Riv. Mat. Univ. Parma (2) 2 (1961), 115-132

WILLIAM A. PIERCE (*)

Binary systems for finite planes. (**)

1. - Introduction.

An affine plane consists of things, called « points », and sets of points, called « lines », satisfying the following postulates.

1. Two distinct points are contained in (are joined by, lie on, determine) exactly one line.
2. Lines being defined as « parallel » if and only if they have no common point, EUCLID's parallel postulate holds; that is, given a point P not lying on a line q, $\exists$ exactly one line m through (i.e., containing) P parallel to q.
3. There exist three non-collinear points (i. e., 3 points not on any single line).

From these postulates, various well-known properties can be derived (for example **[5]** [1]). If one line has n points, every line has n points, the whole plane has n^2 points, and there are exactly $n \cdot (n+1)$ lines altógether. An affine plane can be completed by adding a line of ideal points in the usual way; the resulting plane is called a «projective» plane, and is characterized by the projective axioms of incidence:

1. two distinct points determine exactly one line;
2. two distinct lines have a common point;
3. there exist four points, no three collinear.

(*) Indirizzo: Dept. of Mathematics, Syracuse University (U.S.A.).

(**) Ricevuto il 10-9-1960.

[1] I numeri in neretto e tra [ ] si riferiscono alla Bibliografia posta al termine del lavoro.

The structures of affine and projective planes have not been completely investigated; but developments of the past decade have helped to establish the usefulness of these structures in Geometry and Combinatorial Analysis.

A number of authors have discussed planar coordinate; (cf. the bibliography); yet the literature contains no answer to the following specific question. What is the *most general* « double binary system » which may serve to coordinatize affine and projective planes? It is the purpose of this paper to give the answer for the *finite* case. In fact, I shall obtain a simple set of necessary and sufficient conditions-and these will be proved independent. The kernel of the idea was suggested by G. Birkhoff [3]. It will also be of interest to study the transformations that can be made on these double-composition systems without destroying their assential affine property.

2. - The meaning of « most general ».

Let A denote a finite set of n elements, on which are defined single-valued binary operations of addition $(+)$ and multiplication $(\cdot)$. Assume that the ordered pairs (x, y) of elements from A give the points of an affine plane π and that equations of the forms $x = k$ and $y = b + m \cdot x$, for $k, b, m \in A$, represent all the lines of π [2]. Since π has exactly $(n^2 + n)$ lines and since there are exactly $(n^2 + n)$ equations of the forms $x = k$ and $y = b + m \cdot x$, distinct equations represent distinct lines. We might expect, from the analogy of the real plane, that n of the equation $y = b + m \cdot x$ would give lines having constant y-coordinates. Such is not necessarily the case, however, as shown by the following example $(n = 3)$.

The points

(0,2)	(1,2)	(2,0)
(0,1)	(1,1)	(2,2)
(0,0)	(1,0)	(2,1)

The operations [3]

$+$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

$\cdot$	0	1	2
0	0	0	1
1	0	1	0
2	0	2	2

[2] As usual, multiplication takes precedence over addition in the order of operations.

[3] Throughout this paper, I shall adopt the convention that $a + b$ appears in the addition table opposite a and under b. A similar convention will hold for $a \cdot b$.

Tabulation of the lines

$y = 0 + 0\cdot x$	(0,0)	(1,0)	(2,1)
$y = 1 + 0\cdot x$	(0,2)	(1,2)	(2,0)
$y = 2 + 0\cdot x$	(0,1)	(1,1)	(2,2)
$y = 0 + 1\cdot x$	(0,0)	(1,1)	(2,0)
$y = 1 + 1\cdot x$	(0,2)	(1,0)	(2,2)
$y = 2 + 1\cdot x$	(0,1)	(1,2)	(2,1)
$y = 0 + 2\cdot x$	(0,0)	(1,2)	(2,2)
$y = 1 + 2\cdot x$	(0,2)	(1,1)	(2,1)
$y = 2 + 2\cdot x$	(0,1)	(1,0)	(2,0)
$x = 0$	(0,0)	(0,1)	(0,2)
$x = 1$	(1,0)	(1,1)	(1,2)
$x = 2$	(2,0)	(2,1)	(2,2)

A second example shows that the main body of the multiplication table need not even contain all n elements of A and that some columns for addition may be completely arbitrary.

+	0	1	2 [4]
0	0	1	a
1	1	2	b
2	2	0	c

·	0	1	2
0	0	0	1
1	0	1	0
2	1	0	0

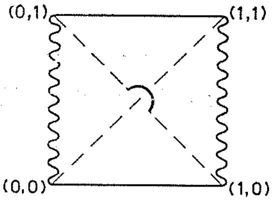
(0,2)	(1,2)	(2,0)
(0,1)	(1,1)	(2,2)
(0,0)	(1,0)	(2,1)

[4] Each of a, b, c is an arbitrary element of A.

$0 + 0\cdot x = y$	(0,0)	(1,0)	(2,1)	$a + 1\cdot x = y$	(0,0)	(1,1)	(2,0)
$1 + 0\cdot x = y$	(0,1)	(1,1)	(2,2)	$1 + 1\cdot x = y$	(0,1)	(1,2)	(2,1)
$2 + 0\cdot x = y$	(0,2)	(1,2)	(2,0)	$2 + 1\cdot x = y$	(0,2)	(1,0)	(2,2)
$0 + 2\cdot x = y$	(0,1)	(1,0)	(2,0)	$x = 1$			
$1 + 2\cdot x = y$	(0,2)	(1,1)	(2,1)	also: $x = 2$			
$2 + 2\cdot x = y$	(0,0)	(1,2)	(2,2)	$x = 0$			

These examples indicate that some of the systems obtained under the assumptions of this section are too general to be useful.

