrak{m})}{\mathcal{P}(\mathfrak{m})} \cong \frac{J^+_{K,\mathfrak{m}}}{(K^\times \cap J^+_{K,\mathfrak{m}})\mathcal{E}^+_{K,\mathfrak{m}}} = \frac{J^+_{K,\mathfrak{m}}}{K^\times \mathcal{E}^+_{K,\mathfrak{m}} \cap J^+_{K,\mathfrak{m}}}$$

Por el segundo teorema de isomorfía se tiene que:

$$\frac{J^+_{K,\mathfrak{m}}}{K^\times \mathcal{E}^+_{K,\mathfrak{m}} \cap J^+_{K,\mathfrak{m}}} \cong \frac{J^+_{K,\mathfrak{m}} F^\times \mathcal{E}^+_{K,\mathfrak{m}}}{K^\times \mathcal{E}^+_{K,\mathfrak{m}}}$$

Falta probar que $J^+_{K,\mathfrak{m}} F^\times \mathcal{E}^+_{K,\mathfrak{m}} = J_K$. Para probar esto, dado $(a_v) \in J_K$ y dado $\epsilon > 0$ para todo v infinito y para todo v tal que $\mathfrak{p}_v \mid \mathfrak{m}$, se elige $b_v \in K$ tal que $\|a_v - i_v(b_v)\|_v < \frac{\epsilon}{2}$. Esto existe por la definición de completación. Por el teorema de aproximación existe un $\alpha \in K$ tal que $\|i_v(b_v) - i_v(\alpha)\|_v = \|b_v - \alpha\|_v < \frac{\epsilon}{2}$. Por tanto, usando la desigualdad triangular $\|a_v - i_v(\alpha)\|_v \leq \|a_v - i_v(b_v)\|_v + \|i_v(b_v) - i_v(\alpha)\|_v < \epsilon$. Si ϵ es suficientemente chico se tiene que:

- $\text{signo}(a_v) = \text{signo}(i_v(\alpha))$ para cada lugar v infinito.
- $i_v(\alpha)^{-1}a_v \equiv 1 \bmod \mathfrak{p}_v^{\text{ord}_v(\mathfrak{m})}$ para cada lugar $\mathfrak{p}_v \mid \mathfrak{m}$.

Por tanto, el idèle $\alpha^{-1}(a_v)$ está en $J^+_{K,\mathfrak{m}}$ y por tanto existe un idèle $(b_v) \in J^+_{K,\mathfrak{m}}$ tal que $(a_v) = \alpha(b_v)$. Por tanto, $(a_v) \in J^+_{K,\mathfrak{m}}K^\times$ y por tanto, $J_K = J^+_{K,\mathfrak{m}}K^\times$. Como $\mathcal{E}^+_{K,\mathfrak{m}} \subseteq J^+_{K,\mathfrak{m}}$, entonces, $J^+_{K,\mathfrak{m}}F^\times\mathcal{E}^+_{K,\mathfrak{m}} = J^+_{K,\mathfrak{m}}F^\times$ □

Se definirá ahora la aplicación:

$$N_{K/F}\colon \mathcal{I}_K \to \mathcal{I}_F$$

De la siguiente forma:

Definición 10. *Si w es un lugar de K y v un lugar de F, si ambos son finitos, se dice que w divide a v y se denota $w \mid v$ si $\mathfrak{P}_w \mid \mathfrak{P}_v$ y si ambos son infinitos, se dice que w divide a v si para un σ tal que $\|\cdot\|_\sigma = \|\cdot\|_w$ y para un τ tal que $\|\cdot\|_\tau = \|\cdot\|_v$, entonces, $\sigma_{|F} = \tau$ ó $\sigma_{|F} = \overline{\tau}$.*

Si $\mathbf{a} = (a_w)_{w\in V_K} \in J_K$ entonces, dado $v \in V_K$ se denota $b_v = \prod_{w|v} N_{K_w/F_v}(a_w)$.

Así se define $N_{F/K}(\mathbf{a}) = (b_v)_{v\in V_F}$. Habiendo definido esta aplicación se dará la última proposición de la sección:

Proposición 4. *Dada una extensión abeliana K/F de cuerpos de números. Sea $\mathcal{H} = F^\times N_{K/F}J_K$. Entonces:*

1. *$\mathcal{H}$ es abierto y existe un ideal $\mathfrak{m}$ tal que $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq \mathcal{H}$*
2. *La imagen de $\mathcal{H}$ bajo el isomorfismo*

$$\frac{J_F}{F^\times\mathcal{E}^+_{F,\mathfrak{m}}} \cong \frac{\mathcal{I}_F(\mathfrak{m})}{\mathcal{P}^+_{F,\mathfrak{m}}}$$

   Dado en la proposición anterior es $\frac{\mathcal{P}^+_{F,\mathfrak{m}}N_{K/F}(\mathfrak{m})}{\mathcal{P}^+_{F,\mathfrak{m}}}$.

3. *Se tiene el isomorfismo*

$$\frac{J_F}{F^\times N_{K/F}J_K} \cong \frac{\mathcal{I}_F(\mathfrak{m})}{\mathcal{P}^+_{F,\mathfrak{m}}N_{K/F}(\mathfrak{m})}$$

Idea de la demostración. Para probar el primer apartado, la idea es primero probar que $N_{F/K}\mathcal{E}$ y ver que si $\mathbf{a} \in \mathbb{H}$, entonces $\mathbf{a} \in \mathbf{a}N_{F/K}\mathcal{E} \subseteq \mathbb{H}$ y por tanto $\mathbb{H}$ es abierto. Luego, a partir de la proposición 3 se deduce la segunda parte del apartado. Para la parte 2. hay que trabajar a partir de la definición del homomorfismo η_m definido en la proposición 3

Para probar el segundo apartado, [NC, prop 5.6, cap 4] □

1.3. Reciprocidad de Artin

Sea K/F una extensión de cuerpos de números, sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_F$ y $\mathfrak{P}$ un ideal primo de $\mathcal{O}_K$ que divide a $\mathfrak{p}$, entonces se define $N_{K/F}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$ donde $f(\mathfrak{P}/\mathfrak{p}) = [\frac{\mathcal{O}_K}{\mathfrak{P}} : \frac{\mathcal{O}_F}{\mathfrak{p}}]$. Haciendo que sea multiplicativa, esta aplicacion se extiende a ideales fraccionarios, es decir:

$$N_{K/F}(\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_k^{e_k}) = N_{K/F}(\mathfrak{P}_1)^{e_1} \cdots N_{K/F}(\mathfrak{P}_k)^{e_k}$$

Definición 11. *Dada una extensión de cuerpos K/F y un ideal $\mathfrak{m}$ no nulo de $\mathcal{O}_F$, se define $\mathcal{N}_{K/F}(\mathfrak{m}) = \{\mathfrak{a} \in \mathcal{I}_F(\mathfrak{m}) \mid \mathfrak{a} = N_{K/F}(I) \text{ para algún } I \in I_K\}$*

Se tiene el siguiente resultado:

Proposición 5. *(Segunda desigualdad fundamental de teoría de cuerpos de clase). Sea K/F una extensión de Galois de cuerpos de números, sea (m) un ideal no nulo de $\mathcal{O}_f$ y sea $\mathcal{H} = \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})$, entonces:*

$$[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] \leq [K : F]$$

. [NC, Thm 2.6, cap 3] □

En esta sección se probará la reciprocidad de Artin que da un isomorfismo explícito entre el grupo de Galois de una extensión abeliana K/F y el grupo $\frac{\mathcal{I}_F(\mathfrak{m})}{\mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})}$ para un cierto ideal $\mathfrak{m}$.

Definición 12. *Dada una extensión de Galois K/F con grupo de Galois G, un primo $\mathfrak{p}$ de $\mathcal{O}_F$ y un primo $\mathfrak{P}$ de $\mathcal{O}_K$ tal que $\mathfrak{P}$ divide a $\mathfrak{p}$, se define el* ***grupo de descomposición*** *como:*

$$Z(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

A partir de aquí K/F siempre será una extensión de Galois de cuerpos de números y será abeliana cuando se especifique. Dado un primo $\mathfrak{P}$ de $\mathcal{O}_K$ que divide a un primo $\mathfrak{p}$ de $\mathcal{O}_F$, existe un homomorfismo natural $Z(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(\frac{\mathcal{O}_K}{\mathfrak{P}}/\frac{\mathcal{O}_F}{\mathfrak{p}})$ que consiste en restringir a $\mathcal{O}_k$ y pasar al cociente que es sobreyectivo. Su núcleo se denota como $T(\mathfrak{P}/\mathfrak{p})$. Se puede notar que $[Z(\mathfrak{P}/\mathfrak{p}) : T(\mathfrak{P}, \mathfrak{p})] = [\frac{\mathcal{O}_K}{\mathfrak{P}} : \frac{\mathcal{O}_F}{\mathfrak{p}}]$ y que además $\#(T(\mathfrak{P}/\mathfrak{p})) = \mathrm{ord}_{\mathfrak{P}}(\mathfrak{p})$. [DL, Cap 3.8]

Si $\mathfrak{p}$ no ramifica este homomorfismo es un isomorfismo. Además, como $\mathrm{Gal}(\frac{\mathcal{O}_K}{\mathfrak{P}}/\frac{\mathcal{O}_F}{\mathfrak{p}})$ es un grupo cíclico que está generado por el automorfismo de Frobenius, entonces, si σ es la contraimagen, se tiene que $Z(\mathfrak{P}/\mathfrak{p}) = \langle\sigma\rangle$. Se tiene que σ es el único automorfismo que cumple que $\sigma(\alpha) \cong \alpha^{\mathcal{N}_F(p)} \bmod \mathfrak{P}$. Si K/F es una extensión abeliana, además σ no depende de $\mathfrak{P}$.

Definición 13. *Si K/F es una extensión abeliana y $\mathfrak{p}$ un primo de $\mathcal{O}_F$ que no ramifica, se define el* ***automorfismo de Artin para*** *$\mathfrak{p}$ al automorfismo σ mencionado anteriormente. Se denotará $\left(\frac{\mathfrak{p}}{K/F}\right)$. Si está clara la extensión también se denotará $\sigma_{\mathfrak{p}}$.*

Con todo esto se puede definir el homomorfismo que nos dará la biyección.

Definición 14. *Sea K/F una extensión abeliana, y $\mathfrak{m}$ un ideal de $\mathcal{O}_F$ divisible por todos los ideales que ramifican, entonces se puede definir el homomorfismo:*

$$\begin{aligned} \mathcal{A}_{K/F} \colon \mathcal{I}_F(\mathfrak{m}) &\to Gal(K/F) \\ I &\mapsto \sigma_I = \sigma_{\mathfrak{p}_1}^{e_1} \cdots \sigma_{\mathfrak{p}_k}^{e_k} = \left(\frac{I}{K/F}\right) \end{aligned}$$

Donde $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$ y cada $\mathfrak{p}_i$ con $i = 1, ..., k$ ideales primos. A este homomorfismo se le llama ***Aplicación de Artin****. Si no hay ambiguidad con la extensión de cuerpos a veces se notará sólo $\mathcal{A}$. Hay que notar que $\left(\frac{I}{K/F}\right)$ no depende de $\mathfrak{m}$, A esta aplicación se le llamará el* ***símbolo de Artin****.*

Nos interesará saber cómo se comporta el símbolo de Artin en extensiones intermedias y para esto se tiene la siguiente proposición:

Proposición 6. *(Propiedad de consistencia) Sean $F \subseteq L \subseteq K$, $F \subseteq E \subseteq K$ cuerpos de números tal que K/F es una extensión abeliana. Sean $\mathfrak{p}$ un ideal de $\mathcal{O}_F$ que no ramifica en K/F, $\mathfrak{P}$ un ideal de $\mathcal{O}_K$ que divide a $\mathfrak{p}$, $\mathfrak{P}_L = \mathfrak{P} \cap L$ y $\mathfrak{P}_E \cap E$.*

Entonces $\left(\frac{\mathfrak{P}_E}{K/E}\right)\Big|_L = \left(\frac{\mathfrak{p}}{L/F}\right)^f$ donde $f = [\frac{\mathcal{O}_E}{\mathfrak{P}_E} : \frac{\mathcal{O}_F}{\mathfrak{p}}]$.

Demostración. Sea $\sigma_{\mathfrak{p}} = \left(\frac{\mathfrak{p}}{L/F}\right)$, $\sigma_{\mathfrak{p}}$ está caracterizado por:

$$\sigma_{\mathfrak{p}}(\alpha) \equiv \alpha^{\mathcal{N}_F(\mathfrak{p})} \bmod \mathfrak{P}_L$$

Sea $\sigma_{\mathfrak{P}_E} = \left(\frac{\mathfrak{P}_E}{K/E}\right)$, entonces $\sigma_{\mathfrak{P}_E}$ está caracterizado por:

$$\sigma_{\mathfrak{P}_E}(\alpha) \equiv \alpha^{\mathcal{N}_K(\mathfrak{P}_E)} \bmod \mathfrak{P}_K$$

Si $\alpha \in \mathcal{O}_L$, entonces $\sigma_{\mathfrak{P}_E}(\alpha) \equiv \alpha^{\mathcal{N}_E(\mathfrak{P}_E)} \bmod \mathfrak{P}_K \cap L$. Como $\mathfrak{P}_L$, entonces, se tiene que $\sigma_{\mathfrak{P}_E} \mid_L (\alpha) \equiv \alpha^{\mathcal{N}_E(\mathfrak{P}_E)} \bmod \mathfrak{P}_L$.

Como $\mathcal{N}_E(\mathfrak{P}_E) = \mathcal{N}_F(\mathfrak{p})^f$, entonces

$$\sigma_{\mathfrak{p}}^f(\alpha) \equiv \alpha^{\mathcal{N}_F(\mathfrak{p})^f} \equiv \alpha^{\mathcal{N}_E(\mathfrak{P}_E)} \bmod \mathfrak{P}_L$$

. Por tanto, $\sigma_{\mathfrak{p}}^f(\alpha) \equiv \sigma_{\mathfrak{P}_E} \mid_L \alpha \bmod \mathfrak{P}_L$ y esto prueba el resultado. □

Corolario 1. *Sean $F \subseteq E \subseteq K$ donde K/F es una extensión de Galois abeliana. Sea $\mathfrak{p}$ un primo de $\mathcal{O}_F$ que no ramifica en K/F y $\mathfrak{P}$ un primo de $\mathcal{O}_E$ tal que $\mathfrak{P} \mid \mathfrak{p}$. Entonces:*

$$\left(\frac{\mathfrak{P}}{K/E}\right) = \left(\frac{N_{E/F}(\mathfrak{P})}{K/F}\right)$$

Demostración. Eligiendo en el teorema $K = L$, se tiene. □

Teorema 3. *(Reciprocidad de Artin) Sea K/F una extensión abeliana de cuerpos de números, $\mathfrak{m}$ un ideal de $\mathcal{O}_F$ divisible por todos los primos que ramifican y $G = Gal(K/F)$:*

1. *$\mathcal{A}_{K/F} \colon \mathcal{I}(\mathfrak{m}) \to G$ es sobreyectiva*
2. *Se puede elegir $\mathfrak{m}$ tal que sólo lo dividan los primos que ramifican y $\mathcal{P}^+_{F,\mathfrak{m}} \subseteq \ker \mathcal{A}_{K/F}$. De manera que se puede definir un homomorfismo sobreyectivo:*
$$\frac{\mathcal{I}(\mathfrak{m})}{\mathcal{P}^+_{F,\mathfrak{m}}} \to G$$
3. *$\mathcal{N}_{K/F}(\mathfrak{m}) \subseteq \ker \mathcal{A}_{K/F}$*

Eligiendo $\mathfrak{m}$ como en el segundo apartado se tiene un homomorfismo sobreyectivo:

$$\frac{\mathcal{I}(\mathfrak{m})}{\mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})} \to G$$

Además el homomorfismo es un isomorfismo.

Demostración. Primero se probará 1. Sea $H = \mathcal{A}(I_F(\mathfrak{m})) \subseteq G$ y sea L el cuerpo fijo de H, entonces, si $\mathfrak{p}$ es un ideal primo con $\mathfrak{m}$, usando el teorema de consistencia para $E = F$ se tiene que:

$$\left(\frac{\mathfrak{p}}{L/F}\right) = \left(\frac{\mathfrak{p}}{K/F}\right)|_L$$

En concreto, por definición de H, se tiene que:

$$\left(\frac{\mathfrak{p}}{K/F}\right)|_L = \left(\frac{\mathfrak{p}}{L/F}\right) = 1$$

Entonces si $\mathfrak{P}$ es un primo de $\mathcal{O}_L$ que divide a $\mathfrak{p}$, $\left(\frac{\mathfrak{p}}{L/F}\right) = 1$ genera $Z(\mathfrak{P}/\mathfrak{p})$ y por tanto se tiene que $[Z(\mathfrak{P}/\mathfrak{p}) : T(\mathfrak{P}, \mathfrak{p})] = [\frac{\mathcal{O}_K}{\mathfrak{P}} : \frac{\mathcal{O}_F}{\mathfrak{p}}] = 1$ y que además $\#(T(\mathfrak{P}/\mathfrak{p})) = \mathrm{ord}_{\mathfrak{P}}(\mathfrak{p}) = 1$.

