ALTURAS Y DISTRIBUCIóN DE PUNTOS ALGEBRAICOS

RICARDO MENARES

Abstract. Las raíces del polinomio $x^n - 1$ se sitúan sobre el círculo unitario formando los vértices de un polígono regular de n lados. Cuando n crece, los polígonos aproximan al círculo cada vez mejor. En otras palabras, las raíces de la unidad se reparten de manera uniforme sobre el círculo cuando el orden tiende a infinito. Por otro lado, la familia de polinomios $(x-1)^n$ tiene sólo una raíz. El contraste entre la distribución límite de las raíces (uniforme en el primer ejemplo, concentrada en un punto en el segundo) se explica por la manera en que crecen los coeficientes del polinomio (nada en el primer caso y exponencialmente en el segundo). El ejemplo de las raíces de la unidad se extiende, más generalmente, al caso de sucesiones de puntos algebraicos "pequeños" en una curva (Teoremas de equidistribución de Bilu y de Szpiro-Ullmo-Zhang). La manera correcta de cuantificar el tamaño de los puntos algebraicos es a través de la teoría de alturas, que presentaremos en la primera parte del curso. La demostración de los teoremas de equidistribución mencionados requiere herramientas de geometría algebraica, teoría de números y análisis armónico. Trataremos de presentar, en líneas generales, la interacción de estas técnicas en este contexto.

Contents

1. Introducción

Estas notas corresponden a dos charlas a dictarse el contexto de la escuela Aritmética, Grupos y Análisis 2, que tendrá lugar en el Cusco, Perú, en Agosto de 2015. Aprovecho este espacio para agradecer a los organizadores la posibilidad de exponer el presente tópico.

Se ha tratado de mantener los requisitos necesarios para seguir estas charlas al mínimo. Para poder exponer el tema en el tiempo que se nos ha dado, hemos decidido concentrarnos en un caso especial del Teorema de Bilu, que data de 1997 (Teorema 5.1 en el texto).

2. Números algebraicos

Definición 2.1. Un elemento $\alpha \in \mathbb{C}$ se dice *número algebraico* si existe un polinomio no constante, con coeficientes racionales, $f(x) \in \mathbb{Q}[x]$, tal que $f(\alpha) = 0$.

Notar que todo número racional es algebraico. En efecto, si $\alpha = \frac{a}{b}$, con $a, b \in \mathbb{Z}$ y $b \neq 0$, entonces podemos tomar $f(x) = x - \frac{a}{b}$. Más ejemplos:

Ejemplos 2.1.
(1) $\alpha = i, \quad f(x) = x^2 + 1$
(2) $\alpha = \sqrt{2}, \quad f(x) = x^2 - 2$
(3) $\alpha = \sqrt[3]{2}, \quad f(x) = x^3 - 2$
(4) $\alpha = \zeta_n := e^{2\pi i/n}, \quad f(x) = x^n - 1, \quad n \in \mathbb{Z}_{>0}$
(5) $\alpha = \frac{1+\sqrt{5}}{2}, \quad f(x) = x^2 - x - 1$

Denotamos $\overline{\mathbb{Q}}$ al conjunto de los números algebraicos. Notar que $\overline{\mathbb{Q}}$ es un conjunto numerable. En efecto, $\mathbb{Q}[x]$ es numerable y cada elemento no constante de $\mathbb{Q}[x]$ tiene a lo más un número finito de raíces. Dado que $\mathbb{C}$ no es numerable, se desprende que existen números que no son algebraicos (y de hecho son mayoría). Sin embargo, no es fácil identificar un número no algebraico. Por ejemplo, se sabe que e (Hermite 1873) y π (Lindemann 1882) no son algebraicos, pero a la redacción de estas líneas no se sabe decidir si $e+\pi$ es algebraico o no.

El polinomio $f(x)$ que figura en la Definición 2.1 no es único. Cualquier polinomio de la forma $h(x) = f(x)g(x)$, con $g(x) \in \mathbb{Q}[x]$, sirve también. Sin embargo, nos será útil contar con un polinomio asociado de manera canónica a un número algebraico.

Proposición 2.1. *Sea $\alpha \in \overline{\mathbb{Q}}$. Entonces existe un único polinomio no constante $f_\alpha(x)$ que cumple*

(1) *$f_\alpha(x)$ tiene coeficientes racionales*
(2) *$f_\alpha(\alpha) = 0$*
(3) *$f_\alpha(x)$ es mónico (es decir, el coeficiente del término dominante es 1)*
(4) *el grado de $f_\alpha(x)$ es mínimo entre los polinomios que satisfacen (1), (2) y (3)*

Demostración: el principio del buen orden nos asegura que existe un polinomio $f(x) \in \mathbb{Q}[x]$ que satisface las cuatro propiedades del enunciado. Si $g(x)$ es otro polinomio que cumple las mismas propiedades, entonces podemos aplicar división de polinomios

$$f(x) = q(x)g(x) + r(x), \quad q(x), r(x) \in \mathbb{Q}[x], \quad \deg r(x) < \deg g(x).$$

Como $r(\alpha) = f(\alpha) - q(\alpha)g(\alpha) = 0$, de la minimalidad del grado de $f(x)$ concluímos que $r(x)$ es el polinomio nulo, es decir $f(x) = q(x)g(x)$. Como f y g tienen el mismo grado y son mónicos, entonces $f = g$ ■

Definición 2.2.
- Decimos que el polinomio $f_\alpha(x)$ dado por la Proposición (2.1) es el *polinomio mínimo* de α.
- Definimos el *grado de* α por $\deg \alpha := \deg f_\alpha$.

Definición 2.3. Un polinomio $f(x) \in \mathbb{Q}[x]$ se dice $\mathbb{Q}$-reductible si se puede escribir como producto de polinomios, con coeficientes racionales, de menor grado. Un polinomio en $\mathbb{Q}[x]$ que no es $\mathbb{Q}$-reductible se dice $\mathbb{Q}$-irreductible.

