El Grupo Modular

Subgrupos, espacios de órbitas y generalización.

escrito por

ÁLVARO NOEL JIMÉNEZ HUEDO

Tutor: Francisco Javier Cirre

Facultad de Ciencias
UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA

Trabajo presentado para la obtención del título de
Máster Universitario en Matemáticas Avanzadas de la UNED.
Especialidad Geometría y Topología

SEPTIEMBRE 2018

Abstract

Abstract en español:

En este trabajo se aborda el estudio del grupo modular y su generalización como grupo de Hecke. Tras una introducción para establecer el marco teórico relacionado con superficies de Riemann y el grupo $PSL_2(\mathbb{R})$, se define el grupo modular, así como la presentación del grupo en términos de generadores y relaciones, y se estudia su región fundamental. En el núcleo del documento se aborda la descripción de sus subgrupos normales, en especial los subgrupos de congruencia, y se describen las superficies de Riemann que aparecen como espacio de órbitas por la acción de los subgrupos normales más relevantes sobre el semiplano superior complejo. En la última parte del trabajo, se definen los grupos de Hecke y se estudian sus propiedades y subgrupos de mayor importancia, para terminar estableciendo la relación con el grupo modular.

Abstract in English:

The aim of this document is to review the modular group and understand it as a Hecke group. After a preview about Riemann surfaces and the $PSL_2(\mathbb{R})$ group, the modular group is defined and also a presentation in terms of generators and relators is given, ending with a discussion about the fundamental region. In the core of the document, normal subgroups are described, specially the congruence groups and the quotient space caused by the action of the most important subgroups over the upper-half plane. Finally, the modular group is extended to the concept of Hecke group and its properties and main subgroups are briefly studied.

Keywords: Superficie de Riemann; grupo modular; grupo de Hecke

Dedicatoria y agradecimientos

A mis alumnos de Secundaria y Bachillerato, cuya implicación en las Matemáticas, su inconformismo y, a veces, exceso de inquietud, me han contagiado para seguir investigando.

Este trabajo no hubiera sido posible sin el ánimo que me han dado mi familia, mis amigos y mi pareja, así como sin la guía y supervisión de mi tutor, Francisco Javier Cirre.

Tabla de Contenidos

Página

ÍNDICE DE CUADROS

Índice de figuras

Figura **Página**

CAPÍTULO 1

INTRODUCCIÓN

La geometría hiperbólica es, sin lugar a dudas, uno de los campos de investigación más fructíferos de la matemática moderna del último siglo. El desarrollo de métodos aritmético-geométricos para estudiar el plano complejo y el efecto de distintas transformaciones sobre él ha hecho que se entrelacen resultados y técnicas de Análisis Complejo, Teoría de Grupos, Teoría de Números y Topología Algebraica. De este modo, es complicado abordar un estudio profundo en este campo sin requerir maquinaria teórica de todas los campos mencionados.

Como transformaciones en el plano complejo, destacan las transformaciones de Möbius, cuyas caracterísitcas y efectos geométricos han sido ampliamente estudiados. Las restricciones a las que estén sujetos los coeficientes de estas transformaciones determinan el efecto de las mismas sobre el plano. Así, parece evidente que si elegimos coeficientes enteros, necesitaremos resultados de la Teoría de Números para realizar un estudio profundo de estos grupos de transformaciones. Añadiendo restricciones a los coeficientes, entramos al estudio de los distintos subgrupos, que pueden ser o no subgrupos normales, finitos o infinitos, con lo que necesitamos resultados de la Teoría de Grupos que iremos introduciendo según se requiera.

La acción de los distintos grupos de transformaciones sobre el plano complejo, que restringiremos al semiplano superior, genera mediante identificación de los elementos de las distintas clases de equivalencia (que llamaremos *órbitas*) superficies orientables que pueden ser dotadas de una *estructura compleja*, teniendo así el carácter de superficie de Riemann. El estudio de estas superficies incluye conceptos como el *género*, la *característica de Euler* o el *grupo fundamental* que provienen de la Topología Algebraica.

En concreto, en este trabajo nos centraremos en el estudio del *grupo modular*, partiendo de un enfoque como grupo de matrices de 2×2 con entradas enteras y determinante unidad, grupo al que denotaremos $SL_2(\mathbb{Z})$, y asociando después transformaciones de Möbius a las matrices de

este grupo, con lo que hablaremos del grupo $PSL_2(\mathbb{Z})$. Estudiaremos la relación entre ambos grupos modulares, así como entre el índice de los subgrupos desde ambos enfoques, a partir de numerosos resultados de T. Miyake y B. Schoeneberg. Revisaremos con especial atención los subgrupos normales del grupo modular, basándonos en los estudios de M. Newman y R. Fricke, entre otros, y recogeremos algunas de las cuestiones que aún están parcialmente abiertas, y en cuya respuesta han trabajado grandes matemáticos como M. Knopp e I. Reiner. Tras un pequeño guiño a la Criptografía, nos centraremos en el estudio de las superficies de Riemann como espacios de órbitas del grupo modular y algunos de sus subgrupos en el semiplano superior, y estableceremos isomorfismos con grupos de simetrías conocidos gracias a los trabajos de F. Klein, G. Jones y D. Singerman. Como inicio a trabajos futuros, estudiaremos los grupos de Hecke como generalización del grupo modular y revisaremos, con menor profundidad, sus subgrupos normales más importantes, tendiendo puentes con la Teoría de Grafos, y la relación con las superficies de Riemann más conocidas, tomando recientes publicaciones de I. N. Cangül y E. Hecke.

En conclusión, este trabajo pretende ubicar al grupo modular en una posición accesible desde distintas ramas de las Matemáticas, y con el objetivo principal de servir de guía base para el estudio del grupo, o bien desde un enfoque puramente consultivo, ya que si bien existen multitud de publicaciones sobre el tema es complicado unificar sus objetivos, resultados e incluso notación, o bien desde un enfoque investigador para continuar con trabajos futuros. Por otra parte, en este trabajo no se aborda la teoría de funciones automórficas y formas modulares, que supone otro amplio campo de estudio en el que varios de los autores consultados presentan publicaciones, como T. Miyake y B. Schoeneberg, y que permite conectar esta teoría con cuestiones recientes como la *hipótesis de Riemann* y los trabajos de Ramanujan. Con todo ello, iniciemos el camino.

1.1. Superficies de Riemann

En esta primera sección introductoria, recogemos tanto la definición de superficie de Riemann como varios resultados relevantes, tomando como fuente principalmente los trabajos de G. A. Jones y D. Singerman (ver [44]) y de R. Miranda (ver [28]). El objetivo de estos preliminares es introducir el concepto de superficie de Riemann para, en capítulos posteriores, referirnos a ellas desde la perspectiva del estudio del grupo modular, utilizando si es necesario algunos de los resultados que se van a exponer. Fue Riemann el que introdujera este concepto en su tesis doctoral *Foundations for a General Theory of Functions of a Complex Variable* en el año 1851 desde un marcado enfoque topológico, como una forma de visualizar las llamadas *funciones multivaluadas*. Durante el siglo XIX, y más especialmente durante la segunda mitad del siglo, la teoría de superficies de Riemann fue ampliamente desarrollada en forma de importantes resultados, aunque la falta de maquinaria analítica de la época demandó las futuras aportaciones de otros matemáticos como Weierstrass para dotar de rigor a las principales demostraciones. A este respecto, otros grandes matemáticos como F. Klein o H. Weyl publicaron libros en los que

dotaban de un carácter analítico a la teoría de superficies de Riemann, durante la primera mitad del siglo XX. El concepto general de *superficie* es previo al que nos atañe:

Definicion 1.1. (Superficie) Una superficie S es un espacio topológico Hausdorff[1] en el que cada punto $s \in S$ tiene un entorno abierto homeomorfo a un abierto del plano $\mathbb{R}^2$ (o $\mathbb{C}$).

Dado un recubrimiento de S por conjuntos abiertos U_i, existen homeomorfismos

$$\phi_i : U_i \longrightarrow W_i \in \mathbb{C}$$

que dotan a las superficies de las mismas características topológicas que el plano. Así, el par (U_i, ϕ_i) se denomina *carta*, siendo los puntos $p_i = \phi_i(s)$ *coordenadas locales* para el punto $s \in S$. La familia de cartas se denomina *atlas*, y se denota como $\mathscr{A} = \{U_i, \phi_i\}$. En este sentido, dos atlas $\mathscr{A} = \{U_i, \phi_i\}$ y $\mathscr{B} = \{V_i, \psi_i\}$ son *compatibles* si los *cambios de coordenadas* $\psi_i \circ \phi_j^{-1}$ son *analíticos* en el sentido clásico, y esta compatibilidad es una *relación de equivalencia* cuyas clases dotan a la superficie S de una *estructura compleja*. Así, podemos introducir el concepto central de la sección:

Definicion 1.2. (Superficie de Riemann) Una superficie de Riemann S es una superficie dotada de una estructura compleja.

Como ejemplos principales a los que aludiremos con frecuencia, se tienen el plano complejo $\mathbb{C}$, la *esfera de Riemann* $\Sigma = \mathbb{C} \cup \{\infty\}$ o el toro complejo $\mathbb{T} \cong \mathbb{C}/\Omega$, siendo Ω un *retículo* en el plano complejo. Recordemos la definición de *retículo*:

Definicion 1.3. (Retículo) Un *retículo* Ω es un grupo discreto tal que, dados dos números complejos $\omega_1, \omega_2 \neq 0$ tales que $\omega_1/\omega_2 \notin \mathbb{R}$, puede definirse como

$$\mathscr{L} = \left\{ \; m\omega_1 + n\omega_2 \;\middle|\; m, n \in \mathbb{Z} \; \right\}.$$

En particular, dado un complejo $z \in \mathbb{C}$, el conjunto

$$\Omega(z) = \left\{ \; cz + d \;\middle|\; c, d \in \mathbb{Z} \; \right\}$$

es un retículo.

El carácter analítico de una función entre superficies de Riemann

$$f : S_1 \longrightarrow S_2$$

depende de qué superficies relacione:

Proposicion 1.1. *Sea $f : S_1 \longrightarrow S_2$ una función entre superficies de Riemann, se tiene que:*

[1] Un espacio topológico X es *Hausdorff* si para cualquier par de puntos distintos p, q existen entornos abiertos V_p, V_q disjuntos.

- $f : S_1 \longrightarrow \mathbb{C}$ *es analítica si para toda carta* (U, ϕ) *la aplicación* $f \circ \phi^{-1} : \phi(U) \longrightarrow \mathbb{C}$ *es analítica en el sentido clásico.*
- $f : \mathbb{C} \longrightarrow \mathbb{C}$ *es analítica si lo es en el sentido tradicional.*
- $f : \Sigma \longrightarrow \mathbb{C}$ *es analítica si* f *lo es en todo* $z \in \mathbb{C}$ *y* $f(1/z)$ *lo es en* $z = 0$.

Con esta base, podemos definir el concepto de *función holomorfa entre superficies de Riemann*:

Definicion 1.4. (Función holomorfa) Una función $f : S_1 \longrightarrow S_2$ es *holomorfa* si la composición

$$\phi_2 \circ f \circ \phi_1^{-1} : \phi_1\left(U_1 \cap f^{-1}(U_2)\right) \longrightarrow \mathbb{C}$$

lo es, para toda carta $\left(U_1, \phi_1\right)$ en S_1 y $\left(U_2, \phi_2\right)$ en S_2.

Como consecuencia, cualquier función $f : S_1 \longrightarrow S_2 \subseteq \mathbb{C}$ es holomorfa si y sólo si es analítica. Un atlas es *orientable* si sus cambios de coordenadas preservan la orientación, esto es, si los *jacobianos* J_i cumplen $J_i \geq 0$. Así, como una función analítica cumple las *ecuaciones de Cauchy-Riemann*, es inmediato comprobar que toda función analítica preserva la orientación. Como consecuencia, *toda superficie de Riemann es orientable*, y las dos orientaciones posibles vienen dadas por la clase de compatibilidad de atlas $[\mathscr{A}]$ y su conjugada $\left[\overline{\mathscr{A}}\right]$.

Existe un importante teorema que clasifica todas las posibles superficies simplemente conexas, esto es, las que tienen grupo fundamental trivial. Veamos antes una definición que alude a cuándo dos superficies pueden considerarse *la misma*.

Definicion 1.5. (Transformación conforme) Una función $f : S_1 \longrightarrow S_2$ es una *transformación conforme* si es holomorfa y además es un homeomorfismo. En ese caso, se dice que S_1 y S_2 son *conformemente equivalentes*, y se denota de la manera usual $S_1 \cong S_2$[2].

Por ejemplo, es fácil ver que el *disco abierto unidad* $\mathscr{D}$ y el *semiplano superior hiperbólico*

$$\mathscr{U} = \left\{ \; z \in \mathbb{C} \;\middle|\; \mathrm{Im}(z) > 0 \; \right\}$$

son conformemente equivalentes por la transformación conforme

$$f(z) = \frac{z - i}{z + i}.$$

El *Teorema de Uniformización* (F. Klein, H. Poincaré y P. Koebe), cuya prueba puede consultarse en [3], se enuncia como sigue:

Teorema 1.1. *(Teorema de Uniformización) Toda superficie de Riemann simplemente conexa es conformemente equivalente a una única de las siguientes:*

[2]En algunos textos se dice que S_1 y S_2 son isomorfas, o simplemente que son homeomorfas por la función holomorfa f.

- *La esfera de Riemann* Σ.
- *El plano complejo* $\mathbb{C}$.
- *El semiplano superior* $\mathscr{U}$ *(o al disco abierto unidad* $\mathscr{D}$*).*

Una consecuencia de este teorema es la clasificación de los *grupos de automorfismos* de una superficie,

$$\mathrm{Aut}(S) = \left\{ \; f : S \longrightarrow S \;\middle|\; f \text{ es una transformación conforme} \; \right\},$$

que exponemos en el siguiente teorema (ver demostración en [44], p. 200-202):

Teorema 1.2. *Toda superficie de Riemann S simplemente conexa tiene como grupo de automorfismos un único de los siguientes:*

- $Aut(\Sigma) = PSL_2(\mathbb{C})$.
- $Aut(\mathbb{C}) = \left\{ \; f(z) = az + b \;\middle|\; a, b \in \mathbb{C}, a \neq 0 \; \right\}$.
- $Aut(\mathscr{U}) = PSL_2(\mathbb{R})$.

Todos los grupos anteriores son grupos de *transformaciones de Möbius*, y en concreto los grupos $PSL_2(\mathbb{C})$ y $PSL_2(\mathbb{R})$ serán inmediatamente definidos en la próxima sección.

Fórmula de Riemann-Hurwitz.
Terminamos esta breve sección con el resultado más importante de cara a estudiar el género de los grupos, regiones y superficies que nos encontraremos más adelante. Sea una función $f : S_1 \longrightarrow S_2$ holomorfa no constante entre superficies de Riemann compactas, se tiene que

$$2g_1 - 2 = \deg(f)(2g_2 - 2) + \sum_{p \in S_1} \left(\mathrm{mult}_p(f) - 1 \right), \tag{1.1}$$

donde g_i es el género de la superficie. Si $\mathrm{mult}_p(f)$ es la multiplicidad de f en un punto p y $\deg(f)$ es el grado de f, para cualquier $q \in S_2$ cumple

$$\deg(f) = \sum_{p \in f^{-1}(q)} \mathrm{mult}_p(f).$$

Para mayor detalle, incluyendo la demostración del teorema mediante la triangulación de las superficies, consultar la página 52 de [28].

1.2. El grupo $PSL_2(\mathbb{R})$

Hemos visto que las tres superficies de Riemann simplemente conexas distintas tienen, como grupo de automorfismos, transformaciones de Möbius con ciertas condiciones para los coeficientes. En esta sección introduciremos la definición del grupo de transformaciones $PSL_2(\mathbb{R})$, así como

sus propiedades y los teoremas relacionados de mayor relevancia. Como no es el objetivo principal de nuestro estudio, no expondremos las demostraciones, que pueden consultarse en [44], pero es importante contar con estos conceptos, ya que el grupo modular $PSL_2(\mathbb{Z})$ del que trataremos enseguida es un subgrupo del mismo, y por tanto hereda muchas propiedades.

Definicion 1.6. (Grupo $PSL_2(\mathbb{C})$) Se define el *grupo de transformaciones* $PSL_2(\mathbb{C})$ como

$$PSL_2(\mathbb{C}) = \left\{ \; A(z) = \tfrac{az+b}{cz+d} \;\middle|\; a,b,c,d \in \mathbb{C} \text{ y } ad-bc = 1 \; \right\} \tag{1.2}$$

De este grupo de transformaciones, obtenemos el subgrupo $PSL_2(\mathbb{R})$, que sirve de grupo marco de cara al posterior estudio del grupo modular $PSL_2(\mathbb{Z})$.

Definicion 1.7. (Grupo $PSL_2(\mathbb{R})$) Se define el *grupo de transformaciones* $PSL_2(\mathbb{R})$ como

$$PSL_2(\mathbb{R}) = \left\{ \; A(z) = \tfrac{az+b}{cz+d} \;\middle|\; a,b,c,d \in \mathbb{R} \text{ y } ad-bc = 1 \; \right\} \tag{1.3}$$

Las transformaciones de $PSL_2(\mathbb{R})$ son isometrías en el plano complejo, conservando así la métrica hiperbólica. En concreto, según el teorema (1.2) estas transformaciones en su totalidad conforman el grupo de automorfismos del semiplano superior $\mathscr{U}$. Además, este grupo es *transitivo* en $\mathscr{U}$ y *doblemente transitivo* en $\mathbb{R}\cup\{\infty\}$, esto es, para cualquier par $z_1, z_2 \in \mathscr{U}$ existe $A \in PSL_2(\mathbb{R})$ tal que $A(z_1) = z_2$ y cualquier par ordenado $(a,b) \in \mathbb{R}\cup\{\infty\}$ con $a \neq b$ puede ser transformado mediante un elemento de $PSL_2(\mathbb{R})$ en cualquier otro par $(c,d) \in \mathbb{R}\cup\{\infty\}$ con $c \neq d$. Dejamos la clasificación de transformaciones para el capítulo siguiente, donde el grupo de referencia será el grupo modular, pero sí vamos a comentar un aspecto importante relativo a los *puntos fijos* :

Definicion 1.8. (Centralizador) Sea g un elemento de un grupo G, se define su *centralizador* $C_G(g)$ como el conjunto de elementos del grupo que conmutan con g, esto es,

$$C_G(g) = \left\{ \; h \in G \;\middle|\; gh = hg \; \right\}. \tag{1.4}$$

Definicion 1.9. (Clase de conjugación) Sea g un elemento de un grupo G, se define su *clase de conjugación* $[g]$ como el conjunto de elementos conjugados de g, esto es,

$$[g] = \left\{ \; h \in G \;\middle|\; h = aga^{-1}, a \in G \; \right\}. \tag{1.5}$$

El centralizador de un elemento g es un subgrupo de G y además se cumple que

$$C_G\left(hgh^{-1}\right) = hC_G(g)h^{-1}.$$

Como además es inmediato comprobar que dos transformaciones conmutan si y sólo si comparten el conjunto de puntos fijos, se deduce la siguiente

Proposicion 1.2. *El centralizador en* $PSL_2(\mathbb{R})$ *de una transformación hiperbólica (repectivamente parabólica, elíptica) consiste en todas las transformaciones hiperbólicas (respectivamente parabólicas, elípticas) con el mismo conjunto de puntos fijos, junto con la identidad.*

Cuando hablemos del efecto geométrico de las transformaciones del grupo modular sobre el semiplano superior, necesitaremos entender los conceptos de *línea hiperbólica* y *segmento hiperbólico*. Aquí la definición:

Definicion 1.10. (H-línea) Se define una *línea hiperbólica* o *H-línea* como el conjunto de todos los puntos del plano complejo sobre una dirección que es o bien paralela al eje Im(z) o bien una circunferencia con centro en el eje Re(z).

Definicion 1.11. (H-segmento) Se define un *segmento hiperbólico* o *H-segmento* entre dos puntos $z_1, z_2 \in \mathbb{C}$ como el camino de extremos z_1 y z_2 sobre la H-línea que pasa por ambos. En particular, si Re(z_1) =Re(z_2) el H-segmento es paralelo al eje Im(z) y si Re(z_1) $\neq$Re(z_2) el H-segmento es un arco de circunferencia que pasa por ambos y que tiene centro en el eje real.

Las transformaciones de $PSL_2(\mathbb{R})$ mandan H-líneas en H-líneas y H-segmentos en H-segmentos. Podemos ahora crear *polígonos hiperbólicos* tomando n H-segmentos y n vértices en $\mathbb{R} \cup \{\infty\}$, que pueden ser *convexos* si el H-segmento que conecta dos puntos cualesquiera del polígono está contenido en el mismo. Para calcular su área, contamos con la conocida fórmula de Gauss-Bonnet:

Teorema 1.3. *(Fórmula de Gauss-Bonnet) Sea P_n un polígono hiperbólico convexo de n lados, cuyos ángulos son $\alpha_1, \alpha_2, \cdots, \alpha_n$. Su área viene dada por*

$$\mu(P_n) = \pi - \sum_{k=1}^{n} \alpha_k. \tag{1.6}$$

En particular, un triángulo hiperbólico tiene área

$$\mu(P_3) = \pi - \alpha_1 - \alpha_2 - \alpha_3.$$

Grupos fuchsianos.
El grupo de estudio de este trabajo, el grupo modular, es un subgrupo discreto de $PSL_2(\mathbb{R})$, y es un ejemplo de lo que se denomina *grupo fuchsiano*.

Definicion 1.12. (Grupo fuchsiano) Un *grupo fuchsiano* es un subgrupo discreto de $PSL_2(\mathbb{R})$.

El concepto de grupo fuchsiano fue posterior a la definición del propio grupo modular o de los grupos triangulares, de los que hablaremos más adelante. Fue Poincaré quien, en 1880, desarrolló el concepto como grupo de isometrías del plano complejo. Pues bien, igual que los espacios de órbitas $\mathbb{C}/\Omega$, siendo Ω un retículo, son superficies de Riemann homeomorfas al *toro* (ver [44], Capítulo 3), un grupo fuchsiano Γ es un grupo de isometrías hiperbólicas cuyo espacios de órbitas $\mathscr{U}/\Gamma$ es una superficie de Riemann. De hecho, aunque no es materia de este trabajo, cabe señalar que las funciones invariantes por retículos se llaman *funciones elípticas*, mientras que análogamente las funciones invariantes por grupos fuchsianos se denominan *funciones*

automórficas. Para un mayor estudio de estas funciones, consultar [29] o [42]. Al clasificar los grupos fuchsianos en función de los elementos generadores, cobran importancia los grupos cíclicos de los siguientes tipos:

- *Grupos cíclicos hiperbólicos*, generados por un elemento cuya matriz asociada cumple $|a+d|>2$, como $A(z)=\lambda z$, $\lambda>1$.
- *Grupos cíclicos parabólicos*, generados por un elemento cuya matriz asociada cumple $|a+d|=2$, como $A(z)=z+\lambda$.
- *Grupos cíclicos elípticos*, generados por un elemento cuya matriz asociada cumple $|a+d|<2$, como $A(z)=-1/z$. Estos grupos son fuchsianos si y sólo si son finitos.

No obstante, el grupo modular tiene como generadores elementos elípticos y parabólicos. Otra característica de los grupos fuchsianos es que actúan de forma *propiamente discontinua* en $\mathscr{U}$, esto es, si para todo punto $z\in\mathbb{C}$ existe un entorno U_z tal que si

$$A(U_z)\cap U_z\neq\emptyset$$

entonces A es la identidad, siendo A un elemento del grupo. A este respecto, enunciamos más propiedades en la siguiente

Proposicion 1.3. *(Puntos fijos por grupos fuchsianos) Sea Γ un subgrupo de $PSL_2(\mathbb{R})$. Es fuchsiano si y sólo si actúa de forma propiamente discontinua en $\mathscr{U}$. Además, si Γ es fuchsiano, para todo $p\in\mathscr{U}$ fijo por una transformación $A\in\Gamma$ existe un entorno U_p que no contiene ningún otro punto $q\neq p$ fijo por elementos de Γ (salvo por la identidad), y de hecho el conjunto de transformaciones que fijan p es discreto para cualquier $p\in\mathscr{U}$.*

Aunque se definirá más adelante, adelantamos que el conjunto de elementos de un grupo G que fijan un punto p, y del que hablábamos en la proposición anterior, se denomina *estabilizador* del punto, y suele expresarse como

$$G_p=\left\{\ g\in G\ \middle|\ g(p)=p\ \right\}.$$

Teselaciones del plano complejo.
Supongamos ahora que tenemos un triángulo hiperbólico T de vértices $v_1,v_2,v_3\in\mathscr{U}\cup\mathbb{R}\cup\{\infty\}$, ángulos $\pi/m_1,\pi/m_2,\pi/m_3$ y lados opuestos M_1,M_2,M_3. Es evidente que, por la fórmula de Gauss-Bonnet, $\pi/m_1+\pi/m_2+\pi/m_3<\pi$, luego $1/m_1+1/m_2+1/m_3<1$. Apliquemos ahora reflexiones sobre los puntos del interior del triángulo, con ejes los lados del triángulo, de acuerdo a la siguiente definición:

Definicion 1.13. (Reflexión hiperbólica) Una transformación R distinta de la identidad se denomina *reflexión hiperbólica* o *H-reflexión* con eje M si es una isometría hiperbólica que fija cada punto $m\in M$.

Si el eje M coincide con el eje imaginario Imz, se puede comprobar que la transformación $R_0(z) = -\overline{z}$ es una H-reflexión, mientras que si M es cualquier otra H-línea, existirá $T \in PSL_2(\mathbb{R})$ tal que $T(M)$ =Imz y con ello $R = T^{-1}R_0T$ es una H-reflexión en M. Partiendo del triángulo T y llamando R_i a la reflexión con eje el lado M_i, es evidente que $R_i(T) = T'$ es otro triángulo con los mismos ángulos, ya que las H-reflexiones conservan ángulos, si bien invierten la orientación y por ello $R_i \notin PSL_2(\mathbb{R})$. Así, los productos de reflexiones que fijan un vértice concreto v_i pueden entenderse como rotaciones con centro v_i y ángulo de giro $2\pi/m_i$, ya que es necesario aplicar m_i rotaciones alrededor de v_i para dar la vuelta completa al vértice.

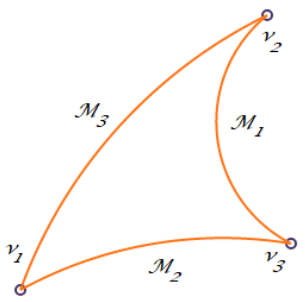

Figura 1.1: Triángulo hiperbólico.

De esta manera, se tiene que las rotaciones que fijan el vértice v_i son elementos de orden finito m_i, de forma que en general

$$(R_iR_j)^{m_k} = I, i \neq j \neq k.$$

Aplicando reflexiones no sólo al triángulo original sino a los triángulos reflejados que van apareciendo, cubrimos el semiplano $\mathscr{U}$ con lo que se denomina una *teselación*. Es algo que haremos más en detalle cuando hablemos del grupo modular, pero es importante tratar de antemano el concepto ya que permite introducir la noción de *grupo triangular*: si Γ^* es el grupo generado por las reflexiones R_1, R_2, R_3, se puede ver fácilmente que es fuchsiano puesto que un punto p tendrá tantas imágenes por rotaciones como triángulos en la teselación. De hecho, si restringimos al semiplano $\mathscr{U}$ definiendo $G = \Gamma^* \cap PSL_2(\mathbb{R})$, se tiene el grupo triangular $G \subset PSL_2(\mathbb{R})$, que puede ser definido de una forma más general:

Definicion 1.14. (Grupo triangular) Un grupo G fuchsiano se denomina *grupo triangular* si está generado por dos elementos X_1, X_2 con órdenes finitos m_1, m_2 y admite la presentación

$$G_{m_1,m_2,m_3} = \left\langle X_1, X_2 \;\middle|\; X_1^{m_1} = X_2^{m_2} = (X_1X_2)^{m_3} = I \right\rangle,$$

siendo m_3 el orden del elemento $X_3 = X_1X_2$.

De hecho, el subgrupo $H_i \subset G$ generado por el elemento X_i es un grupo finito cíclico (elíptico, por tanto) de orden m_i, $i \in \{1,2,3\}$, y este hecho lo utilizaremos tras ver la presentación del grupo modular. El último resultado relevante de esta breve introducción viene dado en el siguiente

Teorema 1.4. *Toda superficie de Riemann S es el espacio de órbitas $\mathscr{U}/\Gamma$ para algún grupo fuchsiano Γ. Además, la superficie $S = \mathscr{U}/\Gamma$ es conformemente equivalente a la superficie $S' = \mathscr{U}/\Gamma'$ para cualquier otro grupo fuchsiano conjugado $\Gamma' = A\Gamma A^{-1}$, con $A \in PSL_2(\mathbb{R})$.*

En particular, la esfera de Riemann es, como veremos, el espacio de órbitas $\mathscr{U}/\Gamma$ para Γ triangular. Veremos cómo obtener las superficies de Riemann mediante identificaciones de H-segmentos en $\mathscr{U}$, y la estrecha relación entre el grupo modular y los grupos de simetrías de los sólidos platónicos que podemos inscribir en la esfera. Respecto a las características de las superficies obtenidas, es de sobra conocido el concepto de *género* de una superficie orientable, siendo por ejemplo $g = 0$ para la esfera y $g = 1$ para el toro. No obstante, recordemos el concepto:

Definicion 1.15. (Género de una superficie orientable) Se denomina *género* de la superficie conexa orientable S al número de toros que hay que adjuntar a la esfera (mediante suma conexa) para obtener una superficie homeomorfa a S.

Así, una superficie orientable de género g es homeomorfa a una esfera a la que se *pegan* g asas, como se describe en numerosos textos (por ejemplo en [15]). Pues bien, para $g \geq 2$ se tiene que, si S es compacta, su grupo de automorfismos está acotado:

$$|\mathrm{Aut}(S)| \leq 84(g-1),$$

dándose la igualdad si el grupo es *de Hurwitz* :

Definicion 1.16. (Grupo de Hurwitz) Un grupo H no trivial se denomina *grupo de Hurwitz* si es el grupo de automorfismos de orden $84(g-1)$ para alguna superficie de Riemann de género $g \geq 2$, y cuya presentación viene dada por

$$H = \left\langle \; X, Y \;\middle|\; X^2 = Y^3 = (XY)^7 = I, \mathscr{R} \; \right\rangle, \tag{1.7}$$

siendo $\mathscr{R}$ un conjunto de relaciones que hacen al grupo finito.

Como ejemplo Estos grupos tendrán su lugar en el estudio que, por fin, comenzamos.

CAPÍTULO 2

EL GRUPO MODULAR

En este capítulo introduciremos el grupo de estudio de este trabajo, el grupo modular, visto como grupo de matrices y también como grupo de transformaciones lineales racionales. Tras dar una presentación del grupo en términos de generadores y relaciones, clasificaremos las distintas transformaciones en función de su traza en *elípticas*, *hiperbólicas* y *parabólicas*, y analizaremos el efecto geométrico que estas transformaciones tienen sobre el semiplano superior hiperbólico, $\mathscr{U}$.

2.1. Definición: $SL_2(\mathbb{Z})$ y $PSL_2(\mathbb{Z})$

Comenzamos definiendo el *grupo modular (de matrices)* $\Gamma = SL_2(\mathbb{Z})$ como sigue:

$$\Gamma = SL_2(\mathbb{Z}) = \left\{ \ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ \middle| \ a,b,c,d \in \mathbb{Z} \text{ y } ad-bc = 1 \ \right\}. \tag{2.1}$$

Si asociamos a cada matriz $A \in \Gamma$ una transformación lineal racional mediante el homomorfismo de grupos dado por

$$\phi : A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto A(z) = \frac{az+b}{cz+d}, \tag{2.2}$$

obtenemos el *grupo modular (de transformaciones)* $\overline{\Gamma} = PSL_2(\mathbb{Z})$ definido como

$$\overline{\Gamma} = PSL_2(\mathbb{Z}) = \left\{ \ A(z) = \tfrac{az+b}{cz+d} \ \middle| \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \ \right\} = \left\{ \ A(z) = \tfrac{az+b}{cz+d} \ \middle| \ a,b,c,d \in \mathbb{Z} \text{ y } ad-bc = 1 \ \right\}. \tag{2.3}$$

Como ocurría en el caso del grupo $PSL_2(\mathbb{R})$, las transformaciones del grupo modular son isometrías en el plano hiperbólico. Además, la matriz identidad I y su opuesta $-I$ tienen la misma

transformación asociada $I(z) = (-I)(z) = z$, con lo que el subgrupo $\{\pm I\}$ es normal en Γ, lo que expresaremos utilizando la notación usual $\{\pm I\} \lhd \Gamma$. Así, se puede entender el grupo $PSL_2(\mathbb{Z})$ como el grupo de matrices $SL_2(\mathbb{Z})$ en el que se identifica cada matriz con su opuesta, de manera que inmediatamente se deduce el isomorfismo $\overline{\Gamma} \cong \Gamma/\{\pm I\}$, esto es,

$$PSL_2(\mathbb{Z}) \cong SL_2(\mathbb{Z})/\{\pm I\} \tag{2.4}$$

Comentario sobre la notación.
Siempre que no provoque confusión, denominaremos indistintamente A tanto a una matriz $A \in \Gamma$ como a la transformación asociada, entendiéndose si se trata de matriz o de transformación según el contexto. De igual forma, en secciones posteriores se hablará del grupo modular $PSL_2(\mathbb{Z})$ o bien como grupo de matrices 2×2 con la identificación de cada matriz con su opuesta o bien como grupo de transformaciones, siendo el enfoque elegido indiferente.

2.2. Presentación del grupo

Nuestro objetivo es establecer una presentación del grupo $PSL_2(\mathbb{Z}) = \overline{\Gamma}$ en términos de generadores y relaciones. Para ello, comencemos con un teorema:

Teorema 2.1. *Sean las matrices* $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *y* $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$*, se tiene que* U *(de orden infinito) y* T *(de orden 4) generan el grupo* Γ.

