Note di Matematica Vol. VII, 113-148(1987)

DESIGNS EMBEDDABLE IN A PLANE CUBIC CURVE

(Part 2 of Planar Projective Configurations)

N.S.MENDELSOHN, R. PADMANABHAN and B.WOLK (*)

To Donald Coxeter on his eightieth birthday

INTRODUCTION. A configuration or a design K is a system of p points and m lines such that each point lies on π of the lines and each line contains μ of the points. It is usually denoted by the symbol (p_π, m_μ), with $p\pi = m\mu$. A configuration $K = (p_\pi, m_\mu)$ is said to have a geometric representation if we can draw it in the given geometry meaning that the points and lines of K correspond to points and lines in the geometry such that a point is incident with a line in K iff the same is true in the corresponding geometry. In this paper, we consider the problem of representing such combinatorial designs in the geometry of non-singular cubic curves over the complex projective plane. i.e. we study the problem of embedding them into a non-singular cubic curve in the complex projective plane in such a way that (ijk) is an element of the combinatorial design iff the points corresponding to i,j and k in the cubic curve are collinear. Since a line and a cubic has exactly three common points (counting multiplicity, of course), all our configurations have $\mu = 3$ and hence $p\pi = 3m$. The most

(*) This research of all the three authors was supported by the NSERC of Canada.

classically well-known result of this sort is the design $(9_4,12_3)$ corresponding to the affine plane Z_3xZ_3 which is realized as the nine inflexion points on a non-singular complex cubic (Cf.[1],[4], |10|). In the process of proving such general embedding theorems we witness an enjoyable interplay among several tools of mathematics:

arithmetic notions such as solving equations in the complex torus S^1xS^1
number theoretic notions such as primitive roots and quadratic residues
universal algebraic notions such as identities,implications and term conditions
topological notions such as projective varieties being complete
analytic and geometric notions of tangential relations,inflexions etc.
use of electronic computers in solving equations over large fields.

In terms of universal algebra, a configuration is simply a partial non-associative algebra and our techniques may be construed as embedding this partial algebra into the full incidence algebra <C;*> of a non-singular cubic curve C in the complex projective plane. Using the properties of primitive roots in the Galois fields, we prove that given a prime number $p \geq 11$, there exists a natural number $r \geq 3$ such that the combinatorial difference set design $\{(0,1,r);\ \mathrm{mod}(p-1)\}$ can be embedded into a non-singular cubic curve in the complex projective plane. For several prime numbers p,; r=3 already works.

In the first section, we give the definitions and collect all the necessary algebro-geometric and universal algebraic results needed in the sequel. In Section 2, we prove certain non-embeddability theorems of elementary nature to give the reader a taste of the geometric properties of cubics which allow or deny the inscribing of certain configurations in a cubic curve. In spite of striking similarities between the Pappus and Desargues configurations, it turns out that the latter is not so embeddable. In spirit, this is comparable to the classical result that the Fano configuration is not drawable in the real or complex projective plane - which, in fact, is derived as a consequence. In Section 3, we prove a general embedding theorem which generate infinitely many examples of difference set designs drawable on complex cubics. In the final action 4, we include a partial list of difference set designs obtained using this equational process and include an algorithm of finding arbitrary large difference set designs {(0,1,3); mod N} which can be embedded as sub-partial algebras of a full incidence algebra <C;*> of a non-singular cubic curve in the complex projective plane.

§1. TOOLS AND TECHNICAL LEMMAS.

An irreducible non-singular cubic curve C in the projective plane over the complex field (or, any algebraically closed field, for that matter) is the simplest non-trivial example of the so-called complete algebraic varieties admitting a binary law of composition * which has several nice properties:

(i) *:CxC → C is defined by the familiar geometrically defined chord-tangent construction i.e. P*Q=R where R is the unique third point where the chord PQ meets the curve C again. (if Q=P, then replace the word 'chord' by 'tangent'; see Figure 1)

(ii) The mapping * is regular (i.e. it is a rational function over the field in question)

(iii) The full incidence algebra $<C;*>$ is a symmetric Steiner quasigroup i.e. the binary morphism * satisfies the two identities (SSQ) : $\{x*y=y*x,\ x*(y*x) = y\}$ (Fig.1).

(iv) Given a complex point E on C, the mapping * induces a regular group law, say $+_E$, on C with E as the identity element of the group; simply define $x+y=(x*y)*E$ (Fig.1)

For all the basic concepts connected with projective varieties, complete varieties, rational mappings and regular functions, we refer to the relevant sections of I.R.Shafarevich [20]. For a complete discussion on the chord-tangent construction on cubic curves, see the relevant sections in [9],[13],[15],[16],[18],[20], [21] and [25]. We need the following fundamental lemma (the so-called Rigidity Principle) which serves as a tool for the equational logic of the first order theory of regular functions in a projective curve or a complete variety C (see the Lemma on page 152 of [20] or Lemma 7.1.3 of [22] or Section 2 of [17],[18]).

Let $x = (x_1,x_2,\dots,x_m)$, $y = (y_1,y_2,\dots,y_n)$, $b = (b_1,b_2,\dots,b_n)$ and $z = (z_1,z_2,\dots,z_m)$.

LEMMA 1.1. Let f be a regular function on m+n variables of some projective (or more generally, a complete) variety. Then we have

$$\exists b\ \exists c\ \forall x(f,x,b) = c \Longrightarrow \forall x \forall y \forall z\ f(x,y) = f(z,y).$$

To express it in plain English, this lemma asserts that if the value of f(x,b) does not depend upon the variables x_i for some b in C then the function f is already independent of the variables x_i for all i. In other words, $f(x,y) = f(z,y)$ is an identity in C. This, therefore, can be viewed as a powerful technique for deriving stronger identities from apparently weaker ones. This equational aspect of the first order theory of morphisms of projective varieties was first stated formally in [17] though its use in the literature is very common. Thus the most direct proof of the fact that every complete group variety must be commutative as a group stems from this observation (see e.g. Theorem 7.1.4. of [22]). Also, this property is very close to the so-called Term condition - another equational tool ((G5) of Theorem 1) - found to be very useful in generalizing the notion of commutators to Universal algebra (for brief history, survey and applications to congruence varieties, see [5],[19] and references there).

We now demonstrate the power of the lemma by deriving a few equations which we need in our sequel. Let Σ , Σ' be a sets of equations or implications in, say one binary operation *. Following the notation in [13], we say that

$$\Sigma \models_C \Sigma'$$

if whenever a non-singular plane cubic curve C over the field of complex numbers satisfies the conditions Σ for some binary morphism * then C must satisfy the conditions Σ' as well. This relation "$\models_C$" is, conceptually, very similar to Taylor's notion of "obeying in homotopy" (see [25]). For example, the above result on group laws in projective varieties may now be stated as

$$m \text{ is a group law } \models_C m(x,y) = m(y,x) .$$

LEMMA 1.2. $\{x*y=y*x, x*(y*x)=y\} \models_C \{(((((x*y)*z)*t)*y)*z)*t=x\}$

Proof. Consider the derived 5-ary composite morphism f(x,y,z) defined by

$$f(x,y,z,t) = (((x*y)*z)*t)*y)*z)*t$$

$f(x,b,z,b) = x$ by two applications of the hypothesis $x*y = y*x$, $x*(y*x) = y$ and hence, by the Lemma 1, we conclude that the composite morphism f is independent of the variable z. So we get

$$\begin{aligned} f(x,y,z,t) &= f(x,y,u,t) \quad \text{for all } x,y,z,t,u \\ &= f(x,y,y,t) \quad \text{substituting } u = y \\ &= x \end{aligned}$$

which is the desired conclusion. See Figure 2 for the configuration theorem corresponding to the above identity drawn on a cubic curve.

LEMMA 1.3. The algebra $<C;*>$ satisfies the following conditions:

(G1) $((((x*y)*z)*t)*y)*z)*t = x$

(G2) $(((x*y)*z)*t = (((x*t)*z)*y)$

(G3) $(x*y)*(z*t) = (x*z)*(y*t)$

(G4) $f(x,y)*(u*f(x,z))$ is independent of x for all binary words $f(x,y)$ in the algerba $<C;*>$

(G5) The Term Condition: $f(a,b) = f(a,c) \implies f(x,b)=f(x,c)$ for all x.

Proof. (G1) was obtained in Lemma 1.2. Post-multiplying both sides of (G1) by t,z and y successively and employing $(x*y)*x=y$

each time, we get the identity (G2). Substituting t=x*u and y=x*v in (G2) and using (x*y)*x = y twice we get the median law (G3). We prove the implication (G4) by induction on the length of polynomial f (in the sense of [4]). It is obvious if the word f is of length 1 because of the identity x*(u*x)=u which is free from x. Let now $f(x,y) = f_1(x,y)*f_2(x,y)$. Then

$$\begin{aligned} f*(u * f) &= (f_1 * f_2) * (u *(f_1 * f_2)) \\ &= (f_1 * u) * (f_2 * (f_1 * f_2) \quad \text{by} \quad (G3) \\ &= (f_1 * u) * f_1 \end{aligned}$$

which is now free from the variable x by the induction hypothesis. Finally, we prove the Term Condition by a simple application of (G4). Let f(a,b) = f(a,c) for some binary word f and for some a,b,c in the algebra < C;* >

We have

$$\begin{aligned} f(x,b)*(u*f(x,c) &= (a,b)*(u*f(a,c) && \text{by (G4)} \\ &= u && \text{by (SQ)} \\ &= f(x,c)*(u*f(x,c)) && \text{by (SQ)} \end{aligned}$$

and hence, by right cancellation, we get f(x,b) = f(x,c) for all x in C.

