Vo.Bo. (f)

Doctor Juan Escamilla
Asesor

Tribunal: (f)

Doctor Juan Escamilla

(f)

Doctor Raúl B. González

(f)

Lic. Roberto Molina

Fecha de aprobación: 12 de junio de 1990

CONTENIDO

I. INTRODUCCION

El presente trabajo fue desarrollado durante y después de los cursos de Investigación en Matemática I y II, que fueron impartidos por el doctor Juan Escamilla en 1989.

Es un trabajo de graduación y trata fundamentalmente sobre álgebra, pero tiene conceptos de geometría algebraica, teoría de números, geometría y teoría de Galois. La tesis es mostrar la relación existente entre grupos y las áreas antes mencionadas.

Aparte de la Introducción Histórica, el trabajo consta de tres temas; el primero es de curvas sobre los racionales, el segundo es sobre teoría de números y el método de Fermat y el último es sobre la teoría de Galois. En todos estos capítulos se ha introducido el concepto de conjuntos algebraicos. También existen otras relaciones menos evidentes que las ya descritas, por ejemplo el primero y el segundo capítulo se relacionan entre sí por las ternas pitagóricas y el último teorema de Fermat; el tercero y el segundo, por la resolución de las ecuaciones cúbicas. Todo esto hace que el trabajo pertenezca a lo que hoy en día se conoce como algebrización de la matemática.

Los teoremas más importantes del trabajo son la caracterización de los grupos de Galois de los polinomios de segundo, tercero y cuarto grado, también la estructura de grupo de los números racionales de una curva elíptica y la demostración en base a ideales del teorema de Fermat.

Agradezco a la licenciada Rocío Marbán, del ICAITI, por permitirme usar la computadora para mecanografiar el manuscrito, y al doctor Juan Escamilla su atención y sus ideas aportadas luego de leer el manuscrito.

II. RESEÑA HISTORICA

Al igual que la teoría de números, la geometría algebraica tiene la particularidad de poseer una larga historia y que a su vez es muy desconocida.

Pretendemos en las siguientes páginas describir brevemente el desarrollo histórico de la geometría algebraica.

Contrario a la creencia muy difundida del surgimiento independiente de la geometría y el álgebra, éstas surgen en Grecia pero dependen la una de la otra pues los griegos usaron el álgebra para resolver problemas geométricos. También es conocida la multitud de problemas que se resuelven por regla y compás que no fue aclarado sino hasta el siglo XIX. La geometría en Grecia puede denominarse como geometría sin coordenadas. El concepto de coordenadas lo introdujo Descartes en el siglo XVII y se trata de que los mismos ejes sirven para describir todas las curvas que intervienen en un problema dado.
Con esto surge el concepto de curvas algebraicas y curvas trascendentales y Fermat logra introducir el concepto de dimensión, pues dice que una simple ecuación en dos dimensiones define una curva y en tres una superficie. También a finales del siglo XVII se supo que el concepto de grado es invariante al cambio de coordenadas. Euler, en el siglo XVIII aporta el concepto de curva paramétrica y clasificó las cónicas como intersección de dos superficies. Newton y Leibniz trabajaron en el problema de la intersección de dos curvas algebraicas planas e intro-

dujeron el concepto de proceso de eliminación cuya idea es que dos curvas algebraicas tienen una raíz en común. Usando este proceso, en 1780 Newton notó que las absisas de los puntos de intersección de dos curvas de grados m y n respectivamente surgen de una ecuación de grado menor o igual que mn. Esta fue la base para que Bézout desarrollara el concepto de proceso de eliminación y multiplicidad, esto en el siglo XVIII. También nació la geometría proyectiva, cuando Desargues trató de darle un fundamento matemático a las perspectivas artísticas de los pintores. Fue Desargues quien en el siglo XVII contribuyó con el concepto de punto en el infinito. En este siglo Euler, formuló la existencia de puntos imaginarios y con esto dos círculos se intersectan en cuatro puntos al igual que dos cónicas cualesquiera .

Con estas nuevas herramientas ya se cuenta con casi todas los conceptos necesarios para hablar de un campo algebraicamente cerrado y del plano proyectivo complejo P(C).

Móbius , Plúcker y Cayley sentaron las bases para lo que fue posteriormente el programa de Erlangen de Klein. Además con ellos se desarrolló la teoría de correspondencias.

Se llama una (α, β) correspondencia a una relación entre dos puntos M y M' ,tales que para cada punto M existen α puntos M' relacionados con M y para cada punto M' existen β puntos relacionados con M , cuando M y M' varían en la misma línea proyectiva.

En general, la geometría algebraica se había ocupado por problemas netamente enumerativos (en P(C)) tales como por ejemplo : Cuál es el número de cónicas tangentes a 5 cónicas dadas en posición cualquiera?

Esta escuela, la llamada geometría algebraica proyectiva culminó con los trabajos de Plücker, quien con sus fórmulas encontró una relación entre el grado de una curva, su clase, sus puntos dobles, etc.

Por los trabajos de Cauchy sobre variables complejas, se creía más o menos en 1850 que la geometría algebraica era parte del análisis complejo . Riemann aportó mucho de lo que es el análisis y la topología a la geometría algebraica; él es el creador de las funciones multiformes basado en la teoría de superficies de Cauchy para la resolución de integrales abelianas. Lo interesante aquí es que nació la geometría birracional, cuya idea central es la siguiente: Dada una variedad irreducible V se define en ella un campo de funciones de las 0-formas que ella genera y luego se estudian los isomorfismos en estos campos que definen equivalencias birracionales. El concepto de variedad irreducible se debió a Kronecker o a Dedekind. También trabajando con las ideas de Riemann, Dedekind y Weber utilizaron los elementos integrales sobre un anillo de polinomios y para ésto usaron la teoría de ideales que desarrolló Dedekind en 1870. Nuevamente se le dió un enfoque algebraico abstracto, pues la teoría de ideales es parte del álgebra conmutativa. Castelnuovo , Enriques y Severi al introducir el álgebra lineal ,relacionan con sistemas lineales las subvariedades y los divisores de campos racionales, ellos son los padres de la escuela italiana de geometría algebraica.

En la década de los veinte deeste siglo existió una corriente por tratar de generalizar la matemática por medio de estructuras. La estrecha rela-

ción entre variedades algebraicas y variedades complejas por un lado y por el otro los números algebraicos se habían vuelto conceptos fundamentales en la geometría algebraica. En estos tiempos (1920) se dió mucho énfasis a la noción de estructura y quedaron relegados a un segundo plano los objetos matemáticos sobre los que se definió la estructura.

Consecuencia lógica de esto es que se pensara en una extensión abstracta de la geometría algebraica, donde tanto los coeficientes de las ecuaciones ,así como las coordenadas pertenecen a cualquier campo arbitrario. Estos trabajos se deben a E. Noether, W. Krull y van der Waerden hasta antes de 1940 y posteriormente a Zariski y a Weil. Por ejemplo, la descomposición en ideales primarios sobre anillos noeterianos, las propiedades de los anillos íntegros cerrados y la noción de localización se debió a Noether.

(Un anillo local es un anillo conmutativo en donde sólo existe un ideal maximal. El ejemplo típico de anillo local es el siguiente:

$A_P = \{ \frac{f(x)}{g(x)} \in C(x) \mid g(P) \neq 0 \}$ donde $C(x)$ es el conjunto de las funciones racionales sobre el campo de los complejos C .Y el ideal maximal es $M = \{ f(x) \in A \mid f(P) = 0 \}$.

En estos años Zariski desarrolló su topología y van der Waerden y Weil, el concepto de punto genérico de una variedad. A partir de 1945 Leray introdujo al álgebra conceptos como haces, cuyo origen procede de la topología algebraica y ha dado lugar a muchos problemas en la que los geómetras algebraicos trabajan hoy en día. Por ejemplo el problema de la desingularización o el problema del moduli de Riemann que consiste en probar la existencia de una variedad o esquema cuyos

puntos deben corresponder a unas clases de isomorfismo de curvas cuyo género se conoce. Está todavía incompleto el estudio de las integrales abelianas de segundo y tercer tipo que es un tema de la geometría algebraica clásica. También queda mucho por hacer en la caracterización de clases de superficies por propiedades de sus invariantes pero generalizado a un campo algebraicamente cerrado de característica $p>0$. Estos trabajos los comenzaron los matemáticos italianos Castelnuovo y Enriques.

A mediados de la década de los cincuentas, utilizando el concepto de anillos de funciones, A. Grothendieck logró una definición más abstracta y general que el concepto de variedad algebraica, que fué el concepto de esquema.

III. CONJUNTOS ALGEBRAICOS Y SUS PROPIEDADES

El estudio principal de la geometría algebraica son las variedades y los conjuntos algebraicos que también es el tema central de este capítulo. Un grupo es un conjunto G con una operación (llamada producto interno) que asocia a cada par ordenado (a,b) de elementos de G un elemento ab de G de tal forma que:

- Para tres elementos cualesquiera a, b, $c \in G$ (ab)c = a(bc);
- Existe un único elemento $e \in G$ tal que ea = a = ae para todo elemento $a \in G$;
- Para todo elemento $a \in G$ existe un elemento $\bar{a}^{1} \in G$ tal que $a \cdot a^{-1} = e = \bar{a}^{1} \cdot a$

De forma más precisa, un producto interno debería considerarse como una aplicación $\varphi : G \times G \rightarrow G$, y el grupo debería representarse como (G, φ) para hacer patente el papel del producto. Esto sirve para diferenciar grupos que tienen el mismo conjunto pero diferente producto interno.

Un anillo es un conjunto R con dos operaciones internas que representaremos por + y • de modo que :

- (R,+) es grupo abeliano
- la multiplicación es distributiva con respecto a la suma; es decir, cualesquiera que sean los elementos de a,b, $c \in R$

  $a(b + c) = ab + ac$ y $(a + b)c = ac + bc$;
- es asociativa; es decir, dados tres elementos cualesquiera $a,b,c \in R$

  $a(bc) = (ab)c$;

si además el producto es conmutativo el anillo se llamará conmutativo, y si existe un elemento unidad $1 \in R$ tal que $1 \cdot a = a = a \cdot 1$ para todo a R el anillo se llamará anillo unitario o con unidad.
Cuando nos refiramos a anillo, todo anillo será conmutativo y tendrá elemento unidad.