Sea $\mathcal{S}_{L/F} = \{\mathfrak{p} \mid [\frac{\mathcal{O}_K}{\mathfrak{P}} : \frac{\mathcal{O}_F}{\mathfrak{p}}] = 1 \text{ y } \mathrm{ord}_{\mathfrak{P}}(\mathfrak{p}) = 1\}$, y sea $\mathcal{S}_F = \{\mathfrak{p} \mid \mathfrak{p} \text{ es un primo de } \mathcal{O}_F\}$, entonces $\mathcal{S}_{L/F} \setminus \mathcal{S}_F$ es finito y por [NC][Cor 5.2, cap 2] (en la prueba, usa que la extensión es Galois porque usa que los primos que descomponen totalmente cumplen $[\frac{\mathcal{O}_K}{\mathfrak{P}} : \frac{\mathcal{O}_F}{\mathfrak{p}}] = 1$ y $\mathrm{ord}_{\mathfrak{P}}(\mathfrak{p}) = 1$ así que realmente el resultado es el mismo)

$\frac{1}{[L:F]} = \delta_F(\mathcal{S}_{L/F}) = \delta_F(\mathcal{S}_F) = 1$

Por tanto, $L = F$ y por el teroema fundamental de teoría de Galois $H = G$.

Para probar 2. se empieza probando en el caso $F = \mathbb{Q}$ y $K = \mathbb{Q}(\zeta_m)$ siendo ζ_m una raíz primitiva m-ésima de la unidad. Sea $\langle p\rangle$ un primo de $\mathbb{Z}$ donde p y m son coprimos. Entonces se denotará $\sigma_p = \left(\frac{\langle p\rangle}{K/F}\right)$ que está definido como $\sigma_p(\zeta_m) = \zeta_m^p$. Esta definición es compatible con la anterior dado que si $[K : F] = k$, un elemento de $\mathcal{O}_K$ se puede escribir como $x = a_0 + a_1\zeta_m + ... + a_k\zeta_m^{k-1}$ y entonces $x^p \equiv a_0^p + a_1^p\zeta_m^p + ... + a_k\zeta_m^{p(k-1)} \equiv a_0^p + a_1^p\zeta_m^p + ... + a_k\zeta_m^{p(k-1)} \equiv a_0 + a_1\sigma_p(\zeta_m) + ... + a_k\sigma_p(\zeta_m^{k-1}) \equiv \sigma_p(x) \bmod p$. Por tanto, también se da la igualdad módulo un primo que divide a $\langle p\rangle$.

Sea $a \in \mathbb{Z}_+$ tal que a se factoriza como $a = p_1^{e_1} \cdots p_r^{e_r}$, y es coprimo con m. Entonces, denotando $\sigma_a = \left(\frac{\langle a\rangle}{K/F}\right)$, $\sigma_a(\zeta_m) = \zeta_m^a$.

Sea $a = \frac{b}{c}$ con $b, c \in \mathbb{Z}_+$, entonces se tiene que $\sigma_c\sigma_a = \sigma_{ca} = \sigma_b$. Es decir, $\sigma_a = \sigma_b\sigma_c^{-1}$. Eligiendo $d \in \mathbb{Z}_+$ tal que $dc \equiv 1 \bmod m$, $\sigma_c^{-1} = \sigma_d$. Por tanto $\sigma_a = \sigma_{bd}$. Si $\langle a\rangle \in \mathcal{P}^+_{\mathbb{Q},\langle m\rangle}$, entonces $cd \equiv 1 \bmod m$. Y eso implica que $\sigma_a = 1$. Por tanto $\mathcal{P}^+_{\mathbb{Q},\langle m\rangle} \subseteq \ker \mathcal{A}$.

Si ahora F es un cuerpo de números cualquiera y $K = F(\zeta_m)$, por la propiedad de consistencia se tiene que:

$$\left(\frac{\mathfrak{a}}{K/F}\right)|_{\mathbb{Q}(\zeta_m)} = \left(\frac{N_{F/\mathbb{Q}}\mathfrak{a}}{\mathbb{Q}(\zeta_m)/\mathbb{Q}}\right)$$

Como un automorfismo σ de $\mathrm{Gal}(K/F)$ fija F, entonces este es trivial si y sólo si $\sigma\,|_{\mathbb{Q}(\zeta_m)} = 1$.

Sea $\mathfrak{m} = \langle m\rangle$, y sea $\mathfrak{a} \in \mathcal{P}^+_{F,\mathfrak{m}}$. Entonces $\mathfrak{a} = \langle\alpha\rangle$ para un α tal que $\alpha \overset{\times}{\equiv} 1 \bmod \mathfrak{m}$ y $\alpha \gg 0$. Por tanto:

$$\left(\frac{\mathfrak{a}}{K/F}\right)|_{\mathbb{Q}(\zeta_m)} = \left(\frac{\langle\alpha\rangle}{K/F}\right)|_{\mathbb{Q}(\zeta_m)} = \left(\frac{N_{F/\mathbb{Q}}(\langle\alpha\rangle)}{\mathbb{Q}(\zeta_m)/\mathbb{Q}}\right) = \left(\frac{\langle N_{F/\mathbb{Q}}(\alpha)\rangle}{\mathbb{Q}(\zeta_m)/\mathbb{Q}}\right)$$

Como $\alpha \gg 0$, enonces $N_{F/\mathbb{Q}}(\alpha) > 0$. Como además $\alpha \overset{\times}{\equiv} 1 \bmod \mathfrak{m}$, entonces se debe tener $N_{F/\mathbb{Q}}(\alpha) \overset{\times}{\equiv} 1 \bmod \mathfrak{m}$. Como vimos antes, eso implica que

$$\left(\frac{\langle N_{F/\mathbb{Q}}(\alpha)\rangle}{\mathbb{Q}(\zeta_m)/\mathbb{Q}}\right) = 1$$

Por tanto, se tiene que

$$\left(\frac{\mathfrak{a}}{K/F}\right) = 1$$

Por tanto $\mathfrak{a} \in \ker \mathcal{A}$ cumpliendose 2.

Si ahora se tiene $F \subseteq E \subseteq K$ como en el apartado anterior, por la propiedad de consistencia, se tiene que $\mathcal{P}^+_{F,\mathfrak{m}} \subseteq \ker \mathcal{A}_{E/F}$.

Si K/F es una extensión cíclica arbitraria, por [NC, Cor 5.11, cap 4] se tiene que existe un ideal $\mathfrak{m}$ de $\mathcal{O}_F$ tal que $[K : F] = [\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})]$. Como $\mathcal{A}$ es sobreyectiva, se tiene que:

$$[\mathcal{I}_F(\mathfrak{m}) : \ker \mathcal{A}] = \#G = [K : F] = [\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}^+_{F\mathfrak{m}}\mathcal{N}_{K/F}]$$

Por [NC, Prop 2.2, cap 5] se tiene que $\ker A \subseteq \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}$. Por tanto, se debe dar $\mathcal{P}^+_{F,\mathfrak{m}} \subseteq \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F} = \ker \mathcal{A}$ y por lo tanto se da 2.

Si K/F es una extensión abeliana arbitraria, entonces para cada cada extensión cíclica E/F se tiene que existe un ideal $\mathfrak{m}_E$ tal que $\mathcal{P}^+_{F,\mathfrak{m}_E} \subseteq \ker \mathcal{A}_{E/F}$. Se define $\mathfrak{m} = \prod_{E/F\text{cíclica}E\subseteq K} \mathfrak{m}_E$. Como $\mathcal{P}^+_{F,\mathfrak{m}} \subseteq \mathcal{P}^+_{F,\mathfrak{m}_E}$ para cada E como en el producto, entonces, si $\mathfrak{a} \in \mathcal{P}^+_{F,\mathfrak{m}}$ y E/F es una extensión cíclica con $E \subseteq K$, se tiene que si $\sigma = \left(\frac{\mathfrak{a}}{K/F}\right)$, por la propiedad de consistencia, se tiene que $\sigma\,|_E = 1$.

Si $\sigma \neq 1$, entonces existe un caracter no trivial $\overline{\chi}\colon \langle\sigma\rangle \to \mathbb{C}^\times$. Este caracter se puede extender a un caracter χ de G. Sea $H = \ker \chi$, entonces $\frac{G}{H}$ es cíclico.

Efectivamente, primero si dado un grupo T, $\hat{T}$ denota el grupo de caracteres de T, se tiene que $H \cong \langle\chi\rangle^\perp = \{\psi \in \hat{\hat{G}} \mid \psi(\chi) = 1\}$ Por el homomorfismo $\phi\colon G \to \hat{\hat{G}}$ que se ha definido y probado que es isomorfismo en [NC, Prop 1.2, cap 2] restringido a H. La imagen es $\langle\chi\rangle$ porque si $g \in G \setminus H$ $\chi(g) \neq 1$. Entonces, se tiene que $\langle\chi\rangle \cong H^\perp$ Por [NC, Prop 1.3, cap 2] se tiene que $H^\perp \cong \widehat{(\frac{G}{H})}$ y por [NC, Prop 1.1, cap 2] se tiene que $\widehat{(\frac{G}{H})} \cong \frac{G}{H}$ y por tanto es cíclico.

Si E es cuerpo fijo de H, entonces $\mathrm{Gal}(E/F) \cong \frac{G}{H}$ via el morfismo que restringe un automorfismo de G a E. Como es cíclico, se tiene que $\sigma\,|_E = 1$ y por tanto $\sigma \in H = \ker \chi$, lo cual está en contradicción con que $\chi\,|_{\langle\sigma\rangle}$ es no trivial.

Para probar 3. usando el corolario 1. y usando $K = E$ se tiene que si $\mathfrak{p}$ es un primo de $\mathcal{O}_F$ que no ramifica y $\mathfrak{P}$ un primo de $\mathcal{O}_K$ tal que $\mathfrak{P} \mid \mathfrak{p}$

$$\left(\frac{N_{K/F}(\mathfrak{P})}{K/F}\right) = \left(\frac{\mathfrak{P}}{K/K}\right) = 1$$

Si I es un ideal K primo con cada primo que ramifica en K/F, entonces

$$\left(\frac{N_{K/F}(I)}{K/F}\right) = 1$$

Finalmente el homomorfismo es biyectivo porque por la segunda desigualdad fundamental, se tiene que $[\mathcal{I}(\mathfrak{m}) : \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})] \leq \#G$.

□

Finalmente se dará una reinterpretación en idèles de la reciprocidad de Artin. Esta consistirá en, dado un ideal $\mathfrak{m}$ como en la proposición 4 tal que $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq F^\times N_{K/F}J_K$ componer los siguientes morfismos:

$$J_F \twoheadrightarrow \frac{J_F}{F^\times N_{K/F}J_K} \overset{\cong}{\underset{3}{\to}} \frac{\mathcal{I}(\mathfrak{m})}{\mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})} \xrightarrow[\text{Aplicación de Artin}]{\cong} G$$

Siendo el primer morfismo sobreyectivo el canónico. Componiendo se define la aplicación de Artin en idèles:

$$\rho_{K/F} \colon J_F \to G$$

Se dirá que K es el cuerpo de clase de $F^\times N_{K/F}J_K$.

1.4. Correspondencia de subgrupos abiertos y extensiones abelianas.

El objetivo de esta sección será dar una correspondencia entre las extensiones abelianas de un cuerpo de números F y ciertos subgrupos abiertos de J_F.

Proposición 7. *Sea*

$\phi \colon \{$*Extensiones abelianas finitas de* $F\} \to \{$*Subgrupos abiertos de* J_F *que contienen a* $F^\times\}$

La aplicación dada por $\phi(K) = F^\times N_{K/F}J_K$. *Entonces si* K, K' *y* E *son extensiones finitas de* F, *se tiene:*

1. $K \subseteq K'$ *si y sólo si* $\phi(K') \subseteq \phi(K)$
2. $\phi(KK') = \phi(K) \cap \phi(K')$

3. $\phi(K \cap K') = \phi(K)\phi(K')$

4. *Si* $\mathcal{H} = \phi(E) = F^{\times} N_{E/F} J_E$ *y* $E \subseteq K$, *entonces* E *es el cuerpo fijo de* $\rho_{K/F}(\mathcal{H})$

Demostración. Sean $\mathcal{H} = \phi(K)$ y $\mathcal{H}' = \phi(K')$, entonces se tiene que $\mathcal{H} = \ker \rho_{K/F}$ y $\mathcal{H}' = \ker \rho_{K'/F}$. Sea $\mathbf{a} \in \mathcal{I}_F$ entonces, $\rho_{K/F}$ y $\rho_{KK'/F}$ vienen dados de la siguiente forma para ideales $\mathfrak{m}$ y $\mathfrak{m}'$ adecuados y siendo $G = \mathrm{Gal}(K/F)$ y $G' = \mathrm{Gal}(KK'/F)$:

$$\begin{array}{rccccccc}
\rho_{K/F}\colon & J_F & \to & \frac{J_F}{F^{\times} N_{K/F} J_K} & \to & \frac{\mathcal{I}(\mathfrak{m})}{\mathcal{P}^{+}_{F,\mathfrak{m}} \mathcal{N}_{K/F}(\mathfrak{m})} & \to & G \\
& \mathbf{a} & \mapsto & \mathbf{a} & \mapsto & \langle \alpha \mathbf{a} \rangle & \mapsto & \left(\frac{\langle \alpha \mathbf{a} \rangle}{K/F}\right) \\
\rho_{KK'/F}\colon & J_F & \to & \frac{J_F}{F^{\times} N_{KK'/F} J_K} & \to & \frac{\mathcal{I}(\mathfrak{m}')}{\mathcal{P}^{+}_{F,\mathfrak{m}'} \mathcal{N}_{KK'/F}(\mathfrak{m}')} & \to & G' \\
& \mathbf{a} & \mapsto & \mathbf{a} & \mapsto & \langle \alpha' \mathbf{a} \rangle & \mapsto & \left(\frac{\langle \alpha' \mathbf{a} \rangle}{KK'/F}\right)
\end{array}$$

Donde $\alpha, \alpha' \in F^{\times}$ están definidos en la proposición 3. Como

$$\left(\frac{\langle \alpha \mathbf{a} \rangle}{K/F}\right)\left(\frac{\langle \alpha' \mathbf{a} \rangle^{-1}}{K/F}\right) = \left(\frac{\langle \alpha \alpha^{-1} \rangle}{K/F}\right) = 1$$

Entonces

$$\left(\frac{\langle \alpha \mathbf{a} \rangle}{K/F}\right) = \left(\frac{\langle \alpha' \mathbf{a} \rangle}{K/F}\right)$$

Por el la propiedad de consistencia del símbolo de Artin se tiene que:

$$\rho_{KK'/F}(\mathbf{a}) \mid_K = \left(\frac{\langle \alpha' \mathbf{a} \rangle}{KK'/F}\right)\mid_K = \left(\frac{\langle \alpha' \mathbf{a} \rangle}{K/F}\right) = \left(\frac{\langle \alpha \mathbf{a} \rangle}{K/F}\right) = \rho_{K/F}(\mathbf{a})$$

Por tanto, $\ker \rho_{KK'/F} \subseteq \ker \rho_{K/F}$. Haciendo lo mismo con K' se consigue $\ker \rho_{KK'/F} \subseteq \ker \rho_{K'/F}$. Por tanto, como $\phi(KK') = \ker \rho_{KK'/F}$, entonces $\phi(KK') \subseteq \phi(K) \cap \phi(K')$.

De la misma forma si $\mathbf{a} \in \ker \rho_{K/F}$ y, $\mathbf{a} \in \ker \rho_{K'/F}$. Entonces $\rho_{KK'/F}(\mathbf{a}) \in G'$ es trivial en K y en K'. Por tanto debe ser la identidad y por esto $\phi(KK') \supseteq \phi(K) \cap \phi(K')$. Así que se tiene 2.

1. se prueba porque en este caso $KK' = K'$. Por tanto $\phi(K') = \phi(K) \cap \phi(K') \subseteq \phi(K)$. Por otro lado si $\phi(K') \subseteq \phi(K)$, entonces $\phi(K') = \phi(K) \cap \phi(K')$ por el apartado 2.

$$[K' : F] = \#\left(\frac{J_F}{\phi(K')}\right) = \#\left(\frac{J_F}{\phi(K') \cap \phi(K)}\right) = \#\left(\frac{J_F}{\phi(KK')}\right) = [KK' : F]$$

Como $K' \subseteq KK'$, entonces se tiene que $KK' = K'$ y por tanto $K \subseteq K'$.

Para probar 4. si $\mathbf{a} \in \mathcal{H}$ entonces $\rho_{K/F}(\mathbf{a})|_E = \rho_{E/F}(\mathbf{a})$. Como $\mathcal{H} = \ker \rho_{E/F}$ entonces, $1 = \rho E/F = \rho_{K/F} \mid E$. Por tanto, el cuerpo fijo de $\rho_{K/F}$ contiene a E

Si $\rho_{K/F}$ fija $x \in K$, entonces fija $E(x)$. Por tanto, para $\mathbf{a} \in \mathcal{H}$, $1 = \rho_{K/F}(\mathbf{a}) \mid_{E(x)} = \rho_{E(x)/F}(\mathbf{a})$. Por tanto, $\mathbf{a} \in \ker \rho_{E(x)/F}$ y por ello $\mathcal{H} \subseteq \phi(E(x))$. Usando 1. $E(x) \subseteq E$ y por tanto $x \in E$. Así que E es el cuerpo fijo de $\rho_{K/F}(\mathcal{H})$. Por tanto 4. es cierto.

Falta probar 3. para ello, como $K, K' \subseteq K \cap K'$, por 1. $\phi(K), \phi(K') \subseteq \phi(K \cap K')$. Por tanto $\phi(K)\phi(K') \subseteq \phi(K \cap K')$.

