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

Problemas con esta definición

i) Requiere $\mathrm{mcd}\left(a, a', \frac{b+b'}{2}\right) = 1$ $\quad (*)$

Veremos que, dadas dos clases en $C(D)$, siempre se pueden encontrar representantes que cumplan $(*)$

ii) ¿ Por qué existe B ?

iii) B no es único, luego $f*g$ depende de la elección de B, no solo de f, g.

La clase de $f*g$ no depende de B. Esto no lo demostraremos hoy, quedará para la charla "Relación con formas cuadráticas, finitud del número de clases"

iv) $f*g$ induce una ley de grupo abeliano en $C(D)$

ídem

v) ¿ $f*g \in C(D)$?

Existencia de B bajo la hipótesis $\mathrm{mcd}\left(a, a', \frac{b+b'}{2}\right) = 1$.

De hecho, mostraremos que B es único mod 2 a a'.

Lema Sean $p_1, q_1, \dots, p_r, q_r, m \in \mathbb{Z}$ con

$\mathrm{mcd}(p_1, \dots, p_r, m) = 1$ Entonces las congruencias

$p_i x \equiv q_i \bmod m \quad i = 1, \dots, r$

tienen solución única mod m $\iff p_i q_j \equiv p_j q_i \bmod m \ \forall i, j$.

Dem no usar el teo chino

Existencia:

Sean $\alpha, \alpha_1, \dots, \alpha_r \in \mathbb{Z}$ con $\alpha m + \alpha_1 p_1 + \dots + \alpha_r p_r = 1$

$\Rightarrow \forall i, \quad \alpha m q_i + \alpha_1 p_1 q_i + \alpha_2 p_2 q_i + \dots + \alpha_r p_r q_i = q_i$

$\Rightarrow \sum_{j=1}^{r} \alpha_j p_j q_i \equiv q_i \bmod m$

$\equiv q_j p_i$

$\therefore p_i \left(\sum_{j=1}^{r} \alpha_j q_j \right) \equiv q_i \bmod m, \ \forall i$

$\Rightarrow x := \sum_{j=1}^{r} \alpha_j q_j$ es una solución

Unicidad: argumento estándar ∎

i') Afirmación los congruencias que satisface B son equivalentes a

$$a' \cdot B \equiv a'b \mod 2aa'$$
$$a \cdot B \equiv ab' \mod 2aa'$$
$$\left(\frac{b+b'}{2}\right) \cdot B \equiv \frac{bb'+D}{2} \mod 2aa'$$

(sale de manipulaciones simples). Luego el lema asegura que $\exists!$ B mod $2aa'$ que cumple las congruencias.

(aquí usamos (*)).

Justifiquemos i)

Lema 1 f representa propiamente a $m \in \mathbb{Z}$ si y solo si

$$f \sim mx^2 + Bxy + Cy^2, \quad B, C \in \mathbb{Z}.$$

$\Leftarrow$] claro tomando $(x,y) = (1,0)$

$\Rightarrow$] si $m = f(u,v)$ con $\mathrm{mcd}(u,v) = 1$,

elegimos $\alpha, \beta \in \mathbb{Z}$ con $u\alpha - v\beta = 1$. Sea $\gamma = \begin{pmatrix} u & \beta \\ v & \alpha \end{pmatrix}$

tenemos $\gamma \cdot f(x,y) = f(ux+\beta y, vx+\alpha y)$

$$= \underbrace{f(u,v)}_{m} x^2 + \tilde{b}xy + \tilde{c}y^2$$

$f = ax^2 + bxy + cy^2$

~~Lema 2 Dado $f(x,y)$ primitiva y $m \in \mathbb{Z}$, entonces f representa al menos un entero primo con m~~

Lema 2 Dado $f(x,y)$ primitiva y $k \in \mathbb{Z}-\{0\}$ existe $m \in \mathbb{Z}$, propiamente representado por f, tal que $\text{mcd}(m,k)=1$

Dem: • Si $|k|=1$, tenemos $a_1 = f(1,0)$ es propiamente representado y $(a_1, \pm 1) = 1$.