Thus we have proved the following

THEOREM 1.1. $\{SQ\} \models_C \Gamma = \{(G1),(G2),(G3),(G4),(G5)\}$.

Historical Remark: The identity (G1) was first noticed by Yu. I.Manin while studying the various quasigroup structures arising on cubic hypersurfaces (see page 14, [13]). The identity (G3) for plane cubics was first proved by E.M.S. Etherington [3] using the classical Bezout Theorem (see [17] and also [23]). In fact, modulo the two-variable laws {SQ} of Lemma 2, the three identities {(G1), (G2), (G3)} are equivalent. Naturally, the configuration theorems corresponding to these laws must all be the same and is, in fact, equivalent to the associativity of the group law defined on cubics (see Figure 2). In what follows, we will use all the five rules without further comment. We need just two more facts connecting geometry and algebra on the plane cubic curves before proving the embedding theorems.

LEMMA 1.4. For a point P on C the following statements are equivalent:

(i) P is an inflexion point of the cubic curve C

(ii) $P*P = P$ in the full incidence algebra $<C;*>$

(iii) Three points X,Y,Z form a complete linear cycle on C iff $X +_p Y +_p Z = P$

Proof. By the definition of the chord-tangent construction, it is obvious that (i) and (ii) are equivalent. Let P be an idempotent element of the groupoid * and consider the induced group operation $+_p$. Now, X,Y and Z will be collinear iff $X*Y = Z$. Writing + for $+_p$,

$$\begin{aligned} X + Y + Z &= X + Y + X*Y \\ &= (((X*Y)*P)*(X*Y))*P \\ &= P*P \\ &= P. \end{aligned}$$

Conversely, if $X+Y+Z = P$, then $(((X*Y)*P)*Z)*P=P$ or $((X*Y)*P)*Z=P$ or $((X*Y)*P = Z*P$ or simply, $X*Y = Z$, i.e. the three points X,Y and Z are collinear. Thus (ii) → (iii). Finally, applying (iii) to the complete linear cycle $\{P,P,P*P\}$, we get that

$$(((P*P)*P)*(P*P))*P = P, \text{ or simply, } P*P = P$$

which is (ii). It is because of the ease and importance of this celebrated connection (iii) between the algebra and geometry (see Theorem 7.33 in [15] or Theorem 19.4 in [16]), one always chooses an inflexion point P for defining the group law $+_P$. We do this without further comment. Note, in particular, that a point Q is an inflexion point of the cubic C iff $3Q=P$, the zero of the group.

Associativity of this group operation $+_E$ is simply a restatement of - and is equivalent to - the equational identities of Lemma 1.3 (see Fig. 2). As a topological group, it is known that C is a connected compact complex Lie group of complex dimension 1 and so is isomorphic to the product of two circles i.e. it is a torus S^1xS^1 (Cf. p.347 in [20], p.15 in [23], or §6 in [24]). From this information, we can readily extract several first order sentences valid for the incidence algebra $<C;*>$ of a non-singular complex cubic curve C. For example, let us derive the well-known geometric property mentioned above that C has precisely nine points of inflexion. As we saw before, P is a flex iff $P*P=P$ or $P+_EP+_EP=E$, i.e. $3P = 0$ in the group S^1xS^1. Treating the elements of S^1xS^1 as, say unimodular complex numbers, we see right away that the equation $3x=0$ has exactly $3x3=9$ solutions in the group. Similarly, there are exactly four solutions to the equation $2x=0$ and so on.

More generally, there are precisely n^2 points of order n. For future use, we record this as

LEMMA 1.5 (Cf. p.329 in [9]; see also p.18 in [23]). Given any natural number n, there are precisely n^2 points of order n in the group <C;+,E>.

This last Lemma will be very useful in both constructing an actual representation for a given combinatorial design as a configuration on a complex cubic curve as well to prove the impossibility of such an embedding in certain other designs.

§2. CERTAIN NON-EMBEDDABILITY THEOREMS.

Let C be the set of all points on a complex cubic curve. A subset K of C is said to be closed if its points satisfy the following two closure conditions:

(1) If P and Q are members of K then the line PQ meets the cubic only in points of K

(2) If P is a member of K then the tangent at P to the curve meets C only in points of K.

In other words, a closed set K is simply a subalgebra of the full incidence algebra <C;*> where * is the chord-tangent construction defined in the introduction. If M is a subset of C, then we define the closure of M to be the smallest closed set containing M. If a closed set is finite then we call it the point set of a *cubic cluster* and if it has n points, then we call it the point set of an *n-cluster*. The *n-cluster* itself consists of its point set together with all lines joining points of its set and the set of tangents at the points of its set.

Let $a,b<n$ be such that the six elments $\{a,-a,b,-b,a-b,b-a\}$ are pairwise different mod n. Then we define

$$\{(0,a,b);\text{mod } n\} = \{(i,a+i,b+i)\,|\,i=0,1,\ldots,n-1\} \subseteq Z_n^3$$

and call it a cyclic difference set design. Such a design can also be viewed as a partial binary algebra satisfying the laws SQ where $a*b = c$ iff the triple (a,b,c) belongs to the design. Sometimes, it can be drawn geometrically in the real plane RxR in such a-way that (a,b,c) belongs to the design iff the points corresponding to a,b and c are collinear in the geometric configuration (see [1],[5],[10] and [14]). Here we show that the Desargues configuration $(10_3,10_3)$ cannot be inscribed in a cubic cluster of any non-singular complex cubic curve. This may be compared with the related Pappus configuration $(9_3,9_3)$; this can be extended to a $(9_4,12_3)$ configuration, the affine plane over the field Z_3; this latter design cannot be drawn on the plane RxR but, however, it can be realized as the 9 inflexion points on a complex cubic (see e.g. [1],[4],[10],[23] and also Theorem 3.1 below).

Let $\partial(o,a,b,c;p,q,r,u,v,w)$ denote the statement that the ten points lie on a non-singular complex cubic curve and also form the configuration $(10_3,10_3)$ which is isomorphic to the classical Desargues configuration with the two triangles $\{a,b,c\}$ and $\{p,q,r\}$ being centrally persepective through o (see Figure 5). Because the complex projective plane satisfies the Desargues Theorem, the two triangles are axially perspective, with $\{u,v,w\}$ being the axis of perspectivity. Since a straingh line and a cubic can have atmost three points in common, we have the equalities

$$b*c = q*r = u, \; a*c = p*r = v, a, \; a*b = p*q = u*v = w.$$

We now show that these equations are incompatible with the laws valid on a plane cubic curve. More precisely, we prove that

LEMMA 5. $\partial(o;a,b,c;p,q,r,u,v,w) \models_C |\{o,a,b,c,p,q,r,u,v,w\}| \leq 4.$

Proof.

$$\begin{aligned} o*o &= (p * a) * (q * b) \\ &= (p * q) * (a * b) \\ &= w * w \end{aligned}$$

and so, by symmetry, $o*o=u*u=v*v=w*w$.

Also $$\begin{aligned} a*a &= (b * w) * (c * v) \\ &= (b * c) * (w * v) \\ &= u * u = o * o \end{aligned}$$

and hence

$$x * x = y * y = E \quad \textit{for all } x,y \in \{o,a,b,c,p,q,r,u,v,w\}$$

where E is a fixed point on the cubic.

Moreover, $$\begin{aligned} E*E &= (a *a) * (b * b) \\ &= (a * b) * (a * b) \\ &= w * w \\ &= E \end{aligned}$$

and hence E is a point of inflexion of the cubic curve.

Since $x * x = E$ for all $x \in \{o,a,b,c,p,r,u,v,w\}$, we have ten points on the cubic from which we can draw tangents to meet the cubic curve again at E. This is clearly impossible because, choosing this E as the origin for the group law, we have $-2x=0$ for all x in the configuration. But, by Lemma 3, the underlying group S^1xS^1 cannot accommodate more than four points of order 2. Thus we have completed the proof of the

THEOREM 2.1. *No Desargues configuration containing more than four points can be inscribed in any cubic cluster of a non-singular cubic curve over the complex field.*

COROLLARY 2.1. The Fano configuration $D_7=(7_3,7_3)\cong\{(1,2,4);\text{mod } 7\}$ cannot be inscribed in any cubic cluster of a non-singular cubic curve over the complex field.

