Universidad de Valladolid

Facultad de Ciencias

Trabajo de Fin de Grado

Grado en Matemáticas

El Teorema de Cayley-Bacharach y Matemática Discreta

Autor: Eduardo Quintana Adeva
Tutor: Antonio Campillo
Julio 2020

1 Introducción:

El estudio de la geometría algebraica tiene un largo recorrido en el campo de las matemáticas y es que entender su comportamiento ha supuesto un gran avance en estas.

En este texto empezaremos estudiando algunas de las propiedades más básicas de las curvas algebraicas planas, representaremos algunas figuras clásicas y caracterizaremos la relación que poseen estas con sus implícitas. Dos de los principales estudios precursores en esta rama vendrían de la mano de Maclaurin *C. Maclaurin, (6)* y *C. Maclaurin, (7)* en los que se asentaron las primeras de las bases sobre los conceptos que vamos a tratar a continuación. Posteriormente su trabajo sería ampliado en *G. Cramer, (4)* en el que se propusieron 250 ejemplos de curvas distintas. Aunque el estudio de curvas sobre cuerpos finitos ofrece una gran herramienta, especialmente en el ámbito de la criptografía y los códigos correctores, nos centraremos únicamente en curvas algebraicas en espacios sobre cuerpos infinitos.

Apoyados en la teoría que ya conocemos trabajaremos con resultados muy poderosos como el Teorema Débil de Bezout, dado a conocer por primera vez en *E. Bezout, (2)*, en el cual nos apoyaremos para demostrar resultados muy importantes en el campos de las ecuaciones algebraicas como el Teorema de los Ceros de Hilbert o el Lema de Study.

Como aplicación al Teorema Débil de Bezout, estudiaremos los teoremas de geometría clásicos sobre cónicas y cúbicas proyectivas. Entre ellos pueden destacar el teorema de Pascal, cuya primera demostración formal se remonta a *B. Pascal, (8)* y sería generalizado por Möbius en 1847 para polígonos de $4n + 2$ lados; el Teorema de Pappus, atribuido a Pappus de Alejandría en el año 340; el Teorema de Caracterización de Cónicas que nos dice que una cónica proyectiva se encuentra inequívocamente identificada por 5 puntos siempre y cuando cuatro de estos no se encuentren alineados; este resultado sería generalizado por Cramer para curvas no degeneradas de grado arbitrario. Particularmente nos centraremos en los Teoremas de Cayley-Bacharach, el Teorema de Chasles probado por este en *M. Chasles, (3)* y su generalización probada en *I. Bacharach. (1)*.

Tras el estudio de estos teoremas clásicos nos centraremos en caracterizar y explicar el grupo inducido por una curva elíptica a través del Teorema de Cayley-Bacharach y en explicar la relevancia que posee esta estructura a día de hoy para la ciberseguridad y la protección de datos.

Finalmente se trabajará sobre la hipótesis de Dirac-Montzkin desde un punto de vista histórico, partiendo desde el teorema de Sylvester-Gallai (1944) como punto de inicio y finalizando en la cota dada por Ben Green y Terence Tao *B. Green et Al, (7)*.

En esto esperamos ofrecer un punto de vista pedagógico e introductorio de las ecuaciones algebraicas. Un contexto en el trabajo de curvas proyectivas para grado dos y tres; y abrir la vista a sus actuales aplicaciones a través de los grupos inducidos y el estudio precursor de Green-Tao.

2 Curvas Algebraicas:

2.1 Ecuaciones Implícitas:

A lo largo de este texto utilizaremos la notación $\mathbb{A}_k^n$ y $\mathbb{P}_k^n$ para referirnos al **Espacio Afín** y **Espacio Proyectivo** de dimensión n y sobre el cuerpo k respectivamente.

En el caso del espacio afín, un polinomio $f \in k[X_1, ..., X_n]$ induce una función polinomial $A_k^n \to k$ a través del homomorfismo de sustitución. Sin embargo, podemos encontrar el problema de que dos polinomios distintos inducen la misma función.

A ejemplo veamos que dado p primo los polinomios $X^pY - 1$ y $XY - 1$ inducen la misma función sobre $\mathbb{A}^2_{\mathbb{Z}_p}$.

Este problema se resuelve inmediatamente limitándonos a trabajar con cuerpos infinitos.

Lema 2.1 *Si k es un cuerpo infinito, entonces para todo $f \in k[X_1, ..., X_n]$ no nulo existe algún $a \in A_k^n$ tal que $f(a) \neq 0$. Como consecuencia, dos polinomios distintos definen funciones distintas.*

Demostración: Razonemos por inducción.

En el caso $n = 1$, y como resultado del teorema fundamental del álgebra, se tiene que un polinomio de grado d puede tener a lo sumo d raíces.

Ahora supongamos que esto se cumple para el caso $n - 1$ y veamos que ocurre para el caso n.

Sea $f \in k[X_1, ..., X_n]$ s.p.g. este puede ser expresado en función de X_n de la siguiente forma:

$$f = g_0(X_1, ..., X_{n-1}) + ... + g_d(X_1, ..., X_{n-1})X^d; \quad g_0, ..., g_d \in k[X_1, ..., X_{n-1}]$$

Como $g_d \neq 0$, por hipótesis de inducción, existe $a \in \mathbb{A}_k^{n-1}$ tal que $g_d(a) \neq 0$. Así pues:

$$g_0(a) + ... + g_d(a)X^d \in k[X_n]$$

Y nuevamente, en virtud del teorema fundamental del álgebra, podemos encontrar $b \in k$ tal $g_0(a) + ... + g_d(a)b^d \neq 0$.

Una vez probado el resultado principal, tomemos $f, g \in k[X_1, ..., X_n]$ distintos. Claramente su diferencia $f - g$ sigue perteneciendo a $k[X_1, ..., X_n]$ y es distinta del polinomio nulo, así pues, existe $a \in \mathbb{A}_k^n$ tal que $(f - g)(a) \neq 0$ definiendo así f y g funciones distintas.

□

Definición 2.1 *La hipersuperficie algrabraica asociada al polinomio $f \in k[X_1, ..., X_n]$ es el conjunto de valores:*

$$V(f) := \{(x_1, ..., x_n) \in \mathbb{A}_k^n : f(x_1, ..., x_n) = 0\}$$

Si $n = 2$ denotaremos el conjunto $V(f)$ por curva plana afín.

Entrando de lleno en el terreno del proyectivo, definir este tipo de funciones nos ocasiona muchos más problemas. Tomando por ejemplo el polinomio $f = X^3 - Y \in \mathbb{R}[X, Y, Z]$ y tomemos a su vez el punto $(1 : 1 : 0) \in \mathbb{P}_{\mathbb{R}}^2$. Si sustituimos de forma natural las coordenadas en el polinomio obtenemos el valor $f(1, 1, 0) = 0$; ahora bien, acudiendo a la equivalencia entre las coordenadas del proyectivo se tiene que $(2 : 2 : 0) = (1 : 1 : 0)$ y sin embargo $f(2, 2, 0) = 6$.

Vamos a intentar generalizar el concepto de hipersuperfice al espacio proyectivo. Para ello nos interesará conocer la clase de polinomios que se anulan en un punto del proyectivo con independencia de las coordenadas escogidas.

Definición 2.2 *Se dice un polinomio es homogéneo si todos sus monomios son del mismo grado.*

Lema 2.2 *Sea $F \in k[X_0, ..., X_n]$ un polinomio no nulo de grado d. Entonces F es homogéneo sí y sólo sí $F(TX_0, ..., TX_n) = T^d F(X_0, ..., X_n)$.*

Demostración: Es claro que si F es homogéneo entonces $F(TX_0, ..., TX_n) = T^d F(X_0, ..., X_n)$ (bastaría sacar factor común a cada variable y cada monomio).

Por otro lado, supongamos que F cumple la propiedad en la que $F(TX_0, ..., TX_n) = T^d F(X_0, ..., X_n)$. Ahora, todo polinomio se puede descomponer en suma de polinomios homogéneos, así pues expresemos F de la siguiente manera:

$$F = F_0(TX_0, ..., TX_n) + ... + F_d(TX_0, ..., TX_n)$$

Donde cada F_i es un polinomio homogéneo de grado i (o nulo).

Aplicando ahora que $F(TX_0, ..., TX_n) = T^d F(X_0, ..., X_n,$ y que esta misma propiedad se cumple sobre los polinomios homogéneos se tiene que:

$$T^d F(X_0, ..., X_n) = F(TX_0, ..., TX_n) = T^0 F_0(X_0, ..., X_n) + ... + T^d F_d(X_0, ..., X_n)$$

Igualando término a término respecto a las potencias de T concluimos que $F = F_d$ y por tanto este es un polinomio homogéneo.

□

El lema anterior nos indica que cualquier punto del proyectivo que se anule sobre un polinomio homogéneo lo hará con independencia de sus coordenadas.

Definición 2.3 *La hipersuperficie algebráica proyectiva asociada al polinomio homogéneo $F \in k[X_0, ..., X_n]$ viene dada por el conjunto:*

$$V(F) := \{(a_0 : ... : a_n) \in \mathbb{P}_k^n : F(a_0, ..., a_n) = 0\}$$

En caso de que $n = 2$ diremos que $V(F)$ es una curva proyectiva plana.

Una propiedad importante a tener en cuenta a lo largo de nuestro estudio de los polinomios homogéneos sería la siguiente:

Teorema 2.1 *Sea $F \in k[X_0, X_1]$ un polinomio homogéneo no nulo de grado d entonces $V(F)$ posee a lo sumo d puntos sobre $\mathbb{P}_k^1$. De hecho, si k es algebraicamente cerrado la cota anterior se convierte en igualdad, siempre que cada raíz se cuente con su multiplicidad.*

Demostración: Tomemos $F \in k[X_0, X_1]$ de grado d sin pérdida de generalidad y descompongamos este en $X_0^r \hat{F}$ donde $\hat{F}$ es no divisible por X_0.

Es claro que si $r > 0$ entonces $(0 : 1) \in F$ y viceversa. Tomemos a continuación y sin pérdida de generalidad un punto $(a_0 : a_1) \in \mathbb{P}_k^1$ tal que $a_0 \neq 0$. La siguiente cadena de implicaciones se cumple de forma inmediata:

$$F(a_0, a_1) = 0 \Rightarrow \hat{F}(a_0, a_1) = 0 \Rightarrow \hat{F}(1, a_0^{-1} a_1) = 0$$

La primera de las implicaciones se debe a que k es un cuerpo, $a_0 \neq 0$ y por tanto $a_0^r \neq 0$; haciendo uso a continuación de la ley de anulación se llega a la conclusión de que $\hat{F}(a_0, a_1)$. Para la segunda hemos de percatarnos que $\hat{F}$ es homogéneo y por tanto $\hat{F}(a_0, a_1) = a_0 \hat{F}(1, a_0^{-1} a_1) = 0$, nuevamente por ley de anulación $\hat{F}(1, a_0^{-1} a_1) = 0$

Por último, $\hat{F}(1, a_0^{-1} a_1)$ puede ser entendido como un polinomio de grado $d - r$ sobre una indeterminada, así pues y en virtud del Teorema Fundamental del Álgebra

se tiene que este posee a lo sumo $d - r$ raíces.

Esto probaría que F se anula a lo sumo en d puntos de $\mathbb{P}^1_k$.

Por último, se k es algebraicamente cerrado $F(1, X)$ descompone en $d-r$ factores lineales y por tanto la cota anterior se convierte en igualdad, teniendo en cuenta la multiplicidad de las raíces.

□

A continuación veremos que podemos estudiar las curvas proyectivas a través de las curvas afines y viceversa:

Definición 2.4 *Sea $f \in k[X, Y]$ de grado d se define el homogenizado de este como:*

$$F(X, Y, Z) = Z^d f(X/Z, Y/Z)$$

Proposición 2.1 *El homogenizado de un polinomio es un polinomio homogéneo:*

Demostración: Primero debemos probar que efectivamente el homogenizado es un polinomio. Tomemos $f \in k[X, Y]$ de grado d y veamos que esta sustitución define un monomio en tres variables sobre cualquier monomio de f, y por ende, la sustitución define un polinomio en tres variables:

Sea así pues $\lambda X^i Y^j$ tal que $0 \leq i, j \leq d$ y $i + j \leq d$. El homogenizado de este monomio sería $\lambda Z^{d-i-j} X^i Y^j$ y como $d - i - j \geq 0$ este es un monomio sobre $k[X, Y, Z]$, concluyendo así que el homogenizado de un polinomio es un polinomio.

Veamos ahora que es homogéneo. Se tiene que $F(TX, TY, TZ) =$
$= (TZ)^d f(X/Z, Y/Z) = T^d F(X, Y, Z)$ así pues, por (2.2) F es homogéneo.

□

Definición 2.5 *Sea $F \in k[X, Y, Z]$ de grado d y homogéneo se define el deshomogenizado de este como:*

$$f(X, Y) = F(X, Y, 1)$$

De las definiciones anteriores se tiene que toda curva proyectiva define una curva afín y viceversa. De hecho vamos a ver que nos da lo mismo estudiar el soporte en una u otra en virtud del siguiente resultado:

Antes de siquiera enunciarlo, convenimos que la recta del infinito sobre $\mathbb{P}^2_k$ es aquella generada por la ecuación $Z = 0$.