Observación: la minimalidad del grado de $f_\alpha(x)$ asegura que éste es un polinomio $\mathbb{Q}$-irreductible. Recíprocamente, se tiene

Proposición 2.2. *Sea $\alpha \in \overline{\mathbb{Q}}$ y sea $f(x) \in \mathbb{Q}[x]$ un polinomio $\mathbb{Q}$-irreductible y mónico tal que $f(\alpha) = 0$. Entonces $f = f_\alpha$.*

Demostración: aplicar división de polinomios ■

Definición 2.4. Dado un polinomio

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0 \in \mathbb{C}[x],$$

definimos el *polinomio reverso*

$$f^*(x) = a_0 x^n + a_1 x^{n-1} + \cdots a_{n-1}x + a_1 \in \mathbb{C}[x].$$

Lema 2.1. *Si $f(x) \in \mathbb{Q}[x]$ es $\mathbb{Q}$-irreductible, entonces $f^*(x)$ también lo es.*

Demostración: basta notar que $f^*(x) = x^{\deg f} f(1/x)$ y usar la Definición 2.3 ■

De la Proposición 2.2 y el Lema 2.1, se deduce

Corolario 2.1. *Si $\alpha \in \overline{\mathbb{Q}}$ y $\alpha \neq 0$, entonces $1/\alpha \in \overline{\mathbb{Q}}$. Más aún, $f_{1/\alpha} = f_\alpha^*$.*

No siempre es fácil determinar el polinomio mínimo de un número algebraico. En los ejemplos (2.1), los polinomios indicados son todos irreductibles (luego coinciden con el polinomio mínimo) excepto en el ejemplo (2.1), (4). En efecto,

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$

Dos herramientas básicas para decidir la irreductibilidad de un polinomio con coeficientes racionales son el Lema de Gauss y el Criterio de Eisenstein, que procedemos a explicar.

Definición 2.5. Un polinomio con coeficientes enteros $p(x) \in \mathbb{Z}[x]$ se dice $\mathbb{Z}$-reductible si existen polinomios $f(x), g(x) \in \mathbb{Z}[x]$ tales que

- $\deg f, \deg g < \deg p$
- $p(x) = f(x)g(x)$

Diremos que $p(x) \in \mathbb{Z}[x]$ es $\mathbb{Z}$-irreductible si no es $\mathbb{Z}$-reductible.

Un polinomio $\mathbb{Q}$-irreductible es inmediatamente $\mathbb{Z}$-irreductible. Un resultado notable es que la recíproca también es cierta.

Teorema 2.1. *(Lema de Gauss) Un polinomo $p(x) \in \mathbb{Z}[x]$ es $\mathbb{Q}$-irreductible si y sólo si es $\mathbb{Z}$-irreductible.*

Teorema 2.2. *(Criterio de Eisentein) Sea $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ un polinomio con coeficientes enteros. Suponga que existe un primo p tal que*

- $p | a_i, \quad i = 0, 1, \ldots, n-1$
- $p \nmid a_n$
- $p^2 \nmid a_0$

Entonces $f(x)$ es $\mathbb{Z}$-irreductible.

La demostración de estos teoremas está esbozada en los Ejercicios (2.1), (4) y (5).

Denotamos por $\Phi_n(x)$ al polinomio mínimo de $\zeta_n = e^{2\pi i/n}$.

Observación 2.1. Se tiene que $\Phi_n(x)$ es un divisor (en $\mathbb{Q}[x]$) del polinomio $x^n - 1$ (cf. Ejercicio 2.1 (1)). Del lema de Gauss, deducimos que $\Phi_n(x) \in \mathbb{Z}[x]$.

Como aplicación de los teoremas anteriores, demostraremos el siguiente

Lema 2.2. *Sea p un número primo. Entonces $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. En particular,*

$$x^p - 1 = (x-1)\Phi_p(x).$$

Demostración: Sea $w(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Veamos que $w(x)$ es un polinomio $\mathbb{Q}$-irreductible. Por el Lema de Gauss, basta con probar que es $\mathbb{Z}$-irreductible. Esto último equivale a demostrar que $h(x) := w(x+1)$ es $\mathbb{Z}$-irreductible. Usando la identidad $x^p - 1 = (x-1)w(x)$, se tiene

$$h(x) = w(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \left(\sum_{k=2}^{p-1} \binom{p}{k} x^{k-1} \right) + p.$$

Dado que $p | \binom{p}{k}$, para todo $0 < k < p$, el criterio de Eisentein permite concluir que $h(x)$ es $\mathbb{Z}$-irreductible. Tenemos entonces que $w(x)$ es $\mathbb{Q}$-irreductible y mónico, luego $w(x) = \Phi_p(x)$ por la Proposición 2.2 ■

Ejercicios 2.1.

(1) Sea $f(x) \in \mathbb{Q}[x]$ un polinomio $\mathbb{Q}$-irreductible y sea $\alpha \in \mathbb{C}$ tal que $f(\alpha) = 0$. Sea $g(x) \in \mathbb{Q}[x]$ un polinomio no constante tal que $g(\alpha) = 0$. Demuestre que existe un polinomio $h(x) \in \mathbb{Q}[x]$ tal que $g(x) = f(x)h(x)$.

(2) Un polinomio $p(x)$ se dice que tiene raíces repetidas si se puede factorizar sobre $\mathbb{C}$ de la forma

$$p(x) = (x-z)^2 h(x), \quad z \in \mathbb{C}, \quad h(x) \in \mathbb{C}[x]$$

(de manera equivalente, $p(z) = p'(z) = 0$). Demuestre que un polinomio $\mathbb{Q}$-irreductible $p(x) \in \mathbb{Q}[x]$ no puede tener raíces repetidas.

