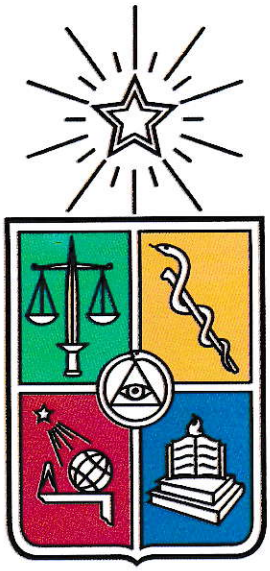


UNIVERSIDAD DE CHILE

FACULTAD DE CIENCIAS

DEPARTAMENTO DE MATEMATICAS

TESIS DE MAGISTER:

PUNTOS FIJOS Y VALORES PROPIOS EN ENDOMORFISMOS DE TOROS COMPLEJOS

Matías Nicolas Alvarado Torres

Director:
Robert Frederick Auffarth Ii

FACULTAD DE CIENCIAS

UNIVERSIDAD DE CHILE

INFORME DE APROBACIÓN
TESIS MAGÍSTER

Se informa a la Escuela de Postgrado de la Facultad de Ciencias que la Tesis de Magíster presentada por el candidato

Matias Nicolas Alvarado Torres

Ha sido aprobada por la Comisión de Evaluación de la Tesis como requisito para optar al grado de Magíster en Ciencias con mención en Matemáticas, en el examen de Defensa de Tesis rendido el día 5 de Enero del 2018.

Director de Tesis

Dr. Robert Auffarth _____

Co-Director de Tesis

Dr. Yves Martin _____

Comisión de Evaluación de la Tesis

Dra. Rubí Rodriguez _____

Dra. Anita Rojas _____

Dedicado a mi familia
y amigos, muy
especialmente mis padres

AGRADECIMIENTOS

Antes que todo, quiero agradecer a mis Padres Fernando y Yanet, por su apoyo incondicional, porque si he llegado hasta aquí es gracias a ellos. Gracias también a mis tíos y abuelos por su preocupación y apoyo, gracias a mis primos y a mis "primos"por tantos buenos momentos.

A los funcionarios del departamento como Santiago Andrews y Cecilia Aguirre. A los profesores, sobretodo a Alicia Labra, Luis Arenas, Yves Martin, Eduardo Friedman, Giancarlo Lucchini, y en especial a Robert Auffarth por ser mi tutor, por la disposición y paciencia que ha tenido conmigo estos 3 años.

Por otro lado quiero a gradecer a todos mis amigos, quienes han sido pilares fundamentales en el día a día, a los que conocí recién entrado en la universidad, a los que conocí en el DIM, los de JGM que me recibieron de forma muy acogedora cuando llegué, a los de Puerto Montt, y en general a todas las personas con las que he compartido estos años. Me encantaria nombrarlos uno por uno, pero por miedo a olvidar a alguien no lo haré.

Por último quiero agradecer a conicyt por otorgarme la beca de magister el segundo año, por los fondos recibidos del proyecto Fondecyt 1150943 del profesor Yves Martin, y al proyecto anillo CONICYT PIA ACT1415 por financiar mi participación en diferentes congresos.

RESUMEN

Dado X un toro complejo y f una función holomorfa de X en X se quiere estudiar el número de puntos fijos de las funciones iteradas f^n y más específicamente el comportamiento asintótico cuando n tiende a infinito. En [4] se demuestra que para dimensión 2 esta sucesión puede tener solo tres tipos de comportamientos, y que esto dependerá de los valores propios de la función. Lo que se hará en este trabajo es introducir algunas herramientas de teoría de números y aproximación diofantina para extender el resultado a dimensiones arbitrarias.

Índice general

Capítulo 1

Preliminares

1.1. Toros complejos y variedades abelianas

Sea V un $\mathbb{C}-$espacio vectorial de dimensión g y L un reticulado en V; es decir, un subgrupo discreto de rango maximal, y por lo tanto isomorfo a $\mathbb{Z}^{2g}$. Entonces a la variedad compleja $T = V/L$ se le llama toro complejo de dimensión g. Se observa que T es un grupo abeliano por ser cuociente de grupos abelianos, y es una variedad compacta por ser L un subgrupo de rango maximal.

Ejemplo 1.1. Consideramos dos vectores $\{z_1, z_2\}$ en $\mathbb{C}$, linealmente independientes sobre $\mathbb{R}$ y definimos $L = \{nz_1 + mz_2 : n, m \in \mathbb{Z}\}$. Entonces $T = \mathbb{C}/L$ es un toro complejo de dimensión uno.

Ejemplo 1.2. Un caso particular del ejemplo anterior es considerar los vectores $\{1, i\}$ en $\mathbb{C}$, que claramente son linealmente independientes sobre $\mathbb{R}$. En este caso el reticulado L es el grupo de los enteros de Gauss $\mathbb{Z}[i]$ (de hecho este tiene estructura de anillo, pero para lo que se quiere hacer esto no hace diferencia). De este modo obtendremos un toro complejo de dimensión 1.

$$T = \mathbb{C}/\mathbb{Z}[i]$$

La gracia de este ejemplo es que podemos ver este toro haciendo la identificación de lados opuestos de un cuadrado de lado 1, de la misma manera que se contruye el toro real de dimensión 2 como un complejo de celdas (ver figura 1.1).

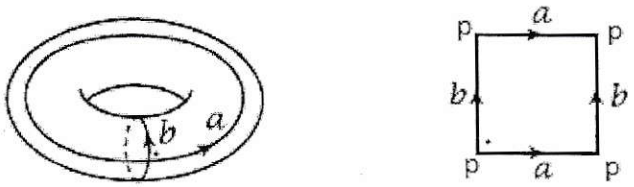


Figura 1.1: incrustación del toro bidimensional real en $\mathbb{R}^3$ y su respectiva representación como CW-complejo de dimensión 2.

En general para representar un toro complejo de la forma $T = V/L$ se escogen bases $\mathcal{V} = \{v_1, ..., v_g\}$ de V como $\mathbb{C}$-espacio vectorial y $f_1, ..., f_{2g}$ de L como $\mathbb{Z}$-módulo. De esta manera al ser $\mathcal{V}$ base de V, se tiene que $f_j = \sum_{i=1}^{g} \pi_{ij} v_i$; con $\pi_{ij} \in \mathbb{C}$. De este modo denotemos por $\pi_{1j}, ..., \pi_{gj}$ las coordenadas de f_j con respecto a la base $\mathcal{V}$.
La matriz

$$\Pi = \begin{pmatrix} \pi_{1,1} & \cdots & \pi_{1,2g} \\ \vdots & \ddots & \vdots \\ \pi_{g,1} & \cdots & \pi_{g,2g} \end{pmatrix}$$

En $\mathbb{M}(g \times 2g, \mathbb{C})$ se llama la matriz período de T (con respecto a las bases escogidas).
Nos preguntamos en este punto ¿es toda matriz $\Pi \in \mathbb{M}(g \times 2g, \mathbb{C})$ la matriz período de algún toro complejo? Para responder a esta interrogante debemos ir a la siguiente proposición.

Proposición 1.3. *$\Pi \in \mathbb{M}(g \times 2g, \mathbb{C})$ es la matriz período de algún toro analítico si y sólo si la matriz $P = \begin{pmatrix} \Pi \\ \overline{\Pi} \end{pmatrix}$ es no singular.*

Demostración. Por lo visto previamente, una matriz Π es la matriz período de un toro complejo si y solamente si los vectores columnas de éste generan un reticulado en el espacio vectorial, y esto pasa si y solo si los vectores columnas son $\mathbb{R}$-linealmente independientes.
Supongamos que las columnas de Π no son linealmente independientes sobre $\mathbb{R}$, es decir, podemos encontrar $x \in \mathbb{R}^{2g}$ no nulo, con $\Pi x = 0$. Luego se tendrá que $Px = 0$.
Reciprocamente si suponemos que P es una matriz no invertible, entonces hay vectores $x, y \in \mathbb{R}^{2g}$, no ambos cero, tales que $P(x+iy) = 0$. Pero esto significa que $\Pi(x+iy) = 0$ y $\overline{\Pi}(x+iy)) = 0$.

Luego $\Pi(x-iy) = \overline{\overline{\Pi}(x+iy)} = 0$. De esta manera como $\Pi(x+iy) = \Pi(x-iy) = 0$, concluimos que $\Pi x = \Pi y = 0$, donde $x \neq 0$ o $y \neq 0$. Luego las columnas de Π no pueden ser linealmente independientes sobre $\mathbb{R}$. Así se concluye que Π no puede ser una matriz período.

□

Ejemplo 1.4. Sean $z_1 = 1$, $z_2 = i$ en $\mathbb{C}$. Podemos tomar la base $\{v = 1\}$ de $\mathbb{C}$ como $\mathbb{C}$-espacio vectorial, y $\{f_1, f_2\} = \{1, i\}$ base de L como $\mathbb{Z}$-módulo. Entonces la matriz período de $T = \mathbb{C}/L$ es $(1\ i)$, y la matriz P de la proposición anterior es $P = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$ que es claramente no singular (determinante no nulo).

Definición 1.5. Sean T_1 y T_2 dos toros complejos. Un homomorfismo de T_1 en T_2 es una función analítica $f : T_1 \to T_2$ compatible con la estructura de grupo.

Definición 1.6. Sea T un toro complejo, y $z_0 \in T$, se define la traslación por z_0 como la función analítica $t_{z_0} : T \to T$ dada por $t_{z_0}(z) = z + z_0$.

Observación. La traslación t_{z_0} no es un homomorfismo de toros complejos (salvo que $z_0 = 0$), ya que no preserva la estructura de grupo, pero sí es una función holomorfa.

Proposición 1.7. *Sea $h : T_1 \to T_2$ una función analítica, con $T_1 = V_1/L_1$ y $T_2 = V_2/L_2$, entonces*

1. *Existe un único homomorfismo de grupos $f : T_1 \to T_2$ tal que*

$$h = t_{h(0)} \circ f$$

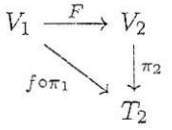
   es decir, $h(z) = f(z) + h(0)\ \forall z \in T_1$.

2. *Existe una única aplicación $\mathbb{C}$-lineal $F : V_1 \to V_2$ con $F(L_1) \subseteq L_2$ que induce el homomorfismo f.*

Demostración. Definimos $f = t_{h(0)} \circ h$, y consideremos la siguiente composición de funciones

$$V_1 \xrightarrow{\pi_1} T_1 \xrightarrow{f} T_2$$

Por otro lado como V_2 es el recubrimiento universal de T_2, la función $f \circ \pi_1$ puede ser levantada a una función $F : V_1 \longrightarrow V_2$ analítica de forma única de manera que el diagrama siguiente conmute



y tal que $F(0) = 0$.
De la conmutatividad del diagrama vemos que $F(v+l) - F(v) \in L_2$, para todo $l \in L_1$ y $v \in V_1$. Entonces esta función de v es constante. Así

$$F(v + l) = F(v) + F(l)$$

para todo $l \in L_1$ y $v \in V_1$, y por lo tanto las derivadas parciales de F son periódicas con períodos L_1, y por lo tanto constantes. Como $F(0) = 0$, se sigue que F es $\mathbb{C}$-lineal.

□

El conjunto de todos los homomorfismos de T_1 en T_2 forman un grupo abeliano (con la operación suma punto a punto), denotado por $Hom(T_1, T_2)$. La proposición anterior nos entrega un monomorfismo de grupos

$$\rho_a : Hom(T_1, T_2) \to Hom_{\mathbb{C}}(V_1, V_2)$$

(donde $Hom_{\mathbb{C}}(V_1, V_2)$ es el espacio vectorial complejo de transformaciones $\mathbb{C}$-lineales entre los $\mathbb{C}$-espacios vectoriales V_1 y V_2) dado por $\rho_a(f) = F$ y llamada la representación analítica de $Hom(T_1, T_2)$. $\rho_a(f)$ recibe el nombre de representación analítica de f.