Proposición 2.2 *Sea $F \in k[X,Y,Z]$ un polinomio homogéneo de grado d y $f \in k[X,Y]$ su deshomogenizado se tiene que si $(x_0 : x_1 : x_2) \in V(F) \setminus V(Z)$ entonces $(x_0x_2^{-1}, x_1x_2^{-1}) \in V(f)$.*

Demostración: Fijémonos que como $(x_0 : x_1 : x_2) \notin V(Z)$ entonces $x_2 \neq 0$ y por tanto $(x_0 : x_1 : x_2) = (x_0x_2^{-1} : x_1x_2^{-1} : 1)$. Además por (2.2) se tiene que $0 = F(x_0 : x_1 : x_2) = x_2^{-1}F(x_0x_2^{-1} : x_1x_2^{-1} : 1) = x_2^{-1}f(x_0x_2^{-1}, x_1x_2^{-1})$

□

Proposición 2.3 *Sea $f \in k[X,Y]$ un polinomio de grado d y $F \in k[X,Y,Z]$ su homogenizado se tiene que si $(x_0, x_1) \in V(f)$ entonces $(x_0, x_1, 1) \in V(F)$.*

Demostración: Aplicamos simplemente la definición.

□

2.2 Teoría Clásica. Teorema Débil de Bezout. Lema de Study

Supongamos ahora que poseo dos curvas algebraicas planas. Una inquietud podría ser conocer en que puntos del plano se van a cortar estas y cuantas veces.

Como veremos a continuación, en el caso de que se tenga una parametrización de las curvas, esta será una tarea relativamente fácil. Pero puedo estar en el caso contrario y sólo poseer la ecuación implícita de estas. De hecho, la parametrización global no existe para toda curva sino sólo para aquellas conocidas como *curvas racionales*.

A lo largo de esta sección veremos como paliar esta serie de problemas en muchos de los casos.

Definición 2.6 *Sea A un DFU, se llama resultante de los polinomios $f = a_0 + a_1X + ... + a_nX^n$ y $g = b_0 + b_1X + ... + b_mX^m$ al determinante:*

$$res(f,g) = \begin{vmatrix} a_0 & a_1 & \cdots & a_n & 0 & 0 & \cdots & 0 \\ 0 & a_0 & \cdots & a_{n-1} & a_n & 0 & \cdots & 0 \\ & & \vdots & & & \vdots & & \\ 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n \\ b_0 & b_1 & \cdots & b_{m-1} & b_m & 0 & \cdots & 0 \\ 0 & b_0 & \cdots & b_{m-2} & b_{m-1} & b_m & \cdots & 0 \\ & & \vdots & & & \vdots & & \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_{m-1} & b_m \end{vmatrix}$$

Entre muchas de las propiedades de la resultante podemos destacar un resultado fundamental en nuestro estudio.

Teorema 2.2 *Sean $f, g \in k[X]$, entonces $res(f, g) = 0$ sí y sólo sí f y g poseen al menos un factor en común.*

La demostración de esta propiedad para cuerpos algebraicamente cerrados necesita de notación compleja. Es por esto que dejamos al lector interesado en el resultado una posible vía para demostrar este en *Algebra, Lang, p.200-202, Prop 8.1.* o en las notas de álgebra del grado.

Corolario 2.1 *Sea k algebraicamente cerrado y $f, g \in k[X]$ dos polinomios, entonces el conjunto*

$$C = \{(p(t), q(t)) : t \in k\}$$

es una curva algebraica plana sobre $\mathbb{A}^2_k$.

Demostración: Es claro que el punto $(a, b) \in C$ sí y sólo sí los polinomios $f(X) - a$ y $g(X) - b$ poseen una raíz en común, o equivalentemente por el teorema anterior, si $res(f(X) - a, g(X) - b) = 0$, así pues definimos el polinomio $h(X, Y) = res_Z(f(Z) - X, g(Z) - Y)$ teniendo de forma directa que $V(h) = C$ y por tanto siendo C curva.

□

Proposición 2.4 *Sean $f, g \in k[X, Y]$. Si $(a, b) \in V(f) \cap V(g)$ entonces a es raíz de $res_Y(f, g)(X)$ y b es raíz de $res_X(f, g)(Y)$. En particular, si f y g no poseen factores comunes entonces $V(f) \cap V(g)$ es un conjunto finito.*

Demostración: Asumiendo la primera parte cierta, la segunda sería inmediata. Como f y g son coprimos entre sí, $res_X(f, g)(Y)$ y $res_Y(f, g)(X)$ serían polinomios en una variable y por el Teorema Fundamental del Álgebra sólo podrían tener un número finito de raíces.

Puesto que el enunciado de la primera parte es simétrico, nos bastará probar que a es raíz de $res_Y(f, g)(X)$. Denotemos por $F(Y) = f(a, y)$ y $G(Y) = g(a, y)$. Puesto que b es raíz común a F y G se tiene que $0 = res(F, G) = res_Y(f, g)(a)$.

□

Teorema 2.3 *(Teorema Débil de Bezout) Sean F, G dos polinomios homogéneos sobre $k[X_0, X_1, X_2]$ de grados e y d y primos entre sí, respectivamente. Entonces, si k es infinito, $V(F) \cap V(G)$ posee a lo sumo $d \cdot e$ puntos.*

Demostración: Veamos en primer lugar que $V(F) \cap V(G)$ es finito.

Tomemos $(a_0 : a_1 : a_2) \in V(F) \cap V(G)$ sin pérdida de generalidad y veamos que los valores que pueden tomar a_0 y (a_1, a_2) son finitos.

En primer lugar, como k es infinito podemos tomar coordenadas de tal manera que $(0 : 0 : 1) \notin V(FG)$ (recordemos que por ser k infinito existe $a \in \mathbb{A}^3_k$ tal que $(FG)(a) \neq 0$ y puesto que FG es un polinomio homogéneo de grado positivo a necesariamente ha de ser distinto de 0).

Tomemos a continuación $(a_0 : a_1 : a_2) \in V(F) \cap V(G)$ sin pérdida de generalidad y definamos $f(X_2) := F(a_0, a_1, X_2)$ y $g(X_2) := G(a_0, a_1, X_2)$. Puesto que a_2 es raíz común a f y g se tiene que $res(f, g) = 0$, es más, como $(0 : 0 : 1) \notin V(FG)$ se tiene que la resultante es un determinante de rango completo y por tanto $res(f, g) = res_{X_2}(F, G)(a_0, a_1)$.

El razonamiento anterior prueba que si $(a_0 : a_1 : a_2) \in V(F) \cap V(G)$ entonces $(a_0 : a_1)$ es raíz de $res_{X_2}(F, G)(X_0, X_1)$, que como sabemos es un polinomio homogéneo de grado a lo sumo $d \cdot e$ por la definición de resultante y en virtud del teorema (2.1) se anula en a lo sumo $d \cdot e$ puntos de $\mathbb{P}^1_k$.

Finalmente, para cada $(a_0 : a_1)$ se tendría que $F(a_0, a_1, X_2)$ se anula en una cantidad finita de puntos en virtud del Teorema Fundamental del Álgebra, así pues las posibilidades para a_2 también son finitas.

Una vez visto que el conjunto de intersecciones de valores $V(F) \cap V(G)$ es finito veamos que es a lo sumo *de*.

Supongamos que $V(F) \cap V(G) = \{p_1, ..., p_n\}$ y denotemos por L_{ij} a la recta que pasa por los puntos p_i y p_j respectivamente. Como k es infinito podemos escoger una referencia tal que $(0 : 0 : 1) \notin V(FG \prod L_{ij})$.

Por comodidad denotemos por $p_i = (a_{0i} : a_{1i} : a_{2i})$ a los puntos de $F(V) \cap F(G)$. Por un razonamiento análogo al anterior podemos ver que $(a_{0i} : a_{1i})$ puede tomar a lo sumo *de* valores sobre $\mathbb{P}^1_k$, a su vez es claro que $p_i \in V(a_{1i}X_0 - a_{0i}X_1) =: R_i$ ergo esta posee intersección no vacía con L_{ij} para todo j distinto de i. Ahora bien, también es claro que $(0 : 0 : 1) \in R_i$ para todo i ergo la intersección de R_i con L_{ij} es unipuntual pues por caracterización $(0 : 0 : 1) \notin R_i$ para ningún j. De aquí concluimos que para cada i a_{2i} sólo posee un posible valor.

□

Cabe resaltar que si k es algebraicamente cerrado la cota que nos ofrece el Teorema de Bezout se convierte en una igualdad.

Corolario 2.2 *(Lema de Study) Sea $f \in k[X, Y]$ un polinomio irreducible tal que $V(f)$ posee infinitos puntos. Entonces para todo $g \in k[X, Y]$ se tiene que $V(f) \subset V(g)$ sí y sólo sí f divide a g.*

Demostración: La segunda de las implicaciones es obvia, si f divide a g entonces $g = hf$ para algún $h \in k[X,Y]$ así pues si $f(a,b) = 0 \Rightarrow g(a,b) = h(a,b)f(a,b) = 0$ y por tanto $V(f) \subset V(g)$.

El recíproco es simple. Si $V(f) \subset V(g)$ es infinito, por la proposición (2.1) se sigue que f y g poseen factores en común y como f es irreducible se tiene que este ha de dividir a g.

□

Corolario 2.3 *(Lema de Study Proyectivo) Sea $F \in k[X_0, X_1, X_2]$ un polinomio homogéneo irreducible tal que $V(F)$ posee infinitos puntos. Entonces para todo $G \in k[X_0, X_1, X_2]$ homogéneo se tiene que $V(F) \in V(G)$ sí y sólo sí F divide a G.*

Demostración: La segunda de las implicaciones se prueba a partir de un razonamiento análogo al anterior.

Para el recíproco sabemos que $V(F) \cap V(G)$ es infinito y por ende a consecuencia del Teorema Débil de Bezout F y G han de poseer factores en común y como F es irreducible este ha de dividir a G.

□

3 Aplicaciones al Teorema de Bezout. Los Teoremas de Cayley-Bacharach

En esta nueva sección veremos que algunos de los teoremas más conocidos sobre triángulos proyectivos son consecuencia directa del Teorema Débil de Bezout. Ofreceremos demostraciones alternativas del teorema de Pappus, Desargues y Pascal a las clásicas realizadas a través de coordenadas y como resultado final de la sección demostraremos el Teorema de Cayley-Bacharach.

Teorema 3.1 *Sean $A_1, A_2, A_3, B_1, B_2, B_3$ de $\mathbb{P}_k^2$ tal que ningún A_i está alineado con dos B_i y viceversa. Denotemos por:*

$$C_1 = A_2B_3 \cap A_3B_2$$

$$C_2 = A_1B_3 \cap A_3A_1$$

$$C_3 = A_1B_2 \cap A_2B_1$$

entonces $A_1, A_2, A_3, B_1, B_2, B_3$ están en una misma cónica sí y sólo sí C_1, C_2 y C_3 están alineados.

Demostración:

Por comodidad denotaremos por F_{ij} a las respectivas ecuaciones implícitas de las rectas A_iB_j. Es obvio que las cúbicas $G = F_{12}F_{23}F_{31}$ y $H = F_{21}F_{32}F_{13}$ se anulan en los puntos $A_1, A_2, A_3, B_1, B_2, B_3, C_1, C_2, C_3$ y para todos $\lambda, \mu \in k$ la cúbica de ecuación $\lambda G + \mu H$ también lo hace, y para cada punto $P \in \mathbb{P}_k^2$ se pueden tomar elementos $\lambda, \mu \in k$ (no nulos simultáneamente) tales que $P \in V(\lambda G + \mu H)$.

(Cometiendo un abuso de notación, supongamos que $G(P) = a$ y $H(P) = b$. Supongamos si a o b son cero nos bastaría con tomar $\lambda = 0$ y $\mu \neq 0$, o viceversa. Si por el contrario $a \neq 0 \neq b$ entonces nos basta tomar $\lambda = b$ y $\mu = -a$)

Supongamos que $A_1, A_2, A_3, B_1, B_2, B_3$ pertenecen a una única cónica C. Tomemos $P \in C$, entonces existen $\lambda, \mu \in k$ tales que $A_1, A_2, A_3, B_1, B_2, B_3, P \in V(\lambda G + \mu H) = D$. Tenemos pues que C y D poseen 7 puntos en común y en virtud del Teorema Débil de Bezout esto significa que las curvas C y D poseen necesariamente componentes en común.

- Si la ecuación asociada a C es irreducible, en virtud del Lema de Study, $C \subset D$ y por ende existe una recta L tal que $D = C \cup L$. A continuación veremos que $C_1, C_2, C_3 \in L$ irremediablemente. Razonemos por reducción al absurdo y supongamos que $C_1 \in C$, entonces la recta A_2B_3 interseca a C en 3 puntos, en virtud del teorema de Bezout, esto significa que existe otra recta L' tal que $C = A_2B_3 \cup L'$ llegando así a contradicción y teniéndose $C_1 \in L$. Razonando de manera análoga conseguiríamos probar que $C_2, C_3 \in L$ y por tanto estos están alineados.