In an affine plane, two sheafs of parallel lines may be singled out to visualize as the « verical » and « horizontal » lines respectively. The remaining lines can be pictured as curves winding through the « horizontal-vertical » square lattice. Thus it seems reasonable to require that the equations $y = k$ should also represent straight lines (in addition to equations $x = k$ and $y = b + m\cdot x$). Assuming that points are given by the ordered pairs (x, y) and that equations $x = k$, $y = k$, $y = b + m\cdot x$ represent straight lines, it is still not necessary that certain equations $y = b + (m\cdot x)$ represent the same lines as do the equations $y = k$. In fact, it is no longer necessary that distinct equations represent distinct lines, as *I* now show by an example $(n = 2)$.



+	0	1
0	0	1
1	1	0

·	0	1
0	0	1
1	0	1

Here two sets of parallel lines are given by $x = k$ and $y = k$. Both $y = 0 + 0\cdot x$ and $y = 0 + 1\cdot x$ represent the single line $\{(0,0), (1,1)\}$, while both $y = 1 + 0\cdot x$ and $y = 1 + 1\cdot x$ represent the single line $\{(0,1), (1,0)\}$. If the restriction is added that distinct equations of the form $y = b + m\cdot x$ represent distinct lines, the resulting system becomes an interesting generalization of a Galois Field. In the next section I shall discuss the properties of such systems.

3. - Affine Systems.

Definition I. A finite set A with two single-valued binary operations, $+$ (addition) and $\cdot$(multiplication), will be called an affine system $\Longleftrightarrow$

(i) Each ordered pair (x, y) of elements from A represents exactly one point of an affine plane π. [π and A will be said to « correspond »].

(ii) Each equation of the form $x = k$, $y = k$, or $y = b + m \cdot x$ represents a line, distinct equations of the form $y = b + m \cdot x$ giving distinct lines.

Lemma 1. If A is an affine system of n elements corresponding to the plane π, then every line of π is represented by an equation $x = k$, $y = k$, or $y = b + m \cdot x$. The n equations $y = k$ represent exactly the same lines as the n equations $y = b + 0 \cdot x$ for some fixed element $0 \in A$. Moreover, $0 \cdot x$ is constant, independent of x. If $m \neq 0$, then $m \cdot u = m \cdot v \Longrightarrow u = v$.

Proof. No line $y = b + m \cdot x$ can coincide with a line $x = k$, since b, m, c uniquely determine $b + m \cdot c$. Thus the n^2 distinct equations $y = b + m \cdot x$ represent the remaining n^2 lines of π, and n of these equations represent the same lines as the n equations $y = c$.

To show the existence of the required element 0, suppose that for *every* $m \in A$, $m \cdot u = m \cdot v \Longrightarrow u = v$; i.e., for any fixed m, $m \cdot x$ assumes all values $\in A$ as x varies over A. Pick $y = c$ and $y = b^* + m^* \cdot x$, both representing the same line. Then $c = b^* + m^* \cdot x$ for all $x \in A$, i.e., $c = b^* + u$ for all $u \in A$, whence $c = b^* + m \cdot x$, for *all* m and *all* $x \in A$, contradicting the fact that distinct equations $y = b + m \cdot x$ give distinct lines.

Thus $\exists$ elements 0, x_1, $x_2 \in A$ with $0 \cdot x_1 = 0 \cdot x_2$, but with $x_1 \neq x_2$. For any $b \in A$, the equation $y = b + 0 \cdot x$ must represent the same line as $y = b + 0 \cdot x_1$, since the points $(x_1, b + 0 \cdot x_1)$ and $(x_2, b + 0 \cdot x_2)$ determine a line and since $0 \cdot x_1 = 0 \cdot x_2$. All n lines $y = b + 0 \cdot x$ thus correspond to the lines $y = k$.

If $m \neq 0$, no equation $y = b + m \cdot x$ can give the same line as $y = k$. Therefore, if $m \neq 0$, $m \cdot x_1 = m \cdot x_2 \Longrightarrow x_1 = x_2$.

Theorem I. Let A denote a finite set (of n elements) with single-valued binary operation $+$ (addition) and $\cdot$(multiplication. Then A is an affine system if and only if the following algebraic conditions, (i)-(iv), are valid.

(i) A contains at least two elements $\in A$.

(ii) For all $m \neq$ one particular element $0 \in A$, $m \cdot u = m \cdot v \Longrightarrow u = v$.

(iii) For all b, u, $v \in A$, $b + u = b + v \Longrightarrow u = v$.

(iv) If a, b, e, $f \in A$, with $a \neq b$, then $\exists$ an ordered pair t, s of elements from A for which $t + s \cdot a = e$ and $t + s \cdot b = f$.

The following additional properties hold in any affine system (being derivable from i-iv).

(a) The solution t, s in condition (iv) is unique.

(b) $0 \cdot x$ is identically constant, independent of x.

Proof. Assume that A is affine. Any line $x = k$ has at least two points so A also must have at least two elements.

Condition (ii) is part of the lemma.

To prove (iii), pick $m \neq 0$. There exist unique elements x_1 and x_2 such that $m \cdot x_1 = u$ and $m \cdot x_2 = v$ respectively. The points $(x_1, b + u)$ and $(x_2, b + u)$ satisfy the equation $y = b + m \cdot x$, whence $x_1 = x_2$ and $u = v$.

Condition (iv) states that distinct points (a, e) and (b, f) with $a \neq b$ satisfy an equation of the form $y = t + s \cdot x$.

Assume, conversely, that A is a finite set (of n elements) with two single-valued binary operations $+$ and $\cdot$ and satisfying (i)-(iv). We must check that the ordered pairs (x, y), for x, $y \in A$, meet the requirements for points of an affine plane when a « line » is taken to be the set of all pairs (x, y) satisfying an equation of the form $x = k$, $y = k$, or $y = b + m \cdot x$, for k, b, $m \in A$. First it is convenient to establish the extra properties (a) and (b) stated in the theorem. To show the uniqueness of the solution t, s given elements $a \neq b$, e, and f, note that for fixed $a \neq b$ every pair e, f leads to a pair t, s, and every pair t, s determines a pair e, f; since A is finite, the correspondence between the pairs, e, f and t, s is one-to-one. To prove condition (b), let an element $a \neq 0$ be given, and let elements t, s satisfy $t + s \cdot a = a$, $t + s \cdot 0 = a$. Then $t + s \cdot a = t + s \cdot 0 \Longrightarrow s \cdot a = s \cdot 0$ by (iii), and $s \cdot 0 = s \cdot a \Longrightarrow s = 0$ by (ii). Thus $0 \cdot a = 0 \cdot 0$ for all a. Moreover, the one-to-one correspondence of t, s onto e, f established by $t + sa = e$ and $t + sb = f$ maps the n pairs t, $s = 0$ onto the n pairs $e = f$. Hence the n sets of paires (x, y) which satisfy the n equations $y = b + 0 \cdot x$ coincide with the n sets given by $y = c$.

