BULL. AUSTRAL. MATH. SOC. 12K05, 20N05
VOL. 7 (1972), 163-168.

Pseudo-fields and doubly transitive groups

F.W. Wilke

A sharply doubly transitive group which acts on a set of at least two elements is isomorphic to the group of affine transformations on a system S. This statement is true if S is replaced by either strong pseudo-field or pseudo-field. The additive system of a strong pseudo-field is a loop while the additive system of a pseudo-field need not be a loop. We show that any pseudo-field is either a strong pseudo-field or can be obtained from a strong pseudo-field in a nice way. Every near-field is a strong pseudo-field. The converse is an open question.

DEFINITION 1 (Tits, [2]). A (left) pseudo-field $(F, +, \cdot)$ is a set F of cardinality at least two with binary operations $+$ and $\cdot$ such that

(1) there exists $0 \in F$ such that $x + 0 = 0 + x = x$ and $x \cdot 0 = 0 \cdot x = 0$ for all $x \in F$;

(2) for each $a \in F$ there exists $-a \in F$ such that $a + (-a) = (-a) + a = 0$;

(3) $F - \{0\}$ is a group under $\cdot$ with identity 1 ;

(4) $x \cdot (y+z) = x \cdot y + x \cdot z$ for all $x, y, z \in F$;

(5) for $a, b \in F$ there exists an element $\rho(a, b) \in F$ such that $(x+a) + b = \rho(a, b) \cdot x + (a+b)$ for all $x \in F$.

Received 11 April 1972.

THEOREM 1 (Tits, [2]). *A sharply doubly transitive group of permutations acting on a set of cardinality at least two is isomorphic to the group of affine transformations* $x \to a \cdot x + b$ *on a pseudo-field.*

DEFINITION 2. A (left) near-field $(N, +, \cdot)$ is a system of cardinality at least two such that $(N, +)$ is an abelian group with identity 0, $N - \{0\}$ is a group under $\cdot$ with identity 1, $0 \cdot x = 0$ for all $x \in N$ and $x \cdot (y+z) = x \cdot y + x \cdot z$ for all $x, y, z \in N$. If, in addition, $r, s, t \in N$ with $r \neq s$ implies there exists $x \in N$ such that $r \cdot x = s \cdot x + t$, then $(N, +, \cdot)$ is called a planar near-field.

In [1, Theorem 20.7.1] Hall proves

THEOREM 2. *If* G *is a sharply doubly transitive group of permutations acting on a set* E *of cardinality at least two such that either*

(1) E *is finite or*

(2) i *and* j *distinct elements of* E *implies there exists at most one* $g \in G$ *such that* $g(i) = j$ *and* g *has no fixed point*

then G *is isomorphic to the group of affine transformations* $x \to a \cdot x + b$ *on a planar near-field.*

Zemmer [3] has constructed a class of non-planar near-fields. The group of affine transformations on such a near-field is sharply doubly transitive but does not satisfy either (1) or (2) of Theorem 2.

Suppose G is a permutation group acting on a set E which satisfies the conditions of Theorem 2. Let $0, 1$ be distinct elements of E and let G_0 be the stabilizer of 0. For each $i \in E$, $i \neq 0$, let g_i be the unique element of G such that $g_i(0) = i$ and $g_i(k) \neq k$ for all $k \in E$ and let m_i be the unique element of G_0 such that $m_i(1) = i$. Finally, let g_0 be the identity. Then Hall shows that $(E, +, \cdot)$ is a planar near-field where $+$ and $\cdot$ are defined by

$$x + y = g_y(x)$$

and

$$x \cdot y = \begin{cases} 0 & \text{if } x = 0 , \\ m_x(y) & \text{if } x \neq 0 . \end{cases}$$

The group of affine transformations on this near-field is isomorphic to the group G .

Even without assuming (1) and (2) of Theorem 2 an element of G may be chosen to play the role of g_y as follows. For each $x \in E$, $x \neq 0$, let t_x be the unique involution which maps 0 onto x . In any doubly transitive group the involutions occur in a single conjugate class. Thus, either

(a) each involution has a unique fixed point and t_0 is defined to be the unique involution fixing 0 or

(b) no involution has a fixed point and t_0 is defined to be the identity.

Then, if $+$ is defined by

$$x + y = t_y t_0(x)$$

and $\cdot$ is defined as above then $(E, +, \cdot)$ is a system called a strong pseudo-field, and G is isomorphic to the group of affine transformations $x \to a \cdot x + b$ on $(E, +, \cdot)$.

DEFINITION 3. A strong pseudo-field $(F, +, \cdot)$ is a set F of cardinality at least two such that

(1) $(F, +)$ is a loop with identity 0 ;

(2) $F - \{0\}$ is a group under $\cdot$ with identity 1 ;

(3) $x \cdot (y+z) = x \cdot y + x \cdot z$ for all $x, y, z \in F$;

(4) $0 \cdot x = 0$ for all $x \in F$;

(5) for $a, b \in F$ there exists an element $\rho(a, b) \in F$ such that $(x+a) + b = \rho(a, b) \cdot x + (a+b)$ for all $x \in F$.

It is immediate that a near-field is a strong pseudo-field which, in turn, is a pseudo-field. Example 1 (see [2, 5.6]) below, shows that there are pseudo-fields which are not strong pseudo-fields. It is not known whether or not there exist strong pseudo-fields which are not near-fields.

