WILLIAM M. KANTOR

PROJECTIVE PLANES OF TYPE I-4*

1. Introduction

During the last few years, there has been a mild surge of interest in projective planes of type I-4. This paper is intended to both provide a survey of some recent theorems, and to present some new results concerning these planes.

In Section 2, we describe the algebraic setting for these planes. Special attention is given to the structure of the relevant homology groups. In Section 3, some recent existence theorems are stated. Sections 4 and 5 are concerned with the most basic open question concerning these planes: the existence problem in the finite case. Both structural and numerical properties are studied in some detail. This is probably the most fascinating aspect of these planes, involving the interplay of geometric, algebraic, and difference set methods.

Finally, in Section 6, we discuss the related problem of planes of type I-3. A technique is described which gives a minuscule amount of new information concerning finite planes of that type. There is some hope that this approach will turn out to be useful in the study of planes of type I-3 or I-4.

Our notation and terminology will generally be that of Dembowski [4].

2. Neofields

Let $\mathscr{P}$ be a projective plane of type I-4 which is (U, OV)-, (V, OU)-, and (O, UV)-transitive. Coordinatizing as usual – with $(1, 1)$ any point not on OU, OV, or UV – yields a planar ternary ring (R, T) satisfying the following conditions.

(i) $T(m, x, c) = mx + c$ for all $m, x, c \in R$ (linearity).

(ii) $(R^*, \cdot)$ is a group, where $R^* = R - \{0\}$.

(iii) $(a+b)\,c = ac + bc$, $c(a+b) = ca + cb$ for all $a, b, c \in R$.

(iv) If $m, n, c, d \in R$ and $m \neq n$, then $mx + c = nx + d$ and $ym + c = yn + d$ have unique solutions x, y.

(v) If $a, b, c, d \in R$ and $a \neq c$, then the equations $xa + y = b$, $xc + y = d$, have a unique solution x, y.

We will call R a *neofield*. (This is not the usual terminology: Hughes [8]

* Supported in part by NSF Grant GP-37982-X.

introduced the term 'planar division neo-ring'. However, this seems unnecessarily cumbersome.) Conversely, each neofield coordinatizes a projective plane which is either of type I-4 or desarguesian.

If $0, 1 \in S \subseteq R$ and $(S, T \mid S)$ is a neofield, S is called a *subneofield* of R. Clearly, $(S, +)$ is a subloop of $(R, +)$ and $(S^*, \cdot)$ is a subgroup of $(R^*, \cdot)$. For brevity, S^* will always denote the group $(S^*, \cdot)$. Any intersection of subneofields is a subneofield.

Clearly, R is a skew field if $(R, +)$ is associative. $(R, +)$ is said to satisfy the left (right) inverse property if $x'+x=0$ implies $x'+(x+y)=0$ for all y(or $x+x'=0$ implies $(y+x)+x'=0$ for all y); $(R, +)$ has the inverse property if both of these conditions hold.

Let $\mathrm{Aut}\,R$ denote the automorphism group of the neofield R. If $\gamma \in \mathrm{Aut}\,R$ then $(x, y) \rightarrow (x^\gamma, y^\gamma)$ determines an automorphism of $\mathscr{P}$. Here $C_R(\gamma)$ is a subneofield of R.

(2.1) LEMMA. *Each inner automorphism of R^* determines an automorphism of R. Namely, if $r \in R^*$ then $x \rightarrow r^{-1}xr$, $x \in R$, is an automorphism. Its fixed neofield is $C_R(r) = \{0\} \cup C_{R^*}(r)$, where $C_{R^*}(r)$ is the centralizer of r in R^*.*

Proof. This follows immediately from distributivity.

(2.2) LEMMA. *If $\mathscr{H} \subseteq R$ then $C_R(\mathscr{H}) = \{r \in R \mid rx = xr$ for all $x \in \mathscr{H}\}$ is a subneofield.*

Proof. (2.1).

In particular, the *center* $Z(R) = C_R(R)$ of R is a subneofield.

The next results show that the group R^* must satisfy some relatively severe restrictions.

(2.3) THEOREM. *R^* has at most one involution.*

Proof. [7], II.3, or [12] and [15], or [4], p. 120.

