BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(80), 2016, Pages 64–69
ISSN 1024–7696

Linear groups that are the multiplicative groups of neofields

Anthony B. Evans

Abstract. A neofield N is a set with two binary operations, addition and multiplication, for which N is a loop under addition with identity 0, the nonzero elements of N form a group under multiplication, and both left and right distributive laws hold. Which finite groups can be the multiplicative groups of neofields? It is known that any finite abelian group can be the multiplicative group of a neofield, but few classes of finite nonabelian groups have been shown to be multiplicative groups of neofields. We will show that each of the groups $GL(n,q)$, $PGL(n,q)$, $SL(n,q)$, and $PSL(n,q)$, q even, $q \neq 2$, can be the multiplicative group of a neofield.

Mathematics subject classification: 20N05, 12K99.
Keywords and phrases: neofield, linear group, orthomorphism, near orthomorphism.

1 Introduction

Neofields were introduced by Paige [7] in 1949. A *neofield* is a set N with two binary operations, addition and multiplication, satisfying the following:

1. The elements of N form a loop under addition, with identity 0.
2. The nonzero elements of N form a group under multiplication.
3. The left and right distributive laws hold: $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$ for all $a, b, c \in N$.

For a neofield N we will use 1 to denote the multiplicative identity. If N is a neofield, then the additive loop of N is completely determined by its multiplicative group and its *presentation function* $T\colon x \mapsto 1 + x$, as

$$x + y = \begin{cases} y & \text{if } x = 0; \\ x & \text{if } y = 0; \\ xT(x^{-1}y) & \text{if } x, y \neq 0. \end{cases}$$

In fact, N is completely determined by its multiplicative group and its presentation function as an easy argument shows that $a0 = 0a = 0$ for all $a \in N$.

The question that will concern us is, Which finite groups can be multiplicative groups of neofields? For abelian groups, this question was answered by Paige [7].

His answer illustrates a divide between neofields in which $1+1=0$ and neofields in which $1+1\neq 0$. In fact Johnson [4] showed that a finite group cannot be both the multiplicative group of a neofield in which $1+1=0$ and the multiplicative group of a neofield in which $1+1\neq 0$.

Theorem 1 (Paige, 1949)**.** *Any finite abelian group G can be the multiplicative group of a neofield. G can be the multiplicative group of a neofield in which $1+1=0$ if and only if G does not contain a unique element of order two; and G can be the multiplicative group of a neofield in which $1+1\neq 0$ if and only if G contains a unique element of order two.*

Thus, the question of which finite groups can be multiplicative groups of neofields reduces to the question, Which finite nonabelian groups can be multiplicative groups of neofields? Johnson [4] answered this question for dihedral groups.

Theorem 2 (Johnson, 1986)**.** *No dihedral group can be the multiplicative group of a neofield.*

In a list of unsolved problems Keedwell [5] posed a closely related problem, For which finite orders do there exist nonabelian groups that can be multiplicative groups of neofields?

For a group G, a bijection $\theta\colon G\to G$ is an *orthomorphism* of G if the mapping $\delta\colon x\mapsto x^{-1}\theta(x)$ is a bijection: θ is *normalized* if $\theta(1)=1$. A *near orthomorphism* of G is a bijection $\theta\colon G\setminus\{h\}\to G\setminus\{1\}$, $h\neq 1$, for which the mapping $\delta\colon g\mapsto g^{-1}\theta(g)$ is a bijection $\theta\colon G\setminus\{h\}\to G\setminus\{k\}$, for some $k\in G$, $k\neq h^{-1}$. A near orthomorphism θ is *normalized* if $k=1$, in which case h is the *exdomain element* of θ.

Orthomorphisms and near orthomorphisms of G that commute with all inner automorphisms of G, i. e., $\theta(g^{-1}xg)=g^{-1}\theta(x)g$ for all $g\in G$, are particularly useful in the construction of neofields. Orthomorphisms are used to construct neofields in which $1+1=0$, and near orthomorphisms to construct neofields in which $1+1\neq 0$.

Theorem 3. *Let G be a finite group. There exists a neofield, with multiplicative group G, in which $1+1=0$ if and only if G admits normalized orthomorphisms that commute with all inner automorphisms of G.*

There exists a neofield, with multiplicative group G, in which $1+1\neq 0$ if and only if G admits normalized near orthomorphisms that commute with all inner automorphisms of G.