(3) Sea p un primo. Denotamos $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, el cuerpo finito de p elementos. Sea

$$\nu : \mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

el morfismo canónico. Para un polinomio con coeficientes enteros $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, definimos

$$\bar{f}(x) = \nu(a_n)x^n + \nu(a_{n-1})x^{n-1} + \cdots + \nu(a_1)x + \nu(a_0) \in \mathbb{F}_p[x].$$

Muestre que la operación $f \mapsto \bar{f}$ define un morfismo de anillos $\mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x]$ (es decir, verifique $\overline{f+g} = \bar{f} + \bar{g}$ y $\overline{fg} = \bar{f}\bar{g}$).

(4) *Lema de Gauss.* Decimos que un polinomio $f(x) \in \mathbb{Z}[x]$ es *reducido* si el máximo común divisor de sus coeficientes es 1.

(a) Sean $f(x), g(x) \in \mathbb{Z}[x]$ dos polinomios y sea $h(x) = f(x)g(x)$. Sea N el máximo común divisor de los coeficientes de $h(x)$. Suponga $N \neq 1$ y tome un primo p tal que $p|N$. Usando el morfismo de anillos del ejercicio anterior, demuestre que p o bien divide a todos los coeficientes de $f(x)$ o bien divide a todos los coeficientes de $g(x)$

(b) Deduzca que el producto de dos polinomios reducidos es reducido
(c) Demuestre el Teorema 4

(5) *Criterio de Eisenstein.* Sean $f(x) \in \mathbb{Z}[x]$ un polinomio y p un primo que satisfacen las hipótesis del Teorema 5.
(a) Suponga que se puede factorizar $f(x) = g(x)h(x)$ con $g(x), h(x) \in \mathbb{Z}[x]$. Muestre que entonces se tiene

$$\nu(a_n)x^n = \bar{g}(x)\bar{h}(x), \qquad \text{en } \mathbb{F}_p[x].$$

(b) Justifique que $\bar{g}(x) = ux^a, \bar{h} = vx^b$, con $u, v \in \mathbb{F}_p^*$ y $a + b = n$
(c) Demuestre el Teorema 5.

(6) Pruebe que $\overline{\mathbb{Q}}$ es un cuerpo. Es decir,

$$\alpha, \beta \in \overline{\mathbb{Q}}, \alpha \neq 0 \Rightarrow \frac{1}{\alpha}, \alpha\beta, \alpha + \beta \in \overline{\mathbb{Q}}.$$

2.1. Órbita galoisiana.

Definición 2.6.
- Sean $\alpha \in \overline{\mathbb{Q}}$ y $f_\alpha(x)$ su polinomio mínimo. Decimos que $\beta \in \mathbb{C}$ *es un conjugado de* α si $f_\alpha(\beta) = 0$.
- Definimos la *órbita galoisiana* de α por

$$\begin{aligned} G(\alpha) : &= \{\beta \in \mathbb{C} : \beta \text{ es un conjugado de } \alpha\} \\ &= \{\beta \in \mathbb{C} : f_\alpha(\beta) = 0\} \end{aligned}$$

Observación 2.2. El número de conjugados de α es exactamente el grado de $f_\alpha(x)$ (ver ejercicio (2.1), (2)).

Ejemplos 2.2.
- $G(i) = \{i, -i\}$
- $G(\sqrt{2}) = \{\sqrt{2}, -\sqrt{2}\}$
- $G(\sqrt[3]{2}) = \{\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}\}$
- $G(\frac{1+\sqrt{5}}{2}) = \{\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\}$

Es de interés para nosotros calcular la órbita galoisiana de ζ_n. Definimos

$$\begin{aligned} \mu_n : &= \{z \in \mathbb{C} : z^n = 1\} = \{\text{raíces de la unidad de orden } n\} \\ \tilde{\mu}_n : &= \{z \in \mu_n : z^k \neq 1, \quad \forall 1 \leq k < n\} = \{\text{raíces primitivas de la unidad de orden } n\} \end{aligned}$$

Notar que $(\mu_n, \cdot)$ es un grupo cíclico de orden n. Más precisamente, si $\zeta_n = e^{2\pi i/n}$, entonces $\mu_n = \{\zeta_n^j : 0 \leq j \leq n-1\}$. Más aún, se tiene

$$\tilde{\mu}_n = \{\zeta_n^j : mcd(j, n) = 1\}. \tag{2.1}$$

En particular, el número de elementos de $\tilde{\mu}_n$ es

$$\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*| = \#\{1 \leq j \leq n-1 : mcd(j, n) = 1\}$$

(función de Euler).

Proposición 2.3. *Sea* $\zeta_n = e^{2\pi in}$. *Entonces*

$$G(\zeta_n) = \tilde{\mu}_n.$$

La demostración de este hecho está esbozada en los Ejercicio 2.2, (3) y (4).

Corolario 2.2. *Se tiene* $\deg \Phi_n = \varphi(n)$, *para todo entero positivo* n.

Ejercicios 2.2.
(1) Demuestre (2.1).
(2) (a) Demuestre que para todo $\alpha \in \overline{\mathbb{Q}}$ y todo entero positivo k, se tiene

$$G(\alpha^k) = \{\beta^k : \beta \in G(\alpha)\}.$$

Deduzca $\deg(\alpha^k) \leq \deg(\alpha)$.
(b) Muestre que para $\alpha \in \overline{\mathbb{Q}}^*$, se tiene $G(1/\alpha) = \{1/\beta : \beta \in G(\alpha)\}$. Deduzca $\deg(\alpha) = \deg(1/\alpha)$.

(3) Sean n un entero y p un número primo que no divide n. Sea $\alpha \in \mathbb{C}$ tal que $\Phi_n(\alpha) = 0$. El objetivo de este problema es demostrar que $\Phi_n(\alpha^p) = 0$.
(a) Muestre que $\alpha^p \in \overline{\mathbb{Q}}$ y que su polinomio mínimo tiene coeficientes enteros.