Proof. Let, if possible, $\{a,b,c,p,q,r,o\} \simeq (7_3,7_3)$ be drawable somewhere on a non-singular complex cubic curve. These seven points do contain the closed Desargues configuration $\partial\{o;a,b,c;p,q,r;r,p,q\}$ as can easily be checked from Figure 6. This is a contradiction to our Theorem 4, since 7>4.

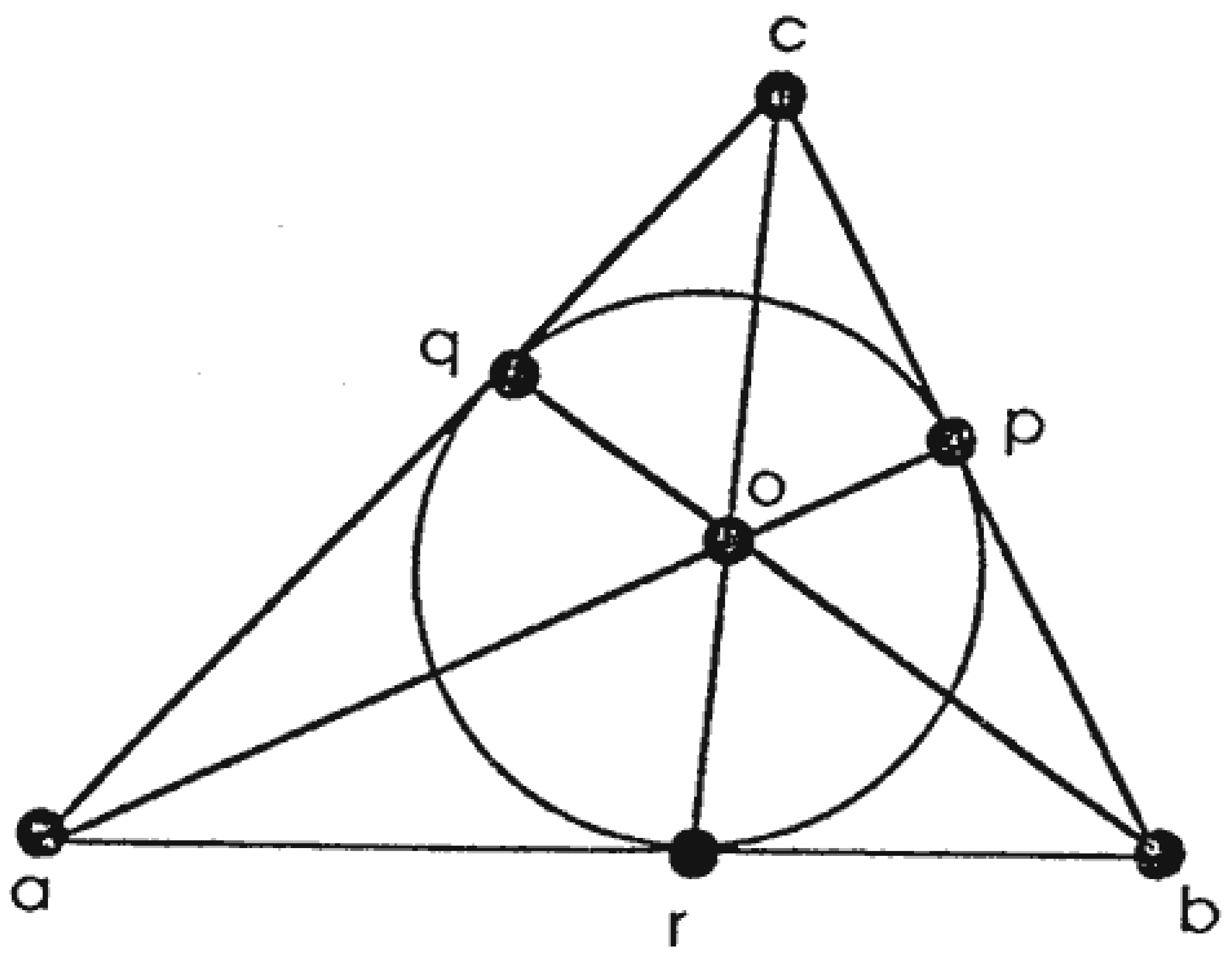


Figure 6.

From this we can derive a classically known result (see e.g. p.100 in [7]) that the Fano configuration is not drawable anywhere in the complex plane. This is because of the simple fact that given seven complex points such that no four of them collinear one can find a doubly infinite family of plane cubic curves passing through all of them (see e.g. p.110) in [6]) and hence once again we have the situation as in the hypothesis of the last corollary. Of course, this is like killing a fly with an armada. The usual proof of this fact is that the presence of this 7_3 configuration anywhere in the projective plane over a field will imply the existence of elements of order 2 in that field and of course, the complex field has no such elements. On the contrary, the complex torus $S^1 x S^1$ does contain elements of order 2 but not sufficient enough to label all the elements of the Fano configuration. We mention this just to show the inter-relations among the various realizations of designs thus demonstrating the unity of mathematics! We conclude this section by giving two more examples of results of impossibility.

THEOREM 2.2. *The two cyclic difference set designs* {(1,2,4);mod 14} *cannot be embedded in any non-singular complex cubic curve.*

Proof. Recall the definition of the respective designs as sets of triples:

1,2,4
2,3,5
3,4,6
4,5,0
5,6,1
6,0,2
0,1,3

{(0,1,3); mod 7}

1,2,4
2,3,5
3,4,6
4,5,7
5,6,8
6,7,9
7,8,10
8,9,11
...
...
0,1,3

{(1,3); mod 14}

Now, if an incidence algebra <C;*> contains the cyclic design D_{14} = {(1,2,4) mod 14} for some complex cubic C then it must contain a subalgebra D_7 of seven points isomorphic to the anti Fano configuration as shown in Figure 3(b) above. Let us prove, say, one of those collinearity relations:

$$(1*8)*(3*10) = (1*3)*(8*10) = 14*7$$

and thus the three points 1*8,3*10 and 14*7 must be collinear on C. However, we have already establised that the design D_7 cannot be a subalgebra of the incidence algebra <C;*>. This proves that the design D_{14} cannot be embedded either.

THEOREM 2.3. *The cyclic difference set design* {(0,1,4); mod 13} *cannot be embedded in any complex cubic curve.*

Proof. In fact, what we really prove is that $\{(0,1,4)\text{:mod } 13\} \models_C \{i*i=I\ \forall i\}$ which simply demonstrates the inconsistency of the the defining conditions of the 14-point geometric configuration {(0,1,4); mod 13} with the laws on a complex cubic. By Lemma 1.4, i*i=i iff the point corresponding to i is an inflexion point on the curve but, by Lemma 1.5, a cubic curve cannot have more than 9 inflexion points. Let us now compute to derive the desired contradiction:

$$0*0=(1*4)*0=(11*10)*4)*0=((0*10)*4)*11=(9*4)*11=(12*8)*4)*11=(11*8)*4)*12=0.$$

Since adding '1' is an automorphism for all cyclic designs, we really have proved that i*i=i for all i. It will rather be illuminating to give a quick proof of Theorem 2.1 using the parametric representation of the doubly periodic elliptic functions of Weiestrass.

§3. EMBEDDING CYCLIC DIFFERENCE SETS INTO CUBIC CLUSTERS.

Let I be the set of all inflexion points of a non-singular complex cubic C. We already know that I is closed for the binary operation * of chord-tangent construction. The structure of I is completely well-known: it is precisely the classical 9-point configuration of Pappus-Pascal Theorem (se e.g. [1],[4],[10] and [17]) and, to quote from Hilbert and Cohn-Vossen (see p.132 in [10]), it is completely well-known: it is precisely the classical 9-point configuration of Pappus-Pascal Theorem (se e.g. [1],[4],[10] and [17]) and, to quote from Hilbert and Cohn-Vossen (see p.132 in [10]), it is perhaps the single most important configuration in the whole of geometry. In the Theorem below we demonstrate its embeddability into a cubic curve by our equational approach.

THEOREM 3.1.

(i) *Algebraically, the algebra* $\langle I,*\rangle$ *is isomorphic to the idempotent reduct of the abelian group* $\langle Z_3 \times Z_3;*\rangle$ *where now* $x*y = 2x + 2y \pmod 3$.

