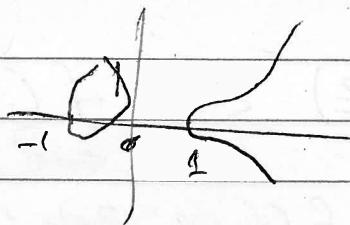


$$E: y^2 = x(x^2 - 1)$$

de, es:

$$g(x, y) \in K[x, y]$$



$$g(x, y) = y^2 - x^3 \quad \text{induce función } e \in E$$

$$g(0, 0) = 0$$

$$g(x, y) = y^2 - x(x^2 - 1) \quad \text{induce la función constante } 0.$$

¿Cuándo g_1 y g_2 inducen la misma función?

$$\text{Por todo } P \in E \quad (g_1 - g_2)(P) = 0 \Leftrightarrow g_1 - g_2 = y^2 - x(x^2 - 1)h(x) = 0$$

$$\Leftrightarrow g_1 - g_2 = (y^2 - x(x^2 - 1))h(x) = 0$$

Funciones polinómicas en la curva elíptica.

$$\text{Tomemos } x(-1, 0) = -1$$

$$x(0, 0) = 0$$

$$x(1, 0) = 1$$

o vale cero en $(0, 0)$, y

nada más.

$$\mathbb{P}^2: ZY^2 = X(X^2 - Z^2)$$

$$x = \frac{X}{Z} \quad y = \frac{Y}{Z}$$

$$(-1, 0)$$

función racional en E :

Es un cociente de dos polinomios $\in K[X, Y, Z]$ homogéneos, y del mismo grado.

$H_1(\mathbb{Q}, 1, 0)$

$$\phi = f(x, y, z) \iff f(\lambda x, \lambda y, \lambda z) = 0$$

$$f = x y^2 \quad f(x, y, z)$$

$$f(\lambda x, \lambda y, \lambda z) = \lambda^3 f(x, y, z)$$

$$\frac{f}{g}(x, y, z) = \frac{f(\lambda x, \lambda y, \lambda z)}{g(\lambda x, \lambda y, \lambda z)}$$

$$E: y^2 = x(x^2 - 1)$$

es decir $(-1, 0), (0, 0), (1, 0)$.

$$\theta = (9, 16)$$

$$\frac{y}{z} \quad y(P_\infty) = \infty$$

$$f(x) = 2$$

$$\frac{1}{f(x)} = \frac{1}{2}$$

$$\frac{1}{y} = \frac{z}{y} = \phi$$

Los ceros de $\frac{1}{f}$ se llaman polos de f

Decimos que es racional si $f: E \rightarrow K \cup \{\infty\} = \mathbb{P}^1$

Siempre que $P \in E$ y $f(P) \neq \infty$

si $\exists F, G$ homogéneos de grado igual

$$\text{t.q. } f = \frac{F}{G} \quad \text{y } G(P) \neq 0$$

Siempre que $G(Q) \neq 0$.

$$\forall Q \in E.$$

$$zy^2 = x(x^2 - z^2)$$

2015-V-27

$$f: E \rightarrow \mathbb{P}^1$$

$$(x, y) \mapsto x$$

$$P_\infty \mapsto \infty$$

$$(x, y, z) \mapsto (x:1)$$

$$(0:1:0) \mapsto (1:0)$$

$$\frac{x}{z}$$

$$f: \frac{z}{x} \quad (0:1:0)$$

$$f: E \rightarrow \infty$$

$$P_\infty \mapsto \emptyset$$

$$(x, y) \mapsto 1/x \quad x \neq 0$$

$$(0, 0) \mapsto \infty$$

$$(0, 0, 1)$$

Es recíproco si es un cociente.

