PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 113, Number 4, December 1991

INTERCONNECTIONS BETWEEN THE STRUCTURE THEORY OF SET ADDITION AND REWRITABILITY IN GROUPS

GREGORY A. FREIMAN AND BORIS M. SCHEIN

(Communicated by Warren J. Wong)

ABSTRACT. An approach to groups and semigroups stemming from the structure theory of set addition turns out to have much in common with the so-called permutation or rewritable properties. We explain these connections and show how these properties take their place in a wider class of interesting and naturally arising problems. As an example, we characterize some classes of groups and group elements.

1. INTRODUCTION

In recent years semigroups and groups satisfying the so-called permutation or rewritable properties attracted considerable attention (see [1]).

From the early sixties the first author studied general aspects of the additive number theory in the sense of Schnirelmann-Mann (summarized in [6]). These results and approaches can be generalized naturally in abstract algebraic setting (see [7, 8, 10]).

Problems connected with permutation and rewritable properties of groups and semigroups find their natural place in the structure theory of set addition.[1] The goal of this paper is to show how the problems of rewritability and a class of analogous problems can be approached from the point of view of the structure theory of set addition. This approach gives rise to many new and natural questions about rewritability and may indicate possible ways of solving these problems. To consider rewritability-like problems, we give a classification of three-element subsets in groups and cancellative semigroups from a point of view compatible with the structure theory of set addition (Theorem 1). This classification is used to obtain two concrete results in Theorems 2 and 3. These theorems serve as detailed examples, rather than *per se*, as results of their own, because our aim is not so much in proving new concrete results as in pointing

Received by the editors May 1, 1990 and, in revised form, September 27, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20F99, 20F26, 20F05, 20F12.

[1]The word "addition" reflects number-theoretic origins of this theory. In abstract algebra setting we consider operations that are usually called "multiplication" (rather than "addition") in our algebraic systems.

0002-9939/91 $1.00 + $.25 per page

at a new approach to a class of natural problems. Hence Theorem 2 is close to a result first proved in [5], and our proof of it is not dissimilar to a proof given in [5], although based on a new approach, while Theorem 3 appears to be new.

We are grateful to Professors Ya. G. Berkovich and D. Gorenstein for drawing our attention to possible connections between the structure theory of set addition and rewritability, and to Professor D. J. S. Robinson for a helpful observation on the original form of Theorem 2.

Now we give a few definitions, remarks, and examples. Our aim is to give the reader at least some flavor of the character of numerous problems arising when our approach is used for groups. The definitions are used in the subsequent sections of this paper.

Let S and T be two semigroups (sets with a binary operation, not necessarily associative, can be considered too; n-ary operations can be considered as well). Let $A \subset S$ and $B \subset T$ be subsets of S and T, respectively, and let n be a positive integer. Then $A^n = AA\cdots A$ (n times), so that $A^n = \{x \in S | x = a_1 a_2 \cdots a_n$ for some $a_1, a_2, \cdots, a_n \in A\}$. Let $A^{[n]} = \{x \in S | x = a_1 a_2 \cdots a_n$ with all factors $a_1, a_2, \cdots, a_n \in A$ pairwise distinct$\}$. An *n-isomorphism* of A onto B is a pair (φ, ψ) of bijections $\varphi: A \to B$ and $\psi: A^n \to B^n$ such that $\psi(a_1 a_2 \cdots a_n) = \varphi(a_1)\varphi(a_2)\cdots\varphi(a_n)$ for all $a_1, a_2, \ldots, a_n \in A$. If this last property holds for *pairwise disjoint* $a_1, a_2 \ldots, a_n \in A$, then (φ, ψ) is called a *permutational n-isomorphism* or an *$[n]$-isomorphism.*

Example 1. Let Z be the additive group of integers, N the subsemigroup of nonnegative integers, and L the subsemigroup of all integers greater than 2. Define $\varphi: N \to L$ by $\varphi(n) = n+3$ and $\psi: N^3 \to L^3$ by $\psi(m) = m+9$. Then (φ, ψ) is a 3-isomorphism of N onto L. As semigroups, N and L are not isomorphic.

Example 2. Let $Z \times Z$ be the direct product of two copies of Z. Let $A = \{0, 1, 3, 4\} \subset Z$ and $B = \{(0, 0,), (1, 0), (0, 1), (1, 1)\} \subset Z \times Z$. Then A and B are 2-isomorphic, where (φ, ψ) is such that φ maps $0, 1, 3, 4$ into $(0, 0)$, $(1, 0)$, $(0, 1)$, and $(1, 1)$, respectively, and ψ is naturally induced by φ. It is easy to see that A and B are not 3-isomorphic.

The concept of n-isomorphism of sets is of fundamental importance for this paper; this is why we discuss it in more detail now.