(ii) *Combinatorially, the incidence structure* I *is isomorphic to the direct product of two copies of the unique Steiner triple system on three elements.*

(iii) *Geometrically, the configuration system* I *is the Pappus configuration* $(9_4,12_3)$ *and it closes to a 9-cluster by simply adding the nine tangents to* C *at the individual flexes.*

Proof. Since I contains 9 elements and any straight line can meet C in atmost three points, we can find three elements of I which are not collinear in the complex projective plane. Let {a,b,d} be three such flexes of the the complex curve C. This simply means that $a*b \neq d$; $a*d \neq b$; $b*d \neq a$. Already we know that any two flexes must go through a third. We now claim that the nine flexes of the cubic are precisely the following (see Figure 5):

$$\{a,b,d,a*b,a*d,b*d,a*(b*d),b*(a*d),d*(a*b)\}.$$

It is clear that all these points are flexes because they are all idempotent, thanks to the median law. The only question is that whether they are distinct. Since a,b and d are linearly independent, it is clear that $|\{a,b,d,a*b,a*d,b*d\}|=6$. If $a=a*(b*d)$ then we have $a*a = a*(b*d)$ and hence $a = b*d$, a contradiction to the choice of a,b and d. And since a cubic cannot accommodate more than nine flexes, the above set must be the set of all flexes. Still, it is not clear why the collinearities indicated in the Pappus configuration above must be valid at all! They are simple consequences of the laws on the cubic we have already established. Let us prove these additional collinearities now.

$$(b*d)*((a*b)*d) = (b*(a*b))*(d*d) = a*d$$
$$d*(a*(b*d)) = b*(a*(d*d)) = b*(a*d)$$

and

$$(a*b)*(a*d) = (a*a)*(b*d) = a*(b*d) \ .$$

Even though the above proofs are equational, they all are concealed applications of the classical Bezout theorem (or "intersection theorems") valid for projective plane curves (see pp. 124-125 in [6] and also [3]). Also, for some universal algebraists, this proof should be reminiscent of enumerating the set of all of essentially ternary polynomials of a free algebra having the polynomial sequence (0,0,1,3,5,...), see Theorem 3 in [8]. This completes the proof of the remaining collinearities of the Pappus configuration. Let us define

c = a*b, e = a*(b*d), f = b*(a*d), g = b*d, h = (a*b)*d and i=a*d.

Now the full incidence algebra < I,* > is given by the following table:

*	a	b	c	d	e	f	g	h	i
a	a	c	b	i	g	h	e	f	d
b	c	b	a	g	h	i	d	e	f
c	b	a	c	h	i	g	f	d	e
d	i	g	h	d	f	e	b	c	a
e	g	h	i	f	e	d	a	b	c
f	h	i	g	e	d	f	c	a	b
g	e	d	f	b	a	c	g	i	h
h	f	e	d	c	b	a	i	h	g
i	d	f	e	a	c	b	h	g	i

The isomorphisms mentioned in the theorem are illustrated in the Figure 7.

We will now generalize the above construction to any three arbitrary points {a,b,d} of general position on the cubic curve. For three non-collinear points a,b and d, let $\pi(a,b,d)$ denote the specific statement that the subgoupoid {a,b,d,a*b,a*(b*d),d*(a*(b*d)), b*d,(a*b)*d } is a Pappus configuration as shown in Figure 5. We first prove a lemma establishing a connection between the two points a and d, which is automatically satisfied when a and d happen to be points of inflexions as in the case of Theorem 2.

LEMMA 3.1. $\pi(a,b,d) \models_C \{a*(d*d) = (a*a)*d\}$.

Proof. Assume $\pi(a,b,d)$. As in the proof of Theorem 2, define

$$c = a*b,\ e=a*(b*d),\ f=d*(a*(b*d)),\ g=b*d \text{ and } h=(a*b)*d.$$

Now the assumption $\pi(a,b,d)$ implies that a,b and f are collinear. This means that

$$a*((a*b)*d) = d*(a*(b*d)).$$

But, by applying the second identity proved in Theorem 1 to both sides of the above equality, we obtain

$$b*((a*a)*d = b*(a*(d*d))$$

and left-cancelling the common element b we get the desired result

$$\pi(a,b,d) \models_C \{a*(d*d) = (a*a)*d\}.$$

Using the equational laws SSQ and the two identities of Theorem 1, it is not hard to show that the nine points

$$\{a,b,d,c,e,f,g,h \text{ and } i = a*(d*d) = (a*a)*d\}$$

do form a closed configuration $(9_3,9_3)$ on the complex cubic which is, obviously, isomorphic to the Pappus configuration (see Figure 5). Let us prove two of the three remaining collinearities:

$$c*e = (a*b)*(a*(b*d)) = (a*a)*(b*(b*d)) = (a*a)*d = i$$

and

$$g*h = (b*d)*((a*b)*d) = (b*(a*b))*(d*d) = a*(d*d) = i.$$

In fact, the groupoid generated by them is identical to that of the table given in Theorem 2 but for the entries in the main diagonal. Since these points need not be flexes, they need not be idempotent.

Thus we have completed the proof of the following

THEOREM 3.2. *The Pappus configuration can be realized as a cubic cluster of a non-singular cubic curve with two degrees of freedom.*

REMARK. As mentioned in the introduction, this result is *not* new. Feld gave a proof of this fact in 1936 (see [4]) using the complex elliptic function of Weierstass. See Berman [1] for a nice generalization, again using the doubly periodic meromorphic functions.

THEOREM 3.3. *The cyclic different set design based* {(0,1,3);mod 10}*can be embedded in a cubic cluster. The closure of the points of the design form a* 11-*cluster.*

Proof. If the design

0,1,3
1,2,4
2,3,5
3,4,6
4,5,7
5,6,8
6,7,9
7,8,0
8,9,1
9,0,2

{(0,1,3); mod 10}

is embeddable into a cubic cluster, then the above partial algebra must satisfy all the cubic laws Γ . As before, using these, we derive further incidence relations among these points, in particular, the tangency relations.

$$\begin{aligned} 0*0 &= (1*3)*0 \\ &= ((9*8)*3)*0 \\ &= (9*0)*3)*8 \quad \text{......... by G2} \\ &= (2*3)*8 \\ &= 5*8 \\ &= 6 \end{aligned}$$

and i → i+k is an automorphism of the design, we see that $i*i=i+6 \pmod{10}$ for all i. Geometrically, this means that the tangent at the point corresponding to i must pass through the point corresponding to 1+6 on the cubic curve (see Figure 4).

Also,

$$\begin{aligned} 0*5 &= (9*2)*(7*4) \\ &= (9*7)*(2*4) \quad \text{.... by G3} \\ &= 6*1 \end{aligned}$$

and similarly,

$$i*(i+5) = j*(j+5) = -\infty \quad \text{, say.}$$

Now

$$\begin{aligned} (-\infty)*(-\infty) &= (0*5)*(0*5) \\ &= (0*0)*(5*5) \\ &= 6*1 \\ &= 0*5 \\ &= (-\infty). \end{aligned}$$

and so the point corresponding to $-\infty$ must be an inflexion point on the cubic. Choosing this inflexion point as the identity element we define the group law on the cubic as

$$x + y = (x * y)*(-\infty)$$

where now the binary morphism '*' stands for the classical chord-tangent construction described in the Section 1. We need to derive one more relation among the points in the design before we achieve our actual embedding of it as a cubic cluster. Writing i^2 for $i*i$,

$$((((i^2)^2)^2)^2)^2 = ((((i+6)^2)^2)^2)^2=(((i+2)^2)^2)^2=((i+8)^2)^2=(i+4)^2=i.$$

In other words, the point P corrsponding to any i must satisfy the equation $-32P = P$ or $33P = -\infty$. This will be case if we choose P to be a point of order 11 (3 is no good because then P will itself be an inflexion point but 0 is not idempotent: $0*0=6\neq 0$). From Lemma 4 we know that there are 121 points of order 11 on a non-singular cubic curve in the complex plane. Choose any such point P and define

$$\phi(i) = 2^i P$$

where 2^i is calculated (mod 11), of course.

We also know that three points P,Q and R on the cubic will be collinear iff $P+Q+R=0$ under the group law. Let us now verify the preservation of collinearities under this embedding:

$$(01j) \text{ iff } P+2P+2^jP=-\infty \text{ iff } (1+2+2^j)=0 \pmod{11} \text{ iff } 2^j=8 \pmod{11} \text{ iff } j=3$$

and thus we have embedded our initial design {(0,1,3);mod 10} into a cubic cluster.

Now 2 is a primitive root of the prime number 11 and moreover it is a root of the equation

$$x^3 + x + 1 = 0$$

in the field Z[11]. A primitive root of a prime p satisfying the above cubic equation is the real essence of our embedding the partial algebraic structure obtained from the design based on (013) as a full incidence algebra on a complex cubic curve. See the Appendices I and II for more examples of embeddings using primitive roots. It is this interplay between geometry, combinatorics, arithmetic and algebra that we would like to capture in a most general set up in our next section where we show that for every prime $p \geq 11$, there is a p-cluster which is the closure of a $(p-1)_3$ design.

§4. A GENERAL REPRESENTATION THEOREM.

LEMMA 4.1. Let $p \geq 11$ be a prime number. Then there are numbers k and a such that

(i) k is a primitive root of the field GF(p);

(ii) $1+k+k^a=0 \pmod p$ and

(iii) (0,1,a) is a difference set mod (p-1).

