INTRODUCCIÓN A GRUPOS ARITMÉTICOS

EMILIO A. LAURET, ROBERTO J. MIATELLO, AND BENJAMIN LINOWITZ

Índice

Date: 18 de Julio de 2018.

Estas notas corresponden al curso dictado por Emilio A. Lauret, Roberto J. Miatello, y Benjamin Linowitz en la escuela AGRA III, Aritmética, Grupos y Análisis, del 9 al 20 de Julio de 2018 en Córdoba, Argentina. Las primeras cinco secciones fueron redactadas por Lauret y Miatello de manera conjunta, mientras que las últimas cuatro fueron hechas por Linowitz.

El tercer autor agradece a Ángel Villanueva por la excelente traducción del inglés.

Parte 1. Fundamentos de grupos aritméticos

1. Introducción

El objetivo de estas notas es introducir y describir las principales propiedades de ciertos subgrupos discretos de covolumen finito de un grupo de Lie semisimple real G, los *subgrupos aritméticos*.

En estas notas G denotará un grupo de Lie, es decir, un grupo que es a la vez una variedad diferenciable real donde la función $(x, y) \to xy^{-1}$ es de clase C^∞. Requeriremos además, que G tenga un número finito de componentes conexas. El lector no familiarizado con grupos de Lie, puede pensar en ejemplos concretos de grupos de matrices tales como $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{C})$, $\mathrm{SL}_n(\mathbb{R})$, $\mathrm{SL}_n(\mathbb{C})$, $\mathrm{SO}(n, m)$, $\mathrm{SU}(n, m)$, que iremos definiendo de manera precisa durante el curso.

El primer caso que surge naturalmente es el de un subgrupo discreto L de $\mathbb{R}^n$, es decir $L = \sum_{j=1}^m \mathbb{Z} v_j$ donde $v_1, \ldots, v_m$ son vectores $\mathbb{R}$-linealmente independientes de $\mathbb{R}^n$. Un subgrupo L discreto de rango máximo ($m = n$) es denominado retículo. En ese caso, el cociente $\mathbb{R}^n/L$ es isomorfo a un toro n-dimensional.

Otro ejemplo importante es el plano hiperbólico, que se identifica al semiplano superior H de $\mathbb{R}^2$ munido de la métrica hiperbólica. En H el grupo $\mathrm{SL}(2, \mathbb{R})$ actúa por transformaciones de Möbius, esto es, dado $g = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ sea $g \cdot z := \frac{az+b}{cz+d}$. El subgrupo de isotropía de i es el subgrupo $\mathrm{SO}(2)$ y de este modo se tiene la identificación $\mathrm{SO}(2)\backslash\mathrm{SL}(2, \mathbb{R}) \simeq H$.

Los subgrupos discretos de $\mathrm{SL}(2, \mathbb{R})$ tales que el cociente H/Γ tiene medida finita son llamados subgrupos Fuchsianos de primera clase y el espacio cociente está representado por la llamada región fundamental. Se prueba que tal grupo admite una región fundamental dada por un polígono hiperbólico con un número finito de lados. Estos tienen área hiperbólica finita.

Los casos más simples son los llamados subgrupos principales de congruencia $\Gamma(N)$, con $N \in \mathbb{N}$, donde

$$\Gamma(N) = \{g \in G : g \equiv \mathrm{Id} \pmod{N}\}. \tag{1.1}$$

Se tiene la sucesión exacta

$$1 \to \Gamma(N) \to \mathrm{SL}(2, \mathbb{Z}) \to \mathrm{SL}(2, \mathbb{Z}_N) \to 1 \tag{1.2}$$

que muestra que $\Gamma(N)$ tiene índice finito en $\mathrm{SL}(2, \mathbb{Z})$.

Una región fundamental estándar para $\mathrm{SL}(2, \mathbb{Z})$ es la región triangular con área $\pi/3$ dada por

$$\mathcal{F} = \left\{z \in H : |Re(z)| \leq \tfrac{1}{2},\ |z| \geq 1\right\}.$$

En el caso del grupo $\Gamma(2)$ que tiene índice 6 en $\mathrm{SL}(2, \mathbb{Z})$ se puede tomar

$$\mathcal{F} = \left\{z \in H : |Re(z)| \leq 1\ \ |z - \tfrac{1}{2}| \geq 1,\ |z + \tfrac{1}{2}| \geq 1\right\}.$$

Observemos que en estos casos H/Γ no es compacto, luego tampoco lo es $\mathrm{SL}(2,\mathbb{Z})/\Gamma$, pero sí es de área finita. En el caso de $\Gamma(2)$, el área es igual a 2π.

Definición 1.1. Si G es un grupo de Lie y $\Gamma \subset G$ es un subgrupo, Γ es un retículo si Γ es discreto y de volumen finito; Γ se dice cocompacto si G/Γ es compacto.

Ejemplo 1.2.
1. (i) Si $\{v_j\}_1^n$ es una base de $\mathbb{R}^n$, $L = \sum_1^n \mathbb{Z}v_j$ es un retículo en $\mathbb{R}^n$. Todo retículo en $\mathbb{R}^n$ es de este tipo.
   (ii) $\Gamma(N)$ es un retículo en $\mathrm{SL}(2,\mathbb{R})$, para todo $N \in \mathbb{N}$.
   (iii) $\mathrm{SL}_n(\mathbb{Z})$ es un retículo en $\mathrm{SL}_n(\mathbb{R})$ para todo n. Esto será probado más adelante.
   (iv) Sea $\mathrm{O}(p,q) = \{g \in \mathrm{GL}(p+q,\mathbb{R}) : gJg^t = J\}$ donde $J = \begin{bmatrix} I_p & 0 \\ 0 & -I_q \end{bmatrix}$ es el grupo de transformaciones lineales en $\mathbb{R}^{p+q}$ que preservan la forma cuadrática $\sum_1^p x_j^2 - \sum_1^q x_i^2$. Este grupo contiene el retículo $\mathrm{O}(p,q)_{\mathbb{Z}}$ de matrices enteras en $\mathrm{O}(p,q)$.

Los ejemplos (ii), (iii) y (iv) son casos de los llamados grupos aritméticos. Nos interesarán particularmente los subgrupos cocompactos, que son más difíciles de construir. Estos serán tratados en la parte final de las notas.

2. Preliminares

En esta sección introduciremos algunos conceptos necesarios para el desarrollo de los temas de este curso.

2.1. Medidas. Un *grupo topológico* G es un grupo que es a la vez un espacio topológico donde la función $G \times G \ni (x,y) \mapsto xy^{-1} \in G$ es continua. Además, G se dice *localmente compacto* si, tal como su nombre lo sugiere, para cada punto existe un entorno compacto. Se asume además que tal grupo es Hausdorff, esto es dados dos puntos distintos x e y, existen entornos disjuntos U_x e U_y de x e y. Todo grupo topológico localmente compacto admite una medida invariante a izquierda positiva Boreliana que es única salvo múltiplos positivos. Es la llamada *medida de Haar*.

Sean G un grupo topológico localmente compacto. Se denota $C_c(G)$ al espacio de funciones continuas complejas sobre G con soporte compacto. Fijamos μ_G una medida de Haar invariante a izquierda de G. Si $f \in C_c(G)$, la integral de f con respecto a μ_G es

$$\int_G f(g) d\mu_G(g).$$

Para cada $x \in G$, la aplicación

$$f \mapsto \int_G f(gx) d\mu_G(g)$$

define una nueva medida invariante a izquierda en G. Por la unicidad de la medida de Haar a menos de un múltiplo positivo, existe $\Delta_G : G \to \mathbb{R}^+$ ($\mathbb{R}^+ := \{t \in \mathbb{R} : t > 0\}$) en G, la llamada *función modular*, definida por la ecuación

$$\Delta_G(x) \int_G f(g) d\mu_G(g) = \int_G f(gx) d\mu_G(g),$$

para cada $f \in C_c(G)$. Se puede ver que Δ_G es un morfismo continuo (Ejercicio 2.1).

Se dice que G es unimodular si $\Delta_G \equiv 1$ esto es, si toda medida de Haar invariante a izquierda es también invariante a derecha. Se prueba que todos los grupos compactos son unimodulares, así como los grupos conmutativos y nilpotentes (ver Ejercicio 2.2). También lo son los grupos con conmutador denso (e.g. semisimples), esto es $\overline{[G,G]} = G$, ya que $\Delta_G([x,y]) = \Delta_G(xyx^{-1}y^{-1}) = 1$ para todo $x, y \in G$ pues $\mathbb{R}^+$ es abeliano.

Ejemplo 2.1. El siguiente grupo no es unimodular:

$$\left\{ \begin{pmatrix} y & x \\ 0 & y^{-1} \end{pmatrix} : x \in \mathbb{R},\, y \in \mathbb{R}^+ \right\} \simeq \mathbb{R}^+ \ltimes \mathbb{R}.$$

Sea H un subgrupo cerrado de G. Denotamos por $C_c(G/H)$ al espacio de funciones complejas sobre G/H con soporte compacto.

Teorema 2.2. *Si G es unimodular y H es un subgrupo cerrado unimodular, el espacio homogéneo G/H admite una medida G-invariante. Esta medida es única salvo un múltiplo escalar positivo.*

Su demostración se puede encontrar en [12, Lem. 1.4].

2.2. Grupos de Lie. Un grupo de Lie G es un grupo topológico que a la vez es una variedad diferenciable real en el cual las operaciones $(x, y) \to xy$ y $x \to x{-}1$ son de clase C^∞. En particular, si $g \in G$, las traslaciones a izquierda y a derecha, $l_g : x \mapsto gx$ y $r_g : x \mapsto xg$ respectivamente, son difeomorfismos de G.

Un grupo de Lie mantiene todas las propiedades locales de $\mathbb{R}^n$, por ejemplo es localmente compacto y localmente conexo. Además, la componente conexa de la identidad G^0 de G es un subgrupo abierto normal de G y $\#|G/G^0|$ es igual al número de componentes conexas de G. En estas notas trabajaremos con grupos que poseen un número finito de componentes conexas.

Observamos que todo subgrupo abierto H de un grupo de Lie G es también cerrado pues

$$G = \Big(\bigcup_{g \notin H} gH \Big) \cup H$$

y como gH es abierto, para todo $g \in G$, vemos que el complemento de H es también abierto.

Un grupo de Lie G posee un cubrimiento simplemente conexo $\widehat{G}$, llamado cubrimiento universal, y existe una aplicación $\pi : \widehat{G} \to G$ que es un isomorfismo local suryectivo, en particular $\ker(\pi)$ es un subgrupo normal discreto que está contenido en el centro de G (Ejercicio 2.6). Si G es simplemente conexo, se puede decir que G coincide con $\hat{G}$.

Un grupo G se dice simple si no posee subgrupos normales propios de dimensión mayor o igual que 1 y se dice semisimple si su cubrimiento universal es isomorfo a un producto de factores simples. Los grupos de Lie reales simples están ya clasificados (E. Cartan) y los grupos simples simplemente conexos están en correspondencia con las álgebras de Lie reales simples (ver [9] o [8]).

A modo de ejemplo, en estas notas trabajaremos con varios grupos semisimples: los grupos compactos $\mathrm{SO}(n)$ y $\mathrm{SU}(n)$ de matrices ortogonales o unitarias de determinante 1, los grupos lineales especiales $\mathrm{SL}_n(\mathbb{R})$ y $\mathrm{SL}_n(\mathbb{C})$, y los grupos $\mathrm{O}(p, q)$ de transformaciones inversibles de $\mathbb{R}^n$, $n = p + q$, que preservan una forma cuadrática no degenerada de signatura (p, q).

2.3. Retículos. Ahora consideremos el caso en que $H = \Gamma$ es un subgrupo discreto de G, es decir, todo punto de Γ es abierto con la topología relativa de G.

Lema 2.3. *Todo grupo discreto es unimodular.*

Demostración. Sea Γ un grupo discreto. Como μ_Γ es una medida de Haar invariante a izquierda, tenemos que

$$\mu_\Gamma(\{x\}) = \int_\Gamma \chi_x(h) d\mu_\Gamma(h) = \int_\Gamma \chi_e(x^{-1}h) d\mu_\Gamma(h) = \int_\Gamma \chi_e(h) d\mu_\Gamma(h) = \mu_\Gamma(\{e\})$$

para cualquier $x \in \Gamma$, donde χ_x denota la función característica sobre el conjunto $\{x\} \subseteq \Gamma$. Luego, todo punto de Γ tiene la misma medida (positiva).

Si $f \in C_c(\Gamma)$, entonces f es idénticamente nula salvo en un conjunto finito, digamos $\{h_1, \ldots, h_d\} \subset \Gamma$, por lo tanto

$$\int_\Gamma f(h) d\mu_\Gamma(h) = \left(\sum_{i=1}^{d} f(h_i) \right) \mu_\Gamma(\{e\}).$$

Por otro lado, para cada $x \in \Gamma$ se tiene que

$$\int_\Gamma f(hx) d\mu_\Gamma(h) = \sum_{i=1}^{d} f(h_i) \mu_\Gamma(\{h_i x^{-1}\}) = \left(\sum_{i=1}^{d} f(h_i) \right) \mu_\Gamma(\{e\}).$$

Luego $\Delta_\Gamma \equiv 1$. □

Definición 2.4. Un subgrupo discreto Γ de G es un *retículo* (o *lattice*) si G/Γ admite una medida G-invariante finita. Además, Γ se dice *cocompacto* o *uniforme* si G/Γ es compacto.

Nota 2.5. Todo subgrupo discreto y cocompacto es un retículo.

Ejemplo 2.6. Sea V un espacio vectorial real. Un subgrupo $\mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_m$ con $v_i \in V$ para todo i es un retículo si y sólo si el conjunto $\{v_1, \ldots, v_m\}$ es una base de V. Más aún, en este caso, es un retículo cocompacto pues $V/\mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_m$ es homeomorfo a un toro de dimensión m.

Teorema 2.7. *Sea G un grupo de Lie con un número finito de componentes conexas. Sea Γ un retículo en G y sea $\pi : G \to G/\Gamma$ la proyección canónica. Entonces, las siguientes condiciones son equivalentes:*

(i) *G/Γ es compacto.*
(ii) *No existen $g_n \in G$ y $\gamma_n \in \Gamma$ tales que $g_n \gamma_n g_n^{-1} \to e$ cuando $n \to \infty$ y $g_n \gamma_n g_n^{-1} \neq e$ para todo n.*
(iii) *Existe U un entorno abierto de e en G tal que $\pi_g|_U$ es inyectiva para todo $g \in G$, donde $\pi_g(x) = \pi(xg)$.*

Demostración. Mostremos primero que la condición (i) implica la (ii), razonando por el absurdo. Supongamos que $g_n \gamma_n g_n^{-1} \to e$ y $g_n \gamma_n g_n^{-1} \neq e$ para todo n. Como G/Γ es compacto, existe una subsucesión convergente $g_{n_j}\Gamma \to g\Gamma$. Luego, existen $\beta_{n_j} \in \Gamma$ tal que $g_{n_j}\beta_{n_j} \to g$ en G, o sea $g_{n_j} = \varepsilon_{n_j} g \beta_{n_j}^{-1}$, con $\varepsilon_{n_j} \to e$. Por lo tanto, la subsucesión $\alpha_j := \beta_{n_j}^{-1} \gamma_{n_j} \beta_{n_j}$ de Γ cumple $\alpha_j \neq e$ para todo j y a su vez tiene límite e, un absurdo pues Γ es discreto.

Ahora asumamos (ii) y supongamos que (iii) es falsa. Fijemos una base de entornos abiertos conexos U_m de e con $U_m = U_m^{-1}$, $U_{m+1} \subset U_m^2$ para todo m y tales que $\cap_m U_m = \{e\}$. Supongamos que para todo m existe $g_m \in G$ tal que $\pi_{g_m}|_{U_m}$ no es inyectiva. Entonces, existen u_m, v_m en U_m y $\gamma_m \in \Gamma$ con $u_m \neq v_m$ y $u_m g_m = v_m g_m \gamma_m$. Luego, $v_m^{-1} u_m = g_m \gamma_m g_m^{-1} \to e$ y $v_m^{-1} u_m \neq e$ para todo m, lo cual contradice (ii).

Ahora supongamos que G/Γ no es compacto asumiendo (iii). Sea U un entorno abierto conexo de e con $\bar{U}$ compacto, $U = U^{-1}$ y sea $V = U^2$. Probaremos que $\pi_g|_U$ no es inyectiva para algún $g \in G$. Sea C compacto en G/Γ. Entonces $G/\Gamma \setminus VC \neq \emptyset$. Sea $g_1 \in G$ con $\bar{g_1} \notin G/\Gamma \setminus VC$. Entonces, $U\bar{g_1} \subset G/\Gamma \setminus UC$. Similarmente existe $g_2 \in G$ con $\bar{g_2} \in G/\Gamma \setminus VC \cup V\bar{g_1}$. Iterando este procedimiento se obtiene una sucesión de conjuntos disjuntos conexos $U\bar{g_n}$ en G/Γ para $n \in \mathbb{N}$. Si $\pi_g|_U$ es inyectiva para todo n entonces $\pi_g|_U : U \to \pi_g(U)$ es un homeomorfismo y $\mu_{G/\Gamma}(\pi_g(U)) = \mu_G(U)$ para todo n. Luego $\mu(G/\Gamma) = \infty$, un absurdo pues Γ es un retículo. □

2.4. Conmensurabilidad. La siguiente noción será muy útil en el resto de estas notas.

Definición 2.8. Dos subgrupos A y B en un grupo G se dicen *conmensurables* si la intersección es de índice finito en ambos, es decir, si $|A/(A\cap B)| = [A : A\cap B] < \infty$ y $|B/(A\cap B)| = [B : A\cap B] < \infty$.

Se puede ver que la conmensurabilidad es una relación de equivalencia (Ejercicio 2.7)

Proposición 2.9. *Sean Γ y Γ' subgrupos conmensurables de un grupo topológico localmente compacto G. Entonces, si Γ es discreto, un retículo, ó un retículo cocompacto, Γ' también lo es.*

Demostración. Supongamos que Γ es discreto, por lo tanto $\Gamma\cap\Gamma'$ es discreto. Para probar que Γ' es discreto, es suficiente ver que toda sucesión convergente en Γ' es estacionaria.

Sea $x_n \in \Gamma'$ una sucesión convergente a x. Sea $\{\gamma_1 = e, \gamma_2, \dots, \gamma_d\} \subset \Gamma'$ los distintos representantes de $\Gamma'/\Gamma\cap\Gamma'$. Para cada $n\in\mathbb{N}$, existe $\theta_n \in \Gamma\cap\Gamma'$ tal que $x_n = \gamma_{i_n}\theta_n$ con $i_n \in \{1,\dots,d\}$. Luego, existe al menos un t tal que $i_n = t$ para una cantidad infinita de índices $n\in\mathbb{N}$. Definimos la subsucesión n_j, $j\in\mathbb{N}$ dada por tales índices.

Tenemos que $x_{n_j} = \gamma_t\theta_{n_j} \to x$ cuando $j\to\infty$, por lo tanto $\theta_{n_j} \to \gamma_t^{-1}x$. Como para cada $j\in\mathbb{N}$, θ_{n_j} vive en el conjunto discreto $\Gamma\cap\Gamma'$, resulta que la sucesión θ_{n_j} es estacionaria, es decir, $\theta_{n_j} = \theta \in \Gamma\cap\Gamma'$ para todo $j\geq J$ con $J\in\mathbb{N}$ suficientemente grande. Luego la subsucesión x_{n_j} es estacionaria.

