Seminario CM, 25/3/2020

Formas cuadráticas binarias

1. Generalidades

Nos interesaremos en formas cuadráticas del tipo

$$f(x,y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x,y]$$

- Diremos que f es primitiva si $m.c.d.(a,b,c) = 1$.
- $m \in \mathbb{Z}$ es representado por f si $\exists\, u, v \in \mathbb{Z}$ con

$$f(u,v) = m.$$

Diremos que m es primitivamente representado si $m.c.d.(u,v) = 1$.

Notar que si m es representado por f y libre de cuadrados, entonces también es primitivamente representado.

Motivados por la clasificación de enteros representables por una forma cuadrática, Lagrange, Legendre y Gauss consideraron la siguiente noción de equivalencia:

f, g formas cuadráticas se dicen equivalentes si $\exists\, p,q,r,s \in \mathbb{Z}$ con $ps - qr = 1$ y

$$f(x,y) = g(px+qy, rx+sy).$$

En otras palabras, si $SL_2(\mathbb{Z}) := \left\{ \begin{pmatrix} p & q \\ r & s \end{pmatrix} \gamma \in M_2(\mathbb{Z}) \text{ con } \det \gamma = 1 \right\}$

Entonces $f \sim g$ si $\exists\, \gamma \in SL_2(\mathbb{Z})$ con

$$f(x,y) = g\left(\gamma \cdot \begin{pmatrix} x \\ y \end{pmatrix}\right).$$

Es fácil ver que $\sim$ es una relación de equivalencia y que formas equivalentes representan los mismos enteros.

Lo mismo vale para representaciones propias.

El discriminante de $f(x,y) = ax^2 + bxy + cy^2$ se define por $D := b^2 - 4ac$. Notar que

- $D \equiv 0$ ó $1 \mod 4$
- La relación $\sim$ preserva el discriminante.
- La identidad $4a\,f(x,y) = (2ax + by)^2 - Dy^2$ muestra que
  - i) Si $D > 0$, entonces f representa enteros tanto negativos como positivos $\rightsquigarrow f$ es indefinida
  - ii) Si $D < 0$ y $a > 0$, f representa solo enteros > 0 $\rightsquigarrow f$ es definida positiva

$D < 0$ y $a < 0 \Rightarrow f$ es def. < 0.

El problema de representar enteros siempre puede reducirse a estudiar formas primitivas. Esto motiva definir, para $D < 0$:

$$C(D) = \left\{ \begin{array}{c} \text{clases de equivalencia de formas cuadráticas} \\ \text{binarias primitivas y def. } > 0 \text{ de discriminante } D \end{array} \right\}$$

Obs: i) $C(D) \neq \emptyset \Leftrightarrow D \equiv 0, 1 \bmod 4$.

Esta charla tiene dos objetivos

1) Mostrar que $C(D)$ es finito

2) Describir una ley de grupo en $C(D)$, que más adelante veremos se relaciona con la ley del grupo de clases de $\mathbb{Q}(\sqrt{D})$.

Comentario: para $D > 0$ hay un $C(D)$ análogo para el que se cumple 1) y una variante de 2), pero las teorías detrás son distintas.

Finitud

Hay una "teoría de la reducción" cuyo fin es describir el elemento más "pequeño" en una clase en $C(D)$.

Una forma primitiva $f = ax^2 + bxy + cy^2$ se dice reducida si

$$|b| \leq a \leq c \quad \text{y además} \quad (|b| = a \text{ ó } a = c) \Rightarrow b \geq 0$$

Teorema A Toda forma primitiva y def. > 0 es equivalente a una única forma reducida.

Teorema A Toda forma primitiva y def >0 es equivalente a una única forma reducida.

Teorema B Sea $f(x,y) = ax^2 + bxy + cy^2$ es una forma reducida de discriminante $D<0$. Entonces

$$a \leq \sqrt{\frac{-D}{3}}.$$

Afirmación: Teorema A + B $\Rightarrow$ $C(D)$ es finito.

En efecto, Teorema A $\Rightarrow$ basta mostrar que hay a lo más un nº finito de formas reducidas en $C(D)$.

Si f es def >0 y reducida, entonces $a>0$
Theorema B $\Rightarrow$ hay a lo más un nº finito de a's.

Como $|b| \leq a$ $\Rightarrow$ hay a lo más un nº finito de b's.

Como $D = b^2 - 4ac$, hay a lo más un nº finito de c's. ∎

Dem. del Teorema B: f reducida $\Rightarrow b^2 \leq a^2$, $0 < a \leq c$,

luego $D = \underbrace{b^2}_{\leq a^2} - 4a\underbrace{c}_{\geq a} \leq a^2 - 4a^2 = -3a^2$

$$\Rightarrow a \leq \sqrt{\frac{-D}{3}}$$ ∎

(existencia)

Dem. del Teorema A: ↓ tomemos $\alpha \in C(D)$

Sea $f(x,y) = ax^2 + bxy + cy^2 \in \alpha$ tal que $|b|$ es mínimo.

Afirmación: $a \geq |b|$

Dem: si $a < |b|$, entonces usar que $\forall m \in \mathbb{Z}$,

$$\gamma = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z}) \quad y \quad g(x,y) := \gamma \cdot f(x,y) = f(x+my, y)$$

es equivalente a f. Pero

$$g(x,y) = ax^2 + (2am + b)xy + \tilde{c}y^2$$

Como $a < |b|$, $\exists m$ t.q. $|2am + b| < |b|$, lo que contradice la elección de $f(x,y)$. $\rightarrow \leftarrow$

Supongamos $a > c$. Entonces usamos $S = \begin{pmatrix} 0 & -1 \\ +1 & 0 \end{pmatrix}$

$$g(x,y) := S \cdot f(x,y) = f(-y, x) = ay^2 - bxy + cx^2$$

es equivalente y los roles de a y c han sido intercambiados.

