PLANAR DIVISION NEO-RINGS

BY

D. R. HUGHES

Introduction. The notion of a division ring can be generalized to give a system whose addition is not necessarily associative, but which retains the property of coordinatizing an affine plane. Such a system will be called a planar division neo-ring (PDNR); examples of (infinite) PDNRs which are not division rings are known.

If $(R, +, \cdot)$ is a finite power-associative PDNR, then $(R, +)$ is shown to be commutative and to possess the inverse property. The center of an arbitrary PDNR, and the nucleus of a finite PDNR, are shown to be PDNRs. By means of these and similar properties it is demonstrated that all associative PDNRs of order $\leqq 250$ are actually abelian.

The main result is the following: if $(R, +, \cdot)$ is a finite associative and commutative PDNR of order n, and if p is any prime dividing n, then the mapping $x \to x^p$ is an automorphism of $(R, +, \cdot)$. Chiefly by means of this result, all associative and commutative PDNRs of order $\leqq 250$ are shown to have prime-power order.

Chapter I contains results about the planar ternary rings developed by Marshall Hall [7], with a sketch of their connection with the complete sets of orthogonal latin squares associated with affine planes. Chapter II is devoted to strictly algebraic theory of PDNRs, mostly for the finite case. Chapter III contains the main theorem about automorphisms mentioned above, and examples of its application. In the Appendix will be found examples of infinite PDNRs which are not division rings.

These results are from the author's doctoral dissertation at the University of Wisconsin; the author wishes to take this opportunity to express his gratitude to Professor R. H. Bruck for invaluable assistance in carrying out this research.

CHAPTER I. PLANAR TERNARY RINGS AND LATIN SQUARES

1. **Introduction.** In [7] Hall has given the definition of algebraic systems, called planar ternary rings, which coordinatize (arbitrary) affine planes. In this chapter we develop some algebraic properties of finite planar ternary rings, and we investigate the connection between these rings and the complete sets of orthogonal latin squares associated with affine planes. Using a coordinatizing scheme similar to Hilbert's (see [10; 12]) we find a simple relation between the affine planes, the ternary rings, and the sets of squares.

Presented to the Society, April 22, 1955; received by the editors December 16, 1954 and, in revised form, March 18, 1955.

2. **Coordinatizing.** Given a projective plane Π of order n, let L_∞ be any (fixed) line of Π; L_∞ will be "the line at infinity." Let L_1 and L_2 be any other two distinct lines of Π, and let Y, X, and O be the points in common to L_∞ and L_1, L_∞ and L_2, L_1 and L_2, respectively. Let I be any fixed point on L_∞, I distinct from X and Y. Now let R be a set of symbols of cardinal n, and for the sake of simplicity, let us suppose that 0 (*zero*) and 1 (*one*, or the *identity*) are two distinct symbols of R. Let the point O be assigned the symbol 0, and let every other point of L_1, except Y, be assigned exactly one nonzero symbol from R.

For any point P on L_2, P distinct from X, consider the line IP; IP meets L_1 in exactly one point Q, and Q is not Y. If Q was assigned the symbol b from R, let P also be assigned the symbol b. Now if P' is an arbitrary point of Π, P' not on L_∞, consider the two lines XP' and YP'. Suppose YP' meets L_2 at the point which was assigned the symbol b, and suppose XP' meets L_1 at the point which was assigned the symbol c. Then let us name the point P' as (b, c).

Now for any point Q on L_∞, Q not Y, consider the line L through Q and $(1, 0)$. There exists a unique point $(0, m)$ on L_1 which is also on L; let Q be named (m). Let us name the point Y as (∞). (We are assuming that "∞" is not in R.)

The line L_1 is called the y-axis and the line L_2 is called the x-axis. If L is any line of Π not containing Y, let (m) be the intersection of L with L_∞, and let $(0, k)$ be the intersection of L with the y-axis. Then L will be named $[m, k]$. If L is not L_∞ and L contains Y, let $(k, 0)$ be the intersection of L with the x-axis; let L be named $[\infty, (k, 0)]$. The name for L_∞ will be simply L_∞.

It is fairly clear that we now have a one-to-one correspondence between the points and lines of Π and the various "names" given above. We shall freely employ customary terminology when speaking of the points and lines of Π: the point (b, c) has x-coordinate b and y-coordinate c; the line $[m, k]$ has slope m and y-intercept k; the line $[\infty, (k, 0)]$ has slope ∞ and x-intercept k.

Let $a, b, c \in R$; the point (b, c) has a unique line of slope a containing it, and suppose this line is $[a, k]$. Then we define $F(a, b, c) = k$; i.e., $F(a, b, c)$ is the y-intercept of the unique line of slope a which contains the point (b, c), and so F is a well-defined function.

A *ternary ring* (S, G) is defined to consist of a nonempty set S together with a *ternary operation* $G(a, b, c)$, defined for all $a, b, c \in S$, where $G(a, b, c)$ is a (unique) element of S. The *order* of (S, G), or of S, is the number of elements in S.

As in [7], it is easy to verify that (R, F) as defined above is a ternary ring satisfying:

(A) $F(a, 0, c) = F(0, b, c) = c$, for all $a, b, c \in R$;

(B) $F(a, 1, 0) = F(1, a, 0) = a$, for all $a \in R$;

(C) if $a, b, c, d \in R$, $a \neq c$, then there exists a unique $x \in R$ such that $F(x, a, b) = F(x, c, d)$;

(D) if $a, b, c \in R$, then there exists a unique $x \in R$ such that $F(a, b, x) = c$;

(E) if $a, b, c, d \in R$, $a \neq c$, then there exists a unique ordered pair $x, y \in R$ such that $F(a, x, y) = b$, $F(c, x, y) = d$.

It is of some interest that these axioms are the same as Hall's, even though different coordinatizing schemes were used. As in [7], the "converse" holds; if (R, F) is a ternary ring containing at least the two distinct elements 0 and 1, and if (R, F) satisfies (A)–(E), then (R, F) defines an affine (or projective) plane, in an obvious fashion.

We shall refer to a ternary ring with at least two distinct elements 0 and 1, which satisfies (A)–(E) as a *planar ternary ring.*

3. **Algebraic properties of planar ternary rings.** We prove some theorems about planar ternary rings which are independent of the coordinatizing scheme used.

THEOREM I.1. *If (R, F) is a finite ternary ring which satisfies* (D), *then (R, F) satisfies* (C) *if and only if it satisfies* (E).

Proof. Assume (C) and (D) hold, and let n be the order of R. Let a, b, c, d be fixed elements of R, where $a \neq c$. Consider the n^2 ordered pairs $(F(a, x, y), F(c, x, y))$, as x and y range over R. If the equation of (E) has no solution, then some ordered pair occurs at least twice among these pairs, since (b, d) does not occur; if there is more than one solution for (E), then (b, d) occurs at least twice among these pairs. So we shall be done if we can show that

$$F(a, x, y) = F(a, u, v), F(c, x, y) = F(c, u, v)$$

is impossible unless $x = u$, $y = v$.

Now if $x = u$, $y \neq v$, then $F(a, x, y) = F(a, x, v)$, which contradicts (D). So we can assume $x \neq u$. But then the equation $F(z, x, y) = F(z, u, v)$ has the two distinct solutions $z = a$, $z = c$, which contradicts (C). So (E) holds.

Now assume (D) and (E) hold in (R, F). Let a, b, c, d be fixed elements of R, $a \neq c$. For each $x \in R$ determine $xT \in R$ from $F(x, a, b) = F(x, c, xT)$; by (D) this is possible in exactly one way. If $x \neq y$ but $xT = yT$, then $F(x, a, b) = F(x, c, xT)$ and $F(y, a, b) = F(y, c, xT)$. Let $p = F(x, a, b)$, $q = F(y, a, b)$. Then the equations

$$F(x, u, v) = p, F(y, u, v) = q,$$

where $x \neq y$, have the solutions $u = a$, $v = b$, and $u = c$, $v = xT$; since $a \neq c$, this contradicts (E). So the mapping $x \to xT$ is one-to-one of R upon R, since R is finite. Hence $xT = d$ for exactly one $x \in R$; for this x, and only this x, we have $F(x, a, b) = F(x, c, d)$. So (C) holds, and the theorem is proven.

LEMMA I.1. *If (R, F) is a finite ternary ring satisfying* (D), *and if, for all*

$a, b, c, d \in R$, $a \neq c$, there exists at most one $x \in R$ such that $F(x, a, b) = F(x, c, d)$, then there exists exactly one such x.

Proof. Let a, b, c, d be fixed elements of R, $a \neq c$. For each $x \in R$, define $xT \in R$ by $F(x, a, b) = F(x, c, xT)$; by (D), this is possible in a unique way. If $x \neq y$, but $xT = yT$, then $F(x, a, b) = F(x, c, xT)$ and $F(y, a, b) = F(y, c, xT)$, and this contradicts the hypothesis of the lemma, since the equation $F(z, a, b) = F(z, c, xT)$ has at most one solution $z \in R$. Hence the mapping $x \to xT$ is one-to-one of R upon R, so there is a unique $x \in R$ such that $xT = d$, and for this x, $F(x, a, b) = F(x, c, d)$.

THEOREM I.2. *If S is a finite nonempty subset of the planar ternary ring (R, F), and if (S, F) is a ternary ring, then (S, F) is a planar ternary ring, or consists of the zero alone.*

Proof. Let a, b be fixed elements of S; the mapping $x \to F(a, b, x)$ is one-to-one of S upon S, since (R, F) satisfies (D) and S is finite. Thus (S, F) satisfies (D). Also, since S is a subset of a planar ternary ring, the hypotheses of Lemma I.1 are satisfied, so (S, F) satisfies the conclusion of Lemma I.1; this is (C).

If there is only one element $a \in S$, then $F(a, a, a) = a$. If $a \neq 0$, then in R the unique solution to the equation $F(x, a, a) = F(x, 0, a) = a$ is $x = 0$; this is a contradiction, so $a = 0$. If there are two distinct elements $a, b \in S$, consider the equation $F(x, a, c) = F(x, b, c)$, for an arbitrary $c \in S$; this equation has the unique solution $x = 0$, so $0 \in S$. The equation $F(x, a, 0) = F(x, 0, a)$, $a \neq 0$, has the unique solution $x = 1$, so $1 \in S$. Thus, in view of Theorem I.1, (S, F) is a planar ternary ring, and we are done.

Now if (R, F) is a planar ternary ring, let us define $a \cdot b$, or ab, as $F(a, b, 0)$; similarly, define $a + b$ as $F(1, a, b)$ (where a and b are arbitrary elements of R). Then the set R^* of nonzero elements of R forms a loop under the operation $(\cdot)$, with identity 1; the set R forms a loop under the operation $(+)$, with "identity" 0. We refer to these loops as the multiplicative loop $(R^*, \cdot)$ and the additive loop $(R, +)$. In general, $F(a, b, c)$ is not the same as $ab + c = F(1, F(a, b, 0), c)$ (see [7]). A planar ternary ring for which $F(a, b, c) = ab + c$ holds for all $a, b, c \in R$ will be called *linear*.

4. **Latin squares.** Given a complete set of orthogonal latin squares of order n, we can assume that the squares all use the symbols $0, 1, \cdots, n-1$, and that the set is in normal form: the top row of each square consists of the symbols $0, 1, \cdots, n-1$, in that order, from left to right, and one square of the set has the transpose of this common top row in its left column. In the row under the top row and in the left column, each square of the set has a different symbol, hence the squares can be conveniently named (1), (2), $\cdots$, $(n-1)$, according to the element in this position (the element 0 never occurs in this position). (See [1; 11; 14; 17] for proofs.)