$$\frac{z}{x} = \frac{zy^2}{xy^2} = \frac{x(x^2 - z^2)}{xy^2}$$

$$\frac{x^2 - z^2}{y^2} = \emptyset \quad (0, 1, 0) = P_\infty$$

$$y^2 = x(x^2 - 1)$$

función: x

Piensa en todas las funciones polinómicas en E tales que

$$t.g. \quad f(0, 0) = 0$$

$$A = K[x, y] / (y^2 - x(x^2 - 1))$$

Anillo de fracciones

moviendo es igual módulo

la ecuación de la curva

$$\mathfrak{m}_P = \{f \in A \mid f(P) = 0\}$$

es ideal de A

Lo muevamos en un anillo es

una unidad

$$f(P) = 0, g(P) = 0$$

$$(f+g)(P) = f(P) + g(P) = 0$$

$$x+1 = \frac{x}{z} + 1$$

$$= \frac{x+z}{z}$$

$$\frac{1}{x+1} = \frac{z}{x+z}$$

non single zero

$$\mathcal{M}_P^2 = \{f \cdot g \mid f, g \in \mathcal{M}_P\}$$

$$= \left\{ \sum_{i=1}^n f_i \cdot g_i \mid f_i, g_i \in \mathcal{M}_P \right\}$$

$$\frac{\partial h}{\partial x} = -3x^2 + 1$$

$$\frac{\partial h}{\partial x}(0, 1) = 1$$

Si una es zero,
la otra no es.

$$\frac{\partial h}{\partial y} = 2y$$

$$\frac{\partial h}{\partial y}(0, 0) = 0$$

Si $\frac{\partial h}{\partial x} \neq 0$, y es uniformizador.

El uniformizador está en
 $\mathcal{M}_P - \mathcal{M}_P^2$.

Si $\frac{\partial h}{\partial y} \neq 0$, x es uniformizador.

x, y

$$x(0,0) = 0$$

$$y(0,0) = 0 \longrightarrow y \text{ es uniformizador}$$

$$y^2 = x^3 - x$$

$$\longrightarrow x = x^3 - y^2$$

$$= y^2 \left(-1 + \frac{x^3}{y^2} \right)$$

$$\frac{x^3}{y^2} = \frac{x^3}{x^3 - x} = \frac{x^2}{x^2 - 1} = 0$$

vale ϕ en $(0,0)$.

Expresar $x = y^2 \cdot g$ - recorda t.g. $g(P) \neq 0$

el grado es el orden del 0, o multiplicidad.

Es un cero de orden 2

X tiene un cero de orden 2 en $(0,0)$
 tiene un polo en P_∞

$$P_\infty = (0, 1, 0)$$

$\frac{X}{Z}$ polos son ceros de $\frac{Z}{Y}$

$$u = \frac{X}{Y} \quad \frac{Z}{X} = \frac{\frac{Z}{Y}}{\frac{X}{Y}} = \frac{v}{u}$$

$$\frac{ZY^2}{Y^3} = \frac{X^3 - XZ^2}{Y^3} \sim v = u^3 - uv^2$$

$$P_\infty = (0, 0)$$

$$\frac{Z}{X} = \frac{ZY^2}{XY^2} = \frac{X^3 - XZ^2}{X^2Y^2} = \frac{X^2 - Z^2}{Y^2} = u^2 - v^2$$

$$h = u^3 - uv^2 - v$$

$$\frac{\partial h}{\partial u} = 3u^2 - v^2 \quad \frac{\partial h}{\partial u}(0,0) = 0 \quad \text{¡o } u \text{ es un factor de } h$$

$$\frac{\partial h}{\partial v} = 2uv - 1 \quad \frac{\partial h}{\partial v}(0,0) = -1$$

$$u^2 - v^2 = u^2 \left(1 - \frac{v^2}{u^2}\right)$$

el uniformizador se encuentra
 por 2 funciones que no se
 anulan en $(0,0)$

$$\underbrace{\frac{v^2}{u^2}}_{\substack{\text{¡que vale 0 en} \\ = 1}}$$

~~Si~~ Orden = 2

Las funciones generadas en M_p que no están en
 $M_p^{\geq 2}$ son uniformizadoras

Thm.

si f es función racional en E tiene el mismo número de ceros que polos, (contando multiplicidades)

Ejemplo:

x cero doble en $(0,0)$
 polo doble en P_∞

y ceros simples en $(-1,0), (0,0), (1,0)$
 y un polo triple en P_∞

Divisores:

Una suma

$$\text{Div}(E) := \{n_1[P_1] + \dots + n_t[P_t] : n_i \in \mathbb{Z}, t \in \mathbb{N}, P_i \in E\}$$