Proof. Choose a primitive root k such that $2k+1 \neq 0 \pmod p$ and $k+2 \neq 0 \pmod p$. This is certainly possible because $p \geq 11$ and there are $\phi(p-1)$ primitive roots for the prime number p. The non-zero elements of the field are

$$\{1, k, k^2, k^3, \dots, k^{p-1}\} .$$

The element $-1-k \neq 0$ since otherwise $k=-1$ and $k^2 = 1 \pmod p$ impossible since $p>3$. Hence $-1-k=k^a$ for some number $a \leq p - 1$ and so

$$1 + k + k^a = 0 \pmod{p} \quad ....(1).$$

If (0,1,a) is not a difference set over mod(p-1) then the six elements

$$\{\pm 1, \pm a, \pm(a-1)\}$$

are not pairwise distinct (mod (p-1)). We will arrive at a contradiction from each one of the possible equalities.

If $1=a$ mod(p-1) then $a=p$ itself and $1+k+1=0$ (mod p) which contradicts the choice of k.

If $1=-a$ mod(p-1) then (1) becomes $1+k+k^{p-2}=0$ or $1+k+k^{-1}=0$ or $k^2= =-k-1=k^{-1}$ or simply $k^3=1$ which is impossible since k is a primitive root of p and $p>4$.

If $a=-a$ mod(p-1) then $a=0$ mod(p-1) or else $a=(p-1)/2$(modp-1).

If $a=0$ (mod p-1) then $a=p-1$ and hence $k^a=1$, so the equation (1) becomes $2+k=0$ which contradicts the choice of k.

If $a=(p-1)/2$ then $k^a=-1$ (mod p) and hence, by the equation (1),

$$1+k+(-1)=0 \pmod{p} \text{ or } k = 0,$$

which is plainly impossible.

If $a=1-a$ (mod p-1) then $2a=1$ (mod p-1) or $a=(1/2)$ mod (p-1) so that, by equation (1),

$$\begin{aligned} 0 &= 1+k+k^{\frac{1}{2}} \\ &= 1+k+k^{(\frac{1}{2})+p-1} \\ &= 1+k+k^{-(p-1)/2} \\ &= 1+k+(-1) \\ &= k, \text{ which is impossible.} \end{aligned}$$

Finally, if $a-1=1-a \bmod (p-1)$ then $2a=p+1$ and hence $(-1-k)^2=k^{2a}=$ $=k^{p+1}=k^2$ or $2k=-1 \pmod p$ which is one of the two values we already precluded. Since $\phi(p-1) \geq 3$ for all primes $p \geq 11$, there is always a primitive root k in the field $Z[p]$ satisfying the conditions of the Lemma.

THEOREM 4.1. *For all primes* $p \geq 11$ *there exists a difference set design on* $\{0,1,2,...,p-1\}$ *which can be embedded as a cubic cluster which is, in fact, a* p-*cluster.*

Proof. By the Lemma 4.1, there exists a primitive root k in $Z|p|$ and a number $a \leq p-1$ such that

(i) $1+k+k^a=0 \pmod p$

(ii) $(0,1,a)$ is a difference set over mod $(p-1)$.

Choose the difference set to be $\{(0,1,a); \bmod (p-1)\}$. Let now C be a non-singular cubic curve in the complex projective plane. By Lemma 1.5 we know that C has p^2 points of order p. Let P be one such point. As in the proof of Theorem 3.1, define the map $\phi : \{0,1,2,...,p-1\} \to C$ by the rule $\phi(i)=k^iP$.

Clearly the map ϕ is one-to-one. Indeed, if $\phi(i)=\phi(j)$ for some $i \neq j$ in $Z[p]$, then $(k^i-k^j)P=0$ under the group law, and since P is of order p, this forces that $k^i=k^j \pmod p$. But k being a primitive root in the field $Z[p]$, we get that $i=j$. Moreover,

$$\begin{aligned}\phi(i)+\phi(i+1)+\phi(i+a) &= k^iP+k^{i+1}P+k^{i+a}P \\ &= k^i(1+k+k^a)P \\ &= 0\end{aligned}$$

by the choice of the primitive root k and the index a and hence the three points corresponding to the three elements i,i+1 and i+a in the difference set design will be collinear in the cubic curve C. Thus we have represented the cyclic difference set {(0,1,a); mod(p-1)} as a cubic cluster.

The technique of the above process of embedding is applicable to designs n_3 where n+1 is not necessarily a prime number. If n+1 is not prime, then one looks for the least prime number p of the form jq+1 where q is a prime factor of n and embed the original n_3 design in the resulting p-cluster using the above technique of finding k and a satisfying the equation $1+k+k^a=0$ (mod p).

Let us conclude this section by giving one example of this last kind:

THEOREM 4.2. *The cyclic difference design* {(0,1,9);mod 13} *can be embedded in a cubic cluster.*

Proof. Here 53 = 13 x 4 + 1 is the least prime of the form 13j+1. Now the collinearity of the three points corresponding to 0,1 and 9 'translates algebraically' to the polynomial equation

$$1+x+x^9 = 0 \pmod{53}$$

and 16 happens to be a root of this equation in the field Z[13]. Moreover, the element 16 is of order 13 in the multiplicative group Z*[13] and hence we can realize the original design {(0,1,9); mod 13} as a subalgebra of the 53-cluster in the cubic curve. Here is the actual mapping:

$$\begin{array}{cccccccccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 0 \\ \varphi : & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 1 & 16 & 44 & 15 & 28 & 24 & 13 & 49 & 42 & 36 & 46 & 47 & 10 \end{array}$$

In other words, choose an arbitrary point P of order 53 in the cubic curve and let Q = f(P) be the point on the curve defined by

$$\varphi(P)=(((P*P)*(P*P))*((P*P)*(P*P)))*(((P*P)*(P*P))*((P*P)*(P*P)))$$

where $*$ now stands for the binary morphism of chord-tangent construction. Notice that $\varphi(P) = 16P$ under the group law. Now simply follow the above map and send the element 1 to the point P, 2 to 16P, 3 to the point 44P etc. The three points $\varphi(1), \varphi(2), \varphi(10)$ on the cubic will be collinear because

$$\varphi(1) + \varphi(2) + \varphi(10) = P+16P+36P=53P=0$$

under the group law since P was chosen to be a point of order 53. This represents the cyclic difference set design {(0,1,9); mod 13} as a subalgebra of a cubic cluster with 53 points. In the Appendix II below, we give a partial list of difference set designs of type (0,1,3) and (0,1,4) based on primes as well as non-primes and the corresponding mappings which realize the given designs as sub-configurations of cubic clusters in the complex projective plane.

The theme connecting the arithmetic, equational logic, algebra and geometry which is merely touched upon in these Theorems as well as in the several examples given in the Appendix II will be studied in detail in our forthcoming publications on this topic.

APPENDIX I

A method of embedding difference set designs {(0,m,n);mod 14} in cubic clusters.

14+1 = 15 is not a prime but 2x14+1=29 is prime. The least primitive root of 29 is 2.

Hence all primitive roots of 29 = $\{2^i \mid (i,28)=1\}$
= {2,8,3,19,18,14,27,21,26,10,11,15}

Now the elements of order 14 in the multiplication group Z*[29] are precisely the squares of the primitive roots, viz

{4,6,9,13,5,22}.

The element 4 is a root of the equation

$$1+x+x^4 = 0$$

in the field Z[29] and hence the cubic cluster C1 generated by point a P of order 29 in the underlying group of a complex cubic must contain a geometric sub-configuration isomorphic to the cyclic difference set design {(0,1,4);mod 14} and the actual embedding is achieved by the mapping

φ : {(0,1,4);mod 14} → C1 where $\varphi(i)=4^iP$ and 4^i is calculated modulo 29.

Now the triples of the configuration {(0,1,4); mod 14} automatically become collinear points under this mapping: $(4^m+4^{m+1}+4^{m+4})P=$ $= 4^m(1+4+4^4)P = 0$ and hence the three points $\varphi(m)$, $\varphi(m+1)$ and $\varphi(m+4)$ are indeed collinear in the cubic curve.

This gives a proof of the second half of line 6 in the Appendix

II claiming the embeddability of {(1,2,5); mod 14}. Continue similarly with other generators of order 14 to find the corresponding difference set designs they determine. The following table gives all such designs embeddable in Z[29]. In fact, these apparently different designs are all isomorphic to one another. We will now describe the isomorphism from {(0,1,4);mod 14} to say, {(0,1,9); mod 14} . It is clear that 0 and 7 are fixed points. To find the image of 1, notice that 1 goes to 4 in (0,1,4) and 4 is the image of 5 in the mapping to (0,1,9) and hence send 1 to 5 and similarly 2 to 10 etc. Thus the required isomorphism is simply the permutation given by the four cycles (0),(7),(1,5,11,13,9,3) and (2,10,8,12,4,6).