En un anillo no trivial un elemento no nulo a puede tener un inverso multiplicativo, es decir, puede existir un elemento a^{-1} tal que $a\,a^{-1} = 1 = a^{-1}a$. Este elemento se denomina unitario del anillo. Un elemento no nulo que no tiene inverso multiplicativo se llama elemento propio. Así, los elementos de qualquier anillo se dividen en tres clases: el cero, los unitarios y los elementos propios.
Un campo es un anillo no trivial en el que todo elemento no nulo es unitario.

Un elemento a de un anillo R es un divisor de cero si ab=0 para algún elemento b no nulo que pertenezca a R.
Un dominio de integridad es un anillo que no tiene divisores de cero (salvo el propio cero). Un campo es un dominio de integridad.
Si Z es el anillo de los enteros el conjunto de las clases de congruencias módulo n forman un anillo con la suma

$$[a]_n + [b]_n = [a+b]_n \text{ y la multiplicación } [a]_n\,[b]_n = [ab]_n$$

Un ideal de un anillo R es un subgrupo aditivo $\mathcal{Q}$ de R con la propiedad de que si $a \in \mathcal{Q}$ implica $ra \in \mathcal{Q}$ para todo $r \in R$.

Evidentemente, el conjunto que sólo contiene al elemento 0 y el conjunto formado por todo el anillo R son ideales, llamados los ideales triviales o banales.

Un ideal se llama propio si $\mathfrak{a} \neq (0)$ y $\mathfrak{a} \neq R$.

Para todo elemento a de un anillo R , el conjunto

$(a) = \{ x \in R \mid x = ra \ , \ r \in R \}$ es un ideal, llamado ideal principal generado por a.

Los dominios de integridad en los que todo ideal es principal tienen una importancia excepcional en la teoría de anillos. LLamamos, en forma abreviada, a estos dominios de integridad, dominios de ideales principales.

Un dominio euclidiano es un dominio de integridad no trivial R junto con una función, llamada norma, $\varphi : R^* \to N$ (donde R^* significa R - {0}) tal que:

- para todo $a,b \in R^*$, $\varphi(ab) = \varphi(a) \cdot \varphi(b)$,
- para todo $a,b \in R^*$ existen unos elementos $q,r \in R$ tales que $a = qb + r$ siendo $r < b$ o $r = 0$.

Una factorización $r = r_1 r_2 \ldots r_k$ de un elemento r de un anillo R es una factorización propia si todo factor r_i es un elemento propio (no unitario ni nulo) de R. La factorización que contiene algún elemento unitario o nulo entre sus factores se denomina impropia. Todo elemento de un anillo tiene una factorización impropia $r = 1r$, pero no todos los elementos tienen una factorización propia.

Se denominan primos los elementos de un anillo que no tienen factorización propia. Un elemento propio que es primo se llama primo propio.

Como ejemplos de anillos interesantes están Z(i) y Z(w).

Z(i) es el anillo de los enteros gaussianos y se define así:

$Z(i) = \{ a + bi \mid a , b \in Z \}$, donde $i = \sqrt{-1}$. La suma y la multiplicación quedan definidas de la siguiente forma :

$$(a + bi) + (c + di) = (a+c) + (b+d)i$$

$$(a + bi) (c + di) = (ac - bd) + (ad + bc) i$$

Z(i) tiene características importantes que son por ejemplo:

- Z(i) es un dominio euclidiano con la norma $\delta : Z(i)^* \to N$

  $\delta(a + bi) = a^2 + b^2$

- Z(i) es un anillo de factorización única

- Z(i) es un anillo de ideales principales

Los elementos unitarios de Z(i) son $\pm i$ y ± 1. Los elementos primos de Z(i) se llaman primos gaussianos.

Sea $w = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ y $Z(w) = \{ a + b w \mid a , b \in Z \}$.

w es una de las raíces del polinomio $z^2 + z + 1$.

Z(w) tendrá estructura de anillo con la suma y la multiplicación definidas de la siguiente manera:

$$(a + bw) + (c + dw) = (a+c) + (b +d)w$$

$$(a+bw) (c+dw)= (ac + bd) + (ad + bc -bd)w$$

Es fácil ver que $\overline{w} = w^2 = -1 - w$

Z(w) también es un dominio euclidiano con la norma :

$\delta : Z(w) \to N$

$\delta(a + bw) = a^2 - ab + b^2$

Z(w) es también un dominio de ideales principales y un dominio de factorización única , y sus unitarios son $\pm 1, \pm w , \pm w^2$.

Los elementos $z = a + bw$ que no se pueden escribir como $z = r_1 \ldots r_n$ tal que r no sea un unitario se llaman primos en Z(w). Así $1 - w$ es primo de Z(w) ya que un elemento $a + bw$ Z(w) es primo de Z(w), ssí su norma a^2-ab+b^2 es un elemento primo de Z (referencia [2]).

Dos elementos de un anillo son asociados si cada uno de ellos puede expresarse como producto del otro por un unitario.

Sea K un campo. El conjunto de las n-eadas $(x_1,\ldots,x_n)$ de elementos de K se llama el n-espacio afín sobre K y por conveniencia lo denotamos por K^n Cada $(x_1,\ldots, x_n)$ se llama punto del espacio afín. Y por simplicidad, un punto $(x_1,.\quad x_n)$ del espacio afín lo denotaremos por (x).

Al anillo de polinomios con coeficientes en K y con n indeterminadas lo denotaremos por $K[X_1,\ldots, X_n]$ y un polinomio se denotará por P(X).

Si F $K[X_1,..,X_n]$ un punto $P=(a_1 \ldots. a_n)$ K^n es un cero de F si $F(P) = F(a_1\ldots. a_n)= 0$.

Si F no es un polinomio constante, el conjunto de ceros de F se llama la hipersuperficie definida por F. Y se denota por V(F).

Si E $K[X_1.. X_n]$; al conjunto V(E) = { (x) K 1 P(x) = 0 para todo P E } se le llama conjunto algebraico afín de K . 0 , por simplicidad, sólo conjunto algebraico.

Dicho brevemente, un conjunto algebraico es el conjunto de ceros comunes a una colección de polinomios.

Citemos ahora algunos ejemplos:

- Las variedades lineales. Estas son el conjunto solución de sistemas de ecuaciones lineales con coeficientes en K^2. El estudio de estas variedades forma parte del álgebra lineal.

- Curvas Algebraicas Planas que son las hipersuperficies en K^2.

Así si $K = R$ y $f = aX^2 + bX\,Y + cY^2 + dX + eY + f$ con $a,b,\ldots f \in R$ una forma cuadrática

- $V(aX^2 + bXY + cY^2 + dX + eY + f)$ con $a, \ldots, f \in R$ es una curva en R por lo que los círculos, las parábolas, las elipses, etc pueden ser vistas como variedades algebraicas afines del R .

La variedad $V(Y^2 - X^3)$ es la curva "cúspide" o parábola de Neil, su gráfica se muestra en la figura 1.

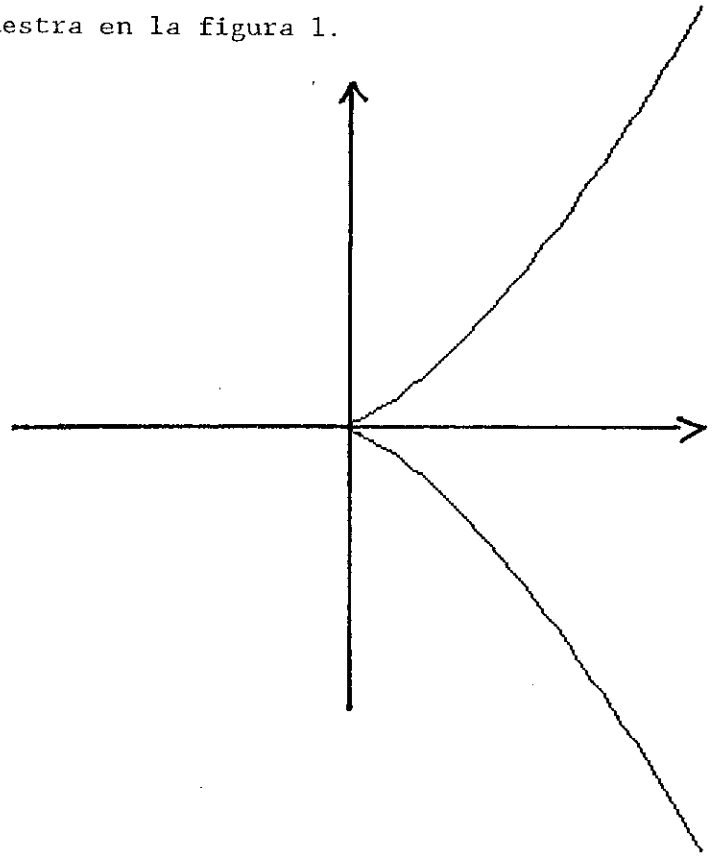


figura 1

-- La variedad $V(Y^2 - X^2(X + 1))$ es la curva "alfa" y su gráfica se muestra en la figura 2

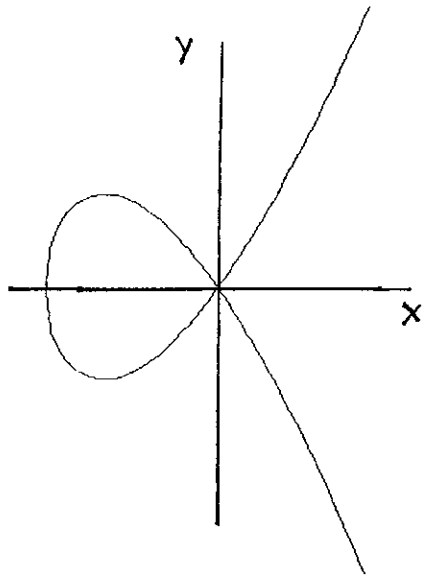


figura 2

-- La variedad $V(Y^2 - X(X^2 - 1))$ es una curva elíptica . Este ejemplo muestra que las curvas algebraicas en R no tienen por que ser conexas.