Postulate 1. The points (x_1, y_1) and (x_1, y_2), with $y_1 \neq y_2$, satisfy $x = x_1$; they cannot satisfy a relation $y = b + mx$ because the given binary operations are single-valued.

If $x_1 \neq x_2$, and y_1, y_2 are given, there is exactly one choice of b and m for which $b + mx_i = y_i$ $(i = 1, 2)$. [This includes the possibility $y_1 = y_2$]. Clearly the given points cannot satisfy an equation $x = c$.

Postulate 2. Given $y = b + mx$, with $m \neq 0$, each value of x determines exactly one value of y, and x may assume just n values; any equation $x = k$ or $y = k$ is satisfied by exactly n points; hence every line has just n points. Given *a* line r and a point P not on r, the lines joining P to points of r are n in number and contain altogether exactly $1 + n \cdot (n-1)$ points. If there are q other lines through P, there must be $q \cdot (n-1)$ points on them besides P itself. The total number of points being n^2, we obtain $n^2 = 1 + n \cdot (n-1) + q \cdot (n-1)$, whence $q = 1$ and the parallel postulate holds.

Postulate 3 follows at once from (i).

The independence of conditions (*i*)-(*iv*). The trivial set $\{0\}$ satisfes all properties except (i), $0 + 0$ and $0 \cdot 0$ being defined $= 0$.

The following system satisfies all properties except (ii).

+	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

·	0	1	2
0	0	0	1
1	0	1	0
2	0	2	2

Although it is not immediately obvious that this system satisfies (iv), that fact is easily verified by tabulating the lines.

The next example proves the independence of (iii), and the accompanying table shows that this example fails to satisfy (iv).

+	0	1	2
0	0	0	1
1	1	1	2
2	2	2	0

·	0	1	2
0	0	2	0
1	0	1	2
2	2	0	1

Tabulation

$0 + 0 \cdot 0 = 0,\quad 0 + 1 \cdot 0 = 0,\quad 0 + 2 \cdot 0 = 1,\quad 1 + 0 \cdot 0 = 1,\quad 1 + 1 \cdot 0 = 1,$

$0 + 0 \cdot 1 = 1,\quad 0 + 1 \cdot 1 = 0,\quad 0 + 2 \cdot 1 = 0,\quad 1 + 0 \cdot 1 = 2,\quad 1 + 1 \cdot 1 = 1,$

$0 + 0 \cdot 2 = 0,\quad 0 + 1 \cdot 2 = 1,\quad 0 + 2 \cdot 2 = 0,\quad 1 + 0 \cdot 2 = 1,\quad 1 + 1 \cdot 2 = 2,$

$1 + 2 \cdot 0 = 2,\quad 2 + 0 \cdot 0 = 2,\quad 2 + 1 \cdot 0 = 2,\quad 2 + 2 \cdot 0 = 0,$

$1 + 2 \cdot 1 = 1,\quad 2 + 0 \cdot 1 = 0,\quad 2 + 1 \cdot 1 = 2,\quad 2 + 2 \cdot 1 = 2,$

$1 + 2 \cdot 2 = 1,\quad 2 + 0 \cdot 2 = 2,\quad 2 + 1 \cdot 2 = 0,\quad 2 + 2 \cdot 2 = 2,$

In general, systems that satisfy (i)-(iii) fail to satisfy (iv). For example, consider

$+$	0	1
0	1	0
1	0	1

$\cdot$	0	1
0	1	0
1	0	1

Here the system

$$t + s\cdot 0 = 0 \qquad t + s\cdot 1 = 0$$

has no solution, although (i)-(iii) are valid.

The generality of affine systems. An example to illustrate the generality of affine planes is given below.

$+$	0	1	2
0	1	0	2
1	0	1	2
2	1	2	0

$\cdot$	0	1	2
0	1	1	1
1	0	1	2
2	2	1	0

Theorem II. In an affine system (of n elements), the following conditions are all equivalent. (The preceding example shows that they are not necessary).

1) The equation $a + m\cdot x = b + m'\cdot x$ (with $m \neq m'$) has at least (hence exactly) one solution for x.

2) For a given « slope » $m \neq 0\cdot 0$, the lines $y = b + m\cdot x$ are all « parallel » [i.e., nonintersecting].

3) $b + c = a + c \Longrightarrow b = a$ [5].

Proof The equation $a + m\cdot x = b + m'\cdot x$ (where $m \neq m'$) can never have distinct solutions x_1 and x_2. If it did, then a, m and b, m' would constitute distinct solutions of the system $t + s\cdot x_1 = a + m\cdot x_1$, $t + s\cdot x_2 = a + m\cdot x_2$.

(1) $\Longleftrightarrow$ (2). Any given line, $y = b + m_0\cdot x$, meets exactly n^2 other lines. The n lines $x = k$ and the $n\,(n-1)$ lines $y = b + m'\cdot x$ where $m' \neq m_0$ constitute a set of n^2 lines. Those lines all intersect $y = b + m_0\cdot x \Longleftrightarrow a + m\cdot x = b +$

[5] Each of these conditions is equivalent to BIRKHOFF's condition (i) on p. 111 of [3].

$+ m'\cdot x$ always has a solution; moreover, they all intersect $y = b + m_0\cdot$ $\cdot x \Longleftrightarrow$ lines $y = b + m_0\cdot x$ and $y = b' + m_0\cdot x$ fail to meet unless $b = b'$.