- Si la curva C es reducible, por hipótesis no queda otra que $C = A_1A_2A_3 \cup B_1B_2B_3$. Supongamos sin pérdida de generalidad que $P \in A_1A_2A_3$, como $A_1A_2A_3$ corta a D en cuatro puntos, en virtud del teorema de Bezout, existe una cónica D' tal que $C = A_1A_2A_3 \cup D'$. Por hipótesis $B_1, B_2, B_3 \in D'$ ergo D' contiene tres puntos alineados y por ende se pude descomponer como unión de dos rectas, ergo existe una recta L tal que $D = A_1A_2A_3 \cup B_1B_2B_3 \cup L$. Finalmente bastaría probar que $C_1, C_2, C_3 \in L$, para ello razonemos por reducción al absurdo y supongamos sin pérdida de generalidad que $C_1 \in A_1A_2A_3$, entonces se tienen as siguientes igualdades $A_1A_2A_3 = A_2C_1 = A_2B_3$ y lo que implica que B_3 se encuentra necesariamente entre dos A_i llegando así a contradicción por hipótesis. Replicando este argumento con C_2 y C_3 se prueba que $C_1, C_2, C_3 \in L$.

Vayamos ahora a por el recíproco y supongamos que existe una recta L tal que $C_1, C_2, C_3 \in L$. Tomemos ahora $P \in L \setminus \{C_1, C_2, C_3\}$ (recordemos que esto lo podemos hacer puesto que k es infinito). Como antes existirá una cúbica $D = V(\lambda G + \mu H)$ conteniendo los puntos $A_1, A_2, A_3, B_1, B_2, B_3, C_1, C_2, C_3, P$ y nuevamente la intersección de D con L consistirá en 4 puntos o más, en virtud del Teorema Débil de Bezout se tiene que L es una componente de D por ende existe una cúbica C tal que $D = C \cup L$. Finalmente razonemos por reducción al absurdo y supongamos que $A_1 \in L$ entonces se dan las siguientes igualdades $A_1B_3 = A_1C_2 = A_1C_3 = A_1B_2$ y deducimos que A_1 se encuentra entre B_2 y B_3, llegando a absurdo por hipótesis, ergo $A_1 \in C$. Argumentando de forma similar con A_2, A_3, B_1, B_2, B_3 concluimos que todos ellos se encuentran en C.

□

Como veremos a continuación el Teorema de Pappus y de Pascal son casos particulares de este más general.

Teorema 3.2 *(Pascal) Dada una cónica irreducible $C \in \mathbb{P}^2_k$ y seis puntos diferentes $A_1, A_2, A_3, B_1, B_2, B_3$ entonces:*

$$C_1 = A_2B_3 \cap A_3B_2$$
$$C_2 = A_1B_3 \cap A_3B_1$$
$$C_3 = A_1B_2 \cap A_2B_1$$

están alineados.

Teorema 3.3 *(Pappus) Dadas dos rectas distintas L_1, L_2 y puntos distintos $A_1, A_2, A_3 \in L_1$, $B_1, B_2, B_3 \in L_2$ (ninguno de ellos $L_1 \cap L_2$) entonces:*

$$C_1 = A_2B_3 \cap A_3B_2$$
$$C_2 = A_1B_3 \cap A_3B_1$$
$$C_3 = A_1B_2 \cap A_2B_1$$

están alineados.

Fijémonos que realmente estos teoremas se dedican a particularizar el anterior para el caso en el que los 6 puntos iniciales se encuentren en una cónica reducible o irreducible.

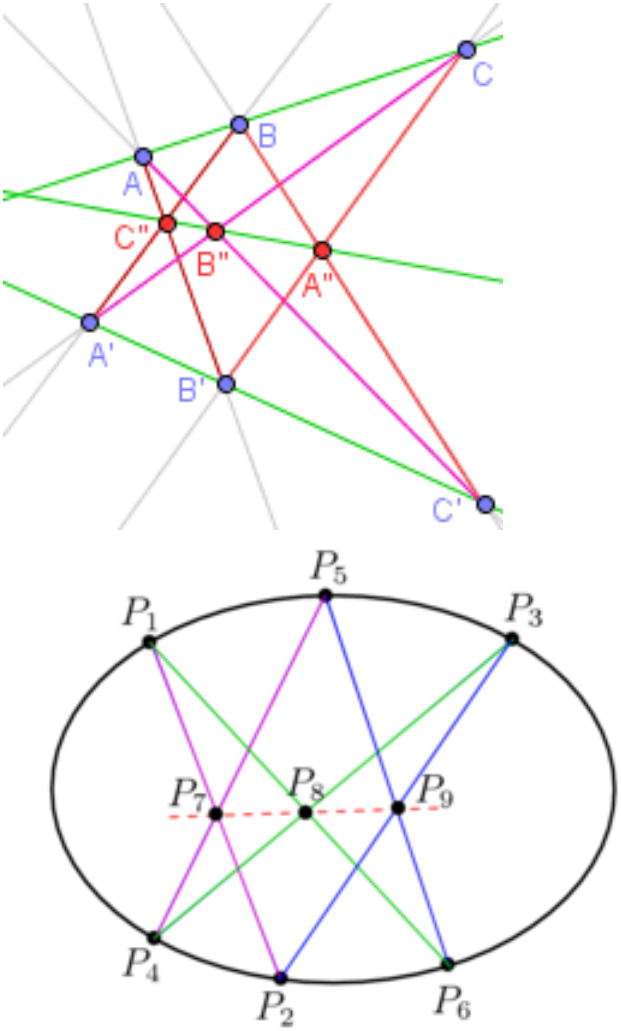

Figure 1: Teorema de Pappus y Pascal

Notación: Denotaremos por V_d al espacio vectorial de polinomios homogéneos de grado de sobre $k[X_0, X_1, X_2]$. De igual manera nos referiremos por $\mathbb{P}_d$ al proyectivizado de este. Es claro que existe una aplicación inyectiva natural entre las curvas de grado d en $\mathbb{P}^2_k$ y los puntos de $\mathbb{P}_d$ a través de las ecuaciones minimales, así pues cometeremos un abuso de notación e identificaremos estos puntos con las curvas.

Los elementos de $\mathbb{P}_d = \mathbb{P}(V_d)$ se denotaran por $[F]$ donde F es una ecuación polinómica que engendra la curva de grado d.

Este nuevo punto de vista nos permite entender las curvas algebraicas proyectivas elementos de un espacio proyectivo y no sólo como un subconjunto de puntos sobre

el plano. Permitiéndonos más versatilidad a la hora de definir nuevos conceptos.

Definición 3.1 *Denotamos por sistema lineal de curvas a los subespacios lineales proyectivos de* $\mathbb{P}_d$*. A su vez, si estos espacios poseen dimensión proyectiva 1 diremos que son haces de curvas.*

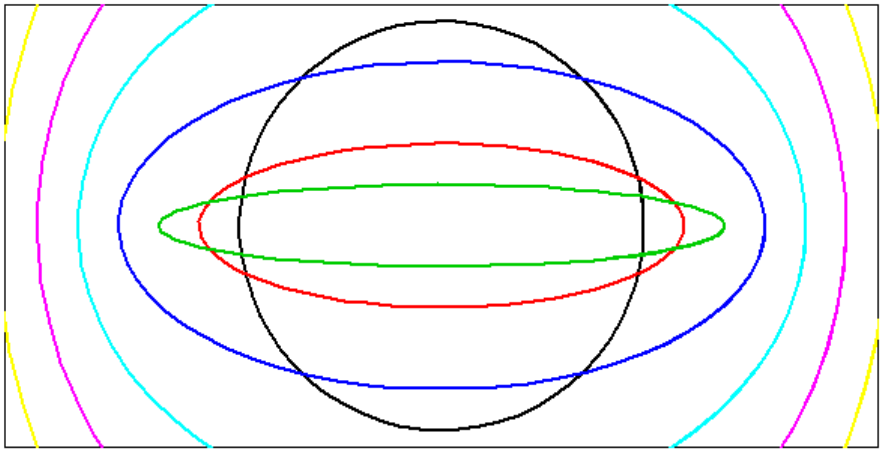

Figure 2: Haz de cónicas dado por las curvas $X_0^2 + X_1^2 + X_2^2$ y $X_0^2 - 3X_1^2 + 5X_2^3$

Diremos que un sistema lineal de curvas $\nabla \subset \mathbb{P}_d$ tiene a $P \in \mathbb{P}_k^2$ como *punto base* si para todo $[F] \in \nabla$ se tiene que $F(P) = 0$.

Lema 3.1 *(Fórmula de Grassman) Sea* H *un espacio proyectivo de dimensión finita y* $U, V \subset H$ *subespacios de este, entonces se cumplen las siguiente igualdad:*

$$dim(U + V) + dim(U \cap V) = dim(U) + dim(V)$$

La demostración de esta fórmula se considera conocimiento que el lector debe haber adquirido antes de familiarizarse con este texto. Sin embargo, para aquella persona que necesite familiarizarse con ella puede encontrar una demostración para espacios vectoriales en *L.Merino et Al, Álgebra y Geometría Lineales* y en las notas de álgebra y geometría lineales del grado. La demostración al proyectivo es consecuencia directa de las propiedades del proyectivizado.

Lema 3.2 *La dimensión del espacio* $\mathbb{P}_d$ *es* $\binom{d+2}{2} - 1$.

Demostración: Sólo debemos encontrar una base para V_d, y es claro que los polinomios de la forma $X_1^i X_2^j X_3^k$ con $i + j + k = d$ y $i, j, k \in 0, ..., d$ conforman una base para este, así pues sólo debemos encontrar el número de soluciones a la ecuación anterior. A través de combinatoria sabemos que las soluciones a esta ecuación son $\binom{d+2}{2}$. Teniendo la dimensión de V_d, su proyectivizado poseerá uno menos.

□

Lema 3.3 *El sistema lineal de las curvas proyectivas de grado d que pasan por un punto* $a \in \mathbb{P}_k^2$ *conforma un hiperplano de* $\mathbb{P}_d$ *que tiene al punto a como único punto base.*

Demostración: Vayamos a V_d y notemos que el morfismo de evaluación

$$\begin{array}{rccc} \phi_a : & V_d & \to & k \\ & F & \to & F(a) \end{array}$$

induce un homomorfismo de espacios vectoriales en el que $Ker(\phi_a)$ conformaría el espacio de los polinomios homogéneos de grado d que se anulan en a poseyendo dimensión $dim(V_d) - 1$ (puesto que $dim(Ker(\phi_a)) = dim(V_d) - dim(Im(\phi_a) = dim(V_d) - dim(k) = dim(V_d) - 1$).

A partir de aquí hemos notar que el proyectivizado de $Ker(\phi_a)$ sería efectivamente el espacio de las curvas que pasan por el punto a y además poseería dimensión $dim(\mathbb{P}_d) - 1$ por caracterización del espacio proyectivo.

Finalmente a es el único punto base de ∇ pues para cualquier otro punto $b \neq a$ existe $[F] \in \nabla$ tal que $F(b) \neq 0$ (nos basta tomar la ecuación de una recta que pase por a y no por b y elevarla a d).

□

Lema 3.4 *Sea* ∇ *un sistema de curvas de dimensión mayor o igual que 1 son equivalentes:*

a) ∇ es un haz.

b) Existe un punto $a \in \mathbb{P}_k^2$ tal que hay una única curva $C \in \nabla$ que pasa por este.

c) Existen dos puntos $a, b \in \mathbb{P}_k^2$ tales que ninguna curva de ∇ pasa por estos de forma simultánea.

Demostración:

$a \Rightarrow b$. Supongamos que ∇ es un haz y tomemos un punto $a \in \mathbb{P}_k^2$ tal que alguna curva de ∇ no pase por este (recordemos que esto es posible puesto que k es infinito). A partir de aquí tomemos el hiperplano de curvas que pasen por a y denotemos este por H_a, en virtud de la Fórmula de Grassman se tiene que la dimensión de ∇ con H_a es un espacio de dimensión 0, es decir, una única curva.

$b \Rightarrow c$. Sea $a \in \mathbb{P}_k^2$ tal que $C \in \nabla$ es la única curva en ∇ pasa por a. Nos basta tomar $b \notin C$ para ninguna curva de ∇ pase simultáneamente por a y b.