Points	0	1	2	3	4	5	6	7	8	9	10	11	12	13	(0,m,n)
Generators															
4	1	4	16	6	24	9	7	28	25	13	23	5	20	22	(0,1,4)
6	1	6	7	13	20	4	24	28	23	22	16	9	25	5	(0,1,9)
9	1	9	23	4	7	5	16	28	20	6	25	22	24	13	(0,2,5)
13	1	13	24	22	25	6	20	28	16	5	7	4	23	9	(0,3,5)
5	1	5	25	9	16	22	23	28	24	4	20	13	7	6	(0,1,6)
22	1	22	20	5	23	13	25	28	7	9	24	6	16	4	(0,3,4)

APPENDIX II

A partial list of designs embeddable as cubic clusters: $\varphi(x)=k^x \pmod p$

{(124); mod n}			{(125); mod n}		
n	k	p	n	k	p
9	7	27	9	22	27
10	2	11	10	7	11
10	13	33	11	18	23
11	4	23	11	64	69
12	7	13	12	13	45
13	36	53	14	4	29
15	14	31	16	3	17
15	76	93	16	37	51
16	11	17	16	88	255
16	28	51	17	93	103
18	25	37	18	2	19
19	16	457	18	40	57
20	37	61	19	30	191
21	38	43	20	13	25
22	58	67	20	18	55
23	25	47	20	73	165
23	34	47	21	50	127
26	51	131	22	19	23
27	61	81	24	7	73
28	26	29	26	57	79
28	55	87	27	49	81
30	3	31	27	73	109
30	34	93	28	21	29
30	79	99	28	33	145
33	142	207	28	79	87
36	7	351	30	40	99
36	23	73	32	42	193
37	67	149	34	34	307
39	11	79	35	5	631
39	142	477	35	10	71
40	47	241	36	35	73
42	124	379	36	78	95
43	136	173	37	63	149
46	35	47	39	76	79
46	82	141	42	4	261
48	79	153	42	28	43
49	133	197	44	18	115
56	20	617	44	88	115
57	16	4113	46	10	47
60	46	143	46	39	47
60	98	793	48	48	193
65	5	131	49	54	197
65	75	131	53	27	107
65	136	393	53	50	1697
66	13	67	53	92	107
66	63	67	57	75	229
66	80	67	60	13	225
66	130	201	60	35	61
69	25	423	63	13	127
69	34	423	68	93	515
75	121	151	70	62	319
80	79	187	79	43	317
82	35	83	80	88	425
82	118	249	82	18	83
84	124	559	83	100	167
84	142	261	84	28	215
86	47	431	84	50	3683
87	12	1741	88	15	89
87	114	523	88	21	353
87	141	567	88	31	89
88	14	89	90	40	209
88	103	89	94	33	8179
90	34	837	96	87	97
92	37	277	98	25	197
99	142	621	100	88	125

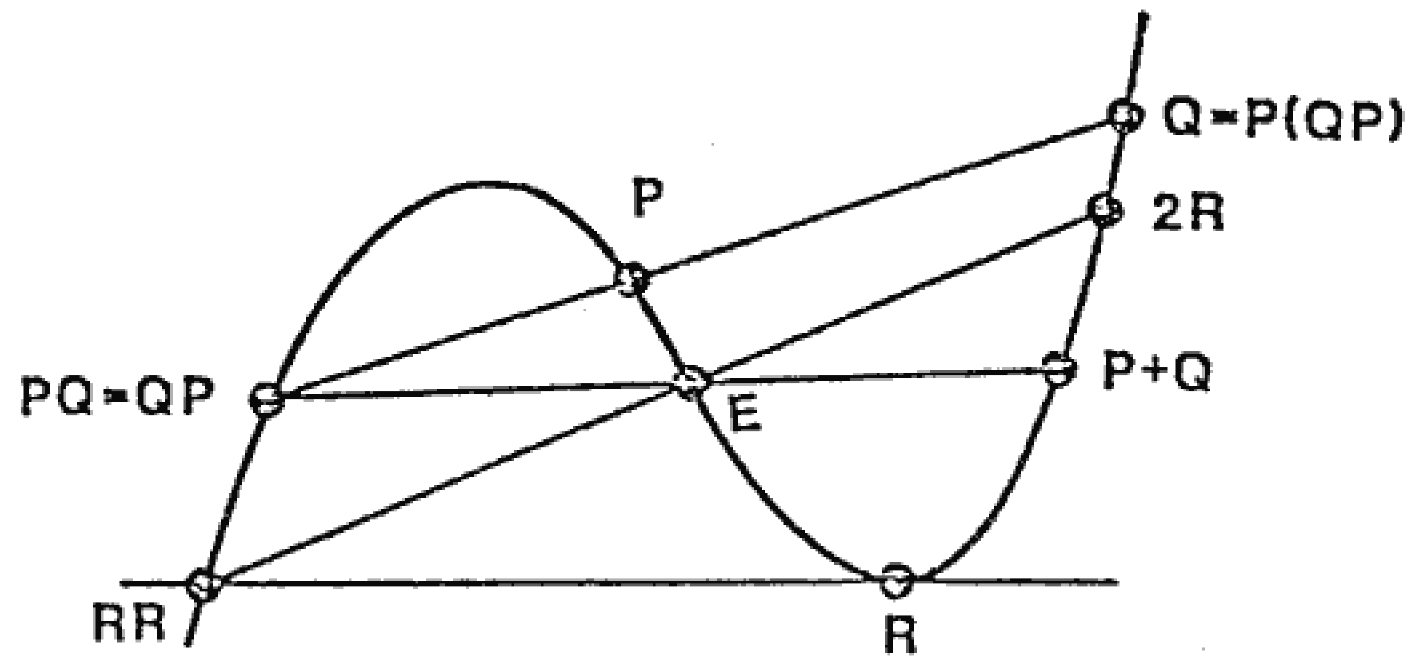
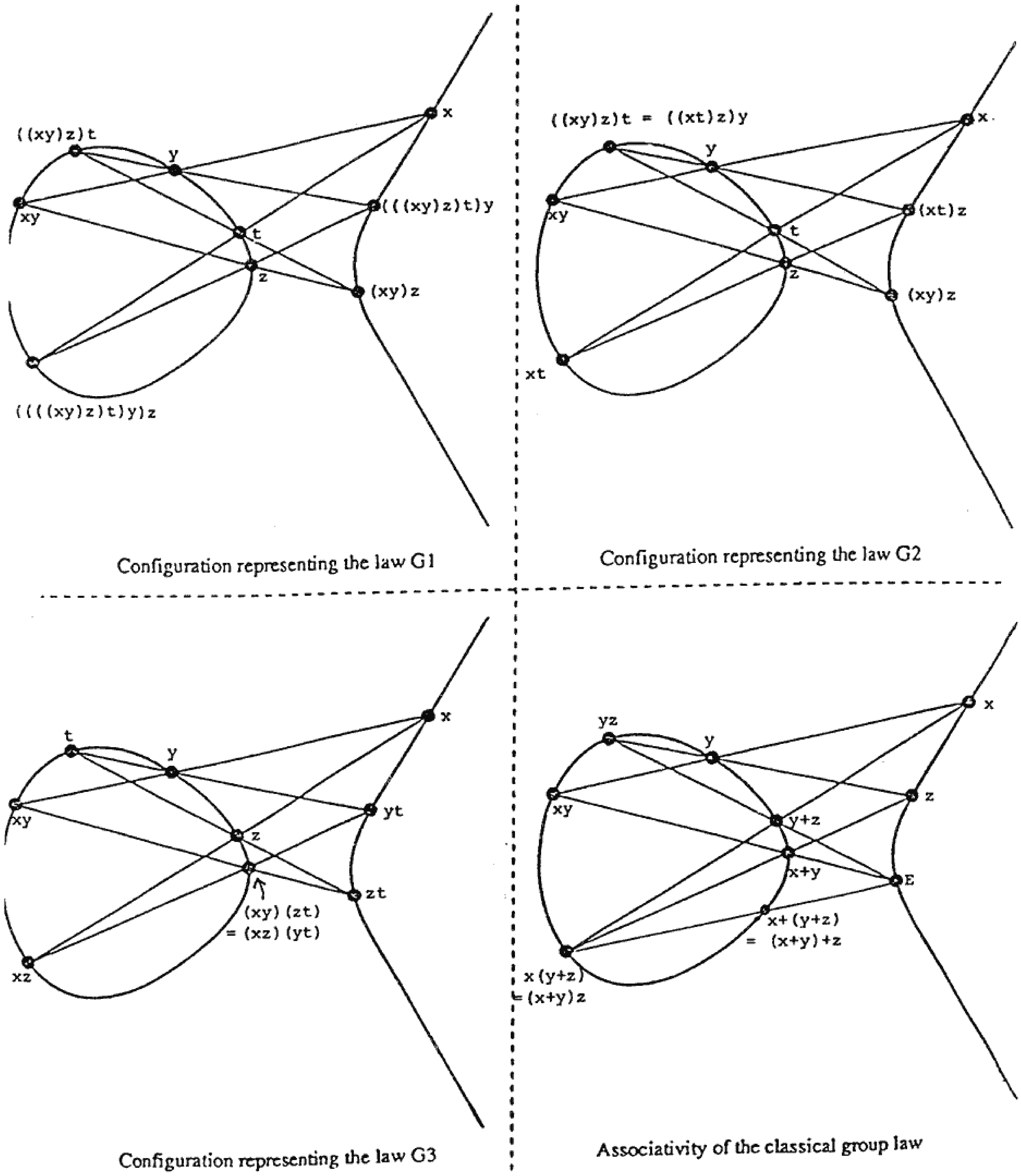


Figure 1

Equivalence of identities G1, G2, G3 and the associativity of the group law.