We recall the well-known construction of an affine plane Π_1' from the set of orthogonal latin squares. For $u, v=0, 1, \cdots, n-1$, (u, v) is a point; for $u, v=0, 1, \cdots, n-1$, $[u, v]$ is a line; for $u=0, 1, \cdots, n-1$, $[\infty, (u, 0)]$ is a line. The point (u, v) is on $[x, y]$, $x\neq 0$, if y occurs in position (u, v) of square (x); (u, v) is on $[0, y]$ if $v=y$; (u, v) is on $[\infty, (x, 0)]$ if $u=x$. (Note that the upper leftmost position in a square is position (0, 0), etc.)

Let (R, F) be a planar ternary ring whose elements, besides 0 and 1, are taken as $2, 3, \cdots, n-1$, where n is the order of R. For each $x\in R^*$, let (x) be a square array with $F(x, u, v)$ in its (u, v) position.

The square (x) is latin. For in the uth row of (x), the elements are $F(x, u, z)$ and the equation $F(x, u, z)=b$ has exactly one solution for z, for any given $b\in R$. In the uth column of (x), the elements are $F(x, z, u)$, and since

$$F(x, z, y) = b, \qquad F(0, z, y) = u$$

has a unique solution for z and y, and since in fact, $y=u$, every element $b\in R$ occurs exactly once in this column.

If (u) and (v) are two squares, $u\neq v$, then (u) and (v) are orthogonal. For the equations

$$F(u, x, y) = a, \qquad F(v, x, y) = b$$

have exactly one solution x, y for a given pair $a, b\in R$, so there is exactly one position (x, y) such that a occurs in this position in (u) and b occurs in this position in (v).

Now suppose (R, F) is linear; i.e., $F(a, b, c)=F(1, F(a, b, 0), c)$, all $a, b, c\in R$. Then the square (u) has $F(u, v, w)=uv+w$ in its (v, w) position. Let us consider a fixed row in (u); i.e., the set of all elements $F(u, v, x)$, u and v fixed. Let $y=uv$; then the elements in row y of square (1) are the elements $F(1, y, x)=y+x=F(u, v, x)$, so row y of (1) is the same as row v of (u). Thus the rows of any square are the same as the rows of any other, but their position in the square is permuted.

Conversely, suppose the rows of (u), for any $u\in R^*$, are the same as the rows of (1), excepting that their position in the square is permuted; i.e., row v of (u) is row vT of (1). Then $F(u, v, w)=F(1, vT, w)$, all $w\in R$; in particular, $uv=F(u, v, 0)=F(1, vT, 0)=vT$. Then $F(u, v, w)=F(1, uv, w)=uv+w$; i.e., (R, F) is linear.

Under any circumstances, the square (1) is the Cayley table for the additive loop $(R, +)$; the array whose uth row is the transpose of the left column (the 0th column) of square (u) and whose 0th row consists of zeros is the Cayley table for $(R, \cdot)$ (not for $(R^*, \cdot)$).

Finally, suppose that we are given a complete set of orthogonal latin squares of order n; we assume that each square uses the symbols $0, 1, \cdots, n-1$, and that the set is in normal form. Furthermore, let us name the squares $(1), (2), \cdots, (n-1)$, as above. Let R be the set of elements $0, 1, \cdots, n-1$,

and define a ternary function $F(a, b, c)$ on R as follows: $F(0, b, c)=c$, all $b, c\in R$; if $a\neq 0$, then $F(a, b, c)$ is the element in position (b, c) of square (a). It is easy to verify that (R, F) is a planar ternary ring. Using the coordinatizing scheme of this paper, (R, F) defines an affine plane Π_2', and Π_2' is the same as the plane Π_1' defined above by the set of squares.

Chapter II. Planar division neo-rings

1. **Introduction.** In this chapter we shall examine those types of linear planar ternary rings which satisfy both distributive laws; our methods will be purely algebraic, in contradistinction to the somewhat "mixed" methods of Chapter III. Several results due to Paige [15] will be extended, and some new results obtained, preparatory to Chapter III.

2. **Algebraic properties.** We recall some definitions. If G is a loop, the set A of all elements $g\in G$ such that $g(xy)=(gx)y$, $x(gy)=(xg)y$, $x(yg)=(xy)g$ for all $x, y\in G$ forms an associative subloop of G, called the *nucleus* of G. The set Z of all elements of A which commute with every element of G is an abelian group, called the *center* of G. (For the necessary proofs, see [2].)

Let $(R, +, \cdot)$ be a nonempty set of elements with at least two distinct elements 0 and 1, and with two operations $(+)$ and $(\cdot)$ (where we often write xy for $x\cdot y$); let R^* denote the set of elements of R different from 0. Suppose $(R, +, \cdot)$ satisfies:

(i) $(R, +)$ is a loop with 0 as identity;

(ii) $(R^*, \cdot)$ is a loop with 1 as identity;

(iii) $0\cdot x=x\cdot 0=0$, for all $x\in R$;

(iv) $a(b+c)=ab+ac$, for all $a, b, c\in R$;

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

Then, following Bruck [5], we shall call $(R, +, \cdot)$ a *division neo-ring* (DNR). Unless otherwise stated, a qualifying adjective (commutative, associative, etc.) preceding the phrase "DNR" will mean that the multiplicative loop of the system has the particular property. The nucleus or the center of a DNR will be the subset of $(R^*, \cdot)$ with the designated property, plus the zero element. Furthermore, we shall use "abelian" to mean "commutative and associative."

A DNR is not, in general, a linear planar ternary ring, as Paige [15] has shown; in fact, there is an associative DNR of every finite order, and there is an infinite class of orders for which there is no planar ternary ring at all [6]. Clearly, a DNR $(R, +, \cdot)$ is a linear planar ternary ring (with $F(a, b, c)=ab+c$) if and only if:

(vi) $xa+b=xc+d$ has a unique solution x for all $a, b, c, d\in R$, $a\neq c$, and

(vii) $ax+y=b$, $cx+y=d$, has a unique solution x, y for all $a, b, c, d\in R$, $a\neq c$.

In view of Theorem I.1, if $(R, +, \cdot)$ is a finite DNR, either (vi) or (vii) alone is necessary and sufficient in order that $(R, +, \cdot)$ be planar. A DNR

which satisfies (vi) and (vii) will be called a *planar division neo-ring* (PDNR). See the Appendix for examples of PDNRs that are not divison rings.

The additive loop of a finite DNR is either an abelian p-group of type $(p, p, \cdots, p)$, or is a simple not-associative loop [3]. We now show that certain subsets of a DNR are themselves DNRs.

LEMMA II.1. *The nucleus of a DNR is an associative DNR.*

Proof. Let A be the nucleus of the DNR $(R, +, \cdot)$. Then $(A^*, \cdot)$ is a group. Let $a, b \in A$, $x, y \in R$. Then:

$$(xy)(a+b) = (xy)a + (xy)b = x(ya) + x(yb) = x(ya + yb)$$
$$= x[y(a+b)].$$

By similar computation with respect to the other two associative laws, we have $a+b \in A$. If $a+p=b$, then:

$$(xy)(a+p) = (xy)a + (xy)p = x(ya) + (xy)p$$

and also:

$$(xy)(a+p) = (xy)b = x(yb) = x[y(a+p)] = x(ya) + x(yp).$$

By comparison, we have $x(yp) = (xy)p$; by two other similar computations, we have $p \in A$. Similarly, if $q+a=b$, then $q \in A$. Thus $(A, +)$ is a loop, so $(A, +, \cdot)$ is a DNR.

LEMMA II.2. *The center of a DNR is an abelian DNR.*

Proof. Completely analogous to the proof of Lemma II.1.

THEOREM II.1. *Any finite sub-DNR of a PDNR is a PDNR.*

Proof. Immediate from Theorem I.2.

COROLLARY II.1. *The nucleus of a finite PDNR is a PDNR.*

COROLLARY II.2. *The center of a finite PDNR is a PDNR.*

But we can improve Corollary II.2.

THEOREM II.2. *The center of an arbitrary PDNR is a PDNR.*

Proof. Let $(R, +, \cdot)$ be a PDNR with center Z; we know that $(Z, +, \cdot)$ is a DNR. Let $a, b, c, d \in Z$, $a \neq c$, and let $ua+b = uc+d$; we shall show that $u \in Z$. Let y be an arbitrary element of R. Then:

$$(yu)a + yb = y(ua) + yb = y(ua + b) = y(uc + d) = y(uc) + yd$$
$$= (yu)c + yd,$$

and

$$(uy)a + yb = (ua)y + by = (ua + b)y = (uc + d)y = (uc)y + dy$$
$$= (uy)c + yd.$$

But the equation $za+yb=zc+yd$ has a unique solution $z\in R$, so $z=yu=uy$; i.e., u commutes with all of R.

Let $x, y\in R$; we shall demonstrate $(xu)y=x(uy)$, the other associative laws being similar. We have:

$$(xu)a + xb = x(ua) + xb = x(uc) + xd = (xu)c + xd,$$

and

$$(xu\cdot y)a + (xy)b = (xu\cdot a)y + (xb)y = (xu\cdot c)y + (xd)y = (xu\cdot y)c + (xy)d.$$

Similarly:

$$(uy)a + yb = (ua)y + by = (uc)y + dy = (uy)c + yd,$$

and

$$(x\cdot uy)a + (xy)b = x(uy\cdot a) + x(yb) = x(uy\cdot c) + x(yd) = (x\cdot uy)c + (xy)d.$$

By comparison, the unique solution z for the equation $za+(xy)b=zc+(xy)d$ is $z=(xu)y=x(uy)$. By two similar computations, we have $u\in Z$.

A completely analogous proof shows that the solution u, v of the equations $au+v=b$, $cu+v=d$, must be in the center. So $(Z, +, \cdot)$ is planar.

3. **Planar division neo-rings.** Paige has shown [15] that in a finite abelian DNR, the unique element e satisfying $e+1=0$ also satisfies $1+e=0$, and $e^2=1$. Since e must lie in the center of any DNR, the same result must hold in any finite DNR. We shall need the following results from [15], so we list them for reference purposes:

PAIGE'S THEOREM. *If $(R, +, \cdot)$ is a finite abelian PDNR, and $e\in R$ satisfies $e+1=0$, then:*

(i) *$x\in R$, $x^2=1$, implies that $x=1$ or $x=e$, so there is at most one element of multiplicative order two in R;*

(ii) *$(R, +)$ is commutative and has the inverse property (see [2] for the definition).*

Throughout this paper we shall use the symbol e for the element satisfying $e+1=0$; then $x+xe=xe+x=0$, for all $x\in R$, if R is finite. Next we prove a sequence of results which culminate in a strong extension of Paige's Theorem. First we note the following.

THEOREM II.3. *If $(R, +, \cdot)$ is an (arbitrary) associative PDNR, then R contains at most one element of multiplicative order two.*

Proof. Suppose, on the contrary, that $a\neq 1$, $b\neq 1$, $a\neq b$, $a^2=b^2=1$. There exists a unique pair $u, v\in R$ such that $u+v=1$, $bau+v=b$, and it is clear that $u\neq 0$, $v\neq 0$. Multiplying both of these equations by b, we have $bu+bv=b$, $au+bv=1$, or $ba\cdot au+bv=b$, $au+bv=1$.

Then the equations $x+y=1$, $ba\cdot x+y=b$ have solutions $x=u$, $y=v$, and $x=au$, $y=bv$; thus $a=b=1$, a contradiction.

Note that we do not prove that if an infinite abelian PDNR has a unique element x of order two, then $x+1=0$; in the Appendix will be found a counter-example.

