Pontificia Universidad Católica de Chile
Facultad de Matemáticas

Profesor: Héctor Pastén
Ayudante: José Cuevas Barrientos
Curso: Teoría de Números
Sigla: MAT2225
Fecha: 10 de noviembre de 2023

Dinámicas aritméticas

1. Dinámicas aritméticas

Para no complicarnos la vida, diremos que un morfismo $f\colon \mathbb{P}^1 \to \mathbb{P}^1$ es una función que en las cartas afines (es decir, sobre puntos de la forma $[x:1]$ e $[1:y]$) viene dado por funciones racionales (i.e., fracciones formales de polinomios). Si estas fracciones tienen ceros en los denominadores, entonces diremos que determina una aplicación racional $f\colon \mathbb{P}^1 \dashrightarrow \mathbb{P}^1$ (y se denotara con esta flecha quebrada). Nótese que todo morfismo está dado por funciones racionales, necesariamente del mismo grado y homogéneas (para que estén bien definidas en la recta proyectiva); llamaremos el ***grado*** de la aplicación racional al grado de las funciones que le definen por coordenadas.

Nótese que toda aplicación racional de $\mathbb{P}^1(\mathbb{C})$ de grado 1 viene dada por:

$$\mu_{a,b,c,d}([x:y]) := [ax+by : cx+dy], \qquad a,b,c,d \in \mathbb{C}.$$

Donde excluimos la posibilidad de que $a=b=c=d=0$.

1. Demuestre que las siguientes condiciones son equivalentes:
   a) $\mu_{a,b,c,d}$ es un morfismo (¡y no una aplicación racional!).
   b) $\mu_{a,b,c,d}$ es no constante.
   c) $\mu_{a,b,c,d}$ es inyectivo.
   d) $\mu_{a,b,c,d}$ es sobreyectivo.
   e) $ad-bc \neq 0$.

   Concluya que los automorfismos (i.e., isomorfismos de $\mathbb{P}^1 \to \mathbb{P}^1$) de grado 1 están en biyección con
   $$\mathrm{PGL}_2(\mathbb{C}) := \mathrm{GL}_2(\mathbb{C})/\mathbb{C}^\times.$$
   Los elementos de PGL_2 se dicen ***transformaciones de Möbius***.
2. Sean $(\alpha_1,\alpha_2,\alpha_3)$ y $(\beta_1,\beta_2,\beta_3)$ dos ternas de puntos distintos de $\mathbb{P}^1$. Demuestre que existe una transformación de Möbius $\mu \in \mathrm{PGL}_2(\mathbb{C})$ tal que cada $\mu(\alpha_i)=\beta_i$.

Definición 1.1: Sea $f\colon X \to X$ una función sobre un conjunto cualquiera. Dado un punto $x \in X$ su ***órbita*** es[1]

$$f^{\mathbb{N}}(x) := \{f^n(x) : n \in \mathbb{N}\},$$

donde f^n denota la composición n veces y donde $f^0 := \mathrm{Id}_X$. Denotaremos

$$\mathrm{Per}_n(f) := \{x \in X : f^n(x) = x\}, \qquad \mathrm{Per}_n^{**}(f) := \{x \in \mathrm{Per}_n(f) : \forall 0<m<n, \quad x \notin \mathrm{Per}_m(f)\}.$$

Se dice que x es ***periódico*** si $x \in \bigcup_{n=1}^{\infty} \mathrm{Per}_n(f)$. Se dice que x es ***preperiódico*** si su órbita $f^{\mathbb{N}}(x)$ es finita, de lo contrario se dice que x es un ***punto errante***. Se dice que x es ***estrictamente preperiódico*** si es preperiódico, pero no periódico.

3. Sea $\varphi(z) \in \mathbb{C}(z)$ una función racional de grado (geométrico)[2] $d \geq 2$.
   a) Demuestre que $|\mathrm{Per}_n(f)| \leq d^n+1$.
   b) Demuestre que $\lim_n |\mathrm{Per}_n(f)| = \infty$.
   c) Concluya que $\mathrm{Per}_n^{**}(f)$ no es vacío para infinitos n's.

[1] Otros textos también emplean $\mathcal{O}_f(x)$ u $O_f^+(x)$.

[2] El *grado geométrico* de una función racional $\varphi(z) = g(z)/h(z)$, donde $g,h \in \mathbb{C}[z]$ son polinomios coprimos es $\max\{\deg g, \deg h\}$.

4. Dada una curva elíptica $\mathcal{E}\colon y^2 = x^3 + Ax^2 + Bx + C$ con $A, B, C \in \mathbb{Q}$ en forma de Weierstrass, la fórmula explícita para la duplicación de un punto con coordenadas $P := [u : v : 1]$ es

$$x(2 \cdot P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6},$$

donde los b_i's son racionales en función de A, B, C. Se pueden explicitar como $b_2 = 4A, b_4 = 2B, b_6 = 4C, b_8 = B^2 - 4AC$. La fórmula anterior se conoce como ***fórmula de duplicación***.

Demuestre que $\mathcal{E}$ posee finitos puntos *racionales* de torsión cuyo orden sea de la forma 2^n.

5. Sea $f(x) \in \mathbb{Z}[x]$ un polinomio tal que el 0 sea un punto estrictamente preperiódico de f. Denotemos $\ell(f) := \operatorname{mcm}(f(0), f^2(0))$; para todo punto errante x_0 definamos:

$$a_n := \frac{f^n(x_0)}{\operatorname{mcd}(f^n(x_0), \ell(f))}.$$

a) Demuestre que $(a_n)_n$ es una sucesión de enteros coprimos dos a dos.
b) Con ello dé una nueva demostración de la infinitud de primos.

2. Comentarios adicionales

En el ejercicio 4 vimos un caso muy particular de torsión de una curva elíptica. Uno igual puede llevar el argumento más al extremo empleando fórmulas de para calcular n veces un punto P. Éstas fórmulas existen y vienen dadas por los llamados ***polinomios de división*** (cfr. Silverman **[3,** págs. 105-106], ex. 3.7). Aunque el argumento general que se emplea es identificando a una curva elíptica (¡sobre $\mathbb{C}$!) con un cociente de grupos topológicos $\mathbb{C}/\Lambda$, donde Λ es un reticulado pleno (i.e., es de la forma $\Lambda = \alpha\mathbb{Z} + \beta\mathbb{Z}$, donde $\alpha, \beta \in \mathbb{C}^\times$ son complejos no nulos tales que $\alpha/\beta \notin \mathbb{R}$); con ello no solo se concluye finitud general de la torsión, sino que la torsión (¡en $\mathbb{C}$!) se puede calcular completamente y $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$ (cfr. **[3,** pág. 106], ex. 3.8).

El último ejercicio fue una idea original de Granville **[1].**

Referencias y lecturas adicionales

1. Granville, A. Using Dynamical Systems to Construct Infinitely Many Primes. *Amer. Math. Monthly* **125,** 483-496. doi:10.1080/00029890.2018.1447732 (2018).
2. Silverman, J. H. *The arithmetic of dynamical systems.* (Springer-Verlag, 2007).
3. Silverman, J. H. *The arithmetic of elliptic curves.* 2.ª ed. (Springer-Verlag, 2009).

Correo electrónico: josecuevasbtos@uc.cl