Si probamos que existe $N\in\mathbb{N}$ tal que $i_n = t$ para todo $n\geq N$, la prueba estará completa. Supongamos contrariamente que existen infinitos índices $m\in\mathbb{N}$ tal que $i_m \neq t$. En ese caso, existe $s\in\{1,\dots,d\}$ con $s\neq t$ e índices m_k tales que $m_k = s$ para todo $k\in\mathbb{N}$ y así $x_{m_k} = \gamma_s\theta_{m_k}$. Entonces

$$\begin{cases} x_{n_j} = \gamma_t\theta_{n_j} \text{ con } \theta_{n_j} = \theta \text{ para todo } j\geq J, \\ x_{m_k} = \gamma_s\theta_{m_k} \text{ con } \theta_{m_k} = \theta_1 \text{ para todo } k\geq K. \end{cases}$$

Además, como x_{n_j} y x_{m_k} convergen a x, obtenemos que

$$\gamma_s^{-1}\gamma_t = \theta_{m_k}x_{m_k}^{-1}x_{n_j}\theta_{n_j}^{-1} \to \theta_1\theta^{-1},$$

por lo tanto $\gamma_s^{-1}\gamma_t = \theta_1\theta^{-1} \in \Gamma\cap\Gamma'$, lo que es una contradicción pues γ_s y γ_t son representantes distintos de $\Gamma/\Gamma\cap\Gamma'$, lo que prueba que Γ' es discreto.

Veamos ahora que si Γ es un retículo, entonces $\Gamma\cap\Gamma'$ es también un retículo. En efecto

$$\mathrm{vol}(G/\Gamma\cap\Gamma') = \mathrm{vol}(G/\Gamma)\cdot[\Gamma : \Gamma\cap\Gamma'] < \infty.$$

Por otro lado, Γ' es un retículo pues

$$\mathrm{vol}(G/\Gamma') = \mathrm{vol}(G/\Gamma\cap\Gamma')[\Gamma' : \Gamma\cap\Gamma']^{-1} < \infty.$$

Supongamos finalmente que G/Γ es compacto. Para ver que G/Γ' es compacto basta ver que $G/\Gamma\cap\Gamma'$ es compacto. Sea $\pi' : G \to G/\Gamma\cap\Gamma'$ la proyección canónica. Como G/Γ es compacto, existe $\Omega\subset G$ compacto tal que $\pi(\Omega) = G/\Gamma$. Ahora $\Gamma/\Gamma\cap\Gamma' = \bigcup_{i=1}^d \gamma_i(\Gamma\cap\Gamma')$. Probaremos que

$$\pi'\left(\bigcup_{i=1}^d \Omega\gamma_i\right) = G/\Gamma\cap\Gamma'. \tag{2.1}$$

Si $x\in G$, como $\pi(\Omega) = G/\Gamma$, entonces $k^{-1}x\in\Gamma$ para algún $k\in\Omega$. Luego, $\gamma_i^{-1}k^{-1}x = \theta\in\Gamma\cap\Gamma'$ para algún $i\in\{1,\dots,d\}$. Por lo tanto

$$\pi'(x) = \pi'(k\gamma_i\theta) = \pi'(k\gamma_i) \in \pi'\left(\bigcup_{i=1}^d \Omega\gamma_i\right).$$

Esto verifica (2.1), lo cual implica que $G/\Gamma\cap\Gamma'$ es compacto y concluye la prueba. □

2.5. Ejercicios.

Ejercicio 2.1. Demostrar que la forma modular $\Delta_G : G \to \mathbb{R}^+$ sobre un grupo topológico localmente compacto G es un morfismo (i.e. $\Delta_G(x_1x_2) = \Delta_G(x_1)\Delta_G(x_2)$ para todo $x_1, x_2 \in G$) continuo.

Ejercicio 2.2. Demostrar que las siguientes clases de grupos son unimodulares:

1. Grupos compactos.
2. Grupos conmutativos.
3. Grupos topológicos localmente compactos que admiten un retículo.

Ejercicio 2.3. Demostrar que el grupo en Ejemplo 2.1 no es unimodular. Además, encontrar el isomorfismo señalado en tal ejemplo.

Ejercicio 2.4. Probar que $\int f(x^{-1})dx = \int f(x)\Delta(x^{-1})dx$.

Ejercicio 2.5. Sea Γ un retículo en un grupo de Lie G. Probar que Γ es finito si y sólo si G es compacto.

Ejercicio 2.6. Sea G un grupo de Lie con cubrimiento universal $\pi : \widehat{G} \to G$. Mostrar que $\ker(\pi)$ es un subgrupo normal discreto que está contenido en el centro de G (Ejercicio 2.6).

Ejercicio 2.7. Demostrar que la conmensurabilidad es una relación de equivalencia.

Ejercicio 2.8. Un grupo se llama sin torsión si no tiene subgrupos finitos no triviales. Mostrar que $\mathrm{SL}_n(\mathbb{Z})$ tiene un subgrupo de índice finito sin torsión.

3. Grupos aritméticos

En esta sección introduciremos los llamados grupos aritméticos, haciendo uso de los grupos algebraicos definidos sobre Q. Los puntos reales de tales grupos son grupos de Lie semisimples.

3.1. Grupos algebraicos. Sean V un espacio vectorial sobre $\mathbb{C}$ de dimensión finita y $\mathbb{K}$ un subcuerpo de $\mathbb{C}$. Sea $V_{\mathbb{K}}$ una $\mathbb{K}$-forma de V, esto es, $V_{\mathbb{K}}$ es un espacio vectorial sobre $\mathbb{K}$ incluido en V tal que $V \simeq V_{\mathbb{K}} \otimes_{\mathbb{K}} \mathbb{C}$, o equivalentemente, $V_{\mathbb{K}}$ tiene una $\mathbb{K}$-base que también es $\mathbb{C}$-base de V.

Denotamos $\mathbb{C}[V]$ al espacio de funciones polinomiales en V con coeficientes complejos. Esto es, $P \in \mathbb{C}[V]$ si $P : V \to \mathbb{C}$, y para $\{v_1, \ldots, v_n\}$ una base de V se tiene que

$$P(a_1v_1 + \ldots + a_nv_n) = \sum_{\alpha=(\alpha_1,\ldots,\alpha_n)\in\mathbb{N}_0^n} c_\alpha\, a_1^{\alpha_1} \ldots a_n^{\alpha_n},$$

con $c_\alpha \in \mathbb{C}$ todos nulos salvo una cantidad finita. Sea $\mathbb{K}[V]$ a las funciones polinomiales en V que, restringidas a $V_{\mathbb{K}}$, tienen coeficientes en $\mathbb{K}$ (ver Ejercicio 3.3).

Una *variedad algebraica* Z es un subconjunto de V que a su vez es el conjunto de ceros de una familia de funciones polinomiales en V. Sea $I(Z) \subseteq \mathbb{C}[V]$ el ideal de polinomios en V que se anulan en Z y $\mathbb{C}[Z] := \mathbb{C}[V]/I(Z)$ el anillo de funciones regulares en Z. Diremos que Z *está definida sobre* $\mathbb{K}$ (o que es una $\mathbb{K}$-*variedad algebraica*), si $I(Z)$ es generado como ideal por la intersección $I(Z)\cap\mathbb{K}[V]$. Esto es equivalente a que la variedad puede ser definida como los ceros de funciones polinomiales en $\mathbb{K}[V]$ (ver Ejercicio 3.4). Denotemos $\mathbb{K}[Z] := \mathbb{K}[V]/(I(Z) \cap \mathbb{K}[V])$ al anillo de *funciones regulares de* Z. Un $\mathbb{K}$-*morfismo* de $\mathbb{K}$-variedades $\varphi : Z_1 \to Z_2$ es un mapeo tal que $f \circ \varphi \in \mathbb{K}[Z_1]$ para todo $f \in \mathbb{K}[Z_2]$. También diremos que φ está definido sobre $\mathbb{K}$.

El grupo de transformaciones lineales invertibles $\mathrm{GL}(V)$ hereda una estructura de variedad algebraica del espacio vectorial $\mathrm{End}_{\mathbb{C}}(V) \times \mathbb{C}$ de tal modo que $\mathrm{GL}(V)$ se identifica con la variedad algebraica $\{(T, t) \in \mathrm{End}_{\mathbb{C}}(V) \times \mathbb{C} : \det(T)t - 1 = 0\}$ por $T \mapsto (T, \det T^{-1})$. Más aún, $\mathrm{GL}(V)$ está definido sobre $\mathbb{Q}$, y por lo tanto sobre cualquier subcuerpo $\mathbb{K}$ de $\mathbb{C}$.

Definición 3.1. Un grupo algebraico lineal definido sobre $\mathbb{K}$ es un subgrupo $\mathbf{G} \subset \mathrm{GL}(V)$ que es una $\mathbb{K}$-variedad algebraica de $\mathrm{End}_{\mathbb{C}}(V)$ con respecto a la $\mathbb{K}$-forma isomorfa a $\mathrm{End}(V)_{\mathbb{K}}$.

Nota 3.2. La $\mathbb{K}$-forma $\mathrm{End}(V)_{\mathbb{K}}$ de $\mathrm{End}_{\mathbb{C}}(V)$ está definida en el Ejercicio 3.2.

En lo sucesivo, abreviaremos llamando $\mathbb{K}$-*grupo algebraico* a un grupo algebraico lineal definido sobre $\mathbb{K}$. Además, cuando $\mathbb{K} = \mathbb{C}$, diremos simplemente grupo algebraico.

Nota 3.3. Cada vez que tomamos un $\mathbb{K}$-grupo algebraico $\mathbf{G} \subset \mathrm{GL}(V)$, estamos asumiendo que V posee una $\mathbb{K}$-forma $V_{\mathbb{K}}$, que a la vez induce la $\mathbb{K}$-forma $\mathrm{End}_{\mathbb{C}}(V)_{\mathbb{K}}$ que define la estructura de $\mathbb{K}$-variedad algebraica de $\mathbf{G}$. Fijada $\{v_1, \ldots, v_n\}$ una $\mathbb{K}$-base arbitraria de $V_{\mathbb{K}}$, se tiene la identificación $\mathrm{GL}(V) \equiv \mathrm{GL}_n(\mathbb{C})$ dada por $T \mapsto (a_{i,j})_{i,j}$ donde $Tv_i = \sum_j a_{i,j} v_j$. También se tienen las identificaciones $V \equiv \mathbb{C}^n$ y $V_{\mathbb{K}} \equiv \mathbb{K}^n := \{(z_1, \ldots, z_n) \in \mathbb{C}^n : z_i \in \mathbb{K} \text{ para todo } i\}$.

Usaremos la convención de que cada vez escribamos $\mathrm{GL}_n(\mathbb{C})$, estaremos asumiendo que la $\mathbb{K}$-forma escogida en $V = \mathbb{C}^n$ es $V_{\mathbb{K}} = \mathbb{K}^n$. Además, si $\mathbf{G} \subset \mathrm{GL}_n(\mathbb{C})$ es un grupo algebraico y A es un subanillo de $\mathbb{C}$, denotaremos $\mathbf{G}_A = \mathbf{G} \cap \mathrm{GL}_n(A)$.

Un $\mathbb{K}$-*morfismo* de $\mathbb{K}$-grupos $\varphi : \mathbf{G}_1 \to \mathbf{G}_2$ es un $\mathbb{K}$-morfismo de $\mathbb{K}$-variedades que es también un morfismo de grupos. Un caso especial es el de una $\mathbb{K}$-*representación* de $\mathbf{G}$, que es un $\mathbb{K}$-morfismo de la forma $\rho : \mathbf{G} \to \mathrm{GL}(V)$

Nota 3.4. Si $\mathbf{G} \subseteq \mathrm{GL}_n(\mathbb{C})$ es un $\mathbb{K}$-grupo, $\mathbf{G}_{\mathbb{R}}$ es un grupo de Lie con un número finito de componentes conexas. Diremos que un grupo algebraico $\mathbf{G}$ es *semisimple* si el álgebra de Lie del grupo de Lie $\mathbf{G}_{\mathbb{R}}$ es semisimple o equivalentemente, si el cubrimiento universal es un producto de grupos simples.

Terminaremos esta subsección con algunos ejemplos de grupos algebraicos definidos sobre $\mathbb{K}$. En lo que sigue, dada una matriz A, denotaremos con $a_{i,j}$ a sus entradas.

Ejemplo 3.5. Como ya mencionamos, $\mathrm{GL}(V)$ es un $\mathbb{Q}$-grupo algebraico. De manera similar, $\mathrm{SL}(V)$ también lo es ya que el polinomio que lo define, $\det(T) - 1 = 0$, tiene coeficientes racionales.

Ejemplo 3.6. Sea J una matriz simétrica real, $n \times n$, no degenerada, con coeficientes en $\mathbb{K}$. Entonces,

$$\mathrm{O}(J) := \{A \in \mathcal{M}_d(\mathbb{C}) : A^t J A = J\}$$

es un grupo algebraico definido sobre $\mathbb{K}$. En efecto, el ideal de polinomios que lo define está generado por las coordenadas de la matriz $A^t J A - J$, las cuales pueden verse como polinomios en las entradas $a_{i,j}$ con coeficientes claramente en $\mathbb{K}$.

El grupo de Lie $\mathrm{O}(J)_{\mathbb{R}}$ es el grupo transformaciones lineales de $\mathbb{R}^n$ que preservan la forma cuadrática $F(x) := x^t J x$ para $x = (x_1, \ldots, x_n)^t \in \mathbb{R}^n$, esto es, $\mathrm{O}(J)_{\mathbb{R}} = \{g \in \mathrm{GL}_n(\mathbb{R}) : F(gx) = F(x)\ \forall\, x \in \mathbb{R}^n\}$.

Claramente el grupo $\mathrm{SO}(J) := \mathrm{O}(J) \cap \mathrm{SL}_n(\mathbb{C})$ es también un $\mathbb{Q}$-grupo algebraico.

Ejemplo 3.7. Como caso particular del ejemplo anterior, tomemos $n = p + q$, y

$$\mathrm{diag}(r_1, \ldots, r_m, -s_1, \cdots - s_n),$$

con r_i, s_j racionales positivos para todo i y j. En este caso es más simple ver quiénes son los polinomios que definen $\mathrm{O}(J)$. Por ejemplo, $P_{1,1}(A) = P_{1,1}(a_{1,1}, a_{1,2}, \ldots, a_{d,d}) = r_1 a_{1,1}^2 + \cdots + r_p a_{p,1}^2 - s_1 a_{p+1,1}^2 - \cdots - s_n a_{n,1}^2 - 1$. Además, $\mathrm{O}(J)_{\mathbb{R}}$ es el grupo transformaciones lineales de $\mathbb{R}^n$ que preserva la forma cuadrática

$$F(x) := x^t J x = r_1 x_1^2 + \ldots, r_p x_p^2 - s_1 x_{p+1}^2 - \cdots - s_q x_n^2.$$

Nota 3.8. Para

$$I_{p,q} := \mathrm{diag}(\underbrace{1,\dots,1}_{p\text{-veces}},\underbrace{-1,\dots,-1}_{q\text{-veces}}),$$

denotamos $\mathrm{O}(p,q) = \mathrm{O}(I_{p,q})$ y $\mathrm{SO}(p,q) = \mathrm{SO}(I_{p,q})$.

Se puede ver que para cualquier matriz simétrica real J no degenerada $n \times n$, existen enteros p y q tales que $n = p + q$ y los grupos $\mathrm{O}(J)$ y $\mathrm{O}(p,q)$ son conjugados (ver Ejercicio 3.6). En particular, son isomorfos como grupos algebraicos (sobre $\mathbb{C}$). También son conjugados $\mathrm{O}(J)_{\mathbb{R}}$ y $\mathrm{O}(p,q)_{\mathbb{R}}$, por lo que son isomorfos como grupos de Lie. A pesar de esto, $\mathrm{O}(J)$ y $\mathrm{O}(p,q)$ son en general diferentes como $\mathbb{Q}$-grupos algebraicos, y definirán grupos aritméticos esencialmente distintos.

3.2. Subgrupos aritméticos. Sea $\mathbf{G}$ un subgrupo algebraico de $\mathrm{GL}(V)$ definido sobre $\mathbb{Q}$, donde V es un $\mathbb{C}$-espacio vectorial munido de una $\mathbb{Q}$-estructura $V_{\mathbb{Q}}$. Sea L un retículo contenido en $V_{\mathbb{Q}}$, i.e., un $\mathbb{Z}$-submódulo libre de $V_{\mathbb{Q}}$, generado por una base de V. [1]

Denotamos $\mathbf{G}_{\mathbb{Q}} = \{g \in \mathbf{G} : gV_{\mathbb{Q}} = V_{\mathbb{Q}}\}$, el grupo de puntos $\mathbb{Q}$-racionales de $\mathbf{G}$, y para L un retículo en $V_{\mathbb{Q}}$,

$$\mathbf{G}_L := \{g \in \mathbf{G}_{\mathbb{Q}} : g(L) = L\}.$$

Definición 3.9. Sea $\mathbf{G} \subseteq \mathrm{GL}(V)$ un subgrupo algebraico definido sobre $\mathbb{Q}$. Un subgrupo *aritmético* de $\mathbf{G}$ es un subgrupo Γ de $\mathbf{G}_{\mathbb{Q}}$ que es conmensurable con $\mathbf{G}_L$ para algún retículo L contenido en $V_{\mathbb{Q}}$.

Ejemplo 3.10. Por ejemplo, en el caso $\mathbf{G} \subset \mathrm{GL}_n(\mathbb{C})$ (i.e. $V = \mathbb{C}^n$ y $V_{\mathbb{Q}} = \mathbb{Q}^n$), tomando el retículo $L = \mathbb{Z}^n$ obtenemos $\mathbf{G}_L = \mathbf{G}_{\mathbb{Z}} = \mathbf{G} \cap \mathrm{GL}_n(\mathbb{Z})$.

Más aún, si L es cualquier retículo en $\mathbb{Q}^n$ con $\mathbb{Z}$-base $\mathcal{B}$, y si $C \in \mathrm{GL}_n(\mathbb{Q})$ es la matriz de cambio de base de $\mathcal{B}$ a la base canónica $\mathcal{C}$, entonces se tiene que $\mathbf{G}_L = C^{-1}\mathbf{G}_{\mathbb{Z}}C$, y se puede verificar que $\mathbf{G}_L \subset \mathbf{G}_{\mathbb{Q}}$ es conmensurable con $\mathbf{G}_{\mathbb{Z}} \subset \mathrm{GL}_n(\mathbb{Z})$, pero $\mathbf{G}_L$ no es necesariamente un subgrupo de $\mathrm{GL}_n(\mathbb{Z})$.

Nota 3.11. Mencionamos en Nota 3.3 que, tomando cualquier $\mathbb{Q}$-base de $V_{\mathbb{Q}}$, todo $\mathbb{Q}$-grupo algebraico $\mathbf{G} \subset \mathrm{GL}(V)$ puede realizarse dentro de $\mathrm{GL}_n(\mathbb{C})$ con respecto a la $\mathbb{Q}$-forma estándar $\mathbb{Q}^n$ en $\mathbb{C}^n$. Esto nos permitirá asumir (sin perder generalidad) en algunos de los siguientes enunciados que los grupos algebraicos sobre $\mathbb{Q}$ están contenidos en $\mathrm{GL}_n(\mathbb{C})$ (con respecto a la $\mathbb{Q}$-forma $\mathbb{Q}^n$ en $\mathbb{C}^n$).