(2.4) THEOREM. *If A is an Abelian normal subgroup of R^*, then $A \leqslant Z(R^*)$.*

Proof. (This is essentially the Cartan-Brauer-Hua Theorem; see [21], p. 427.) Suppose $A \nleqslant Z(R^*)$. Clearly $C_{R^*}(A) \trianglelefteq R^*$, while $C_R(A)$ is a subneofield by (2.2). Set $S = Z(C_R(A))$. Then S is a subneofield, S^* is Abelian, $A \leqslant S^* \trianglelefteq R^*$, and $S \nleqslant Z(R)$.

We can find $a \in S^*$ and $b \in R^*$ such that $bab^{-1}a^{-1} = u \neq 1$. Then $b \notin S$, as S^* is Abelian. Let $a(b+1) = v(b+1)\,a$. Then $u, v \in S$ as $S^* \trianglelefteq R^*$. Also, $ab + a = v(ba + a) = (vua)\,b + va$. Since a, vua, $va \in S$, if $a \neq vua$ then the equation $ax + a = (vua)\,x + va$ has exactly one solution $x \in R$ and x must be in S. Since $b \notin S$, we must have $a = vua$. But now $a = va$ also, so $v = 1$, and hence $u = 1$, which is not the case.

(2.5) THEOREM. *The center of $R^*/Z(R)^*$ is trivial.*
Proof. See the proof of [21], 14.2.4.

(2.6) THEOREM. (i) *If S is a proper subneofield of R, then* $|R^*:S^*|\geqslant|S|+1$.
(ii) *If $x\in R^*-Z(R^*)$, then* $|R^*:C_{R_*}(x)|\geqslant|C_R(x)|+1$.

For this and further results of these types see [21], (14.1.1), (14.1.2), (14.2.1), (14.2.2), and (14.3.1). None of the other proofs presented in [21], Chapter 14, seem to extend to the neofield case. Different types of results concerning subneofields of neofields are found in [8], Chapter II; for example, each abelian subgroup of R^* generates a subneofield with commutative multiplication.

Using (2.4), (2.5), or (2.6), it is easy to construct groups, each of whose nontrivial elements has infinite order (compare (2.3)), and yet which cannot be the multiplicative group of any neofield.

(2.7) THEOREM. *Suppose $(R, +)$ satisfies the inverse property.*
(i) *If* $1+(-1)=0$, *then* $(-1)+1=0$, $(-1)a=a(-1)$ *is the additive inverse of a for all $a\in R$, and* $(-1)^2=1$.
(ii) ([19]). *$(R, +)$ is commutative.*
(iii) If $a^2=1$ *then* $a=1$ or -1.
(iv) Let $a\neq 1$. *Then* $a+1=(-1)a^2$ *if and only if* $a^3=1$.

Proof. (i) Write $\varepsilon=-1$. $1+\varepsilon=0$ implies $1=1+(\varepsilon+1)$, so $\varepsilon+1=0$. Also, $a+\varepsilon a=0=a+a\varepsilon$, while $\varepsilon+\varepsilon^2=0$ implies $\varepsilon^2=1$.
(ii) Write $-a=\varepsilon a$. Then, for any a, $b\in R$, $-(a+b)+((a+b)+(-b))= =-b$, so $-(a+b)+a=-b$, or $-(a+b)=-b+(-a)$. Multiplying through by ε, we find $a+b=b+a$.
(iii) $a^2=1\neq a$ implies $a(a+1)=1+a=a+1$, so $a=-1$.
(iv) Suppose $\varepsilon a^2=a+1$. Then $\varepsilon a+\varepsilon a^2=1$ and $\varepsilon a^3=a^2+a=\varepsilon(\varepsilon a+\varepsilon a^2)=\varepsilon$, so $a^3=1$. Conversely, assume $a^3=1\neq a$. Write $u=a+1$ and $v=\varepsilon(a^2+1)$. The points (a, u) and $(v, \varepsilon a^2)$ are both on the lines $y=x+1$ and $y=a^2x+a$, since $a+1=u$, $v+1=\varepsilon a^2$, $a^2a+a=1+a=u$, and $a^2v+a=(\varepsilon a^4+\varepsilon a^2)+a= =(\varepsilon a^2+\varepsilon a)+a=\varepsilon a^2$. Since $a\neq 1$, we must have $(a, u)=(v, \varepsilon a^2)$, as required.
(v) Suppose $a^3=1\neq a$, $b^3=1\neq b$, $ab=ba$, and $a\neq b$. The points $(a^2, \varepsilon b^2)$ and $(b^2, \varepsilon a^2)$ are both on the lines $y=abx+1$ and $y=a^2b^2x+a^2b^2$; for example, $aba^2+1=b+1=\varepsilon b^2$ and $a^2b^2a^2+a^2b^2=a^2b^2(a^2+1)=a^2b^2\varepsilon a= =\varepsilon b^2$. Since $a^2\neq b^2$, we must have $ab=a^2b^2=1$.