Configuration representing the law G1

Configuration representing the law G2

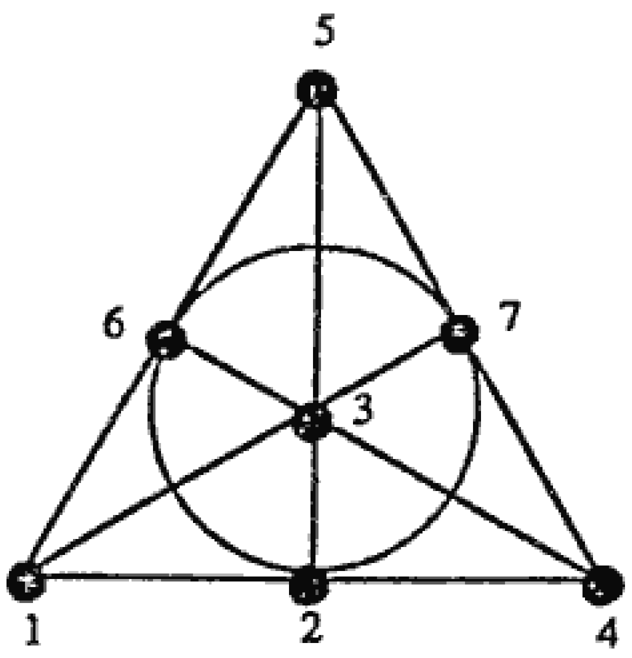
Configuration representing the law G3

Associativity of the classical group law

Figure 2.

1,2,4
2,3,5
3,4,6
4,5,7
5,6,1
6,7,2
7,1,3

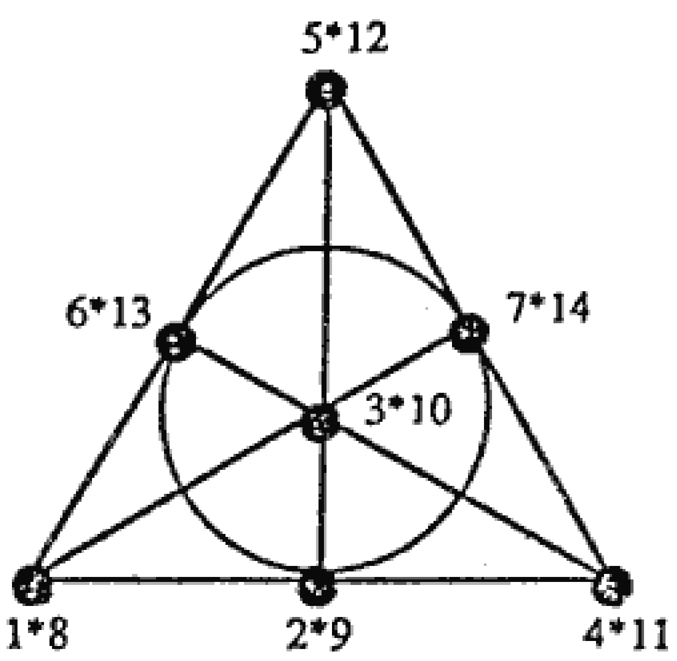
{(124); mod 7}



The classic anti-Fano configuration realized as a {(124); mod 7} design

Figure 3(a)

≅

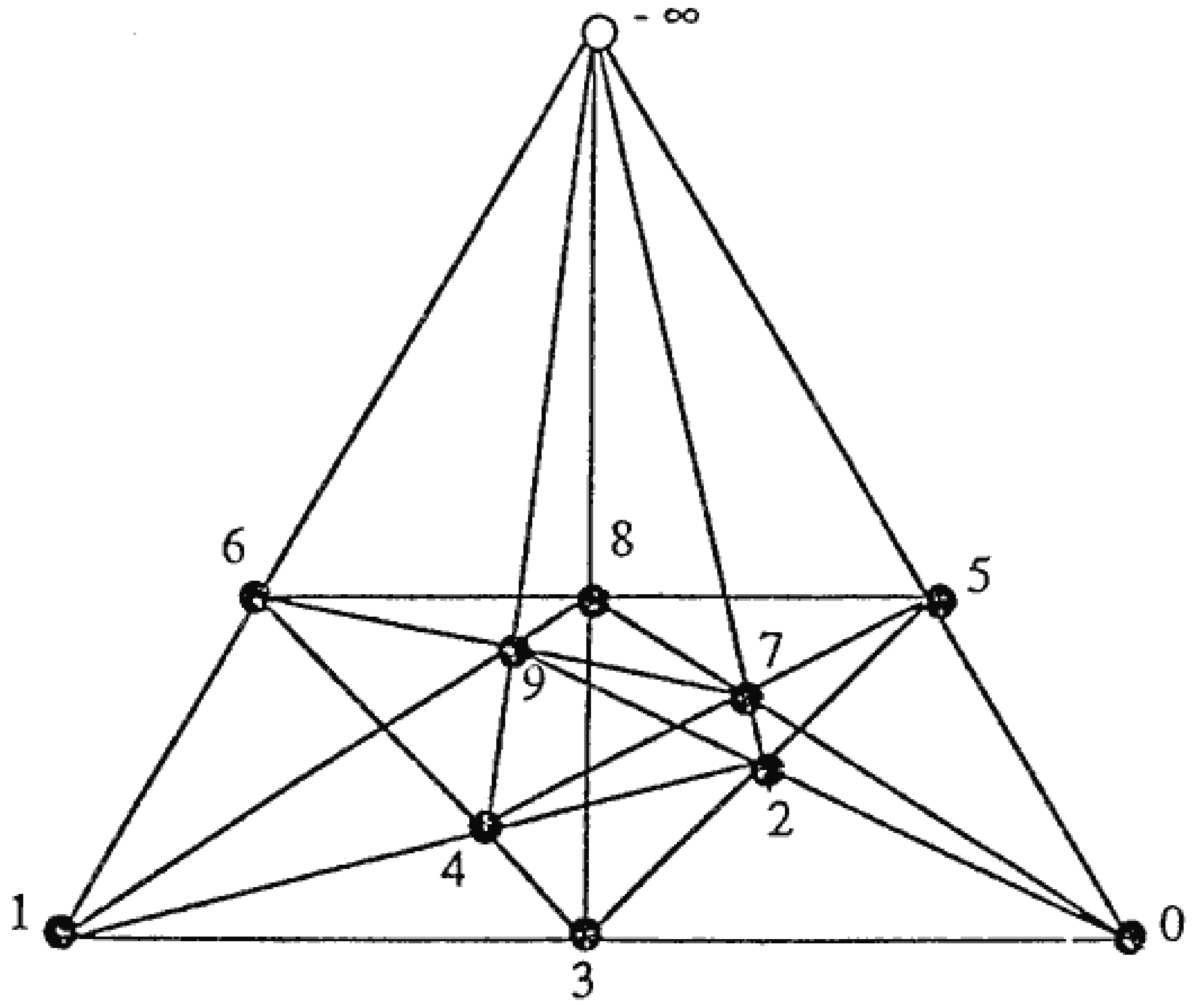


A subalgebra in any algebra $\langle\Gamma,\cdot\rangle$ satisfying the laws on a cubic curve and generated by the cyclic design {(124); mod 14}.

Figure 3(b)

1,2,4
2,3,5
3,4,6
4,5,7
5,6,8
6,7,9
7,8,10
8,9,11
9,10,12
10,11,13
11,12,14
12,13,1
13,14,2
14,1,3

{(124); mod 14}



The Complete Configuration {(124); mod 10}

(the tangents at the various points are not shown)