• Si k es primo, afirmamos que al menos uno entre $f(1,0) = a$, $f(1,1) = a+b+c$, $f(0,1) = c$ no es divisible por k.

De lo contrario $k \mid f(1,1) - f(1,0) - f(0,1) = b$ y f no es primitiva.

• Si $|k| \geq 2$, factorizamos $k = \pm \prod_{i=1}^{r} p_i^{e_i}$.

Por el caso anterior, $\forall i = 1, \dots, r \;\; \exists (u_i, v_i) \in \mathbb{Z}^2$ con

$\text{mcd}(u_i, v_i) = 1$ y $p_i \nmid f(u_i, v_i)$

Por el teo. chino del resto $\exists (u_0, v_0) \in \mathbb{Z}^2$ con

$u_0 \equiv u_i \bmod p_i$, $v_0 \equiv v_i \bmod p_i$, $\forall i = 1, \dots, r$.

Pero entonces $\forall i$ se cumple $f(u_0, v_0) \equiv f(u_i, v_i) \not\equiv 0 \bmod p_i$

Luego $m_0 := f(u_0, v_0)$ cumple $\text{mcd}(m_0, k) = 1$.

Sea $d := \text{mcd}(u_0, v_0)$. Tenemos que $m := \frac{m_0}{d^2} = f\left(\frac{u_0}{d}, \frac{v_0}{d}\right)$ cumple los requisitos ■

Dem de (i)

Sean $f, g \in C(D)$; $f = ax^2 + bxy + cy^2$

Lema 2 $\Rightarrow$ $\exists\, a' \in \mathbb{Z}$, con $(a, a') = 1$, tal que a' es propiamente representado por g.

Lema 1 $\Rightarrow$ $g \sim a'x^2 + b'xy + c'y^2$

como $\mathrm{mcd}\left(a, a', \frac{b+b'}{2}\right) \mid \mathrm{mcd}(a, a') = 1$, esto justifica (i). ∎

Justificación de +v)

Lema 3 dados $f, g \in C(D)$, existen

$$\alpha_1(x,y,z,w) = a_1xz + b_1xw + c_1yz + d_1yw \in \mathbb{Z}[x,y,z,w]$$

$$\alpha_2(x,y,z,w) = a_2xz + b_2xw + c_2yz + d_2yw$$

tales que $f(x,y)\cdot g(z,w) = f*g\left(\alpha_1(x,y,z,w), \alpha_2(x,y,z,w)\right)$

Dem: en los notas definitivos ∎

+v) $\mathrm{disc}\, f*g = D$ sigue del cálculo directo.

$f*g$ primitiva. Si no, $\exists\, p$ primo que divide a todos los coeficientes de $f*g$.

Luego $p \mid$ todos los enteros representados por $f * g$.

Lema 3 $\Rightarrow$ $p \mid$ todos los productos de la forma $f(u,v)\,g(s,t)$ con $u,v,s,t \in \mathbb{Z}$.

Pero esto contradice Lema 2. ∎

Dem del teorema

Sea $$I(x,y) = \begin{cases} x^2 - \frac{D}{4} y^2 & \text{si } D \equiv 0 \bmod 4 \\ x^2 + xy + \left(\frac{1-D}{4}\right) y^2 & \text{si } D \equiv 1 \bmod 4. \end{cases}$$

Veamos que es el neutro.

Sea $f(x,y) = ax^2 + bxy + cy^2$. Claramente (*) se cumple.

B puede tomarse $= b$: $\quad a' = 1$

p.d. $b \equiv b' \bmod 2$ (0)

$b^2 \equiv D \bmod 4a$ (⁂)

(⁂) es obvio de la def. de D

(0) $D \equiv 0\ (4) \Rightarrow b' = 0$. Pero $D = b^2 - 4ac \Rightarrow b$ par.

$D \equiv 1\ (4) \Rightarrow b' = 1$. " " $\Rightarrow b$ impar.