$c \Rightarrow a$. Tomemos puntos a y b según hipótesis, denotemos por H_a y H_b al espacio de las curvas que pasan por a y b, por D a la dimensión de $\mathbb{P}_d$. Razonemos por reducción al absurdo y supongamos que la intersección de ∇ con H_a y H_b es vacía y ∇ posee dimensión mayor que 1. Aplicando la Fórmula de Grassman se tiene que $D-2 \leq dim(H_a \cap H_b) \leq D-1$ y $dim(\nabla + H_a \cap H_b) \geq D$ y a su vez $dim(\nabla + H_a \cap H_b) \leq D$ (por ser D la dimensión del total). Utilizando nuevamente esta fórmula llegamos a absurdo pues:

$$1 < dim(\nabla) = dim(\nabla + H_a \cap H_b) + dim(\nabla \cap H_a \cap H_b) - dim(H_a \cap H_b) \leq$$

$$\leq D - 1 - (D-2) = 1$$

Llegando así a absurdo.

□

Teorema 3.4 *Todo sistema lineal de cónicas que pase por cuatro puntos es un haz sí y sólo sí los cuatro puntos no se encuentran alineados.*

Demostración: Denotemos por A_1, A_2, A_3 y A_4 a los puntos en cuestión y por ∇ al sistema de cónicas que pasa por este. Como estamos trabajando con un sistema lineal de cónicas su dimensión es mayor que 1 por el lema (3.4) y en virtud del lema (3.3), ∇ será un haz sí y sólo sí existe un punto $a \in \mathbb{P}_k^2$ tal que sólo pase por este una única curva de ∇. Ahora razonemos por casuística.

- Si A_1, A_2, A_3 y A_4 están alineados entonces están contenidos en una recta y por ende cualquier cónica $C \in \nabla$ tendrá por componente a L. Fijémonos que para cada $a \in \mathbb{P}_k^2$ fijo puedo tomar infinitas rectas que, unidas con L, conformarán una cónica perteneciente a ∇; así pues para cada punto del plano existen infinitas curvas de ∇ que pasan por este y por tanto ∇ no puede ser un haz.

- Supongamos sin pérdida de generalidad que A_1, A_2, A_3 están alineados. Entonces toda cónica de ∇ será la unión de la recta L que contiene a A_1, A_2 y A_3, con otra recta que contiene a A_4. Así pues, tomemos un punto $a \in P_k^2 \setminus L \cup \{A_4\}$, entonces la cónica $L \cup A_4 a$ será la única curva de ∇ que pase por a y por tanto es un haz.

- Finalmente supongamos que los puntos están en posición general, es decir, que no hay tres de ellos alineados. Entonces la cónica $A_1A_2 \cup A_3A_4$ estará contenida en ∇ y será la única cónica que pase por el punto de intersección entre ambas rectas.

□

Corolario 3.1 *Una cónica está unívocamente identificada por 5 de sus puntos sí y sólo sí 4 de estos no están alineados. Además si los tres puntos están en posición general la cónica es irreducible.*

Demostración: Procedamos por casuística:

- Si 4 de los 5 puntos están contenidos en una recta L, entonces cualquier recta que pase por el quinto conjunto a L conforman una cónica (y existen infinitas rectas que pasen por este).

- Supongamos que 3 de los 5 puntos pertenecen a una recta L, entonces no queda otra que los dos restantes pertenezcan a una recta R y la cúbica en cuestión sería la unión de ambas.

- Supongamos ahora que los puntos están en posición general. En virtud del teorema (3.4) las cónicas que pasan por 4 de estos cinco puntos conforman un haz que denotaremos ∇. A este haz pertenece una cónica conformada por la unión de dos rectas, una que contiene a 2 de estos cuatro puntos y otra que contiene a los 2 restantes. Por hipótesis, esta cónica no se encuentra contenida dentro del hiperplano de cónicas que pasan por el quinto punto. Por tanto la cónica buscada es la intersección de ∇ con el hiperplano de las cónicas que pasan por el quinto punto y en función de la Fórmula de Grassman esta consiste en un único punto, ergo esta es única.

Por otro lado, la cónica en cuestión es irreducible puesto que si fuese la unión de dos rectas, 3 de los 5 puntos deberían estar contenidos en alguna de las rectas a la fuerza.

□

Los resultados sobre cónicas anteriores nos permiten encontrar la ecuación minimal para cualquier cónica a través de 5 puntos que pasen por esta trabajando mediante haces. En particular esto nos será de interés en el caso de que estos cinco puntos estén en posición general, pues sino será la unión de dos rectas.

Teorema 3.5 *El sistema lineal de cúbicas que pasan por ocho puntos es un haz sí y sólo sí no están todos en una cónica o cinco en una recta.*

Demostración: Denotemos por $A_1, ..., A_8$ a los puntos por los que pasa el sistema lineal de cúbicas que definen y por ∇ a este. Por la Fórmula de Grassman este poseerá dimensión mayor o igual que 1 (pues estamos intersecando 8 hiperplanos en un espacio de dimensión nueve) y por el lema (3.3) ∇ será un haz si existe a por el que pase una única cúbica de ∇. Razonemos por casuística:

- Supongamos que $A_1, ..., A_8$ pertenecen a una misma cónica C, entonces para cada $a \in \mathbb{P}^2$ la unión de C y una recta que pase por a será una cónica teniendo así, en virtud del lema (3.4) que ∇ no es un haz.

Fijémonos que otra forma de argumentar el caso anterior es decir que hay tres cúbicas con ecuaciones linealmente independientes que pasan por ocho puntos.

- Supongamos, sin pérdida de generalidad, que $A_1, ..., A_5$ pertenecen a una recta L. En virtud de (3.3), fijado $a \in \mathbb{P}^2_k$ sin pérdida de generalidad existe un sistema lineal de cónicas de dimensión mayor o igual que 1 que pasa por $A_6, ..., A_8, a$. La unión de cualquiera de estas cónicas con L conforman una cúbica que pasa por a y en virtud de (3.4) ∇ no puede ser un haz.

Restaría ver para los casos no valorados en la hipótesis:

- Supongamos sin pérdida de generalidad que a lo sumo $A_1, ..., A_4$ se encuentran alineados en una recta L. Si $A_5, ..., A_8$ se encuentran en una recta L' entonces todos ellos recaerían en una cónica ergo no se encuentran alineados. Por (3.4) las cónicas que pasan por $A_5, ..., A_8$ conforman un haz. Así pues, tomando $a \in \mathbb{P}^2_k \setminus L \cup \{A_iA_j\}$ con $i, j = 5, 6, 7, 8$ (pues fijémonos que tres de los cuatro puntos si pueden estar alineados), se tendría que $A_5, ..., A_8, a$ no están alineados y por (3.1) existe una única cónica que pasaría por estos cinco e inercialmente la unión de esta con la recta L sería la única cúbica en ∇ que pasa por a.

- Supongamos ahora que existen a lo sumo tres puntos alineados. Sin pérdida de generalidad podemos asumir que son A_1, A_2, A_3. Como entre A_4, A_5, A_6, A_7, A_8 no existen cuatro alineados, estos definen, en virtud de (3.1) una cónica única. Tomando $a \in L \setminus \{A_1, A_2, A_3\}$ se tiene que la unión de esta cónica con la recta L será la única cúbica de ∇ que pasa por a.

Por último resta comprobar los casos en los que no existen tres puntos alineados.

- Si siete de los puntos, $A_1, ..., A_7$, se encuentran contenidos en una cónica C, para todo $a \in \mathbb{P}^2 \setminus C \cup \{A_8\}$ se tiene que la recta aA_8 unión con C será la única cúbica de ∇ que pasa por a, probando que ∇ es un haz por (3.4).

- Si seis de los puntos, asumamos $A_1, ..., A_6$, se encuentran contenidos en una cónica C, entonces para todo $a \in A_7A_8 \setminus \{A_7, A_8\}$, la cúbica conformada por C unión A_1A_8 será la única cúbica de ∇ que pasa por a, probando que ∇ es un haz por (3.4).

- Por último, supongamos que no existe una cónica que pase por seis de los puntos. Tomemos pues una cónica C que pase por cinco de ellos, asumamos sin pérdida de generalidad que estos son A_1, A_2, A_3, A_4 y A_5, y tomemos $a, a' \in C \setminus \{A_1, ..., A_5\}$

(esto siempre se puede hacer pues cinco puntos definen una cónica unívocamente siempre que cuatro de ellos no estén alineados). A continuación si suponemos que C es componente de alguna cúbica en ∇, entonces no quedaría otra y $A_6, ..., A_8$ deberían estar contenidos en alguna recta L lo cual es absurdo pues por hipótesis no podía haber tres puntos alineados. Esto implica que no existe ninguna cúbica en ∇ que pase por a y a' simultáneamente y por (3.4) esta es un haz.

□

Tras todas esta teoría totalmente necesaria, vamos a probar uno de los resultados principales en nuestro estudio, el Primer Teorema de Cayley-Bacharach.

Teorema 3.6 *(Cayley-Bacharach I) Si C es una cúbica irreducible, entonces el sistema lineal de cúbicas por ocho puntos distintos de C es un haz. En particular, si otra cúbica D corta a C en nueve puntos distintos entonces cualquier cúbica que pase por ocho de esos nueve puntos también pasará por el noveno.*

Demostración: Como C es una cúbica irreducible, en virtud del Teorema Débil de Bezout, no puede tener más de seis puntos en una cónica o tres alineados, así pues, por (3.5) las cúbicas que pasen por ocho puntos de de C forman un haz, que denotaremos ∇. Si otra cúbica D corta a C en estos 8 y uno más, en particular, pertenecerá a ∇. Así pues, como ∇ es un haz, toda curva perteneciente a este se encontrará generada por una combinación lineal de las ecuaciones minimales de C y D ergo cualquier otra curva que corte a C en esos ocho puntos, es decir, que pertenezca a ∇, se anulará de forma inmediata en ese noveno punto por caracterización de su ecuación implícita.

□

Eliminando la condición de irreducibilidad obtenemos un enunciado similar, conocido como *Teorema de Chasles* y probado por este mismo en *M. Chasles, Traité des Sections Coniques, 1841.*

Teorema 3.7 *(Cayley-Bacharach II) Si C es una cúbica sobre $\mathbb{P}^2_k$ y D otra cúbica que corte a la anterior en nueve puntos, entonces cualquier otra cúbica que corte a las anteriores en 8 de los puntos también lo hará en el noveno.*

Demostración: Denotemos por $A_1, ..., A_9$ a los puntos de intersección entre C y D y razonemos por casuística.

- Supongamos, sin pérdida de generalidad, que $A_1, ..., A_8$ no pertenecen a una misma cónica y cualesquiera cinco de ellos no se encuentran alineados entre sí, por (??) las cúbicas que pasan por estos puntos conforman un haz. En virtud de esto

cualquier cónica será generada por una combinación lineal de las ecuaciones lineales de C y D (puesto que estos pertenecen al haz) y por tanto cualquier cúbica que contenga a $A_1, ..., A_8$ contendrá también a A_9.

- Supongamos ahora, nuevamente sin pérdida de generalidad, que $A_1, ..., A_8$ están contenidos en una cónica R. En virtud del Teorema Débil de Bezout se tiene que a la fuerza que R es componente de C, D y cualquier otra cónica que los corte. Así pues, nos basta con tomar A_9 en R.

- Supongamos que existen al menos 5 puntos alineados, asumamos $A_1, ..., A_5$ en una recta L. En virtud del Teorema Débil de Bezout esta recta formaría una componente de irreducible de cualquier cúbica que contenga estos cinco puntos. Así pues cualquier cúbica que pase por $A_1, ..., A_8$ lo hará también por A_9 si fijando este dentro de la recta L.

□

Este resultado puede ser nuevamente generalizable a curvas de grado genérico, pero no podemos realizar la demostración por el momento pues necesitaremos de teoría más avanzada para ello como el *Teorema Fundamental de las Curvas Algebraicas*. Simplemente nos limitaremos a enunciar el resultado:

Teorema 3.8 *(Cayley-Bacharach III) Dadas dos curvas de grado d_1 y d_2 que se cruzan en $d_1 d_2$ puntos diferentes. Cada curva plana de grado k, con $k \geq d_1$, $k \geq d_2$ y $k \leq d_1 + d_2 - 3$ pasando por todos los puntos de intersección menos $\binom{d_1+d_2-k-1}{2}$ también pasarán por el resto de puntos a menos que estos pertenezcan a una curva de grado $d_1 + d_2 - k - 3$.*

El resultado anterior sería enunciado por Cayley en *A.Cayley, On the Intersection of Curves, 1843* pero la prueba que este ofreció tenía ciertas carencias. En un futuro no muy lejano, y apoyándose en los trabajos de Noether y von Brill, Bacharach ofrecería una prueba completa publicada en *I. Bacharach, Ueber den Cayley'schen Schnittpunktsatz, 1886.*

A partir de este se ha conseguido elaborar una teoría altamente compleja que podemos encontrar representada en *D. Eisenbud et Al, (1).* Destacando especialmente que $k[X_0, ..., X_n]$ es Gorenstein (esto es que es un anillo local Noetheriano con dimensión inyectiva como modulo).

