Seminario de Geometría Aritmética
PUC Chile, 2^{do} semestre de 2018

CHARLA: EL TEOREMA DEL SUBESPACIO

HÉCTOR PASTÉN

1. Versión clásica

En lo siguiente, $\|-\|$ es la norma del máximo. También fijamos una clausura algebraica $\mathbb{Q}^{alg}$ con una inclusión $\mathbb{Q}^{alg} \to \mathbb{C}$, de forma que se extiende el valor absoluto usual de $\mathbb{Q}$ a $\mathbb{Q}^{alg}$.

Teorema 1.1 (Schmidt 1972)**.** *Sean $L_1, ..., L_n \in \mathbb{Q}^{alg}[x_1, ..., x_n]$ homogéneas de grado 1, linealmente independientes sobre $\mathbb{Q}^{alg}$. Sea $\epsilon > 0$. Existe un conjunto finito $H_1, ..., H_r$ de subespacios lineales propios de $\mathbb{Q}^n$ tales que para todo punto entero $\mathbf{a} = (a_1, ..., a_n) \in \mathbb{Z}^n$ fuera de los H_j se cumple*

$$\prod_{j=1}^{n} |L_j(\mathbf{a})| > \frac{1}{\|\mathbf{a}\|^\epsilon}.$$

Ejemplo. Sea $\alpha \in \mathbb{C}$ algebraico de grado $d \geq 2$. Las formas lineales

$$L_1(x_1, x_2) = x_1 - \alpha x_2, \quad L_2(x_1, x_2) = x_2$$

tienen coeficientes algebraicos y son linealmente independientes sobre $\mathbb{Q}^{alg}$. Sea $\epsilon > 0$. Entonces hay finitos $H_1, ..., H_r \subseteq \mathbb{Q}^2$ subespacios lineales propios tales que para todo $(p, q) \in \mathbb{Z}^2$ fuera de ellos se cumple

$$|(p - \alpha q)q| > \frac{1}{\max\{|p|, |q|\}^\epsilon}$$

es decir

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^2 \max\{|p|, |q|\}^\epsilon}.$$

Vamos a restringirnos a los puntos primitivos, es decir, con $\gcd(p, q) = 1$. Entonces los finitos subespacios H_j solo prohiben finitos de estos puntos. Obtenemos que, salvo finitas excepciones, se cumple

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^2 \max\{|p|, |q|\}^\epsilon}.$$

Esto es el *Teorema de Roth* que ya hemos estudiado anteriormente en el seminario.

Observaciónes.

- La norma $\|-\|$ puede cambiarse por cualquier otra (e.g. L^2) en lugar de usar la L^∞.
- El teorema en el caso de puntos enteros primitivos implica el caso general.
- Salvo jugar con la elección de $\epsilon > 0$, la desigualdad del teorema es equivalente a

$$\prod_{j=1}^{n} \frac{|L_j(\mathbf{a})|}{\|\mathbf{a}\|} > \frac{1}{\|\mathbf{a}\|^{n+\epsilon}}.$$

  pero ahora el lado izquierdo no cambia bajo proporcionalidad de $\mathbf{a}$.

Date: 11 de Octubre de 2018.

Teorema 1.2 (Versión proyectiva)**.** *Sean $L_0, ..., L_n$ hiperplanos de $\mathbb{P}^n_{\mathbb{Q}^{alg}}$ definidos sobre $\mathbb{Q}^{alg}$ en posición general (i.e. sus ecuaciones son linealmente independientes). Sea $\epsilon > 0$. Existen finitos subespacios lineales propios de $\mathbb{P}^n$ definidos sobre $\mathbb{Q}$ tales que fuera de ellos, todo punto racional $x \in \mathbb{P}^n(\mathbb{Q})$ cumple*

$$\sum_{j=0}^{n} \lambda_\infty(L_j, x) < (n + 1 + \epsilon)h(x).$$

Recordamos que la altura de un punto racional $x \in \mathbb{P}^n(\mathbb{Q})$ es

$$h(x) = \log \max\{|x_0|, ..., |x_n|\} \quad \text{con } x = [x_0 : ... : x_n], x_j \in \mathbb{Z}, \gcd(x_0, ..., x_n) = 1.$$

Además, para L hiperplano, $\lambda_\infty(L, x)$ es la *función de proximidad* (o *función de Weil*, o *altura local*) con respecto al lugar ∞ de $\mathbb{Q}$, y se define por

$$\lambda_\infty(L, x) = -\log \frac{|L(x_0, ..., x_n)|}{\max_{0\le i\le n} |x_i|}, \quad x = [x_0 : ... : x_n]$$

donde $L(x_0, ..., x_n)$ es una ecuación para el hiperplano L. Esta ecuación se elige y se fija; de esta forma la función $\lambda_\infty(L, -)$ es bien definida salvo un error acotado (que viene de la elección de una ecuación para L).

Salvo un error acotado, $\lambda_\infty(L, x)$ es lo mismo que

$$\log \frac{1}{\text{dist}_\infty(L, x)} \ge 0, \quad \text{con dist}_\infty \text{ la métrica de Fubini-Study.}$$

2. Versión general

Definición. Hiperplanos $L_1, ..., L_q$ de $\mathbb{P}^n$ están en *posición general* si la intersección de cualquier subcolección de ellos tiene la dimensión esperada. Para $q = n + 1$ es lo mismo que "linealmente independiente".

