Lecture Notes in Mathematics 1535

Anthony B. Evans

Orthomorphism Graphs of Groups

Springer-Verlag

Preface

The study of orthomorphism graphs of groups has its origin in the use of orthomorphisms and complete mappings to construct mutually orthogonal sets of Latin squares. To help other mathematicians who wish to work in this area, a reference work is needed. None exists at present and work on the subject is scattered throughout the literature, often in a form that does not suggest any connection to orthomorphisms.

In writing this monograph I have tried to do more than survey work done so far. In this monograph I have attempted to consolidate known results and applications, to create a unified body of knowledge and to provide other mathematicians with the tools needed to work in this area. I have tried to lay down the beginnings of a framework for the theory of orthomorphism graphs of groups and their applications, incorporating topics from algebra and geometry into this theory. As one of the hopes for this project was that it would stimulate research in this area, I have suggested many problems and directions for future research in this field, which should provide algebraists and geometers as well as other researchers in combinatorics with questions to work on.

The material in this book should be accessible to any graduate student who has taken courses in group theory and field theory.

I would like to thank Wright State University for its support during the writing of this manuscript, part of which was written while on sabbatical, and my colleagues Manley Perkel, who worked with me in generating orthomorphisms using Cayley, and Terry McKee, who read part of the manuscript, and the referees for their helpful suggestions.

Chapter 1: Introduction.

Section 1. Definitions and elementary results.

If G is a finite group we shall call any mapping $G \rightarrow G$ that permutes the elements of G a *permutation* of G. For a finite group G, written multiplicatively with identity e, let θ be a permutation of G fixing e. Then θ is an *orthomorphism* of G if the mapping $x \rightarrow x^{-1}\theta(x)$ is a permutation of G, and a *complete mapping* of G if the mapping $x \rightarrow x\theta(x)$ is a permutation of G. Orthomorphisms and complete mappings are closely related as θ is an orthomorphism of G if and only if the mapping $x \rightarrow x^{-1}\theta(x)$ is a complete mapping of G and a complete mapping of G if and only if the mapping $x \rightarrow x\theta(x)$ is an orthomorphism of G.

Complete mappings were first defined and studied by Mann (1942) and the term orthomorphism was first used by Johnson, Dulmage and Mendelsohn (1961). While other terminologies have been used the most common alternative for orthomorphism has been orthogonal mapping, a term first used by Bose, Chakravarti, and Knuth (1960).

In this book we are concerned with mutually adjacent sets of orthomorphisms. These are used principally in the construction of mutually orthogonal Latin squares, nets, transversal designs, affine and projective planes, difference matrices, and generalized Hadamard matrices. Historically these are among the first applications found for orthomorphisms. Many applications of individual orthomorphisms have since been discovered. The intimate connection between neofields and near orthomorphisms (a generalization of orthomorphisms) will be described in section 4 of this chapter. For applications to the construction of triple systems, Mendelsohn designs, Room squares, and group sequencings, the interested reader should consult the papers in the reprint volumes edited by Hsu (1985 & 1987). These volumes also contain several papers dealing with neofields. Dénes and Keedwell's (1991) book on Latin squares also contains material on complete mappings, neofields, and group sequencings. One special type of orthomorphism deserves mention as it is the probably the most used in these constructions: A *starter* is an orthomorphism θ for which $\theta^{-1} = \theta$. A recent survey article by Dinitz and Stinson (to appear) contains much material on the use of starters in the construction of Room squares.

Let θ, ϕ: $G \rightarrow G$. Then θ is *adjacent* to ϕ, written $\theta \sim \phi$, if the mapping $x \rightarrow \theta(x)^{-1}\phi(x)$ is a permutation of G. Clearly $\theta \sim \phi$ if and only if $\phi \sim \theta$. Now θ: $G \rightarrow G$ is a permutation if adjacent to the mapping $x \rightarrow e$, and if $\theta(e) = e$ then θ is an orthomorphism if adjacent to the mappings $x \rightarrow e$ and $x \rightarrow x$, and a complete mapping if adjacent to the mappings $x \rightarrow e$ and $x \rightarrow x^{-1}$.

While we could have left out the condition that $\theta(e) = e$ in defining orthomorphisms and complete mappings, there is little to be gained by doing so. To see this, suppose that we do not require orthomorphisms to fix the identity and for each mapping θ: $G \rightarrow G$ and each

$a \in G$ we define the mapping θ_a: $G \to G$ by $\theta_a(x) = \theta(x)a$. Then it is easy to check that θ is an orthomorphism if and only θ_a is an orthomorphism, θ is a complete mapping if and only if θ_a is a complete mapping, θ is adjacent to ϕ if and only if θ_a is adjacent to ϕ_b, and θ_a cannot be adjacent to θ_b. A simple characterization of adjacency of permutations follows.

Theorem 1.1. Let θ and ϕ be permutations of G. Then θ is adjacent to ϕ if and only if the mapping $x \to x^{-1}\theta\phi^{-1}(x)$ is a permutation of G.

Proof. The mapping $x \to x^{-1}\theta\phi^{-1}(x)$ is a permutation of G if and only if the mapping $y = \phi^{-1}(x) \to x = \phi(y) \to \phi(y)^{-1}\theta(y)$ is a permutation of G if and only if θ is adjacent to ϕ. ∎

As an easy corollary we obtain a characterization of adjacency of orthomorphisms.

Corollary 1.1. Let θ and ϕ be orthomorphisms of G. Then θ is adjacent to ϕ if and only if $\theta\phi^{-1}$ is an orthomorphism of G.

The *orthomorphism graph* of G has as its vertex set the orthomorphisms of G, adjacency being defined as above. An *orthomorphism graph* of G is any induced subgraph of the orthomorphism graph of G. We shall use the symbol Orth(G) to denote both the set of orthomorphisms of G and the orthomorphism graph of G. Orthomorphism graphs were first studied by Johnson, Dulmage, and Mendelsohn (1961).

We shall borrow terminology from graph theory. In particular, if $\theta \in \mathcal{H}$, an orthomorphism graph of G, then the *degree* of θ in $\mathcal{H}$ is the number of orthomorphisms in $\mathcal{H}$ that are adjacent to θ. Any orthomorphism (in $\mathcal{H}$), adjacent to θ, will be called a *neighbor* of θ (in $\mathcal{H}$). The *degree* of an orthomorphism of G is its degree in Orth(G). An *r-clique* of an orthomorphism graph $\mathcal{H}$ of G is a set of r mutually adjacent orthomorphisms in $\mathcal{H}$. The *clique number* of $\mathcal{H}$, denoted $\omega(\mathcal{H})$, is the largest value of r for which $\mathcal{H}$ admits an r-clique.