Suppose that S and T are given by their Cayley multiplication tables. Each such table is a finite or infinite square array of elements of S (or of T), and its rows and columns are labelled by the elements of S (or of T). Suppose that $n > 1$ is given. We can construct an analog of the Cayley multiplication table for $S \times S \times \cdots \times S \to S^n$, which maps any n-tuple $(a_1, a_2, \ldots, a_n)$ of elements of S into their product $a_1 a_2 \cdots a_n$. This table can be geometrically represented as an n-dimensional cube. Now suppose that $A \subset S$ is chosen. Consider an n-dimensional "subcube" $A \times A \times \cdots \times A \to A^n$. If A is a subsemigroup, A^n consists of elements of A and thus $|A^n| \leq |A|$, where $|A|$ denotes the

cardinality of A. It is easy to see that if S is a cancellative semigroup, then $|A^n| = |A|$. However, if A is an arbitrary subset of S, then the cardinality of A^n can be larger than $|A|$. In fact, $|A^n| = |A|^n$ is possible. Clearly, $A \subset S$ and $B \subset T$ are n-isomorphic if their "n-dimensional Cayley tables" have the same form. If (φ, ψ) is an n-isomorphism, then φ "rearranges" columns and rows (in all n dimensions) of the Cayley table of B so that ψ becomes a one-to-one correspondence between the tables.

For example, if $n = 2$ and $|A| = |B| = 2$, then A and B are 2-isomorphic if there exists a pair (φ, ψ) of mappings with the above properties. Without loss of generality, we can assume that $A = B = \{a, b\}$, and thus φ is the identity mapping. In this case ψ becomes the identity mapping, too. Which forms can the Cayley tables for A and B have? If we assume that S (and T) are cancellative semigroups or groups, then no two elements in the same row or the same column of the table can be equal. A^2 can have at least two and at most four different elements. Denoting these elements by s, t, u, and v, we see that the tables can have only four different forms:

$$\begin{array}{cccc} s\,t & s\,t & s\,t & s\,t \\ t\,s & t\,u & u\,s & u\,v. \end{array}$$

The first two of these tables are symmetric and occur when a and b commute. The first and third of these tables have the same element on the main diagonal, i.e. they occur when $a^2 = b^2$. The infinite cyclic group Z is abelian, and so the third and fourth of these tables are impossible in Z. It is obvious that the first table is impossible. Thus, all two-element subset of Z are 2-isomorphic and their Cayley 2-tables are isomorphic to the second of the above tables. Classes of 2-isomorphic 2-element and 3-element sets in groups were described in [8]. There are forty-five noncommutative and seven commutative types of 2-isomorphism of 3-element subsets of groups. Classes of 3-isomorphic 2-element subsets of groups are found in [2], there are twenty-two types of them.

Various problems of classification of groups (and semigroups) arise. For example, suppose that a group cannot contain n-element subsets of certain types of m-isomorphism. What is the structure of this group? As a trivial example consider groups that do not contain 2-element subsets with the Cayley 2-tables of the above types 1, 3, and 4. Clearly, such groups are abelian and no two elements in them can have the same square. In other words, they are abelian groups without elements of order 2. If the groups are finite, they are abelian groups of odd order. What are the groups in which type 4 of the Cayley 2-table is impossible for any two elements? Clearly, they are groups in which $|A^2| \leq 3$ for every two-element subset A. An easy argument shows that they are the groups in which, for every two elements a and b, $ba \in \{ab, (ab)^{-1}\}$. A somewhat more involved argument (see [8]) shows that these are either abelian groups or direct products of Q, the eight-element quaternion group, and an elementary abelian 2-group. An analogous result holds for cancellative semigroups (see [10]).

Other problems of this type are discussed in [4, 7, and 10].

Now we turn to subsets of the form $A^{[n]}$. Recall that subsets $A \subset S$ and $B \subset T$ are called permutationally n-isomorphic (or $[n]$-isomorphic) if there exists a pair (φ, ψ) of bijections $\varphi: A \to B$ and $\psi: A^{[n]} \to B^{[n]}$ such that $\psi(a_1 a_2 \cdots a_n) = \varphi(a_1)\varphi(a_2)\cdots\varphi(a_n)$ for all pairwise distinct $a_1, a_2, \ldots, a_n \in A$ (that is, $a_i \neq a_j$ for any $1 \leq i \neq j \leq n$). Clearly, if A and B are n-isomorphic, then they are $[n]$-isomorphic, and hence every class of $[n]$-isomorphic m-element sets is a union of classes of n-isomorphic m-element sets. In other words, each permutational n-isomorphism type is a union of several n-isomorphism types.

The concept of permutational n-isomorphism makes it possible to approach the concepts of n-rewritability in a different way.