Note that (2.7v) can fail if R^* is nonabelian.

3. Examples

The most elementary example of a neofield is as follows [14]. Let F denote any subfield of the real numbers. Choose $k\in R$ with $k\neq 1$, $k>0$, and define $(R, \oplus, \cdot)$ by: $R=F$, $a\cdot b=ab$, and

$$a\oplus b=\begin{cases} a+b & \text{if } ab\geqslant 0 \\ ka+b & \text{if } ab<0 \text{ and } |ka|\leqslant |b| \\ a+k^{-1}b & \text{if } ab<0 \text{ and } |ka|>|b|. \end{cases}$$

More generally, the same construction works for any ordered field F. Note that $R^*=F^*$. Also, $1\oplus(-1)=1-k^{-1}\neq 0$ if $k>1$, so here -1 is not the additive inverse of 1, even though (if F has characteristic $\neq 2$) -1 is the involution in R^*.

Another example using the real numbers is given in [20]. In that example, $(R, +)$ is commutative and has the inverse property.

While (2.3)–(2.5) restrict the possibilities for R^*, only (2.3) has any effect when R^* is Abelian. That this is the only restriction for infinite R is seen from the following basic existence theorem.

(3.1) THEOREM. *Let G be an infinite Abelian group having at most one involution. Then* [13] *there is a neofield R with $R^*\approx G$ such that* $1+1=0$. *There is also a neofield S with $S^*\approx G$ such that $(S, +)$ has the left, but not the right, inverse property* [1].

Special cases of (3.1) are found in [7] and [8].

Similarly, (2.7v) has the following converse in the infinite case.

(3.2) THEOREM ([1]). *Let G be an infinite Abelian group having at most one involution and at most one subgroup of order* 3. *Then there is a neofield R with $R^*\approx G$ such that $(R, +)$ has the inverse property.*

The preceding results contrast greatly with the situation for commutative yields. For, if $p\neq 2$ is prime, $x^p=1$ can hold for all $x\in R$.

4. Finite neofields: structure

The basic problem concerning finite neofields is whether they must be fields – if this were so, finite planes of type I-4 would not exist. The next two sections are concerned with structural and numerical properties of a finite neofield R. Let $|R|=n$.

(4.1) THEOREM ([8, 16]). *$(R, +)$ is commutative and has the inverse property.*

(4.2) COROLLARY. *If* $(-1)+1=0$, *then* $(-1)^2=1$. *Moreover,* $r^2=1$, $r\in R$, *implies* $r=1$ or -1.

Proof. (2.7).

(4.3) THEOREM ([11]). *R^* is an Abelian group.*

This is the analogue of Wedderburn's theorem. The next natural step would be to show that R^* is cyclic. All that is known in general is the following immediate consequence of (2.7) and (4.1)–(4.3).

(4.4) COROLLARY. *R^* has cyclic Sylow 2- and 3-subgroups.*

From (4.3) and [8], III.1, we get the following basic result.

(4.5) THEOREM. *Let $m \mid n$. Then the mapping $r \to r^m$, $r \in R$, is an automorphism of R.*

We will call an integer m a *multiplier* if $r \to r^m$, $r \in R$, is an automorphism of R. This terminology, together with the proof of (4.5) and (4.6), are due to the similarity between finite neofields and planar difference sets (cf. [3]; [4], pp. 89, 209; [8]). Thus, write $G = R^* \times R^*$, $D = \{(a, b) \in G \times G\ b = a+1\}$, $G_1 = 1 \times R^*$, $G_2 = R^* \times 1$, and $G_3 = \{(r, r) \mid r \in R^*\}$. Then $|D| = n-2$, and

$$(4.6) \qquad (\sum_{d \in D} d)(\sum_{d \in D} d^{-1}) = n + \sum_{g \in G} g - \sum_{g \in G} g - \sum_{g \in G_2} g - \sum_{g \in G_3} g$$

where the sums are taken in the rational group algebra QG of G.