EXAMPLE 1. Let $(F, +, \cdot)$ be a strong pseudo-field in which $1 + 1 \neq 0$. Define

$$x \oplus y = \begin{cases} -x + y & \text{if } y \neq 0 , \\ x + y & \text{if } y = 0 . \end{cases}$$

Then $(F, \oplus, \cdot)$ is a pseudo-field but is not a strong pseudo-field since $(F, \oplus)$ is not a loop. In particular, for any $a \neq 0$ the equation $a \oplus x = -a$ has no solution. On the other hand, in any pseudo-field,

$$-a = \big((-a)+a\big) + (-a) = \rho(a, -a) \cdot (-a) + \big(a+(-a)\big) = \rho(a, -a) \cdot (-a) ,$$

so that $\rho(a, -a) = 1$. Thus $(x+a) + (-a) = x$ for all x, $a \in F$ and the equation $x + a = b$ has the solution $x = b + (-a)$. Also, since $0 = (-1) \cdot [1+(-1)] = (-1) + (-1) \cdot (-1)$ we have $(-1) \cdot (-1) = 1$ in any pseudo-field.

THEOREM 3. *If* $(F, +, \cdot)$ *is a pseudo-field then* $(F, +, \cdot)$ *is a strong pseudo-field or may be obtained from a strong pseudo-field by the procedure in Example* 1.

Proof. Let $(F, +, \cdot)$ be a pseudo-field. For $a, b \in F$ with $a \neq 0$ let $T_{a,b}$ be the permutation of F given by $T_{a,b}(x) = a \cdot x + b$. If $G = \{T_{a,b} \mid a, b \in F , a \neq 0\}$ then G is a sharply doubly transitive group acting on F; (see [2, 5.3]). Let G_0 be the stabilizer of 0. Each element of G_0 is of the form $T_{a,0}$ for $a \in F$, $a \neq 0$. For each $x \in F$, $x \neq 0$, let t_x be the unique involution in G which interchanges 0 and x. If the involutions of G have fixed points then t_0 is the unique involution fixing 0. Otherwise t_0 is the identity mapping. Define $x \oplus y = t_y t_0(x)$. As noted above, $(F, \oplus, \cdot)$ is a strong pseudo-field.

Suppose the involutions of G have no fixed points. If $a \cdot a = 1$ then $T_{a,0}T_{a,0} = T_{1,0}$. Thus $a = 1$, since otherwise $T_{a,0}$ is an involution fixing 0. Since $(-1) \cdot (-1) = 1$ we see that $-x = x$ and

$x + x = 0$ for all $x \in F$. Therefore, $T_{1,x}T_{1,x}(z) = (z+x) + x = z$ since $\rho(x, -x) = \rho(x, x) = 1$. Thus, $t_x = T_{1,x}$ and

$$z + x = T_{1,x}(z) = t_x t_0(z) = z \oplus x$$

for all $z, x \in F$. Therefore, if the involutions of G have no fixed points then $(F, +, \cdot)$ is a strong pseudo-field.

Suppose the involutions of G have fixed points. Then $t_0 = T_{a,0}$ for some $a \in F$ such that $a \cdot a = 1$. Since t_0 is not the identity mapping, $a \neq 1$. In fact, a is the unique element of F of multiplicative order two. Since $(-1) \cdot (-1) = 1$ we must have $-1 = a$ or $-1 = 1$.

If $-1 = a$ then $T_{-1,y} = t_y$ and

$$x + y = T_{1,y}(x) = T_{-1,y}T_{-1,0}(x) = t_y t_0(x) = x \oplus y \text{ ,}$$

and $(F, +, \cdot)$ is a strong pseudo-field.

If $-1 = 1$ then $x + x = 0$ for all $x \in F$ and $T_{1,x} = t_x$ if $x \neq 0$. Thus

$$\begin{aligned} x + y = T_{1,y}(x) &= T_{1,y}T_{a,0}T_{a,0}(x) \\ &= \begin{cases} t_y t_0(a \cdot x) & \text{if } y \neq 0 \text{ ,} \\ x & \text{if } y = 0 \text{ ,} \end{cases} \\ &= \begin{cases} (a \cdot x) \oplus y & \text{if } y \neq 0 \text{ ,} \\ x & \text{if } y = 0 \text{ .} \end{cases} \end{aligned}$$

Since for $x \neq 0$, $0 = x + x = a \cdot x \oplus x$ we have $a \cdot x = \ominus x$ where $\ominus$ denotes the negative with respect to $\oplus$. Therefore,

$$x + y = \begin{cases} \ominus x \oplus y & \text{if } y \neq 0 \text{ ,} \\ x & \text{if } y = 0 \text{ ,} \end{cases}$$

so that $(F, +, \cdot)$ can be obtained from the strong pseudo-field $(F, \oplus, \cdot)$ by the procedure in Example 1.

To give the reader some idea of how "close" a strong pseudo-field is to being a near-field we list, without proof, some properties of the additive loop $(F, +)$ of a strong pseudo-field.

1. $(F, +)$ is a right Bol loop.

2. $(F, +)$ has the automorphic inverse property.

3. $(F, +)$ has a sharply simply transitive group of automorphisms.

4. If $(F, +)$ satisfies any one of the properties - left inverse, weak inverse, crossed inverse - then $(F, +)$ is an abelian group and hence $(F, +, \cdot)$ is a near-field.

References

[1] Marshall Hall, Jr, *The theory of groups* (The Macmillan Company, New York, 1959).

[2] J. Tits, "Sur les groupes doublement transitifs continus", *Comment. Math. Helv.* 26 (1952), 203-224.

[3] J.T. Zemmer, "Near-fields, planar and non-planar", *Math. Student* 32 (1964), 145-150.

Department of Mathematics,
University of Missouri - St Louis,
St Louis,
Missouri,
USA.

https://doi.org/10.1017/S0004972700044944 Published online by Cambridge University Press