Por otro lado, la restricción $F_{L_1} : L_1 \to L_2$ de F al reticulado L_1 es $\mathbb{Z}$ -lineal. Así se tiene un monomorfismo

$$\rho_r : Hom(T_1, T_2) \to Hom_{\mathbb{Z}}(L_1, L_2)$$

(donde $Hom_{\mathbb{Z}}(L_1, L_2)$ es el grupo de homomorfismos de $\mathbb{Z}$ - módulos entre L_1 y L_2) dado por $\rho_r(f) = F_{L_1}$ y llamado la representación racional de $Hom(T_1, T_2)$, y a $\rho_r(f)$ la representación racional de f.

Definición 1.8. Cuando $T_1 = T_2$, los homomorfismos $f : T_1 \to T_1$ son llamados endomorfismos de T_1. Al conjunto de todos los endomorfismos lo denotamos por $End(T_1)$.

Ejemplo 1.9. Dado un toro $T = V/L$ y un entero n, se tiene el endomorfismo $n_T : T \to T$, cuya representación analítica esta dada por $\rho_a(n_T) : V \to V$, $\rho_a(n_T)(z) = nz$.

Definición 1.10. Sea $T = V/L$ un toro y S un subconjunto de T. Se dice que S es un subtoro de T si existe un subespacio W de V y un reticulado M en W tal que $M \subseteq W \cap L$ y tal que $S = W/M$.

Proposición 1.11. *Sea $f : T_1 \to T_2$ un homomorfismo de toros. Entonces*

(1) Imf es un subtoro de T_2.

(2) $Kerf$ es un subgrupo compacto de T_1. Su componente conexa que contiene a 0, denotada por $(kerf)_0$, es un subtoro de T_1 de índice finito en $kerf$.

Demostración. Lo primero que se debe notar es que $V_3 := F(V_1) \subseteq V_2$ es un subespacio vectorial. Por otra parte $L_3 := L_2 \cap F(V_1)$ es discreto, pues está contenido en L_2 y además genera a V_3 como $\mathbb{R}$-espacio vectorial. De esta manera se concluye que $Imf = V_3/L_3$. Así queda demostrado (1).
Ahora se probará (2). Como $kerf = f^{-1}(0_{T_2})$, se tiene que $kerf$ es un subgrupo cerrado de T_1, y por lo tanto compacto (cerrado en un compacto es compacto). Luego tiene una cantidad finita de componentes conexas, y cada una compacta. De esta manera $(kerf)_0$ es conexa, por lo que sólo basta probar que este es un subtoro.
Como la representación analítica F de f es lineal, se tiene que $V_4 := F^{-1}(L_2)_0$ es un subespacio vectorial de V_1. De esta manera se ve que $(kerf)_0 = V_4/L_1 \cap V_4$, pero como $(kerf)_0$ es compacto, se tiene que $L_1 \cap V_4$ tiene que ser de rango maximal, luego es un reticulado en V_4. De esta manera se concluye que $(kerf)_0$ es un subtoro de T_1.

□

Observación. Para todo toro $T = V/L$ y un entero $n \neq 0$, el endomorfismo n_T de T definido anteriormente tiene como núcleo a los puntos de orden n en T, también llamados puntos de n-torsión, y denotados por $T[n]$. Además se tiene que $T[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$

A continuación se introducirá la noción de variedad abeliana, objetos particularmente importantes en geometría algebraica y geometría compleja. La definición que se dará es la más cómoda para trabajar en este contexto, sin embargo, se pueden encontrar otras definiciones equivalentes en la literatura.

Definición 1.12. Sea dirá que un toro $T = V/L$ es una variedad abeliana si es que tiene una inmersión a algún espacio proyectivo.

Ejemplo 1.13. Se define una curva elíptica E como una curva proyectiva de género 1. Estas curvas tienen estructura de grupo abeliano (ver [18] para mayor detalle de la estructura de éste), luego las curvas elípticas son variedades abelianas.

Veremos en la siguiente proposición que podemos considerar productos de variedades abelianas para obtener nuevamente una variedad abeliana

Proposición 1.14. *Dado X, Y dos variedades abelianas, entonces el producto $X \times Y$ es una variedades abeliana.*

Demostración. Decir que X e Y son variedades abelianas, es equivalentes a decir que son toros complejos, con estructura de variedad algebraica proyectiva. Luego X, Y son proyectivas, por lo tanto $X \times Y$ es proyectiva (ver [17, Sección 5, Capítulo 1]). Además, por otro lado, es directo que producto de toros es un toro. Así concluimos que producto de variedades abelianas es abeliana. □

1.2. Álgebra y teoría de números algebraicos

1.2.1. Teoría de cuerpos y Galois

En lo que sigue, aparecerán frecuentemente extensiones finitas de $\mathbb{Q}$ y sus respectivos anillos de enteros, por lo que se repasará y establecerá cierta notación y convenciones.
Todas las extensiones de cuerpos que consideraremos serán finitas (por lo tanto algebraicas) sobre $\mathbb{Q}$, por lo tanto pensaremos que todas ellas están dentro de una misma clausura algebraica $\overline{\mathbb{Q}}$ de $\mathbb{Q}$, más aún supondremos que esta clausura está contenida en el cuerpo de los números complejos $\mathbb{C}$.

$$\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$$

Definición 1.15. Sea K una extensión finita de $\mathbb{Q}$, entonces diremos que K es un cuerpo de números.

Otro hecho importante es que en la teoría general, dada una extensión de cuerpos L/K, existen s incrustaciones $L \hookrightarrow \overline{K}$ que fijan K, donde s es el grado de separabilidad de la extensión. Afortunadamente como se trabajará sólo con cuerpos de números, el grado de separabilidad coincide con el grado de la extensión.
De este modo un cuerpo de números K tiene n incrustaciones en $\overline{\mathbb{Q}}$, pero se acostumbra a decir (y es como se dirá en este trabajo) que K tiene n incrustaciones en $\mathbb{C}$. Otro hecho importante digno de recalcar es el siguiente.

Observación. Dada una incrustación, digamos τ, entonces $\overline{\tau}$ también define una incrustación, y de hecho esta será distinta si τ no toma sólo valores reales. De esta manera, podemos escribir el siguiente resultado.

Proposición 1.16. *Un cuerpo de números K de grado n, tiene n incrustaciones a $\mathbb{C}$, r de las cuales son reales y $2s$ son no reales, para ciertos números $r, s \in \mathbb{N}$, con $r + 2s = n$*

Demostración. Es directo del hecho que los cuerpos de números son extensiones separables de $\mathbb{Q}$, de la observación anterior, y de que se fijó una clausura algebraica de $\mathbb{Q}$ dentro de los números complejos. □

Observación. La configuración o tupla (r, s) recibe el nombre de signatura de K.

Una función muy importante en teoría de cuerpos, álgebras y teoría de números, es la norma asociada a una extensión. En lo que sigue se definirán y expondrán algunos resultados y hechos básicos.

Sea L/F una extensión finita de cuerpos de grado n. Entonces podemos ver a L como un F-espacio vectorial de dimensión n. Tomemos un elemento $\alpha \in L$ diferente de cero y definamos la aplicación F-lineal

$$\begin{aligned} m_\alpha \quad : L \quad &\longrightarrow \quad L \\ x \quad &\longmapsto \quad \alpha x \end{aligned}$$

Una comprobación rápida muesta que m_α es invertible, de hecho $m_\alpha^{-1} = m_{\alpha^{-1}}$. Como m_α es una aplicación F-lineal, tenemos que dada una F-base de L, existe una matriz M_α con coeficientes en F que representa a m_α. Como m_α es invertible, se tiene que $\det M_\alpha \neq 0$. De esta manera definimos la siguiente función:

$$\begin{aligned} N_{L/F} \quad : L^* \quad &\longrightarrow \quad F^* \\ \alpha \quad &\longmapsto \quad \det M_\alpha \end{aligned}$$

A esta aplicación se le llama la norma de L/F

Lo primero que debemos observar es que al estar la norma definida como el determinante de una matriz, esta debería tener alguna propiedad de tipo multiplicativo, y de hecho es así y se verá en la siguiente proposición.

Proposición 1.17. *La función norma recién definida es un homomorfismo entre los grupos multiplicativos L^* y F^*.*

Demostración. Es directo del hecho que $M_\alpha M_\beta = M_{\alpha\beta}$ □

Una de las características de la norma es que aparece frecuentemente, y de distintas maneras, es por eso que se darán las caracterizaciones más usadas que ésta tiene.

Proposición 1.18. *Dada una extensión de cuerpos L/F, la norma $N_{L/F}$ se puede calcular de siguientes formas equivalentes.*

a) *El determinante de la matriz M_α asociada a la función m_α*

b) *si $\alpha \in L$, y $\alpha_1, \alpha_2, ..., \alpha_m$ son sus conjugados (en el sentido de Galois), entonces* $N_{L/F}(\alpha) = \left(\prod_{i=1}^{m} \alpha_i\right)^{n/m}$

c) *Si $p(t) = t^m + a_{m-1}t^{m-1} + ... + a_1 t + a_0 \in F[t]$ es el polinomio minimal de α sobre F, entonces $N_{L/F}(\alpha) = a_0^{n/m}$*

d) si $\sigma_1, ..., \sigma_n$ son las distintas n incrustaciones de L en $\overline{F}$, entonces $N_{L/F}(\alpha) = \left(\prod_{i=1}^{m} \sigma_i(\alpha)\right)^{[L:F]_i}$ *donde $[L : F]_i$ es el grado de inseparabilidad de la extensión L/F (en el caso de cuerpos de números este grado es 1).*

Demostración. Una demostración puede ser encontrada en [15, Teorema 8.6 y Teorema 8.12] □

1.2.2. Teoría de números algebraicos

Los anillos que se usarán siempre serán asociativos, conmutativos y con elemento unidad, además cuando se tengan contenciones de anillos ($A \subseteq B$) se asumirá que $1_B = 1_A$.

Sean A, B anillos tales que $A \subseteq B$ como subanillo. Entonces diremos que un elemento $b \in B$ es entero (o integral) sobre A si este satisface un polinomio mónico con coeficientes en A; es decir, existen $a_0, ..., a_{n-1} \in A$ tales que

$$b^n + a_{n-1}b^{n-1} + ... + a_1 b + a_0 = 0$$

Si todo elemento $b \in B$ es entero sobre A, entonces diremos que B es entero sobre A.

A continuación se darán caracterizaciones equivalentes a que un elemento en B sea entero sobre un anillo A.

Proposición 1.19. *Sean A, B dos anillos tales que $A \subseteq B$, y sea $b \in B$. Entonces las siguientes afirmaciones son equivalentes:*

i. b es un elemento entero sobre A

ii. $A[b]$ es un A-módulo finitamente generado

iii. Existe un anillo intermedio $A \subseteq C \subseteq B$ que contiene a b y que es finitamente generado como A-módulo

Demostración. La demostración de esta proposición se puede encontrar en [2, Proposición 5.1]. □

Vamos a ver ahora que dada cualquier extensión de anillos $A \subseteq B$, el conjunto de elementos enteros es interesante y tiene buenas propiedades.

Proposición 1.20. *Sea $A \subseteq B$ una extensión de anillos, consideremos el conjunto $C := \{b \in B \mid b$ es entero sobre $A\}$. Entonces el conjunto C es un anillo. Este anillo es conocido como la clausura integral de A sobre B*

Demostración. Ver [2, Corolario 5.3]. □

El tipo de extensiones de anillos que nos va a interesar es el siguiente:

Sea K un cuerpo de números, de esta manera tenemos la extensión de anillos $\mathbb{Z} \subseteq K$. Se define $\mathcal{O}_K$ como la clausura integral de $\mathbb{Z}$ en K.