Definición 3.12. Sea $\mathbf{G} \subset \mathrm{GL}_n(\mathbb{C})$ un $\mathbb{Q}$-subgrupo algebraico. Para $N \in \mathbb{N}$, definimos el subgrupo principal de congruencia de nivel N como

$$\mathbf{G}_{\mathbb{Z}}(N) = \{g \in \mathbf{G}_{\mathbb{Z}} : g \equiv \mathrm{Id} \pmod{N}\}.$$

El siguiente resultado nos muestra que $\mathbf{G}_{\mathbb{Z}}$ no depende, salvo conmensurabilidad, de la realización de $\mathbf{G}$ como grupo algebraico definido sobre $\mathbb{Q}$.

Proposición 3.13. *Sea $\boldsymbol{G} \subseteq \mathrm{GL}_n(\mathbb{C})$ un subgrupo algebraico definido sobre $\mathbb{Q}$, y sea $\rho : \boldsymbol{G} \to \mathrm{GL}(V)$ una $\mathbb{Q}$-representación.*

(i) *Si L es un retículo en $V_{\mathbb{Q}}$, entonces existe $N \in \mathbb{N}$ tal que $\rho(\boldsymbol{G}_{\mathbb{Z}}(N)) \cdot L = L$.*

(ii) *$\rho(\boldsymbol{G}_{\mathbb{Z}})$ preserva algún retículo de $V_{\mathbb{Q}}$.*

Demostración. Sea L un retículo en $V_{\mathbb{Q}}$, y fijemos una $\mathbb{Z}$-base de L. Sea m la dimensión de V. Para cada $g \in \mathbf{G}$, sea $[\rho_{i,j}(g)]_{i,j}$ la matriz de $\rho(g) : V \to V$ con respecto a la base fijada. Se tiene que $\rho(g)_{i,j} \in \mathbb{Q}[g] = \mathbb{Q}[g_{1,1}, g_{1,2}, \dots, g_{n,n}]$ por ser ρ definida sobre $\mathbb{Q}$.

Para cada $1 \leq i, j \leq m$, consideremos

$$P_{i,j}(g - \mathrm{Id}) = \rho_{i,j}(g) - \delta_{i,j}.$$

[1] Usar la palabra *retículo* para L en $V_{\mathbb{Q}}$ es un abuso del lenguaje muy útil. Asimismo, L es un retículo en el sentido usual en el $\mathbb{R}$-espacio vectorial $V_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{R}$.

Claramente $P_{i,j}$ es un polinomio con coeficientes racionales. La razón de tomar como variables las coordenadas de $g - \mathrm{Id} = (g_{k,l} - \delta_{k,l})_{k,l}$ en lugar de g es para obtener un polinomio sin término constante. En efecto, $P_{i,j}(0) = \rho_{i,j}(\mathrm{Id}) - \delta_{i,j} = 0$ para todo i, j ya que $\rho(\mathrm{Id}) = \mathrm{Id}$.

Sea $N \in \mathbb{N}$ elegido de modo que el polinomio $NP_{i,j}$ tenga coeficientes enteros para todo i, j. Supongamos $g \in \mathbf{G}_{\mathbb{Z}}(N)$, entonces $g_{k,l} - \delta_{k,l} \equiv 0 \pmod{N}$ para todo $1 \leq k, l \leq n$. Como $P_{i,j}$ no tiene término constante, obtenemos que $P_{i,j}(g - \mathrm{Id}) \in \mathbb{Z}$ para todo i, j. Luego $\rho_{i,j}(g) \in \mathbb{Z}$ para todo $g \in \mathbf{G}_{\mathbb{Z}}(N)$, lo que significa que $\rho(g) \cdot L \subset L$. Como $\mathbf{G}_{\mathbb{Z}}(N)$ es un grupo, $\rho(g) \cdot L = L$ para todo $g \in \mathbf{G}_{\mathbb{Z}}(N)$. Esto prueba (i).

Para la segunda afirmación, tomamos cualquier retículo L en $V_{\mathbb{Q}}$. Por (i), existe un subgrupo de índice finito Γ de $\mathbf{G}_{\mathbb{Z}}$ que deja estable a L. Sean $\{\gamma_1, \ldots, \gamma_r\}$ representantes de $\mathbf{G}_{\mathbb{Z}}/\Gamma$, y definimos

$$L' := \sum_{k=1}^{r} \rho(\gamma_k)(L).$$

Se puede ver que L' es discreto (Ejercicio 3.8). Además, claramente L' es invariante por $\rho(\mathbf{G}_{\mathbb{Z}})$, lo que prueba (ii). □

Proposición 3.14. *Sea $\boldsymbol{G}$ un subgrupo algebraico de $\mathrm{GL}(V)$ definido sobre $\mathbb{Q}$. Si L y L' son dos retículos en $V_{\mathbb{Q}}$, entonces $\boldsymbol{G}_L$ y $\boldsymbol{G}_{L'}$ son conmensurables.*

Demostración. Por la Proposición 3.13 (i) con ρ la identidad, existe un subgrupo Γ de índice finito en $\mathbf{G}_{\mathbb{Z}}$ que deja invariante a L'. Por lo tanto $\Gamma \subset \mathbf{G}_{L'}$, luego $\Gamma \subset \mathbf{G}_L \cap \mathbf{G}_{L'} \subseteq \mathbf{G}_L$, lo que implica que $\mathbf{G}_L \cap \mathbf{G}_{L'}$ es de índice finito en $\mathbf{G}_L$. Intercambiando L con L' se ve que $\mathbf{G}_L \cap \mathbf{G}_{L'}$ es de índice finito también en $\mathbf{G}_{L'}$. □

Nota 3.15. A raíz de la proposición anterior, concluimos que todos los subgrupos aritméticos de un $\mathbb{Q}$-grupo algebraico fijo $\mathbf{G} \subset \mathrm{GL}(V)$ son conmensurables. En efecto, cada uno de ellos es conmensurable a $\mathbf{G}_L$ para cualquier L retículo de $V_{\mathbb{Q}}$, y la conmensurabilidad es transitiva (ver Ejercicio 2.7). En particular, todos los subgrupos aritméticos serán cocompactos o no cocompactos simultáneamente.

Corolario 3.16. *Sea $\varphi : \boldsymbol{G} \to \boldsymbol{G}'$ un $\mathbb{Q}$-isomorfismo de $\mathbb{Q}$-grupos algebraicos. Si Γ es un subgrupo aritmético de $\boldsymbol{G}$, entonces $\varphi(\Gamma)$ es un subgrupo aritmético de $\boldsymbol{G}'$.*

El siguiente teorema es uno de los resultados fundamentales sobre grupos aritméticos.

Teorema 3.17. *Sea $\boldsymbol{G} \subset \mathrm{GL}_n(\mathbb{C})$ un grupo algebraico semisimple definido sobre $\mathbb{Q}$. Entonces $\boldsymbol{G}_{\mathbb{R}}/\boldsymbol{G}_{\mathbb{Z}}$ tiene medida de Haar finita.*

En particular, este resultado asegura que todo subgrupo aritmético en $\mathbf{G}$ es un retículo en $\mathbf{G}_{\mathbb{R}}$. Su demostración, debida a Borel y Harish-Chandra [3], es muy técnica y extensa. En la siguiente sección, demostraremos el caso particular de $\mathrm{SL}_n(\mathbb{Z})$ como retículo de $\mathrm{SL}_n(\mathbb{R})$ usando los llamados dominios de Siegel. El caso general se basa en una generalización de estos dominios a grupos arbitrarios.

Ejemplo 3.18. Sea $J = \mathrm{diag}(2, 3, -1)$ y definamos $B : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$ la forma bilineal dada por $B(x, y) = 2x_1y_1 + 3x_2y_2 - x_3y_3$ para $x = (x_1, x_2, x_3)^t, y = (y_1, y_2, y_3)^t \in \mathbb{R}^3$. Claramente B es no degenerada, aunque no es definida positiva sino que es indefinida de signatura $(2, 1)$. El grupo $\mathrm{O}(J)_{\mathbb{Z}}$ está dado por matrices enteras g cuyas columnas $g_1, g_2, g_3 \in \mathbb{Z}^3$ cumplen $B(g_1, g_1) = 2$, $B(g_2, g_2) = 3$, $B(g_3, g_3) = -1$, y $B(g_i, g_j) = 0$ para $i \neq j$.

No es fácil mostrar que $\mathrm{O}(J)_{\mathbb{Z}}$ tiene una cantidad infinita de elementos (cf. Ejercicio 3.10). El Teorema 3.17 nos dice que $\mathrm{O}(J)_{\mathbb{Z}}$ es un retículo en el grupo de Lie no compacto $\mathrm{O}(J)_{\mathbb{R}}$, lo cual implica en particular que $\mathrm{O}(J)_{\mathbb{Z}}$ debe tener una cantidad infinita de puntos (Ejercicio 2.5).

3.3. Ejemplos de grupos aritméticos. Terminamos esta sección con una serie de ejemplos particulares de grupos aritméticos.

Ejemplo 3.19. Como ya hemos visto, $\mathrm{SL}_n(\mathbb{Z})$ (y cualquier subgrupo de $\mathrm{SL}_n(\mathbb{Q})$ conmensurable a él) es un subgrupo aritmético de $\mathbf{G} = \mathrm{SL}_n(\mathbb{C})$. Por lo tanto, $\mathrm{SL}_n(\mathbb{Z})$ es un retículo de $\mathbf{G}_\mathbb{R} = \mathrm{SL}_n(\mathbb{R})$. En la próxima sección mostraremos que no es cocompacto.

Ejemplo 3.20. De manera similar al ejemplo anterior, se tiene que $\mathrm{SL}_2(\mathbb{Z}[\sqrt{-1}])$ es un retículo en el grupo de Lie (real) $\mathrm{SL}_2(\mathbb{C})$. Para ello, es necesario mostrar un $\mathbb{Q}$-grupo algebraico $\mathbf{G}$ cuyos puntos reales sean $\mathbf{G}_\mathbb{R} = \mathrm{SL}_n(\mathbb{C})$. Lo mismo vale cuando reemplazamos los enteros de Gauss $\mathbb{Z}[\sqrt{-1}]$ por los enteros algebraicos $\mathcal{O}_\mathbb{K}$ de cualquier extensión cuadrática imaginaria $\mathbb{K}$ de $\mathbb{Q}$. Estos grupos aritméticos son conocimos como los *grupos de Bianchi*.

Ejemplo 3.21. Ahora mostraremos que $\mathrm{SL}_2(\mathbb{Z}[\sqrt{2}])$ es un grupo aritmético, es decir, construiremos un $\mathbb{Q}$-grupo algebraico $\mathbf{G} \subset \mathrm{GL}(V)$ y un retículo en L en $V_\mathbb{Q}$ tal que $\mathbf{G}_L$ es isomorfo a $\mathrm{SL}_2([\sqrt{2}])$. Notar que $\mathbf{G}_\mathbb{R}$ no puede ser $\mathrm{SL}_2(\mathbb{R})$, ya que $\mathrm{SL}_2(\mathbb{Z}[\sqrt{2}])$ ni siquiera es discreto con la topología relativa (Ejercicio 3.11).

Por supuesto, $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \sqrt{2}\mathbb{Z}$. Tomemos en $V = \mathbb{C}^2 \times \mathbb{C}^2$ la $\mathbb{Q}$-forma dada por

$$V_\mathbb{Q} = \{(v + \sqrt{2}w, v - \sqrt{2}w) : v, w \in \mathbb{Q}^2\}.$$

Sea

$$G = \left\{ g = \left(\begin{smallmatrix} g_1 & g_2 \\ g_3 & g_4 \end{smallmatrix}\right) \in \mathrm{GL}(\mathbb{C}^2 \times \mathbb{C}^2) : \det(g_1) = \det(g_4) = 1,\ g_2 = g_3 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \right\},$$

el cual claramente es un grupo algebraico definido sobre $\mathbb{Q}$. Además, es isomorfo (como grupo abstracto) a $\mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C})$, y $\mathbf{G}_\mathbb{R} \simeq \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$ como grupos de Lie.

Sea

$$L = \{(v + \sqrt{2}w, v - \sqrt{2}w) : v, w \in \mathbb{Z}^2\}.$$

Resta ver que $\mathrm{SL}_2(\mathbb{Z}[\sqrt{2}])$ puede ser identificado con $\mathbf{G}_L$. En efecto, si $\sigma : \mathbb{Q}[\sqrt{2}] \to \mathbb{C}$ denota la inmersión no trivial (i.e. $\sigma(a + \sqrt{2}b) = a - \sqrt{2}b$ para $a, b \in \mathbb{Q}$), y la extendemos a las matrices 2×2, entonces

$$g \mapsto \begin{pmatrix} g & 0 \\ 0 & \sigma(g) \end{pmatrix}$$

identifica $\mathrm{SL}_2(\mathbb{Z}[\sqrt{2}])$ con $\mathbf{G}_L$.

Los tres ejemplos anteriores pueden ser enmarcados dentro de un método general llamado *restricción de escalares* que ahora describiremos sin precisar mayores detalles (ver [15, §5E]). Sea $\mathbb{K}$ un cuerpo de números (i.e. una extensión finita de $\mathbb{Q}$) con r inmersiones reales y $2s$ inmersiones complejas, y sea $\mathbf{G} \subset \mathrm{GL}_n(\mathbb{C})$ un grupo algebraico definido sobre $\mathbb{K}$. Entonces existe un $\mathbb{Q}$-grupo algebraico $\mathbf{G}' \subset \mathrm{GL}_m(\mathbb{C})$, con $m = n(r + 2s)$, tal que $\mathbf{G}_{\mathcal{O}_\mathbb{K}} = \mathbf{G} \cap \mathrm{GL}_n(\mathcal{O}_\mathbb{K})$ se identifica de una manera natural con $\mathbf{G}'_\mathbb{Z}$ usando las inmersiones de $\mathbb{K}$ a $\mathbb{C}$. Más aún, $\mathbf{G}'_\mathbb{R} \subset \mathrm{GL}_n(\mathbb{R})^r \times \mathrm{GL}_n(\mathbb{C})^s$.

Un buen ejercicio puede ser intuir cómo definir $\mathbf{G}'$, en términos de una familia de polinomios con coeficientes en $\mathbb{K}$ que definen $\mathbf{G}$.

En la siguiente sección estudiaremos condiciones para que el subgrupo aritmético $\mathrm{O}(J)_\mathbb{Z}$ como en Ejemplo 3.6 sea cocompacto en $\mathrm{O}(J)_\mathbb{R}$. Otro método muy usado para construir subgrupos aritméticos Γ en $\mathrm{SL}_2(\mathbb{R})$ y $\mathrm{SL}_2(\mathbb{C})$ utiliza las álgebras de cuaterniones. Se darán más detalles en las últimas secciones, donde propiedades aritméticas de estas álgebras se relacionarán con propiedades geométricas de los cocientes H^2/Γ y H^3/Γ respectivamente.

3.4. Ejercicios.

Ejercicio 3.1. Sea V un subespacio de $\mathbb{R}^n$. Probar que las siguientes afirmaciones son equivalentes:

1. $V \cap \mathbb{Z}^n$ es un retículo cocompacto en V.
2. V es generado por $V \cap \mathbb{Z}^n$.
3. $V \cap \mathbb{Q}^n$ es denso en V.
4. V puede ser definido por un conjunto de ecuaciones lineales con coeficientes racionales

Ejercicio 3.2. Sea $V_{\mathbb{K}}$ una $\mathbb{K}$-forma en el $\mathbb{C}$-espacio vectorial V. Mostrar que $\mathrm{End}(V)_{\mathbb{K}} := \{T \in \mathrm{End}_{\mathbb{C}}(V) : T(V_{\mathbb{K}}) \subset V_{\mathbb{K}}\}$ es una $\mathbb{K}$-forma de $\mathrm{End}_{\mathbb{C}}(V)$, y que $\mathrm{End}(V)_{\mathbb{K}} \simeq \mathrm{End}_{\mathbb{K}}(V_{\mathbb{K}})$ como $\mathbb{K}$-espacio vectorial.

Ejercicio 3.3. Sea $\mathbb{K}$ un subcuerpo de $\mathbb{C}$, sea $V_{\mathbb{K}}$ una $\mathbb{K}$-forma del espacio vectorial V sobre $\mathbb{C}$ con base $\{v_1, \ldots, v_n\}$. Si $P : V \to \mathbb{C}$ es una función polinomial, entonces

$$P(a_1 v_1 + \ldots + a_n v_n) = \sum_{\alpha=(i_1,\ldots,i_n)} c_\alpha a_1^{i_1} \ldots a_n^{i_n},$$

con $c_\alpha \in \mathbb{C}$ todos nulos salvo una cantidad finita. Mostrar que $P(v) \in \mathbb{K}$ para todo $v \in V_{\mathbb{K}}$ si y sólo si $c_\alpha \in \mathbb{K}$ para todo α.

Ejercicio 3.4. Sea Z una variedad algebraica. Mostrar que Z está definida sobre $\mathbb{K}$ si y sólo si Z es el conjunto de ceros de una familia de polinomios en $\mathbb{K}[V]$.

Ejercicio 3.5. Sea $\mathbb{K}$ un subcuerpo de $\mathbb{C}$. Demostrar que si $\mathbf{G} \subset \mathrm{GL}(m, \mathbb{C})$ y $\mathbf{H} \subset \mathrm{GL}(m, \mathbb{C})$ son grupos algebraicos sobre $\mathbb{K}$, entonces $\mathbf{G} \times \mathbf{H}$ también lo es.

Ejercicio 3.6. Probar que los grupos $\mathrm{O}(J)$ y $\mathrm{O}(p, q)$ como en Nota 3.8 son conjugados. Para J como en Ejemplo 3.7, dar explícitamente la matriz que conjuga $\mathrm{O}(J)$ en $\mathrm{O}(p, q)$. Notar que en general sus coeficientes no son racionales, por lo que la conjugación por ella no es un $\mathbb{Q}$-morfismo.

Ejercicio 3.7. Mostrar que el subgrupo principal de congruencia $\mathbf{G}_{\mathbb{Z}}(N)$ de nivel N (ver Definición 3.12) tiene índice finito en $\mathbf{G}_{\mathbb{Z}}$.

Ejercicio 3.8. Probar que L' es un retículo en la demostración de la Proposición 3.13. Ayuda: Es suficiente mostrar que es discreto, para lo cual hay que encontrar $m \in \mathbb{Z}$ tal que $mL' \subset L$.

Ejercicio 3.9. Demostrar el Corolario 3.16.

Ejercicio 3.10. Mostrar (sin usar el Teorema 3.17) que $\mathrm{O}(J)_{\mathbb{Z}}$ como en el Ejemplo 3.18 tiene infinitos elementos.

Ejercicio 3.11. Mostrar que $\mathrm{SL}_2(\mathbb{Z}[\sqrt{2}])$ no es discreto en $\mathrm{SL}_2(\mathbb{R})$.

4. Dominios de Siegel

El objetivo de esta sección es construir ciertos dominios fundamentales aproximados para la acción de $\mathrm{GL}_n(\mathbb{Z})$ en $\mathrm{GL}_n(\mathbb{R})$ llamados conjuntos de Siegel.

Borel y Harish-Chandra [3] generalizaron esta construcción a todo subgrupo aritmético de un grupo algebraico semisimple $\mathbf{G}$ definido sobre los números racionales, demostrando que $\mathbf{G}_{\mathbb{Z}}$ tiene covolumen finito en el grupo de Lie $\mathbf{G}_{\mathbb{R}}$ (Teorema 3.17), es decir, es un retículo $\mathbf{G}_{\mathbb{R}}$.

Los conjunto de Siegel tiene aplicaciones a la teoría de reducción de formas cuadráticas, tal como lo mostraremos en la Subsección 4.2.

4.1. Descomposición de Iwasawa. En el resultado siguiente se describe la llamada descomposición de Iwasawa $G = KAN$ del grupo $G = \mathrm{GL}_n(\mathbb{R})$. La misma continúa válida para todo grupo de Lie semisimple real.

