# Miscellaneous results on sum-sets in ordered semigroups and magmas

Salvatore Tringali

# MISCELLANEOUS RESULTS ON SUM-SETS IN ORDERED SEMIGROUPS AND MAGMAS

SALVATORE TRINGALI

Abstract. We generalize recent results by G.A. Freiman, M. Herzog and coauthors on the structure theory of set addition from the context of linearly (i.e., strictly and totally) ordered groups (LOGs) to the one of linearly ordered semigroups (LOSs). In particular, we find that, in a LOS, the commutator and the normalizer of a finite set are equal to each other. On the road to this goal, we also extend an old lemma of B.H. Neumann on commutators of LOGs to the setting of LOSs and classical lower bounds on the size of sum-sets of finite subsets of LOGs to linearly ordered magmas. The whole is accompanied by a number of examples, one of these including a proof that the multiplicative semigroup of all upper (respectively, lower) triangular matrices with positive real entries is linearly orderable.

## 1. Introduction

Semigroups and magmas are ubiquitous in mathematics. Apart from being a subject of continuous interest to algebraists, they are the natural framework for the introduction of several broadly-scoped concepts and for the development of some large parts of theories traditionally presented in somewhat richer settings. Semigroups serve, for instance, as fundamental models for linear time-invariant systems and, as a result of the pioneer work of Hille and Phillips on their use in functional analysis [7], have been successfully applied for decades to the study of partial [5] and stochastic [15] differential equations (e.g., in relation to the method of strongly continuous one-parameter semigroups). Also, finite semigroups have been of primary importance in theoretical computer science since the 1950s due to the their natural link with finite automata.

Our personal interest in semigroups is related here to some recent results by G.A. Freiman, M. Herzog and collaborators on the structure theory of sum-sets in the (non-abelian) setting of linearly (i.e., strictly and totally) ordered groups, which the authors refer to simply as ordered groups [6]. This is an active area of research, with notable applications, e.g., to additive combinatorics [14], Freiman's structure theory [13], invariant measures [2], and spectral gaps [3]. The present work fits into this background and aims to be a contribute to the efforts of extending some parts of the theory from the scenery of groups to the one of semigroups (and indeed of magmas). Specifically, our first result is as follows:

**Corollary 1.** *Let $\mathfrak{A} = (A, \cdot, \preceq)$ be a linearly ordered semigroup (written multiplicatively) and $a, b \in \mathfrak{A}$. If $a^n b = ba^n$ for some $n \in \mathbb{N}^+$, then $ab = ba$.*

Corollary 1 is actually a generalization of an old lemma by N.H. Neumann [12] on commutators of linearly ordered groups, appearing as Lemma 2.2 in [6]; we prove it in Section 2.3.

2010 *Mathematics Subject Classification.* 06A07, 06F05, 20M10, 20N02.

*Key words and phrases.* Sum-sets, product-sets, ordered magmas, ordered semigroups, Freiman's theory.

The author is funded from the European Community's 7th Framework Programme (FP7/2007-2013) under Grant Agreement No. 276487 (project ApProCEM).

The next proposition is an extension of classical lower bounds on the size of sum-sets of finite subsets of linearly ordered groups to the setting of linearly ordered magmas.

**Proposition 1.** *Suppose that $\mathfrak{A} = (A, \cdot, \preceq)$ is a linearly ordered magma (written multiplicatively). Pick $n \in \mathbb{N}^+$ and let $S_1, S_2, \ldots, S_n$ be nonempty finite subsets of $\mathfrak{A}$. Then*

$$|(S_1 S_2 \cdots S_n)_{\mathrm{P}}| \ge 1 - n + \textstyle\sum_{i=1}^{n} |S_i| \tag{1}$$

*for any given parenthetization $\mathrm{P}$ of $\mathfrak{A}$ of length $n$.*

The reader might want to consult [4] and the references therein for similar results in the context of arbitrary groups (notably including the Cauchy-Davenport theorem). Proposition 1 is proved in Section 2.3. Here, as is expected, we use $\ge$ (and its dual $\le$) for the standard order of the real numbers (unless an explicit statement to the contrary) and, if $S$ is a set, we denote by $|S|$ the cardinality of $S$. More notation and terminology used in this introduction without explanation will be clarified below, in Section 2.1.

We give a couple of applications of Proposition 1, none of them covered by less general formulations of the same result such as the classical one presented in [6] for linearly ordered groups. One of these applications concerns the set of all upper (respectively, lower) triangular matrices with positive real entries, which we prove to be a linearly orderable semigroup (with respect to the usual matrix multiplication) in Example 5 of Section 2.2. In this respect, we raise the question (open to us) whether the same holds true for the set of all matrices which are a (finite) product of upper or lower triangular matrices with positive real entries.