Alguna propiedades importantes que tiene $\mathcal{O}_K$ y que pueden ser de interés, es que es un dominio Noetheriano, normal y de dimensión 1. A este tipo de anillos se le llama dominio de Dedekind (ver [16, Sec 8, Capítulo 1]).

Otros hechos importantes son los siguientes:

Proposición 1.21. *Sea $K/\mathbb{Q}$ un cuerpo de números de grado n, entonces $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo de rango n, es decir, genera a K como $\mathbb{Q}$-espacio vectorial ($\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_K = K$)*

Demostración. Ver [16, Proposición 2.10, Capítulo 1]. □

Teorema 1.22 (Teorema de las unidades de Dirichlet). *Sea k un cuerpo de números, entonces el grupo de unidades $\mathcal{O}_k^*$ de $\mathcal{O}_k$ es isomorfo al producto del grupo finito $\mu(k)$ y el grupo abeliano libre de rango $r + s - 1$; donde $\mu(k)$ es el grupo de raíces de la unidad contenidas en k, y (r, s) es la signatura de k.*

Demostración. Ver [16, Teorema 7.4 Capítulo 1] □

1.2.3. Polinomios y teoría de números

El comportamiento de $\#Fix(f^n)$ está íntimamente relacionado con los valores propios de la representación analítica de f. Pero estos valores propios también aparecen como raíces del polinomio característico de la representación racional de f (ver 1.1). La particularidad de este polinomio es que es mónico y tiene coeficientes en $\mathbb{Z}$. Este hecho crea un lazo entre el problema que se está estudiando y teoria de números, ya que, dicho en otro lenguaje, los valores propios que gobiernan el comportamiento estudiado son enteros algebraicos, tema central en teoría algebraíca de números.

Se necesitará algunos lemas de esta teoría que nos ayudarán mas adelante en el desarrollo del trabajo.

Lo primero que debemos ver es qué sucede cuando en un polinomio mónico con coefientes enteros aparecen solo raíces con módulo igual a 1.

Teorema 1.23 (Kronecker). *Sea $T(X) \in \mathbb{Z}[X]$ un polinomio mónico con coeficientes enteros. Supongamos que todas las raíces de T tienen módulo igual a 1. Entonces todas las raíces de T son raíces de la unidad.*

Demostración. Sin pérdida de generalidad podemos suponer que el polinomio $T(X)$ es irreducible, pues si no lo es, podemos aplicar el resultado a cada factor irreducible de este. Si $\alpha_1, ..., \alpha_n$ son todas las raíces, entonces podemos escribir $T(X) = \prod_{1 \leqslant i \leqslant n} (X - \alpha_i)$ y para cada $k \geqslant 1$ consideramos el polinomio $T_k(X) = \prod_{1 \leqslant i \leqslant n} (X - \alpha_i^k)$. Los coeficientes de $T_k(X)$ están en $\mathbb{Z}$, ya que, sus raíces son enteros algebraicos, pues los α_i son enteros algebraicos. Además, como siempre, los coeficientes de $T_k(X)$ son polinomios simétricos , luego el coeficiente de X^{n-m} está acotado por $\binom{n}{m}$, pues $|\alpha_i^k| = 1$. Lo que esto nos dice es que en total hay un número finito de posibles polinomios $T_k(X)$, en particular el número de posibilidades para α_i^k es finito. Luego existen dos enteros $k_1 \neq k_2$ tales que $\alpha_i^{k_1} = \alpha_i^{k_2} \Rightarrow \alpha_i^{k_1 - k_2} = 1$, es decir α_i es raíz de la unidad. Luego como habíamos supuesto $T(X)$ irreducible, se tiene que todas las otras raíces deben ser raíces de la unidad, pues son conjugados de α_i (basta aplicar el grupo de Galois de la clausura normal de $T(X)$). □

Ahora veremos que los enteros algebraicos de módulo 1 tienen polinomios minimales especiales, los cuales tienen bastantes propiedades interesantes.

Proposición 1.24. *Sea $a \in \mathbb{C}$ un entero algebraico de valor absoluto 1 y diferente de ± 1. Entonces su polinomio minimal es un polinomio sobre $\mathbb{Z}$ de grado par con coeficientes simétricos, cuyas raíces aparecen en pares conjugados.*

Demostración. Claramente el polinomio minimal es mónico y tiene coeficientes en $\mathbb{Z}$ pues el elemento a es entero. Ahora nos resta probar la simetría del polinomio.

Como $|a| = 1$ tenemos que $1/a = \overline{a}$, además sabemos que $\overline{a}$ es raiz del polinomio (pues tiene coeficientes reales). Por otra parte tenemos que

$$h(1/\overline{a}) = h(a) = 0$$

Así, $\overline{a}$ es también raíz del polinomio $t^n h(1/t)$ que es de grado n, luego $t^n h(1/t) = c \cdot h(t)$ para algun $c \in \mathbb{Q}$. Tomando $t = 1$ tenemos que $h(1) = c \cdot h(1)$, pero como supusimos que a era distinto de ± 1 se tiene que $h(1) \neq 0$, luego $c = 1$. de esta manera

$$t^n h(1/t) = h(t)$$

con esto se concluye que las raíces aparecen a pares recíprocos y por lo tanto el polinomio tiene grado par. □

Observación. A este tipo de polinomios también se le llama palindrómico, pues los coeficientes se leen igual de derecha a izquierda que de izquierda a derecha.

1.3. Algunos resultados de análisis armónico y criterio de equidistribución de Weyl.

En la demostración del Teorema principal todo se reducirá a estudiar el comportamiento de la sucesión $\{\lambda^n\}_{n\in\mathbb{N}}$, donde λ es un elemento algebraico que no es raíz de la unidad. Usaremos algunas herramientas de análisis armónico para decir con mayor certeza como es que se distribuyen estas potencias en el círculo unitario.

A continuación desarrollaremos un poco de esta teoría, basandonos en [10].

Una observación muy importante es que estudiaremos distribuciones en el círculo unitario y en el intervalo, usando la parte entera, sin hacer mayor distinción entre ellas. Estas son dos formas distintas, pero equivalentes de hablar de lo mismo, ya que, el círculo unitario lo podemos ver como un toro real unidimensional, que se obtiene como el cuociente de grupos topologicos abelianos $\mathbb{R}/\mathbb{Z}$ (el equivalente unidimensional de la figura 1.1).

Dado un número real cualquiera u, se puede considerar $[u]$ como la parte entera de u, y (u) como la parte fraccionaria. Claramente $u = [u] + (u)$. Se observa que $0 \leq (u) < 1$. Si u es irracional, entonces la sucesión (ku), $k = 1, 2, ...$ se mueve a lo largo del intervalo $(0, 1)$ (no puede ser cero,

pues en ese caso ku seria un entero, pero esto no puede pasar). Haciendo el análogo a lo que nosotros queremos, ver la sucesión $\{(ku)\}_{k\in\mathbb{N}}$ es equivalente que ver la sucesión que nos importa en el círculo, pues hay una biyección entre las raíces de la unidad y el conjunto $\mathbb{Q}\cap[0,1)$.
Sea u_k una sucesión de números reales contenidos en un intervalo I. Para cualquier subintervalo $J\subseteq I$, tomaremos $\mu(J)$ la medida en el sentido de Lebesgue, y $J(n)$ el número de elementos de $u_1,...,u_n$ que pertenecen a J. Esta secuencia de puntos se llamará equidistribuida o uniformemente distibuida en I si para cada J subintervalo contenido en I.

$$\lim_{n\to\infty}\frac{J(n)}{n}=\frac{\mu(J)}{\mu(I)}$$

Ahora veremos un teorema que nos permite ver esta definición de secuencias equidistribuidas en lenguaje netamente analítico.

Teorema 1.25. *(Criterio de equidistribución de Weyl) Una secuencia $\{u_k\}$ contenida en el intervalo $[0,2\pi)$ es uniformemente distribuida en el intervalo si y solamente si*

$$\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}f(u_k)=\int f(t)d\mu \tag{1.1}$$

para toda función f que es continua y 2π-periódica.
De hecho se tiene que es suficiente que 1.1 se cumpla para las funciones e^{ijt}(para todo entero j), es decir, de debe cumplir que

$$\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}e^{iju_k}=0 \tag{1.2}$$

Demostración. Una demostración de este teorema puede ser encontrada en [10]. No se demostrará aquí debido a que la demostración de esto no juega un papel preponderante en lo que sigue, sumado a lo técnica que ésta es. □

En esta sección usaremos la siguiente notación: Para un número real $\alpha\in\mathbb{R}$, $||\alpha||$ denota la distancia al entero más cercano

Lema 1.26. *Sean $\alpha,\beta\in\mathbb{R}$. Entonces para $N\in\mathbb{N}$,*

$$|\sum_{n=1}^{N}e(\alpha n+\beta)|\leq min\{N,(2||\alpha||)^{-1}\}$$

Demostración. Primeramente debemos observar que la constante β no afecta la desigualdad, pues

$$\left|\sum_{n=1}^{N} e(\alpha n+\beta)\right| = |e(\beta)|\left|\sum_{n=1}^{N} e(\alpha n)\right| = \left|\sum_{n=1}^{N} e(\alpha n)\right|$$

Si $\alpha = 0$, entonces la suma es N $(e(0) = 1)$. Si $\alpha \neq 0$, entonces la suma es $e(\alpha)\dfrac{1-e(\alpha n)}{1-e(\alpha)}$, pues es una suma geométrica. Por otra parte sabemos que el seno complejo cumple con la siguiente identidad

$$sin(z) = \frac{1}{2i}(e^{iz} - e^{-iz})$$

Luego la suma anterior es a lo más $|sin\pi\alpha|^{-1}$. como $sin\pi\alpha \geq 2||\alpha||$ se concluye la desigualdad.

□

Teorema 1.27. *(Teorema de equidistribución de Weyl): Sea α un número real irracional. Entonces la sucesión $\{(\alpha n)\}$ es equidistribuida*

Demostración. Por el criterio de equidistribución de Weyl, nos basta con probar que para todo $k \in \mathbb{N}$ se tiene

$$\lim_{N\to\infty} \frac{1}{N}\left|\sum_{n=1}^{N} e(k\alpha n)\right| = 0$$

Como $k\alpha$ es irracional, entonces por Lema 1.26, si N es suficientemente grande entonces las sumas parciales dan a los mas $1/2||k\alpha||$. Lo importante de todo esto es que esta cota es independiente del N (cuando este es grande por supuesto). Luego

$$\frac{1}{N}\left|\sum_{n=1}^{N} e(k\alpha n)\right| \leq \frac{1}{2N||k\alpha||} \longrightarrow 0$$

Así concluimos que la sucesión que nos interesa es equidistribuida en el círculo unitario.

□

Capítulo 2

Puntos fijos y valores propios

2.1. Fórmula para el número de puntos fijos

Consideremos X un toro complejo de dimensión g y $f : X \to X$ una aplicación holomorfa, que no tiene que ser necesariamente un homomorfismo de grupos. Se probó en la Sección 1.1 que f es una traslación ($f = h + a$) de un endomorfismo de toros $h \in End(X)$ por algún elemento a en la variedad X.

