Miscelánea Matemática **63** (2016) 77-92 SMM

Estructura de grupo en una curva elíptica

Jhon Jane Aguilar Alarcón*,
Jesús Romero Valencia†
Facultad de Matemáticas - UAGro.
*jonisps@live.com, †jromv@yahoo.com

Resumen

En este trabajo explicamos, desde un punto de vista geométrico, la estructura de grupo que posee una curva elíptica de la siguiente manera: definimos una operación binaria sobre esta y probamos que el conjunto de puntos de la curva junto con esta operación satisface las propiedades de grupo abeliano. Posteriormente verificamos que el conjunto de puntos racionales de una curva elíptica racional es un subgrupo, el cual es uno de los más interesantes e importantes de una curva elíptica.

1. Introducción

Uno de los principales quehaceres en matemáticas es estudiar conjuntos que posean algún tipo de estructura, por ejemplo conjuntos con estructura algebraica como lo son monoides, grupos, anillos, campos, espacios vectoriales, módulos y álgebras, por mencionar algunos. La mayoría de estas estructuras pueden construirse a partir de la definición de grupo, lo cual nos muestra que este concepto es fundamental y trascendente para entender las demás estructuras.

Recordemos que *un grupo* es una pareja $(G, *)$ donde G es un conjunto no vacío y $* : G \times G \to G$ es una operación binaria que satisface las siguientes propiedades:

- $*$ es asociativa;
- existe un elemento neutro en G para $*$;
- dado un elemento de G existe su inverso.

Si además $*$ es conmutativa, diremos que *el grupo es abeliano*.

De manera muy general, podemos clasificar los grupos en dos categorías: abelianos y no abelianos. Dentro de los primeros existe una infinidad de ejemplos, muchos de los cuales nos son muy conocidos, como los enteros $(\mathbb{Z}, +)$, los racionales $(\mathbb{Q}, +)$, los reales $(\mathbb{R}, +)$, los complejos $(\mathbb{C}, +)$ y las matrices $(Mat_{m\times n}(\mathbb{R}), +)$. Sin embargo, existen ejemplos que no son tan comunes y que no es natural pensar que posean tal estructura, como *las curvas elípticas*, tema central de este artÃculo.

Desde la antigüedad el estudio de las curvas ha sido abordado por diferentes matemáticos. Entre los siglos II y III d.C. aparecieron por primera vez las curvas elípticas en el libro *Arithmetica* escrito por Diofanto (aunque Diofanto no tenía idea acerca de este tipo de curvas), estas aparecieron de la siguiente forma, utilizando notación moderna:

$$y(a - y) = x^3 - x.$$

Posteriormente en el año 1630 Fermat consiguió una copia del libro *Arithmetica* de Diofanto que años antes había sido traducido al latín y Fermat trabajó con problemas que involucraban curvas elípticas; uno de ellos fue la conjetura de que los únicos enteros que satisfacen la ecuación $y^2 = x^3 - 2$ son $(x, y) = (3, 5)$ y $(3, -5)$.

Alrededor de 1670 Newton utilizó herramientas de la geometría analítica para clasificar curvas cúbicas. Al hacerlo explicó algunos misterios detrás tanto de los problemas de *Arithmetica* de Diofanto como del teorema de Bachet acerca de las soluciones racionales de una curva elíptica. En el siglo XIX, Jacobi y Weierstrass conectaron estos esfuerzos con las integrales elípticas y las funciones elípticas. Ya en el siglo XX Poincaré unificó y generalizó este trabajo a curvas algebraicas, también conjeturó que el grupo de puntos racionales de una curva elíptica racional es finitamente generado.

2. Preliminares

Nuestros objetos de estudio serán curvas cúbicas, planas, proyectivas y no-singulares, así que definiremos cada uno de los conceptos anteriores. Consideremos primero el plano proyectivo complejo:

$$\mathbb{P}^2 = \{(x : y : z) : (x, y, z) \in \mathbb{C}^3 \text{ y } (x, y, z) \neq (0, 0, 0)\},$$

donde $(a : b : c)$ es el conjunto de todos los múltiplos no cero del vector no nulo (a, b, c), es decir:

$$(a : b : c) = \{\lambda(a, b, c) : \lambda \in \mathbb{C},\ \lambda \neq 0\},$$

así, $(a : b : c)$ es *casi* el subespacio $1-$dimensional de $\mathbb{C}^3$ generado por (a, b, c), pues le falta $(0, 0, 0)$.

Notemos que $\mathbb{P}^2$ es, de hecho, el conjunto de órbitas dadas por la acción natural del grupo $\mathbb{C}^* = \mathbb{C} - \{0\}$ sobre el conjunto $\mathbb{C}^3 - \{(0,0,0)\}$, así la órbita de $\alpha = (x, y, z)$ es:

$$[\alpha] = \{(cx, cy, cz) : c \in \mathbb{C}^*\}.$$

Al conjunto de polinomios con coeficientes complejos e indeterminadas x, y y z lo denotamos por $\mathbb{C}[x, y, z]$. Diremos que $F(x, y, z) \in \mathbb{C}[x, y, z]$ *es homogéneo de grado* d, si el grado de cada uno de sus monomios es d, por ejemplo:

$$F(x, y, z) = 3x^2 + y^2 + z^2 + xy + xz$$

es un polinomio homogéneo de grado 2.

