Riv. Mat. Univ. Parma (4) **12** (1986), 241-247

S. B. NESBITT-STOBERT and C. W. L. GARNER (*)

A direct proof that all Hall planes of the same finite order are isomorphic (**)

Introduction

The usual proof ([2], p. 215) that all Hall planes of the same finite order are isomorphic uses Ostrom's concept of derivation and related results ([3] or [2], Chapter X). In this paper we present an elementary proof of this result, showing actual isomorphisms between planes. To do so, we show how to obtain one Hall quasifield from another by changing the multiplication, but consider separately quasifields which are defined over fields of characteristic 2 or $\neq 2$.

1 - Definition of Hall quasifields and Hall planes

Let K be a finite field and $f(x) = x^2 - px - q$ an irreducible quadratic over K. Let H be a 2-dimensional right vector-space over K with basis elements 1 and λ. Addition in H is ordinary vector addition, but multiplication in H is defined by

$$(\lambda c + d)\cdot(\lambda a + b) = \lambda(cb - da + pa) + db - c^{-1}af(d) \qquad \text{if } c \neq 0$$

(1)

$$d(\lambda a + b) = \lambda(da) + db\,.$$

Then H is a quasifield ([2], pp. 183-185) called a *Hall quasifield.* If K is $GF(h)$, H is clearly of order h^2.

(*) Indirizzo degli AA.: S. B. NESBITT-STOBERT, National Health and Welfare, Ottawa, Ontario, Canada; C. W. L. GARNER, Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario K1S 5B6, Canada.

(**) Ricevuto: 11-VII-1985.

Lemma 1.1. *If $h = p^r$ for a prime p and positive integer r, then there are $\frac{1}{2}h(h-1)$ non-isomorphic Hall quasifields of order h^2.*

Proof. In $K = GF(h)$, there are h^2 quadratic polynomials of the form $x^2 - px - q \cdot \frac{1}{2}h(h+1)$ of these are reducible since they can be factored into $(x-a)(x-b)$ with $a, b \in K$. This leaves $\frac{1}{2}h(h-1)$ irreducible quadratic polynomials, and each one determines (by (1)), a unique Hall quasifield.

If H is any Hall quasifield, then the *Hall plane* $\pi(H)$ is the projective plane coordinatized by H in the usual way ([2], p. 126; [5], p. 98). A point (x, y) and line $[m, k]$ are defined to be incident if and only if $y = mx + k$.

2 - Classes of Hall quasifields

Let H be a Hall quasifield of order h^2 defined over $K = GF(h)$, with irreducible polynomial $f(x) = x^2 - px - q$. For any $a \in K$, let H_a be the algebraic system consisting of the same elements as H, addition as in H and multiplication $\dot{a}$ defined by

$$x \mathbin{\dot{a}} y = (x + a) \cdot y - a \cdot y \tag{2}$$

where $\cdot$ denotes multiplication in H. Note that $x \mathbin{\dot{a}} y = x \cdot y$ if $y \in K$.

Lemma 2.1. *For any $a \in K$, H_a is a quasifield.*

The proof of this lemma consists in a straightforward checking of the properties of a quasifield.

Lemma 2.2. *Let H be a Hall quasifield over $K = GF(h)$ with associated polynomial $f(x) = x^2 - px - q$. Then the Hall quasifield H_a as constructed above has associated polynomial*

$$g(x) = x^2 - (p - 2a)x - (q + ap - a^2)\ . \tag{3}$$

Proof. Let $x \in H - K$ so that $f(x) = x^2 - px - q = 0$.

Now by definition of multiplication $\dot{a}$ in H_a,

$$(x-a) \mathbin{\dot{a}} x = (x - a + a) \cdot x - a \cdot x = x \cdot x - a \cdot x$$

and so, by (3),

$$(x-a) \mathbin{\dot{a}} (x - a + a) = px + q - a \cdot x\ .$$

Then by right distributivity of $\underset{a}{\cdot}$,

$$(x-a) \underset{a}{\cdot} (x-a) + (x-a) \underset{a}{\cdot} a = px + q - a \cdot x \ .$$

Using (2) again, we have

$$(x-a) \underset{a}{\cdot} (x-a) + x \cdot a - a \cdot a = px + q - a \cdot x$$

and so

$$(x-a) \underset{a}{\cdot} (x-a) = px - (a \cdot x + x \cdot a) + a \cdot a + q \ .$$

