

# A CLASS OF PROJECTIVE PLANES<sup>(1)</sup>

BY  
DONALD E. KNUTH

1. **Introduction.** Finite non-Desarguesian projective planes have been known for all orders  $p^n$ , where  $p$  is prime,  $n \geq 2$ , and  $p^n \geq 9$ , except when  $p = 2$  and  $n$  is a prime  $\geq 5$ . In this paper a new class of projective planes is defined, having the orders  $2^n$  where  $n \geq 5$  is not a power of two, thus establishing, in particular, the existence of non-Desarguesian planes of the missing orders. The new planes are coordinatized by *semifields* (sometimes called division algebras, non-associative division rings, or distributive quasifields), which are algebraic systems satisfying the axioms for a field except with a loop replacing the multiplicative group. It is easy to show that finite *proper* semifields, i.e., semifields which are not fields, must have the orders  $p^n$  where  $p$  is prime,  $n \geq 3$ , and  $p^n \geq 16$ . Proper semifields of these orders have been known to exist except as above, when  $p = 2$  and  $n$  is prime; therefore the new systems show that proper semifields do exist for any order not excluded by simple arguments. A detailed treatment of the general theory of semifields and their relation to projective planes may be found in [3].

The manner in which these planes were discovered is perhaps as interesting as the planes themselves, since computers played a key role in the discovery. The author had received copies of two tables prepared by R. J. Walker (see [4]), which listed all commutative semifields of order 32 for which, if  $x$  is a generating element,  $x(x(x^2)) = x + 1$  or  $x^2 + 1$ , respectively. There were 24 solutions in each table, and so it seemed plausible that a rule could be found yielding a correspondence between one set of solutions and the other. A few hours of "cryptanalysis" did, in fact, result in the discovery of such a rule; and, since one of the solutions for the table  $x(x(x^2)) = x^2 + 1$  was the field GF(32), the corresponding system for the other table could be written in a simple algebraic form [2]. After this, there was little difficulty showing that the same construction could be generalized to the construction of proper semifields of all orders  $2^{2k+1}$  with  $k > 1$ , and subsequent generalizations yielded the systems described in this paper. Therefore, we have an example in which a rather well-known conjecture in combinatorial analysis has been com-

---

Presented to the Society, March 29, 1962 under the title *Non-Desarguesian planes of order  $2^{2m+1}$* ; received by the editors April 17, 1964.

<sup>(1)</sup> The research reported in this paper was submitted as partial fulfillment of the requirements for the degree of Doctor of Philosophy at the California Institute of Technology.

pletely resolved because the smallest unknown case was analyzed by computer; presumably many more such examples will be known in future years.

The new semifields are defined in §2 of the present paper, and certain automorphisms are exhibited in §3. The collineation group of the corresponding projective planes is completely determined in §4. Since the semifields constructed are commutative, the new planes are self-dual.

**2. Construction of the semifields.** Let  $K = \text{GF}(2^{mn})$ , where  $n$  is odd,  $n > 1$ ; let  $K_0$  be the subfield  $\text{GF}(2^m)$ . Considering  $K$  as a vector space over  $K_0$ , let  $f$  be any nonzero linear functional from  $K$  to  $K_0$ , i.e.,

$$(2.1) \quad f(\lambda a + \mu b) = \lambda f(a) + \mu f(b),$$

for all  $a, b \in K$  and all  $\lambda, \mu \in K_0$ .

Define a new multiplication in  $K$  as follows:

$$(2.2) \quad a \circ b = ab + (f(a)b + f(b)a)^2.$$

**THEOREM 1.** *The algebraic system  $(K, +, \circ)$  is a pre-semifield, i.e., it satisfies all properties of a semifield except that it lacks a multiplicative identity.*

**Proof.** Since the mapping  $a \rightarrow a^2$  is an automorphism of  $K$ , the product  $a \circ b$  is clearly linear in both variables, so both distributive laws hold. Therefore, we need only show that there are no zero divisors.