Sea $F(x, y, z) \in \mathbb{C}[x, y, z]$ homogéneo de grado d, observemos que no tiene sentido evaluar $F(x, y, z)$ en puntos de $\mathbb{P}^2$, por ejemplo, si consideramos:

$$F(x, y, z) = 2x^2 + yz + z^2$$

y $(1 : 1 : 1) \in \mathbb{P}^2$ entonces $F(1, 1, 1) = 4$, pero $F(2, 2, 2) = 16$ y $(1 : 1 : 1) = (2 : 2 : 2)$. En cambio, lo que sí tiene sentido son los ceros de este polinomio, pues si $P = (a : b : c) \in \mathbb{P}^2$ y $F(a, b, c) = 0$, entonces $F(\beta(a, b, c)) = 0$ para $\beta \in \mathbb{C}$, $\beta \neq 0$. En efecto, si:

$$F(x, y, z) = \sum t_{ijk} x^i y^j z^k$$

donde $i + j + k = d$, entonces:

$$\begin{aligned} F(\beta(a, b, c)) &= F(\beta a, \beta b, \beta c) = \sum t_{ijk} (\beta a)^i (\beta b)^j (\beta c)^k \\ &= \sum t_{ijk} \beta^d a^i b^j c^k = \beta^d \sum t_{ijk} a^i b^j c^k \\ &= \beta^d 0 = 0. \end{aligned}$$

Lo anterior nos asegura que la siguiente definición tiene sentido. Sea $F(x, y, z)$ un polinomio homogéneo, al conjunto:

$$\mathcal{C} = \{(u : v : w) \in \mathbb{P}^2 : F(u, v, w) = 0\}$$

lo llamaremos *la curva plana proyectiva, definida por* $F(x, y, z)$. La nomenclatura usual es la siguiente: $\mathcal{C}$ *es una recta, cónica o cúbica*, si el polinomio que define a $\mathcal{C}$ es de grado 1, 2 o 3, respectivamente. Sea $P \in \mathcal{C}$, diremos que $\mathcal{C}$ *es no-singular en* P, si las derivadas parciales de $F(x, y, z)$ no se anulan simultáneamente en P, es decir;

$$\frac{\partial F}{\partial x}(P) \neq 0, \ \frac{\partial F}{\partial y}(P) \neq 0 \ \text{ o } \ \frac{\partial F}{\partial z}(P) \neq 0.$$

Una curva elíptica es una curva cúbica, plana, proyectiva y no-singular, es decir, una curva definida por un polinomio homogéneo $F(x, y, z)$ de grado tres que satisface lo anterior.

Lo que haremos a continuación será bosquejar un procedimiento de cambio de coordenadas que nos permite escribir la ecuación de una curva elíptica $\mathcal{C}$ de manera conveniente para nuestros propósitos (para mayores detalles véase [14, p. 22]). Supongamos que $\mathcal{C}$ está dada por la ecuación:

$$F(x, y, z) = a_{300}x^3 + a_{210}x^2y + \cdots + a_{012}yz^2 + a_{003}z^3.$$

Podemos suponer que $(1 : 0 : 0) \in \mathcal{C}$ y que su tangente en ese punto es la recta $\ell_1 = \{z = 0\}$. También podemos suponer que el otro punto de intersección de $\mathcal{C}$ y ℓ_1 es $(0 : 1 : 0)$ y que la tangente en este punto es $\ell_2 = \{x = 0\}$. Bajo estas consideraciones tenemos que la ecuación de $\mathcal{C}$, en un principio es de la forma:

$$x^2z + a_{020}xy^2 + a_{111}xyz + a_{102}xz^2 + a_{012}yz^2 + a_{003}z^3 = 0.$$

Haciendo el cambio x por $\frac{x}{z}$ y y por $\frac{y}{z}$ obtenemos la siguiente expresión:

$$xy^2 + (ax + b)y = cx^2 + dx + e,$$

multiplicando por x esta expresión tenemos:

$$(xy)^2 + (ax + b)xy = cx^3 + dx^2 + ex$$

intercambiando xy por y obtenemos:

$$y^2 + (ax + b)y = \text{polinomio cúbico en } x,$$

reemplazando y por $y - \frac{1}{2}(ax+b)$ llegamos a una expresión de la forma:

$$y^2 = \text{ polinomio cúbico en } x.$$

Homogenizando la expresión anterior, tenemos que el polinomio se ve como sigue:

$$F_1(x, y, z) = a(x - x_1z)(x - x_2z)(x - x_3z) - y^2z.$$

A partir de ahora podemos considerar a una curva elíptica como una curva cúbica definida por un polinomio de la forma anterior, donde $x_1, x_2, x_3 \in \mathbb{C}$ son todos distintos.

Por ejemplo, la figura 1 es una representación en $\mathbb{R}^2$ de la curva elíptica definida por el polinomio $x^3 + 2x^2z - 3xz^2 + 2z^3 - y^2z$, lo cual se logra deshomogenizando al polinomio haciendo $z = 1$.

3. Estructura de grupo

En esta sección dotaremos de estructura de grupo a una cúbica, construyendo una operación binaria de manera puramente geométrica.