(4.7) LEMMA. *If m is a multiplier, then $S = \{x \in R \mid x^m = x\}$ is the subneofield of R coordinatizing the subplane of $\mathscr{P}$ consisting of the fixed points and lines of the collineation induced by m.*

Proof. Clear.

(4.8) LEMMA. *Let t be a multiplier, $x \in R^*$, and suppose t induces an automorphism group of even order on $\langle x \rangle$. Then n is a square, and R has a subneofield of order $\sqrt{n}$. If, moreover, $x^t = x^{-1} \neq 1$, x, then $x^{\sqrt{n}} = x$* or *x^{-1}.*

Proof. Clearly t induces an automorphism τ of R of even order, so τ^i is a involution for some i. This proves the first assertion. By (4.7), $x^{t^i} = x^{\tau^i} = x^{\sqrt{n}}$, where $x^{t^i} = x$ or x^{-1} according to whether i is even or odd.

We next discuss some consequences of the preceding results. Let $\mathscr{P}$ be the plane coordinatized by R.

(4.9) LEMMA ([7]). *The mapping $\sigma: (x, y) \to (y, x)$ induces an involutory perspectivity of $\mathscr{P}$.*

Proof. If $y = mx + b$ with $m \neq 0$, then $y + (-b) = (mx + b) + (-b) = mx$ by (4.1), so $x = m^{-1}y + m^{-1}(-b)$. It follows readily that σ induces a collineation. Since $(x, x)^\sigma = (x, x)$, σ is a perspectivity.

(4.10) THEOREM. *Suppose $\mathscr{P}$ is nondesarguesian and Γ is its collineation group. Then $\Gamma=(GA)\times S$, where $S\approx S_3$, $A\approx \mathrm{Aut}\,R$, $G\approx R^*\times R^*$, $G\lhd\Gamma$, $GA\lhd\Gamma$, and $G\cap A=1$.*

Proof. By (4.9), there are involutory perspectivities σ and τ with $O^\sigma=O$, $U^\sigma=V$, $U^\tau=U$, $O^\tau=V$. Set $S=\langle\sigma,\tau\rangle$. Let A consist of the collineations $(x,y)\to(x^\alpha,y^\alpha)$ with $\alpha\in\mathrm{Aut}\,R$. Clearly, $A\approx\mathrm{Aut}\,R$.

As $\mathscr{P}$ has type I-4, Γ fixes $\{O, U, V\}$, and permutes these 3 points. Here GA is the kernel of this permutation representation (since G is transitive on the points on none of the lines OU, OV, UV). By (2.3), σ and τ centralize GA. Thus, $S\approx S_3$, and (4.10) follows.

(4.11) THEOREM. *Aut R has at most one involution.*

Proof. If $\alpha\in\mathrm{Aut}\,R$ is an involution, it induces a Baer involution on $\mathscr{P}$, so $|C_R(\alpha)|=\sqrt{n}$. By (4.5), $\beta:r\to r^{\sqrt{n}}$ is an involutory automorphism. Suppose $\alpha\neq\beta$. Clearly $\alpha\beta=\beta\alpha$, and $|C_R(\beta)|=|C_R(\alpha\beta)|=\sqrt{n}$. Let q be a prime dividing $\sqrt{n}+1$, and Q be the Sylow q-subgroup of R^*. If $q\neq 2$, then $\langle\alpha,\beta\rangle$ is fixed-point-free on Q, which is impossible. Thus, $q=2$ and $\sqrt{n}+1=2^i$ for some i. Now Q is cyclic by (4.4), and since $4\nmid\sqrt{n}-1$ we must have $|C_Q(\gamma)|=2$ for $\gamma=\alpha,\beta,\alpha\beta$. This is also impossible.

Beyond (4.1) and (4.2), very little is known about the loop $(R,+)$.

(4.12) LEMMA ([8], II, 11). (i) *If n is even then $1+1=0$ and* GF(2) *is a subneofield of R. Conversely, $1+1=0$ implies $2\mid n$.*

(ii) *If $3\mid n$ then $(1+1)+1=0$ and* GF(3) *is a subneofield of R. Conversely, $(1+1)+1=0$ implies $3\mid n$.*

(4.13) LEMMA. (i) *If n is even and $3\mid n-1$, then* GF(4) *is a subneofield of R, and n is a square.*

(ii) *If $3\mid n$ and $4\mid n-1$, then* GF(9) *is a subneofield of R, and n is a square.*