Suppose  $a \circ b = 0$ , and  $a, b \neq 0$ ; then let  $x = ab^{-1}$ . This implies

$$x + f(a)^2 + f(b)^2 x^2 = 0.$$

We have a quadratic equation with coefficients in  $K_0$ ; but since the degree of  $K/K_0$  is odd, this equation must be reducible. Therefore,  $x \in K_0$ . But then,  $a = xb$  implies

$$a \circ b = ab + [f(xb)b + f(b)xb]^2 = ab \neq 0,$$

and this contradiction completes the proof.

There are, in general, many ways to convert the pre-semifield  $(K, +, \circ)$  into a semifield. Perhaps the simplest way is to define a new product  $a * b$  by the equation

$$(2.3) \quad (1 \circ a) * (1 \circ b) = a \circ b.$$

Then  $(K, +, *)$  is a commutative semifield, since it is easily verified that the distributive laws hold, there are no zero divisors, and 1 is a multiplicative identity.

Notice that we have now defined three different "multiplications" on the elements of  $K$ :  $ab$ ,  $a \circ b$ , and  $a * b$ . It is important to keep this distinction in mind, since all three multiplications are used simultaneously in several proofs of this paper. The powers of an element,  $a^2$ ,  $a^3$ , etc., will always refer to the multiplication of the field.

**THEOREM 2.** *If  $mn > 3$ , it is possible to choose the function  $f$  of (2.1) in such a way that the system  $(K, +, *)$  is a proper semifield, i.e., is not a field.*

**Proof.** Let  $\{1, x, x^2, \dots, x^{n-1}\}$  be a basis of  $K$  over  $K_0$ ; set

$$(2.4) \quad f(1) = f(x) = \dots = f(x^{n-2}) = 0, f(x^{n-1}) = 1.$$

With this definition we find that, for  $\lambda \in K_0$ ,

$$1 \circ \lambda = \lambda, \quad 1 \circ \lambda x = \lambda x, \dots, 1 \circ \lambda x^{n-2} = \lambda x^{n-2}, \quad 1 \circ \lambda x^{n-1} = \lambda x^{n-1} + \lambda^2;$$

and therefore, for all  $a, b \in K$  we have in particular

$$(2.5) \quad 1 \circ (1 \circ a) = a, (a * b) = (1 \circ a) \circ (1 \circ b).$$

Now if  $n > 3$ , let  $k = (n-1)/2$ ; then  $1 < k < n-2$ , and

$$x * (x^k * x^k) = x * x^{n-1} = x^n + x^2 + x \neq x^n = x^{k+1} * x^k = (x * x^k) * x^k.$$

Thus, multiplication is not associative in this case.

If  $n = 3$ , let  $\lambda$  be an element of  $K_0$ ; we have

$$(x * x) * \lambda x = x^2 * \lambda x = (x^2 + 1) \circ \lambda x = \lambda x(x^2 + 1) + \lambda^2 x^2.$$

$$x * (x * \lambda x) = x * \lambda x^2 = x \circ (\lambda x^2 + \lambda^2) = (\lambda x^2 + \lambda^2)x + \lambda^2 x^2.$$

Thus, multiplication is not associative unless  $\lambda^2 = \lambda$ . We can always choose  $\lambda \neq \lambda^2$  unless  $K = \text{GF}(8)$ , which is excluded by hypothesis. This completes the proof. The condition  $mn > 3$  will be assumed in the remainder of the paper.

We now consider the effect of choosing different functions  $f$  in equation (2.1).

**LEMMA 1.** *If  $f, g$  are nonzero linear functionals from  $K$  to  $K_0$ , there exists an element  $z \in K$  such that  $f(az) = g(a)$ , for all  $a$  in  $K$ .*

**Proof.** A simple counting argument will prove this lemma. If

$$\{x_1, x_2, \dots, x_n\}$$

is a basis of  $K$  over  $K_0$ , a linear functional  $f$  is completely determined by the  $n$  choices of  $f(x_i) \in K_0$ ,  $1 \leq i \leq n$ , and these choices are independent provided they are not all zero. Hence, there are  $2^{mn} - 1$  nonzero linear functionals.