(b) Suponga que $\Phi_n(\alpha^p) \neq 0$. Sea $g(x) \in \mathbb{Z}[x]$ el polinomio mínimo de α^p. Sea $h(x) = g(x^p)$. Muestre que $\Phi_n(x)|h(x)$ en $\mathbb{Z}[x]$.
(c) Sea $j(x) \in \mathbb{F}_p[x]$ un factor irreductible de $\overline{\Phi}_n(x) \in \mathbb{F}_p[x]$ (cf. la operación

$$f \in \mathbb{Z}[x] \mapsto \bar{f} \in \mathbb{F}_p[x]$$

definida en el Ejercicio 2.1 (3)). Muestre que $j(x)|\bar{g}(x)$.
(d) Use lo anterior para mostrar que $j(x)^2|x^n - 1$. Concluya.

(4) Use el ejercicio anterior para demostrar la Proposición 2.3.

3. Medida de Mahler de un polinomio en una variable

Sea $f(x) \in \mathbb{C}[x]$ un polinomio no nulo con coeficientes complejos. Definimos su *medida de Mahler* por

$$M(f) = \exp\Big(\frac{1}{2\pi}\int_0^{2\pi} \log|f(e^{i\theta})|d\theta\Big).$$

No es difícil ver que la integral es absolutamente convergente, incluso si el polinomio tiene raíces sobre el círculo unitario.

Lema 3.1. *Para todo polinomio no nulo $f \in \mathbb{C}[x]$, se tiene $M(f) = M(f^*)$.*

Demostración: si $n = \deg f$, tenemos $f^*(x) = x^n f(1/x)$, luego

$$M(f^*) = \exp\Big(\frac{1}{2\pi}\int_0^{2\pi} \log|f(e^{-i\theta})|d\theta\Big).$$

El enunciado resulta entonces de un cambio de variable apropiado ■

Nos será útil en lo que sigue usar la función $\log^+$, dada por

$$\log^+ z = \begin{cases} \log z & \text{si } z \geq 1 \\ 0 & \text{si } 0 < z < 1 \end{cases}$$

La medida de Mahler satisface las propiedades siguientes:

Teorema 3.1. (1) *$M(fg) = M(f)M(g)$, para todo $f, g \in \mathbb{C}[x], fg \neq 0$.*
(2) *$M(f) > 0$, para todo $f \in \mathbb{C}[x]$, no nulo.*
(3) *(Fórmula de Jensen) Sea $f(x) \in \mathbb{C}[x]$, un polinomio no nulo de grado n, que escribimos de la forma*

$$f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n), \quad a, \alpha_1, \ldots, \alpha_n \in \mathbb{C}. \tag{3.2}$$

Entonces

$$\log M(f) = \log|a| + \sum_{i=1}^{n} \log^+|\alpha_i|. \tag{3.3}$$

Demostración: Las primeras dos propiedades se deducen directamente de la defínción. Usando (1), nos reducimos a mostrar que para todo $\alpha \in \mathbb{C}$, se tiene

$$\frac{1}{2\pi}\int_0^{2\pi} \log|e^{i\theta} - \alpha|d\theta = \log^+|\alpha|. \tag{3.4}$$

Para demostrar esta identidad, usaremos que el promedio de una función armónica h sobre el borde del círculo unitario es $h(0)$.

Si $|\alpha| > 1$, entonces la función $h(x) = \log|x - \alpha|$ es armónica en el disco unitario, de manera que el término izquierdo de (3.4) es $h(0) = \log|\alpha|$.

Si $|\alpha| < 1$, entonces la función $w(x) = \log|1 - \alpha\bar{x}|$ es armónica en el disco unitario y coincide con $h(x)$ cuando $|x| = 1$. Por lo tanto el término izquierdo de (3.4) es $w(0) = \log|1| = 0$.

El caso $|\alpha| = 1$ se deduce por la continuidad de la función $\alpha \mapsto \int_0^{2\pi} \log|e^{i\theta} - \alpha|d\theta$■

3.1. **Discriminante y Resultante.** Representamos al polinomio $f(x) \in \mathbb{C}[x]$ de la forma (3.2). Notar que las raíces $\alpha_1, \alpha_2, \ldots, \alpha_n$ no son necesariamente distintas. Se define el *discriminante* de f por

$$D(f) = a^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Es inmediato de la definición que $D(f) = 0$ si y sólo si f tiene raíces repetidas.

Definición 3.1. Sean

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots a_1 x + a_0 \in \mathbb{C}[x] \\ g(x) &= b_m x^m + b_{m-1} x^{m-1} + \cdots b_1 x + b_0 \in \mathbb{C}[x]. \end{aligned}$$

Formamos la siguiente matriz de tamaño $(n+m) \times (n+m)$

$$M(f,g) = \begin{pmatrix} a_n & a_{n-1} & \ldots & a_0 & & & \\ 0 & a_n & a_{n-1} & \ldots & a_0 & & \\ & \ldots & & & & & \\ 0 & 0 & \ldots & a_n & a_{n-1} & \ldots & a_0 \\ b_m & b_{m-1} & \ldots & b_0 & & & \\ 0 & b_m & b_{m-1} & \ldots & b_0 & & \\ & \ldots & & & & & \\ 0 & 0 & \ldots & b_m & b_{m-1} & \ldots & b_0 \end{pmatrix}$$

Definimos la *resultante* $R(f,g)$ por

$$R(f,g) := \det M(f,g).$$

Teorema 3.2. *([Lan84], Proposition 8.3, p. 202) Escribimos $g(x) = b_m(x-\beta_1)\cdots(x-\beta_m)$. Entonces se tiene*

$$R(f,g) = a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j). \tag{3.5}$$

Observación 3.1. De este Teorema vemos que $R(f,g) = 0$ si y sólo si f y g tienen una raíz en común.

