UNA NOTA SOBRE CUBICAS PLANAS

por Horacio Tapia-Recillas(*)

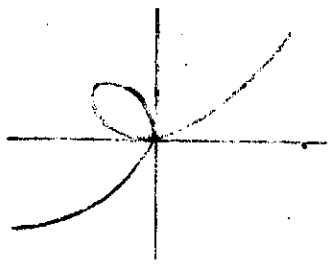
En memoria de mi amigo Ruy Alvarez.

El propósito de ésta nota es de presentar en forma elemental y geométrica una de las varias estructuras de que estan dotadas las curvas cúbicas planas no-singulares. Nos referimos a la estructura de grupo abeliano. Más concretamente, si $F(x,y) = a\,x^3 + b\,x^2\,y + c\,x\,y^2 + d\,y^3 + e\,x^2 + f\,x\,y + g\,y^2 + h\,x + i\,y + j$ es un polinomio cúbico con coeficientes en el campo k (donde k denota al campo de los números racionales $\mathbb{Q}$, reales $\mathbb{R}$ ó complejos $\mathbb{C}$) con descriminante $\Delta \neq 0$ y si C_k es el conjunto de soluciones en el campo k del polinomio F, entonces se puede definir una operación binaria en C_k con la cual este conjunto (si no es vacio) resulta ser un grupo abeliano. A C_k lo llamaremos el conjunto de puntos k-racionales de $F(x,y) = 0$ ó de la curva C definida por el polinomio F.

(*) Departamento de Matemáticas del CIEA del IPN.

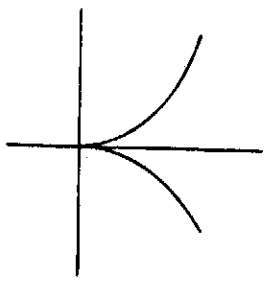
Antes de ver que C_k tiene la estructura de grupo abeliano, consideremos algunos casos particulares del polinomio cúbico $F(x,y)$ y algunas propiedades elementales de las cúbicas.

Ejemplos



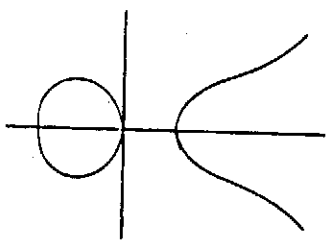
$F(x,y) = x^3 - y^3 - xy$

$\Delta = 0$



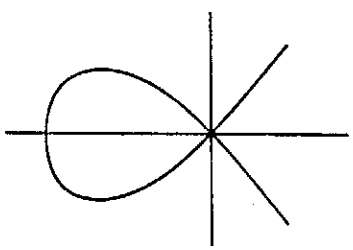
$F(x,y) = y^2 - x^3$

$\Delta = 0$



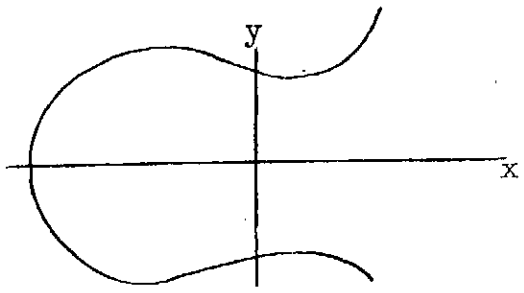
$F(x,y) = y^2 - x^3 + x$

$\Delta \neq 0$



$F(x,y) = y^2 - x^3 + x^2$

$\Delta = 0$



$$F(x,y) = x^3 + px + q$$

$$\Delta = -4p^3 - 27q^2.$$

Observación: es obvio que si los polinomios de los ejemplos anteriores son tomados con coeficientes complejos, solo podemos "dibujar" la parte real de la curva determinada por el polinomio.

§1 ALGUNAS PROPIEDADES ELEMENTALES DE LAS CUBICAS.