Suppose  $f$  is a nonzero linear functional; then if we define  $g(a) = f(az)$ , for  $z \neq 0 \in K$ ,  $g$  is also a nonzero linear functional. There are  $2^{mn} - 1$  such elements  $z$ , so we need only show that no two of these give the same function. But if  $f(az_1) = f(az_2)$  for all  $a$ , we have  $f(a(z_1 - z_2)) = 0$  for all  $a$ , hence  $z_1 - z_2 = 0$  as desired.

An *isotopism* between algebraic systems  $(S, +, *)$  and  $(S', +', *')$  is a triple  $(F, G, H)$  of 1-1 functions from  $S$  onto  $S'$ , such that

$$\begin{aligned}(a+b)F &= aF + {}'bF, (a+b)G = aG + {}'bG, \\ (a+b)H &= aH + {}'bH, (a*b)H = aF * {}'bG.\end{aligned}$$

**THEOREM 3.** *For a given  $K$  and  $K_0$ , any two semifields  $(K, +, *)$  determined by different functionals  $f$  in (2.1) are isotopic.*

**Proof.** Since each semifield is isotopic to its corresponding pre-semifield, we need only show that any two of the pre-semifields are isotopic. Suppose we have

$$\begin{aligned}a \circ b &= ab + [f(a)b + f(b)a]^2, \\ a \cdot b &= ab + [g(a)b + g(b)a]^2.\end{aligned}$$

Apply Lemma 1 to find  $z \in K$  with  $f(az) = g(a)$  for all  $a$ . Then

$$az \circ bz = abz^2 + [g(a)bz + g(b)az]^2 = (a \cdot b)z^2.$$

**COROLLARY.** *If  $mn > 3$ , all systems  $(K, +, *)$  defined in this section are proper semifields.*

This corollary follows from Theorem 2 and the well-known fact that a field is never isotopic to a proper semifield. Moreover, the content of Theorem 3 is that all semifields constructed for  $K$  and  $K_0$  coordinatize the same projective plane, by the well-known theorem of Albert [1] that two finite semifields coordinatize the same plane if and only if they are isotopic.

**3. The binary semifield of  $K/K_0$ .** In this section we will show that if the functional  $f$  is chosen appropriately we obtain a semifield possessing at least  $mn$  automorphisms. This particular semifield, with  $f$  defined by Theorem 4, will be called the binary semifield of  $K/K_0$ .

**THEOREM 4.** *Let  $q = 2^m$ , and let  $f$  be such that  $f(a) = x$  whenever*

$$(3.1) \quad a = x + b + b^q, \quad x \in K_0, b \in K.$$

*Then  $f$  is a linear functional from  $K$  to  $K_0$ , and  $f(a^2) = f(a)^2$ .*

**Proof.** First we show that  $f$  is well defined. Suppose  $x + b + b^q = y + c + c^q$  for  $x \neq y \in K_0$ ; then  $(b+c)^q = (b+c) + x + y$ , i.e.,  $a^q = a + z$  for some  $a \in K$ ,  $z \in K_0$ . Applying the rule again, we find

$$a^{q^2} = a^q + z^q = a^q + z = a.$$

Since  $n$  is odd, we have  $a^{q^{n+1}} = a$ . But  $a^{q^{n+1}} = a^q$ , hence  $z = 0$ . Thus  $f(x + b + b^q)$  is well defined.

Furthermore, every element of  $K$  can be represented in the form  $x + b + b^q$ , since there are precisely  $q$  elements  $c \in K$  for which  $b + b^q = c + c^q$ . For  $(b+c)^q = (b+c)^q$  holds if and only if  $b + c = \lambda \in K_0$ . Therefore,  $f$  is uniquely defined. Finally,

$$\begin{aligned}
 f(x + b + b^q + y + c + c^q) &= f(x + y + (b + c) + (b + c)^q) = x + y \\
 &= f(x + b + b^q) + f(y + c + c^q), \\
 f(y(x + b + b^q)) &= f(yx + yb + (yb)^q) = yx = yf(x + b + b^q),
 \end{aligned}$$

and

$$f((x + b + b^q)^2) = f(x^2 + b^2 + (b^2)^q) = x^2 = f(x + b + b^q)^2.$$

**THEOREM 5.** *The binary semifield of  $K/K_0$  has the automorphism  $a \rightarrow a^2$ ; hence there are at least  $mn$  automorphisms of the binary semifield.*