(2) $\Longleftrightarrow$ (3). $b + c = a + c \Longleftrightarrow$ for some $m \neq 0\cdot 0$ and for some x, $b + m\cdot$ $\cdot x = c + m\cdot x$; the latter implies that $b = c$ if and only if (2) is satisfied.

4. - Normalizations and transformations of affine coordinates.

When a plane can be represented over an affine system, it is natural to inquire if more standard coordinates can be introduced into the same plane. The question remains open whether the affine system I have introduced must have a prime-power number of elements. In studying this question, it is important to know if an affine system can be modified toward a GALOIS field without changing the number of elements involved, or at least if the existence of an affine system with n elements implies the existence of a field of order n. In that case, n is of course a prims-power. Conversely, it is instructive to transform GALOIS fields into affine systems having more general properties.

Definition II. Two affine systems will be called isotopic $\Longleftrightarrow$ their corresponding planes are geometrically isomorphic.

Lemma 2. If the columns of the multiplication table for an affine system are subjected to an arbitrary permutation, addition being kept invariant, the resulting number system is still affine and, in fact, isotopic to the original system.

Proof. It is convenient to regard the given permutation as a transformation $a \rightarrow a'$ acting on the top title row of the multiplication table (with the columns themselves left fixed). Denote the original operation of multiplication by $\cdot$, and define the new multiplication * by the condition $b * a' = b\cdot a$. Define a map, ψ, from the set of all points under $\{+, *\}$ by the relation $\psi\{(x, y\} =$ $= (x', y)$; ψ is one-to-one since $x \rightarrow x'$ is one-to-one. The points satisfying $x = k$ are mapped onto points satisfying $x = k'$. Also points which satisfy $y = b + m\cdot x$ are mapped onto points which satisfy $y = b + m * x$, since $y = b + m\cdot x \Longleftrightarrow y = b + m * x'$. Thus ψ is the desired geometric isomoprhism.

Lemma 3. Assume that A is an affine system under $\{+, \cdot\}$. Let $+$ remain fixed, while the rows in the multiplication table are subjected to any permutation that leaves the top row $(0\cdot x)$ unchanged. The new multiplication, *, thus obtained, combines with $+$ to form an affine system isotopic to the original.

Proof. The permutation on the rows for multiplication may be regarded as a permutation $a \rightarrow a'$ on the left-hand title column for $\cdot$, with $0 \rightarrow 0$. Thus

$a\cdot b = a'{*}b$. The identity map $\psi\{(x, y)\} = (x, y)$ is now a geometric isomorphism of the plane for $\{+, \cdot\}$ onto the plane for $\{+, *\}$. In fact, the points (k, y) still satisfy $x = k$ and the points satisfying $y = b + m\cdot x$ are exactly those wich satisfy $y = b + m'{*}x$.

Lemma 4. Two affine systems having the same elements are equivalent if their multiplications are the same and if the rows in one addition table form a permutation of the rows in the other.

Proof. For some transformation $a \rightarrow a'$ (on the common elements of the two systems) $a + x = a' \oplus x$ (all x); and $\oplus$ denoting the two operations of addition. The identity map $\psi\{(x, y)\} = (x, y)$ is a geometric isomorphism since any point (k, y) satisfies $x = k$ and since the points which satisfy $y = b + m\cdot x$ are exactly those which satisfy $y = b' \oplus m\cdot x$.

Given an affine system with operations $\{+, \cdot\}$, and given an operation $\oplus$, obtained by permuting the columns for $+$, it is not true in general that $\{\oplus, \cdot\}$ will be affine. For example, start with the field of integers (mod 5), and alter its addition table, interchanging the columns $x + 2$ and $x + 4$, to form a new addition $\oplus$, but leaving multiplication unchanged. No solution exists for the simultaneous system $t \oplus s\cdot 1 = 2$, $t \oplus s\cdot 3 = 3$.

It is possible, however, to establish the following restricted result.

Lemma 5. Let A be an affine system with operations $\{+, \cdot\}$ and let $\oplus$ be an operation satisfying $x + a \equiv x \oplus a'$, where $a \rightarrow a'$ is an arbitrary one-to-one transformation on A. Then a new multiplication, $*$, can be constructed on A so that A is affine under $\{\oplus, *\}$ with the new system isotopic to the original.

Proof. Define $m^*(a') = (m\cdot a)'$, for all $m, a \in A$, so that $b + m\cdot a = b \oplus m^*(a')$, for all $m, b, a \in A$. Obviously A is affine under $\oplus, *$.

To establish the equivalence, set $\psi\{(a, y)\} = (a', y)$. Any line $x = k$ is mapped by ψ onto the line $x = k'$. Any line $y = b + m\cdot x$ is mapped onto the line $y = b \oplus m^*(x')$.

Theorem III. If a (finite) affine plane admits a representation by an affine system $\{+, \cdot\}$, then coordinates from an affine system $\{\oplus, *\}$ can be introduced into the plane in such a way that $0 \oplus x \equiv x \oplus 0 \equiv x$, $0^* x \equiv 0$, and $1^* x \equiv x$. (Such an affine system will be called « standard »).

Proof. The elements $b + 0\cdot 0$ comprise all of the system $\{+, \cdot\}$. (Otherwise, the lines $y = k$ would not all be given by the equations $y = b + 0\cdot x$). After applying Lemma 4, we can assume that $b + 0\cdot 0 = b$. In particular $0 + 0\cdot 0 = 0$. Next apply Lemma 5 to permute the columns of the $+$ table, obtaning a new addition, $\oplus$, which satisfies $0 + a \equiv 0 \oplus a' \equiv a'$, and a new multiplication, $\#$, where $m \# (a') \equiv (m\cdot a)'$. Thus, $0 = 0 + 0\cdot 0 = 0 \oplus$

$\otimes\ (0\cdot 0)' = (0\cdot 0)'$, and $0 \# x' \equiv (0\cdot x)' \equiv (0\cdot 0)' = 0$. A permutation on the columns for $\#$ gives a final multiplication, $*$, which satisfies $1 * x \equiv x$, for some element $1 \neq 0$, with $0 * x \equiv 0$.