Teorema 2.1 (Schmidt, Schlickewei, Lang)**.** *Sea K campo de números, sea $S \subseteq M_K$ finito, y sean $q, n \ge 1$. Para cada $v \in S$ fijar una extension de v a K^{alg}, y sean $L_{v,1}, ..., L_{v,q}$ hiperplanos de $\mathbb{P}^n_{K^{alg}}$ en posición general. Sea $\epsilon > 0$. Existe un conjunto finito de subespacios lineales propios $H_1, ..., H_r \subseteq \mathbb{P}^n_K$ (dependiendo de todo lo anterior) tales que para todo $x \in \mathbb{P}^n(K)$ fuera de ellos se cumple*

$$\sum_{v\in S} \sum_{j=1}^{q} \lambda_v(L_{v,j}, x) < (n + 1 + \epsilon)h_K(x).$$

Aquí, la función de proximidad se define por

$$\lambda_v(L, x) = -\log \frac{\|L(x_0, ..., x_n)\|_v}{\max_{0\le j\le n} \|x_j\|_v}, \quad \|\alpha\|_v = \begin{cases} |\alpha|_v & \text{si } v \text{ es real o no-arquimedeano} \\ |\alpha|_v^2 & \text{si } v \text{ es complejo.} \end{cases}$$

Observaciónes.

- Las funciones de proximidad a hiperplanos están bien definidas salvo un error acotado, debido a la elección de una ecuación para el hiperplano. Además, son acotadas inferiormente.
- Podría parecer que q arbitrario es más fuerte que $q = n+1$ (cf. versión anterior con $K = \mathbb{Q}$). Pero la hipótesis de posición general (y un argumento de subsecuencias) permite mostrar que el resultado para $q = n + 1$ implica el caso de q arbitrario: básicamente, un punto no puede estar v-ádicamente cerca de más de $n + 1$ de los $L_{v,j}$ a la vez.

3. Aplicación: la ecuación S-unidad

Teorema 3.1. *Sea K campo de números, $S \supseteq M_K^\infty$ conjunto finito de lugares. Sea $n \geq 0$ y sean $A_0, ..., A_n \in K^\times$. Todas salvo finitas soluciones en $O_{K,S}^\times$ de la ecuación*

$$A_0 x_0 + ... + A_n x_n = 1$$

cumplen que alguna sub-suma se anula.

Ejemplo. Si $K = \mathbb{Q}$ y $S = \{\infty, 2\}$ entonces la ecuación $x + y + z = 1$ tiene infinitas soluciones en $\mathbb{Z}_S^\times$, por ejemplo, $(2^k, -2^k, 1)$. Pero el teorema dice que solamente tiene finitas soluciones en $\mathbb{Z}_S^\times$ sin sub-sumas nulas, como por ejemplo $(2, -1/2, -1/2)$.

Demostración del teorema. El resultado es trivial para $n = 0$. Vamos a suponer $n \geq 1$.

En $\mathbb{P}_K^n$ tomamos los $n + 2$ hiperplanos

$$\begin{aligned} L_0 &= \{x_0 = 0\} \\ &\vdots \\ L_n &= \{x_n = 0\} \\ L_{n+1} &= \{A_0 x_1 + ... + A_n x_n = 0\}. \end{aligned}$$

Estos hiperplanos están en posición general.

De manera 1-1, a cada solución $u_0, ..., u_n$ en $O_{K,S}^\times$ asociamos el punto $u = [u_0 : ... : u_n] \in \mathbb{P}^n(K)$ con coordenadas $u_i \in O_{K,S}^\times$. Estos puntos cumplem que para cualquier $1 \leq j_0 \leq n$

$$\begin{aligned} \sum_{v \in S} \lambda_v(L_{j_0}, u) &= \sum_{v \in S} -\log \frac{\|u_{j_0}\|_v}{\max_{0 \leq i \leq n} \|u_i\|_v} \\ &= \sum_{v} -\log \frac{\|u_{j_0}\|_v}{\max_{0 \leq i \leq n} \|u_i\|_v} \quad \text{porque } u_i \in O_{K,S}^\times \\ &= \sum_{v \in S} \log \max_{0 \leq i \leq n} \|u_i\|_v \quad \text{por la fórmula del producto} \\ &= h_K(u). \end{aligned}$$

Además, como $A_0 u_0 + ... + A_n u_n = 1$ obtenemos

$$\sum_{v \in S} \lambda_v(L_{n+1}, u) = \sum_{v \in S} -\log \frac{\|A_0 u_0 + ... + A_n u_n\|_v}{\max_{0 \leq i \leq n} \|u_i\|_v} = \sum_{v \in S} \log \max_{0 \leq i \leq n} \|u_i\|_v = h_K(u).$$

Así que para estos puntos $u \in \mathbb{P}^n(K)$ obtenemos

$$\sum_{v \in S} \sum_{j=0}^{n+1} \lambda_v(L_j, u) = (n+2) h_K(u).$$

Por el teorema del subespacio (con $\epsilon = 1/2$), estos puntos están en finitos subespacios propios. Si u no está en uno de los subespacios que corresponde a una sub-suma nula, entonces $u_j \neq 0$ para cada j y además satisface una de entre *finitas* relaciones del tipo

$$x_n = b_0 x_0 + ... + b_{n-1} x_{n-1}, \quad b_j \in K^\times.$$

Dividiendo por $u_n \neq 0$ podemos aplicar inducción. $\square$

Departamento de Matemáticas, PUC Chile
E-mail address, H. Pasten: hpasten@gmail.com