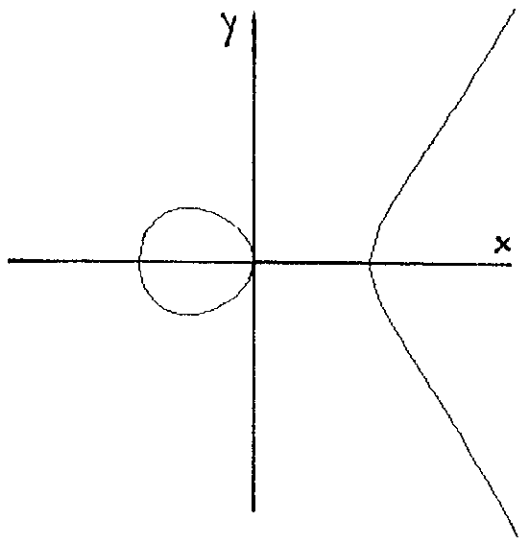


figura 3

La variedad $V[(X^2+Y^2-1)\ (X^2+Y^2-4\ )]$ define la unión de dos círculos concéntricos.

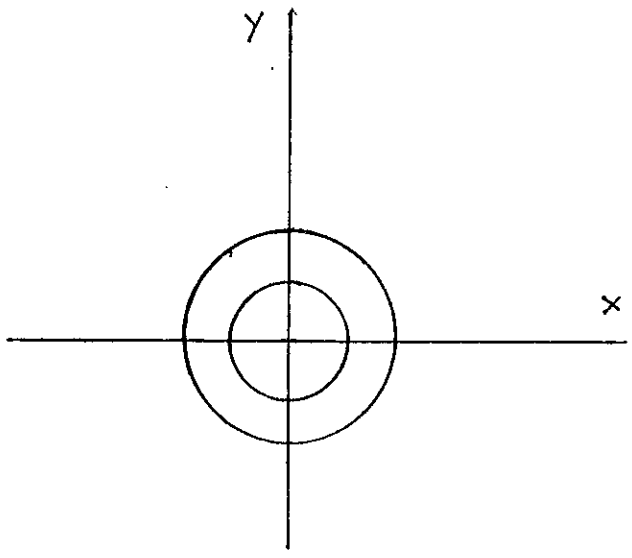


figura 4

<u>Puntos racionales de una variedad algebraica.</u> Sea $V \subset K^h$ una variedad y $L \subset K$ un subanillo de K. Interesa saber si existen puntos de V con coordenadas en L.

La variedad $V' = V\ (Y - X^2)$ define una parábola en R^2 y $\tilde{V} = V\ (Y - X^2)$ define también una parábola en Q^2.

$\tilde{V}$ es densa en V.

En efecto, sea (r, r^2) un punto de V' queremos ver si podemos encontrar un punto (q, q^2) tan cerca como se quiera de (r, r^2), con $q \in Q$. Consideremos el intervalo $(r^2 - \sqrt{\varepsilon/2}\ ,\ r + \sqrt{\varepsilon/2})$ como $f(x) = x^2$ es continua existe un $\delta > 0$ tal que $f[(r-\delta\ ,\ r+\delta\ )] \subset (r^2 - \sqrt{\varepsilon/2}\ ,\ r^2 + \sqrt{\varepsilon/2}\ )$, tomando $\delta' = \min(\delta\ \sqrt{\varepsilon/2}\ )$, podemos encontrar $q \in (r - \delta'\ r + \delta')$, tal que $(q, q^2) \in B_\varepsilon\ (r, r^2)$. En efecto $(q-r)^2 + (q^2 - r^2)^2 < \delta'^2 + \frac{\varepsilon}{2} < \varepsilon^2$.

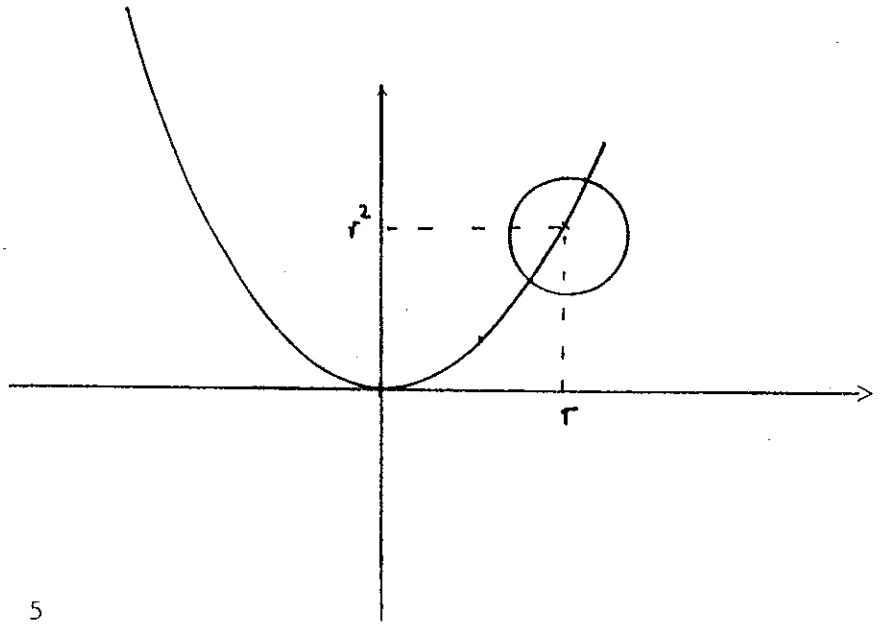


figura 5

El círculo racional.

La variedad $V(X^2 + Y^2 - 1)$ define un círculo en R^2. Siendo $Q \subset R$ subcampo de R, interesa saber cómo es la gráfica de $V(X^2 + Y^2 - 1)$ en Q^2. Vamos a demostrar que este conjunto es denso en $V(X^2 + Y^2 - 1)$ en R^2.

Sea $(r, s) \in V(X^2 + Y^2 - 1) \subset Q^2$ podemos suponer sin pérdida de generalidad que r y s tienen el mismo denominador.

Escribimos $r = \frac{a}{c}$ $\quad s = \frac{b}{c}$.

Luego, $r^2 + s^2 = 1$ implica que $a^2 + b^2 = c$, donde se podrán encontrar enteros u , v tales que $\frac{a}{c} = \frac{v^2 - u^2}{u^2 + v^2}$ $\quad \frac{b}{c} = \frac{2uv}{u^2 + v^2}$

La cuestión de que si el conjunto de puntos $(r , s) = (\frac{a}{c}, \frac{b}{c})$ es denso en el círculo real, es equivalente a responder la siguiente cuestión

Podemos aproximar la pendiente $\frac{a/c}{b/c} = \frac{a}{b} = \frac{v^2 - u^2}{2uv}$ tan

cerca como se quiera a alguna pendiente $m \in R$?

Dado m un real no racional, y $\varepsilon > 0$ cualquiera, existe un racional de la forma $\frac{v^2 - u^2}{2uv} = r$ tal que $r \in B_\varepsilon(m)$.

Consideremos:

$$\frac{v^2 - u^2}{2uv} - m$$

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

$$\frac{1}{2}\left(x - \frac{1}{x} - 2m\right)$$

$$\frac{1}{2}\left(x^2 - 2mx - 1\right) = \frac{1}{2x}(x - q_1)(x - q_2) < \frac{1}{2x}\varepsilon$$

Las raíces del polinomio $z^2 - 2mz - 1$ son $m + m^2 + 1$

(este polinomio posee siempre una raíz positiva q_1 y una negativa q_2)

x es un racional cualquiera $\frac{v}{u}$ $u, v \in Z$.

Para ε lo suficientemente pequeño $\exists$ un racional $x \in B_\varepsilon(q_1)$ y $x > q_1$

si escogemos ε tal que $0 < \varepsilon < 1/10$.

$\frac{v^2 - u^2}{2uv} - m = 1/2\,(x^2 - 2mx - 1) = 1/2x\,(x - q_1)(x - q_2) < 1/2q_1\varepsilon(q_1 - q_2 + \frac{1}{10})$

por lo que m puede ser aproximado por un racional de la forma $\frac{v - u}{2uv}$.

en el grado que se quiera.

Y como último ejemplo citaremos el problema de Fermat; que se ocupa de la existencia de las soluciones no triviales de puntos racionales de las variedades $V(X^n + Y^n - 1)$ en Q^2. La variedad $V(X^n + Y^n - 1)$ no tiene soluciones no triviales en Q^2, según Fermat.

Estudiaremos el caso para $n = 3$ i.e. $V(X^3 + Y^3 - 1)$ en los racionales.

Si X y Y son racionales podemos suponer sin pérdida de generalidad que tienen el mismo denominador y el problema se transforma en demostrar que $X^3 + Y^3 = Z^3$ no tiene soluciones en Z.

Demostraremos algo más: que $X^3 + Y^3 = Z^3$ no tiene soluciones en Z(w). Supongamos que X, Y ,Z son tres elementos no nulos de Z(w), tales que

$$X^3 + Y^3 = Z^3$$

Evidentemente no hay nada que nos impida suponer que X, Y y Z son primos relativos dos a dos, que expresado en términos de ideales, es:

$$(X,Y) = (Y,Z) = (Z,X) = (1) = Z(w).$$

En efecto , si dos de las tres cantidades X, Y y Z tienen un máximo común divisor d que no es unitario, toda la ecuación puede dividirse por d^3 y (X/d), (Y/d) (Z/d) , podría ser una solución que cumpliría la hipótesis. Observemos que 1-w tiene la norma

$$1-w = (1-w)(1-\bar{w}) = (1-w)(1-w^2) = 3$$

Y que por tanto es primo en Z(w). Además su complejo conjugado es

$$1-w = 1 - w^2 = w^3 - w^2 = w^2(w-1) = -w^2(1-w).$$

Al ser $-w^2$ un elemento unitario, 1-w y 1-w son asociados. En consecuncia si 1-w divide a $\alpha \in Z(w)$, 1-w también divide a $\bar{\alpha}$, complejo conjugado de α . Observemos que todo elemento de Z(w) es congruente con 0,1 ó 2 módulo (1-w): dado $a+bw \in Z(w)$, tenemos $a+b = 3q + r$ donde $0 \leq r < 3$ y

$$a + bw \equiv a+b \equiv 3q + r \equiv r \text{ mód.}(1-w).$$

(Por supuesto que 2=-1 módulo (1-w), ya que 1-w divide a 3.)