**Proof.** First we show that  $a \rightarrow a^2$  is an automorphism of the pre-semifield.

$$\begin{aligned}
 (a \circ b)^2 &= (ab + [f(a)b + f(b)a]^2)^2 \\
 &= a^2b^2 + [f(a)^2b^2 + f(b)^2a^2]^2 \\
 &= a^2b^2 + [f(a^2)b^2 + f(b^2)a^2]^2 = a^2 \circ b^2.
 \end{aligned}$$

The automorphism carries over to the semifield, since

$$\begin{aligned}
 ((1 \circ a) * (1 \circ b))^2 &= (a \circ b)^2 = a^2 \circ b^2 \\
 &= (1 \circ a^2) * (1 \circ b^2) \\
 &= (1^2 \circ a^2) * (1^2 \circ b^2) = (1 \circ a)^2 * (1 \circ b)^2.
 \end{aligned}$$

Theorem 9 below shows, conversely, that all automorphisms are given by Theorem 5.

**4. Collineations.** If  $G$  is the collineation group of a projective plane coordinatized by a finite proper semifield, it is well known [1] that  $G$  has subgroups  $G_1$  and  $G_2$ , where  $G = G_1G_2$  and  $G/G_1$  is isomorphic to  $G_2$ . Here  $G_1$ , the "translations and shears," is essentially the same for all semifields; so the collineation group is known once  $G_2$ , the group of all collineations fixing the three points  $(0, 0)$ ,  $(0)$ , and  $(\infty)$ , has been determined. Furthermore,  $G_2$  is isomorphic to the group of all *autotopisms* of the semifield, i.e., the isotopisms of the semifield onto itself. Therefore, we will investigate the autotopisms of  $(K, +, *)$  in this section.

The autotopisms of the semifields may be easily derived from autotopisms of their pre-semifields, so we will first consider the latter. Thus, if  $aF \circ bG = (a \circ b)H$  for all  $a, b \in K$ , we need to find  $F, G$ , and  $H$ . The following theorem reduces these two degrees of freedom to essentially only one degree.

**THEOREM 6.** *If  $(F, G, H)$  is an autotopism of the pre-semifield  $(K, +, \circ)$ , we have  $F = Gz$  for some  $z \neq 0$  in  $K_0$ ; i.e.,*

$$(4.1) \quad aF = (aG)z \quad \text{for all } a \in K.$$

**Proof.** We have, for all  $a, b \in K$ ,

$$(4.2) \quad aF \circ bG = (a \circ b)H = (b \circ a)H = bF \circ aG = aG \circ bF.$$

(Our proof will rest solely on the fact that  $aF \circ bG = aG \circ bF$ .) Thus,

$$(4.3) \quad \begin{aligned} (aF)(bG) + [f(aF)bG + f(bG)aF]^2 \\ = (aG)(bF) + [f(aG)bF + f(bF)aG]^2. \end{aligned}$$

Let  $V_1 = \{a \mid f(aF) = 0\}$ ,  $V_2 = \{a \mid f(aG) = 0\}$ ,  $V_3 = V_1 \cap V_2$ .

Here  $V_1$  and  $V_2$  are vector spaces of dimension  $m(n-1)$  over  $\text{GF}(2)$ , since the kernel of  $f: K \rightarrow K_0$  must have dimension  $n-1$  over  $K_0$ . Also,  $\dim V_3 = \dim V_1 + \dim V_2 - \dim V_1 \cup V_2 \geq 2m(n-1) - mn = m(n-2) \geq 2$ . Therefore  $V_3$  contains at least two nonzero elements.