Demostración. Las afirmaciones sobre los órdenes de U y T son inmediatas, puesto que

$$U^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \ \forall k \in \mathbb{Z} \text{ y } T^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Generemos una matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ mediante los generadores U y T. Teniendo en cuenta que $U^k A = \begin{pmatrix} a+kc & b+kd \\ c & d \end{pmatrix}$ y que $TA = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$, supongamos sin pérdida de generalidad que $|c| \leq |a|$ y distingamos dos casos:

- Si $c = 0$, como $\det A = ad - bc = ad$ es necesario que $|a| = |d| = 1$, luego $A = \pm U^{k_0}$ para cierto $k_0 \in \mathbb{Z}$.
- Si $c \neq 0$, podemos aplicar el algoritmo de Euclides a a y c (asumiendo que $|c| \leq |a|$, tomando en otro caso la matriz TA), hasta llegar a que $(a, c) = 1$, como sigue:

  $$a = k_0 c + r_1, \ -c = k_1 r_1 + r_2, \ r_1 = k_2 r_2 + r_3, \cdots, (-1)^n r_{n-1} = k_n r_n + 0,$$

  terminando con $r_n = \pm 1$. Así, se tiene que $TU^{-k_n} T \cdots TU^{-k_0} A = \pm U^{k_{n+1}}$ con k_{n+1} entero, con lo que finalmente se puede despejar A en función de los generadores.

□

Por ejemplo, para la matriz $A = \begin{pmatrix} 6 & 7 \\ 5 & 6 \end{pmatrix}$ se tiene:

$$6 = 1 \cdot 5 + 1 \text{ y } -5 = (-5) \cdot 1 + 0,$$

siendo en este caso $k_1 = -5$ y $k_0 = 1$. Ocurre que $TU^5TU^{-1}A = -U$, y por tanto $A = UT^{-1}U^{-5}T^{-1}(-U)$ o bien, como $-U = T^2U$, $A = UT^{-1}U^{-5}TU$.

Teorema 2.2. *Dada la matriz* $R = TU = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ *y considerando* $R_1 = -R$, *el grupo* Γ *también tiene como generadores a* T *y* R_1 *y, de hecho, se tiene el sistema completo de relaciones*

$$T^4 = R_1^3 = I, R_1T^2 = T^2R_1. \tag{2.5}$$

Con ello, se tiene la presentación

$$\Gamma = \left\langle \ T, R_1 \ \middle| \ T^4 = R_1^3 = I, R_1T^2 = T^2R_1 \ \right\rangle.$$

Análogamente, podemos llegar a una presentación para $\overline{\Gamma}$. Para ello, recuperemos las transformaciones generadoras

$$U(z) = z + 1,\ T(z) = \frac{-1}{z} \text{ y } TU(z) = R(z) = \frac{-1}{z+1}.$$

Es claro que $T^2(z) = z$ y que $R^3(z) = z$, luego tienen órdenes 2 y 3 respectivamente. Además, dado que las matrices T y $R_1 = -R$ generan Γ, análogamente las transformaciones asociadas T y R generan $\overline{\Gamma}$, con lo que tenemos el siguiente teorema:

Teorema 2.3. *El grupo modular* $PSL_2(\mathbb{Z})$ *admite la presentación*

$$\overline{\Gamma} = PSL_2(\mathbb{Z}) = \left\langle \ T, R \ \middle| \ T^2 = R^3 = I \ \right\rangle.$$

También se puede ver $\overline{\Gamma}$ como producto libre de los grupos cíclicos generados por cada generador, para lo cual necesitamos la siguiente proposición.

Proposicion 2.1. *Sean los grupos*

$$G_1 = \left\langle \ X_1, X_2, \cdots, X_{n_1} \ \middle| \ R_1, R_2, \cdots, R_{m_1} \ \right\rangle \text{ y } G_2 = \left\langle \ Y_1, Y_2, \cdots, Y_{n_2} \ \middle| \ F_1, F_2, \cdots, F_{m_2} \ \right\rangle,$$

entonces el producto libre $G = G_1 * G_2$ *tiene presentación*

$$G = \left\langle \ X_1, X_2, \cdots, X_{n_1}, Y_1, Y_2, \cdots, Y_{n_2} \ \middle| \ R_1, R_2, \cdots, R_{m_1}, F_1, F_2, \cdots, F_{m_2} \ \right\rangle.$$

De esta proposición se deduce automáticamente el siguiente teorema:

Teorema 2.4. $\overline{\Gamma}$ *es isomorfo al producto libre del grupo cíclico de orden 2 por el grupo cíclico de orden 3, esto es,* $\overline{\Gamma} \cong C_2 * C_3$.

2.3. Clasificación de transformaciones

En próximas secciones necesitaremos estudiar el efecto que las distintas transformaciones del grupo $PSL_2(\mathbb{Z})$ tienen sobre el semiplano superior hiperbólico a nivel local. Dicho efecto depende del carácter de la transformación.

Definicion 2.1. Sea $A(z) = \frac{az+b}{cz+d}$ una transformación en $PSL_2(\mathbb{Z})$.

- Se dice que A es una *transformación elíptica* si $|\mathrm{Tr}(A)| = |a+d| < 2$.
- Se dice que A es una *transformación parabólica* si $|\mathrm{Tr}(A)| = |a+d| = 2$.
- Se dice que A es una *transformación hiperbólica* si $|\mathrm{Tr}(A)| = |a+d| > 2$.

Para obtener los puntos fijos, basta con resolver la ecuación

$$A(z) = \frac{az+b}{cz+d},$$

de donde se deduce que si $A(z)$ es una transformación elíptica, entonces fija dos números complejos conjugados; si es parabólica fija un único punto $\frac{a-d}{2c} \in \mathbb{Q} \cup \{\infty\}$ y finalmente si es hiperbólica fija dos conjugados en el cuerpo cuadrático $\mathbb{Q}\left[\sqrt{N}\right]$, con $N > 0$ entero . En [42], se demuestra la conexión entre los autovalores de la matriz y los puntos fijos de la transformación asociada:

Proposicion 2.2. *Si* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ *tiene dos autovalores* $\lambda_1 \neq \lambda_2$*, entonces la transformación asociada* $A(z)$ *tiene los puntos fijos*

$$z_j = \frac{\lambda_j - d}{c} = \frac{b}{\lambda_j - a},\ j \in \{1,2\}.$$

Esta proposición permite realizar un estudio de los puntos fijos de $A(z)$ a partir de los autovalores de $A \in \Gamma$. Comenzamos calculando su *polinomio característico* :

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow \det(|A - \lambda I|) = (a-\lambda)(d-\lambda) - bc = \lambda^2 - (a+d)\lambda + ad - bc = \lambda^2 - \mathrm{Tr}(A)\lambda + 1.$$

Estudiemos las posibilidades atendiendo al discriminante $\Delta = \mathrm{Tr}^2(A) - 4$:

- Si $\mathrm{Tr}(A) = 0$ entonces $\sqrt{\Delta} = \pm 2i$ y con ello $\lambda = \pm i$. Obsérvese que estos autovalores son unidades[1] en el cuerpo $\mathbb{Q}[i]$. Así, en el caso $(a+d) = 0$ la matriz A tiene asociada una transformación elíptica. La tranformación generadora T tiene punto fijo $z = i$ en $\mathscr{U}$.

[1] Un elemento x en un anillo H es una *unidad* o *elemento invertible* si existe otro elemento $y \in H$ tal que $x \cdot y = Id$, siendo Id el elemento identidad para la multiplicación.

- Si $|\mathrm{Tr}(A)| = 1$ entonces $\sqrt{\Delta} = \sqrt{-3}$ y con ello $\lambda = \pm\rho^{\pm 1}$ o bien $\lambda = (-\rho)^{\pm 1}$, siendo $\rho = e^{2\pi i/3}$. En este caso, los autovalores son unidades en el cuerpo $\mathbb{Q}\left[\sqrt{-3}\right]$. Así, en el caso $|a+d| = 1$ la matriz A tiene asociada una transformación que también es elíptica. Obsérvese que la tranformación generadora $R = TU$ tiene tiene como punto fijo $\rho = -\frac{1}{2} + \sqrt{3}i/2 \in \mathscr{U}$, que está entre los autovalores estudiados.

- Si $|\mathrm{Tr}(A)| = 2$ entonces $\sqrt{\Delta} = 0$ y con ello $\lambda = \pm 1$, unidades en $\mathbb{Q}$. Así, en el caso $|a+b| = 2$ la transformación es parabólica. El generador U es un ejemplo, que fija únicamente ∞.

- Si $|\mathrm{Tr}(A)| > 2$ entonces $\sqrt{\Delta} = \sqrt{\mathrm{Tr}^2(A) - 4}$ y con ello $\lambda = \frac{1}{2}\left(\mathrm{Tr}(A) \pm \sqrt{\mathrm{Tr}^2(A) - 4}\right)$, unidades en $\mathbb{Q}\left[\sqrt{(a+d)^2 - 4}\right]$. Así, en el caso $|a+d| > 2$ la transformación es hiperbólica.

Equivalencia de puntos bajo $\overline{\Gamma}$.
Con la mencionada clasificación de transformaciones, vamos a revisar en qué sentido dos puntos son *equivalentes* y qué propiedades algebraicas se derivan de ello. Comencemos con una definición:

Definicion 2.2. Dos puntos $z_1, z_2 \in \Sigma = \mathbb{C} \cup \{\infty\}$, se dice que son $\overline{\Gamma}$-*equivalentes* si $\exists A \in \overline{\Gamma}$ tal que $A(z_1) = z_2$. Así, esta relación entre puntos es de equivalencia y podemos hablar de la *órbita* de z por la acción de $\overline{\Gamma}$:

$$\overline{\Gamma} z = \left\{ \; w \in \Sigma \;\middle|\; w = A(z) \text{ con } A \in \overline{\Gamma} \; \right\}. \tag{2.6}$$

En relación a la definición anterior, se puede hablar de *clases u órbitas parabólicas, elípticas e hiperbólicas* en función de qué tipo de transformaciones actúan en la equivalencia entre los puntos de la clase:

Definicion 2.3. Sea una transformación $A \in \overline{\Gamma}$, se denomina *clase de conjugación* de A a

$$[A] = \left\{ \; B \in \overline{\Gamma} \;\middle|\; B = XAX^{-1}, X \in \overline{\Gamma} \; \right\}.$$

La clase de conjugación será parabólica, elíptica o hiperbólica en función de la naturaleza de A.

Cuando la transformación es parabólica, mediante conjugaciones es sencillo llegar de un punto p a cualquier otro q si $p, q \in \mathbb{Q} \cup \{\infty\}$. Veámoslo en el siguiente

Teorema 2.5. *Si $A \in \overline{\Gamma}$ es parabólica, entonces tiene como conjunto de puntos fijos $\bar{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$. Así, todo racional $q \in \mathbb{Q}$ es equivalente a ∞ en $\overline{\Gamma}$ y además A es conjugada de U^k, esto es, $A = XU^kX^{-1}$ para cierta $X \in \Gamma$. Las transformaciones parabólicas que comparten puntos fijos forman un grupo infinito cíclico.*

Demostración. Como indicación, obsérvese que si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ con $c = 0$ entonces $A = \pm \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, luego $A = U^k$, que fija ∞; pero si $c \neq 0$ entonces por ser $|a+d| = 2$ se obtiene, sin más que operar,

que el único punto fijo es $\frac{a-d}{2c} \in \mathbb{Q}$. Por otra parte, dados dos enteros coprimos a' y c' existirán, por la *Identidad de Bezout*, b' y d' tales que $a'd' - b'c' = 1$. Por consiguiente, podemos formar la correspondiente matriz $X \in \Gamma$ con $X(\infty) = a'/c'$ y tal que $A = XUX^{-1}$ fija a'/c', con lo que A es parabólica. La última parte se reduce a observar el caso en que el punto fijo es ∞: tal transformación es U^k que tiene orden infinito. □

Teorema 2.6. *Si $A \in \overline{\Gamma}$ es elíptica, entonces fija $\left\{ \; q = \frac{\pm i - d}{c} \in \mathbb{Q}[i] \;\middle|\; d^2 \equiv -1 \mod c \; \right\}$ (caso $a+d=0$) o bien $\left\{ \; q = \frac{\rho^{\pm 1} - d}{c} \in \mathbb{Q}[\rho] \;\middle|\; d^2 \equiv -1 \mod c \; \right\}$ (caso $|a+d|=1$). Las transformaciones elípticas del grupo modular son de orden 2 ó 3. Además, toda $A \in \overline{\Gamma}$ elíptica es conjugada de R, R^2 o T.*

Demostración. La primera parte se deduce de los cálculos derivados del polinomio característico (detalles en [42], p.10-12). Por otra parte, si A es la matriz asociada a la transformación y tiene polinomio característico $P(X) = X^2 + 1$ se tiene que $P(A) = A^2 + I = 0$, luego $A^2 = -I$ y por tanto $A^2(z) = z$. Se comprueba análogamente el caso en que $P(X) = X^2 \pm X + 1$, para el que $A^3(z) = z$. La última afirmación es fácil de comprobar si se tiene en cuenta que tanto los autovalores como la traza son invariantes bajo conjugación. □

Para el último teorema a este respecto, necesitamos un par de definiciones:

Definicion 2.4. Sean dos enteros x, y, se define su *espacio de módulos* o simplemente *módulo* como

$$(x,y) = \left\{ \; \alpha x + \beta y \;\middle|\; \alpha, \beta \in \mathbb{Q}\left[\sqrt{n}\right], n > 0 \; \right\}. \tag{2.7}$$

Teorema 2.7. *Si $A \in \overline{\Gamma}$ es hiperbólica, entonces fija pares de conjugados en un cuerpo cuadrático $\mathbb{Q}\left[\sqrt{n}\right]$. Las transformaciones hiperbólicas con los mismos puntos fijos forman un grupo infinito cíclico y dos puntos $z_1 = a_1/a_2$ y $z_2 = b_1/b_2$ son equivalentes si existe $\omega \in \mathbb{Q}\left[\sqrt{n}\right]$ tal que $(a_1, a_2) = \omega(b_1, b_2)$, siendo (a_1, a_2) y (b_1, b_2) módulos.*

Demostración. Dejamos al lector consultar la página 13 de [42], dado que las transformaciones hiperbólicas no son de gran relevancia para nuestro estudio. □

Conclusión: T y R son transformaciones elípticas con puntos fijos i, ρ y órdenes 2 y 3 respectivamente, mientras que U es parabólica con punto fijo ∞ y orden infinito. Como consecuencia, los subgrupos generados correspondientes $\langle T \rangle$, $\langle R \rangle$ y $\langle U \rangle$ son cíclicos de órdenes 2, 3 e ∞, respectivamente.

Para terminar la sección y, como consecuencia de lo visto hasta ahora, podemos clasificar los puntos fijos en tres categorías, según la siguiente definición.

Definicion 2.5. Sea $A \in \overline{\Gamma}$ con punto fijo $z_0 \in \mathscr{U} \cup \mathbb{Q} \cup \{\infty\}$, entonces:

- El punto fijo z_0 se denomina *punto elíptico* si A es una transformación elíptica.

- El punto fijo z_0 se denomina *punto parabólico* o *cúspide* si A es una transformación parabólica.
- El punto fijo z_0 se denomina *punto hiperbólico* si A es una transformación hiperbólica.

Como observación, es importante recalcar que una transformación no puede ser parabólica e hiperbólica a la vez. A continuación veremos qué importancia tiene a nivel geométrico la naturaleza de las transformaciones y sus puntos fijos, de cara a obtener teselaciones a partir de un triángulo hiperbólico.

2.4. Región fundamental

En esta sección vamos a definir el concepto de región fundamental tanto para $\overline{\Gamma}$ como para cualquier subgrupo de índice finito en $\overline{\Gamma}$, y estudiaremos la acción de los generadores de $\overline{\Gamma}$ sobre su región fundamental para obtener finalmente una teselación de $\mathcal{U}$.

2.4.1. Región fundamental de $PSL_2(\mathbb{Z})$

Comencemos con la definición general de región fundamental para un grupo fuchsiano G, como subconjunto del *semiplano superior extendido* al que denotaremos

$$\mathcal{U}^* = \mathcal{U} \cup \mathbb{Q} \cup \{\infty\}. \tag{2.8}$$

Definicion 2.6. Sea H un subgrupo de índice finito en G, se dice que el conjunto $\mathcal{F} \subset \mathcal{U}$ es una *región fundamental* para H si es cerrado en $\mathcal{U}$ y además:

1. $\bigcup_{T \in H} T(\mathcal{F}) = \mathcal{U}$.
2. $T(\mathring{\mathcal{F}}) \bigcap \mathring{\mathcal{F}} = \emptyset$ para todo $T \in H - I$, donde la notación $\mathring{\mathcal{F}}$ se refiere al *interior* de $\mathcal{F}$.

En el caso que nos ocupa, en el que el grupo fuchsiano es $\overline{\Gamma} = PSL_2(\mathbb{Z})$, la definición es equivalente a la siguiente:

Lema 2.1. *Sea G un subgrupo de índice finito en $\overline{\Gamma}$ (o el propio $\overline{\Gamma}$), $\mathcal{F} \subset \mathcal{U}$ es una región fundamental para G si su interior contiene como mucho un punto de cada clase de puntos $\overline{\Gamma}$-equivalentes en $\mathcal{U}^*$, esto es,*

$$\forall z \in \mathring{\mathcal{F}} \text{ si } A(z) \in \mathring{\mathcal{F}} \text{ entonces } A = I.$$

En particular, la órbita de los puntos del conjunto $\mathbb{Q} \cup \{\infty\}$ no corta al interior de $\mathcal{F}$.

Así pues, se tiene la siguiente afirmación:

Teorema 2.8.

$$\mathcal{F} = \left\{ \; z \in \mathcal{U} \;\middle|\; |Re z| \leq \tfrac{1}{2} \; y \; |z| \geq 1 \; \right\} \text{ es una región fundamental para el grupo modular } \overline{\Gamma}.$$

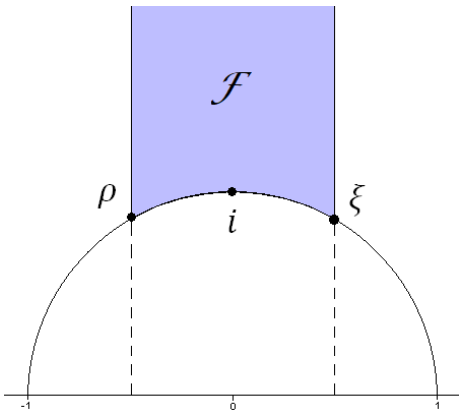

Figura 2.1: Región fundamental para Γ.

Demostración. Sea $z \in \mathcal{U}$, tomemos el *retículo* L definido como

$$L = \left\{ \; cz + d \in \mathcal{U} \;\middle|\; c, d \in \mathbb{Z} \; \right\}.$$

Es claro que cualquier subconjunto no vacío de L contendrá un elemento con módulo mínimo, y en concreto dicho valor mínimo aparecerá en el conjunto

$$\left\{ \; |A(z)| \;\middle|\; A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \; \right\}.$$

Además, sin más que operar sabemos que

$$\mathrm{Im}(A(z)) = \frac{\mathrm{Im}(z)}{|cz+d|^2},$$

y debe existir un punto z_0 equivalente a z y que cumpla

$$\mathrm{Im}(z_0) \geq \mathrm{Im}(A(z_0)), \forall A \in \Gamma.$$

Recuperamos ahora la conocida matriz U^m, reemplazamos z_0 por $U^m(z_0)$ si es necesario y asumimos $|\mathrm{Re}(z_0) \leq 1/2|$. A su vez, cogemos la transformación asociada a la matriz T, a saber $T(z) = -1/z$, y observamos que

$$\mathrm{Im}(z_0) \leq \mathrm{Im}(-1/z_0) = \mathrm{Im}(z_0)/|z_0|^2$$

de modo que $|z_0| \geq 1$, implicando $z_0 \in \mathcal{F}$ y con ello $\mathcal{U} = \bigcup_{A \in \Gamma} A(\mathcal{F})$.

Tomemos ahora $\mathcal{F}_1$ como el interior de la región $\mathcal{F}$, para verificar que $A(\mathcal{F}_1) \cap \mathcal{F}_1 = \emptyset$ si $A \neq \pm I$. Para ver esto, supongamos que $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ es tal que $A(\mathcal{F}_1) \cap \mathcal{F}_1 \neq \emptyset$ y un complejo z tal que $A(z) \in \mathcal{F}_1$, asumiendo que $\mathrm{Im}(A(z)) \geq \mathrm{Im}(z)$ (si es necesario tomamos A^{-1} en lugar de A). Se tiene

$$|c|\,\mathrm{Im}(z) \leq |cz+d|^2 \leq 1,$$

y como $z \in \mathscr{F}_1$ entonces $\mathrm{Im}(z) > \sqrt{3}/2$ y con ello $|c| \leq 1$, por lo que o bien $c = 1$ o bien $c = 0$. Si $|c| = 1$, entonces $|z + d| \leq 1$ y además $|z + d| \geq 1$ para cualquier d entero (porque $z \in \mathscr{F}_1$), luego llegamos a contradicción. De este modo, $c = 0$ y A tiene la forma

$$A = \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \pm U^b, A(z) = z + b$$

y sólo queda pensar que z y $U(z)$ pertenecen a $\mathscr{F}_1$ sólo en el caso en que $b = 0$, esto es, cuando $A = \pm I$. Queda entonces demostrado que $\mathscr{F}$ es una región fundamental para Γ. □

Como se observa en la figura, los puntos $\rho = e^{2\pi i/3}, \xi = e^{\pi i/3}$ son las intersecciones del arco de circunferencia unidad con las H-líneas $\mathrm{Re}(z) = \pm\frac{1}{2}$. Veamos una definición seguida de una interesante propiedad a este respecto.

Definicion 2.7. (Orden de un punto) Un punto $z_0 \in \mathscr{U}^*$ es de *orden* k, $k > 0$ entero, si es fijo por una transformación A de orden k, esto es, si $A^k(z) = z$ para todo $z \in \mathscr{U}^*$ y $A(z_0) = z_0$.

Proposicion 2.3. *Todo punto elíptico $z_0 \in \mathscr{U}$ de $\overline{\Gamma}$ es equivalente o bien a i o bien a ρ en $\overline{\Gamma}$. De hecho, i es un punto elíptico de orden 2 con estabilizador*

$$\Gamma_i = \{\pm I, \pm T\}$$

mientras que ρ es de orden 3 con estabilizador

$$\Gamma_\rho = \left\{ \pm I, \pm \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \right\} = \left\{ \pm I, \pm UT, \pm TU^{-1} \right\}.$$

Análogamente, todo punto parabólico es equivalente a ∞, con lo que el conjunto de puntos parabólicos (o cúspides) de $\overline{\Gamma}$ es $\mathbb{Q}^* = \mathbb{Q} \cup \{\infty\}$. En ocasiones se dice que ∞ tiene orden infinito.

Demostración. En el caso parabólico, basta con elegir $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ de forma que $a/c \in \mathbb{Q}$ sea irreducible (así, $X(\infty) = a/c$ y se tiene la equivalencia). Además, puede considerarse que ∞ tiene orden infinito ya que es fijo por U, que tiene orden infinito. En el caso elíptico, como $\mathscr{F}$ sólo contiene un representante de cada clase de equivalencia de puntos y como las transformaciones T, U generan $\overline{\Gamma}$, es claro que todo punto interior de $\mathscr{F}$ será *ordinario* (en el sentido de tener estabilizador trivial), así como todo punto del borde de $\mathscr{F}$, denotado como $\partial\mathscr{F}$, que no esté en $\{\rho, \xi, i\}$, por lo que todo punto elíptico debe ser equivalente a un elíptico de $\partial\mathscr{F}$. Además, ρ y ξ son $\overline{\Gamma}$-equivalentes puesto que $U(\rho) = \xi$, relación que denotaremos como $\rho \sim \xi$. □

Consideraciones acerca de $\mathscr{F}$.

Los puntos del interior de $\mathscr{F}$ son representantes únicos de sus clases de equivalencia de puntos,

es decir, no existen dos puntos equivalentes en el interior de la región fundamental. Los lados de la región se presentan como pares de conjugados

$$(\rho,\infty) \sim (-\overline{\rho},\infty) \text{ y } (\rho,i) \sim (-\overline{\rho},i),$$

donde $U^{\pm 1}$ y T transforman cada lado en su conjugado, recibiendo así el nombre de *transformaciones de borde*. Cuando veamos la región fundamental de los subgrupos de Γ, utilizaremos la idea de que las transformaciones de borde generan dichos subgrupos. Si pensamos en puntos fijos (elípticos, hiperbólicos o parabólicos), los representantes de sus clases de equivalencia vendrán dados por los puntos fijos de estos generadores. Una consecuencia directa de la región fundamental es la siguiente

Proposicion 2.4. *Sean los generadores conocidos T y $R = TU$, se tiene que:*

1. *Todas las matrices A con $Tr(A) = 0$ son conjugadas de T.*
2. *Todas las matrices A con $|Tr(A)| = 1$ son conjugadas o bien de R o bien de R^2.*

Demostración. Probemos como ejemplo la primera afirmación (la segunda es análoga): es claro que $T(i) = i$, esto es, i es fijo por T, y es el representante de su clase de equivalencia de puntos en $\mathscr{F}$. Así, si tenemos una matriz $A \in \Gamma$ con $\mathrm{Tr}(A) = 0$ con puntos fijos elípticos z y $\overline{z}$, hemos visto que deben ser equivalentes a i, y de hecho sabemos que debe existir $S \in \Gamma$ tal que $S(z) = i$, con lo que entonces

$$SAS^{-1}(i) = i \text{ y con ello } SAS^{-1} = T.$$

En conclusión, las únicas transformaciones en Γ que fijan puntos equivalentes a i son conjugadas de T. □

2.4.2. Teselación del plano hiperbólico

Vamos a analizar el efecto que tiene la aplicación de distintas transformaciones del grupo modular sobre la región fundamental $\mathscr{F}$, para terminar observando que se obtiene una triangulación de $\mathscr{U}$.
Para ello, considérese $A \in \overline{\Gamma}$ y $\mathscr{F}$ la región fundamental del teorema 2.8.

Definicion 2.8. Se define un *triángulo modular* como $\mathscr{F}_A = A(\mathscr{F})$, es decir, la imagen por A de $\mathscr{F}$.

Es evidente que el conjunto de triángulos $\mathscr{F}_A$ cubre el semiplano superior, luego

$$\bigcup_{A\in\Gamma} \mathscr{F}_A = \mathscr{U} \tag{2.9}$$

Es importante realizar varias observaciones sobre la teselación de la figura 2.2[2] :

[2]Imagen creada con el software **FunDomain**, escrito por Helena A. Verrill, y bajo licencia GNU GPL. Disponible en https://wstein.org/Tables/fundomain/

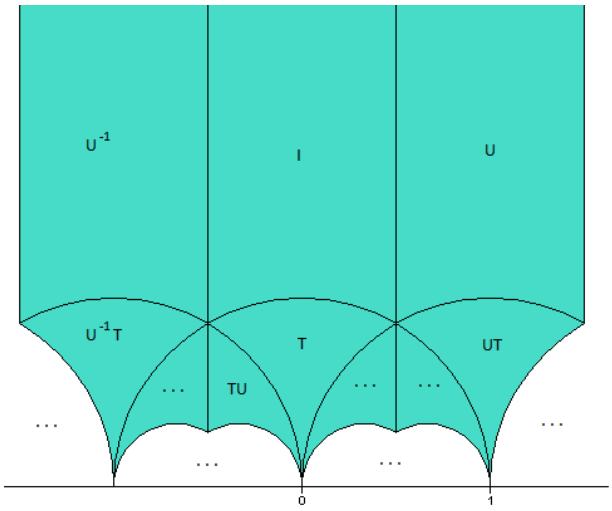

Figura 2.2: Teselación del semiplano hiperbólico.

- Como una transformación en $PSL_2(\mathbb{R})$ lleva H-líneas en H-líneas, se tiene que la imagen de una H-línea de la teselación por $A \in \overline{\Gamma}$ viene determinada por la imagen de uno de sus puntos (distinto de ρ, i, ∞).
- Todo punto de $\mathscr{U}^*$ no perteneciente a la órbita de ρ, i, o ∞, es la imagen de un único punto de $\mathscr{F}$, mientras que ρ, i, ∞ son los puntos de intersección de 3, 2 e infinitas H-líneas de la teselación, coincidiendo con los órdenes de las transformaciones R, T, U respectivamente.
- Cada triángulo modular $\mathscr{F}_A$ es adyacente exactamente a otros tres, dado que $A^{-1}(\mathscr{F}_A) = \mathscr{F}$ y $T(\mathscr{F})$, $U(\mathscr{F})$ y $U^{-1}(\mathscr{F})$ son adyacentes a $\mathscr{F}$ porque T manda $\mathscr{F}$ al triángulo de vértices $\rho, \xi, 0$, y U desplaza $\mathscr{F}$ una unidad a la derecha (U^{-1} a la izquierda).

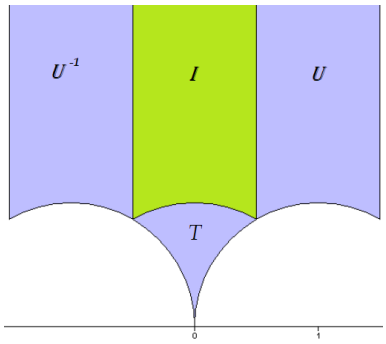

Figura 2.3: Triángulo modular $\mathscr{F}$ (en verde) y sus adyacentes: $U(\mathscr{F})$, $T(\mathscr{F})$ y $U^{-1}(\mathscr{F})$.

- En cada punto equivalente a ρ se encuentran 6 triángulos con ángulo de incidencia $\pi/3$. Las transformaciones de la forma SRS^{-1} son rotaciones (en el plano hiperbólico) con centro $S(\rho)$ y ángulo $2\pi/3$.

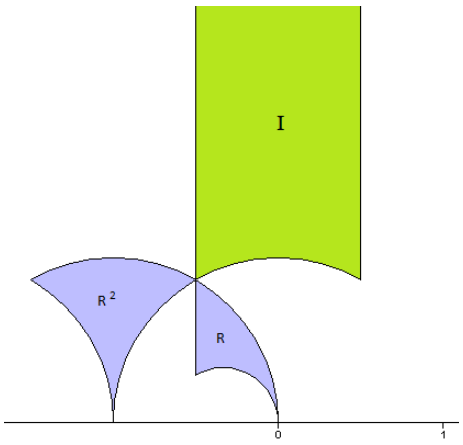

Figura 2.4: Triángulo modular $\mathscr{F}$ (en verde) y sus rotados con centro ρ: $R(\mathscr{F})$ y $R^2(\mathscr{F})$.

- En cada punto equivalente a i se encuentran 2 triángulos. Las tranformaciones de la forma STS^{-1} son rotaciones con centro $S(i)$.

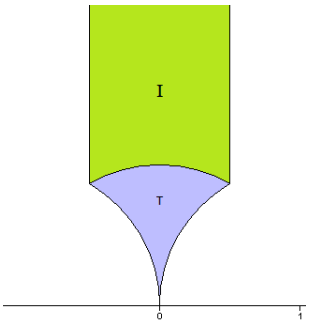

Figura 2.5: Triángulo modular $\mathscr{F}$ (en verde) y su rotado con centro i: $T(\mathscr{F})$.

Existen más consideraciones goemétricas que iremos introduciendo a lo largo de las secciones siguientes.

CAPÍTULO 3

SUBGRUPOS DEL GRUPO MODULAR

A continuación vamos a estudiar en detalle los distintos tipos de subgrupos del grupo modular. En primer lugar definiremos los subgrupos principales de congruencia y veremos cúando un subgrupo es de congruencia. Seguidamente veremos el subgrupo conmutador y su relación con el subgrupo potencia y las condiciones necesarias para que un subgrupo normal de $\overline{\Gamma}$ sea de congruencia. Para terminar el capítulo y con el objetivo de aportar cierto sentido práctico a tanta carga teórica, veremos brevemente cómo utilizar los elementos y las propiedades del grupo modular para encriptar texto plano sin formato.

3.1. Subgrupos de congruencia

Comencemos estudiando un tipo importante de subgrupos de Γ que aparece cuando aplicamos el concepto de *clases de residuos módulo N* en nuestro contexto.

Definicion 3.1. Sea $\Gamma = SL_2(\mathbb{Z})$ y $N \in \mathbb{N}$, se define el *subgrupo principal de congruencia de nivel N* como

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}. \tag{3.1}$$

Se puede comprobar que, efectivamente, $\Gamma(N)$ es un subgrupo de Γ, y además si $M|N$ entonces $\Gamma(N) \subset \Gamma(M)$. Si identificamos cada matriz con su opuesta, obtenemos una caracterización matricial de los elementos del subgrupo principal de congruencia, como grupo de transformaciones:

$$\overline{\Gamma}(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}, \tag{3.2}$$

de modo que claramente

$$\overline{\Gamma}(N) \cong \Gamma(N)/\{\pm I\}, \tag{3.3}$$

y evidentemente se tiene la caracterización mediante transformaciones

$$\overline{\Gamma}(N) = \left\{ \; A(z) = \tfrac{az+b}{cz+d} \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N) \; \right\}. \tag{3.4}$$

Así, en posteriores secciones trataremos $PSL_2(\mathbb{Z})$ o bien como grupo de matrices en el que $A \equiv -A$, o bien como grupo de transformaciones asociadas a las matrices de $SL_2(\mathbb{Z})$, esperando que esto no provoque la confusión del lector.

