Luis Ramírez

El conjunto $S = \{ x + y\sqrt[3]{3} + z\sqrt[3]{9} ; x, y, t \in \mathbb{Q} \}$

#1 es un anillo con respecto a la adición y la multiplicación en $\mathbb{R}$

A01638402

Cerradura bajo la suma.

$$x_1 + y_1\sqrt[3]{3} + z_1\sqrt[3]{9} + x_2 + y_2\sqrt[3]{3} + z_2\sqrt[3]{9} =$$

$$(x_1 + x_2) + (y_1 + y_2)\sqrt[3]{3} + (z_1 + z_2)\sqrt[3]{9}$$

$(x_1 + x_2) \in \mathbb{Q}$, $(y_1 + y_2) \in \mathbb{Q}$, $(z_1 + z_2) \in \mathbb{Q}$

Cerradura al producto

$$(x_1 + y_1\sqrt[3]{3} + z_1\sqrt[3]{9}) * (x_2 + y_2\sqrt[3]{3} + z_2\sqrt[3]{9})$$

$$= (x_1x_2 + x_1y_2\sqrt[3]{3} + x_1z_2\sqrt[3]{9})$$

$$+ (\sqrt[3]{3}\, y_1x_2 + y_1y_2\sqrt[3]{9} + y_1z_2\sqrt[3]{27})$$

$$+ (x_2z_1\sqrt[3]{9} + z_1x_2\sqrt[3]{27} + z_1z_2\sqrt[3]{81})$$

$$= x_1x_2 + x_1y_2\sqrt[3]{3} + x_1z_2\sqrt[3]{9}$$

$$+ 3y_1z_2 + x_2y_1\sqrt[3]{3} + y_1y_2\sqrt[3]{9}$$

$$+ 3x_2z_1 + 3z_1z_2\sqrt[3]{3} + x_2z_1\sqrt[3]{9}$$

$$= (x_1x_2 + 3y_1z_2 + 3x_2z_1) + (x_1y_2 + x_2y_1 + 3z_1z_2)\sqrt[3]{3}$$

$$+ (x_1z_2 + y_1y_2 + x_2z_1)\sqrt[3]{9} \notin S$$

Elemento identidad.

$$x_1 + y_1 \sqrt[3]{3} + z_1 \sqrt[3]{9} + e = x_1 + y_1 \sqrt[3]{3} + z_1 \sqrt[3]{9}$$

$$\therefore \quad e = 0$$

Inverso.

$$S = (x_1 + y_1 \sqrt[3]{3} + z_1 \sqrt[3]{9})$$

$$S^{-1} = (-x_1 - y_1 \sqrt[3]{3} - z_1 \sqrt[3]{9})$$

$$S^{-1} \text{ f } S$$

$$SS^{-1} = 0 = e$$

Dada $y^2 = x^3 + x + 1$ $\quad P = (3, 10)$

$y^2 - x^3 - x - 1 = 0$

a) La recta tangente a la curva.

$$\nabla f (P)(x - x_0)(y - y_0) = 0$$

$$\nabla f = \left\langle \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y} \right\rangle = \langle -3x_p^2 - 1, 2y_p \rangle$$

$$= (-3x_p^2 - 1)(x - 3) + 2y_p (y - 10) = 0$$

$$2y_p (y - 10) = -(-3x_p^2 - 1)(x - 3)$$

$$2y_p (y - 10) = (3x_p^2 + 1)(x - 3)$$

$$y - 10 = \frac{(3x_p^2 + 1)(x - 3)}{2y_p}$$

$$y = \frac{(3x_p^2 + 1)(x - 3)}{2y_p} + 10$$

$$y = \frac{29(x - 3)}{20} + 10$$

$$y = \frac{29(x - 3)}{20} + 10$$

$$y = \frac{7}{5}x + \frac{29}{5}$$

$x_3 ; y_3$

$P \oplus P$ $\quad$ $P + P$

$y^2 = x^3 + x + 1$ $\qquad$ $y = \frac{7}{5}x + \frac{29}{5}$

$y = \sqrt{x^3 + x + 1}$

$\left(y = \frac{7}{5}\left(-\frac{101}{25}\right) + \frac{29}{5}\right)$

$\frac{7}{5}x + \frac{29}{5} = \sqrt{x^3 + x + 1}$ $\qquad$ $y_3 = \frac{15}{125}$

$\left(\frac{7}{5}x + \frac{29}{5}\right)^2 = x^3 + x + 1$

$\frac{49}{25}x^2 + \frac{72}{5}x + \frac{841}{25} = x^3 + x + 1$ $\qquad$ $\frac{49}{25} = x_3 + 6$