But $a \cdot x = x \cdot a$ (from (1) since $a = \lambda 0 + a \in K$) and so, since $p, 2a \in K$,

$$(x-a) \underset{a}{\cdot} (x-a) = (p-2a) \cdot x + a \cdot a + q \ .$$

Thus

$$\begin{aligned}(x-a) \underset{a}{\cdot} (x-a) &= (p-2a) \cdot (x-a) + a \cdot a + q + (p-2a) \cdot a \\ &= (p-2a) \cdot (x-a) + (q + a \cdot p - a^2)\end{aligned}$$

so that $x-a$ satisfies the equation

$$g(x) = x^2 - px - q = 0 \qquad \text{for all elements } x - a \in H_a - K$$

where $x^2 = x \underset{a}{\cdot} x$.

Hence all elements in $H_a - K$ satisfy the quadratic equation $g(x) = 0$, which must now be shown to be irreducible. Suppose $g(z) = 0$ for some $z \in K$. Then $z^2 - (p-2a)z - (q + ap - a^2) = 0$, which implies $z^2 - pz + 2az - q - ap + a^2 = 0$ since $z \in K$, and so $(z-a)^2 - p(z-a) - q = 0$. But then $f(x) = x^2 - px - q$ is reducible in K which yields a contradiction.

Let $C_H = \{H_a | a \in K\}$ be the class of all Hall quasifields constructed from a given Hall quasifield H. We wish to show that all quasifields in a class C_H coordinatize isomorphic planes.

Lemma 2.3. *For all* $H_a \in C_H$, $\pi(H_a) \simeq \pi(H)$.

Proof. Consider the mapping $\psi : \pi(H) \to \pi(H_a)$ given by

$$\begin{aligned}\psi : (x, y) &\to (x, y - ax) & [m, k] &\to [m - a, k] \\ (x) &\to (x - a) & [k] &\to [k] \\ (\infty) &\to (\infty) & [\infty] &\to [\infty] \ .\end{aligned}$$

Since ψ is clearly one-to-one and onto, we need only check incidence preservation. Omitting the trivial incidences, (x, y) incident with $[m, k]$ implies $y = m \cdot x + k$ and so $y - a \cdot x = m \cdot x - a \cdot x + k$. Then using (2), we have $y - a \cdot x = (m - a) \,_{a}\dot{} \, x + k$ and so $(x, y - a \cdot x)$ is incident with $[m - a, k]$. Thus $\psi(x, y)$, $\psi[m, k]$ are incident and the two planes $\pi(H)$, $\pi(H_a)$ are isomorphic.

Lemma 2.4. *If H is Hall quasifield defined over a field K and $a, b \in K$, then $(H_a)_b = H_{a+b}$.*

Proof. Using (2) to first change multiplication to $_{a\dot{+}b}$ we obtain

$$\begin{aligned} x \,_{a\dot{+}b}\, y &= (x + a + b) \cdot y - (a + b) \cdot y \\ &= (x + b + a) \cdot y - a \cdot y - (b + a) \cdot y + a \cdot y \\ &= (x + b) \,_{a}\dot{} \, y - b \,_{a}\dot{} \, y \end{aligned}$$

and we see that multiplication $_{a\dot{+}b}$ is accomplished by first changing to $_{a}\dot{}$ multiplication and then to $_{b}\dot{}$ multiplication. Since the sets of elements H, $H_a (a \in K)$ are identical and the same addition is involved, the lemma is proved.

As an immediate corollary we obtain

Corollary 2.5. *$C_H = C_{H_a}$ for all $a \in K$.*

By this corollary, we have that any class of Hall quasifields is determined by any quasifield in it and thus by its irreducible polynomial. Thus in view of Lemma 2.3, to accomplish the main goal of showing that all Hall planes of the same finite order are isomorphic, we need only consider planes from distinct classes. For this purpose, it is necessary to distinguish between planes whose coordinatizing quasifields are defined over fields of characteristic 2 or characteristic $\neq 2$.