We apply formula (4.3) to find

$$\frac{aF}{aG} = \frac{bF}{bG} = z \quad \text{for all } a, b \in V_3 - \{0\},$$

for some  $z \in K$ . This proves (4.1) for all elements  $a \in V_3$ .

Now let  $a \in V_3 - \{0\}$ , and let  $b$  be arbitrary. Then

$$z(aG)(bG) + [zf(bG)(aG)]^2 = (aG)(bF) + [f(bF)(aG)]^2,$$

i.e.,

$$(4.4) \quad z(bG) + bF = (aG)[zf(bG) + f(bF)]^2.$$

Replace  $a$  by another element  $a'$  of  $V_3 - \{0\}$ ; since the left-hand side of (4.4) remains constant, but  $aG \neq a'G$ , we have

$$zf(bG) + f(bF) = 0, \quad \text{for all } b \in K.$$

In particular, if we take  $b \notin V_2$ , we conclude that  $z \in K_0$ .

Finally, equation (4.4) becomes

$$z(bG) + bF = 0, \quad \text{for all } b \in K,$$

and this is precisely equation (4.1).

**COROLLARY.** Let  $A_0$  be the set of all autotopisms of  $(K, +, \circ)$  for which  $F = G$ . Then the complete set of all autotopisms is the set

$$A = \{(F\lambda, F\lambda^{-1}, H) \mid 0 \neq \lambda \in K_0 \text{ and } (F, F, H) \in A_0\}.$$

**Proof.** It is immediate that if  $(F, G, H)$  is an autotopism, so is  $(F\lambda, G\lambda^{-1}, H)$ , for  $\lambda \in K_0$ ; therefore, every element of  $A$  is an autotopism. Conversely, if  $(F, G, H)$  is an autotopism we must have  $F = Gz$ , by Theorem 6. Let  $\lambda = \sqrt{z} \in K_0$ ; then  $(F\lambda^{-1}, G\lambda, H)$  is an autotopism belonging to  $A_0$ .

**THEOREM 7.** If  $(F, F, H)$  is an autotopism of  $(K, +, \circ)$ , there is an automorphism  $\tau$  of  $K_0$  such that

$$(4.5) \quad (\lambda a)F = \lambda'(aF), \quad (\lambda a)H = \lambda'(aH) \quad \text{for all } \lambda \in K_0, a \in K.$$

**Proof.** Let  $\lambda \neq 0$  be a fixed element of  $K_0$ , and define the 1-1 mapping  $G$  by the rule

$$(4.6) \quad aG = (\lambda a)F.$$

Then, since  $a \circ \lambda b = \lambda a \circ b$  for all  $\lambda \in K_0$ , we have

$$(4.7) \quad aF \circ bG = (a \circ \lambda b)H = (\lambda a \circ b)H = aG \circ bF.$$

Notice that this result is precisely the same as equation (4.2), which was the basis for the proof of Theorem 6. By the same proof, therefore, we establish the existence of an element  $1/z = \lambda' \neq 0 \in K_0$  such that

$$(\lambda a)F = \lambda'(aF) \quad \text{for all } a \in K.$$

In particular,  $\lambda' = (\lambda F)/(1F)$ .

Let  $0' = 0$ , and let  $\lambda_1, \lambda_2 \in K_0$ . Then

$$\begin{aligned} (\lambda_1 + \lambda_2)' &= (\lambda_1 + \lambda_2)F/1F = \lambda_1' + \lambda_2', \\ (\lambda_1 \lambda_2)' &= (\lambda_1 \lambda_2)F/1F = \lambda_1'(\lambda_2 F)/1F = \lambda_1' \lambda_2', \end{aligned}$$

so  $\lambda' = \lambda^\tau$  for some automorphism  $\tau$  of  $K_0$ . The remaining part of the theorem follows immediately from the fact that  $a^2H = (aF)^2$  for all  $a \in K$ .