$x_3 = \frac{49}{25} - 6$

$x^3 - \frac{49}{25}x^2 - \frac{67}{5}x - \frac{316}{25} = 0$ $\qquad$ $x_3 =$

$(x - \quad)^2 (x - x_3) = 0$

$(x^2 - 6x + 9)(x - x_3) = 0$

$x^3 - x^2 x_3 - 6x^2 + 6x x_3 + 9x - 9x_3 = 0$

$x^3 + (-x_3 - 6)x^2 + (6x_3 + 9)x - 9x_3 = 0$

$x_3 = -\frac{101}{25}$ $\qquad$ $y_3 = -\frac{116}{125}$

c) $\mathcal{O}10P$? A partir de $P \oplus P = 2P$:

$2P \oplus 2P = 4P$

$4P \oplus 4P = 8P$

$8P \oplus 2P = 10P$

3. Considere $y^2 = x^3 - 5x + 13$ ($\in F_{37}$)

$P = (6, 3)$, $Q(9, 10)$, $2P(35, 11)$, $3P(34, 25)$

$P \oplus Q = (11, 10)$

Encontre $R = 3P \oplus 4Q$ em F_{37}

$2Q = Q \oplus Q$

$x_3 = \frac{3x^2 - 5}{2y_1} - 2x_1 = \frac{3(81) - 5}{2(10)} + 18 \quad \frac{3(7) - 5}{20} - 18$

$= \left(\frac{16}{20}\right)^2 - 18 = \left(\frac{4}{5}\right)^2 + 19 = 11 + 19 = 30 \bmod 37$

