International Journal of Mathematical Archive-8(1), 2017, 200-205
Available online through www.ijma.info ISSN 2229 – 5046

CUBICS IN PROJECTIVE SPACES (IJM)

Dr. S. VASUNDHARA*

**Asst. Prof of Mathematics, G. Narayanamma Institute of Technology & science for Women,
Shaikpet, Hyderabad, Telengana, India.**

(Received On: 12-12-16; Revised & Accepted On: 05-01-17)

ABSTRACT

In this paper we discussed about the properties of projective Spaces and described the cubic curve and its group law.

Key words: *Projective spaces, projective planes, finite translation planes.*

1. INTRODUCTION

Assume K is an Algebraically closed field not of characteristic 2 and let g(x) be a cubic with no repeated roots where $g(x) = ax^3 + bx^2 + cx + d$. Let $f(x, y) = y^2 - g(x)$ and $F(X, Y, Z) = ZY^2 - aX3 - bZX^2 - cZ^2X - dZ^2$ be irreducible cubics so that neither contains a line or a conic. Suppose $E \in K[X, Y, Z]$ is a cubic form defining a non-empty plane curve $C: (E = 0) \subset P^2(K)$. Then the set is a cubic form defining a non-empty plane curve C: (E = 0) $P^2(K)$. Then the set

$$E = \{(X: Y: Z) \in P^2(K) \setminus F(X, Y, Z) = 0\}$$
$$= \{(x, y) \in A^2(K) \setminus f(x, y) = 0\} \cup \{(0: 1: 0)\}$$

is called an Elliptic curve.

Now we define our zero elements,

Definition: Let O = (0: 1: 0) be the point at infinity on E. Then we define $T_O(E) = L_\infty$. We note that F/L_∞ has a triple root at O. Next we define the addition of points on E by first defining the third point of intersection and its negative.

Definition: Let $L_{PQ}(E)$ denote the third point on $L_{PQ} \cap E$.That is

1. If $P \neq Q$, $L_{PQ} \neq T_PE$, then there is a genuine third point on E that is neither P nor Q and which we define as $L_{PQ}(E) = P$.
2. If $P \neq Q$, $L_{PQ} = T_PE$, then we define $L_{PQ}(E) = P$.
3. If $P = Q$, $L_{PQ} = T_PE = T_QE$, then there exists a genuine third point that we define as $L_{PQ}(E) = $).

Definition: For any point P we define $-P = L_{PO}(E)$..

Theorem: If $P = (a, b) = (a, b, 1) \in E$ then $-P = (a, -b)$. Furthermore, -O = O.

Proof: We observe that

$$L_{PO} = \{(X: Y: Z) / X - aZ = 0\}$$
$$= \{(x, y) / x = a\} \cup \{(0: 1: 0)\}.$$

Then $L_{PQ} \cap E = \{(a, y) / f(a, y) = y^2 - g(a) = 0\}$.This implies that $b^2 = g(a)$ and so $(-b)^2 = g(a)$ as well. Thus the points on $L_{PQ} \cap E$ are

$$\{P = (a, b), O, -P = (a, -b)\}.$$

Corollary: Fir any point P, we have – (- P = P.

Proof: We know $L_{PQ}(E) = -P$. Furthermore, the point $-(-P) = L_{(-P)O}(E)$, but $L_{(-P)O} = L_{PQ}$ by definition of –P. Thus $L_{(-P)O}(E) = P$.

Corresponding Author: Dr. S. Vasundhara,*
Asst. Prof of Mathematics, G. Narayanamma Institute of Technology & science for Women,
Shaikpet, Hyderabad, Telengana, India.

Finally we arrive at our definition of a sum of two points on a conic.

Definition: We define n operation "+" on E by P + Q = - L_{PQ}(E).

The construction of (A + B) + C above can be seen in the graphic that follows.

Theorem: The set (E, +) is an abelian group where the identity is O and the inverse of P is –P.