Si $\mathbf{a} \in \phi(K)$ y $\mathbf{b} \in \phi(K')$, entonces:

$$\rho_{KK'/F}(\mathbf{ab}) \mid_{K\cap K'} = \rho_{KK'/F}(\mathbf{a}) \mid_{K\cap K'} \rho_{KK'/F}(\mathbf{a}) \mid_{K\cap K'} = 1$$

Por tanto, $\rho_{KK'/F}(\mathbf{ab})$ fija $K \cap K'$. En concreto $\rho_{KK'/F}(\phi(K)\phi(K'))$ fija $K \cap K'$. Por tanto, si E es el cuerpo fijo de $\rho_{KK'/F}(\phi(K)\phi(K'))$, entonces $K \cap K' \subseteq E$. Por 4. E es el cuerpo fijo de $\rho_{KK'/F}(\phi(E))$ y por el teorema fundamental de teoría de Galois se tiene que $\rho_{KK'/F}(\phi(K)\phi(K')) = \rho_{KK'/F}\phi(E)$. Esto implica que si $\mathbf{a} \in \phi(E)$, entonces existen $\mathbf{b} \in \phi(K)$ y $\mathbf{b}' \in \phi(K')$ tales que $\rho_{KK'/F}(\mathbf{a}) = \rho_{KK'/F}(\mathbf{bb}')$. Por tanto, $\mathbf{a}(\mathbf{bb}')^{-1} \in \ker \rho_{KK'/F} = \phi(KK') = \phi(K) \cap \phi(K')$. Por tanto $\mathbf{a} = \mathbf{a}(\mathbf{bb}')^{-1}(\mathbf{bb}') \in (\phi(K) \cap \phi(K'))\phi(K)\phi(K') = \phi(K)\phi(K')$.

□

Este teorema tiene el siguiente corolario

Corolario 2. *Si K es el cuerpo de clases asociado a un subgrupo abierto $\mathcal{H}$ de J_F que contiene a $F^\times$ y $\mathcal{H}' \supseteq \mathcal{H}$ es un subgrupo abierto de J_F, entonces $\mathcal{H}'$ tiene cuerpo de clases.*

Demostración. Sea E el cuerpo fijo de $\rho_{K/F}(\mathcal{H}')$, como $\mathcal{H} \subseteq \mathcal{H}'$ y K es el cuerpo fijo de $\rho_{K/F}(\mathcal{H})$, entonces $F \subseteq E \subseteq K$.

Sea $\mathbf{a} \in J_F$, como $\phi(E) = \ker \rho_{E/F}$, entonces $\mathbf{a} \in \phi(E)$ si y sólo si $\mathbf{a} \in \ker \rho_{E/F}$. Como $\rho_{E/F} = \rho_{K/F} \mid_E$, entonces $\mathbf{a} \in \ker \rho_{E/F}$ si y sólo si $\rho_{K/F} \mid_E (\mathbf{a}) = 1$ y esto es si y sólo si $\rho_{K/F}(\mathbf{a})$ fija E, es decir, si $\rho_{K/F}(\mathbf{a}) \in \rho_{K/F}(\mathcal{H}')$. Esto último es equivalente a que exista un $\mathbf{b} \in \mathcal{H}'$ tal que $\rho_{K/F}(\mathbf{a}) = \rho_{K/F}(\mathbf{b})$ o lo que es lo mismo, que exista un $\mathbf{b} \in \mathcal{H}'$ tal que $\mathbf{ab}^{-1} \in \ker \rho_{K/F}$. Como $\ker \rho_{K/F} = \mathcal{H}$, esto equivale a que $\mathbf{a} \in \mathcal{H}\mathcal{H}' = \mathcal{H}'$. □

Teorema 4. *(Teorema de existencia) Sean F un cuerpo de números, todo subgrupo abierto $\mathcal{H}$ de J_F que contiene a $F^\times$ tiene cuerpo de clase.*

Demostración. Primero hay que probar que si F es un cuerpo que contiene todas las raices n-ésimas de la unidad, $\mathcal{S}$ un conjunto finito de lugares que contiene a todos los lugares infinitos, los lugares v tal que $\mathfrak{p}_v \mid n$ y tal que $J_F = F^\times J_{F,\mathcal{S}}$, si $B = \prod_{v\in\mathcal{D}} (F^\times)^n \prod_{v\notin\mathcal{S}} U_v$, entonces $F^\times B$ tiene cuerpo de clases. El resto de la prueba consiste en ver que para todo subgrupo abierto $\mathbb{H}$ de J_F que contiene a $F^\times$ existe un $\mathcal{S}$ como antes, tal que el B correspondienbte cumple que $B \subseteq \mathcal{H}$. De aquí se deduce que $F^\times B \subseteq F^\times \mathbb{H} = \mathbb{H}$ y el teorema te lo da el corolario. 2.

La prueba completa está en [NC, thm 2.7, cap 6] □

Capítulo 2

Formas modulares

2.1. Grupos Fuchsianos.

Se denota $\mathbb{P} = \mathbb{C} \cup \{\infty\}$. Se puede definir la acción del grupo $GL_2(\mathbb{C})$ de la siguiente forma: sea $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C})$

$$\sigma z = \frac{az+b}{cz+d} \quad \forall z \in \mathbb{P}$$

.

Se pueden conseguir identidades interesantes denotando $j(\sigma, z) = cz + d$. Con esta notación, es una comprobación directa que:

$$\sigma \begin{pmatrix} z \\ 1 \end{pmatrix} = j(\sigma, z) \begin{pmatrix} \sigma z \\ 1 \end{pmatrix}$$

Si $\tau \in GL_2(\mathbb{C})$, entonces, usando esta identidad se tiene que:

$$j((\tau\sigma), z) \begin{pmatrix} (\tau\sigma)z \\ 1 \end{pmatrix} \tau\sigma \begin{pmatrix} z \\ 1 \end{pmatrix} = \tau \Big(j(\sigma, z) \begin{pmatrix} \sigma(z) \\ 1 \end{pmatrix} \Big) = j(\sigma, z) j(\tau, \sigma z) \begin{pmatrix} \tau\sigma z \\ 1 \end{pmatrix}$$

Obteniendo de aquí las siguientes dos identidades:

$$j(\tau\sigma, z) = j(\sigma, z) j(\tau, \sigma z) \tag{2.1}$$

$$(\tau\sigma)z = \tau(\sigma z) \tag{2.2}$$

Como Id es la transformación identidad, entonces, la última identidad implica que σ^{-1} también es la inversa de σ como transformación en $\mathbb{P}$. Por otro lado, se tiene que:

$$\sigma\begin{pmatrix} z+h & z \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} j(\sigma, z+h)\sigma(z+h) & j(\sigma,z)\sigma(z) \\ j(\sigma, z+h) & j(\sigma,z) \end{pmatrix}$$

tomando determinantes queda:

$$\det(\sigma)h = j(\sigma,z)j(\sigma,z+h)(\sigma(z+h)-\sigma z)$$

Dividiendo por h y tomando límite cuando h tiende a 0 se tiene:

$$\det(\sigma) = \lim_{h\to 0} j(\sigma,z)j(\sigma,z+h)\frac{(\sigma(z+h)-\sigma z)}{h} = (j(\sigma,z)^2)\frac{\mathrm{d}\sigma(z)}{\mathrm{d}z} \tag{2.3}$$

A partir de ahora nos restringiremos a $SL_2(\mathbb{R})$. Aquí, obtendremos una nueva identidad a partir de la igualdad:

$$\sigma\begin{pmatrix} \bar{z} & z \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} j(\sigma,\bar{z})\sigma\bar{z} & j(\sigma,z)\sigma z \\ j(\sigma,\bar{z}) & j(\sigma,z) \end{pmatrix} = \begin{pmatrix} \overline{j(\sigma,z)}\overline{\sigma z} & j(\sigma,z)\sigma z \\ \overline{j(\sigma,z)} & j(\sigma,z) \end{pmatrix}$$

.

Tomando determinante, se obtiene la identidad:

$$\det(\sigma) = \|j(\sigma,z)\|^2\frac{\mathrm{Im}(\sigma z)}{\mathrm{Im}(z)} \tag{2.4}$$

Si se define $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$, entonces, $\mathbb{H}$ es estable bajo la acción de $SL_2(\mathbb{R})$.

Se quieren buscar cómo son los puntos fijos en $\mathbb{P}$ bajo esta acción del grupo $SL_2(\mathbb{R})$. Para ello, hay que coger un elemento $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$ y los puntos fijos de σ son las soluciones a la ecuación:

$$\frac{az+b}{cz+d} = z$$

Si $c = 0$, $ad = 1$ y entonces ∞ es un punto fijo. Para $z \neq \infty$, z es punto fijo si y sólo si $az + b = dz$ tiene solución, pero en este caso la solución sería real.

Si $c \neq 0$, entoncs, $\sigma\infty = \frac{a}{c}$ y por tanto ∞ no es un punto fijo. Si $z \neq \infty$, $cz + d = 0$ si $z = -\frac{d}{c}$, pero en este caso z no es un punto fijo. Por tanto, z es un punto fijo si y sólo si $az + b = dz^2 + cz$ tiene solución. Esto da tres posiblidades: o bien tiene dos puntos fijos reales, o bien tiene dos puntos fijos complejos (no reales) y conjugados o bien sólo tiene un punto fijo real.

Entorno a esto, se pueden clasificar las transformaciones de $SL_2(\mathbb{R})$.

Definición 15. *Dada $\sigma \in SL_2(\mathbb{R})$, entonces:*

- *Se dice que σ es una transformación* ***elíptica*** *si tiene un punto fijo $z \in \mathbb{H}$ y su otro punto fijo es $\bar{z}$*
- *Se dice que σ es una transformación* ***parabólica*** *si sólo tiene un punto fijo $z \in \mathbb{R} \cup \{\infty\}$*
- *Se dice que σ es una transformación* ***hiperbólica*** *si tiene dos puntos fijos en $\mathbb{R} \cup \{\infty\}$.*

Se fijará hasta el final de esta sección un subgruo discreto (con la topología inducida de la euclídea) Γ de $SL_2(\mathbb{R})$. A los puntos fijos también se les puede dar nombres:

Definición 16. *Un punto $z \in \mathbb{H}$ se dice* ***punto elíptico de*** *Γ si existe una transformación elíptica $\sigma \in \Gamma$ con $\sigma z = z$. Un punto $s \in \mathbb{R} \cup \{\infty\}$ se llama una* ***cúspide de*** *Γ si existe una transformación $\sigma \in \Gamma$ tal que $\sigma s = s$.*

Se define el conjunto $\mathbb{H}^*$ como la unión de $\mathbb{H}$ y las cúspides. En $\mathbb{H}^*$ se define la relación de equivalencia $z \sim z'$ si y sólo si existe $\sigma \in \Gamma$ tal que $\sigma z = z'$. El conjunto de las clases de equivalencia se denota $\Gamma\backslash\mathbb{H}^*$ y el conjunto de las clases de equivalencia en $\mathbb{H}$ se denota $\Gamma\backslash\mathbb{H}$.

Se puede definir una topología en $\Gamma\backslash\mathbb{H}^*$ definiendo una base de abiertos que consistirá en para cada $z \in \mathbb{H}$ todas las bolas abiertas de centro z y para cada cúspide $s \in \mathbb{R}$, los conjuntos de la forma $\{s\} \cup \{$ el interior de un círculo en $\mathbb{H}$ tangente a la recta real en $s\}$ y los conjuntos de la forma $\{\infty\} \cup \{z \in \mathbb{H} \mid \operatorname{Im} z > c\}$ para cada $c > 0$.

Definición 17. *Se dice que un subgrupo dicreto Γ de $SL_2(\mathbb{R})$ es un* ***grupo Fuchsianos de primer tipo*** *si $\Gamma\backslash\mathbb{H}^*$ es compacto.*

Se llama grupo modular a cualquier subgrupo de $SL_2(\mathbb{Z})$ de índice finito pero aquí cuando hablemos del grupo modular nos referiremos sólamente a $SL_2(\mathbb{Z})$.

2.2. Dominio fundamental.

Para estudiar $\Gamma/\mathbb{H}$ es conveniente encontrar un subconjunto de $\mathbb{H}^*$ que modelice bien este espacio topológico. Para ello se da la siguiente definición:

Definición 18. *Dado un subgrupo discreto Γ de $SL_2(\mathbb{R})$ y un subconjunto F de $\mathbb{H}$, se dice que F es un* ***dominio fundamental*** *de Γ si satisface:*

- $\mathbb{H} = \bigcup_{\sigma \in \Gamma} \sigma F$

- *existe un subconjunto abierto* U *de* F *tal que* $\overline{U} = F$
- $U \cap \sigma U = \emptyset \ \forall \sigma \in \Gamma \setminus Z(\Gamma)$ *siendo* $Z(\Gamma)$ *el centralizador de* Γ.

En esta sección el objetivo será encontrar un dominio fundamental para $SL_2(\mathbb{Z})$ y sacar de esto algunas conclusiones. Para ello, primero, se considerarán las siguientes matrices:

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ y } S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Se tienen las siguientes identidades:

$$Tz = z + 1, \ Sz = -\frac{1}{z}, \ S^2 z = z, \ (ST)^3 z = z$$

Se define el conjunto $F = \{z \in \mathbb{H} \mid |z| \geq 1, |\mathrm{Re}(z)| \leq \frac{1}{2}\}$. Para probar que F es un nominio fundamental se usará la siguiente proposición:

Proposición 8. *1. Para toda* $z \in \mathbb{H}$ *existe* $\sigma \in SL_2(\mathbb{Z})$ *tal que* $\sigma z \in F$.

2. Si $z \in F$ *y* $z' \in F$ *son distintos y tales que existe un* $\sigma \in SL_2(\mathbb{Z})$ *con* $\sigma z = z'$, *entonces,* $\mathrm{Re}(z) = \pm\frac{1}{2}$ *y* $z = z' \pm 1$ *ó* $|z| = 1$ *y* $z' = -\frac{1}{z}$.

3. Si $I(z) = \{\sigma \in SL_2(\mathbb{Z}) \mid \sigma z = z\}$, *entonces* $I(z) = \{\pm Id\}$ *excepto en tres casos:*

- *Si* $z = i$, *entonces* $I(z)$ *es el grupo de orden* 4 *generado por* S *y* $-Id$.
- *Si* $z = \rho = e^{\frac{2\pi i}{3}}$ *en cuyo caso* $I(z)$ *es el grupo de orden* 6 *generado por* ST *y* $-Id$
- *Si* $z = \bar{\rho} = e^{\frac{\pi i}{2}}$, *en cuyo caso* $I(z)$ *es el grupo de orden* 6 *generado por* TS *y* $-Id$.

Demostración. Para probar 1., si $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, entonces $\mathrm{Im}(\sigma z) = \frac{\mathrm{Im}(z)}{|cz+d|^2}$. Se tiene que $cz + d \in B(0, r)$ si y sólo si $z \in B(-\frac{d}{|c|}, \frac{r}{|c|})$. Fijado un r tal que existan un c' y un d' con $z \in B(-\frac{d'}{|c'|}, \frac{r}{|c'|})$, como $z \notin \mathbb{R}$, entonces, se tiene que existe un $\epsilon > 0$ tal que $\left|z + \frac{d}{|c|}\right| > \epsilon$. Por tanto, debe ocurrir que $\epsilon < \frac{r}{|c|}$ y como $c \in \mathbb{Z}$ hay un número finito de c. Fijado una c, como los d son enteros, sólo hay un número finito de d tal que $z \in B(-\frac{d}{|c|}, \frac{r}{|c|})$. Esto prueba que debe existir un $\sigma \in G$ (donde G es el grupo generado por T y S) para el cual $|cz + d|^2$ alcance el mínimo y por tanto, que $\mathrm{Im}(\sigma z)$ alcance un máximo.

Se puede elegir un n entero tal que $-\frac{1}{2} \leq \mathrm{Re}(T^n\sigma z) \leq \frac{1}{2}$. Si $|T^n\sigma z| < 1$, entonces $\mathrm{Im}(ST^n\sigma z) = \frac{1}{|ST^n\sigma z|}\mathrm{Im}(T^n\sigma z) > \mathrm{Im}(T^n\sigma z)$. Por tanto $|T^n\sigma z| \geq 1$ y por tanto $T^n\sigma z \in F$.

2. y 3. se pueden probar a la vez. Sea $z \in \mathbb{H}$ y $\sigma \in SL_2(\mathbb{Z})$ que cumplan 2., entonces, sin pérdida de generalidad se puede suponer que $\mathrm{Im}(\sigma z) \geq \mathrm{Im}\, z$ porque si no, se elige σz como z y σ^{-1} como σ. Para que esto ocurra, si $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, entonces, $|cz + d| \leq 1$. Como $|z| \geq 1$, eso implica que $\mathrm{Im}^2(z) \geq \frac{3}{4}$. Por tanto, $|\mathrm{Im}(cz + d)| = |c||\mathrm{Im}(z)| \geq |c|\sqrt{\frac{3}{4}}$ y por tanto $|c| < 2$. Esto deja las posiblidades $c = 0, c = 1$ y $c = -1$.

Si $c = 0$, entonces, $d = 1$, en cuyo caso $a = 1$ y σ es la translación por b o $d = -1$, en cuyo caso $a = -1$ y σ es la translación por $-b$. Esto implica $b = \pm 1$ y $\mathrm{Re}(z) = \pm\frac{1}{2}$.

Si $c = 1$, entonces, como $|z + d| \leq 1$, dado que $|z + d| = \mathrm{Im}^2(z) + \mathrm{Re}^2(z + d) \geq \frac{3}{4} + \mathrm{Re}^2(z + d)$, debe ocurrir $|\mathrm{Re}(z + d)| \geq \frac{1}{2}$. Esto puede ocurrir en varios casos:

si $d = 0$, en cuyo caso se tiene $|z| \leq 1$ y por tanto $|z| = 1$ y como $ad - cb = 1$, $b = -1$. En ese caso $\sigma z = a - \frac{1}{z}$. Tomando la parte real, se tiene que $\mathrm{Re}(a - \frac{1}{z}) = \mathrm{Re}(a - \frac{\bar{z}}{z\bar{z}}) = \mathrm{Re}(a - z) = \mathrm{Re}(a) - \mathrm{Re}(z)$. Esto implica $a = 0$ excepto si $\mathrm{Re}(z) = \frac{1}{2}$ o si $\mathrm{Re}(z) = -\frac{1}{2}$. En el primer caso $z = -\bar{\rho}$ y por tanto $a = 1$ o $a = 0$. Si $a = 1$, $\sigma = TS$ y $\sigma(-\bar{\rho}) = -\bar{\rho}$ y si $a = 0$, se tiene 2. En el caso $\mathrm{Re}(z) = -\frac{1}{2}$, entonces, $z = \rho$ y $a = -1$ o $a = 0$. Si $a = -1$, entonces $\sigma = (ST)^2$ $\sigma\rho = \rho$ y si $a = 0$ se tiene 2.