THEOREM II.4. *Let $(R, +, \cdot)$ be a finite DNR, and let K be a subloop of $(R^*, \cdot)$; let K' be the subloop of $(R, +)$ generated by K. Then $(K', +, \cdot)$ is a DNR.*

Proof. Let T be the set of all $t \in K'$ such that $tk \in K'$ for all $k \in K$. Certainly $K \subseteq T$. If $t, t' \in T$, $k \in K$, then $(t+t')k = tk + t'k \in K'$, since $tk, t'k \in K'$. So $t+t' \in T$. Thus, since R is finite, $(T, +)$ is a loop, and $K \subseteq T \subseteq K'$, so $T = K'$.

Let S be the set of all $s \in K'$ such that $ks \in K'$ for all $k \in K'$; we have just shown that K is contained in S. If $s, s' \in S$, $k \in K'$, then $k(s+s') = ks + ks' \in K'$, since $ks, ks' \in K'$. So $s+s' \in S$, and $(S, +)$ is a loop; since $K \subseteq S \subseteq K'$, we have $S = K'$. I.e., K' is closed under multiplication, so $(K', +, \cdot)$ is a DNR.

THEOREM II.5. *Let $(R, +, \cdot)$ be a finite DNR, and let K be a subgroup of $(R^*, \cdot)$; then the DNR $(K', +, \cdot)$ generated by K is associative.*

Proof. The proof is quite similar to that of Theorem II.4. Let T be the set of all $t \in K'$ such that $t(ab) = (ta)b$ for all $a, b \in K$; certainly $K \subseteq T$. As above, we show that $(T, +)$ is a loop, whence $T = K'$, since K' is additively generated by K. Then we let S be the set of all $s \in K'$ such that $k(sa) = (ks)a$ for all $k \in K'$, all $a \in K$. Again, $S = K'$. Finally, let Q be the set of all $q \in K'$ such that $k(k'q) = (kk')q$ for all $k, k' \in K'$. We show $Q = K'$ and we are done.

THEOREM II.6. *Let $(R, +, \cdot)$ be a finite DNR, and let K be a commutative subloop of $(R^*, \cdot)$; let $(K', +, \cdot)$ be the DNR generated by K. Then $(K', +, \cdot)$ is commutative.*

Proof. Using the methods of the two previous theorems, the proof is quite straightforward.

COROLLARY II.3. *Let $(R, +, \cdot)$ be a finite DNR, let S be a subset of R, and let S' denote the set union of S and the zero element. Then if S is a maximal commutative subloop of $(R^*, \cdot)$, or a maximal associative subloop of $(R^*, \cdot)$, or a maximal abelian subloop of $(R^*, \cdot)$, then $(S', +, \cdot)$ is a DNR.*

Applying Theorems II.5 and II.6 with K as the identity subgroup of $(R^*, \cdot)$, we see that the element 1 additively generates an abelian DNR. As further corollaries, we have:

COROLLARY II.4. *Any multiplicatively power-associative element of a finite DNR is contained in an abelian sub-DNR.*

COROLLARY II.5. *Let G be a finite loop containing a maximal abelian subgroup H with a unique element f of order two, such that f is not in the center of G. Then G is not the multiplicative loop of any DNR.*

Proof. Suppose the contrary; i.e., G is the multiplicative loop of the finite DNR $(R, +, \cdot)$. Let S be the set union of H and the zero element; by Corollary II.3, $(S, +, \cdot)$ is an abelian DNR, so by a theorem due to Paige [15, Theorem II.2], $1+f=0$. But f is not in the center of R, while in $(R, +, \cdot)$, $1+e^{-1}=0$, where e is in the center. Thus $f \neq e^{-1}$, and this is a contradiction.

If we let the G of Corollary II.5 be a not-abelian group of order $2p$, p an odd prime, then H can be taken as any one of the Sylow 2-groups of G, thus satisfying the hypotheses of Corollary II.5, since the center of G is trivial. So G is not the multiplicative loop of any DNR. Paige obtained this result by different methods, and he also raised the question of the truth of the following:

COROLLARY II.6. *The symmetric group S_n on n symbols, $n>2$, is not the multiplicative loop of any DNR.*

Proof. If n is even, let $b=(1, 2, \cdots, n)$; if n is odd, let $b=(1, 2, \cdots, n-1)$. Then it is easy to show that the cyclic group H generated by b is maximal abelian in S_n and contains a unique element of order two. Since the center of S_n, $n>2$, is trivial, this proves the corollary.

LEMMA II.3. *If $(R, +, \cdot)$ is a DNR with commutative addition, then R contains at most one element of multiplicative order two.*

Proof. Let f be an element of multiplicative order two. Then:

$$(1+f)^2 = (1+f)+(1+f)f = (1+f)+(f+1) = (1+f)+(1+f) = (1+f)(1+1).$$

If $1+f \neq 0$, then $(1+f)^2=(1+f)(1+1)$ implies $1+f=1+1$, or $f=1$, a contradiction. So $1+f=0$, whence f is certainly unique. Furthermore, we see that if $1+1=0$, then there is no element of multiplicative order two.

THEOREM II.7. *If $(R, +, \cdot)$ is a finite PDNR, then R contains at most one element of multiplicative order two.*

Proof. Let f be an element of multiplicative order two; we shall show that $f+1=0$, whence f is certainly the only element of multiplicative order two in R.

Since $f^2=1$, f is power-associative, so the PDNR generated by f is abelian, by Corollary II.4; thus by Paige's Theorem, the PDNR generated by f has commutative addition. Hence by Lemma II.3, f is the unique element of order two in this sub-PDNR, so $f+1=0$.

COROLLARY II.7. *If $(R, +, \cdot)$ is a finite PDNR, and if T is a subgroup of $(R^*, \cdot)$ whose order is 2^k for some integer k, then either T is cyclic or T is a generalized quaternion group.*

Proof. Since T contains exactly one element of order two, it contains ex-

actly one subgroup of order two. Hence (see, for instance, [19, p. 118]) the corollary follows.

We recall that under the circumstances of Corollary II.7, T contains an element of order 2^{k-1}, hence contains an abelian subgroup of order 2^{k-1}.

THEOREM II.8. *If $(R, +, \cdot)$ is a finite power-associative PDNR, then $(R, +)$ is commutative and has the inverse property.*

Proof. Let a be an arbitrary element of R^*; the PDNR generated by a has commutative and inverse property addition, by Corollary II.4 and by Paige's Theorem; the element 1 is in this PDNR. So $1+a=a+1$, $(a+1)+e=a$, all $a\in R$. Multiplying these two equations on the left by an arbitrary element of R, we have the equations for commutative and inverse property addition between any two elements of R.

Let K be any subset of the DNR $(R, +, \cdot)$, and let $Z(K)$ be the subset of R consisting of all the elements of R which commute and associate with the elements of K. Let $A(K)$ be the subset of R consisting of all the elements of R which associate with the elements of K. Let $C(K)$ be the subset of R consisting of all the elements of R which commute with the elements of K.

THEOREM II.9. *Let K be a subset of the finite DNR $(R, +, \cdot)$ and let N be a subloop of $(R^*, \cdot)$ such that $N\subseteq Z(K)$ (or $N\subseteq A(K)$, or $N\subseteq C(K)$), and let $(N', +, \cdot)$ be the DNR generated by N. Then $N'\subseteq Z(K)$ (or $N'\subseteq A(K)$, or $N'\subseteq C(K)$).*

Proof. The proof is a straightforward application of the methods of Theorem II.4.

The next theorem will be needed in Chapter III, but we give it here since it is purely algebraic in proof.

THEOREM II.10. *If $(R, +, \cdot)$ is an associative DNR (not necessarily finite) then the equations $ax+b=cx+d$, all $a, b, c, d\in R$, $a\neq c$, have at most one solution for x if and only if the equations $xa+b=xc+d$, all $a, b, c, d\in R$, $a\neq c$, have at most one solution for x.*

Proof. Suppose the equations $xa+b=xc+d$, $a\neq c$, have at most one solution. Let us assume that $ax+b=cx+d=p$, $ay+b=cy+d=q$, where $a\neq c$; we wish to show that $x=y$.

If $a=0$, then $c\neq 0$, so $b=cx+d=cy+d$, and $x=y$. If $b=0$, then $ax=cx+d$, $ay=cy+d$; if $x=0$, then $d=0$, so $ay=cy$, whence $y=0=x$. So for $b=0$, we can assume $x\neq 0$ and similarly, $y\neq 0$. Then $a=c+dx^{-1}=c+dy^{-1}$, whence $x=y$ or $d=0$; but $d=0$ is impossible, since $a\neq c$.

So we can assume a, b, c, d all nonzero. If $p=q$, then $x=y$, so in particular, we can assume that at least one of p and q is nonzero; suppose $p\neq 0$. Then let $z=p^{-1}q$, whence:

$$axz + bz = pz = q = ay + b, \quad \text{and } cxz + dz = pz = q = cy + d.$$

If we multiply the second of these equations on the left by bd^{-1}, we have:

$$a(xz) + bz = ay + b, \quad \text{and} \quad (bd^{-1}c)(xz) + bz = (bd^{-1}c)y + b.$$

But the equation $v(xz)+bz=vy+b$ has at most one solution for v, if $xz \neq y$. So either $a=bd^{-1}c$ or $xz=y$.

If $xz=y$, then from $axz+bz=ay+b$, we have $bz=b$, so $z=1$, and $x=y$.

If $a=bd^{-1}c$, then from $ax+b=cx+d$ we have $bd^{-1}cx+b=cx+d$, or $(bd^{-1})(cx+d)=cx+d$, whence $bd^{-1}=1$, since $cx+d=p\neq 0$. Thus $b=d$, $ax=cx$, and $x=0$; similarly, $ay=cy$, so $y=0=x$.

Thus in all cases $x=y$. The other half of the proof is omitted, since it is completely similar.

We conclude this chapter with some results that help to classify PDNRs, but which are rather fragmentary. If $(R, +, \cdot)$ is a finite DNR of order n, with commutative addition, let us consider the Cayley table for addition. For each $b\in R$, b occurs n times in the table; if b occurs k times above the main diagonal, then it occurs k times below it, so b occurs $n-2k$ times on the main diagonal. If n is odd, then every element occurs at least once on the main diagonal, so it occurs exactly once on the main diagonal. Thus $1+1\neq 0$, for otherwise $b+b=0$, all $b\in R$, and then only 0 occurs on the main diagonal. If n is even, then $(R^*, \cdot)$ has odd order, so the center of $(R^*, \cdot)$ has odd order, hence possesses no element of order two; thus $1+1=0$. So a finite DNR with commutative addition has even order if and only if $1+1=0$. Note that for any finite DNR, even order implies $1+1=0$.

Now let $(R, +)$ have the inverse property, as well as being commutative. Consider all triples (a, b, c) of distinct nonzero elements of R which have the property $a+b=ce$, where $e+1=0$. Then, using the inverse property, $a+c=be$, $b+c=ae$. Given $a\in R^*$, b can be chosen as any element in R^*, excepting that $a(1+1)e\neq b$, $ae\neq b(1+1)$, $ae\neq b$, $a\neq b$; for otherwise we would have $c=a$, $c=b$, $c=0$, or $a=b$, respectively. Then c is uniquely determined by $c=(a+b)e$. Now if n is even, or equivalently, $e=1$, b must avoid only the value a, whence there are $(n-1)(n-2)/2$ pairs a, $b\in R$ that determine a triple. Each triple determines 3 pairs, so $(n-1)(n-2)$ must be divisible by 6. Using the fact that n is even, this is equivalent to $n\equiv 2 \pmod 6$, or $n\equiv 4 \pmod 6$.