$\therefore$ $f * I(x,y) = ax^2 + bxy + \underbrace{\frac{b^2 - D}{4a}}_{c} y^2 = f$

Cálculo de f^{-1}.

Sea $f' = ax^2 - bxy + cy^2$.

P. d. $[f] * [f'] = [I]$.

$$g := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot f' = cx^2 + bxy + ay^2$$

$$\Rightarrow \gcd\left(a, c, \frac{b+b}{2}\right) = 1$$

$B = b$ cumple las congruencias, como antes.

$$\Rightarrow f * g(x,y) = acx^2 + bxy + \frac{b^2 - D}{4ac} y^2$$

$$= acx^2 + bxy + y^2 .$$

$$\gamma = \begin{pmatrix} 0 & -1 \\ 1 & s \end{pmatrix} \in SL_2(\mathbb{Z})$$

$$\Rightarrow \gamma \cdot f * g(x,y) = x^2 + (2s - b)xy + \underbrace{(ac - bs + s^2)}_{f*g(-1,s)} y^2$$

Si $D \equiv 0 \bmod 4 \Rightarrow b$ es par $\quad s := \frac{b}{2}$

$$\Rightarrow \gamma \cdot f * g(x,y) = x^2 - \frac{D}{4} y^2$$

Si $D \equiv 1 \bmod 4 \Rightarrow b$ es impar, $\quad s := \frac{b+1}{2}$

$$\Rightarrow \gamma \cdot f * g(x,y) = x^2 + xy + \left(\frac{1-D}{4}\right) y^2$$

■

Sobre la estructura de $C(D)$

Prop: $f = ax^2 + bxy + cy^2 \in C(D)$, reducida, tiene orden $\leq 2 \iff b = 0 \vee a = b \vee a = c$

Dem: f tiene orden $\leq 2 \iff [f] = [f]^{-1}$

Sea $g = ax^2 - bxy + cy^2$, $[f]^{-1} = [g]$

$\therefore$ f tiene orden $\leq 2 \iff f \sim g$

Caso 1 $|b| < a < c$:

g es reducida, luego $f \sim g \iff f = g \iff b = 0$.

Caso 2 $a = b \vee a = c$

$a = b \Rightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot g(x,y) = a(x+y)^2 - ay(x+y) + cy^2$

$f = ax^2 + axy + cy^2$

$g = ax^2 - axy + cy^2$

$= ax^2 + axy + cy^2$

$= f(x,y)$

$a = c \Rightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot g = f$ ∎

~~Ej: $C(-56) = \{[x^2 + 14y^2], [2x^2 + 7y^2], [3x^2 - 2xy + 5y^2], [3x^2 + 2xy + 5y^2]\}$~~

Ej: $C(-56) = \{[x^2 + 14y^2], [2x^2 + 7y^2], [3x^2 - 2xy + 5y^2], [3x^2 + 2xy + 5y^2]\}$

Hay solo 1 elemento de orden 2, luego $C(-56) \simeq \mathbb{Z}/4\mathbb{Z}$

$D = -56 = b^2 - 4ac \Rightarrow -2^3 \cdot 7 \Rightarrow$ b par

$a \leq \sqrt{\frac{56}{3}} = 4.3204\ldots \Rightarrow a \in \{1,2,3,4\}$.

$a=1 \Rightarrow b=0 \Rightarrow c = \frac{+56}{4} = 14 \Rightarrow \boxed{x^2 + 14y^2}$

$a=2 \Rightarrow b \in \{-2, 0, 2\}$.