Finalmente señalemos que $\alpha = \pm 1$ módulo (1-w) implica que $\alpha^3 = \pm 1$ mód(1-w)

Para ver esto, escribimos $\alpha \equiv \pm 1 + \beta\,(1-\omega)^{\lambda}$ y entonces :

$$\alpha^3 \mp 1 = (\alpha \mp 1)(\alpha \mp \omega)(\alpha \mp \omega^2)$$
$$= \beta(1-\omega)^{\lambda}(\beta(1-\omega)^{\lambda} \pm 1 \mp \omega)(\beta(1-\omega)^{\lambda} \pm 1 \mp \omega^2)$$

y si $\lambda = 1$

$$\alpha^3 \mp 1 = (1-\omega)^{\lambda+2}\,\beta(\beta \pm 1)(\beta \pm (1+\omega))$$

Una de las tres cantidades β , $\beta + 1$ y $\beta + (1+w)$ debe ser divisible por 1 - w. Por tanto, $\alpha^3 \mp 1$ es divisible por $(1-\omega)^{\lambda+3}$.

La aritmética de Z(w) es de suma importancia, ya que precisamente en Z(w) es donde la ecuación $X^3 + Y^3 = Z^3$ tiene la factorización

$$X^3 + Y^3 = (X + Y)(Xw + Yw^2)(Xw^2 + Y w).$$

los tres factores $(X + Y)$, $(Xw + Yw^2)$, $(Xw^2 + Y w)$ son todos ellos congruentes módulo(1-w) y su suma es nula, puesto que $1 + w + w^2 = 0$. Además si los tomamos dos a dos, arbitrariamente, serán primos relativos, o bien tendrán 1-w como máximo común divisor, como se deduce de las ecuaciones siguientes:

$$1-w = \begin{cases} (V - Uw)(X+Y) + w^2(V-U)(Xw + Yw^2) \\ (Vw - U)(Xw + Yw^2) + (Uw - V)(Xw^2 + Yw) \\ w^2(V-U)(Xw^2 + Yw) + (U - Vw)(X + Y) \end{cases}$$

donde $UX + VY = 1$.

Una de las tres cantidades X, Y, Z tiene que ser divisible por el elemento primo 1-w. De lo contrario tendríamos que X Y y Z son congruentes con $\pm$1módulo (1-w), de donde deduciríamos que X^3 , Y^3 y Z^3 serían congruentes con +1 módulo $(1-w)^4$. Luego, $X^3 + Y^3 = Z^3$ implicaría :

$$\pm 1 \pm 1 = \pm 1 \text{ mód}(1-w)^4,$$

que nos lleva a las congruencias imposibles:

$$0 \equiv \pm 1 \text{ mód.}(1-w)^4 \qquad \text{y} \quad \pm 2 \equiv \pm 1 \text{ mód.}(1-w)^4.$$

Además podemos cambiar siempre la notación para estar seguros de que es Z quien es divisible por 1-w. Ya que $X^3 + Y^3 = Z^3$ es equivalente a las ecuaciones $X^3 + (-wZ)^3 = (-wY)^3$ e $Y^3 + (-Z)^3 = (-wX)^3$

Entre todas las soluciones no triviales de $X^3 + Y^3 = Z^3$ en Z(w) para las que 1-w divide a Z, debe existir una tal que 1-w divida a Z un número de veces tan pequeño como sea preciso. Podemos resumir lo conseguido hasta aquí en la siguente proposición.

Si la ecuación $X^3 + Y^3 = Z^3$ tiene una solución no trivial en Z(w), entonces debe tener una solución no trivial tal que:

1) X, Y, Z sean primos relativos dos a dos;

2) 1-w divide a Z;

3) existe un número $\lambda \in \mathbb{N}$ tal que $(1-w)^\lambda$ es divisor de z ; pero $(1-w)^{\lambda+1}$ no.

4) en cualquier otra solución con las propiedades 1) y 2) $(1-w)^\lambda$ divide a Z.

Vamos a demostrar que, dada una solución mínima de este tipo, podemos encontrar otra para la que Z sea divisible sólo por $(1-w)^{\lambda-1}$, lo que estaría en contradicción con 4).

Sea X, Y y Z una solución no trivial de $X^3 + Y^3 = Z^3$ que satisface las condiciones 1) a 4). Entonces Z = módulo(1-w) implica que

$$X + Y = Xw + Yw^2 = Xw^2 + Yw = 0 \text{ mód.}(1-w),$$

y tenemos $X + Y = (1-w)\,A$, $Xw + Yw^2 = (1-w)\,B$, y $Xw^2 + Yw = (1-w)\,C$, donde $A, B, C \in Z(w)$ y $A + B + C = 0$. Además, puesto que

$$(X+Y, Xw + Yw^2) = (Xw + Yw^2, Xw^2 + Yw) = (X^2 + Yw, X+Y) = (1-w),$$

se deduce que

$$(A,B) = (B,C) = (C,A) = (1).$$

Dicho de otra forma, las cantidades A, B y C son primos relativos dos a dos. Por otra parte, tenemos $(Z/(1-w))^3 = ABC$, y la única factorización en Z(w) implica que A, B, C son elementos asociados de potencias cúbicas, esto es,

$$A = \alpha \zeta^3 \qquad B = \beta \eta^3 \qquad C = \gamma \theta^3 \ ,$$

donde α , β , γ son elementos unitarios de Z(w) y ζ , η y θ son primos relativos dos a dos. Tenemos que $\alpha\beta\gamma = (z/(1-w)\zeta\eta\theta)^3$ es, al mismo tiempo, unitario y cúbico en Z(w) . Puesto que los elementos unitarios de Z(w) son precisamente las seis raíces de la unidad, se deduce que $\alpha\beta\gamma = \pm 1$. Sabemos que 1-w divide a X + Y pero no a X o Y. Por tanto :

$$X = +1 \text{ mód.}(1-w), \qquad Y = -X \text{ mód.}(1-w),$$

y

$$X^3 = +1 \text{ mód}(1-w)^4 \qquad Y^3 = - X^3 \text{ mód.}(1-w)^4$$

luego,

$$Z^3 = X^3 + Y^3 = 0 \text{ mód.}(1-w)^4 \ .$$

En consecuencia, $(1-w)^4$ divide a $Z^3 = (1-w)^3$ ABC, y (1-w) divide a una y sólo una de las cantidades A, B y C, ya que son primos relativos. Esto prueba que 1-w divide sólamente a uno de los elementos $\zeta, \eta, \theta \in Z(w)$. La demostración no pierde generalidad al suponer que 1-w divide a θ .

Puesto que 1-w no divide a ζ ni a η , tenemos que ζ^3 y η^3 son congruentes con $\pm$ 1 mód.$(1-w)^4$. Resulta entonces que A+B+C=0 implica que

$$\alpha\zeta^3 + \beta\eta^3 + \gamma\theta^3 = \pm\alpha + \beta = 0 \text{ mód.}(1-w)^3 \ .$$

Puesto que α y β son unitarios, esto basta para demostrar que $\alpha = \pm\beta$. Esto trae consigo que $\alpha\beta\gamma = \pm\alpha^2\gamma = \pm 1 = +\alpha^3$ y $\gamma = \pm\alpha$

Por tanto, al eliminar α, β y γ obtenemos de A + B + C = 0 una ecuación de la forma

$$\varepsilon_1 \zeta^3 + \varepsilon_2 \eta^3 + \varepsilon_3 \theta^3 = 0$$

donde $\varepsilon_i = \pm 1$. Entonces, tomando $X_0 = \varepsilon_1\zeta$, $Y_0 = \varepsilon_2\eta$ y $Z_0 = -\varepsilon_3\theta$ tenemos que $X_0^3 + Y_0^3 = Z_0^3$.

Además Z_0 es como máximo divisible por $(1-w)^{-1}$, ya que

$Z^3 = (1-w)^3(\alpha\zeta^3)(\beta\eta^3)(\gamma\theta^3)$

es divisible por $(1-w)^3$ y 1-w divide únicamente a θ. Hemos llegado, por tanto, a una contradicción. (Esta demostración es del libro de Clark.)

IV. NUMEROS CONGRUENTES Y CURVAS ELIPTICAS

En esta sección analizaremos el método de Fermat que, tiene una aplicación en el estudio de los números congruentes .
Este método consiste en que a un problema aritmético se le da una solución geométrica.
Problema y ejemplo: La ecuación $x^3+ y^3=9$ tiene las soluciones (1,2) y (2,1) como soluciones racionales; el problema consiste en encontrar más soluciones racionales positivas.
El teorema general de Bézout dice *que dos curvas planas algebraicas de órdenes m,n , que no tienen ninguna curva parcial común, se cortan en mn puntos propios o impropios, reales o imaginarios, distintos o coincidentes.*

Cada una de las locuciones empleadas no representa solamente un modo de hablar o convención arbitraria, sino que responde a un hecho matemático concreto: así puntos impropios comunes significa direcciones asintóticas comunes; puntos comunes coincidentes significa que son multiples para una o ambas curvas, o que hay contacto, etc.

Sabemos por el teorema de Bézout que una recta cualquiera corta a una curva de grado n en a lo más n puntos contados con multiplicidad.
Y también si el corte es tangencial, este punto cuenta doble.
Si una recta corta a la curva $x^3+ y^3= 9$ en dos puntos racionales, el tercero es racional también.