Lastly, we establish the following:

**Proposition 2.** *Let $\mathfrak{A} = (A, \cdot, \preceq)$ be a linearly ordered semigroup (written multiplicatively) and $S$ a nonempty finite subset of $\mathfrak{A}$ of size $m$. If $y \in \mathfrak{A} \setminus \mathrm{C}_{\mathfrak{A}}(S)$, then*

$$|yS \cup Sy| \ge m + 1. \tag{2}$$

*In particular, there exist $a, b \in S$ such that $ya \notin Sy$ and $by \notin yS$.*

Proposition 2 is a generalization of [6, Proposition 2.4]. We prove it in Section 3. Finally we mention the following interesting result concerning linearly ordered semigroups, which in turn generalizes [6, Corollary 1.5] and is a straightforward consequence of Proposition 2.

**Corollary 3.** *If $S$ is a finite subset of a linearly ordered semigroup $\mathfrak{A}$, then $\mathrm{N}_{\mathfrak{A}}(S) = \mathrm{C}_{\mathfrak{A}}(S)$.*

## 2. Definitions, examples and basic properties

The present section is divided into three parts. First, we fix notation and terminology and recall the definitions of ordered (and orderable) magmas, semigroups and groups. Then, we mention some relevant examples for each of these structures. Finally, we derive a few basic properties that will be used to prove, later in Section 3, our main results.

### 2.1. Notation and terminology.

For all purposes and intents, and especially to avoid misunderstandings due to different conventions, let us first clarify some basic points and recall a few definitions. Our main references for this section are [1] and [8]. In particular, for order-theoretic concepts used here but not defined, the reader should consult [8, § 1.3].

Given a set $A$, an order on $A$ is a binary relation $\preceq$ on $A$ which is reflexive, antisymmetric and transitive. One then refers to the pair $(A, \preceq)$ as a poset and writes $a \prec b$ for $a, b \in A$ to mean that $a \preceq b$ and $a \ne b$. If $(A, \preceq)$ is a poset, we denote by $\preceq_{\mathrm{op}}$ the dual order of $\preceq$, defined by taking $a \preceq_{\mathrm{op}} b$ for $a, b \in A$ if and only if $b \preceq a$.

**Definition 1.** A magma is a pair $\mathfrak{A} = (A, \star)$, consisting of a (possibly empty) set $A$, the magma carrier, and a binary operation $\star : A \times A \to A$, the magma product.

Note that [8, § 1.1] refers to magmas as groupoids. A magma $\mathfrak{A} = (A, \star)$ is associative if $\star$ is associative, i.e. $a \star (b \star c) = (a \star b) \star c$ for all $a, b, c \in A$; abelian if $a \star b = b \star a$ for all $a, b \in A$; and unital if there exists a distinguished element $e \in A$ (which is, in fact, unique and called the magma identity) such that $a \star e = e \star a = a$ for every $a \in A$. An associative magma is a semigroup and a unital semigroup is identified with a monoid, which is formally a triple of type $(A, \star, e)$, where $(A, \star)$ is a semigroup and $e \in A$ the identity thereof. Something analogous holds for groups, formally defined as 4-tuples of type $(A, \star, \sim, e)$ for which $(A, \star, e)$ is a monoid and $\sim$ is a unary operation $A \to A$ such that $a \star (\sim a) = (\sim a) \star a = e$ for every $a \in A$.

**Definition 2.** An ordered magma is a pair of the form $(\mathfrak{A}, \preceq)$, or equivalently a triple of type $(A, \star, \preceq)$, where i) $\preceq$ is an order on $A$ and ii) $a \star c \preceq b \star c$ and $c \star a \preceq c \star b$ for all $a, b, c \in A$ with $a \preceq b$. If $(\mathfrak{A}, \preceq)$ is such a pair, one says that $\mathfrak{A}$ is ordered by $\preceq$. In particular, $(\mathfrak{A}, \preceq)$ is a totally ordered magma if $\preceq$ is total; a strictly ordered magma if $a \star c \prec a \star c$ and $c \star a \prec c \star b$ for all $a, b, c \in A$ with $a \prec b$; and a linearly ordered magma if it is both strictly and totally ordered. Accordingly, $\mathfrak{A}$ is said to be totally orderable in the first case, strictly orderable in the second, and linearly orderable in the latter. Also, one says that $\mathfrak{A}$ is totally, strictly, or linearly ordered by $\preceq$ as appropriate.

Since semigroups and monoids can be viewed as a special kind of magmas (forgetting some of their structure as appropriate), one will safely speak of ordered semigroups, totally orderable monoids, etc. Similar considerations apply to groups, provided that an ordered group is defined as a 5-tuple of type $(A, \star, \sim, e, \preceq)$ such that $(A, \star, \sim, e)$ is a group, $(A, \star, e, \preceq)$ is an ordered monoid, and $(\sim b) \preceq (\sim a)$ for all $a, b \in A$ with $a \preceq b$.