Es bien conocido que el número de raices comunes a dos polinomios de grado 3, contando multiplicidades, es 9. Esto quiere decir en términos geométricos que dos cúbicas se intersectan en 9 puntos, contando estos propiamente, por ejemplo puntos de tangencia se toman con multiplicidad mayor que 1. En general se tiene el siguiente resultado básico en la teoría de curvas planas debido a Bezout: si C_1 y C_2 son dos curvas definidas por polinomios de grado m y n respectivamente, éstas se cortan en mn puntos contando estos propiamente. Para la demostración de este resultado ver por ejemplo [13], [17], [20], ó bien el lector puede intentar demostrar el Teorema de Bezout.

También es bien conocido que un polinomio está determinado cuando se conocen todos sus coeficientes. En particular un polinomio $F(x,y)$ de grado 3 está determinado si se conocen sus 10 coeficientes a,b,c,d,e,f,g,h,i,j. Obsérvese que si λ es cualquier constante no cero, las raices de los polinomios $F(x,y)$ y $\lambda F(x,y)$ son las mismas, i.e. las curvas definidas por F y λF son la misma. Así podemos decir que el conjunto de todas las cúbicas es de "dimensión 9", ya que se puede tomar uno de los coeficientes igual a 1.

Ahora bien si una cúbica pasa por un punto P dado, se está imponiendo una condición lineal en los coeficientes del polinomio que determina a la cúbica, es decir se puede expresar un coeficiente en función de los restantes y de las coordenadas del punto P. Entonces para determinar el conjunto de cúbicas que pasan por un punto dado basta determinar 8 coeficientes del polinomio que determina cada cúbica. Así podemos decir que este conjunto es de "dimensión 8". Cada vez que una cúbica pase por un punto, se impone una condición lineal extra en los coeficientes del polinomio que determina a la cúbica y por lo tanto la "dimensión" de la familia de cúbicas disminuye en 1. En particular el conjunto de cúbicas que pasan por 8 puntos dados tiene dimensión 1.

Usaremos el argumento anterior para dar una idea de que el siguiente resultado es cierto: si una cúbica C pasa por 8 de los puntos de intersección de otras dos cúbicas C_1 y C_2, entonces C también pasa por el noveno punto de intersección de C_1 y C_2.

Consideremos la familia $\mathcal{C}$ de cúbicas que pasan por 8 de los puntos de intersección de C_1 y C_2. Como se vió antes ésta familia tiene dimensión 1.

Se pueden encontrar cúbicas que pasen por esos mísmos 8 puntos tomando combinaciones lineales $\alpha_1 C_1 + \alpha_2 C_2$ de los polinomios que definen a C_1 y C_2. Si C es elemento de la familia $\mathcal{C}$, entonces C se puede escribir como $C = \alpha_1 C_1 + \alpha_2 C_2$ para alguna α_1 y α_2.

Ahora bien como el noveno punto de intersección de C_1 y C_2 anula a la ecuación que define a C_1 y a C_2 se sigue inmediatamente que éste punto está en C ya que la ecuación que define a C también se anula en éste punto, y nuestra afirmación queda establecida.

Este resultado será usado para demostrar que la operación binaria que se definirá sobre C_k es asociativa. cf §2.

§2 CONSTRUCCION GEOMETRICA DE LA ESTRUCTURA DE GRUPO ABELIANO.

Recordemos brevemente la definición de grupo abeliano. (cf p. ejemplo: Carmichael, R.D. Groups of finite order)

Un grupo abeliano es una pareja $(G,+)$ donde G es un conjunto no vacío y $+$ es una operación binaria en G que satisface las siguientes propiedades:

i) G es cerrado bajo la operación $+$

ii) la operación $+$ es asociativa, i.e. $(a+b)+c = a+(b+c)$ para todo elemento a,b,c de G.

iii) existe un elemento $0 \in G$ tal que $a + 0 = a$ para toda $a \in G$. (elemento neutro)

iv) para cada $a \in G$, existe $b \in G$ tal que $a + b = 0$ (existencia de inverso)

v) la operación $+$ es conmutativa, i.e. $a+b = b+a$ para toda $a,b \in G$.