Central en lo que sigue es la siguiente

Proposición 3.1. *Si $f(x)$ tiene coeficientes enteros y a_n es el coeficiente del término dominante, entonces $a_n D(f) \in \mathbb{Z}$.*

Demostración: tomemos $g = f'$ en (3.5). Entonces $m = n-1$ y $b_m = n a_n$. Si escribimos

$$f'(x) = n a_n (x-\beta_1)\cdots(x-\beta_{n-1}),$$

entonces

$$R(f,f') = n^n a_n^{2n-1} \prod_{i=1}^{n} \frac{f'(\alpha_i)}{n a_n} = a_n^{n-1} \prod_{i=1}^{n} f'(\alpha_i).$$

Pero $f'(\alpha_i) = a_n \prod_{\substack{j=1 \\ j\neq i}}^{n} (\alpha_i - \alpha_j)$, luego obtenemos

$$R(f,f') = a_n^{2n-1} \prod_{i=1}^{n} \prod_{\substack{j=1 \\ j\neq i}}^{n} (\alpha_i - \alpha_j) = (-1)^{n(n-1)/2} a_n^{2n-1} \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2} a_n D(f).$$

Como f y f' tienen coeficientes enteros, de la definición de resultante tenemos $R(f,f') \in \mathbb{Z}$■

Ejercicio 3.1. Demostrar

$$|D(f)| \leq n^n M(f)^{2n-2}.$$

Indicación: exprese el discriminante como un determinante de Van der Monde.

Sea $\alpha \in \overline{\mathbb{Q}}^*$ y sea $f_\alpha(x) \in \mathbb{Q}[x]$ su polinomio mínimo. Existe un único entero positivo m tal que el polinomio

$$g_\alpha(x) := m f_\alpha(x)$$

satisface

- $g_\alpha(x)$ tiene coeficientes enteros
- el máximo común divisor de los coeficientes de $g_\alpha(x)$ es 1.

Decimos que $g_\alpha(x)$ es el *polinomio mínimo sobre* $\mathbb{Z}$ *de* α.
El claro que la órbita galoisiana de α se calcula por

$$G(\alpha) = \{\beta \in \mathbb{C} : g_\alpha(\beta) = 0\}$$

(cf. Definición 3).

Definición 4.1. Sea $\alpha \in \overline{\mathbb{Q}}^*$. Definimos su *altura* (de Weil) por

$$h(\alpha) = \frac{1}{\deg \alpha} \log M(g_\alpha).$$

De los Lemas 2.1 y 3.1 deducimos

Lema 4.1. *Para todo* $\alpha \in \overline{\mathbb{Q}}^*$, *se tiene* $h(\alpha) = h(1/\alpha)$.

Escribiendo

$$g_\alpha(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

de la fórmula de Jensen (3.3) se tiene

$$h(\alpha) = \frac{1}{\deg \alpha}\Big(\log a_n + \sum_{\beta \in G(\alpha)} \log^+ |\beta|\Big). \tag{4.6}$$

Proposición 4.1. *Se tiene que* $h(\alpha) \geq 0$, *para todo* $\alpha \in \overline{\mathbb{Q}}^*$. *Más aún,* $h(\alpha) = 0$ *si y sólo si* α *es una raíz de la unidad.*

Demostración: en la expresión (4.6), a_n es un entero positivo, de donde es claro que $h(\alpha) \geq 0$. Si α es una raíz de la unidad, la Proposición 2.3 asegura que $|\beta| = 1$, para todo $\beta \in G(\alpha)$. Además, de la Observación 2.1 tenemos que su polinomio mínimo sobre $\mathbb{Z}$ es mónico. Usando nuevamente (4.6), tenemos $h(\alpha) = 0$.

Supongamos ahora $h(\alpha) = 0$. Sea $n = \deg(\alpha)$. Escribamos

$$g_\alpha(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_i \in \mathbb{Z}. \tag{4.7}$$

Entonces la expresión (4.6) garantiza que $a_n = 1$ y

$$|\beta| \leq 1, \tag{4.8}$$

para todo $\beta \in G(\alpha)$.

La desigualdad (4.8) también vale para productos de elementos en $G(\alpha)$. Entonces, de la fórmula $g_\alpha(x) = \prod_{\beta \in G(\alpha)}(x - \beta)$, vemos que los coeficientes de $g_\alpha(x)$ satisfacen

$$|a_j| \leq n, \quad \forall j = 0, 1, 2, \ldots, n. \tag{4.9}$$

Se S_n el conjunto formado por todos los polinomios con coeficientes enteros, de grado a lo más n, de la forma (4.7) que además satisfacen (4.9). Tenemos que S_n es un conjunto finito.

Ahora bien, si k es un entero positivo, usando el Ejercicio 2.1, (2) vemos que el razonamiento anterior también se aplica a α^k, es decir, $\{g_{\alpha^k}(x) : k \in \mathbb{Z}_{>0}\} \subseteq S_n$. Como S_n es finito, el conjunto de raíces de polinomios en S_n también lo es, luego el conjunto

$$\{\alpha^k : k \in \mathbb{Z}_{>0}\}$$

es finito. Por lo tanto, existen enteros $k_1 \neq k_2$ tales que $\alpha^{k_1} = \alpha^{k_2}$ (equivalentemente, $\alpha^{k_1 - k_2} = 1$), lo que prueba que α es una raíz de la unidad ■

Terminamos esta sección con un problema abierto.

Pregunta 4.1. (Lehmer [Leh33]). Decidir si la siguiente afirmación es cierta: existe una constante $c > 0$ tal que

$$h(\alpha) \geq \frac{c}{\deg \alpha}, \quad \forall \alpha \in \overline{\mathbb{Q}}^* \text{ que no es una raíz de la unidad.}$$

Ejercicio 4.1. Adapte la demostración de la Proposición 4.1 para demostrar el teorema de Northcott: Sean $A, B > 0$. El conjunto

$$\{\alpha \in \overline{\mathbb{Q}}^* : \deg(\alpha) \leq A, \quad h(\alpha) \leq B\}$$

es finito.