Si $d = 1$, entonces $\mathrm{Re}(z) = -\frac{1}{2}$ y por tanto $z = \rho$. Además debe ocurrir $ad - cb = 1$ y por tanto $a = b + 1$. Por esto, $\sigma\rho = \frac{(b+1)\rho+b}{\rho+1} = \frac{b(\rho+1)+\rho}{\rho+1} = b + \frac{\rho}{\rho+1} = b - \bar{\rho}$ y por tanto, para que siga en F, $b = 0$ o $b = -1$. Si $b = 0$, entonces, $\sigma\rho = -\bar{\rho} = \rho + 1$ cumpliendo 2. y si $b = -1$, entonces $\sigma = ST$ y $\sigma\rho = 1$

Si $d = -1$, entonces $\mathrm{Re}\{z\} = \frac{1}{2}$. Análogamente al caso anterior, $z = -\bar{\rho}$ o bien $\sigma = (TS)^2$ y $\sigma(-\bar{\rho}) = -\bar{\rho}$, o bien $\sigma(-\bar{\rho}) = \rho = -\bar{\rho} - 1$.

El caso $c = -1$ traspone al caso $c = 1$ considerando la matriz $-Id\sigma$.

Falta considerar que $\sigma z = z \pm 1$ no da ningún punto fijo, pero $\sigma z = -\frac{1}{z}$ da i como punto fijo en F. Por tanto se ha probado 2. y 3. □

Corolario 3. *F es un dominio fundamental de $SL_2(\mathbb{Z})$*

Como primera aplicación del dominio fundamental se tiene el siguiente resultado:

Proposición 9. *$SL_2(\mathbb{Z})$ está generado como grupo por S, T y $-Id$*

Demostración. Dado $z \in \text{int}F$ y $\sigma \in SL_2(\mathbb{Z})$, entonces, se probó en la proposición anterior que existe un τ en el grupo generado por S y T tal que $\tau\sigma z \in F$. Como $z \in F$, por el segundo apartado de la anterior proposición como z no pertenece a la frontera de F, $z = \tau\sigma z$ y por el apartado 3. eso implica que $\tau\sigma = \pm Id$. Por tanto $\sigma = \pm\tau^{-1}$ y por tanto, está en el grupo generado por S, T y $-Id$. □

Para conocer $\mathbb{H}^*$ se calcularán las cúspides.

Lema 1. *Las cuspides de $SL_2(\mathbb{Z})$ son $\mathbb{Q} \cup \{\infty\}$ y son todas equivalentes.*

Demostración. Si $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, si σ es una transformación parabólica y $s \in \mathbb{R}$ un punto fijo, entonces $cs^2 + (d-a)s - b = 0$. Como sólo hay una solución el discriminante es 0 y por tanto, $s = \frac{a-d}{2c} \in \mathbb{Q}$. Además ∞ es un punto fijo de T y por tanto es una cúspide.

Sólo queda probar que todos los racionales son cúspides para ello, si p y q son enteros coprimos y $s = \frac{p}{q}$, existen enteros λ y β tales que $1 = \lambda p - \beta q$. Si $\sigma = \begin{pmatrix} \lambda & \beta \\ q & p \end{pmatrix}$, entonces $\sigma^{-1}T\sigma s = s$. Para ver que $\sigma^{-1}T\sigma$ es una transformación parabólica, si $r \in \mathbb{R} \cup \{\infty\}$ es tal que $\sigma^{-1}T\sigma r = r$, entonces $T(\sigma r) = \sigma r$, por tanto $\sigma r = \infty$ y eso implica que $s = r$.Se deduce de aquí que $\sigma^{-1}T\sigma$ es una transformación parabólica y entonces s es una cúspide. □

Por el lema 1, $SL_2(\mathbb{Z})/\mathbb{H}^* = SL_2(\mathbb{Z})/\mathbb{H}^* \cup \{\infty\}$. Se tiene una aplicación sobreyectiva y contínua: $F \cup \{\infty\} \to \mathbb{H}^*$. $F \cup \{\infty\}$ es compacto porque si U es un entorno de ∞, entonces $F \setminus U$ es un subconjunto cerrado y acotado de F. Por tanto $SL_2(\mathbb{Z})$ es un grupo Fuchsiano de primer tipo.

2.3. Funciones modulares.

Dada $\sigma \in GL_2(\mathbb{R})$ una matriz con determinante positivo, $k \in \mathbb{Z}$ y $f\colon \mathbb{H} \to \mathbb{C}$, se denota:

$$f \mid [\sigma]_k = \det(\sigma)^{\frac{k}{2}} f(\sigma(z)) j(\sigma, z)^{-k}$$

Se tiene que si $\sigma, \tau \in \Gamma$, entonces:

$$\begin{aligned} f \mid [\tau\sigma] &= \det(\tau\sigma)^{\frac{k}{2}} f(\tau(\sigma(z)))j(\tau\sigma, z)^{-k} \\ &= \det(\sigma)^{\frac{k}{2}}(\det(\tau)^{\frac{k}{2}} f(\tau\sigma(z))j(\tau, \sigma z)^{-k}) \cdot j(\sigma, z)^{-k} \\ &= \det(\sigma)^{\frac{k}{2}} f(\sigma(z)) \mid [\tau]_k j(\sigma, z)^{-k} \\ &= (f(z) \mid [\tau]_k) \mid [\sigma]_k \end{aligned}$$

Definición 19. *Sea k un entero y Γ un grupo Fuchsianos de primer tipo, una función $f\colon \mathbb{H} \to \mathbb{C}$ se llama una* ***forma automorfa de peso k con respecto a*** *Γ si satisface las siguientes condiciones:*

1. *f es meromorfa en $\mathbb{H}$.*
2. *$f \mid [\sigma]_k = f$ para todo $\sigma \in \Gamma$.*
3. *f es meromorfa en las cúspides de Γ.*

Para entender esta definición hay que explicar qué significa que f sea meromorfa en las cúspides de Γ. Primero, si Γ es un subgrupo discreto de $SL_2(\mathbb{R})$, tal y como se prueba en [SH][prop 1.17], si $\Gamma_s = \{\sigma \in \Gamma \mid \sigma s = s\}$, y $\rho \in SL_2(\mathbb{R})$ es tal que $\rho(s) = \infty$, entonces, $\rho\Gamma_s\rho^{-1} \cdot \{\pm Id\}$ es un grupo generado por la matriz $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ para algún h y $\pm Id$. Por 2. se tiene que si $\sigma \in \rho\Gamma_2\rho^{-1}$, y si τ es tal que $\sigma = \rho\tau\rho^{-1}$, entonces:

$$(f \mid [\rho^{-1}]_k) \mid [\sigma]_k = (((f \mid [\rho^{-1}]_k) \mid [\rho]_k) \mid [\tau]_k) \mid [\rho^{-1}]_k = (f \mid [\tau]_k) \mid [\rho^{-1}]_k =$$

$$f \mid [\rho^{-1}]_k$$

Si k es par, entonces $f \mid [\rho^{-1}]_k$ es invariante bajo $z \mapsto z + h$. Por tanto, existe una función meromorfa $\Phi(q)$ en el dominio $0 < |q| < r$ para algún r positivo tal que:

$$f(z) \mid [\rho^{-1}]_k = \Phi(e^{\frac{2\pi i z}{h}})$$

Se dice que f es meromorfa en las cúspides si Φ es meromorfa en 0.

Si k es impar, entonces si $-Id \in \Gamma$, por 2. se tiene que $f = -f$ y por tanto f es 0. Si $-Id \notin \Gamma$, entonces o bien $\rho\Gamma_s\rho^{-1}$ está generado por $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$, en cuyo caso la definición es como en el caso k par o bien $\rho\Gamma_s\rho^{-1}$ está generado por $-\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ y por tanto es invariante bajo $z \mapsto z + 2h$. Así que existe una

función meromorfa $\Phi(q)$ en el dominio $0 < |q| < r$ para algún r positivo tal que:

$$f(z) \mid [\rho^{-1}]_k = \Phi(e^{\frac{\pi i z}{h}})$$

Se dice que f es meromorfa en las cúspides si Φ es meromorfa en 0.

En ambos casos, la función Φ, como es meromorfa en el 0, se puede expandir en series de Laurent alrededor del 0 como $\Phi(q) = \sum_{n \geq n_0} c_n q^n$ para un $n_0 \in \mathbb{Z}$.

Se denotará como $\mathcal{A}(\Gamma)_k$ el conjunto de las formas automorfas de peso k con respecto a Γ. Con la notación de antes denotará $\mathcal{G}(\Gamma)_k$ al conjunto de elementos $f \in \mathcal{A}(\Gamma)_k$ tal que $c_n = 0$ para todo $n < 0$. A los elementos de este conjunto se les llamará **formas íntegras de peso k con respecto a Γ**. Finalmene se denotará $\mathcal{S}(\Gamma)_k$ al conjunto de elementos $f \in \mathcal{A}(\Gamma)_k$ tal que $c_n = 0$ para todo $n \leq 0$ A los elementos de ese conjunto se les llamará **formas cuspidales de peso k con respecto a Γ**. Para cada k, estos conjuntos tienen estructura de espacio vectorial sobre $\mathbb{C}$ y además se cumple que :

- $f \in \mathcal{A}(\Gamma)_k, g \in \mathcal{A}(\Gamma)_{k'}$ implica que $fg \in \mathcal{A}(\Gamma)_{k+k'}$
- $f \in \mathcal{G}(\Gamma)_k, g \in \mathcal{G}(\Gamma)_{k'}$ implica que $fg \in \mathcal{G}(\Gamma)_{k+k'}$
- $f \in \mathcal{S}(\Gamma)_k, g \in \mathcal{S}(\Gamma)_{k'}$ implica que $fg \in \mathcal{S}(\Gamma)_{k+k'}$

Por tanto $\bigoplus_{k\geq 0} \mathcal{A}(\Gamma)_k$, $\bigoplus_{k\geq 0} \mathcal{G}(\Gamma)_k$, y $\bigoplus_{k\geq 0} \mathcal{S}(\Gamma)_k$, tienen estructuras de álgebras graduadas.

Una función $f\colon \mathbb{H} \to \mathbb{C}$ se llama **función modular de peso k** si es una forma automorfa de peso k con respecto a $SL_2(\mathbb{Z})$ y se llama **forma modular** si es una forma íntegra y es holomorfa en todo $\mathbb{H}$.

Como $-Id \in SL_2(\mathbb{Z})$, entonces no hay funciones modulares de peso impar a parte del 0. Para un peso k se tiene un resultado que hace más sencillo comprobar la segunda parte de la definición:

Proposición 10. *Dado $k \in \mathbb{N}$, una función $f\colon \mathbb{H} \to \mathbb{C}$ cumple que $f \mid [\sigma]_{2k} = f$ para todo $\sigma \in SL_2(\mathbb{Z})$ si y sólo si cumple: $f(z+1) = f(z)$ para y $f(-\frac{1}{z}) = z^{2k} f(z)$.*

Demostración. De acuerdo con la proposición 9 $SL_2(\mathbb{Z})$ está generado por S, T y $-Id$. por tanto una función $f\colon \mathbb{H} \to \mathbb{C}$ cumple que $f \mid [\sigma]_{2k} = f$ para todo $\sigma \in SL_2(\mathbb{Z})$ si y sólo si lo cumple para $\sigma = S$, $\sigma = T$ y $\sigma = -Id$. Usando las siguientes identidades, se tiene el siguiente resultado.

$$f \mid [T]_{2k} = f(z+1)$$
$$f \mid [S]_{2k} = z^{-2k} f(-\frac{1}{z})$$
$$f \mid [-Id]_{2k} = (-1)^2 k f(z)$$

□

Usando este resultado, es inmediato comprobar que si $f \in \mathcal{A}(SL_2(\mathbb{Z}))_k$ y $g \in \mathcal{A}(SL_2(\mathbb{Z}))'_k$ con k y k' ambos números naturales pares tales que $k \geq k'$, entonces $\frac{f}{g} \in \mathcal{A}(SL_2(\mathbb{Z}))_{k-k'}$

Esta sección la terminaremos dando ejemplos de algunas formas modulares relevantes. Dado L un retículo sobre $\mathbb{C}$ y $\{w_1, w_2\}$ una base de L tal que $\frac{w_1}{w_2} \in \mathbb{H}$, entonces para un k par, se define:

$$G_k(\Gamma) = G_k(w_1, w_2) = \sum_{w \in L \setminus \{0\}} \frac{1}{w^k}$$

Esta serie es absolutamente convergente para $k \geq 4$ y eso se tiene por el siguiente lema:

Lema 2. *Sea L un retículo, la serie*

$$\sum_{w \in L \setminus \{0\}} \frac{1}{|w|^s}$$

es convergente para $s > 3$.

Demostración. Primero se tiene que:

$$\sum_{w \in L \setminus \{0\}} \frac{1}{|w|^s} = \sum_{(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{|aw_1 + bw_2|^s} \tag{2.5}$$

Para cada natural m define el conjunto $A_m = \{(a,b) \mid a = \pm m \text{ y } |b| \leq m \text{ ó } b = \pm m \text{ y } |a| \leq m\}$. Se tiene que $A_m \cap \mathbb{Z}^2$ tiene $8m$ elementos. Y es compacto. Si se llama $M = \text{mín}\{|aw_1 + bw_2| \mid (a,b) \in A_1\}$ (existe porque A_1 es compacto y la función $(a,b) \mapsto |aw_1 + bw_2|$ es contínua) entonces se tiene que para cada m natural $(a,b) \in A_m$ implica que $|aw_1 + bw_2| = \left|\frac{a}{m} w_1 + \frac{b}{m} w_2\right| m \geq Mm$. Por tanto:

$$\sum_{(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{|aw_1 + bw_2|^s} \leq \sum_{m \in \mathbb{N}} \frac{8m}{(Mm)^s}$$

Como esta última serie converge si $s > 2$, entonces se tiene el resultado.

□

Se define

$$G_k^*(z) = \sum_{(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(az+b)^k}$$

Proposición 11. *Dado un entero par $k \geq 4$ entoces se tiene que para todo $z \in \mathbb{H}$ $G_k^*(z+1) = G_k^*(z)$ y que $G_k^*(-\frac{1}{z}) = z^k G_k^*(z)$*

Demostración. La identidad $G_k^*(z+1) = G_k^*(z)$ se tiene porque:

$$\sum_{(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(az+b)^k} = \sum_{(a,a+b)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(az+a+b)^k} = \sum_{(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(a(z+1)+b)^k}$$

La identidad $G_k^*(-\frac{1}{z}) = z^k G_k^*(z)$ se tiene porque:

$$G_k^*(-\frac{1}{z}) = \sum_{(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(-a\frac{1}{z}+b)^k} = \sum_{(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(a\frac{1}{z}+b)^k}$$

$$= \sum_{(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}} z^k \frac{1}{(a+bz)^k} = z^k \sum_{(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(az+b)^k} = z^k G_k^*(z)$$

. □

Para probar que las funciones G_k^* son formas modulares de peso k faltaría probar que son holomorfas en $\mathbb{H}$, que meromorfa en las cúspides y que es una forma íntegra. Respecto a esto se tienen los siguientes resultados:

Proposición 12. *Para cada número par $k \geq 4$ la función G_k^* es holomorfa en $\mathbb{H}$*

Demostración. Si F es el dominio fundamental de $SL_2(\mathbb{Z})$, dados $a, b \in \mathbb{Z}$ y $z \in F$ tiene que $|az+b|^2 = (az+b)(a\bar{z}+b) = a^2|z|^2 + ab\,\mathrm{Re}(z) + b^2 \geq a^2 - ab + b^2 = (ae^{\frac{2\pi i}{3}}+b)(ae^{2\frac{2\pi i}{3}}+b) = (ae^{\frac{2\pi i}{3}}+b)(ae^{\frac{2\pi \bar{i}}{3}}+b) = \left|ae^{\frac{2\pi i}{3}}+b\right|$. Por eso:

$$\sum_{(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{|az+b|^k} \leq \sum_{(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{\left|ae^{\frac{2\pi i}{3}}+b\right|^k} < \infty$$

Y por tanto G_k^* es holomorfa en F. Para ver que G_k^* es holomorfa en $\mathbb{H}$, dado $z \in \mathbb{H}$ existe un $\sigma \in SL_2(\mathbb{Z})$ tal que $\sigma z \in F$. Como por la proposición 11

$$G(z)_k^* = \det(\sigma)^{\frac{k}{2}} G_k^*(\sigma(z)) j^{-k}(\sigma, z)$$

Entonces, como σ es holomorfa en z y G_k^* en $\sigma(z)$, entonces $G_k^* \circ \sigma$ es holomorfa en z y como $j(\sigma, z)$ es holomorfa en z entonces G_k^* es holomorfa en z y por tanto G_k^* es holomorfa en $\mathbb{H}$

□

Proposición 13. *Se tiene una expansión de Fourier en ∞ de la forma:* $G_k^*(z) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}q^n$ *Siendo* $q = e^{2\pi iz}$ *y* $\sigma_s(n) = \sum_{d|n} d^s$.