As is usual, if the magma product is written multiplicatively as $\cdot$ and there is no likelihood of confusion, we use the notation $ab$ instead of $a \cdot b$. Moreover, if $\mathfrak{A}$ is a magma and $A$ its carrier, we abuse notation and write $a \in \mathfrak{A}$ to mean that $a \in A$, especially in contexts or statements implicitly involving, along with $a$, the structure of $\mathfrak{A}$. This principle applies also to sets (and not only to elements) and to other structures such as posets, semigroups, ordered groups, etc.

**Remark 1.** If $(A, \star, \preceq)$ is an ordered, totally ordered, or strictly ordered magma, then the same is also true for $(A, \star, \preceq_{\mathrm{op}})$, $(A, \star_{\mathrm{op}}, \preceq)$ and $(A, \star_{\mathrm{op}}, \preceq_{\mathrm{op}})$, where $\preceq_{\mathrm{op}}$ is the dual order of $\preceq$ and $\star_{\mathrm{op}}$ the dual product of $\star$, i.e. the binary operation $A \times A \to A : (a, b) \mapsto b \star a$.

With this in mind, let $\mathfrak{A} = (A, \star)$ be a magma. Given $n \in \mathbb{N}^+$, we define recursively $\mathcal{P}_1 := \{\mathrm{id}_A\}$, where $\mathrm{id}_A$ is the map $A \to A : a \to a$, and $\mathcal{P}_{n+1} := \mathcal{P}^{\mathrm{L}}_{n+1} \cup \mathcal{P}^{\mathrm{R}}_{n+1}$, where

1. $P^{\mathrm{L}}_{n+1}$ is the set of all functions $\mathfrak{A}^{n+1} \to \mathfrak{A}$ sending, for some $f \in \mathcal{P}_n$, a $(n+1)$-tuple $(a_1, a_2, \ldots, a_{n+1})$ to the product $a_1 \star f(a_2, a_3, \ldots, a_{n+1})$.
2. $P^{\mathrm{R}}_{n+1}$ is the set of all functions $\mathfrak{A}^{n+1} \to \mathfrak{A}$ mapping, for some $f \in \mathcal{P}_n$, a $(n+1)$-tuple $(a_1, a_2, \ldots, a_{n+1})$ to the product $f(a_1, a_2, \ldots, a_n) \star a_{n+1}$.

For $n \in \mathbb{N}^+$, we then refer to an element P of $\mathcal{P}_n$ as a parenthetization of $\mathfrak{A}$ of length $n$, or also a $n$-parenthetization of $\mathfrak{A}$. Moreover, for $a_1, a_2, \ldots, a_n \in \mathfrak{A}$, we write $(a_1 \star a_2 \star \cdots \star a_n)_{\mathrm{P}}$ in place of $\mathrm{P}(a_1, a_2, \ldots, a_n)$ and, whenever $S_1, S_2, \ldots, S_n$ are nonempty subsets of $A$, we let

$$(S_1 \star S_2 \star \cdots \star S_n)_{\mathrm{P}} := \{(a_1 \star a_2 \star \cdots \star a_n)_{\mathrm{P}} : a_1 \in S_1, a_2 \in S_2, \ldots, a_n \in S_n\}. \tag{3}$$

If $\mathfrak{A}$ is a semigroup or $n \leq 2$, then $(a_1 \star a_2 \star \cdots \star a_n)_{\mathrm{P}}$ does not really depend on P, and we can simply write it as $a_1 \star a_2 \star \cdots \star a_n$; at the end of the day, parenthetization is, in fact, just a formal

way to deal with long products in a magma whose operation is not associative. In particular, if $a \in \mathfrak{A}$ and $S \subseteq \mathfrak{A}$, we use $a \star S$ in place of $\{a\} \star S$ (and similarly with $S \star a$). These notations are then simplified in the obvious way in the case where $\mathfrak{A}$ is written multiplicatively (and there is no danger of ambiguity).

Finally, if $\mathfrak{A} = (A, \star)$ is a magma, or $\mathfrak{A} = (A, \star, \preceq)$ is an ordered magma, and $S$ is a subset of $\mathfrak{A}$, we use $\mathrm{C}_{\mathfrak{A}}(S)$ for the centralizer of $S$ in $\mathfrak{A}$, i.e. the set of all $a \in \mathfrak{A}$ such that $a \star y = y \star a$ for every $y \in S$, and $\mathrm{N}_{\mathfrak{A}}(S)$ for the normalizer of $S$ in $\mathfrak{A}$, i.e. the set $\{a \in \mathfrak{A} : a \star S = S \star a\}$.