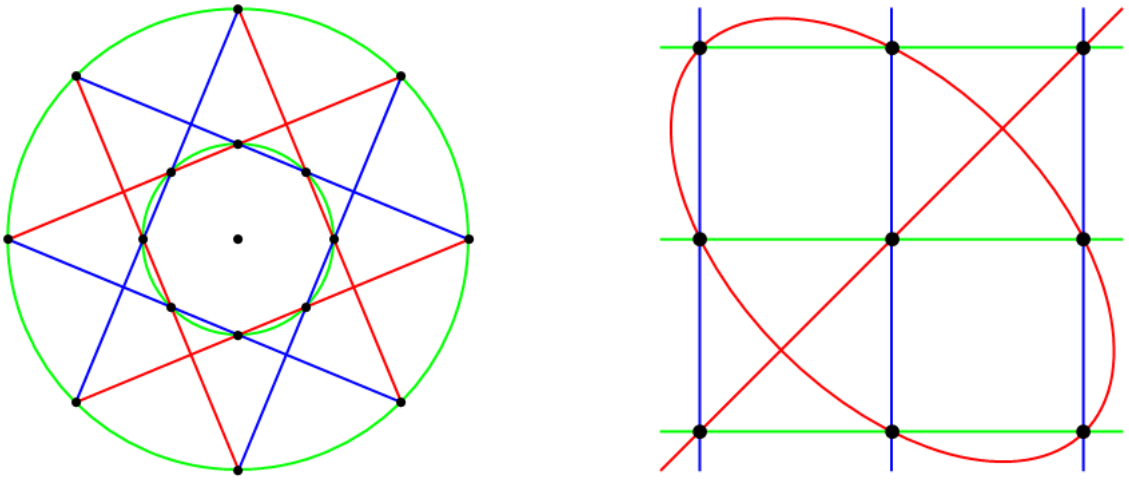

Figure 3: Aplicaciones del Teorema CB

4 Grupo Inducido por una Curva Elíptica:

En esta sección vamos a mostrar como el Teorema de Cayley-Bacharach induce una estructura de grupo sobre los puntos de una curva elíptica. Pero para ello necesitaremos entender primero que es una curva elíptica.

4.1 Teoría Local de Curvas (I):

Fijémonos que podemos extender la noción de derivada de un polinomio $F \in k[X_1, ..., X_n]$ de grado d genérico natural a través de la definición clásica, así pues, representando F sobre una indeterminada X_i de la forma:

$$F = F_0 + F_1 X_i + ... F_d X_i^d$$

Con $F_0, ..., F_d \in k[X_0, ..., X_{i-1}, X_{i+1}, ..., X_n]$, definimos su derivada respecto de X_i como:

$$\frac{\partial F}{\partial X_i} := F_0 + ... d F_d X_i^{d-1}$$

Donde se utiliza la notación:

$$nG = \sum_{i=1}^{n} G$$

Para todo polinomio con coeficientes en k y natural n.

A partir de esta definición podemos generalizar el concepto de singularidad en curvas algebraicas.

Definición 4.1 *Sea $F \in k[X, Y]$ un polinomio, diremos que la curva afín inducida por este posee una singularidad en el punto $(a, b) \in \mathbb{A}_k^2$ si:*

$$\left(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}\right)(a,b) = (0,0)$$

Definición 4.2 *Sea $F \in k[X_0, X_1, X_2]$ un polinomio homogéneo, diremos que la curva proyectiva inducida por este posee una singularidad en el punto $(x_0 : x_1 : x_2) \in \mathbb{P}^2_k$ si:*

$$\left(\frac{\partial F}{\partial X_0}, \frac{\partial F}{\partial X_1}, \frac{\partial F}{\partial X_2}\right)(x_0, x_1, x_2) = (0,0,0)$$

Como veremos en la proposción 4.1, la condición definida en 4.2 equivale a la de 4.1 para la ecuación de la curva en una carta afín de $\mathbb{P}^2_k$.

Podemos definir también el orden de una singularidad extendiendo de manera natural el concepto heredado del análisis.

En efecto, el orden o multiplicidad de una curva en uno de sus puntos es el primer entero para el que la parte homogénea de ese grado (en el desarrollo de Taylor del punto en cuestión) no es nula. El orden es mayor que uno sí y sólo sí el punto es una singularidad.

Este concepto se puede extender a curvas proyectivas estudiando el orden en uno de sus por medio de la ecuación en una carta afín y utilizando de nuevo la proposición (4.1).

Así pues, tomando la cuádrica de ecuación $f(x,y) = x^2 - 2x + 1 - 2yx - 2y$ y calculando sus derivadas vienen dadas por:

$$\partial f/\partial x = 2x - 2y - 2$$

$$\partial f/\partial y = 2x - 2$$

que se anulan simultánea y únicamente en $(1,0)$, como este punto pertenece al soporte, si presenta una singularidad en él, para calcular el orden de la derivada calculamos el desarrollo formal del polinomio de Taylor de f en el punto $(1,0)$:

$$f(x,y) = (x-1)^2 + 2(x-1)y$$

Teniéndose que el orden de la singularidad es 2 puesto que es el menor grado de los monomios que componen a f (en base de Taylor).

Proposición 4.1 *Una curva con polinomio homogéneo $F \in k[X_0, X_1, X_2]$ de grado d posee una singulariadad sobre un punto $P = (x_0 : x_1 : x_2)$ sí y sólo sí pasando al afín (a través de una referencia adecuada) la curva definida por su deshomogeneizado también posee una singularidad en $(x_1/x_0, x_2/x_0)$.*

Denotaremos por *Gradiente* del polinomio $F \in k[X_0, ..., X_n]$ a la n-upla conformada por sus derivadas parciales.

A los puntos singulares de orden dos les llamaremos *puntos dobles* y a los de orden tres *puntos triples*, etc...

Demostración: Fijémonos que simplemente tomamos una referencia adecuada para evitar que la coordenada x_0 en P sea distinta de cero y conseguir que este se encuentre fuera de la recta del infinito.

Por comodidad denotemos por f al homogenizado de F. Como ya vimos podemos expresar F como:

$$F = F_0 + X_0F_1 + ... + X_0^rF_r$$

Donde r es el máximo grado sobre X_0 en los monomios de F y $F_0, ..., F_r$ son polinomios homogéneos sobre $k[X_1, X_2]$. Es claro que el gradiente de F vendrá dado por la terna:

$$\nabla F = \left(F_1 + 2X_0F_2 + ... + rX_0^{r-1}F_r, \frac{\partial F_0}{\partial X_1} + ... + X_0^r\frac{\partial F_r}{\partial X_1}, \frac{\partial F_0}{\partial X_2} + ... + X_0^r\frac{\partial F_r}{\partial X_2} \right)$$

. A su vez, de la descomposición anterior se tiene de forma clara que el gradiente de f sería:

$$\nabla f = \left(\frac{\partial F_0}{\partial X_1} + ... + \frac{\partial F_r}{\partial X_1}, \frac{\partial F_0}{\partial X_2} + ... + \frac{\partial F_r}{\partial X_2} \right)$$

De esto podemos obtneer la siguiente cadena de implicaciones:

$$\nabla F(x_0, x_1, x_2) = 0 \Rightarrow$$
$$\nabla F(1, x_1/x_0, x_2/x_2) = 0 \Rightarrow$$
$$\nabla f(x_1/x_0, x_2/x_0) = 0$$

Así pues el gradiente del homogenizado se anula en la el punto afín a corresponder con P.

El recíproco se obtiene reescribiendo este mismo argumento en sentido contrario.

□

El resultado anterior implica que podemos estudiar las singularidades en una curva proyectiva a través de su ecuación implícita, o pasando al afín sobre su deshomogenizado y estas serán las mismas (si se toma una referencia adecuada).

A su vez también implica que podemos estudiar las singularidades de una curva afín generada por un polinomio f proyectivizando esta y trabajando con su polinomio homogéneo.

Definición 4.3 *Dada una cúbica afín generada por una ecuación del tipo:*

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

se dice que es elíptica si no posee singularidades ni en $\mathbb{A}^2$ *ni en la recta del infinito en su simplección proyectiva.*

Si C es una curva y esta puede ser generada por una ecuación similar a la de la definición anterior, dicha ecuación se conoce como *Forma de Weiesstrass* de C. Un resultado importante es que toda cúbica sobre un cuerpo de característica cero es reducible a Forma de Weiestrass, así pues toda cúbica no singular sobre un cuerpo de característica cero es una curva elíptica.

Proposición 4.2 *Sea C una curva elíptica sobre $\mathbb{A}^2_k$. Si $char(k) \not| 2,3$ entonces podemos encontrar una ecuación reducida para la curva de la forma:*

$$y^2 = x^3 + ax^3 + bx + c$$

Demostración:
Tomemos una curva C generada por el polinomio $y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6$ y realicemos un cambio de variable de tal manera que $y = (1+1)^{-1}(y-a_1x-a_3)$, realizando a las cuentas pertinentes concluimos que la nueva ecuación posee la forma:

$$y^2 = b_1x^3 + b_2x^2 + b_3x + b_4$$

aplicando ahora el cambio de variable $(x,y) = (x-(1+1+1)b_2)(\sum_{i=1}^{36} 1)^{-1}, y(\sum_{i=1}^{108} l)^{-1}$ y realizando las cuentas pertinentes encontramos la siguiente ecuación:

$$y^2 = x^3 - c_1x - c_2$$

□

Esta ecuación es conocida como *Forma Reducida de Weiestrass* para la curva.

Lema 4.1 *Sea C una cúbica afín y $P, Q \in C$, entonces la recta PQ corta a la recta C en tres puntos (pudiendo ser P o Q ese tercer punto).*

Demostración: Podemos tomar una referencia adecuada tal que $P = (1,0)$ y $Q = (0,1)$. Tomemos ahora $F \in k[X,Y]$ ecuación minimal generadora de C en dicha referencia y $X + Y - 1$ ecuación generadora de PQ también en esta. Denotemos ahora por $G(X) = F(X, 1-X)$, fijándonos en la construcción de G se tiene que si $(a,b) \in PQ \cap C$ entonces a es raíz de G, por ende G descompone en $G(X) = X(X-1)H(X)$ e igualando grados con se tiene que $H(X)$ es un polinomio de grado 1, ergo es de la forma $X - z$ para cierto $z \in k$. Despejando la coordenada Y en la ecuación de PQ concluimos que el punto $(z, 1-z)$ pertenece a la cónica.

□

Vamos a realizar una observación antes de continuar. Dada una cúbica C y $P \in C$, si C es un punto simple entonces toda recta que pase por este cortará a C en tres puntos distintos o un punto doble y otro punto (en este caso esa recta será la tangente a C por P), pero no podrá nunca ser nunca un punto triple pues esto significaría que C no es realmente cúbica sin singularidades.

Lema 4.2 *Sea E una curva elíptica, entonces no existe ninguna recta que corte a E en un mismo punto tres veces.*

Demostración:
Supongamos que existe una recta L tal que esta corta a E en un mismo punto P tres veces.

Existe una referencia en la que la ecuación de E tiene la forma:

$$y^2 - x^3 - ax^2 - bx - c$$

. Supongamos que en esta el punto P posee coordenadas (A, B) y la recta que pasa por este es de la forma $Cx + Dy + J$.

-Supongamos que $C = 0$, entonces $B = JD^{-1}$. Sustituyendo entonces, sustituyendo el valor de la coordenada Y del punto P en la ecuación de E se llega a la siguiente igualdad:

$$(x - A)^3 = F(x, JD^{-1})$$

Aplicando la regla de la cadena y derivando se llega a que las parciales de F se anulan en el punto (A, B) llegando así a absurdo pues E es curva regular.

-Supongamos ahora que $D = 0$, en este caso $A = JC^{-1}$. Igualando igual que antes se tendría que:

$$(y - B)^3 = F(JC^{-1}, y) = y^2 + \hat{c}$$

Llegando así a absurdo.
-Por último, supongamos que $C \neq 0 \neq D$, entonces la recta se encuentra parametrizada por la dupla $(x, C^{-1}(J - Dx))$ y nuevamente:

$$(x - A)^3 = F(x, C^{-1}(J - Dx))$$

Calculando nuevamente las derivadas a través de la regla de la cadena se termina deduciendo que las parciales de F se anulan en el punto A, B llegando así a absurdo.