If n is odd, but $e=1+1$, then b must avoid the two distinct values a and ae, so there are $(n-1)(n-3)/2$ pairs, whence as above, $(n-1)(n-3)\equiv 0 \pmod 6$. This yields $n\equiv 1 \pmod 6$, or $n\equiv 3 \pmod 6$.

If n is odd, and $e\neq 1+1$, then b must avoid the four distinct values $a(1+1)e$, $a(1+1)^{-1}e$, ae, and a. So there are $(n-1)(n-5)/2$ pairs, hence $(n-1)(n-5)\equiv 0 \pmod 6$, and $n\equiv 1 \pmod 6$, or $n\equiv 5 \pmod 6$.

We can summarize these results in the following:

THEOREM II.11. *If* $(R, +, \cdot)$ *is a finite DNR of order* n, *with commutative, inverse property addition, then* n *is never divisible by* 6; $n \equiv 2$ *or* 4 (mod 6) *if and only if* $1+1=0$; $n \equiv 3$ (mod 6) *implies* $e=1+1$; $n \equiv 5$ (mod 6) *implies* $e \neq 1$, $e \neq 1+1$.

If $(R, +, \cdot)$ is a DNR which contains no proper sub-DNR, then we shall say that $(R, +, \cdot)$ is a prime DNR; if R is finite, then R is additively generated by any one of its nonzero elements, and $(R^*, \cdot)$ is an abelian group. For an arbitrary finite DNR, define the characteristic of the DNR to be the order of the (clearly unique) prime DNR contained in it. For PDNRs, Theorem II.11 implies:

COROLLARY II.8. *If* $(R, +, \cdot)$ *is a finite power-associative PDNR of order* n, *then* $n \not\equiv 0$ (mod 6); R *has characteristic two if and only if* $n \equiv 2$ *or* 4 (mod 6); $n \equiv 3$ (mod 6) *implies that* R *has characteristic three*; $n \equiv 5$ (mod 6) *implies that* R *has characteristic greater than three.*

Suppose $(R, +, \cdot)$ is a finite PDNR of order n, and suppose R is not abelian. Let there be a PDNR $(S, +, \cdot)$ of order k contained in the center of R (e.g., the prime PDNR, or the center itself), and let there be a power-associative element $a \in R$, $a \notin S$ (e.g., R is power-associative). Then since S^* is contained in the center of $(R^*, \cdot)$, there is an abelian subgroup of $(R^*, \cdot)$ which contains S^* and a, hence there is an abelian PDNR $(T, +, \cdot)$ which properly contains S and is properly contained in R. Suppose T has order t; let Π_1, Π_2, and Π_3 be the projective planes associated with S, T, and R respectively. Then Π_3 properly contains Π_2, and Π_2 properly contains Π_1. Thus we know (see, for instance, [4]) that $k^2=t$, or $k^2+k \leqq t$, and $t^2=n$, or $t^2+t \leqq n$. Combining these, we have $k^4=n$, or $k^4+k^2 \leqq n$. Thus:

LEMMA II.4. *If* $(R, +, \cdot)$ *is a finite power-associative not-abelian PDNR of order* n, *and if* R *has characteristic* k, *then* $k^4=n$ *or* $k^4+k^2 \leqq n$.

THEOREM II.12. *If* $n=PQ+1$, *where* P *and* Q *are powers of distinct primes, both cube-free, then any associative PDNR of order* n *is abelian.*

Proof. Suppose $(R, +, \cdot)$ has order n, where $(R^*, \cdot)$ is a not-abelian group. Assume $P<Q$; there is an abelian subgroup of $(R^*, \cdot)$ of order Q, hence there is an abelian sub-PDNR of order m, where $n>m \geqq Q+1$. But $m^2 \geqq (Q+1)^2 = Q^2+2Q+1 > Q^2+1 > PQ+1 = n$. This is impossible.

CHAPTER III. DIFFERENCE SETS AND AUTOMORPHISMS

1. **Difference sets.** Unless explicitly stated to the contrary, $(R, +, \cdot)$ will be assumed to be an associative PDNR of finite order n throughout this chapter. Thus we know that if $e+1=0$, then $1+e=0$, $e^2=1$, and the only

elements of R which satisfy $x^2=1$ are 1 and e. Furthermore, $(R, +)$ is commutative and has the inverse property.

Let $\mathfrak{G}$ be the direct product group of $(R^*, \cdot)$ with itself, and let $\mathfrak{H}_i$, $i=1, 2, 3$, be respectively the subgroups of $\mathfrak{G}$ consisting of all elements $(1, a)$, $(a, 1)$, and (a, a). $\mathfrak{H}_1$ and $\mathfrak{H}_2$ are normal in $\mathfrak{G}$, and $\mathfrak{H}_i\mathfrak{H}_j=\mathfrak{G}$ if $i\neq j$. Let $\mathfrak{D}$ be the subset of $\mathfrak{G}$ consisting of all (a, b) such that $a+b=1$ in R.

Now we demonstrate the following:

(i) if $\mathfrak{g}\in\mathfrak{G}$, $\mathfrak{g}\notin\mathfrak{H}_i$ for any i, then $\mathfrak{g}$ can be represented in exactly one way as $\mathfrak{d}_1\mathfrak{d}_2^{-1}$, and in exactly one way as $\mathfrak{d}_3^{-1}\mathfrak{d}_4$, $\mathfrak{d}_i\in\mathfrak{D}$;

(ii) if $\mathfrak{h}\in\mathfrak{H}_i$ for some i, $\mathfrak{h}\neq(1, 1)$, then $\mathfrak{h}$ has no representation as $\mathfrak{d}_1\mathfrak{d}_2^{-1}$, and none as $\mathfrak{d}_3^{-1}\mathfrak{d}_4$, where $\mathfrak{d}_i\in\mathfrak{D}$.

For if $\mathfrak{d}_1$, $\mathfrak{d}_2\in\mathfrak{D}$, then $\mathfrak{d}_1=(x, 1+xe)$, $\mathfrak{d}_2=(y, 1+ye)$, where x and y are not 0 or 1. Then $(a, b)=\mathfrak{d}_1\mathfrak{d}_2^{-1}$ if and only if $a=xy^{-1}$, $b=(1+xe)(1+ye)^{-1}$; or $x=ay$, $b(1+ye)=1+aye$; or $x=ay$, $bye+b=aye+1$. But by Theorem II.10, $bye+b=aye+1$ has exactly one solution for y if $a\neq b$; so no element of $\mathfrak{H}_3$ is represented as $\mathfrak{d}_1\mathfrak{d}_2^{-1}$. If $b=1$, $a\neq1$, then the only solution is $y=0$, so $\mathfrak{d}_2$ is not in $\mathfrak{G}$; if $a=1$, $b\neq1$, then $b(ye+1)=ye+1$, so $ye+1=0$, whence $y=1$ and again $\mathfrak{d}_2$ is not in $\mathfrak{G}$. For all other values of a and b, $a\neq b$, there is exactly one y and x such that $(a, b)=(x, 1+xe)(y, 1+ye)^{-1}$. Similarly, all elements not in any $\mathfrak{H}_i$ have exactly one representation $\mathfrak{d}_1^{-1}\mathfrak{d}_2$, $\mathfrak{d}_1$, $\mathfrak{d}_2\in\mathfrak{D}$.

Thus $(\mathfrak{G}, \mathfrak{D})$ is a system similar to the *difference sets* of [4, 9](1).

There are $n-2$ elements in $\mathfrak{D}$, and the $(n-2)^2$ products $\mathfrak{d}_1\mathfrak{d}_2^{-1}$ will represent the identity $(1, 1)$ exactly $n-2$ times.

Now if $\mathfrak{d}_1$, $\mathfrak{d}_2\in\mathfrak{D}$, and if $\mathfrak{H}_i\mathfrak{d}_1=\mathfrak{H}_i\mathfrak{d}_2$ for some i, then $\mathfrak{d}_1=\mathfrak{h}\mathfrak{d}_2$, $\mathfrak{h}\in\mathfrak{H}_i$, so $\mathfrak{h}=\mathfrak{d}_1\mathfrak{d}_2^{-1}$, which implies $\mathfrak{h}=(1, 1)$ and thus $\mathfrak{d}_1=\mathfrak{d}_2$. So the $n-2$ cosets $\mathfrak{H}_i\mathfrak{d}$, as $\mathfrak{d}$ ranges over $\mathfrak{D}$, are distinct. Since $\mathfrak{H}_i$ has order $n-1$ and $\mathfrak{G}$ has order $(n-1)^2$, there is exactly one coset $\mathfrak{H}_i\mathfrak{t}_i$ not of the form $\mathfrak{H}_i\mathfrak{d}$. For $i=1, 2$, $\mathfrak{H}_i$ itself is this coset; i.e., we can assume $\mathfrak{t}_1=\mathfrak{t}_2=(1, 1)$.

If $\mathfrak{H}_3(1, e)$ were a coset $\mathfrak{H}_3\mathfrak{d}$, $\mathfrak{d}\in\mathfrak{D}$, then we would have $\mathfrak{d}=\mathfrak{h}(1, e)$, $\mathfrak{h}\in\mathfrak{H}_3$. If $\mathfrak{d}=(x, 1+xe)$, this yields $x=a$, $1+xe=ae=xe$, or $1=0$. This is impossible, so we can choose $\mathfrak{t}_3=(1, e)$.

2. **Existence of multipliers.** We shall be concerned with the group algebra A of $\mathfrak{G}$ over the field of rationals, and the congruence $a\equiv0 \pmod p$, where p is an integer, $a\in A$, will mean that the coefficients of the summands from $\mathfrak{G}$ occurring in a are integers which are congruent to zero, modulo p. Furthermore, we can identify the identity $(1, 1)$ of $\mathfrak{G}$ with the element 1 of the field of rationals. For another discussion of a very similar situation, see [4, 9]; the author owes much of his inspiration for the following result to the former paper, by R. H. Bruck.

Let us assume that $(R, +, \cdot)$ is abelian; then $\mathfrak{G}$ is abelian. Let $D=\sum\mathfrak{d}$, all $\mathfrak{d}\in\mathfrak{D}$, let $s=\sum\mathfrak{g}$, all $\mathfrak{g}\in\mathfrak{G}$, let $s_i=\sum\mathfrak{h}$, all $\mathfrak{h}\in\mathfrak{H}_i$, and let $s_0=s_1+s_2+s_3$.

(1) See the Appendix for the characterization corresponding to (i) and (ii) in the special case that $(R, +, \cdot)$ is infinite and abelian.

Then s_iD is the sum of all the elements of $\mathfrak{G}$ in cosets $\mathfrak{H}_i\mathfrak{d}$, $\mathfrak{d}\in\mathfrak{D}$, so $s_0D = 3s - \sum s_it_i$.

Define $f_1 = 3$, and $f_k = (n-2)f_{k-1} + 3(-1)^{k-1}$ for $k > 1$. We shall prove:

$$s_0D^k = f_ks + (-1)^k \sum s_it_i^k. \tag{1}$$

We have already shown (1) for $k = 1$; assume (1) holds for $k-1$. Then:

$$\begin{aligned} s_0D^k &= [f_{k-1}s + (-1)^{k-1} \sum s_it_i^{k-1}]D \\ &= (n-2)f_{k-1}s + (-1)^{k-1} \sum (t_i^{k-1}s_iD) \\ &= (n-2)f_{k-1}s + (-1)^{k-1} \sum (st_i^{k-1} - s_it_i^k) \\ &= (n-2)f_{k-1}s + (-1)^{k-1} \sum (s - s_it_i^k) \\ &= [(n-2)f_{k-1} + 3(-1)^{k-1}]s + (-1)^k \sum s_it_i^k \\ &= f_ks + (-1)^k \sum s_it_i^k. \end{aligned}$$

Thus we have proven (1).