An n-element subset $\{a_1, a_2, \ldots, a_n\}$ of a group or a semigroup S is called *rewritable* if there exist two different permutations σ and τ of $\{1, 2, \ldots, n\}$ such that $a_{\sigma(1)}a_{\sigma(2)}\cdots a_{\sigma(n)} = a_{\tau(1)}a_{\tau(2)}\cdots a_{\tau(n)}$. A semigroup S is called *n-rewritable* (or satisfying the property Q_n) if every n-element subset A of S is rewritable. Clearly, $A = \{a_1, a_2, \ldots, a_n\}$ is rewritable exactly if $A^{[n]}$ contains less than $n!$ elements, and S satisfies Q_n precisely when $|A^{[n]}| < n!$ for every n-element subset $A \subset S$. This alternative statement of Q_n shows that Q_n can be naturally considered as a problem belonging to the structure theory of set addition.

An ordered n-tuple $(a_1, a_2, \ldots, a_n)$ of elements of S is called *rewritable* if there exists a nonidentity permutation τ of $\{1, 2, \ldots, n\}$ such that $a_1 a_2 \cdots a_n = a_{\tau(1)}a_{\tau(2)}\cdots a_{\tau(n)}$. A semigroup S is *totally n-rewritable* (or satisfies the property P_n) if every n-tuple of its elements is rewritable. Obviously, P_n implies Q_n. The product $a_1 a_2 \cdots a_n$ is called the value of $(a_1, a_2, \ldots, a_n)$. It is easy to see that a semigroup S is totally n-rewritable if each element of $A^{[n]}$ is the value of more than one n-tuple of elements of A for every n-element subsets $A \subset S$. Thus S satisfies P_n exactly when, for every n-element subset A of S, no entry in the n-dimensional Cayley multiplication table of A is "isolated" (that is, each entry appears more than once in the table). As Blyth proved (cf. [1]), $\bigcup_n P_n = \bigcup_n Q_n$, where P_n and Q_n denote the classes of groups which satisfy P_n and Q_n, respectively.

As an example consider $n = 3$. If $A = \{a, b, c\}$, then $A^{[3]} = \{abc, acb, bac, bca, cab, cba\}$. The cardinality of $A^{[3]}$ is at most $3! = 6$. A is rewritable precisely when $A^{[3]}$ contains less than six different elements. A semigroup S satisfies P_3 precisely when the value of each of the words $abc, acb, \ldots$ equals the value of another word in this set for every three-element subset A of S. Of course, in such a case $|A^{[3]}| \leq 3$ for every A.

2. Classification of permutational classes

In this section we classify all three-element subsets of cancellative semigroups up to permutational 3-isomorphisms. Without loss of generality, we can assume

that $A = \{a, b, c\}$ is our subset of cardinality 3. We classify A according to the cardinality of $A^{[3]}$. Theorem 1 shows that there exist exactly nineteen three-element subsets that are not permutationally 3-isomorphic.

Theorem 1. *In cancellative semigroups a three-element subset* $A = \{a, b, c\}$ *can have the following nineteen types of permutational* 3*-isomorphism:*

(1) $abc = acb = bac = bca = cab = cba$ (*all elements of* A *commute*);
(2) $abc = bac = bca$ *and* $acb = cab = cba$ (*two pairs of elements of* A *commute*);
(3) $abc = bac = cab = cba$ *and* $acb = bca$ (*one pair of elements of* A *commutes*);
(4) $abc = bca = cab$ *and* $acb = bac = cba$;
(5) $abc = bac$, $cab = cba$, *and* $acb = bca$ (*one pair of elements of* A *commutes*);
(6) $abc = bac = cab = cba$, *with* acb *and* bca *isolated* (*one pair of elements of* A *commutes*);
(7) $abc = bca$, $bac = cab$ *and* $acb = cba$;
(8) $abc = cba$, $acb = bca$, *and* $bac = cab$;
(9) $acb = bac = cba$, $bca = cab$, *and* abc *isolated*;
(10) $abc = bac$, $cab = cba$, *with* acb *and* bca *isolated* (*one pair of elements of* A *commutes*);
(11) $abc = bca = cab$, *with* acb, bac, *and* cba *isolated*;
(12) $abc = bca$, $acb = bac$, *with* cab *and* cba *isolated*;
(13) $abc = bca$, $acb = cba$, *with* bac *and* cab *isolated*;
(14) $abc = bca$, $bac = cab$, *with* acb *and* cba *isolated*
(15) $abc = bca$, $bac = cba$, *with* acb *and* cab *isolated*;
(16) $abc = cba$, $acb = bca$, *with* bac *and* cab *isolated*;
(17) $abc = bca$ *with* acb, bac, cab, *and* cba *isolated*;
(18) $abc = cba$ *with* acb, bac, bca, *and* cab *isolated*;
(19) *all products* abc, acb, bac, bca, cab, *and* cba *are isolated.*

No two of nineteen types are permutationally 3*-isomorphic. For each of them there exists a finite group* G *and a three-element subset* A *of* G *such that* A *belongs to the given type.*

Proof. Clearly, $|A^{[3]}| = 1$ if and only if $abc = acb = bac = bca = cab = cba$ or, equivalently, when all elements of A commute. This gives us type (1) of Theorem 1. Obviously, A belongs to type (1) if and only if any two elements of A commute.