□

4.2 Grupos Inducidos por Curvas Elípticas:

Definición 4.4 *(Ley de Grupo) Sea E curva elíptica $O \in E$. Dados dos puntos P y Q se define la operación $P * Q = R$, donde R es el tercer punto de corte de la recta que une a P y Q (y puede ser no necesariamente distinto a P o Q). Definimos así pues la operación $P + Q = O * (P * Q)$.*

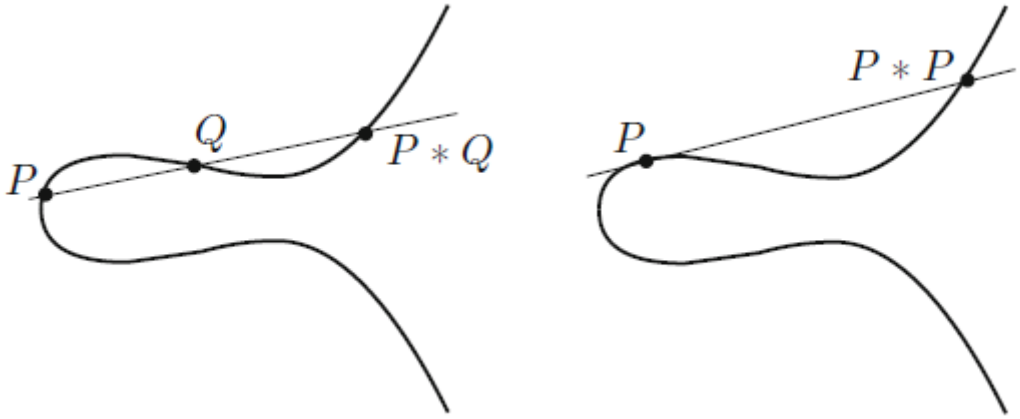

Figure 4: Ejemplo de la Operación $*$

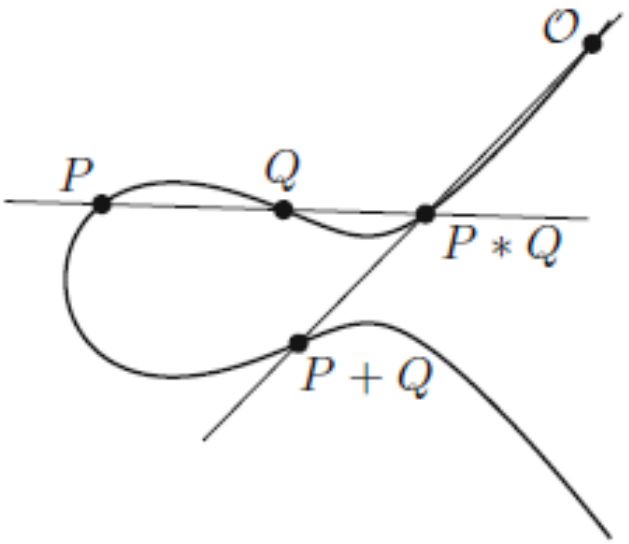

Figure 5: Ejemplo de la Ley de Grupo

Teorema 4.1 *Sea E una curva elíptica y $O \in E$, la terna $(E, +; O)$ posee estructura de grupo abeliano.*

Demostración:

Debemos probar que se cumplen las propiedades de elemento inverso, elemento neutro, propiedad distributiva y propiedad conmutativa.

- Conmutativa: Es claro que la operación $*$ es conmutativa pues la recta que cruza puntos $A, B \in E$ es única y por tanto el tercer punto de corte también lo sera, por eso mismo $E*P = P*E$ y por herencia $E+P = O*(E*P) = O*(P*E) = P+E$.

- Elemento Neutro: Veamos que el elemento inverso en este caso es O. Tomemos un punto P sin pérdida de generalidad, entonces $P + O = O * (P * O)$, denotemos por $Q = P * O$, como Q es el tercer punto de corte de la recta $PO = QO$ no queda otra que $Q * O = P$.

- Elemento Inverso: Dado un punto $P \in E$ y denotemos por $O * O = Q$ al tercer punto de corte que posee E con la recta tangente por O. Ahora, tracemos la recta que pasa por QP y denotemos al tercer punto de corte con esta por G, entonces se tiene que $G + P = O * (G * P) = O * Q = O$.

- Asociatividad: Tomemos tres puntos $P, Q, R \in E$ y veamos que $(P+Q)+R = P + (Q + R)$. Por un lado tomemos los puntos:

$$P * Q, P + Q, (P + Q) * R, (P + Q) + R$$

; a su vez tomemos los puntos $Q * R, Q + R, P * (Q + R), P + (Q + R)$ y finalmente denotemos por S al punto de intersección entre las rectas $P(Q + R)$ y $(P + Q)R$. Finalmente tomemos las cúbicas:

$$C_1 = P(Q + R) \cup (P * Q)O \cup QR$$
$$C_2 = PQ \cup (P + Q)R \cup (Q * R)O$$

Los puntos de intersección de estas serán:

$$O, P, Q, R, P * Q, Q * R, P + Q, Q + R, S$$

Como C_1 y C_2 se cortan en nueve puntos y E pasa por ocho de estos nueve entonces, por el Teorema de Cayley-Bacharach, $S \in E$. Finalmente, la intersección entre E y $P(Q+R)$ se encuentra conformada por los puntos $P, Q+R$ y $P*(Q+R)$, ergo $S = P * (Q + R)$. Análogamente la intersección entre E y $(P + Q) + R$ se conforma por $P, Q + R$ y $(P + Q) * R$ ergo $(P + Q) * R = S$. Finalmente:

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

□

4.3 Criptografía de Curvas Elípticas:

Este tipo de grupos inducidos es sumamente útil en algoritmos de criptografía asimétricos y firmas digitales. Para ello se escoge un cuerpo finito $\mathbb{F}_p$ (generalmente con p primo y lo suficientemente alto), una curva elíptica E y un punto $O \in E$ sobre esta. Se toma un valor k entero aleatorio como clave privada, se denota por

$Q = \sum_{i=1}^{k} P$ (según la ley de grupo inducido por la curva E y el punto O).

Bajo este punto de vista, supongamos existen dos individuos A y B que precisan de tener una conversación con autentificación. En virtud del parrafo anterior denotamos por k_A y k_B a las claves privadas de A y B respectivamente; y por Q_A y Q_B a las claves públicas de estos. Fíjese ahora que el valor $Z = \sum_{i=1}^{k_A} P = \sum_{i=1}^{k_B} P = \sum_{i=1}^{k_A k_B} P$, así pues podemos definir un Secreto Compartido de forma sencilla y muy óptima computacionalmente hablando.

Entre los algoritmos más conocidos y utilizados podríamos resaltar *ECDH* y el inducido por la curva *ED25519*, utilizado por el gobierno de los Estados Unidos.

5 La Hipótesis de Dirac-Montzkin:

En nuevo apartado vamos a estudiar, de manera histórica, los avances sobre un problema abierto, *La Hipótesis de Dirac-Montkin.*

Para ello empezaremos dando la siguiente definición:

Definición 5.1 *Sea $C \subset \mathbb{R}^2$ un conjunto finito de puntos. Diremos que una recta es $k-$incidente en C si solamente pasa por k puntos de C. En particular, si $k = 2$ diremos que la recta es ordinaria sobre C.*

Si C es un conjunto denotaremos al número de rectas $k-$incidentes en este por N_k. El problema reza de la siguiente manera:

¿Cuál es el máximo valor para N_2 en un conjunto de N puntos?

El matemático I. Driac conjeturó que este valor podría ser $N/2$ y aunque parezca extraño, sólo se conocen dos ejemplos que no lo cumplan. En el año 1958 por los matemáticos Kelly y Moser dieron el contraejemplo conocido como *El Plano de No Fano*, con 3 rectas ordinarias y 7 puntos:

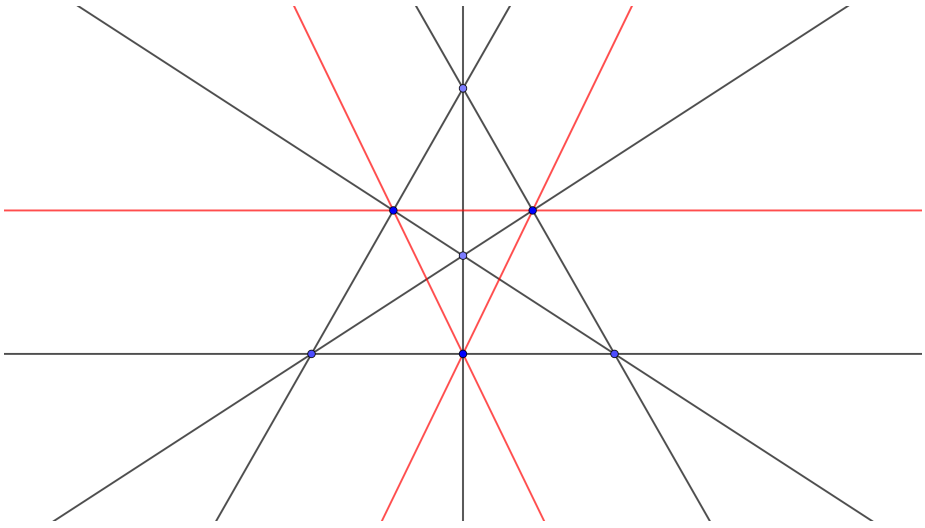

Figure 6: Conjunto de Kelly - Moser

A parte de este, el otro contraejemplo, es el conjunto de McKee consistente en 13 puntos y 6 rectas ordinarias:

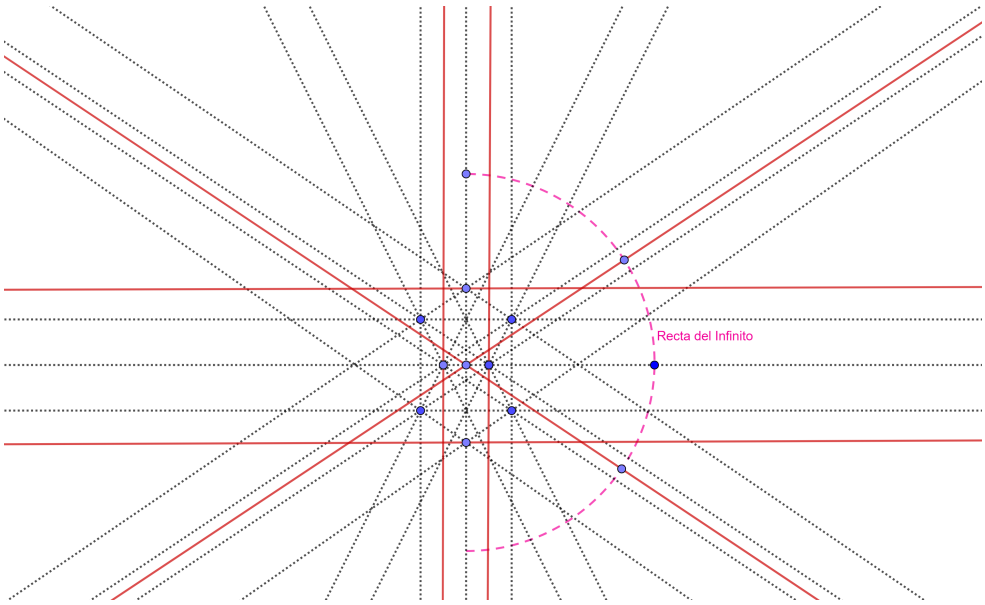

Figure 7: Conjunto de McKee

5.1 Encontrando una Cota Inferior:

El primer resultado influyente en nuestro estudio es el *Teorema de Sylvester-Gallai*. En el año 1893 el matemático J. Sylvester planteó un problema que reza:

> Todo conjunto de $N \geq 2$ puntos en el plano, no todos ellos alineados, posee una recta ordinaria, es decir incidente a dos y sólo dos de su spuntos.

La primera prueba de esta conjetura se debe a Melchior en el año 1941, no percatándose que la había resuelto (y de hecho probaba que si $N \geq 3$ existen al menos tres rectas ordinarias asociadas). En el año 1944 Gallai ofreció una demostración alterna a la de Melchior en la que sólo probaba la existencia de una recta ordinaria asociada. Por último, en el año 1986 L.M. Kelly aportó la demostración más sutil hasta la fecha de este resultado (sobre $\mathbb{R}$ o $\mathbb{C}$) y es la que vamos a aportar:

Teorema 5.1 *(Sylvester-Gallai) Sea C un conjunto de puntos sobre el plano real o complejo, no todos ellos alineados. Entonces C posee asociada al menos una recta ordinaria.*

Demostración: Empecemos razonando por los casos triviales:

- Si N es 2 es obvio.

- Si N es 3 los puntos pueden estar alineados o conformar los vértices de un triángulo, el primer caso no es posible por hipótesis y en el segundo tenemos 3 rectas ordinarias asociadas.

- Si N es 4 pueden estar todos ellos alineados, 3 de ellos alineados o en posición general. El primer caso no es posible por hipótesis, en el segundo tenemos 3 rectas ordinarias y en el tercero tenemos 6.

Por último trataremos el resto de casos con el resto de casos:

Si N es igual a 5, denotemos estos por $P_1, ..., P_N$ y razonaremos por reducción al absurdo. Supongamos que no existen rectas ordinarias asociadas al conjunto. Por finitud podemos tomar el punto y la recta que minimicen distancias entre sí, sin pérdida de generalidad podemos asumir que dicha recta es P_1P_2 y el punto P_3. Como P_1P_2 no es ordinaria existe otro punto de C contenida en esta, podemos asumir que este es P_4 y se encuentra entre P_1 y P_2 (de no ser así bastaría una reordenación en los índices para que fuese el caso), finalmente hemos llegado a absurdo, por construcción, una de las rectas P_2P_3 o P_1P_3 se encuentra más cerca del punto P_4 que la recta P_1P_2 del punto P_3.

□

En las siguientes figuras se pueden apreciar todos los argumentos expuestos en la demostración anterior.