Example 1.1. Let $\mathcal{P}(G) = \{\phi_r\colon \phi_r(x) = x^r, \phi_r \in \text{Orth}(G)\}$. Now ϕ_r is a permutation of G if and only if r is relatively prime to $|G|$. Hence $\phi_r \in \mathcal{P}(G)$ if and only if r and $r - 1$ are both relatively prime to $|G|$ and $\phi_r \sim \phi_s$ if and only if $r - s$ is relatively prime to $|G|$. Thus if p is the smallest prime divisor of $|G|$ then the set $\{\phi_i\colon i = 2, \dots, p - 1\}$ is a $(p - 2)$ - clique of $\mathcal{P}(G)$. Using the pigeonhole principle it is easy to prove that no larger clique of $\mathcal{P}(G)$ can be constructed and so $\omega(\mathcal{P}(G)) = p - 2$.

What is the value of $\omega(\text{Orth}(G))$? This question has been answered for very few classes of groups. One easily obtained upper bound is the following.

Theorem 1.2. If G is non-trivial then $\omega(\text{Orth}(G)) \leq |G| - 2$.

Proof. Let $\theta_1, \dots, \theta_r$ be an r-clique of Orth(G). If $a \neq e$ then $\theta_1(a), \dots, \theta_r(a)$ are all distinct and equal to neither e nor a. Hence $r \leq |G| - 2$. ▮

In view of this result we will define a *complete set of orthomorphisms of G* to be an ($|G|$ - 2) - clique of Orth(G). Does any group admit a complete set of orthomorphisms?

Example 1.2. Let G be an elementary abelian group. We may think of G as the additive group of a finite field. Then the mapping $x \rightarrow ax$ will be an orthomorphism of G if and only if $a \neq 0, 1$ and two such mappings $x \rightarrow ax$ and $x \rightarrow bx$ will be adjacent if and only if $a \neq b$. Thus the set $\{x \rightarrow ax\colon a \neq 0, 1\}$ is a complete set of orthomorphisms of G.

The elementary abelian groups are the only groups known to admit complete sets of orthomorphisms. Are there other groups that admit complete sets of orthomorphisms? In particular, are there groups of non-prime power order that admit complete sets of orthomorphisms? The latter question is important as it relates to the question of the existence of projective (equivalently affine) planes of non-prime power order. Such planes have long been conjectured not to exist.

We now give a direct product construction for orthomorphisms. This construction was given in difference matrix form by Jungnickel (1978). This yields lower bounds for the clique numbers of orthomorphism graphs. These bounds, though weak, are the best lower bounds presently available for many groups.

Theorem 1.3. Let $\theta \in$ Orth(G) and $\theta' \in$ Orth(G') and define $\theta \times \theta'\colon G \times G' \rightarrow G \times G'$ by $\theta \times \theta'(x, x') = (\theta(x), \theta'(x'))$. Then $\theta \times \theta' \in$ Orth($G \times G'$). Further, if $\theta, \phi \in$ Orth(G) and $\theta', \phi' \in$ Orth(G') then $\theta \times \theta'$ is adjacent to $\phi \times \phi'$ if and only if $\theta \sim \phi$ and $\theta' \sim \phi'$.
Proof. Routine calculation. ▮

The following are immediate corollaries.

Corollary 1.2. $\omega(\text{Orth}(G \times G')) \geq \text{Min}\{\omega(\text{Orth}(G)), \omega(\text{Orth}(G'))\}$.

Corollary 1.3. $\omega(\text{Orth}(G_1 \times \dots \times G_n)) \geq \text{Min}\{\omega(\text{Orth}(G_1)), \dots, \omega(\text{Orth}(G_n))\}$.

We shall consider two types of mappings Orth(G) → Orth(G) that are important in studying the structure of orthomorphism graphs. If θ is a permutation of G and T maps permutations of G into permutations of G then we shall use T[θ] to denote the image of θ under T. A bijection T: Orth(G) → Orth(G) is an *automorphism* of Orth(G) if T[θ] ~ T[ϕ] if and only if $\theta \sim \phi$ and a *congruence* of Orth(G) if the neighborhood of T[θ] is isomorphic to the neighborhood of θ. In general we cannot determine the full automorphism group or the full congruence group of Orth(G) without knowing completely the structure of Orth(G). We do however know some classes of automorphisms and congruences of orthomorphism graphs.

Let us define the following mappings from Orth(G) into Orth(G).

此为试读，需要完整PDF请访问：www.ertongbook.com

(i) H_α is defined by $H_\alpha[\theta] = \alpha\theta\alpha^{-1}$, $\alpha \in \mathrm{Aut}(G)$.

(ii) T_g is defined by $T_g[\theta](x) = \theta(xg)\theta(g)^{-1}$.

(iii) R is defined by $R[\theta](x) = x\theta(x^{-1})$.

(iv) I is defined by $I[\theta](x) = \theta^{-1}(x)$.

We will call H_α an *homology*, T_g a *translation*, R a *reflection*, and I an *inversion*. These mappings and their relations were described implicitly in Singer (1960), for cyclic groups. The definitions of translations, homologies, and inversions used here are those of Johnson, Dulmage, and Mendelsohn (1961), though they used different notation and terminology. Chang, Hsiang, and Tai (1964) defined reflections for non-abelian groups.

Theorem 1.4. H_α, T_g and R are automorphisms of $\mathrm{Orth}(G)$ and I is a congruence of $\mathrm{Orth}(G)$.

Proof. If θ is an orthomorphism of G then $H_\alpha[\theta]$, $T_g[\theta]$, $R[\theta]$, and $I[\theta]$ are all permutations fixing e. To show that these are also orthomorphisms of G we use $\eta(x)$ to denote $x^{-1}\theta(x)$ and note that $x^{-1}H_\alpha[\theta](x) = x^{-1}\alpha\theta\alpha^{-1}(x) = \alpha(\alpha^{-1}(x^{-1})\theta(\alpha^{-1}(x))) = \alpha\eta\alpha^{-1}(x)$, $x^{-1}T_g[\theta](x) = x^{-1}\theta(xg)\theta(g)^{-1} = g\eta(xg)\theta(g)^{-1}$, $x^{-1}R[\theta](x) = x^{-1}x\theta(x^{-1}) = \theta(x^{-1})$, and $x^{-1}I[\theta](x) = x^{-1}\theta^{-1}(x) = (\eta\theta^{-1}(x))^{-1}$. These are clearly permutations.