Suppose that two pairs of elements of A commute. Without loss of generality (since we consider A up to [3]-isomorphisms), we may assume that $ab = ba$ and $ac = ca$. In this case $abc = bac = bca$ and $acb = cab = cba$, and hence $|A^{[3]}| = 2$. This gives us type (2). It is obvious that the converse statement holds: if A belongs to type (2), then exactly two (but not all three) pairs of elements of A commute. We use this simple observation in the sequel without special references.

If $|A^{[3]}| = 2$ and exactly one pair of elements of A commutes, we can assume, without loss of generality, that $ab = ba$. Then $abc = bac$ and $cab = cba$. If $abc \neq cab$, then each of the products acb and bca equals either abc or cab. If $acb = abc$, then $cb = bc$ contrary to our assumption about A. Thus, $acb = cab$, so that $ac = ca$, again contrary to our assumption about A. It follows that $abc = bac = cab = cba$. Since $|A^{[3]}| = 2$, we obtain $acb = bca$. This gives us type (3).

Let $|A^{[3]}| = 2$ and no elements of A commute. Let U and V be subsets of equal products in $A^{[3]}$. Clearly, $abc \neq bac$, $bca \neq bac$, $bca \neq cba$, $cab \neq cba$, and $cab \neq acb$, and so if $abc \in U$, then $bac \in V$, $bca \in U$, $cba \in V$, $cab \in U$, and $acb \in V$. This produces type (4).

Let $|A^{[3]}| = 3$. This rules out types (1) and (2), and hence at most one pair of the elements of A commutes. If one pair of the elements of A commutes, then, without loss of generality, let $ab = ba$. Then $abc = bac$ and $cab = cba$. Since only one pair of the elements of A commutes, $acb \notin \{cab, abc\}$. If $bac \neq cab$, then $acb = bca$, and we have type (5). If $bac = cab$, we obtain type (6).

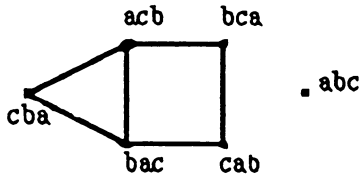
Let $|A|^{[3]}| = 3$ and no elements of A commute. First suppose that $A^{[3]}$ has no isolated products. Then no three products in $A^{[3]}$ can be equal, and so every product in $A^{[3]}$ equals one other product. As no elements of A commute, $abc \in \{bca, cab, cba\}$. Let $\varphi = (a, c, b)$ be the cyclic permutation of $\{a, b, c\}$. Applying φ to $bca = abc$ we obtain $abc = cab$. So, up to [3]-isomorphisms, we can exclude the case when $abc = cab$, considering only $abc = bca$. In such a case $cab = bac$, and hence $acb = cba$ and we obtain type (7). If $abc = cba$, then $bca \in \{acb, cab\}$. If $bca = acb$, the remaining two products bac and cab must be equal, and we have type (8). If φ is applied to the equality $bca = cab$, we obtain $abc = bca$, thus returning to an already considered case.

Suppose that $|A^{[3]}| = 3$, no elements of A commute, and one of the products in $A^{[3]}$ is isolated (that is, it does not equal any other product of a, b, and c). Without loss of generality, assume that abc is this isolated product. Let U, V, and W be subsets of $A^{[3]}$, each consisting of products with equal value. If $U = \{abc\}$ and $cba \in V$, then bca, $cab \in W$, as no two elements of A commute. For the same reason, bac, $acb \notin W$. This produces type (9).

Now let $|A^{[3]}| = 4$. Types (1) and (2) are impossible, and only one pair of elements of A may commute. If, without loss of generality, $ab = ba$, then $abc = bac$ and $cab = cba$, so that the products acb and bca are isolated. We obtain type (10).

Suppose that $|A^{[3]}| = 4$ and no elements of A commute. If there are three equal products, we can assume, without loss of generality, that abc is one of them. Then $abc \in \{bca, cab, cba\}$. If $abc = cba$, then these two products cannot equal a third one. It follows that $abc = bca = cab$, with the other three products isolated. This is type (11).

If no three products are equal, we have two isolated products and two pairs



of equal products. Without loss of generality, let abc be isolated. In the above graph the adjacent vertices may be equal, while the nonadjacent vertices are not equal.