Theorem IV. If a standard of fine system $\{+, \cdot\}$ has one element x_0 such that the elements $x\cdot x_0$ comprise all of the system, then an isotopic standard system exists with an element 1 which is both a left and a right unit.

Proof. Permute the rows of the multiplication table to obtain $x\cdot x_0 \equiv x$. In particular, $x_0\cdot x_0 = x_0$. Permute the columns to obtain $x_0\cdot x \equiv x$, so that x_0 becomes the unit element.

Remark. Unfortunately, the hypothesis of Theorem IV may fail to hold even in a standard system. For example:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	2	1	0

Lemma 6. Let π denote a one-to-one transformation on a standard affine system A such that, given s, $a \neq b \in A$, there exists an $s' \in A$ for which $s'\cdot a = \pi\,\{s\cdot a\}$ and $s'\cdot b = \pi\,\{s\cdot b\}$. Then s' is unique.

Proof. If $s''\cdot a = s'\cdot a$ and $s''\cdot b = s'\cdot b$, then $\{x = 0,\ y = s'\}$ and $\{x = 0,\ y = s''\}$ both satisfy the system $x + y\cdot a = s'\cdot a$, $x + y\cdot b = s'\cdot b$. Hence $s' = s''$.

Theorem V. Let A denote a standard affine system under $\{+,\ \cdot\}$. For fixed $u_0 \in A$, define $t \oplus x = t + x$, if $t \neq u_0$; $u_0 \oplus \pi(x) = u_0 + x$, where π is a one-to-one permutation on A. The following is a necessary and sufficient condition that A be affine under $\{\oplus,\ \cdot\}$: given s, $a \neq b \in A$, there exists one (and hence exactly one) s' such that $s'\cdot a = \pi\,\{s\cdot a\}$ and $s'\cdot b = \pi\,\{s\cdot b\}$.

Proof. (The sufficiency) It is enough to show that $u_0 + s\cdot a = e$ and $u_0 + s\cdot b = f$, for $a \neq b$, imply the existance of s' such that $u_0 \oplus s'\cdot a = e$ and $u_0 \oplus s'\cdot b = f$. This is immediate since $\pi\,(s\cdot a) = s'\cdot a$, and $\pi\,(s\cdot b) = s'\cdot b$.

(The necessity) If $u_0 + s\cdot a = e$, and $u_0 + s\cdot b = f$, with $a \neq b$, then $u_0 \oplus \pi(sa) = e$ and $u_0 \oplus \pi\,(sb) = f$. In the affine plane relative to $\{\oplus,\ \cdot\}$, there exists s' such that $u_0 \oplus s'\cdot a = e$ and $u_0 \oplus s'\cdot b = f$; by additive cancellation, $\pi\,\{s\cdot a\} = s'\cdot a$ and $\pi\,\{s\cdot b\} = s'\cdot b$.

Remark. A one-to-one transformation π of the type described in Theorem V must fix 0. In fact, corresponding to given elements $a \neq b$, there is exactly one $s' \in A$ for which both $s' \cdot a = \pi \{s \cdot a\} = \pi (0)$ and $s' \cdot b = \pi \{s \cdot b\} = \pi \{0\}$. Thus $s' \cdot a = \pi \{ 0 \} = s' \cdot b$, with $a \neq b$, implies $s' = 0$.

In the process of transforming a standard affine system $\{ +, \cdot \}$, we may wish to alter exactly one row $u_0 + x$ $(u_0 \neq 0)$ of the addition table by defining $u_0 \oplus x = u_0 + s_0 \cdot x$, for fixed s_0. When does this preserve the affine property? The answer follows easily from Theorem V, and is given below.

Corollary 1. If A forms a standard affine system under $\{ +, \cdot \}$, and if we define $u_0 \oplus x = u_0 + s_0 \cdot x$, for fixed s_0 and fixed $u_0 \neq 0$, then A is affine relative to $\{ \oplus, \cdot \} \Longleftrightarrow$ (i) $s_0 \neq 0$, and (ii) given s, $a \neq b$, there is a unique $s' \in A$ such that $s' \cdot a = s_0 \cdot (sa)$ and $s' \cdot b = s_0 \cdot (s \cdot b)$.

Proof. For $s_0 \in A$, $x \rightarrow s_0 \cdot x$ is one-to-one $\Longleftrightarrow s_0 \neq 0$. Take $\pi : x \rightarrow s_0 \cdot x$, for $s_0 \neq 0$; and apply Theorem V.

Remark. Condition (ii) of Corollary 1 is equivalent to Condition (ii)$'$: given $a \neq b$, $s' \in A$, there is a unique s such that $s' \cdot a = s_0 \cdot (sa)$ and $s' \cdot b = s_0 \cdot (sb)$, for $s_0 \neq 0$.

Proof. It is enough to show that if $s' \cdot a = s_0 \cdot (sa)$ and $s' \cdot b = s_0 \cdot (sb)$, while $s' \cdot a = s_0 (ra)$ and $s' \cdot b = s_0 \cdot (rb)$, then $s = r$. (That establishes a one-to-one correspondence between s and s', for fixed $s_0 \neq 0$, $a \neq b$). We have $s_0 \cdot (ra) = s' \cdot a = s_0 \cdot (sa)$; and $s_0 (rb) = s' \cdot b = s_0 \cdot (sb)$. Hence $(x = 0,\ y = r)$ and $(x = 0,\ y = s)$ both satisfy $x + y \cdot a = 0 + s \cdot a$, $x + y \cdot b = 0 + s \cdot b$; implying $r = s$.

Remark. Special cases in which the conditions of Corollary 1 are valid include the following:

(i) $s_0 \neq 0$; and given s, there is an r (depending on s and s_0), such that $s_0 \cdot (s \cdot x) \equiv r \cdot x$, all $x \in a$ [proof-if $s_0 \cdot (s \cdot x) \equiv r \cdot x$, then $r \cdot a = s_0 \cdot (s \cdot a)$, and $r \cdot b = s_0 \cdot (s \cdot b)$];

(ii) $s_0 \neq 0$; and $s_0 \cdot (y \cdot x) \equiv (s_0 \cdot y) \cdot x$ [proof-given s, take $r = s_0 \cdot s$];

(iii) $s_0 \neq 0$; and $x \cdot (y \cdot z) \equiv (x \cdot y) \cdot z$ [proof obvious].