To show that H_α is an automorphism of $\mathrm{Orth}(G)$ note that, by Corollary 1.1, $H_\alpha[\theta] \sim H_\alpha[\phi]$ if and only if $\alpha\theta\alpha^{-1}(\alpha\phi\alpha^{-1})^{-1} = \alpha\theta\phi^{-1}\alpha^{-1}$ is an orthomorphism if and only if $\theta\phi^{-1}$ is an orthomorphism if and only if $\theta \sim \phi$. We shall use $\delta(x)$ to denote $\theta(x)^{-1}\phi(x)$. To show that T_g is an automorphism of $\mathrm{Orth}(G)$ note that $T_g[\theta](x)^{-1}T_g[\phi](x) = \theta(g)\delta(xg)\phi(g)^{-1}$, which is a permutation if and only if $\theta \sim \phi$. To show that R is an automorphism of $\mathrm{Orth}(G)$ note that $R[\theta](x)^{-1}R[\phi](x) = \theta(x^{-1})^{-1}x^{-1}x\phi(x^{-1}) = \delta(x^{-1})$, which is a permutation if and only if $\theta \sim \phi$.

To show that I is a congruence note that if $\phi_1, \dots, \phi_r$ are the neighbors of θ then, by Corollary 1.1, $\phi_1\theta^{-1}, \dots, \phi_r\theta^{-1}$ are orthomorphisms and are neighbors of θ^{-1} as $(\phi_i\theta^{-1})(\theta^{-1})^{-1} = \phi_i$ is an orthomorphism for $i = 1, \dots, r$. Further, as $(\phi_i\theta^{-1})(\phi_j\theta^{-1})^{-1} = \phi_i\phi_j^{-1}$, it follows that $\phi_i\theta^{-1} \sim \phi_j\theta^{-1}$ if and only if $\phi_i \sim \phi_j$. Thus the neighborhood of θ is isomorphic to an induced subgraph of the neighborhood of $I[\theta]$. Similarly the neighborhood of $I[\theta]$ is isomorphic to an induced subgraph of the neighborhood of θ, and so the neighborhood of θ is isomorphic to the neighborhood of $I[\theta]$. ▮

Note that in general I is not an automorphism of $\mathrm{Orth}(G)$. We list products of congruences in the next theorem.

Theorem 1.5.

(i) $H_\alpha H_\beta = H_{\alpha\beta}$.

(ii) $T_g T_h = T_{gh}$.

(iii) $R^2 = I^2 =$ identity.

(iv) $H_\alpha R = RH_\alpha$.
(v) $H_\alpha T_g = T_{\alpha(g)}H_\alpha$.
(vi) $T_gR = RT_{g^{-1}}H_\alpha$, where α is the inner automorphism $\alpha(x) = gxg^{-1}$.
(vii) $H_\alpha I = IH_\alpha$.
(viii) $(IR)^3$ = identity.
(ix) $T_gI[\theta] = IT_{\theta^{-1}(g)}[\theta]$

Proof. Routine calculations. ▮

Groups of congruences can be used to classify orthomorphisms and orthomorphism graphs. Some examples of this will be seen in later chapters. In particular, in Chapter 3 we will define and study the orthomorphism graphs $\mathcal{C}_e \subseteq \mathrm{Orth}(GF(q)^+)$. If $e \mid q - 1$ then let H be the unique subgroup of $GF(q)^*$ of order e and define $\mathbf{H}_e = \{H_\alpha\colon \alpha(x) = ax, a \in H\}$. Then an orthomorphism θ of $GF(q)^+$ is in $\mathcal{C}_e$ if and only if $H_\alpha[\theta] = \theta$ for all $H_\alpha \in \mathbf{H}_e$. Further, in chapter 4 we will study the orthomorphism graph $\mathcal{A}(G)$, consisting of those orthomorphisms of G that are also automorphisms of G. These are precisely the orthomorphisms of G for which $T_g[\theta] = \theta$ for all $g \in G$. In section 4 of this chapter we will show how congruences have been used to classify neofields.

In studying orthomorphism graphs, what type of questions should we be asking? Given a group G and an orthomorphism graph $\mathcal{H}$ of G, the problems that concern us are as follows.

i) Determine exact values of, or bounds for, $\omega(\mathcal{H})$.
ii) What can we say about the structure of $\mathcal{H}$?
iii) Can $\mathcal{H}$ contain a complete set of orthomorphisms?
iv) Given a clique of $\mathcal{H}$ can we extend it to a larger clique of $\mathcal{H}$ or Orth(G)?

While we are interested in the special case $\mathcal{H}$ = Orth(G), we have few tools available for treating this case. We have data only for small groups, which will be presented in Chapter 6, and this data is mainly the result of computer searches. Thus this case seems for the moment to be beyond us. We therefore restrict ourselves to finding interesting orthomorphism graphs for which these problems might be tractable.

Section 2. Latin squares and difference matrices.

In this section we will describe applications of cliques of orthomorphism graphs in the construction of mutually orthogonal Latin squares and maximal sets of mutually orthogonal Latin squares. We shall also describe the close relationship that exists between difference matrices and cliques of orthomorphism graphs, and between generalized Hadamard matrices and complete sets of orthomorphisms.

While the study of orthomorphism graphs and their structures is of intrinsic interest, the original impetus for their study arose from the desire to construct large sets of mutually orthogonal Latin squares. A *Latin square of order n* is an $n \times n$ matrix with entries from a symbol set of order n such that each symbol appears exactly once in each row and exactly once in each column.

Example 1.3. Let $g_1, \dots, g_n$ be the elements of a group of order n. Then the matrix with ijth. entry $g_i g_j$ is a Latin square, which we will refer to as the *Cayley table* of the group.

We say that two Latin squares L_1 and L_2, of the same order and on the same symbol set, are orthogonal if for any pair of symbols a, b there is a uniquely determined pair of integers i, j such that the ijth. entry of L_1 is a while the ijth. entry of L_2 is b. Essentially, if the two Latin squares are superimposed then each ordered pair of symbols will appear exactly once.

Example 1.4. Suppose that F is the finite field of order q. Let $0 = f_1, \dots, f_q$ be the elements of F. For $k = 2, \dots, q$ define a matrix L_k whose ijth. entry is $f_k f_j + f_i$. Then $L_2, \dots, L_q$ form a set of q - 1 mutually orthogonal Latin squares of order q.