Choosing the second isolated product among $\{acb, bac, bca, cab, cba\}$, we obtain six possible cases: (i) abc, acb, $bac = cba$, $bca = cab$; (ii) abc, bac, $acb = cba$, $bca = cab$; (iii) abc, bca, $acb = cba$, $bac = cab$; (iv) abc, cab, $acb = bca$, $bac = cba$; (v) abc, cba, $acb = bac$, $bca = cab$; (vi) abc, cba, $acb = bca$, $bac = cab$. The cyclic permutation $\varphi = (a, c, b)$ transforms (iii) into (iv), (i) into (12), (v) into (13), (ii) into (15), and (vi) into (16), while the transposition $\psi = (c, b)$ turns (iii) into type (14).

If $|A^{[3]}| = 5$, then two products of a, b, and c are equal and the remaining four isolated. Thus, no elements of A commute. Without loss of generality, let abc be not isolated. Then $abc = bca$, or $abc = cba$, or $abc = cab$. The first two equalities give types (17) and (18), and our cyclic permutation $\varphi = (a, c, b)$ turns the first equality into the last one.

Finally, if $|A^{[3]}| = 6$, then no two products in $A^{[3]}$ are equal, and we obtain type (19).

We have listed all possible types up to [3]-isomorphisms. It remains to prove that no two of them are [3]-isomorphic.

Any [3]-isomorphism preserves the cardinality of $A^{[3]}$, the number of products in each group of equal products, and the number of commuting pairs of elements. Thus types (1)–(6), (9)–(11), and (19) are not [3]-isomorphic to any other types. In type (7) one element commutes with any product of two other elements: $a(bc) = (bc)a$ and $a(cb) = (cb)a$, and [3]-isomorphisms preserve this property. Thus, types (7) and (8) are not [3]-isomorphic, and hence each of them is not [3]-isomorphic to any other type. The same argument shows that each of the types (17) and (18) is not [3]-isomorphic to any other type, type (16) is not [3]-isomorphic to types (12)–(15), and so (16) is not [3]-isomorphic to any other type. Type (13) differs from other types by containing an element that commutes with both products of the remaining elements: $a(bc) = (bc)a$ and $a(cb) = (cb)a$, while type (14) has an element commuting with only one product of the remaining two elements: $a(bc) = (bc)a$. Thus, types (13) and (14) are not [3]-isomorphic to other types. Types (12) and (15) are not [3]-isomorphic because the first factors of the isolated products are the same in (12) and different in (15). Clearly, this property is preserved under [3]-isomorphisms.

To see that each of the nineteen types can be realized by a three-element

subset of a finite group, we list a series of corresponding examples, where $G = S_9$, its elements written as products of disjoint cycles, with Δ denoting the identity element of S_9. Functions are written as right operators; that is, in a product fg the permutation f acts first.

(1) $a = \Delta$, $b = (123)$, $c = (132)$;
(2) $a = \Delta$, $b = (12)$, $c = (13)$;
(3) $a = (1234)$, $b = (1432)$, $c = (12)(34)$;
(4) $a = (1234)$, $b = (24)$, $c = (14)(23)$;
(5) $a = (123)$, $b = (123)(45)$, $c = (12)$;
(6) $a = (123)$, $b = (132)$, $c = (12)$;
(7) $a = (123456789)$, $b = (147)(285)$, $c = (183426759)$;
(8) $a = (12)$, $b = (13)$, $c = (23)$;
(9) $a = (12)$, $b = (132)$, $c = (13)$;
(10) $a = (1234)$, $b = (13)(24)$, $c = (12)$;
(11) $a = (123)$, $b = (134)$, $c = (142)$;
(12) $a = (123)(45)$, $b = (12)(456)$, $c = (13)(46)$;
(13) $a = (123)(456)$, $b = (123546)$, $c = (1356)(24)$;
(14) $a = (123)$, $b = (234)$, $c = (124)$;
(15) $a = (123)(46)$, $b = (12)(45)$, $c = (13)(456)$;
(16) $a = (12)$, $b = (1234)$, $c = (1342)$;
(17) $a = (1234)$, $b = (1324)$, $c = (12)$;
(18) $a = (1234)$, $b = (14)$, $c = (1324)$;
(19) $a = (12)$, $b = (13)$, $c = (14)$.

This completes the proof of Theorem 1.

The classification given in Theorem 1 can be used to suggest (and solve) many meaningful problems. The following two sections serve as examples for that claim.

3. Structure of $R(3, 2)$-groups

A group is called an $R(3, n)$-group if $|A^{[3]}| \leq n$ for all of its three-element subsets A. We can assume that $1 \leq n \leq 6$. If $R(3, n)$ is the class of $R(3, n)$-groups, then $R(3, 1)$ is the class of abelian groups, by Theorem 2, $R(3, 2) = P_3$ (the class of all P_3-groups), $R(3, 5) = Q_3$ (the class of Q_3-groups), and $R(3, 6)$ is the class of all groups, so that $R(3, 1) \subset R(3, 2) = P_3 \subset R(3, 3) \subset R(3, 4) \subset R(3, 5) = Q_3 \subset R(3, 6)$. Since no structural description of Q_3-groups is known, descriptions of $R(3, 3)$ and $R(3, 4)$ can give insight into the structure of Q_3-groups. Theorem 2 suggests that $R(3, 3)$-groups G may be characterized by a weaker version of the condition $|G'| \leq 2$, where G' is the commutator subgroup of G. Indeed, $R(3, 3)$-groups turn out to be precisely those groups G, for which $|G'| \leq 3$. Our elementary proof of that fact is too long for this article.