$y_3 = \left(\frac{3x^2 - 5}{2y}\right)(x_1 - x_3) - y_1$

$= 23(16) - 10$

$= 35 - 10 = 25 \bmod 37$ $\qquad 2Q = (30, 25)$

$2Q = (30, 25)$

$2Q \oplus 2Q$

$x_3 = 28^2 - 60 \mod 37 = 7 + 111 = 21$

$y_3 = \left(\frac{3x_1^2 + A}{2y_1}\right)(x_1 - x_3) - y_1$

$= \left(\frac{3(30) - 5}{2(25)}\right)(30 - 21) - 25$

$= (28)(30 - 21) - 25$

$= 28 \cdot 9 - 25 = 5$ $\quad 4Q = (21, 5)$

$3P = (34, 25) \quad 4Q = (21, 5)$

$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$

$y_3 = \left(\frac{5 - 25}{21 - 34}\right)(34 - x_3) - y_1$

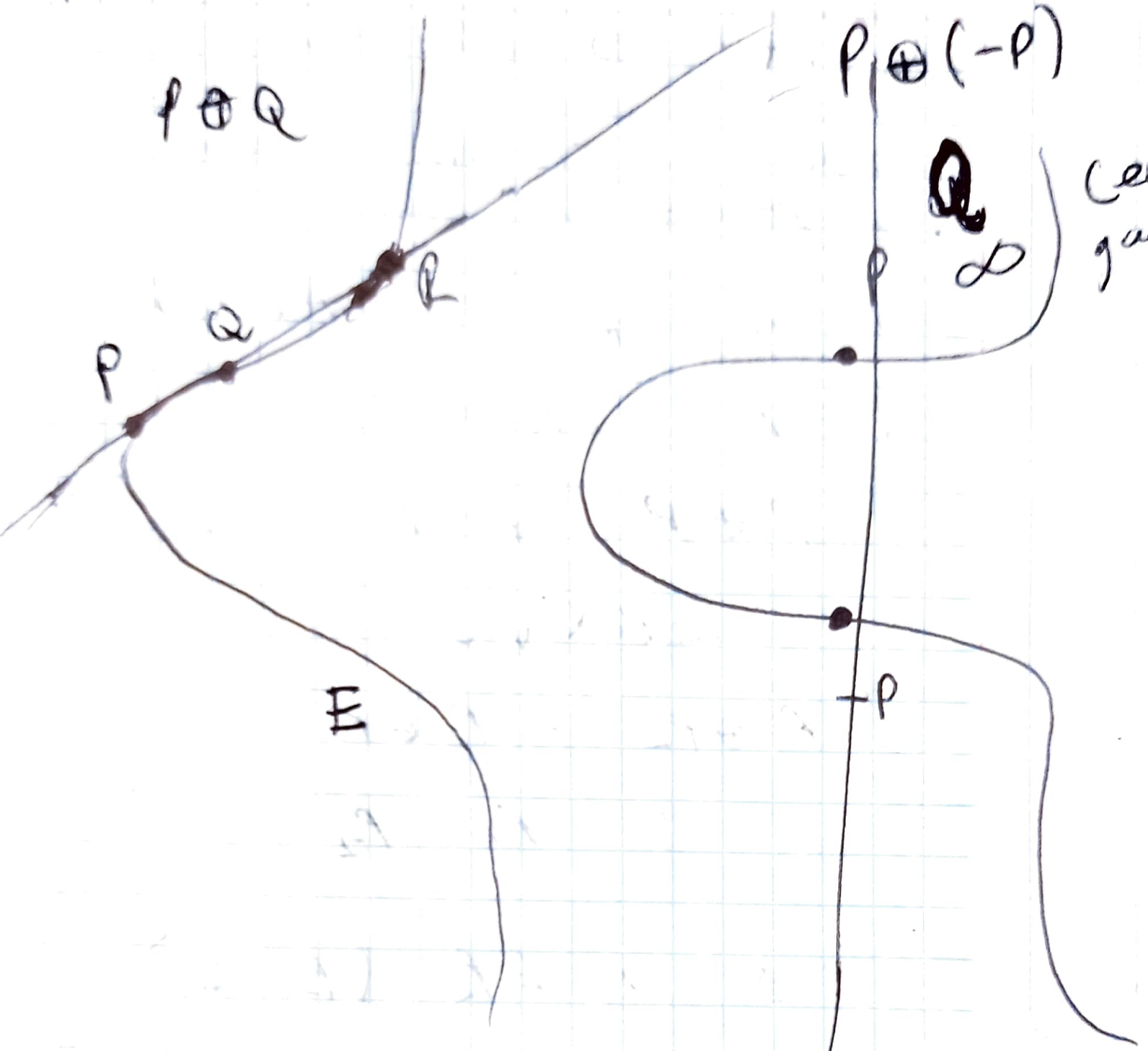
$y_3 = 30 \cdot (34 - 31) - 25$

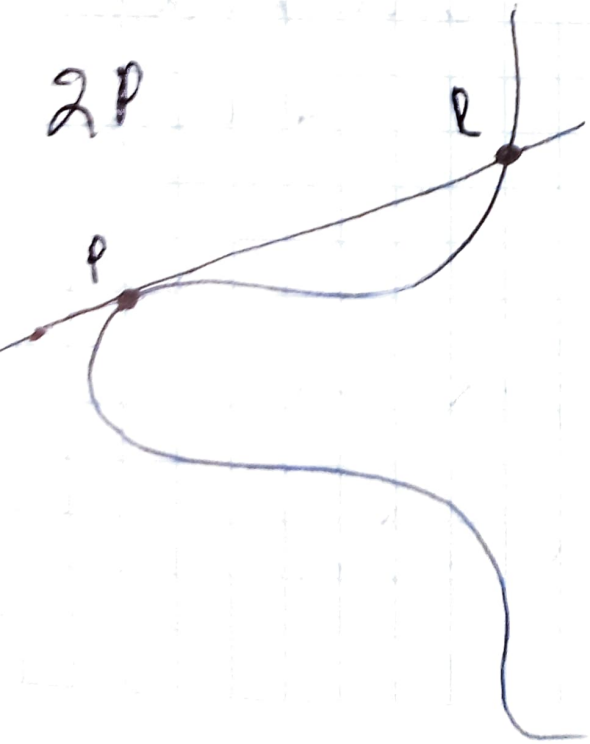
$= 30 \cdot 3 - 29$

$= 16 - 25 = -9 = 28$

$3P + 4Q = (31, 29)$

4





$(C, +)$ es abeliano

donde C es una curva elíptica de la forma $y^2 = x^3 + Ax + B$

$P_1 = P$, $P_2 = P$

$P \oplus P = P \oplus P$

Reflexiva

$P_1 \oplus P_2 = P_2 \oplus P_1$

Si $P_1 = P_2$

Si $P_1 \neq P_2$ $(P_2 = Q)$

$P \oplus Q = Q \oplus P$ donde $P = (x_1, y_1)$

$Q = (x_2, y_2)$

$P \oplus Q = (x_3, y_3)$

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

$$\frac{y_2 - y_1}{x_2 - y_1} = \frac{y_1 - y_2}{x_1 - x_2}$$, $x_1, x_2, y_1, y_2 \in \mathbb{R}$

$\therefore$ Es conmutativo.

$$-x_1 - x_2 = -x_2 - x_1 \quad x_1, x_2 \in \mathbb{R}$$

$\therefore$ Es conmutativo

~~$(x_2 - x_3) = y_1$~~

$$\left(\frac{y_2 - y_1}{x_2 - x_1}\right) = \lambda \quad , \quad (x_1 - x_3) = \ell$$

$$\lambda \ell = \ell \lambda \quad , \quad \lambda, \ell \in \mathbb{R}$$

$\therefore$ Es conmutativo

$\square$