3 - Hall quasifields defined over a field of characteristic $\neq 2$

Lemma 3.1. *Let K be a field of characteristic $\neq 2$. The Hall quasifields over $K = GF(h)$ can be partitioned into $\frac{1}{2}(h-1)$ classes of cardinality h, where each class is characterized by an irreducible polynomial of the type $x^2 - q$.*

Proof. In $K = GF(h)$ there are $\frac{1}{2}(h-1)$ non-squares and so $\frac{1}{2}(h-1)$ irreducible polynomials of the form $x^2 - q$. If H is a Hall quasifield over K with

associated polynomial $x^2 - q$, then by Lemma 2.2, the irreducible polynomials determining the Hall quasifields in C_H will have the form

$$g(x) = x^2 + 2ax - (q - a^2)$$

for all $a \in K$. Since the characteristic of K is not 2, these polynomials are all distinct and so there are h of them. Thus the class C_H has cardinality h.

Theorem 3.2. *Hall quasifields over a finite field K of characteristic $\neq 2$ coordinatize isomorphic planes.*

Proof. Let H_1, H_2 be two Hall quasifields defined over K which are in distinct classes. By the previous lemma, we may assume that their associated polynomials are $x^2 - q_1$ and $x^2 - q_2$ respectively. Consider the mapping $\theta : \pi(H_1) \to \pi(H_2)$ given by

$$\begin{aligned} \theta : (x, y) &\to (rx, y) & [m, k] &\to [r^{-1}m, k] \\ (x) &\to (r^{-1}x) & [m] &\to [rm] \\ (\infty) &\to (\infty) & [\infty] &\to [\infty] \end{aligned}$$

where $r = (q_2^{-1} q_1)^{\frac{1}{2}}$.

Since both q_1 and q_2 are non-squares, $q_2^{-1} q_1$ is a square, as the squares form a subgroup of index 2 in the multiplicative group of K. Thus $r = (q_2^{-1} q_1)^{\frac{1}{2}}$ exists.

Since θ is clearly 1-1 and onto, it is sufficient to show that θ preserves the (non-trivial) incidences.

(x, y) is incident with $[m, k]$ if and only if $y = m \,\dot{}\, x + k$. Let $y = \lambda y_1 + y_2$, $x = \lambda x_1 + x_2$, $m = \lambda m_1 + m_2$, $k = \lambda k_1 + k_2$ $(y_i, x_i, m_i, k_i \in K \quad (i = 1, 2))$. Then $y = m \,\dot{}\, x + k$ becomes

$$\begin{aligned} &\lambda y_1 + y_2 = (\lambda m_1 + m_2) \,\dot{}\, (\lambda x_1 + x_2) + (\lambda k_1 + k_2) \\ &= \lambda(m_1 x_2 - m_2 x_1) + m_2 x_2 - m_1^{-1} x_1 f(m_2) + (\lambda k_1 + k_2) \\ &= \lambda(m_1 x_2 - m_2 x_1) + m_2 x_2 - m_1^{-1} x_1 (m_2^2 - q_1) + (\lambda k_1 + k_2) \\ &= \lambda(m_1 r^{-1} r x_2 - m_2 r^{-1} r x_1) + m_2 r^{-1} r x_2 - (m_1^{-1} r^{-1} r x_1)(m_2^2 - q_1) + (\lambda k_1 + k_2) \\ &= \lambda(m_1 r^{-1} r x_2 - m_2 r^{-1} r x_1) + m_2 r^{-1} r x_2 - (m_1 r^{-1})^{-1} r x_1 ((m_2 r^{-1})^2 - q_2) + (\lambda k_1 + k_2) \\ &= (r^{-1} m) \,\dot{}\, (rx) + k \,. \end{aligned}$$

Thus $y = m \,\dot{}\, x + k$ if and only if $y = (r^{-1} m) \,\dot{}\, (rx) + k$, that is, (x, y) is incident with $[m, k]$ if and only if $\theta(x, y)$ is incident with $\theta[m, k]$.

4 - Hall quasifields defined over a field of characteristic = 2

Lemma 4.1. *Let K be a field of characteristic $=2$. The Hall quasifields over $K = GF(h)$ can be partitioned into $h-1$ classes of cardinality $h/2$, where each class is characterized by the middle term of its associated irreducible polynomials.*

Proof. If H is a Hall quasifield over $K = GF(h)$ where $h = 2^r$ for some positive integer r with associated polynomial $f(x) = x^2 - px - q$, then by Lemma 2.2, the other Hall quasifields in C_H have associated polynomials $f_a(r) = x^2 - (p - 2a)\cdot x - (q + ap - a^2)$ for $a \in K$. Since K has characteristic 2, $f_a(x) = x^2 - px - (q + ap - a^2)$. Thus each Hall quasifield in C_H has the identical middle term in its associated polynomial.