Theorem 2. *A group is an $R(3, 2)$-group if and only if it is a P_3-group.*

Proof. As proved in [5], P_3-groups G are characterized by the condition $|G'| \leq 2$. Theorem 2 is trivial for abelian groups, and so we assume that our groups are nonabelian.

Necessity. Let G be a nonabelian $R(3, 2)$-group. Then there exist noncommuting elements $a, b \in G$. Let $A = \{a, b, ab\}$. Since $ab \neq ba$, no elements of A commute. Thus, A does not belong to the first three types, and hence it belongs to type (4). Since no permutation of $\{a, b, c\}$ changes the equalities of type (4), we can substitute $c = ab$ into them, obtaining $abab = baba$ and $aabb = abba = baab$, so that $(ab)^2 = (ba)^2$, $ab^2 = b^2a$, and $a^2b = ba^2$ for any noncommuting $a, b \in G$. These equalities hold if $ab = ba$, and so they hold for any elements of G. Thus, $a^2 \in Z(G)$ for every $a \in G$, where $Z(G)$ is the center of G. Therefore, $G/Z(G)$ is abelian, and hence $G' \subset Z(G)$. Using standard commutator identities $[xy, z] = [x, z]^y[y, z]$ and $[x, y] = [y, x^{-1}]^x$, we obtain $[a, b]^2 = [a, b]^a[a, b] = [a^2, b] = 1$, so that $[b, a] = [a, b]^{-1} = [a, b]$, and also $[a^{-1}, b] = [b, a]^{a^{-1}} = [b, a] = [a, b]$. Analogously, $[a, b^{-1}] = [b^{-1}, a] = [b, a] = [a, b]$ and $[a^{-1}, b^{-1}] = [a, b]$ for all $a, b \in G$.

Let $C(a) = \{x \in G | ax = xa\}$ denote the centralizer of a. Let c commute neither with a nor with b. If a, b, and c are three different elements, they must belong to one of the above types (1)–(4). As only a and b among these elements may commute, only types (3) and (4) are possible. In either case $abc = cab$. If $a = b$, then $ab = a^2 \in Z(G)$ and again $abc = cab$. Thus, $[a, c][b, c] = [a, c]^b[b, c] = [ab, c] = 1$, and hence $[a, c] = [b, c]^{-1} = [b, c]$. We proved that if $a, b, c \in G$ and c does not commute with a or b, then $[a, c] = [b, c]$.

Now let $a, b, c, d \in G$, where $[a, b] \neq 1$ and $[c, d] \neq 1$. Then b, $c \notin Z(G)$, and hence $C(b)$ and $C(c)$ are proper subgroups of G. Therefore, $C(b) \cup C(c) \neq G$, and so there exists $e \in G$ with $e \notin C(b) \cup C(c)$. Thus the commutators $[a, b]$, $[e, b]$, $[e, c]$, $[c, d]$ are different from 1, and hence $[a, b] = [e, b] = [e, c] = [d, c] = [c, d]$. It follows that G' contains at most one element different from 1, that is, $|G'| \leq 2$.

Sufficiency. Let $|G'| \leq 2$ for a group G. Since $ab = ba \Leftrightarrow ba^{-1} = a^{-1}b$ for any $a, b \in G$, we have $[a, b] = 1 \Leftrightarrow [b, a^{-1}] = 1$, and $|G'| \leq 2$ implies $[a, b] = [b, a^{-1}]$. Thus $a^{-1}b^{-1}ab = b^{-1}aba^{-1}$, so that

$$\begin{aligned}[a^2, b] &= a^{-2}b^{-1}a^2b = a^{-1}(a^{-1}b^{-1}ab)b^{-1}ab = a^{-1}[a, b]b^{-1}ab \\ &= a^{-1}[b, a^{-1}]b^{-1}ab = a^{-1}b^{-1}aba^{-1}b^{-1}ab = [a, b]^2 = 1.\end{aligned}$$

The last equality follows from $|G'| \leq 2$. Thus, $[a^2, b] = 1$, that is, $a^2 \in Z(G)$ for every $a \in G$.