Procedamos ahora a probar que el conjunto C_k (si no es vacío) de puntos k-racionales de una curva cúbica plana no singular tiene estructura de grupo abeliano.

Sean $P, Q \in C_k$ i.e. P y Q son puntos en la curva C con coordenadas en el campo k. La recta $\ell_{P,Q}$ que pasa por

P y Q intersecta a la curva C en un tercer punto el cual denotaremos por PQ fig. 1. Nótese que el punto PQ puede coincidir con P ó Q, por ejemplo si la recta $\ell_{P,Q}$ es tangente a P ó Q, o bién se pueden tener otras posibilidades. Para nuestra discusión no interesa mucho donde se encuentra el punto PQ.

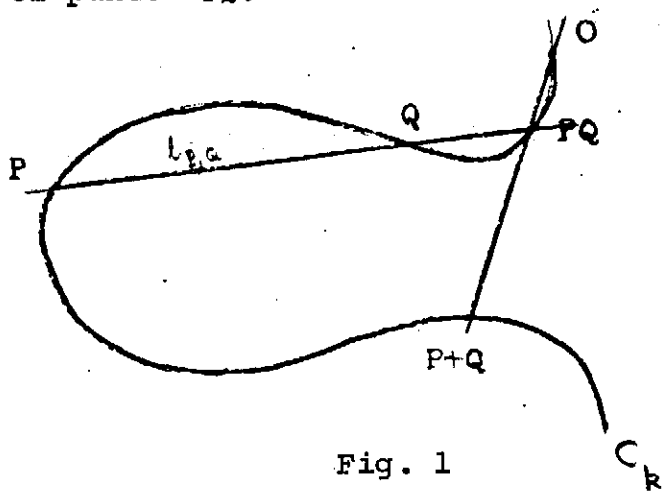


Fig. 1

Como los puntos P y Q tienen coordenadas en k, y la ecuación de la recta $\ell_{P,Q}$ tiene coeficientes en k, el punto PQ también tiene coordenadas en k. Lo anterior sugiere que en C_k se puede definir en forma natural la operación: $(P,Q) \longrightarrow PQ$.

Como nuestro fin es definir una operación en C_k con la cual éste conjunto resulte ser un grupo abeliano es natural preguntarse si C_k es grupo con la operación definida arriba.

Ciertamente esta operación satisface todos los axiomas

para que C_k sea grupo abeliano excepto una: bajo ésta operación no existe la identidad ! . Si el lector no cree ésta afirmación, lo invitamos a que haga algunos intentos para encontrar un punto en C_k que funcione como la identidad bajo la operación antes mencionada.

Para definir una operación en C_k que sirva para nuestro fin, vamos a aprovechar la operación definida anteriormente y modificarla de tal manera que sí exista la identidad en C_k y por supuesto los axiomas restantes sigan siendo válidos.

Para conseguir nuestro objetivo tomemos un punto arbitrario en C_k i.e. con coordenadas en k, y fijémoslo. Denotemos a éste punto por 0.

Con la ayuda de 0 y la operación definida anteriormente vamos a definir otra operación en C_k: sean P, Q dos puntos de C_k y sea PQ el tercer punto de intersección de C con la recta $\ell_{P,Q}$ como se hizo anteriormente. Sea $\ell_{0,PQ}$ la recta que pasa por los puntos 0 y PQ. La intersección de $\ell_{0,PQ}$ con la curva C es un tercer punto sobre C el cual denotaremos por $P+Q$.

Como el lector se podrá imaginar, la operación que andamos buscando y la cual denotaremos con el símbolo $+$ está dada por: $+:C_k \times C_k \longrightarrow C_k$ $(P,Q) \longrightarrow P+Q$, donde el punto $P+Q$ es el tercer punto de intersección de la recta $\ell_{0,PQ}$

con la curva C. (ver fig. 2).