Tomando residuos módulo N.
Sea

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}),$$

con $M_2(\mathbb{Z})$ el grupo de matrices 2×2 con entradas enteras y la aplicación

$$\lambda_N : M_2(\mathbb{Z}) \longmapsto M_2(\mathbb{Z}_N) \text{ con } \lambda_N(A) = \begin{pmatrix} a_N & b_N \\ c_N & d_N \end{pmatrix} \tag{3.5}$$

siendo $a_N := a \mod N$ y $M_2(\mathbb{Z}_N)$ el grupo de matrices 2×2 con entradas enteras módulo N. Es claro que se tiene un homomorfismo de $SL_2(\mathbb{Z})$ en $SL_2(\mathbb{Z}_N)$ que, además, verifica el siguiente teorema:

Teorema 3.1. *Sea λ_N el homomorfismo de $SL_2(\mathbb{Z})$ en $SL_2(\mathbb{Z}_N)$. Se tiene:*

1. *λ_N es un epimorfismo.*
2. *$\ker(\lambda_N) = \Gamma(N)$ es normal en Γ, y como consecuencia directa se tiene el isomorfismo*

$$\Gamma_N := \Gamma/\Gamma(N) \cong SL_2(\mathbb{Z}_N).$$

3. *λ_N induce un homomorfismo de $PSL_2(\mathbb{Z})$ en $PSL_2(\mathbb{Z}_N)$.*

Para la demostración, utilizaremos un conocido resultado sobre congruencias:

Lema 3.1. *Para cada solución de la congruencia $ad - bc \equiv 1 \mod N$ existen $a' \equiv a, b' \equiv b, c' \equiv c, d' \equiv d$ tales que $a'd' - b'c' = 1$.*

Demostración. Basta con probar la primera afirmación, para la cual cogemos $\begin{pmatrix} a_N & b_N \\ c_N & d_N \end{pmatrix} \in SL_2(\mathbb{Z}_N)$. Sea la matriz

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \equiv \begin{pmatrix} a_N & b_N \\ c_N & d_N \end{pmatrix} \mod N, \tag{3.6}$$

entonces $a'd' - b'c' \equiv 1 \mod N$ con $(c', d', N) = 1$ (y podemos suponer $(c', d') = 1$). Elegimos $k \in \mathbb{Z}$ tal que $a'd' - b'c' = 1 + kN$ y $a", b"$ tales que $a"d' - b"c' = -k$. Finalmente, tomamos

$$a = a' + a"N,\ b = b' + b"N,\ c = c',\ d = d'$$

con lo que $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ y $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a_N & b_N \\ c_N & d_N \end{pmatrix} \mod N.$ □

Nuestro siguiente objetivo es obtener expresiones para calcular el orden de estos subgrupos. Antes de ello, debemos detenernos unos instantes a estudiar la relación entre los subgrupos de $\Gamma = SL_2(\mathbb{Z})$ y los de $\overline{\Gamma} = PSL_2(\mathbb{Z})$. Ya vimos que el homomorfismo dado por

$$\phi(A) = A(z) = \frac{az + b}{cz + d} \tag{3.7}$$

asocia una transformación lineal racional a una matriz del grupo modular $SL_2(\mathbb{Z})$.

Proposicion 3.1. *Si Ω es un subgrupo de Γ entonces la restricción $\phi : \Omega \longrightarrow \phi(\Omega)$ es un epimorfismo con $\ker(\phi) = \{\pm I\}$ si $-I \in \Omega$ y es un isomorfismo si $-I \notin \Omega$. Para estos $\Omega \subset \Gamma$ que no contienen a la matriz $-I$, podemos aplicar la extensión $\Omega^* = \Omega \cup (-I)\Omega$ y se cumple*

$$\overline{\Omega} = \phi(\Omega) = \phi(\Omega^*).$$

Independientemente de que ocurra $-I \in \Omega$ se tiene que si Ω es normal en Γ entonces $\overline{\Omega}$ es normal en $\overline{\Gamma}$. No obstante, la pertenencia o no de la matriz $-I$ al subgrupo $\Omega \subset \Gamma$ es importante a la hora de hallar los órdenes de los subgrupos que hemos definido, puesto que determina el cálculo del índice $|\Gamma : \Omega|$. Así, si llamamos $\mu = |\Gamma : \Omega|$ y $\bar{\mu} = \left|\overline{\Gamma} : \overline{\Omega}\right|$ (ambos finitos), se tiene

$$\bar{\mu} = \begin{cases} \mu & si \quad -I \in \Omega \\ \\ \frac{1}{2}\mu & si \quad -I \notin \Omega \end{cases}, \tag{3.8}$$

puesto que, si $-I \in \Omega$, la descomposición

$$\Gamma = \bigcup_{k=1}^{\mu} \Omega S_k,\ S_k \in \Gamma \tag{3.9}$$

implica la descomposición

$$\overline{\Gamma} = \bigcup_{k=1}^{\mu} \Omega \overline{S}_k,\ \overline{S}_k \in \overline{\Gamma} \tag{3.10}$$

mientras que, si $-I \notin \Omega$, en la primera descomposición debe haber el doble de términos en la unión que en la segunda, esto es,

$$\Gamma = \left(\bigcup_{k=1}^{\bar{\mu}} \Omega S_k \right) \cup \left(\bigcup_{k=1}^{\bar{\mu}} (-I)\Omega S_k \right).$$

Subgrupo principal de congruencia extendido.
En el caso particular $\Omega = \Gamma(N)$, se suele tomar la *extensión*

$$\Gamma[N] = \Gamma(N) \cup (-I)\Gamma(N), \tag{3.11}$$

que sólo coincide con $\Gamma(N)$ cuando $N = 2$ (ya que $-I \in \Gamma(2)$). Para $N > 2$, $\Gamma(N) \neq \Gamma[N]$ aunque siempre $\overline{\Gamma}[N] = \overline{\Gamma}(N)$, de modo que en cualquier caso se tiene $\phi(\Gamma(N)) = \phi(\Gamma(N) \cup (-I)\Gamma(N)) = \overline{\Gamma}(N)$.

Definicion 3.2. (Grupo modular de nivel N) El grupo $\overline{\Gamma}_N = PSL_2(\mathbb{Z}_N)$ se denomina *grupo modular de nivel N*.

Así, las transformaciones del grupo modular de nivel N tienen coeficientes en el anillo de enteros $\mathbb{Z}_N$. Se verifica el siguiente

Teorema 3.2. *Sean los grupos modulares $\overline{\Gamma} = PSL_2(\mathbb{Z})$ sobre $\mathbb{Z}$ y $PSL_2(\mathbb{Z}_N)$ sobre $\mathbb{Z}_N$, se tiene el isomorfismo*

$$\overline{\Gamma}_N := PSL_2(\mathbb{Z}_N) \cong \overline{\Gamma}/\overline{\Gamma}(N), \tag{3.12}$$

donde el grupo $\overline{\Gamma}_N$ tiene orden $\left|\overline{\Gamma}_N\right|$ igual al índice de $\overline{\Gamma}(N)$ en $\overline{\Gamma}$ y se relaciona con $|\Gamma_N| = |\Gamma/\Gamma(N)|$ como sigue:

$$\left|\overline{\Gamma}_N\right| = |\Gamma/\Gamma[N]| = \frac{1}{2}|\Gamma/\Gamma(N)|.$$

Ahora sí, calculemos el orden de los subgrupos principales y especiales de congruencia, para lo cual comenzamos con un lema (demostrado en [29], p.106) que involucra la factorización de un número natural en factores primos, y seguidamente un teorema.

Lema 3.2. *Sea $N = \prod_p p^\alpha$ donde cada p es primo, entonces*

$$SL_2(\mathbb{Z}_N) \cong \prod_p SL_2(\mathbb{Z}_p). \tag{3.13}$$

Teorema 3.3. *Si p es primo, se tiene la siguiente expresión para el orden:*

$$\left|SL_2\left(\mathbb{Z}_p\right)\right| = p(p^2-1). \tag{3.14}$$

Demostración. Sea $GL_2\left(\mathbb{Z}_p\right)$ el grupo de matrices invertibles con entradas residuos módulo p, como $|A| \neq 0 \ \forall A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2\left(\mathbb{Z}_p\right)$ los vectores (a,b) y (c,d) son linealmente independientes. Para cada una de los p^2-1 posibles (a,b) (todos menos el $(0,0)$) hay p^2-p posibles (c,d) (todos menos los paralelos al vector (a,b)), con lo que $\left|GL_2(\mathbb{Z}_p)\right| = (p^2-1)(p^2-p)$. Para finalizar, como $\det(B) = 1 \ \forall B \in SL_2\left(\mathbb{Z}_p\right)$ entonces $GL_2(\mathbb{Z}_p)/SL_2(\mathbb{Z}_p) \cong \mathbb{Z}_p - \{0\}$ y por tanto $\left|GL_2(\mathbb{Z}_p)\right| / \left|SL_2(\mathbb{Z}_p)\right| = \left|\mathbb{Z}_p - \{0\}\right|$, esto es,

$$\left|\Gamma_p\right| = \left|SL_2\left(\mathbb{Z}_p\right)\right| = (p^2-1)(p^2-p)/(p-1) = p(p^2-1). \tag{3.15}$$

□

Además, como $\overline{\Gamma} \cong \Gamma/\{\pm I\}$ y además $-I \in \Gamma(N)$ si y sólo si $N = 2$, entonces:

Teorema 3.4. *El orden del grupo modular de nivel p con p primo viene dado por*

$$\left|\overline{\Gamma}_p\right| = \left|PSL_2\left(\mathbb{Z}_p\right)\right| = \begin{cases} \frac{p(p^2-1)}{2} & si \quad p > 2 \\ \\ 6 & si \quad p = 2 \end{cases}. \tag{3.16}$$

Veamos qué ocurre con el caso más general, en el que N puede ser o no un número primo. Para ello, necesitamos algunos resultados de Teoría de Números cuyas demostraciones se pueden encontrar en [29]. Comencemos, pues, con una proposición que nos permitirá relacionar el número de soluciones de una congruencia con el orden de los subgrupos, para a continuación exponer en un teorema la fórmula para el cálculo del orden.

Proposicion 3.2. *El orden del subgrupo $SL_2(\mathbb{Z}_N)$, coincide con el número de soluciones (no congruentes entre sí) de la ecuación $ad - bc \equiv 1 \mod N$. Si $N = \prod_p p^\alpha$ entonces*

$$|SL_2(\mathbb{Z}_N)| = \prod_p \left|SL_2(\mathbb{Z}_{p^\alpha})\right|. \tag{3.17}$$

Demostración. Es deducción directa del Teorema Chino del Resto, puesto que los p^α son evidentemente coprimos. □

Teorema 3.5.

$$|\Gamma_N| = |SL_2(\mathbb{Z}_N)| = \prod_{p|N} p^{3\alpha}\left(1 - 1/p^2\right) = N^3 \prod_{p|N}\left(1 - 1/p^2\right), \tag{3.18}$$

$$\left|\overline{\Gamma}_N\right| = |PSL_2(\mathbb{Z}_N)| = \begin{cases} \frac{N^3}{2}\prod_{p|N}\left(1 - \frac{1}{p^2}\right) & si \quad N > 2 \\ \\ 6 & si \quad N = 2 \end{cases}. \tag{3.19}$$

Demostración. Sea $\phi(N)$ el cardinal del conjunto de coprimos menores que N, donde ϕ es la *función de Euler*. Veamos cómo utilizar dicha función para calcular el orden en el caso simplificado $N = p^\alpha$, con lo que podríamos obtener una fórmula general para el orden de $SL_2(\mathbb{Z}_N)$ basándonos en la proposición (3.2). Es claro que existen $\phi(p^\alpha)$ soluciones para a (mód p^α) con a, p coprimos, y para cada solución podemos elegir p^α valores de b y p^α valores de c, quedando d determinado. Análogamente, si $p|a$ existen $p^{\alpha-1}$ posibles elecciones de a (mód p^α) (múltiplos de p menores que p^α e incluyendo el 0), cada una de las cuales permite elegir p^α posibles residuos d (mód p^α) y $\phi(p^\alpha)$ valores para b y para c. Por tanto, utilizando la proposición (3.2) se tiene

$$\left|SL_2(\mathbb{Z}_{p^\alpha})\right| = \phi(p^\alpha)p^{2\alpha} + \phi(p^\alpha)p^{2\alpha-1} = p^{3\alpha}(1 - 1/p^2).$$

Con este razonamiento unido a (3.8) llegamos a las expresiones buscadas. □

Corolario 3.1.

$$|SL_2(\mathbb{Z}_N)| = \phi(N)\,|GL_2(\mathbb{Z}_N)| \tag{3.20}$$

Demostración. Sea la aplicación *determinante*

$$\det : GL_2(\mathbb{Z}_N) \longmapsto \{\text{elementos invertibles en } \mathbb{Z}_N\}.$$

Es claro que, como ocurre en el caso $N = p$ primo, $\ker(\det) = SL_2(\mathbb{Z}_N)$. Ahora bien, el conjunto de llegada de la aplicación corresponde, por definición, al *anillo de unidades de* $\mathbb{Z}_N$, denominado $\mathbb{U}(\mathbb{Z}_N)$, y cuyo orden es $\phi(N)$. Por tanto, se tiene $|SL_2(\mathbb{Z}_N)| = |GL_2(\mathbb{Z}_N)|/\phi(N)$. □

Definimos ahora un tipo de subgrupos más general:

Definicion 3.3. (Subgrupo de congruencia) Sea $\Gamma(N)$ subgrupo principal de congruencia de nivel N, y $\Omega \subseteq \Gamma$ un subgrupo del grupo modular. Se dice que Ω es un *subgrupo de congruencia* si $\Gamma(N) \subseteq \Omega$. Al menor N tal que $\Gamma(N) \subseteq \Omega$ se le denomina *conductor* de Ω (nomenclatura según T. Miyake, ver [29]) o simplemente *nivel* (según Klein).

El concepto de nivel de un subgrupo tiene una gran profundidad e irá tomando lugar en posteriores secciones. Por ello, reservamos un apartado en el núcleo del capítulo para discutir distintas definiciones del concepto, según Klein y Wohlfahrt, así como la equivalencia entre las mismas bajo ciertas condiciones. De momento, nos conviene para el propósito actual de esta sección adelantar un teorema de considerable importancia, y que es consecuencia de que

$$U^N = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma(N).$$

Teorema 3.6. *Si* $\Gamma(N) \subseteq \Omega$*, entonces* $\forall A \in \Gamma$ *se cumple*

$$AU^N A^{-1} \in \Omega. \tag{3.21}$$

En particular, el conductor (o nivel) es el menor N que cumple dicha propiedad.

Dedicaremos una sección completa a la definición y estudio del concepto de nivel. Definimos ahora una clase especial de subgrupos de congruencia:

Definicion 3.4. (Subgrupos especiales de congruencia) Sea $\Gamma = SL_2(\mathbb{Z})$ y $N \in \mathbb{N}$, definamos una serie de *subgrupos especiales de congruencia*[1].

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \mod N \right\} \tag{3.22}$$

[1] Algunos autores como T. Miyake los denominan *subgrupos de congruencia de tipo Hecke*, por ejemplo en [29], pero evitaremos tal nombre para no provocar confusión con los *grupos de Hecke* que veremos más adelante.

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; b \equiv 0 \mod N \right\} \tag{3.23}$$

$$\Gamma_0^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; b \equiv c \equiv 0 \mod N \right\} \tag{3.24}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \text{ y } a \equiv d \equiv 1 \mod N \right\} \tag{3.25}$$

El número natural N de todos los subgrupos definidos coincide con el *nivel* del subgrupo.

Proposicion 3.3. *Para los subgrupos anteriores, se tiene la siguiente igualdad cuando $N = 1$:*

$$\Gamma = \Gamma(1) = \Gamma_0(1) = \Gamma^0(1) = \Gamma_0^0(1) = \Gamma_1(1). \tag{3.26}$$

Además, si $M|N$ entonces $\Gamma(N) \subset \Gamma(M)$, $\Gamma_0(N) \subset \Gamma_0(M)$, $\Gamma^0(N) \subset \Gamma^0(M)$, $\Gamma_0^0(N) \subset \Gamma_0^0(M)$ y $\Gamma_1(N) \subset \Gamma_1(M)$.

Índice de los subgrupos de congruencia.
Calculemos ahora el índice de los subgrupos de congruencia vistos:

Teorema 3.7. *Sean $\Gamma_0(N), \Gamma^0(N), \Gamma_0^0(N)$ y $\Gamma_1(N)$ los subgrupos de congruencia definidos en (3.4), su índice viene dado por:*

1. $\left|\overline{\Gamma} : \overline{\Gamma}(N)\right| = \begin{cases} \frac{1}{2}|\Gamma : \Gamma(N)| = \frac{1}{2}N^3 \prod_{p|N}(1 - 1/p^2) & si \quad N > 2 \\ |\Gamma : \Gamma(2)| = 6 & si \quad N = 2 \end{cases}$.
2. $|\Gamma : \Gamma_0(N)| = \left|\overline{\Gamma} : \overline{\Gamma}_0(N)\right| = N \prod_{p|N}(1 + 1/p)$ *(ídem para $\left|\Gamma : \Gamma^0(N)\right|$).*
3. $\left|\Gamma : \Gamma_0^0(N)\right| = \left|\overline{\Gamma} : \overline{\Gamma}_0^0(N)\right| = N^2 \prod_{p|N}(1 + 1/p)$.
4. $\left|\overline{\Gamma}_0(N) : \overline{\Gamma}_1(N)\right| = \begin{cases} \frac{1}{2}|\Gamma_0(N) : \Gamma_1(N)| = \phi(N)/2 & si \quad N > 2 \\ |\Gamma_0(2) : \Gamma_1(2)| = 1 & si \quad N = 2 \end{cases}$.

Demostración. Dado un subgrupo $\Omega \subset \Gamma$, retomemos la notación $\mu = |\Gamma : \Omega|$ y $\overline{\mu} = \left|\overline{\Gamma} : \overline{\Omega}\right|$. Vimos que $\mu = \overline{\mu}$ si $-I \in \Omega$ y $\frac{1}{2}\mu = \overline{\mu}$ si $-I \notin \Omega$, de donde se desprende que

$$|\Gamma : \Gamma_0(N)| = \left|\overline{\Gamma} : \overline{\Gamma}_0(N)\right| = \left|\Gamma : \Gamma^0(N)\right| = \left|\overline{\Gamma} : \overline{\Gamma}^0(N)\right| \tag{3.27}$$

y además, como la congruencia $ad - bc \equiv 1 \mod N$ tiene $\phi(N)$ soluciones si $b \equiv c \equiv 0$ y $N\phi(N)$ soluciones si $b \equiv 0$ o bien $c \equiv 0$, se tiene

$$|\Gamma : \Gamma_0(N)| = \frac{|\Gamma(N)|}{N\phi(N)} = \{\text{teorema (3.5)}\} = N \prod_{p|N}(1 + 1/p) \tag{3.28}$$

y

$$\left|\Gamma : \Gamma_0^0(N)\right| = \frac{|\Gamma(N)|}{\phi(N)} = N^2 \prod_{p|N}(1 + 1/p). \tag{3.29}$$

□

Corolario 3.2. $\left|\Gamma_0(N) : \Gamma_0^0(N)\right| = N$ *y si* $N > 2$ *entonces* $|\Gamma : \Gamma_1(N)| = \prod_{p|N}\left(1 + \frac{2}{p-1}\right)$.

Demostración. En la última igualdad se ha utilizado que

$$\phi(N) = |\Gamma_0(N) : \Gamma_1(N)| = |\Gamma_0(N) : \Gamma_1(N)|/|\Gamma : \Gamma_1(N)| = \frac{N\prod_{p|N}(1 + 1/p)}{|\Gamma : \Gamma_1(N)|}$$

luego

$$|\Gamma : \Gamma_1(N)| = \frac{N\prod_{p|N}(1 + 1/p)}{N\prod_{p|N}(1 - 1/p)} = \prod_{p|N}\frac{p+1}{p-1} = \prod_{p|N}\left(1 + \frac{2}{p-1}\right).$$

□

Consideraciones sobre la notación.
En las secciones que completan este capítulo eliminaremos, por simplicidad, la distinción entre los grupos modulares $\overline{\Gamma}$ y Γ, y denotaremos simplemente como Γ al grupo modular de matrices 2×2 con $ad - bc = 1$, en el que se identifica cada matriz con su opuesta[2]. Análogamente, hablaremos de subgrupos principales de congruencia (extendidos) $\Gamma[N]$ considerando que en ellos se da también la identificación $I \sim -I$. Asimismo, se hablará indistintamente de la matriz A y de su transformación asociada A.

3.2. Subgrupo conmutador y subgrupo potencia

En esta sección vamos a presentar y estudiar dos subgrupos normales de gran relevancia dentro del retículo de subgrupos normales del grupo modular. En la penúltima sección del capítulo se darán varios resultados sobre subgrupos normales que requerirán algunos de los conceptos que se van a exponer inmediatamente. Haremos referencia a Γ como el grupo modular de matrices 2×2 con $ad - bc = 1$, identificando cada matriz con su opuesta. Como desde el inicio de este documento, trabajemos con las matrices generadoras

$$T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, R = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

y teniendo en mente que $U = TR$ y $R = TU$.

[2]Esta notación no debe causar confusión, dado que en multitud de artículos se define precisamente Γ de esta manera, y se toman subgrupos conteniendo a $-I$ para evitar problemas con el cálculo de índices.

3.2.1. Subgrupo conmutador

Necesitamos unos preliminares generales sobre el subgrupo conmutador de un grupo:

Definicion 3.5. (Subgrupo conmutador) Sea un grupo G, se define su *subgrupo conmutador* G' como sigue:

$$G' = \left\langle \ [x,y] = xyx^{-1}y^{-1} \ \middle| \ x,y \in G \ \right\rangle. \tag{3.30}$$

Proposicion 3.4. *Sea G un grupo y G' su subgrupo conmutador. Entonces $G' \lhd G$ y además G es abeliano si y sólo si G' es trivial.*

Demostración. La segunda afirmación es inmediata, pues dos elementos $x,y \in G$ conmutan si y sólo si $[x,y] = 1$. Para la primera, tomamos $h \in G'$, $g \in G$ y comprobamos que $ghg^{-1} = ghg^{-1}h^{-1}h = [g,h]h \in G'$. □

Definicion 3.6. (Abelianización) Sea G un grupo y G' su subgrupo conmutador. El grupo G/G' se denomina *abelianización* de G.

Proposicion 3.5. *Sea G un grupo y G' su subgrupo conmutador. La abelianización G/G' es un grupo abeliano y, de hecho, cualquier otro subgrupo $H \lhd G$ tal que G/H es abeliano contiene a G'.*

La última proposición pone de manifiesto que el subgrupo conmutador G' es el mínimo subgrupo normal H tal que el cociente G/H es abeliano, de donde se desprende el siguiente lema:

Lema 3.3. *Sea $G = \langle x,y \rangle$ y $N \lhd \Omega$, si se cumple $[x,y] \in N$ entonces $G' \subset N$.*

Demostración. Cojamos un subgrupo $H \lhd G$ tal que G/H es abeliano. Entonces, para todo conmutador $[x,y] \in G$ se tiene que $[x,y] \equiv 1 \mod H$ puesto que G/H es abeliano. Por consiguiente, $[x,y] \in H$, y con ello $G' \subseteq H$. □

Así, para nuestro grupo de estudio Γ, tenemos el subgrupo conmutador $\Gamma' \lhd \Gamma$. Vamos a comenzar viendo su rango y su índice en Γ, tomando resultados de J.Nielsen y M.Newman ([37] y [30]):

Proposicion 3.6. *Sea $\Gamma' \lhd \Gamma$ el subgrupo conmutador, tiene índice $\left|\Gamma : \Gamma'\right| = 6$ y rango 2, esto es, el mínimo conjunto de generadores tiene 2 elementos:*

$$\Gamma' = \left\langle a = TRTR^2, b = TR^2TR \right\rangle, \tag{3.31}$$

donde los generadores a y b son las transformaciones con representación matricial

$$a = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},\ b = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}. \tag{3.32}$$

Obsérvese que, como $T^2 = I$ *y* $R^3 = I$ *entonces* $a = [T,R]$ *y* $b = \left[T,R^{-1}\right]$. *Además, el grupo modular se puede descomponer como*

$$\Gamma = \sum_{k=0}^{5} U^k \Gamma'. \tag{3.33}$$

Demostración. Ver artículos de M.Newman y J.Nielsen ([30] y [37], respectivamente). □

De la proposición anterior se deduce que la abelianización Γ/Γ' es un grupo abeliano cíclico de 6 elementos, generado por $T\Gamma'$ y $R\Gamma'$ (recordemos que T y R generan el grupo modular). Así, la abelianización del grupo modular admite la presentación

$$\Gamma/\Gamma' = \left\langle \ T,R \ \middle| \ T^2 = R^3 = I, TR = RT \ \right\rangle. \tag{3.34}$$

Segundo subgrupo conmutador.
Extendamos la noción de subgrupo conmutador, para poder afrontar el arduo desarrollo de la teoría relativa a la clasificación de los subgrupos normales de Γ, con la siguiente definición:

Definicion 3.7. Sea un grupo G y G' el subgrupo conmutador. Se define su *segundo subgrupo conmutador* G'' como sigue:

$$G'' = \left\langle \ [x,y] = xyx^{-1}y^{-1} \ \middle| \ x,y \in G' \ \right\rangle. \tag{3.35}$$

Este subgrupo Γ'' es normal en Γ y, además, es un grupo libre de rango infinito y con índice $\left|\Gamma' : \Gamma''\right|$ infinito (Kurosh, [24]). Este hecho no es cierto para la abelianización Γ'/Γ'' que veremos más adelante. Este subgrupo permite establecer una relación de equivalencia en Γ:

$$x,y \in \Gamma \text{ cumplen } x \sim y \text{ si y sólo si } xy^{-1} \in \Gamma''. \tag{3.36}$$

Si denominamos $e_a(w)$ (respectivamente $e_b(w)$) a la suma de los exponentes de base $a = [T,R]$ (respectivamente $b = \left[T,R^{-1}\right]$) en la palabra $w \in \Gamma'$, se tiene la siguiente caracterización:

Proposicion 3.7. *Sean* $x,y \in \Gamma$ *con la relación de equivalencia vista, entonces si* $x,y \in \Gamma'$ *se tiene que*

$$x \sim y \text{ si y sólo si } e_a(x) = e_a(y) \text{ y } e_b(x) = e_b(y). \tag{3.37}$$

La gran utilidad de los subgrupos conmutadores Γ' y Γ'' reside en su estrecha relación con todos los subgrupos normales de Γ de *género* 1, donde el concepto de género, que estudiaremos más adelante, tiene que ver con el *número de agujeros* de la superficie de Riemann que aparece como espacio de órbitas $\mathscr{U}/\Omega$. En esta búsqueda de subgrupos normales destacan los trabajos de Newman ([30],[32] y [35]). Para profundizar en la relación mencionada, necesitamos una propiedad y un lema previos:

Proposicion 3.8. *Sea $C(w) = UwU^{-1}$ la conjugación de $w \in \Gamma$ por U, se tiene que $C(a) = ab^{-1}$ y $C(b) = a$.*

Demostración. $C(a) = C(TRTR^2) = UTRTR^2U^{-1} = \begin{pmatrix} 3 & -1 \\ 1 & 0 \end{pmatrix}$, y se comprueba igualmente que $C(a) = ab^{-1} = TRTR^2(TR^2TR)^{-1} = \begin{pmatrix} 3 & -1 \\ 1 & 0 \end{pmatrix}$. El caso de $C(b) = a$ es similar. □

Lema 3.4. *Sea $\Omega \lhd \Gamma'$, entonces $\Omega \lhd \Gamma$ si y sólo si $C(\Omega) \subset \Omega$.*

La demostración se sigue inmediatamente de (3.33). Veamos con más detalle el siguiente resultado:

Lema 3.5. *Sea $\Omega \lhd \Gamma$ y $\Gamma'' \subset \Omega$. Si $U^{\alpha_1}a^{\alpha_2}b^{\alpha_3} \in \Omega$ y $U^{\beta_1}a^{\beta_2}b^{\beta_3} \in \Omega$ entonces $U^{\alpha_1+\beta_1}a^{\alpha_2+\beta_2}b^{\alpha_3+\beta_3} \in \Omega$.*

Demostración. Sea $U^{\beta_1}a^{\beta_2}b^{\beta_3} \in \Omega$, como $\Omega \lhd \Gamma$ entonces $U^{-\beta_1}U^{\beta_1}a^{\beta_2}b^{\beta_3}U^{\beta_1} = a^{\beta_2}b^{\beta_3}U^{\beta_1} \in \Omega$, y como $U^{\alpha_1}a^{\alpha_2}b^{\alpha_3} \in \Omega$ entonces $U^{\alpha_1}a^{\alpha_2}b^{\alpha_3}a^{\beta_2}b^{\beta_3}U^{\beta_1} \in \Omega$, con lo que de nuevo por normalidad $U^{\beta_1}U^{\alpha_1}a^{\alpha_2}b^{\alpha_3}a^{\beta_2}b^{\beta_3}U^{\beta_1}U^{-\beta_1} = U^{\beta_1+\alpha_1}a^{\alpha_2}b^{\alpha_3}a^{\beta_2}b^{\beta_3} \in \Omega$. Ahora bien, por la relación (3.36) se tiene que $a^{\alpha_2}b^{\alpha_3}a^{\beta_2}b^{\beta_3} \sim a^{\alpha_2+\beta_2}b^{\alpha_3+\beta_3}$, y como $\Gamma'' \subset \Omega$ hemos terminado. □

Establezcamos por fin el resultado más importante de la sección:

Teorema 3.8. *Sea $\Omega \lhd \Gamma$ con género 1, entonces $\Gamma'' \subset \Omega \subset \Gamma'$.*

De cara a demostrar este teorema, necesitamos recuperar el concepto de *género*, esta vez en el contexto de un grupo fuchsiano:

Definicion 3.8. (Género de un grupo fuchsiano) Sea Γ un grupo fuchsiano. Se llama *género* del grupo al género de la superficie $S = \mathscr{U}/\Gamma$, entendido como número de asas de S.

Así, el género de un subgrupo normal del grupo modular Γ coincide con el género de la superficie de Riemann que, como veremos, aparece como espacio de órbitas $\mathscr{U}/\Gamma$. Otra propiedad que necesitamos utilizar es que Γ'' es el subgrupo normal de Γ más pequeño que contiene a U^6, hecho que vamos a demostrar inmediatamente a través del siguiente lema (Newman, [31]):

Lema 3.6. *Sea $\Delta(6)$ el subgrupo normal de Γ más pequeño que contiene a U^6, y Γ'' el segundo subgrupo conmutador de Γ. Entonces:*

$$\Delta(6) = \Gamma''. \tag{3.38}$$

Demostración. Ya vimos que Γ' es un subgrupo libre, de rango 2 y generado por los elementos

$$a = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \text{ y } b = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

En este caso, tomaremos los generadores

$$a = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \text{ y } b' = b^{-1} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix},$$

de forma que el conmutador $[a, b']$ resulta ser

$$[a, b'] = ab'a^{-1}b'^{-1} = \begin{pmatrix} -1 & -6 \\ 0 & -1 \end{pmatrix} = U^6,$$

luego $U^6 \in \Gamma''$. Como Γ'' es normal en Γ y $[a, b'] = U^6 \in \Delta(6)$ entonces $\Gamma'' \subseteq \Delta(6)$. Para terminar, como $\Delta(6)$ es el subgrupo más pequeño que contiene a U^6, necesariamente se tiene la igualdad. □

Utilizaremos un último lema debido a R.C.Gunning (demostración en [14]) que retoma el concepto de nivel de un subgrupo normal, el mínimo N entero tal que U^N pertenece al subgrupo:

Lema 3.7. *Todo subgrupo normal $\Omega \lhd \Gamma$ con género 1 tiene nivel 6.*

De este último lema se deduce que todo subgrupo normal en Γ con género 1 contiene a U^6 pero no a U^k si $k \leq 6$ y, por consiguiente, nos permite observar que, en particular, el subgrupo principal de congruencia $\Gamma[6]$ tiene género 1. Tras estos resultados previos, estamos en condiciones de comenzar la prueba del teorema.

Demostración. (Teorema (3.8)) En primer lugar, $U^6 \in \Omega$ dado que Ω tiene género 1, luego se tiene que $\Gamma'' \subset \Omega$. Entonces, por ser U generador de Γ podemos escribir $g = U^k g' \in \Omega$ con $g' \in \Gamma'$ y $k = 0, 1, \cdots, 5$. Como a su vez $g' = a^{\alpha_1} b^{\alpha_2} g''$ con $g'' \in \Gamma''$ entonces $g = U^k a^{\alpha_1} b^{\alpha_2} g''$ y además $U^k a^{\alpha_1} b^{\alpha_2} \in \Omega$ porque $\Gamma'' \subset \Omega$. Con ello, utilizando que $\Omega \lhd \Gamma$ se tiene $C(U^k a^{\alpha_1} b^{\alpha_2}) \in \Omega$, con lo que aplicando reiteradamente (3.8) se llega a que $g \in \Gamma'$, con lo que $\Omega \subset \Gamma'$. □

Estudio de Ω/Γ'' con $\Omega \lhd \Gamma$.
Visto que todo $\Omega \lhd \Gamma$ con género 1 cumple $\Gamma'' \subset \Omega \subset \Gamma'$, es claro que Γ/Γ' y Γ'/Γ'' son abelianos, con lo que cabe preguntarse qué ocurre con Ω/Γ''. Asimismo, al igual que Γ/Γ' tiene generadores $T\Gamma'$ y $R\Gamma'$, veamos que el grupo Ω/Γ'' también se puede generar con dos elementos.