Demostración. Se usará la fórmula:

$$\pi\cot\pi z = z^{-1} + \sum_{m=1}^{\infty}(\frac{1}{z+m} + \frac{1}{z-m}) = \sum_{m=-\infty}^{\infty}(z+m)^{-1}$$

Por otro lado se tiene que:

$$\pi\cot\pi z = \pi\frac{\cos\pi z}{\sin\pi z} = \pi\frac{e^{\pi iz}+e^{-\pi iz}}{i^{-1}(e^{\pi iz}-e^{-\pi iz})} = \pi i\frac{e^{\pi iz}}{e^{\pi iz}}\frac{e^{\pi iz}+e^{-\pi iz}}{(e^{\pi iz}-e^{-\pi iz})}$$

$$= \pi i\frac{q+1}{q-1} = \pi i(1-2\sum_{n=0}^{\infty}q^n)$$

Si se igualan las ecuaciones queda:

$$\sum_{m=-\infty}^{\infty}(z+m)^{-1} = \pi i(1-2\sum_{n=0}^{\infty}q^n)$$

Si se deriva $r-1$ veces queda:

$$(-1)^r(r-1)!\sum_{m=-\infty}^{\infty}(z+m)^{-r} = (2\pi i)^r\sum_{n=1}^{\infty}n^{r-1}q^n$$

Efectivamente, porque para $r=1$ se tiene:

$$\frac{\mathrm{d}\sum_{m=-\infty}^{\infty}(z+m)^{-1}}{\mathrm{d}z} = \sum_{m=-\infty}^{\infty}\frac{\mathrm{d}(z+m)^{-1}}{\mathrm{d}z} = -\sum_{m=-\infty}^{\infty}(z+m)^{-2}$$

y

$$\frac{\mathrm{d}\pi i(1-2\sum_{n=0}^{\infty}q^n)}{\mathrm{d}z} = -\pi i2\sum_{n=1}^{\infty}\frac{\mathrm{d}q^n}{\mathrm{d}z} = -2\pi i\sum_{n=1}^{\infty}(2n\pi i)q^n = -(2\pi i)^2\sum_{n=1}^{\infty}nq^n$$

Multiplicando ambas expresiones por -1 e igualandolas se tiene el resultado. Si es cierto para r entonces para $r-1$ se prueba derivando una vez más:

$$\frac{\mathrm{d}(-1)^r(r-1)!\sum_{m=-\infty}^{\infty}(z+m)^{-r}}{\mathrm{d}z} = (-1)^r(r-1)!\sum_{m=-\infty}^{\infty}\frac{\mathrm{d}(z+m)^{-r}}{\mathrm{d}z} =$$

$$(-1)^{(r+1)}r(r-1)!\sum_{m=-\infty}^{\infty}(z+m)^{-r-1} = (-1)^{(r+1)}r!\sum_{m=-\infty}^{\infty}(z+m)^{-r-1}$$

y

$$\frac{\mathrm{d}(2\pi i)^r\sum_{n=1}^{\infty}n^{r-1}q^n}{\mathrm{d}z} = (2\pi i)^r\sum_{n=1}^{\infty}\frac{\mathrm{d}n^{r-1}q^n}{\mathrm{d}z} = (2\pi i)^r\sum_{n=1}^{\infty}2\pi i n^r q^n$$

$$= (2\pi i)^{(r+1)}\sum_{n=1}^{\infty}n^r q^n$$

Entonces, el resultado se obtiene finalmente porque:

$$G_k^*(z) = \sum_{(m,n)\in\mathbb{Z}\setminus\{(0,0)\}}(mz+n)^{-k} = 2\sum_{n=1}^{\infty}n^{-k} + 2\sum_{m=1}^{\infty}\sum_{n=infty}^{\infty}(mz+n)^{-k}$$

$$= 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}n^{k-1}q^{mn} = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{d=1}^{\infty}\sum_{d|n}(\frac{n}{d})^{k-1}q^n$$

$$= 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sum_{d|n}(\frac{n}{d})^{k-1}q^n = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sum_{d|n}d^{k-1}q^n$$

□

Estas tres últimas proposiciones prueban que G_k^* es una forma modular de peso k para cada par $k \geq 4$.

Sabiendo esto, se definen las siguientes formas modulares:

- $g_2(z) = 60G_4^*(z)$

- $g_6(z) = 140G_6^*(z)$
- $\Delta(z) = g_2(z)^3 - 27g_3(z)^2$
- $J(z) = 12^3 \frac{g_2^3(z)}{\Delta(z)}$

Por la estructura de álgebra graduada que se vio antes, es fácil comprobar que Δ es una fórma modular de peso 12. Además como los valores de $\zeta(k)$ son conocidos [IR][Cap 15.] se tiene que $\Delta(\infty) = 0$.

Proposición 14. *J(z) es una forma modular de nivel 1 cuya expansión de Fourier en el infinito es:*

$$J(z) = q^{-1}(1 + \sum_{n=1}^{\infty} c_n q^n)$$

con $c_n \in \mathbb{Z}$

Demostración. Se define $X = \sum_{n=1}^{\infty} \sigma_3(n)q^n$ e $Y = \sum_{n=1}^{\infty} \sigma_5(n)q^n$ donde $\sigma_k(n)$ denota la suma de las potencias k-ésimas de los divisores de n. Con esta notación $g_2(z) = (2\pi)^4(\frac{1}{12} + 20X)$ y $g_3(z) = (2\pi)^6(\frac{1}{216} - \frac{7}{3}Y)$. Por tanto, se tiene que $(2\pi)^{-12}\Delta(z) = (2\pi)^{-12}(g_2(z)^3 - 27g_3(z)^2) = \frac{5X+7Y}{12} + 100X^2 + 20^3X^3 - 3 \cdot 7^2Y^2 = \sum_{n=1}^{\infty} \sum_{d>0, d|n} \frac{5d^3 + 7d^5}{12} q^n + \sum_{n>1}^{\infty} a_n q^n$ donde los $a_n \in \mathbb{Z}$ dado que corresponden a la expansión de $100X^2 + 20^3X^3 - 3 \cdot 7^2Y^2$.

Como $d^5 \equiv d^3 \bmod 12$ y $5 \equiv -7 \bmod 12$, entonces $\frac{5d^3+7d^5}{12}$ es un número entero para cada d. Por tanto $(2\pi)^{-12}\Delta(z) = \sum_{n=1}^{\infty} b_n q^n$ con $b_n \in \mathbb{Z}$ y $b_1 = 1$.

Finalmente, $J(z) = 12^3 \frac{(\frac{1}{12}+20X)^3}{q + \sum_{n=2}^{\infty} b_n q^n} = \frac{\sum_{n=0}^{\infty} a_n q^n}{q + \sum_{n=2}^{\infty} b_n q^n}$ con los a_n y b_n enteros. Por tanto, finalmente se obtiene una serie como la de la proposición.

□

2.4. Dimensiones

En esta sección se calculará la dimensión del espacio vectorial de las formas modulares de peso k para cada $k \geq 0$. Para ello hay que introducir

algunas herramientas. Como las funciones modulares son meromorfas en $\mathbb{H}$, entonces para cada $p \in \mathbb{H}$ existe un único entero n tal que $g(z) = \frac{f(z)}{(z-p)^n}$ es holomorfa en p y además $g(p) \neq 0$. Se define entonces $v_p(f) = n$. Esta función tiene las siguientes propiedades.

Proposición 15. *Dado $p \in \mathbb{H}$ y dos funciones modulares f y g, entonces $v_p(fg) = v_p(f) + v_p(g)$ y $v_p(f+g) \geq \min\{v_p(f), v_p(g)\}$*

Si $p \in \mathbb{H}$, $\sigma \in SL_2(\mathbb{Z})$ y $k > 0$, entonces $v_p(j(\sigma, z)^{-k}) = 0$. Por tanto, si $p \in \mathbb{H}$ y f es una forma modular, entonces $v_p(f \mid [\sigma]_k) = v_{\sigma(p)}(f)$. Por tanto, para cada $p \in SL_2(\mathbb{Z})\backslash\mathbb{H}$ y cada forma modular f se puede definir $v_p(f)$ como el valor de uno de los representantes. Se define $v_\infty(f)$ como el orden de la función Φ que fue definida para ver que f es meromorfa en las cúspides. Para ∞ también se dan los resultados de la proposición 13

Proposición 16. *Dada una función modular f de peso $2k$ no nula, se tiene que:*

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{p \in SL_2(\mathbb{Z})/\mathbb{H}\backslash\{i,\rho\}} v_p(f) = \frac{k}{6}$$

Demostración. Primero hay que probar que esta expresión tiene sentido. Es decir, que el número de polos y ceros es finito. Como f es meromórfa en las cúspides, entonces existe una función Φ meromorfa para $0 < |q| < r$ para algún r con $f(z) = \Phi(q)$ siendo $q = e^{\frac{2\pi i}{z}}$. Como es meromorfa se puede suponer sin pérdida de generalidad que en $0 < |q| < r$ no hay ceros ni polos. Por tanto, f no tiene ni ceros ni polos en $\mathrm{Im}(z) > \frac{1}{2\pi}\log\left(\frac{1}{r}\right)$. Por tanto, todos los ceros y polos deben estar en el conjunto $F \cap \{z \mid \mathrm{Im}(z) \leq \frac{1}{2\pi}\log\left(\frac{1}{r}\right)\}$. Como este conjunto es compacto sólo tiene un número finito de ceros y polos. Por tanto se tiene que la expresión tiene sentido.

Ahora se probará la fórmula. Para ello se consideran dos casos:

Caso 1 Si f no tiene ni ceros ni polos, en el borde de $F \cap \{z \mid \mathrm{Im}(z) \leq \frac{1}{2\pi}\log\left(\frac{1}{r}\right)\}$ excepto quizás i, ρ y $-\bar{\rho}$, entonces, existe un $\epsilon > 0$ tal que en $B(i,\epsilon) \cup B(\rho,\epsilon) \cup B(-\bar{\rho},\epsilon)$ no tiene ceros o polos salvo, quizás, i, ρ y $-\bar{\rho}$. Si se llama Γ al borde de $(F \cap \{z \mid \mathrm{Im}(z) \leq \frac{1}{2\pi}\log\left(\frac{1}{r}\right)\}) \setminus B(i,\epsilon) \cup B(\rho,\epsilon) \cup B(-\bar{\rho},\epsilon)$ recorrido en sentido antihorario, por el teorema de los resíduos se tiene que:

$$\frac{1}{2\pi i}\int_\Gamma \frac{f'}{f} = \sum_{p \in SL_2(\mathbb{Z})/\mathbb{H}\backslash\{i,\rho\}} v_p(f)$$

Por otro lado, si se llama Γ_1, Γ_2 y Γ_3, a la parte de Γ que es entorno de $B(i,\epsilon), B(\rho,\epsilon)$ y $B(-\bar{\rho},\epsilon)$ respectivamente, se llaman Γ_4, Γ_5 y Γ_6 a las rectas que van de $\frac{1}{2}+i\frac{1}{2\pi}\log\left(\frac{1}{r}\right)$ a $-\frac{1}{2}+i\frac{1}{2\pi}\log\left(\frac{1}{r}\right)$, de $-\frac{1}{2}+i\frac{1}{2\pi}\log\left(\frac{1}{r}\right)$ a $\rho+i\epsilon$ y de $-\bar{\rho}+i\epsilon$ a $\frac{1}{2}+i\frac{1}{2\pi}\log\left(\frac{1}{r}\right)$ respectivamente y se llaman Γ_7 a la parte de Γ que cumple $|z|=1$ y tiene parte real negativa y Γ_8 a la que tiene parte real positiva. Entonces:

$$\frac{1}{2\pi i}\int_\Gamma \frac{f'}{f} = \frac{1}{2\pi i}\Big(\int_{\Gamma_1}\frac{f'}{f}+\int_{\Gamma_2}+\frac{f'}{f}\int_{\Gamma_3}+\frac{f'}{f}\int_{\Gamma_4}+\frac{f'}{f}\int_{\Gamma_5}+\frac{f'}{f}\int_{\Gamma_6} +\frac{f'}{f}\int_{\Gamma_7}\frac{f'}{f}+\int_{\Gamma_8}\frac{f'}{f}\Big)$$

Primero se usa que T transforma Γ_5 en $-\Gamma_6$. Como además $f(Tz)=f(z)$, se tiene que

$$\frac{1}{2\pi i}\int_{\Gamma_5}\frac{f'}{f}+\frac{1}{2\pi i}\int_{\Gamma_6}\frac{f'}{f}=0$$

Por otro lado el cambio $q=e^{2\pi i z}$ transforma Γ_4 es un círculo ω en sentido anihorario centrado en el 0. Por tanto,

$$\frac{1}{2\pi i}\int_{\Gamma_4}\frac{f'}{f}=\frac{1}{2\pi i}\int_\omega\frac{\Phi'}{\Phi}=-v_\infty(f)$$

Siendo $f(z)=\Phi(q)$ para $0<|q|<r$.

Si Γ_1 va de B a B', Γ_2 va de C a C' y Γ_3 va de D a D', entonces, la integral de $\frac{1}{2\pi i}\frac{f'}{f}$ en el círculo que contiene el arco Γ_1 es decir, de $\delta B(i,\epsilon)$ es $-v_i(f)$. Por tanto, como el ángulo $B\hat{i}B'=\pi$.

$$\lim_{\epsilon\to 0}\frac{1}{2\pi i}\in_{\Gamma_1}\frac{f'}{f}=-\frac{1}{2}v_i(f)$$

De la misma forma, como el ángulo $C\hat{\rho}C'=\frac{2\pi}{6}$:

$$\lim_{\epsilon\to 0}\frac{1}{2\pi i}\int_{\Gamma_2}\frac{f'}{f}=-\frac{1}{6}v_\rho(f)$$

Y análogamente se hace para probar que

$$\lim_{\epsilon\to 0}\frac{1}{2\pi i}\int_{\Gamma_3}\frac{f'}{f}=-\frac{1}{6}v_\rho(f)$$

Finalmente, se tiene que S transforma Γ_7 en $-\Gamma_8$. Como $f(Sz) = z^{2k}f(z)$, entonces $\frac{f'(Sz)}{f(Sz)} = \frac{2k}{z} + \frac{f'(z)}{f(z)}$. Por tanto:

$$\frac{1}{2\pi i}\int_{\Gamma_7}\frac{f'}{f} + \frac{1}{2\pi i}\int_{\Gamma_8}\frac{f'}{f} = \frac{1}{2\pi i}\int_{\Gamma_2}(\frac{f'(z)}{f(z)} - \frac{f'(S(z))}{f(S(z))} = \frac{1}{2\pi i}\int_{\Gamma_2} -\frac{2k}{z}$$

Y si ϵ tiende a 0, eso tiende a $\frac{k}{6}$.

Sustituyento todo, se tiene la igualdad

Caso 2 Si f tiene un cero o un polo en el borde distinto de i, se puede suponer que la parte real es negativa y entonces, o bien p y Tp están en F o bien p y Sp están en F. Si A es el conjunto de estos polos y ceros p, y A' el conjunto de los Tp y Sp que estén en F con $p \in A$, este resultado se prueba de una forma análoga solo que se usa el borde del conjunto:
$([(F \cup (\bigcup_{p\in A} B(p,\epsilon))) \setminus (\bigcup_{p\in A'} B(A,\epsilon))] \cap \{z \mid \mathrm{Im}(z) \leq \frac{1}{2\pi}\log\left(\frac{1}{r}\right)\}) \setminus B(i,\epsilon) \cup B(\rho,\epsilon) \cup B(-\bar{\rho},\epsilon)$.

□

Dado un k par, se puede definir el homomorfismo $\varphi\colon \mathcal{G}_k(SL_2(\mathbb{Z})) \to \mathbb{C}$ definido como $\varphi(f) = f(\infty)$. Entonces, se tiene que $\mathcal{S}_k(SL_2(\mathbb{Z}))$ es el núcleo y por tanto, $\dim \mathcal{S}_k(SL_2(\mathbb{Z})) \leq \dim \mathcal{G}_k(SL_2(\mathbb{Z})) \leq \dim \mathcal{S}_k(SL_2(\mathbb{Z})) + 1$. Además, si $k \geq 4$, se tiene que $G_k^* \in \mathcal{G}_k(SL_2(\mathbb{Z})) \setminus \mathcal{S}_k(SL_2(\mathbb{Z}))$ y por tanto, si $k > 4$ se tiene que $\mathcal{G}_k(SL_2(\mathbb{Z})) \cong \mathcal{S}_k(SL_2(\mathbb{Z})) \oplus \mathbb{C}G_k^*$. Usando esto y la siguiente proposición se podrá calcular la dimensión de $\mathcal{G}_k(SL_2(\mathbb{Z}))$.

Teorema 5. *1. $\mathcal{G}_k(SL_2(\mathbb{Z})) = \{0\}$ para $k < 0$, $k = 2$ y k impar.*

2. $\dim \mathcal{G}_{2k}(SL_2(\mathbb{Z})) = 1$ para $k = 0, 2, 3, 4$ y 5 y sus generadores son $1, G_4^*, G_6^*, G_8^*$ y G_{10}^* respectivamente. Además $\mathcal{S}_{2k}(SL_2(\mathbb{Z})) = \{0\}$ en estos casos.

3. Multiplicar por Δ define un isomorfismo de $\mathcal{G}_{2k}(SL_2(\mathbb{Z}))$ a $\mathcal{S}_{2k+12}(SL_2(\mathbb{Z}))$

Demostración. Sea $f \in \mathcal{G}_{2k}(SL_2(\mathbb{Z}))$, entonces se tiene que:

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{p\in(SL_2(\mathbb{Z})\setminus\mathbb{H}\setminus)\{i,\rho\}} v_p(f) = \frac{k}{6}$$

Además como f es holomorfa en $\mathbb{H}$ y es una forma íntegra, se tiene que $v_p(f) \geq 0$ para cada $p \in SL_2(\mathbb{Z})\setminus\mathbb{H}^*$. Por tanto, no hay formas modulares

de peso par negativo. Igualmente, si $k = 1$, se debe tener que para algún $p \in SL_2(\mathbb{Z})\backslash\mathbb{H}^*$, $v_p(f) \geq 1$. Eso significa que si f es una forma modular de peso 2 $v_p(f) > \frac{1}{2}v_p(f) > \frac{1}{3}v_p(f) \geq \frac{1}{3}$. Por tanto,

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{p\in(SL_2(\mathbb{Z})\backslash\mathbb{H})\backslash\{i,\rho\}} v_p(f) \geq \frac{1}{3} > \frac{1}{6}$$

Y por tanto no hay formas modulares de peso 2. Esto prueba 1.