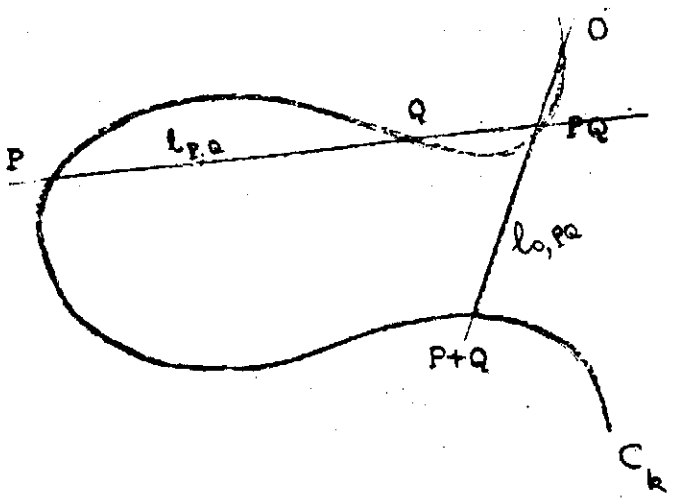


fig. 2

Veamos ahora que efectivamente la operación que se acaba de definir es adecuada para nuestro fin, i.e. veamos que C_k es un grupo abeliano con esta nueva operación.

Por principio de cuentas, como se mencionó antes si P y Q tienen coordenadas en k, así también el punto PQ tiene coordenadas en k. Como se tomó 0 con coordenadas en k se sigue que también el punto P + Q de la curva tiene coordenadas en k. Es decir C_k es <u>cerrado</u> bajo la operación +.

Veamos ahora que el punto 0 de C_k que seleccionamos desde un principio funciona como la <u>identidad</u> (ó el cero), i.e. para todo punto $P \in C_k$ se debe cumplir que: P + 0 = P.

Esta propiedad de + es inmediata de la definición de la

operación. En efecto, sea $\ell_{P,0}$ la recta que pasa por P y 0, y sea PO el tercer punto de intersección de $\ell_{P,0}$ con la curva C. Al tomar la recta $\ell_{0,PO}$ e intersectarla con C se obtiene el punto P + 0 que es precisamente P ya que las rectas $\ell_{P,0}$ y $\ell_{0,PO}$ son la misma. Ver fig. 3.

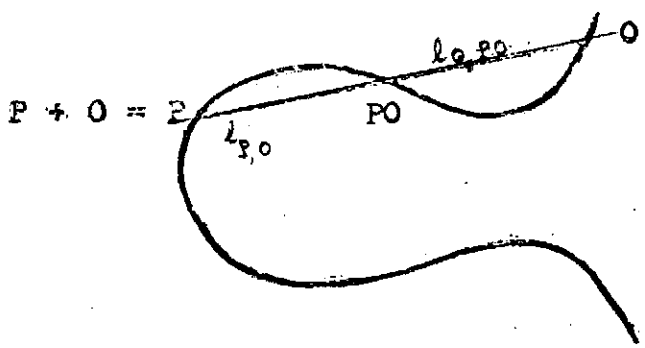


fig. 3

Debemos ahora probar que cada punto de C_k tiene un <u>inverso</u> (en C_k), i.e. dado $P \in C_k$ existe $Q \in C_k$ tal que $P + Q = 0$, ó bien que la ecuación $P + X = 0$ tiene solución en C_k.

Supongamos por un momento que la ecuación $P + X = 0$ tiene solución y llamemos a ésta Q. Geométricamente esto nos dice que la recta $\ell_{0,PQ}$ "pasa" dos veces por el punto 0 i.e. $\ell_{0,PQ}$ es tangente (con multiplicidad 2) a la curva en el punto 0. Ver fig. 4.