Teorema 3.9. *Sea Ω normal en Γ y tal que $\Omega \neq \Gamma''$. El grupo Ω/Γ'' es abeliano no cíclico con dos generadores.*

Demostración. Comenzamos recordando que Γ'' es libre con índice infinito en Γ'. Así, como $\Omega/\Gamma'' \subset \Gamma'/\Gamma''$ y Γ'/Γ'' es abeliano libre con dos generadores ($a\Gamma''$ y $b\Gamma''$), se tiene que o bien Ω/Γ'' es cíclico o bien es abeliano libre. Supongamos que es cíclico con generador $a^s b^t \Gamma''$. En esta situación, como $\Omega \lhd \Gamma$ debe existir k entero tal que

$$C(a^s b^t) \sim (a^s b^t)^k, \ \left((ab^{-1})^s a^t\right) \sim (a^s b^t)^k$$

con la relación de equivalencia descrita en (3.36). De esta última expresión se desprende que $(k-1)s-t=0$ y $s+kt=0$, sistema cuya única solución es $s=t=0$, valores que implican que $\Omega=\Gamma''$, imposible puesto que $\Omega\neq\Gamma''$ por hipótesis. El grupo Ω/Γ'' no puede ser cíclico y, por tanto, es abeliano libre con dos generadores $A\Gamma''$ y $B\Gamma''$, A,B descritos en los siguientes teoremas. □

Existe una correspondecia uno a uno entre los $\Omega\lhd\Gamma$ de género 1, que según hemos visto cumplirían $\Gamma''\subset\Omega\subset\Gamma'$, y las tripletas ordenadas de enteros positivos bajo ciertas condiciones (Newman, [32]). Veamos esta equivalencia, que permite además deducir numerosas propiedades.

Teorema 3.10. *Buscar los $\Omega\lhd\Gamma$ tales que $\Gamma''\subset\Omega\subset\Gamma'$ es equivalente a buscar $(p,m,d)\in\mathbb{Z}^3$ cumpliendo:*

1. $p>0$
2. $m\in[0,d-1]$
3. $m^2+m+1\equiv 0$ *(mód d)*

y además se tiene la descomposición $\Omega=\sum A^kB^l\Gamma''$, con $A=a^pb^{mp}$ y $B=b^{dp}$. Así, el grupo Ω/Γ'' está generado por $A\Gamma''=a^pb^{mp}\Gamma''$ y $B\Gamma''=b^{dp}\Gamma''$.

Encontrados estos tres enteros p, m y d, podemos aplicar la notación $\Omega:=(p,m,d)$. A continuación enunciamos algunos teoremas y resultados útiles demostrados en los trabajos de Newman, y que relacionan la teoría de subgrupos conmutadores vista con relaciones de congruencia.

Teorema 3.11. *Sea $\Omega=(p,m,d)$, se tiene que*

$$\left|\Gamma':(p,m,d)\right|=dp^2$$

y

$$\Gamma'=\sum a^rb^s\Omega,$$

donde $r\in[0,p-1]$ y $s\in[0,dp-1]$. Además, no existe un único $\Omega\lhd\Gamma$ con el índice descrito, existiendo de hecho una expresión para el número $\psi(q^n)$ de subgrupos normales en Γ con género 1 e índice $6q^n$ (en Γ), siendo q primo:

$$\psi(q^n)=\begin{cases}\frac{1+(-1)^n}{2} & si\quad q=2\\ 1 & si\quad q=3\\ \frac{1+(-1)^n}{2}+\left(\left[\frac{n}{2}\right]-(-1)^n\right)(1+q/3) & si\quad q>3\end{cases}, \tag{3.39}$$

donde $\left[\frac{n}{2}\right]$ *es la parte entera y* $q/3$ *el símbolo de Legendre-Jacobi de reciprocidad cuadrática, definido como*

$$a/p = \begin{cases} 0 & si \quad p|a \\ 1 & si \quad \exists x / x^2 \equiv a \ (mód\ p) \\ -1 & si \quad otro\ caso \end{cases} . \tag{3.40}$$

Teorema 3.12. *Sea* $\Gamma[N]$ *el subgrupo principal de congruencia de nivel* N *(con la identificación* $I \sim -I$*), se cumple* $\left|\Gamma' : \Gamma[6]\right| = 72$ *y además* $\Gamma[6] := (2,1,3)$.

Demostración. Ya hemos visto que $|\Gamma : \Gamma[6]| = 72$ y por otro lado $\left|\Gamma : \Gamma'\right| = 6$, con lo que

$$\left|\Gamma' : \Gamma[6]\right| = |\Gamma[6] : \Gamma| / \left|\Gamma' : \Gamma\right| = 72/6 = 12.$$

Obsérvese que $\Gamma'' \subset \Gamma[6] \subset \Gamma'$ dado que $\Gamma[6]$ es normal en Γ y tiene género 1. Así, $\left|\Gamma' : \Gamma[6]\right| = 12 = dp^2$ y la única solución posible bajo las condiciones del teorema (3.10) es $(p,m,d) = (2,1,3)$. □

Los resultados de esta sección permiten caracterizar los subgrupos normales de género 1, hecho que cobra forma en el siguiente corolario:

Corolario 3.3. *Sea la terna* (p,m,d) *de enteros bajo las condiciones del teorema (3.10), entonces existe un grupo* $\Omega \lhd \Gamma$ *de género 1 tal que*

$$\Omega = \left\{ \ w \in \Gamma' \ \middle| \ e_a(w) \equiv 0 \mod p \text{ y } e_b(w) \equiv m \cdot e_a(w) \mod dp \ \right\}. \tag{3.41}$$

Por ejemplo, $\Gamma[6] := (2,1,3) = \left\{ \ w \in \Gamma' \ \middle| \ e_a(w) \equiv 0 \mod 2 \text{ y } e_b(w) \equiv 1 \cdot e_a(w) \mod 6 \ \right\}$.

3.2.2. Subgrupo potencia

Como último tipo importante de subgrupos normales de Γ, vamos a estudiar el subgrupo potencia y vamos a establecer como conclusión las conexiones existentes entre Γ, ciertos subgrupos potencia y el subgrupo conmutador. Comencemos por tanto con la definición:

Definicion 3.9 (Subgrupo potencia)**.** Se define el subgrupo potencia Γ^m, con $m \in \mathbb{Z}$, como

$$\Gamma^m = \left\langle \ A^m \ \middle| \ A \in \Gamma, m \in \mathbb{Z} \ \right\rangle. \tag{3.42}$$

Este subgrupo es normal en Γ y además cumple las siguientes propiedades de naturaleza evidente:

1. $\Gamma^{mn} \subset \Gamma^m$, $\forall m,n \in \mathbb{Z}$.
2. $\Gamma^{mn} \subset (\Gamma^m)^n$, $\forall m,n \in \mathbb{Z}$.

3. $\Gamma^m\Gamma^n = \Gamma^{(m,n)}$, $\forall m,n \in \mathbb{Z}$, con $(m,n) := \text{MCD}(m,n)$. Como consecuencia directa, se tiene

$$\Gamma = \Gamma^2\Gamma^3. \tag{3.43}$$

Demostración. (de la afirmación 2) En primer lugar, como $\Gamma^m, \Gamma^n \subset \Gamma^{(m,n)}$ se sigue que $\Gamma^m\Gamma^n \subset \Gamma^{(m,n)}$, con lo que falta ver la otra inclusión. Si $A \in \Gamma^{(m,n)}$ y, por la identidad de Bezout, $\alpha m + \beta n = (m,n)$ con $\alpha, \beta \in \mathbb{Z}$, entonces como $A^{\alpha m} \in \Gamma^m$ y $A^{\beta n} \in \Gamma^n$ se deduce que $A^{\alpha m}A^{\beta n} = A^{\alpha m+\beta n} = A^{(m,n)} \in \Gamma^m\Gamma^n$, por tanto $\Gamma^{(m,n)} \subset \Gamma^m\Gamma^n$ y hemos terminado. □

Detengámonos unos instantes en la identidad $\Gamma = \Gamma^2\Gamma^3$ para estudiar la estructura algebraica de Γ^2 y Γ^3 a través de dos teoremas que demostró Newman en [30]:

Teorema 3.13. *Sea* $\Gamma^2 = \left\langle \; A^2 \;\middle|\; A \in \Gamma \; \right\rangle$*, se cumplen los siguientes enunciados:*

- Γ^2 *es el producto libre de 2 grupos cíclicos de orden 3. Así,* $\left|\Gamma : \Gamma^2\right| = 2$ *y con ello podemos expresar* $\Gamma = \Gamma^2 + T\Gamma^2$.
- Γ^2 *es isomorfo al grupo generado por* R *y* TRT.
- $\Gamma^2 = \left\{ \; A \in \Gamma \;\middle|\; e_T(A) \equiv 0 \mod 2 \; \right\}$.

Teorema 3.14. *Sea* $\Gamma^3 = \left\langle \; A^3 \;\middle|\; A \in \Gamma \; \right\rangle$*, se cumplen los siguientes enunciados:*

- Γ^3 *es el producto libre de 3 grupos cíclicos de orden 2. Así,* $\left|\Gamma : \Gamma^3\right| = 3$ *y con ello podemos expresar* $\Gamma = \Gamma^3 + R\Gamma^3 + R^2\Gamma^3$.
- Γ^3 *es isomorfo al grupo generado por* R, RTR^2 *y* R^2TR.
- $\Gamma^3 = \left\{ \; A \in \Gamma \;\middle|\; e_T(A) \equiv 0 \mod 3 \; \right\}$.

Antes de establecer la conexión con el subgrupo conmutador, necesitamos establecer tres identidades en las que intervienen congruencias:

Proposicion 3.9. *Sea* Γ^m *el grupo potencia, se cumplen las siguientes relaciones:*

- $\Gamma^m = \Gamma$ *si* $(m,6) = 1$,
- $\Gamma^{2m} = \Gamma^2$ *si* $(m,3) = 1$,
- $\Gamma^{3m} = \Gamma^3$ *si* $(m,2) = 1$.

Demostración. Indicación: se utiliza el hecho de que $T^2 = I$ y $R^3 = I$, con lo que para probar la inclusión de derecha a izquierda (la otra es inmediata) sólo hay que probar, en cada caso, que los generadores están contenidos en los miembros de la izquierda, tarea sencilla puesto que $T = T^m$ y $R = R^{\pm m}$ en el primer caso, $R = R^{\pm 2m}$ en el segundo caso y $T = T^{3m}$ en el último caso. □

Por fin, llegamos a la conclusión fundamental que establece el puente con el subgrupo conmutador:

Teorema 3.15. *Sea Γ' el subgrupo conmutador, se cumple que $\Gamma' = \Gamma^2 \cap \Gamma^3$.*

Demostración. Como Γ/Γ^2 y Γ/Γ^3 son abelianos (por ser cíclicos), tanto Γ^2 como Γ^3 contienen a Γ' y por ello $\Gamma' \subset \Gamma^2 \cap \Gamma^3$. Ahora, como Γ^2 y Γ^3 son normales en Γ, se tiene el isomorfismo

$$(\Gamma^2\Gamma^3)/\Gamma^3 \cong \Gamma^2/(\Gamma^2 \cap \Gamma^3),$$

y como $\Gamma^2\Gamma^3 = \Gamma$ y $\left|\Gamma : \Gamma^3\right| = 3$, necesariamente $\left|\Gamma^2/(\Gamma^2 \cap \Gamma^3)\right| = 3$, y además se tiene

$$\left|\Gamma : \Gamma^2 \cap \Gamma^3\right| = \left|\Gamma : \Gamma^2\right| \cdot \left|\Gamma^2 : \Gamma^2 \cap \Gamma^3\right| = 2 \cdot 3 = 6 = \left|\Gamma : \Gamma'\right|,$$

de donde se desprende la igualdad $\Gamma^2 \cap \Gamma^3 = \Gamma'$. □

Existe una prueba más sencilla, que se basa en la caracterización de los elementos de Γ', Γ^2 y Γ^3 que da Petersson en [38]:

Proposicion 3.10. *Sea $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, se cumple que:*

- *$A \in \Gamma'$ si y sólo si $ab + 3bc + cd \equiv 0 \mod 6$,*
- *$A \in \Gamma^2$ si y sólo si $ab + bc + cd \equiv 0 \mod 2$,*
- *$A \in \Gamma^3$ si y sólo si $ab + cd \equiv 0 \mod 3$.*

Así, la identidad $\Gamma^2 \cap \Gamma^3 = \Gamma'$ es deducción directa.

El teorema anterior es importante de cara a demostrar, por ejemplo, que Γ^{6m} es un grupo libre para cualquier m entero (basta con apreciar que $\Gamma^{6m} \subset \Gamma^6 \subset \Gamma^2 \cap \Gamma^3 = \Gamma'$, y recordar que todo subgrupo de un grupo libre es libre). Asimismo, podemos estudiar si el subgrupo potencia Γ^6 cumple $\Gamma'' \subset \Gamma^6 \subset \Gamma'$ o bien $\Gamma^6 \subset \Gamma'' \subset \Gamma'$, obteniendo una serie de conclusiones en forma de corolario:

Corolario 3.4. *Sean Γ y Γ' los subgrupos conmutador y segundo conmutador respectivamente, y sea el subgrupo potencia Γ^6. Se cumplen los siguientes enunciados:*

1. *$\Gamma = \langle a, b \rangle$, con a, b definidos en (3.32).*
2. *$\left[a, b^{-1}\right] = U^6 \in \Gamma^6$.*
3. *$\Gamma'' \subset \Gamma^6$.*
4. *Γ'/Γ^6 es abeliano.*

Demostración. Las dos primeras afirmaciones son inmediatas. Para la tercera afirmación, poner $G = \Gamma'$ y $N = \Gamma^6$ en el lema (3.3). La cuarta de deduce inmediatamente de la tercera. □

La familia de subgrupos $\Gamma'(p,q)$.
Para p,q enteros y positivos, se denota como $\Gamma'(p,q)$ al subgrupo normal de Γ' que cumple que todo elemento $w = a^{r_1}b^{s_1}\cdots a^{r_n}b^{s_n} \in \Gamma'$ pertenece a $\Gamma'(p,q)$ si y sólo si

$$e_a(w) = \sum_{k=0}^{n} r_i \equiv 0 \mod p,\ e_b(w) = \sum_{k=0}^{n} s_i \equiv 0 \mod q. \tag{3.44}$$

Es trivial que $\Gamma'' \subset \Gamma'(p,q)$. El índice de $\Gamma'(p,q)$ como subgrupo de Γ' es

$$\left|\Gamma' : \Gamma'(p,q)\right| = pq, \tag{3.45}$$

puesto que si tomamos el subgrupo normal

$$\Gamma'(p,1) = \left\{ \ w \in \Gamma' \ \middle| \ e_a(w) \equiv 0 \mod p \ \right\}$$

se puede ver que $\left|\Gamma' : \Gamma'(p,1)\right| = p$ y $\left|\Gamma'(p,1) : \Gamma'(p,q)\right| = q$, de modo que (por el Tercer Teorema de Isomorfía)

$$\left|\Gamma' : \Gamma'(p,1\right| = \left|\Gamma' : \Gamma'(p,q)\right| / \left|\Gamma'(p,1) : \Gamma'(p,q)\right| \text{ implica } \left|\Gamma' : \Gamma'(p,q)\right| = pq.$$

Así, se tiene la descomposición

$$\Gamma' = \sum_{r,s} a^r b^s \Gamma'(p,q), \tag{3.46}$$

con $r = 0,1,\cdots,p-1$ y $s = 0,1,\cdots,q-1$. Si queremos obtener su rango como subgrupo de Γ', que tiene - según hemos visto - rango 2 como grupo libre, podemos utilizar una fórmula debida a Schreirer para calcular el rango r de un subgrupo de un grupo libre de rango R, teniendo índice i:

$$r = 1 + i(R-1). \tag{3.47}$$

Como $i = pq$ y $R = 2$ se deduce que $r = 1 + pq$.

Vamos estudiar el caso concreto en que $p = q = 6$, para establecer un puente con los subgrupos potencia ya vistos:

Teorema 3.16. *Se tiene la siguiente igualdad entre subgrupos:*

$$\Gamma'(6,6) = \Gamma^6. \tag{3.48}$$

En particular, $\left|\Gamma : \Gamma^6\right| = 216$ y Γ^6 es libre con 37 generadores, con lo que se puede descomponer Γ' como $\Gamma' = \sum_{0\le r,s\le 5} a^r b^s \Gamma^6$.

Demostración. Comencemos con la parte más sencilla. Si $\Gamma'(6,6) = \Gamma^6$ entonces por (3.45)

$$\left|\Gamma' : \Gamma^6\right| = \left|\Gamma' : \Gamma(6,6)\right| = 6^2$$

y como $\left|\Gamma : \Gamma'\right| = 6$ se deduce que $\left|\Gamma : \Gamma^6\right| = 6pq = 6^3 = 216$, y además, por la fórmula de Schreirer (3.47), el rango es $1 + pq = 1 + 6^2 = 37$, siendo así Γ^6 subgrupo libre de Γ' con 37 generadores. La siguiente fase es demostrar las inclusiones $\Gamma'(6,6) \subset \Gamma^6$ y $\Gamma^6 \subset \Gamma'(6,6)$:

- ($\subset$). Un elemento de $\Gamma'(6,6)$ puede escribirse como $w = a^{r_1}b^{s_1}\cdots a^{r_n}b^{s_n}$, con $e_a(w) \equiv_b (w) \equiv 0$ (mód 6). Como Γ'/Γ'' es abeliano, podemos escribir $w = a^{r_1+\cdots+r_n}b^{s_1+\cdots+s_n}w'$ con $w' \in \Gamma''$. La inclusión $\Gamma'' \subset \Gamma^6$ permite dar por finalizada la prueba, esto es, $w \in \Gamma^6$ $\forall w \in \Gamma'(6,6)$.

- ($\supset$). En primer lugar, tomemos un elemento $v \in \Gamma$. Ya vimos en (3.33) que existe $k \in [0,5]$ entero tal que $v = U^k v'$, con $v' \in \Gamma'$. Si elevamos este elemento,

$$v^6 = \left(U^k v'\right)^6 = \left(U^k v' U^{-k}\right)\left(U^{2k} v' U^{-2k}\right)\cdots\left(U^{6k} v' U^{-6k}\right)U^{6k},$$

  y como $U^6 = ab^{-1}a^{-1}b$ está en Γ'' (porque $e_a(U^6) = e_b(U^6) = 0$), entonces $U^6 \in \Gamma'(6,6)$. Retomando la operación de conjugación de un elemento por U, esto es, $C(v) = UvU^{-1}$, podemos expresar v^6 como sigue:

$$v^6 = C^k(v')C^{2k}(v')\cdots C^{6k}(v')U^{6k} \in \Gamma', \tag{3.49}$$

  ya que tanto v' como $C(v')$ pertenecen a Γ'. Además, como $C^j(xy) = C^j(x)C^j(y)$ para cualquier par de elementos $x, y \in \Gamma$, deben existir α y β enteros tales que $v' = a^\alpha b^\beta v_0''$, con $v_0'' \in \Gamma''$. Sustituyendo y operando en la expresión (3.49) teniendo en cuenta que Γ' es abeliano módulo Γ'', se obtiene

$$v^6 = \left(C^k(a)C^{2k}(a)\cdots C^{6k}(a)\right)^\alpha \left(C^k(b)C^{2k}(b)\cdots C^{6k}(b)\right)^\beta v'', \; v'' \in \Gamma''. \tag{3.50}$$

  Observando los exponentes de las expresiones $C^k(a)$ y $C^k(b)$ para $k = 0,\cdots,5$ (ver p.486 de [30]), se comprueba que si $k \neq 0$ entonces $v^6 \in \Gamma'' \subset \Gamma'(6,6)$, mientras que si $k = 0$ ocurre que $v^6 \in \Gamma'(6,6)$, de modo que en cualquier caso $v^6 \in \Gamma'(6,6)$.

□

Por último, no queremos dejar sin señalar y probar una última conexión entre subrupo potencia, subgrupo conmutador y subgrupo principal de congruencia con nivel 6:

Teorema 3.17. $\Gamma^6 \subset \Gamma[6] \subset \Gamma'$.

Demostración. Un primer enfoque se reduce a recordar que $\Gamma[6] = (p,m,d) = (2,1,3)$. Otra prueba consiste en apreciar, en primer lugar, que como $\Gamma[2]$ y $\Gamma[3]$ están generados por elementos de Γ^2 y Γ^3 respectivamente, utilizamos el hecho trivial de que $\Gamma[2] \cap \Gamma[3] = \Gamma[6]$, con lo que se tiene $\Gamma[6] \subset \left(\Gamma^2 \cap \Gamma^3\right) = \Gamma'$. Por otro lado, toda matriz $A \in \Gamma$ cumple, sin más comprobación que operar, la relación

$$A^2 = A \cdot \mathrm{Tr}(A) - I, \tag{3.51}$$

con lo que se llega fácilmente a $A^6 \equiv \pm I \mod 6$ (aplicando módulos 2 y 3), deduciéndose así que $A^6 \in \Gamma[6]$. □

Otros autores han trabajado en el estudio del subgrupo conmutador y su relación con otros subgrupos. En particular, J.H. van Lint llegó a resultados vinculados al teorema anterior y pueden consultarse en [45].

3.3. Profundizando en los subgrupos normales

Tras la fuerte carga teórica de las secciones anteriores, recogemos en este apartado algunos resultados recientes relacionados con ciertas cuestiones abiertas relativas a los subgrupos normales del grupo modular Γ. Podemos englobar los principales temas sobre los que han hecho recientes conjeturas, demostraciones y debates entre matemáticos en estos puntos:

1. Hemos hablado del concepto de nivel de un subgrupo de Γ. Recuperaremos el concepto y veremos la equivalencia entre las diferentes definiciones.

2. Ya vimos que un grupo Ω es de congruencia si contiene algún subgrupo principal $\Gamma[m]$, y recogimos varios ejemplos importantes de subgrupos de congruencia conocidos. Pero, ¿es cierto que todos los subgrupos normales de Γ son de congruencia? Veremos que no, y estableceremos las condiciones para que sí se cumpla.

3. Si $\Gamma[m]$ es el subgrupo principal de congruencia de nivel m y $\Delta(m)$ el mínimo subgrupo normal de Γ que contiene a $U^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$, ¿es cierto que $\Gamma[m] = \Delta(m)$? Veremos que depende de ciertas condiciones sobre m.

4. ¿Cuántos subgrupos normales de índice μ existen? Pese a que no existe todavía una respuesta general, veremos que si μ cumple ciertas condiciones, sí somos capaces de contar esta cantidad.

3.3.1. Nivel de un subgrupo

Si bien hemos recurrido varias veces en las secciones anteriores al concepto de nivel de un subgrupo descrito por Klein en el contexto de un subgrupo de congruencia, esta definición es equivalente, para ciertos subgrupos, a otra mucho más general establecida por Wohlfahrt en [47]. Recordemos:

Definicion 3.10. (Nivel de Klein) Sea $\Gamma[n]$ subgrupo principal de congruencia y $\Omega \subset \Gamma$ que contiene a $\Gamma[n]$, entonces Ω es un subgrupo de congruencia y el mínimo n que cumple la condición se denomina nivel (de Klein), que denotaremos en algunas ocasiones como n_K.

Los trabajos de Fricke, en especial el teorema que lleva su nombre (ver [12]) nos permiten consolidar las definiciones y los conceptos previos necesarios para comprender la nueva definición de nivel de Wohlfahrt. Consideremos un elemento $L \in \Gamma$ que tiene como punto fijo $p \in \mathbb{Q}$ o bien ∞, y por lo tanto es una *transformación parabólica*. Este elemento se puede expresar como

$$L = A^{-1}U^nA \text{ para cierto } n > 0,$$

con $A \in \Gamma$, y así el punto fijo $p = A^{-1}(\infty)$ se denomina punto fijo parabólico o, más ilustrativo si tenemos en mente las regiones fundamentales, *cúspide* de *amplitud* n. Consideremos también

un subgrupo Ω conteniendo a $-I$ (para tener el isomorfismo $\Omega/\{\pm I\} \cong \overline{\Omega}$), y el estabilizador de p expresado como

$$\Omega_p = \left\{ \; X \in \Omega \;\middle|\; X(p) = p \; \right\}.$$

Se puede demostrar que Ω_p está generado por $-I$ y por un elemento parabólico P con amplitud n, esto es,

$$P = A^{-1} U^n A$$

para algún $A \in \Gamma$. Además, si dos puntos p_1, p_2 son equivalentes por L, evidentemente tendrán la misma amplitud como cúspides de Ω. Con todo esto claro, veamos la definición de Wohlfahrt:

Definicion 3.11. (Nivel de Wohlfahrt de un subgrupo) Sea un subgrupo $\Omega \subset \Gamma$ y considérese el subconjunto

$$\text{Cúsp}(\Omega) = \left\{ \; n_i > 0, \text{ entero} \;\middle|\; n_i \text{ es la amplitud de alguna cúspide } p_i \; \right\}.$$

Si este conjunto es no vacío y está acotado (en los enteros positivos), se denomina *nivel (de Wohlfahrt, n_W)* del subgrupo al mínimo común múltiplo de las amplitudes de las cúspides, esto es:

$$n_W = \text{mcm}_i \{n_i\}, \tag{3.52}$$

mientras que si Cúsp(Ω) no cumple las condiciones, el nivel será 0.

En estas condiciones, se tiene la siguiente implicación: si $\mu = |\Gamma : \Omega|$ es finito, entonces el número t de cúspides (no equivalentes en Ω) será mayor que cero y finito, con lo que el grupo Ω tendrá nivel $n_W > 0$ finito. El subgrupo de todos los elementos parabólicos P con amplitud n fue tratado en primer lugar por Fricke ([12]) y recuperado posteriormente por Reiner y Brenner ([40] y [6]) y no es más que el subgrupo $\Delta(n)$, el mínimo subgrupo normal que contiene a U^n. Wohlfahrt demostró que

Teorema 3.18. *Si $\Omega \subset \Gamma$ tiene nivel $n_W = n > 0$, entonces $\Delta(n) \subset \Omega$. Recíprocamente, si $\Delta(m) \subset \Omega$ para algún $m > 0$ y Ω tiene nivel $n_W = n$, entonces $n|m$ con $m > 0$.*

Corolario 3.5. *Si $\Omega_1 \subset \Omega_2$, con niveles n_1 y n_2 respectivamente, entonces $n_2|n_1$.*

Como hemos visto a lo largo de la sección, los niveles de Klein y Wohlfahrt están relacionados, con lo que vamos a establecer finalmente la equivalencia entre ambas definiciones. En el caso de que el subgrupo sea $\Omega = \Gamma[n]$, esto es, subgrupo principal de congruencia, es claro que las definiciones son equivalentes puesto que todas las amplitudes n_i de cúspides de $\Gamma[n]$ son iguales a n, con lo que

$$\text{mcm}_i \{n_i\} = n = n_W$$

y evidentemente $\Delta(n) \subset \Gamma[n]$, con lo que el nivel de Klein sería $n_K = n = n_W$. El resultado más poderoso de Wohlfahrt a este respecto viene en forma de teorema:

Teorema 3.19. *Si $\Omega \subset \Gamma$ es de congruencia con nivel (de Wohlfahrt) n, entonces $\Gamma[n] \subset \Omega$.*

La conclusión del teorema es la respuesta perfecta a la pregunta del inicio del apartado: si un subgrupo es de congruencia los niveles de Klein y Wohlfahrt coinciden.

3.3.2. ¿Todos los subgrupos normales son de congruencia?

De antemano, y con lo visto unas líneas más arriba, la respuesta es no, sin más que aplicar el último teorema visto (3.19) para poner un ejemplo. En [47], Wohlfahrt propone el subgrupo $\Omega \lhd \Gamma$ con $\mu = 7$ y 2 cúspides no equivalentes ($t = 2$) con amplitudes $n_1 = 1$ y $n_2 = 6$. Si fuera de congruencia, entonces contendría a $\Gamma[6]$, pero $|\Gamma : \Gamma[6]| = 72$, que no es múltiplo de 7, por lo que no puede ser de congruencia.

Varios matemáticos como I.Reiner y M.Knopp han tratado esta cuestión en recientes publicaciones ([40] y [21], respectivamente), si bien podemos remontarnos a los trabajos que R.Fricke ([12]) y G.Pick ([39]) publicaron en 1887, afirmando que no todos los subgrupos normales de Γ de índice finito contienen subgrupos principales de congruencia, o lo que es equivalente, no todos son subgrupos de congruencia. Como premisa, se tiene que si un subgrupo Ω es normal en Γ y contiene a $\Gamma[m]$ para algún $m > 0$, entonces $|\Gamma : \Omega| < \infty$.

Para abordar la respuesta que dieron Fricke y Pick, recurriremos a una clase de subgrupos normales de Γ que todavía no han aparecido.

Subgrupos normales $\Omega(p,s)$.
Dado un primo p, el correspondiente subgrupo principal $\Gamma[p]$ y el conmutador del mismo, $\Gamma'(p)$. Tomemos el cociente $\Theta(p) = \Gamma[p]/\Gamma'[p]$ y la proyección usual

$$\pi : \Gamma[p] \longrightarrow \Theta(p).$$

Si $\Theta^s(p)$ es subgrupo potencia de $\Theta(p)$, se tiene que $\Theta(p)/\Theta^s(p)$ es finito. Tomemos entonces el grupo

$$\Omega(p,s) = \pi^{-1}\left(\Theta^s(p)\right) \subset \Gamma[p]$$

que, como $\Gamma[p]$ es normal y $\Theta^s(p)$ es normal en $\Gamma[p]$, también es normal en $\Gamma[p]$. Así, podemos establecer el isomorfimo

$$\Gamma[p]/\Omega(p,s) \cong \Theta(p)/\Theta^s(p). \tag{3.53}$$

Nuestro objetivo es demostrar que si $(p,s) = 1$ con $s > 1$, entonces $\Omega(p,s)$ no contiene subgrupos principales de congruencia. Para ello, supongamos lo contrario, que existe k tal que $\Gamma[k] \subset \Omega(p,s)$. Como $\Gamma[\lambda k] \subset \Gamma[k]\ \forall \lambda$ entero positivo, vamos a tomar como hipótesis

$$\Gamma\left(p^r st\right) \subset \Gamma(p,s) \text{ con } (t,p) = 1,\ r \geq 1. \tag{3.54}$$

Ahora, partamos de las matrices

$$V = U^p = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}, W = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}$$

y cojamos $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Supongamos que $A = W^q V W V^{st-1}$ para cierto valor de q entero. Operando el miembro derecho, queda la igualdad

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} p^2+1 & p(p^2+1)(st-1)+p \\ pq+p(p^2q+1) & p^2q+p\big(pq+p(p^2q+1)\big)(st-1)+1 \end{pmatrix}$$

de donde despejamos $b/p = p^2(st-1)+st$ y $(d-1)/p^2 = q(b/p)+st-1$. Dado que $(b/p, pst) = 1$, podemos elegir q tal que $(d-1)/p^2 \equiv 0 \pmod{p^r st}$, y en consecuencia $d \equiv 1 \pmod{p^r st}$. Utilizamos el hecho de que $ad - bc = 1$, obteniendo que $a \equiv 1 + bc \pmod{p^r st}$. Así, llegamos a

$$A \equiv B = \begin{pmatrix} 1+bc & b \\ c & 1 \end{pmatrix},$$

con lo que $AB^{-1} \in \Gamma[p^r st]$ y, por la hipótesis (3.54) se da la inclusión $AB^{-1} \in \Omega(p,s)$. Ahora, es fácil probar (simplemente cálculo) que $B = V^{b/p} W^{c/p}$, y sustituyendo en la expresión para b/p, llegamos a

$$AB^{-1} = W^q V W V^{st-1} W^{-c/p} V^{-b/p}$$

y como $e_W(AB^{-1}) \equiv 0 \pmod{s}$[3], se tiene $1 + st - 1 - b/p \equiv 0 \pmod{s}$, o bien sustituyendo b/p por su expresión, $st - p^2(st-1) + st \equiv 0 \pmod{s}$, lo que obliga a que $p^2 \equiv 0 \pmod{s}$, y llegamos a contradicción ya que $(p,s) = 1$.

Dada su importancia, rescatamos en forma de lema un resultado de los utilizados en la demostración:

Corolario 3.6. *Toda palabra $w \in \Omega(p,s)$ cumple que la suma de los exponentes de W (que es generador de $\Gamma[p]$) es múltiplo de s, esto es, $e_W(w) \equiv 0$ (mód s).*

En [34], Newman da una condición necesaria y suficiente para que un subgrupo de la forma (p,m,d) sea de congruencia:

Teorema 3.20. *Sea $\Omega = (p,m,d)$ subgrupo normal de género 1. Es de congruencia si y sólo si*

$$(p,m,d) = (1,0,1),(1,1,3),(2,0,1) \text{ ó } (2,1,3).$$

[3]H.Frasch demostró en [11] que W y V pertenecen al conjunto de generadores de $\Gamma[p]$, hecho que permite caracterizar $\Gamma'(p)$ como el conjunto de productos de generadores g_i de $\Gamma[p]$ tales que la suma de exponentes de cada generador es cero, esto es, $e_{g_i}(w) = 0 \; \forall w \in \Gamma'(p)$. De aquí se deduce que $\Omega(p,s)$ es el conjunto de productos de W y U cuyas sumas de exponentes son múltiplos de s.

Demostración. Recuperamos el concepto de nivel (de Wohlfahrt) de un subgrupo de índice finito en Γ como mínimo común múltiplo de las amplitudes de las cúspides (no equivalentes) del grupo en cuestión, y que coincide con la definición dada por F.Klein cuando se trata de subgrupos de congruencia. Así, si $\Omega = (p,m,d)$, ya vimos que tiene nivel 6, por ello será de congruencia si y sólo si $\Gamma[6] \subset (p,m,d)$. Como $\left|\Gamma' : (p,m,d)\right| = dp^2$ y $\left|\Gamma' : \Gamma[6]\right| = 12$, necesariamente $dp^2|12$, con lo que enumerando las combinaciones posibles llegamos al enunciado del teorema. □

Terminemos viendo un enunciado más poderoso si cabe, debido a Wohlfahrt (con demostración en [47]):

Teorema 3.21. *Si un subgrupo $\Omega \subset \Gamma$ tiene índice $\mu \leq 6$ en Γ, entonces es de congruencia.*

En conclusión, no todos los subgrupos normales de Γ son de congruencia, pero al menos existen condiciones que permiten afirmar si un subgrupo en concreto lo es. Toda la discusión reflejada en esta sección puede generalizarse, y de hecho aún hoy queda la cuestión sigue abierta para el caso más general en que el grupo de referencia es $PSL_n(\mathbb{Z})$.