Ejemplo

$$3[(0,0)] \in \text{Div}(E)$$

$$4[(-1,0)] - 2[(0,0)] + 3[(1,0)]$$

función x

El divisor de una función racional

$$\text{Div}(x) = 2[(0,0)] - 2[P_\infty]$$

$$\text{Div}(y) = [(-1,0)] + [(0,0)] + [(1,0)] - 3[P_\infty]$$

$$\text{Div}\left(\frac{1}{x}\right) = 2[P_\infty] - 2[(0,0)]$$

Prop

$$\text{Div}(f \cdot g) = \text{Div}(f) + \text{Div}(g)$$

$$\text{Div}(\lambda f) = \text{Div}(f), \lambda \in K \setminus \{0\} \quad (f \cdot g)(P) = 0$$

$$\text{Div}\left(\frac{1}{f}\right) = -\text{Div}(f)$$

$$\Leftrightarrow f(P) \cdot g(P) = 0$$

$$\Leftrightarrow f(P) = 0, \text{ o } g(P) = 0$$

El grado de un divisor es la suma de sus coeficientes.
 $\deg(\sum n_i [P_i]) := \sum n_i$

El thm dice, si f es racional $\deg(\text{Div}(f)) = 0$

Los divisores que provienen de funciones se llaman Principales
 $\text{PDN}(E) \quad \text{Div}_f(E)$

El soporte de un divisor es el conjunto de puntos con coeficiente no cero

¿Cuándo un divisor viene de una función?

Se necesita que $\deg(D) = 0$. $\text{Div}^0(E) := \{D \in \text{Div}(E) \mid \deg D = 0\}$
 $\text{Div}^0(E) := \{D \in \text{Div}(E) \mid \deg(D) = 0\}$

$$D = [P] - [Q] \quad [P+Q]$$

$$P, Q \in E$$

Thm: $D = \sum n_i P_i$ es principal si y solo si

$$\sum n_i D_i = \mathcal{O}$$

$$\deg(D) = 0$$

$D = [(1,0)] - [P_\infty]$ Como $(1,0) - P_\infty = (1,0)$,
D no es principal

$$D = 2[(0,0)] - 2[P_\infty] = \mathcal{O}$$

"

$D_N(\infty)$

La ley de grupo en la d.N. es p.m. a la ley de grupo en la am.

~~$D_1 \sim D_2$~~

Dado

$D_1 \sim D_2$ (equivalencia lineal)

Si $D_1 \sim D_2$ es principal

Que la diferencia de los potenciales de los ceros, que se multiplican

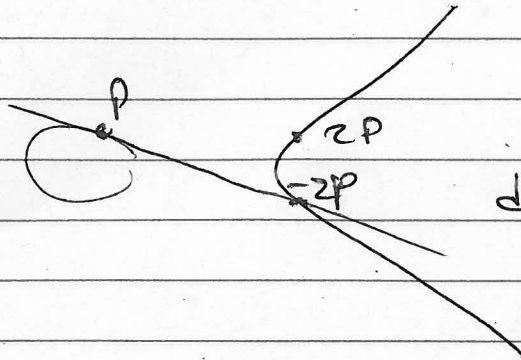
$$\frac{D_N(E)}{(P_N(E))} \cong (E, +)$$

$$\mathbb{Z} \quad m\mathbb{Z}$$

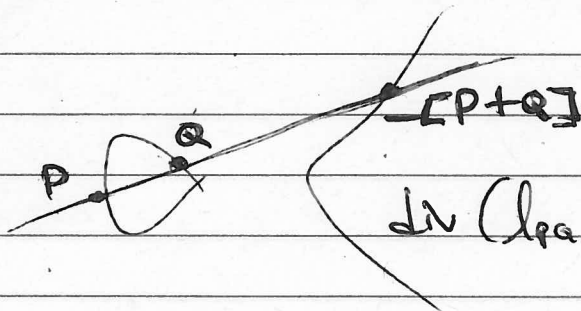
$$a \equiv b(m)$$

$$\text{for } m \mid a-b$$

2015-D-27



$$dN(l_{pp}) = 2[P] + [-2P] - 3[P_\infty]$$



$$dN(l_{pq}) = [P] + [Q] + [- (P+Q)] - 3[P_\infty]$$