Observación. $f^n = h^n + b$, donde b es un elemento de X. Por inducción se demuestra que $f^n(x) = h^n(x) + \left(\sum_{i=0}^{n-1} h^i(a)\right)$

Definición 2.1. Dado una aplicación holomorfa $f : X \to X$, se define el conjunto:

$$Fix(f) = \{x \in X | f(x) = x\}$$

Además junto con esto, definimos:

$$\#Fix(f) = \begin{cases} \text{El cardinal del conjunto } Fix(f) \text{ si este es finito} \\ 0 \text{ en caso contrario} \end{cases}$$

Proposición 2.2. *Sea $f : X \to X$ una aplicación holomorfa, y sea $h : X \to X$ el endomorfismo de toros que es un trasladado de f. Entonces*

$$\#Fix(f) = \#Fix(h)$$

Demostración. Ver [5, Lema 1.1]. □

La importancia de la proposición precedente es que si queremos entender el número de puntos fijos de las funciones holomorfas de X en X, nos basta con estudiar los puntos fijos de los endomorfismos de X.

Corolario 2.3. *Sea $f : X \to X$ una aplicación holomorfa, y sea $h : X \to X$ el endomorfismo de toros que es un trasladado de f. Entonces*

$$\#Fix(f^n) = \#Fix(h^n)$$

Demostración. Es directo de la proposición y la observación precedentes □

Proposición 2.4. *Dado $f : X \to X$ un endomorfismo de un toro complejo g-dimensional, y $\lambda_1, ..., \lambda_g$ los valores propios de la representación analítica de f, entonces se tiene que*

$$\#Fix(f^n) = \left|\prod_{i=1}^{g}(1 - \lambda_i^n)\right|^2$$

Demostración. Por la Fórmula de Puntos Fijos de Lefschetz para funciones holomorfas (ver [5, Teorema 1.2]), el número de puntos fijos puede ser calculado de la representación analítica $\rho_a(f) \in \mathbb{M}_g(\mathbb{C})$,

$$\#Fix(f^n) = |\det(1_g - \rho_a(f)^n)|^2.$$

Como los valores propios de $\rho_a(f^n)$ son $\lambda_1^n, ..., \lambda_g^n$, concluimos que el número de puntos fijos viene dado por la fórmula anterior. □

Por comodidad diremos que $\lambda_1, ..., \lambda_g$ son los valores propios de f.
La proposición nos dice que la asignación $n \mapsto \#Fix(f^n)$ está gobernada por los valores propios de f, y más aún, por el tamaño de estos.

De esta proposición podemos sacar directamente el siguiente corolario.

Corolario 2.5. *Sea $f : X \to X$ un endomorfismo de un toro complejo, tal que, todos sus valores propios tienen módulo mayor a 1, entonces la sucesión de números de puntos fijos $\{\#Fix(f^n)\}$ tiene crecimiento exponencial.*

Ejemplo 2.6. Sea X un toro complejo de dimensión g y sea $f = m_X$, es decir la función multiplicación por m. Observamos que la representación analítica de f viene dada por la función $F : V \to V$, tal que $v \mapsto mv$. Es fácil darse cuenta que los valores propios de F son m con multiplicidad g. Luego

$$\#Fix(f^n) = (m^n - 1)^{2g}$$

A continuación vamos a mostrar un ejemplo en dimensión 2.

Ejemplo 2.7. Sea E una curva elíptica, con esta construimos el toro $X = E \times E$ y definimos la aplicación

$$f : X \to X \ , \ (x, y) \mapsto (x - y, x)$$

f tiene como valores propios a $\frac{1+\sqrt{-3}}{2}$ y $\frac{1-\sqrt{-3}}{2}$

Observamos que ambos valores propios son raíces sextas de la unidad, por lo que para calcular la cantidad de puntos fijos de la función iterada nos basta con calcular las primeras 6 potencias de ambos.

- $(\frac{1+\sqrt{-3}}{2})^2 = (\frac{-1+\sqrt{-3}}{2}), (\frac{1-\sqrt{-3}}{2})^2 = (\frac{-1-\sqrt{-3}}{2})$
- $(\frac{1+\sqrt{-3}}{2})^3 = -1, (\frac{1-\sqrt{-3}}{2})^3 = -1$
- $(\frac{1+\sqrt{-3}}{2})^4 = (\frac{-1-\sqrt{-3}}{2}), (\frac{1-\sqrt{-3}}{2})^4 = (\frac{-1+\sqrt{-3}}{2})$
- $(\frac{1+\sqrt{-3}}{2})^5 = (\frac{1-\sqrt{-3}}{2}), (\frac{1-\sqrt{-3}}{2})^5 = (\frac{1+\sqrt{-3}}{2})$
- $(\frac{1+\sqrt{-3}}{2})^6 = 1, (\frac{1-\sqrt{-3}}{2})^6 = 1$

De esta manera concluimos que

$$\#Fix(f^n) = \begin{cases} 0, & \text{if } n \equiv 0 \pmod 6 \\ 1, & \text{if } n \equiv 1 \ o \ n \equiv 5 \pmod 6 \\ 9, & \text{if } n \equiv 2 \ o \ n \equiv 4 \pmod 6 \\ 16, & \text{if } n \equiv 3 \pmod 6 \end{cases}$$

2.2. El problema para dimensión 2

En esta sección nos enfocaremos específicamente al estudio de endomorfismos de toros complejos de dimensión 2, en particular desarrollaremos el trabajo de Thomas Bauer y Thorsten Herrig sobre este tema (ver [4]).
El método que se pretende usar para lograr entender el comportamiento de la sucesión $\{\#Fix(f^n)\}$ es tratar de ver todos los posibles tipos de valores propios que puede tener un endomorfismo de toro. A continuación veremos que están estos valores muy restringidos, por lo que se puede dar una caracterización completa mediante una serie de resultados.
Lo primero que veremos es que no todos los valores propios de un endomorfismo pueden tener módulo menor a 1.

Proposición 2.8. *Sea X un toro complejo de dimensión 2 y $f : X \to X$ un endomorfismo. Si f tiene un valor propio no nulo y de módulo menor a 1, entonces también tiene un valor propio de módulo mayor a 1.*

Demostración. Ver [4] □

Una Proposición parecida a esta se puede enunciar para el caso en que el toro tenga dimensión arbitraria, pero eso se verá más adelante.
Ahora nos gustaría estudiar el caso particular de los valores propios que tienen módulo igual a uno. La siguiente proposición nos dirá exactamente qué es lo que pasa cuando aparece un valor propio con valor absoluto igual a 1.

Proposición 2.9. *Sea X un toro complejo 2-dimensional y $f : X \to X$ un endomorfismo. Si λ_1 es un valor propio de f, con $|\lambda_1| = 1$, entonces λ_1 es una raíz de la unidad.*

Demostración. Ver [4, Proposición 1.7] □

Luego de estas dos proposiciones previas, estamos en condiciones de enunciar el teorema principal de [4], en el que se caracteriza por completo el comportamiento asintótico del número de puntos fijos de un endomorfismo de toros complejos bidimensional.

Teorema 2.10. *Sea X un toro complejo 2-dimensional y sea $f : X \longrightarrow X$ un endomorfismo. Entonces la función de puntos fijos $n \mapsto \#Fix(f^n)$ tiene uno de los siguientes comportamientos.*

(C1) Su crecimiento es exponencial en n; es decir, existen constantes reales $A, B > 1$ y un entero N tal que para todo $n \geq N$,

$$A^n \leq \#Fix(f^n) \leq B^n.$$

En este caso ambos valores propios de f tienen módulo distinto de 1

(C2) Es una función periódica. En este caso los valores propios distintos de cero de f son raíces de la unidad, y ellos están contenidos en el conjunto de las k-ésimas raíces de la unidad, donde $k \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$

(C3) Es de la forma

$$\#Fix(f^n) = \begin{cases} 0 & si\ n \equiv 0\ (mod\ r) \\ h(n) & en\ otro\ caso \end{cases}$$

Donde $r \geq 2$ es un entero y h es una función de crecimiento exponencial. En este caso uno de los valores propios de f es de valor absoluto mayor que 1 y el otro es una raíz de la unidad.

Cada uno de estos tres casos ocurren en toros proyectivos, es decir, en superficies abelianas.

Demostración. Sean λ_1, λ_2 los valores propios de f, sin pérdida de generalidad podemos suponer que $|\lambda_1| \leq |\lambda_2|$. Sabemos que

$$\#Fix(f^n) = |(1 - \lambda_1^n)(1 - \lambda_2^n)|^2$$

Supongamos primero que $|\lambda_1| > 1$. Entonces por la suposición que acabamos de hacer tenemos que $|\lambda_2| > 1$, entonces las sucesión de puntos fijos tendrá el comportamiento (C1).
Ahora veamos el caso en que $0 < |\lambda_1| < 1$. Sigue de la Proposición 2.8 que $|\lambda_2| > 1$, y en este caso también se tendrá crecimiento exponencial, pues $|(1 - \lambda_2^n)| \longrightarrow \infty$ de forma exponencial,

mientras que $|(1-\lambda_1^n)| \longrightarrow 1$.

Ahora nos queda solo el caso en que $|\lambda_1| = 1$, por Proposición 2.9 se tiene que λ_1 debe ser una raíz de la unidad. Observamos que $|\lambda_2|$ no puede ser menor que uno por Proposición 2.8. Si $|\lambda_2| = 1$, entonces λ_2 es una raíz de la unidad, luego es claro que el comportamiento de $\#Fix(f^n)$ es periódico, es decir, tiene el comportamiento (C2). Finalmente si $|\lambda_2| > 1$, entonces la función de puntos fijos tiene el comportamiento (C3). En cualquier caso, las raíces de la unidad que aparecen son enteros algebraicos de grado menor o igual a 4, entonces ellas son raíces k-ésimas de la unidad solo para $k \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$(que son los números tal que $\phi(k) \leq 4$, donde la función ϕ es la función de Euler).

Para concluir veremos qué pasa si $\lambda_1 = 0$. En este caso tendremos comportamiento (C1) si $|\lambda_2| > 1$ y comportamiento (C2) si $|\lambda_2| = 1$. Recordemos que por Proposición 2.8 no se puede dar el caso en que $|\lambda_2| < 1$.

Para concluir debemos ver que cada uno de estos comportamientos aparece en algún endomorfismo de superficie abeliana.

El comportamiento (C1) ocurre en la multiplicación por un entero $x \mapsto mx$ en cualquier superficie abeliana X y para $|m| \geq 2$. El Ejemplo 2.11 a continuación mostrará el comportamiento (C3), y el Ejemplo 2.7 muestra el comportamiento (C2).

Es importante observar que los dos últimos ejemplos son superficies abelianas por ser producto de curvas elípticas, las cuales son proyectivas tal como se concluye del Ejemplo1.13 y Proposición 1.14.

□

Ejemplo 2.11. (un valor propio de valor absoluto mayor a 1 y otro raíz de la unidad)
Consideremos una curva elíptica E con multiplicación en $\mathbb{Z}[i]$, y consideramos la superficie abeliana $X = E \times E$. Dado el endomorfismo

$$X \longrightarrow X,\ (x, y) \mapsto (ix, 2iy),$$

se ve que la matriz que representa a ρ_f^a es $\begin{pmatrix} i & 0 \\ 0 & 2i \end{pmatrix}$. Luego los valores propios de f son i y $2i$, y entonces la función de puntos fijos tienen comportamiento (C3):

$$\#Fix(f^n) = \begin{cases} 0 & \text{si } n \equiv 0 \pmod 4 \\ h(n) & \text{en otro caso} \end{cases}$$

Aquí la función h crece exponencialmente ($h(n) \sim 2^{2n}$).

Capítulo 3

Generalización del problema a cualquier dimensión

3.1. Teorema principal

Ahora estudiaremos los puntos fijos de endomorfismos de toros complejos g-dimensionales. Al igual que en el caso de dimensión 2, debemos estudiar el tipo de valores propios que aparecen para los endomorfismos, por lo que necesitaremos una serie de resultados sobre estos. Algunos son muy similares a los ya vistos en las secciones precedentes, pero lamentablemente, ahora aparecen casos que antes no se veían. Para dimensiones mayores nos encontramos con endomorfismos que tienen valores propios de módulo 1 y que no son raíces de la unidad, y ésta es la gran piedra de tope cuando uno quiere generalizar el trabajo de Bauer y Herrig. Efectivamente si λ es un entero algebraico con las características recién mencionadas, entonces por Teorema 1.27, se tiene que la órbita de la sucesión $\{\lambda^n\}_{n\in\mathbb{N}}$ es densa en el círculo unitario complejo, y mas aún, la distribución de los puntos es uniforme. Salvo este caso el resto es en general muy parecido a lo anterior. Dicho esto veremos algunos resultados previos que nos ayudarán a la generalización.