In a field of characteristic 2, a quadratic $x^2 + bx + c$ with $b \neq 0$ is irreducible if and only if c/b^2 is not in P, the set of all elements expressible in the form $x^2 + x$ for $x \in K$ ([1], p. 934). The cardinality of P is $\frac{1}{2}h$. Since there are no irreducible polynomials of the type $f(x) = x^2 + q$ in $GF(2^r)$, there are precisely $h - 1$ classes of Hall quasifields, each of cardinality $h/2$, and each class is characterized by the middle term of the associated polynomials.

Theorem 4.2 *Hall quasifields over a finite field K of characteristic $=2$ coordinatize isomorphic planes.*

Proof. First note that $x^2 - px - p^2q$ is irreducible over K if and only if $p^2q/p^2 \notin P$, and this is equivalent to $x^2 - x - q$ being irreducible over K ([1], p. 934). Thus, without loss of generality, let H_1 and H_2 be two Hall quasifields over K with associated irreducible polynomials $f_1(x) = x^2 - x - q$ and $f_2(x) = x^2 - px - p^2q$ respectively. Let $\dot{1}$ and $\dot{2}$ denote their respective multiplications. We shall show that the mapping $\dot{\varphi}: \pi(H_1) \to \pi(H_2)$ defined by

$$\begin{array}{ll} (x, y) \to (p^{-1}x, y) & [m, k] \to [pm, k] \\ (x) \to (px) & [m] \to [p^{-1}m] \\ (\infty) \to (\infty) & [\infty] \to [\infty] \end{array}$$

is an isomorphism.

Clearly, $\dot{\varphi}$ is 1-1 and onto.

Letting $y = \lambda y_1 + y_2$, $x = \lambda x_1 + x_2$, $k = \lambda k_1 + k_2$, we have

$$\lambda y_1 + y_2 = (\lambda m_1 + m_2)\,\dot{1}\,(\lambda x_1 + x_2) + (\lambda k_1 + k_2)$$

and so, using (1) with $f(x) = f_1(x)$,

$$\begin{aligned}\lambda y_1 + y_2 &= \lambda(m_1 x_2 - m_2 x_1 + x_1) + m_2 x_2 - m_1^{-1} x_1(m_2^2 - m_2 - q) + (\lambda k_1 + k_2)\\ &= \lambda(m_1 pp^{-1} x_2 - m_2 pp^{-1} x_1) + \lambda pp^{-1} x_1 + m_2 pp^{-1} x_2\\ &\qquad - (pm_1)^{-1}(p^{-1} x_1)(p^2 m_2^2 - p(pm_2) - p^2 q) + (\lambda k_1 + k_2)\\ &= (\lambda pm_1 + pm_2) \,\dot{2}\, (\lambda p^{-1} x_1 + p^{-1} x_2) + (\lambda k_1 + k_2)\\ &= pm_1 \,\dot{2}\, p^{-1} x + k\ .\end{aligned}$$

Thus $y = m \,\dot{1}\, x + k$ if and only if $y = (pm) \,\dot{2}\, (p^{-1} x) + k$, and so (x, y) is incident with $[m, k]$ if and only if $\phi(x, y)$ is incident with $\phi[m, k]$.

Since by Lemma 2.3 planes coordinatized by Hall quasifields in the same class are isomorphic, we now have a complete proof that all Hall planes of the same finite order are isomorphic.

References

[1] D. R. HUGHES, *Collineation groups of non-Desarguesian planes* (I). *The Hall Veblen-Wedderburn systems*, Amer. J. Math. **81** (1959), 921-938.

[2] D. R. HUGHES and F. C. PIPER, *Projective planes*, Springer, 1973.

[3] T. G. OSTROM, *A class of non-Desarguesian affine planes*, Trans. Amer. Math. Soc. **104** (1962), 483-487.

[4] G. PANELLA, *Le collineazioni nei piani di Marshall Hall*, Riv. Mat. Univ. Parma (2) **1** (1960), 171-184.

[5] G. PICKERT, *Projektive Ebenen*, Springer, 1955.

Die Zusammenfassung

Der gewöhnliche Beweis, dass alle Hall-Ebenen derselben endlichen Ordnung isomorph sind, hängt von dem von Ostrom eingeführten Begriff "derivation" ab. In dieser Arbeit geben wir einen direkte Beweis, in dem wir die explicite Isomorphismen zwischen den Ebenen beschreiben.

* * *