Proposición 4.1. *Sean $G = \mathrm{GL}_n(\mathbb{R})$, $K = \mathrm{O}(n)$ el subgrupo de matrices ortogonales, A el subgrupo de matrices diagonales con entradas positivas, y N el subgrupo de matrices unipotentes triangulares superiores. Entonces la función $\Phi : K \times A \times N \to G$, dada por $\Phi(k, a, n) = kan$ es un difeomorfismo.*

Demostración. Veamos primero la inyectividad de Φ. Si $g = kan = k'a'n'$ con $k, k' \in \mathrm{O}(n)$, $a, a' \in A$ y $n, n' \in N$, entonces $k'^{-1}k = a'n'n^{-1}a^{-1}$ es triangular superior con entradas diagonales positivas. Como $k'^{-1}k \in \mathrm{O}(n)$ y además $an = a'n'$ (Ejercicio 4.1), o sea $a'^{-1}a = n'n^{-1}$. Como $n'n^{-1}$ es diagonal con 1's en la diagonal se deduce que $a' = a$, $n' = n$ y $k' = k$.

Ahora definiremos la inversa de Φ. Sea $g \in \mathrm{GL}_n(\mathbb{R})$ y sean $v_i = g^{-1}e_i$ donde $e_1, \ldots, e_n$ es la base canónica de $\mathbb{R}^n$. Aplicamos el método de Gram-Schmidt a $v_1, \ldots, v_n$. Definamos $u_1 = \|v_1\|^{-1}v_1$ e inductivamente, sean

$$u_{k+1} = \left\| v_{k+1} - \sum_{j=1}^{k} \langle v_{k+1}, u_j \rangle u_j \right\|^{-1} \left(v_{k+1} - \sum_{j=1}^{k} \langle v_{k+1}, u_j \rangle u_j \right).$$

Entonces $u_i = \sum_{j \le i} a_{ji} v_j$, donde la matriz a_{ij} es triangular superior y $a_{ii} > 0$ para todo i. Esto define $a(g) \in A$ y $n(g) \in N$ tales que $(a_{ij})_{ij} = a(g)n(g)$ y $k(g) \in \mathrm{O}(n)$ de modo que para todo i, $a(g)n(g)g^{-1}e_i = k(g)^{-1}e_i$.

Se tiene así que $g = k(g)a(g)n(g)$, luego la función $\Psi : g \mapsto (k(g), a(g), n(g))$ es la inversa de Φ. Claramente Φ y Ψ son continuas, luego Φ es un homeomorfismo. Además Φ y Ψ son diferenciables. Omitiremos esta última verificación. □

Definición 4.2. Sean $t, u > 0$. Un conjunto de Siegel en $\mathrm{GL}_n(\mathbb{R})$ es un conjunto de la forma $\mathcal{S}_{t,u} = KA_tN_u$, donde

$$A_t = \{a \in A : a_{i,i} \le t a_{i+1,i+1} \quad i = 1, \ldots, n-1\},$$
$$N_u = \{n \in N : |n_{i,j}| \le u \quad 1 \le i < j \le n\}.$$

Nota 4.3. Recordemos que N es difeomorfo a $\mathbb{R}^{n(n-1)/2}$ y $A \cong (\mathbb{R}^*)^n$. Observemos también que si $\omega \subset N$ es relativamente compacto, entonces el conjunto

$$\bigcup_{a \in A_t} a\omega a^{-1}$$

es también relativamente compacto. En efecto, si $n = (n_{i,j}) \in \omega$, entonces $(ana^{-1})_{i,j} = \frac{a_{i,i}}{a_{j,j}} n_{i,j}$. Luego

$$|(ana^{-1})_{i,j}| \le t^{j-i} |n_{i,j}|$$

para todo $i < j$.

Para cada $a \in A$, sea σ_a el automorfismo de N dado por $\sigma_a(n) = ana^{-1}$. Entonces se verifica que $|\det(\sigma_a)| = \prod_{i<j} a_{i,i}/a_{j,j}$.

El siguiente es uno de los principales resultados de la sección.

Teorema 4.4. *Sea $G = \mathrm{GL}_n(\mathbb{R})$ y $\Gamma = \mathrm{GL}_n(\mathbb{Z})$. Entonces $G = \mathcal{S}_{t,u}\Gamma$ para todo $t \ge 2/\sqrt{3}$ y $\|u\| \le 1/2$.*

Demostración. En primer lugar vemos que

$$N = N_{1/2}N_{\mathbb{Z}}, \tag{4.1}$$

donde $N_{\mathbb{Z}} = N \cap \mathrm{GL}_n(\mathbb{Z})$. En efecto, si $u \in N, z \in N_{\mathbb{Z}}$, entonces

$$(uz)_{i,j} = z_{i,j} + u_{i,i+1}z_{i+1,j} + \ldots + u_{i,j}$$

para $1 \leq i < j \leq n$, lo que permite definir $z_{i,j}$ por recurrencia desde $z_{n-1,n}$.

Definamos $\Phi : G \to \mathbb{R}^+$ dada por $\Phi(g) = \|ge_1\|$. Claramente $\Phi(kan) = \|ae_1\| = a_{1,1} = \Phi(a)$. Si $g \in G$ fijo, la función $z \to \Phi(gz)$ con $z \in \Gamma$ tiene un mínimo positivo en Γ pues $\{g\gamma e_1 : \gamma \in \Gamma\}$ es un subconjunto de elementos no nulos del retículo $g(\mathbb{Z}^n)$. Notar también que para $u \in N_{\mathbb{Z}}$ se verifica que $\Phi(gu)\Phi(g)$ y $a_{gu} = a_g$.

Afirmación 1. *Si $\Phi(g) \leq \Phi(g\gamma)$ para todo $\gamma \in \Gamma$, entonces $a_{1,1} \leq (2/\sqrt{3})a_{2,2}$.*

Demostración. En efecto, sea $\sigma \in \Gamma$ que permuta e_1 y e_2 y fija los otros e_i. Entonces

$$g\sigma(e_1) = g(e_2) = ka(e_2 + n_{1,2}e_1) = k(a_{2,2}e_2 + a_{1,1}n_{1,2}e_1).$$

Luego $\|g\sigma(e_1)\|^2 = a_{2,2}^2 + a_{1,1}^2 n_{1,2}^2 \leq a_{1,1}^2/4 + a_{2,2}^2$. Entonces

$$\Phi(g)^2 = a_{1,1}^2 \leq a_{1,1}^2/4 + a_{2,2}^2,$$

lo que implica la afirmación. ■

Afirmación 2. *Si $g \in G$, el mínimo de Φ en $g\Gamma$ se alcanza en $g\Gamma \cap \mathcal{S}_{2/\sqrt{3},1/2}$.*

Demostración. Probaremos la afirmación por inducción. Si $n = 1$ no hay nada que probar.

Si $x \in G$, existe $y \in x\Gamma$ tal que $\Phi(y) \leq \Phi(x\gamma)$ para todo $\gamma \in \Gamma$. Fijemos tal y. Escribamos $k_y^{-1}y = \left[\begin{smallmatrix} a_{1,1} & * \\ 0 & b \end{smallmatrix}\right]$, con $b \in \mathrm{GL}_{n-1}(\mathbb{R})$. Entonces, por hipótesis inductiva, existe $z' \in \mathrm{GL}_{n-1}(\mathbb{Z})$ tal que $bz' \in \mathcal{S}^{n-1}_{2/\sqrt{3},1/2}$.

Escribamos $bz' = k'a'n'$. Luego

$$k_y{}^{-1}yz = \begin{bmatrix} a_{1,1} & * \\ 0 & k'a'n' \end{bmatrix} = k''a''n'',$$

con $z = \left[\begin{smallmatrix} 1 & 0 \\ 0 & z' \end{smallmatrix}\right]$, $k'' \in K$, $a'' = \left[\begin{smallmatrix} a_{1,1} & 0 \\ 0 & a' \end{smallmatrix}\right]$ y $n'' = \left[\begin{smallmatrix} 1 & * \\ 0 & n' \end{smallmatrix}\right] \in N$ y donde $a_{i,i} \leq (2/\sqrt{3})a_{i+1,i+1}$ para todo i. Además $\Phi(yz) = \Phi(y)$ y $\Phi(yz) \leq \Phi(yz\gamma)$ para todo γ.

Como además por la Afirmación 1 se tiene que $a''_{1,1} \leq (2/\sqrt{3})a''_{2,2}$, resulta que $yz \in KA_{2/\sqrt{3}}N$, luego usando (4.1), $x \in y\Gamma \subset KA_{2/\sqrt{3}}N_{1/2}\Gamma = \mathcal{S}_{2/\sqrt{3},1/2}\Gamma$, lo que prueba la afirmación. ■

Claramente, la Afirmación 2 completa la demostración del teorema. □

En el caso de $G = \mathrm{SL}_n(\mathbb{R})$, la descomposición de Iwasawa es la misma que para $\mathrm{GL}_n(\mathbb{R})$, es decir $\mathrm{SL}_n(\mathbb{R}) = \mathrm{SO}(n)A^*N$, con $A^* = \mathrm{SL}_n(\mathbb{R}) \cap A$. El conjunto de Siegel $\mathcal{S}^*_{t,u}$ para $\mathrm{SL}_n(\mathbb{R})$ se define igual que en el caso de $\mathrm{GL}_n(\mathbb{R})$ y se tiene $S^*_{t,u} = \mathrm{SL}_n(\mathbb{R}) \cap S_{t,u}$.

El siguiente resultado nos dice que una medida de Haar invariante a izquierda en G está dada por $\rho(a)dkdadn$ donde $\rho(a) = \prod_{i<j} a_{i,i}/a_{j,j}$.

Proposición 4.5. *Sean $G = \mathrm{GL}_n(\mathbb{R})$, K, A y N como en Proposición 4.1, y sean dk, da, dn medidas de Haar en K, A y N respectivamente. Entonces existe $C > 0$ tal que para toda $f \in C_c(G)$,*

$$\int_G f(g)\,dg = C \int_{K\times A\times N} f(kan) \left(\prod_{i<j} a_{i,i}/a_{j,j}\right) dk\,da\,dn.$$

Demostración. Por la fórmula del cambio de variable, existe una función suave $h(k,a,n)$ tal que

$$\int_G f(g)\,dg = \int_{K\times A\times N} f(kan)h(k,a,n)\,dk\,da\,dn.$$

Como dg es invariante a izquierda y a derecha, h es independiente de k y n. Entonces podemos escribir $h(k,a,n) = h(a)$. Luego

$$\int_G f(g)\,dg = \int_{K\times A\times N} f(kan)h(a)\,dk\,da\,dn. \tag{4.2}$$

Ahora, si $a_0 \in A$,

$$\begin{aligned}\int_G f(g)\,dg = \int_G f(ga_0)\,dg &= \int_{K\times A\times N} f(kana_0)h(a)\,dk\,da\,dn \\ &= \int_{K\times A\times N} f(kan)h(aa_0{}^{-1})|\det(jac(n\to a_0na_0^{-1})\,dk\,da\,dn \\ &= \int_{K\times A\times N} f(kan)h(aa_0{}^{-1})\prod_{i<j} a_{0i,i}/a_{0j,j}\,dk\,da\,dn.\end{aligned} \tag{4.3}$$

Por lo tanto, de (4.2) y (4.3) resulta que

$$h(a) = h(aa_0{}^{-1})\prod_{i<j} a_{0i,i}/a_{0j,j}$$

para todo $a, a_0 \in A$. Tomando $a = a_0$ se tiene que $h(a_0) = h(e)\prod_{i<j} a_{0i,i}/a_{0j,j}$, lo que prueba el lema. □

Proposición 4.6. *El volumen de un conjunto de Siegel $\mathcal{S}^*_{t,u}$ en $\mathrm{SL}_n(\mathbb{R})$ con respecto a la medida de Haar es finito.*

Demostración. Si $K^* = \mathrm{SO}(n)$ y $B^* = A^*N$, sean dk, da, dn medidas de Haar en K^*, A^* y N, todas biinvariantes ya que estos grupos son unimodulares. De manera análoga a Proposición 4.5, $\rho(a)dkdadn$, con $\rho(a) = \prod_{i<j} a_{i,i}/a_{j,j}$, es una medida de Haar en $G = \mathrm{SL}_n(\mathbb{R})$.

Se tiene entonces que existen $r_i \in \mathbb{N}$ y $C_u > 0$ tales que

$$(C_u)^{-1}\int_{\mathcal{S}_{t,u}} dg \le \int_{A_t}\rho(a)da = \int_{A_t}\prod(a_{i,i}/a_{i+1,i+1})^{r_i}da = \prod_{1\le i<n}\int_{-\infty}^{log(t)}(\exp\, r_iy_i)\,dy_i,$$

el cual es claramente finito, lo que completa la demostración. □

4.2. Teoría de reducción de formas cuadráticas.

Corolario 4.7. *(Hermite) Si $g \in G$, entonces*

$$\min_{\lambda\in\mathbb{Z}^n\smallsetminus\{0\}}\|g(\lambda)\| \le (2/\sqrt{3})^{(n-1)/2}\,|\det(g)|^{1/n}.$$

Demostración. Sea $g' \in g\Gamma \cap \mathcal{S}_{2/\sqrt{3},1/2}$. Se tiene

$$\min_{\lambda\in\mathbb{Z}^n\smallsetminus\{0\}}\|g(\lambda)\| \le \min_{\gamma\in\Gamma}\|g\gamma(e_1)\| = \|g'(e_1)\| = a'_{1,1},$$

donde $g' = k'a'n'$ es la descomposición de Iwasawa de g'. Luego

$$(a'_{1,1})^n \le (a'_{1,1})^{n-1}(2/\sqrt{3})\,a'_{2,2} \le (2/\sqrt{3})^{n(n-1)/2}\,a'_{1,1}a'_{2,2}\dots\dots a'_{n,n}.$$

□

En particular, existe $C > 0$ tal que

$$\min_{\lambda\in\mathbb{Z}^n\smallsetminus\{0\}}\|g(\lambda)\| \le C\,|\det(g)|^{1/n}.$$

4.3. Ejercicios.

Ejercicio 4.1. Mostrar que una matriz real triangular superior con entradas diagonales positivas que a su vez es ortogonal, es necesariamente la matriz identidad.

5. Criterio de compacidad

En esta sección daremos un criterio de compacidad de G/Γ, donde Γ es un retículo en un grupo de Lie semisimple G.

5.1. Espacio de retículos. Denotaremos $\mathcal{L}$ el espacio de retículos de $\mathbb{R}^n$. Sea la aplicación $\mathrm{GL}_n(\mathbb{R}) \to \mathcal{L}$ dada por $g \mapsto g(\mathbb{Z}^n)$. Se ve fácilmente que ésta es suryectiva. Además, si $g(\mathbb{Z}^n) = h(\mathbb{Z}^n)$ para $g, h \in \mathrm{GL}_n(\mathbb{R})$, entonces $h^{-1}g(\mathbb{Z}^n) = \mathbb{Z}^n$ y por lo tanto $h^{-1}g \in \mathrm{GL}_n(\mathbb{Z})$ y en consecuencia tenemos la identificación $\mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z}) \simeq \mathcal{L}$. Damos a $\mathcal{L}$ la topología inducida por esta identificación.

La siguiente proposición ayuda a comprender la topología de $\mathcal{L}$.

Proposición 5.1. *Una sucesión $\{L_n\}_{n=1}^{\infty}$ en $\mathcal{L}$ converge a L_0 si y sólo si existe una base $\mathcal{B}_n := \{v_1^{(n)}, \dots, v_d^{(n)}\}$ de L_n para cada $n \in \mathbb{N}_0$ tal que $v_i^{(n)} \to v_i^{(0)}$ para cada $1 \leq i \leq n$.*

Demostración. Denotamos $\pi : \mathrm{GL}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z})$ la proyección canónica; π es abierta pues si U es abierto, $\pi^{-1}\pi(U) = \bigcup_{A \in \mathrm{GL}_n(\mathbb{Z})} A \cdot U$ es abierto.

Sea $g_m \in \mathrm{GL}_n(\mathbb{Z})$ tal que $f(\pi(g_m)) = L_m$. Luego $\pi(g_m) \to \pi(g_0)$. Sea U un abierto de $\mathrm{GL}_n(\mathbb{R})$ que contiene a g_0, luego existe $N \in \mathbb{N}$ tal que $\pi(g_m) \in \pi(U)$ para todo $m \geq N$. Entonces $g_m \in \pi^{-1}\pi(U)$, por lo tanto existen $h_m \in \mathrm{GL}_n(\mathbb{Z})$ tal que $h_m^{-1}g_m \in U$ para todo $m \geq N$, o equivalentemente, $h_m^{-1}g_m \to g_0$. Si $m \geq 0$, definimos $v_i^{(m)}$ la i-ésima columna de la matriz $h_m^{-1}g_m$, donde $h_0 = \mathrm{Id}$. Se tiene claramente que $v_i^{(m)} \to v_i^{(0)}$ para $1 \leq i \leq n$, luego las bases $\langle_n = \{v_1^{(m)}, \dots, v_n^{(m)}\}$ tienen la propiedades requeridas.

Ahora consideremos la recíproca. Para cada $m \geq 0$ sea

$$g_m = \begin{pmatrix} | & & | \\ v_1^{(m)} & \cdots & v_d^{(m)} \\ | & & | \end{pmatrix}.$$

Como $v_i^{(m)} \to v_i^{(0)}$, se tiene que $g_m \to g_0$ en el espacio de matrices reales $n \times n$, luego $\pi(g_m) \to \pi(g_0)$ en $\mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z})$ y como $L_m = g_m\mathbb{Z}^n$, resulta que $L_m \to L_0$. □

Para cada $L \in \mathcal{L}$, definamos $\Delta(L) = |\det(v_1, \dots, v_n)|$ para cualquier base $\{v_1, \dots, v_n\}$ de L (ver Ejercicio 5.1 para la buena definición).

Teorema 5.2. *(Criterio de Mahler) Para $\mathcal{M} \subset \mathcal{L}$, las siguientes afirmaciones son equivalentes:*

(i) *$\mathcal{M}$ es relativamente compacto,*
(ii) *$\Delta|_{\mathcal{M}}$ está acotada y existe U un entorno abierto de 0 en $\mathbb{R}^n$ tal que $L \cap U = \{0\}$ para todo $L \in \mathcal{M}$.*

Demostración. Sea $\mathcal{S}_{t,u}$ un conjunto de Siegel mapeado sobre $\mathcal{L}$ por la aplicación $g \mapsto g(L_0)$ con $L_0 = \mathbb{Z}^n$. Es claro que (i) equivale a la existencia de $M' \subset S_{t,u}$ relativamente compacto tal que $M'(L_0) = \mathcal{M}$.

Por otra parte, por la definición de $S_{t,u}$, $M' \subset S$ es relativamente compacto si y sólo si las componentes a_x, $x \in M'$ forman un subconjunto relativamente compacto de A. Esto es, si y sólo si existen constantes $\alpha, \beta > 0$ tales que

$$\alpha \leq (a_g)_{i,i} \leq \beta \quad g \in M' \tag{5.1}$$

para todo $1 \leq i \leq n$.

Por otro lado, (ii) equivale a decir que $g \mapsto |\det(g)|$ está acotado en M' y existe $c > 0$ tal que $\|g(\lambda)\| \geq c$ para todo $g \in M'$ y $\lambda \in \mathbb{Z}^n$. Teniendo en cuenta estas equivalencias, veremos que las condiciones (i) y (ii) son equivalentes.