En efecto, sea la recta $y = ax + b$ y la curva $x^3 + y^3 = 9$, al hacer una sustitución tenemos $(1+a^3)x^3 + 3a^2bx^2 + 3ab^2x + b^3 - 9 = 0$ y si x_1, x_2, x_3 son soluciones de la ecuación cúbica, se debe cumplir que

$$x_1 + x_2 + x_3 = -\frac{3a^2b}{1+a^3}$$

(estas son las llamadas fórmulas de Newton) (ref.[9]).

Por consiguiente; si x_1 x_2 , a, b, son racionales, lo será también x_3 . Ahora tenemos un método muy simple de encontrar soluciones a nuestra ecuación, es decir, dado un punto simple, con coordenadas racionales encontrar una tangente a éste y continuar así indefinidamente. Este es el método de Fermat y debe aplicarse a sólo a una curva de tercer grado, tal como en este caso.

A (2,1) le corresponde la recta tangente $y=-4x+9$, de donde tenemos que

$x_1 + x_2 + x_3 = \frac{48}{7}$ y como $x_1 = x_2 = 2$

se deduce que $x_3 = \frac{20}{7}$ y $y_3 = \frac{-13}{7}$.

Aplicando nuevamente el método de fermat al punto $(\frac{20}{7}, \frac{-13}{7})$ obtenemos otro racional que es $(\frac{919}{438}, \frac{-271}{438})$ y una última aplicación del método nos da un resultado con ambas coordenadas positivas.

Ver figura 6.

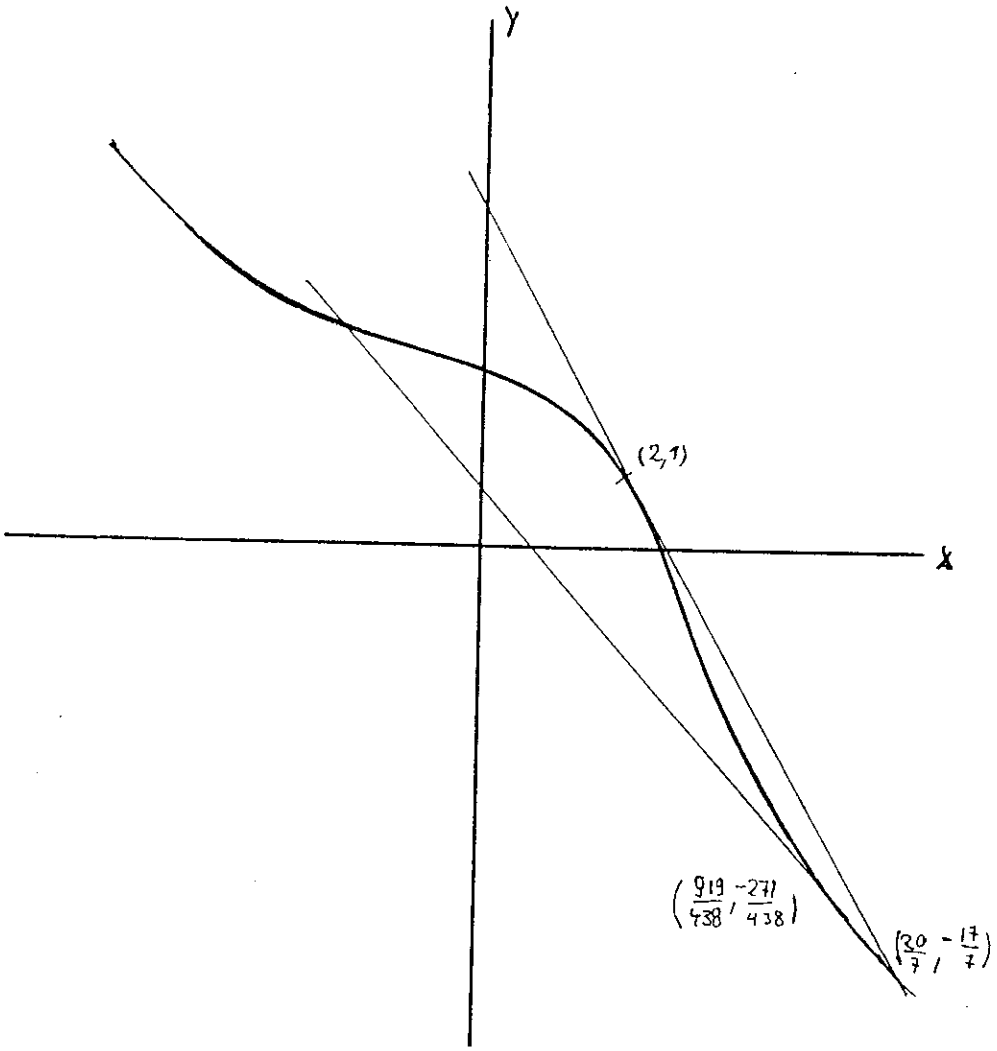


figura 6

Curvas Elípticas

La definición de una curva elíptica es a la vez algebraica como geométrica. Se dice que una curva es elíptica ssi se puede escribir de la forma $y^2 = x^3 + ax + b$ donde a y b son racionales y $4a^3+27b^2 = 0$. Esta última condición significa geométricamente que la curva no tiene puntos dobles ni puntos de retroceso.

Un punto doble es un punto de una curva en donde ésta se corta a sí misma y por punto de retroceso se entiende un punto doble en donde las dos tangentes a la curva (en ese punto) son coincidentes.

Problema: Cuál es la condición para que $x^3+ax + b$ no tenga raices múltiples?

Solución: $x^3+ ax + b$ tendrá raíces múltiples si él y su polinomio derivado $3 x^2+ a$ poseen un cero común.

$$x^3 + a x + b = \frac{1}{3}x(3x^2+ a) + \frac{2}{3}ax + b$$

Un cero en común anularía el resto, es decir $\frac{2}{3}ax + b = 0$, con lo que el cero en común es $\frac{-3b}{2a}$.

Es suficiente escribir que tal valor es un cero de uno de los polinomios, digamos de $3x^2 + a$, $3(\frac{-3b}{2a}) + a$ nos lleva a $4a^3+27b^2 = 0$.

Por lo tanto; la condición para que $x^3+ax + b$ no tenga raíces múltiples es que $4a^3 + 27b^2 \neq 0$.

Denominaremos a la expresión $4a^3 + 27b^2$; ϱ.

Si ϱ es negativo, la curva es elíptica y corta al eje x en tres puntos distintos. Si ϱ es positivo, la curva corta al eje x en un punto y si ϱ es cero, la curva deja de ser elíptica pues tendrá o un punto doble o un punto de "retroceso".

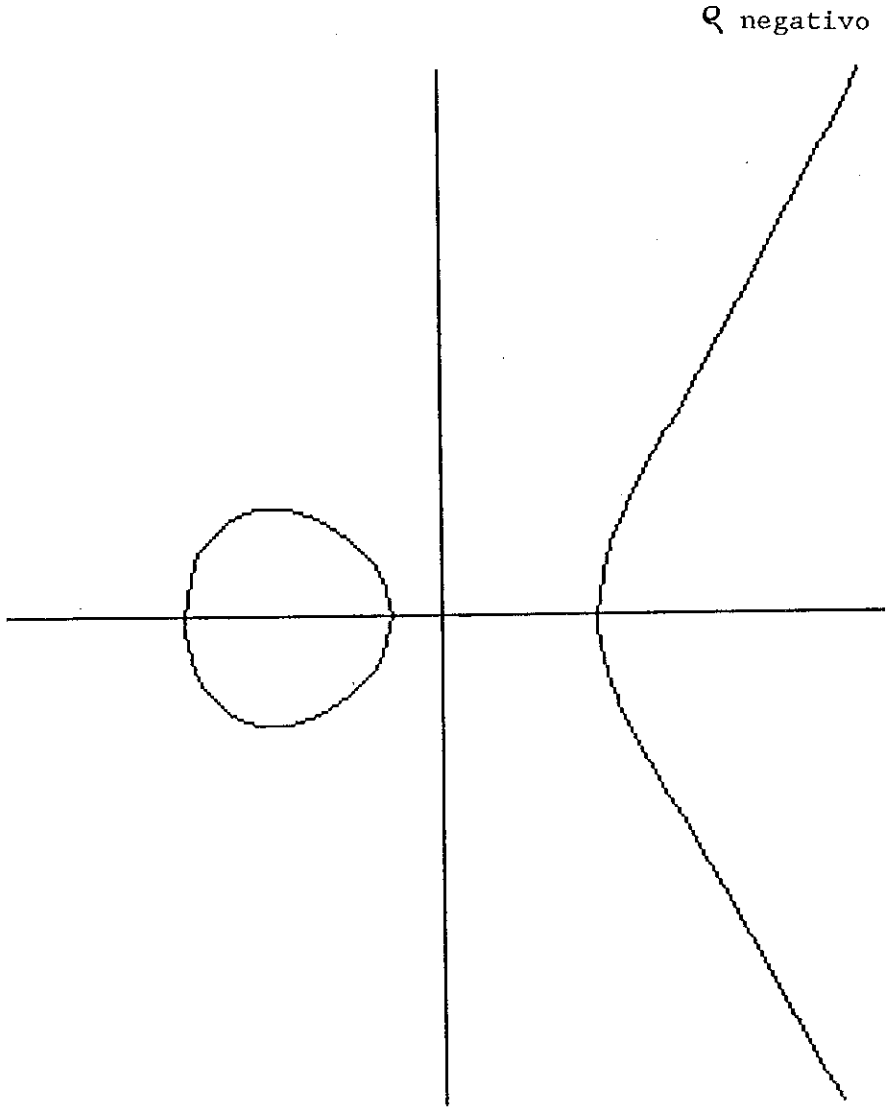
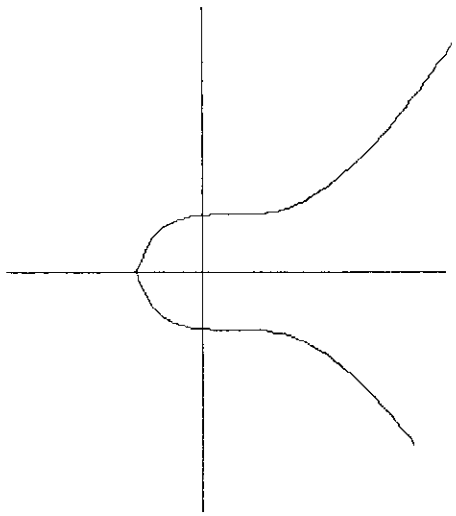
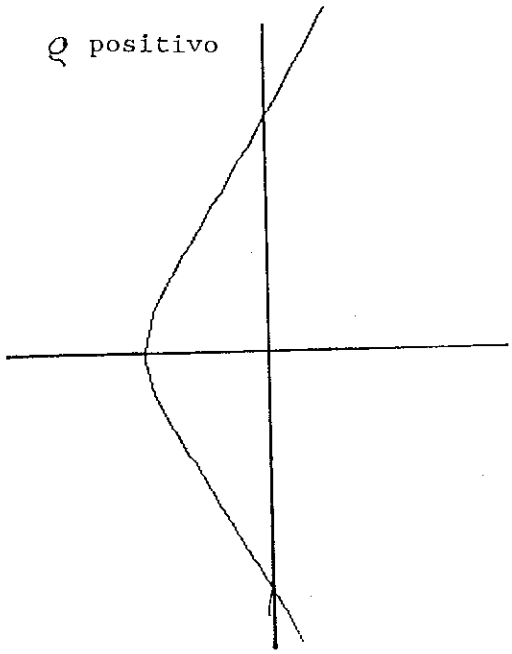