El objetivo es demostrar el siguiente teorema.

Teorema 3.1. *Sea X un toro complejo de dimensión g y sea f un endomorfismo de X. Entonces $\#Fix(f^n)$ tiene alguno de los siguientes comportamientos:*

(1) Tiene crecimiento exponencial en n, es decir, existen constantes reales $A, B > 1$ y un entero N tal que, $\forall n \geq N$, $A^n \leq \#Fix(f^n) \leq B^n$

(2) Es una función periódica, y los valores propios distintos de cero de f son raíces k-ésima de la unidad, donde k está contenido en el conjunto $\{n \in \mathbb{N} : \ \phi(n) \leq 2g\}$, donde ϕ es la función de Euler.

(3) Existen enteros $n_1, ..., n_r \geq 2$ y una función de crecimiento exponencial $h : \mathbb{N} \to \mathbb{N}$ tal que

$$\#Fix(f^n) = \begin{cases} 0 & si\ n \equiv 0 \ (mod\ n_i)\ para\ algún\ i \\ h(n) & en\ otro\ caso \end{cases}$$

El primer lema que veremos es una generalización de la Proposición 2.8, que como se mencionó en su momento es en cierta medida aplicable a toros de dimensión g.

Lema 3.2. *Sea X un toro complejo de dimensión g, y $f : X \to X$ un endomorfismo que tiene un valor propio que satisface $0 < |\lambda_1| < 1$. Entonces f tiene otro valor propio con valor absoluto mayor a 1.*

Demostración. El argumento de la demostración es el mismo que en dimensión 2.
Se tiene que el polinomio característico de la representación racional tiene la forma

$$P_f^r(t) = P_f^a(t)\overline{P_f^a(t)} = \prod_{i=1}^{g}(t - \lambda_i)(t - \overline{\lambda_i})$$

Supongamos que todos los valores propios son distintos de cero, entonces $\prod_{i=1}^{g} |\lambda_i|^2$ es un entero pues es el coeficiente libre de $P_f^r(t)$ (que tiene coeficientes enteros). Si todos los valores propios tienen módulo menor que 1, entonces el elemento mencionado recientemente es un entero mayor que 0 y menor que 1, lo que es una contradicción. Luego al menos uno de los valores propios debe tener módulo mayor a 1.
Ahora bien si alguno de los valores propios es igual a cero, entonces $P_f^r(t)$ es divisible por una potencia de t. Luego de hacer la división obtenemos un polinomio $\hat{P}(t)$ que no es divisible por t y tiene coeficientes enteros, además el termino libre de este polinomio es $\prod_j |\lambda_j|^2$ donde j corre entre 1 y g tal que $|\lambda_j| \neq 0$. Igual que en el primer caso este último producto es un entero, por lo que alguno de los valores propios tiene módulo mayor a 1. □

Proposición 3.3. *Sea X un toro complejo y $f \in End(X)$. Si todos los valores propios de f que tienen valor absoluto igual a 1 son raíces de la unidad, entonces $\#Fix(f^n)$ exhibe exactamente uno de los comportamientos del Teorema 3.1.*

Demostración. Si $P_f^r(t)$ no tiene raíces que sean raíces de la unidad, entonces por Lema 3.2, hay valores propios con valor absoluto mayor a 1. Luego, de la fórmula general para la cantidad de puntos fijos se observa que estos crecen exponencialmente, pues los valores propios con módulo mayor a 1 aportan el crecimiento exponencial, mientras que los de módulo menor a 1 aportan una sucesión acotada que se acerca a 1. Además por suposición no hay valores propios con módulo 1.

Si $P_f^r(t)$ tiene sólo raíces que son raíces de la unidad, entonces la función $\#Fix(f^n)$ es periódica, con período $m.c.m.\{n_1, ..., n_r\}$(mínimo común múltiplo), donde los n_i son los grados de las raíces de la unidad que aparecen como valores propios.

Supongamos ahora que hay valores propios que son raíces de la unidad y otros que no lo son, entonces podemos factorizar $P_f^r(t)$ como sigue:

$$P_f^r(t) = P(t)Q(t)$$

Donde $P(t), Q(t) \in \mathbb{Z}[t]$ son tal que, las raíces de $P(t)$ son raíces de la unidad y las de $Q(t)$ no lo son (esto es pues los conjugados de raíces de la unidad son también raíces de la unidad). Tenemos entonces

$$\#Fix(f^n) = \left(\prod_{|\lambda|=1} |1 - \lambda^n|^2 \right) \left(\prod_{\lambda \neq 1} |1 - \lambda^n|^2 \right)$$

Una observación útil a esta altura es el hecho que $\prod_{|\lambda|=1}(1-\lambda^n)$ y $\prod_{|\lambda|\neq 1}(1-\lambda^n)$ son elementos en $\mathbb{Z}$ pues son enteros algebraicos (ver Subsección 1.2.2) y son invariantes bajo la acción del grupo de Galois de $P(t)$ y $Q(t)$ respectivamente. Sean $n_1, ..., n_r$ los ordenes de las diferentes raíces de $Q(t)$

$$\#Fix(f^n) = \begin{cases} h(n) & \text{si } n \not\equiv 0 \pmod{n_1, \ldots, n_r} \\ \prod_{|\lambda|\neq 1} |1 - \lambda^n|^2 & \text{en otro caso} \end{cases}$$

donde h es una función de crecimiento exponencial. Esto da un crecimiento del tipo (3) en el Teorema 3.1 □

A continuación se mostrará una serie de ejemplos de toros complejos de dimensión mayor a dos en donde se muestre que estos comportamientos existen.

Ejemplo 3.4. Para cualquier toro X siempre podemos considerar el endomorfismo multiplicación por m, donde m es un entero. A este endomorfismo lo hemos denotado por m_X, y cuyos valores propios son m repetido g veces. Luego

$$\#Fix(m_X^n) = (m^n - 1)^{2g}.$$

Como la función Fix tiene esa forma, el crecimiento es evidentemente exponencial.

Ejemplo 3.5. Sean X, E y f como en el Ejemplo 2.7. Consideremos $Y = X \times E$ con el siguiente endomorfismo:

$$\begin{array}{rccc} g: & Y & \longrightarrow & Y \\ & (x,z) & \longmapsto & (f(x), iz) \end{array}$$

La matriz que corresponde a la representación analítica de f viene dado por

$$\begin{pmatrix} 1 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & i \end{pmatrix}$$

cuyos valores propios son $\frac{1+\sqrt{3}}{2}$, $\frac{1-\sqrt{3}}{2}$, i. Todos ellos raíces de la unidad, por lo tanto, esto muestra un ejemplo del comportamiento periódico (C2) en una variedad abeliana.

Nos vamos a aprovechar de este último ejemplo, haciéndole una pequeña modificación para obtener comportamiento del tipo (C3).

Ejemplo 3.6. Modifiquemos la función del Ejemplo 3.5 de la siguiente manera:

$$\begin{array}{rccc} g' & : Y & \longrightarrow & Y \\ & (x,z) & \longmapsto & (f(x), mz) \end{array}$$

para $m \in \mathbb{Z}$, $|m| \leq 2$. La matriz de la representación analítica es

$$\begin{pmatrix} 1 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & m \end{pmatrix}$$

cuyos valores propios son $\frac{1+\sqrt{3}}{2}, \frac{1-\sqrt{3}}{2}, m$. Los dos primeros son raíces de la unidad, y el último de módulo mayor a 1. Por lo tanto este endomorfismo muestra crecimiento del tipo (C3). Además como se especificó en el Ejemplo 3.5, Y es una variedad abeliana.

3.2. Medida de Mahler

La demostración del teorema principal pasa por dinámica algebraica y aproximación diofantina, y una de las herramientas que se usa para simplificar las notaciones es la llamada medida de Mahler.

Definición 3.7. Para cualquier polinomio no nulo

$$F(x) = a_d x^d + a_{d-1} x^{d-1} + ... + +a_0 = a_d \prod_{i=1}^{d} (x - \alpha_i)$$

en $\mathbb{C}[x]$ (donde los α_i son las raíces del polinomio $F(x)$), se define la medida de Mahler de F como

$$M(F) = |a_d| \prod_{i=1}^{d} max\{1, |\alpha_i|\}$$

En esta definición, un producto vacío se supone como 1, es decir, la medida de Mahler de los polinomios constantes $F(x) = a_0$ es $|a_0|$.

Observación. La medida de Mahler de un polinomio nos da una idea de cuán lejos estań sus raíces del disco unitario, salvo por la constante que está al frente del producto. Esto se verá mucho mejor si consideramos sólo polinomios mónicos.

Ejemplo 3.8. Sea $F(x) = \phi_n(x)$ el polinomio ciclotómico n-ésimo, este tiene grado $\phi(n)$ (la función de Euler). Por definición el polinomio ciclotómico tiene como raíces a las raíces de la unidad (digamos ζ_n) y sus potencias, entonces máx$\{1, |\zeta_n^k|\} = 1$. Luego se concluye que la medida de Mahler de los polinomios ciclotómicos es 1.

Observación. La medida de Mahler tiene gran interés dentro del mundo de la teoría de números, principalmente se buscan cotas inferiores para polinomios con coeficientes enteros. Este problema

es conocido como el problema de Lehmer. De hecho hay un conjetura conocida como la conjetura de Lehmer sobre medidas de Mahler, que dice que existe $\mu \in \mathbb{R}$ tal que todo polinomio con coeficientes enteros tiene medida de Mahler mayor o igual μ, o bien tiene medida de Mahler igual a 1.

Hasta ahora el polinomio con medida de Mahler mas pequeña conocida es el llamado polinomio de Lehmer.

$$P(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

cuya medida de Mahler es $M(P) = 1{,}176280818...$. A esta constante se le llamó μ, y es la cota que aparece en la conjetura. Una de las cosas interesantes de μ es que es un número de Salem.

Los polinomios que tienen medida de Mahler igual a 1 no son de tanto interés, ya que si $M(F) = 1$, significa que tiene todas sus raíces en el disco unitario, pero por Lema 3.2 si tiene una raíz de módulo menor a 1, entonces debe tener una de módulo mayor a 1, lo cual no es el caso, así todas las raíces tienen módulo 1 y por el Teorema de Kronecker (ver 1.23, Sección 1.2.3) se tiene que todas las raíces de F son raíces de la unidad, luego F es un producto de polinomios ciclotómicos. Por lo tanto los polinomios con medida unidad están totalmente clasificados.

Por otro lado también se han hecho avances dependiendo del tipo de extensión que generan. Por ejemplo en [1] demuestran un resultado cuando la extensión de cuerpos $\mathbb{Q}(\alpha)/\mathbb{Q}$ es Galois, donde α es la raíz de un polinomio F.

El teorema dice que existe $c > 0$ tal que si la extensión $\mathbb{Q}(\alpha)/\mathbb{Q}$ es de Galois y α es distinto de cero y de alguna raíz de la unidad, entonces $M(F) \geq c$

Otros resultados de teoía algebraica de números dan otras cotas, por ejemplo se demostró que si α es un entero algebraico de grado d tal que exista un primo no menor que $d \log d$ que es no ramificado en $\mathbb{Q}(\alpha)$, entonces $M(F) \geq 1{,}2$.