5. - Projective systems.

The usual homogeneous coordinates for a projective plane can be regarded as the set of number-triples $(x, y, 1)$, $(x, 1, 0)$, and $(1, 0, 0)$, with lines given by the linear equations $(x \cdot 1 + y \cdot a) + z \cdot b = 0$, $y \cdot 1 + z \cdot c = 0$, $z \cdot 1 = 0$. VEBLEN and WEDDERBURN [8] have introduced systems more general than fields (later called « VEBLEN-WEDDERBURN Systems ») whose triples and linear equations still lead to projective planes.

In this section, I shall describe the most general binary system whose triples and linear equations determine a finite projective plane, and relate such homogeneous coordinates to the affine systems already studied. Once again, only finite planes will be considered.

Definition III. A finite set A will be called a *projective system* $\Longrightarrow$ (i) two single-valued binary operations, addition $(+)$ and multiplication $(\cdot)$, are defined on A; (ii) $\exists$ elements 0 and $\Phi \in A$ such that the triples (x, y, Φ), $(x, \Phi, 0)$, and $(\Phi, 0, 0)$, for $x, y \in A$ represent uniquely the points of a projective plane π; (iii) equations of the forms $(x \cdot \psi + y \cdot a) + z \cdot b = 0$, $y \cdot \psi + z \cdot c = 0$, and $z \cdot \psi = 0$ represent all the lines of π.

Lemmas 7-11 concern a projective sustem P.

Lemma 7. Distinct equations represent distinct lines, $0 \cdot \psi = 0$, $\Phi \cdot \psi \neq 0$, $0 \neq \Phi$, and the points $(x, \Phi, 0)$, $(\Phi, 0, 0)$ comprise line $z \cdot \psi = 0$.

Proof. Denote by n the number of elements in P. There are $1 + n + n^2$ equations of the designated form and $1 + n + n^2$ triples (x, y, Φ), $(x, \Phi, 0)$, $(\Phi, 0, 0)$. Hence the corresponding plane π has $1 + n + n^2$ lines, so that distinct equations represent distinct lines.

Since exactly $n + 1$ points satisfy $z \cdot \psi = 0$, we must have $0 \cdot \psi = 0$ but $\Phi \cdot v \neq 0$; whence $0 \neq \Phi$, and line $z \cdot \psi = 0$ consists exactly of the points $(x, \Phi, 0)$ and $(\Phi, 0, 0)$.

Remark. The element ψ may or may not coincide with 0. Also ψ may or may not coincide with Φ. To see this, consider a finite filed, in which we may take $\psi = \Phi = 1 \neq 0$; also the system shown below, in which $\Phi = 1 \neq \neq 0 = \psi$.

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	1	0

Lemma 8. Each line of the form $y \cdot \psi + z \cdot c = 0$ contains $(\Phi, 0, 0)$ and n points (x, y_0, Φ), for some fixed y_0. Distinct values of c correspond to distinct values of y_0. The equation $y \cdot \psi + \Phi \cdot c = 0$ establishes a one-to-one correspondence between y and c.

Proof. By Lemma 7, each equation $y \cdot \psi + z \cdot c = 0$ must be satisfied by a point of the form (x_0, y_0, Φ) and hence by all n points (x, y_0, Φ) but by no other points (x, y, Φ). Since every equation $y \cdot \psi + z \cdot c = 0$ represents a line, and since two points determine exactly one line, distinct values of c give distinct values of y. Hence a one-to-one correspondence between y and c is established by the relation $y \cdot \psi + \Phi \cdot c = 0$.

Each equation $y \cdot \psi + z \cdot c = 0$ must be satisfied by a *single* point having $z = 0$, and so that point must also satisfy $y = 0$. Therefore, the point $(\Phi, 0, 0)$ lies on $y \cdot \psi + z \cdot c = 0$, for every c.

Corollary 2.
$$u \cdot \psi = v \cdot \psi \Longrightarrow u = v$$
$$\Phi \cdot a = \Phi \cdot b \Longrightarrow a = b.$$

The equations $x \cdot \psi = a$ and $\Phi \cdot y = b$ have unique solutions for x amd y respectively.

Proof. If $u \cdot \psi = v \cdot \psi$, let c denote the unique element such that $u \cdot \psi + \Phi \cdot c = 0$. Then $v \cdot \psi + \Phi \cdot c = 0$ and $u = v$.

Similarly, $\Phi \cdot a = \Phi \cdot b \Longrightarrow a = b$.

The uniqueness of the solutions follows from the fact that P is finite.

Corollary 3. The equation $a + x = 0$ has a unique solution for x.

Proof. Let a' denote the unique element for which $a' \cdot \psi = a$. Then $a' \cdot \psi + \Phi \cdot u = 0$ for exactly one u, and $x = \Phi \cdot u$ is the unique solution desired.

Corollary 4. $0 + 0 = 0$ and $0 \cdot u \equiv 0$.

Proof. Since $(\Phi, 0, 0)$ lies on every line $y \cdot \psi + z \cdot u = 0$, it follows that $0 \cdot \psi + 0 \cdot u \equiv 0$. But $0 \cdot \psi = 0$ (Lemma 7), so that $0 + 0 \cdot u \equiv 0$. Thus, regardless of u, $0 \cdot u$ is the unique solution of the equation $0 + x = 0$ and this solution is itself o since $0 + 0 = 0 + 0 \cdot \psi = 0$.

Lemma 9. $u + a = v + a \Longrightarrow u = v$. That is, the equation $x + b = c$ has a unique solution for x.