Proof: We need to check for associativity, identity, inverse, and commutativity under the operation In E. Let P and Q be the points on E.

1. P + Q = - L_{PQ}(E) = - L_{QP}(E) = Q + P, so (E, +) is commutative.

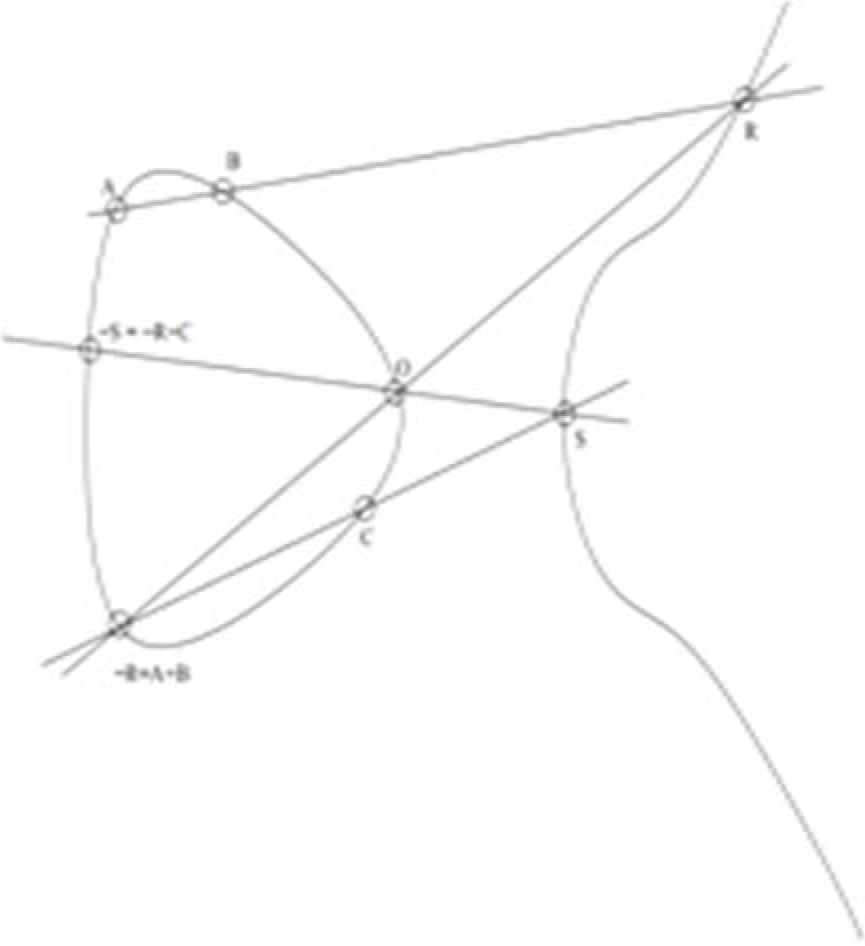

Figure -1.1: Cubic curve and its group law.

P + Q = - L_{PQ}(E) = - (-P), by definition of –P and thus –(-P) = P, so O is the identity element.

1. –P + P = - $L_{(-P)P}$(E) = - O by definition of –P as the third point on the line through O and P, and thus –O=O. So each point has an additive inverse.
2. Proof of Associativity for a special case follows (for a complete proof see silverman [Sil86]). Let A, B and C be the points on E. We begin by constructing (A + B) + C.
   - Let L_{AB}(E) = R.
   - Then $L_{RO(E)=-R=A+B}$, by definition.
   - Now let $L_{(-R)C}$(E) = S.
   - Then $L_{(SO}$(E) = - S = (A + B) + C.
   - Next we construct A + (B + C).
   - Let L_{BC}(E) = Q.
   - Then L_{QO}(E) = - Q = B + C, by definition.
   - Now let $L_{(-Q)A}$(E) = T.
   - Then L_{TO}(E) = - T = A + (B + C).

So we need to show that –S = -T, but it is sufficient to show that S = T.