Como la única forma de escribir $a + \frac{1}{2}b + \frac{1}{3}c + d = \frac{2}{6}$ con números enteros positivos es con $a = 0, b = 0, c = 1$ y $d = 0$, entonces, como G_4^* es una fórma modular de peso 4, se tiene que $v_p(G_6^*) = 1$ si $p = \rho$ y $v_p(G_6^*) = 0$ en otro caso.

De la misma forma, como la única forma de escribir $a + \frac{1}{2}b + \frac{1}{3}c + d = \frac{3}{6}$ con números enteros positivos es con $a = 0, b = 1, c = 1$ y $d = 0$, entonces, como G_6^* es una fórma modular de peso 6, se tiene que $v_p(G_6^*) = 1$ si $p = i$ y $v_p(G_6^*) = 0$ en otro caso.

De esta forma, se tiene que $G_4^*(i) \neq 0$ y $G_6^*(i) = 0$. Por tanto, se tiene que $\Delta(i) = (60G_4^*(i))^3 - 27(140G_6^*(i))^2 = (60G_4^*(i))^3 \neq 0$. Por tanto Δ es no nula. Como tiene peso 12, debe cumplir:

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{p\in(SL_2(\mathbb{Z})\backslash\mathbb{H})\backslash\{i,\rho\}} v_p(f) = 1$$

Como $v_\infty(\Delta) \geq 1$, entonces, debe ocurrir que $v_p(\Delta) = 0$ si $p \neq \infty$ y $v_\infty(\Delta) = 1$. Eso implica que $\Delta(z) \neq 0$ para todo $z \in \mathbb{H}$.

La función $f \to f\Delta$ que va de $\mathcal{G}_{2k}(SL_2(\mathbb{Z}))$ en $\mathcal{S}_{2k+12}(SL_2(\mathbb{Z}))$ está bien definida porque $v_\infty(f\Delta) = v_\infty(f) + v_\infty(\Delta) = v_\infty(\Delta)$. Para ver que es biyectiva se construye una inversa. Se usa que $\frac{f}{\Delta}$ es una función modular que es holomorfa en $\mathbb{H}$ por ser cociente de una función holomorfa por una función holomorfa sin ceros en $\mathbb{H}$, y $v_\infty(\frac{f}{\Delta}) = v_\infty(f) - v_\infty(\Delta) = v_\infty(f) - 1$. Como $f \in \mathcal{S}_{2k}(SL_2(\mathbb{Z}))$ entonces $v_\infty(f) \geq 1$ y por tanto $v_\infty(\frac{f}{\Delta}) \geq 0$ por lo que la función $f \to \frac{f}{\Delta}$ va de $\mathcal{S}_{2k+12}(SL_2(\mathbb{Z}))$ a $\mathcal{G}_{2k}(SL_2(\mathbb{Z}))$ y es la inversa. Esto prueba 3.

Para probar 2. Se usa:

$\mathcal{G}_k(SL_2(\mathbb{Z})) \cong \mathcal{S}_k(SL_2(\mathbb{Z})) \oplus \mathbb{C}G_k^*$

Y se usa que para $k = 0, 2, 3, 4, 5$, $\mathcal{G}_{2k-12}(SL_2(\mathbb{Z})) = \{0\}$. Entonces, aplicando 1. y 3. se tiene 2.

□

Corolario 4. *Si* $k \equiv 1$ *mod* 6 *y* $k \geq 0$, *entonces* $\dim \mathcal{G}_{2k}(SL_2(\mathbb{Z})) = \left\lfloor \frac{k}{6} \right\rfloor$ *y si* $k \not\equiv 1$ *mod* 6 *y* $k \geq 0$ *entonces* $\dim \mathcal{G}_{2k}(SL_2(\mathbb{Z})) = \left\lfloor \frac{k}{6} \right\rfloor + 1$.

Capítulo 3

Curvas elípticas.

3.1. Divisores.

Una curva elíptica sobre un cuerpo K es una variedad proyectiva no singular de género 1, con un punto base. El primer objetivo de este capítulo será definir qué significa el género de una curva. Para ello, comenzaremos introduciendo los divisores.

En este capítulo, al referirnos a una curva proyectiva nos referiremos siempre a una curva irreducible. Dada una curva proyectiva C sobre un cuerpo K, se define el **grupo de divisores** de C como el gupo libre generado por los puntos de P y se denota como $Div(C)$. Así mismo un **divisor** de C es un elemento $D \in Div(C)$ y se puede escribir de la forma $D = \sum_{P \in C} n_P P$ con $n_P \in \mathbb{Z}$ y $n_P = 0$ excepto para una cantidad finita de $P \in C$. En este caso, se denota $v_P(D) = n_P$ y $\deg(D) = \sum_{P \in C} n_P$. Además, se denota $D \geq 0$ si $n_P \geq 0$ para todo $P \in C$. Finalmente, dados dos divisores A y B, se denota $A \geq B$ si $A - B \geq 0$, es decir, si $v_P(A) \geq v_P(B)$ para todo P.

Si K es un cuerpo algebraicamente cerrado C una curva y $P \in C$, se denota como $\mathcal{O}_{C,P}$ al anillo local de C en P y $K(C)$ al cuerpo de funciones racionales de C. Si P es regular, entonces $\mathcal{O}_{C,P}$ es íntegramente cerrado y su cuerpo de fracciones es $K(C)$. Como además es un anillo local, entonces tiene factorización única de ideales.

Si M_P es el ideal maximal de $\mathcal{O}_{C,P}$, entonces, análogamente a como se hizo en el capítulo 1, para cada $f \in \mathcal{O}_{C,P}$, se puede definir $v_P(f) = \mathrm{ord}_{M_P}(f)$. Por tanto, si $f \in K(C)^*$, se puede definir el divisor asociado a f como $\mathrm{div}(f) = \sum_{P \in C} v_P(f) P$.

Proposición 17. *Dada una curva elíptica C y $f \in K(C)^*$, entonces:*

1. *div*$(f) = 0$ *si y sólo si* $f \in K^*$
2. $\deg(div(f)) = 0$

Demostración. 1. Esto ocurre porque si $\text{div}(f) = 0$ entonces no tiene polos y por tanto es una función regular. Las funciones racionales de una variedad proyectiva irreducible son sobreyectivas o constantes y por tanto, deben tener algún cero.

La otra implicación es trivial.

2. [SIL, Prop 3.1]

□

3.2. Diferenciales y teorema de Riemman-Roch

Definición 20. *Dada una curva* C *y un* $K(C)$*-espacio vectorial* Ω_C *de dimensión* 1 *junto con un homomorfismo:*

$$d\colon K(C) \to \Omega_C$$

que cumple:

- $d(fg) = fd(g) + gd(f)$ *para todo* $f, g \in K(C)$
- $d(f) = 0$ *si y sólo si* $f \in K$.

Se llama a Ω_C*,* ***espacio de formas diferenciales (meromorfas)*** *en* C *y a sus elementos* ***formas diferenciales (meromorfas) (de grado 1)*** *en* C.

Se puede notar que dada $f \in K(C)$ no constante, $\Omega_C = K(C) \cdot d(f)$ y por tanto, toda forma diferencial $\omega \in \Omega_C$, se puede escribir como $\omega = hd(f)$ con $h \in K(C)$. Por tanto, para cada forma diferencial ω y $f \in K(C)$ no constante (i.e. $div(f) \neq 0$), $\frac{\omega}{d(f)} \in K(C)$ está bien definido.

Se pueden definir los divisores de las formas diferenciales definiendo para cada $\omega \in \Omega_C$, y $P \in C$, $v_P(\omega) = v_P(\frac{\omega}{df})$ para un f tal que $v_P(f) = 1$. Entonces $div(\omega) = \sum_{P \in C} v_p(\omega)$.

Esto está bien definido porque si $f, g \in K(C)$ cumplen que $v_P(f) = v_P(g) = 1$, como $\mathcal{O}_{C,P}$ es un anillo de Dedekind y anillo local, entonces es dominio de ideales principales [DL, Prop 2.7., cap 3]. Por tanto, existe h con $v_P(h) = 0$ tal que $g = hf$. Por tanto: $d(g) = hd(f) + fd(h)$ y por esto, $\frac{d(g)}{d(f)} = h + f\frac{d(h)}{d(g)}$. Como $h(P) \neq 0$ y $f(P) = 0$, entonces, $\frac{d(g)}{d(f)} \neq 0$ y eso implica que $v_P(\frac{d(g)}{d(f)}) = 0$.

Definición 21. *Dada $D \in Div(C)$, se define el conjunto:*
$L(D) = \{f \in K(C)^* \mid div(f) \geq -D\} \cup \{0\}$
El conjunto $L(D)$ tiene estructura de espacio vectorial y tiene dimensión finita [SIL, prop 5.2., cap 2]. Se denota a su dimensión como $l(D)$

Finalmente, se tiene el siguiente teorema que se puede usar como la definición del género:

Teorema 6 (Riemman-Roch)**.** *Sea C una curva no singular. ω una forma diferencial no nula C. $K_C = div(\omega)$. Existe un entero $g \geq 0$ llamado el* ***género*** *que cumple que para todo $D \in Div(C)$:*

$$l(D) - l(K_C - D) = \deg D - g - 1$$

.

Demostración. [RH, Thm 1.3., cap 4] □

3.3. Curvas elípticas.

Ya entendemos la definición de curva elíptica, y ahora toca empezar a manipularlas. Dada una curva elípica C, si denotamos O como el punto base, entonces, por el teorema de Riemman-Roch, se tiene que $l(nO) = n$. Eligiendo dos funciones $x, y \in K(C)$ y otra tales que $\{1, x\}$ es una base de $L(2O)$ y $\{1, x, y\}$ es una base de $L(3O)$, se puede comprobar que $L(6O)$ contiene las funciones $1, x, y, x^2, xy, y^2, x^3$.

Como $L(6O)$ tiene dimensión 6, entonces, existen $A_1, ..., A_7 \in K$ tales que:

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0$$

.

Entonces, existe un isomorfismo de C a la curva en $\mathbb{P}^2_k$ definida por la ecuación anterior homogeneizada. Dado por $\phi = [x, y, 1]$ y $\phi(O) = [0 : 1 : 0]$. Finalmente, si K no tiene característica 2 o 3, tras unos cambios de variables se puede probar que toda curva elíptica es isomorfa a una curva proyectiva de ecuación:

$$y^2z = 4x^3 - g_2xz^2 - g_3z^3$$

Con $g_2, g_3 \in K$ tales que $\Delta = g_2^3 - 27g_3^2 \neq 0$ (Δ se llamará el **discriminante** de C). Todo esto está detallado en [SIL][Cap III]. Se elige entonces

como punto base el punto $[0:1:0]$. Además, por comodidad, normalmente se escribirá la ecuación en su forma afín como:

$$y^2 = 4x^3 - g_2x - g_3$$

Las curvas que nos interesan estarán definidas sobre $\mathbb{C}$. Este dominio, nos permite estudiar la estructura de grupo de las curvas elípticas de una forma muy visual. Para ello, se usará un **retículo** L sobre $\mathbb{C}$ generado por ω_1 y ω_2. Se usará a partir de ahora la notación $L = [\omega_1, \omega_2]$. Dado un retículo L, se puede definir el toro complejo $\mathbb{C}/L$. Este toro tiene una estructura natural de grupo derivada de la estructura de grupo de $\mathbb{C}$ con la suma. Veremos cómo esta estructura puede dotar de estructura de grupo a las curvas elípticas y además veremos cómo se pueden estudiar los morfismos entre curvas elípticas gracias a esto.

Definición 22. *Una función elíptica con respecto al retículo L es una función meromorfa sobre $\mathbb{C}$ tal que $f(z+\omega) = f(z)$ para todo $\omega \in L$ y todo $z \in \mathbb{C}$.*

Se debe notar que si $L = [\omega_1, \omega_2]$, entonces, f es una función elíptica si y sólo si $f(z+\omega_1) = f(z+\omega_2) = f(z)$ para todo $z \in \mathbb{C}$.

Definición 23. *Dado un retículo L, se define la función $\wp$* ***de Weierstrass*** *relativa a L como:*

$$\wp(z; L) = \frac{1}{z^2} + \sum_{0 \neq \omega \in L} \Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \Big)$$

Si se sobrentiende el retículo sólo se denotará $\wp(z)$

De la definición es fácil comprobar que $\wp$ es una función elíptica. Además, su derivada es:

$$\wp'(z) = \sum_{\omega \in L} \frac{1}{(z-\omega)^3}$$

Que también es una función elíptica. Usando que $\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \sum_{n=1}^{\infty} (n+1) \frac{z^n}{\omega^{n+2}}$ se puede obtener la siguiente expresión de $\wp$:

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2}(L) z^{2n}$$

Proposición 18. *Dado un retículo L, se tiene que:*

$$\wp'(z) = 4\wp(z)^3 - 60G_4(L)\wp(z) - 140G_6(L)$$

Demostración. Se define la función $f(z) = \wp'(z) - 4\wp(z)^3 + 60G_4(L)\wp(z) + 140G_6(L)$. Por ser suma de funciones elípticas, esta es una función elíptica. Además dado que:

$$\wp(z)^3 = \frac{1}{z^6} - 24G_4(L)\frac{1}{z^2} - 80G_6(L) + ...$$
$$\wp(z) = \frac{1}{z^2} + ...$$
$$\wp'(z)^2 = -\frac{4}{z^6} - 24G_4(L)\frac{1}{z^2} - 80G_6(L)...$$

Se tiene que f es holomorfa y $f(0) = 0$. Como f es una función elíptica, entonces $f(\omega) = 0$ para todo $\omega \in L$ por tanto f es la función nula. □

Esta proposición nos da pistas para pensar que la función $\wp$ parametriza una curva elíptica. Sin embargo, para que eso sea cierto, la curva debe ser no singular. Para probar esto, se tiene el siguiente resultado:

Proposición 19. *Dado un retículo L, sean $g_2 = 60G_4(L)$ y $g_3 = 80G_6(L)$, el polinómio:*

$$4x^3 - g_2x - g_3$$

tiene raices distintas.

Demostración. Para probar este resultado, se elige una base ω_1, ω_2 de L y se nota que $\wp'$ es una función impar y elíptica. Como $\wp$ es impar, si se denota $\omega_3 = \omega_1 + \omega_2$ se tiene que para cada $i = 1, 2, 3$:

$\wp'(\frac{\omega_i}{2}) = -\wp'(-\frac{\omega_i}{2}) = -\wp'(\frac{\omega_i}{2})$

Por tanto, $\wp'(\frac{\omega_i}{2}) = 0$ y por tanto, cada $\wp(\frac{\omega_i}{2})$ es un cero del polinómio. Se considera la función elíptica:

$$\wp(x) - \wp(\frac{\omega_i}{2})$$

Como es una función elíptica, tal que en el paralelogramo fundamental $P = \{-\frac{\omega_1}{2+\epsilon} - \frac{\omega_2}{2+\epsilon} + t_1\omega_1 + t_2\omega_2 \mid 0 \leq t_1, t_2 \leq 1\}$ (con un $\epsilon > 0$ tal que $\epsilon \in P$ y el único punto del retículo es 0) sólo tiene un polo de orden 2 (dado que sólo tiene polos de orden 2 en los puntos del retículo), eso significa que sólo puede tener dos ceros en P_i. Estos dos ceros son para $x = \frac{\omega_i}{2}$ y para $x = -\frac{\omega_i}{2}$. Por tanto, $\wp(\frac{\omega_i}{2}) \neq \wp(\frac{\omega_j}{2})$.

□

Este resultado implica que el discriminante es distinto de cero y por tanto, que la curva no sigular (por [DL, Lema 2.6., cap 2] teniendo en cuenta que Δ es el resultante de $4x^3 - g_2x - g_3$ y su derivada) por tanto la curva el elíptica.

Para probar que dados g_2 y g_3 tales que $g_2^3 - 27g_3^2 \neq 0$ existe un retículo L tal que la curva

$$\wp'(z;L) = 4\wp(z)^3 - g_2\wp(z;L) - g_3$$

se necesita el siguiente lema:

Lema 3. *La aplicación $j\colon SL_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}$ es una biyección.*

Demostración. Usando la proposición 16 se tiene que:

$$v_\infty(J-c) + \frac{1}{2}v_i(J-c) + \frac{1}{3}v_\rho(J-c) + \sum_{p\in SL_2(\mathbb{Z})/\mathbb{H}\setminus\{i,\rho\}} v_p(J-c) = 0$$

Como $J - c$ tiene un polo simple en el infinito, se tiene que:

$$\frac{1}{2}v_i(J-c) + \frac{1}{3}v_\rho(J-c) + \sum_{p\in SL_2(\mathbb{Z})/\mathbb{H}\setminus\{i,\rho\}} v_p(J-c) = 1$$

Esto implica que $J(z) - c = 0$ para algún z. Por tanto, existe z tal que $J(z) = 12^3\frac{g_2^3}{g_2^3-27g_3^2}$. □

Se definen ahora para un retículo $g_2(L) = 60G_4(L)$ y $g_3(L) = 140G_6(L)$. Por tanto, se tiene que si $L = [\omega z, \omega]$, $g_2(L) = \omega^{-4}g_2(z)$ y $g_3(L) = \omega^{-6}g_3(z)$. Entonces:

- si $g_2 = 0$, enotonces $J(z) = 0$ y por tanto $g_2(z) = 0$. Se elige ω tal que $\omega^{-6}g_3(z) = g_3$ y entonces, $L = [\omega z, \omega]$ funciona.
- si $c_2 \neq 0$, se elige ω tal que si $j(z) = 12^3\frac{g_2^3}{g_2^3-27g_3^2}$ $\omega^{-4}g_2(z) = g_2$ y por tanto se tiene que $12^3\frac{g_2}{g_2^3-27g_3^2} = j(z) = 12^3\frac{g_2(z)^3}{g_2(z)^3-27g_3(z)^2} = \frac{(\omega^{-4}g_2(z))^3}{(\omega^{-4}g_2(z))^3-27(\omega^6g_3(z))^2}$. Por tanto se tiene que $\omega^6g_3(z) = g_3$ y por tanto, $L = [\omega z, \omega]$ funciona.