(iii) *If $5\mid n$ and $3\mid n-1$, then* GF(25) *is a subneofield of R, and n is a square.*

(iv) *If $7\mid n$ and $8\mid n-1$, then* GF(49) *is a subneofield of R, n is a square, and $48\mid n-1$.*

Proof. $m=2, 3, 5$, or 7 is a multiplier in the appropriate parts of the lemma. By hypothesis, there exists $x\in R^*$ satisfying $x^m=x^{-1}\neq\pm1$, so n is a square by (4.8). Note that m^2-1 has the form 2^i3^j. Thus, if S is defined for m^2 as in (4.7), then S^* is cyclic by (4.4), and hence $|S^*|\mid m^2-1$. This proves (i). As n is a square, $8\mid n-1$ in (ii), and hence $|S^*|=8=m-1$ there; that S is GF(9) follows, for example, from (5.12). The proofs of (iii) and (iv) are similar, also requiring the use of (5.9) and (5.12ii).

We leave to the reader the exercise of inventing variations on the theme of (4.13).

(4.14) LEMMA. *If m is a multiplier, then $(n-1, m-1)=1$ implies $1+1=0$, while $(n-1, m-1)=2$ implies $(1+1)+1=0$.*

Proof. Assume $1+1\neq 0$. Then $(1+1)^m=1+1$ implies $(1+1)^{m-1}=1$. Since $1+1\neq 1$, $(n-1, m-1)\neq 1$. If $(n-1, m-1)=2$, then $1=(1+1)^2=(1+1)+(1+1)$, so $1+1=1+(-1-1)=-1$ (by the inverse property), as required.

Note that the first parts of (4.12i, ii) are contained in (4.14), (with $m=2$ or 3). Arguments similar to that used in (4.14) will reappear in the next section.

A polarity θ of $\mathscr{P}$ is called *orthogonal* if it has exactly $n+1$ absolute points, and *unitary* if n is a square and each nonabsolute line has exactly $\sqrt{n}+1$ absolute points.

(4.15) THEOREM. *$\mathscr{P}$ has an orthogonal polarity. If n is a square, $\mathscr{P}$ also has a unitary polarity.*

Proof. Define θ by

$$\begin{aligned}(a, b)&\leftrightarrow y = ax - b\\ (m)&\leftrightarrow x = m\\ (\infty)&\leftrightarrow L_\infty .\end{aligned}$$

Then θ is an orthogonal polarity. Let n be a square, and let α be the Baer involution induced by the involutory automorphism of R. Then $\theta\alpha=\alpha\theta$ is a polarity, which is readily seen to be unitary by using [22].

5. Finite planes: numerical restrictions

Finite neofields are subject to numerous numerical restrictions, mostly derived from (4.5). Nevertheless, it is still not known whether the order n of R must be a prime power.

Let m denote any multiplier – in particular, m may be any divisor of n.

(5.1) THEOREM. *If $n>4$ is even, then $8 \mid n$.*

Proof. By (4.6), $\mathscr{P}$ has an involutory elation. Consequently, by [9], $4 \mid n$. Suppose $n\equiv 4 \pmod 8$. Then $2/(n-1)=-1$ by an elementary property of the Jacobi symbol ([5], p. 298). Thus, 2 is a non-residue mod q for some prime $q \mid n-1$. Consequently, the multiplier 2 has even order. By (4.8), n is a square, and there is a neofield of order $\sqrt{n}\equiv 2 \pmod 4$. Again by [9], this is impossible.

(5.2) LEMMA. *If n has a divisor m such that $(m+1, n-1)>2$, then n is a square.*

Proof. (4.8), using $2\neq |x| \mid (m+1, n-1)$.

(5.3) LEMMA. *If n is even, then $3 \mid n-1$ if and only if n is a square. In this case, R contains* GF(4).

Proof. If $n=s^2$, then $3 \nmid s$ by (4.12). Also, $s^2 \equiv -1 \pmod 3$ is impossible, so $s^2 \equiv 1 \pmod 3$. The remaining assertions follow from (4.13i).