3.3.3. Sobre la minimalidad de los subgrupos principales de congruencia

El matemático J.L.Brenner se planteó, y así reflejó en 1960 en [6], si todos los subgrupos principales de congruencia $\Gamma[m]$ son minimales respecto a contener al elemento U^m. Así, si retomamos el subgrupo $\Delta(m)$, que recordamos es el menor subgrupo normal que contiene a U^m, la pregunta se traduce en:

$$¿\Gamma[m] = \Delta(m),\ \forall m > 0?$$

En primer lugar, es sencillo ver que $\Delta(m) \subset \Gamma[m]$ puesto que $U^m \in \Gamma[m]$ para todo m. Faltaría comprobar si, igualmente, $\Gamma[m] \subset \Delta(m)$, labor que debemos a Brenner, a través del siguiente

Teorema 3.22. *Si $m > 1$ no es potencia de ningún primo p, entonces $\Delta(m)$ no contiene ningún subgrupo principal de congruencia.*

Demostración. Sea $m = p^r s$, con $r \geq 1$, $s > 1$, $(p,s) = 1$. Utilizaremos el subgrupo $\Omega(p,s)$ visto y el corolario (3.6). Así pues, como $U^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ es potencia de U^{ps}, entonces $\Delta(m) \subset \Delta(ps)$, y además $U^{ps} = (U^p)^s$, con lo que podemos pensar en U^{ps} como un elemento de $\Omega(p,s)$. Como $\Omega(p,s) \lhd \Gamma$ y como $U^{ps} \in \Omega(p,s)$, se tiene la cadena de inclusiones

$$\Delta(m) \subset \Delta(ps) \subset \Omega(p,s),$$

y como $\Omega(p,s)$ no contiene subgrupos principales de congruencia, $\Delta(m)$ tampoco. □

En [6], Brenner acotó aún más los posibles valores de m para los que $\Gamma[m] = \Delta(m)$, dando una demostración del siguiente teorema de Klein y Frike ([20]), que da respuesta a la pregunta del inicio de este apartado:

Teorema 3.23. *Sean los grupos* $\Delta(m)$ *y* $\Gamma[m]$. *Se tiene que* $\Delta(m) = \Gamma[m]$ *si* $m \in \{1,2,3,4,5\}$, *mientras que si* $m \geq 6$ *entonces* $\Delta(m)$ *tiene índice infinito en* $\Gamma[m]$ *y por consiguiente* $\Gamma[m] \neq \Delta(m)$.

A este respecto, existe aún la cuestión abierta: *si n es potencia de un número primo, ¿el grupo* $\Delta(n)$ *contiene algún subgrupo principal de congruencia?* Lo único avanzado hasta ahora viene de la mano de H.Frasch [11], cuyos estudios demostraron el siguiente

Teorema 3.24. *Si* $p \geq 7$ *con p primo entonces* $\Delta(p) \neq \Gamma[p]$.

Una consecuencia directa de la relación entre $\Gamma[n]$ y $\Delta(n)$ es la relación entre el grupo modular de nivel n y los llamados *grupos triangulares* :

Definicion 3.12. Se denomina *grupo triangular* con *signatura* $(0;l,m,n)$ al grupo con presentación

$$G_{l,m,n} = \left\langle \; X,Y \;\middle|\; X^l = Y^m = (XY)^n = I \; \right\rangle.$$

El valor 0 hace referencia al *género* del grupo, concepto al que aludiremos más adelante. En concreto, para los grupos triangulares con presentación

$$\left\langle \; X,Y \;\middle|\; X^2 = Y^3 = (XY)^n = I \; \right\rangle.$$

se suele emplear la notación simplificada $G_n = (0;2,3,n)$.

Atendiendo a las presentaciones, parece evidente que existe una relación entre los grupos triangulares G_n y los grupos $PSL_2(\mathbb{Z}_n)$. Para detallarla, vamos a utilizar el epimorfismo

$$\phi_n : PSL_2(\mathbb{Z}) \longrightarrow PSL_2(\mathbb{Z}_n),$$

inducido por la reducción $\mathbb{Z} \mapsto \mathbb{Z}_n$ y que tiene núcleo $\Gamma[n]$; el epimorfismo

$$\theta_n : PSL_2(\mathbb{Z}) \longrightarrow G_n,$$

que realiza la correspondencia entre generadores

$$T(z) \mapsto X,\; R(z) \mapsto Y,$$

tiene núcleo $\ker(\theta_n) = \Delta(n)$ y por tanto $PSL_2(\mathbb{Z})/\Delta(n) \cong G_n$. Además tenemos un último epimorfismo

$$\Phi_n : G_n \longrightarrow PSL_2(\mathbb{Z}_n),$$

tal que $\phi_n = \Phi_n \circ \theta_n$. Como hemos visto, tenemos la igualdad $\Gamma[n] = \Delta(n)$ si $n \in \{1,2,3,4,5\}$, por tanto en estos casos podemos establecer el isomorfismo

$$G_n \cong PSL_2(\mathbb{Z})/\Delta(n) = PSL_2(\mathbb{Z})/\Gamma[n] \cong PSL_2(\mathbb{Z}_n), \tag{3.55}$$

esto es, $PSL_2(\mathbb{Z}_n)$ es la imagen por el isomorfismo Φ_n del grupo triangular G_n, o lo que es equivalente, $PSL_2(\mathbb{Z}_n) \cong G_n$. Sin embargo, para $n \geq 6$ el grupo G_n es infinito[4] mientras que $PSL_2(\mathbb{Z}_n)$ es finito, por tanto no pueden ser isomorfos (Φ_n es simplemente un epimorfismo con núcleo $\ker(\Phi_n) = \Delta(n) \neq \Gamma[n]$). En el caso específico en que $n = 7$, se puede demostrar ([44], teorema 5.11.2) que $H = \Phi_7(G_7) = PSL_2(\mathbb{Z}_7)$, de orden 168 por la fórmula dada en (3.16), es un *grupo de Hurwitz* de orden $84(g-1)$ por definición, y con ello podemos adelantar que será, como veremos más adelante, el grupo de automorfismos de alguna superficie de Riemann de género $g = 3$.

Presentación para el grupo modular de nivel N.
Como conclusión, al ser los grupos G_n y $PSL_2(\mathbb{Z}_n)$ isomorfos cuando $n \in \{1,2,3,4,5\}$, podemos determinar una presentación para $PSL_2(\mathbb{Z}_n)$ en el siguiente

Teorema 3.25. *Si $n \in \{1,2,3,4,5\}$, se tiene la siguiente presentación de grupos:*

$$PSL_2(\mathbb{Z}_n) \cong \left\langle \; T,R \;\middle|\; T^2 = R^3 = U^n = I \; \right\rangle, \tag{3.56}$$

siendo $T,R,U = TR$ las conocidas transformaciones generadoras de $PSL_2(\mathbb{Z})$.

3.3.4. Contando subgrupos normales

Cabe lugar preguntarse si, dado un índice μ, existen finitos o infinitos subgrupos de Γ con tal índice. De hecho, si añadimos la restricción de que los subgrupos sean normales, sería deseable averiguar si hay finitos subgrupos o no, y más aún, ser capaces de contarlos. Si $\mu \in \{1,2,3\}$ sólo existe un subgrupo normal con índice μ, que es el subgrupo potencia Γ^μ. En otro caso, los posibles subgrupos normales deben tener índice μ múltiplo de 6 (R.C.Gunning [14], [33]). Además, dado un índice μ, existe un número finito de subgrupos normales con tal índice en Γ, ya que el número de subgrupos de índice finito de un grupo finitamente generado es finito (G.Behrendt y P.M.Newmann, [5]). El objetivo sería, pues, encontrar una función $N(\mu)$ que proporcione el número de subgrupos normales con índice μ. Como consecuencia de los razonamientos expuestos se tiene que $N(1) = N(2) = N(3) = 1$, mientras que si $\mu > 3$ y no es múltiplo de 3, entonces $N(\mu) = 0$.

Lamentablemente, no se ha encontrado aún dicha fórmula para $N(\mu)$. De momento, la respuesta general a la primera pregunta, acerca de cuántos subgrupos con existen con índice μ (normales o no), cantidad que llamaremos $M(\nu)$, fue dada por M. S. Dey (en [10]) a través de la siguiente fórmula de recurrencia para $\mu > 1$:

$$M(\mu) = \mu\alpha_\mu - \sum_{k=1}^{\mu-1} \alpha_{\mu-k} M(k), \tag{3.57}$$

donde se utilizan las fórmulas

$$\alpha_k = \frac{\tau_2(k)\tau_3(k)}{k!}$$

[4] Recordemos que si $n \geq 6$ entonces $\Delta(n)$ tiene índice infinito en $\Gamma[n]$, y por tanto también en Γ.

y

$$\tau_p(k) = \sum_{r\in[0,k/p]} \frac{k!}{r!(k-rp)!p^r}.$$ [5]

Sería muy buena noticia encontrar una recurrencia similar para $N(\mu)$, pero de momento vamos a intentar acotar esta cantidad retomando los conceptos de nivel (n) y número de cúspides (t) ya mencionados.

Consideración previa.
En lo que resta de sección, tomaremos Ω tal que $-I \in \Omega$[6].

Proposicion 3.11. *Sea $\Omega \subset \Gamma$ con índice $\mu > 3$ y múltiplo de 6, y sea n el nivel (de Klein) de Ω. Entonces $n|\mu$ y, de hecho,*

$$\mu = tn \tag{3.58}$$

donde t es el número de cúspides no equivalentes de Ω y μ el nivel.

Por ejemplo, si $\Omega = \Gamma[5]$, como $\mu = 60$ (calculado mediante las expresiones (3.15) y (3.16)) y $n = 5$, se tienen $t = 12$ cúspides no equivalentes.

De forma más general, y según los trabajos de Wolhfahrt y Newman entre otros, el índice de un subgrupo es la suma de las amplitudes de las cúspides no equivalentes, esto es:

Proposicion 3.12. *Sean $\Omega \subset \Gamma$ con índice μ, y sean $n_1, n_2, \cdots, n_t$ las amplitudes de las t cúspides. Entonces*

$$\mu = \sum_{i=1}^{t} n_i. \tag{3.59}$$

Por supuesto, la ecuación (3.58) no es más que un caso concreto en el que todas las amplitudes coinciden con el nivel, como también ocurre en los subgrupos principales de congruencia. En esta línea, Gunning demuestra (en [14]) que el *género* de este subgrupo Ω cumple la relación

$$g = 1 + \mu/12 - t/2 = 1 + \mu\frac{n-6}{12n} \tag{3.60}$$

que permitirá, en secciones posteriores, estudiar la superficie de Riemann generada como espacio de órbitas por la acción de Ω en $\mathscr{U}$. A su vez, permite afirmar que todo subgrupo normal con género 1 debe tener nivel $n = 6$, como también demostró Newman en [32]. Recordemos que si Ω es normal en Γ y tiene género 1, entonces tiene nivel 6, y además los enteros positivos p, m, d son tales que $p > 0$, $m \in [0, d-1]$, $m^2 + m + 1 \equiv 0 \pmod{d}$. Así, teníamos la siguiente caracterización del grupo:

$$\Omega = (p, m, d) = \left\{ \; w \in \Gamma' \;\middle|\; e_a(w) \equiv 0 \mod p,\, e_b(w) \equiv 0 \mod dp \; \right\}.$$

[5] Esta fórmula proporciona el número de homomorfismos del grupo cíclico de orden p en el grupo simétrico S_k.
[6] El objetivo es evitar confusión por la fórmula (3.8).

Por consiguiente, $\Omega = (p, m, d)$ tiene índice $\mu = 6dp^2$ y, por la relación (3.58), el número de cúspides no equivalentes será $t = dp^2$ porque $n = 6$. En definitiva, la fórmula para el cálculo del índice está en concordancia con el teorema (3.11).

Vistas estas relaciones, estamos en condiciones de recoger los resultados que Newman enunció y demostró en [35] para intentar contar (o al menos acotar) el número de subgrupos normales con cierto índice μ. Comencemos con el siguiente

Teorema 3.26. *Existe un número finito de subgrupos normales de* Γ *con* $t \leq 11$.

El teorema es relevante puesto que afirma que dado un número $t \leq 11$, podremos encontrar un número finito de subgrupos normales con t cúspides. En particular, los únicos subgrupos normales en Γ con $t = 1$ son $\Gamma, \Gamma^2, \Gamma^3$ y Γ'. Pero, ¿qué ocurre en general para cualquier t? La respuesta viene de los trabajos de L. Greenberg ([13]) y Petersson ([38]), cuyas aportaciones unificamos en el siguiente teorema:

Teorema 3.27. *Dado un número* t *de cúspides no equivalentes, entonces:*

1. *Existe un número finito de subgrupos normales* $\Omega \lhd \Gamma$ *con dicho* t.
2. *Si no exigimos normalidad, existe un número infinito de subgrupos* $\Omega \subset \Gamma$ *con dicho* t.

Demostración. (Afirmación (2) del teorema) Como el conmutador Γ' tiene $t = 1$ (ya que $\mu = tn$ y en este caso $\mu = n = 6$) podemos elegir una matriz parabólica representante de la clase que fija la cúspide p de amplitud n. Llamemos a esta matriz

$$P = aba^{-1}b^{-1}$$

donde a y b son de la forma expuesta en (3.31), esto es,

$$a = TRTR^2, b = TR^2TR$$

con T y R los conocidos generadores de Γ. Cojamos la siguiente clase de subgrupos del subgrupo conmutador:

$$\Gamma'(t) = \left\{ \; w \in \Gamma' \;\middle|\; e_a(w) \equiv 0 \mod t \; \right\} \tag{3.61}$$

Este subgrupo es normal en Γ', es fácil ver que $\mu = t$ en Γ', $P \in \Gamma'(t)$ y tiene tantas cúspides como Γ' (consultar [36]). Como $\Gamma'(t)$ es libre, tiene género $g = 1 + \mu/12 - t/2 = 1$. Así, $\Gamma'(t)$ es de rango $t+1$, con conjunto de generadores $a_1, b_1, P_1, P_2, \cdots, P_{t-1}$ tales que

$$P_t = a_1 b_1 a_1^{-1} b_1^{-1} P_1 P_2, \cdots, P_{t-1}$$

siendo P_j la matriz representante de la clase parabólica j-ésima. Cojamos ahora un subgrupo de $\Gamma'(t)$:

$$\Gamma'(t,n) = \left\{ \; w \in \Gamma'(t) \;\middle|\; e_{P_i}(w) \equiv 0 (\text{mód } n) \; \forall i = 1, 2, \cdots, t \; \right\} \tag{3.62}$$

Es claro que $P_i^n \in \Gamma'(t,n)$, además este grupo es normal en $\Gamma'(t)$ con índice $\mu = n$ y el número de cúspides es (ver [36])

$$t = \mu \sum_{i=1}^{t} \frac{1}{n_i} = n\frac{t}{n} = t,$$

de modo que como n es arbitrario, se da por finalizada la prueba. □

Cabe preguntarse si, ya que hemos intentado cuantificar el número de subgrupos dado el valor t, podríamos hacer lo mismo si el valor que conocemos es el nivel n. Pues bien, Newman afirmó y probó que

Teorema 3.28. *Dado el nivel n, existe un número finito de subgrupos normales $\Omega \subset \Gamma$ si $n \leq 5$, mientras que la cantidad será infinita si $n \geq 6$.*

Volviendo a nuestro objetivo principal, que era hallar el número $N(\mu)$ de subgrupos normales con índice μ en Γ, vamos a enunciar una serie de teoremas cuyas demostraciones debemos a Newman (ver [35]). Estos teoremas conforman la aproximación más cercana a la respuesta general que, todavía hoy, no se ha encontrado.

Teorema 3.29. *Sea el índice $\mu = 6q$, con $q > 3$ primo. Si $(q/3) = 1$ (donde $(q/3)$ denota el símbolo de Legendre-Jacobi de reciprocidad cuadrática definido en (3.40)) entonces existen dos subgrupos normales de género 1 con tal índice en Γ, mientras que si $(q/3) = -1$, no existe ninguno.*

Teorema 3.30. *Sea el índice $\mu = 12q$, con $q > 11$ primo, no existe ningún subgrupo normal con tal índice en Γ.*

Teorema 3.31. *Sea $\Omega \subset \Gamma$ tal que no contiene subgrupos normales de índice $\mu = m$ para algún m entero positivo, y sea $p > m$ primo. Entonces Ω tampoco contiene subgrupos normales de índice $p^k m$, $\forall k > 0$.*

Antes de enunciar los dos últimos teoremas, necesitamos un lema que sí vamos a demostrar:

Lema 3.8. *Sean $\Omega_1, \Omega \lhd \Gamma$ con índice finito y $\Omega \subset \Omega_1$. Si Ω_1 y Ω tienen niveles n_1 y n en Γ y número de cúspides t_1 y t respectivamente, entonces $n_1 | n$ y $t_1 | t$.*

Demostración. Sea el índice $|\Omega_1 : \Omega| = r$, se tiene $nt = rn_1t_1$ y es claro que $n_1|n$ ya que $U^{n_1} \in \Omega_1$ y $U^n \in \Omega \subset \Omega_1$. Además, la inclusión $U^{n_1} \in \Omega_1$ implica que $U^{rn_1} \in \Omega$, porque Ω_1/Ω tiene orden r. Por consiguiente, $n|rn_1$ (porque $U^n \in \Omega$). Así, $t = (rn_1/n)t_1$, con lo que $t_1|t$. □

Finalicemos, pues, con un último teorema sobre la cantidad de subgrupos normales de índice μ, y con otro teorema que recoge la lista de todos los subgrupos normales de índice $\mu \leq 66$.

Teorema 3.32. *No existe ningún subgrupo normal con $t = q$ primo cumpliendo $(q/3) = -1$.*

Recopilamos a continuación la lista de todos los subgrupos normales de índice $\mu \leq 66$ en Γ:

μ	1	2	3	6	12	18	24	30
Subgrupo	Γ	Γ^2	Γ^3	$\Gamma[2], \Gamma'$	$\Gamma[3]$	$(1,1,3)$	$\Gamma[4], (2,0,1)$	-

Cuadro 3.1: Todos los subgrupos normales de índice $\mu \leq 30$ en Γ.

μ	36	42	48	54	60	66
Subgrupo	-	$(1,2,7), (1,4,7)$	$G_{4,2}, G_{3,4}$	$(3,0,1)$	$\Gamma[5]$	-

Cuadro 3.2: Todos los subgrupos normales de índice $36 \leq \mu \leq 66$ en Γ.

En conclusión, pese a que no es posible determinar cuántos subgrupos normales hay de manera general para un índice μ, hemos visto que en ciertos casos sí es posible determinar si la cantidad es finita o no, y al menos conocemos la lista de todos ellos hasta $\mu \leq 66$. La última aportación a esta ardua búsqueda viene del trabajo de Newman y Knopp en [36], donde encuentran una cota inferior para el caso $\mu = 6q^{2r}$, q primo tal que $(q/3) = 1$:

$$N\left(6q^{2r}\right) \geq 2r - 1,$$

dándose la igualdad si el género es 1.

3.4. Encriptando códigos con el grupo modular

Como última sección de este capítulo, de fuerte carácter teórico, vamos a dedicar unas líneas a comentar una aplicación práctica relativamente reciente en el campo de la Criptografía, y es que se puede utilizar la presentación del grupo modular $PSL_2(\mathbb{Z})$ para encriptar mensajes en texto plano (sin formato). El algoritmo que vamos a exponer se enmarca dentro de la clase de algoritmos de *clave pública*, en los que el método de encriptación es publicado por el emisor del mensaje, pero el método de desencriptado necesita un aspecto clave que es privado, y sólo es compartido entre emisor y receptor. Los más conocidos y utilizados son los algoritmos **RSA** y **Anshel-Goldfeld**.

En primer lugar expondremos un método sencillo para codificar un mensaje utilizando matrices del grupo modular, basado en el método de Yamamura ([48]) y cuyas vulnerabilidades han provocado que los ataques de los hackers sean capaces de descubrir el mensaje. La aportación de Baumslag, Fine y Xu ([2]) mejora y fortalece el método criptográfico, con lo que parece que una posible vía de trabajo consiste en continuar buscando vulnerabilidades a este método y proponer nuevos blindajes.

Retomemos entonces la notación simplificada Γ para el grupo modular en el que se identifica cada matriz con su opuesta, y recordemos la presentación del grupo:

$$PSL_2(\mathbb{Z}) \cong \left\langle\ T, U \ \middle|\ T^2 = (TU)^3 = I\ \right\rangle \cong \left\langle\ T, R \ \middle|\ T^2 = R^3 = I\ \right\rangle, \tag{3.63}$$

donde las matrices T, U y $R = TU$ son las conocidas

$$T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, R = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

De este modo, cualquier matriz $A \in \overline{\Gamma}$ puede expresarse en términos de T y U por ser generadores, y la demostración de este hecho supone un primer algoritmo a tener en cuenta:

1. Sea $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \overline{\Gamma}$, es conocido el efecto que sobre ella tiene el producto por la izquierda por los generadores T y U:
$$TA = \begin{pmatrix} \gamma & \delta \\ -\alpha & -\beta \end{pmatrix}$$
y
$$U^k A = \begin{pmatrix} \alpha + k\gamma & \beta + k\delta \\ \gamma & \delta \end{pmatrix}.$$

2. Multiplicando A por la izquierda por la adecuada combinación de generadores, llegaríamos a una matriz U^p para algún p, esto es,
$$U^{k_1} T U^{k_2} T \cdots U^{k_n} T^{\epsilon} A = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} = U^p \in \Gamma$$
con $\epsilon = 0$ o bien $\epsilon = 1$. Por ejemplo, sea la matriz $A = \begin{pmatrix} 3 & 4 \\ 5 & 7 \end{pmatrix} \in \Gamma$, es fácil llegar a que
$$TU^3 TU^2 TA = U.$$

3. Así, podríamos expresar A como producto de generadores del grupo modular.

Recordado el método, veamos la base teórica necesaria para abordar la versión previa del criptosistema:

Definicion 3.13. (Transversal de Schreirer) Sea G un grupo libre finitamente generado y un subgrupo $H \subset G$. Sea $S = \{s_1, s_2, \cdots, s_t\}$ un subconjunto tal que se tiene la descomposición

$$G = \bigcup_{i=1}^{t} H s_i,$$

se dice que S es una *transversal de Schreirer* para H en G si toda palabra $w = x_1 \cdots x_n$ reducida[7] en términos de los generadores de G que pertenezca a S cumplirá que $w x_n^{-1} = x_1 \cdots x_{n-1} \in S$.

En los trabajos de Schreier y Reidemeister, recogidos en [26], se demuestra el siguiente

[7] Las relaciones de la presentación del grupo no permiten encontrar una expresión más simple para la palabra.

Lema 3.9. *Si G es libre y $H \subset G$, entonces existe una transversal de Schreier para H en G.*

Particularizamos a nuestro caso de estudio los resultados de los matemáticos mencionados en la siguiente

Proposicion 3.13. *Todo subgrupo $\Omega \subset \Gamma$ con índice finito tiene un conjunto finito de generadores que pueden expresarse en términos de una transversal de Schreier.*

Dada una transversal de Schreier $s_1, \cdots, s_t$ y un conjunto de generadores, el método utilizado para expresar estos en términos de la transversal se denomina *método de Reidemeister-Schreier* (y aparece en [9]). Dejamos en manos del lector profundizar en el método, dado que se escapa del alcance de esta sección. Utilizando la expresión de cualquier palabra o matriz en términos de T y U, y conociendo la existencia del método de Reidemeister-Schreier, estamos en condiciones de describir el algoritmo previo de encriptación:

Algoritmo 3.1. *(Versión previa) Sea $\mathscr{A} = \{a, b, c, \cdots, z\}$ un alfabeto, y una cadena de texto plano A a transmitir. Se elige un subgrupo $\Omega \subset \Gamma$, con transversal de Schreier $s_1, \cdots, s_t$ y conjunto de generadores $W_1, \cdots, W_k$ hallados mediante el método de Reidemeister-Schreier a partir de la transversal, y cumpliendo $k > |\mathscr{A}|$. Entonces:*

1. *El emisor del mensaje publica el subrupo Ω elegido, así como la aplicación biyectiva que asigna a cada generador W_i su letra correspondiente del alfabeto. No publica la transversal de Schreier tomada, la comparte únicamente con el receptor.*

2. *Obtenidos los $W_1, \cdots, W_k$, se fabrica la matriz M como producto de las matrices correspondientes a las letras del texto a encriptar, en el orden del texto.*

3. *El emisor envía la matriz M.*

4. *El receptor utiliza el procedimiento visto para expresar M en términos de los generadores T y U.*

5. *El receptor aplica el método de Reidemeister-Schreier sobre el producto de potencias de generadores obtenido en el paso anterior, para obtener una expresión en términos de $W_1, \cdots, W_k$ a partir de la transversal, que sólo conocen emisor y receptor.*

6. *El receptor aplica la inversa de la aplicación inyectiva que asigna letras a generadores W_i, con lo que obtiene finalmente el mensaje original.*

Este algoritmo, similar al expuesto por Yamamura ([48]), presenta problemas de seguridad que tienen que ver con la evidente acción geométrica de las matrices T y U sobre el semiplano superior complejo $\mathscr{U}$, ya que observando los diferentes patrones de los mensajes encriptados, un hacker podría averiguar el subgrupo Ω empleado y, con ello, se comprometería la seguridad de

la transacción entre el emisor y el receptor. En el año 2006, los matemáticos Baumslag, Fine y Xu ([2]) perfeccionaron el método para hacerlo más robusto frente a posibles ataques, añadiendo una clave (m,q,t) de enteros positivos a compartir con el receptor mediante algún método de cifrado de clave pública conocido como **RSA**. La idea consiste en utilizar no un único subgrupo, sino un conjunto de subgrupos, y elegir en función de los valores (m,q,t) la manera de encriptar el mensaje de forma análoga al algoritmo previo. El procedimiento detallado sería:

Algoritmo 3.2. *(Versión definitiva) Sea $\mathscr{A} = \{a,b,c,\cdots,z\}$ un alfabeto, y una cadena de texto plano A a transmitir. Se elige una familia de subgrupos $\Omega_i \in \Gamma$, con transversales de Schreier $h_{1,i},\cdots,h_{t,i}$ y conjunto de generadores $W_{1,i},\cdots,W_{k_i,i}$ hallados mediante el método de Reidemeister-Schreier a partir de las transversales, cumpliendo $k > |\mathscr{A}|$. Entonces:*

1. *El emisor del mensaje publica la lista de subgrupos elegidos $\{\Omega_i\}$. No publica las transversales de Schreier tomadas, las comparte únicamente con el receptor.*

2. *El emisor elige el subgrupo m-ésimo de la lista para encriptar, y aplica la asignación $a \mapsto W_{m,q}$, $b \mapsto W_{m,q+1}$, ..., para codificar el alfabeto con los generadores de Ω_m a partir del q-ésimo generador.*

3. *El emisor agrupa el mensaje en bloques de t letras, y con ello fabrica s matrices $M_1, M_2, \cdots, M_s$ resultado de multiplicar las matrices correspondientes a las letras del bloque, en el orden en que aparecen en el texto.*

4. *El emisor introduce matrices de ruido $XM_i \in \Gamma$ que multiplica por cada M_i por la derecha. Así, finalmente quedan s matrices enteras que encriptan el mensaje original por bloques.,*

5. *El emisor envía el mensaje cifrado $M_1XM_1, M_2XM_2, \cdots, M_sXM_s$ y además transmite la clave (m,q,t) mediante **RSA** al receptor.*

6. *El receptor desencripta mediante **RSA** la terna (m,q,t), de modo que ya conocería que el subgrupo elegido de la lista pública es Ω_m, que cada una de las s matrices recibidas encripta t letras y que el alfabeto comienza a codificarse a partir del generador $W_{m,q}$.*

7. *El receptor expresa cada M_iXM_i en términos de los generadores T y U.*

8. *El receptor, conocedor de la transversal de Schreier utilizada por el emisor, aplica el método de Reidemeister-Schreier de izquierda a derecha sobre el producto de potencias de generadores obtenido en el paso anterior, para obtener una expresión en términos de los generadores de Ω_m, finalizando cuando haya obtenido t generadores*[8].

[8] Este paso es el que marca la diferencia respecto al propuesto por Yamamura o la versión previa del algoritmo expuesto, ya que un atacante intentará aplicar el algoritmo de Reidemeister-Schreier sin saber cuándo parar de obtener generadores.

9. *El receptor aplica la inversa de la aplicación inyectiva que asigna letras a generadores $W_{m,q+i}$, con lo que obtiene finalmente el mensaje original.*

Para aportar mayor robustez al proceso, es conveniente que la tupla (m,q,t) cambie con cada mensaje enviado, así como el subgrupo elegido de la lista publicada. En [22], el lector podrá profundizar en aspectos de seguridad de este tipo de algoritmos. Para un ejemplo completamente desarrollado, es recomendable consultar el expuesto en [2], donde se codifica el mensaje *STOP THE WAR* con la clave $(256,6,3)$.

En cualquier caso, queda patente el aprovechamiento potencial de las propiedades del grupo modular y sus subgrupos para encriptar y desencriptar información. Es evidente que una vía futura de trabajo vendría marcada por la profundización en este tipo de algoritmos, así como intentar obtener algoritmos que utilicen clases concretas de subgrupos para beneficiarse de sus propiedades: algoritmos específicos que utilicen matrices de los subgrupos principales de congruencia, de los subgrupos potencia o del subgrupo conmutador.

CAPÍTULO 4

EFECTOS GEOMÉTRICOS DE $PSL_2(\mathbb{Z})$ Y SUS SUBGRUPOS

El efecto geométrico en el semiplano superior hiperbólico $\mathscr{U}$ de la acción de algunos de los subgrupos normales establece el puente entre el punto de vista más algebraico y el punto de vista geométrico de nuestro grupo de estudio. Podemos pensar también que, al actuar los grupos vistos sobre $\mathscr{U}$, se da forma a las numerosas propiedades expuestas, escenificadas como superficies de Riemann. En primera instancia, retomamos la noción de región fundamental de Γ y la generalizamos para cualquier subgrupo $\Omega \subset \Gamma$, estableciendo la conexión con los conceptos de puntos no equivalentes por un subgrupo. En el núcleo del capítulo, nos centramos en la exposición y estudio de las regiones fundamentales de los subgrupos principales de congruencia, dada su relevancia como subgrupo. Abordamos el estudio de las superficies de Riemann generadas como espacios de órbitas por la acción de Γ y sus subgrupos sobre el semiplano superior $\mathscr{U}$, introduciendo como motivación la esfera de Riemann y continuando con las propiedades generales de la superficie $\mathscr{U}/\Omega$, con $\Omega \subset \Gamma$. A continuación, obtenemos el género de las superficies y regiones fundamentales expuestas y exploramos su relación con el número de puntos (elípticos, hiperbólicos o parabólicos) no equivalentes. Finalmente, se aborda la relación entre el grupo modular y los grupos de rotaciones de los poliedros regulares.

4.1. Regiones fundamentales de los subgrupos de congruencia

En esta sección extenderemos la definición de región fundamental al caso de un subgrupo $\Omega \subseteq \Gamma$, y estudiaremos las regiones fundamentales de algunos de los subgrupos de congruencia estudiados. Durante este proceso, aparecerán conceptos clave como el *número de puntos elípticos/parabólicos no equivalentes*, que tendrán trascendencia en esta y posteriores secciones.

4.1.1. Número de puntos no equivalentes por un subgrupo

Recordemos que dos puntos $z_1, z_2 \in \mathscr{U} \cup \{\infty\}$ son Γ-equivalentes si existe una transformación $A \in \Gamma$ tal que $A(z_1) = z_2$. Asimismo, un punto z_0 es de orden k en $\Omega \subseteq \Gamma$ si es fijo por alguna transformación $A \in \Omega$ cumpliendo $A^k(z_0) = z_0$. Pues bien, llamemos $\nu_i(\Omega)$ (respectivamente $\nu_\rho(\Omega)$) al número de puntos elípticos de orden 2 (respectivamente 3) en Ω que no son Ω-equivalentes a i (respectivamente ρ), y $\nu_\infty(\Omega)$, al número de cúspides de Ω que no son Ω-equivalentes a ∞.

Antes de mostrar expresiones para estas cantidades, cabe mencionar la forma general de calcular el número de puntos parabólicos (cúspides) no Ω-equivalentes que son Γ-equivalentes, si Ω tiene índice finito en Γ:

Proposicion 4.1. *Con las notaciones anteriores, se tiene*

$$\nu_\infty(\Omega) = \frac{|\Gamma : \Omega|}{|\Gamma_\infty : \Omega_\infty|}, \tag{4.1}$$

donde Ω_∞ es el estabilizador de ∞ en Ω.