Definición 3.9. Definiremos la medida logarítmica de Mahler como

$$m(F) = \log M(f)$$

Además extenderemos esta definición para incluir al polinomio nulo, para eso diremos que la medida logarítmica de Mahler del polinomio nulo es $m(0) = \infty$.

Observación. Existen otros tipos de medidas para polinomios que en algún sentido son más naturales como la altura ($H(F)$) y el largo ($L(F)$) que se definen como

$$H(F) = \text{máx}\{|a_i|\}, \qquad L(F) = \sum_{i=0}^{d} |a_i|$$

Para un polinomio $F(x) = a_d x^d + ... + a_1 x + a_0$.
Se puede demostar que existe una estrecha relación entre estas medidas y la de Mahler, de hecho se satisfacen las siguientes propiedades:

$$2^{-d} H(F) \leq M(F) \leq d \cdot H(F)$$

y

$$2^{-d} L(F) \leq M(F) \leq L(F)$$

donde d es el grado del polinomio F.

Antes de seguir vamos a introducir un poco de notación. Esta es usada en [8].
Escribiremos $\log^+ \lambda$ para referirnos a $\log \text{máx}\{1, \lambda\}$.

Dado un polinomio mónico

$$F(x) = x^d + a_{d-1} x^{d-1} + ... + a_1 x + a_0 \in \mathbb{Z}[x],$$

con factorización en $\mathbb{C}[x]$

$$F(x) = \prod_{i=1}^{d} (x - \alpha_i),$$

entonces, para cada $n \in \mathbb{N}$ (distinto de cero) se define

$$\Delta_n(F) = \prod_{i=1}^{d} (\alpha_i^n - 1).$$

Si alguno de los α_i es una raíz de la unidad entonces existe $N \in \mathbb{N}$ tal que $\alpha_i^N = 1$, luego $\Delta_n(F) = 0$ para cada n que divida a N, por esta razón no nos interesaremos tanto en este caso.

Observación. El elemento $\Delta_n(F)$ es un entero, pues se obtiene como el resultado de productos y sumas de elementos algebraicos, luego es un elemento algebraico. Por otro lado como aparecen todos los conjugados de cada uno de los α_i, se tiene que $\Delta_n(F)$ es invariante por la acción de algún grupo de Galois, luego es un racional. Concluimos que es un entero por ser un entero algebraico racional.

Observación. Debemos notar que nos interesa de sobremanera el elemento $\Delta_n(F)$ y el comportamiento asintótico que este tiene cuando $n \to \infty$, por la similitud que tiene con $\#Fix(f^n)$. De hecho se tiene que si $P(t)$ es el polinomio característico de la representación racional de algún endomorfismo f de un toro X, entonces

$$\#Fix(f^n) = \Delta_n(P)$$

y esto sale del hecho que

$$\begin{aligned}
\#Fix(f^n) &= \left| \prod_{i=1}^{g} (1 - \lambda_i^n) \right|^2 \\
&= \prod_{i=1}^{g} |1 - \lambda_i^n|^2 \\
&= \prod_{i=1}^{g} \left(|1 - \lambda_i^n| \, |1 - \overline{\lambda_i^n}| \right) \\
&= \prod_{i=1}^{g} (1 - \lambda_i^n) \left(1 - \overline{\lambda_i^n}\right) \\
&= \Delta_n(P)
\end{aligned}$$

Esta última igualdad se tiene pues las raíces de la representación racional $P(t)$ son las raíces $\lambda_1, ..., \lambda_g$ de la represention analítica más los conjugados de estas. pues $\rho_f^r \simeq \rho_f^a \oplus \overline{\rho_f^a}$ (Ver [13, Proposición 1.2.3])

A continuación mostraremos la primera conexión entre $\Delta_n(F)$ y la medida de Mahler $M(F)$.

Lema 3.10. *Si $F(x) \in \mathbb{Z}[x]$ mónico, tal que no tiene raíces de módulo 1, entonces*

$$\lim_{n\to\infty} \left| \frac{\Delta_{n+1}(F)}{\Delta n(F)} \right| = \prod_{i=1}^{d} max\{1, |\alpha_i|\} = M(F)$$

Demostración. Esto es directo, sólo hay que ponerse en los dos distintos casos en que el módulo de cada raíz α de F es menor o mayor a 1

$$\lim_{n\to\infty} \left| \frac{\alpha^{n+1} - 1}{\alpha^n - 1} \right| = \begin{cases} |\alpha| \text{ si } |\alpha| > 1 \\ 1 \text{ si } |\alpha| < 1 \end{cases}$$

□

A continuación enunciaremos el Teorema de Baker, que es un resultado de aproximación diofantina, el cual será la clave para demostrar nuestro teorema pricipal.

Teorema 3.11 (Teorema de Baker). *Sean $\alpha_1, ..., \alpha_r$ números algebraicos, y $\boldsymbol{n} \in \mathbb{Z}$ un vector con coeficientes en los enteros, escribimos $|\boldsymbol{n}| = \max\{|n_i|\}$. Entonces para cualquier elección de ramas del logaritmo, si $|n_1 \log \alpha_1 + ... + n_r \log \alpha_r| \neq 0$, existe c que depende sólo de $\alpha_1, ..., \alpha_r$ tal que*

$$|n_1 \log \alpha_1 + ... + n_r \log \alpha_r| \gg \frac{1}{|\boldsymbol{n}|^c}$$

Demostración. Ver [3, Teorema 3.1] □

Lema 3.12. *Sea α un entero algebraico con $|\alpha| = 1$ que no sea raíz de la unidad, entonces existen constantes A, B que dependen solo de α (no de n) tal que*

$$|\alpha^n - 1| > \frac{A}{n^B} \qquad \forall n \geqslant 1$$

Demostración. Como sabemos que la sucesión de potencias de α es equidistribuida en el círculo unitario, el problema se produce cuando α^n está muy cerca de 1, y este es el caso del que nos vamos a preocupar.
Escribamos $\alpha = e^{i\theta}$ para algun $\theta \in \mathbb{R}$. Observamos que α^n está cerca de 1 si y solamente si existe algún $m \in \mathbb{Z}$ para el cual $n\theta + 2\pi m$ está cerca de 0, o equivalentemente que $n\theta$ está cerca de un multiplo de 2π. Entonces

$$\alpha^n - 1 = e^{i(n\theta + 2\pi m)} - 1 \backsim i(n\theta + 2\pi m)$$

para valores pequeños de $n\theta + 2\pi m$ (expansión de Taylor de primer orden de la función exponencial). Luego es suficiente encontrar una cota inferior para

$$in\theta + 2\pi im \tag{3.1}$$

Eligiendo alguna rama de logaritmo podemos escribir $e^{i\theta} = \alpha = e^{log\alpha}$. Luego tomando una rama no principal, y del hecho que $e^{2\pi i} = 1$, podemos reescribir la expresión 3.1 de la forma

$$n \log \alpha + m \log 1$$

Esta última expresión es distinta de cero, pues α no es raíz de la unidad, entonces por Teorema de Baker (3.11) se tiene que

$$|in\theta + 2\pi im| = |n \log \alpha + m \log 1| \gg \frac{1}{(\text{máx}\{|n|, |m|\})}.$$

Por otra parte, $n\theta + 2\pi m$ es pequeño, entonces n y m están muy cerca de múltiplos constantes uno del otro, esto muestra

$$|n \log \alpha + m \log 1| \gg \frac{1}{|n|^c}.$$

La desigualdad buscada sigue de la conocida desigualdad del logaritmo

$$|z - 1| > |\log z| \text{ para } |z - 1| < 1.$$

□

El Teorema 3.11 y el Lema 3.12 dan cotas para la expresión $|\alpha^n - 1|$ las cuales son de extrema utilidad, para calcular el número de puntos fijos de un endomorfismo de un toro, y mejor aún, el Lema 3.12 nos dice qué pasa cuando α no es una raíz de la unidad.
A continuación enunciaremos un teorema que nos dejará en buen pie para poder demostrar el teorema principal del trabajo (Teorema 3.1).

Teorema 3.13. *Sea F un polinomio no nulo que no tiene raíces de la unidad como raíces. Entonces el límite*

$$\lim_{n \to \infty} \frac{1}{n} \log |\Delta_n(F)|$$

siempre existe, y es igual a $m(F)$.

Demostración. Primero debemos observar que como

$$\Delta_n(F) = \prod_{i=1}^{d} (\alpha_i^n - 1),$$

se tiene que

$$\log |\Delta_n(F)| = \sum_{i=1}^{d} \log |\alpha_i^n - 1|.$$

Debemos ver cada sumando por separado. Por esto, debemos ver qué pasa en los casos en que el módulo de α_i sea menor, igual o mayor a 1.

- Si $|\alpha_i| > 1$, entonces

$$\frac{1}{n}\log|\alpha_i^n - 1| \to \log|\alpha_i| = \log^+|\alpha_i|$$

- Si $|\alpha_i| < 1$, entonces

$$\frac{1}{n}\log|\alpha_i^n - 1| \to 0 = \log^+|\alpha_i|$$

- Si $|\alpha_1| = 1$, entonces existe una subsucesión $n_j \to \infty$ con la propiedad que $\alpha_i^{n_j} \to 1$, esto existe por la equidistribución de las potencias de elementos de módulo 1 que no son raíces de la unidad. Entonces

$$\log|\alpha_i^{n_j} - 1| \to -\infty$$

como los α_i no son raíces de la unidad, por Teorema 3.11 tenemos que existen constantes positivas A, B independientes de n tales que

$$|\alpha_i^n| > \frac{A}{n^B} \quad \forall n \geq 1.$$

Luego se tiene que

$$\log|\alpha_i^n - 1| = O(\log n),$$

Por lo tanto

$$\frac{1}{n}log|\alpha_i^n - 1| \longrightarrow 0 = \log^+|\alpha_i|.$$

□

3.3. Demostración del Teorema principal

Lema 3.14. *Sea X un toro complejo g-dimensional, y f un endomorfismo de X. Supongamos que f tiene un valor propio en el círculo unitario que no es raíz de la unidad, entonces debe tener otro de módulo mayor a 1*

Demostración. Supongamos que el resultado es falso, es decir, no existen valores propios con módulo mayor a 1.

- **Caso 1**: Supongamos que todos los valores propios tienen módulos igual a 1, esto implica que todas las raíces del polinomio característico de la representación racional tienen módulo 1, pero recordemos que este polinomio tiene coeficientes en $\mathbb{Z}$. Luego por el Teorema 1.23 todas las raíces son raíces de la unidad, lo que es una contradicción con las hipótesis.
- **Caso 2**: Supongamos que f tiene al menos un valor propio de módulo menor a 1, pero por Lema 3.2 existe uno con módulo mayor a 1, lo que es una contradicción a lo que habíamos supuesto.