(5.4) THEOREM. *If $(n-1, m-1)=1$ then n is even. If also $(n-1, m+1) \neq 1$, then $(n-1, m+1)=3$ and n is a square.*

Proof. The first assertion is just (4.14) and (4.12). Let $1 \neq |x| \mid (n-1, m+1)$. Then $(x+1)^m = x^m+1 = x^{-1}+1$, so $(x+1)^{m-1}=x^{-1}$. As $(n-1, m-1)=1$, $x+1 \in \langle x \rangle$, so $(x+1)^{m+1}=1$ also. Consequently, $1=x^{-1}(x+1)^2$, so $x= =(x^2+x)+(x+1)$. By (4.12i), $x^2+x=x+(x+1)=1$, so $x^3=1$ by (2.7). Now (4.4) implies that $(n-1, m+1)=3$, and (5.2) completes the proof.

(5.5) COROLLARY. *If n is even and $(n-1, 2^i+1)>3$, where $i \geqslant 1$, then $(n-1, 2^i-1) \neq 1$. Moreover, n is a square.*

Proof. Use $m=2^i$ in (5.4).

(5.6) COROLLARY. *Suppose n is even.* (i) *If $5 \mid n-1$ then $3 \mid n-1$ and n is a fourth power.* (ii) *If $9 \mid n-1$ then $7 \mid n-1$ and n is a square.*

Proof. For (i), use $2^i=4$ in (5.5), and then use (5.3). For (ii), use $2^i=8$ in (5.5).

(5.7) THEOREM. *Suppose $(n-1, m-1)=2<(n-1, m+1)$. Then $3 \mid n$, n is a square, and $(n-1, n+1)=4$. Moreover, $(1+1)+1=0$, and R contains* GF(9).

Proof. Take $x \neq -1$ with $x^{m+1}=1$. Then $(x+1)^m=x^m+1=x^{-1}+1$, so $(x+1)^{m-1}=x^{-1}$. Consequently, as $(n-1, m-1)=2$,

$$(x+1)^2 \in \langle x \rangle.$$

If $|x|$ is odd, then $(x+1)^{m+1}=1$, so $x=(x+1)^2$. Now $x=(x^2+x)+(x+1)$, so $-1=x+(-x-1)=x^2+x$. By (2.7), $x^3=1$, so by (4.12) and (4.14), $x=1$.

Thus, $(n-1, m+1)$ is a power of 2. Now suppose $2|x| \mid m+1$. Then $x^{(m+1)/2}=1$, so $(x+1)^{m+1}=1$, and the above argument yields $x=1$. That is, $x^{m+1}=1$ and $x \neq \pm 1$ imply $2|x| \nmid m+1$. Consequently, $8 \nmid m+1$, so $(n-1, m+1)=4$.

The remaining assertions follow from (4.13) and (4.14).

Let $\exp R^*$ denote the exponent of R^*.

(5.8) THEOREM. *Let m, m', m'', m''' be multipliers such that $m-m' \equiv \equiv m''-m''' \pmod{\exp R^*}$. Then $(m-m')(m-m'') \equiv 0 \pmod{\exp R^*}$.*

Proof. Let D be as in (4.6). Then D is fixed by each automorphism of R.

Let $d\in D$. Then $d^m d^{-m'}=dm'' d^{-m'''}$. By (4.6), $d^m=d^{m'}$ or $d^{m''}$. Thus, $d^{(m-m')(m-m'')}=1$. Since D generates $G=R^*\times R^*$ by (4.6), the result follows. The next result follows primarily from (5.8).

(5.9) THEOREM ([8], III.3). *n is not divisible by* $2\cdot 3$, $2\cdot 5$, $2\cdot 7$, $2\cdot 13$, $3\cdot 5$, $3\cdot 7$, $3\cdot 11$, $3\cdot 13$, $3\cdot 17$, $3\cdot 19$, $5\cdot 7$, *or* $5\cdot 11$.

Several of the preceding results are very reminiscent of analogous results concerning planar difference sets. We leave it to the reader to formulate more analogues of results presented in [3], Chapter IV. In particular, statements can be made concerning the orders of multipliers mod$p$ for odd prime divisors p of $n-1$. A different sort of result concerning orders is given by the following theorem.

(5.10) THEOREM ([17]). *Suppose $n\geqslant 8$, p is a prime divisor of n, and e is th exponent of p* (mod$n-1$). *Then R^* cannot be cyclic if $3\nmid e$ and either e is odd and $e>[(n-2)/6]$, or e is even and $e>2[(n-2)/6]$.*

Finally, yet another different type of restriction is provided by the following result.

(5.11) THEOREM ([10]). *If n is even and p is a prime dividing $n-1$, then there are integers x, y, z, not all* 0, *satisfying*

$$nx^2+(-1)^{(p-1)/2}py^2=z^2.$$

The most decisive known results concern planes of small order.