Now let $g_k = (n-2)^k - f_k$; g_k can also be defined inductively: $g_1 = n-5$, $g_k = (n-2)g_{k-1} + 3(-1)^k$ for $k > 1$. Then

$(s - s_0)D^k = sD^k - s_0D^k = (n-2)^ks - s_0D^k = (n-2)^ks - f_ks - (-1)^k \sum s_it_i^k$, or:

$$(s - s_0)D^k = g_ks + (-1)^{k-1} \sum s_it_i^k. \tag{2}$$

Now if we reduce modulo n, we can write: $g_1 \equiv -5$, $g_2 \equiv 2(5) + 3$, $g_3 \equiv -[2^2(5) + 2(3) + 3]$, $g_4 \equiv 2^3(5) + 2^2(3) + 2(3) + 3$, all mod n, etc. Thus it is clear that:

$$\begin{aligned} g_k &\equiv (-1)^k[2^{k-1}(5) + 3(2^{k-2} + 2^{k-3} + \cdots + 1)] \pmod{n} \\ &\equiv (-1)^k[2^{k-1}(5) + 3(2^{k-1} - 1)] \pmod{n} \\ &\equiv (-1)^k(2^{k+2} - 3) \pmod{n}. \end{aligned}$$

Now let p be any prime which divides n; congruences modulo n certainly hold modulo p. So we write:

$$g_{p-1} \equiv (-1)^{p-1}(2^{p+1} - 3) \pmod{p}.$$

But $2^p \equiv 2 \pmod{p}$, so $2^{p+1} \equiv 4 \pmod{p}$; if p is odd, then $(-1)^{p-1} \equiv +1 \pmod{p}$, and if $p = 2$, then $(-1)^{p-1} \equiv -1 \equiv +1 \pmod{p}$. So if p is any prime divisor of n, we have:

$$g_{p-1} \equiv 1 \pmod{p}. \tag{3}$$

LEMMA III.1. *If s, s_0, D are defined as above, and if p is any prime divisor of n, then*

$$(s - s_0)D^{p-1} \equiv s - s_0 \pmod{p}. \tag{4}$$

Proof. From (2) and (3), $(s-s_0)D^{p-1} \equiv s+(-1)^p \sum s_i t_i^{p-1} \pmod{p}$. If p is odd, then $t_i^{p-1}=1$, all i; if $p=2$, then n is even, so $(R, +, \cdot)$ has characteristic two, and $t_i=1$, all i. So we have (4).

If p is any prime divisor of n, the mapping $x \to x\phi = x^p$ is an automorphism of $(R^*, \cdot)$, so the mapping $(x, y) \to (x, y)\phi = (x^p, y^p)$ is an automorphism of $\mathfrak{G}$. Let us denote the linear extension of ϕ to the group algebra A by the same symbol ϕ; furthermore, let us denote the linear extension to A of the automorphism $\mathfrak{g} \to \mathfrak{g}^{-1}$ of $\mathfrak{G}$ by $a \to a^*$. Then, by the definition of $\mathfrak{D}$, we have $D^* \cdot D = n + s - s_0$. Let $a = D^* \cdot D\phi - s$. Using the fact that $s_i\phi = s_i$ and $s_i s_j = s$ if $i \neq j$, we have:

$$
\begin{aligned}
s_0^2 &= s_1^2 + s_2^2 + s_3^2 + 2s_1s_2 + 2s_2s_3 + 2s_3s_1 = (n-1)s_0 + 6s, \\
a^* \cdot a &= (D^*\phi \cdot D - s)(D^* \cdot D\phi - s) \\
&= D^*\phi(D \cdot D^*)D\phi - 2(n - 2(^2s + (n-1)^2 s \\
&= (n + s - s_0)^2 - 2(n-2)^2 s + (n-1)^2 s \\
&= n^2 + 6s - (n+1)s_0 \\
&= (n - s_0)^2.
\end{aligned}
$$

Since $D\phi = \sum \mathfrak{d}^p$, $\mathfrak{d} \in \mathfrak{D}$, we have $D\phi \equiv D^p \pmod{p}$, and $D^* \cdot D\phi \equiv (D^* \cdot D)D^{p-1} \equiv (n+s-s_0)D^{p-1} \equiv (s-s_0)D^{p-1} \equiv s - s_0 \pmod{p}$, from (4), and since p divides n. So $a \equiv -s_0 \pmod{p}$, or $a = pC - s_0$, where C is an integral element of A.

If $\mathfrak{g} \in \mathfrak{G}$ occurs as a summand in C, with (integral) coefficient k, then since $D^* \cdot D\phi = pC + s - s_0$ has non-negative coefficients, we have:

(i) if $\mathfrak{g} \notin \mathfrak{H}_i$ for any i, then $pk+1 \geqq 0$, so $k \geqq 0$;

(ii) if $\mathfrak{g} \in \mathfrak{H}_i$ for some i, $\mathfrak{g} \neq (1, 1)$, then $pk+1-1 \geqq 0$, so $k \geqq 0$;

(iii) if $\mathfrak{g} = (1, 1)$, then $pk+1-3 = pk-2 \geqq 0$, so $k \geqq 1$.

Thus C has non-negative coefficients, and the coefficient of the identity is positive.

Again, $a = D^* \cdot D\phi - s = pC - s_0$; so $D^* \cdot D\phi = pC + (s - s_0)$. Also, we have $D^* \cdot D = n + (s - s_0)$; subtracting, we have $D^*(D\phi - D) = pC - n$, or:

$$D(D^*\phi - D^*) = pC^* - n. \tag{5}$$

Also, $D^*\phi \cdot D\phi = (D^* \cdot D)\phi = (n + s - s_0)\phi = n + s - s_0$, and this gives:

$$(D^*\phi - D^*)D\phi = n - pC. \tag{6}$$

LEMMA III.2. *If D and C are defined as above, then*

$$D\phi(pC^* - n) = D(n - pC). \tag{7}$$

Proof. Multiply (5) by $D\phi$, (6) by D, and equate the right sides.

Suppose $\mathfrak{g} \in \mathfrak{G}$ is a summand in C, $\mathfrak{g} \neq (1, 1)$, and the coefficient of $\mathfrak{g}$ is positive. The term $D\mathfrak{g}$ can contain at most one element of $\mathfrak{D}$, since $\mathfrak{g}$ is

represented at most one time as $\mathfrak{g}=\mathfrak{d}_1\mathfrak{d}_2^{-1}$ and hence $\mathfrak{d}_1=\mathfrak{g}\mathfrak{d}_2$ holds at most once. Thus the right side of (7) must contain at least $n-3$ distinct elements of $\mathfrak{G}$ with negative coefficients. If $\mathfrak{g}$ and $\mathfrak{h}$ are two distinct nonidentity elements of $\mathfrak{G}$, and if both occur in C with positive coefficients, then since $\mathfrak{d}_1\mathfrak{g}=\mathfrak{d}_2\mathfrak{h}$ holds for at most one pair $\mathfrak{d}_1, \mathfrak{d}_2\in\mathfrak{D}$, there are at least $2(n-3)-1=2n-7$ distinct elements on the right side of (7) with negative coefficients.

On the left side of (7), the only elements with negative coefficients are the elements of $D\phi$ (and perhaps not all of these). Thus the left side of (7) contains at most $n-2$ distinct elements with negative coefficients. So if two distinct nonidentity elements of $\mathfrak{G}$ occur in C with positive coefficients, we have $n-2\geqq 2n-7$, or $n\leqq 5$.

If $n\leqq 5$, then the PDNR is known to be a field, and we leave this case for the moment, and assume $n>5$. In this latter case, C can contain at most one nonidentity element of $\mathfrak{G}$ with a nonzero coefficient. Assume $C=q+k\mathfrak{g}$, where $\mathfrak{g}\neq(1, 1)$, $k>0$, and q is the coefficient of the identity. Then $a=pq+pk\mathfrak{g}-s_0$, and $a^*\cdot a=(n-s_0)^2=n^2-2ns_0+s_0^2=(pq+pk\mathfrak{g})(pq+pk\mathfrak{g}^{-1})-2pqs_0-pks_0(\mathfrak{g}+\mathfrak{g}^{-1})+s_0^2$, so:

$$p^2(q^2+k^2)+p^2qk(\mathfrak{g}+\mathfrak{g}^{-1})-2pqs_0-pks_0(\mathfrak{g}+\mathfrak{g}^{-1})=n^2-2ns_0. \tag{8}$$

The fourth term on the left of (8) contributes at least $n-1$ distinct elements of $\mathfrak{G}$, not in any $\mathfrak{H}_i$, with negative coefficients, while the first two terms on the left of (8) contribute at most two distinct nonidentity elements of $\mathfrak{G}$ with positive coefficients. Since no nonidentity element occurs on the right side of (8) with negative coefficient unless the element is in some $\mathfrak{H}_i$, we must have $2\geqq n-1$, or $n\leqq 3$; this contradicts our assumption that $n>5$. So $k\geqq 1$ is impossible, and therefore $C=q$, where $pq=n$.

Thus $a=n-s_0$, or $D^*\cdot D\phi=n+s-s_0=D^*\cdot D$; if we know that D^* is a nonsingular element of A, then we have:

$$D\phi=D. \tag{9}$$

In order to show the nonsingularity of D^*, it is sufficient to show the nonsingularity of $D^*\cdot D$; this in turn will be proven if we show that $D^*\cdot DQ$ is a rational number, for some $Q\in A$.

Let $Q=Bn+Cs+Es_0^2$, where B, C, and E are undetermined for the moment. Then:

$$D^*\cdot DQ=Bn^2+[Cn^2+(B-4C+3E)n+(4C-9E)]s+(E-Bn)s_0.$$

If we let $E=Bn$, $C=an+b$, $E=cn^2+dn+e$, where a, b, c, d, e are to be rational numbers, and demand that the coefficient of s above be zero, we have:

$$(a+3c)n^3+(-4a+b-8c+3d)n^2+(4a-4b-8d+3e)n+(4b-8e)=0.$$

This gives the set of equations:

$$
(10)\qquad \begin{aligned} a \quad &+ 3c \quad &&= 0,\\ -4a + b &- 8c + 3d \quad &&= 0,\\ 4a - 4b \quad &- 8d + 3e &&= 0,\\ 4b \quad &- 8e &&= 0. \end{aligned}
$$

(10) is a set of four equations in five unknowns, and has nonzero rational solutions. So Q can be determined such that $D^* \cdot DQ$ is a rational number, whence D^* is nonsingular. Therefore (9) holds, for $n > 5$.

Equation (9) is essentially the proof of the existence of *multipliers* (see [4, 9]).

3. **Automorphisms of an abelian planar division neo-ring.** The result of the previous section permits both an algebraic and a geometric interpretation, although the author has found it necessary to "mix" the two in order to get the best results. As a preliminary to the interpretation, we define an automorphism of a DNR $(R, +, \cdot)$ to be a one-to-one mapping ϕ of R upon R such that $(ab)\phi = a\phi \cdot b\phi$ and $(a+b)\phi = a\phi + b\phi$, all $a, b \in R$. Then:

THEOREM III.1. *If $(R, +, \cdot)$ is a finite abelian PDNR of order n, and if p is any prime dividing n, then the mapping $\phi: x \to x^p$ is an automorphism of $(R, +, \cdot)$.*

Proof. If $n \leqq 5$, then $(R, +, \cdot)$ is a field, since all projective planes of order less than eight are coordinatized only by fields; hence the theorem certainly holds if $n \leqq 5$. So we assume $n > 5$, in which case (9) of the previous section holds.