Proof. If θ is a normalized orthomorphism of G that commutes with all inner automorphisms of G and $0\notin G$, then the function $T\colon G\cup\{0\}\to G\cup\{0\}$ defined by

$$T(x)=\begin{cases}1 & \text{if } x=0,\\ 0 & \text{if } x=1,\\ \theta(x) & \text{if } x\neq 0,1,\end{cases}$$

is the presentation function of a neofield, with multiplicative group G, in which $1+1=0$.

If T is the presentation function of a neofield, with multiplicative group G, in which $1 + 1 = 0$, then the mapping $\theta\colon G \to G$ defined by

$$\theta(x) = \begin{cases} 1 & \text{if } x = 1, \\ T(x) & \text{otherwise,} \end{cases}$$

is a normalized orthomorphism of G that commutes with all inner automorphisms of G.

A similar proof establishes the relationship between neofields, with multiplicative group G, in which $1+1 \neq 0$ and normalized near orthomorphisms of G that commute with all inner automorphisms of G. □

As an example.

Corollary 1. *Any group of odd order can be the multiplicative group of a neofield in which* $1 + 1 = 0$.

Proof. If G is a group of odd order, then the mapping $x \mapsto x^2$ is a normalized orthomorphism of G that commutes with all inner automorphisms of G. The result then follows from Theorem 3. □

In this paper we will show that, if G is one of $GL(n, q)$, $SL(n, q)$, $PGL(n, q)$ or $PSL(n, q)$, q even, $q \neq 2$, then G can be the multiplicative group of a neofield in which $1 + 1 = 0$. We will do this by constructing normalized orthomorphisms of G that commute with all inner automorphisms of G. We will adapt techniques that were used in [3] to construct sets of mutually orthogonal latin squares based on $GL(n, q)$, q even, $q \neq 2$: a remark in this paper claimed that the orthomorphisms constructed yield neofields with multipicative group $GL(n, q)$, q even, $q \neq 2$, in which $1 + 1 = 0$. For more information on neofields and orthomorphisms consult [1] and [2].

2 The even-odd decomposition

Throughout this paper G will denote a finite group, U the set of 2–elements of G, and S the set of odd–order elements of G. Note that $U \cap S = \{1\}$. We will make extensive use of the even-odd decomposition, described in the following lemma.

Lemma 1 (even-odd decomposition)**.** *Each $g \in G$ can be uniquely written as a product $g = us$, where $us = su$, $u \in U$, and $s \in S$.*

Proof. See [6], Lemma 2.2.4 with $p = 2$, for instance. □

For this paper we need to define orthomorphisms of U and S. We call a bijection $\theta\colon U \to U$ an *orthomorphism* of U if the mapping $x \mapsto x^{-1}\theta(x)$ is also a bijection $U \to U$: θ is *normalized* if $\theta(1) = 1$. Orthomorphisms of S are defined similarly. We are interested in normalized orthomorphisms of U and S that commute with all inner automorphisms of G.

We first present a method for constructing orthomorphisms of G from orthomorphisms of U and S, using even-odd decompositions. Given two mappings $\theta\colon U \to U$ and $\phi\colon S \to S$, we will define the *product of θ and ϕ* (with respect to U and S), written $\theta \times_J \phi$, by $\theta \times_J \phi(g) = \theta(u)\phi(s)$, where $g = us$ is the even-odd decomposition of g. A product construction of orthomorphisms is described in the following lemma. Note that $C_U(s)$ denotes the centralizer of s in U and $C_S(u)$ the centralizer of u in S.

Lemma 2. *Let θ be an orthomorphism of U that acts on $C_U(s)$ for each $s \in S$, and let ϕ be an orthomorphism of S that acts on $C_S(u)$ for each $u \in U$. Then $\theta \times_J \phi$ is an orthomorphism of G.*

Proof. See Lemma 2 in [3]. □

Theorem 4. *Let θ be a normalized orthomorphism of U that acts on $C_U(s)$ for each $s \in S$, and let ϕ be a normalized orthomorphism of S that acts on $C_S(u)$ for each $u \in U$. If θ and ϕ commute with all inner automorphisms of G, then there exists a neofield in which $1 + 1 = 0$, with multiplicative group G.*