(5.12) THEOREM ([7], [18]). (i) *If $n\leqslant 1000$, then n is a prime power.*

(ii) *If* $n=9$, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32, 37, 41, 43, 47, 49, 64, 81, or 128, *then R is a field (and hence, no plane of order n and type* I-4 *can exist).*

6. Planes of type I-3

Let $\mathscr{P}$ be a projective plane of type at least I-3. Suppose $\mathscr{P}$ is (V, OU)- and (U, OV)-transitive. Then the corresponding planar ternary ring R is linear, R^* is a group, and $a(b+c)=ab+ac$ for all a, b, $c\in R$. Examples are provided by planar nearfields. A trivial but basic observation is the following fact.

(6.1) LEMMA. *If $\mathscr{P}$ has type* I-3, *then* $(R, +)$ *is not a group, and R^* is nonabelian.*

The first infinite examples of R with $\mathscr{P}$ of type I-3 were obtained by Yaqub [23], by replacing F in the first paragraph of Section 3 by a proper ordered planar nearfield. Recently, Bachmann [2] proved the following existence theorem.

(6.2) THEOREM. *Let G be an infinite nonabelian group. Assume:* (i) *G has at most one involution*; (ii) *for each $a \in G$, $|\{x \in G|\ x^2 = a\}| < |G|$; and* (iii) *for each $a \in G - Z(G)$, $|G : C_G(a)| = |G|$. Then there is a plane of type* I-3 *such that $R^* \approx G$.*

However, the precise determination has yet to be made of all infinite groups G such that $G \approx R^*$ for some R (as above) coordinatizing a plane of type I-3.

Most of the results of the preceding sections do not hold. However, (2.3) holds by [12] and [15], as does (5.10). Also, (4.6) still holds.

(6.3) THEOREM. *If R is finite, and $|R| = n$ is not a square, then R^* does not have a non-cyclic Abelian* 2*-group as a homomorphic image.*

Proof. Suppose R^* has a Klein group K as a homomorphic image. Then there is a homomorphism from QG onto QK (where $G = R^* \times R^*$ again). Apply this homomorphism to (4.6), solve the resulting system of 4 equations in 4 unknowns, and find that n is a square. (Alternatively, the resulting system can be interpreted as an integral matrix equation of the form $AA^t = B$, where det B is a square only when n is.) Unfortunately, this approach does not seem to work in other situations; we do, however, believe that some variation of it will imply both here and for neofields that R^* has no noncyclic elementary Abelian factor group, at least if n is not a square.

By (2.3), the Sylow 2-subgroups of a finite R^* must be cyclic or generalized quaternion. It follows that the noncyclic composition factors of R^* are known. (6.3) yields further restrictions on R^*. For example, if n is odd and not a square, and has noncyclic Sylow 2-subgroups, then $2 \mid n-1$. The following is a more straightforward consequence.

(6.4) COROLLARY. *If $n > 9$ then $n-1$ is not a power of* 2.

(5.11) still holds. Using this, (2.3), the noncommutativity of R^*, and the Bruck-Ryser theorem, Yaqub [24] has shown that most non-prime-powers $n \leqslant 100$ cannot be the orders of planes of type I-3. One of the difficulties in working with type I-3 (alluded to in [24] is that finite examples of planar ternary rings R exist satisfying the conclusions of (6.1), but coordinatizing nearfield planes).

7. Concluding remarks

The proofs of the following results are similar to those of (4.9) and (4.3).

(7.1) THEOREM. *Let A be a sharply transitive collineation group of a finite projective plane.* (i) *There is no Klein group of collineations normalizing A.*

(ii) *If A is Abelian, there is at most one involutory collineation normalizing A.*

(7.2) THEOREM. *Let R be a finite linear planar ternary ring with R^* a group. Suppose*

$$t^{-1}(a+b)\,t = (t^{-1}at) + (t^{-1}bt)$$

for all a, b, $t \in R^*$. Then R^* is Abelian.

Finally, we note that we have not mentioned topological projective planes of type I-4. These have been studied by K. H. Hoffman – see [6] for a survey. We mention one of his results.