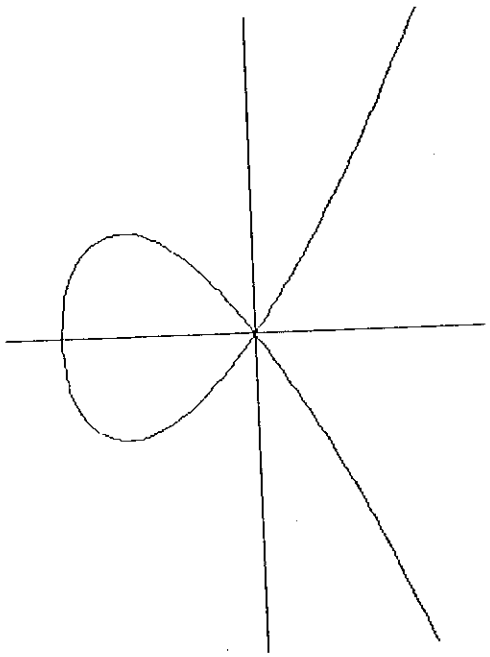
figura 7

ϱ positivo



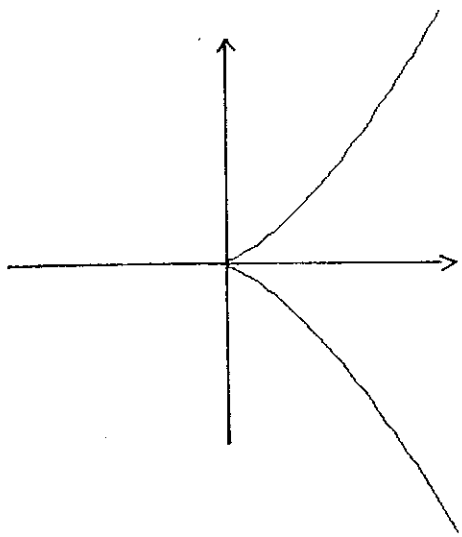
ϱ positivo





ϱ nulo

figura 8



ϱ nulo

Números Congruentes

Se dice que un número entero es congruente, si es igual al área de un triángulo rectángulo, cuyos lados son todos números racionales.

Es fácil demostrar que un entero n es congruente si se puede escribir como $n = \frac{pq(p^2-q^2)}{s^2}$ donde p,q y s son enteros positivos.

En efecto, un número n queda caracterizado por los valores a,b,c, del triángulo rectángulo correspondiente que verifican la relación pitagórica $a^2 + b^2 = c^2$.

Nuestro problema se transforma en encontrar los puntos racionales del círculo unitario, que como vimos anteriormente son infinitos.

Si w es el punto del círculo cuyas coordenadas son (-1,0) y M un punto del círculo , entonces M tiene coordenadas racionales sí y sólo sí la pendiente t de la recta wM es un número racional. (Ver figura 9).

Pues las coordenadas x y y de la recta se expresan en función de t ,

$$x = \frac{1-t^2}{1+t^2} \qquad y = \frac{2t}{1+t^2}$$

entonces $a = \frac{c(1-t^2)}{1+t^2}$ y $b = \frac{2tc}{1+t^2}$ donde t es un número racional.

El área del triángulo rectángulo en cuestión es $A = \frac{ab}{2}$

$$A = \frac{c^2 t(1-t^2)}{(1+t^2)^2}$$

entonces n es congruente si existen dos números racionales α y t tales

que $n=\alpha^2 t(1-t^2)$, $\alpha = \dfrac{c}{1+t}$

Poniendo $t = \dfrac{p}{q}$, se obtiene $A = \dfrac{c^2 \frac{p}{q}\left(\frac{q^2-p^2}{q^2}\right)}{\left(1+\frac{p^2}{q^2}\right)^2} = \dfrac{c^2 pq\,(q^2-p^2)}{(q+p)}$

y como $p^2 + q^2 = s\,c$; n se transforma en $\dfrac{pq(q^2-p^2)}{S^2}$

que es lo que queríamos demostrar.

Si en la fórmula $n = \alpha^2 t\,(1-t^2)$ hacemos $y = \dfrac{h^2}{\alpha}$ y $x = -nt$, obtenemos $y^2 = x^3 - n^2 x$ que es la ecuación de una curva elíptica .

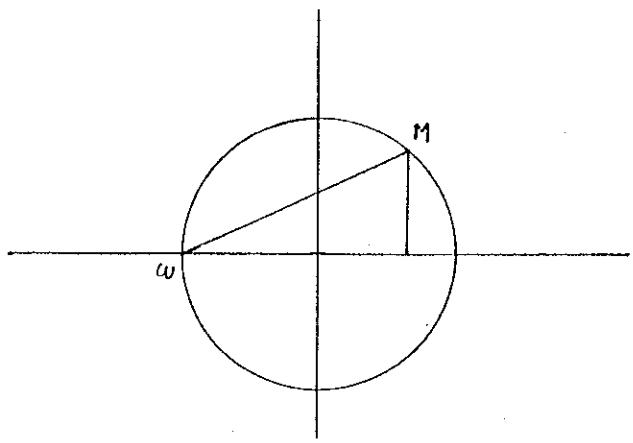


figura 9

Ahora se ve por qué el problema de los números congruentes se inscribe dentro del estudio de las cúrvas elípticas.

A dos puntos racionales, pertenecientes a una curva elíptica, se les puede asociar un tercero, de la siguiente forma:

Si P y Q son dos puntos pertenecientes a la curva, su "suma" P + Q = S donde S será un punto simétrico respecto del eje x del punto T. El punto T es la intersección de la curva con la recta que pasa por P y Q y puede ser el "punto al infinito " (ver definición más abajo)

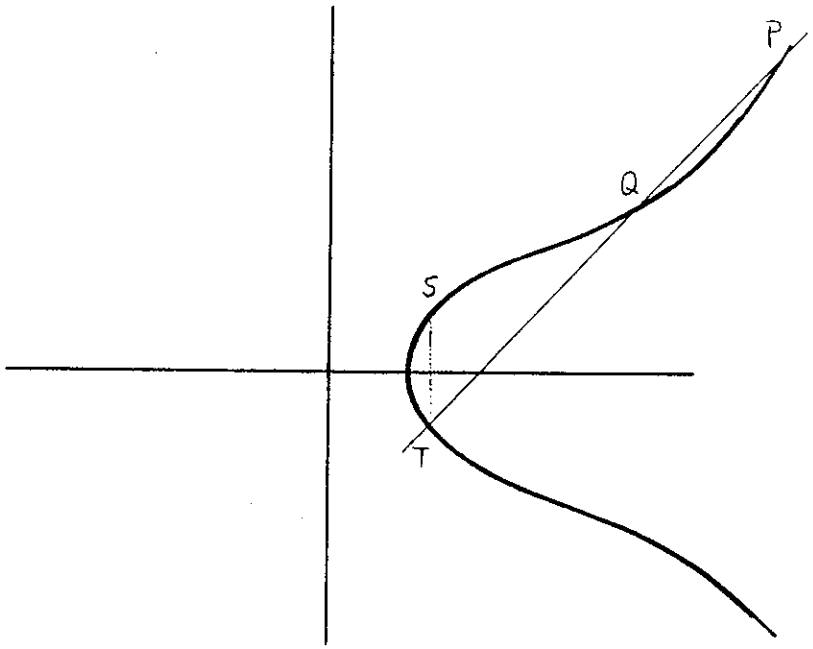


figura 10

Es evidente que esta suma es comuntativa. S= P+Q = Q + P pues proviene de la misma recta. Esta ley es interna y cerrada, es decir que la suma de dos puntos pertenecientes a la curva será otro punto perteneciente a la curva, con la única condición de añadir otro punto. El punto al infinito (∞) .

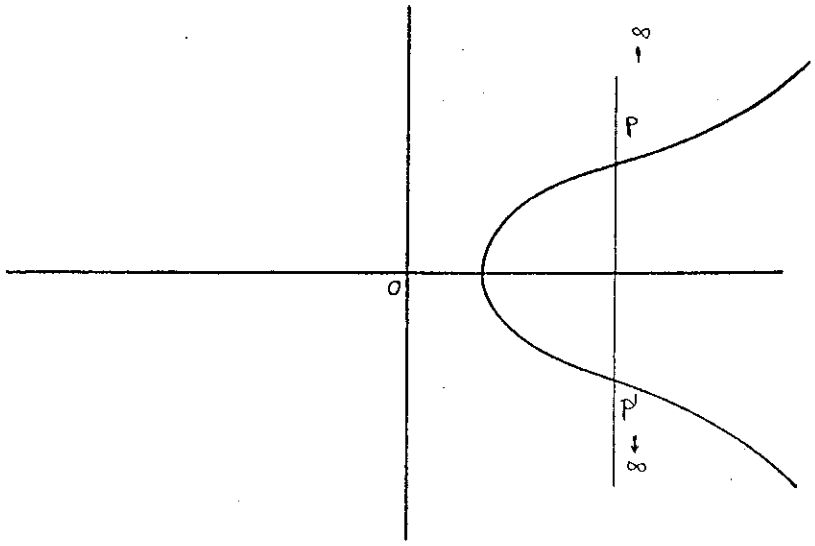


figura 11

El punto al infinito será el elemento neutro en la estructura de grupo. La suma de dos puntos P y P' simétricos al eje X será el punto en el infinito. A este punto lo denotaremos por O .