Note that each of these Latin squares is obtained from the Cayley table of F^+ by permuting columns. A natural correspondence exists between cliques of orthomorphism graphs and sets of mutually orthogonal Latin squares obtained from Cayley tables by permuting columns.

Let L be the Cayley table of G, $|G| = n$, and let θ be a mapping $G \to G$. Define $L(\theta)$ to be the $n \times n$ matrix with ijth entry $g_i\theta(g_j)$. Then it is easy to establish that $L(\theta)$ is a Latin square if and only if θ is a permutation of G, that if θ is a permutation of G then $L(\theta)$ can be obtained from L by permuting columns, and that if M can be obtained from L by permuting columns then $M = L(\theta)$ for some permutation θ of G.

Lemma 1.1. Let L be the Cayley table of G and let θ, ϕ be permutations of G. Then $L(\theta)$ is orthogonal to L if and only if the mapping $x \to x^{-1}\theta(x)$ is a permutation of G and $L(\theta)$ is orthogonal to $L(\phi)$ if and only if $\theta \sim \phi$.

Proof. Let $g_i g_j = a$ and $g_i\theta(g_j) = b$. Then $g_j^{-1}\theta(g_j) = a^{-1}b$ and j will be uniquely determined if and only if the mapping $x \to x^{-1}\theta(x)$ is a permutation of G. But then i will be uniquely determined also. The proof of the second part is similar. ▮

We shall refer to a set of mutually orthogonal Latin squares obtained from the Cayley table of a group G, by permuting columns, as a set of mutually orthogonal Latin squares *based on* G. The following theorem now needs no proof.

Theorem 1.6. The maximum number of squares possible in a set of mutually orthogonal Latin squares based on G is $\omega(\mathrm{Orth}(G)) + 1$. This maximum is attained.

We shall use N(n) to denote the maximum number of squares possible in a set of mutually orthogonal Latin squares of order n, and R(n) to denote the maximum number of squares possible in a set of mutually orthogonal Latin squares based on a group of order n.

Theorem 1.7.

i) R(n) = max{ω(Orth(G)) + 1: G a group of order n}.

ii) R(n) ≤ N(n) ≤ n - 1.

Proof.

i) This follows from Theorem 1.6 and the definition of R(n).

ii) Given a set of r mutually orthogonal Latin squares of order n, permuting the columns or rows of each square in the same way, changing the symbol set, or permuting the symbols of any given square gives rise to another set of r mutually orthogonal Latin squares of order n. Thus we may assume the symbol set to consist of the integers $\{1, \dots, n\}$ and the first row of each square to be 1 2 ... n. Now the symbol 1 cannot appear in the second row, first column in any square and no other symbol can appear in this position in more than one square and so N(n) ≤ n - 1. The fact that R(n) ≤ N(n) follows immediately from the definitions. ▮

We shall call any set of n - 1 mutually orthogonal Latin squares of order n a *complete set of mutually orthogonal Latin squares of order n.* For what values of n is R(n) = N(n), and for what values of n is R(n) < N(n)? For n a prime power, Example 1.2 shows R(n) to be n - 1 and so R(n) = N(n) = n - 1. On the other hand, if n is congruent to 2 modulo 4 then R(n) = 1. This will be proved in Section 5 of this chapter. In this case R(n) < N(n) for $n > 6$ as N(n) ≥ 2 for all $n > 2$ (See for example Dénes and Keedwell (1974, Chapter 11) or Beth, Jungnickel, and Lenz (1984, Chapter IX, Theorem 4.9)).

We shall call a mutually orthogonal set of Latin squares *maximal* if there is no Latin square orthogonal to each square of the set. Maximal sets of orthomorphisms correspond maximal sets of mutually orthogonal Latin squares based on groups. This was proven implicitly in Ostrom (1966).

Theorem 1.8. Let L be the Cayley table of a finite group G. Then $\theta_1, \dots, \theta_r$ is a maximal clique of Orth(G) if and only if $L, L(\theta_1), \dots, L(\theta_r)$ is a maximal set of mutually orthogonal Latin squares.

Proof. Let $e = g_1, \dots, g_n$ be the elements of G. We need only prove that the maximality of $\theta_1, \dots, \theta_r$ implies the maximality of $L, L(\theta_1), \dots, L(\theta_r)$. Thus assume $\theta_1, \dots, \theta_r$ to be a maximal clique of Orth(G). The ijth. entry of L is $g_i g_j$ and the ijth. entry of $L(\theta_k)$ is $g_i\theta_k(g_j)$, $k = 1, \dots, r$. Assume there exists a Latin square M orthogonal to each of L, $L(\theta_1), \dots, L(\theta_r)$. We may further assume that the entry of M in row 1 and column 1 is e. Let the $i\phi(i)$th. cells of M be precisely those with entry e and define $\psi(g_i) = (g_{\phi^{-1}(i)})^{-1}$. Then $\theta_1, \dots, \theta_r, \psi$ is a clique of Orth(G) contradicting the maximality of $\theta_1, \dots, \theta_r$. ▮

Difference matrices and generalized Hadamard matrices are closely related to cliques of orthomorphism graphs. Let $D = \{d_{ij}\}$ be an $r \times \lambda n$ - matrix with entries from a group G of order n. We call D an $(n, r; \lambda, G)$ - *difference matrix* if for each i, j, $i \neq j$, the sequence $\{d_{jk}{}^{-1}d_{ik}$: $k = 1, \dots , \lambda n\}$ contains each element of G exactly λ times. D is a *maximal difference matrix* if there exists no $(n, r + 1; \lambda, G)$ - difference matrix $D' = \{d_{ij}'\}$ satisfying $d_{ij}' = d_{ij}$ for $i = 1, \dots , r$ and $j = 1, \dots , \lambda n$. A *generalized Hadamard matrix* is an $(n, \lambda n; \lambda, G)$ - difference matrix. There are various operations that can be performed on difference matrices that always yield difference matrices with the same parameters. We can permute the rows, permute the columns, multiply all the entries, in any given row, on the right by any given element of G, and multiply all the entries, in any given column, on the left by any given element of G. Thus we may assure that every entry in the first row and column of a difference matrix is the identity element of G.There is a natural correspondence between $(n, r; 1, G)$ - difference matrices and $(r - 2)$ - cliques of Orth(G). Let $\theta_1, \dots , \theta_r$ be a clique of Orth(G) and let $g_1 \dots , g_n$ be the elements of G. Define an $(r + 2) \times n$ matrix $D = (d_{ij})$ by $d_{1j} = e$ for $j = 1, \dots , n$, $d_{2j} = g_j$ for $j = 1, \dots , n$, and $d_{ij} = \theta_{i-2}(g_j)$ for $i = 3, \dots , r + 2$ and $j = 1, \dots , n$. Then D is an $(n, r + 2; 1, G)$ - difference matrix. Let D be an $(n, r + 2; 1, G)$ - difference matrix with every entry in the first row and column of D equal to e. Define θ_i: $G \to G$ by $\theta_i(d_{2j}) = d_{i+2\,j}$ for $i = 1, \dots , r$. Then $\theta_1, \dots , \theta_r$ is a clique of Orth(G). It is easy to see that an $(n, r + 2; 1, G)$ - difference matrix is maximal if and only if the corresponding clique of Orth(G) is maximal. For more information on difference matrices and generalized Hadamard matrices see the survey papers by De Launey (1986, and 1987), and Jungnickel (1979), the book by Beth, Jungnickel, and Lenz (1985, Chapter VIII), and the papers reprinted in Evans (To appear - a).