Let $D_1 = L_{AB} \cup L_{QO} \cup L_{9-Q)A}$.The equations of 3 lines multiplied together yield a cubic, so D_1, D_2 are cubics. Then

$$E \cap D_1 = \{A, B, R, Q, O, - Q, - R, C, S\}$$

And $$E \cap D_2 = \{B, C, Q, R, o, - R, - Q, A, T\}$$

Where these are the only possible points in $E \cap D_1$ and $E \cap D_2$ because F is irreducible so $E \cap D_2 = (E \cap L_{BC}) \cup (E \cap L_{RO})\ (E \cap L_{(-Q)A}$, and similarly $E \cap D_1 = (E \cap L_{AB}) \cup (E \cap L_{Q(O)} \cup (E \cap L_{(-R)C})$. not ethat the first 8 points of each intersection are distinct and in common (here we make the assumption that the 9 points of the first intersections are distinct), so by corollary D_2 passes through the 9 th point as well. That is, S = T and associativity is true.

Corollary: Let k be a subfield of K. Let E be an Elliptic curve defined by $y^2 = x^3 + bx^2 + cx + d$ with a b, c, d $\in$ k. Then

$$E(k) = \{(x, y) \in k^2 \setminus y^2 = ax^3 + bx^2 + cx + d\} \cup \{O\}$$

Is a subgroup of E(k).

Recall that a subset H of a group G is a subgroup of G if and only if H is closed under the operation of G, the identity element of G is in H, and for any element in H it is true that its inverse is also in H

Proof: We first show that if $P \in E(k)$, then $- P \in E(k)$. Let $y \in k$; then $- y \in k$ since k is field. So if $P = (x, y) \in E(k)$, then $-P = (x, -y) \in E(k)$. since $(-y)^2 = ax^3 + bx^2 + cx + d$. Also, $(O) \in E(k)$ by definition.

We now want to show that if P, Q$\in$ E(k) then their third point of intersection on E, $L_{PQ}(E)$, is also in E(k), since it then follows that $P + Q = - L_{PQ}(E) \in E(k)$.

Case-1: Suppose $P \neq Q$ such that P, Q $\in$ E(k). let P = (l, m) and Q = (n, p). Notre that if l = n then
$L_{PQ}(E) = O \in E(k)$. Otherwise,
L_{PQ}: $y = p + \frac{m-p}{l-n}(x - n)$ and
$L_{PQ} \cap E$ is the solution set to
$0 = ax^3 + bx^2 + cx + d - (p+\frac{m-p}{l-n}(x - n))^2$,

A cubic equation in x. since we know that (x = l) and (x = n) be in the intersection they must be rooted of the equation so we may factor them out and this leaves a third root, (x = r), with r in k. Furthermore, we substitute x = r into
$Y = p + \frac{m-p}{l-n} (x - n)$ to get our y-coordinate and so y $\in$ k as well.

Case-2: Suppose P = Q, then L_{PQ} is the tangent line to the curve E at P which is given by the equation $0 = f_x(l, m) (x - l) + f_y(l, m)(y - m)$, where $f_x(l, m)\ 3al^2+2bl+c \in k$ and $f_y(l, m) = 2m \in k$.This equation can be simplified to one of the form $y = \lambda x + v$ for some $\lambda, v \in k$.Substituting into the equation for E we find that $L_{PQ} \cap E$ has a double root at point P = Q so we may factor out (x = l) twice and we are left with a third root, (x = r), with r $\in$ k.

Again we substitute x = r into $y = p + \frac{m-p}{l-n}(x - n)$ to get our y-coordinate and so y $\in$ k as well.

So the third point $L_{PQ}(E) = (r, y)$ in $L_{PQ} \cap E$, is also in E(k).
Thus E(k) is a subgroup of E(K).