2.2. **Some examples.** To start with, we exhibit a totally orderable semigroup which is not linearly orderable. Then, we mention some special classes of linearly orderable groups, some linearly orderable monoids (respectively, semigroups) which are not groups (respectively, monoids), and a linearly orderable magma which is not a semigroup.

**Example 1.** Every set $A$ can be turned into a semigroup by the operation $\star : A \times A \to A : (a, b) \to a$; some authors refer to $(A, \star)$ as the left zero semigroup (e.g., see [8, p. 3]). It is trivial that, if $\preceq$ is a total order on $A$, then $(A, \star, \preceq)$ is a totally ordered semigroup. However, since $a \star b = a \star c$ for all $a, b, c \in A$, it is clear that $(A, \star)$ is not linearly orderable if $|A| \geq 2$.

**Example 2.** A notable example of strictly totally ordered groups is provided by torsion-free groups, as first proved by F.W. Levi in [10]. In the same lines of thought, K. Iwasawa [9], A.I. Mal'cev [11] and B.H. Neumann [12] showed, independently from each other, that the class of torsion-free nilpotent groups is contained in the class of strictly totally orderable groups. These are already mentioned in [6], along with further references to existing literature on the subject.

**Example 3.** As for strictly totally ordered monoids which are not strictly totally ordered groups, one can consider, for instance, the set $\mathbb{R}^+$ of all positive real numbers with the ordinary multiplication as the monoid operation, or a submonoid of this such as the positive integers not divisible by any member of a given set $S$ of (natural) primes or, in alternative, divisible only by primes in $S$. On the other hand, the same $\mathbb{R}^+$ with the usual addition as an operation provides a simple example of a strictly totally orderable semigroup which is not even a monoid.

**Example 4.** Let $A$ be the open interval $]1, +\infty[$ of the real line and $\star$ the operation $A \times A \to A : (a, b) \mapsto a^b$. Then, $(A, \star)$ is a linearly orderable magma (just consider the usual order on the real numbers and restrict it to $A$), but not a semigroup.

The next example might be interesting in its own right: Not only it gives a class of strictly totally ordered semigroups which are neither abelian (the semigroups in Example 3 are all abelian in character) nor groups in disguise (at least in general), it also shows that, for each $n \in \mathbb{N}^+$, the set of all $n$-by-$n$ upper (respectively, lower) triangular matrices with positive real entries is a strictly totally orderable semigroup when endowed with the usual row-by-column multiplication (which applies especially to matrices of positive integers).

**Example 5.** Let $\mathfrak{A}$ be a semiring, i.e. a 4-tuple of type $(A, +, \cdot, 0)$ consisting of a (nonempty) set $A$, associative operations $+$ and $\cdot$ from $A \times A$ to $A$ (referred to, respectively, as the semiring addition and the semiring multiplication), and a distinguished element $0 \in A$ such that

i. $(A, +, 0)$ is an abelian monoid and $(A, \cdot)$ a semigroup.
ii. multiplication by 0 annihilates $A$, i.e. $0 \cdot a = a \cdot 0 = 0$ for every $a \in A$.
iii. multiplication distributes over addition (from the left and the right), i.e. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in A$.

One refers to $(A,+,0)$ and $(A,\cdot)$ as the additive monoid and the multiplicative semigroup of $\mathfrak{A}$, respectively, and $\mathfrak{A}$ is said to be unital if $(A,\cdot)$ is a unital semigroup. A semiring is similar to a ring, except for the fact that elements in semirings do not necessarily have an inverse for the addition. We denote by $\mathfrak{A}_0$ the set of non-zero-divisors of $\mathfrak{A}$, i.e. the elements $a \in A$ such that $a \cdot b, b \cdot a \neq 0$ for every $b \in A \setminus \{0\}$. The elements of $\mathfrak{A} \setminus \mathfrak{A}_0$ are called the zero divisors of $\mathfrak{A}$ (note that, for our convenience, we are including 0 among the zero divisors) and $\mathfrak{A}$ has no zero divisors if $\mathfrak{A}_0 = A \setminus \{0\}$.

We say that $\mathfrak{A}$ is an orderable (respectively, totally orderable) semiring if there exists an order (respectively, a total order) $\preceq$ on $A$ such that $(A,+,\preceq)$ and $(A,\cdot,\preceq)$ are ordered semigroups. When this occurs, the pair $(\mathfrak{A},\preceq)$, or equivalently the 5-tuple $(A,+,\cdot,0,\preceq)$, is said an ordered (respectively, totally ordered) semiring. If, on the other hand, the following conditions hold:

i. $(A,+,\preceq)$ is a strictly ordered semigroup;
ii. if $a,b \in A$ and $a \prec b$, then $a \cdot c \prec b \cdot c$ and $c \cdot a \prec c \cdot b$ for every $c \in \mathfrak{A}_0$,

then $\mathfrak{A}$ is said to be strictly orderable and $(\mathfrak{A},\preceq)$ is called a strictly ordered semiring. Lastly, we say that $\mathfrak{A}$ is linearly orderable if it is both strictly and totally orderable, and accordingly we refer to $(\mathfrak{A},\preceq)$ as a linearly ordered semiring. The class of linearly ordered semirings includes, as notable examples, the nonnegative real numbers (equipped with the standard order and the usual algebraic structure) and interesting subsemirings of this one such as the nonnegative rationals or the nonnegative integers.