Luego debe existir algún valor propio de módulo mayor a 1. □

Ahora se dará la demostración del teorema principal de este trabajo (Teorema 3.1)

Demostración. En la Proposición 3.3 se demuestra que para un endomorfismo f que no tenga valores propios de módulo 1 que no son raíces de la unidad, entonces el Teorema 3.1 se cumple, y de hecho se dan ejemplos de cada uno de esos comportamientos en variedades abelianas.
Para concluir la demostración solo debemos abordar el caso en que f tenga valores propios unimodulares que no son raíces de la unidad. Para esto recordemos que si P es el polinomio característico de la representación racional de f, entonces

$$\#Fix(f^n) = \Delta_n(P)$$

y por Teorema 3.13

$$\lim_{n\to\infty} \frac{1}{n} \log\left(\#Fix(f^n)\right) = m(P)$$

Como f tiene un valor propio unimodular que no es raíz de la unidad, por Lema 3.14, debe existir alguno con módulo mayor a 1. De esta manera $M(P) > 1$, por lo que $m(P) > 0$.
De esta forma se concluye que

$$\#Fix(f^n) = o(e^{n \cdot m(P)})$$

donde $o(a(n))$ representa notación asintótica o-chica de $a(n)$, es decir, $\#Fix(f^n)$ crece de forma exponencial como función de n.
Ahora solo nos basta mostrar un ejemplo para demostrar que en realidad se puede dar este tipo de comportamientos, pero más adelante habrá una sección exclusiva a la construcción de este tipo de toros y de endomorfismos. Por ahora para acabar la demostración podemos ver el Ejemplo 4.7. □

Observación. Una acotación interesante es que este problema tiene una interpretación desde el punto de vista de sistemas dinámicos que no se profundizara mayormente por la naturaleza del enfoque que se ha dado a lo largo del trabajo. Básicamente un endomorfismo de toros complejos induce un sistema dinamico en el toro, además este endomorfismo visto como transformación μ-invariante (donde μ es la medida de Haar asociada al toro como grupo topologico localmente compacto Hausdorff) es ergódica si y solamente si no aparecen valores propios que sean raíz de la unidad. Por otra parte el número $\#Fix(f^n)$ puede interpretarse como el número de elementos n-periódicos de la transformación. Por último la entropia topológica del sistema corresponde a la medida de Mahler del polinomio caracteristico de la transformación.

Un corolario

Lo que veremos ahora es una consecuencia analítica aplicada a algo algebraico que se sigue de la demostración de Teorema 3.1 .
Lo primero que debemos hacer es relacionar $\#Fix(f^n)$ con la norma $N_{K/\mathbb{Q}}$ (la norma sobre un cuerpo de números).
Como siempre, se toma f un endomorfimo de un toro complejo X. Consideremos $P(t)$ el polinomio característico de la representación racional de f. Sabemos que $P(t)$ es un polinomio con coeficientes en $\mathbb{Z}$, y consideremos su factorización en polinomios irreducibles sobre $\mathbb{Z}[t]$

$$P(t) = P_1(t) \cdots P_r(t)$$

Sea α una raíz de $P_1(t)$, y supongamos $[\mathbb{Q}(\alpha) : \mathbb{Q}] = s$, entonces por la Proposición 1.18

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(1-\alpha^n) = \prod_{i=1}^{s} \sigma_i(1-\alpha^n)$$

donde $\sigma_1, ..., \sigma_s$ son las s incrustaciones distintas de $\mathbb{Q}(\alpha)$ en $\mathbb{C}$.
De esta manera se tiene que si $\alpha_1, ..., \alpha_r$ son raíces de $P_1(t), ..., P_r(t)$ respectivamente, entonces se tiene que

$$\#Fix(f^n) = N_{\mathbb{Q}(\alpha_1)/\mathbb{Q}}(1-\alpha_1^n) \cdots N_{\mathbb{Q}(\alpha_r)/\mathbb{Q}}(1-\alpha_r^n)$$

Por el Teorema 3.1 sabemos que cuando aparece una unidad unimodular que no es raíz de la unidad como valor propio, entonces $\#Fix(f^n)$ crece de forma exponencial. Entonces lo que podemos sacar como corolario de este resultado y de lo mencionado previamente en esta sección es lo siguiente

Corolario 3.15. *Sea $\alpha \in \mathbb{C}$ un entero algebraico que no es raíz de la unidad, que viene entonces*

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(1-\alpha^n) \xrightarrow[n\to\infty]{} \infty$$

mas aún, el orden de crecimiento es exponencial.

Demostración. Como se mencionó previamente, este resultado es consecuencia directa del Teorema 3.1 □

Una propiedad aritmética de la función Fix

Si bien el comportamiento de $\#Fix(f^n)$ —como función de n— puede ser un tanto extraño a priori, hemos visto que su definición es básicamente operaciones aritméticas de enteros algebraicos, más aún, de enteros algebraicos y todos sus conjugados. Por este motivo $\#Fix(f^n)$ tiene una propiedad interesante desde el punto de vista aritmético.
Como siempre sea X un toro complejo de dimensión g y $f \in End(X)$. Sea λ_1 un valor propio de f, y $\lambda_1, ..., \lambda_g$ los conjugados de λ_1.

Proposición 3.16. *Bajo las hipótesis recién mencionadas se tiene que $n|k \Rightarrow \#Fix(f^n)|\#Fix(f^k)$.*

Lema 3.17. *Sea λ_1 un entero algebraico, y $\lambda_1, ..., \lambda_g$ sus conjugados, entonces $\prod_{i=1}^{g} \phi_n(\lambda_i) \in \mathbb{Z}$, donde ϕ_n es el n-ésimo polinomio ciclotómico.*

Demostración. Como el conjunto de los enteros algebraicos es cerrado bajo suma y producto se tiene que cada $\phi_n(\lambda_i)$ es un entero algebraico, luego $\prod_{i=1}^{g} \phi_n(\lambda_i)$ es un entero algebraico. Por otra parte, el grupo de Galois $Gal(K/\mathbb{Q})$ actúa en este producto, donde K es un cuerpo suficientemente grande para que contenga a λ_1 y a todos sus conjugados (basta tomar la clausura normal de $\mathbb{Q}(\lambda_1)$). Por otro lado

$$\sigma\left(\prod_{i=1}^{g} \phi_n(\lambda_i)\right) = \prod_{i=1}^{g} \sigma(\phi_n(\lambda_i)) = \prod_{i=1}^{g} \phi_n(\sigma(\lambda_i)) = \prod_{i}^{g} \phi_n(\lambda_i)$$

pues en el producto aparecen todos los conjugados de λ_1. Luego como es invariante bajo la acción de $Gal(K/Q)$, se tiene que $\prod_{i=1}^{g} \phi_n(\lambda_i) \in \mathbb{Q}$. Luego como es entero algebraico y racional se tiene que está en $\mathbb{Z}$. □

Demostración. (**Demostración de la Proposición 3.16**) Como tenemos que

$$\#Fix(f^n) = \prod_{d|n} \Phi_n(\lambda),$$

Donde $\Phi_n(\lambda) = |\prod \phi_n(\lambda_i)|^2$, tendremos que $\#Fix(f^n)|\#Fix(f^k)$ si y solamente si $\prod_{d|k, d\nmid n} \Phi_d(\lambda) \in \mathbb{Z}$, pero por lo demostrado en el lema, cada $\Phi_d(\lambda) \in \mathbb{Z}$, luego $\#Fix(f^n)|\#Fix(f^k)$. □

Capítulo 4

Construcción de toros complejos y endomorfismos con valores propios en el círculo unitario

Antes de dar ejemplos explicitos de estos toros con este tipo de endomorfismo, necesitamos algunos resultado previos que ayudaran en la construcción de estos.

Algunos hechos sobre polinomios con raíces en el círculo unitario

A lo largo del trabajo nos hemos dado cuenta que la mayoría de los polinomios que aparecen y que nos interesan estudiar son polinomios irreducibles con coeficientes enteros y palindrómicos, es decir, que sus coeficientes se leen igual de derecha a izquierda que de izquierda a derecha. Por este motivo en esta subsección expondremos un resultado que nos será bastante útil. Este y otros resultados pueden verse en mas detalle en [12]

Una buena observación para comenzar es el hecho que nos interesaremos principalmente en polinomios de grado par, pues si un polinomio palindrómico tiene grado impar, entonces -1 es una raíz del polinomio, por lo que este caso pierde interés al ser reducible.

El resultado a continuación nos da condiciones suficientes sobre los coeficientes para que tenga raíces en el círculo unitario.

Proposición 4.1. *Sea $f(x)$ un polinomio palíndrome con coeficientes reales y de grano n par, tal que*

$$\text{máx}\{|a_k| : k \in \{0, 1, 2, ..., n/2 - 1\}\} \geq |a_{n/2}|$$

tal polinomio tiene una raíz en el círculo unitario. En particular polinomio palindrómicos con coeficientes 0 y 1 tienen una raíz en el círculo unitario.

Demostración. Ver [12, Corolario 1]. □

4.1. Existencia

Como hemos visto hasta ahora la generalización del resultado expuesto en [4] no tiene mayores inconvenientes y se pueden usar casi las mismas técnicas, salvo que eventualmente podrían aparecer elementos de módulo 1 que no sean raíces de la unidad como valores propios del endomorfismo f. Primeramente debemos responder a la siguiente interrogante ¿Existen enteros algebraicos que tengan módulo 1 pero que no sean raíz de la unidad?
Para probar la existencia vamos a presentar algunos resultados expuestos en [7], los cuales garantizan la existencia bajo ciertas hipótesis. Luego de eso daremos algunos ejemplos para ilustrar un poco mejor lo que en realidad está sucediendo.
Dado un cuerpo de números K denotaremos por V_K al conjunto de enteros algebraicos de módulo 1. W_K denota el grupo de raíces de la unidad que están en K y R_K será el conjunto de unidades reales, es decir $R_K = \mathcal{O}_K^* \cap \mathbb{R}$

Observación. Los elementos del conjunto V_K son unidades en $\mathcal{O}_K$, pues si $u \in V_K$, entonces $\overline{u}$ es también raíz del polinomio irreducible de u sobre $\mathbb{Q}$, pero al tener u módulo 1, se concluye que $\overline{u} = u^{-1}$, luego $u^{-1} \in \mathcal{O}_K$.

De este modo V_K es un subgrupo del grupo de unidades $\mathcal{O}_K^*$. De esto último se tiene que V_K es un grupo abeliano finitamente generado, y por el Teorema de las unidades de Dirichlet conocemos una cota para el rango y sabemos además cuál es su parte de torsión.

Lo que se quiere estudiar es cuando $V_K \neq W_K$. Una respuesta parcial a esta pregunta es dada por MacCluer y Parry cuando la extensión $K/\mathbb{Q}$ es de Galois. En [14] se demuestra que si la extensión es de Galois entonces $W_K \neq V_K$ si y solo si K es un cuerpo imaginario y no un

cuerpo CM.

A continuación se enunciará el resultado principal de [7], que caracteriza la existencia de elementos unimodulares en cuerpos de números.

Teorema 4.2. *Sea K un cuerpo de números y $L = K \cap \overline{K}$, donde $\overline{K}$ es el cuerpo que se obtiene al conjugar (en el sentido complejo) los elementos de K. Entonces K contiene unidades unimodulares que no son raíces de la unidad si y solamente si L es un cuerpo imaginario y no un cuerpo CM.*

Demostración. Ver [7, Teorema 3] □

Antes de comenzar con las construcciones, vamos a dar un ejemplo de un elemento algebraico de este tipo.

Ejemplo 4.3. Consideremos el polinomio $P(t) = t^6 + 4t^5 + 4t^4 + 4t^2 + 4t + 1$, por la Proposición 4.1, sumado al hecho que 1 y -1 no son raíces de $P(t)$, se tiene que este polinomio tiene a lo menos dos raíces en el círculo unitario. Por otra parte, es posible ver que es un polinomio irreducible (bastó una comprobación con SAGE) y también se puede ver que este polinomio no divide a ningún polinomio ciclotómico. Una forma de ver esto último es que el primer polinomio ciclotómico con coeficientes distintos de 1 es el de grado 105 $(3 \cdot 5 \cdot 7)$.

4.2. Construcciones

4.2.1. Primera construcción

En la sección anterior vimos que en general existen elementos que son enteros algebraicos de módulo 1 pero que no son raíces de la unidad, pero a nosotros nos interesa ver si es que estos aparecen como valores propios de endomorfismos de toros complejos. A priori no es obvia la respuesta. Por ahora lo que se sabe es que en dimensión 2 no pueden aparecer como consecuencia de Proposición 2.9.