Supongamos que (i) es cierta. Claramente $|\det(M')| < C$. Sea $\lambda \in \mathbb{Z}^n \smallsetminus \{0\}$, $\lambda = \sum_1^n m_i e_i$ con $m_k \neq 0$. Entonces $\|g(\lambda)\| = \|a_g n_g(\lambda)\|$ y la k-ésima coordenada de $a_g n_g(\lambda)$ es $(a_g)_{k,k} m_k$ lo cual implica que $\|g(\lambda)\| \geq \alpha$, y por lo tanto (ii) es válida.

Asumiendo (ii), tenemos que $\|g(e_1)\| = (a_g)_{1,1} \geq c$. Como $a_g \in A_t$, esto implica que existe $\alpha > 0$ tal que $(a_g)_{i,i} \geq \alpha$ para todo i. Como el producto de los $(a_g)_{i,i}$ está acotado, se obtiene (5.1). □

5.2. Criterio de compacidad. Para probar los resultados principales de la sección, serán de suma utilidad los siguientes lemas.

Lema 5.3. *(Jacobson-Morosov) Sea G un grupo de Lie real conexo semisimple con centro finito. Para todo elemento unipotente $u \in G$, existe un homomorfismo continuo $\varphi : \mathrm{SL}(2,\mathbb{R}) \to G$ tal que*

$$\varphi\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right) = u.$$

Lema 5.4. *Sea $\boldsymbol{G} \subset \mathrm{GL}_n(\mathbb{C})$ un subgrupo algebraico definido sobre $\mathbb{Q}$ sin $\mathbb{Q}$-caracteres no triviales (i.e. todo $\mathbb{Q}$-morfismo desde $\boldsymbol{G}$ a $\mathrm{GL}_1(\mathbb{C}) \simeq \mathbb{C}^\times$ es trivial). Supongamos que existe un polinomio $\boldsymbol{G}$-invariante $P \in \mathbb{Q}[x_1, \ldots, x_n]$ tal que*

$$\text{si } v \in \mathbb{Q}^n, \quad P(v) = 0 \iff v = 0.$$

Entonces $\boldsymbol{G}_\mathbb{R}/\boldsymbol{G}_\mathbb{Z}$ es compacto.

Demostración. Escribimos

$$P(x_1, \ldots, x_n) = \sum_{\alpha=(\alpha_1,\ldots,\alpha_d)} a_\alpha \, x_1^{\alpha_1} \ldots x_d^{\alpha_d},$$

con $a_\alpha \in \mathbb{Q}$ para todo α. Como $P(0) = 0$, $a_{(0,\ldots,0)} = 0$, es decir, P no tiene término constante. Sea $m \in \mathbb{N}$ tal que $m a_\alpha \in \mathbb{Z}$ para todo α. Entonces $P(mx_1, \ldots, mx_n) \in \mathbb{Z}$ si $x_i \in \mathbb{Z}$ para todo i, o equivalentemente $P(m\mathbb{Z}^n) \subseteq \mathbb{Z}$. Es suficiente ver que $\mathbf{G}_\mathbb{R}/\mathbf{G}_{m\mathbb{Z}}$ es compacto por la Proposición 3.14.

Bajo la identificación $\mathcal{L} \simeq \mathrm{GL}(d,\mathbb{R})/\mathrm{GL}(d,\mathbb{Z})$, el cociente $\mathbf{G}_\mathbb{R}/\mathbf{G}_\mathbb{Z}$ se identifica con el conjunto $\mathcal{M} := \{g(\mathbb{Z}^n) : g \in \mathbf{G}_\mathbb{R}\}$. Demostremos que $\mathcal{M}$ es compacto usando el Teorema 5.2. Para esto debemos probar que existen $\alpha, \beta > 0$ tales que

$$(i)\ \Delta(g(\mathbb{Z}^n)) \leq \beta, \qquad\qquad (ii)\ \inf_{\lambda \in \mathbb{Z}^n - \{0\}} ||g(\lambda)|| \geq \alpha.$$

El $\mathbb{Q}$-carácter $\det : \mathbf{G} \to \mathbb{C}^\times$ es trivial por hipótesis, por lo que $\mathbf{G} \subset \mathrm{SL}_n(\mathbb{C})$. Luego, (i) sigue pues $\Delta(g(\mathbb{Z}^n)) = \det g$. Para ver (ii), supongamos que es falsa, entonces existen sucesiones $g_j \in \mathbf{G}_\mathbb{R}$ y $\lambda_j \in \mathbb{Z}^n \smallsetminus \{0\}$ tales que $g_j(\lambda_j)$ converge a cero. Como P es $\mathbf{G}$-invariante, tenemos que $|P(g_j(\lambda_j))| = |P(\lambda_j)| \to 0$ y a la vez $|P(\lambda_j)| \geq 1$ pues $P(\mathbb{Z}^n) \subseteq \mathbb{Z}$ y $P(\lambda) \neq 0$ para todo $\lambda \neq 0$, lo cual es una contradicción. □

Teorema 5.5. *(Criterio de compacidad de Godement) Sea $\boldsymbol{G} \subset \mathrm{GL}_n(\mathbb{C})$ un $\mathbb{Q}$-grupo algebraico semisimple. Entonces, $\boldsymbol{G}_\mathbb{R}/\boldsymbol{G}_\mathbb{Z}$ es compacto si y sólo si $\boldsymbol{G}_\mathbb{Z}$ no tiene elementos unipotentes distintos de la matriz identidad.*

Demostración. Supongamos que $\mathbf{G}_\mathbb{R}/\mathbf{G}_\mathbb{Z}$ es compacto. Sea $u \in \mathbf{G}_\mathbb{Q}$ un elemento unipotente. Por Lema 5.3, existe un homomorfismo continuo $\varphi : \mathrm{SL}(2,\mathbb{R}) \to \mathbf{G}_\mathbb{R}$ con

$$\varphi\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right) = u$$

Sea $a = \varphi\left(\begin{bmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{bmatrix}\right) \in G$. Entonces

$$a^{-n}ua^n = \varphi\left(\begin{bmatrix} 2^{-n} & 0 \\ 0 & 2^n \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 2^n & 0 \\ 0 & 2^{-n} \end{bmatrix}\right)$$

$$= \varphi\left(\begin{bmatrix} 1 & 2^{-2n} \\ 0 & 1 \end{bmatrix}\right) \longrightarrow \varphi\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = e$$

cuando $n \to \infty$. Si $u \neq e$, entonces $a^{-n}ua^n \neq e$ para todo n, luego $\mathbf{G}_{\mathbb{R}}/\mathbf{G}_{\mathbb{Z}}$ no es compacto por el Teorema 2.7, lo cual es una contradicción. Por lo tanto $u = e$.

Ahora veamos la recíproca, razonando por el absurdo, es decir, supongamos que $\mathbf{G}_{\mathbb{R}}/\mathbf{G}_{\mathbb{Z}}$ es no compacto. Como $\mathbf{G}_{\mathbb{Z}}$ es un retículo en $\mathbf{G}_{\mathbb{R}}$ por el Teorema 3.17, el Teorema 2.7 implica que existen sucesiones $g_n \in \mathbf{G}_{\mathbb{R}}$ y $\gamma_n \in \Gamma$ tales que $g_n\gamma_n g_n^{-1} \to e$ si $n \to \infty$ y $g_n\gamma_n g_n^{-1} \neq e$ para todo $n \in \mathbb{N}$.

Ahora bien, esto implica que el polinomio característico de $g_n\gamma_n g_n^{-1}$, que es igual al de g_n, tiende al polinomio característico de e, que es igual a $(x-1)^n$. Como $\gamma_n \in \mathbf{G}_{\mathbb{Z}} \subset \mathrm{GL}_n(\mathbb{Z})$, su polinomio característico $\chi_{\gamma_n}(x)$ tiene coeficientes enteros. Luego, si $\chi_{\gamma_n}(x) \to (x-1)^n$, necesariamente $\chi_{\gamma_n}(x) = (x-1)^n$, para todo $n \geq n_0$, por lo que $\mathbf{G}_{\mathbb{Z}}$ tiene elementos unipotentes no triviales ya que $\gamma_n \neq e$ para todo $n \in \mathbb{N}$. □

5.3. Ejemplos de subgrupos aritméticos cocompactos. Como ya vimos en el Ejemplo 3.6, si J es una matriz simétrica racional no degenerada, entonces $\mathrm{O}(J)_{\mathbb{Z}}$ es un retículo en el grupo de Lie $\mathrm{O}(J)_{\mathbb{R}}$. Aplicaremos el Teorema 5.5 para obtener un criterio de compacidad para $\mathrm{O}(J)_{\mathbb{R}}/\mathrm{O}(J)_{\mathbb{Z}}$. Supongamos que $J[x] := x^tJx \in \mathbb{Q}$ para todo $x \in \mathbb{Q}^n$.

Teorema 5.6. *El cociente $\mathrm{O}(J)_{\mathbb{R}}/\mathrm{O}(J)_{\mathbb{Z}}$ es compacto si y sólo si $J[x] \neq 0$ para cualquier $x \in \mathbb{Q}^d$ no nulo (i.e. la forma cuadrática asociada a J no representa al cero en $\mathbb{Q}^d$ de manera no trivial).*

Demostración. Supongamos que $\mathrm{O}(J)_{\mathbb{R}}/\mathrm{O}(J)_{\mathbb{Z}}$ no es compacto. Por el Teorema 5.5, existe un elemento unipotente $U \neq \mathrm{Id}$ en $\mathrm{O}(J)_{\mathbb{Q}}$. Entonces $N := U - \mathrm{Id}$ es nilpotente, por lo que podemos elegir $v_1 \in \mathbb{Q}^d$ tal que $Nv_1 \neq 0$ y $N^2v_1 = 0$. Mostraremos que $J[Nv_1] = 0$. Denotemos $B(x,y) = x^tJy$, la forma bilineal asociada a J, la cual es no degenerada. Para $x, y \in W := \mathbb{C}v_1 \oplus \mathbb{C}Nv_1$, usando que $U \in \mathrm{O}(J)_{\mathbb{Q}}$, tenemos que

$$\begin{aligned} B(Nx,y) &= B((U-\mathrm{Id})x,y) = B(Ux,y) - B(x,y) \\ &= B(x,U^{-1}y) - B(x,y) = B(x,(\mathrm{Id}-N)y) - B(x,y), \end{aligned}$$

pues $N^2|_W \equiv 0$. Por lo tanto $B(Nx,y) = -B(x,Ny)$ para todo $x, y \in W$. En particular

$$J[Nv_1] = B(Nv_1, Nv_1) = -B(v_1, N^2v_1) = 0.$$

Esto prueba la recíproca.

Ahora supongamos que existe $v_0 \in V_{\mathbb{Q}} \smallsetminus \{0\}$ tal que $J[v_0] = B(v_0,v_0) = 0$. Como la forma es no degenerada, existe $\widetilde{v}_1 \in V_{\mathbb{Q}}$ tal que $B(v_0,\widetilde{v}_1) \neq 0$. Sea $q \in \mathbb{Q}$ la solución a la ecuación

$$0 = B(\widetilde{v}_1 + qv_0, \widetilde{v}_1 + qv_0) = B(\widetilde{v}_1,\widetilde{v}_1) + 2qB(\widetilde{v}_1, v_0).$$

Sea $v_1 = \widetilde{v}_1 + qv_0$. Tenemos que $B(v_0,v_1) = c \neq 0$ y $B(v_i,v_i) = 0$ for $i = 1,2$.

Sea $W = \mathbb{C}v_0 \oplus \mathbb{C}v_1$, y $W^\perp$ el subespacio de V ortogonal a W con respecto a $B(\cdot,\cdot)$. Veamos que $V = W \oplus W^\perp$. Supongamos que $w \in W \cap W^\perp$, luego $w = k_0v_0 + k_1v_1$ ya que $w \in W$, pero como $w \in W^\perp$ tenemos $0 = B(w,v_0) = k_1c$, lo que implica que $k_1 = 0$. Análogamente $0 = B(w,v_1) = B(k_0v_0,v_1) = k_0c$, por lo tanto $k_0 = 0$. Entonces $W \cap W^\perp = \{0\}$. Resta ver que $V = W + W^\perp$. Veamos que es exacta la sucesión de espacios vectoriales

$$0 \to W^\perp \to V \xrightarrow{\eta} W^* \to 0,$$

donde $\eta(v)(\cdot) = B(v,\cdot)$. Claro está que el núcleo de η coincide con $W^\perp$, por lo tanto sólo resta mostrar que η es sobre. Sea $\gamma \in W^\perp$, y llamamos $\gamma' \in V^*$ a su extensión a V, pero la aplicación $V \to V^*$ es sobre pues tienen la misma dimensión, por lo tanto existe $v_0 \in V$ que cumple $\gamma(w) = \gamma'(w) = B(v_0, w) = \eta(v_0)(w) \quad \forall w \in W$. Finalmente concluimos que $V = W \oplus W^\perp$ pues la sucesión exacta nos dice que $\dim W + \dim W^\perp = \dim V$.

Veamos que existe $v_2 \in W_{\mathbb{Q}}^\perp$ tal que $B(v_2, v_2) = c \neq 0$. Supongamos que $B(v,v) = 0$ para todo $v \in W^\perp$. Sea $w \in W^\perp$, luego existe $w' \in W^\perp$ tal que $B(w,w') \neq 0$. Entonces $0 \neq 4B(w,w') = B(w+w', w+w') - B(w-w', w-w') = 0 - 0 = 0$ lo cual es un absurdo.

Sea ahora la transformación lineal $N : V \to \mathbb{C}v_0 \oplus \mathbb{C}v_2$ dada por $x \mapsto -B(x,v_0)v_2 + B(x,v_2)v_0$, es decir,

$$N \sim \begin{pmatrix} 0 & 0 & c & \\ 0 & 0 & 0 & * \\ 0 & -c & 0 & \\ & & & \\ & 0 & & 0 \\ & & & \end{pmatrix}$$

con respecto a una base con primeros elementos v_0, v_1 y v_2. Claramente N es nilpotente, pues N^2 es triangular superior con ceros en la diagonal.

Similar al método recién utilizado, tenemos $W^\perp = \mathbb{C}v_2 \oplus \{v_2\}^\perp$, donde $\{v_2\}^\perp$ denota el subespacio de $W^\perp$ ortogonal a v_2. Luego si $x = k_0v_0 + k_1v_1 + k_2v_2 + w$, $y = k_0'v_0 + k_1'v_1 + k_2'v_2 + w' \in V$ con $k_i, k_i' \in \mathbb{C}$ y $w, w' \in \{v_2\}^\perp$, tenemos

$$\begin{aligned} B(Nx,y) &= B(N(k_0v_0 + k_1v_1 + k_2v_2 + w), k_0'v_0 + k_1'v_1 + k_2'v_2 + w') \\ &= cB(-k_1v_2 + ck_2v_0, k_1'v_1 + k_2'v_2) \\ &= c^2(-k_1k_2' + k_2k_1') \end{aligned}$$

Similarmente $B(x,Ny) = c^2(-k_1'k_2 + k_2'k_1)$, por lo tanto

$$B(x,Ny) = -B(Nx,y)$$

Sea $U := e^N = \sum_{i=1}^{m} \frac{1}{i!}N^i$, luego

$$\begin{aligned} B(Ux,Uy) &= \sum_{i,j=0}^{m} \tfrac{1}{i!}\tfrac{1}{j!}B(N^ix, N^jy) = \sum_{i,j=0}^{m} \tfrac{(-1)^j}{i!j!}B(N^{i+j}x, y) \\ &= B(\left(\textstyle\sum_{i,j=0}^{m} \frac{(-1)^j}{i!j!}N^{i+j}\right)x, y) \end{aligned}$$

Más aún,

$$\sum_{i,j=0}^{m} \tfrac{(-1)^j}{i!j!}N^{i+j} = \sum_{k=0}^{m}\left(\sum_{j=0}^{k} \tfrac{1}{(k-j)!j!}(-1)^j\right)N^k = \sum_{k=0}^{m}\frac{1}{k!}\left(\cdot\sum_{j=0}^{k}\binom{k}{j}(-1)^j\right)N^k = \mathrm{Id},$$

lo que implica que $U \in \mathrm{O}(J)$.

Para finalizar, es claro que $U = e^N \neq \mathrm{Id}$ pues $N \neq 0$, y además $U \in \mathrm{O}(J)_{\mathbb{Q}}$, pues $\{v_0, v_1, v_2\} \subset V_{\mathbb{Q}}$, y si a este conjunto lo completamos a una base de $V_{\mathbb{Q}}$, se ve que $N(V_{\mathbb{Q}}) \subseteq V_{\mathbb{Q}}$, por lo tanto $U(V_{\mathbb{Q}}) \subseteq V_{\mathbb{Q}}$. □

5.4. Ejercicios.

Ejercicio 5.1. Sea L un retículo en $\mathbb{R}^n$ y sean $\{v_1, \ldots, v_n\}$ y $\{w_1, \ldots, w_n\}$ dos $\mathbb{Z}$-bases de L. Demostrar que $\det(v_1, \ldots, v_n) = \pm\det(w_1, \ldots, w_n)$.

Parte 2. Geometría espectral de 3-variedades hiperbólicas aritméticas

6. Álgebras de cuaterniones

Uno de los temas a tratar en estas notas es la idea de que muchos aspectos de la geometría de una 3-variedad hiperbólica pueden ser caracterizados de una manera algebraica y estudiados usando técnicas provenientes del álgebra no conmutativa y la teoría de números. Es crucial para esta caracterización la noción de álgebra de cuaterniones, ya que veremos que todo grupo Kleineano aritmético de covolumen finito es un álgebra de cuaterniones definido sobre un cuerpo de números. En esta sección veremos algunas de las propiedades básicas de las álgebras de cuaterniones. Muchos resultados de esta sección serán mencionados sin demostración. Para las pruebas, ver [14].

6.1. Álgebras de cuaterniones: Generalidades. Sea k un cuerpo de característica distinta que 2.

Definición 6.1. Un **álgebra de cuaterniones** sobre k es un álgebra simple central de dimensión 4 sobre k con base $\{1, i, j, ij\}$ que satisface las relaciones

$$i^2 = a, \qquad j^2 = b, \qquad ij = -ji,$$

para algún $a, b \in k^*$.

Denotaremos al álgebra de cuaterniones en la Definición 6.1 por su *símbolo de Hilbert* $\left(\frac{a,b}{k}\right)$. Notar que la terminología "álgebra de cuaterniones" está motivada por el hecho de que las álgebras definidas arriba generalizan la construcción de Hamilton de $\mathbb{H}$, que con nuestra notación se corresponde al álgebra $\left(\frac{-1,-1}{\mathbb{R}}\right)$.

Teorema 6.2. *El álgebra de cuaterniones $\left(\frac{a,b}{k}\right)$ es un álgebra simple central de dimensión cuatro. Recíprocamente, si A es un álgebra simple central de dimensión cuatro sobre k entonces existen $a, b \in k^*$ tales que $A \cong \left(\frac{a,b}{k}\right)$.*

En su total generalidad, el Teorema de Estructura de Wedderburn implica que toda álgebra central simple es isomorfa a un álgebra de matrices sobre un álgebra de división central.

Teorema 6.3 (Teorema de Estructura para Álgebras de Cuaterniones de Wedderburn)**.** *Sea A un álgebra de cuaterniones sobre un cuerpo k. Si A no es un álgebra de división entonces $A \cong \mathrm{M}_2(k)$.*

Notar que si bien el Teorema 6.2 asegura que si A es un álgebra central simple de dimensión cuatro sobre k entonces existen $a, b \in k^*$ tales que $A \cong \left(\frac{a,b}{k}\right)$, esto no implica que a, b determinen unívocamente la clase de isomorfismo de A. Esto se explica en el siguiente resultado, que dice que la clase de isomorfismo de $\left(\frac{a,b}{k}\right)$ no cambia si multiplicamos a a o b por cuadrados.