Example 1.5. Jungnickel (1980) constructed $(p^n, r + 1; 1, Z_{p^n})$ - difference matrices, p a prime, $1 \leq r \leq p - 1$, by setting the ijth entry equal to $(i - 1)(j - 1)$ modulo p^n, for $i = 1, \dots , r + 1$ and $j = 1, \dots , p^n$. The corresponding $(r - 2)$ - clique of Orth(Z_{p^n}), is $\{x \to mx$: $m = 2, \dots , r\}$. For $r = p - 1$ this difference matrix is maximal. Thus there exists a maximal set of $p - 1$ mutually orthogonal Latin squares of order p^n. This will be proved in Chapter 5, Section 4.

Theorem 1.9. Jungnickel (1979). Let G be an abelian group. Then H is a generalized Hadamard matrix over G if and only if its transpose is also a generalized Hadamard matrix over G.

Proof. See Jungnickel (1979, Theorem 2.2) or Brock (1988, Theorem 4.1). ▮

Theorem 1.10. Suppose that a group G, of order nm, admits a homomorphism ϕ onto a group H, of order m, and let $D = \{d_{ij}\}$ be an $(nm, r; 1, G)$ - *difference matrix*. Then the matrix $D' = \{\phi(d_{ij})\}$ is an $(nm, r; n, H)$ - *difference matrix*. In particular if G admits a complete set of orthomorphisms then there exists a generalized Hadamard matrix of order mn over H.

Proof. Routine calculation. ▮

An immediate corollary.

Corollary 1.4. Let $q = p^r$, p a prime. Then there exists a generalized Hadamard matrix of order $p^s q$ over GF$(q)^+$, for all non-negative integers s.

Theorem 1.10 is not of great use in the construction of generalized Hadamard matrices, as the only groups that are known to admit complete sets of orthomorphisms are the elementary abelian groups. It is, however, useful for establishing the non-existence of complete sets of orthomorphisms for many groups. We shall see examples of this in Chapter 5, Section 5.

Section 3. Nets and affine planes.

The well known correspondence between mutually orthogonal Latin squares and nets or equivalently transversal designs, and between complete sets of Latin squares and affine (equivalently projective) planes, implies that orthomorphisms can be used in the construction of such incidence structures. We will give direct constructions of these incidence structures from cliques of orthomorphism graphs.

A *net* of order n and degree k is an incidence structure with n^2 points and nk lines, partitioned into k parallel classes of n lines each, satisfying the following properties.

i) Each line is incident with n points.

ii) Each point is incident with k lines.

iii) Two distinct lines have no points in common if they are in the same parallel class and exactly one point in common if they are in different parallel classes.

Consider the dual of a net of order n and degree k. This is an incidence structure with nk lines and n^2 points, partitioned into k point classes of n points each, each point incident with n lines, each line incident with k points, two distinct points being joined by a unique line if in different point classes and no line if in the same point class. Such an incidence structure is called a *transversal design* of order n and degree k. A transversal design is *resolvable* if its lines can be partitioned into parallel classes, the lines of each parallel class partitioning the point set.

A net of order n and degree $n + 1$ is called an *affine plane* of order n. A *projective plane* of order n is an incidence structure with $n^2 + n + 1$ points and $n^2 + n + 1$ lines, $n + 1$ points on each line, and $n + 1$ lines through each point, each pair of points being incident with a unique common line, and each pair of lines being incident with a unique common point. It is well known that if we remove a line, and all points incident with it, from a projective plane of order n the incidence structure obtained is an affine plane of order n. By reversing this construction we can construct a projective plane of order n from an affine plane of order n as follows. For each parallel class P adjoin an ideal point $[P]$, incident with each line of P but no line of any other parallel class. Adjoin a new line, the ideal line, incident with each of the ideal points. The ideal points are often referred to as points at infinity and the ideal line as the line at infinity.

For more information on nets, transversal designs, affine and projective planes see Dembowski (1968), Dénes and Keedwell (1974), and Beth, Jungnickel, and Lenz (1985).

此为试读，需要完整PDF请访问：www.ertongbook.com

Example 1.6. Let F be a finite field of order q and define an incidence structure as follows. The points will be ordered pairs of elements of F and the lines will be described by equations $x = c$, and $y = mx + b$, where m, b, and $c \in F$. This is the *Desarguesian* affine plane of order q. The parallel classes are $\{x = c\colon\ c \in F\}$, and $\{y = mx + b\colon\ b \in F\}$, $m \in F$. If $r < q + 1$ then a net of order q and degree r can be constructed from this affine plane by removing all lines from $q + 1 - r$ parallel classes.

We have thus shown that there exist affine planes of order q, whenever q is a prime power. No planes of non-prime power order are known and it is conjectured that none exist. For planes of prime power order a great many non-Desarguesian planes have been constructed. However, the only known planes of prime order are Desarguesian and it is conjectured that no non-Desarguesian planes of prime order exist.