Figure 4

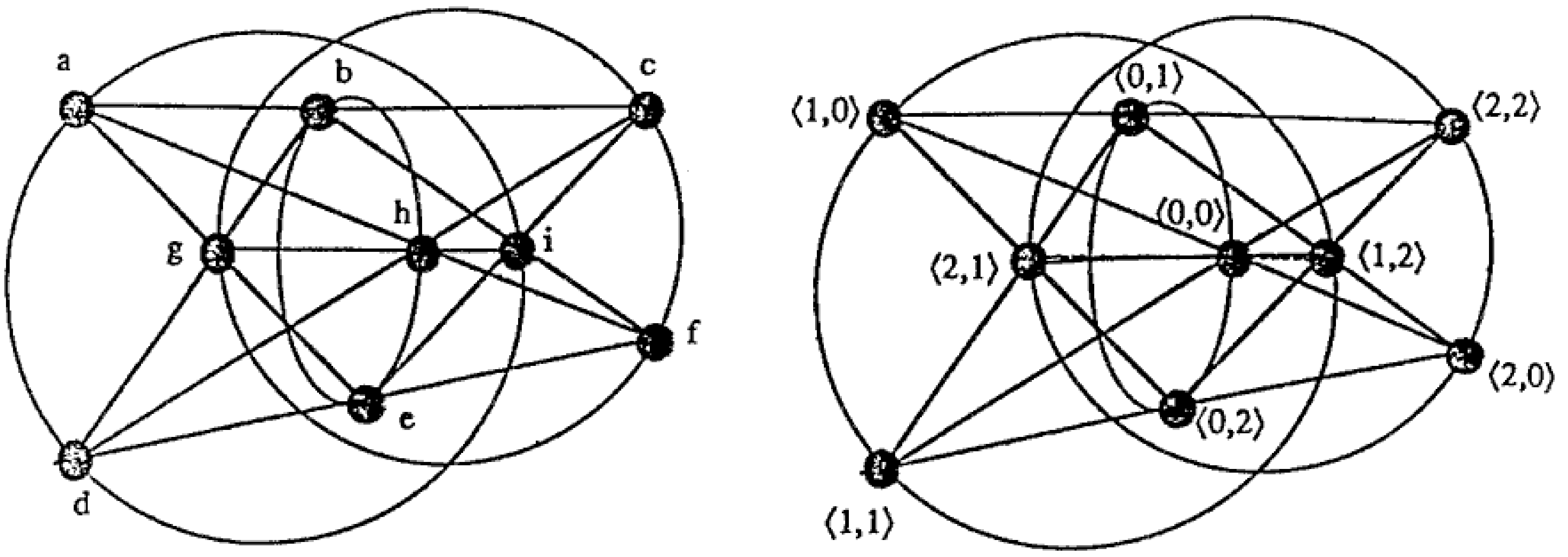


Figure 5. $P + Q + R = 0$ in $Z_3 \times Z_3$ iff P,Q and R are collinear.

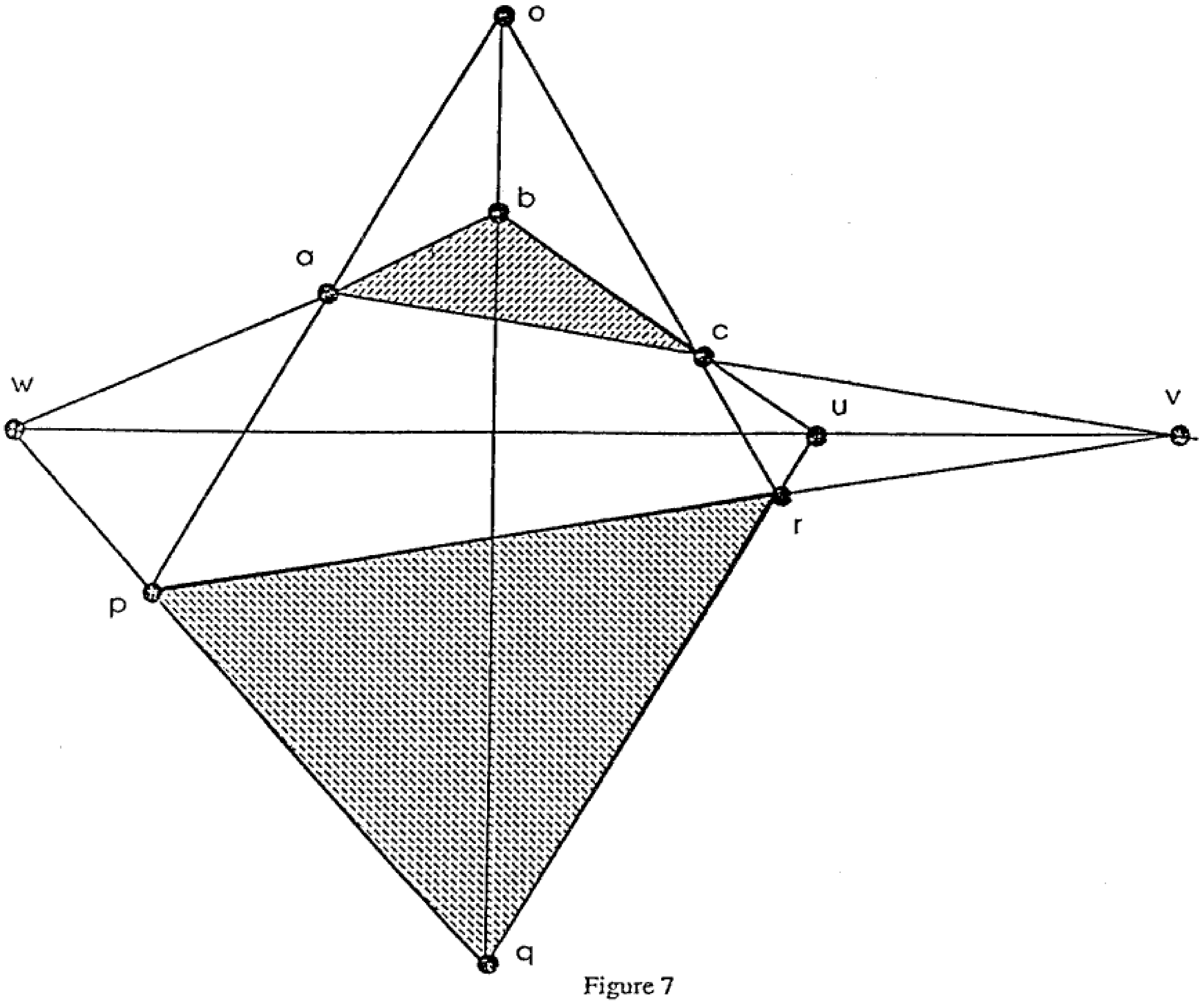


Figure 7

REFERENCES

[1] G.BERMAN: "A generalization of Pappus configuration" *Canadian J.Math.* 3(1951) 299-303.

[2] H.S.M.COXETER: "Self-dual configurations and regular graphs", *Bull. Amer.Math.Soc.*56(1950) 413-453.

[3] I.M.H.ETHERINGTON: "Quasigroup and Cubic curves", *Proc. Edinburgh Math. Soc.* **14**(1965) 273-291.

[4] J.M.FELD: "Configurations inscriptable in cubic curves", *Amer. Math. Monthly* 43(1936) 413-455.

[5] R.FREESE & R.McKENZIE: "*Commutator Theory for congruence modular varieties* (Preprint).

[6] W.FULTON: "*Algebraic curves*", Benjamin, New York, 1968.

[7] G.GRÄTZER: "*Universal Algebra*", Springer-Verlag, New York, 1979 (and Ed.)

[8] G.GRÄTZER and R.PADMANABHAN: "On idempotent, commutative and non-associative groupoids", *Proc. Amer.Math.Soc.* **28**(1971) 75-80.

[9] R.HARTSHORNE: "*Algebraic Geometry*", Springer-Verlag, New York, 1977.

[10] HILBERT& COHEN-VOSSEN: "*Geometry and the Imagination*",Chelsea, New York.

[11] S.KANTOR: "*Die Configuration* $(3,3)_{10}$; Sitz-ber.Kais.Akad.Wiss. **34**(1881) 2 Abt. 1291-1314.

[12] H.LAKSER and R.PADMANABHAN: "Implications valid over a plane cubic curve (to appear).

[13] I.YU.MANIN: "*Cubic Forms*", North-Holland Pub.Co.,Amsterdam, 1973.

[14] N.S.MENDELSOHN, R.PADMANABHAN and B.WOLK: "Planar Projective Configurations I" , *Note Mat.* VII(1987), 91-112.

[15] D.MUMFORD: "*Algebraic Geometry I, Complex Projective Varieties*" Springer Verlag, New York, 1976.

[16] G.ORZECH & M.ORZECH: "*Plane Algebraic Curves*", Marcel Dekker, New York, 1981.

[17] R.PADMANABHAN: "Logic of Equality in Geometry", *Ann. Discrete Math.* 15(1982) 319-331.

[18] R.PADMANABHAN: "Configuration Theorems on Cubic Quasigroups", 1984 *Conference on Finite Geometries*, Marcel Dekker, New York and Basel, 1985.

[19] R.W.QUACKENBUSH: "Quasi-affine algebras", *Alg.Univ.* 20(1985) 318-327.

[20] I.R.SHAFAREVICH: "*Basic Algebraic Geometry*", Springer-Verlag, New York, 1977.

[21] J.H.SILVERMAN: "Points of finite order on elliptic curves" *Amer. Math. Monthly* 93(1986) 793-795.

[22] T.A.SPRINGER: "*Linear Algebraic Groups*", Birkhaüser,Boston, 1980.

[23] M.SZUREK: "*Playing with Bezout*", Preprint #72, University of Regina, 1984.

[24]. J.TATE: "Arithmetic of elliptic curves", *Invent. Math.* 23(1974) 179-206.

[25] W.TAYLOR: "Varieties obeying homotopy laws", *Canad. J. Math.* 29 (1979) 498-527.

Department of Mathematics
University of Manitoba
Winnipeg, Manitoba
CANADA R3T 2N2