Pues la recta que une a P con O es la vertical que pasa por O y también por P' y luego pasa otra vez por P así:

$$P + O = P$$

También se tiene que todo punto tiene un simétrico . Incluso el punto A que es un caso especial (ver figura 13) .

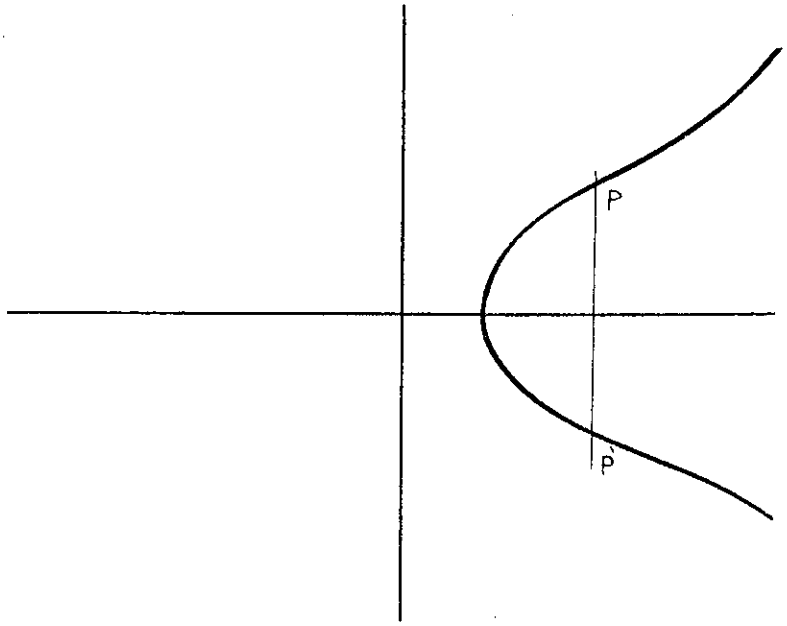


figura 12

Su simétrico es el punto en el infinito O.

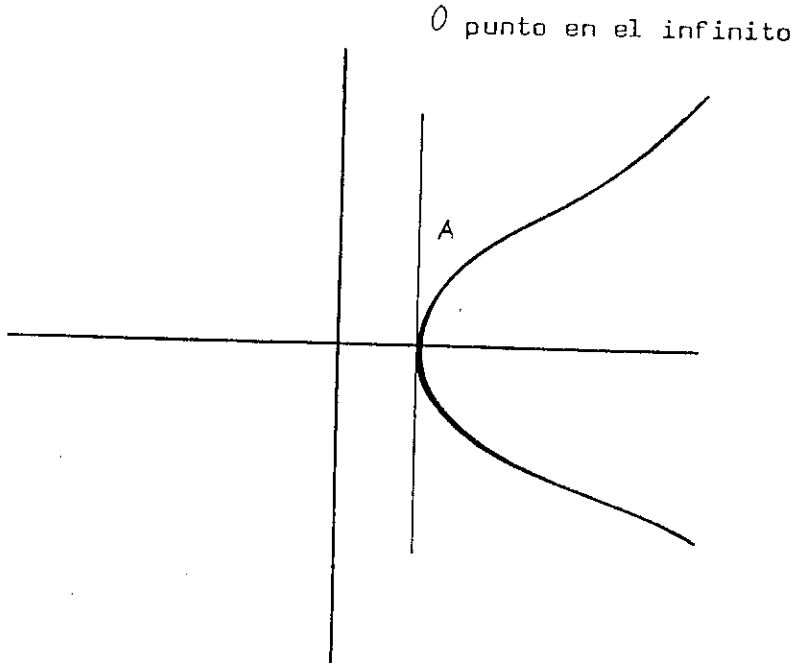


figura 13

Pero también sucede que es asociativa, es decir que al sumar tres puntos se puede efectuar sin que importe el orden, haciéndose esta suma dos a dos.

Y con esto demostramos la estructura de grupo.

En un grupo , un elemento se llama de torsión si existe un $n \in Z_+$ tal que $nP = O$. En este caso, un punto de la curva es de torsión si aplicando el método de fermat a P un número finito de veces, obtenemos nuevamente P.

Se puede mostrar que los puntos de torsión de la curva V $(y^2 - x^3 - n^2 x)$ tienen coordenada igual a cero y son solamente tres $(n,0);(-n,0)$ y $(0,0)$

Teorema: Un entero n es congruente si y sólo si la variedad

$$V(y^2 - (x^3 - n^2 x)) \cap Q$$

es no trivial. Es decir, posee infinitos puntos racionales.

Demostración: Si n es congruente, entonces vale que $n = \alpha t(t-t^2)$ con t y racionales. $x = -nt$ y $y = \frac{n^2}{\alpha}$ es un punto con coordenadas racionales que está sobre la curva $y^2 = x^3 - n^2 x$.

De forma inversa; sea (x,y) un punto que satisface la ecuación $y^2 = x^3 - nx$ haciendo $x = -nt$ y $y = \frac{n^2}{\alpha}$ se tiene que $\frac{n^4}{\alpha^2} = n^3(t - t^3)$ y $n = \alpha^2 t(1-t^2)$, si t es racional se puede escribir como p/q con p y q enteros. Entonces se tiene que

$$n = \alpha^2 \frac{p}{q}\left(1 - \frac{p^2}{q^2}\right) = \alpha^2 \frac{p}{q}\left(\frac{q^2 - p^2}{q^2}\right) = \frac{c^2 pq(q-p)}{(q^2+p^2)^2}$$

y como $p^2 + q^2 = sc$ $\qquad n = \frac{pq(q^2 - p^2)}{s^2}$

V. CONJUNTOS ALGEBRAICOS Y GRUPOS

En esta sección trataremos de caracterizar mediante grupos, algunos conjuntos algebraicos en Q.

Algunos grupos importantes que utilizaremos son:

El grupo de permutaciones de n elementos o grupo simétrico S_n , el grupo alternante de 4 elementos A_4 que es el grupo de todas las permutaciones pares de S_4.

El grupo cíclico C_n de orden n generado por el elemento x. $C_n=\{x^0, x^1, \ldots, x^{n-1}\}$ además $x^n = 1$ y x^h es la menor potencia positiva que es igual a 1.

El viergruppe de Klein V_4 que se define como $C_2 \times C_2$ y el grupo diedral D_4 definido como el grupo de simetrías de un cuadrado.

Sea $N_n = \{ 1,2,3 \ldots n \}$, un subgrupo H de S_n es transitivo si para todo par de elementos $i, j \in N_n$ existe un elemento $\pi \in H$ tal que $\pi(i) = j$

Por ejemplo, el ciclo $\alpha = (123\ldots n)$ genera un subgrupo transitivo de S_n el elemento α^{j-i} cambia a i en j.

Un campo E es una ampliación o extensión de Galois del campo F si F es un campo fijo del grupo de autmorfismos de E, al que llamaremos grupo de Galois de E sobre F y representaremos por G(E/F) .

Sea $f(x) \in Q[x]$ un polinomio de grado n y supongamos que f(x) se descompone en $E \supseteq Q$ $f(x) = \prod (x-w_i)$ en E[x].

El discriminante de f(x) es Δ^2 donde $\Delta = \prod_{i<j} (w_i - w_j)$.

$Q_2 = \{ k^2 / k \in Q \}$ el conjunto de los cuadrados de Q

Teorema: Sea E el campo de descomposición de $f(x) \in Q[x]$.
Si el discriminante Δ^2 de f está en Q entonces $[\, Q(\Delta) : Q \,] = 1$ ó 2 dependiendo de si $\Delta \in Q$ ó $\Delta \notin Q$.

Demostración: Sea E el campo de descomposición de f(x) sobre Q, cualquier permutación σ de los ceros de f(x) transforma Δ en $\pm \Delta$.
$\sigma(\Delta^2) = \Delta^2$; Δ_2^2 pertenece al campo fijo de G(E/Q) que es Q.
Luego, Δ es un cero de $x^2 - \Delta^2 \in Q[x]$. $x^2 -$ ^{2} puede ser reducible o irreducible. Si fuera reducible $\Delta \in Q$, $[Q(\Delta):Q\,] = 1$ y si $x^2 - \Delta^2$ fuera irreducible entonces $\Delta \notin Q$ y $[Q(\Delta) : Q\,] = 2$.

Teorema: Si $f(x) \in Q[x]$ es un polinomio de grado n . El grupo de f(x) sobre Q es un subgrupo del grupo alternante A_n ssi $\Delta \in Q$.

Demostración: Sea E el campo de descomposición de f sobre Q. Si $\Delta \in Q$, entonces toda permutación de G(E/Q) deja fijo Δ . Como toda permutación $\sigma \in S_n$ transforma Δ en $\pm \Delta$ y como A_n es por definición el conjunto de las permutaciones que transforman Δ en Δ , se sigue que toda permutación de G(E/Q) debe pertenecer a A_n .
De forma inversa, si $\Delta \notin Q$ entonces alguna permutación $\sigma \in G(E/Q)$ no fija Δ . De ahí que $\sigma(\Delta) = -\Delta$ y así $\sigma \notin A_n$. Así $G(E/Q) \not\subseteq A_n$.