Example: Let E be the elliptic curve defined by $y^2 = x^3 - x$ over the field F_{11} (i.e., $E = E(F_{11})$. Note that the square numbers (mod 110 are $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 5$ and $5^2 = 3$.computation shows that the values of x that give us a perfect square on the right side of the equation, mod(11), are x = 0, -1, -2, -3, -4, -5, which yield the 12 points on
E: (0, 0), (1, 0), (-1, 0), (-2, 4), (-2, -4), (-3, 3), (-3, -3), (4, 4), (4, -4), (-5, 1), (-5,-1), O

Example: Let E be the elliptic curve defined by $y^2 = x^3 - x$ over the field F_{11}. Let A = (0, 0), B = (1, 0) and C = (-5, 1).

0	0
1	0
-1	0
-2	4
-2	-4
-3	3
-3	-3
4	4
4	-4
-5	1
-5	-1

The graph is given by:

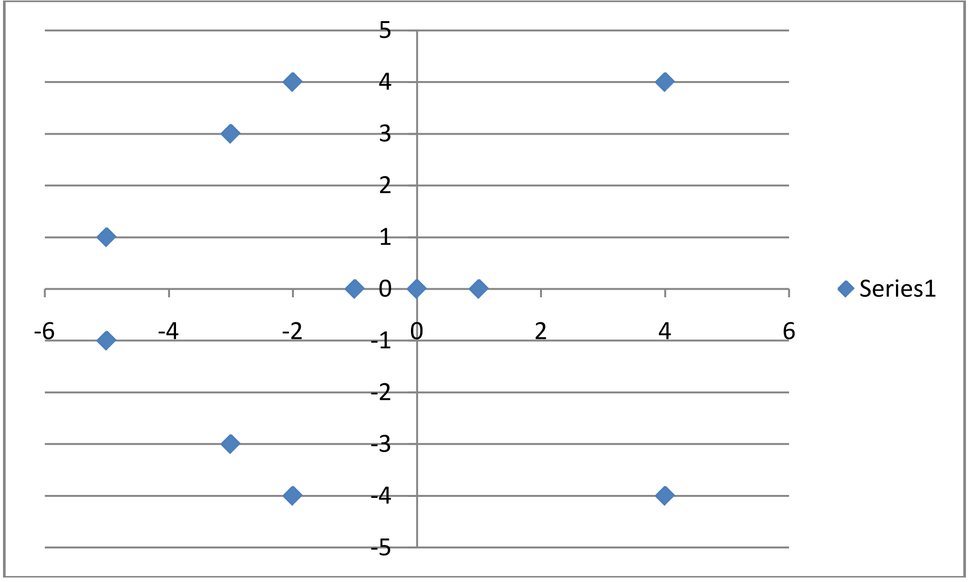

Figure-1

We will illustrate the associativity of points with points A, B, and C. Note that L_{AB}:y = 0,

So

$L_{AB}\cap E$.That is, $L_{AB}(E) = (-1, 0)$. Thus $A + B = - L_{AB}(E) = (-1, 0)$.

Now

$L_{(A+B)C}: Y = \frac{-1}{4}(X + 5) + 1 = - 3(X + 5) + 1) = -3X – 14 = - 3X - 3$ (Mod 11)

So $L_{(A+B)C}\cap E - 3(x + 1))^2 = x^3 – x = x^2 - 1)$.

Simplifying both sides of this equation we see that $(x + 1) (9x + 9) = (x^2 - x) (x + 1)$\

And thus $0 = (x + 1) (x^2 - 10x -9)$ where after division by (x+5) we note that x = - 1, -5, 4 are the three roots to the cubic equation $L_{(A+B)C}\cap E$ however the first two roots correspond to points A+B and C, respectively, so the third root yields the third point of $L_{(A+B)C}\cap E$.That is, since y = - 3(4) - 3,

$L_{(A+B)C}(E) = (4, -4)$.

Thus.

$(A+B)+C= - L_{(A+B)C}\cap (E) = (4, 4)$.