Proposición 6.4. *Si $a, b, x, y \in k^*$ entonces*

$$\left(\frac{a,b}{k}\right) \cong \left(\frac{ax^2, by^2}{k}\right).$$

Demostración. Sean $\{1, i, j, ij\}$ y $\{1, i', j', i'j'\}$ bases para $\left(\frac{a,b}{k}\right)$ y $\left(\frac{ax^2,by^2}{k}\right)$ respectivamente, y sea

$$\phi : \left(\frac{ax^2, by^2}{k}\right) \to \left(\frac{a,b}{k}\right)$$

el homomorfismo obtenido al definir $\phi(1) = 1$, $\phi(i') = xi$, $\phi(j') = yj$, $\phi(i'j') = xyij$ y extenderlo linealmente. La imagen de ϕ es la k-subálgebra de $\left(\frac{a,b}{k}\right)$ con base $\{1, xi, yj, xyij\}$.

Como esta subálgebra tiene dimensión cuatro sobre k, debe coincidir con $\left(\frac{a,b}{k}\right)$. En otras palabras, ϕ es suryectiva. Cualquier homomorfismo suryectivo entre k-álgebras de la misma dimensión es un isomorfismo, por lo que la proposición sigue. □

Naturalmente, es muy útil saber cuándo $\left(\frac{a,b}{k}\right)$ es isomorfo a $\mathrm{M}_2(k)$ y cuándo lo es a un álgebra de división (que por el Teorema de Wedderburn son las únicas dos posibilidades). La siguiente proposición será muy útil en este aspecto.

Proposición 6.5. *Las álgebras de cuaterniones* $\left(\frac{1,b}{k}\right)$ *y* $\mathrm{M}_2(k)$ *son isomorfas para cualquier* $b \in k^*$.

Demostración. El isomorfismo buscado está dado por

$$\psi : \left(\frac{1,b}{k}\right) \longrightarrow \mathrm{M}_2(k),$$

donde

$$\psi(x + yi + zj + wij) = \begin{pmatrix} x+y & z+w \\ b(z-t) & x-y \end{pmatrix}.$$

La inversa está dada por

$$\psi^{-1}\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right) = \frac{1}{2}(\alpha + \delta + (\alpha - \delta)i + (\beta + b^{-1}\gamma)j + (\beta - b^{-1}\gamma)ij).$$

□

6.2. Álgebra de cuaterniones sobre los números complejos. Las álgebras de cuaterniones sobre $\mathbb{C}$ son muy fáciles de entender. Hay una única álgebra de cuaterniones sobre $\mathbb{C}$: $\mathrm{M}_2(\mathbb{C})$.

Teorema 6.6. *Si* A *es un álgebra de cuaterniones sobre* $\mathbb{C}$ *entonces* $A \cong \mathrm{M}_2(\mathbb{C})$.

Demostración. El teorema fundamental del álgebra implica que todo elemento de $\mathbb{C}^*$ es un cuadrado, entonces $A \cong \left(\frac{1,1}{\mathbb{C}}\right)$ por Proposición 6.4. Esta última álgebra de cuaterniones es isomorfa a $\mathrm{M}_2(\mathbb{C})$ por Proposición 6.5. □

6.3. Álgebras de cuaterniones sobre los números reales. La estructura de las álgebras de cuaterniones sobre $\mathbb{R}$ es más complicada que sobre $\mathbb{C}$. Hay sólo dos álgebras de cuaterniones sobre $\mathbb{R}$ salvo isomorfismos: $\mathrm{M}_2(\mathbb{R})$ and $\mathbb{H}$.

Teorema 6.7. *Si* A *es un álgebra de cuaterniones sobre* $\mathbb{R}$ *entonces es* $A \cong \mathrm{M}_2(\mathbb{R})$ *ó* $A \cong \mathbb{H}$.

Demostración. La Proposition 6.4 implica que A es isomorfa a una de las siguientes tres álgebras de cuaterniones: $\left(\frac{-1,-1}{\mathbb{R}}\right)$, $\left(\frac{1,-1}{\mathbb{R}}\right)$ o $\left(\frac{1,1}{\mathbb{R}}\right)$. La primera de estas álgebras es isomorfa a $\mathbb{H}$ por definición, mientras que la segunda y la tercera son isomorfas a $\mathrm{M}_2(\mathbb{R})$ por Proposición 6.5. □

6.4. Álgebras de cuaterniones sobre cuerpos p-ádicos. Sea K un cuerpo p-ádico con uniformizador fijo π. Como ocurrió en el caso sobre $\mathbb{R}$, hay precisamente dos clases de isomorfismos de álgebras de cuaterniones sobre k. Además, otra vez tenemos una descripción explícita de la única álgebra de cuaterniones de división sobre k. Como la demostración nos llevaría demasiado lejos, sólo citamos el siguiente resultado y remitimos al lector a [14] para ver más detalles.

Teorema 6.8. *La* k*-álgebra* $\left(\frac{u,\pi}{k}\right)$ *es la única álgebra de cuaterniones de división sobre* k*, donde* $k(\sqrt{u})$ *es la única extensión cuadrática no ramificada de* k.

6.5. Álgebras de cuaterniones sobre cuerpos de números. Sea k un cuerpo de números, $a, b \in k^*$ y consideramos el álgebra de cuaterniones $\left(\frac{a,b}{k}\right)$. Si K es un cuerpo que contiene a k entonces podemos obtener una K-álgebra de cuaterniones de $\left(\frac{a,b}{k}\right)$ por extensión de escalares: $\left(\frac{a,b}{k}\right) \otimes_k K \cong \left(\frac{a,b}{K}\right)$. En el estudio de la estructura de las álgebras de cuaterniones sobre cuerpos de números a veces se elige como K a la completación de k (i.e., $\mathbb{C}, \mathbb{R}$ o un cuerpo p-ádico $k_{\mathfrak{p}}$ para algún primo $\mathfrak{p}$ de k) y estudia el álgebra sobre K obtenida por extensión de escalares. Por supuesto, uno espera poder obtener información acerca de la estructura del álgebra original sobre k.

Para hacer todo esto más preciso, sea $\{1, i, j, ij\}$ la base estándar de $\left(\frac{a,b}{k}\right)$ y $\sigma : k \hookrightarrow K$ un embedding fijo.

Lema 6.9. *Tenemos el siguiente isomorfismo*

$$\left(\frac{a,b}{k}\right) \otimes_\sigma K \cong \left(\frac{\sigma(a), \sigma(b)}{K}\right).$$

Demostración. Sea $\{1, i', j', i'j'\}$ la base estándar para $\left(\frac{\sigma(a),\sigma(b)}{K}\right)$. El isomorfismo es el que asigna

$$(a_0 + a_1 i + a_2 j + a_3 ij) \otimes_\sigma \alpha \mapsto \alpha(\sigma(a_0) + \sigma(a_1)i' + \sigma(a_2)j' + \sigma(a_3)i'j').$$

□

Como una aplicación de esto, consideramos el álgebra de cuaterniones $\left(\frac{-1,-1}{\mathbb{Q}}\right)$. Si $\sigma : \mathbb{Q} \to \mathbb{R}$ es la inclusión estándar, entonces el Lema 6.9 implica que $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ es un álgebra de división (ya que $\sigma(-1) = -1$ y $\left(\frac{-1,-1}{\mathbb{R}}\right)$ es un álgebra de división). Un hecho interesante en la teoría de las álgebras de cuaterniones sobre cuerpos de números es que a diferencia de lo que sucede sobre $\mathbb{R}$, no hay una única álgebra de división sobre un cuerpo de números. De hecho, sobre todo cuerpo de números ¡hay infinitas clases de isomorfismos de álgebras de cuaterniones!

Definición 6.10. Sea k un cuerpo de números, v un lugar de k correspondiente al embedding σ, y sea k_v la correspondiente completación de k. Decimos que un álgebra de cuaterniones A sobre k es **ramificada en σ y v** si $A \otimes_\sigma k_v$ es un álgebra de división. Si no, decimos que A **se parte en σ y v**.

Nota 6.11. Por conveniencia, usualmente diremos que un álgebra de cuaterniones A sobre k es ramificada en un lugar v de k y omitiremos mencionar el embedding asociado σ.

Nota 6.12. Notar que si $A = \mathrm{M}_2(k)$ entonces $A \otimes_\sigma k_v \cong \mathrm{M}_2(k_v)$ para todo σ, v. En particular, todo lugar de k se parte en $\mathrm{M}_2(k)$.

Recordar que por Teorema 6.6, toda álgebra de cuaterniones sobre k se parte en todos los lugares complejos. Entonces sólo los lugares reales o p-ádicos podrían ramificar.

Supongamos ahora que k tiene r_1 lugares reales y r_2 lugares complejos. Denotamos por S_∞ el conjunto de lugares arquimedeanos de k. Tenemos entonces los isomorfismos

$$\begin{aligned} A \otimes_{\mathbb{Q}} \mathbb{R} &\cong \bigoplus_{v \in S_\infty} A \otimes_k k_v \\ &\cong \mathrm{M}_2(\mathbb{C})^{r_2} \times \bigoplus_{\sigma : k \hookrightarrow \mathbb{R}} A \otimes_\sigma k_v \\ &\cong \mathrm{M}_2(\mathbb{C})^{r_2} \times \mathrm{M}_2(\mathbb{R})^s \times \mathbb{H}^{r_1 - s}, \end{aligned}$$

donde s es el número de lugares reales de k en los que A se parte. En la Sección 8 veremos que los grupos Kleineanos aritméticos se construyen a partir de las álgebras de

cuaterniones en que $r_2 = 1$ y $s = 0$. Una manera simple de ver esto es tomando como k un cuerpo cuadrático imaginario, en cuyo caso $s = 0$ ya que allí no hay lugares reales.

Sea $\mathrm{Ram}(A)$ el conjunto de lugares de k (pueden ser finitos o infinitos) en que A es ramificado. El siguiente teorema clasifica las álgebras de cuaterniones sobre cuerpos de números e implica, como fue dicho arriba, que hay infinitas clases de isomorfismos de álgebras de cuaterniones de división sobre todo cuerpo de números. Para la demostración de esto, ver [14, Chapitre III.3].

Teorema 6.13 (Clasificación de Álgebras de Cuaterniones sobre cuerpos de números)**.** *Sea k un cuerpo de números. Si A es un álgebra de cuaterniones sobre k entonces* $\mathrm{Ram}(A)$ *es finito y de cardinalidad par. Recíprocamente, dado cualquier conjunto finito S de lugares (finitos o infinitos) de k con cardinalidad par, existe una única álgebra de cuaterniones A sobre k tal que* $\mathrm{Ram}(A) = S$.

El siguiente es un corolario inmediato del Teorema 6.13.

Corolario 6.14. *Si k es un cuerpo de números y A, A' son álgebras de cuaterniones sobre k entonces $A \cong A'$ si y sólo si* $\mathrm{Ram}(A) = \mathrm{Ram}(A')$.

7. Órdenes en álgebras de cuaterniones: un primer vistazo

En esta sección introducimos la noción de orden en álgebras de cuaterniones y exploramos algunas de sus propiedades básicas. Nuestro objetivo es proveer los conocimientos necesarios para describir la construcción de subgrupos discretos de $\mathrm{PSL}_2(\mathbb{C})$ a partir de órdenes en álgebras de cuaterniones definidas sobre ciertos cuerpos de números. Esto nos permitirá dar la definición de una 3-variedad hiperbólica.

7.1. Definiendo órdenes. Sea R un dominio de Dedekind con cuerpo cociente K. En la práctica siempre tomaremos K un cuerpo de números o su completación en un primo finito y R denotará su anillo de enteros. Sea A un álgebra de cuaterniones sobre K.

Definición 7.1. Un elemento $\alpha \in A$ es **integral** con respecto a R si su polinomio característico (reducido) $x^2 - \mathrm{tr}(\alpha)x + n(\alpha)$ tiene coeficientes en R. Llamamos a $\mathrm{tr}(\alpha)$ la **traza** (reducida) de α y a $n(\alpha)$ la **norma** (reducida) de α.

Recordar que el conjunto de todos los elementos integrales de un cuerpo de números forman un anillo (y muy importante para lo que sigue, un $\mathbb{Z}$-módulo finitamente generado). Sin embargo, esto no es cierto en el caso de álgebra de cuaterniones. Considerar los siguientes dos elementos de $\mathrm{M}_2(\mathbb{Q})$:

$$A = \begin{pmatrix} \frac{5}{4} & -\frac{1}{8} \\ \frac{1}{2} & \frac{3}{4} \end{pmatrix}, \qquad B = \begin{pmatrix} \frac{11}{6} & \frac{1}{2} \\ \frac{5}{18} & \frac{7}{6} \end{pmatrix}.$$

Los polinomios característicos de A y B son $p_A(x) = x^2 - 2x + 1$ y $p_B(x) = x^2 - 3x + 2$. Entonces A y B son integrales (con respecto a $\mathbb{Z}$). Sin embargo, ni $A + B$ ni AB son integrales; sus polinomios característicos son $p_{A+B}(x) = x^2 - 5x + \frac{809}{144}$ y $p_{AB}(x) = x^2 - \frac{487}{144}x + 2$. Veremos que el hecho de que el conjunto de elementos integrales en un álgebra de cuaterniones no es un anillo hace que la teoría de órdenes en álgebras de cuaterniones sea significativamente más complicada que el estudio de órdenes en cuerpos de números. Por otro lado, esto también hace que la teoría sea mucho más rica. En efecto, este hecho hace posible la construcción de Vignéras de 3-variedades hiperbólicas isospectrales.

Definición 7.2. Sea V un espacio vectorial sobre K. Un **R-retículo** en V es un R-módulo finitamente generado contenido en V. Un R-retículo L se dice **completo** si $L \otimes_R K \cong V$.

El siguiente es un resultado básico en álgebra conmutativa.

Proposición 7.3 ([1, Prop. 5.1])**.** *Un elemento $\alpha \in A$ es integral si y sólo si $R[\alpha]$ es un R-retículo en A.*

Ahora somos capaces de dar nuestra primera definición de órdenes en álgebra de cuaterniones.

Definición 7.4. Un **orden** $\mathcal{O}$ en A es un R-retículo completo en A que es también un subanillo de A. Un **orden maximal** es un orden en A que es maximal con respecto a la inclusión.

Ejemplo 7.5. Damos algunos ejemplos de órdenes.

1. El anillo $\mathrm{M}_2(R)$ es siempre un orden de $\mathrm{M}_2(K)$. (Ver Lema 7.7 abajo.)
2. Supongamos que $A = \left(\frac{a,b}{K}\right)$, donde a, b son elementos integrales de K. (Notar que A puede escribirse siempre de esta forma ya que el símbolo de Hilbert está definido salvo cuadrados, por lo que podemos 'limpiar denominadores' multiplicando a a y b por un cuadrado de K.) Entonces $R[1, i, j, ij]$ es un orden de A.

Proposición 7.6. *$\mathcal{O}$ es un orden en A si y sólo si $\mathcal{O}$ es un anillo de elementos integrales en A que contiene a R y satisface $\mathcal{O} \otimes_R K = A$. Además, todo orden está contenido en un orden maximal.*

Demostración. Sea $\mathcal{O}$ un orden de A y $\alpha \in \mathcal{O}$. Como $\mathcal{O}$ es un R-retículo, también lo es $R[\alpha]$. Sigue entonces de la Proposición 7.3 que α es integral. Que $\mathcal{O}$ satisface las otras propiedades sigue de nuestra definición de orden.

Probamos ahora la recíproca. Como $\mathcal{O} \otimes_R K = A$, podemos elegir una base $\{x_1, x_2, x_3, x_4\}$ de A en la que todos los x_i están en $\mathcal{O}$. Como la traza reducida determina una forma bilineal simétrica no singular sobre A, $d = \det(\mathrm{tr}(x_i x_j)) \neq 0$. Sea $L = \{\sum a_i x_i : a_i \in R\}$. Entonces $L \subset \mathcal{O}$ pues $R \subset \mathcal{O}$ y $x_i \in \mathcal{O}$ para todo i. Supongamos que $\alpha \in \mathcal{O}$ con $\alpha = \sum b_i x_i$ y $b_i \in K$. Para cada j tenemos que $\alpha x_j \in \mathcal{O}$, entonces $\mathrm{tr}(\alpha x_j) = \sum b_i \,\mathrm{tr}(x_i x_j) \in R$. Por lo tanto $b_i \in \frac{1}{d} R$ y $\mathcal{O} \subset \frac{1}{d} L$. Sigue entonces que $\mathcal{O}$ es finitamente generado, lo que prueba la primera afirmación. La segunda afirmación se demuestra utilizando el Lema de Zorn. □

Lema 7.7. *El orden $\mathrm{M}_2(R)$ es un orden maximal de $\mathrm{M}_2(K)$.*

Demostración. Si $\mathrm{M}_2(R)$ no es maximal, entonces sea $\mathcal{O}$ un orden maximal que contiene a $\mathrm{M}_2(R)$ y algún elemento $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ con al menos uno de los x, y, z, w que no pertenezca a R. Sumando y multiplicando elementos de R podemos conseguir un elemento $\alpha \in \mathcal{O}$ de la forma $\alpha = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ con $a \notin R$. Tal elemento claramente no es integral, lo cual es una contradicción. □

Hemos demostrado que si $\mathcal{O}$ es un orden en A entonces todo elemento de $\mathcal{O}$ es integral. La siguiente proposición nos provee una recíproca de este enunciado.

Proposición 7.8. *Si $\alpha \in A$ es integral entonces α está contenido en un orden maximal de A.*

Demostración. Si $\alpha \in R$ entonces α está en *todo* orden A por Proposición 7.6. Podemos asumir entonces que $\alpha \notin R$. En tal caso, $K(\alpha)$ es una extensión cuadrática de K que está contenida en A. Sea $\beta \in A^*$ tal que $\beta\alpha\beta^{-1} = \overline{\alpha}$. La existencia de tal elemento es debida al Teorema de Skolem–Noether y podemos tomar β integral simplemente limpiando denominadores. El R-módulo generado por α y β es $R + R\alpha + R\beta + R\alpha\beta$ y es claramente un orden de A. Este orden podría no ser maximal, pero hemos visto que todo orden está contenido en un orden maximal. □

7.2. Números de tipo. Supongamos que $\mathcal{O}_1$ y $\mathcal{O}_2$ son órdenes en A que son isomorfos via algún isomorfismo $f : \mathcal{O}_1 \to \mathcal{O}_2$. Por extensión de escalares, la función f induce induce un isomorfismo $\hat{f} : \mathcal{O}_1 \otimes_R K \to \mathcal{O}_2 \otimes_R K$ en el que $\hat{f}(x) = f(x)$ para todo $x \in \mathcal{O}_1$. Como $\mathcal{O}_1$ y $\mathcal{O}_2$ son órdenes en A, $\mathcal{O}_1 \otimes_R K \cong A \cong \mathcal{O}_2 \otimes_R K$. Por lo tanto $\hat{f}$ es un automorfismo de A y está dado por conjugar por un elemento $a \in A^*$ por el Teorema de Skolem–Noether. En particular, $\mathcal{O}_2 = a\mathcal{O}_1 a^{-1}$. Concluimos que en un álgebra de cuaterniones, dos órdenes son isomorfos si y sólo si son conjugados.

Definición 7.9. El **número de tipo** de un álgebra de cuaterniones es el número de clases de conjugación de órdenes maximales.