Consideremos el siguiente polinomio cúbico en $\mathbb{C}[x, y, z]$:

$$F(x, y, z) = x^3 + ax^2z + bxz^2 + cz^3 - y^2z,$$

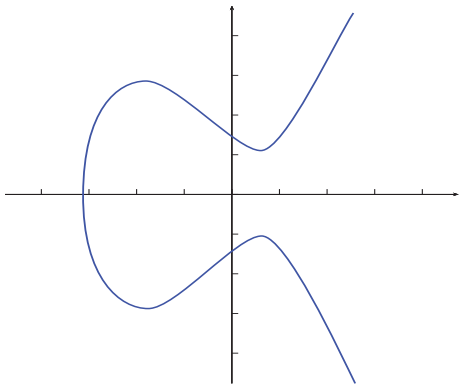

Figura 1. Representación gráfica en $\mathbb{R}^2$ de una curva elíptica.

y $\mathcal{C}$ la curva plana proyectiva definida por el polinomio anterior, es decir:

$$\mathcal{C} = \{(u : v : w) \in \mathbb{P}^2 : F(u, v, w) = 0\}.$$

Observemos que $\mathcal{C}$ es no-singular, ya que no hay punto de $\mathcal{C}$ en el cual las derivadas parciales de $F(x, y, z)$ se anulen de manera simultánea, por lo que $\mathcal{C}$ es una curva elíptica.

Si P y Q son dos puntos en $\mathbb{P}^2$, denotaremos por $\mathcal{L}_{P,Q}$ a la recta que pasa por P y Q. Si $\mathcal{L}$ es una recta, digamos:

$$\mathcal{L} = \{(u : v : w) \in \mathbb{P}^2 : G(u, v, w) = 0\},$$

donde $G(x, y, z)$ es un polinomio lineal, entonces, el *teorema de Bezout*[1] y el hecho de que $\mathcal{C}$ es no-singular implican que $\mathcal{C}$ y $\mathcal{L}$ tienen tres puntos de intersección, digamos, P_1, P_2 y P_3. La notación que usaremos será la siguiente:

$$\mathcal{C} \cdot \mathcal{L} = P_1, P_2, P_3.$$

Consideramos adecuado evitar escribir lo anterior como un conjunto, ya que puede suceder que dos de estos puntos coincidan, por ejemplo $P_1 = P_2$, y en notación conjuntista deberíamos escribir $\{P_1, P_3\}$, con lo cual se pierde información.

Definamos ahora la operación binaria $* : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$, dada por:

$$P * Q = R,$$

donde R es el tercer punto de intersección de $\mathcal{L}_{P,Q}$ con $\mathcal{C}$.

Es importante mencionar que cuando $P = Q$, entonces $\mathcal{L}_{P,Q}$ será la recta tangente a $\mathcal{C}$ en P.

Notemos que $*$ es conmutativa pues si $P, Q \in \mathcal{C}$, entonces la recta $\mathcal{L}_{P,Q}$ es la misma que $\mathcal{L}_{Q,P}$ y así $P * Q = R = Q * P$. Sin embargo, para

[1] **Teorema de Bezout**: Sean $\mathcal{C}$ y $\mathcal{C}'$ curvas planas proyectivas de grados n y m, respectivamente, sin componentes en común, entonces $\mathcal{C}$ y $\mathcal{C}'$ se intersecan en mn puntos, contados con multiplicidad. (Para una demostración véase [17, p. 112].)

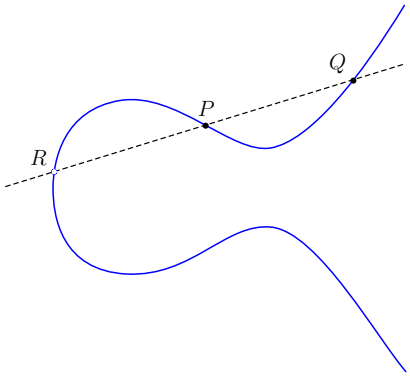

Figura 2. Representación de la operación $*$ sobre $\mathcal{C}$.

esta operación no existe elemento neutro. En efecto: supongamos que existe $O \in \mathcal{C}$ tal que $O * P = P$ para todo $P \in \mathcal{C}$. Consideremos la recta $\mathcal{L}_{P,P}$, entonces $\mathcal{L} \cdot \mathcal{C} = P, P, O$, así para cualquier $Q \in \mathcal{C}$ se tiene que $\mathcal{L} \cdot \mathcal{C} = Q, Q, O$ lo cual no es posible, por lo tanto no existe neutro.

La afirmación anterior se sigue del hecho de que dada X una curva plana proyectiva (sobre $\mathbb{C}$), no existe un punto por el cual pasen todas las tangentes a X.[2]

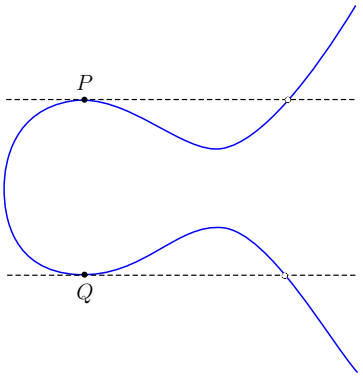

Figura 3. Imposibilidad de existencia de neutro para $*$.

Esto nos fuerza a considerar otra operación sobre $\mathcal{C}$, lo cual haremos usando la anterior. Fijemos un punto $O \in \mathcal{C}$ y definamos la operación binaria $+ : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$, dada por:

$$P + Q = R, \quad \text{donde } R = (P * Q) * O. \tag{1}$$

[2]**Teorema de Samuel:** Las únicas curvas extrañas en $\mathbb{P}^n$ son las rectas y las cónicas, sobre un campo de característica 2.