Theorem 7 can now be strengthened, and indeed, the entire collineation group can be determined, as follows:

**THEOREM 8.** *If  $(F, F, H)$  is an autotopism of the pre-semifield  $(K, +, \circ)$ , there is an automorphism  $\sigma$  of  $K$  and an element  $x \in K$  such that*

$$(4.8) \quad f(a)^\sigma = f(aF), \quad aF = a^\sigma x, \quad aH = a^\sigma x^2 \quad \text{for all } a \in K.$$

**Proof.** The equation satisfied by  $H, F$  is

$$(4.9) \quad \begin{aligned} (ab)H + (f(a)^2 b^2)H + (f(b)^2 a^2)H \\ = (aF)(bF) + f(aF)^2 (bF)^2 + f(bF)^2 (aF)^2. \end{aligned}$$

Let  $\tau$  be the automorphism of  $K_0$  given by Theorem 7. Since  $a^2H = (aF)^2$ , equation (4.9) takes the following form:

$$(4.10) \quad (ab)H = (aF)(bF) + g(a)^2 (b^2H) + g(b)^2 (a^2H),$$

where

$$(4.11) \quad g(a) = f(a)^\tau + f(aF).$$

Note that  $g\tau^{-1}$  is a linear functional over  $K_0$ . Let  $z \in K$  be a nonzero element such that  $g(z) = 0$ . We now define new functions  $g_1, F_1, H_1$  as follows:

$$(4.12) \quad g_1(a) = g(az), \quad aF_1 = (az)F/(zF), \quad aH_1 = (az^2)H/(zF)^2.$$

Equation (4.10) transforms into

$$(4.13) \quad (ab)H_1 = (aF_1)(bF_1) + g_1(a)^2(b^2H_1) + g_1(b)^2(a^2H_1)$$

and, in particular, for  $b = 1$ , we have the important identity

$$(4.14) \quad aH_1 = aF_1 + g_1(a)^2.$$

We will prove that  $g_1(a) = 0$  for all  $a \in K$ , from which the rest of the theorem follows immediately with  $x = 1F$ . If  $m > 1$  the result is quite easy; for if  $\lambda \in K_0$  we have

$$(\lambda a)H_1 = \lambda'(aH_1) = \lambda'(aF_1 + g_1(a)^2) = (\lambda a)F_1 + \lambda'g_1(a)^2,$$

and also  $(\lambda a)H_1 = (\lambda a)F_1 + g_1(\lambda a)^2$ . But  $g_1(\lambda a) = \lambda'g_1(a)$  by (4.12), (4.11), and (4.5), hence,  $\lambda' = (\lambda')^2$  or else  $g_1(a) = 0$ . If  $m > 1$  and  $\lambda \neq 0, 1$  we cannot have  $\lambda' = (\lambda')^2$ .

In the case  $m = 1$  the problem seems to be more difficult. We prove the following lemma:

**LEMMA 2.** *Let  $V = \{a | g_1(a) = 0\}$ . If  $a \in V$  and  $a^2 \in V$ , then  $a^k \in V$  for all  $k \geq 0$ .*

**Proof.** We show by induction on  $k$  that  $a^k \in V$  and, simultaneously, that  $(a^k)H_1 = (aF_1)^k$ . This is certainly true for  $k = 1$ . Assume  $k > 1$  and that it is true for  $k - 1$ . Then

$$\begin{aligned} (a^k)H_1 &= (aF_1)(a^{k-1}F_1) = (aF_1)(a^{k-1}H_1) = (aF_1)^k; \\ (a^{k+1})H_1 &= (a^2F_1)(a^{k-1}F_1) = (a^2H_1)(a^{k-1}H_1) = (aF_1)^{k+1}; \\ (a^{k+1})H_1 &= (aF_1)(a^kF_1) + g_1(a^k)^2(a^2H_1) \\ &= (aF_1)(a^kH_1) + g_1(a^k)^2(aF_1 + (aF_1)^2). \end{aligned}$$

Therefore,  $g_1(a^k)^2(aF_1 + (aF_1)^2) = 0$ . If  $g_1(a^k) \neq 0$ , we have  $aF_1 = (aF_1)^2$  which implies  $a = 0$  or  $1$ . Hence,  $g_1(a^k) = 0$ , proving the lemma.