Since $(p, n-1) = 1$, ϕ is an automorphism of $(R^*, \cdot)$ and is one-to-one of R upon R. Now (9) is equivalent to $\mathfrak{D}\phi = \mathfrak{D}$, or: if $a+b=1$, then $a\phi + b\phi = 1$. Let $a, b \in R$, $a+b=c \neq 0$; then $c^{-1}a + c^{-1}b = 1$, so $(c^{-1}a)\phi + (c^{-1}b)\phi = 1$, or $(c\phi)^{-1}(a\phi) + (c\phi)^{-1}(b\phi) = 1$, or $a\phi + b\phi = c\phi = (a+b)\phi$. If $a+b=0$, then $b = ae$, and $a\phi + (ae)\phi = a\phi + (a\phi)(e\phi)$; since e is either 1, or is the unique element of order two, we must have $e\phi = e$. So $a\phi + (a\phi)(e\phi) = 0$. Thus ϕ is an automorphism of $(R, +)$, hence is an automorphism of $(R, +, \cdot)$.

Conversely, if ϕ is any automorphism of $(R, +, \cdot)$, then $\mathfrak{D}\phi = \mathfrak{D}$ is easy to prove, so (9) of the previous section holds for all values of n.

Now since a prime PDNR of finite order is additively generated by the element 1, every automorphism of a prime PDNR (of finite order) must fix every element. Let $(E, +, \cdot)$ be a prime PDNR of finite order n, and let p be any prime divisor of n. Suppose $q_1, q_2, \cdots, q_t$ are the distinct odd prime divisors of $n-1$, and suppose 2^k is the greatest power of two that divides $n-1$ (n is not even unless $n=2$). There are elements in E with multiplicative order q_i for each i, and there are elements of multiplicative order 2^k. Since the mapping $x \to x^p$ fixes every element of E, every nonzero element of E must satisfy $x^{p-1} = 1$; i.e., every q_i must divide $p-1$, and 2^k must divide $p-1$, for all primes p that divide n. This gives a condition on n which is satisfied by only two non-prime integers less than 50,000. These are:

$$n = 2501 = 41 \cdot 61, \qquad n - 1 = 2^2 \cdot 5^4,$$

$$n = 8749 = 13 \cdot 673, \qquad n - 1 = 2^2 \cdot 3^7.$$

So with the possible exception of 2501 and 8749, all prime PDNRs of order less than 50,000 have prime order(2). The author does not know if these two exceptional values are actually possible or not; note that if we knew that the multiplicative group of a prime PDNR was cyclic, then we could conclude that all prime PDNRs have prime order.

4. Nonexistence of certain abelian planar division neo-rings. Geometrically, the statement $\mathfrak{D}\phi = \mathfrak{D}$, in conjunction with (i) and (ii) of §III.1, enables us to decide that there is no abelian PDNR of many composite orders; this is essentially the "repeated difference" technique of Hall [9]. Together with certain algebraic implications of (9), these methods are strong enough to prove that all abelian PDNRs of order $\leqq 250$ actually have prime-power order, with the exception of the single value 74; by other methods, the author has been able to reject $n = 74$.

First we prove a theorem which helps to reject some values.

THEOREM III.2. *Let $(R, +, \cdot)$ be an abelian PDNR of order n, where $p_1, p_2, \cdots, p_r$ are the distinct prime divisors of n. Suppose $x^q = 1$ for all $x \in R^*$, where $q-1$ is an integer whose only distinct prime divisors are among the p_i, $i = 1, 2, \cdots, r$. Then n is 2, 3, or 4.*

Proof. The mapping $x \to x^{q-1}$ is an automorphism of $(R, +, \cdot)$, by Theorem III.1, and if $x \neq e$, $x \neq 0$, we have:

$$1 = (1 + x)^q = (1 + x)^{q-1}(1 + x) = (1 + x^{q-1})(1 + x) = (1 + x^{-1})(1 + x)$$
$$= (1 + x) + x^{-1}(1 + x) = (1 + x) + (1 + x^{-1}).$$

So $1 + x = 1 + e(1 + x^{-1}) = ex^{-1}$, for all x, $x \neq e$, $x \neq 0$. But if $x \neq e$, $x \neq 0$, then $ex^{-1} = 1 + x = x + 1 = x(1 + x^{-1}) = x(ex) = ex^2$. So $x^3 = 1$, all $x \in R^*$, $x \neq e$.

If $e \neq 1$, then let $x \in R^*$, $x \neq e$. We have $(xe)^3 = x^3e = e$, whence $(xe)^3 \neq 1$, so we must have $xe = e$, or $x = 1$. Thus 0, 1, e are the only elements of R, so $n = 3$.

If $e = 1$, and $n > 2$, let $a \in R^*$, $a \neq 1$; then $1 + a = a^2$. Hence a^2 is not 0, 1, or a. Let $b \in R^*$, $b \neq 1$, $b \neq a$. The equation $x + a = b(x + 1)$ has a unique solution $x \in R$. Since $b \neq a$, we have $x \neq 0$; since $b \neq 0$ and $a \neq 1$, we have $x \neq 1$, $x \neq a$. So $bx^2 = b(x + 1) = x + a = x(1 + ax^{-1}) = x(x^{-1}a)^2 = x^{-1}a^2$, or $a^2 = bx^3 = b$. Thus R^* has only the three elements 1, a, a^2. So if $n > 2$, we have $n = 4$.

THEOREM III.3. *There is no abelian PDNR whose order is divisible by any of the following pairs of primes*: (2, 3), (2, 5), (2, 7), (2, 13), (3, 5), (3, 7), (3, 11), (3, 13), (3, 17), (3, 19), (5, 7), (5, 11). *If an abelian PDNR has order divisible by any of the following pairs of primes, then $x^k = 1$ for all nonzero x in*

(2) Professor Lowell Paige has informed the author of the existence of two more such integers: $n = 236197 = 13 \cdot 18169$, $n - 1 = 2^2 \cdot 3^{10}$, and $n = 1562501 = 1201 \cdot 1301$, $n - 1 = 2^2 \cdot 5^8$.

the PDNR: (7, 13), $k=6$; (2, 11), (2, 29), $k=7$; (5, 13), $k=12$; (2, 17), (2, 19), (2, 31), $k=15$; (2, 23), $k=105$.

Proof. The proofs are all quite simple and depend upon finding a "repeated difference." For example:

(3, 11). If $\mathfrak{d}\in\mathfrak{D}$, then $\mathfrak{d}^3$, $\mathfrak{d}^9$, $\mathfrak{d}^{11}\in\mathfrak{D}$, and $\mathfrak{d}^{11}\mathfrak{d}^{-9}=\mathfrak{d}^3\mathfrak{d}^{-1}=\mathfrak{d}^2$, so $\mathfrak{d}^8=1$ all $\mathfrak{d}\in\mathfrak{D}$. Thus $x^8=1$, all nonzero x. But then the multiplicative group of the PDNR has order 2, 4, or 8 (see Corollary II.7), so the PDNR has order 3, 5, or 9, none of which are divisible by 11.

(5, 7). If $\mathfrak{d}\in\mathfrak{D}$, then $\mathfrak{d}^m\in\mathfrak{D}$, for $m=5$, 7, 25, 35, 49. Then $\mathfrak{d}^{49}\mathfrak{d}^{-25}=\mathfrak{d}^{25}\mathfrak{d}^{-1}=\mathfrak{d}^{24}$, so $\mathfrak{d}^{24}=1$, all $\mathfrak{d}\in\mathfrak{D}$. Then $\mathfrak{d}$, $\mathfrak{d}^5$, $\mathfrak{d}^7$, $\mathfrak{d}^{11}\in\mathfrak{D}$, and $\mathfrak{d}^{11}\mathfrak{d}^{-7}=\mathfrak{d}^5\mathfrak{d}^{-1}=\mathfrak{d}^4$, so $\mathfrak{d}^4=1$ or $\mathfrak{d}^{12}=1$, all $\mathfrak{d}\in\mathfrak{D}$. Hence $x^{36}=1$, all nonzero x in the PDNR. But $36-1=5\cdot 7$, and this is impossible by Theorem III.2.

Another technique which is used to reject non-prime-power orders is typified by $n=161$, $n-1=2^5\cdot 5$. There are no "repeated differences," but suppose $(R, +, \cdot)$ has order 161 and S is the subset of R consisting of all x which satisfy $x=x^{49}$. Since S consists of all the elements fixed by the automorphism $x\to x^{49}$, $(S, +, \cdot)$ is a sub-PDNR; if $x\neq 0$, then $x\in S$ if and only if $x^{16}=1$. The Sylow 2-group of $(R^*, \cdot)$ is cyclic, so S has order 17. But $17^2>161$, so no plane of order 161 contains a subplane of order 17.

The exceptional case $n=74$ could not be rejected by any method known to the author, excepting by a tedious computation of all "possible" sets $\mathfrak{D}$, and the discovery of a "repeated difference" for each.

5. **Nonexistence of certain associative planar division neo-rings.** The results of the preceding section are unsatisfactory in the sense that no general proof can be given that all finite abelian PDNRs have prime-power order. In view of cases like $n=74$ it appears that such a theorem, if true, could not be proven from the results of this chapter.

In a somewhat similar fashion, the next topic is also unsatisfactory. By a straightforward analysis, all associative PDNRs of order equal to or less than 250 can be shown actually to be abelian; but the author cannot find a method of supplying a general proof. Since any such proof would probably have to contain the classical Wedderburn theorem, the result, if true, probably lies fairly deep.

The techniques are all fairly simple. For instance, if $n\equiv 5 \pmod 6$, $n\neq 625$, $n<650$, then by Corollary II.8 and Lemma II.4 any associative (even power-associative) PDNR of order n is abelian. Also, we apply Theorem II.12, or we apply well-known results from group theory about the order of abelian subgroups, and use Theorem II.6.

Appendix

1. The author wishes to thank Mr. H. Naumann for an example of an infinite abelian PDNR which is not a division ring; his example is R_2 of the following. (See also [12].)

Let $(R, +, \cdot)$ be any field of real numbers, and let $r>1$ be any fixed element of R. Then define $R_r=(R, \oplus, \cdot)$ by $a\cdot b=ab$, and:

$$a\oplus b=\begin{cases} a+b & \text{if } ab\geqq 0,\\ a+rb & \text{if } ab\leqq 0, \text{ and } |a|\geqq |rb|,\\ a/r+b & \text{if } ab\leqq 0, \text{ and } |a|\leqq |rb|.\end{cases}$$

If we were to let $r=1$, then R_1 is merely the field R; if we allow $1>r>0$, then the resulting system R_r has addition which is anti-isomorphic to the addition in R_s, where $s=1/r$.

We shall not complete the proof that R_r is a PDNR, since it is straightforward, if somewhat long([3]). But we note that since $(-r)\oplus(1)=(1)\oplus(-1/r)=0$, $(R, \oplus)$ is not associative, not commutative, and does not possess the inverse property. Furthermore, R_r contains a unique element of multiplicative order two, and this element is not the additive "inverse" of 1, on either side. So the restriction to finiteness for many of the theorems of Chapter II cannot be removed.