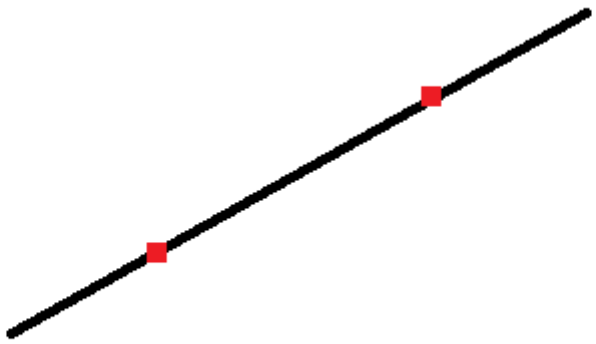

Figure 8: $N = 2$

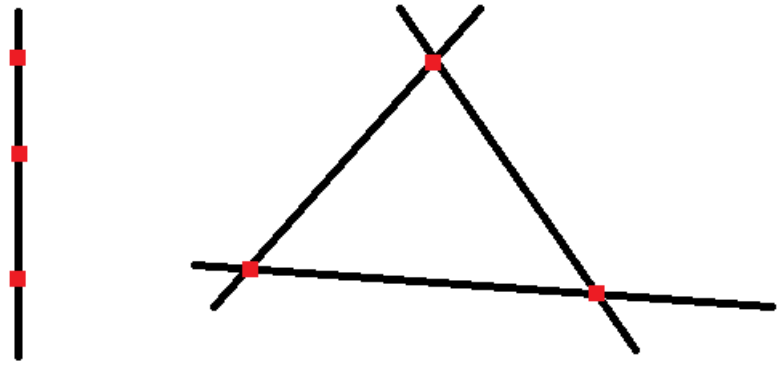

Figure 9: $N = 3$

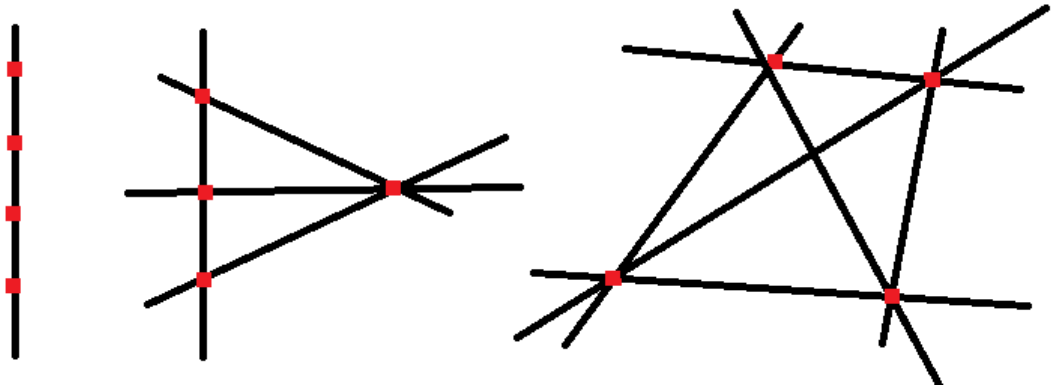

Figure 10: $N = 4$

Este teorema asegura que para cualquier número de puntos no alineados $N_2 \geq 1$. Esta cota puede ser mejorada a través del Teorema de Melchor, pero para ello necesitamos acudir a la teoría de grafos:

Para la siguiente definición necesitamos establecer ciertos términos en nuestra notación. Sean $P, Q \in \mathbb{P}^2_{\mathbb{R}}$ puntos sobre el proyectivo denotamos por P^* y Q^* a sus rectas duales. Por otro lado, denotamos por PQ^* al dual de la recta que une P y Q.

Recuérdese que la recta dual asociada a un punto $(a_0 : a_1 : a_2)$ viene dada por $a_0X + a_1Y + a_2Z = 0$ y viceversa.

Definición 5.2 *Sea $C \subset \mathbb{P}^2_{\mathbb{R}}$ un subconjunto finito. Definimos el Grafo Inducido por P es la dupla (V, E) donde:*

$$V = \{P^* \cap Q^* : P, Q \in C, C \neq P\}$$
$$E = \{[P, Q] : P, Q \in V, P \neq Q\}$$

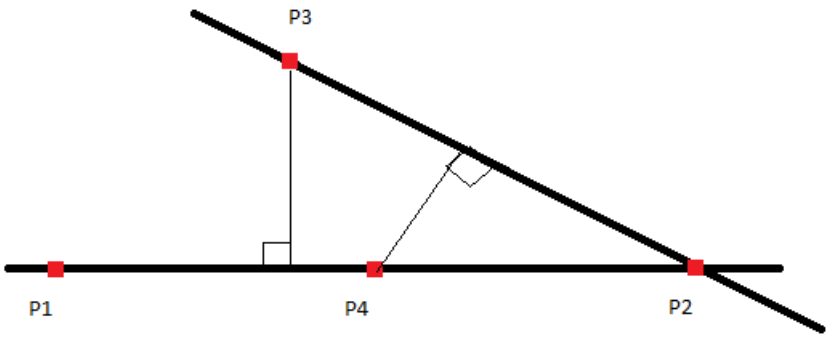

Figure 11: $N \geq 5$

Los grafos no son un concepto nuevo ni mucho menos y gran parte de esta gran disciplina se la debemos a *L. Euler, (5)* y que poco a poco se iría generalizando con el nacimiento de la Topología. De todo este gran estudio vamos a quedarnos con las siguientes formulas:

Dado un grafo (V, E) se denotarán por *vértices* a los elementos de V, por *aristas* a los elementos de E y por caras a aquellas regiones del plano encerradas entre aristas.

Antes de continuar debemos introducir un nuevo concepto de notación. Sea Γ un grafo, entonces denotamos por V a su número de vértices, F a su número de caras y E a su número de aristas. A su vez, F_k es el número de caras colindantes a k aristas y V_k es el número de vértices en los que concurren k aristas.

Teorema 5.2 *Sea Γ un grafo sobre el plano proyectivo entonces se cumplen las siguientes fórmulas:*

i) $V - E + F = 1$

ii) $2E = \sum_{k=2}^{\infty} kV_k = \sum_{i=2}^{\infty} 2kN_k$

iii) $2E = \sum_{k=3}^{\infty} kF_k$

Demostración:

La primera de las igualdades se debe a que la característica de Euler del plano proyectivo es 1. Para ii) Se tiene que cada vértice del grafo es el dual de una recta $k-$incidente L, es decir, que pasa por k puntos de P y por tanto su grado será $2Card(P \cap L)$. Por último, iii) se debe a que cada cara del plano se encuentra encerrada por al menos tres aristas y que cada arista es colindante a al menos dos caras.

□

Corolario 5.1 *Para todo grafo sobre un plano proyectivo se tiene la siguiente igualdad:*

$$\sum_{k=2}^{\infty}(k-3)V_k + 3 + \sum_{s=3}^{\infty}(k-3)F_k = 0$$

Demostración:

La demostración pasa por utilizar las fórmulas del lema anterior. Tomando 3(i) y sustituyendo $3E$ por $(ii)/2 + (iii)$ habremos terminado.

□

Corolario 5.2 *(Teorema de Melchior) Todo conjunto P sobre el plano proyectivo con al menos tres puntos, no todos ellos alineados, posee al menos tres rectas ordinarias:*

Demostración:

Fijémonos que en el grafo inducido por P, V_k se corresponde con N_k, así pues, despejando en la ecuación dada por el corolario anterior llegamos al resultado deseando.

$$N_2 = \sum_{k=3}^{\infty}(k-3)N_k + 3 + \sum_{k=3}^{\infty}(k-3)F_k \geq 3$$

□

En las demostraciones vistas hasta ahora hemos probado ciertas propiedades que son generales a toda familia de conjuntos, pero podemos encontrar familias particulares de conjuntos que posean una cantidad de rectas ordinarias muy cercanas a la cota conjeturada por Dirac.

Para ello se denota por $D_{n,2}$ al máximo número de rectas ordinarias que puede tener un conjunto de n elementos.

Definición 5.3 *Se definen los conjuntos X_{2m} como:*

$$X_{2m} := \{(cos\frac{2\pi j}{m} : sen\frac{2\pi j}{m} : 1) : 0 \leq j < m\} \cup \{(-sin\frac{\pi j}{m} : cos\frac{\pi j}{m} : 0) : 0 \leq j < m\}$$

Definición 5.4 *Se definen los conjuntos conjuntos de Böröczky de n elementos como de la siguiente manera:*

- *Si $n = 2m$ entonces el conjunto es X_{2m}.*

- *Si $n = 4m + 1$ entonces el conjunto es $X_{4m} \cup \{(0 : 0 : 1)\}$.*

- *Si $n = 4m - 1$ entonces el conjunto es $X_{4m} \setminus \{(0 : 1 : 0)\}$*

- *Si $n = 4m + 2$ entonces el conjuntos es X_{4m+2} menos cualquier punto de la línea del infinito.*

Teorema 5.3 *(Teorema de Böröczky) Los conjuntos de Böröczky poseen $n/2$ rectas ordinarias si n es par, de lo contrario poseen $3\lfloor n/4 \rfloor$ rectas ordinarias.*

Y de este resultado obtenemos inercialmente la siguiente cota para $D_{2,n}$, siendo $D_{2,n}$ el máximo valor valor para N_2 de los conjuntos de n elementos del proyectivo:

Corolario 5.3

$$D_{2,n} \geq O(n)$$

Es decir, existe una constante K tal que $D_{2,n} \geq Kn$.

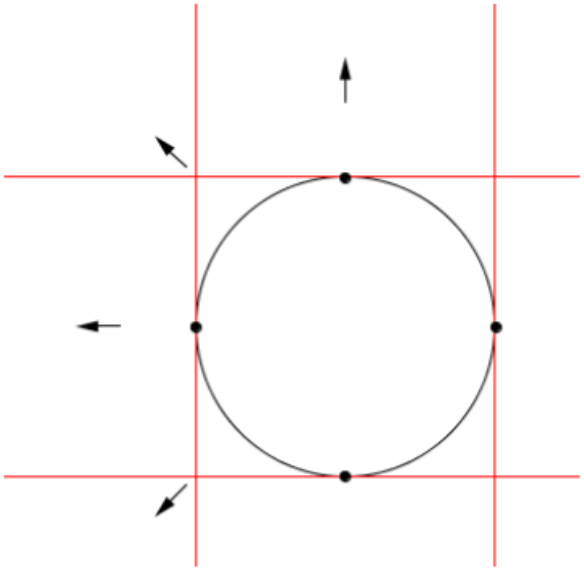

Figure 12: 8 puntos y 4 rectas ordinarias

En las siguientes figuras las flechas representan las direcciones de los puntos en la recta del infinito que forman parte de P.

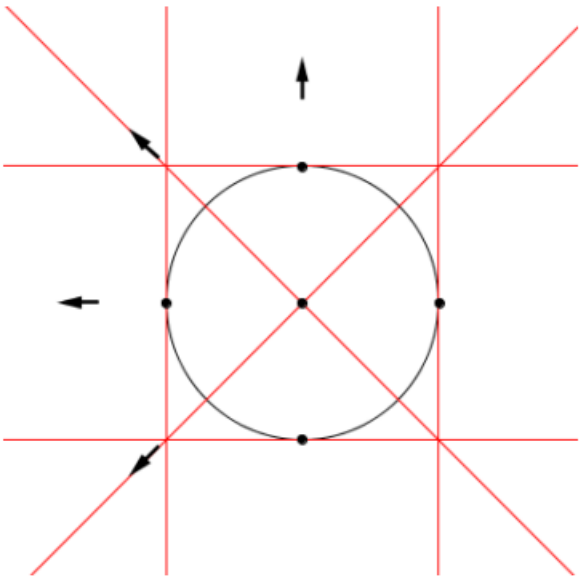

Figure 13: 9 puntos y 6 rectas ordinarias

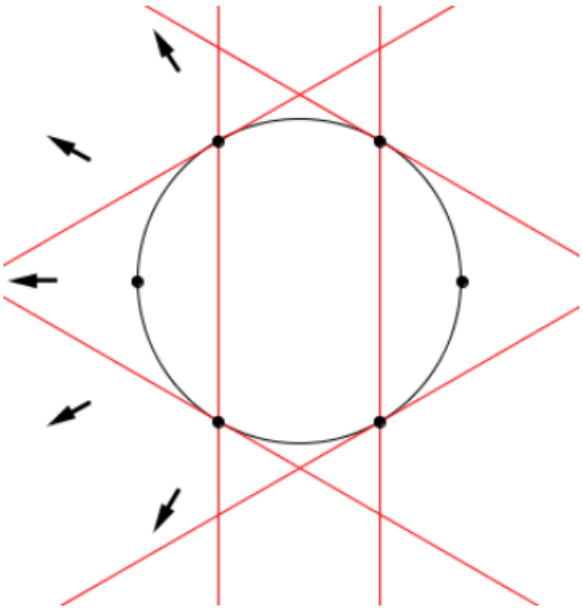

Figure 14: 11 puntos y 6 rectas ordinarias

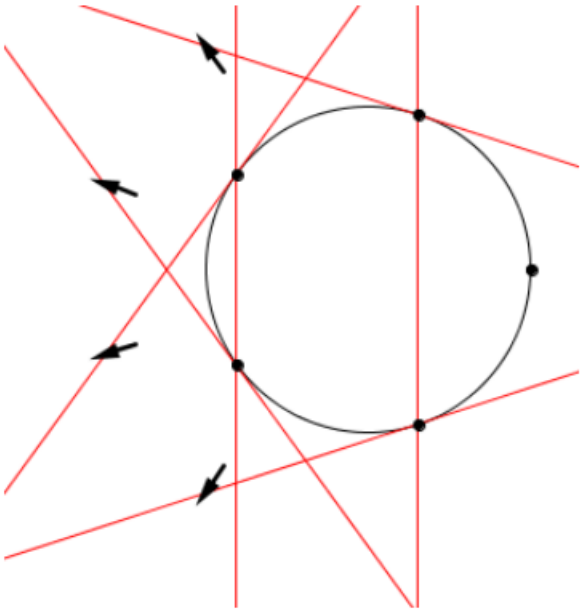

Figure 15: 9 puntos y 6 rectas ordinarias

5.2 Encontrando una Cota Superior:

Esta nueva sección se centrará en encontrar cotas superiores para $D_{2,n}$. Se empezará por un resultado combinatorio clásico basado en el Teorema de Exclusión-Inclusión.