Una curva se llama *extraña*, si existe un punto por el cual pasen todas las rectas tangentes a esta curva.

(Para una demostración véase [12, p. 312])

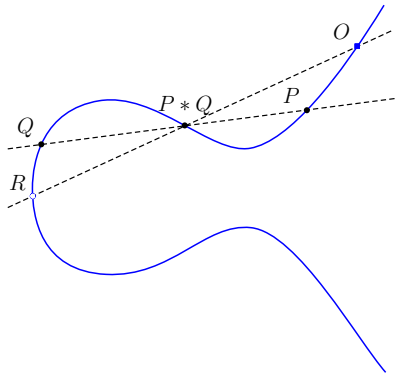

Figura 4. Representación de la operación $+$ sobre $\mathcal{C}$

A continuación veremos las propiedades que satisface esta operación definida sobre $\mathcal{C}$.

Asociatividad. Sean $P, Q, R \in \mathcal{C}$, primero calculemos $(P+Q)+R$ obteniendo $P * Q$, $P+Q$, $(P+Q) * R$ y $(P+Q)+R$, en este orden.

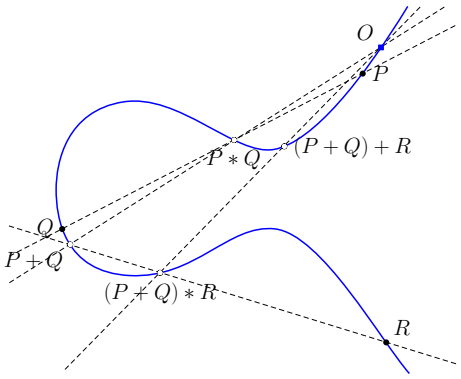

Figura 5. Construcción de $(P+Q)+R$.

Por otro lado, para calcular $P+(Q+R)$ obtenemos $Q*R$, $Q+R$, $P*(Q+R)$ y $P+(Q+R)$. Sea S el punto de intersección de las rectas $\mathcal{L}_{P+Q,R}$ y $\mathcal{L}_{P,Q+R}$ y consideremos las cúbicas:

$$\mathcal{C}_1 = \mathcal{L}_{P,Q+R}\mathcal{L}_{P*Q,O}\mathcal{L}_{Q,R} \quad \text{y} \quad \mathcal{C}_2 = \mathcal{L}_{P,Q}\mathcal{L}_{P+Q,R}\mathcal{L}_{Q*R,O}.$$

Entonces los puntos de intersección de $\mathcal{C}_1$ con $\mathcal{C}_2$ son:

$$\mathcal{C}_1 \cdot \mathcal{C}_2 = O, P, Q, R, P*Q, Q*R, P+Q, Q+R, S.$$

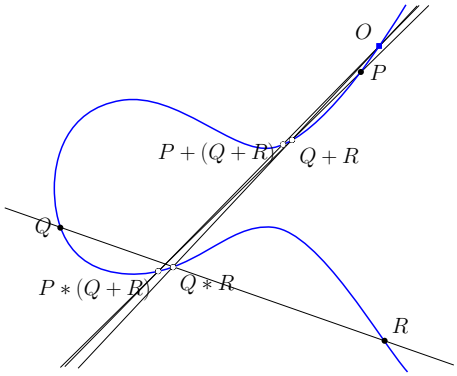

Figura 6. Construcción de $P + (Q + R)$.

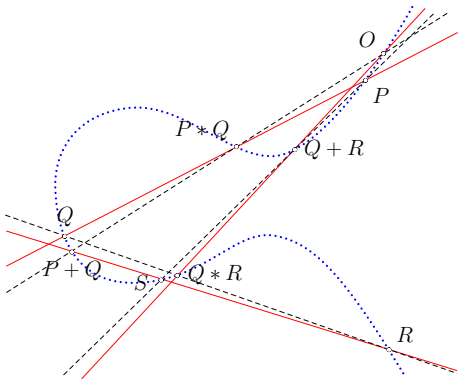

Figura 7. Representación de la asociatividad de $+$.

Como ocho de los nueve puntos anteriores están sobre $\mathcal{C}$, el *Teorema de los nueve puntos*[3] nos asegura que $S \in \mathcal{C}$.

Ahora, como $\mathcal{C} \cdot \mathcal{L}_{P+Q,R} = P + Q, R, (P + Q) * R$, entonces $S = (P+Q)*R$ y, análogamente, $\mathcal{C} \cdot \mathcal{L}_{P,Q+R} = P, Q+R, P*(Q+R)$ implica $S = P * (Q + R)$, de donde, $(P + Q) * R = P * (Q + R)$ y, por lo tanto:

$$\begin{aligned}(P + Q) + R &= ((P + Q) * R) * O \\ &= (P * (Q + R)) * O = P + (Q + R).\end{aligned}$$

Conmutatividad. Sean $P, Q \in \mathcal{C}$, entonces:

$$P + Q = (P * Q) * O = (Q * P) * O = Q + P.$$

[3]**Teorema de los nueve puntos**: Sean $\mathcal{C}$, $\mathcal{C}_1$ y $\mathcal{C}_2$ tres cúbicas. Si $P_1, \ldots, P_9$ son los nueve puntos de intersección de $\mathcal{C}_1$ con $\mathcal{C}_2$ y $P_1, \ldots, P_8 \in \mathcal{C}$, entonces $P_9 \in \mathcal{C}$.
(Para una demostración véase [17, p. 62].)

