La ley del grupo para curvas cúbicas (es decir, curvas algebráicas del grado 3)

Brian Harbourne

Department of Mathematics
University of Nebraska-Lincoln

Matemáticas en español: December 2, 2021

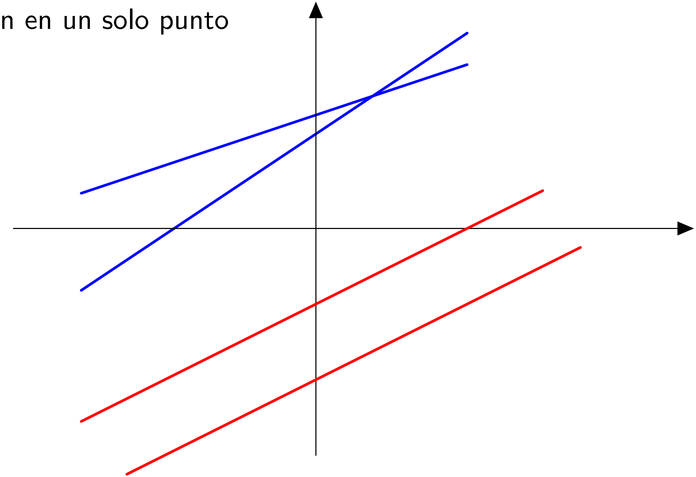
Resumen

Título: La ley del grupo para curvas cúbicas (es decir, curvas algebráicas del grado 3).

Resumen: Describiremos como una curva cúbica tiene una ley del grupo. Veremos la ley desde tres perspectivas: geométricamente, algebráicamente y topológicamente.

Curvas y líneas

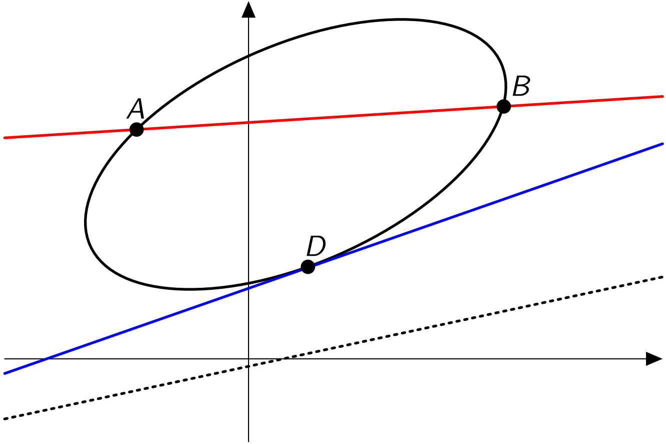
Una línea se encuentra con una curva algebráica del grado d en d puntos, contado con multiplicidad (e incluyendo puntos del infinito). Por ejemplo, líneas son curvas del grado 1, y dos líneas se encuentran en un solo punto



incluso si son paralelas (donde el punto está en el infinito).

Más curvas y líneas

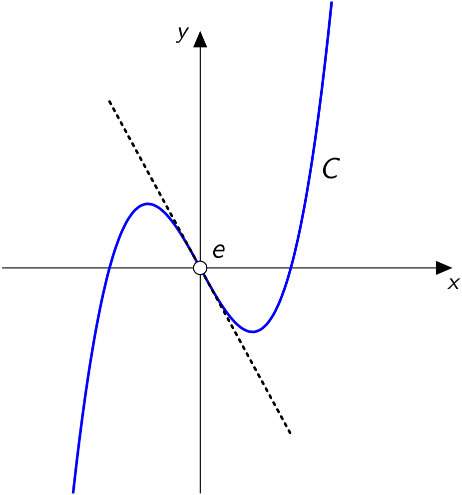
Ahora, considera las cónicas (es decir, curvas del grado 2). Cuando una línea se encuentra con una cónica, podemos tener dos puntos de multiplicidad 1, o un punto de multiplicidad 2:



No vemos los puntos de intersección de la cónica con la línea punteada, porque sus coordenadas son complejas.