Upon these premises, assume that $(\mathfrak{A},\preceq)$ is an ordered semiring with $\mathfrak{A} = (A,+,\cdot,0)$. We denote by $\mathfrak{A}^+$ the set $\{a \in \mathfrak{A} : 0 \prec a\}$. Note that, if $\mathfrak{A}$ has no zero divisors and $\preceq$ is total, one can assume without loss of generality that $\mathfrak{A}^+ = A \setminus \{0\}$. If $n$ is a fixed positive integer, we then use $\mathcal{M}_n(A)$ for the set of all $n$-by-$n$ matrices with entries in $A$. Together with the usual operations of entry-wise addition and row-by-column multiplication implied by the algebraic structure of $\mathfrak{A}$, $\mathcal{M}_n(A)$ becomes a semiring in its own right, referred to as the semiring of the $n$-by-$n$ matrices over $\mathfrak{A}$ and indicated here by $\mathcal{M}_n(\mathfrak{A})$.

Now, suppose for the sequel that $\mathfrak{A}$ has no zero divisors and denote by $\mathrm{U}_n(\mathfrak{A}^+)$ the subsemigroup of the multiplicative semigroup of $\mathcal{M}_n(\mathfrak{A})$ consisting of all upper triangular matrices whose entries are elements of $\mathfrak{A}^+$. Note that $\mathrm{U}_n(\mathfrak{A}^+)$ is not, in general, a group (e.g., the inverse of a regular 2-by-2 matrix with positive real entries has not positive real entries), and not even a monoid unless $\mathfrak{A}$ is unital. More interestingly, $\mathrm{U}_n(\mathfrak{A}^+)$ is linearly orderable, as we are going to prove by the following theorem.

**Theorem 1.** $\mathrm{U}_n(\mathfrak{A}^+)$ *is a linearly orderable semigroup.*

*Proof.* Set $I_n := \{1,2,\dots,n\}$, $\Xi_n := \{(i,j) \in I_n \times I_n : i \leq j\}$ and define a binary relation $\leq_n$ on $\Xi_n$ by taking $(i_1,j_1) \leq_n (i_2,j_2)$ for $(i_1,j_1),(i_2,j_2) \in \Xi_n$ if and only if i) $j_1 - i_1 < j_2 - i_2$ or ii) $j_1 - i_1 = j_2 - i_2$ and $j_1 < j_2$. It is easily seen that $\leq_n$ is a total order. When combined with $\preceq$, this in turn defines a binary relation $\preceq_n^{\mathrm{U}}$ on $\mathrm{U}_n(\mathfrak{A}^+)$ as follows: If $\alpha = (a_{i,j})_{i,j=1}^n$ and $\beta = (b_{i,j})_{i,j=1}^n$ belong to $\mathrm{U}_n(\mathfrak{A}^+)$, then $\alpha \preceq_n^{\mathrm{U}} \beta$ if and only if i) $\alpha = \beta$ or ii) there exists $(i_0,j_0) \in \Xi_n$ such that $a_{i_0,j_0} \prec b_{i_0,j_0}$ and $a_{i,j} = b_{i,j}$ for all $(i,j) \in \Xi_n$ such that $(i,j) <_n (i_0,j_0)$.

It is routine to check that $\preceq_n^{\mathrm{U}}$ is a total order. Reflexivity and antisymmetry are quite clear. To prove that $\preceq_n^{\mathrm{U}}$ is transitive, let $\alpha = (a_{i,j})_{i,j=1}^n$, $\beta = (b_{i,j})_{i,j=1}^n$ and $\gamma = (c_{i,j})_{i,j=1}^n$ be matrices of $\mathrm{U}_n(\mathfrak{A}^+)$ such that $\alpha \preceq_n^{\mathrm{U}} \beta$ and $\beta \preceq_n^{\mathrm{U}} \gamma$. The claim is obvious if $\alpha = \beta$ or $\beta = \gamma$. Otherwise, there exist $(i_1,j_1),(i_2,j_2) \in \Xi_n$ such that $a_{i_1,j_1} \prec b_{i_1,j_1}$, $b_{i_2,j_2} \prec c_{i_2,j_2}$ and $a_{i,j} = b_{i,j} = c_{i,j}$ for all $(i,j) \in \Xi_n$ with $(i,j) <_n (i_0,j_0)$, where $(i_0,j_0)$ denotes the minimum of $(i_1,j_1)$ and $(i_2,j_2)$ in $(\Xi_n,\leq_n)$. Since $a_{i_0,j_0} \prec c_{i_0,j_0}$, we have done.