Next we will calculate A + (B + C). Note that

$L_{BC}: y = \frac{1}{-6}(x - 1) = - 2(x - 1)$ (mod 11),

So $L_{BC}\cap E: (-2(x-1))^2 = x^3-x = x(x^2-1)$,

Simplifying both sides we arrive at $(x - 1) (4x - 4) = (x^2 + X) (X - 1)$ and finally $0 = (x^2 - 3X + 4) (X - 1)$ where upon dividing by (x + 5) we note that x =1,-5,-3 are the three roots to the cubic l$L_{BC}\cap E$. That is since y = - 2 (-3-1), $L_{BC}(E) = (-3, 3)$.

Now

$L_{(B+C)A}\cap E = (-x)^2 = x(x^2-1)$.

Simplifying both sides of the equation we see that $0 = (x^2 – x - 1)$ where after division by (x+3) we note that x = 0,-3, 4 are the three roots to the cubic $L_{(B+C)A}\cap E$. Howevwer, the first two roots corresponding to points B + C and A, respectively, so that third root yields the third root of $L_{(B+c)A}\cap E$.That is, since

y = - 4, $L_{(B+C)A}(E) = (4, -4)$.

Thus,

$A + (B + c) = - L_{(B+C)A}\cap E) = (4, 4)$.

So we have illustrated that (A + B) +c = A+ (B + C).

Let E be the elliptic curve defined by $y^2 = x^3 - x$ over the field F_{11}. Let P = (4, 4). Then $T_P(E)$: $- 3(x-4) + 8(y-4) = 0$ or $y=\frac{3x-2}{8}$. Furthermore, $L_{PP}\cap E$:$(\frac{(3x-2)}{8})^2 = x^3 - x$. Simplifying this equation we arrive at $0 = 2(x^3 - x^2 + 4x + 2)$ and after division by (x - 4) twice we note that the third root is also (x = 4). Thus since y = $(\frac{3(4)-2}{8}$, $L_{PP}(E) = (4, 4)$ and

So P + P = (4, - 4) = - P. So we have that (P + P) + P = (-P) + P = O, that is, the order of P is 3.

1.2 PROJECTIVE PLANES

In this chapter we give the background material for the study of finite translation planes, this material can be found in any standard textbook on finite projective planes. For the sake of notation and nomenclature we have used F.Dembowski (6), D.R.Hughes and F.C Piper (12) M.J, Kallahar (13), F.W.Stevenson, Marshall Hall Jr.() and L.M. Blue menthol( ).

A finite projective plane of order n is formally defined as a set of $n^2 + n + 1$ points with the properties that:

1.2.1 Let P be a set of points, let L be a set of lines where each line is a subset of P and .Let I be an incidence relation between elements of P and elements of L. Then the triple (P, L, I) is called a projective plane if:

1. Any two distinct points are incident with a unique line.
2. Any two distinct lines are incident with a unique point.
3. There exists four points no three of which are incident with one line.

1.2.2 Let P, L and I be defined as in 1.1.Then (P, L, I) is called an affine plane if:

i) Any two distinct points are incident with a unique line.
ii) Given a line L and a point P not incident with L, there is a unique line m such that p is incident with m and there is no point incident with both I and m.
iii) There three points not incident with a line.

1.2.3 It is observed that conditions I and ii of definition 1.1 are symmetric with respect to “points “and “lines”. This gives rise to an important principle called the principle of duality. The principle of duality states that any valid theorem or statement in projective plane

remains valid if the words “points” and “lines” are interchanged.5.2.4 If the number of points in a projective plane is finite, the plane is called a finite plane. If the number of points is infinite then it is called an infinite plane.

1.2.5 If a finite projective plane π such that a line L is incident with (n+1) points, then every line of the plane is incident with exactly (n+1) points and every point of π is incident with exactly (n+1) lines. The number n is called the order of the projective plane. A projective plane of order n has n^2+n+ 1 point and n^2+n+ 1 line.

1.2.6 An affine plane A is said to be of order n if each line of A is incident with n points and each Point of A is incident with (n+1) lines. A finite affine plane of order n has n^2 points and n^2+n lines.