To complete the proof of Theorem 8, we let  $m = 1$ , hence  $n \geq 5$ . The number of elements of  $K$  which lie in proper subfields is at most  $2^{d_1} + \dots + 2^{d_r}$ , where  $d_1, \dots, d_r$  are the divisors of  $n$  less than  $n$ . But let  $V' = \{a | a^2 \in V\}$ ,  $V'' = V \cap V'$ . Since  $\dim V'' = \dim V + \dim V' - \dim V \cup V' \geq (n-1) + (n-1) - n = n-2$ ,  $V''$  must contain an element  $a$  which lies in no proper subfield of  $K$ . But then by Lemma 2,  $V''$  contains all polynomials in  $a$ , i.e.,  $V'' \supseteq K$ . Therefore,  $V = K$  and Theorem 8 follows.

**THEOREM 9.** *All autotopisms with  $F = G$  for the binary semifield of  $K/K_0$  are the automorphisms generated by  $a \rightarrow a^2$ .*

**Proof.** Let  $f$  be the function defined in Theorem 4, and apply Theorem 8 to the resulting pre-semifield. Any autotopism  $(F, F, H)$  of  $(K, +, \circ)$  must be an automorphism of  $K$ , since  $f(a^x) = f(a)^x = f(aF) = f(a^x x)$  for all  $a \in K$  implies  $x = 1$ . Therefore, by the Corollary to Theorem 6, all



autotopisms  $(F, G, H)$  of  $(K, +, \circ)$  are given by

$$(4.15) \quad (F, G, H) = (\sigma\lambda, \sigma\lambda^{-1}, \sigma), \quad \sigma \text{ an automorphism of } K, \quad \lambda \in K_0.$$

If  $aU = 1 \circ a$ , the autotopisms of  $(K, +, *)$  are simply  $(U^{-1}FU, U^{-1}GU, H)$ , where  $(F, G, H)$  is an autotopism of  $(K, +, \circ)$ . The fact that  $U^{-1}FU = F$  whenever  $F = \sigma$  is an automorphism of  $K$  (see the proof of Theorem 5) completes the proof of Theorem 9. Note also that the group of all autotopisms for the binary semifield of  $K/K_0$ , being conjugate to (4.15), is isomorphic to the group of permutations of  $K$  with elements  $(\sigma, \lambda)$ , where  $a(\sigma, \lambda) = a^\sigma \lambda$ .

Finally, we state the following theorem, which follows immediately from the remarks above.

**THEOREM 10.** *The group of collineations fixing  $(0, 0)$ ,  $(0)$ , and  $(\infty)$  in the projective plane coordinatized by the binary semifield of  $K/K_0$  is of order  $mn(2^m - 1)$ . Hence, the projective planes for different choices of  $K_0$  are non-isomorphic. The subgroup of collineations which fix all points of the line  $x = 0$  is a cyclic, normal subgroup of order  $2^m - 1$ . The quotient group, isomorphic to the subgroup of all collineations which fix the points  $(0, 0)$ ,  $(1, 1)$ ,  $(0)$ , and  $(\infty)$ , is a cyclic subgroup of order  $mn$ .*

#### REFERENCES

1. A. A. Albert, *Finite division algebras and finite planes*, Proc. Sympos. Appl. Math. Vol. 10, pp. 53-70, Amer. Math. Soc., Providence, R. I., 1960.
2. D. E. Knuth, *Non-Desarguesian planes of order  $2^{2m+1}$* , Abstract 62T-137, Notices Amer. Math. Soc. 9 (1962), 218.
3. ———, *Finite semifields and finite planes*, J. Algebra (to appear).
4. R. J. Walker, *Determination of division algebras with 32 elements*, Proc. Sympos. Appl. Math. Vol. 15, pp. 83-85, Amer. Math. Soc., Providence, R. I., 1962.

CALIFORNIA INSTITUTE OF TECHNOLOGY,  
PASADENA, CALIFORNIA