Let G be a finite group, which we shall write additively with identity 0, whether abelian or not. Let 1 be a given element of $G - \{0\}$, let S be a subset of the elements of G, where $0, 1 \in S$, and let $\mathbb{F} = \{\phi_x\colon\ x \in S\}$, where ϕ_0 is defined by $\phi_0(x) = 0$ for all x, ϕ_1 is defined by $\phi_1(x) = x$ for all x, and $\phi_x\colon\ G \to G$ is a mapping satisfying $\phi_x(1) = x$ and $\phi_x(0) = 0$. We may think of $\phi_m(x)$ as defining a product $x{\bullet}m$ of elements of G. Define an incidence structure $N(\mathbb{F})$ as follows. The point set of $N(\mathbb{F})$ is $\{(x, y)\colon\ x, y \in G\}$. The lines are $x = a$ and $y = \phi_m(x) + b$. Define a second incidence structure $T(\mathbb{F})$ in a similar manner. The points of $T(\mathbb{F})$ are the ordered pairs (i, b), $i \in S$, $b \in G$, and the lines are the sets B_{xy}, $x, y \in G$, $B_{xy} = \{(i, y + \phi_i(x))\colon\ i \in S\}$, incidence being set inclusion. $T(\mathbb{F})$ is the dual of the incidence structure obtained from $N(\mathbb{F})$ by removing the lines $x = a$. To see this equate the point $(x, -y)$ of $N(\mathbb{F})$ with the line B_{xy} of $T(\mathbb{F})$ and the line $y = \phi_i(x) - b$ of $N(\mathbb{F})$ with the point (i, b) of $T(\mathbb{F})$.

Theorem 1.11. $N(\mathbb{F})$ is a net if and only if $\{\phi_x\colon\ x \in S - \{0, 1\}\}$ is a clique of Orth(G), in which case $N(\mathbb{F})$ will have order $|G|$ and degree $|S| + 1$.

Proof. Let $k = |S| + 1$.

Let $P_i = \{y = \phi_i(x) + b\colon\ b \in G\}$ and $P_\infty = \{x = a\colon\ a \in G\}$. For convenience we shall call these parallel classes.

Note that $N(\mathbb{F})$ contains n^2 points and nk lines, the lines being partitioned into k parallel classes of n lines each. Each line passes through exactly n points. The lines of each parallel class partition the point set of $N(\mathbb{F})$ and each line not in P_∞ intersects each line in P_∞ in exactly one point.

Thus $N(\mathbb{F})$ is a net if and only if lines from distinct parallel classes P_i, $i = 0, \dots, k - 1$, intersect in exactly one point.

For $i \neq 0$, a line $y = \phi_i(x) + b$ intersects each line of P_0 in exactly one point if and only if ϕ_i is a permutation.

For $i \neq 0, 1$, a line $y = \phi_i(x) + b$ intersects each line $y = x + c$ in exactly one point if and only if for each c the equation $-x + \phi_i(x) = c - b$ uniquely determines x, i.e. if and only if $\phi_i \in \text{Orth}(G)$.

For $i, j \neq 0, 1, i \neq j$, each line of P_i intersects each line of P_j in exactly one point if and only if for each b the equation $-\phi_i(x) + \phi_j(x) = b$ uniquely determines x, i.e. if and only if $\phi_i \sim \phi_j$. Hence the result. ▮

In the course of proving Theorem 1.11 we have established the following.

Corollary 1.5. i) Repphun (1965). $N(\mathbb{F})$ is an affine plane if and only if $S = G$ and $\{\phi_x\colon x \in S - \{0, 1\}\}$ is a complete set of orthomorphisms of G.
ii) Jungnickel (1979). $T(\mathbb{F})$ is a resolvable transversal design if and only if $\{\phi_x\colon x \in S - \{0, 1\}\}$ is a clique of Orth(G), in which case $T(\mathbb{F})$ will have order $|G|$ and degree $|S|$.

Corollary 1.6. Let G be a group of order n. G cannot admit a complete set of orthomorphisms if $n \equiv 1$ or 2 modulo 4 and n is not the sum of two squares.
Proof. This follows from Corollary 1.5 and the Bruck-Ryser theorem (See Dembowski (1968, p. 144)). ▮

A *collineation* of a net, transversal design, or affine plane is any permutation of the points that induces a permutation of the lines that preserves incidence. Nets and affine planes constructed from orthomorphisms admit a special class of collineations. Specifically the mapping $(x, y) \rightarrow (x, y + g)$ is a collineation for all $g \in G$. The induced line permutations are $x = c \rightarrow x = c$, and $y = \phi_m(x) + b \rightarrow y = \phi_m(x) + (b + g)$. These collineations form a group under composition. Each collineation of this group fixes any line of the form $x =$ constant, fixes all parallel classes, and the group acts sharply transitively on the points of any line of the form $x =$ constant. Affine planes that admit such a collineation group we shall call *Cartesian planes* and the corresponding collineation group we shall call a *Cartesian group.* The existence of such a collineation group actually characterizes nets and affine planes constructed from orthomorphisms. A collineation of an affine plane that fixes all parallel classes, and all lines of one parallel class is called a *translation*, and the parallel class whose lines are fixed by the translation is called the *direction* of the translation.

Theorem 1.12. a) Let N be a net of degree $r + 3$ and let G be a group of collineations of N that fixes all lines of one parallel class, acts sharply transitively on the points of any line in this class, and fixes all parallel classes. Then there exists an r-clique of Orth(G) such that the net constructed from this clique is isomorphic to N.
b) Let T be a resolvable transversal design of degree $r + 2$ and let G be a group of collineations of T that fixes all point classes, acts sharply transitively on the points of any point class, and semiregularly on the lines of T. Then there exists an r-clique of Orth(G) such that the transversal design constructed from this clique is isomorphic to T.
Proof. See Jungnickel (1979). ▮

Corollary 1.7. Repphun (1965). Let A be a Cartesian plane and let G be the corresponding Cartesian group. Then $A = N(\mathbb{F})$ for some $\mathbb{F}$, where $\mathbb{F} - \{\phi_0, \phi_1\}$ is a complete set of orthomorphisms of G.

As we know certain automorphisms of Orth(G) we might ask what effect these have on the net $N(\mathbb{F})$. This will give us some insight into the relationship between automorphisms of Orth(G) and collineations of $N(\mathbb{F})$.

Theorem 1.13. Let T be a translation, homology, or reflection and let N be the net constructed from the clique $\phi_2, \dots, \phi_r$ of Orth(G). Then the net N' constructed from $\mathrm{T}[\phi_2], \dots, \mathrm{T}[\phi_r]$ is isomorphic to N.

Proof. If $\mathrm{T} = \mathrm{T}_g$ then it is routine to check that the following is an isomorphism.