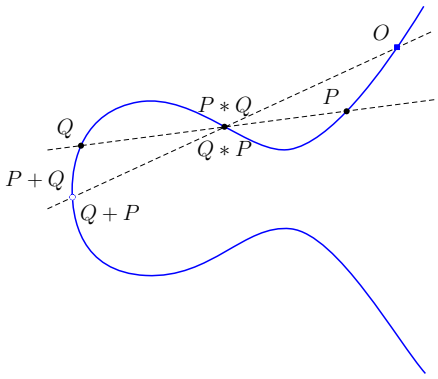

Figura 8. Representación de la conmutatividad de $+$.

Existencia de elemento neutro. Consideremos el punto $O \in \mathcal{C}$ fijado al principio y sea $P \in \mathcal{C}$, entonces la recta $\mathcal{L}_{O,P}$ es, claramente, la misma que $\mathcal{L}_{O*P,P}$, de donde:

$$O + P = (O * P) * O = P.$$

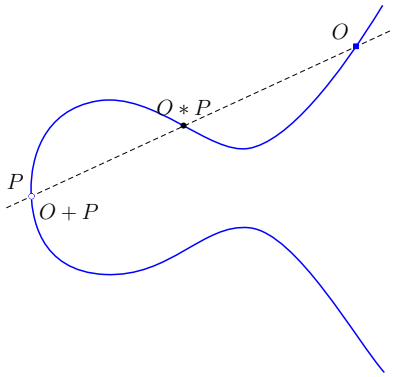

Figura 9. Representación del elemento neutro de $+$.

Existencia de inversos. Sea $P \in \mathcal{C}$, consideremos la recta $\mathcal{L}_{O,O}$, es decir, la tangente a $\mathcal{C}$ en O, y supongamos que $Q = O * O$. Sea R el otro punto de intersección de la recta $\mathcal{L}_{P,Q}$ con $\mathcal{C}$, es decir, $P * Q = R$. Afirmamos que R es el inverso de P, en efecto:

$$P + R = (P * R) * O = Q * O = O.$$

En resumen, hemos demostrado el siguiente resultado:

Teorema 3.1. *Sean $\mathcal{C}$ una curva elíptica y $+$ la operación binaria definida sobre $\mathcal{C}$ en la ecuación 1, entonces $(\mathcal{C}, +)$ es un grupo abeliano.*

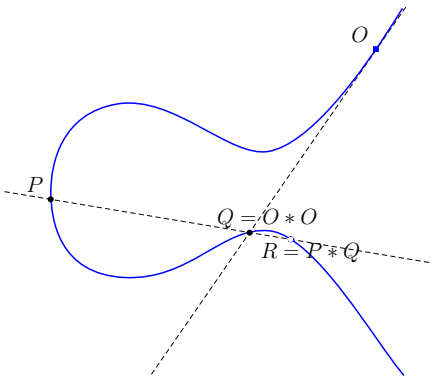

Figura 10. Representación de los elementos inversos.

4. El subgrupo de puntos racionales

En esta sección veremos uno de los subgrupos de mayor interés de $(\mathcal{C}, +)$, cuando la ecuación de $\mathcal{C}$ se puede escribir con coeficientes en $\mathbb{Q}$. Recordemos que *un grupo* $(G, *)$ *se llama finitamente generado*, si existe un número finito de elementos de G, digamos $x_1, \ldots, x_k \in G$ tales que $G = \langle x_1, \ldots, x_k \rangle$, donde:

$$\langle x_1, \ldots, x_k \rangle = \bigcap_{H_i < G} H_i, \quad x_1, \ldots, x_k \in H_i.$$

Comenzando con un poco de historia acerca del grupo de puntos racionales de una curva elíptica, alrededor del año 1908 Poincaré conjeturó lo siguiente:

> El conjunto de puntos racionales de una curva elíptica racional es un grupo finitamente generado,

sin embargo, esto no fue demostrado hasta 14 años después cuando en 1922 Louis Mordell lo demostró, por lo que este resultado pasaría a llamarse *teorema de Mordell*. Años más tarde André Weil generalizó este teorema a curvas elípticas sobre cualquier campo, y esta generalización obtuvo el nombre de *Teorema de Mordell-Weil*.

Comencemos definiendo los siguientes conceptos sobre racionalidad.

Definición 4.1. Sea $P = (u, v) \in \mathbb{C}^2$, diremos que P *es un punto racional*, si $u, v \in \mathbb{Q}$. Si $\mathcal{C} \subset \mathbb{P}^2$ es una curva, diremos que $\mathcal{C}$ *es racional,* si existe un polinomio de coeficientes racionales que la defina.