G(V(y-p(x))) es el grupo de Galois de la variedad V(y-p(x)) sobre Q.
Teorema: $G(V(y-(x^2 + px + q))) = \{e\}$ ssi $p^2 - 4q$ es un elemento de Q_2 .
De otra manera (i.e. $p^2 - 4q \notin Q_2$) , $G(V(y - (x^2 + px + q))) = C_2$.

(Aunque aquí $C_2 \cong A_2$ escribimos C_2 para ser consecuente con la teoría)

Demostración: E= Q ssi $p^2 - 4q$ Q_2 o sea, Q es su propio campo de descomposición y el único automorfismo de E (=Q) en Q que deja fijo Q es $\{i\}$ también si $p^2 - 4q \in Q_2$ esto quiere decir que la raíz cuadrada de un elemento de los cuadrados de Q es un elemento de Q y la extensión será $E = \{ a + b\sqrt{p^2 - 4q} \mid a,b \in Q \}$, lo que implica que E= Q.
Si $p^2 - 4q \in Q_2$ entonces $E = \{ a + b\sqrt{p^2 - 4q} \mid a, b \in Q \}$ y el conjunto de automorfismos de E en E que dejan fijo Q son $i, \psi_{\sqrt{\Delta}, -\sqrt{\Delta}}$
Como $\psi^2 = i$ tenemos que $G(V(y-(x^2 + px +q)))= C_2$.

Consideremos el caso de $G(V(y-x^3 + p x^2 + qx + r))$
Mediante la transformación $x = x_1 + \frac{p}{3}$ reducimos el polinomio a $x_1^3 + bx_1 + c$ que en el más general de los casos será irreducible y separable en Q.
Por las fórmulas de Cardano tenemos que

$$x= \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

de cada radical resultan tres raíces cúbicas y por consiguiente existirán seis soluciones en total, de las cuales tres son soluciones extrañas.
Como es un polinomio cúbico, este tendrá al menos una solución real, sea esta w_1 con $w_1 \notin Q$, pues el polinomio se supuso irreducible.
Tanto $\Delta = (w_1 - w_2)(w_1 - w_3)(w_2 - w_3)$ y w_i están en alguna extensión de Q. Es fácil ver que $[Q(w):Q]=3$ y como $[Q(\Delta) : Q]$ es 1 ó 2 dependiendo de si $\Delta \in Q$ ó $\Delta \notin Q$ tenemos que $[Q(\Delta, w):Q] = 3$ ó 6 dependiendo de si $\Delta \in Q$ o no.

Entonces $G(V(y-x^3 + px^2 + qx + r)) = A_3$ ssi $-4b^3 - 27c^2$ $(= \Delta)$ tiene raíz cuadrada en Q y $G(V(y- x^4 + p x^2 + q x + r)) = S_6$ ssi no tiene raíz cuadrada en Q.

Consideremos por último los polinomios de cuarto grado.

Sea $p(x) = \prod_{1 \le i \le 4} (x-\alpha_i) = x^4 + a x^3 + b x^2 + c x + d$

y cuyo campo raíz o campo de descomposición es E (sobre Q)

Si p(x) es irreducible y separable (i.e. no tiene raíces repetidas), entonces su grupo de galois actúa transitivamente sobre las cuatro raíces de p(x), y debe ser isomorfo a alguno de los subgrupos de S_4^4 .

Al vierguppe de Klein V_4

Al grupo cíclico C_4

Al grupo dihedro D_4

Al grupo alternante A_4

Al mismo S_4

Como la característica de Q no es dos, esto garantiza que p(x) es separable si es irreducible.

El polinomio $r(x) = x^3 - bx^2 + (ac-4d)x - (a^2d-4bd + c^2)$ cuyas raíces son $t_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$ $t_2 = \alpha_1\alpha_3 +$ $t =$

se llama resolvente cúbica de p(x) y su campo de descomposición sobre Q lo denotaremos por F.

Tanto r(x) como p(x) tienen el mismo discriminante.

$$\Delta = \prod_{i<j} (\alpha_i - \alpha_j)^2 = \prod_{i<j} (t_i - t_j) .$$

$$\Delta = -4bA + b B + 18 dBA - B - 27 A$$

donde $A = a^2d + c^2 - 4bd$ y $B = ac - 4d$

Teorema : Supongamos a p(x) irreducible sobre Q , r(x) su resolvente cúbica con campo de descomposición F y el discriminante.

Entonces:

i) $G(V(y-p(x))) = S_4$ ssi r(x) es irreducible sobre Q y $\Delta \notin Q_2$

ii) $G(V(y-p(x))) = A_2$ ssi r(x) es irreducible sobre Q y $\Delta \in Q_2$

iii) $G(V(y-p(x))) = V$ ssi r(x) se descompone en factores lineales en Q

iv) $G(V(y-p(x))) = C_4$ ssi r(x) tiene sólo una raíz en Q y $g(x) = (x^2 - tx + d)(x^2 + ax + (b-t))$ se descompone sobre F.

v) $G(V(y-p(x))) = D_4$ ssi r(x) tiene sólo una raíz en Q y g(x) no se descompone sobre F.

Demostración: Sea $V = \{(1), (12)(34), (13)(24), (14)(23)\}$, el único subgrupo transitivo de S_4 que es isomorfo a V.

El campo de descomposición F de la resolvente r(x) está contenido en E,

$$Q \subseteq F \subseteq E$$

Como p(x) es separable e irreducible , el discriminante no es cero y r(x) tendrá distintas raíces dependiendo si r(x) es irreducible o no.

Se puede verificar por cálculo directo que toda permutación de $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ deja fija las tres raíces de r(x) ssi la permutación actúa sobre los índices como un elemento de V .

Por lo tanto $|G(E/F)| = |G(E/Q) \cap V_4|$ y vemos que :

a) r(x) se descompone en factores lineales sobre Q ssi $G(E/Q) \simeq V_4$

b) r(x) es irreducible sobre Q ssi $|G(E/Q)| = |G(E/F)|\,|G(F/Q)|$ es divisible por 3.

Como p(x) es irreducible sobre Q $|G(E/Q)|$ es divisible por 4 y de ahí que su orden sea de por lo menos 4. Entonces en el primer caso tenemos $G(V(y-p(x))) \cong A_4$ o a S_4 Será a A_4 si el discriminante $\Delta = \overline{\prod}(\alpha_i - \alpha_j)^2$ es un cuadrado en Q y a S_4 si no lo es.

Ahora asumamos que r(x) tiene sólo una raíz en Q.

Sea esta $t = t_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$ y el grupo de Galois será isomorfo a C_4 o a D_4 (Ya hemos excluído a S_4 , V_4 y A_4)

Consideremos el polinomio $g(x) = (x^2 - tx + d)\,(x^2 + ax + (b-t))$ sobre Q.

Las raíces del primer factor son $\alpha_1\alpha_2$ y $\alpha_3\alpha_4$ y las del segundo: $\alpha_1+\alpha_2$ y $\alpha_3+\alpha_4$

Si G(E/Q) C entonces F es la única extensión cuadrática de Q contenida en F. Por eso cada uno de los factores cuadráticos de g(x) se descompone en F .

De forma inversa, asumamos que g(x) se descompone completamente en F. Entonces el polinomio $k(x) = x^2 - (\alpha_1+\alpha_2) + \alpha_1\cdot\alpha_2$ con raíces α_1 , α_2 tiene coeficientes en F.

Sea L el campo de descomposición de k(x) sobre F.

Así $F \subseteq L \subseteq E$ y de ahí que $\alpha_1, \alpha_2, t_2, t_3$ y $t_1 = t$ están en L;

también $\alpha_3+\alpha_4 \in L$ porque $\alpha_3 - \alpha_4 = -a - (\alpha_1 - \alpha_2)$

Además $\alpha_1 - \alpha_2 \neq 0$ pues $(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4) = t_2 - t_3$

lo que implica que $\alpha_3 - \alpha_4$ están en L y así también α_3 y $\alpha_4 \in L$.

Esto quiere decir que E = L y que $|G(E/L)| = 1$ Como

$$|C_4| < |G(E/Q)| = |G(E/L)| \cdot |G(L/F)| \cdot |G(F/Q)| \leq 1 \cdot 2 \cdot 2 = 4 < |D_4|$$

$G(E/Q)$ debe ser isomorfo a C_4 .

Así que si $r(x)$ tiene sólo una raíz y $g(x)$ se descompone en F , $G(V(y-p(x)))$ es isomorfo a C_4

La condición $G(V(y-p(x))) \simeq D_4$ se da por exclusión mutua

Con esto terminamos esta demostración y la sección.

Ya no demostraremos que en general el grupo de galois para un polinomio de grado n es un subgrupo de S ,este es un resultado clásico de la teoría de Galois.

Queda así concluida la tarea de caracterizar conjuntos algabraicas por medio de grupos, pero sólo variedades muy específicas i.e. de la forma $V(y - p(x))$.

VI. BIBLIOGRAFIA

[1] Dean, R. Elements of Abstracts Algebra 1 st. ed.
1966 John Wiley & Sons. 289 pp.

[2] Clark, A. Elementos de Algebra Abstracta 1 ra. ed.
1974 Editorial Alhambra S.A. 272 pp.

[3] Cohen,H.;Nordon,D. "L'arihmétique assistée par la géometrie
1989 et l'ordinateur". La Recherche. Francia 352-358

[4] Fulton, W. Algebraic Curves.3rd ed.
1976 W.A.Benjamin Inc.

[5] Herstein, I.N,;Topics in Algebra. Mass.,Xerox.
1964

[6] Kendig. K.; Elementary Algebraic Geometry. 2nd.ed. New York
1984 Springer Verlag. 303pp.

[7] Kendig. K "Algebra, Geometry and Algebraic Geometry"
1983 American Mathematical Montly USA: 161-174.

[8] Kunz, E. Einführung in die Konmuntative Algebra und
Algebraische Geometrie. Vieveg Verlag

[9] Rey Pastor, J. Analisis Matemático t.1 8 ed.
1969 Editorial Kapelusz.

[10] van der Waerden, B.L. Modern Algebra 2 V.
1949 New York, Frederick Ungar Publishinc Co.