Proof. By Corollary 2, $\exists$ m, n, c such that $m \cdot \psi = u$, $n \cdot \psi = v$ and $0 \cdot c = a$. By Corollaries 1 and 2, $\exists$ k for which $(m \cdot \psi + \Phi \cdot c) + \Phi \cdot k = 0$. Then also $(n \cdot \psi + \Phi \cdot c) + \Phi \cdot k = 0$, and the points $(m, \Phi, 0)$, (n, Φ, Φ) satisfy the equation $(x \cdot \varphi + y \cdot c) + z \cdot k = 0$. Unless $m = n$, the unique line determined by these two points would have the form $y \cdot \psi + z \cdot d = 0$. Hence $m = n$, and $u = m \cdot \psi = n \cdot \psi = v$.

Lemma 10. The lines through an « ideal point » $(m, \Phi, 0)$ comprise, beside $x \cdot \psi = 0$, exactly n lines $(x \cdot \psi + y \cdot a) + z \cdot b = 0$ for some *fixed* a.

Proof. Assume that $(m, \Phi, 0)$ lies on both of the lines $(x \cdot \psi + y \cdot a) + z \cdot b = 0$ and $(x \cdot \psi + y \cdot a') + z \cdot b' = 0$. Then $(m \cdot \psi + \Phi \cdot a) + 0 = 0$ and $(m \cdot \psi +$

$+ \Phi\cdot a') + 0 = 0$. From Lemma 9, it follows that $m\cdot\psi + \Phi\cdot a = 0 = m\cdot\psi + \Phi\cdot a'$; whence, by Lemma 8, $a = a'$.

Lemma 11. The points of the form (x, y, Φ) which lie on a given line $(x\cdot\psi + y\cdot a) + z\cdot c = 0$ are exactly those which satisfy $x\cdot\psi + y\cdot a = k$. The value of k is determined by c, there being a one-to-one correspondence between c and k.

Proof. For given c, $\exists$ a unique k such that $k + \Phi\cdot c = 0$ (by Lemma 9). Conversely a given k determines uniquely the value c (by Corollaries 2 and 3).

Theorem VI. A (finite) projective system P is also an affine system.

Proof. It will be sufficient to establish conditions (i)-(iv) which characterize an affine system.

(i) $\exists$ *distinct elements*, since $\Phi \neq 0$.

(iv) *If* $a, b, e, f \in P$, *with* $a \neq b$, *then* $\exists$ *a unique ordered pair* t, s, *of elements from* P *for wich* $t + s\cdot a = e$ *and* $t + s\cdot b = f$. In fact, since $a \neq b$, it follows from Lemma 10 that two lines $(x\cdot\psi + y\cdot a) + z\cdot c = 0$ and $(x\cdot\psi + y\cdot b) + z\cdot d = 0$ must meet in a « finite » point. By Lemma 11, equations $x\cdot\psi + y\cdot a = e$ and $x\cdot\psi + y\cdot b = f$ represent the « finite parts » of two distinct lines, hence have a unique solution x, y. Take $t = x\cdot\psi$ and $s = y$.

(iii) $b + u = b + v \Longrightarrow u = v$.

Assume $b + u = b + v = k$. Then, $b + \Phi\cdot m = k$, and $b + \Phi\cdot n = k$, where $\Phi\cdot m = u$ and $\Phi\cdot n = v$. By Lemma 9, $\exists$ x such that $x + 0 = k$. We have disinct solutions $t = x$, $s = 0$ and $t = b$, $s = \Phi$ for the system $t + s\cdot m = k$, $t + s\cdot n = k$. Hence, by Condition (iv), $m = n$ and $u = \Phi\cdot m = \Phi\cdot n = v$.

(ii) *If* $m \neq 0$, $m\cdot u = m\cdot v \Longrightarrow u = v$. Assume that $m\cdot u = m\cdot v$, with $m \neq 0$. Choose any $q \in P$. Then $q + m\cdot u = q + m\cdot v$. Let r be the unique element for which $r + 0 = q + m\cdot u$. Then $t = r$, $s = 0$, and $t = q$, $s = m$ are distinct solutions of the system $t + s\cdot u = q + m\cdot u$, $t + s\cdot v = q + m\cdot v$. This is possible only if $u = v$.

Remark. The converse of the preceding theorem is not true. The example shown below is affine but not projective.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	1	1
1	1	0

If we add to the algebraic postulates (i)-(iv) of an affine system the condition (v) $\equiv 0\cdot x \equiv 0$, (vi) $0+0=0$, (vii) $x\cdot\varphi = y\cdot\varphi \Longrightarrow x = y$, and (viii) $x + a = y + a \Longrightarrow x = y$, we obtain a set of necessary and sufficient conditions that a system be projective. These conditions are not independent, however, since (ii) and (iii) can be established from (i) and (iv)-(viii). The properties (i), (iv)-(viii) are independent, as will be shown.

Theorem VII. A (finite) system P with single-valued binary operations of addition and multiplication is projective $\Longleftrightarrow$

(i) $\exists$ at least two elements $\in P$.

(iv) If, $a, b, e, f \in P$, with $a \neq b$, then $\exists$ an ordered pair t, s, of elements from P for which $t + s\cdot a = e$ and $t + s\cdot b = f$.

(v) $0\cdot x \equiv 0$, for some fixed element $0 \in P$ and for all $x \in P$.

(vi) $0 + 0 = 0$.

(vii) For some fixed element $\psi \in P$, $x\cdot\psi = y\cdot\psi \Longrightarrow x = y$.

(viii) $x + a = y + a \Longrightarrow x = y$.

Proof. These properties have already been proved necessary for a projective system. The proof of the sufficiency follows.

Let Φ be any element $\neq 0$. As « points », take the triples (x, y, Φ), $(x, \Phi, 0)$, $(\Phi, 0, 0)$, for all $x, y \in P$, with distinct triples regarded as distinct points. A « line » shall consist exactly of those points (x, y, z) which satisfy an equation of the form $z\cdot\psi = 0$, $y\cdot\psi + z\cdot a = 0$, or $(x\cdot\psi + y\cdot a) + z\cdot b = 0$.

It is convenient to show first that (i) and (iv)-(viii) imply (ii) and (iii):

(ii) $a\cdot u = a\cdot v$ and $a \neq 0 \Longrightarrow u = v$.