$\therefore$ podemos suponer $|b| \leq a \leq c$.

Supongamos que f no es reducida, es decir

$$b < 0 \ ; \ (a = -b \ \vee \ a = c)$$

Si $a = -b$, $f(x,y) = ax^2 - axy + cy^2$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot f(x,y) = f(x+y, y) = ax^2 + axy + cy^2$$

es reducida!

Si $a = c$, usar $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Unicidad: Usamos el

Lema: Sea $f = ax^2 + bxy + cy^2$ una forma reducida, $\det > 0$.
Si $u, v \in \mathbb{Z}$ cumplen $\mcd(u,v) = 1$ y $f(u,v) \leq c$,
entonces $f(u,v) \in \{a, c\}$, $(u,v) \in \{\pm(1,0), \pm(0,1), \pm(1,-1)\}$.

Más aún, el nº de representaciones propias de a es

2	si	$a < c$
4	si	$0 \leq b < a = c$
6	si	$a = b = c$

Sean $[f], [g] \in C(D)$, reducidas, primitivas con $f \sim g$.

p.d. $f = g$.

$f = ax^2 + bxy + cy^2$, $g = a'x^2 + b'xy + c'y^2$

$f \sim g \Rightarrow$ representan los mismos enteros.
Lema $\Rightarrow$ a es el menor entero propiamente representado
$\Rightarrow a = a'$.

Caso 1: $a < c$

Lema $\Rightarrow$ hay exactamente 2 reps. primitivas de a por f.
Lo mismo vale para g.
Lema $\Rightarrow$ $a' < c'$.

Entonces

Entonces c es el segundo menor entero prop. rep. por f

y c' " " " " " " " " " " " " y

Como son equivalentes, $c = c'$.

Como $D = b^2 - 4ac = b'^2 - 4ac$

$\Rightarrow \quad b = \pm b'$

Pero si $g = \gamma \cdot f$, $\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$, entonces

$a = g(1,0) = f(p,r)$ Como $ps - rq = 1$,

$c = g(0,1) = f(q,s)$ estas representaciones son propias.

Lema.

$\Rightarrow \quad (p,r) = \pm (1,0)$, $(q,s) \in \{ \pm(0,1), \pm(1,-1) \}$.

Pero $f(1,-1) = \underbrace{a - b}_{>0} + c > c$

$\therefore \quad (q,s) \in \pm (0,1)$

Así, $\gamma = \pm Id$ y $f = g$.

Caso 2 $a = c$. Lema $\Rightarrow$ f representa al menos 4 veces a.

$f \sim g \Rightarrow$ lo mismo vale para g. Lema $\Rightarrow$ $a = c'$.

Luego $0 \le b \le a$, $0 \le b' \le a$ y $D = b^2 - 4a^2 = b'^2 - 4a^2$

$\Rightarrow b = \pm b' \Rightarrow b = b'$ pues ambos son ≥ 0.

Ej: 1) $C(-4) = \{[x^2+y^2]\}$

$f = ax^2+bxy+cy^2 \Rightarrow a \leq \sqrt{\frac{4}{3}} \Rightarrow a \in \{0,1\}$.

$a=0 \Rightarrow b=0 \Rightarrow D=0 \rightarrow \leftarrow$

$a=1 \Rightarrow b \in \{-1,0,1\}$ Pero $-4 = b^2-4c \Rightarrow b$ par.

Luego $b=0$. Así, $-4 = -4c \Rightarrow c=1$.

$\therefore f = x^2+y^2$

2) $C(-20) = \{[x+5y^2], [2x^2+2xy+3y^2]\}$

$a \leq \sqrt{\frac{20}{3}} = 2,581\ldots \Rightarrow a \in \{1,2\}$

$\underline{a=1} \Rightarrow b=0$ como antes. Luego

$-20 = -4c \Rightarrow c=5, \therefore f = x^2+5y^2$.

$\underline{a=2}$ $-20 = b^2-8c \Rightarrow b$ par

~~$\Rightarrow b \in \{0,\pm 2\}$~~ $\Rightarrow b \in \{-2,0,2\}$.

$b=-2$ no puede ser pues $|b| = a$ en tal caso $\Rightarrow b \geq 0$.

$b=0$ lleva a $-20 = -8c \Rightarrow c \notin \mathbb{Z} \rightarrow \leftarrow$

$\therefore b=2$ y $-20 = 2^2-8c \Rightarrow c=3$.

$\Rightarrow f = 2x^2+2xy+3y^2$

Ley de composición (Dirichlet)

Sean $f(x,y) = ax^2 + bxy + cy^2$

$g(x,y) = a'x^2 + b'xy + c'y^2$

primitivas, def > 0. Suponemos que $D = \text{disc } f = \text{disc } g$ y

$\text{mcd}\left(a, a', \frac{b+b'}{2}\right) = 1$.

Definimos $f * g(x,y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'} y^2$,

donde B es un entero que satisface

$$B \equiv b \mod 2a$$
$$B \equiv b' \mod 2a'$$
$$B^2 \equiv D \mod 4aa'$$

Teorema $D < 0$; $D \equiv 0, 1 \mod 4$. La operación $*$ induce una ley de grupo abeliano en $C(D)$. El elemento identidad es la clase de

$$x^2 - \frac{D}{4} y^2 \quad \text{si } D \equiv 0 \mod 4$$

$$x^2 + xy + \left(\frac{1-D}{4}\right) \cdot y^2 \quad \text{si } D \equiv 1 \mod 4$$

Además, $[ax^2 + bxy + cy^2]^{-1} = [ax^2 - bxy + cy^2]$