Now let $A = \{a, b, c\}$ be a three-element subset of G. If two pairs of elements of A commute, then A belongs to either type (1) or (2). Suppose that only one pair of the elements of A commutes, say, $ab = ba$. Then $abc = bac$

and $cab = cba$. Now, $[a, c] \neq 1$, $[b^{-1}, c] \neq 1$ and $|G'| \leq 2$ imply $[a, c] = [b^{-1}, c]$. We have $[ab, c] = [a, c]^b[a, c] = [a, c][b, c] = 1$, since clearly G' is a subgroup of $Z(G)$. Thus $abc = cab$, and so $abc = bac = cab = cba$. Since $bc \neq cb$, none of these four products is either acb or bca. Now, $b^2 \in Z(G)$ shows that $acb = b^{-1}(bac)b = b^{-1}(cab)b = (b^{-1}ca)b^2 = b^2(b^{-1}ca) = bca$, and so A belongs to type (3).

If no elements of A commute, then, by $|G'| \leq 2$, $[a, b] = [b, c] = [c, a]$. Then $[a, c] = [b^{-1}, c]$, which, as we have just seen, implies $abc = cab$. Analogously, $[c, b] = [a^{-1}, b]$ implies $cab = bca$. Now $[a, b] = [c^{-1}, b]$ and $[c, a] = [b^{-1}, a]$ imply $acb = bac$ and $cba = acb$, so that we obtain type (4). This completes the proof of Theorem 2.

4. The characteristic subgroup of [3]-2-elements

An element a of a group G is called a [3]-n-*element* if, for any $b, c \in G$, $|\{a, b, c\}^{[3]}| \leq n$. For example, G is an $R(3, n)$-group if and only if it consists of [3]-n-elements. The [3]-1-elements are just the elements of the center, so they form the characteristic subgroup $Z(G)$. The [3]-6-elements constitute the entire group, again a characteristic subgroup. We may assume that $1 \leq n \leq 6$. For which other n is the set of all [3]-n-elements a characteristic (and hence normal) subgroup? Theorem 3 shows that this is so for $n = 2$. Another result of this nature was proved in [4].

Theorem 3. [3]-2-*elements of any group form a characteristic subgroup.*

Proof. Let N denote the set of all [3]-2-elements of a group G. Clearly, $Z(G) \subset N$, so that $N \neq \varnothing$. If $a \in N$, then for any $b, c \in G$, $|\{a^{-1}, b, c\}^{[3]}| = |(\{a, b^{-1}c^{-1}\}^{-1})^{[3]}| = |(\{a, b^{-1}, c^{-1}\}^{[3]})^{-1}| = |\{a, b^{-1}, c^{-1}\}^{[3]}| \leq 2$; hence $a^{-1} \in N$. Let $f: N \to N$ be an automorphism of G (in fact, f can be an endomorphism of G *onto* itself). If $a \in N$ and $b, c \in G$, then $b = f(b')$ and $c = f(c')$ for some $b', c' \in G$, so that $|\{f(a), b, c\}^{[3]}| = |f(\{a, b', c'\}^{[3]})| \leq |\{a, b', c'\}^{[3]}| \leq 2$, and hence $f(a) \in N$. Therefore, $f(N) \subset N$. It remains to prove that N is a subsemigroup of G.

Suppose that $a, b \in N$ and let $C = \{ab, x, y\}$, where $x, y \in G$. We must prove that $|C^{[3]}| \leq 2$. Since a and b are [3]-2-elements, we know that the sets $A = \{a, x, y\}$ and $B = \{b, x, y\}$ belong to types (1)–(4).

If a commutes with both x and y, premultiply all equalities in $B^{[3]}$ by a. Then move a to the right in each product, until it stands to the left of b. For example, if $xby = xyb$ is one of the equalities in B, we obtain first $axby = axyb$ and then $x(ab)y = xy(ab)$. Thus, C satisfies the same type of equalities as B does, which shows that C belongs to one of (1)–(4). Analogously, if b commutes with both x and y, then C belongs to one of (1)–(4). Therefore, we can assume now that neither a nor b commutes with both x and y.

An easy consequence of types (1)–(4) is that if a set $\{a, b, c\}$ contains a [3]-2-element and c does not commute with a and b, then it commutes with their product ab. Indeed, the only commuting pair of elements in the set $\{a, b, c\}$ may be $ab = ba$. Hence $\{a, b, c\}$ belongs to either (3) or (4). In both cases $abc = cab$, so that c commutes with ab. We use this simple consequence many times in the sequel. For example, if both a and b do not commute with either x or y, then ab commutes with x and y, and hence C satisfies (2). So we can assume from now on that at least one of the elements a and b commutes with either x or y, but not with both x and y.

Now we consider two major cases: when $xy = yx$ and when $xy \neq yx$.