Por tanto, todas las curvas elípticas en forma de Weierstrass se pueden parametrizar a partir de un toro complejo.

Con la notación de la proposición 16, está claro que si E es la curva definida por la ecuación $y^2 = 4x^3 - g_2x - g_3$ la aplicación $\phi\colon \mathbb{C}/L \to E$ definida como $\phi(z) = (\wp(z), \wp'(z))$ si $z \neq 0$ y $\phi(0) = [0:1:0]$ está bien definida:

Se puede comprobar que es sobreyeciva porque si $(x, y) \in E$, se puede considerar la función elíptica $\wp(z) - x$. Como no es constante, debe tener un cero. Si z_0 alcanza un cero en esta función entonces por la proposición 16 debe ocurrir que $\wp'(z_0)^2 = y^2$. Como $\wp'$ es impar, entonces, o bien $\wp'(z_0) = y$ o bien $\wp'(-z_0) = y$.

La función también es inyectiva dado que si $\phi(z_1) = \phi(z_2)$, entonces, la función $\wp(z) - \wp(z_1)$ es una función elíptica de orden 2 que tiene como ceros $z_1, -z_1$ y z_2. Por tener orden 2, tiene que tener como mucho dos ceros diferentes en $\mathbb{C}/L$ contando multiplicidad. Entonces, si $2z_1 \notin L$, se tiene que $z_1 \not\equiv -z_1 \bmod L$ y por tanto, $z_2 \equiv \pm z_1 \bmod L$. Si $z_2 \equiv -z_1 \bmod L$, entonces $\wp'(z_1) = \wp'(z_2) = \wp(-z_1) = -\wp(z_1)$ y por tanto, $\wp(z_1) = 0$, pero eso implica que $z_1 \equiv \frac{\omega_1}{2}, \frac{\omega_2}{2}$ ó $\frac{\omega_3}{2}$. Pero entoces $z_1 \equiv -z_1 \bmod L$. En el caso en el que $2z_1 \in L$, entonces, se tiene que z_1 es un cero doble de $\wp(z) - \wp(z_1)$ (se puede comprobar con la serie de Laurent) por tanto, debe ocurrir que $z_2 \equiv z_1 \bmod L$.

Que ϕ sea biyectiva permite darle a E una estructura de grupo de forma que $\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$.

3.4. Ordenes e isogenias.

En este capítulo nos centraremos en estudiar los morfismos de curvas elípticas, en concreto de aquellas definidas sobre $\mathbb{C}$ (en este capítulo todas las curvas serán así), y esto se empezará a relacionar con los anillos de enteros vía la multiplicación compleja.

Definición 24. *Sean E_1 y E_2 dos curvas elípticas, se dice que un morfismo $\phi\colon E_1 \to E_2$ es una isogenia si $\phi(0) = 0$.*

Se denota como $\mathrm{Hom}(E_1, E_2)$ al conjunto de isogenias de E_1 a E_2. Se define la suma de isogenias como $(\phi+\psi)(P) = \phi(P)+\psi(P)$ y así se convierte a $\mathrm{Hom}(E_1, E_2)$ en un grupo. Se denotará también $\mathrm{End}(E) = \mathrm{Hom}(E, E)$. En este caso, se pueden componer isogenias. Se denotará $\phi\psi = \phi \circ \psi$. Con esta operación $\mathrm{End}(E)$ es un anillo.

Definición 25. *Dada una curva elíptica E, se dice que tiene multiplicación compleja si $End(E) \ncong \mathbb{Z}$*

Un resultado importante es que todas las isogenias son homorfismos de grupos para la suma definida anteriormente. [SIL][Thm III4.8]

Las isogénias se pueden relacionar con los retículos gracias al siguiente teorema:

Teorema 7. *Dados dos retículos L_1 y L_2 y sean E_1 y E_2 sus curvas elípticas correspondientes, entonces existe una biyección entre el conjunto de $\alpha \in \mathbb{C}$ tales que $\alpha L_1 \subseteq L_2$ y las isogénias de E_1 a E_2*

Demostración. [SIL, Thm 4.1., cap 4] □

Definición 26. *Dado un cuerpo de números cuadrático imaginario K, un orden es un subanillo de K que contiene a $\mathbb{Z}$ y es un $\mathbb{Z}$-módulo de rango 2. Para un cuerpo de números algebráicos en general K, se puede dar la misma definición de orden pidiendo que sea un $\mathbb{Z}$-módulo de rango $[K : \mathbb{Q}]$.*

Dado un orden $\mathfrak{a}$, y dado $x \in \mathfrak{a}$, como $\mathfrak{a}$ es un $\mathbb{Z}$-módulo finítamente generado tal que $x\mathfrak{a} \subseteq \mathfrak{a}$, entonces, x es íntegro sobre $\mathbb{Z}$ y por tanto, todo orden está contenido en el anillo de enteros del cuerpo. Además, por ser un $\mathbb{Z}$-módulo de orden $[K : \mathbb{Q}]$, su cuerpo de fracciones debe ser K.

Si el orden $\mathfrak{a}$ se define sobre un cuerpo cuadrático imaginario K, entonces se puede considerar como un retículo. Por tanto, se tiene que $\mathrm{End}(\mathbb{C}/\mathfrak{a}) \cong \{x \in \mathbb{C} \mid x\mathfrak{a} \subseteq a\}$. Como $\mathfrak{a}$ está contenido en K, entonces se tiene que $\mathrm{End}(\mathbb{C}/\mathfrak{a}) \cong \{x \in K \mid x\mathfrak{a} \subseteq \mathfrak{a}\}$. Finalmente, como $\mathfrak{a} \subseteq \{x \in K \mid x\mathfrak{a} \subseteq \mathfrak{a}\} \subseteq K$, entonces, $\mathrm{End}_{\mathbb{Q}}(\mathbb{C}/\mathfrak{a}) := \mathrm{End}(\mathbb{C}/\mathfrak{a}) \otimes \mathbb{Q} \cong K$ y además la curva asociada a $\mathbb{C}/\mathfrak{a}$ tiene multiplicación compleja.

Definición 27. *Dado un $\mathbb{Z}$-submódulo $\mathfrak{a}$ de K, se dice que es un $\mathfrak{o}-$ideal própio si $\mathfrak{o} = \{\lambda \in K \mid \lambda\mathfrak{a} \supseteq \mathfrak{a}\}$.*

Proposición 20. *Sea E una curva elíptica tal que $End_{\mathbb{Q}}(E) \cong K$, entonces, sea $\mathfrak{o}$ el orden correspondiente a $End(E)$, se tiene que existe un $\mathfrak{o}$-ideal propio $\mathfrak{a}$ tal que $End(E) \cong End(\mathbb{C}/\mathfrak{a})$. Además, dado cualquier $\mathfrak{o}-$ideal propio $\mathfrak{a}$, $End(\mathbb{C}/\mathfrak{a})$ es isomorfo a $\mathfrak{o}$. Finalmente, dado dos ordenes $\mathfrak{a}$ y $\mathfrak{b}$, $\mathbb{C}/\mathfrak{a}$ es isomorfa a $\mathbb{C}/\mathfrak{b}$ si y sólo si existe $\mu \in K^\times$ tal que $\mathfrak{a} = \mu\mathfrak{b}$.*

Demostración. Lo primero que se probará es que $\mathfrak{o}$ no depende de la elección de isomorfismo. Esto ocurre porque si $\alpha \in \mathfrak{o}$, entonces, $\bar{\alpha} \in \mathfrak{o}$. Por tanto, no depende de la elección de isomorfismo. Como E es una curva elíptica, entonces, existe un orden $\mathfrak{a}$ tal que E es isomorfa a $\mathrm{End}(\mathbb{C}/\mathfrak{a})$. Como se vio antes, $\mathrm{End}(\mathbb{C}/\mathfrak{a}) \cong \{x \in K \mid x\mathfrak{a} \subseteq \mathfrak{a}\}$. Como $\mathfrak{o}$ no depende de isomorfismos debe ocurrir que $\mathfrak{a}$ es un ideal propio de $\mathfrak{o}$.

Que dado cualquier $\mathfrak{o}-$ideal propio $\mathfrak{a}$, $\mathrm{End}(\mathbb{C}/\mathfrak{a})$ es isomorfo a $\mathfrak{o}$, es evidente de la definición de ideal propio.

□

Corolario 5. *Dadas dos curvas elípticas E y E', si E tiene multiplicación compleja, entonces E' es isomorfa a E si y sólo si $End(E)$ es isomorfo a $End(E')$.*

Corolario 6. *Dado un orden $\mathfrak{o}$ de K, el número de clases de $\mathfrak{o}$-ideales propios es igual al número de clases de isomorfismos de curvas elípticas tal que End(E) $\cong \mathfrak{o}$.*

[SH, Prop 4.9 y 4.10]

3.5. Propiedades del J invariante.

Se probó que $J(z)$ tiene una expansión de la forma:

$$J(z) = q^{-1}(1 + \sum_{n=1}^{\infty} c_n q^n)$$

Donde los c_n son números enteros. Esta función permitirá encontrar una relación entre la teoría algebráica de números y las curvas elípticas. Para ver esto, primero se considera una curva E en forma de Weierstrass.

$$E : y^2 = 4x^3 - g_2 x - g_3$$

A partir de esta curva, se puede definir el J-invariante como:

$$J_E = 12^3 \frac{g_2^3}{\Delta}$$

Proposición 21. *Si $E : y^2 = 4x^3 - g_2 x - g_3$ y $E' : y^2 = 4x^2 - g_2' x - g_3'$ son curvas isomorfas entonces existe un número μ tal que $g_2' = \mu^4 g_2$ y $g_3' = \mu^6 g_3$. Además, si dos curvas tienen el mismo J-invariante, entonces, son isomorfas.*

Demostración. [SIL, Prop 1.4., cap 3] □

Como consecuencia de esta proposición se tiene que dos curvas elípticas son isomorfas si y sólo si tienen el mismo J-invariante. Si $\sigma \in \mathrm{Aut}(\mathbb{C})$, dada la curva E definida como antes, se puede definir E^σ como la curva definida por la ecuación $y^2 = x^3 - \sigma(g_2)x - \sigma(g_3)$. Está claro que $\sigma(J_E) = J_{E^\sigma}$. Por tanto, E y E^σ son isomorfas si y sólo si σ es la identidad en $\mathbb{Q}(J)$.

Dada una curva elíptica E, existe una curva elíptica isomorfa que se puede parametrizar con la función $\wp$ de Weierstrass a partir de un retículo L generado por 1 y un $z \in \mathbb{C}$, teniendo $g_2 = 60G_4(L) = 60G_4(z)$ y $g_3 = 80G_6(L) = 80G_6(z)$. Entonces, $J_E = J(z)$. Conociendo esto, se enunciará la primera proposición que relaciona $J(z)$ con la teoría algebráica de números.

Proposición 22. *Si z pertenece a un cuerpo cuadrático imaginario de números, entonces $J(z)$ es un número algebráico.*

Demostración. Lo primero que hay que notar es que dado un cuerpo cuadrático imaginario, el número de clases de isomorfismos de curvas elípticas es numerable dado que el número de ordenes posible es numerable y por el corolario 6 hay un número finito de clases de isomorfismos con un anillo de endomorfismos isomorfo a cada orden. Como además, dado $\sigma \in \mathrm{Aut}(\mathbb{C})$ si E es isomorfa a E^σ si y sólo si $\sigma(J_E) = J_E$, se tiene que $\{\sigma(J(E)) \mid \sigma \in \mathrm{Aut}(\mathbb{C})\}$ es numerable.

Para terminar la prueba se usarán el siguiente lema:

Lema 4. *Si $\alpha \in \mathbb{C}$ es trascendente, entonces, $\{\sigma(\alpha) \mid \sigma \in Aut(\mathbb{C})\}$ es no numerable.*

Demostración. Para probar esto, se dirá que $A \subseteq \mathbb{C}$ es una base de trascendencia de $\mathbb{C}$ sobre $\mathbb{Q}$ si A es un conjunto algebraicamente independiente sobre $\mathbb{Q}$ y $\mathbb{C}$ es una extensión algebraica de $\mathbb{Q}(A)$. Si existe tal base A, como $\mathbb{C}$ es no numerable, entonces, A debe ser no numerable.

Por [JM, Thm 9.9] existe una base de trascendencia A de $\mathbb{C}$ sobre $\mathbb{Q}$ que contiene a α. Finalmente, dado $\beta \in A$ y una permutación τ de A tal que $\tau(\alpha) = \beta$, τ se puede extender a un homomorfismo $\sigma\colon \mathbb{Q}[A] \to \mathbb{Q}[A]$. Este homomorfismo se puede extender a un homomorfismo entre los cuerpos de fracciones y finalmente a la clausura algebraica. Por tanto, $A \subseteq \{\sigma(\alpha) \mid \sigma \in \mathrm{Aut}(\mathbb{C})\}$ y por esto $\{\sigma(\alpha) \mid \sigma \in \mathrm{Aut}(\mathbb{C})\}$ no es numerable.

□

□

En lo que queda de capítulo, lo dedicaremos a ampliar este resultado hasta llegar al hecho de que $J(z)$, si z pertenece a un cuerpo cuadrático imaginario, es un entero algebraico.

Proposición 23. *Dados $m \in \mathbb{N}$, $n_0 \in \mathbb{Z}$, $\{a_k \in \mathbb{C}\}_{k=0}^m$ y $\{b_n \in \mathbb{C}\}_{n \geq n_0}$, si:*

$$\sum_{k=0}^{m} a_k J(z)^k = \sum_{n \geq n_0} b_n q^n$$

Entonces cada a_k pertenece a $\mathbb{Z}[\{b_n\}_{n \geq n_0}]$.

Demostración. Sustituyendo $J(z)$ por $q^{-1}(1+\sum_{n=1}^{\infty} c_n q^n)$ se tiene que $a_k J(z)^k = a_k q^{-k} + a_k \sum_{n=0}^{\infty} d_n q^n$ con $d_n \in \mathbb{Z}$. Por tanto para cada $k = 0, ..., m$ se tiene que:

$$b_k = a_k + q(a_{k+1}, ..., a_m)$$

Con $q \in \mathbb{Z}[x_{k+1}, ..., x_m]$. Por tanto, $a_m = b_m$ y si $a_k \in \mathbb{Z}[\{b_n\}_{n \geq n_0}$ para $k = k_0, ..., m$, entonces $a_{k_0} = b_{k_0} - q(a_{k_0+1}, ..., a_m) \in \mathbb{Z}[\{b_n\}_{n \geq n_0}]$. □

Para llegar al resultado, se necesitará una proposición algo más técnica que dice lo siguiente:

Proposición 24. *Si* $\Gamma = SL_2(\mathbb{Z})$*, dado* $n \in \mathbb{N}$*,* $\Gamma \cdot \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \cdot \Gamma = \bigcup_{\alpha \in A} \Gamma\alpha$ *donde* A *es el conjunto de matrices* $\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ *con* $d > 0$*,* $ad = n$*,* $0 \leq b < d$ *y* $\gcd(a, b, d) = 1$*.*

Demostración. [SH, Prop 3.36] □

Dado un número natural n, dado A como en la proposición, se considera el polinomio:

$$F_n(X, J) = \prod_{\alpha \in A} (X - J \circ \alpha) = \sum_{m=0}^{M} s_m X^m$$

Donde cada s_m es una función simetrica en las variables $J \circ \alpha$ con $\alpha \in A$. Si $\gamma \in \Gamma$, usando la proposición 24 se puede deducir que $\bigcup_{\alpha \in A} \Gamma\alpha = \bigcup_{\alpha \in A} \Gamma\alpha\gamma$. De aquí se puede deducir que $\{J \circ \alpha \mid \alpha \in A\} = \{J \circ \alpha \circ \gamma \mid \alpha \in A\}$. Finalmente, se puede deducir que $s_m \circ \gamma = s_m$. Por tanto, cada s_m es una función modular de peso 1. Por $J(z)$ es holomorfa en $\mathbb{H}$. por tanto, para cada m s_m es holomorfa en $\mathbb{H}$, por tanto, $s_m = S_m(J)$, siendo S_m un polinómio. Se quiere probar que S_m tiene coeficientes enteros racionales, para ello, se verá que la q-expansión de s_m tiene coeficientes pertenecientes a $\mathbb{Z}$ y se usará la proposición 23.