Observemos por ejemplo que la recta:

$$\mathcal{L} = \{(x : y : z) \in \mathbb{P}^2 : \sqrt{3}x - \sqrt{12}y = 0\},$$

a pesar de estar definida por una ecuación no racional es racional, puesto que podemos encontrar un polinomio con coeficientes en $\mathbb{Q}$ que la defina:

$$\mathcal{L}: \quad 3x - 6y = 0.$$

Notemos que si $F(x, y, z) \in \mathbb{C}[x, y, z]$ es un polinomio homogéneo que define alguna curva $\mathcal{C}_1 \subset \mathbb{P}^2$, entonces $f(x, y) = F(x, y, 1) \in \mathbb{C}[x, y]$ es un polinomio que define una curva $\mathcal{C} \subset \mathbb{C}^2$:

$$\mathcal{C} = \{(u, v) \in \mathbb{C}^2 : f(u, v) = 0\}.$$

También diremos que $\mathcal{C}$ *es racional*, si existe un polinomio $f(x, y)$ con coeficientes racionales que la defina, por ejemplo la curva definida por:

$$f(x, y) = 65x^3 + 195x^2 + 39x + 45 - 65y^2$$

es racional.

Consideremos una curva elíptica $\mathcal{C}_1 \subset \mathbb{P}^2$ definida por un polinomio:

$$F(x, y, z) = x^3 + ax^2z + bxz^2 + cz^3 - y^2z \in \mathbb{C}[x, y, z]$$

y sea $\mathcal{C} \subset \mathbb{C}^2$ la curva definida por el polinomio:

$$f(x, y) = F(x, y, 1) = x^3 + ax^2 + bx + c - y^2 \in \mathbb{C}[x, y].$$

A este tipo de curvas también las llamaremos curvas elípticas. Es importante que observemos que «casi todos» los puntos $P \in \mathcal{C}_1$ son de la forma $(u : v : 1)$. En efecto: sea $P = (u : v : 0) \in \mathcal{C}_1$, entonces:

$$0 = F(u, v, 0) = u^3 + au^2(0) + bu(0)^2 + c(0)^3 - v^2(0) = u^3$$

así $u = 0$, de donde, $P = (0 : v : 0) = (0 : 1 : 0)$ es el único punto de $\mathcal{C}$ que no es de la forma $(u : v : 1)$.

Consideremos la función $\phi : \mathbb{C}^2 \to \mathbb{P}^2$, dada por:

$$(a, b) \longmapsto (a : b : 1).$$

ϕ es una función inyectiva, pues si $(a, b), (c, d) \in \mathbb{C}^2$ satisfacen:

$$\phi(a, b) = \phi(c, d), \quad \text{entonces} \quad (a : b : 1) = (c : d : 1),$$

así, existe $\lambda \in \mathbb{C}$ tal que $a = \lambda c, b = \lambda d$ y $1 = \lambda 1$, de donde $a = c$ y $b = d$. Lo anterior nos asegura que tenemos un encaje $\mathbb{C}^2 \hookrightarrow \mathbb{P}^2$. Lo que haremos a continuación será demostrar un resultado previo que nos ayudará a probar que dada $\mathcal{C} \subset \mathbb{C}^2$ una curva elíptica racional el conjunto de puntos racionales de esta es un subgrupo de $(\mathcal{C}, +)$.

Lema 4.2. *Sean $\mathcal{C} \subset \mathbb{C}^2$ una curva elíptica racional y $P, Q \in \mathcal{C}$ racionales, entonces la recta $\mathcal{L}_{P,Q}$ es racional y el tercer punto de intersección de $\mathcal{L}_{P,Q}$ con $\mathcal{C}$ es otro punto racional.*

Demostración. Primero notemos que la recta determinada por dos puntos racionales $P = (u, v)$ y $Q = (w, t)$ es racional. En efecto: $\mathcal{L}_{P,Q}$ está dada por un polinomio lineal $f(x, y) = mx + ny + p$ y tanto P como Q deben satisfacer dicho polinomio, de esto obtenemos el siguiente sistema de ecuaciones lineales con coeficientes en $\mathbb{Q}$:

$$\begin{aligned} um + vn + p &= 0 \\ wm + tn + p &= 0, \end{aligned}$$

el cual tiene solución no trivial, de donde, $m, n, p \in \mathbb{Q}$.
Ahora verifiquemos que el tercer punto de intersección de $\mathcal{L}_{P,Q}$ con $\mathcal{C}$ es racional, para esto resolvamos el siguiente sistema de ecuaciones:

$$\begin{aligned} mx + ny + p &= 0 \\ x^3 + ax^2 + bx + c - y^2 &= 0. \end{aligned}$$

Supongamos $n \neq 0$, el procedimiento será análogo si $n = 0$ y $m \neq 0$, entonces $y = -\frac{mx+p}{n}$ y sustituyendo en la ecuación de $\mathcal{C}$ obtenemos:

$$x^3 + ax^2 + bx + c - \left(-\frac{mx + p}{n}\right)^2 = 0$$

la cual es una ecuación cúbica de la forma:

$$x^3 + Ax^2 + Bx + C = 0,$$

donde A, B y C son racionales, esta se puede escribir como:

$$(x - x_1)(x - x_2)(x - x_3) = 0$$

donde x_1, x_2 y x_3 son precisamente las raíces del polinomio $x^3 + Ax^2 + Bx + C$ y dado que $P = (u, v)$ y $Q = (w, t)$ son dos de los puntos de intersección $L_{P,Q}$ con $\mathcal{C}$, tenemos que dos de las raíces son racionales digamos $x_1 = u$ y $x_2 = w$, también tenemos que $B \neq 0$ o $C \neq 0$, pues las raíces no se repiten. Supongamos que $C \neq 0$, entonces la relación:

$$(x - u)(x - w)(x - x_3) = x^3 + Ax^2 + Bx + C$$

implica $-uwx_3 = C$ y $u, w, x_3 \neq 0$ de lo cual se tiene que $x_3 = -\frac{C}{uw}$, por lo tanto $x_3 \in \mathbb{Q}$, pues $C, u, w \in \mathbb{Q}$.