Lema 5.1 *Para todo conjunto de C con cardinal $N \geq 2$ se tiene que:*

$$\sum_{k=2}^{N} \binom{k}{2} N_k = \binom{N}{2}$$

Demostración:

Fijémonos que $\binom{N}{2}$ es el número total de pares de puntos que puedo tomar en C. Por otro lado, el numero de pares de puntos que puedo tomar de una recta $k-$incidente es $\binom{k}{2}$. A su vez la cantidad de pares de puntos pertenecientes a rectas $k-$incidentes serían $N_k\binom{k}{2}$ y la suma de todos estos valores serían el número total de pares de puntos que puedo tomar sobre C.

□

A consecuencia directa de esta igualdad se obtiene el siguiente corolario:

Corolario 5.4 *Para todo conjunto de N puntos C sobre el plano, no todos ellos alineados, se tiene la siguiente cota:*

$$N_3 \leq \frac{1}{3}\binom{N}{2} - 1$$

Demostración:

$$\binom{N}{2} = \sum_{k=2}^{N} \binom{k}{2} N_k \geq 3N_3 + N_2 =_* 3N_3 + 3$$

*La última de las desigualdades se debe al teorema de Melchior.

□

A partir de aquí vamos a lanzar otro problema abierto, *El Problema de la Huerta*, en el que nos vamos a apoyar para seguir avanzando en el resultado.

> ¿Cúal es mayor valor que puede tomar N_3 para un conjunto de N puntos arbitrario?

Denotamos por $D_{n,3}$ al máximo valor de N_3 que pueden tomar los conjuntos de n puntos sobre el plano.

Es obvio por el corolario anterior que $D_{n,3} \leq \frac{n^2-n-2}{6}$. Por otro lado, apoyándonos en la estructura de grupo asociada a una curva elíptica veremos que $D_{n,3} \geq \frac{n^2-3n}{6}$.

Teorema 5.4 *Sea E una curva elíptica, $O \in E$ un punto sin pérdida de generalidad, $(E, +; O)$ el grupo inducido por E y $H < (E, +; O)$ un subgrupo de este tal que $ord(H) = n$. Entonces H posee asociadas $\frac{n^2-3n}{6}$ rectas $3-$incidentes.*

Demostración: Por (4.1) toda recta que corte a E en dos de sus puntos o lo hace también en un tercero o es la recta tangente a E por uno de estos puntos y sólo la corta por estos dos, así pues, por herencia, las rectas asociadas a H o son ordinarias o son $3-$incidentes.

Además, el lema (4.1) se sigue cumpliendo sobre H. Véase que si $P_1, P_2 \in H$ entonces el tercer punto de corte $P_1 * P_2$ se encuentra en H por ser el inverso de $P_1 + P_2$ y este ser un subgrupo.

Así pues, las rectas ordinarias en H serán las tangentes a E por esos n puntos, es decir, n. Por otro lado el número de pares de puntos en H es $\binom{n}{2}$, de entre estos,

n pares conforman rectas ordinarias y aplicando que cada recta 3−incidente posee asociados tres pares de puntos de H se tiene que:

$$N_3 = \frac{\binom{n}{2} - n}{3} = \frac{n^2 - 3n}{6}$$

□

El teorema anterior se puede generalizar para grupos inducidos por los puntos regulares de una cúbica y sus clases respecto de un elemento. Al no haber tratado estos detenidamente se limitará a expresar que estos sobre estos grupos $N_3 = \frac{n^2-3n}{6} + O(1)$.

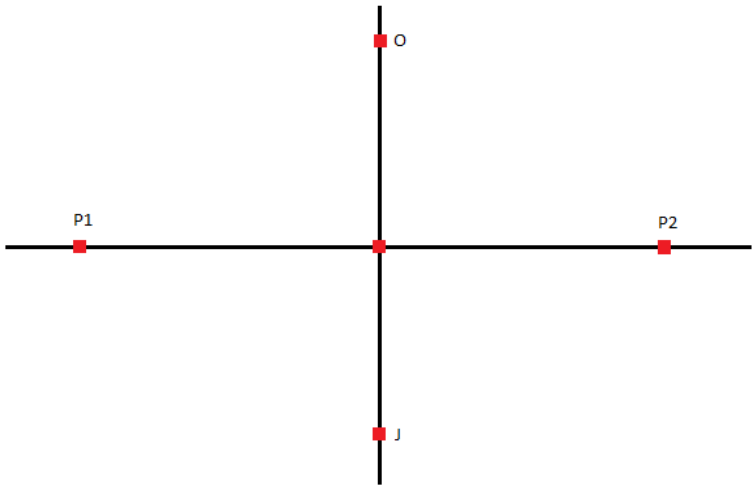

Figure 16: Representación Gráfica del Argumento Anterior

A partir de (5.1) podemos volver a nuestro problema de interés y encontrar una cota superior a N_2 para un caso concreto.

Proposición 5.1 *Sea C un conjunto de n puntos no todos ellos alineados. Si $N_3 \leq \frac{n^2-3n}{6}$ entonces se tiene que $N_2 \leq O(n)$. Es decir $N_2 \leq Kn$ para $K = 1$*

Demostración: Acudiendo a la ecuación del lema (5.1) encontramos que:

$$N_2 \leq \binom{n}{2} - 3N_3 \leq \frac{n^2-n}{2} - \frac{n^2-3n}{2} = n$$

□

5.3 Resultados Asintóticos:

Finalmente se cerrará este escrito con un resultado probado por Terence Tao y Ben Green en el año 2013. No se entrará en detalles sobre su demostración debido a la extensión.

Teorema 5.5 *(Teorema de Estructura Débil) Sea P un conjunto de puntos en posición general del plano. Si P posee asociadas Kn rectas ordinarias con $K > 0$ entonces el conjunto puede ser cubierto con a lo sumo $500Kn$ cúbicas.*

Teorema 5.6 *(Teorema de Estructura Fuerte) Supongamos que C es un conjunto de puntos sobre el plano proyectivo, K un natural y supongamos que C posee asociadas a lo sumo Kn rectas ordinarias. Si $n >> expexp(CK^C)$ para algún C lo suficientemente grande entonces aplicando una proyectividad P difiere a lo sumo en $O(K)$ puntos de de uno de los siguientes conjuntos:*

- *Todos los puntos alineados menos $O(K)$*
- *Un conjunto de Böröczky con $m = n/2 - O(K^{O(1)})$.*
- *Una clase de algún subgrupo inducido por los puntos regulares de una curva cúbica de orden $n - O(K^{O(1)})$.*

En consecuencia todos esos conjuntos poseen a lo sumo $O(Kn)$ rectas ordinarias.

Asumiendo que dicha proyectividad exista los resultados expuestos en esta sección confirman la veracidad del resultado.

Nota: La versión de Chasles y Pappus del Teorema de Cayley-Bacharach se utiliza sistemáticamente en estos problemas, ya que se establece una dualidad entre retículos triangulares dados por rectas en el plano y la aritmética de curvas elípticas.

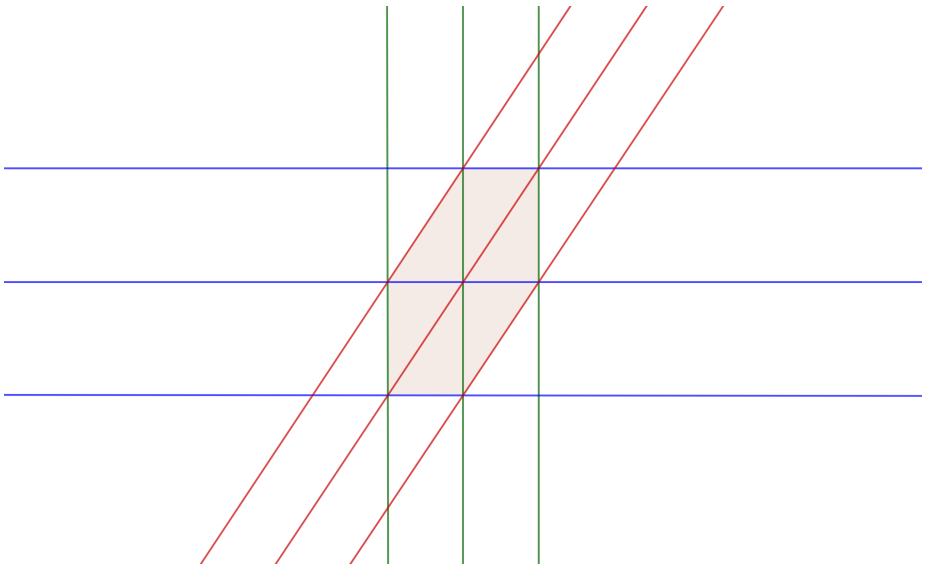

Figure 17: Retículo presentado en la Nota

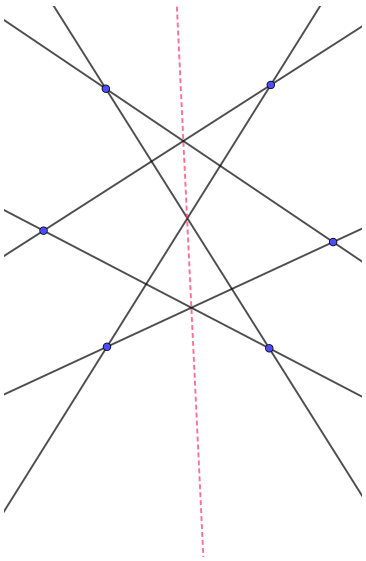

Figure 18: Dual del Retículo

Como ejemplos suficientes se tienen los lemas (4.3) y los teoremas de estructura de Green-Tao. En otras palabra, la dualidad de los grafos dados por retículos se expresa en términos de la ley de grupo inducida por una curva elíptica mediante mediación del Teorema de Cayley-Bacharach.

6 Bibliografía:

(1) D. Eisenbud, M. Green, J. Harris, Cayley-Bacharach Theorems and Conjectures, Bull. Amer. Math. Soc. 33, 1996, p. 295-324

(2) W. Fulton, Curvas Algebraicas, Edición en Español, 2009, Editorial Reverté, p. 80-82

(3) C. Ivorra, Curvas Elípticas, https://www.uv.es/ivorra/Libros/Elipticas.pdf, p. 31-53

(4) E. Melchior, Über Vielseite der Projektiven Ebene, Deutsche Math., 5, 1940, p. 461-475

(5) M.J. de la Puente, Curvas Algebraicas y Planas, Primera Edición, 2007, Universidad de Cádiz, p. 25,32, 39-49

(6) J.R. Smith, Introduction to Algebraic Geometry, Second Edition, 2021, Five Dimension Press, p. 4-9, 13-14, 15-17

(7) T. Tao, B. Green, On Sets Defining Few Ordinary Lines, 2013 p. 1-13, 19-23

7 Referencias:

(1) I. Bacharach. Ueber den Cayley'schen Schnittpunktsatz, Springer Berlin / Heidelberg, 26, 1886, p. 275-299.

(2) E. Bezout, Théorie génerale des équations algébraiques, D. Pierres, Paris, Primera Edición, 1779

(3) M. Chasles, Traité des sections coniques, Gauthier-Villars, Paris, 1861

(4) G. Cramer, Introduction á l'analyse de lignes courbes algébriques, Primera Edición, Génova, 1750

(5) L. Euler, Elementa Doctrinae Solidorum, 1758, p. 119-124

(6) C. Maclaurin, De Linearum Geometricarum Propietatibus, Primera Edición, Londres, 1720

(7) C. Maclaurin, Geometrías Orgánicas, Primera Edición, Londres, 1720

(8) B. Pascal, Essay pour les Coniques, 1640