Proof. By Lemma 2, $\theta \times_J \phi$ is a normalized orthomorphism of G. Further $\theta \times_J \phi$ commutes with all inner automorphisms of G, as, if $g = us$, $u \in U$, $s \in S$, is the even-odd decomposition of g and $h \in G$, then $h^{-1}gh = (h^{-1}uh)(h^{-1}sh)$ is the even-odd decomposition of $h^{-1}gh$. □

Corollary 2. *If there exists a normalized orthomorphism of U that acts on $C_U(s)$ for each $s \in S$, and commutes with all inner automorphisms of G, then there exists a neofield in which $1 + 1 = 0$ with multiplicative group G.*

Proof. The mapping $x \mapsto x^2$ is a normalized orthomorphism of S that acts on $C_S(u)$ for each $u \in U$ and commutes with all inner automorphisms of G. □

3 The construction

For G one of $GL(n,q)$, $SL(n,q)$, $PGL(n,q)$, or $PSL(n,q)$, q even, $q \neq 2$, we will construct normalized orthomorphisms of U that commute with inner automorphisms of G. It will then follow from Corollary 2 that each of these groups can be the multiplicative group of a neofield in which $1 + 1 = 0$.

Let $M_n(q)$ denote the set of $n \times n$ matrices over $GF(q)$, q a power of 2. For each $a \in GF(q)^*$, the multiplicative group of $GF(q)$, we define the mapping

$$\theta_a\colon M_n(q) \to M_n(q) \text{ by } \theta_a(A) = I + a(I + A).$$

Suppose that G is a subgroup of $GL(n,q)$, q a power of 2. Note that, if $A^m = I$, m a power of 2, then $\theta_a(A)^m = I$ and so θ_a maps 2-elements to 2-elements. Thus, if $\theta_a(U) \subseteq G$, then $\theta_a(U) \subseteq U$. The next lemmas establish some properties of this class of mappings.

Lemma 3. *Suppose that G is a subgroup of $GL(n,q)$, q even, $q \neq 2$. If $a \in GF(q)$, $a \neq 0,1$, and $\theta_a(U) \subseteq G$, then $\theta_a \mid_U$ is an orthomorphism of U which acts on $C_U(B)$ for each $B \in S$.*

Proof. See Lemma 4 in [3]. □

Lemma 4. *Suppose that G is a subgroup of $GL(n,q)$, q even, $q \neq 2$. If $a \in GF(q)$, $a \neq 0,1$, and $\theta_a(U) \subseteq G$, then $\theta_a \mid_U$ commutes with all inner automorphisms of G.*

Proof. Routine. □

For the linear groups $GL(n,q)$ and $SL(n,q)$, q even, $q \neq 2$, we give a simple proof that each of these groups can be the multiplicative group of a neofield in which $1+1=0$.

Theorem 5. *If G is one of $GL(n,q)$ or $SL(n,q)$, q even, $q \neq 2$, then G can be the multiplicative group of a neofield in which $1+1=0$.*

Proof. Suppose $G = GL(n,q)$, q even, $q \neq 2$, and $a \in GF(q)^*$, $a \neq 1$. By Lemmas 3 and 4, θ_a is an orthomorphism of U that commutes with inner automorphisms of G and, hence, by Corollary 2, $GL(n,q)$ can be the multiplicative group of a neofield in which $1+1=0$.

As det is a homomorphism from $GL(n,q)$ to $GF(q)^*$, a group of odd order, every element of U has determinant 1. Thus $U \subseteq SL(n,q)$. It follows that $SL(n,q)$ can be the multiplicative group of a neofield in which $1+1=0$. □

In order to extend the result of Theorem 5 to $PGL(n,q)$ and $PSL(n,q)$, q even, $q \neq 2$, we need to describe the relationship between the sets of 2-elements and odd-order elements of $PGL(n,q)$ and $PSL(n,q)$, and those of $GL(n,q)$ and $SL(n,q)$.