Dado $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in A$, se tiene que:

$$J(\alpha(z)) = \zeta_d^{-b} q^{-\frac{a}{d}} (1 + \sum_{m=0}^{\infty} c_m \zeta_d^{mb} q^{\frac{a}{d}})$$

Por tanto, los coeficientes son enteros en $\mathbb{Q}(\zeta_n)$ y en concreto, los coeficientes de s_m son enteros en $\mathbb{Q}(\zeta_n)$. Falta probar que los coeficientes pertenecen a $\mathbb{Q}$. Para probar esto, se elegirá $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ y se verá que fija los coeficientes. Dado $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, $\sigma(\zeta_n) = \zeta_n^l$ con $\gcd(l, n) = 1$. Por tanto:

$$\sigma(\zeta_d^{-b})q^{-\frac{a}{d}}(1+\sum_{m=0}^{\infty}\sigma(c_m\zeta_d^{mb})q^{\frac{a}{d}}) = \zeta_d^{-lb}q^{-\frac{a}{d}}(1+\sum_{m=0}^{\infty}c_m\zeta_d^{lmb}q^{\frac{a}{d}}) = J\circ\beta$$

Donde $\beta = \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix} \in A$ siendo $b' \equiv bl \bmod d$. Aplicar σ a los coeficientes, por tanto, lo que hace es permutar los elementos de A, así que si se aplica σ a los coeficientes de $F(X,J)$, no cambia nada y por tanto, si se aplica σ a los coeficientes de s_m, no los cambia. Por tanto, sus coeficientes son racionales. De aquí, aplicando la proposición 23 se obtiene que $S_m(J)$ tiene coeficientes enteros. Finalmente, de aquí se consigue que $F_n(X,J) \in \mathbb{Z}[X,J]$.

Se considera ahora $H_n(J) = F_n(J,J)$. Está claro que $H_n \in \mathbb{Z}[J]$. Como el objetivo era probar que si z pertenece a un cuerpo de números cuadrático e imaginario, $J(z)$ es un entero algebráico, lo que nos quedaría probar es que el coeficiente lider de H_n es ± 1 y que $H_n(J(z)) = 0$. Encontrar el coeficiente lider es fácil dado que para $\alpha \in A$, el coeficiente lider de $J - J\circ\alpha$ es una raiz de la unidad. Por tanto, el coeficiente lider de H_n es una raiz de la unidad. Como se ha probado que es racional, entonces es ± 1.

Para probar que si $K = \mathbb{Q}(z)$ es un cuerpo cuadrático imaginario $H_n(J(z)) = 0$, lo que se hará es elegir $\mathfrak{o} = End(\mathbb{C}/L)$. Se separará la prueba en dos casos:

caso 1: Si $\mathfrak{o}$ es un orden maximal, entonces existe un $\mu \in \mathfrak{o}$ tal que $N_{K/Q}(\mu) = n$ es libre de cuadrados mayor que 1. Efectivamente, si $K = \mathbb{Q}(\sqrt{-m})$ con m libre de cuadrados y $m > 1$, $\mu = \sqrt{-m}$ y si $K = \mathbb{Q}(i)$, $\mu = 1 + i$.

Si η una matriz con coeficientes en $\mathbb{Z}$ tal que $\mu\begin{pmatrix} z \\ 1 \end{pmatrix} = \eta\begin{pmatrix} z \\ 1 \end{pmatrix}$ que efectivamente existe porque si $m > 1$, $\eta = \begin{pmatrix} 0 & -m \\ 1 & 0 \end{pmatrix}$ y si $m = 1$, $\eta = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ estas matrices cumplen que $\det(\eta) = n$ es libre de cuadrados, por tanto, el máximo común divisor de los coeficientes es 1. Por tanto, existe $\alpha \in A$ tal que $J\circ\alpha = J\circ\eta$. Como $\eta(z) = z$, entonces $J(\alpha(z)) = J(z)$ y por tanto $H_n(J(z)) = 0$. Por tanto, en este caso, z es un entero.

caso 2: Si $\mathfrak{o}$ no es el orden maximal, para reducirnos al caso anterior sólo hay que tener en cuenta que si $J(z)$ es íntegro sobre un anillo compuesto por enteros algebráicos, entonces $J(z)$ es íntegro. Por tanto, si existe un z' tal que $End(\mathbb{C}/L')$ es un orden maximal y $J(z)$ es íntegro sobre $J(z')$ entonces es un entero algebráico por el caso anterior.Por [SH, Prop 4.3]

existe un $\beta \in GL_2^+(\mathbb{Q})$ tal que $End(\mathbb{C}/L')$ es el orden maximal siendo L' el retículo generado por $\beta(z)$ y 1. $J(z)$ es íntegro sobre $\mathbb{Z}[J(\beta(z)]$ por la siguiente proposición.:

Proposición 25. *Para cualquier $\beta \in GL_2(\mathbb{Q})$ con determinante positivo, $J \circ \beta$ es íntegro sobre $\mathbb{Z}[J]$*

Demostración. Como multiplicar la matriz por un número no cambia la transformación, se puede suponer que β es primitiva. Si tiene determinante igual a $n > 1$, entonces $\beta \in \Gamma\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}\Gamma$. Por esto, se tiene que existe un $\alpha \in A$ tal que $\Gamma\beta = \Gamma\alpha$.Por tanto, $J \circ \beta = J \circ \alpha$ y por tanto $F_n(J \circ \beta, J) = 0$. □

Aplicando el resultado en $z = \beta^{-1}(z)$ queda probado.

Capítulo 4

Construcción de cuerpos de clase.

El objetivo de este capítulo será aplicar las herramientas que se vieron en los capítulos anteriores para resolver el problema duodécimo de Hilbert en el caso particular de los cuerpo cuadráticos imaginarios.

4.1. Isomorfismo normalizado.

Dada un cuerpo cuadrático e imaginario de números K, existe una curva elíptica E tal que $\mathrm{End}_{\mathbb{Q}}(E) \cong K$. Como son extensiones isomorfas de dimensión 2 de $\mathbb{Q}$, existen dos isomorfismos posibles, esta sección se concentrará en encontrar un isomorfismo canónico.

Dada una curva proyectiva no singular V, se define $D(V)$ como el subconjunto de los elementos $\omega \in \Omega_V$ tal que $\mathrm{div}(\omega) \geq 0$. Los elementos de $D(V)$ se llaman **formas holomorfas** (En el capítulo anterior a este espacio vectorial se le llamaba $L(0)$). Como se vio en el pasado capítulo, si $f \in K(V)$ es no constante, dada $\omega \in D(V)$, se tiene que existe $h \in K(V)$ $\omega = hd(f)$.

Se consideran dos curvas proyectivas no singulares V y W sobre un cuerpo K y un morfismo $\phi\colon V \to W$. Dada $\omega \in \Omega_W$, si $\omega = hd(f)$ con $h, f \in K(W)$, se puede definir $\omega \circ \phi = (h \circ \phi)d(f \circ \phi) \in \Omega_V$.

Se considera una curva E sobre $\mathbb{C}$ tal que $\mathrm{End}_{\mathbb{Q}}(E)$ es isomorfo a un cuerpo cuadrático imaginario K. Por la proposición 17 se puede probar que $D(E)$ es isomorfo a $\mathbb{C}$ como espacio vectorial dado que si $\omega = hd(f) \in D(E)$, entonces, como $deg(div(h)) = 0$, se tiene que $div(h) \geq 0$ si y sólo si $div(h) = 0$ y esto ocurre si y sólo si $h \in \mathbb{C}$. La prueba está completa teniendo en cuenta que $div(\omega) = div(h)$. Dado $\omega = hd(f) \in D(E)$ y $\alpha \in \mathrm{End}(E)$, como $h \in \mathbb{C}$, $h \circ \alpha = h$ y por tanto $\omega \circ \alpha \in D(E)$. Como $D(E)$ es un $\mathbb{C}$ espacio vectorial

de dimensión 1, existe $\mu_\alpha \in \mathbb{C}$ tal que $\omega \circ \alpha = \mu_\alpha \omega$. Si L es el retículo tal que E es isomorfa a $\mathbb{C}/L$, dado $\mu \in K$, si α se corresponde con el morfismo $u \to \mu u$, entonces $cd(u) \circ \alpha = cd(\mu u) = \mu cd(u)$. Por tanto, si $\omega \in D(E)$, se tiene que $\omega \circ \alpha = \mu\omega$. Con todo esto, se puede definir el isomorfismo θ como el isomorfismo que cumple $\omega \circ \theta(\mu) = \mu(\omega)$. Se dirá que la pareja (E, θ) está **normalizada**.

Un teorema fundamental para la prueba de este caso particular es el teorema fundamental de multiplicación compleja en curvas elípticas. Para enunciarlo, se considerará una pareja normalizada (E, θ). Sea K el cuerpo cuadrático imaginario isomorfo a $\mathrm{End}(E)$, se puede encontrar un orden $\mathfrak{a}$ de K tal que E es isomorfo a $\mathbb{C}/\mathfrak{a}$.Se elige un isomorfismo ξ de $\mathbb{C}/\mathfrak{a}$ en E. Dado $s \in J_K$, dado que para $K \subset L \subset F$ se tiene que $\rho_{F/K}(s) \mid_L = \rho_{L/K}(s)$, se puede definir $[s, K] \in Gal(K_{ab}/K)$ (siendo K_{ab} la extensión abeliana maximal de K) como el automorfismo tal que $[s, K] \mid_L = \rho_{L/K}(s)$ para cada extensión abeliana L de K. El teorema fundamental de multiplicación compleja en curvas elípticas dice lo siguiente.

Teorema 8. *Sean $K, (E, \theta)$, $\mathfrak{a}$ y ξ como antes, y dado un automorfismo de $\mathbb{C}$ sobre K, y $s \in J_K$ tal que $\sigma = [s, K]$ en K_{ab} . Entonces, existe un isormofismo*

$$\xi' \colon K/s^{-1}\mathfrak{a} \to E^\sigma$$

tal que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\ \xi\ } & E \\ {\scriptstyle s^{-1}}\downarrow & & \downarrow{\scriptstyle \sigma} \\ K/s^{-1}\mathfrak{a} & \xrightarrow{\ \xi'\ } & E^\sigma \end{array}$$

Demostración. Para probar esto, primero hay que reducir el caso a cuando $End(E) = \theta(\mathcal{O}_K)$. Luego, a base de reducir módulo pprimo, se obtiene un isomorfismo $\xi'' \colon \mathbb{C}/s^{-1}\mathfrak{a} \to E^\sigma$ tal que $\xi(v)^\sigma = \xi''(s^{-1}v)$ para cada $v \in n^{-1}\mathfrak{a}/\mathfrak{a}$. A partir de aquí se obtiene que $\xi'' = \theta^\sigma(\zeta) \circ \xi'$ para un cierto ξ' que se ha fijado antes y lo que queda probar es que $\zeta = 1$ para que $\xi'' = \xi'$. Los detalles se encuentran en [SH, Prop 5.4] □

4.2. Construcción de la extensión abeliana maximal.

Esta será la última sección de la memoria y lo que se hará será finalmente dar la solución particular al duodécimo problema de Hilbert.

Si se denota $j(\mathfrak{a})$ al invariante de una curva isomorfa a $\mathbb{C}/\mathfrak{a}$, entonces, por el teorema fundamental de multiplicación compleja, se tiene que usando la misma notación que en el teorema $j(\mathfrak{a})^\sigma = j(s^{-1}\mathfrak{a})$. Por tanto, como $j(\mathfrak{a})$ sólo depende de la restricción a K_{ab}, $j(\mathfrak{a}) \in K_{ab}$. Se definirán tres clases de curvas elípticas para ello, hay que notar que si E es una curva con multiplicación compleja y $End(E) \cong \mathfrak{o}$, se tiene que el grupo de automorfismos es isomorfo a $\mathfrak{o}^\times$. Como $\mathfrak{o}$ es un orden de un cuerpo cuadrático imaginario, está contenido en su anillo de enteros donde las posibles unidades son conocidas y son menos que 6 siempre. Además, si $x \in \mathfrak{o}^\times$, entonces $-x \in \mathfrak{o}$. Por tanto, el número de automorfismos es par. Así que una curva elíptica puede tener $2, 4$ o 6 automorfismos. Se dirá que la curva es de clase ϵ_i si tiene $2i$ automorfismos. El teorema que terminará de resolver el problema es el siguiente:

Teorema 9. *Sean $K, E, \mathfrak{a}$ y ξ como se notó en el teorema fundamental de multiplicación compleja, sean:*

- $h_E^1(x, y) = x\frac{c_2 c_3}{\Delta}$
- $h_E^2(x, y) = x^2\frac{c_2^2}{\Delta}$
- $h_E^3(x, y) = x^3\frac{c_3}{\Delta}$

Sea $u \in K/\mathfrak{a}$ y $W = \{s \in J_K \mid s\mathfrak{a} = \mathfrak{a}, su = u\}$ Si E pertenece a la clase ϵ_i, entonces, $K(j_E, h_E^i(\xi(u)))$ es la extensión que corresponde al subgrupo abierto $K^\times W$ de J_K

Demostración. Se elige $\sigma \in Aut(\mathbb{C}/K)$. Dado $s \in J_A$ tal que $\sigma = [s, K]$ en K_{ab}. Se elige entonces ξ' como en el teorema fundamental de multiplicación compleja. Entonces:

Si σ actúa como la identidad en la extensión F correspondiente a $K^\times W$, por la definición de F, se tiene que se puede elegir un $s \in W$, entonces $j(s\mathfrak{a}) = j(\mathfrak{a})$ y por tanto, E es isomorfa a E^σ y por tanto $j_E = j_E^\sigma$. Además, dado un isomorfismo ϵ de E^σ a E tal que $\epsilon \circ \xi' = \xi$, si se define $t = \xi(u)$ entonces se tiene que $h_E^i(\epsilon t^\sigma) = h_{E^\sigma}^i(t^\sigma) = h_E^i(t)^\sigma$. Esto se puede comprobar simplemente sustituyendo en las expresiones de los h^i

Como $\epsilon(t^\sigma) = \epsilon(\xi(u)^\sigma) = \epsilon(\xi'(s^{-1}u)) = \xi(u) = t$, entonces se tiene que $h_E^i(\epsilon t^\sigma) = h_E^i(t)^\sigma$. Por tanto, σ actúa como la identidad sobre $K(j_E, h_E^i(\xi(u)))$ y por tanto, $K(j_E, h_E^i(\xi(u))) \subseteq F$.

Por otro lado, si σ actúa como la identidad en $K(j_E, h_E^i(\xi(u)))$, se tiene que $j(E) = j(E)^\sigma = j(E^\sigma)$. Por tanto, E y E^σ son curvas isomofas. Dado un isomorfismo δ de E^σ a E, existe un elemento $\mu \in K^\times$ tal que $\mu s^{-1}\mathfrak{a} = \mathfrak{a}$ (proposición 20). Se puede elegir entonces un δ tal que el diagrama siguiente es conmutativo:

$$\begin{array}{ccccc} \mathbb{C} & \longrightarrow & \mathbb{C}/s^{-1}\mathfrak{a} & \xrightarrow{\xi'} & E^{\sigma} \\ {\scriptstyle\mu}\downarrow & & \downarrow & & \downarrow{\scriptstyle\delta} \\ \mathbb{C} & \longrightarrow & \mathbb{C}/\mathfrak{a} & \xrightarrow{\xi} & E \end{array}$$

Se tiene que $h_E^i(\delta t^\sigma) = h_{E^\sigma}^i(t^\sigma) = h_E^i(t)^\sigma = h_E^i(t)$. Por tanto, por existe un elemento $\zeta \in K$ tal que $\zeta\mathfrak{a} = \mathfrak{a}$ y $\theta(\zeta)\delta(t^\sigma) = t$ (hay que notar que por esto $\zeta\mu s^{-1}\mathfrak{a} = \mathfrak{a}$). Por otro lado $\delta(t^\sigma) = \delta(\xi(u)^\sigma) = \delta(\xi'(s^{-1}u)) = \xi(\mu s^{-1}u)$. Por tanto, $t = \xi(u) = \xi(\zeta\mu s^{-1}u)$. Por la inyectividad de ξ, se tiene que $\zeta\mu s^{-1}u = u$. Por tanto, se tiene que $\zeta\mu s^{-1} \in W$ y por esto $s \in K^\times W$. Por tanto $\sigma = Id$ en F. Por tanto se tiene que $F \subseteq K(J_E, h_E^i(t))$. □

Este teorema unido al hecho de que J_K es la unión de los subgrupos $K^\times W$ prueba que si E es una curva elíptica que pertenece a ϵ_i, entonces K_{ab} es la extensión de K generada por J_E y los $h_E^i(t)$ donde los t son los puntos de E de orden finito.

Bibliografía

[NC] Nancy Childress. *Class Field Theory.* Oxford University Press. 2009.

[SH] Goro Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton paperbacks. 1971.

[SE] J-P.Serre.*A course in arithmetics*Springer. 1973.

[MI] Toshitsune Miyake.*Modular Forms*.Springer. 1989.

[DL] Dino Lorenzini *An Invitation to Arithmetic Geometry.* American Mathematical Society. 1996.

[IR] Kenneth Ireland, Michael Rosen. *A Classical Introduction to Modern Number Theory.* Springer. 1982.

[CF] J.W.S.Cassels y A.Fölich. *Algebraic Number Theory.* London Mathematical Society. 1967.

[BS] Z.I.Borevich y I.R. Shafarevich. *Number Theory.* Academic Press Inc. 1966.

[SIL] Joseph H. Silverman. *The Arithmetics of Elliptic Curves.* Springer. 1986.

[RH] Robin Hartshorne *Algebraic Geometry* Springer. 1977.

[COX] David A. Cox *Primes of the form* $x^2 + ny^2$ Wiley. 1989.

[RL] R.C.Langland. *Some contemporary problems with origins in the Jugendtraum.* Mathematical Developments arising from Hilbert's problems. American Mathematical Society, Providence R.I.1976.

[JM] J.S.Milne. *Fields and Galois Theory* `https://jmilne.org/math/CourseNotes/FT.pdf`

[AD] Alberto Daza Garcia. *Dominios de Dedekind, factorización de ideales y aplicaciones.* https://idus.us.es/xmlui/bitstream/handle/11441/77507/Daza%20Garc%c3%ada%20Alberto%20TFG.pdf?sequence=1&isAllowed=y.