El número de tipo de un álgebra de cuaterniones sobre un cuerpo de números es de algún modo una reminiscencia del número de clases de un cuerpo de números. Si bien el número de tipo es siempre finito (lo cual a priori no es obvio), puede ser arbitrariamente grande. Además, cuando A es no ramificado en un primo arquimedeano de K veremos que el número de tipo es siempre una potencia de 2.

El número de tipo de un álgebra de cuaterniones sobre un cuerpo de números juega un rol crucial en la construcción de Vignéras de 3-variedades hiperbólicas isospectrales, como también en aplicaciones a otros temas como las formas modulares.

Sea k un cuerpo de números y A/k un álgebra de cuaterniones que cumple que $A \otimes_{\mathbb{Q}} \mathbb{R} \ncong \mathbb{H}^{[k:\mathbb{Q}]}$. Sea k_A la extensión abeliana maximal de k que tiene exponente 2, es no ramificada fuera de los lugares reales en $\mathrm{Ram}(A)$, y en la que todo primo finito de $\mathrm{Ram}(A)$ se parte completamente. El siguiente teorema sigue de los resultados probados en [10, Section 3].

Teorema 7.10. *Las clases de conjugación de órdenes maximales en A están en correspondencia uno a uno con los elementos de* $\mathrm{Gal}(k_A/k)$.

Los números de tipo son muy fáciles de computar usando Magma.

Ejemplo 7.11. Sea $k = \mathbb{Q}(\sqrt{-10})$. Consideramos el álgebra de cuaterniones $A = \left(\frac{-1,-3}{k}\right)$. Veremos que el número de tipo de A es 2 y calcularemos los conjuntos generadores para los representantes de las dos clases de conjugación de órdenes maximales de A (considerados como módulos sobre $\mathcal{O}_k$).

```
>k<t>:=QuadraticField(-10);
>t^2;
-10
>A<i,j,ij>:=QuaternionAlgebra<k|-1,-3>;
>C:=ConjugacyClasses(MaximalOrder(A));
>#C;
2
IsConjugate(C[1],C[2]);
false
>Generators(C[1]);
[ 1, i, 1/2*i + 1/2*j, 1/2 + 1/2*t*i + 1/6*t*j + 1/6*ij ]
>Generators(C[2]);
[ 1, 2*i, 3*t*i, 1 + 1/2*i + 1/2*j, 1/2*(t + 2) + 1/4*(t + 2)*i + 1/4*(t +
2)*j, 1/2*(t + 1) + 1/4*(t + 4)*i - 1/12*t*j + 1/6*ij ]
```

8. Grupos Kleineanos Aritméticos y 3-variedades hiperbólicas

8.1. Espacio hiperbólico tridimensional. Comenzamos definiendo el espacio hiperbólico de dimensión 3, al que siempre consideraremos en el modelo de semiespacio superior

$$\mathbf{H}^3 = \{(z,t) : z \in \mathbb{C}, t > 0\}$$

con la métrica

$$ds^2 = \frac{|dz|^2 + dt}{t^2}.$$

De esta forma, $\mathbf{H}^3$ es la única variedad Riemanniana conexa, simplemente conexa de dimensión 3 con curvatura seccional constante -1. Veremos a la esfera de Riemann $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ como la *esfera al infinito* correspondiente a $t = 0$. Las geodésicas en $\mathbf{H}^3$ son rectas euclideanas verticales o semicírculos ortogonales a $\hat{\mathbb{C}}$.

8.2. Grupos Kleineanos. Un *grupo Kleineano* es un subgrupo discreto de isometrías del espacio hiperbólico $\mathbf{H}^3$ que preserva orientación. Ya era conocido por Poincaré que el grupo $\mathrm{Isom}^+(\mathbf{H}^3)$ de isometrías del espacio hiperbólico de dimensión 3 es isomorfo a $\mathrm{PSL}_2(\mathbb{C})$, entonces un grupo Kleineano es simplemente un subgrupo discreto de $\mathrm{PSL}_2(\mathbb{C})$.

Los elementos de $\mathrm{PSL}_2(\mathbb{C})$ inducen una función biholomorfa de $\hat{\mathbb{C}}$ dada por transformaciones de Moebius:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \left(z \mapsto \frac{az+b}{cz+d} \right).$$

Estas transformaciones fraccionarias lineales de $\hat{\mathbb{C}}$ se extienden a $\mathbf{H}^3$ via la extensión de Poincaré. La extensión de Poincaré puede ser descripta geométricamente como sigue. Toda transformación fraccionaria lineal de $\hat{\mathbb{C}}$ puede escribirse como una composición de inversiones de círculos y rectas de $\hat{\mathbb{C}}$. Dado un círculo o una recta, hay un único hemisferio o plano en $\mathbf{H}^3$ que es ortogonal a $\hat{\mathbb{C}}$ y que corta a $\hat{\mathbb{C}}$ precisamente en dicho círculo o recta. La extensión de Poincaré es simplemente la composición de las inversiones en $\mathbf{H}^3$. Más concretamente, la extensión está dada por la fórmula:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \left((z,t) \mapsto \left(\frac{(az+b)\overline{(cz+d)} + a\bar{c}t^2}{|cz+d|^2 + |c|^2 t^2}, \frac{t}{|cz+d|^2 + |c|^2 t^2} \right) \right).$$

Por ejemplo, la traslación $z \mapsto z+1$ se extiende a $(z,t) \mapsto (z+1,t)$.

Si bien hay varias razones excelentes para estudiar grupos Kleineanos, nuestro interés en ellos se debe principalmente a lo siguiente:

Teorema 8.1. *Si M es una 3-variedad hiperbólica orientable entonces M es isométrica a $\mathbf{H}^3/\Gamma$ donde Γ es un grupo Kleineano libre de torsión.*

8.3. Conmensurabilidad. Damos ahora la definición de *conmensurabilidad*, una noción que estará muy presente en lo que sigue. En efecto, uno de los objetivos principales será asociar a una 3-variedad hiperbólica de volumen finito invariantes que sólo dependan de la clase de conmensurabilidad de la variedad. La noción de conmensurabilidad es natural del punto de vista de las 3-variedades hiperbólicas aritméticas, ya que veremos que la clase de conmensurabilidad de tales variedades corresponden a una cierta *álgebra de cuaterniones*, es decir un objeto de la teoría de números con una teoría de estructura muy rica.

Definición 8.2. Sean Γ_1, Γ_2 subgrupos de $\mathrm{PSL}_2(\mathbb{C})$.

- Decimos que Γ_1 y Γ_2 son **directamente conmensurables** si $\Gamma_1 \cap \Gamma_2$ tiene índice finito en Γ_1 y Γ_2. Decimos que Γ_1 y Γ_2 son **conmensurables en un amplio sentido** si Γ_1 y un conjugado de Γ_2 son directamente conmensurables.
- Sean M_1, M_2 3-variedades hiperbólicas. Decimos que M_1 y M_2 son **conmensurables** si tienen un cubrimiento finito hiperbólico en común.

Notar que en la definición de conmensurabilidad, el cubrimiento común será considerado único salvo isometrías. En este caso, las dos variedades serán conmensurables si y sólo si sus grupos fundamentales son conmensurables en el sentido amplio. Es por esta razón que estaremos interesados en la conmensurabilidad en el sentido amplio.

8.4. Grupos aritméticos Kleineanos. En esta sección construiremos subgrupos discretos de $\mathrm{PSL}_2(\mathbb{C})$ a partir de órdenes en álgebras de cuaterniones y relacionaremos las propiedades geométricas de los grupos Kleineanos resultantes con propiedades algebraicas de las álgebras de cuaterniones asociadas. Esto nos permitirá definir lo que significa que un grupo Kleineano sea aritmético.

A lo largo de esta sección emplearemos la siguiente notación. Sea k un cuerpo de números con anillo de enteros $\mathcal{O}_k$ y sea A un álgebra de cuaterniones sobre k. Un *orden $\mathcal{O}$ de A* significará siempre que $\mathcal{O}$ es un $\mathcal{O}_k$-orden de A. Si B es un subanillo de A entonces denotaremos por B^1 el subgrupo multiplicativo de B^* generado por elementos que tienen norma reducida igual a 1.

Finalmente, recordamos que $\mathrm{Ram}(A)$ (respectivamente $\mathrm{Ram}_f(A)$ o $\mathrm{Ram}_\infty(A)$) denota el conjunto de todos los lugares de k (respectivamente finitos o infinitos) que ramifican en A.

8.5. Grupos discretos de órdenes en álgebras de cuaterniones. Sea k un cuerpo de números de grado n con un único lugar complejo ν. Recordar que esto significa que de los n embeddings $\sigma : k \hookrightarrow \mathbb{C}$, la imagen $\sigma(k)$ de k estará contenida en $\mathbb{R}$ para precisamente $n-2$ embeddings. Los otros dos embeddings estarán dados por ν y $\overline{\nu}$, el conjugado complejo de ν. Denotaremos S_∞ al conjunto de lugares arquimedeanos de k.

Suponemos ahora que A es un álgebra de cuaterniones sobre k que es ramificado en todos los lugares reales de k. Al recordar que siempre hay un isomorfismo

$$A \otimes_{\mathbb{Q}} \mathbb{R} \cong \bigoplus_{v \in S_\infty} A \otimes_k k_v,$$

deducimos que

$$A \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}^{n-2} \times \mathrm{M}_2(\mathbb{C}). \tag{8.1}$$

Sea $\psi : A \hookrightarrow \mathrm{M}_2(\mathbb{C})$. Denotamos por $\psi : A \hookrightarrow \mathrm{M}_2(\mathbb{C})$ la composición del embedding natural $A \hookrightarrow A \otimes_{\mathbb{Q}} \mathbb{R}$ con el isomorfismo en (8.1) y la proyección de $\mathbb{H}^{n-2} \times \mathrm{M}_2(\mathbb{C})$ sobre $\mathrm{M}_2(\mathbb{C})$.

Teorema 8.3. *Sea $\mathcal{O}$ un orden maximal de A y $\Gamma_{\mathcal{O}} = P\psi(\mathcal{O}^1) \subset \mathrm{PSL}_2(\mathbb{C})$.*

1. *$\Gamma_{\mathcal{O}}$ es un subgrupo discreto de $\mathrm{PSL}_2(\mathbb{C})$.*
2. *El volumen de $\mathbf{H}^3/\Gamma_{\mathcal{O}}$ está dado por*

$$\mathrm{Vol}(\mathbf{H}^3/\Gamma_{\mathcal{O}}) = \frac{d_k^{3/2}\zeta_k(2)}{(4\pi^2)^{[k:\mathbb{Q}]-1}} \cdot \left(\prod_{\mathfrak{p} \in \mathrm{Ram}_f(A)} (N(\mathfrak{p}) - 1) \right),$$

donde d_k es el valor absoluto del discriminante de k y $\zeta_k(2)$ es la función zeta de Dedekind de k evaluada en $s = 2$.

Demostración. Para la prueba de que $\Gamma_{\mathcal{O}}$ es discreto, ver [14, Chapitre IV, Theoreme 1.1]. La fórmula para el covolumen de $\Gamma_{\mathcal{O}}$ se debe a Borel [2, Section 7.3]. □

Ahora podemos definir lo que significa que un grupo Kleineano sea aritmético.

Definición 8.4. Sea k un cuerpo de números con un único lugar complejo, sea A un álgebra de cuaterniones sobre k que ramifica en todos los lugares reales de k y sea $\mathcal{O}$ un orden maximal de A. Un subgrupo de $\mathrm{PSL}_2(\mathbb{C})$ es un **grupo Kleineano aritmético** si es conmensurable con $\Gamma_{\mathcal{O}}$ para alguna tripla $(k, A, \mathcal{O})$.

Los grupos $\Gamma_{\mathcal{O}}$ serán lo suficientemente importantes en nuestra discusión de grupos Kleineanos por lo que será muy útil denotarlos de una manera simple. De ahora en adelante, nos referiremos a los grupos de la forma $\Gamma_{\mathcal{O}}$ como **grupos Kleineanos aritméticos del**

tipo más simple. Así, un subgrupo de $\mathrm{PSL}_2(\mathbb{C})$ es un grupo Kleineano aritmético si y sólo si es conmensurable a un grupo Kleineano aritmético del tipo más simple.

Recordar que el Teorema de Wedderburn nos decía que si un álgebra de cuaterniones sobre k no es isomorfo a $\mathrm{M}_2(k)$ entonces es un álgebra de división. En el contexto de las álgebras de cuaterniones A que ramifican en todos los lugares reales de k, esto significa que A no es un álgebra de división si y sólo si k no tiene lugares reales (i.e., $k = \mathbb{Q}(\sqrt{-d})$ para algún entero positivo d libre de cuadrados) y $A \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-d}))$.

Ejemplo 8.5. Considerar un cuerpo cuadrático imaginario $\mathbb{Q}(\sqrt{-d})$ con anillo de enteros $\mathcal{O}_d$. En Lema 7.7 vimos que $\mathrm{M}_2(\mathcal{O}_d)$ es un orden maximal en el álgebra de cuaterniones $\mathrm{M}_2(\mathbb{Q}(\sqrt{-d}))$. El grupo $\mathrm{PSL}_2(\mathcal{O}_d)$ es llamado un **grupo de Bianchi**. Todo grupo de Bianchi contiene la isometría $z \mapsto z + 1$ de $\hat{\mathbb{C}}$ y por lo tanto es no compacto. De hecho, es un resultado conocido que el número de cúspides del grupo de Bianchi asociado a $\mathbb{Q}(\sqrt{-d})$ es igual al número de clases de ideales de $\mathbb{Q}(\sqrt{-d})$. De acuerdo al Teorema 8.3, $\mathrm{PSL}_2(\mathcal{O}_3)$ es el grupo de Bianchi de covolumen más chico. Usando Magma es fácil calcular los covolúmenes de los grupos de Bianchi.

CUADRO 1. Volúmenes de pequeñas orbifolds de Bianchi

d	$\mathrm{Vol}(\mathbf{H}^3/\mathrm{PSL}_2(\mathcal{O}_d))$
1	0.30532186472574...
2	1.00384100334120...
3	0.16915693440160...
5	4.20396925947605...
6	5.18217289781959...
7	0.88891492781635...
10	9.81811844389802...
11	1.38260830790264...
13	13.9979614019778...
14	20.3513407500735...

Dado un entero positivo libre de cuadrados d, el volumen $\mathrm{Vol}(\mathbf{H}^3/\mathrm{PSL}_2(\mathcal{O}_d))$ puede ser computado en Magma con los siguientes comandos:

```
>RR := RealField();
>pi := Pi(RR);
>R<x>:=PolynomialRing(Rationals());
>k:=NumberField(x^2+d);
>Dk:=Abs(Discriminant(Integers(k)));
>Zeta:=Evaluate(LSeries(k),2);
>Dk^(3/2)*Zeta/(4*pi^2);
```

Si bien no es necesario usar un programa computacional para calcular el discriminante de un cuerpo cuadrático, el código anterior puede modificarse fácilmente para calcular el volumen de grupos Kleineanos aritméticos de la forma $\Gamma_{\mathcal{O}}$. Uno simplemente necesita reemplazar $x^2 + d$ por el polinomio que define k y recordar calcular el término

$$\left(\prod_{\mathfrak{p} \in \mathrm{Ram}_f(A)} (N(\mathfrak{p}) - 1) \right)$$

que aparece en el Teorema 8.3, ya que este término es trivial en el caso que $A \cong \mathrm{M}_2(k)$.

El siguiente teorema relaciona la topología de una 3-variedad hiperbólica aritmética $\mathbf{H}^3/\Gamma$ con la estructura de un álgebra de cuaterniones asociada.

Teorema 8.6. *Sea $M = \mathbf{H}^3/\Gamma$ una 3-variedad hiperbólica aritmética y supongamos que Γ es conmensurable con $\Gamma_{\mathcal{O}}$, donde $\mathcal{O}$ es un orden maximal en un álgebra de cuaterniones A sobre un cuerpo de números k. Son equivalentes:*

1. *M es no compacta.*
2. *k es un cuerpo cuadrático imaginario y $A \cong \mathrm{M}_2(k)$.*
3. *Γ es conmensurable en el sentido amplio con un grupo de Bianchi.*

Demostración. Si Γ no es cocompacto entonces tampoco es $\Gamma_{\mathcal{O}}$. Luego $\Gamma_{\mathcal{O}}$ contiene un elemento parabólico γ. Como el elemento $\gamma - \mathrm{Id}$ no es inversible podríamos concluir que A no es un álgebra de división. Por el Teorema de Wedderburn, $A \cong M_2(k)$. Ya vimos que un orden maximal de $\mathrm{M}_2(k)$ será un grupo Kleineano aritmético sólo si k es cuadrático imaginario. Luego (1) implica (2). Que (2) implica (3) sigue de la definición de un grupo de Bianchi y el hecho que los órdenes maximales en la misma álgebra de cuaterniones siempre nos darán grupos Kleineanos aritméticos que son conmensurables. Para probar que (3) implica (1), notar que todos los grupos de Bianchi contienen elementos parabólicos, por lo tanto Γ también lo hará si es conmensurable en un sentido amplio a un grupo de Bianchi. □

Como consecuencia del Teorema 8.6 obtenemos lo siguiente.

Corolario 8.7. *Sea $M = \mathbf{H}^3/\Gamma$ una 3-variedad hiperbólica aritmética y supongamos que Γ es conmensurable con $\Gamma_{\mathcal{O}}$, donde $\mathcal{O}$ es un orden maximal en un álgebra de cuaterniones A sobre un cuerpo de números k. La variedad M es compacta si y sólo si A es un álgebra de división.*

9. Una construcción de Vignéras: ejemplos de 3-variedades hiperbólicas isospectrales

Sea M una 3-variedad hiperbólica aritmética compacta y $\mathcal{E}(M)$ el multiconjunto de autovalores del operador de Laplace-Beltrami actuando sobre $L^2(M)$. Llamamos $\mathcal{E}(M)$ al **espectro de autovalores de Laplace** de M. Es conocido que $\mathcal{E}(M)$ es un subconjunto discreto e infinito de los números reales positivos. Si M y N son 3-variedades hiperbólicas aritméticas compactas para las que $\mathcal{E}(M) = \mathcal{E}(N)$, entonces decimos que M y N son **isospectrales**.

En esta sección construiremos pares de 3-variedades hiperbólicas aritméticas compactas con el mismo espectro de autovalores del operador de Laplace. El método es debido originalmente a Vignéras [13]. De hecho, las 3-variedades hiperbólicas que construiremos serán siempre **fuertemente isospectrales**; esto es, tendrán el mismo espectro de autovalores con respecto a cualquier operador diferencial elíptico autoadjunto natural, e.g., el Laplaciano actuando sobre p-formas.

9.1. Generalidades sobre isospectralidad. Sea G un grupo de Lie semisimple y Γ un subgrupo discreto cocompacto de G. Denotamos por $L^2(\Gamma\backslash G)$ el espacio de funciones de cuadrado integrable sobre $\Gamma\backslash G$ con respecto a la medida de Haar inducida de G y por $C_c(G)$ el espacio de funciones a valores complejos con soporte compacto e infinitamente diferenciables sobre G. Definimos un operador unitario R_Γ de G en $L^2(\Gamma\backslash G)$ por

$$(R_\Gamma(g)f)(x) = f(xg)$$

donde $f \in L^2(\Gamma\backslash G), x \in \Gamma\backslash G$, y $g \in G$. Si Γ' es otro subgrupo discreto y cocompacto de G decimos que Γ y Γ' son **equivalentes en representaciones** si existe un isomorfismo

unitario $T : L^2(\Gamma\backslash G) \to L^2(\Gamma'\backslash G)$ para el que

$$T(R_\Gamma(g)f) = R_{\Gamma'}(g)T(f)$$

para todo $g \in G$ y $f \in L^2(\Gamma\backslash G)$.