Lemma 5. *Let G be one of $GL(n,q)$ or $SL(n,q)$, set $P = \{cI \mid c \in GF(q)^*, cI \in G\}$, let U^* be the set of 2-elements of G/P and let S^* be the set of odd-order elements of G/P. Then $U^* = UP$ and $S^* = SP$. Further, the mapping $A \mapsto AP$ is a bijection $U \to U^*$ and, if $A \in U$ and $B \in S$, then AP commutes with BP if and only if A commutes with B.*

Proof. Clearly $UP \subseteq U^*$. For $XP \in U^*$, $X \in G$, let $X = AB$, $A \in U$, $B \in S$, be the even-odd decomposition of X. Let m be a power of 2 for which $A^m = I$ and $(XP)^m = P$ and let s be an odd positive integer for which $B^s = I$. Then $B^m P = (XP)^m = P$, and so $B^m \in P$. As $\gcd(m,s) = 1$, there exists a positive integer r for which $B^{mr} = B$. Then $B = B^{mr} \in P^r \subseteq P$. It follows that $U^* \subseteq UP$ and hence $U^* = UP$. A similar proof shows that $S^* = SP$

For $A, B \in U$, if $AP = BP$, then $A = cB$ for some $c \in GF(q)^*$. There exists m, a power of 2, for which $A^m = B^m = I$. Thus $I = c^m I$, and so $c^m = 1$. As the multiplicative order of c is odd, $c = 1$. Hence, if $A, B \in U$, then $AP = BP$ if and only if $A = B$. It follows that the mapping $A \mapsto AP$ is a bijection $U \to U^*$.

Clearly, if $A \in U$ commutes with $B \in S$, then AP commutes with BP. If AP commutes with BP, $A \in U$ and $B \in S$, then $ABP = BAP$. Hence $AB = cBA$ for

some $c \in GF(q)^*$, and so $A = c(BAB^{-1})$. Let m be a power of 2 for which $A^m = I$. Then $I = c^m I$, from which it follows that $c^m = 1$, and, as c is of odd multiplicative order, it must be that $c = 1$. Hence A and B commute. □

For the linear groups $PGL(n, q)$ and $PSL(n, q)$, q even, $q \neq 2$, we can now give a proof that each of these groups can be the multiplicative group of a neofield in which $1 + 1 = 0$.

Theorem 6. *If G is one of $PGL(n, q)$ or $PSL(n, q)$, q even, $q \neq 2$, then G can be the multiplicative group of a neofield in which $1 + 1 = 0$.*

Proof. Let G be one of $GL(n, q)$ or $SL(n, q)$, set $P = \{cI \mid c \in GF(q)^*, cI \in G\}$, let U^* be the set of 2-elements of G/P, and let S^* be the set of odd-order elements of G/P. By Lemma 5, $U^* = UP$ and, if $A, A' \in U$, then $AP = A'P$ if and only if $A = A'$. It follows that, for any mapping $\theta\colon U \to U$, if we define $\theta^*\colon U^* \to U^*$ by $\theta^*(AP) = \theta(A)P$, $A \in U$, then θ^* is well-defined, and is a bijection if and only if θ is a bijection. Thus, if θ is an orthomorphism of U, then, as the mapping $AP \mapsto (AP)^{-1}\theta^*(AP) = A^{-1}\theta(A)P$ is a bijection, θ^* is an orthomorphism of U^*. Hence, if $a \in GF(q)^*$, $a \neq 1$, then θ_a^* is an orthomorphism of U^*. As θ_a commutes with inner automorphisms of G, θ_a^* commutes with inner automorphisms of G/P. The result then follows from Corollary 2. □

References

[1] Colbourn C. J., Dinitz J. H. (eds). *Handbook of combinatorial designs, 2nd ed.* Chapman and Hall, CRC, Florida, 2007.

[2] Evans A. B. *Orthomorphism graphs of groups.* Lecture Notes in Mathematics, **1535**, Springer-Verlag, Berlin, Heidelberg, 1992.

[3] Evans A. B. *Mutually orthogonal latin squares based on general linear groups.* Des. Codes Cryptogr., 2014, **71**, 479–492.

[4] Johnson C. P. *Complete mappings, neofields, and dihedral groups.* J. Miss. Acad. Sci., 1986, **XXXI**, 147–152.

[5] Keedwell A. D. *Sequenceable groups, generalized complete mappings, neofields and block designs.* Combinatorial mathematics, X (Adelaide, 1982), 49–71, Lecture Notes in Math., **1036**, Springer, Berlin, 1983.

[6] Michler G. *Theory of finite simple groups.* Cambridge University Press, Cambridge, 2006.

[7] Paige L. J. *Neofields.* Duke Math. J., 1949, **16**, 39–60.

Anthony B. Evans
Wright State University
E-mail: *anthony.evans@wright.edu*

Received November 23, 2015