(iii) $a + x = a + y \Longrightarrow x = y$.

Suppose that $a \neq b$. Then each ordered pair t, s determines a unique ordered pair e, f, such that $t + s\cdot a = e$ and $t + s\cdot b = f$; conversely, each ordered pair e, f gives rise to at least one pair t, s. Hence the correspondence $(t, s) \to (e, f)$ is one-to-one and the simultaneous solution given by (iv) is unique. By (viii), $t + 0$ ranges over all P as t ranges over P. Hence the unique solution for a system $t + s\cdot a = e$ and $t + s\cdot b = e$ $(a \neq b)$ satisfies $s = 0$.

Assume $c\cdot u = c\cdot v$, with $u \neq v$. Then $0 + c\cdot u = 0 + c\cdot v$, whence $t = 0$, $s = c$, is the unique solution of the system $t + s\cdot v = 0 + c\cdot u$, $t + s\cdot u = 0 + c\cdot u$; and $c = 0$. This establishes (ii).

Assume that $d + x = d + y$. By (ii) $\exists$ unique m and n for which $\Phi\cdot m = x$ and $\Phi\cdot m' = y$. Thus $t = d$ and $s = \Phi$ satisfy $t + s\cdot m = d + \Phi\cdot m$ and

$t + s\cdot m' = d + \Phi\cdot m$. Unless $m = m'$, this implies $\Phi = 0$, which is impossible. Thus $m = m'$ and $x = \Phi\cdot m = \Phi\cdot m' = y$, proving (iii).

Since $0\cdot\psi = 0$ while $0\cdot\psi \neq 0$, the points satisfying $z\cdot\psi = 0$ are exactly those for which $z = 0$. If a point satisfies both $z = 0$ and $y\cdot\psi + z\cdot a = 0$, then the point satisfies $y = 0$ and must be $(\Phi, 0, 0)$. The points (x, y, Φ) for which $y\cdot\psi + z\cdot a = 0$ are exactly those having some fixed value of y, and different values of a give different values of y. Thus the lines $y\cdot\psi + z\cdot a = 0$ are also given by the equations $y = k$ and intersect only at $(\Phi, 0, 0)$. Given a point $(m, \Phi, 0)$ satisfying $(x\cdot\psi + y\cdot c) + z\cdot d = 0$, the value c is definitely determined and all values of d are possible. These remarks make verification of the synthetic projective postulates trivial, except for the proof that two points (m, n, Φ) and (u, v, Φ), with $n \neq v$ are contained in some line $(x\cdot\psi + y\cdot a) + z\cdot b = 0$. To show this, it is enough to prove that $m\cdot\psi + n\cdot a = u\cdot\psi + v\cdot a$ for some a; and to show the latter it is enough to prove that a solution for q always exists in any equation $c + n\cdot q = c' + v\cdot q$, where $n \neq v$. Given q, $\exists\, c$ such that $c + nq = c' + vq$. If distinct values of q lead to distinct values of c, then c will range over P as q ranges over P; so that for any given c, the desired solution q will exist. Suppose that distinct values q, q' satisfied $c + n\cdot q = c' + v\cdot q$, $c + n\cdot q' = c' + v\cdot q'$. Then the simultaneous system $t + s\cdot q = c + n\cdot q$, $t + n\cdot q' = c + n\cdot q'$ would have distinct solutions $t = c\ s = n$, and $t = c'$, $s = v$, which is impossible.

The independence of Properties (i), (iv)-(viii).

The following six systems establish the respective indipendence of the postulates for a projective system.

(i) $\{0\}$, with $0\cdot 0 = 0$ and $0 + 0 = 0$.

(iv)

+	0	1	2	3
0	0	1	2	3
1	2	0	3	1
2	3	2	1	0
3	1	3	0	2

·	0	1	2	3
0	0	0	0	0
1	2	1	0	3
2	1	0	3	2
3	3	2	0	1

A system $t + s\cdot a = e$, $t + s\cdot b = f$, with $a \neq b$, does not necessarily have a solution-for example, take $a = 0$, $b = e = 2$, and $f = 3$. On the other hand, the system with $a = 0$, $b = e = 2$, $f = 1$ has distinct solutions $\{t = s = 3\}$ and $\{t = 1, s = 2\}$.

(v)

+	0	1
0	0	1
1	1	0

·	0	1
0	1	1
1	1	0

(vi)

+	0	1
0	1	0
1	0	1

·	0	1
0	0	0
1	0	1

(vii)

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	2	1	0

(viii)

+	0	1	2
0	0	1	2
1	1	0	2
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

6. - Normalization of Projective Coordinates.

Every projective system is affine. Hence it follows automatically that a given projective system can be transformed into a « standard » system in which $1\cdot x \equiv x\cdot 1 \equiv x$, $0 + x \equiv x + 0 \equiv x$. Again, the standard system is isotopic to the original. The proof of this fact is practically the same as the proof for the affine case and will not be given here.

Bibliography.

[1] Artin, E.: *Geometric Algebra*, Interscience Publishers, Inc., N. Y. (1957).

[2] Baer *R.*: *Homogeneity of Projective Planes*, Amer. J. of Math., **64** (1942), 137-152.

[3] Birkhoff G.: *Lattice Theory*, Colloquium Publications, Amer. Math. Soc., vol. XXV (1948).

[4] Bruck R. H.: *A Survey of Binary Systems*, Springer Springer-Verlag, Berlin-Göttingen-Heidelberg.

[5] Hall M. Jr.: *Projective Planes*, Trans. Amer. Math. Soc., **54** (1943), 229-277.

[6] Pickert G.: *Projektive Ebenen*, Springer, Berlin (1955).

[7] Pierce W. A.: *General Binary Coordinates for Finite Planes*, SCAMP Project Working paper, SCAMP Project, UCLA (1953).

[8] Veblen O. and Wedderbun J. H. M.: *Non-Desarguesian and non-Pascalian Geometries*, Trans. Amer. Math. Soc., **8** (1907), 379-388.