(7.3) THEOREM ([6]). *Let R be a locally compact, not totally disconnected topological neofield. Then the multiplicative semigroup of R (i.e., $(R, \cdot)$), is algebraically and topologically isomorphic to the multiplicative semigroup of the field of real or complex numbers, or of the quaternions.*

The first example in Section 3 shows that R need not be isomorphic to one of the above fields. Other such examples are mentioned in [6], p. 63, in which the complex numbers arise as $(R, \cdot)$ in (7.3).

BIBLIOGRAPHY

1. Bachmann, O.: 'Planare Neokörper mit additiven Kürzungsregeln', *Math. Z.* **126** (1972), 6–30.
2. Bachmann, O.: 'Über projektiven Ebenen des Lenz-Barlotti-Typs I.3.' *Math. Z.* **130** (1973), 119–141.
3. Baumert, L. D.: 'Cyclic Difference Sets', *Lecture Notes in Math.* **182**, Springer, Berlin-Heidelberg-New York, 1961.
4. Dembowski, P.: *Finite Geometries*, Springer, Berlin-Heidelberg New York, 1968.
5. Heaslet, M. A. and Uspensky, J. V.: *Elementary Number Theory*, McGraw-Hill, New York, 1939.
6. Hofmann, K. H.: 'Über die topologische und algebraische Struktur topologischer Doppelloops und einiger topologischer projektiver Ebenen', *Algebraic and Topological Foundations of Geometry*, Pergamon, Oxford 1962, pp. 57–67.
7. Hughes, D. R.: 'Planar Division Neo-Rings', Ph.D. Thesis, University of Wisconsin, Madison, 1955.
8. Hughes, D. R.: 'Planar Division Neo-Rings', *Trans. Am. Math. Soc.* **80** (1955), 502–527.
9. Hughes, D. R.: 'Generalized Incidence Matrices over Group Algebras', *Ill. J. Math.* **1** (1957), 545–551.
10. Hughes, D. R.: 'Collineations and Generalized Incidence Matrices', *Trans. Am. Math. Soc.* **86** (1957), 286–296.
11. Kantor, W. M. and Pankin, M. D.: 'Commutativity in Finite Planes of Type I-4', *Arch. Math.* **23** (1972), 544–547.
12. Lüneburg, H.: 'Zur Frage der Existenz von endlichen Ebenen vom Lenz-Barlotti-Typ III-2', *J. reine angew. Math.* **220** (1965), 63–67.
13. Meschiari, M. and Quattrocchi, P.: 'Gruppi e cappi multiplicativi di annelli ternari lineari', *Annali di Mat. (IV)* **83** (1969), 235–252.
14. Naumann, H.: 'Stufen der Begründung der ebenen affinen Geometrie', *Math. Z.* **60** (1954), 120–141.
15. Ostrom, T. G.: 'Double Transitivity in Finite Projective Planes', *Can. J. Math.* **8** (1956), 563–567.
16. Paige, L. J.: 'Neofields', *Duke Math. J.* (1949), 39–60.

17. Pankin, M. D.: 'On Finite Projective Planes of Lenz-Barlotti Type I-4', Ph.D. Thesis, University of Illinois, Chicago, 1971.
18. Pankin, M. D.: 'Finite Planes of Type I-4?', *Proc. Intl. Conf. Proj. Planes*, Washington State Univ. Press 1973, pp. 215–218.
19. Pickert, G.: 'Projektive Ebenen über Neokörpern', *Wiss. Z. Friedr.-Schiller-Univ. Jena* **5** (1956), 131–135.
20. Salzmann, H.: 'Topologische projektive Ebenen', *Math. Z.* **67** (1957), 436–466.
21. Scott, W. R.: *Group Theory*, Prentice-Hall, New Jersey, 1964.
22. Seib, M.: 'Unitäre Polaritäten endlicher projektiver Ebenen', *Arch. Math.* **21** (1970), 103–122.
23. Yaqub, J. C. D. S.: 'The Existence of Projective Planes of Class I-3', *Arch. Math.* **12** (1961), 374–381.
24. Yaqub, J. C. D. S.: 'The Lenz-Barlotti Classification', *Proc. Proj. Geom. Conf.*, U. of Illinois, Chicago, 1967, pp. 129–160.
25. Yaqub, J. C. D. S.: 'Lenz-Barlotti Classification since 1968', *Proc. Intl. Conf. Proj. Planes*, Washington State Univ. Press 1973, pp. 281–287.

Author's address:
William M. Kantor,
University of Oregon,
Eugene,
Ore. 97403, U.S.A.

(Received February 2, 1974)