5. Teorema de Bilu

5.1. Convergencia de medidas y enunciado del Teorema de Bilu.

Definición 5.1. Sea M el conjunto de medidas de probabilidad sobre $\mathbb{C}$. Definimos

$$C_0(\mathbb{C}) = \{f : \mathbb{C} \to \mathbb{C} \text{ continua y de soporte compacto}\}.$$

Decimos que una sucesión $(\nu_n) \subset M$ converge a $\nu \in M$ si para toda función $f \in C_0(\mathbb{C})$, se tiene

$$\lim_{n\to\infty} \int_{\mathbb{C}} f\nu_n = \int_{\mathbb{C}} f\nu.$$

En este caso, escribimos

$$\lim_{n\to\infty} \nu_n = \nu.$$

Ejemplos 5.1. Algunas medidas de probabilidad:

- Denotamos por $\nu_S \in M$ a la medida uniforme sobre el círculo. Está caracterizada por

$$\int_{\mathbb{C}} f\nu_S = \frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta})d\theta, \quad \forall f \in C_0(\mathbb{C}).$$

- Dado un punto $z \in \mathbb{C}$, denotamos por $\delta_z \in M$ a la medida de Dirac soportada en z. Está caracterizada por

$$\int_{\mathbb{C}} f\delta_z = f(z), \quad \forall f \in C_0(\mathbb{C}).$$

- Más generalmente, sea $E \subset \mathbb{C}$ un conjunto finito. Definimos

$$\delta_E := \frac{1}{\#E} \sum_{z\in E} \delta_z \in M. \tag{5.10}$$

  Esta medida está caracterizada por

$$\int_{\mathbb{C}} f\delta_E = \frac{1}{\#E} \sum_{z\in E} f(z), \quad \forall f \in C_0(\mathbb{C}).$$

  Las medidas de esta forma son ejemplos de *medidas atómicas*.

Definición 5.2. Sean $C \subset \mathbb{C}$ y $\nu \in M$. Decimos que ν *está soportada en* C si para toda $f \in C_0(\mathbb{C})$ cuyo soporte es disjunto a C, se tiene

$$\int_{\mathbb{C}} f\mu = 0.$$

Si ν está soportada en un conjunto compacto, decimos que ν tiene soporte compacto.

Denotamos por $M_C \subseteq M$ al conjunto de medidas soportadas en C.

Es claro que la medida ν_S está soportada en el círculo unitario y una medida de la forma δ_E está soportada en E. Todas estas medidas tienen soporte compacto.

Observación 5.1. Cuando C es compacto, el espacio M_C es secuencialmente compacto ([Bil68]). Es decir, toda sucesión $(\nu_n) \subset M_C$ admite una subsucesión convergente.

Definición 5.3. Consideremos una sucesión $E_n \subset \mathbb{C}$, donde cada E_n es un conjunto finito. Decimos que la familia (E_n) *se equidistribuye con respecto a* $\nu \in M$ si

$$\lim_{n\to\infty} \delta_{E_n} = \nu.$$

En otras palabras, se pide que para toda $f \in C_0(\mathbb{C})$,

$$\lim_{n\to\infty} \frac{1}{\#E_n} \sum_{z\in E_n} f(z) = \int_{\mathbb{C}} f\nu.$$

Definición 5.4. Decimos que una sucesión $(x_n) \subset \mathbb{C}$ es *genérica* si para todo $m \in \mathbb{N}$, el conjunto

$$\{k \in \mathbb{N} : x_k = x_m\}$$

es finito.

Teorema 5.1. *(Bilu, [Bil97]) Sea ν_S la medida de probabilidad uniforme sobre el círculo. Sea $(\alpha_n) \subset \overline{\mathbb{Q}}^*$ una sucesión genérica de números algebraicos tal que*

$$\lim_{n\to\infty} h(\alpha_n) = 0.$$

Entonces la familia de conjuntos $G(\alpha_n)$ se equidistribuye con respecto a ν_S.

En particular, se tiene el siguiente resultado notable:

Corolario 5.1. *La sucesión de conjuntos $(\tilde{\mu}_n)$ se equidistribuye con respecto a la medida ν_S.*

Demostración: tomando en cuenta la Proposición 2.3 y la Proposición 4.1, el enunciado se deduce directamente del Teorema de Bilu ■

Observación 5.2. El propósito de los ejercicios de esta sección es de indicar una demostración del Corolario 5.1 que no utiliza el Teorema de Bilu.

Ejercicios 5.1.

(1) Sea X un espacio métrico compacto. El espacio $M(X)$ (resp. $C_0(X)$) se define análogamente a M (resp. a $C_0(\mathbb{C})$) en la Definición 5.1 reemplazando $\mathbb{C}$ por X (resp. reemplazando $f : \mathbb{C} \to \mathbb{C}$ por $f : X \to \mathbb{C}$). La convergencia de medidas en $M(X)$ se enuncia de manera análoga la Definición 5.1, reemplazando $\int_{\mathbb{C}}$ por $\int_X$ y $C_0(\mathbb{C})$ por $C_0(X)$. El espacio $C_0(X) = C(X)$ se encuentra dotado de la topología dada por la norma supremo:

$$\|f\| = \sup_{z\in X} |f(z)|.$$

Sea $H \subset C(X)$ una subálgebra (es decir, $f, g \in H \to fg, f + g \in H$). Sea $V \subset H$ un conjunto generador (es decir, todo elemento de H es una combinación $\mathbb{C}$-lineal finita de elementos de V). Suponga que H es conjunto denso. Muestre que la sucesión de medidas $(\nu_n) \in M(X)$ converge a $\nu \in M(X)$ si y sólo si

$$\int_X f\nu_n = \int_X f\nu, \quad \forall f \in V.$$

(2) (a) En la notación del ejercicio anterior, tome $X = \{z \in \mathbb{C} : |z| = 1\}$. Para cada $k \in \mathbb{Z}$, definimos $h_k : X \to \mathbb{C}$ por $h_k(x) = x^k$. Sea $H \subset C(X)$ la subálgebra generada por $\{h_k : k \in \mathbb{Z}\}$. Muestre que H es densa en $C(X)$. Indicación: use el teorema de Stone-Weierstrass.