Es un hecho bien conocido que la equivalencia en representaciones implica isospectralidad con respecto al espectro de Laplace. De hecho, es un teorema de DeTurck y Gordon [5] que equivalencia en representaciones implica isospectralidad fuerte.

Teorema 9.1 (DeTurck and Gordon)**.** *Sea G un grupo de Lie que actúa sobre una variedad Riemanniana M por isometrías. Supongamos que $\Gamma, \Gamma' \leq G$ actúan propia y discontinuamente sobre M. Si Γ y Γ' son equivalentes en representaciones entonces $\Gamma\backslash M$ y $\Gamma'\backslash M$ son fuertemente isospectrales.*

Sea $\phi \in C_c(G)$ y definimos el operador $R_\Gamma(\phi)$ on $L^2(\Gamma\backslash G)$ por

$$(R_\Gamma(\phi)f)(x) = \int_G \phi(g)f(xg)dg.$$

Este operador satisface la Fórmula de la Traza de Selberg.

Teorema 9.2 (Fórmula de la Traza de Selberg)**.** *Tenemos*

$$\operatorname{tr} R_\Gamma(\phi) = \sum_{[\gamma]\in A_\Gamma} \int_{C(\gamma,\Gamma)\backslash G} \phi(g^{-1}\gamma g)dg,$$

donde A_Γ denota el conjunto de clases de conjugación de elementos en Γ y $C(\gamma, \Gamma)$ es el centralizador en Γ de γ.

Notar que R_Γ está determinado por su traza. Esto es esencialmente debido a Dixmier [6] y usa el hecho que R_Γ se descompone como suma discreta de representaciones unitarias irreducibles de G con multiplicidades finitas. La idea es como sigue. Sea (π_i) una colección de representaciones unitarias irreducibles de G tal que para toda $\Phi \in C_c(G)$ tenemos

$$\sum m_i \operatorname{tr} \pi_i(\Phi) = \sum n_i \operatorname{tr} \pi_i(\Phi).$$

Supongamos que hay algún i para el que $m_i \neq n_i$. Sin pérdida de generalidad podemos suponer que $m_i > 0$ y $n_i = 0$. Por Dixmier [6, Propositions 5.3.1 and 6.6.5], las representaciones $\sum m_i \operatorname{tr} \pi_i$ and $\sum n_i \operatorname{tr} \pi_i$ son *cuasi-equivalentes*, una condición que implica que $n_i \neq 0$.

Definimos el **peso** de una clase de conjugación $[\gamma]$ en Γ, por una medida sobre $C(\gamma, \Gamma)$, como el volumen $\operatorname{vol}(C(\gamma, \Gamma)\backslash C(\gamma, G))$. Uno entonces deduce lo siguiente de la Fórmula de la Traza de Selberg.

Teorema 9.3. *Si dos subgrupos discretos cocompactos $\Gamma, \Gamma' \leq G$ tienen el mismo número de clases de conjugación con un mismo peso y clase en G, entonces Γ y Γ' son equivalentes en representaciones.*

9.2. Espectro de grupos Kleineanos aritméticos del tipo más simple. Sea k un cuerpo de números que tiene un único lugar complejo y A un álgebra de cuaterniones de división sobre k. Sean $\mathcal{O}, \mathcal{O}'$ órdenes maximales de A y $\Gamma_\mathcal{O}, \Gamma_{\mathcal{O}'}$ los grupos Kleineanos aritméticos asociados. El Corolario 8.7 dice que $\Gamma_\mathcal{O}, \Gamma_{\mathcal{O}'}$ son cocompactos.

Como estamos interesados en construir 3-variedades hiperbólicas, necesitamos asegurarnos que $P\psi(A^1)$ contiene elementos no triviales de orden finito. Supongamos que $P\psi(A^1)$ contiene un elemento de orden n. Entonces $\cos(\pi/n) \in k$ y $k(e^{\pi i/n})$ es una extensión cuadrática de k que se incrusta en A. Hay finitos $n \geq 4$ para los que $[k(e^{\pi i/n}) : \mathbb{Q}] = 2[k : \mathbb{Q}]$, entonces usando apropiadamente el Teorema de Albert-Brauer-Hasse-Noether (que implica que para un álgebra de cuaterniones A sobre k y una extensión cuadrática L de k,

existe un embedding de L en A si y sólo si ningún primo que se parte en L/k ramifica en A) cuando construimos A via el conjunto $\mathrm{Ram}(A)$ de primos que ramifican en A podemos asumir que $P\psi(A^1)$ es libre de torsión. Sigue que $\Gamma_{\mathcal{O}}, \Gamma_{\mathcal{O}'}$ son libres de torsión.

Dado un grupo U y un elemento $x \in U$, denotamos por $[x]_U$ la clase de conjugación de x en U. El siguiente lema se hace claro.

Lema 9.4. *El embedding ψ de A^1 en $G = \mathrm{SL}_2(\mathbb{C})$ induce una biyección entre elementos $\mathcal{O}^1 \setminus \{\pm 1\}$ y $\Gamma_{\mathcal{O}} \setminus \{\pm 1\}$. Sea $x \in \mathcal{O}^1 \setminus \{\pm 1\}$ tal que $\gamma = \psi(x)$ es el elemento correspondiente de $\Gamma_{\mathcal{O}} \setminus \{\pm 1\}$. El centralizador $C(\gamma, \Gamma)$ corresponde a $k(x) \cap \mathcal{O}^1$ y la clase de conjugación $[\gamma]_G \cap \Gamma_{\mathcal{O}}$ corresponde a $[x]_A \cap \mathcal{O}^1$.*

Notar que el cuerpo $k(x)$ es una extensión cuadrática de k que se incrusta en A y $\Omega := k(x) \cap \mathcal{O}$ es un $\mathcal{O}_k$-orden cuadrático de $k(x)$ que es independiente de la elección de x en $[x]_{\mathcal{O}^1}$. Llamaremos B al **orden de la clase de conjugación de** x. Esta discusión, junto con los Teoremas 9.1 y 9.3 y un resultado de Eichler [7, Theorem 2], nos permiten deducir lo siguiente.

Teorema 9.5. *Supongamos que $\mathcal{O}^1$ y $\mathcal{O}'^1$ tienen el mismo número de clases de conjugación de elementos con una traza reducida fija y orden fijos, entonces $\Gamma_{\mathcal{O}} \backslash \mathbf{H}^3$ y $\Gamma_{\mathcal{O}'} \backslash \mathbf{H}^3$ son fuertemente isospectrales.*

Hemos reducido nuestra construcción de 3-variedades hiperbólicas isospectrales al estudio del número de clases de conjugación de elementos en un álgebra de cuaterniones con traza reducida fija. Para simplificar aún más este problema haremos uso del siguiente hecho, probado en [11, Theorem 12.4.5].

Teorema 9.6. *Sea $\mathcal{O}$ como antes y asumimos que $\Gamma_{\mathcal{O}}$ contiene un elemento de traza t_0. Entonces el número de clases de conjugación en $\Gamma_{\mathcal{O}}$ de elementos de $\Gamma_{\mathcal{O}}$ con traza t_0 es independiente de la elección del orden maximal $\mathcal{O}$.*

A la luz de Teoremas 9.5 y 9.6 es suficiente mostrar que si Ω es un $\mathcal{O}_k$-orden cuadrático que se incrusta en $\mathcal{O}$ entonces Ω se incrusta en $\mathcal{O}'$ también. En efecto, si $\Omega = \mathcal{O}_k[x]$ entonces todo embedding de Ω en $\mathcal{O}$ determina (y es determinado por) un elemento de $\mathcal{O}$ con el mismo polinomio característico que x, la imagen en $\mathcal{O}$ de x.

Recordar de la Sección 7.2 que el número de clases de isomorfismos de órdenes maximales de A es llamado el *número de tipo* de A. Resulta que cuando $A \otimes_{\mathbb{Q}} \mathbb{R} \ncong \mathbb{H}^{[k:\mathbb{Q}]}$, es siempre el caso que el número de tipo es una potencia de dos (para una prueba, ver [4]). En particular, en el caso que estamos considerando tiene sentido hablar de Ω incrustado en $\frac{1}{2}$ de las clases de isomorfismos de órdenes maximales de A. (Esto es por supuesto un abuso de lenguaje. Sería más correcto decir que Ω se incrusta en representantes de la mitad de las clases de isomorfismos de órdenes maximales de A).

La pregunta de si todo orden maximal de A admite un embeding de un orden cuadrático fijo Ω tiene una larga historia que retrocede al trabajo de Chevalley en los 1930's. En 1999, Chinburg y Friedman [4] resolvieron completamente este problema y mostraron que la proporción de clases de isomorfismos de órdenes maximales de A que admite un embeding de Ω es igual a 0, $\frac{1}{2}$ o 1. De hecho, su principal teorema da condiciones necesarias y suficientes para que cada una de esas proporciones ocurran. Uno de los resultados de su trabajo, que será suficiente para nuestro propósito, es el siguiente.

Teorema 9.7 (Chinburg-Friedman)**.** *Sea k un cuerpo de números y A un álgebra de cuaterniones sobre k para el que $A \otimes_{\mathbb{Q}} \mathbb{R} \ncong \mathbb{H}^{[k:\mathbb{Q}]}$. Si A es ramificado en un primo finito de k y Ω es un $\mathcal{O}_k$-orden cuadrático que se incrusta en un orden maximal de A entonces todo orden maximal de A admite un embeding de Ω.*

Del Teorema 9.7 y la discusión anterior concluimos lo siguiente.

Teorema 9.8. *Sea k un cuerpo de número con un único lugar complejo y A un álgebra de cuaterniones de división sobre k que ramifica en todos los lugares reales de k. Sean $\mathcal{O}, \mathcal{O}'$ órdenes maximales de A para los que $\Gamma_{\mathcal{O}}$ y $\Gamma_{\mathcal{O}'}$ son libres de torsión. Si A ramifica en un primo finito de k entonces las variedades $\Gamma_{\mathcal{O}}\backslash\mathbf{H}^3$ y $\Gamma_{\mathcal{O}'}\backslash\mathbf{H}^3$ son fuertemente isospectrales.*

Para estar seguros de que las 3-variedades hiperbólicas que construimos no son isométricas primero vemos que si $\Gamma_{\mathcal{O}}\backslash\mathbf{H}^3$ y $\Gamma_{\mathcal{O}'}\backslash\mathbf{H}^3$ fueran isométricas entonces habría un elemento γ en $\mathrm{PGL}_2(\mathbb{C})$ para el que $\Gamma_{\mathcal{O}} = \gamma\Gamma_{\mathcal{O}'}\gamma^{-1}$. La siguiente proposición demuestra que esto a su vez prueba que $\mathcal{O}$ y $\mathcal{O}'$ son conjugados en A^*. Para obtener variedades que no son isométricas es entonces suficiente elegir órdenes maximales que tengan diferentes tipos; esto es, que no sean conjugados en A^*.

Proposición 9.9. *Bajo la misma notación de antes y suponiendo que $\Gamma_{\mathcal{O}} = \gamma\Gamma_{\mathcal{O}'}\gamma^{-1}$ para algún $\gamma \in \mathrm{PGL}_2(\mathbb{C})$, se tiene que $\mathcal{O}$ y $\mathcal{O}'$ son conjugados en A^*.*

Demostración. Sea $\gamma = P(c)$ donde $c \in \mathrm{GL}_2(\mathbb{C})$. Entonces $\psi(A) = A\Gamma_{\mathcal{O}} = A\Gamma_{\mathcal{O}'}$, luego conjugar por c induce un k-automorfismo de A via

$$\sum a_i\gamma_i \mapsto \sum a_i c\gamma_i c^{-1}$$

para $a_i \in k$ y $\gamma_i \in \psi(\mathcal{O}^1)$. Por el Teorema de Skolem–Noether este es un automorfismo interno y existe un elemento $a \in A^*$ tal que $a\mathcal{O}^1a^{-1} = \mathcal{O}'^1$. Ahora consideramos el orden $\mathcal{O}\psi(\mathcal{O}^1)$ de $\psi(A)$ definido por

$$\mathcal{O}\psi(\mathcal{O}^1) := \left\{\sum a_i\gamma_i : a_i \in \mathcal{O}_k, \gamma_i \in \psi(\mathcal{O}^1)\right\}.$$

Supongamos que $\mathcal{D}$ es un orden maximal de A para el que $\psi(D)$ contiene $\mathcal{O}\psi(\mathcal{O}^1)$. Si $\mathcal{D} \neq \mathcal{O}$ entonces $[\Gamma_{\mathcal{O}} : P\psi(\mathcal{D}\cap\mathcal{O})^1] > 1$. Pero $\psi(\mathcal{D}\cap\mathcal{O})^1 \supset (\mathcal{O}\psi(\mathcal{O}^1))^1 \supset \psi(\mathcal{O}^1)$. Luego $\mathcal{D} = \mathcal{O}$ y similarmente, $\mathcal{O}'$ es el único orden maximal de A para el que $\mathcal{O}\psi(\mathcal{O}'^1)$ está contenido en $\psi(\mathcal{O}')$. Como $\psi(a)$ conjuga $\mathcal{O}\psi(\mathcal{O}^1)$ en $\mathcal{O}\psi(\mathcal{O}'^1)$, a debe conjugar $\mathcal{O}$ en $\mathcal{O}'$. □

9.3. Un ejemplo. Sea $k = \mathbb{Q}(\sqrt{-5})$ y consideramos los ideales $\mathfrak{p}_1 = (11)$ y $\mathfrak{p}_2 = (3 + 2\sqrt{-10})$ de $\mathbb{Q}(\sqrt{-5})$. Ambos son ideales primos y tienen norma 121 y 29 respectivamente. Sea A el álgebra de cuaterniones de división sobre k definida por $\mathrm{Ram}(A) = \{\mathfrak{p}_1, \mathfrak{p}_2\}$. En términos de símbolos de Hilbert, A está dada por $\left(\frac{44-11\sqrt{-5}, -38-6\sqrt{-5}}{\mathbb{Q}(\sqrt{-5})}\right)$. Todo esto puede verificarse con el siguiente código de Magma.

```
>k<t>:=QuadraticField(-5);
>Zk:=Integers(k);
>p1:=11*Zk;
>IsPrime(p1);
true
>p2:=(3+2*t)*Zk;
>IsPrime(p2);
true
>Norm(p1);
121
>Norm(p2);
29
>A:=QuaternionAlgebra(p1*p2);
>Basis(A);
[ 1, i, j, k ]
>i:=Basis(A)[2];
```

```
>j:=Basis(A)[3];
>i^2;
(44-11*t)
>j^2;
(-38-6*t)
```

El ideal primo $\mathfrak{p}_1 = (11)$ se parte completamente en $k(\sqrt{-1})$ y $k(\sqrt{-3})$, entonces el Teorema de Albert-Brauer-Hasse-Noether implica que ninguna de estas extensiones se incrusta en A. Ninguna otra extensión ciclotómica de k es cuadrática, entonces A no contiene otras raíces de la unidad aparte de ± 1.

El número de tipo de A es dos, entonces existen órdenes maximales $\mathcal{O}$ y $\mathcal{O}'$ de A que no son conjugados.

```
>#ConjugacyClasses(MaximalOrder(A));
2
```

Hemos mostrado que $\Gamma_{\mathcal{O}}$ y $\Gamma_{\mathcal{O}'}$ son libres de torsión. Sigue del Teorema 9.8 y la Proposición 9.9 que las 3-variedades hiperbólicas aritméticas $\Gamma_{\mathcal{O}}\backslash\mathbf{H}^3$ y $\Gamma_{\mathcal{O}'}\backslash\mathbf{H}^3$ son fuertemente isospectrales pero no isométricas.

Ahora usamos el Teorema 8.3 para calcular el volumen de nuestras 3-variedades hiperbólicas isospectrales. (La ley de Weyl implica que las variedades Riemannianas compactas isospectrales tienen siempre el mismo volumen). En este caso tenemos

$$d_k = 20$$

y

$$\zeta_k(2) = 1{,}855556893747120634762713411 65\ldots$$

entonces

$$\mathrm{Vol}(\Gamma_{\mathcal{O}}\backslash\mathbf{H}^3) = \mathrm{Vol}(\Gamma_{\mathcal{O}'}\backslash\mathbf{H}^3) = \frac{20^{3/2}\cdot(1{,}8555\ldots)\cdot 120\cdot 28}{4\pi^2} = 14,125{,}336712\ldots$$

Nota 9.10. Notar que el Teorema de Rigidez de Mostow implica que cualquier isomorfismo de $\Gamma_{\mathcal{O}}$ y $\Gamma_{\mathcal{O}'}$ debería ser inducido por una isometría de $\Gamma_{\mathcal{O}}\backslash\mathbf{H}^3$ y $\Gamma_{\mathcal{O}'}\backslash\mathbf{H}^3$. Sigue que nuestras 3-variedades fuertemente isospectrales y no isométricas tienen grupos fundamentales no isomorfos.

Referencias

[1] M.F. Atiyah, I.G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] A. Borel, *Commensurability classes and volumes of hyperbolic* 3*-manifolds*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **8**:1, 1–33 (1981).

[3] A. Borel, Harish-Chandra, *Arithmetic subgroups of algebraic groups*, Ann. of Math. (2) **75**, 485–535 (1962).

[4] T. Chinburg, E. Friedman, *An embedding theorem for quaternion algebras*, J. London Math. Soc. (2) **60**:1, 33–44 (1999). DOI: 10.1112/S0024610799007607.

[5] D.M. DeTurck, C. Gordon, *Isospectral deformations. II. Trace formulas, metrics, and potentials*, Comm. Pure Appl. Math. **42**, 1067–1095 (1989). DOI: 10.1002/cpa.3160420803.

[6] J. Dixmier, *Les C^*-algèbres et leurs représentations*, Cahiers Scientifiques, Fasc. XXIX. Gauthier-Villars & Cie, Éditeur-Imprimeur, Paris, 1964.

[7] M. Eichler, *Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörper und ihre L-Reihen*, J. Reine Angew. Math. **179**, 227–251 (1938). DOI: 10.1515/crll.1938.179.227.

[8] S. Helgason, *Differential geometry, Lie groups, and symmetric spaces*, *Grad. Stud. Math.* **34**. Amer. Math. Soc., Providence, 2001.

[9] A.W. Knapp, *Lie groups beyond an introduction*, *Progr. Math.* **140**. Birkhäuser Boston Inc., 2002.
[10] B. Linowitz, *Selectivity in quaternion algebras*, J. Number Theory **132**, 1425–1437 (2012). DOI: 10.1016/j.jnt.2012.01.012.
[11] C. Maclachlan, A.W. Reid, *The arithmetic of hyperbolic 3-manifolds*, Graduate Texts in Mathematics 219, Springer-Verlag, 2003.
[12] M.S. Raghunathan, *Discrete Subgroups of Lie Groups*, Springer-Verlag, New York-Heidelberg, 1972.
[13] M.-F. Vignéras, *Variétés riemanniennes isospectrales et non isométriques*, Ann. of Math. (2) **112**:1, 21–32 (1980). DOI: 10.2307/1971319.
[14] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture notes in mathematics (1980). DOI: 10.2307/1971319.
[15] D. Witte, *Introduction to Arithmetic Groups*, Deductive Press, 2015.

CIEM-FaMAF, Universidad Nacional de Córdoba, Argentina.
Email address: elauret@famaf.unc.edu.ar
Email address: miatello@famaf.unc.edu.ar

Department of Mathematics, Oberlin College, Oberlin, OH, 44074.
Email address: benjamin.linowitz@oberlin.edu