Ahora, si $C = 0$, entonces $B \neq 0$, así la relación:

$$(x - u)(x - w)(x - x_3) = x^3 + Ax^2 + Bx + C$$

implica $ux_3 + wx_3 + uw = B$, como $C = 0$ entonces $u = 0$, $w = 0$ o $x_3 = 0$.

Si $x_3 = 0$, entonces $x_3 \in \mathbb{Q}$.

Si $w = 0$, entonces $x_3 = \frac{B}{u}$ por tanto $x_3 \in \mathbb{Q}$. Análogamente se procede si $u = 0$. Sustituyendo $x = x_3$ en la ecuación:

$$dx + ey + f = 0$$

tenemos que $y = -\frac{dx_3+f}{e}$, lo cual implica que $y \in \mathbb{Q}$. Por lo tanto, podemos concluir que el tercer punto de intersección de $\mathcal{L}_{P,Q}$ con $\mathcal{C}$ es racional. □

Procedamos a demostrar el resultado principal de esta sección.

Teorema 4.3. *Sean $\mathcal{C}$ una curva elíptica racional, con elemento neutro O un punto racional, entonces el conjunto $\mathbb{Q}(\mathcal{C}) = \{P \in \mathcal{C} : P$ es racional$\}$ es un subgrupo de $(\mathcal{C}, +)$.*

Demostración. Verifiquemos las tres condiciones para que un subconjunto sea un subgrupo:

1. Por hipótesis, $O \in \mathbb{Q}(\mathcal{C})$.
2. Por el lema anterior tenemos que si $P, Q \in \mathbb{Q}(\mathcal{C})$, entonces $P * Q \in \mathbb{Q}(\mathcal{C})$ y por lo tanto $P + Q \in \mathbb{Q}(\mathcal{C})$.
3. Por último, si $R \in \mathbb{Q}(\mathcal{C})$, el hecho de que $-R = (O * O) * R$ implica $-R \in \mathbb{Q}(\mathcal{C})$.

Por lo tanto $\mathbb{Q}(\mathcal{C})$ es un subgrupo de $\mathcal{C}$. □

5. Conclusiones

Es fascinante descubrir cómo es posible dotar de estructura de grupo a una curva elíptica de una manera puramente geométrica, partiendo de una operación que no satisface lo que deseamos, pero que sí es útil para definir otra que cumple con las propiedades que buscamos.

Nos parece importante mencionar lo siguiente: dada una curva proyectiva no-singular $\mathcal{X}$, siempre se puede construir un grupo abeliano asociado a ella, su *variedad jacobiana*, la cual, muy a grandes rasgos, se construye como sigue.

El hecho de que $\mathcal{X}$ sea una curva proyectiva no-singular implica que es una superficie de Riemann compacta. Supongamos que es de género g, entonces la jacobiana de $\mathcal{X}$ se define como el grupo cociente:

$$Jac(\mathcal{X}) = \mathbb{C}^g/\Lambda,$$

donde Λ es un subgrupo de $\mathbb{C}^g$ que se construye a partir de $\mathcal{X}$ (para una explicación detallada de lo anterior véase, por ejemplo [11, p. 247]). Podemos ver entonces que $Jac(\mathcal{X})$ es un grupo abeliano. Para el caso particular de una curva elíptica $\mathcal{C}$, la cual es de género 1, se tiene que $\mathcal{C} \cong Jac(\mathcal{C})$ (véase [11, p. 248]). Por lo tanto, $\mathcal{C}$ es un grupo abeliano. De hecho, las únicas curvas no-singulares que admiten estructura de grupo son precisamente las curvas elípticas.

Uno de los subgrupos de mayor interés de una curva elíptica es el de puntos racionales, sobre el cual, como ya mencionamos, existe el importante resultado llamado *el teorema de Mordell*, que, muy a grandes

rasgos, nos dice que este subgrupo es finitamente generado, así, utilizando el teorema fundamental de grupos abelianos finitamente generados[4] podemos escribir:

$$\mathbb{Q}(\mathcal{C}) \cong \mathbb{Z}^r \oplus \mathbb{Q}(\mathcal{C})_{\text{tors}},$$

donde $r \in \mathbb{Z}^+$ y G_{tors} es el subgrupo de torsión de un grupo abeliano G.

5.1 Lecturas recomendadas

Por último queremos concluir estas notas con una serie de referencias recomendadas para el lector que se interese en profundizar en alguno de los aspectos tratados anteriormente.

La literatura existente sobre curvas elípticas puede considerarse variada y abundante. Por ejemplo, para ver una curva elíptica como un toro complejo construido como el cociente de $\mathbb{C}$ por una retícula puede consultarse [8] (Capítulo I: *From Congruent Numbers to Elliptic Curves*). Para ver detalladamente una demostración del teorema de Mordell se puede revisar [7] (Capítulo VI: *Proof of Mordell's Finite Generation Theorem*) o [14] (Capítulo III: *The Group of Rational Points*) y para una generalización de este teorema (el Teorema de Mordell-Weil) puede consultarse [2] (Capítulo 10: *The Mordell-Weil theorem*). Si se está interesado en curvas elípticas sobre campos finitos, así como también de criptosistemas con curvas elípticas se puede leer [9] (Capítulo VI: *Elliptic Curves*).