Para demostar la existencia de toros con estos valores propios lo que haremos es tomar un entero algebraico δ de módulo 1 que no sea raíz de la unidad de grado $2g$ y tal que la extensión de cuerpos $\mathbb{Q}(\delta)/\mathbb{Q}$ sea totalmente compleja, y construiremos un toro complejo de dimensión g que

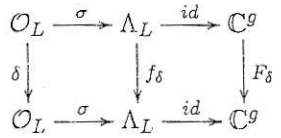


Figura 4.1: Construcción

tenga a δ como valor propio.

Esta construcción está basada en una herramienta análitica clásica que se usa en la teoría de números algebraicos para probar ciertos hecho como el Teorema de las unidades de Dirichlet o la finitud del número de clase en un cuerpo de números (véase 1.22 y [16, Teorema 6.4 Capítulo 1]).

Construcción:

Sea $\delta \in \mathbb{C}$ un entero algebraico de módulo 1 tal que $\mathbb{Q}(\delta)/\mathbb{Q}$ es una extensión totalmente imaginaria de grado $2g$, y $\tau_1, ..., \tau_g : \mathbb{Q}(\delta) \hookrightarrow \mathbb{C}$, g incrustaciones distintas y tal que no existan dos que sean conjugada una de la otra (las otras g incrustaciones son las conjugadas de estas). Llamaremos L al cuerpo $\mathbb{Q}(\delta)$. Es un hecho que la aplicación $\sigma = (\tau_1, ..., \tau_g)$ manda $\mathcal{O}_L$ a un reticulado en $\mathbb{C}^g$ (vease [16, Sección 5 Capítulo 1]) que llamaremos Λ_L.

Observemos el diagrama 4.1 y estudiemos qué es lo que ocurre en cada paso.

La función $\sigma : \mathcal{O}_L \longrightarrow \Lambda_L$ es la aplicación dada por las g-incrustaciones, e id es la inclusión de Λ_L en $\mathbb{C}^g$. Por otro lado la flecha vertical de la izquierda representa el homomorfismo $\mathbb{Z}$-lineal multiplicación por δ .

La función $f_\delta : \Lambda_L \longrightarrow \Lambda_L$ viene dada por la acción de $\mathbb{Z}[\delta]$ en Λ_L de la siguiente manera.

$$\begin{array}{rccc} f: & \Lambda_L & \longrightarrow & \Lambda_L \\ & (\tau_1(x), ..., \tau_g(x)) & \longmapsto & (\tau_1(\delta x), ..., \tau_g(\delta x)) \end{array}$$

Finalmente tenemos la función F_δ que aparece en forma vertical al lado derecho del diagrama. Esta función es la extensión $\mathbb{C}$-lineal de F_δ a todo $\mathbb{C}^g$.

Proposición 4.4. *La función F_δ induce un endomorfismo de toros complejos (en cierto toro) cuyos valores propios son $\tau_1(\delta), ..., \tau_g(\delta)$. Notar que δ es uno de los valores propios de f.*

Demostración. F_δ es una aplicación $\mathbb{C}$-lineal tal que $F_\delta(\Lambda_L) \subseteq \Lambda_L$, luego induce una aplicación en el toro $\mathbb{C}^g/\Lambda_L$:

$$f : \mathbb{C}^g/\Lambda_L \longrightarrow \mathbb{C}^g/\Lambda_L$$

Como el diagrama es conmutativo $F_\delta(x) = \tau_i(\delta)x$, luego $\tau_1(\delta), ..., \tau_g(\delta)$ son los valores propios de F_δ. □

De esta manera probamos lo siguiente:

Teorema 4.5. *Existen toros complejos y endomorfismos tal que tienen como valor propio un entero algebraico de módulo 1 que no es raíz de la unidad.*

Demostración. Esto resulta de la Proposición 4.4 □

Teorema 4.6. *Para cada $g \geq 3$ existen toros complejos X de dimensión g y endomorfismos $f \in End(X)$ que tenga un valor propio en el círculo unitario que no es raíz de la unidad.*

Antes de demostrar este teorema veremos un ejemplo, del cual la demostración será directa

Ejemplo 4.7. Sea E la curva elíptica con un automorfismo de orden 4, $E = \dfrac{\mathbb{C}}{\mathbb{Z}[i]}$. Consideremos la siguiente matriz $M \in \mathbb{M}_3(\mathbb{Z}[i])$ que representa un endomorfismo de E^3.

$$M = \begin{pmatrix} 0 & 0 & -i \\ 1 & 0 & -2i \\ 0 & 1 & -2 \end{pmatrix}$$

Con esto vemos que la representación racional del endomorfismo es $P_f^r(t) = t^6 + 4t^5 + 4t^4 + 4t^2 + 4t + 1$, que se vió en el Ejemplo 4.3 que debe tener una raíz en el círculo unitario que no es raíz de la unidad. Luego este endomorfismo tiene un valor propio con las caracteristicas que se buscaba.

Demostracíon del Teorema 4.6. Sea Y un toro complejo de dimensión $(g-3)$, y definamos el toro $X = Y \times E^3$, donde E es la curva elíptica recién mencionada. Definimos el endomorfismo

$$\widehat{f} = f \times id : X = Y \times E^3 \longrightarrow Y \times E^3$$

Entonces los valores propios de $\widehat{f}$ son los valores propios de f y 1 repetido $(g-3)$-veces. Asi X es un toro de dimensión g con un endomorfismo que tiene como valor propio un elemento unimodular que no es raíz de la unidad. □

Ya sabíamos que en toros complejos de dimensión 2 no pueden aparecer endomorfismos con este tipo de valores propios. Ahora veamos qué sucede si intentamos construir un toro complejo de dimensión dos que tenga un endomorfismo con valor propio de módulo uno que no sea raíz de la unidad mediante la construcción que acabamos de mostrar.
Debemos tomar un entero algebraico δ unimodular no raíz de la unidad de grado 4 con $\mathbb{Q}(\delta)$ cuerpo totalmente imaginario, sin embargo, $[\mathbb{Q}(\delta) : \mathbb{Q}] = 4$, y por otra parte $\delta^{-1} = \bar{\delta}$, luego $\mathbb{Q}(\delta + \delta^{-1})$ es un cuerpo totalmente real con $[\mathbb{Q}(\delta) : \mathbb{Q}(\delta + \delta^{-1})] = 2$. Luego $\mathbb{Q}(\delta)$ es un cuerpo CM. Pero esto es una contradicción con el Teorema 4.2. La contradicción nace al suponer que existe una unidad unimodular que no es raíz de la unidad y totalmente imaginaria de grado 4. Lo que se acaba de mostrar es que hay coherencia entre lo sabido para toros 2-dimensionales y la construcción recién mostrada.

4.2.2. Segunda construcción

En el Teorema 4.6 vimos que para cualquier dimensión mayor o igual a tres podemos encontrar un toro de dicha dimensión con un endomorfismo que tenga como valor propio un elemento unimodular que no es raíz de la unidad.

En la Subsección 4.2.1 se vio una construcción para encontrar toros complejos y endomorfismos en ellos con valores propios unimodulares que no son raíces de la unidad, que básicamente consiste en encontrar un entero algebraico de grado $2g$ en el círculo unitario, y tal que todos sus conjugados sean no reales. Entonces el problema se reduce a encontrar enteros algebraicos de dimensión $2g$ para todo g. ¿De qué manera podemos encontrar estos? Una manera de hacerlo es encontrar polinomios de grado $2g$ tales que se esté seguro que tienen raíces en el círculo unitario. Es en este punto donde los resultados de la Subsección 4 empiezan a jugar un papel importante. Consideremos la siguiente familia de polinomios

$$
\begin{aligned}
p_2(t) &= t^4 - 2t^3 + t^2 - 2t + 1 \\
p_3(t) &= t^6 - 2t^5 + t^4 + t^3 + t^2 - 2t + 1 \\
p_4(t) &= t^8 - 2t^7 + t^6 + t^5 + t^4 + t^3 + t^2 - 2t + 1 \\
p_5(t) &= t^{10} - 2t^9 + t^8 + t^7 + t^6 + t^5 + t^4 + t^3 + t^2 - 2t + 1 \\
&\vdots
\end{aligned}
$$

En general podemos escribir el k-ésimo polinomio de la siguiente forma

$$p_k(t) = \sum_{i=0}^{2k} t^i - 3t - 3t^{2k-1}$$

Por el Corolario 4.1 todos estos polinomios tienen al menos dos raíces en el círculo unitario, por otra parte lo que se conjetura es que ésta es una familia de polinomios irreducibles, no ciclotómicos y que sólo tienen raíces no reales. La irreducibilidad ha sido chequeada hasta $k = 500$ (es decir grado 1000), mientras que el hecho de que no divide a polinomios ciclotómicos se ha comprobado hasta $k = 200$.

Si se pudiera demostrar la conjetura podríamos enunciar el siguiente teorema:

Teorema 4.8. *Para todo entero $g \geq 3$, existe un toro complejo de dimensión g que tiene un endomorfismo con valores propios enteros algebraicos unimodulares totalmente imaginarios que no son raíces de la unidad.*

Demostración. Dado un $g \geq 3$, tomamos el polinomio $p_g(t)$, y hacemos la construcción de la Subsección 4.2.1 con la raíz de este polinomio que está en el círculo unitario. □

Bibliografía

[1] Amoroso, Francesco; David, Sinnou: *The Lehmer problem in higher dimension* J. Reine Angew. Math. 513 (1999), 145-179.

[2] Atiyah; Michael ;Macdonald, Ian Grant: *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass. 1969.

[3] Baker, Alan: *Transcendental Number theory.* Cambridge University Press, London-New York, 1975.

[4] Bauer, Thomas; Herrig, Thorsten: *Fixed points of endomorphisms on two-dimensional complex tori.* J. Algebra 458 (2016), 351-363.

[5] Birkenhake, Chistina; Lange, Herbert: *Fixed-point free automorphism of abelian varieties* Geom. Dedicata 51, no. 3, 201-213 (1994).

[6] Cohen, Henri: *Number theory. Vol. I. Tools and Diphantine equations.* Graduate Texts in Mathematics, 239. Springer, New York, 2007.

[7] Daileda, Ryan : *Algebraic Integers in the Unit Circle.* J. Number Theory 118 (2006), no. 2, 189-191.

[8] Everest, Graham; Ward, Thomas: *Heights of polynomials and entropy in algebraic dynamics.* Universitext. Springer-Verlag London 1999.

[9] Folland, Gerald B.: *Real Analysis, Modern Techniques and Their Applications.* Second edition. A Wiley-Interscience Publication. New york 1999.

[10] Helson, Henry: *Harmonic analysis. Second edition.* Texts and readings in Mathematics, 7. Hindustan Book Agency, New Delhi, 2010.

[11] Hidalgo, Rubén; Rodriguez,Rubí: *Introducción a las variedades abelianas y grupos kleinianos* Monografías Matemáticas UTFSM, 2005.

[12] Konvalina, John; Matache, Valentin: *Palindrome-polynomials with roots on the unit circle.* C.R. Math. Acad. Sci. Soc. R. Can. 26 (2004), no 2, 39-44.

[13] Lange, Herbert; Birkenhake, Christina: *Complex abelian varieties.* Grundlehren der Mathematischen Wissenschaften [Fundamentals Principles of Mathematical Sciences], 302. Springer-Verlag, Berlin, 1992.

[14] MacCluer, C. R.; Parry, Charles J.: *Units of Modulus 1* J. Number Theory 7 (1975), no. 4, 371-375.

[15] Morandi; Patrick: *Field and Galois Theory.* Graduate Texts in Mathematics, 167. Springer-Verlag, New York, 1996.

[16] Neukirch, Jurgen: *Algebaric Number Theory.* Springer-Verlag, Berlin, 1999.

[17] Shafarevich, Igor: *Basic Algebraic Geometry 1. Varieties in projective space.* Third Edition. Springer, Heidelberg, 2013.

[18] Silverman, Joseph H.: *the Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.