We can also show that if R is any field of real numbers, if $r, s\in R$, $r\neq s$, $r>1$, $s>1$, then R_r and R_s are not isomorphic. For suppose that there exists an isomorphism T of R_r upon R_s. We may assume $r>s$. Then there is a rational number a such that $r^2>a>s^2$. Clearly $1T=1$, $0T=0$, so $(-r)T=-s$, $(r^2)T=s^2$. Since $nT=(1\oplus 1\oplus\cdots\oplus 1)T=n$ for any positive integer n, we have $bT=b$ for every positive rational. Moreover, in R_r we have $(r^2-a)\oplus a=a\oplus(r^2-a)=r^2$, and in R_s we have $[s(s^2-a)]\oplus a=a\oplus[(s^2-a)/s]=s^2$. By comparison, $(r^2-a)T=s(s^2-a)=(s^2-a)/s$. Since $s^2-a\neq 0$, this yields $s^2=1$, which is contradictory.

2. The following method allows the construction of a wide class of infinite abelian PDNRs.

Suppose B is an abelian group, e a fixed element of B, and suppose $\mathfrak{G}$ is the direct product group of B with itself. Let $\mathfrak{H}_i$, $i=1, 2, 3$, be respectively the subgroups of $\mathfrak{G}$ consisting of all elements $(1, x)$, $(x, 1)$, and (x, x), $x\in B$. Suppose $\mathfrak{D}$ is a subset of $\mathfrak{G}$, such that the following are satisfied:

(1) $\mathfrak{g}\in\mathfrak{G}$, $\mathfrak{g}\notin\mathfrak{H}_i$, for any i, implies $\mathfrak{g}=\mathfrak{d}_1\mathfrak{d}_2^{-1}$ for exactly one pair $\mathfrak{d}_1, \mathfrak{d}_2\in\mathfrak{D}$.

(2) $\mathfrak{g}\in\mathfrak{H}_i$ for some i, $\mathfrak{g}\neq(1, 1)$, implies $\mathfrak{g}\neq\mathfrak{d}_1\mathfrak{d}_2^{-1}$ for any $\mathfrak{d}_1$, $\mathfrak{d}_2\in\mathfrak{D}$.

(3) For every $a\in B$, $a\neq 1$, there is exactly one $b\in B$ and exactly one $c\in B$ such that $(a, b)\in\mathfrak{D}$, $(c, a)\in\mathfrak{D}$; no element $(1, x)$ or $(x, 1)$ is in $\mathfrak{D}$.

(4) $(be, b)\notin\mathfrak{D}$, all $b\in B$.

(5) If $a\neq be$, then $(a, b)\in(c, c)\mathfrak{D}$ for exactly one $c\in B$.

We have shown in Chapter III that if B is the multiplicative group of an abelian PDNR $(R, +, \cdot)$, and if $\mathfrak{D}$ is the subset of $\mathfrak{G}$ consisting of all elements

([3]) The author's doctoral dissertation contains an algebraic proof; in [12], Naumann refers to the existence of this example without specifically giving it, and states that a geometric proof can be given.

(a, b) such that $a+b=1$, then (1) and (2) are satisfied. It is quite easy to verify that (3), (4), and (5) are also satisfied.

Conversely, if (1)–(5) are satisfied, let R be the set union of B and a new element 0 (zero), and define $(R, +, \cdot)$ as follows: multiplication between non-zero elements of R is the same as in B; $0\cdot x=x\cdot 0=0$, all $x\in R$; $x+0=0+x=x$, all $x\in R$; $be+b=0$, all $b\in B$; $a+b=c$, if $a, b\in B$, $a\neq be$, where c is the unique element determined by $(a, b)\in(c, c)\mathfrak{D}$.

Then it is easy to show that $(R, +)$ is a loop and that both distributive laws hold, so $(R, +, \cdot)$ is an abelian DNR; we wish to show that it is a PDNR.

THEOREM. *Let $(R, +, \cdot)$ be an associative DNR in which:*

(i) *$xa+b=xc+d$ has a unique solution x for all $a, b, c, d\in R$, $a\neq c$;*

(ii) *$ax+b=cx+d$ has a unique solution x for all $a, b, c, d\in R$, $a\neq c$.*

Then $(R, +, \cdot)$ is a PDNR.

Proof. We must show that there is exactly one solution for $ax+y=b$, $cx+y=d$, all $a, b, c, d\in R$, $a\neq c$.

Suppose $a=0$. Then $y=b$, $cx+y=d$ uniquely determine x and y. So we can assume $a\neq 0$, and similarly $c\neq 0$.

Suppose $b=d$. Then we have $ax+y=cx+y$, so $ax=cx$; since $a\neq c$, this implies $x=0$, and thus $y=b$. Clearly x and y are unique.

Suppose $a^{-1}b=c^{-1}d$. Then $x+a^{-1}y=a^{-1}b=c^{-1}d=x+c^{-1}y$, so $a^{-1}y=c^{-1}y$, whence $y=0$, $x=a^{-1}b$ are the unique solutions.

We can assume then that $a\neq 0$, $c\neq 0$, $b\neq d$, and $a^{-1}b\neq c^{-1}d$. If $x=0$ is a solution, then $y=b=d$, and if $y=0$ is a solution, then $x=a^{-1}b=c^{-1}d$. Thus we can also assume $x\neq 0$, $y\neq 0$. Finally, at least one of b and d is not zero; say $b\neq 0$. Then $db^{-1}(ax+y)=d=cx+y$, or $db^{-1}ax+db^{-1}y=cx+y$.

Now suppose that $ax+y=au+v=b$ and $cx+y=cu+v=d$; i.e., a solution exists, but is not necessarily unique. As above, we also have $u\neq 0$, $v\neq 0$, and $db^{-1}au+db^{-1}v=cu+v$.

Thus $(db^{-1}a)(xy^{-1})+db^{-1}=c(xy^{-1})+1$, and $(db^{-1}a)(uv^{-1})+db^{-1}=c(uv^{-1})+1$. But from (ii) this implies that $db^{-1}a=c$ or $xy^{-1}=uv^{-1}$. But if $db^{-1}a=c$, and $d\neq 0$, then $a^{-1}b=c^{-1}d$, which is contradictory; if $d=0$, then $c=0$, which is also contradictory. So $xy^{-1}=uv^{-1}$. Then $a(xy^{-1})+1=by^{-1}$, and $a(uv^{-1})+1=bv^{-1}$, or $y=v$, and thus $x=u$. So the solution, if it exists, is unique.

For the existence, we can assume as above that $a\neq 0$, $c\neq 0$, $b\neq 0$, $a^{-1}b\neq c^{-1}d$, $b\neq d$, and $x\neq 0$, $y\neq 0$ for any possible solutions.

Since $db^{-1}a\neq c$, there is a unique solution z for $db^{-1}az+db^{-1}=cz+1$, and $z\neq 0$, since $b\neq d$.

If $cz+1=0$, then $db^{-1}(az+1)=0$, or $d=0$, since $az+1\neq cz+1=0$. Let $p=az+1\neq 0$, and let $x=zp^{-1}b$, $y=p^{-1}b$. Then $ax+y=azp^{-1}b+p^{-1}b=(az+1)p^{-1}b=b$, and $cx+y=czp^{-1}b+p^{-1}b=(cz+1)p^{-1}b=0=d$. Thus a solution exists in this case.

If $cz+1\neq 0$, then $db^{-1}(az+1)=cz+1$; we have $d\neq 0$, $az+1\neq 0$. Let

$p=cz+1$, $x=zp^{-1}d$, $y=p^{-1}d$. Then $ax+y=azp^{-1}d+p^{-1}d=(az+1)p^{-1}d$ $=[bd^{-1}(cz+1)]p^{-1}d=b$; $cx+y=czp^{-1}d+p^{-1}d=(cz+1)p^{-1}d=d$. Hence in all cases a solution exists, and the theorem is proven.

In view of the above, it is only necessary to show there is a unique solution x for the equations $xa+b=xc+d$, $a\neq c$. If any one of a, b, c, d is zero, then the solution exists and is unique, so we assume a, b, c, d all nonzero.

If $c^{-1}a=d^{-1}b$, then $x=ba^{-1}e=dc^{-1}e$ is a solution, and in fact, $xa+b$ $=xc+d=0$. Since $xa+b=xc+d$ is equivalent to $xd^{-1}ac^{-1}+c^{-1}d^{-1}b=xd^{-1}$ $+c^{-1}$, or to $(xd^{-1}+c^{-1})(ac^{-1})=xd^{-1}+c^{-1}$, or to $x=dc^{-1}e$, this must be the only solution.

Now suppose $b=d$. Then $xa=xc$ has only the solution $x=0$, since $a\neq c$.

Finally, we suppose $b\neq d$, $c^{-1}a\neq d^{-1}b$. Determine (f_1, f_2), $(f_3, f_4)\in\mathfrak{D}$ such that $(a^{-1}c,\ b^{-1}d)=(f_3, f_4)(f_1, f_2)^{-1}$. Then let $p=bf_2^{-1}=df_4^{-1}$, and let $x=pf_1a^{-1}$ $=pf_3c^{-1}$. It is easy to verify that $xa+b=xc+d$, and by a reversal of the above, x is unique.

Thus $(R, +, \cdot)$ is an abelian PDNR.

Now we wish to construct $\mathfrak{D}$ satisfying (1)–(5) for a given B. Let C be any countably infinite abelian group with at most one element of order two. (Then $x^2=b$ is satisfied for at most two values of x, for a given $b\in C$.) Let A either be the group of order one, or let A be the multiplicative group of a finite abelian PDNR $(S, +, \cdot)$; if A contains an element of order two, we demand that C contain no element of order two. Finally, let B be the direct product of A and C.

If A is the identity group, let $\mathfrak{D}_0$ be the empty subset of $\mathfrak{G}$; if A is the multiplicative group of $(S, +, \cdot)$, let $\mathfrak{D}_0$ be the subset of $\mathfrak{G}$ consisting of all elements (a, b), $a, b\in A$, such that $a+b=1$ in $(S, +, \cdot)$. If A is the identity group, let e be any fixed element of B, and if A is the multiplicative group of $(S, +, \cdot)$, let e be the element of A satisfying $e+1=0$ in $(S, +, \cdot)$.

Now we shall assume that $\mathfrak{D}'$ is a finite subset of $\mathfrak{G}$ satisfying (6), (7), and (8); note that $\mathfrak{D}_0$ satisfies these conditions.

(6) All the differences $\mathfrak{d}_1\mathfrak{d}_2^{-1}$, where $\mathfrak{d}_1$, $\mathfrak{d}_2\in\mathfrak{D}'$, are distinct, and none is in any $\mathfrak{H}_i$.

(7) All the differences $f_1f_2^{-1}$, $(f_1, f_2)\in\mathfrak{D}'$, are distinct, and none is equal to e.

(8) $(f_1, f_2)\in\mathfrak{D}'$ implies that neither f_1 nor f_2 is 1.

Now suppose that $\mathfrak{q}=(a, b)$ is an element of $\mathfrak{G}$, not in any $\mathfrak{H}_i$, which is not equal to any of the quantities $\mathfrak{d}_1\mathfrak{d}_2^{-1}$, where $\mathfrak{d}_1$, $\mathfrak{d}_2\in\mathfrak{D}'$. Note that $\mathfrak{q}^2=1$ implies $a, b\in A$ or $\mathfrak{q}\in\mathfrak{H}_i$ for some i; so $\mathfrak{q}^2\neq 1$. We shall construct a set $\mathfrak{D}''$ which contains $\mathfrak{D}'$ and two more elements, such that $\mathfrak{D}''$ satisfies (6), (7), (8), and such that $\mathfrak{q}=\mathfrak{d}_1\mathfrak{d}_2^{-1}$ for some $\mathfrak{d}_1$, $\mathfrak{d}_2\in\mathfrak{D}''$.