Thus, we are left to prove that $(\mathrm{U}_n(\mathfrak{A}^+), \preceq_n^{\mathrm{U}})$ is a linearly ordered semigroup. To see why, let $\alpha$, $\beta$ and $\gamma$ be as above and suppose $\alpha \prec_n \beta$. This means that there exists $(i_0, j_0) \in \Xi_n$ such that $a_{i_0,j_0} \prec b_{i_0,j_0}$ and $a_{i,j} = b_{i,j}$ for all $(i,j) \in \Xi_n$ with $(i,j) <_n (i_0,j_0)$. As a result, one has that $a_{i,k}c_{k,j} \preceq b_{i,k}c_{k,j}$ and $c_{i,k}a_{k,j} \preceq c_{i,k}b_{k,j}$ for all $(i,j) \in \Xi_n$ and $k \in I_n$ such that $(i,k) \leq_n (i_0,j_0)$ and $(k,j) \leq_n (k,j_0)$, and indeed $a_{i_0,j_0}c_{j_0,j_0} \prec b_{i_0,j_0}c_{j_0,j_0}$ and $c_{i_0,i_0}a_{i_0,j_0} \prec c_{i_0,i_0}b_{i_0,j_0}$ for the fact that $(\mathfrak{A}, \preceq)$ is a linearly ordered semiring (to the effect that $\mathfrak{A}^+ = \mathfrak{A} \setminus \{0\}$ or $\mathfrak{A}^+ = \emptyset$). It follows that, for all $(i,j) \in \Xi_n$ with $(i,j) \leq_n (i_0,j_0)$,

$$\sum_{k=1}^n a_{i,k}c_{k,j} = \sum_{k=i}^j a_{i,k}c_{k,j} \preceq_n^{\mathrm{U}} \sum_{k=i}^j b_{i,k}c_{k,j} = \sum_{k=1}^n b_{i,k}c_{k,j} \tag{4}$$

and, similarly, $\sum_{k=1}^n c_{i,k}a_{k,j} \preceq_n^{\mathrm{U}} \sum_{k=1}^n c_{i,k}b_{k,j}$. In particular, these majorizations are equalities for $(i,j) <_n (i_0,j_0)$ and strict inequalities if $(i,j) = (i_0,j_0)$. This completes our proof by showing that $\alpha \cdot \gamma \prec_n \beta \cdot \gamma$ and $\gamma \cdot \alpha \prec_n \gamma \cdot \beta$. ∎

We refer to the order $\preceq_n^{\mathrm{U}}$ defined in the proof of Theorem 1 as the zig-zag order on $\mathrm{U}_n(\mathfrak{A}^+)$. If $\mathrm{L}_n(\mathfrak{A}^+)$ stands for the subsemigroup of the multiplicative semigroup of $\mathcal{M}_n(\mathfrak{A})$ consisting of all *lower* triangular matrices with entries in $\mathfrak{A}^+$, it is then straightforward to prove that $\mathrm{L}_n(\mathfrak{A}^+)$ is itself linearly orderable, as it is in fact linearly ordered by the binary relation $\preceq_n^{\mathrm{L}}$ defined by taking $\alpha \preceq_n^{\mathrm{L}} \beta$ for $\alpha, \beta \in \mathrm{L}_n(\mathfrak{A}^+)$ if and only if $\alpha^\top \preceq_n^{\mathrm{U}} \beta^\top$, where the superscript '$\top$' means 'transpose'. Provided that $\mathrm{T}_n(\mathfrak{A}^+)$ is the smallest subsemigroup of the multiplicative semigroup of $\mathcal{M}_n(\mathfrak{A})$ generated by $\mathrm{U}_n(\mathfrak{A}^+)$ and $\mathrm{L}_n(\mathfrak{A}^+)$, it is then natural to ask:

**Question 1.** Is $\mathrm{T}_n(\mathfrak{A}^+)$ a linearly orderable semigroup?

At present, we do not have an answer, but Carlo Pagano (Università di Roma Tor Vergata) observed, in a private communication, that $\mathcal{M}_n(\mathfrak{A}^+)$, i.e. the subsemigroup of the multiplicative semigroup of $\mathcal{M}_n(\mathfrak{A})$ consisting of *all* matrices with entries in $\mathfrak{A}^+$, is not in general linearly orderable. For a counterexample, let $\mathfrak{A}$ be the semiring of all nonnegative real numbers (with their standard algebraic structure) and take $\alpha$ as the $n$-by-$n$ matrix whose entries are all equal to 1 and $\beta$ as any $n$-by-$n$ matrix with positive entries each of whose columns sums up to $n$. Then, $\alpha^2 = \alpha\beta$ regardless as to whether $\alpha \neq \beta$.