$(x, y) \rightarrow (x', y') = (x - g, y)$

$x = c \rightarrow x' = c - g$

$y = \phi_m(x) + b \rightarrow y' = \mathrm{T}_g[\phi_m](x') + (\phi_m(g) + b).$

If $\mathrm{T} = \mathrm{H}_\alpha$ then again it is routine to check that the following is an isomorphism.

$(x, y) \rightarrow (x', y') = (\alpha(x), \alpha(y))$

$x = c \rightarrow x' = \alpha(c)$

$y = \phi_m(x) + b \rightarrow y' = \mathrm{H}_\alpha[\phi_m](x') + \alpha(b).$

The case $\mathrm{T} = \mathrm{R}$ is similar and the corresponding isomorphism is given below.

$(x, y) \rightarrow (x', y') = (-x, -x + y)$

$x = c \rightarrow x' = -c$

$y = \phi_m(x) + b \rightarrow y' = \mathrm{R}[\phi_m](x') + b.$ ▮

From the isomorphisms described in the proof to Theorem 1.13 we can read off information about collineations of nets constructed from orthomorphisms. Some of this information is presented in the following corollary.

Corollary 1.8. Let N be the net constructed from the clique $\phi_2, \dots, \phi_r$ of Orth(G).

i) If $\mathrm{T}_g[\phi_m] = \phi_m$ for all m then the mapping $(x, y) \rightarrow (x - g, y)$ is a collineation of N.

ii) If $\mathrm{H}_\alpha[\phi_m] = \phi_m$ for all m then the mapping $(x, y) \rightarrow (\alpha(x), \alpha(y))$ is a collineation of N.

iii) If $\mathrm{R}[\phi_m] = \phi_m$ for all m then the mapping $(x, y) \rightarrow (-x, -x + y)$ is a collineation of N.

The last of these collineations applies to few nets due to the next result.

Theorem 1.14. There exists an r-clique of Orth(G) in which each orthomorphism is fixed by R if and only if $|G|$ is odd and $r = 1$.

Proof. Let θ be an orthomorphism fixed by R. Then $x^{-1}\theta(x) = \theta(x^{-1})$ and so $x = x^{-1}$ if and only if $x = e$. Thus $|G|$ must be odd, and if $n = |G|$ is odd then the mapping $x \rightarrow x^{(n+1)/2}$ is an orthomorphism of G, fixed by R.

Let θ and ϕ be two orthomorphisms fixed by R. These cannot be adjacent as $\theta(x^{-1})^{-1}\phi(x^{-1}) = (x^{-1}\theta(x))^{-1}(x^{-1}\phi(x)) = \theta(x)^{-1}\phi(x)$. ▮

If $S = G$ the the dual of $\mathbb{F}$ is $\mathbb{F}^*$ where $\phi^*_x \in \mathbb{F}^*$ is defined by $\phi^*_x(y) = \phi_y(x)$.

Theorem 1.15. *$N(\mathbb{F}^*)$ and $N(\mathbb{F})$* are both affine planes if and only if the elements of $\mathbb{F} - \{\phi_0, \phi_1\}$ form a complete set of orthomorphisms of G, and the mapping $x \rightarrow \phi_y\phi_z^{-1}(x) - x$ is a permutation whenever $y, z \neq 0, 1, y \neq z$.

Proof. It is easy to show that $\phi^*_0 = \phi_0$, $\phi^*_1 = \phi_1$, $\phi^*_x(0) = 0$, and $\phi^*_x(1) = x$. Let $\phi^*_a, \phi^*_b \in \mathbb{F}^*$. Then $-\phi^*_a(c) + \phi^*_b(c) = -\phi^*_a(d) + \phi^*_b(d)$ if and only if $-\phi_c(a) + \phi_c(b) = -\phi_d(a) + \phi_d(b)$ if and only if $\phi_d(a) - \phi_c(a) = \phi_d(b) - \phi_c(b)$ if and only if $a = b$ or $c = d$. For $c, d \neq 0$, setting $x = \phi_c(a)$ and $y = \phi_c(b)$ we see that $\phi_d(a) - \phi_c(a) = \phi_d(b) - \phi_c(b)$ if and only if $\phi_d\phi_c^{-1}(x) - x = \phi_d\phi_c^{-1}(y) - y$. Hence the result. ▮

Corollary 1.9. If G is abelian then *$N(\mathbb{F})$* is an affine plane if and only if *$N(\mathbb{F}^*)$* is also an affine plane.

Note that Corollary 1.9 is actually a special case of Theorem 1.9. Finally let us mention some orthomorphism characterizations of certain types of affine planes. As orthomorphisms have not actually been used in the study of these classes of planes we refer the interested reader to Dembowski (1968) for their definitions. Each of these planes can be coordinatized by quasifields and can be characterized by the properties of the corresponding quasifields. Equating the product $x \bullet m$ with $\phi_m(x)$, the orthomorphism characterizations then follow immediately from the quasifield characterizations.

Theorem 1.16. Let $\mathbb{F} = \{\phi_x\colon x \in G - \{0, 1\}\} \cup \{\phi_0, \phi_1\}$, where $\mathbb{F} - \{\phi_0, \phi_1\}$ is a complete set of orthomorphisms of G.

(i) *$N(\mathbb{F})$* is a translation plane if and only if $\phi_x \in \mathrm{Aut}(G)$ for all $x \neq 0$.

(ii) *$N(\mathbb{F})$* is a dual translation plane if and only if $(\mathbb{F}, +)$ is a group, in which case $\phi_x + \phi_y = \phi_{x+y}$ and $(\mathbb{F}, +) \cong G$.

(iii) *$N(\mathbb{F})$* is a nearfield plane if and only if $\phi_x \in \mathrm{Aut}(G)$ for all $x \neq 0$ and $\mathbb{F} - \{\phi_0\}$ is a group under the operation of composition.

(iv) *$N(\mathbb{F})$* is a semifield plane if and only if $(\mathbb{F}, +)$ is a group, in which case $\phi_x + \phi_y = \phi_{x+y}$ and $(\mathbb{F}, +) \cong G$, and $\phi_x \in \mathrm{Aut}(G)$ for $x \neq 0$.

(v) *$N(\mathbb{F})$* is a Desarguesian affine plane if and only if G, with multiplication defined by $xm = \phi_m(x)$, is a field.

A proof of Theorem 1.16 can be found in Repphun (1965) and proofs of parts i) and ii) can also be found in Evans (1989d).

Section 4. Neofields.