For an arbitrary $\mathfrak{p}=(g, h)\in\mathfrak{G}$, consider the following elements:

(9) $\mathfrak{p}\mathfrak{d}^{-1}$, $\mathfrak{d}\mathfrak{p}^{-1}$, $\mathfrak{q}\mathfrak{p}\mathfrak{d}^{-1}$, $\mathfrak{d}\mathfrak{p}^{-1}\mathfrak{q}^{-1}$, $\mathfrak{q}$, $\mathfrak{q}^{-1}$, $\mathfrak{d}\mathfrak{d}_1^{-1}$, where $\mathfrak{d}$, $\mathfrak{d}_1\in\mathfrak{D}'$, $\mathfrak{d}\neq\mathfrak{d}_1$.

These elements are all distinct unless at least one of the following holds:

(10) $\mathfrak{p}^2=\mathfrak{d}\mathfrak{d}_1$, $\mathfrak{p}^2=\mathfrak{d}\mathfrak{d}_1\mathfrak{q}^{-1}$, $\mathfrak{p}=\mathfrak{d}\mathfrak{d}_1^{-1}\mathfrak{d}_2$, $\mathfrak{p}^2=\mathfrak{d}\mathfrak{d}_1\mathfrak{q}^{-2}$, $\mathfrak{p}=\mathfrak{d}\mathfrak{d}_1^{-1}\mathfrak{d}_2\mathfrak{q}^{-1}$, $\mathfrak{p}=\mathfrak{d}\mathfrak{q}$, $\mathfrak{p}=\mathfrak{d}\mathfrak{q}^{-1}$,

$\mathfrak{p}=\mathfrak{d}$, $\mathfrak{p}=\mathfrak{d}\mathfrak{q}^{-2}$, $\mathfrak{q}=\mathfrak{q}^{-1}$, $\mathfrak{q}=\mathfrak{d}\mathfrak{d}_1^{-1}$; where $\mathfrak{d}$, $\mathfrak{d}_1$, $\mathfrak{d}_2\in\mathfrak{D}'$.
The last cannot occur by hypothesis, and $\mathfrak{q}=\mathfrak{q}^{-1}$ cannot occur since $\mathfrak{q}^2\neq 1$. The rest can only occur for finitely many values of $\mathfrak{p}\in\mathfrak{G}$.

An element of (9) is in some $\mathfrak{H}_i$ only if at least one of the following holds:

(11) $g=f_1$, $h=f_2$, $ag=f_1$, $bh=f_2$, $h^{-1}g=f_2^{-1}f_1$, $h^{-1}g=bf_2^{-1}f_1a^{-1}$; where $(f_1, f_2)\in\mathfrak{D}'$.

These equations are satisfied for only finitely many h, for a given g, and conversely.

Now if we demand that $\mathfrak{p}$ be so chosen that none of the equations of (10) or (11) are satisfied, and if, furthermore, we demand that $g\neq 1$, $h\neq 1$, $ag\neq 1$, $bh\neq 1$, $h^{-1}g\neq e$, $h^{-1}g\neq ba^{-1}e$, then we have infinitely many choices for $\mathfrak{p}$. If we choose such a $\mathfrak{p}$, and adjoin $\mathfrak{p}$ and $\mathfrak{q}\mathfrak{p}$ to $\mathfrak{D}'$, calling the new set $\mathfrak{D}''$, then $\mathfrak{D}''$ satisfies (6), (7), and (8). Furthermore, $\mathfrak{q}=\mathfrak{d}_1\mathfrak{d}_2^{-1}$ for a pair $\mathfrak{d}_1$, $\mathfrak{d}_2\in\mathfrak{D}''$.

Now suppose that $\mathfrak{D}'$ is finite and satisfies (6), (7), (8), and suppose a is an element of B such that $a\neq e$, $f_2^{-1}f_1\neq a$, for any $(f_1, f_2)\in\mathfrak{D}'$. For an arbitrary $\mathfrak{p}=(g, h)\in\mathfrak{D}$, consider the elements:

(12) $\mathfrak{p}\mathfrak{d}^{-1}$, $\mathfrak{d}\mathfrak{p}^{-1}$, $\mathfrak{d}\mathfrak{d}_1^{-1}$, where $\mathfrak{d}$, $\mathfrak{d}_1\in\mathfrak{D}'$, $\mathfrak{d}\neq\mathfrak{d}_1$.

As before, the elements of (12) are all distinct except for finitely many values of $\mathfrak{p}$. An element of (12) is in some $\mathfrak{H}_i$ only if at least one of the following holds:

(13) $g=f_1$, $h=f_2$, $h^{-1}g=f_2^{-1}f_1$, where $(f_1, f_2)\in\mathfrak{D}'$.

For a given g, this is possible for only finitely many h, and conversely.

Now if we demand that $\mathfrak{p}$ be so chosen that none of the equations of (13) are satisfied and so that none of the elements of (12) are identical, and if furthermore, we demand that $g\neq 1$, $h\neq 1$, then we can demand that $h^{-1}g=a$. Then if we adjoin such a $\mathfrak{p}$ to $\mathfrak{D}'$, and call the new set $\mathfrak{D}''$, then $\mathfrak{D}''$ satisfies (6), (7), and (8); also $a=f_2^{-1}f_1$ holds for an element $(f_1, f_2)\in\mathfrak{D}''$.

Now if a is an element of B, $a\neq 1$, and if a does not occur as a first component of an element of $\mathfrak{D}'$, where $\mathfrak{D}'$ is a finite set satisfying (6), (7), and (8), then we consider the following elements, where $\mathfrak{p}=(a, h)$, h an arbitrary element of B:

(14) $\mathfrak{p}\mathfrak{d}^{-1}$, $\mathfrak{d}\mathfrak{p}^{-1}$, $\mathfrak{d}\mathfrak{d}_1^{-1}$, where $\mathfrak{d}$, $\mathfrak{d}_1\in\mathfrak{D}'$, $\mathfrak{d}\neq\mathfrak{d}_1$.

Since h is not restricted, these elements are all distinct except for finitely many values of $\mathfrak{p}$.

If any element of (14) is in some $\mathfrak{H}_i$, then at least one of the following holds:

(15) $a=f_1$, $h=f_2$, $h^{-1}a=f_2^{-1}f_1$, where $(f_1, f_2)\in\mathfrak{D}'$.

The first of these is not true, by hypothesis, and the others are satisfied for only finitely many h.

So we shall demand that h be chosen so that $\mathfrak{p}$ is any one of the infinitely many elements such that the elements of (14) are distinct, such that the equations of (15) are not satisfied, and such that $h\neq 1$, $h^{-1}a\neq e$. Then we let $\mathfrak{D}''$ be the union of $\mathfrak{D}'$ and such a $\mathfrak{p}$; $\mathfrak{D}''$ satisfies (6), (7), and (8), and a occurs as a first component of (exactly) one element of $\mathfrak{D}''$.

We can repeat this last process, so that any preassigned non-identity element of B appears (exactly) once as a second component of an element of $\mathfrak{D}''$.

Hence we can extend a set $\mathfrak{D}'$ to a set $\mathfrak{D}'''$, so that a preassigned element of $\mathfrak{G}$, not in any $\mathfrak{H}_i$, occurs as a difference $\mathfrak{d}\mathfrak{d}_1^{-1}$, $\mathfrak{d}$, $\mathfrak{d}_1 \in \mathfrak{D}'''$; also so that a preassigned element of B, not e, occurs as a difference $f_2^{-1}f_1$, $(f_1, f_2) \in \mathfrak{D}'''$; and such that any preassigned nonidentity elements occur as first and second components in D'''.

Since both $\mathfrak{G}$ and B are countable, and can be well-ordered, it is clear that proceeding in this fashion we can construct $\mathfrak{D}$, the union of all the $\mathfrak{D}'$, so that (1)–(4) hold. To show that (5) holds, we note that $(a, b) = (c, c)(f_1, f_2)$, $(f_1, f_2) \in \mathfrak{D}$, if and only if $c = af_1^{-1} = bf_2^{-1}$, or $b^{-1}a = f_2^{-1}f_1$. But if $a \neq be$, then this last is satisfied for exactly one $(f_1, f_2) \in \mathfrak{D}$, and thus $c = af_1^{-1} = bf_2^{-1}$ is unique.

So B is the multiplicative group of an abelian PDNR $(R, +, \cdot)$. Since addition in the subset of R consisting of A and the zero is defined by $\mathfrak{D}_0$, in case A was the multiplicative group of a PDNR $(S, +, \cdot)$, it is clear that $(R, +, \cdot)$ contains a sub-PDNR isomorphic to $(S, +, \cdot)$.

If either $(S, +, \cdot)$ is not a field, or if we choose $\mathfrak{D}$ so that, for some $a, b \in B$, $(a, b) \in \mathfrak{D}$ but $(b, a) \notin \mathfrak{D}$, then $(R, +, \cdot)$ is not a field. It is clear by inspection of our process for construction of the $\mathfrak{D}'$ that we can always assure that $(R, +, \cdot)$ not be a field. If we take $(S, +, \cdot)$ to be the finite field $GF(p)$, then $(R, +, \cdot)$ has characteristic p.

Hence for a very wide class of infinite abelian groups B, there is an abelian PDNR which is not a field, and which has B as multiplicative group.

This method of constructing nontrivial PDNRs is a generalization of a method used by Hall [9] to construct infinite cyclic difference sets.

Bibliography

1. R. C. Bose, *On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-Latin squares*, Sankhyā vol. 3 (1938) pp. 328–338.

2. R. H. Bruck, *Contributions to the theory of loops*, Trans. Amer. Math. Soc. vol. 60 (1946) pp. 245–354.

3. ———, *Loops with transitive automorphism groups*, Pacific Journal of Mathematics vol. 1 (1951) pp. 481–483.

4. ———, *Difference sets in a finite group*, Trans. Amer. Math. Soc. vol. 78 (1955) pp. 464–481.

5. ———, *Analogues of the ring of rational integers*, Proc. Amer. Math. Soc. vol. 6 (1955) pp. 50–58.

6. R. H. Bruck and H. J. Ryser, *The non-existence of certain finite projective planes*, Canadian Journal of Mathematics vol. 1 (1949) pp. 88–93.

7. M. Hall, *Projective planes*, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 229–277.

8. ———, *Correction to "Projective planes,"* Trans. Amer. Math. Soc. vol. 65 (1949) pp. 473–474.

9. ———, *Cyclic projective planes*, Duke Math. J. vol. 14 (1947) pp. 1079–1090.

10. D. Hilbert, *The foundations of geometry*, Chicago, 1902.

11. H. B. Mann, *On orthogonal Latin squares*, Bull. Amer. Math. Soc. vol. 50 (1944) pp. 249–257.

12. H. Naumann, *Stufen der Begründung der ebenen affinen Geometrie*, Math. Zeit. vol. 60 (1954) pp. 120–141.

13. B. H. Neumann, *On the commutativity of addition*, J. London Math. Soc. vol. 15 (1940) pp. 203–208.

14. H. W. Norton, *The 7×7 squares*, Annals of Eugenics vol. 9 (1939) pp. 269–307.

15. L. Paige, *Neofields*, Duke Math. J. vol. 16 (1949) pp. 39–60.

16. K. Reidemeister, *Grundlagen der Geometrie*, Berlin, 1930.

17. W. L. Stevens, *The completely orthogonalised Latin squares*, Annals of Eugenics vol. 9 (1939) pp. 82–93.

18. O. Veblen and J. W. Young, *Projective geometry*, New York, 1910.

19. H. Zassenhaus, *The theory of groups*, New York, 1949.

THE UNIVERSITY OF WISCONSIN,
MADISON, WIS.