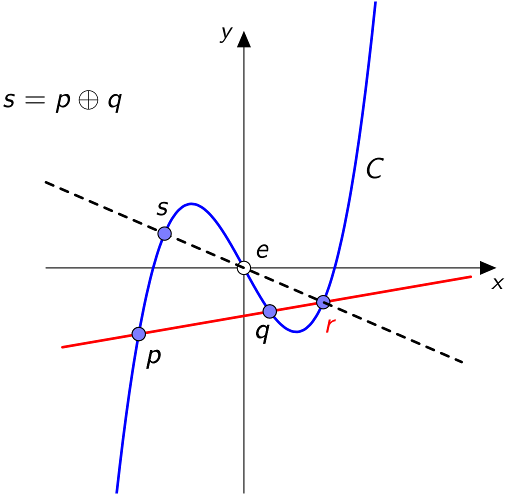
Una ley de un grupo

Recuerda qué es una ley de un grupo G: es una regla que, dado dos elementos $a, b \in G$, nos da un elemento tercero $c = a * b \in G$; pues, es una mapa $G \times G \to G$. Consideremos una curva cúbica C, por ejemplo $y = x^3 - x$; C tiene un punto de inflexión, e:



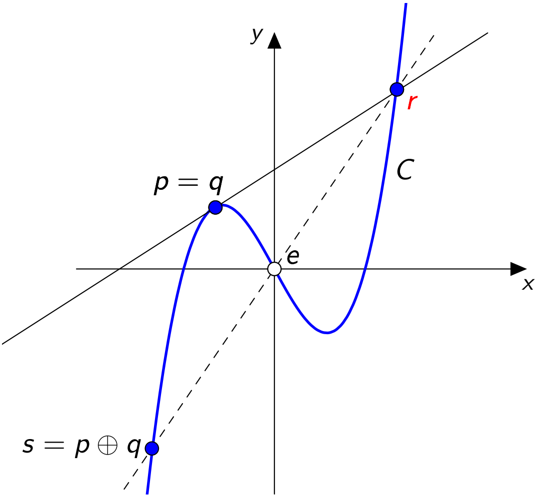
Una ley de un grupo

Recuerda qué es una ley de un grupo G: es una regla que, dado dos elementos $a, b \in G$, nos da un elemento tercero $c = a * b \in G$; pues, es una mapa $G \times G \to G$. Consideremos una curva cúbica C, por ejemplo $y = x^3 - x$; C tiene un punto de inflexión, e:

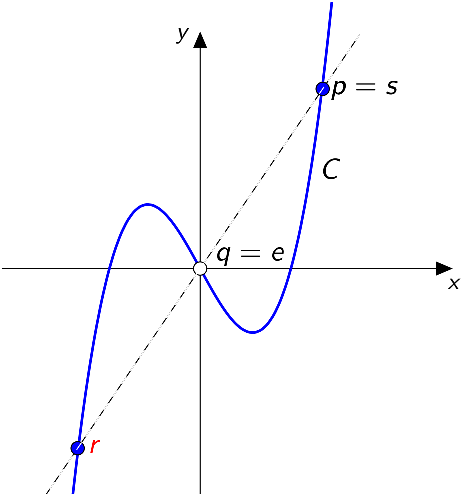


¿Qué es $p \oplus p$?

Se usa la línea tangente a la curva al punto p (así, $p = q$):

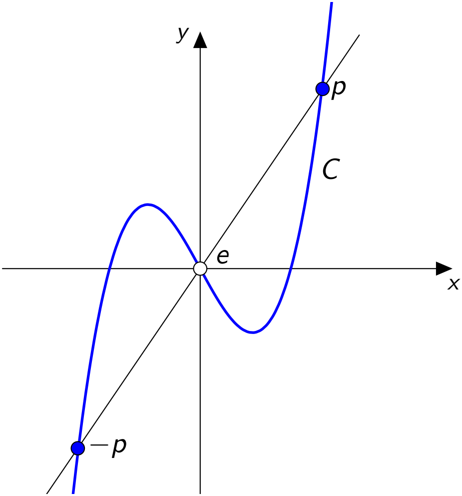


e es el elemento de identidad del grupo: $p \oplus e = p$



Los inversos aditivos

Los puntos situados simétricamente con respecto a e son inversos:



Consideremos la ley algebráicamente en este caso

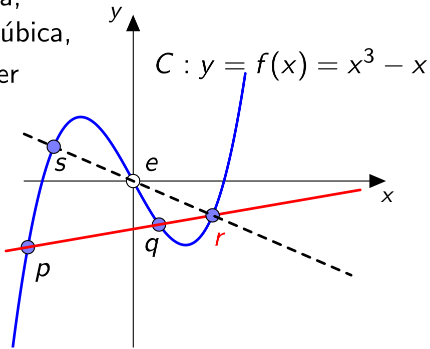
Dado un punto p, denotamos las coordenadas como así: $p = (p_1, p_2)$.

¿Dado puntos $p = (p_1, p_2)$ y $q = (q_1, q_2)$ de C, cuales son las coordenadas de $r = (r_1, r_2)$ y $s = (s_1, s_2)$? Sabemos que $r_2 = f(r_1)$ y $s_2 = f(s_1)$, así necesitamos encontrar los valores de r_1 y s_1.

Sabemos la equación de la línea roja, $y = \frac{p_2 - q_2}{p_1 - q_1}(x - p_1) + p_2$, y la de la cúbica, $y = x^3 - x$; así tenemos que resolver $x^3 - x = \frac{p_2 - q_2}{p_1 - q_1}(x - p_1) + p_2$.

Esta simplifica y factoriza así: $(x - p_1)(x - q_1)(x + p_1 + q_1) = 0$; pues $r_1 = -p_1 - q_1$ y $s = p_1 + q_1$.

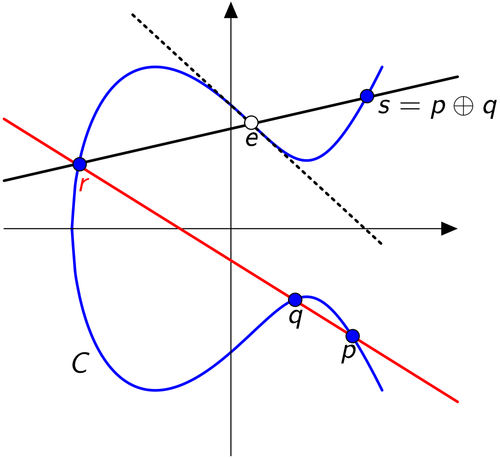
Desde el perspectivo de las coordenadas de x, la ley es suma ordinaria: $(p \oplus q)_1 = p_1 + q_1$!



La ley geométrica funciona en general

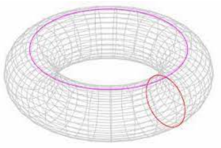
Aquí C es definida por $y^2 = x^3 - 3x + 3$.

Como antes, la identidad es dado por un punto de inflexión (la línea tangente punteada nos indica que el punto denotado e es, de hecho, un punto de inflexión). Ahora, encontramos $p \oplus q$.



Esta ley del grupo funciona sobre los números complejos.

Topológicamente, las soluciones de $y^2 = x^3 - 3x + 3$ sobre los números complejos es $S^1 \times S^1$:



Aquí, S^1 es el conjunto de números complejos de norma 1; así

$$S^1 = \{re^{i\theta} : r = 1, \theta \in \mathbb{R}\}.$$

Por supuesto, S^1 as un grupo, usando multiplicación complejo:

$$e^{ia} * e^{ib} = e^{i(a+b)}.$$

Dado grupos G y H, entonces $G \times H$ es un grupo, usando multiplicación por componentes. Por eso, $S^1 \times S^1$ es un grupo también.

Nuestra ley del grupo es la misma como esta!