In this section we will define (left) neofields and near orthomorphisms, a generalization of the concept of orthomorphism. It will be shown that near orthomorphisms are equivalent to left neofields and as a consequence that orthomorphisms are equivalent to left neofields in which $1 + 1 = 0$. We will establish a strong relationship between properties of left neofields and properties of the corresponding near orthomorphisms. In fact, we will find that the properties of a left neofield, in which $1 + 1 = 0$, are determined by the congruences of $\mathrm{Orth}(G)$ that fix the corresponding orthomorphism. Similar results will be proved for left neofields, in which $1 + 1 \neq 0$, and their corresponding near orthomorphisms.

A *near orthomorphism* of a group G is a bijection θ: $G - \{t\} \rightarrow G - \{e\}$, for which the mapping $x \rightarrow x^{-1}\theta(x)$ is also a bijection from $G - \{t\}$ onto $G - \{e\}$. We call t the *exdomain element* of θ. Orthomorphisms can be regarded as a special class of near orthomorphisms as if the exdomain element of the near orthomorphism θ is e then θ becomes an orthomorphism when we define $\theta(e) = e$. The definition given here differs subtly from that of Hsu (1991). Hsu defines a near orthomorphism of a group G to be a bijection θ: $G \rightarrow G$ for which the set $\{x^{-1}\theta(x)$: $x \in G\} = G - \{e\}$. If $t \neq e$ is the exdomain element of a near orthomorphism θ then setting $\theta(t) = e$ yields a mapping that satisfies Hsu's definition of a near orthomorphism. It should be noted that our definition is consistent with the definition of a (K, λ) - near orthomorphism introduced in Hsu and Keedwell (1984). This is actually called a (K, λ) - near complete mapping in their paper, but both coauthors have since decided to use the term orthomorphism instead. It was proved implicitly in the work of Paige (1947b) that, if G is abelian then the exdomain element of a near orthomorphism of G must be the identity if the Sylow 2-subgroup of G is trivial or noncyclic, or the unique element of order 2 if the Sylow 2-subgroup is nontrivial and cyclic.

A *left neofield* is a set N with two binary operations, addition and multiplication, satisfying the following:

i) The elements of N form a loop under addition, with identity 0.
ii) The nonzero elements of N form a group under multiplication, with identity 1.
iii) $a(b + c) = ab + ac$ for all $a, b, c \in N$.

A *left neofield* is called a *neofield* if the right distributive law is also satisfied. Clearly if the multiplicative group is abelian then the terms neofield and left neofield are synonymous. The *order* of the left neofield N, denoted $|N|$, is the number of elements of N, i.e. one plus the order of its multiplicative group. A left neofield is completely determined by its multiplicative group and the mapping $\theta(x) = 1 + x$, called the *presentation function* of the left neofield.

Neofields were first introduced by Paige (1949). Bruck (see Paige (1949), Theorem I.1) implicitly established the connection between neofields with multiplicative group G and near orthomorphisms of G fixed by the homologies H_α, $\alpha \in \mathrm{Inn}(G)$. Later Hsu and Keedwell (1984) generalized this result to show that there is a 1-1 correspondence between left neofields with multiplicative group G and near orthomorphisms of G.

Theorem 1.17. Hsu and Keedwell (1984). Let G be a group, written multiplicatively with identity 1. Let θ be a near orthomorphism of G, with exdomain element t, and extend θ to a bijection $G \cup \{0\} \to G \cup \{0\}$ by setting $\theta(t) = 0$ and $\theta(0) = 1$. Then θ is the presentation function of a left neofield.

Conversely, Let θ be the presentation function of a left neofield with multiplicative group G. Let t be the unique solution to the equation $\theta(x) = 0$. Then θ restricted to $G - \{t\}$ is a near orthomorphism of G with exdomain element t.

Proof. Let θ be a near orthomorphism of a group G, with exdomain element t, and extend θ to a bijection $G \cup \{0\} \to G \cup \{0\}$ by setting $\theta(t) = 0$ and $\theta(0) = 1$. Let $N = G \cup \{0\}$ and define addition and multiplication in N as follows. Multiplication is as in G except that $0a = a0 = 0$ for all $a \in N$. To define addition, $x + y = y$ if $x = 0$, and $x\theta(x^{-1}y)$ if $x \neq 0$.

We see that $0 + y = y$ for all $y \in N$ and if $y \neq 0$ then $y + 0 = y\theta(0) = y$. Suppose that $a + b = c$. Given a and b the value of c is uniquely determined. Given a and c then $b = c$ if and only if $a = 0$, and b is uniquely determined by the equation $\theta(a^{-1}b) = a^{-1}c$ if $a \neq 0$. Given b and c then $a = 0$ if and only if $b = c$. Otherwise a is uniquely determined by the equation $(a^{-1}b)^{-1}\theta(a^{-1}b) = b^{-1}c$. Thus N is a loop under addition. Next consider $a(b + c)$. This must equal $ab + ac$ if any of a, b, or c is 0. If $a, b, c \neq 0$ then $a(b + c) = (ab)\theta((ab)^{-1}ac) = ab + ac$ and so the left distributive law holds. Thus N is a left neofield.

Conversely, if θ is the presentation function of a left neofield N with multiplicative group G then $\theta(t) = 0$ for a unique element t of N. It is easily seen that θ is a bijection from $G - \{t\}$ onto $G - \{1\}$ and the mapping $x \to x^{-1}\theta(x) = x^{-1} + 1$ is a bijection from $G - \{t\}$ onto $G - \{1\}$. Thus the restriction of θ to $G - \{t\}$ is a near orthomorphism of G. ▮

Corollary 1.10. There is a 1-1 correspondence between orthomorphisms of a group G and left neofields with multiplicative group G in which $1 + 1 = 0$.

We remark that for a left neofield N the mapping $a \to ga$ is an automorphism of the additive loop of N, for each nonzero element g of N. In fact, a loop can be the additive loop of a left neofield if and only if it admits an automorphism group that acts sharply transitively on its nonidentity elements.

Let us define an *automorphism* of a left neofield N to be a bijection α: $N \to N$ for which $\alpha(a + b) = \alpha(a) + \alpha(b)$, and $\alpha(ab) = \alpha(a)\alpha(b)$, for all $a, b \in N$. Clearly the automorphism group of a left neofield is a subgroup of the automorphism group of its multiplicative group, as well as a subgroup of the automorphism group of its additive loop.

此为试读，需要完整PDF请访问：www.ertongbook.com