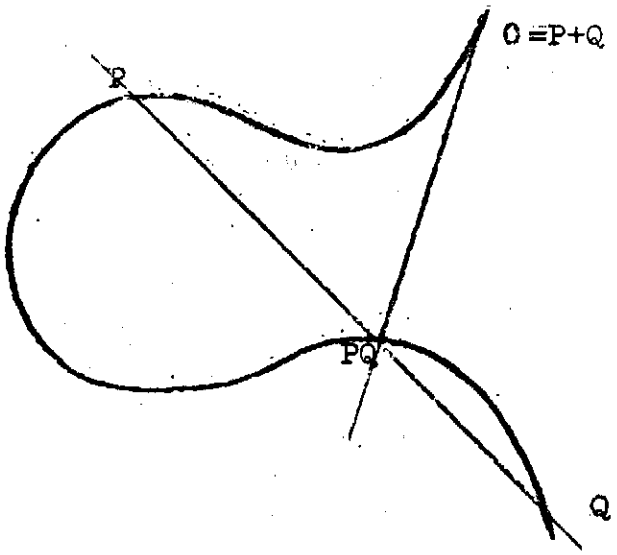


fig. 4

Entonces para obtener el inverso del punto $P \in C_k$ procedemos de la siguiente manera: tomemos una tangente ℓ_0 a la curva C en el punto 0 y llamemos S al tercer punto de intersección de ℓ_0 con C. La recta $\ell_{P,S}$ corta a C en un tercero punto Q.

Afirmamos que éste punto Q es el inverso de P, es decir que $P+Q=0$. En efecto, se tiene que $\ell_{P,Q} \cap C = \{S\}$ i.e. $PQ = S$. La recta $\ell_{0,PQ}$ es precisamente la recta ℓ_0. Como ℓ_0 pasa por 0 y S y es tangente a la curva C en el punto 0, se tiene que el tercer punto de intersección de $\ell_{0,PQ}$ con C es precisamente 0, lo cual implica que $P+Q=0$. Ver fig. 5.

Para concluir que $(C_k, +)$ es un grupo nos falta ver que la operación $+$ es <u>asociativa</u>.

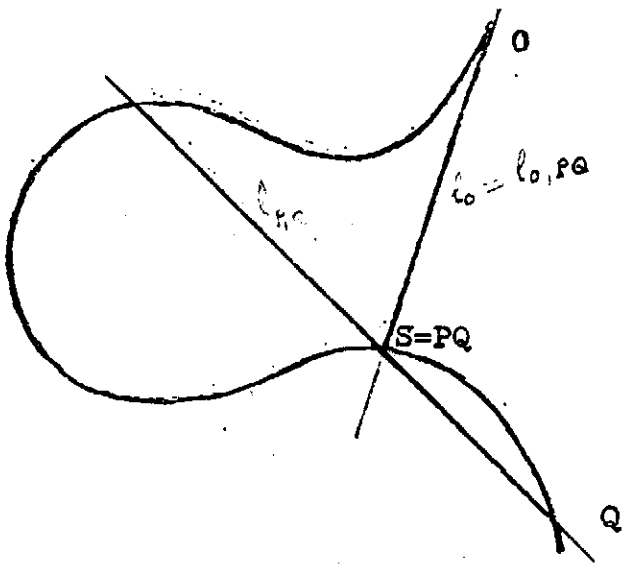


fig. 5

La demostración geométrica de la asociativdad de la operación es un poco mas complicada, en la cual usaremos un resultado básico de curvas cúbicas del cual se bosquejó la demostración en §1.

Para que la operación + sea asociativa se debe satisfacer: $(P+Q)+R = P+(Q+R)$ para todo $P,Q,R \in C_k$.

Sea $\ell_{P,Q}$ la recta que pasa por P y Q y sea PQ su tercer punto de intersección con la curva C. El punto $P+R$ es el tercer punto de intersección de la recta $\ell_{PQ,Q}$ con la curva. Para obtener el punto $(P+Q)+R$ tomese la recta $\ell_{(P+Q),R}$ y sea $(P+Q)R$ su tercer punto de intersección con C. Entonces $(P+Q)+R$ es el tercer punto de intersección de $\ell_{(P+Q)R,O}$ y C. De una manera similar se obtiene, primero el punto QR y así $Q+R$, en seguida $P(Q+R)$. y finalmente $P+(Q+R)$ (Ver fig. 6).