Hemos trabajado particularmente con curvas cúbicas no-singulares, sin embargo, la teoría de curvas algebraicas es mucho más amplia e interesante, para este tema pueden considerarse excelentes libros introductorios como [17], [13] y [16]. Otra fuentes donde se puede leer al respecto de este tema, pero que requiere un poco más de conocimientos previos es [12] (Capítulo IV: *Curves*).

Anteriormente mencionamos que una curva proyectiva no-singular puede considerarse como superficie de Riemann y a esta se le asocia una variedad que tiene estructura de grupo, su jacobiana. Estos temas han sido ampliamente estudiados, por lo cual también existe una amplia bibliografía al respecto, para el lector interesado recomendamos [11], [10] (Apéndice: *Curves and Their Jacobians*) donde se hace un estudio detallado para curvas de géneros 0, 1, 2, 3 y 4, y [4] y [5] (Capítulo 2: *Riemann Surfaces and Algebraic Curves*).

---

[4] **Teorema fundamental de grupos abelianos finitamente generados:** Todo grupo abeliano finitamente generado G es isomorfo a una suma directa finita de grupos cíclicos, cada uno de los cuales es de orden infinito o potencia de un primo.

En símbolos, $G \cong \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus \mathbb{Z}_{p_1^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{r_k}}$, es decir, G es isomorfo a una suma directa de un grupo libre de rango finito y un grupo de torsión.

Para una demostración véase [6, p. 76].

Al enunciar el teorema de Mordell hicimos referencia a un resultado sobre clasificación: el teorema fundamental de grupos abelianos finitamente generados, este es solamente uno de los tantos teoremas que existen sobre clasificación, como por ejemplo, el teorema de clasificación de grupos finitos simples, también conocido como «el teorema enorme», el cual básicamente dice que cualquier grupo finito simple pertenece a alguna de las siguientes clases:

- ◇ grupos cíclicos de orden primo,
- ◇ grupos alternantes de grado ≥ 5,
- ◇ grupos de Chevalley,
- ◇ grupos de Chevalley torcidos,
- ◇ grupos esporádicos.

En realidad este teorema es una recopilación de muchas investigaciones y resultados que se han ido demostrando a través de 200 años, aproximadamente. Para tener una idea de esto recomendamos revisar el artículo [3].

Para ver la aplicación de las curvas elípticas en criptografía, recomendamos ver [1] (Capítulo I: *Introduction*, Sección 1: *Cryptography Based on Groups*) donde se exponen algunos protocolos de seguridad usando un grupo abeliano finito; además del artículo de [15] donde presentan un algoritmo usando la ley de grupo en curvas elípticas y mencionan otros algoritmos tanto simétricos como de clave pública.

Agradecimientos

Nos gustaría agradecer sinceramente a los revisores anónimos de la versión original de este trabajo por sus críticas, comentarios y sugerencias (atendimos casi todas). Creemos, indudablemente, que nos fueron de gran ayuda y esperamos haber obtenido una versión mejorada del manuscrito previo.

Bibliografía

[1] I. Blake, G. Seroussi y N. Smart, *Elliptic Curves in Cryptography*, London Mathematical Society: London Mathematical Society Lecture Note Series, Cambridge University Press, 1999.

[2] E. Bombieri y W. Gubler, *Heights in Diophantine Geometry*, New Mathematical Monographs, Cambridge University Press, 2007.

[3] M. Cartwright, «Ten Thousand Pages to Prove Simplicity», *New Scientists*, vol. 109, 1985, 26–30.

[4] H. M. Farkas y I. Kra, *Riemann Surfaces*, Graduate Texts in Mathematics, Springer-Verlag, 1992.

[5] P. Griffiths y J. Harris, *Principles of Algebraic Geometry*, Wiley Classics Library, Wiley, 2011.

[6] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics, Springer Science & Business Media, 2003.
[7] D. Husemöller, *Elliptic Curves*, Graduate Texts in Mathematics, Springer-Verlag, 2004.
[8] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Graduate Texts in Mathematics, Springer Science & Business Media, 1993.
[9] ———, *A Course in Number Theory and Cryptography*, Graduate Texts in Mathematics, Springer-Verlag, 1994.
[10] D. Mumford, *The Red Book of Varieties and Schemes*, Lecture Notes in Mathematics, Springer Science & Business Media, 1999.
[11] M. Rick, *Algebraic Curves and Riemann Surfaces*, Graduate Studies in Mathematics, American Mathematical Society, 1995.
[12] H. Robin, *Algebraic Geometry*, Graduate Texts in Mathematics, Springer Science & Business Media, 1977.
[13] I. R. Shafarevich, *Basic Algebraic Geometry 1*, Springer-Verlag, 1994.
[14] J. H. Silverman y J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer Science & Business Media, 1994.
[15] K. Vivek, S. A. Vivek y S. Ramesh, «Elliptic Curve Cryptography», *ACM Ubiquity*, vol. 9, 2008, 1–8.
[16] R. J. Walker, *Algebraic Curves*, Princeton Mathematical Series, Springer-Verlag, 1978.
[17] F. William, *Algebraic Curves: An Introduction to Algebraic Geometry*, Advanced book classics, Addison-Wesley Publishing Company, Advanced Book Program, 1989.