New exemplars of linearly orderable magmas can now be obtained from the previous ones using, for instance, the construction outlined by the following:

**Example 6.** Suppose that $\mathcal{I} = (I, \leq)$ is a well-ordered set and let $\{(A_i, \star_i, \preceq_i)\}_{i \in \mathcal{I}}$ be a family of totally ordered magmas indexed by $\mathcal{I}$. Set $\mathfrak{A}_i = (A_i, \star_i, \preceq_i)$ for each $i \in I$ and take $A$ to be the Cartesian product of the $A_i$'s, that is the set of all functions $f : I \to \bigcup_{i \in I} A_i$ such that $f(i) \in A_i$ for each $i \in I$. Also, define $\star$ as the binary operation

$$A \times A \to A : (f,g) \mapsto \Big(I \to \textstyle\bigcup_{i \in I} A_i : i \mapsto f(i) \star_i g(i)\Big), \tag{5}$$

so that $(A, \star)$ is the magma direct product of the family $\{(A_i, \star_i)\}_{i \in \mathcal{I}}$. The product order on $A$ induced by the $\preceq_i$'s is not, in general, total. However, this is happily the case with the lexicographic order, herein denoted by $\preceq$, which is defined by taking $f \preceq g$ for $f, g \in A$ if (and only if) i) $f = g$ or ii) $f(i) \prec_i g(i)$ for some $i \in I$ and $f(j) = g(j)$ for every $j \in I$ with $j < i$. Furthermore, $\preceq$ is compatible with the operation $\star$, in the sense that $\mathfrak{A} = (A, \star, \preceq)$ becomes a totally ordered magma, and indeed a linearly ordered magma whenever $\mathfrak{A}_i$ is linearly ordered for each $i \in I$.

2.3. **A few useful properties.** We aim to derive a few elementary properties of ordered semigroups and magmas. All magmas in this section are written multiplicatively. In particular, if $\mathfrak{A}$ is a magma (or an ordered magma), $a$ an element of $\mathfrak{A}$, $n$ a positive integer and P a parenthetization of $\mathfrak{A}$ of length $n$, we use $(a^n)_{\mathrm{P}}$ for the $n$-fold product $\mathrm{P}(a, a, \ldots, a)$.

Our theorems here are essentially a generalization of some elementary properties reported in [6, § 2] in reference to linearly ordered groups.

**Theorem 2.** *Let $\mathfrak{A} = (A, \cdot, \preceq)$ be an ordered magma. The following holds:*

(i) *If $n \in \mathbb{N}^+$ and $\mathrm{P}$ is a $n$-parenthetization of $(A, \cdot)$, then $(a_1 a_2 \cdots a_n)_{\mathrm{P}} \preceq (b_1 b_2 \cdots b_n)_{\mathrm{P}}$ for all $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in \mathfrak{A}$ such that $a_1 \preceq b_1$, $a_2 \preceq b_2$, …, $a_n \preceq b_n$, and indeed $(a_1 a_2 \cdots a_n)_{\mathrm{P}} \prec (b_1 b_2 \cdots b_n)_{\mathrm{P}}$ if $\mathfrak{A}$ is strictly ordered and $a_i \prec b_i$ for each $i$.*

(ii) *If $a, b \in \mathfrak{A}$ and $a \preceq b$, then $(a^n)_{\mathrm{P}} \preceq (b^n)_{\mathrm{P}}$ for all $n \in \mathbb{N}^+$ and every $n$-parenthetization $\mathrm{P}$ of $(A, \cdot)$, and indeed $(a^n)_{\mathrm{P}} \preceq (b^n)_{\mathrm{P}}$ if $\mathfrak{A}$ is strictly ordered and $a \prec b$.*

(iii) *If $\cdot$ is associative and $a \in \mathfrak{A}$ is such that $a^2 \preceq a$, then $a^n \preceq a^m$ for all $m, n \in \mathbb{N}^+$ with $m \leq n$, and indeed $a^n \prec a^m$ if $\mathfrak{A}$ is strictly ordered, $a^2 \prec a$ and $m < n$.*

*Proof.* (i) If $n = 1$, the claim is obvious. If $n = 2$, then $a_1 \preceq b_1$ and $a_2 \preceq b_2$ implies, as $\mathfrak{A}$ is an ordered magma, that $a_1 a_2 \preceq b_1 a_2 \preceq b_1 b_2$, and indeed $a_1 a_2 \prec b_1 a_2 \prec b_1 b_2$ if $\mathfrak{A}$ is strictly ordered and $a_1 \prec b_1$, $a_2 \prec b_2$. Lastly, if $n \geq 3$, then there exists a parenthetization $\mathrm{Q}$ of $(A, \cdot)$ of length $(n-1)$ such that $(c_1 c_2 \cdots c_n)_{\mathrm{P}} = (c_1 \cdots c_{n-1})_{\mathrm{Q}} \cdot c_n$ or $(c_1 c_2 \cdots c_n)_{\mathrm{P}} = c_1 \cdot (c_2 \cdots c_n)_{\mathrm{Q}}$ for all $c_1, c_2, \ldots, c_n \in \mathfrak{A}$, from which the conclusion follows by a routine induction.