1.2.7 Let π be a projective plane and L be a line of π. Let π^1 be the set of points and lines of π obtained by deleting the line L and the point’s incident with L. Then π^1 is an affine plane.

1.2.8 Given a positive integer n it is not known whether or not a projective plane of that order exists. It has been shown by Mayor Tarry in 1900 by the method of trial and error that a projective plane of order 6 does not exist. There have not been many theorems regarding the existence or the non-existence of projective planes. The only important theorem known as Bruck-Ryser theorem which states that “if n≡1 or 2 (mod 4), then there cannot exist a projective plane of order n unless n can be expressed as a sum of two integral squares”. Bruck Ryser theorem confirms Mayor Tarry’s result and excludes an infinite class of integers to be the orders of projective planes. However there do exist infinite positive integers about which it is not known whether they can be orders of projective planes or not? The smallest of these is 10.however if n is a prime number or a prime power there always exists a finite field of that order and thus finite field can be used to construct a projective plane of order.

1.2.9 Two projective planes π_1 and π_2 are said to be isomorphic if there exists one-one onto mapping α of points of π_1 ontopoints of π_2,lines of π_1 onto lines of π_2 such that if for point P and a line L in π_1 such that p is incidence with L then α(L) in π_2.An isomorphism of a projective plane π on to itself is called a collineation of π. If a collineation of π is such that it fixes all points incident with a line L then there exists a point v in π such that every line is incident with v is fixed by the collineation α exists it is called (v,L) central collineation.The point v is called the centre of the collineation.If v is incident with L then the collineation is called an elation, otherwise it is called a homology. All the collineations of a plane π from a group known as the collineation group of π. We mean by a collineation group a subgroup of the full collineation group.

1.3 PROJECTIVE SPACE& AFFINE SPACE:

A projective space*S* can be defined axiomatically as a set *P* (the set of points), together with a set *L* of subsets of *P* (the set of lines), satisfying these axioms:

Each two distinct point's *p* and *q* are in exactly one line.

Veblen's axiom: If *a*, *b*, *c*, *d* are distinct points and the lines through *ab* and *cd* meet, then so do the lines through *ac* and *bd*.

- Any line has at least 3 points on it.

The last axiom eliminates reducible cases that can be written as a disjoint union of projective spaces together with 2-point lines joining any two points in distinct projective spaces. More abstractly, it can be defined as an incidence structure (*P*,*L*,*I*) consisting of a set *P* of points, a set *L* of lines, and an incidence relation I stating which points lie on which lines.

A subspace of the projective space is a subset *X*, such that any line containing two points of *X* is a subset of *X* (that is, completely contained in *X*). The full space and the empty space are always subspaces. The geometric dimension of the space is said to be *n* if that is the largest number for which there is a strictly ascending chain of subspaces of this form.

REFERENCES

1. The Thesis of on 2-Spreads in PG (5, 3) by K. Hanumanthu under the super vision of Prof. K. Satyanarayana.
2. Thesis of Dr. K .V. Durga Prasad: "Construction of Translation planes and Determinition of their translation complements", Ph.D Thesis, Osmania University.
3. A Scalar Multiplication in Elliptic Curve Cryptography with Binary Polynomial Operations in Galois Field Hero Modares (thesis of master science.
4. Huang, J. "Fpga Implementations of Elliptic Curve Cryptography and Tate Pairing Over Binary Field." *University Of North Texas*, August 2007.
5. Tata, E. "Elliptic Curve Cryptography, An Implementation Guide." In *Anoop MS*. India: Anoop, MS, 2007
6. Dale Husem oller. Elliptic Curves. Springer, New York, second edition, 2004.
7. Neil Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48:203{209, 1987.
8. T.G.Ostrom: Finite translation planes", lecture notes in maths158, springer verlag, berlin and Newyork, (1970).

.

Source of support: Nil, Conflict of interest: None Declared.