(b) (Criterio de Weyl) Sea $E_n \subset X$ una sucesión de conjuntos finitos. Deduzca que la familia (E_n) se equidistribuye con respecto a ν_S si y sólo si para todo $k \in \mathbb{Z}$, con $k \neq 0$, se tiene

$$\lim_{n\to\infty} \frac{1}{\#E_n} \sum_{z\in E_n} z^k = 0.$$

(c) Utilizando el punto anterior, demuestre que la sucesión de conjuntos μ_n se equidistribuye con respecto a ν_S.

(3) El propósito de este ejercicio es demostrar el Corolario 5.1, usando los ejercicios anteriores.

(a) Sea $\mu : \mathbb{N} \to \{-1, 0, 1\}$ la función de Möbius, dada por

$$\mu(n) = \begin{cases} 0 & \text{si existe un entero } m \geq 2 \text{ tal que } m^2|n \\ (-1)^r & \text{si } n \text{ es el producto de } r \text{ primos distintos.} \end{cases}$$

Sea $\delta_1 : \mathbb{N} \to \{0,1\}$ dada por

$$\delta_1(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$$

Demuestre

$$\sum_{d|n} \mu(d) = \delta_1(n).$$

(b) *Sumas de Ramanujan.* Denotamos por (a,b) el máximo común divisor del par a, b. Para $n \in \mathbb{N}$ y $k \in \mathbb{Z} - \{0\}$, definimos

$$S(n,k) = \sum_{\substack{0 \le j \le n-1 \\ (n,j)=1}} \zeta_n^{jk}, \quad \zeta_n = e^{2\pi i/n}.$$

Muestre que

$$S(n,k) = \sum_{d|(n,k)} d\mu\big(\frac{n}{d}\big).$$

Indicación: escriba $S(n,k) = \sum_{j=0}^{n-1} \delta_1\big((n,k)\big)\zeta_n^{jk}$ y aplique el punto anterior.

(c) Demuestre el Corolario 5.1.

5.2. **Energía.** Sea $\nu \in M$ una medida con soporte compacto. Entonces se define su energía por

$$E(\nu) := -\int_{\mathbb{C}}\int_{\mathbb{C}} \log|z-w|\nu(z)\nu(w) \in \mathbb{R} \cup \{\infty\}.$$

Ejemplos 5.2.

- Usando (3.4), vemos que $E(\nu_S) = 0$.
- Para todo conjunto finito $G \subset \mathbb{C}$, se tiene

$$E(\delta_G) = \infty.$$

En vista del último ejemplo, es útil introducir, para todo conjunto finito $G \subset \mathbb{C}$, la cantidad

$$E'(\delta_G) := -\frac{1}{(\#G)^2} \sum_{\substack{z,w \in G \\ z \neq w}} \log|z-w| \in \mathbb{R}.$$

El nexo entre la teoría de alturas y la teoría del potencial está dado por el siguiente

Lema 5.1. *(Comparación Energía-Altura) Sea $\alpha \in \overline{\mathbb{Q}}^*$. Entonces se tiene*

$$E'(\delta_{G(\alpha)}) \le 2h(\alpha).$$

Demostración: sea $n = \deg\alpha$, a_n el coeficiente dominante de g_α y escribimos $G(\alpha) = \{\alpha_1, \ldots, \alpha_n\}$. Como g_α es irreductible, tenemos $D(g_\alpha) \neq 0$. Además, $a_n D(g_\alpha) \in \mathbb{Z}$ (Proposición 3.1), de donde

$$\log(a_n|D(g_\alpha)|) \ge \log 1 = 0. \tag{5.11}$$

Se tiene

$$\begin{aligned} 0 \le \log a_n + \log|D(g_\alpha)| &= (2n-1)\log a_n + 2\sum_{i<j} \log|\alpha_i - \alpha_j| \\ &= (2n-1)\log a_n + \sum_{i \neq j} \log|\alpha_i - \alpha_j| \\ &= (2n-1)\log a_n - n^2 E'(\delta_{G(\alpha)}). \end{aligned}$$

Por otro lado, de (4.6) tenemos

$$\begin{aligned} \log a_n &= nh(\alpha) - \sum_i \log^+|\alpha_i| \\ &\le nh(\alpha) \end{aligned}$$

Combinando ambas desigualdades se obtiene el resultado ■

En lo que sigue utilizaremos dos resultados de la teoría de capacidades. Las demostraciones pueden consultarse en [Rum89].

Proposición 5.1. *Sea $G_n \subset \mathbb{C}$ una sucesión de conjuntos finitos tales que $\#G_n$ tiende a infinito con n. Supongamos que existe $\nu \in M$ tal que la familia (G_n) se equidistribuye con respecto a ν. Entonces se tiene*

$$E(\nu) \leq \liminf_{n\to\infty} E'(\delta_{G_n}).$$

Proposición 5.2. *Sea M_S el conjunto de todas las medidas en M soportadas en $\{z \in \mathbb{C} : |z| = 1\}$. Entonces*

$$E(\nu) \geq 0, \quad \forall \nu \in M_S.$$

Más aún,

$$\nu \in M_S, \quad E(\nu) = 0 \Leftrightarrow \nu = \nu_S.$$

5.3. **Esbozo de la demostración del Teorema de Bilu.** En toda esta sección asumimos que la sucesión $(\alpha_n) \subset \overline{\mathbb{Q}}^*$ es genérica y cumple

$$h(\alpha_n) \to 0, \quad n \to \infty.$$

Unidas al Ejercicio 4.1, estas hipótesis aseguran que $\deg(\alpha_n)$ tiende a infinito con n.

La demostración del enunciado siguiente se encuentra al final de esta sección.