Let $xy = yx$. If both a and b commute with x or both a and b do not commute with x, then ab commutes with x, and hence two pairs of elements in C commute and C satisfies (2). If x is replaced with y here, we arrive at the same conclusion. It remains to look at the case when a commutes with exactly one of the elements x or y, while b commutes with the other element. Without loss of generality, we can assume $ax = xa$ and $by = yb$. If $ab \neq ba$, then each of the sets $\{a, b, x\}$ and $\{a, b, y\}$ has exactly one commuting pair of elements, and hence each of them belongs to type (3). Thus, $axb = xab = bax = bxa$, $abx = xba$, $bya = yba = aby = ayb$, and $bay = yab$. It follows that $(ab)yx = (ab)xy = (abx)y = (xba)y = x(bay) = x(yab) = xy(ab) = yx(ab)$ and $x(ab)y = (xab)y = (bax)y = (ba)xy = (ba)yx = (bay)x = (yab)x = y(ab)x$, and hence C satisfies (3). If $ab = ba$, then by does not commute with a and x, so that $\{a, by, x\}$ satisfies (3), whence $ax(by) = xa(by) = (by)ax = (by)xa$ and $a(by)x = x(by)a$. It follows that $(ab)xy = (ab)yx = a(by)x = x(by)a = x(yb)a = xy(ba) = xy(ab) = yx(ab)$, and hence C satisfies (3).

Now let $xy \neq yx$ and let a commute with one of the elements x or y, while b commutes with the other of these elements. Without loss of generality, let $ax = xa$ and $yb = by$. Then y does not commute with a and bx, and hence $a(bx)y = ya(bx)$. Analogously, x does not commute with ya and b, so that $x(ya)b = (ya)bx$. It follows that $(ab)xy = y(ab)x = xy(ab)$. Now y does not commute with a and x, and x does not commute with b and y, so that $axy = yax$ and $byx = xby$. Thus $yx(ab) = y(xa)b = y(ax)b = (yax)b = (axy)b = ax(yb) = ax(by) = a(xby) = a(byx) = (ab)yx$. Also $x(ab)y = (xa)by = (ax)by = a(xby) = (ab)yx$. Therefore, C satisfies (4).

Now suppose that $xy \neq yx$ and exactly one of the elements a and b commutes with exactly one of the elements x and y. Without loss of generality assume that a or b commutes with x. Let $ax = xa$. Since y does not commute with a and b, nor x with ya and b, we obtain $y(ab) = (ab)y$ and $x(ya)b = (ya)bx$. Thus, $x((ab)y) = x(y(ab)) = x(ya)b = (ya)bx = (y(ab))x = ((ab)y)x$. No elements of B commute, and hence B satisfies (4), so that $bxy = xyb$. The only commuting elements of A are a and x, and hence A satisfies (3). It follows that $axy = yax$. Thus, $a(bxy) = a(xyb) = (axy)b = (yax)b = y(ax)b = y(xa)b$. Therefore, $x(ab)y = xy(ab) = y(ab)x = (ab)yx$ and $(ab)xy = yx(ab)$, so that C satisfies (3). This proves Theorem 3.

References

1. R. D. Blyth and D. J. S. Robinson, *Recent progress on rewritability in groups*, Group Theory (Proc. of the 1987 Singapore Conf.), de Gruyter, Berlin, 1988.
2. L. V. Brailovsky and G. A. Freiman, *On two-element subsets in groups*, Ann. New York Acad. Sci., vol. 373, 1981, New York Acad. Sci., New York, pp. 183–190.
3. ____, *On a product of finite subsets in a torsion-free group*, J. Algebra **130** (1990), 462–476.
4. L. V. Brailovsky, G. A. Freiman, and M. Herzog, *Special elements in groups*, Group Theory (Proc. 2nd Internat. Conf., Bressanone, Italy 1989), Suppl. Rend. Circ. Mat. Palermo, II. Ser. **23** (1990), 33–42.
5. M. Curzio, P. Longobardi, and M. Maj, *Su di un problema combinatorio in teoria dei gruppi*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **74** (1983), 136–142.
6. G. A. Freiman, *Foundations of a structural theory of set addition*, Kazan, 1966 (Russian); English transl.: Trans. Math. Monographs, Amer. Math. Soc., Providence, RI, 1973.
7. ____, *Groups and the inverse problems of the additive set theory*, Number-Theoretic Investigations of the Markov Spectrum and the Structure Theory of Set Addition, Kalinin Univ., Moscow, 1973, pp. 175–183. (Russian)
8. ____, *On two- and three-element subsets of groups*, Aequationes Math. **22** (1981), 140–152.
9. ____, *What is the structure of K if $K + K$ is small*? Lecture Notes in Math., vol. 1240, Springer-Verlag, New York, 1987, pp. 109–134.
10. G. A. Freiman and B. M. Schein, *Group and semigroup theoretic considerations inspired by inverse problems of the additive number theory*, Lecture Notes in Math., vol. 1320, Springer-Verlag, New York, 1988, pp. 121–140.

School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540

School of Mathematical Sciences, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel-Aviv University, Ramat Aviv, Tel-Aviv, Israel

Department of Mathematical Sciences, University of Arkansas, Fayetteville, Arkansas 72701