Para probar la asociatividad de la operación + , basta

ver que los puntos $(P+Q)R$ y $P(Q+R)$ son el mismo. En efecto, supongamos por un momento que $(P+Q)R = P(Q+R)$. Entonces las rectas $\ell_{(P+Q)R,0}$ y $\ell_{P(Q+R),0}$ coinciden. Así el tercer punto de intersección de la curva con cada una de las rectas es el mismo i.e. $(P+Q)+R = P+(Q+R)$ y la asociatividad de $+$ queda demostrada.

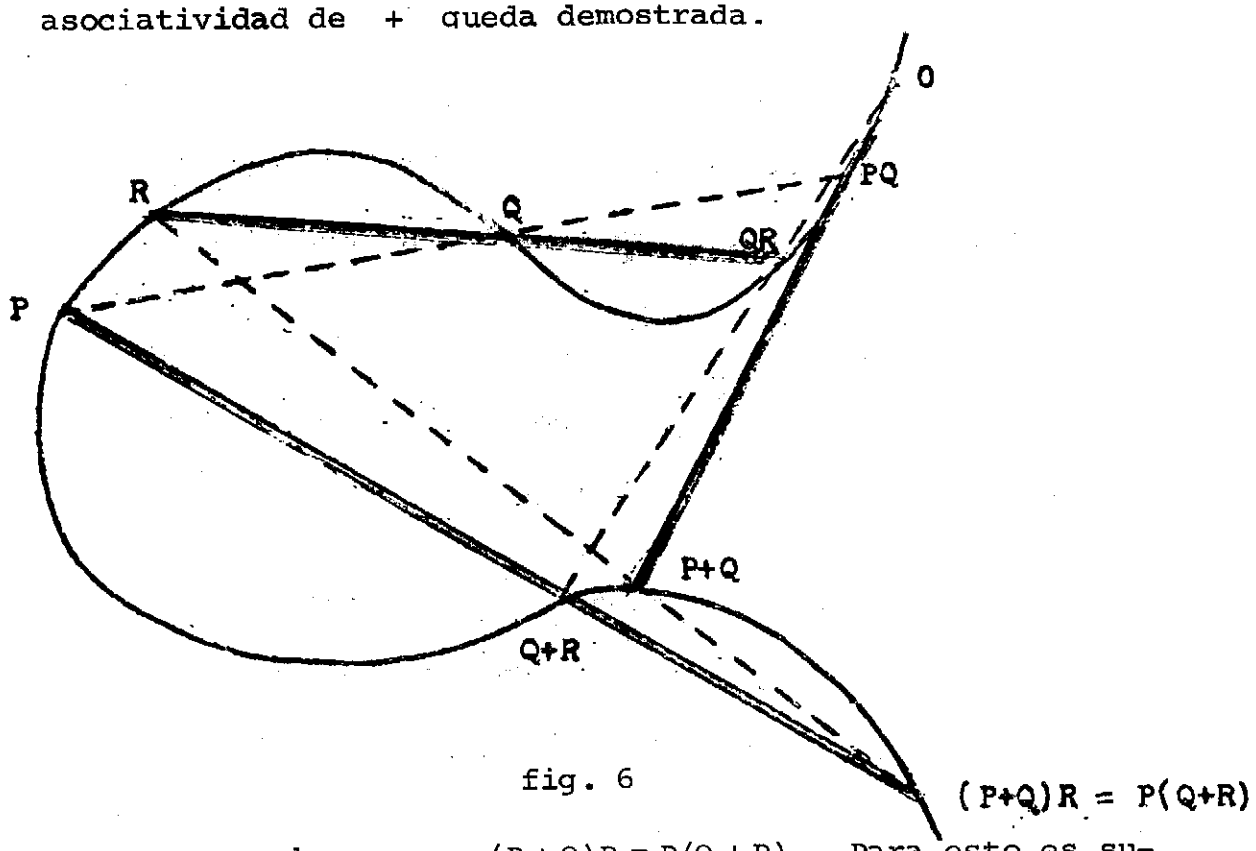


fig. 6

Veamos ahora que $(P+Q)R = P(Q+R)$. Para esto es suficiente ver que la intersección S de las rectas $\ell_{P+Q,R}$ y $\ell_{Q+R,P}$ está en la curva C. Obsérvese que cada uno de los 8 puntos $0,P,Q,R,PQ,P+Q,QR,Q+R$ están en una linea punteada y una linea gruesa. Ver fig. 6. Cada recta punteada está definida por una ecuación lineal las cuales al multiplicarlas se obtiene un polinomio cúbico que determina una curva cúbica degenerada C_1 (los puntos de C_1 son exacta-

mente los puntos de las 3 lineas). De una manera similar, las 3 lineas gruesas determinan una cúbica degenerada C_2. Por construcción las cúbicas C_1 y C_2 pasan por los nueve puntos $0,P,Q,R,PQ,P+Q,QR,Q+R,S$. (de los cuales los primeros 8 de ellos están en C). Aplicando el teorema de §1 a las curvas C_1, C_2 y C se sigue que el punto S está también en C. Entonces la intersección de las lineas $\ell_{P+Q,R}$ y $\ell_{Q+R,P}$ está en C y por lo tanto $(P+Q)R = P(Q+R)$.

De ésta manera concluimos que $(C_k,+)$ es un grupo. La conmutatividad de + es obvia de la misma definición de la operación.

Quisieramos concluir esta nota con algunas observaciones y algunas referencias. Enumerar todas las referencias que existen en la literatura sería prácticamente imposible y sólo mencionaremos algunas de ellas. [16] ha servido de base al autor para la presente nota y la cual recomendamos ampliamente.

Observaciones.

1) Se puede probar que C_k tiene estructura de grupo abeliano por un método más algebraico, usando geometría analítica, i.e. usando las ecuaciones de las rectas y de la curva explícitamente. Esperamos dar una demostración en una nota posterior, aunque el lector puede intentar probar el resultado