Lema 5.2. *(Equidistribución en radio). Para cada $n \in \mathbb{N}$, se puede escoger un conjunto $E_n \subseteq G(\alpha_n)$ de manera que*

(1) $\lim_{n\to\infty} \frac{\#E_n}{\#G(\alpha_n)} = 1$.
(2) *Para todo $\varepsilon > 0$, existe n_0 tal que para todo $n \geq n_0$ se tiene*

$$z \in E_n \Rightarrow 1 - \varepsilon \leq |z| \leq 1 + \varepsilon.$$

Supongamos que podemos establecer que $\delta_{E_n} \to \nu_S$. Entonces la condición (1) en el Lema 5.2 permite mostrar que también se tiene $\delta_{G(\alpha_n)} \to \nu_S$. Luego en lo que sigue, trabajaremos con la familia (E_n).

La condición (2) en el Lema 5.2, permite mostrar que existe un compacto $K \subset \mathbb{C}$ que contiene al círculo unitario tal que $\delta_{E_n} \in M_K$, para todo n. Como M_K es secuencialmente compacto (cf. Observación 5.1), tenemos que la sucesión δ_{E_n} admite una subsucesión $\delta_{E_{n_j}}$ convergente a una medida $\nu \in M_K$.

Usando de nuevo la condición (2) en el Lema 5.2, podemos concluir que ν está soportada en el círculo unitario. De la Proposición 5.2, deducimos que $E(\nu) \geq 0$. Ahora bien,

$$\begin{aligned} E(\nu) &\leq \liminf E'(\delta_{E_{n_j}}) && \text{Proposición 5.1} \\ &\leq \liminf E'(\delta_{G(\alpha_{n_j})}) && \text{condición (1) en el Lema 5.2} \\ &\leq 2 \liminf h(\alpha_{n_j}) && \text{Lema 5.1} \\ &= 0. \end{aligned}$$

Por lo tanto, $E(\nu) = 0$. Aplicando nuevamente la Proposición 5.2, deducimos $\nu = \nu_S$.

Hemos establecido que toda subsucesión convergente de δ_{E_n} tiene como límite a la medida ν_S. Esto muestra que δ_{E_n} converge a ν_S, terminando la demostración del Teorema de Bilu.

Demostración del Lema 5.2: Notar que por el Lema 4.1, también tenemos

$$h(1/\alpha_n) \to 0, \quad n \to \infty.$$

Procederemos por contradicción. Pasando a una subsucesión si fuese necesario, podemos suponer que existen subconjuntos $V_n \subseteq G(\alpha_n)$ tales que

- $\lim_{n\to\infty} \frac{\#V_n}{\#G(\alpha_n)} = c > 0$.
- existe $a > 1$ tal que para todo n, se tiene

$$z \in V_n \Rightarrow |z| > a \text{ ó } \left|\frac{1}{z}\right| > a.$$

Descomponemos $V_n = A_n \cup B_n$, donde

$$z \in A_n \Leftrightarrow |z| > a, \qquad z \in B_n \Leftrightarrow \left|\frac{1}{z}\right| > a.$$

Usando la fórmula de Jensen tenemos

$$\begin{aligned} h(\alpha_n) &\geq \frac{1}{\deg(\alpha_n)}\Big(\sum_{\beta\in A_n}\log|\beta|\Big) \\ &\geq \frac{\#A_n}{\deg(\alpha_n)}\log a \end{aligned}$$

(5.12)

Por otro lado, usando el Ejercicio 2.1 (2) también se tiene

$$\begin{aligned} h(1/\alpha_n) &\geq \frac{1}{\deg(\alpha_n)}\Big(\sum_{\beta\in B_n}\log|1/\beta|\Big) \\ &\geq \frac{\#B_n}{\deg(\alpha_n)}\log a \end{aligned}$$

(5.13)

Luego

$$h(\alpha_n)+h(1/\alpha_n)\geq \frac{\#V_n}{\deg\alpha_n}\log a.$$

Tomando el límite cuando $n\to\infty$, obtenemos

$$0\geq c\log a>0,$$

lo que es absurdo ■

6. Bibliografía sugerida

Hemos presentado el estudio más somero posible de los números algebraicos. Sin embargo, se trata de una teoría profunda e importante dentro de la matemática pura contemporánea. Existen excelentes libros que exponen este material, por ejemplo [BS66], [Neu99], [Mar77].

La noción de altura es una herramienta muy útil en teoría de números, cuyos orígenes se pueden trazar hasta Fermat. En muchos problemas modernos del área la dificultad se concentra en establecer una variante adecuada de esta noción. Recomendamos [BG06] y [Sil86].

El nexo entre la teoría del potencial y la teoría de alturas está bien explicado en [Rum89].

References

[BG06] Enrico Bombieri and Walter Gubler. *Heights in Diophantine geometry*, volume 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

[Bil68] Patrick Billingsley. *Convergence of probability measures*. John Wiley & Sons Inc., New York, 1968.

[Bil97] Yuri Bilu. Limit distribution of small points on algebraic tori. *Duke Math. J.*, 89(3):465–476, 1997.

[BS66] A. I. Borevich and I. R. Shafarevich. *Number theory*. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York, 1966.

[Lan84] Serge Lang. *Algebra*. Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, second edition, 1984.

[Leh33] D. H. Lehmer. Factorization of certain cyclotomic functions. *Ann. of Math. (2)*, 34(3):461–479, 1933.

[Mar77] Daniel A. Marcus. *Number fields*. Springer-Verlag, New York, 1977. Universitext.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Rum89] Robert S. Rumely. *Capacity theory on algebraic curves*, volume 1378 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1989.

[Sil86] Joseph H. Silverman. The theory of height functions. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 151–166. Springer, New York, 1986.

Instituto de Matemáticas, PUCV, Blanco Viel 596, Cerro Barón, Valparaíso, Chile
E-mail address: ricardo.menares@ucv.cl