Demostración. Como $\Omega \lhd \Gamma$ con índice finito, entonces $\Omega\Gamma_\infty \subset \Gamma$ y $|\Omega\backslash\Gamma/\Gamma_\infty| = |\Gamma/\Omega\Gamma_\infty|$. Terminamos observando que:

$$|\Gamma : \Omega| = |\Gamma : \Omega\Gamma_\infty| \cdot |\Omega\Gamma_\infty : \Omega| = |\Gamma : \Omega\Gamma_\infty| \cdot |\Gamma_\infty : \Omega_\infty|.$$

□

Visto el caso general, veamos fórmulas concretas para el cálculo del número de puntos no equivalentes por algunos de los subgrupos estudiados, y cuyas demostraciones pueden ser consultadas en [29] (p.107-111). Recordemos que

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \mod N \right\}$$

y

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \text{ y } a \equiv d \equiv 1 \mod N \right\}.$$

Teorema 4.1. *Sea $\Omega = \Gamma_0(N)$, $N \geq 2$. Se tienen las siguientes expresiones para el cálculo del número de puntos elípticos y parabólicos de Ω que no son Ω-equivalentes:*

$$\nu_i(\Gamma_0(N)) = \begin{cases} 0 & si \quad 4|N \\ \prod_{p|N}(1 - 1/p) & si \quad otro\ caso \end{cases}, \tag{4.2}$$

$$\nu_\rho(\Gamma_0(N)) = \begin{cases} 0 & si \quad 9|N \\ \prod_{p|N}(1 - 3/p) & si \quad otro\ caso \end{cases}, \tag{4.3}$$

$$\nu_\infty(\Gamma_0(N)) = \sum_{0<d|N} \phi((d, N/d)). \tag{4.4}$$

Teorema 4.2. *Sea $\Omega = \Gamma_1(N)$, $N \geq 2$. Se tienen las siguientes expresiones para el cálculo del número de puntos elípticos y parabólicos de Ω que no son Ω-equivalentes:*

$$\nu_i(\Gamma_1(N)) = \begin{cases} \prod_{p|N}(1-1/p) & si \quad N \in \{2,3\} \\ \\ 0 & si \quad N \geq 4 \end{cases}, \tag{4.5}$$

$$\nu_\rho(\Gamma_1(N)) = \begin{cases} \prod_{p|N}(1-3/p) & si \quad N \in \{2,3\} \\ \\ 0 & si \quad N \geq 4 \end{cases}, \tag{4.6}$$

$$\nu_\infty(\Gamma_1(N)) = \begin{cases} \sum_{0<d|N} \phi(d)\phi((d, N/d)) & si \quad N \geq 5 \\ \\ 3 & si \quad N = 4 \end{cases}. \tag{4.7}$$

Y el teorema más importante, por aludir a los subgrupos principales de congruencia:

Teorema 4.3. *Sea $\Omega = \Gamma[N]$ el subgrupo principal de congruencia de nivel N, $N \geq 2$. Se tienen las siguientes expresiones para el cálculo del número de puntos no Ω-equivalentes:*

$$\nu_i(\Gamma[N]) = \nu_\rho(\Gamma[N]) = 0, \tag{4.8}$$

$$\nu_\infty(\Gamma[N]) = \begin{cases} \frac{1}{2}N^2 \prod_{p|N}(1-\frac{1}{p^2}) & si \quad N \geq 3 \\ \\ 3 & si \quad N = 2 \end{cases}. \tag{4.9}$$

Podemos tomar como representantes de las cúspides no equivalentes el conjunto

$$\left\{ \; p/q \in \mathbb{Q} \cup \{\infty\} \;\middle|\; (p,q) = 1 \; y \; (p \; mód \; N, q \; mód \; N) \in M_N/\{\pm 1\} \; \right\} \tag{4.10}$$

donde M_N es el conjunto de elementos de orden N en $(\mathbb{Z}_N)^2$.

La expresión (4.8) se traduce en la poderosa afirmación de que los subgrupos principales de congruencia de nivel $N \geq 2$ no tienen puntos elípticos. Con las herramientas necesarias ya definidas, podemos extender el concepto de región fundamental hasta ahora expuesto:

Definicion 4.1. Decimos que $\mathscr{F}'$ es un *conjunto fundamental* para $\Omega \subseteq \Gamma$ si contiene únicamente un punto de cada clase de equivalencia por Ω. Si $\mathscr{F}_\Omega$ contiene un conjunto con estas características y además ocurre que

$$z \in \mathscr{F}_\Omega \text{ y } S(z) \in \mathscr{F}_\Omega \text{ con } S \neq I \text{ implica } z \in \partial\mathscr{F}_\Omega,$$

entonces $\mathscr{F}_\Omega$ es una *región fundamental* para Ω.

Ahora bien, como la acción de Ω sobre su región fundamental provoca una teselación del plano hiperbólico extendido $\mathscr{U}^*$, y como además se tiene la descomposición

$$\Gamma = \bigcup_{i=1}^{\mu} \Omega S_i, \text{ con } \mu = |\Gamma : \Omega| \text{ y } S_i \in \Gamma, \tag{4.11}$$

entonces podemos escribir la siguiente descomposición del plano extendido:

$$\mathscr{U}^* = \bigcup_{i=1}^{\mu} \Omega S_i(\mathscr{F}), \tag{4.12}$$

donde $\mathscr{F}$ es la región fundamental para Γ . Así, la región fundamental para Ω se puede descomponer como sigue:

$$\mathscr{F}_\Omega = \bigcup_{i=1}^{\mu} S_i(\mathscr{F}). \tag{4.13}$$

Si esta región está formada por triángulos modulares $\mathscr{T}$ que comparten sólo un lado, entonces se demuestra que $\mathscr{F}_\Omega$ es simplemente conexo (B. Schoeneberg, [42]). Por otro lado, siempre existe una región de este tipo, con lo que siempre podemos, si así conviene, establecer una región fundamental simplemente conexa. Si alguno de estos triángulos modulares $\mathscr{T}$ no está en $\mathscr{F}_\Omega$ pero uno de sus lados forma parte del borde, siempre existe una *transformación de borde* $S \in \Omega$ tal que $S(\mathscr{T})$ y $\mathscr{T}$ comparten un lado.

Denotaremos como $\sigma_i(\Omega)$ (respectivamente $\sigma_\rho(\Omega)$) al número de puntos en la región $\mathscr{F}_\Omega$ pertenecientes a la órbita Γi pero no Ω-equivalentes a i (respectivamente ρ), y $\sigma_\infty(\Omega)$, al número de cúspides en $\mathscr{F}_\Omega$ que no son Ω-equivalentes a ∞. En el caso de las cúspides, la cantidad $\nu_\infty(\Omega)$ definida al inicio del apartado (4.1.1) y la cantidad $\sigma_\infty(\Omega)$ recién definida son iguales, puesto que para toda cúspide a/c de la región fundamental del subgrupo existe una matriz parabólica $P = AU^kA^{-1} \in \Omega$ que la fija, tomando $A \in \Gamma$ tal que $A^{-1}(a/c) = \infty$. Por simplificar la notación, se suele hablar del número t de cúspides no Ω-equivalentes, cumpliéndose por tanto la igualdad

$$t = \nu_\infty(\Omega) = \sigma_\infty(\Omega).$$

Concretemos la relación entre las cúspides en $\mathscr{F}_\Omega$ y el nivel de Ω en Γ, a través de la siguiente proposición:

Proposicion 4.2. *(Abanicos de triángulos en torno a una cúspide) Las cúspides en $\mathscr{F}_\Omega$ son siempre puntos fijos por transformaciones parabólicas y pertenecen al borde. La acción de Ω sobre los triángulos que colindan en la cúspide z_∞ genera un abanico de amplitud finita $k > 0$, y como el estabilizador de Γ en z_∞ es cíclico e infinito con generador AU^kA^{-1}, $A(\infty) = z_\infty$, los triángulos que forman dicho abanico son los $AU^i(\mathscr{F}_\Omega)$, $i = 0, 1, \cdots, k-1$. Así, cada abanico de triángulos se apoya en una cúspide y se cumple que el nivel (de Wohlfahrt) de Ω es el mínimo común múltiplo de las amplitudes k_i, $i = 1, \cdots, t$.*

Cabría plantearse la relación entre la región fundamental de un subgrupo y la de su conjugado en Γ. Pues bien, si $P = L\Omega L^{-1}$ con $L \in \Gamma$, entonces $\mathscr{F}_P := L^{-1}(\mathscr{F}_\Omega)$ y por supuesto $L(\mathscr{F}_\Omega)$ también es una región fundamental para Ω por ser normal. De momento, sólo falta una herramienta para poder analizar las regiones fundamentales que entran en nuestro objetivo.

Definicion 4.2. (Semitriángulo) Sea $\mathscr{F}^*$ el cierre de $\mathscr{F}$ junto con $\{\infty\}$. Se define un *semitriángulo* como la imagen de $\mathscr{F}^*$ por las transformaciones del grupo modular extendido con reflexiones (definidas en 1.13). Con ello, denotamos $2n_z$ al número de semitriángulos no Ω-equivalentes que se apoyan en los puntos Γ-equivalentes a z.

Teorema 4.4. *Si Ω es normal en Γ, entonces el número de semitriángulos (no Ω-equivalentes) que forman un abanico en torno a i (respectivamente ∞ y ρ) es igual al número de semitriángulos que forman un abanico en torno a cualquier punto equivalente a i (respectivamente ∞ y ρ).*

Demostración. Supongamos que z_0 es tal que $L(z_0) = z_0$, con $L \in \Omega$, y que $B(z_0) = z_1$ con $B \in \Gamma$. Entonces

$$BLB^{-1}(z_1) = z_1.$$

Si Ω es normal, $BLB^{-1} \in \Omega$. Como $L = AX^kA$ para algún $A \in \Gamma$ tal que $A(\infty) = z_0$, siendo X el generador (supongamos de orden $k > 0$) del estabilizador de z_0 , entonces

$$BLB^{-1} = BAX^kA^{-1}B^{-1} = (BA)X^k(BA)^{-1}$$

con punto fijo z_1, que tiene asociado el mismo valor de k que z_0. □

Esta cantidad n_z es importante dado que a (n_i, n_ρ, n_∞) se le denomina *esquema de ramificación* para $\Omega \lhd \Gamma$ y determina de manera unívoca a los subgrupos normales.

Como consecuencia de todo lo que llevamos desarrollado hasta ahora, se tiene que $n_i \in \{1,2\}$, $n_\rho \in \{1,3\}$ y $n_\infty = \text{mín}\left\{ \; k \in \mathbb{N} \;\middle|\; U^k \in \Omega \; \right\}$. Terminemos este apartado con una importante relación entre el número de semitriángulos y el número de puntos no equivalentes, que no es más que una generalización de la relación $\mu = tn$ dada en (3.58):

Teorema 4.5. *Sea μ el índice de un subgrupo normal $\Omega \lhd \Gamma$, se tiene*

$$\mu = \sigma_i n_i = \sigma_\rho n_\rho = \sigma_\infty n_\infty. \tag{4.14}$$

Esquema de ramificación de los subgrupos principales de congruencia.
En concreto, para los grupos $\Gamma[N]$ cuando $N \geq 2$ (sin olvidar la identificación $I \sim -I$), se tiene el esquema de ramificación

$$(n_i, n_\rho, n_\infty) = (2,3,N), \tag{4.15}$$

ya que su nivel es, como ya hemos estudiado en el capítulo anterior, $N = n_\infty$, y además ni T (que fija i) ni R (que fija ρ) son congruentes con I módulo N si $N \geq 2$.

4.1.2. Regiones fundamentales de los subgrupos principales de congruencia

En este apartado vamos a centrar la atención en los subgrupos principales de congruencia $\Gamma[N]$ con $N \geq 2$, haciendo hincapié en el conjunto de cúspides no equivalentes bajo el subgrupo y en su esquema de ramificación. Antes de comenzar, resumimos el proceso de construcción de las regiones fundamentales:

Proposicion 4.3. *Dado un subgrupo normal $\Omega \lhd \Gamma$ con esquema (n_i, n_ρ, n_∞), podemos construir una región fundamental teniendo en cuenta la ecuación (4.15), y tomando como región la unión de los n_∞ triángulos modulares*[1] *que se apoyan en cada una de las σ_∞ cúspides del subgrupo. Las transformaciones de borde, que conectan los pares de lados equivalentes, generan el subgrupo.*

Particularicemos al caso de los subgrupos más importantes vistos. Como el subgrupo principal extendido $\Gamma[N]$ tiene nivel N e índice μ en Γ, el número de cúspides viene dado por $\sigma_\infty = \mu/N$, luego

Proposicion 4.4. *(Regiones fundamentales de $\Gamma[N]$) Para construir la región fundamental de $\Gamma[N]$ basta con tomar un abanico de N triángulos modulares apoyados en cada cúspide. Podemos establecer un conjunto de cúspides no equivalentes (módulo N) buscando un sistema de σ_∞ números racionales a_i/b_i, $i = 1, 2, \cdots, \sigma_\infty$ tales que a_i/b_i y a_j/b_j no son $\Gamma[N]$-equivalentes si $i \neq j$.*

Consideraciones computacionales.
Existe un algoritmo[2] elaborado por Ravi S. Kulkarni (ver [23]) basado en lo que se llama el *símbolo de Farey* del subgrupo (consultar [25]), y que permite obtener conjuntos completos de cúspides no equivalentes, así como los generadores de los subgrupos $\Gamma[N]$. Existen otros como el *algoritmo de Todd-Coxeter* que también encuentra conjuntos de generadores, pero la ventaja del algoritmo basado en el símbolo de Farey reside en que proporciona los conjuntos mínimos de generadores.

Exponemos a continuación las regiones fundamentales de los subgrupos principales de congruencia para algunos valores de N, con el objetivo de visualizar las cúspides y los abanicos de triángulos:

- En el caso de $\Gamma[2]$, con esquema $(n_i, n_\rho, n_\infty) = (2, 3, 2)$, se tiene la región formada por 3 abanicos de 2 triángulos modulares cada uno, un abanico apoyado en cada cúspide $(\infty, 0, 1)$. Tendría el siguiente aspecto[3] :

[1] Según vimos, son imágenes de $\mathscr{F}$ por transformaciones en Ω.

[2] En la web http://doc.sagemath.org/html/en/reference/arithgroup/sage/modular/arithgroup/farey_symbol.html se pueden consultar las distintas funciones en lenguaje **SAGE**, y se pueden realizar cálculos en entornos en línea como https://sagecell.sagemath.org/.

[3] Imagen creada con el software **FunDomain**, escrito por Helena A. Verrill, y bajo licencia GNU GPL. Disponible en https://wstein.org/Tables/fundomain/

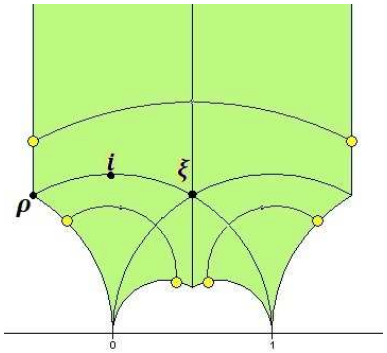

Figura 4.1: Región fundamental para $\Gamma[2]$.

En la figura se han conectado los bordes equivalentes, y se ha marcado el punto $\xi = e^{\pi i/3}$ para una consideración adicional: si tomamos la división de la región en semitriángulos, como en la siguiente figura:

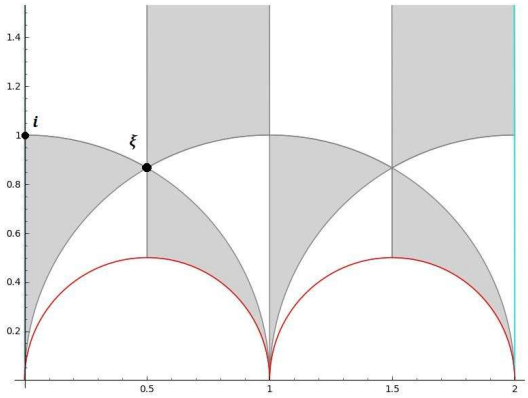

Figura 4.2: Región fundamental para $\Gamma[2]$ mediante semitriángulos.

se observa que hay 6 semitriángulos apoyados en $\rho = e^{2\pi i/3}$ y en ξ, y 4 semitriángulos apoyados en i, conforme a los resultados vistos que afirman que debe haber $2n_z$ semitriángulos apoyados en z, siendo n_z la amplitud de la cúspide (y el nivel del subgrupo) cuando $z = \infty$. Además, los 6 semitriángulos apoyados en ρ (o en cualquiera de los puntos Γ-equivalentes) son $\Gamma[2]$-equivalentes. Podemos elegir como generadores las transformaciones de borde[4]:

$$U^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix}, -I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \tag{4.16}$$

si bien en [42] se fijan los generadores U^2 y $V = (U^2)^T$ y se afirma, sin demostrar, que $\Gamma[2]$ es un grupo libre en dichos generadores.

[4]Calculadas mediante las funciones en **SAGE** creadas por Jordi Quer y David Loeffler (descritas en http://doc.sagemath.org/html/en/reference/arithgroup/sage/modular/arithgroup/congroup_gammaH.html).

- Para $\Gamma[3]$, $(n_i, n_\rho, n_\infty) = (2,3,3)$, se tienen las transformaciones de borde

$$U^3, \begin{pmatrix} -8 & 3 \\ -3 & 1 \end{pmatrix}, \begin{pmatrix} 4 & -3 \\ 3 & -2 \end{pmatrix} \tag{4.17}$$

y la región fundamental

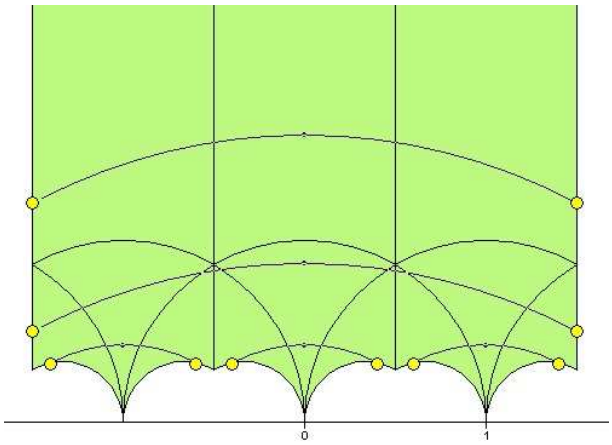

Figura 4.3: Región fundamental para $\Gamma[3]$.

- Para $\Gamma[4]$, con esquema $(n_i, n_\rho, n_\infty) = (2,3,4)$, se tienen los generadores

$$U^4, \begin{pmatrix} -15 & 4 \\ -4 & 1 \end{pmatrix}, \begin{pmatrix} 5 & -4 \\ 4 & -3 \end{pmatrix}, \begin{pmatrix} 9 & -16 \\ 4 & -7 \end{pmatrix}, \begin{pmatrix} 13 & -36 \\ 4 & -11 \end{pmatrix} \tag{4.18}$$

y la región fundamental

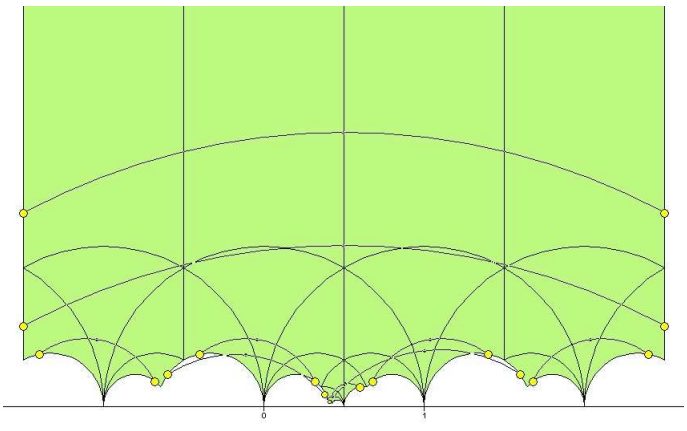

Figura 4.4: Región fundamental para $\Gamma[4]$.

En cada una de las regiones expuestas es evidente el conjunto de cúspides, sin más que elegir los valores racionales sobre los que se apoyan los abanicos de triángulos modulares, además de ∞.

4.2. Superficies de Riemann

Los conceptos fundamentales que se han tratado a lo largo de las secciones previas tienen un sentido geométrico que cobra evidencia al visualizar las regiones fundamentales de Γ y sus subgrupos $\Omega \subset \Gamma$. En esta sección dotaremos de una topología al semiplano superior hiperbólico extendido $\mathscr{U}^*$, y dotaremos al espacio de órbitas $\mathscr{U}^*/\Gamma$ de una estructura de superficie (de Riemann) tomando la topología inducida. Veremos que, para algunos valores de N, el grupo $PSL_2(\mathbb{Z}_N)$ actúa como grupo de rotaciones de ciertos poliedros (según los resultados de Klein en [19]). Asimismo, reubicaremos la conocida fórmula de Euler en este contexto, y la utilizaremos para entontrar expresiones para el cálculo del género de algunas regiones fundamentales.

4.2.1. La esfera de Riemann

Como ejemplo introductorio, obtengamos la esfera de Riemann como espacio de órbitas por la acción de Γ. Partamos de la región fundamental para Γ:

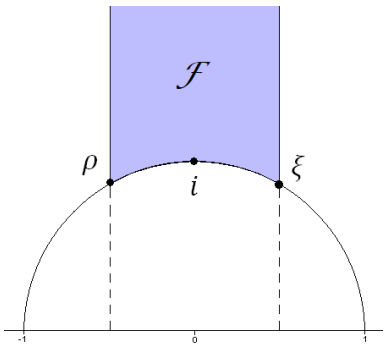

Figura 4.5: Región fundamental para Γ.

Si tomamos el espacio de órbitas $\mathscr{U}/\Gamma$ e identificamos los lados equivalentes por transformaciones de borde (que, recordemos, pueden ser expresadas como productos de los generadores T y U), obtenemos la esfera unidad con un *pinchazo*

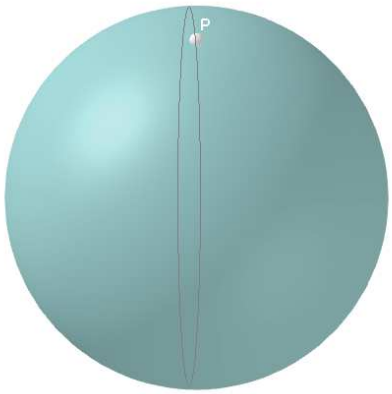

Figura 4.6: Esfera con agujero $\mathscr{U}/\Gamma \cong S^2 - \{P\}$.

que corresponde a la clase de equivalencia de puntos parabólicos en Γ, esto es, a la única cúspide ∞. Como todo punto en $\mathbb{Q}$ es Γ-equivalente a ∞, podemos entender la identificación como un *pegado* de todos los racionales en un único punto P. Esta esfera no es compacta puesto que, al establecer el homeomorfismo pertinente sobre $\mathscr{U}$, no se incluyen las imágenes de $\mathbb{Q}^* = \mathbb{Q} \cup \{\infty\}$ (por no pertenecer al semiplano superior $\mathscr{U}$). Lo que haremos es considerar el semiplano extendido $\mathscr{U}^* = \mathscr{U} \cup \mathbb{Q}^*$ a la hora de definir tanto la topología como las aplicaciones correspondientes, y de esta forma estaremos añadiendo el punto P a la esfera anterior, haciendo que sea compacta. Con ello, tendremos el isomorfismo:

$$\mathscr{U}^*/\Gamma \cong \Sigma \tag{4.19}$$

donde $\Sigma = \mathbb{C} \cup \{\infty\}$ es la *esfera de Riemann*. Cabe esperar, entonces, que si un subgrupo normal de Γ tiene n_∞ cúspides no equivalentes, al considerar el espacio de órbitas aparezcan n_∞ *pinchazos* en la superficie. Hemos obviado el desarrollo matemático, ya que en el siguiente apartado detallaremos el proceso para cualquier cociente $\mathscr{U}^*/\Omega$ con $\Omega \subseteq \Gamma$, con el propósito de obtener superficies, comprobar que son superficies de Riemann y calcular su género.

4.2.2. Superficies de Riemann como espacios de órbitas

Tras la motivación del punto anterior, en el que hemos introducido la esfera de Riemann como espacio de órbitas de una forma cualitativa, veamos cómo podemos dotar al semiplano superior extendido $\mathscr{U}^*$ de una topología, para a continuación obtener la topología inducida en el cociente $\mathscr{U}^*/\Omega$ (con $\Omega \subseteq \Gamma$) y terminar dotando a este último espacio de la estructura de superficie de Riemann $\mathscr{R}$, de modo que

$$\mathscr{U}^*/\Omega \cong \mathscr{R}.$$

Durante toda la sección consideraremos un subgrupo $\Omega \subseteq \Gamma$ tal que $-I \in \Omega$ (o inluso $\Omega = \Gamma$).

Pues bien, comencemos tomando la proyección canónica

$$\pi : \mathscr{U}^* \longrightarrow \mathscr{R}, z \mapsto [z] := \left\{ \; A(z) \;\middle|\; A \in \Omega \; \right\}$$

que asigna a cada complejo del semiplano extendido su clase de puntos equivalentes. El objetivo será obtener la representación de la superficie mediante la identificación de los puntos equivalentes, misión para la que previamente necesitamos una topología en $\mathscr{U}^*$.

Proposicion 4.5. *(Topología en $\mathscr{U}^*$) Sea $\mathscr{U}^*$ el semiplano superior extendido y $z \in \mathscr{U}^*$, se tiene la familia de entornos $\mathscr{B}_z$ definida como:*

- *Si $z \in \mathscr{U}$, entonces*

  $$B_{z,r} = \left\{ \; \tau \in \mathscr{U} \;\middle|\; \left|\frac{\tau - z}{\tau - \bar{z}}\right| < r \; \right\}$$

  con $r \in (0,1)$.

- *Si $z \in \mathbb{Q}^*$, pongamos $z = -d/c$ irreducible, evidentemente z es Γ-equivalente a ∞, con lo que tomamos*

  $$B_{z,r} = \left\{ \; \tau \in \mathscr{U} \;\middle|\; Im\left(\frac{a\tau + b}{c\tau + d}\right) > \frac{1}{r} \; \right\} \cup \{z\}$$

  con $r \in (0,1)$ y $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

Así, un conjunto $V \subset \mathscr{U}^*$ será abierto si $V = \bigcup B_{z,r}$, y como para todo entorno V_z de z existe r tal que $B_{z,r} \subset V_z$, se tiene que $\mathscr{B}_z$ es una base de entornos que dotan a $\mathscr{U}^*$ de la estructura de espacio topológico.

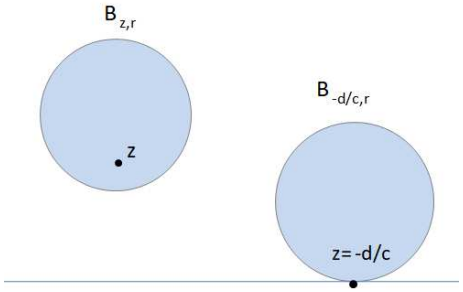

Figura 4.7: Tipos de entornos abiertos en $\mathscr{U}^*$.

De la proposición se deduce inmediatamente que $\mathscr{U}^*$ es un espacio topológico Hausdorff y conexo. Sin embargo, no es *localmente compacto*, pues si lo fuera, un punto racional q tendría un entorno compacto V conteniendo un entorno cerrado y compacto $B_{q,r}$, de forma que si $\{q_i\} \in \partial B_{q,r}$ es una sucesión convergente a q se tendría que cada entorno $B_{z,r'}$ contendría casi todos los q_i, hecho imposible si $r' \leq r$. Obtengamos ahora la topología inducida en $\mathscr{R}$:

Proposicion 4.6. *(Topología en $\mathscr{R} = \mathscr{U}^*/\Omega$) Un conjunto $V \subset \mathscr{R}$ es abierto en la topología cociente si y sólo si $\pi^{-1}(V)$ lo es en la topología definida en $\mathscr{U}^*$. Así, la proyección π es continua y abierta (un homeomorfismo) y $\mathscr{R}$ es un espacio conexo, Hausdorff y compacto.*

Demostración. Si V es un abierto en $\mathscr{U}^*$, entonces $\pi^{-1}(\pi(V)) = \bigcup_{A\in\Omega} A(V)$ es abierto por ser la unión de abiertos, por lo que necesariamente π es una aplicación abierta. Además, $\mathscr{R}$ es conexo y compacto pues contiene al cierre de la región fundamental $\mathscr{F}$ de Ω, que tiene intersección no vacía con todas las clases de Ω-equivalencia de puntos (por definición). Comprobar que es Hausdorff es inmediato tomando los abiertos $B_{z,r}$ adecuados. □

Veamos ahora que, efectivamente, $\mathscr{R}$ es una superficie. Recordemos primero la definición:

Definicion 4.3. (Superficies, cartas y atlas) Un espacio topológico Hausdorff junto con un recubrimiento abierto, del que cada entorno abierto es homeomorfo a un abierto del plano euclídeo $\mathbb{R}^2$, es llamado una *superficie*. Sea uno de estos abiertos V_i del recubrimiento y ϕ_i el homeomorfismo

$$\phi_i : V_i \longrightarrow U_i \subset \mathbb{R}^2,$$

a la dupla $\{U_i, \phi_i\}$ se le denomina *carta* y a la familia de cartas $\mathscr{A} = \{U_i, \phi_i\}_i$ se le denomina *atlas*.

Dotemos entonces a $\mathscr{R}$ de la estructura de superficie, tomando los entornos abiertos de un punto z

$$V_{[z]} = \pi(B_{z,r})$$

en $\mathscr{R}$ con r suficientemente pequeño para que o bien $B_{z,r}$ esté contenido en un triángulo modular o bien en la unión de varios semitriángulos apoyados en z. Si tomamos el mismo r para todos los z equivalentes, podemos simplificar la notación y simplemente indicar B_z. Al ser la proyección π sobreyectiva y abierta, el recubrimiento abierto para $\mathscr{R}$ está bien definido. Necesitamos ahora un homeomorfismo

$$\phi_i : V_{[z]} \longrightarrow U_{[z]} \subset \mathbb{R}^2$$

de forma que la preimagen de un abierto $V_{[z]}$ de $\mathscr{R}$ sería

$$B_z = \pi_z^{-1}\left(V_{[z]}\right),$$

siendo π_z la restricción de π a B_z. Como hicimos al definir la topología para $\mathscr{U}^*$, distingamos dos casos:

1. Si z no es una cúspide de Ω, elegimos un representante z_0 de la clase $[z]$, con lo que cada punto equivalente $z \in [z]$ será $A(z_0)$ para cierta $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Omega$. Definimos

$$\phi_z(\tau) := \left(\frac{\tau - z}{\tau - \overline{z}} \cdot \frac{cz_0 + d}{c\overline{z_0} + d}\right)^k, \tau \in B_z, \tag{4.20}$$

donde $k = 1$ si z no es fijo y $k \in \{2,3\}$ si z es fijo elíptico. Así, el factor $\left(\frac{cz_0+d}{c\overline{z_0}+d}\right)^k$ está determinado por z y z_0, y vale 1 si $k \in \{2,3\}$. De esta manera, π_z^{-1} asigna k valores de B_z a cada $V_{[z]}$ y la aplicación ϕ_z manda todos los B_z exactamente a un único abierto $U_{[z]}$ del plano euclídeo, luego $\phi_z \circ \pi_z^{-1}$ es biyectivo. Como ϕ_z es holomorfa, es continua y abierta, por lo que π_z también lo será, y así será finalmente la composición $\phi_{[z]}$, que en consecuencia es un homeomorfismo.

2. Si z es una cúspide de Ω, pongamos $z = -d/c$ irreducible. Cogemos

$$\phi_z(\tau) := e^{\frac{2\pi i}{k}A'(\tau)}, \tau \in B_z, \tag{4.21}$$

donde k es la amplitud de la cúspide y $A' \in \Gamma$. La cúspide z determina ϕ_z salvo múltiplos de potencias de $e^{\frac{2\pi i}{k}}$, y finalmente la elección de A' determina completamente ϕ_z.

Así, tendríamos el homeomorfismo

$$\phi_{[z]} := \phi_z \circ \pi_z^{-1} : V_{[z]} \longrightarrow U_{[z]} \subset \mathbb{R}^2$$

con ϕ_z continua y abierta. En ambos casos, el representante de la clase de puntos equivalentes es indiferente a la hora de definir la función $\phi_{[z]}$ y el abierto $U_{[z]}$, puesto que si $\tau_0 = A(\tau)$ con $A \in \Omega$ en el primer caso se tiene

$$\frac{\tau - z}{\tau - \overline{z}} = \frac{\tau_0 - z_0}{\tau_0 - \overline{z_0}} \cdot \frac{cz_0 + d}{c\overline{z_0} + d}$$

y en el segundo caso

$$e^{\frac{2\pi i}{k}A'A^{-1}(\tau)} = e^{\frac{2\pi i}{k}A'(\tau)}, \; con\, A'A^{-1}(z) = \infty.$$

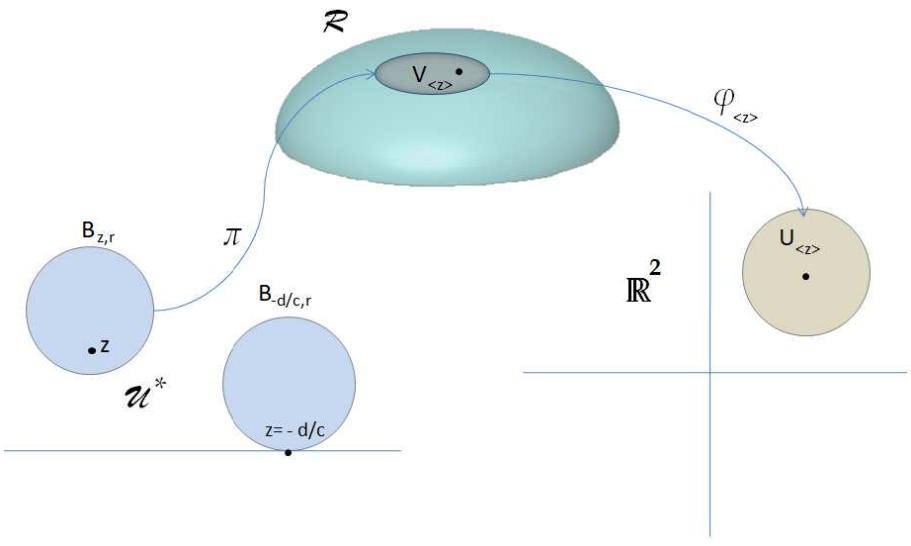

Figura 4.8: Aplicaciones entre $\mathcal{U}^*$, $\mathcal{R}$ y $\mathbb{R}^2$.

Al fin, se tiene el siguiente

Teorema 4.6. *$\mathscr{R}$ es una superficie con atlas* $\mathscr{A} := \left\{ \left(V_{[z]}, \phi_{[z]}\right) \;\middle|\; [z] \in \mathscr{R} \right\}$.

Terminemos comprobando que $\mathscr{R}$ es una superficie de Riemann, para lo cual resumimos la definición que ya vimos:

Definicion 4.4. (Superficie de Riemann) Una superficie se denomina superficie de Riemann si sus cartas son compatibles mediante funciones holomorfas, esto es, si dadas las imágenes en $\mathbb{R}^2$ de distintas intersecciones de pares de abiertos del recubrimiento, existe una función holomorfa entre todas ellas.