por éste método.

Se puede probar que si el polinomio que define a la curva cúbica C tiene coeficientes en un campo K algebraicamente cerrado y de característica distinta de 2 y 3 y C_K no es vacío, entonces C_K tiene estructura de grupo abeliano. Para una demostración de este resultado ver por ejemplo [15].

2) Las cúbicas han sido objeto de estudio de personajes como Wierstrass, Riemann, Abel, Jacobi, Gauss, Picard, Albanese y otros tantos más que sería imposible mencionar a todos, pero que han contribuido enormemente al desarrollo de una gran parte de la matemática.

Las curvas cúbicas además de ser objeto de estudio en algebra, lo son en varias otras ramas de la matemática como es la topología con la estructura topológica que se les puede dar, variable compleja (estructura de variedad compleja), geometría algebraica (estructura de variedad algebraica), topología diferencial (estructura de variedad diferencial), y otras más.

Por ejemplo en geometría algebraica han sido y siguen siendo objeto de estudio y han dado origen a varias teorías entre las que se pueden mencionar a la fascinante y extensa teoría de Curvas Elípticas (relacionada con integrales elípticas) (ver por ejemplo [15], [20], [22], [i], [ii]), y la no menos extensa y también atractiva teoría de Variedades Abelianas

(ver [24]). En variable compleja las cúbicas están ligadas con la teoría de Superficies de Riemann, (ver [10], [22]) en teoría de números con el famoso teorema de Fermat, etc.

A manera de ilustración mencionaremos dos resultados sobre curvas cúbicas relacionadas uno de ellos con variable compleja, geometría algebraica, topología y algebra, el otro con geometría algebraica, algebra y teoría de números.

1) Sea C una curva cúbica no-singular definida sobre el campo de los números complejos $\mathbb{C}$. Entonces existe una latice Λ en $\mathbb{C}$ tal que el grupo $C_{\mathbb{C}}$ de puntos $\mathbb{C}$-racionales de C es isomorfo al grupo $\mathbb{C}/\Lambda$. Además este isomorfismo es analítico.