$b=0 \Rightarrow c = \frac{56}{8} = 7 \Rightarrow \boxed{2x^2 + 7y^2}$

$b=2 \Rightarrow -2^3 \cdot 7 = 2^2 - 4 \cdot 2^2 c \Rightarrow -14 = 1 - 4c$

$\Rightarrow 4c = 15 \rightarrow \lightning$

~~$\Rightarrow 2x^2 + 2xy + 15y^2$~~

$a=3 \Rightarrow b \in \{-2, 0, 2\}$

$b = \pm 2 \Rightarrow -2^3 \cdot 7 = 2^2 - 4 \cdot 3 \cdot c \Rightarrow -2 \cdot 7 = 1 - 3c$

$\Rightarrow 3c = 15 \Rightarrow c = 5$

$\boxed{3x^2 - 2xy + 5y^2}$

$\boxed{3x^2 + 2xy + 5y^2}$

$b=0 \Rightarrow -2^3 \cdot 7 = -4 \cdot 3 \cdot c \Rightarrow -14 = -3 \cdot c \rightarrow \lightning$

$a=4 \Rightarrow b \in \{-2, 0, 2, 4\}$.

$b = \pm 2 \Rightarrow -2^3 \cdot 7 = 2^2 - 4^2 c \Rightarrow -14 = 1 - 4c \Rightarrow 4c = 15 \rightarrow \lightning$.

$b=0 \Rightarrow -2^3 \cdot 7 = -2^4 c \Rightarrow +7 = 2c \rightarrow \lightning$.

$b=4 \Rightarrow -2^3 \cdot 7 = 2^4 - 2^4 c \rightarrow \lightning$.

Número de clases

$$h(D) := \#\, C(D)$$

Teorema (Bolker, Heegner, Stark)

$D < 0$, $D \equiv 0, 1 \bmod 4$.

Entonces $h(D) = 1 \iff D \in \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}$

Hoy probaremos el caso particular en que D es par.

Teorema (Landau) $\quad n > 0 \Rightarrow \left(h(-4n) = 1 \iff n \in \{1, 2, 3, 4, 7\}\right)$

Dem: $x^2 + ny^2 \in C(-4n)$ y es reducida

$\Leftarrow$] se verifica mostrando que es la única, usando la cota $a \leq \sqrt{\frac{4n}{3}}$.

$\Rightarrow$] veremos que cuando n no está en el conjunto indicado, podemos fabricar otra forma reducida.

Caso 1 n no es una potencia de un primo:

$$n = a \cdot c, \quad a, c > 1, \quad \mathrm{mcd}(a, c) = 1, \quad a < c$$

Entonces $ax^2 + cy^2 \in C(-4n)$ y es reducida

$\Rightarrow h(-4ac) \geq 2$.

Caso 2 $n = 8$. Calcular $C(-32) \simeq \mathbb{Z}/2\mathbb{Z}$

Caso 3 $n = 2^r$; $r \geq 4$.

$\Rightarrow 4x^2 + 4xy + (2^{r-2}+1)y^2$

es primitiva, tiene discriminante $4^2 - 4 \cdot 4 \cdot (2^{r-2}+1) = -4 \cdot 2^r = -4n$

y es reducida porque $4 < 2^{r-2} + 1$

Caso 3 ($n = p^r$, p primo ≥ 3 y $n+1$ no es potencia de primo.)

$\Rightarrow n+1 = a \cdot c$; $2 \leq a < c$, $\mathrm{mcd}(a,c) = 1$.

$ax^2 + 2xy + cy^2$ es reducida de discriminante primitiva,

$2^2 - 4ac = 4 - 4(n+1) = -4n$.

Caso 4 $n = p^r$; $n+1 = 2^s$

Si $s \geq 6$; $8x^2 + 6xy + (2^{s-3}+1)y^2$ es reducida

pues $6 < 2^{s-3} + 1$, primitiva de discriminante

$6^2 - 4 \cdot 8 \cdot (2^{s-3}+1) = 36 - 4 \cdot 2^s - 32 = 4 - 4(n+1) = -4n$

Si $s = 5 \Rightarrow n = 31$. Podemos ver que $h(-4 \cdot 31) = 3$ a mano

Si $s = 4 \Rightarrow n = 15$ no es potencia de primo.

Si $s = 3 \Rightarrow n = 7$ O.K.

Si $s = 2 \Rightarrow n = 3$ O.K.

Si $s = 1 \Rightarrow n = 1$ O.K.