Teorema 4.7. *La superficie $\mathscr{R}$ con atlas* $\mathscr{A} := \left\{ \left(V_{[z]}, \phi_{[z]}\right) \;\middle|\; [z] \in \mathscr{R} \right\}$ *es de Riemann.*

Demostración. Sean dos clases distintas $[z_1]$ y $[z_2]$ y $D = V_{[z_1]} \cap V_{[z_2]}$ y las imágenes $U_1 = \phi_{[z_1]}(D)$ y $U_2 = \phi_{[z_2]}(D)$ en el plano euclídeo. De acuerdo al homeomorfismo que establecimos más arriba,

$$\phi_{[z_2]} \circ \phi_{[z_1]}^{-1} = \phi_{z_2} \circ \pi_{z_2}^{-1} \circ \pi_{z_1} \circ \phi_{z_1}^{-1}$$

es, restringido a U_1, una aplicación de U_1 a U_2 y de hecho es holomorfa ya que U_1 no contiene imágenes de puntos Ω-equivalentes a ρ, i ni ∞, y porque la restricción de $\pi_{z_2}^{-1} \circ \pi_{z_1}$ a $\phi_{z_1}^{-1}(U_1)$ es la restricción de un elemento de Ω. □

4.2.3. Género de las regiones fundamentales

Una vez visto que el espacio de órbitas $\mathscr{U}^*/\Omega$, $\Omega \subseteq \Gamma$, es una superficie de Riemann, vamos a estudiar uno de los invariantes topológicos más importantes a la hora de clasificar superficies: el *género*. A partir de la famosa fórmula de Euler para poliedros obtendremos una expresión para el cálculo del género de una región fundamental del subgrupo Ω, correspondiente también al género de la superficie. De esta manera, quedará totalmente determinada (salvo equivalencia conforme) la superficie de Riemann obtenida por la acción de un subgrupo. Comencemos recordando algunas definiciones de índole topológica:

Definicion 4.5. (Arco, curva y polígono.) Sea una superficie de Riemann $\mathscr{R}$, y por tanto orientable y compacta. Dado el homeomorfismo sobre la imagen

$$\phi_1 : [0,1] \longrightarrow \mathscr{R},$$

se denomina *arco* a la imagen $\phi_1([0,1]) \subset \mathscr{R}$. Una sucesión de arcos $a_1, a_2, \cdots, a_n$ se denomina *curva* si el punto final de un arco es el punto inicial del siguiente, y la curva será *cerrada* en caso de que sus puntos inicial y final coincidan. Si tomamos otro homeomorfismo

$$\phi_2 : D \longrightarrow \mathscr{R},$$

donde D es un disco cerrado del plano $\mathbb{R}^2$, se denomina *polígono* a la imagen $\phi_2(D)$ en la superficie. Una colección finita de curvas con un número finito de puntos de intersección tal que el cierre de

cada componente conexa de su complementario es un polígono, y tal que su intersección consta de un único punto o una única arista (o bien es vacía), se denomina *descomposición poligonal* de $\mathscr{R}$. En el capítulo siguiente, en el que hablaremos del concepto más amplio de *grupo de Hecke*, utilizaremos una teoría alternativa pero equivalente denominada *teoría de mapas regulares*.

Al pensar en la descomposición poligonal, podemos visualizar la descomposición de un poliedro regular en caras poligonales. Inscribamos el poliedro en una esfera y proyectemos esta descomposición a la superficie de la esfera. Así, siguen teniendo sentido los conceptos de vértice, arista y cara como los entendemos en su versión clásica. Enunciamos ahora el teorema de Euler para poliedros[5], extendiendo la fórmula conocida para poliedros convexos.

Teorema 4.8. *(Fórmula de Euler) Sea una superficie $\mathscr{R}$, para cualquier par de descomposiones poligonales $\mathscr{P}_i$ y $\mathscr{P}_j$ $(i \neq j)$ se tiene la relación*

$$v_i - a_i + c_i = v_j - a_j + c_j, \tag{4.22}$$

donde v es el número de vértices, a el número de aristas y c el número de caras. Es decir, la cantidad $v - a + c$ es constante, independientemente de la descomposición elegida.

Por ejemplo, en el caso de un poliedro regular como el octaedro, se tiene que

$$v - a + c = 6 - 12 + 8 = 2,$$

y nótese que podemos inscribir el octaedro en una esfera (que tiene género $g = 0$). A nivel topológico, podemos entender una superficie orientable compacta de género g como una esfera a la que se le añaden g *asas* (ver [15]), pero el concepto de género es más complicado que esta idea:

Teorema 4.9. *Sea una superficie de Riemann $\mathscr{R}$, su género como superficie orientable coincide con el número máximo de curvas cerradas disjuntas que no descomponen $\mathscr{R}$ en varias superficies. La expresión del género viene dada por*

$$g = 1 - \frac{v - a + c}{2}. \tag{4.23}$$

Evidentemente, si el género es 0 se tiene $2 = v - a + c$, la versión simplificada de este teorema. El género es un importante invariante topológico (por homeomorfismos, por tanto) y es de gran utilidad a la hora de clasificar superficies. Por ampliar este concepto, recordemos que la llamada *característica de Euler* para superficies orientables se calcula como

$$\chi(\mathscr{R}) = 2 - 2g, \tag{4.24}$$

estando este número relacionado con la *estructura de celdas* de la superficie, concepto desarrollado ampliamente por A.Hatcher en [15].

[5] La demostración aparece en la obra [4] de H. Behnke y F. Sommer.

Volviendo al caso de los subgrupos del grupo modular, tengamos en mente la región fundamental $\mathscr{F}$ como unión de semitriángulos modulares. Pues bien, si recuperamos la proyección

$$\pi : \mathscr{U}^* \longrightarrow \mathscr{R},$$

se tiene que la imagen de un semitriángulo es un polígono en $\mathscr{R}$, con lo que la imagen de todos los semitriángulos forma una descomposición poligonal en $\mathscr{R}$ con 2μ caras (ya que hay μ triángulos modulares en la región fundamental) y r vértices $v_1, v_2, \cdots, v_r$. Como, según nuestra notación, el número de semitriángulos que se apoyan en τ es $2n_\tau$, el número de aristas será $a = n_{v_1} + n_{v_2} + \cdots + n_{v_r}$. Sustituyendo en la expresión (4.23), obtenemos la fórmula

$$g = 1 - \mu + \frac{1}{2}\sum_{k=1}^{r}(n_{v_k} - 1), \tag{4.25}$$

entendible como *género de la superficie* $\mathscr{R}$ o como *género de la región fundamental*. Ya conocemos que si Ω es normal en Γ, el número de semitriángulos que se apoya en cada punto equivalente a i, ρ o ∞ es el mismo independientemente del punto de la clase de equivalencia. Así, teníamos $2n_i$ semitriángulos apoyados en i, $2n_\rho$ en ρ y $2n_\infty$ en ∞, la cantidad n_∞ era el nivel del subgrupo y el número de puntos no Ω-equivalentes venía dado por

$$\sigma_z = \mu / n_z,\ z \in \{i, \rho, \infty\}.$$

Pues bien, en el caso de los vértices $v_1, v_2, \cdots, v_r$, aquellos que sean Ω-equivalentes tendrán el mismo número de semitriángulos $2n_{v_k}$, con lo que podemos concretar la fórmula del género:

$$g = 1 - \mu + \frac{\mu}{2}\left(\sum_{z\in\{i,\rho,\infty\}} \frac{n_z - 1}{n_z}\right). \tag{4.26}$$

Como $n_i \in \{1,2\}$ y $n_\rho \in \{1,3\}$ según vimos (teorema (4.4) y ejemplo posterior), la expresión del género puede transformarse en la siguiente:

$$g = 1 + \frac{\mu}{12} - \frac{\sigma_\rho}{3} - \frac{\sigma_i}{4} - \frac{\sigma_\infty}{2}. \tag{4.27}$$

Sabemos además que los subgrupos principales de congruencia $\Gamma[N]$ tienen esquema $(n_i, n_\rho, n_\infty) = (2, 3, N)$, por tanto se tiene una concreción más para el género, como ya adelantábamos en la relación (3.60) recogida de los trabajos de Gunning:

$$g = 1 + \mu\frac{N-6}{12N}, \tag{4.28}$$

donde μ es el índice del subgrupo.

En la siguiente tabla se muestra el género de las superficies para algunos valores de N:

N	2 a 5	6	7	8	9	10	11	12
g	0	1	3	5	10	13	26	25

Cuadro 4.1: Género de las superficies de Riemann $\mathscr{U}^*/\Gamma[N]$.

Observando los valores de g para $N = 1, 2, \cdots, 5$, vemos que la superficie de Riemann resultante debe ser, en todos estos casos, la esfera de Riemann Σ, mientras que cuando $N = 6$ la superficie de Riemann de género 1 es homeomorfa al toro complejo $\mathbb{C}/\omega$, para algún *retículo* ω (revisar el teorema (1.2)). No podemos dejar de relacionar estos resultados con un artículo de Knopp (ver [21]) en el que afirma:

Teorema 4.10. *Sea el subgrupo normal $\Delta(m)$ de Γ. Si es de índice finito en $\Gamma[m]$, entonces su región fundamental tiene género 0, y por tanto la superficie de Riemann $\mathscr{R} = \mathscr{U}^*/\Delta(m)$ será la esfera de Riemann.*

Complementando este teorema con la afirmación de Klein y Fricke de que el género de la región fundamental del subgrupo $\Gamma[m]$ es $g = 0$ si y sólo si $m \in \{1, 2, 3, 4, 5\}$, y como $\Delta(m) = \Gamma[m]$ en estos casos (Brenner, [6]), se concluye que para $m \geq 6$ el índice $|\Gamma[m] : \Delta(m)|$ tiene que ser infinito (y el género no nulo).

En el siguiente apartado veremos que los valores $N = 1, 2, \cdots 5$ están relacionados con el poliedro regular que se puede inscribir en la esfera, siendo los vértices de apoyo las imágenes de las $t = n_\infty$ cúspides (por ejemplo, un tetraedro en el caso $N = 3$).

4.2.4. Poliedros y grupos de rotaciones

Como adelantamos al inicio de la sección, para el subgrupo principal $\Gamma[N]$ con t cúspides, se tiene que el espacio de órbitas $\mathscr{U}/\Gamma[N]$ es la esfera de Riemann menos t puntos, correspondientes a las cúspides del subgrupo. Por ejemplo, la superficie de Riemann $\mathscr{U}/\Gamma[2]$ es la esfera menos los tres puntos correspondientes a las imágenes de las clases de cúspides $[\infty]$, $[1]$ y $[0]$, que no son $\Gamma[2]$-equivalentes. No obstante, hemos logrado obtener superficies de Riemann compactas al trabajar con una topología en el semiplano superior extendido $\mathscr{U}^*$.

Gracias a los trabajos de Klein y Fricke (ver [19], [12] y [20]), es conocida la clasificación de los grupos modulares de nivel N, $PSL_2(\mathbb{Z}_N)$, para los primeros valores de N. Pese al arduo trabajo que hay detrás de esta clasificación, tratemos de arrojar cierta luz con algunos ejemplos.

- Para el subgrupo principal de congruencia $\Gamma[5] = (2, 3, 5)$, se tiene nivel $N = 5$, índice $\mu = 60$ en Γ y, por tanto, $t = 60/5 = 12$ cúspides no equivalentes. Al tomar la imagen de $\mathscr{U}^*$ por la proyección canónica π, tenemos como superficie la esfera de Riemann, y las imágenes de las 12 cúspides serán vértices de la descomposición poligonal de la misma. Podemos ver la región fundamental (con semitriángulos) proyectada en la esfera como descomposición poligonal en la siguiente imagen:

Figura 4.9: Región fundamental de $\Gamma[5]$ como descomposición poligonal de la esfera.

Vemos que cada cúspide tiene alrededor $2n_\infty = 2N = 10$ semitriángulos, o bien 5 triángulos modulares. Asimismo, cada punto elíptico equivalente a i tiene $2n_i = 4$ semitriángulos alrededor y por último cada punto elíptico equivalente a ρ tiene $2n_\rho = 6$ semitriángulos. Así, podemos inscribir un poliedro regular con 12 vértices, cada uno de los cuales tendrá $N = 5$ caras alrededor como imágenes de los triángulos modulares, y apoyando dichos vértices en las cúspides de la descomposición. En este caso, el poliedro que cumple estas características es el *icosaedro*, de modo que podemos pensar en un icosaedro inscrito en la esfera de Riemann. Así, las caras del poliedro son triángulos equiláteros y habrá un total de $60/3 = 20$ caras por lo que, como la esfera tiene género $g = 0$, habrá $a = v + c - 2 = 12 + 20 - 2 = 30$ aristas, como ya sabemos. Así, como

$$|PSL_2(\mathbb{Z}_5)| = \mu = 60$$

es el orden del cociente $\Gamma/\Gamma[5]$, podemos ver el grupo modular de nivel 5, $PSL_2(\mathbb{Z}_5)$, como el grupo de rotaciones del icosaedro, que tiene 60 elementos y es isomorfo (Klein, [19]) al grupo alternado A_5.

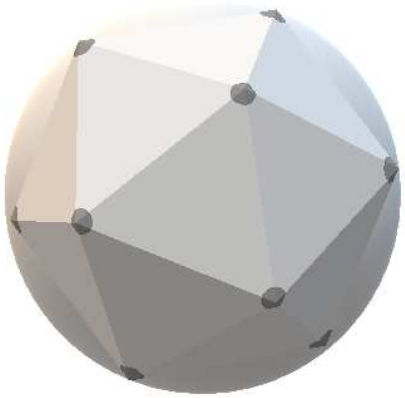

Figura 4.10: Icosaedro inscrito en la esfera.

- Para el grupo principal $\Gamma[4] = (2,3,4)$, tenemos nivel $N = 4$, índice $\mu = 24$ en Γ y, por tanto, $t = 24/4 = 6$ cúspides no equivalentes. Si tomamos la región fundamental de semitriángulos proyectada en la esfera, tendría el siguiente aspecto:

Figura 4.11: Región fundamental de $\Gamma[4]$ como descomposición poligonal de la esfera.

Por el razonamiento realizado en el caso anterior, como $N = 4$, sabemos que cada cúspide (vértice del poliedro regular) tendrá alrededor 4 caras como imágenes de triángulos modulares. El poliedro regular con 6 vértices es el *octaedro*, con lo que habrá un total de $24/3 = 8$ caras triangulares y, en este caso, habrá $a = v + c - 2 = 6 + 8 - 2 = 12$ aristas, como ya sabemos.

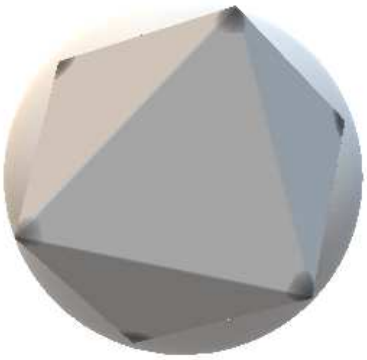

Figura 4.12: Octaedro inscrito en la esfera.

Por tanto, se tiene $\overline{\Gamma}/\overline{\Gamma}[4] \cong PSL_2(\mathbb{Z}_4)$ como grupo de rotaciones del octaedro, isomorfo al grupo de simetrías S_4.

- Para el grupo principal $\Gamma[3] = (2,3,3)$, tenemos nivel $N = 3$, índice $\mu = 12$ en Γ y, por tanto, $t = 12/3 = 4$ cúspides no equivalentes. Si tomamos la región fundamental de semitriángulos proyectada en la esfera, tendría el siguiente aspecto:

Figura 4.13: Región fundamental de $\Gamma[3]$ como descomposición poligonal de la esfera.

Como $N = 3$, sabemos que cada vértice tendrá alrededor 3 caras poligonales (imágenes de triángulos modulares) . El poliedro regular con 4 vértices es el *tetraedro*, con lo que habrá un total de $12/3 = 4$ caras triangulares y, en este caso, un total de $a = v + c - 2 = 4 + 4 - 2 = 6$ aristas, como ya sabemos.

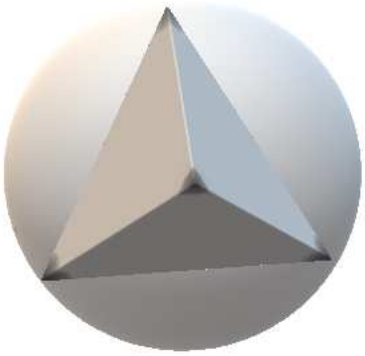

Figura 4.14: Tetraedro inscrito en la esfera.

Por tanto, se tiene $PSL_2(\mathbb{Z}_3)$ como grupo de rotaciones del tetraedro, isomorfo al grupo alternado A_4.

- Para el grupo principal $\Gamma[2] = (2,3,2)$, tenemos nivel $N = 2$, índice $\mu = 6$ en Γ y, por tanto, $t = 6/2 = 3$ cúspides no equivalentes. No existen poliedros regulares con 3 vértices, por lo que en este caso inscribimos un triángulo equilátero con vértices en las imágenes de las cúspides en la esfera.

Figura 4.15: Triángulo equilátero inscrito en la esfera.

Por tanto, se tiene $PSL_2(\mathbb{Z}_2)$ como grupo de simetrías del triángulo, isomorfo al grupo S_3.

Recogemos los ejemplos tratados en la siguiente tabla:

N	**Grupo**	**Descripción**	**Orden**
2	$\cong S_3$	simetrías del triángulo	6
3	$\cong A_4$	grupo tetraédrico	12
4	$\cong S_4$	grupo octaédrico	24
5	$\cong A_5$	grupo icosaédrico	60
7	$PSL_2(\mathbb{Z}_7)$	grupo de Hurwitz	168

Cuadro 4.2: Clasificación de los grupos modulares de nivel N.

Comentamos el caso $N = 7$: $PSL_2(\mathbb{Z}_7)$ tiene orden $\mu = 168$ y $t = 24$ cúspides no equivalentes. Como adelantamos al final del apartado (3.3.3), este grupo resulta ser un *grupo de Hurwitz* con orden $168 = 84(g-1)$, por tanto el género de la superficie de Riemann $\mathscr{R} = \mathscr{U}^*/\Gamma[7]$ debe ser $g = 3$. En términos topológicos, la superficie será homeomorfa a una esfera con 3 asas, a la suma conexa de 3 toros o al llamado *toro triple* (ver [15]), como en la siguiente imagen[6]:

Figura 4.16: Superficie con $g = 3$.

[6]Extraída de Wikipedia, con licencia pública. Disponible en https://en.wikipedia.org/wiki/Torus.

Hemos visto los efectos geométricos que tiene la acción del propio grupo modular y sus subgrupos sobre el semiplano superior hiperbólico y cómo toman forma como superficies de Riemann, lo que ha permitido estudiar ciertos casos importantes que resultan ser grupos de rotaciones de poliedros regulares. Cuando enmarquemos el grupo modular dentro de un tipo mucho más general de grupos, los *grupos de Hecke*, veremos que aparecen efectos geométricos similares.

CAPÍTULO 5

GRUPOS DE HECKE

Durante las secciones anteriores hemos descrito numerosas propiedades relativas al grupo modular, y en especial a cuestiones sobre sus subgrupos normales y las superficies que se generan al actuar sobre el semiplano superior hiperbólico, utilizando para ello de manera reiterada los generadores

$$T(z) = -1/z,\ U(z) = z+1 \text{ y } R(z) = TU(z) = \frac{-1}{z+1}.$$

Así, tanto el par T, U como el par T, R generan el grupo y nos permiten escribir su presentación. Veremos que, si cogemos un generador U más general y se cumplen ciertas relaciones, estaremos hablando de una clase de grupos más general que el grupo modular: los grupos de Hecke. Estos grupos fueron introducidos por E. Hecke en 1938 (en [16]), si bien en la última década del siglo XX y principios del XXI ha cobrado fuerza el estudio de sus propiedades, así como la búsqueda de subgrupos y sus superficies de Riemann asociadas. Entre los matemáticos con publicaciones en este campo, destacan I. Ivrissimtzis, D. Singerman e I. N. Cangül (ver [17], [8] y [7]).

Tras ver la definición de estos grupos, buscaremos el caso concreto en el que el grupo de Hecke es el grupo modular y revisaremos las clases de subgrupos más relevantes. Comprobaremos que varios resultados fundamentales expuestos para el grupo modular se pueden generalizar para ser ciertos en el caso de los grupos de Hecke, y finalmente pondremos el foco en las superficies de Riemann que aparecen como espacios de órbitas por grupos de Hecke, de manera análoga a como se hizo en el capítulo anterior.

5.1. Definición, generadores y presentación

Partimos del grupo de transformaciones $PSL_2(\mathbb{R})$ introducido en (1.2), y recordemos que el grupo modular de transformaciones $PSL_2(\mathbb{Z})$ admitía la presentación

$$PSL_2(\mathbb{Z}) = \left\langle\ T,R\ \middle|\ T^2 = R^3 = I\ \right\rangle = \left\langle\ T,U\ \middle|\ T^2 = (TU)^3 = I\ \right\rangle,$$

y, lógicamente, puede entenderse como el grupo $SL_2(\mathbb{Z})$ identificando cada matriz con su opuesta, esto es,

$$PSL_2(\mathbb{Z}) \cong SL_2(\mathbb{Z})/\langle \pm I\rangle\,.$$

Por este motivo, y como venimos haciendo desde la sección 3.2, utilizaremos simplemente Γ para referirnos al grupo modular con la identificación $A \sim -A$, $\forall A \in \Gamma$.

Comenzamos tomando la familia de generadores $U := U_\lambda(z) = z + \lambda$ con $\lambda \in \mathbb{R}$, de forma que T y U generan un grupo, que será subgrupo de $PSL_2(\mathbb{R})$. Pues bien, E. Hecke demostró en [16] que este grupo es discreto si $\lambda := \lambda_q = 2\cos(\pi/q)$ con $q \geq 3$ entero, o también en el caso $\lambda \geq 2$. Entonces:

Definicion 5.1. Se denomina *grupo de Hecke* al grupo generado por las transformaciones $T := T(z) = -1/z$ y $U := U_\lambda(z) = z + \lambda$, siendo $\lambda := \lambda_q = 2\cos(\pi/q)$ con $q \geq 3$ entero o bien $\lambda \geq 2$.

Para el resto del capítulo nos restringiremos al caso $\lambda := \lambda_q = 2\cos(\pi/q)$ y denotaremos a tal grupo como H_q. En estas condiciones, es evidente que $R = TU$ y por tanto

$$R := R(z) = \frac{-1}{z + \lambda_q},$$

con lo que es fácil comprobar que T es un elemento de orden 2 y R es un elemento de orden q. Así, podemos tomar la *región fundamental* (Hecke, [16])

$$\mathscr{F}_q = \left\{\ z \in \mathscr{U}\ \middle|\ |\mathrm{Re}z| \leq \tfrac{\lambda_q}{2} \text{ y } |z| \geq 1\ \right\} \tag{5.1}$$

y la presentación

$$H_q = \left\langle\ T,R\ \middle|\ T^2 = R^q = I\ \right\rangle = \left\langle\ T,U\ \middle|\ T^2 = (TU)^q = I\ \right\rangle, \tag{5.2}$$

por lo que igual que $PSL_2(\mathbb{Z}) \cong C_2 * C_3$, se tiene que

$$H_q \cong C_2 * C_q,$$

y comenzamos a intuir que se trata de una generalización respecto al caso del grupo modular, que concretamos a continuación.

5.2. Algunos grupos de Hecke

Demos valores a $q \geq 3$ para intentar describir el grupo de Hecke H_q resultante:

1. Si $q = 3$, $\lambda_3 = 1$ y por tanto estamos hablando del grupo modular, esto es,
$$H_3 = PSL_2(\mathbb{Z}).$$
2. Si $q = 4$, $\lambda_4 = \sqrt{2}$ y veremos que las matrices del grupo H_4 tienen una estructura conocida.
3. Si $q = 5$, aparece el *número áureo* $\lambda_5 = \phi = \frac{1+\sqrt{5}}{2}$, cuyas propiedades permiten caracterizar al grupo H_5.
4. Si $q = 6$, $\lambda_6 = \sqrt{3}$ y la caracterización del grupo H_6 es similar a la de H_4.
5. Si $q > 6$, describir los elementos de H_q es complicado y de hecho sólo se conocen algunas propiedades.

En el caso de los grupos H_4 y H_6, sus elementos son bien conocidos:

Proposicion 5.1. *El grupo de Hecke H_4 es un subgrupo de $PSL_2(\mathbb{Z}[\sqrt{2}])$ y sus matrices son de la forma*

$$A = \begin{pmatrix} a & b\sqrt{2} \\ c\sqrt{2} & d \end{pmatrix},\ a,b,c,d \in \mathbb{Z}\ y\ \det A = ad - 2bc = 1 \tag{5.3}$$

o de la forma

$$A = \begin{pmatrix} a\sqrt{2} & b \\ c & d\sqrt{2} \end{pmatrix},\ a,b,c,d \in \mathbb{Z}\ y\ \det A = 2ad - bc = 1. \tag{5.4}$$

Análogamente, las matrices del grupo H_6, que es subgrupo de $PSL_2(\mathbb{Z}[\sqrt{3}])$, tienen la forma

$$A = \begin{pmatrix} a & b\sqrt{3} \\ c\sqrt{3} & d \end{pmatrix},\ a,b,c,d \in \mathbb{Z}\ y\ \det A = ad - 3bc = 1 \tag{5.5}$$

o de la forma

$$A = \begin{pmatrix} a\sqrt{3} & b \\ c & d\sqrt{3} \end{pmatrix},\ a,b,c,d \in \mathbb{Z}\ y\ \det A = 3ad - bc = 1. \tag{5.6}$$

Sin embargo, cuando $q = 5$, $\lambda_5 = \phi$ no es tan inmediato conocer si una matriz (de $PSL_2(\mathbb{Z}[\phi])$) pertenece o no a H_5, aunque existe un método basado en fracciones continuas dado por Rosen en [41]. Ahora bien, igual que para el grupo modular H_3 se tiene que $\mathbb{Q} \cup \{\infty\}$ es el conjunto de *cúspides*, cabe plantear cuál será el conjunto de cúspides para los casos $q \in \{4,5,6\}$. Pues bien, dada la estructura de sus matrices, podemos afirmar:

Proposicion 5.2. *El conjunto de cúspides del grupo H_4 (respectivamente H_6) es un subconjunto de $\mathbb{Q}\left[\sqrt{2}\right] \cup \{\infty\}$ (respectivamente $\mathbb{Q}\left[\sqrt{3}\right] \cup \{\infty\}$), siendo dichas cúspides de la forma $p = a\sqrt{m}/c$, donde $m = 2$ (respectivamente $m = 3$). Las cúspides de H_5 son de la forma*

$$\frac{a\phi + b}{c\phi + d}.$$

Demostración. Es inmediato comprobar que $p = a\sqrt{m}/c$ es una cúspide del grupo de Hecke correspondiente, sin más que observar que si A es de la forma expuesta en la proposición (5.1), se tiene que

$$A(\infty) = a\sqrt{m}/c \in \mathbb{Q}\left[\sqrt{m}\right],$$

con lo que el conjunto de cúspides es un subconjunto de $\mathbb{Q}\left[\sqrt{m}\right]$. Para el grupo H_5, dada la propiedad $\phi^2 = \phi + 1$ del número áureo, cualquier potencia de ϕ se podrá expresar como $a\phi + b \in \mathbb{Z}\left[\phi\right]$. Cuando $q > 6$, no existe un método general para encontrar el conjunto de cúspides de los grupos de Hecke. □

Grupos triangulares como grupos de Hecke.

Recordemos la *signatura* de la forma $(0; l, m, n)$ para grupos triangulares vistos en secciones anteriores, donde l, m y n son los órdenes (o períodos) de los generadores T, R (ambos elípticos) y U (entendido como elíptico de orden infinito) respectivamente. Para el grupo modular podemos escribir $PSL_2(\mathbb{Z}) = (0; 2, 3, \infty)$ dado que U tiene orden infinito, por lo que por extensión $H_4 = (0; 2, 4, \infty)$ y $H_6 = (0; 2, 6, \infty)$, siendo en general

$$H_q = (0; 2, q, \infty). \tag{5.7}$$

Veremos que la signatura será realmente útil para el estudio de los subgrupos más importantes y sus propiedades.

Observación.

Hay que tener cuidado para no confundir los conceptos de *signatura* y *esquema de ramificación*: la signatura $(g; l, m, n)$ hace referencia al género y a los órdenes de los generadores del grupo, mientras que el esquema (n_i, n_ρ, n_∞) hace referencia a subgrupos $\Omega \lhd \Gamma$ de nivel n_∞ y que tienen $2n_i$, $2n_\rho$ y $2n_\infty$ semitriángulos apoyados en cada punto equivalente a i, ρ e ∞, respectivamente.

El subgrupo par.

Pongamos por un momento el foco en H_q con $q \in \{4, 6\}$. Las matrices del tipo

$$A = \begin{pmatrix} a & b\sqrt{m} \\ c\sqrt{m} & d \end{pmatrix}, \; m = q/2$$

se denominan *pares*, mientras que las del tipo

$$A = \begin{pmatrix} a\sqrt{m} & b \\ c & d\sqrt{m} \end{pmatrix}$$

se llaman *impares*. Las matrices pares forman un subgrupo de índice 2 en H_q, denominado *subgrupo par* y denotado como H_q^{par}. Se puede demostrar (Singerman, [43]) que

$$H_q^{par} \cong \mathbb{Z} * C_{q/2}, \tag{5.8}$$

donde $C_{q/2}$ es el grupo cíclico de $q/2$ elementos.

5.3. Subgrupos de grupos de Hecke

En esta sección, vamos a extender las nociones sobre los subgrupos fundamentales del grupo modular para explorar los equivalentes de grupos de Hecke. Así, revisaremos los subgrupos principales de congruencia y comprobaremos cuándo estos coinciden con el núcleo de la reducción módulo N, retomaremos la definición y propiedades del subgrupo conmutador de un grupo de Hecke para observar propiedades que generalizan las vistas para $PSL_2(\mathbb{Z})$, y finalmente abordaremos (de nuevo) la cuestión de contar subgrupos de un índice dado.

5.3.1. Subgrupos principales de congruencia

Partiendo del grupo modular $H_3 = PSL_2(\mathbb{Z})$, podemos redefinir el subgrupo principal de congruencia $\Gamma[N]$ como

$$\Gamma[N] = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H_3 \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\},$$

Este subgrupo es normal en $PSL_2(\mathbb{Z})$ y contiene el elemento U^N. Además, obteníamos los subgrupos principales de congruencia a partir de la aplicación reducción módulo N

$$\lambda_N : PSL_2(\mathbb{Z}) \longrightarrow PSL_2(\mathbb{Z}_N),$$

ya que $\ker(\lambda_N) = \Gamma[N]$. Extendamos esta noción a los grupos de Hecke:

Definicion 5.2. Se define el *subgrupo principal de congruencia* de nivel N del grupo de Hecke H_q como

$$H_q(N) = \left\{ A \in H_q \;\middle|\; A \equiv \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}. \tag{5.9}$$

Se puede entender la reducción módulo N de elementos de la forma $\sqrt{m} \notin \mathbb{Z}$ a partir del siguiente ejemplo: como $9 \equiv 2 \mod 7$ entonces podemos considerar que $3 \equiv \sqrt{2} \mod 7$.

En el contexto de $q > 3$, no siempre ocurre $\ker(\lambda_N) = H_q(N)$ para la reducción

$$\lambda_N : H_q \longrightarrow H_q(\mathbb{Z}_N),$$

como sí ocurría para el grupo modular H_3. Para estudiar las diferentes posibilidades respecto al núcleo de esta aplicación, denotémoslo como $K_q(N)$. En general, se tiene que

$$H_q(N) \lhd K_q(N),$$

y la pregunta es ¿en qué casos $K_q(N) = H_q(N)$? Desde luego no ocurre para, por ejemplo, $q = 4$ y $N = 7$, considerando el homomorfismo

$$\lambda : H_4 \longrightarrow PSL_2(\mathbb{Z}_7)$$

tal que

$$\lambda\left(\begin{pmatrix} a\sqrt{2} & b \\ c & d\sqrt{2} \end{pmatrix}\right) = \begin{pmatrix} 3a & b \\ c & 3d \end{pmatrix},\ \lambda\left(\begin{pmatrix} a & b\sqrt{2} \\ c\sqrt{2} & d \end{pmatrix}\right) = \begin{pmatrix} a & 3b \\ 3c & d \end{pmatrix},$$

que induce el isomorfismo $H_4/K_4(7) \cong PSL_2(\mathbb{Z}_7)$ (Macbeath, [27]) y observando que, por ejemplo,

$$A = \begin{pmatrix} 5\sqrt{2} & 7 \\ 7 & 5\sqrt{2} \end{pmatrix} \in (K_4(7) - H_4(7))$$

con lo que $H_4(7) \neq K_4(7)$. Para más detalles, consultar la página 150 de [8], donde además se expone una descripción de los grupos isomorfos a $H_q/K_q(N)$ y a $H_q/H_q(N)$ para distintos valores de q y N.

5.3.2. Subgrupos potencia y conmutador

Continuando con la generalización de los subgrupos más relevantes de los grupos de Hecke, recordemos que el *subgrupo conmutador* del grupo modular se define como

$$\Gamma' = \left\langle\ [a,b] \ \middle|\ a,b \in \Gamma\ \right\rangle,$$

como siempre con la identificación de cada elemento con su opuesto. La *abelianización* del grupo modular es, entonces

$$\Gamma/\Gamma' = \left\langle\ T,R \ \middle|\ T^2 = R^3 = I, TR = RT\ \right\rangle.$$

Es fácil ver que esta abelianización es isomorfa a $C_2 \times C_3$, y por tanto el orden del grupo es $2 \cdot 3 = 6$. Vimos que el subgrupo conmutador tiene como conjunto generador mínimo $\langle a = TRTR^2, b = TR^2TR\rangle$, siendo así de rango 2. Generalizando al caso de un grupo de Hecke, tenemos la siguiente proposición (basada en [7]) que caracteriza al conmutador H_q' del grupo de Hecke H_q:

Proposicion 5.3. *Todo elemento $A = [a,b] \in H_q'$ es par, así $H_q' \subset H_q^{par}$ y se tiene la abelianización*

$$H_q/H_q' = \left\langle\ T,R \ \middle|\ T^2 = R^q = I, TR = RT\ \right\rangle \cong C_2 \times C_q. \tag{5.10}$$

Como consecuencia, el subgrupo conmutador H_q' es de rango $q-1$ y la abelianización H_q/H_q' tiene orden $2q$.