2) Teorema de Mordell: Sea C una curva cúbica no-singular definida sobre $\mathbb{C}$. Si C tiene un punto $\mathbb{C}$-racional, entonces el grupo $C_{\mathbb{C}}$ de puntos $\mathbb{C}$-racionales de C es finitamente generado.

BIBLIOGRAFIA

Las siguientes son algunas referencias clásicas en la teoría de funciones elípticas y curvas elípticas.

1.- Abel, N.C. Recherches sur les fonctions ellíptiques Jour. für der Math. 2 (1827).

2.- Cayley, A. Elliptic functions. Cambridge 1876.

3.- Euler, L. Leonhardi Euler: Omnia Opera Leipzig, 1912.

4.- Gauss, C.F. Disquisitiones Arithmeticae (english trans.) Yale Univ. Press, New Haven, 1966.

5.- Jacobi, C.G.J. Fundamenta nova functionarum ellipticarum. Ges. Math. Werke 1 (1881).

6.- Jacobi, C.G.J. Gesammelte Werke, erster Band Chelsea Publ. Co. N.Y. 1969.

7.- Picard, E. Quelques applications analytiques de la théorie des curbes et des surfaces algebriques. Gaulthier-Villars et cie. Paris 1931.

8.- Riemann, G.F.B. Gesammelte mathematische Werke Aufl. Leipzig 1892.

9.- Weierstrass, K. Rationale functionen des Paares (x,y). Werke, Vol. iv, Berlin, 1902.

Con un tratamiento más moderno de las curvas elípticas y teoría de curvas en general, se puede mencionar los siguientes textos los cuales son bastante accesibles.

10.- Ahlfors, L. Complex analysis Cap. 7, 2a ed. Mc. Graw-Hill.

11.- Cartan, H. Théorie élémentaire des functions analytiques d' une ou plusieurs variables complexes. Hermann, Paris, 1961.

12.- Hancock, H. Theory of elliptic functions, Dover Publ. Inc. N.Y. 1958.

13.- Fulton, W. Algebraic curves. Benjamin Inc. N.Y. 1969.

14.- Coolidge, J.L. A treatise on algebraic plane curves. Dover Publ. Inc. N.Y. 1959.

15.- Robert, A. Elliptic curves . Lect. Notes in Math Vol. 326 Springer-Verlag.

16.- Tate, J. Rational points on elliptic curves. Coll. Lect. Notes Darthmouth College. Summer 1972.

17.- Seidenberg, A. Elements of the theory of algebraic curves. Addison-Wesley, 1968.

18.- Mumford, D. Introduction to algebraic geometry. Harvard Lect. Notes (red book).

19.- Shafarevich, I. Basic algebraic geometry Springer-Verlag 1974.

20.- Walker, R.J. Algebraic Curves. Dover Publ. Inc. N.Y. 1950.

21.- Hodge, W.V.D. and Pedoe, D. Methods of algebraic Geometry, Cambridge Univ. Press 1968.

Las siguientes referencias son más especializadas y requieren de un conocimiento previo de algunos temas en Geometría Algebraica.

22.- Gunning, R.C. Lectures on Riemann surfaces. Math. Notes, Princeton Univ. Press, N.J. 1972.

23.- Lang, S. Elliptic functions. Addison-Wesley Publ.

24.- Mumford, D. Abelian Varieties. Oxford Univ. Press.

25.- Patrick Du Val. Elliptic functions and elliptic curves. Cambridge Univ. Press 1973.

Existe en la literatura un número considerable de artículos de investigación sobre curvas elípticas y temas afines. Nosotros sólo mencionaremos dos de ellos y recomendamos la extensa bibliografía que tiene cada uno de éstos artículos.

(i) Cassels, J.W.S. Diophantine equations with special reference to elliptic curves. Survey article. Jour. London Math. Soc. 41, 1966 pag. 193-291.

(ii) Tate, J.T. The arithmetic of elliptic curves. Inventiones Math. Vol. 23, 1974 pag. 179-206.