Como ejemplo, observar que cuando $q = 3$ (grupo modular) H_3' tiene rango 2 y $\left|H_3/H_3'\right| = 6$ (visto), mientras que si $q = 4$ entonces H_4' tiene rango 3 y $\left|H_4/H_4'\right| = 8$ y si $q = 6$ entonces H_6' tiene rango 5 y $\left|H_6/H_6'\right| = 12$.

Relación con los subgrupos potencia.
Cuando estudiamos los subgrupos de un grupo de Hecke, nos encontramos con que estos pueden o no contener elementos de orden finito, que en este caso serían elementos elípticos. Este hecho motiva la siguiente definición:

Definicion 5.3. (Grupos de torsión) Se dice que un grupo G es un *grupo de torsión* si todos sus elementos tienen orden o periodo finito. Si el grupo no contiene elementos de orden finito, se denomina grupo *libre de torsión*.

Pues bien, recordemos que para el grupo modular ($q = 3$), los únicos subgrupos normales de índice $\mu \in \{1,2,3\}$ son los de la forma Γ^{μ}. Generalicemos a cualquier grupo de Hecke H_p con p primo:

Proposicion 5.4. *Los únicos subgrupos normales de torsión con índice $\mu \in \{1,2,p\}$ de H_p, siendo p primo, son los subgrupos de la forma H_p^{μ}.*

Demostración. Sea un subgrupo normal $\Omega \lhd H_q$. Al ser Ω de torsión, contiene o bien a R, o bien a T o bien a los dos generadores. Si contiene a los dos, evidentemente se trata del propio H_p; si contiene al generador T pero no a R entonces $H_p/\Omega \cong C_p$ (generado por los conjugados de T), por lo que como R tiene orden p debe tratarse del subgrupo H_p^p. Si contiene a R pero no a T, entonces $H_p/\Omega \cong C_2$ (generado por los conjugados de R), por lo que como T tiene orden 2 debe tratarse del subgrupo H_p^2. □

Para finalizar, cabría esperar que la relación entre los subgrupos potencia y conmutador para el grupo modular dada en el teorema (3.15), y que puede reformularse como

$$H_3' \cong H_3^2 \cap H_3^3,$$

pudiera generalizarse a cualquier H_p con p primo. Así es:

Teorema 5.1.

$$H_p' \cong H_p^2 \cap H_p^p. \tag{5.11}$$

La demostración es la misma que para el caso $q = 3$.

¿Cuántos subgrupos hay?
Para responder a esta pregunta cuando se trata de grupos de Hecke, vamos a introducir algunas nociones sobre la *teoría de mapas regulares* y su correspondencia uno a uno con los subgrupos normales, cuestión que abordaremos en la próxima sección, por su conexión con las superficies de Riemann. Veremos que es similar a los resultados relativos al concepto de *descomposición poligonal* de una superficie.

5.3.3. Signatura de los subgrupos

En la ardua búsqueda de subgrupos normales de un grupo de Hecke H_q interviene de forma práctica, como hemos ido viendo, la signatura $(2,q,\infty)$ del grupo triangular, donde hemos omitido el género. De cara a la próxima sección, en la que se buscarán subgrupos normales y se dará la superficie de Riemann relacionada, vamos a generalizar el concepto de signatura de un grupo triangular y a detallar tanto la presentación como la signatura de cualquier subgrupo de un grupo de Hecke H_q.

Proposicion 5.5. *El grupo con signatura $(g;m_1,\cdots,m_k)$, donde g es el género, $m_1,\cdots,m_r$ son los órdenes (finitos) de los generadores elípticos, y $m_{r+1},\cdots,m_k=\infty$ corresponden a los órdenes infinitos de los generadores parabólicos, se corresponde con el grupo cuya presentación es*

$$\left\langle\ x_1,\cdots,x_k,a_1,b_1,\cdots,a_g,b_g\ \middle|\ x_1^{m_1}=\cdots=x_r^{m_r}=1, x_1\cdots x_k\textstyle\prod_{i=1}^{g}[a_i,b_i]=1\ \right\rangle, \tag{5.12}$$

siendo los x_i los distintos generadores.

En el caso de que el género sea 0, podemos concretar una presentación más simple:

$$\left\langle\ x_1,\cdots,x_k\ \middle|\ x_1^{m_1}=\cdots=x_r^{m_r}=x_1\cdots x_k=1\ \right\rangle, \tag{5.13}$$

de modo que evidentemente H_q tiene signatura $(0;2,q,\infty)$. Cuando el orden de un generador es 1 se suele omitir, y además suele añadirse a cada orden el número de veces que se repite, esto es, el número de clases no H_q-equivalentes[1]. Así, la signatura de cualquier subgrupo de un grupo de Hecke viene dada en el siguiente

Teorema 5.2. *La signatura de un subgrupo Ω de $H_q=(0;2,q,\infty)$ es*

$$\left(g;2^{(s_0)},q_1^{(s_1)},\cdots,q_k^{(s_k)},\infty^{(t)}\right), \tag{5.14}$$

donde los (s_i) muestran el número de elementos no H_q-equivalentes de cada orden. Si el subgrupo es normal en H_q entonces tanto los q_i como t dividen al índice μ.

Demostración. Consecuencia de [7], p.60, Lema 1.2. □

Para calcular el género del subrupo (que luego da información sobre el *número de agujeros* de la superficie de Riemann asociada), tomamos la función holomorfa

$$f:\mathscr{U}^*/\Omega\longrightarrow\mathscr{U}^*/H_q$$

entre superficies de Riemann y concretamos la fórmula de Riemann-Hurwitz dada en (1.1) como sigue:

$$2g-2+\frac{s_0}{2}+\sum_{i=1}^{k}\left(1-\frac{1}{q_i}\right)+t=\mu\left(\frac{1}{2}-\frac{1}{q}\right), \tag{5.15}$$

[1] En nuestra notación, σ_z representa el número de clases no equivalentes con punto fijo z, siendo habitual utilizar $\sigma_\infty=t$ como número de clases parabólicas (igual al número de cúspides).

donde μ es el índice del subgrupo en H_q. Así, para subgrupos libres de torsión la fórmula del género queda simplificada:

$$2g-2+t=\mu\left(\frac{1}{2}-\frac{1}{q}\right). \tag{5.16}$$

En la siguiente sección introduciremos el concepto de *mapa regular*, veremos que existe una correspondencia entre subgrupos normales y mapas regulares y utilizaremos la signatura de los subgrupos reiteradamente para estudiar los subgrupos normales y la superficie de Riemann asociada como espacio de órbitas en $\mathscr{U}^*$.

5.4. Mapas regulares y superficies de Riemann

En el apartado (4.2.2) detallamos la obtención de una superficie de Riemann como espacio de órbitas del semiplano superior por la acción del grupo modular o un subgrupo normal del mismo, utilizando el concepto de descomposición poligonal de una superficie para hablar de los términos vértice, arista y cara. Generalizando esta teoría, se puede establecer un puente entre la teoría de grafos y el estudio de las superficies, de forma que si se tiene un grafo embebido en una superficie entonces bajo ciertas condiciones, podemos relacionar ambos campos de conceptos para obtener resultados. Así, vamos a definir el concepto de *mapa regular*, para ver la conexión con los subgrupos normales de los grupos de Hecke y, además, poder hablar de grupos de automorfismos de superficies de Riemann, como ya hicimos para el grupo modular. Así pues, veamos la primera definición:

Definicion 5.4. (Mapa) Se denomina *mapa* a un grafo G dirigido[2] embebido[3] en la superficie (orientable) S, de forma que las componentes conexas de $S-G$ son simplemente conexas.

Al embeber el grafo G en la superficie S aparecen los vértices y las aristas de G, y además una serie de caras, correspondientes a las componentes conexas de $S-G$. Así, el mapa tendrá V vértices, A aristas y C caras. Normalmente una arista conecta dos vértices, pero puede existir (lo veremos más adelante) un arista conectada a un único vértice, recibiendo así el nombre de *arista libre*.

Definicion 5.5. (Valencia) Se denomina *valencia de una cara* al número de lados (aristas) que la rodean, mientras que la *valencia de un vértice* es el número de aristas que inciden en él. Si m y n son, respectivamente, el mínimo común múltiplo de las valencias de las caras y de los vértices, podemos hablar de un *mapa de tipo* $\{m,n\}$[4].

[2] Sus aristas están orientadas: o bien inciden en un vértice o bien salen de él.

[3] Fijados los vértices sobre la superficie, se conectan por medio de aristas de forma que se conserve la estructura y las propiedades del grafo original.

[4] Se denomina *mapa dual* del mapa $M=\{m,n\}$ al mapa $M^*=\{n,m\}$. Por ejemplo, el cubo y el octaedro son duales entre sí.

Definicion 5.6. (Automorfismos y regularidad) Un *automorfismo* en un mapa M es un homeomorfismo de la superficie S que preserva la orientación de las aristas del mapa. El conjunto de todos los automorfismos de M se denomina *grupo de automorfismos* y se denota como $\mathrm{Aut}(M)$. Un mapa es *regular* si todas sus caras y vértices tienen la misma valencia.

Teorema 5.3. *Un mapa M es regular si y sólo si el grupo $Aut(M)$ actúa transitivamente en S*[5].

En [18], Jones y Singerman demuestran que existe una correspondencia uno a uno entre los mapas regulares $\{m,n\}$ y los subgrupos normales de los grupos triangulares $G_{2,m,n} = (0;2,m,n)$. Precisamente esta relación será la que nos permita estudiar las características de los subgrupos normales de los grupos de Hecke H_q. Así, para cada m divisor de q existe un homomorfismo

$$\Theta : H_q = (0;2,q,\infty) \longrightarrow (0;2,m,n), \tag{5.17}$$

que manda los generadores de H_q en los de $(0;2,m,n)$, y de igual forma para cada mapa regular $\{m,n\}$ existe un subgrupo normal $\Omega \lhd (0;2,m,n)$, de manera que $\Theta^{-1}(\Omega)$ es el subgrupo normal de H_q asociado al mapa regular $\{m,n\}$, y con nivel n (en concordancia con lo visto hasta ahora). Si M es tal que todas sus caras tienen valencia $m|q$, entonces existe un único subgrupo normal $\Omega_M \lhd H_q$ asociado a este mapa. Además, el subgrupo puede contener alguno de los generadores T o R de H_q o a ninguno, hecho que condiciona las características del mapa regular. Veamos una importante reflexión acerca de la relación entre los generadores T y R y las características de los mapas:

Proposicion 5.6. *Si un subgrupo $\Omega \subset H_q$ tiene torsión, necesariamente contiene conjugados de T o bien de alguna potencia de R. Cada conjugado de T corresponde con una arista libre*[6]*, y si un conjugado de R tiene exponente m módulo Ω*[7] *entonces el mapa tiene una cara con valencia m. Recíprocamente, cada arista libre del mapa M corresponde con un conjugado de T en Ω y cada cara con valencia m a un conjugado de R^m en Ω. Por tanto, los mapas $q-gonales$*[8] *se corresponden con los subgrupos libres de torsión de H_q.*

La última afirmación se basa en que los grupos libres de torsión no contienen conjugados de T y contendrían conjugados de $R^q = I$, luego finalmente no contienen elementos de orden finito. De esta forma, si el subgrupo es normal en H_q, el mapa regular asociado o bien no tiene aristas libres o, excepcionalmente, tiene todas sus aristas libres. Para este último caso, tenemos la siguiente definición:

Definicion 5.7. Se denomina *mapa estrellado* de r aristas, y se denota como $\mathscr{S}_r$, al mapa consistente en un único vértice del que emanan r aristas libres. El mapa consiste en una cara r-gonal y un vértice de valencia r.

[5] Se dice que un grupo G actúa *transitivamente* en X si para cualquier par de elementos $x, y \in X$ distintos existe $g \in G$ tal que $x = g(y)$.

[6] Arista conectada a un único vértice.

[7] Es decir, $(R')^m = \left(ARA^{-1}\right)^m$ pertenece al subgrupo Ω.

[8] Mapa consistente en una cara de valencia q, y sin aristas libres.

Así, el subgrupo asociado al mapa estrellado $\mathscr{S}_r$ puede verse como el núcleo del homomorfismo de H_q al grupo cíclico C_r dado por $T \mapsto I$, $R \mapsto a$ siendo a el generador de C_r.

Si el mapa no tiene aristas libres, Ω_M no contiene conjugados de T y en [18] se demuestra el siguiente

Teorema 5.4. *Sea M un mapa regular de género g, sin aristas libres, con C caras de valencia m donde $m|q$, A aristas y V vértices. Entonces el subgrupo normal Ω_M asociado tiene índice $\mu = 2A$ en H_q, $t = V$ clases parabólicas (cúspides) y C clases de elementos elípticos de orden q/m. Por tanto, se tiene la signatura*

$$\Omega_M := (g; (q/m)^{(C)}, \infty^{(V)}). \tag{5.18}$$

Recíprocamente, para un subgrupo normal que no contiene conjugados de T existe un mapa regular M asociado sin aristas libres.

En la sección (3.3.4) nos sumergimos en la búsqueda de una fórmula que proporcione el número de subgrupos normales del grupo modular H_3 dado el índice μ. Para abordar una pregunta semejante sobre cualquier H_q, dividiremos el estudio en los casos de género 0 y de género 1. Esta búsqueda equivale a encontrar mapas regulares en la esfera y en el toro, respectivamente.

5.4.1. Mapas regulares en la esfera

Estudiemos los subgrupos normales de género 0 de H_q, o lo que es lo mismo, los mapas de tipo $\{m,n\}$ en la esfera. Vamos a observar que se generaliza el comportamiento detallado para el grupo modular H_3, esto es, si Ω es normal en H_q entonces H_q/Ω es el grupo de automorfismos de alguna superficie de Riemann $\mathscr{U}^*/\Omega$. Atendiendo al número de elementos de los grupos de automorfismos resultantes, podemos hablar de los grupos alternados A_4, A_5, el grupo simétrico S_4, el grupo cíclico C_n o el dihédrico D_n. Comencemos con un teorema que caracteriza a los subgrupos normales asociados a mapas estrellados:

Teorema 5.5. *Sea $\mathscr{S}_r$ el mapa estrellado de r aristas libres, con $r|q$. Entonces, el subgrupo asociado $\Omega_{\mathscr{S}_r}$ es normal con índice $\mu = r$ en H_q, tendrá r elementos elípticos de orden 2, un elemento elíptico de orden q/r y una clase parabólica. Así, tendrá signatura*

$$\Omega_{\mathscr{S}_r} := (0; 2^{(r)}, q/r, \infty). \tag{5.19}$$

Los mapas estrellados suponen un ejemplo de sólido platónico degenerado, pero existen otras posibilidades que recogemos en la siguiente tabla, en la que para cada mapa se detalla el tipo, el número de vértices, aristas y caras y el grupo de automorfismos H_q/Ω_M correspondiente:

Al contar el número de subgrupos normales con $g = 0$, hay distinguir si q es par o impar:

Proposicion 5.7. *El número de subgrupos normales con género 0 de H_q, que denotamos como N_q^0, es infinito si q es par, mientras que si q es impar la cantidad es finita y se calcula como sigue:*

Mapa regular	Tipo	V	A	C	Aut(M)
Mapa estrellado $\mathscr{S}_r$	-	1	r	1	Cíclico C_r
Polígono regular $\mathscr{P}_r$ y dual $\mathscr{P}_r^*$	$\{r,2\}$, $\{2,r\}$	r, 2	r, r	2, r	Dihédrico D_r
Tetraedro $\mathscr{T}$	$\{3,3\}$	4	6	4	Alternado A_4
Octaedro $\mathscr{O}$ y cubo $\mathscr{C}$	$\{3,4\}$, $\{4,3\}$	6, 8	12, 12	8, 6	Simétrico S_4
Icosaedro $\mathscr{I}$ y dodecaedro $\mathscr{D}$	$\{3,5\}$. $\{5,3\}$	12, 20	30, 30	20, 12	Alternado A_5

Cuadro 5.1: Tabla de sólidos platónicos, incluyendo degenerados.

- $N_q^0 = 2d(q)$, *si* $(q,15) = 1$,
- $N_q^0 = 2d(q)+3$, *si* $(q,15) = 3$,
- $N_q^0 = 2d(q)+1$, *si* $(q,15) = 5$,
- $N_q^0 = 2d(q)+4$, *si* $(q,15) = 15$,

siendo $d(q)$ *el número de divisores positivos de* q.

Utilizando el teorema (5.4) podemos calcular fácilmente la signatura de cada subgrupo normal Ω_M, ya que conocemos el número de vértices, aristas y caras de cada mapa regular M asociado. Por ejemplo, en H_4 es evidente que el subgrupo normal asociado al cubo $\{4,3\}$ tiene signatura $(0;\infty^{(8)})$, puesto que no puede tener elemenos elípticos (ya que serían de orden $q/m = 4/4 = 1$) y tiene $V = 8$ cúspides o clases parabólicas. En síntesis, recogemos en la siguiente tabla una clasificación de los subgrupos normales libres de torsión para distintos valores de q:

Grupo de Hecke	Subgrupo normal	Índice	Signatura
H_3	$\Omega_{\mathscr{T}}$, $\Omega_{\mathscr{O}}$, $\Omega_{\mathscr{I}}$	12, 24, 60	$(0;\infty^{(4)})$, $(0;\infty^{(6)})$, $(0;\infty^{(12)})$
H_4	$\Omega_{\mathscr{C}}$	24	$(0;\infty^{(8)})$
H_5	$\Omega_{\mathscr{D}}$	60	$(0;\infty^{(20)})$
H_q, $(q \geq 3)$	$\Omega_{\mathscr{P}_r}$	$2q$	$(0;\infty^{(q)})$

Cuadro 5.2: Subgrupos normales con género 0 libres de torsión, para distintos grupos de Hecke.

5.4.2. Mapas regulares en el toro

Intentemos contar el número de subgrupos normales de género 1 en H_q, o lo que es lo mismo, los mapas de tipo $\{m,n\}$ en el toro. Ya ha sido estudiado (A. Altshuler, [1]) que estos mapas deben ser de los tipos $\{3,6\}$[9], $\{6,3\}$ (como dual del tipo $\{3,6\}$) y $\{4,4\}$.

[9]Hemos visto el subgrupo principal de nivel 6 y su relación con el grupo triangular $G_6 = (2,3,6)$. La superficie de Riemann $\mathscr{U}/\Gamma[6]$ es, como ya expusimos, homeomorfa al toro complejo.

Subgrupos normales en H_4.
Para el grupo $H_4 = (2,4,\infty)$, los mapas de tipo $\{3,6\}$ y $\{6,3\}$ no pueden corresponder con subgrupos normales porque ni $m = 3$ ni $m = 6$ son divisores de $q = 4$, luego únicamente quedan los mapas de tipo $\{4,4\}$, que por consiguiente deben estar asociados con subgrupos normales del grupo triangular $(2,4,4)$. Los mapas del tipo $\{4,4\}$ se suelen denotar como $\{4,4\}_{r,s}$ $(r,s \in \mathbb{Z})$, y en [18] se demuestra que tienen r^2+s^2 vértices, r^2+s^2 caras y $2(r^2+s^2)$ aristas. El grupo de automorfismos correspondiente tiene orden $|\mathrm{Aut}(M)| = 4(r^2+s^2)$ (igual al índice μ del subgrupo Ω_M en H_4). Un ejemplo de visualización de un mapa de este tipo sobre el toro es la siguiente[10]

Figura 5.1: Mapa regular de tipo $\{4,4\}$ en el toro.

aunque es recomendable consultar [46], donde J.J. van Wijk expone representaciones no sólo de mapas regulares en el toro sino en cualquier superficie orientable de género g. Volviendo a nuestra senda, estamos buscando subgrupos normales con nivel $n = 4$, por lo que según vimos en (3.58), el índice viene dado por

$$\mu = nt = 4t = 4(r^2+s^2),$$

con lo que habrá $t = r^2+s^2$ cúspides o clases parabólicas. Buscando el número de pares $(r,s) \in \mathbb{Z}^2$ no equivalentes tales que $\mu/4 = t = r^2+s^2$, llegamos a la siguiente

Proposicion 5.8. *El número de subgrupos normales de género* 1 *con índice* μ *del grupo de Hecke* H_4 *se denota* $N_4^1(\mu)$ *y se calcula como sigue:*

$$N_4^1(\mu) = \frac{1}{4}\left|\left\{ (r,s) \in \mathbb{Z}^2 \;\middle|\; r^2+s^2 = t = \tfrac{\mu}{4} \right\}\right|. \tag{5.20}$$

Subgrupos normales en H_6.
Por razonamientos análogos a los expuestos para el caso $q = 4$ y por los resultados en [18], existe una correspondencia uno a uno entre los subgrupos normales libres de torsión de H_6 y los mapas regulares de tipo $\{6,3\}_{r,s}$, que tienen $V = 2(r^2+s^2-rs)$ vértices, $C = (r^2+s^2-rs)$ caras y $A = 3(r^2+s^2-rs)$ aristas. El número de clases parabólicas es $t = r^2+s^2-rs$ y, por el teorema (5.4) estos subgrupos no tienen elementos elípticos (puesto que tendrían orden $q/m = 6/6 = 1$),

[10] Imagen extraída de Wikipedia bajo licencia pública y disponible en https://upload.wikimedia.org/wikipedia/commons/6/60/Torus_from_rectangle.gif

siendo por tanto subgrupos normales libres de torsión con índice $\mu = 2A = 6t$ en H_6. En el caso dual, los mapas regulares de tipo $\{3,6\}_{r,s}$, que tienen $V = (r^2+s^2-rs)$ vértices, $C = 2(r^2+s^2-rs)$ caras y $A = 3(r^2+s^2-rs)$ aristas, tienen de nuevo por el teorema (5.4) $C = 2t$ elementos elípticos de orden $q/m = 6/3 = 2$. Obsérvese que, además, los mapas regulares de tipo $\{3,6\}_{r,s}$ corresponden a subgrupos normales del grupo $(0;2,3,6)$. En conclusión, el número de subgrupos normales con género 1 de H_6 responde a la siguiente

Proposicion 5.9. *El número de subgrupos normales de género* 1 *con índice* μ *del grupo de Hecke* H_6 *se denota* $N_6^1(\mu)$ *y se calcula como sigue:*

$$N_6^1(\mu) = \frac{1}{6}\left|\left\{ \ (r,s) \in \mathbb{Z}^2 \ \middle| \ r^2+s^2-st = t = \tfrac{\mu}{6} \ \right\}\right|. \tag{5.21}$$

Subgrupos normales en H_q.
Un resultado más general viene dado en el siguiente teorema, cuya demostración se sigue inmediatamente del teorema (5.4) y de la proposición (5.6):

Teorema 5.6. *El número de subgrupos normales de género* 1 *de un grupo de Hecke* H_q *cumple los siguientes enunciados:*

- *El grupo* H_q *tiene infinitos subgrupos normales de género* 1 *si y sólo si* $(q,12) \geq 3$.
- *El grupo* H_q *no tiene subgrupos normales de género* 1 *si y sólo si* $(q,12) < 3$.
- *El grupo* H_q *tiene infinitos subgrupos normales de género* 1 *libres de torsión si y sólo si* $q \in \{3,4,6\}$.

Tras un largo recorrido teórico, hemos generalizado el grupo modular al marco de los grupos de Hecke para comprobar que lo estudiado para el grupo modular consiste en casos particulares de una teoría mucho más general. Buena muestra de ello es la teoría de mapas regulares, que se concreta en las descomposiciones poligonales vistas, así como el concepto de signatura de un grupo, que etiqueta de forma rápida a cada subgrupo y es verdaderamente útil para establecer relaciones y encontrar propiedades y resultados.

CONCLUSIONES

Tras un extenso estudio, las conclusiones principales que extraemos son:

1. El grupo modular puede ser entendido como grupo de matrices o como grupo de transformaciones. En cualquiera de los casos, el efecto geométrico de sus transformaciones sobre la región fundamental genera una teselación del semiplano superior.

2. La determinación de fórmulas para el cálculo del índice de un subgrupo requiere, dada la naturaleza de los coeficientes de los elementos del grupo modular, de resultados de teoría de números. El índice de un subgrupo de $SL_2(\mathbb{Z})$ puede ser igual o no que el índice del subgrupo asociado $PSL_2(\mathbb{Z})$, dependiendo de si el elemento $-I$ pertenece o no al subgrupo. En este trabajo se exponen fórmulas para el cálculo de distintos índices para subgrupos relevantes.

3. De entre los subgrupos del grupo modular, destacan los subgrupos normales y los subgrupos de congruencia. Se ha demostrado que no todos los subgrupos normales son de congruencia, y que no existe una fórmula para contar el número de subgrupos normales de un índice concreto.

4. La región fundamental de los subgrupos principales de congruencia muestra gráficamente el número de cúspides no equivalentes, y permite obtener el subgrupo en cuestión como grupo generado por las transformaciones de borde de su región.

5. Los espacios de órbitas de estos subgrupos en el semiplano superior son superficies de Riemann. Cuando la superficie es la esfera de Riemann, los grupos modulares de nivel N son isomorfos a los grupos de simetrías de los sólidos platónicos. Existe una estrecha relación, dependiendo de N, entre los grupos modulares de nivel N y los grupos triangulares.

6. El grupo modular es un grupo de Hecke.

7. La teoría de mapas regulares sirve como enfoque para estudiar los subgrupos normales de un grupo de Hecke, dado que existe una correspondencia biyectiva entre mapas regulares y subgrupos normales. Trabajar con la signatura de los subgrupos facilita esta tarea.

8. Los espacios de órbitas por grupos de Hecke en el semiplano superior son superficies de Riemann. Hemos estudiado los mapas regulares correspondientes a distintos grupos de simetrías en la esfera, así como los mapas regulares en el toro.

Como trabajos futuros, se propone continuar el estudio de las regiones fundamentales de los subgrupos de congruencia profundizando en el método del *símbolo de Farey*, así como el análisis de la superficie de Riemann asociada. En el campo más general de los grupos de Hecke, se pueden explorar otros grupos de Hecke aparte de los casos vistos, así como continuar la búsqueda de subgrupos normales mediante mapas regulares en superficies de género mayor que la unidad.

BIBLIOGRAFÍA

[1] A. ALTSHULER, *Construction and enumeration of regular maps on the torus*, Discrete Mathematics, 4 (1973), pp. 201–217.

[2] F. BAUMSLAG AND XU, *A proposed public key cryptosystem using the modular group*, Combinatorial group theory, discrete groups, and number theory, (2006), pp. 35–43.

[3] A. F. BEARDON, *A primer on Riemann surfaces*, no. 78 in London Mathematical Society lecture note series, Cambridge University Press, 1984.

[4] H. BEHNKE AND F. SOMMER, *Theorie der analytischen Funktionen einer complexen Veränderlichen*, Springer, Berlin, reprint of the 3rd edition ed., 1976.

[5] G. BEHRENDT AND P. M. NEWMANN, *On the number of normal subgroups of an infinite group*, Journal of the London Mathematical Society, s2-23 (1981), pp. 429–432.

[6] J. L. BRENNER, *The linear homogeneus group*, Ann. of Math (2), 71 (1960), pp. 210–223.

[7] I. CANGUL AND D. SINGERMAN, *Normal subgroups of Hecke groups and regular maps*, Math. Proc. Cambridge Philos. Soc. 123, (1998), pp. 59–74.

[8] I. N. CANGÜL, *About some normal subgroups of Hecke groups*, Tr. J. of Mathematics, (1997), pp. 143–151.

[9] B. CHANDLER AND W. MAGNUS, *The Reidemeister-Schreier method*, The History of Combinatorial Group Theory: A Case Study in the History of Ideas, (1982), pp. 91–101.

[10] M. S. DEY, *Scheirer systems in free products*, Proc. Glasgow Math. Assoc., 7 (1965), pp. 61–79.

[11] H. FRASCH, *Die erzeugenden der hauptkongruenzgruppen fir primzahlstufen*, Math. Ann., 108 (1933), pp. 229–252.

[12] R. FRICKE, *Über die substitutionsgruppen, welche zu den aus dem Legendre schen integralmodul $k^2(w)$ gezogenen wurzeln gehoren*, Math. Ann., 28 (1887), pp. 99–118.

[13] L. GREENBERG, *Note on normal subgroups of the modular group*, Proceedings of the American Mathematical Society, 17 (1966), pp. 1195–1198.

[14] R. C. GUNNING, *Lectures on modular forms*, no. 48, 1962.

[15] A. HATCHER, *Algebraic Topology*, Cornell University, New York, 2002.

[16] E. HECKE, *Über die bestimmung dirichletscher reihen durch ihre funktionalgleichung*, Math. Ann., 112 (1938), pp. 664–669.

[17] I. IVRISSIMTZIS AND D. SINGERMAN, *Regular maps and principal congruence subgroups of Hecke groups*, European Journal of Combinatorics, (2005), pp. 437–456.

[18] G. JONES AND D. SINGERMAN, *Theory of maps on orientable surfaces*, Proceedings of The London Mathematical Society, s3-37 (1978), pp. 273–307.

[19] F. KLEIN, *Lectures on the Icosahedron (2nd edition)*, Reprinted by Dover Publications Inc. (1963), New York, 1913.

[20] F. KLEIN AND R. FRICKE, *Vorlesungen über die Theorie der automorphen Functionen*, vol. 1, Teubner, Leipzig, 1897.

[21] M. I. KNOPP, *A note un subgroups of the modular group*, Amer. J. Math., (1963), pp. 95–97.

[22] N. KOBLITZ, *Algebraic Methods of Cryptography*, Springer, 1998.

[23] R. S. KULKARNI, *An arithmetic-geometric method in the study of the subgroups of the modular group*, Amer. J. Math., 113 (1991), pp. 1053–1133.

[24] A. G. KUROSH, *The theory of groups*, New York, 1956.

[25] C. KURTH AND L. LONG, *Computations with finite index subgroups of $PSL_2(\mathbb{Z})$ using Farey symbols*, Advances In Algebra And Combinatorics, (2008), pp. 225–242.

[26] R. LYNDON AND P. SCHUPP, *Combinatorial group theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, 1977.

[27] A. M. MACBEATH, *Generators of linear fractional groups*, Proceedings of Symposia in Pure Mathematics, 12 (1969), pp. 14–32.

[28] R. MIRANDA, *Algebraic curves and Riemann surfaces*, Amer. Math. Soc., 1997.

[29] T. MIYAKE, *Modular Forms*, Springer Monographs in Mathematics, 1989.

[30] NEWMAN, *Structure of some subgroups of the modular group*, Illinois J. Math., 6 (1962), pp. 480–487.

[31] M. NEWMAN, *A note on modular groups*, Proc. Am. Math. Soc., 14 (1963), pp. 124–125.

[32] M. NEWMAN, *A complete description of the normal subgroups of genus one of the modular group.*, Amer. J. Math., 86 (1964), pp. 17–24.

[33] M. NEWMAN, *Free subgroups and normal subgroups of the modular group*, Illinois J.Math, 8 (1964), pp. 262–265.

[34] M. NEWMAN, *Normal subgroups of the modular group which are not congruence groups*, Proc. Am. Math. Soc., 16 (1965), pp. 831–832.

[35] M. NEWMAN, *Classification of normal subgroups of the modular group*, Trans. Amer. Math. Soc., (1967), pp. 267–277.

[36] M. NEWMAN AND M. KNOPP, *Congruence subgroups of positive genus of the modular group*, Illinois J. Math, 9 (1965), pp. 577–583.

[37] J. NIELSEN, *The commutator group of the free product of cyclic groups*, Mat. Tidsskr., (1948), pp. 49–56.

[38] H. PETERSSON, *Zur analytischen theorie der grenzkreisgruppen*, Math. Ann., 115 (1937), pp. 175–204.

[39] G. PICK, *Ueber gewisse ganzzahlige lineare substitutionen, welce sich nicht durch algebraische congruenzen erklgren lassen*, Math. Ann., 28 (1887), pp. 119–124.

[40] I. REINER, *Subgroups of the unimodular group*, Proc. Am. Math. Soc., 12 (1961), pp. 173–174.

[41] D. ROSEN, *An arithmetic characterization of the parabolic points of* $g(2cos(\pi/5))$, Proceedings of the Glasgow Mathematical Association, 6 (1963), pp. 88–96.

[42] B. SCHOENEBERG, *Elliptic Modular Functions*, Springer-Verlag, Berlin, Heidelberg, New York, 1974.

[43] D. SINGERMAN, *Subgroups of fuchsian groups and finite permutation groups*, Bull. London Math. Soc., 2 (1979), pp. 319–323.

[44] G. JONES AND D. SINGERMAN, *Complex Functions. An Algebraic and Geometric Viewpoint*, Cambridge University Press, 1987.

[45] J. VAN LINT, *On the multiplier system of the Riemann-Dedekind function* η, Proc. Kon. Nederl. Acad. Wetensch. Ser. A Math. Sci., 61 (1958), pp. 522–527.

[46] J. WIJK, VAN, *Symmetric tiling of closed surfaces: visualization of regular maps*, ACM Transactions on Graphics, 28 (2009), pp. 1–12.

[47] K. WOHLFAHRT, *An extension of F. Klein's level concept*, Illinois J. Math, (1964), pp. 529–535.

[48] A. YAMAMURA, *Public-key cryptosystems using the modular group*, Lecture Notes in Computer Science, 1431 (1998), pp. 203–216.