(ii) It is a straightforward consequence of the previous point.

(iii) Pick $a \in \mathfrak{A}$ and let $a^2 \preceq a$. Again by a routine induction, $a^n \preceq \ldots \preceq a^2 \preceq a$ for all $n \in \mathbb{N}^+$, and indeed $a^n \prec \ldots \prec a^2 \prec a$ if $\mathfrak{A}$ is strictly ordered, $a^2 \prec a$ and $n \geq 2$. ∎

Let $\mathfrak{A} = (A, \cdot)$ be a magma and pick $a \in \mathfrak{A}$. One says that $a$ is left (respectively, right) cancellable (with respect to $\cdot$) if the mapping $A \to A : x \mapsto ax$ (respectively, $A \to A : x \mapsto xa$) is one-to-one, and cancellable if it is both left and right cancellable. Then, $\mathfrak{A}$ is called cancellative if each one of its elements is cancellative. On another hand, we say that $a$ is idempotent if $a = a^2$ and periodic, when $\mathfrak{A}$ is a semigroup, if there exist $n, p \in \mathbb{N}^+$ such that $a^n = a^{n+p}$: One then refers to the smallest $n$ with this property as the index of $a$ and to the smallest $p$ relative to such an $n$ as the period of $a$. Clearly, the concept of period generalizes the notion of order from the setting of groups to that of semigroups. Then, we say that a semigroup is torsion-free if the only periodic elements of it are idempotent. The same definitions now apply to ordered magmas and semigroups, as appropriate, by implicit reference to the underlying algebraic structures.

**Remark 2.** A cancellative magma is linearly orderable if and only if it is totally orderable. Conversely, every linearly orderable magma is cancellative.

**Remark 3.** The unique idempotent element of a group is the identity, so that torsion-free groups are definitely a special kind of torsion-free semigroups.

The next theorem shows that, for $(A, \cdot, \preceq)$ an ordered semigroup and $a$ an element of $A$, the condition $a^2 \prec a$ plays the same role that $a \prec 1$ would play in an ordered group $(A, \cdot, ^{-1}, 1, \preceq)$, while being more general than the latter. Along with Remark 3, this highlights the importance of idempotents (at least in the setting of this paper) in the absence of an identity element.

**Theorem 3.** *Let $\mathfrak{A} = (A, \cdot, \preceq)$ be a linearly ordered semigroup.*

(i) *If $a \in \mathfrak{A}$ and $a^2 \prec a$, then $ab \prec b$ and $aba \prec b$ for all $b \in \mathfrak{A}$.*

(ii) *If $a, b \in \mathfrak{A}$ and $aba = b$, then $a^2 = a$.*

(iii) $\mathfrak{A}$ *is torsion-free.*

*Proof.* (i) Let $a, b \in \mathfrak{A}$ and assume $a^2 \prec a$. Then $a^2 b \prec ab$, and hence $ab \prec b$ thanks to Remark 2. It follows from Theorem 2 that $aba^2 \prec ba$, whence $aba \prec b$ again in the light of Remark 2.

(ii) Let $a, b \in \mathfrak{A}$ be such that $aba = b$. Due to Remark 1, we can suppose without loss of generality that $a^2 \preceq a$. The claim is then straightforward from the previous point (i).

(iii) It is immediate from Remark 1 and point (iii) of Theorem 2. ∎

We are now ready to prove the following:

**Theorem 4.** *Let $\mathfrak{A} = (A, \cdot, \preceq)$ be a linearly ordered semigroup and pick $a, b \in \mathfrak{A}$. If $ab \prec ba$, then $a^n b \prec a^{n-1}ba \prec \ldots \prec aba^{n-1} \prec ba^n$ for all $n \in \mathbb{N}^+$.*

*Proof.* Assume that $a^n b \prec a^{n-1}ba \prec \ldots \prec aba^{n-1} \prec ba^n$ for some $n \in \mathbb{N}^+$. Then, multiplying by $a$ on the left gives $a^{n+1}b \prec a^n ba \prec \ldots \prec a^2 ba^{n-1} \prec aba^n$, while multiplying by $a$ on the right yields $aba^n \prec ba^n$. Since $ab \prec ba$, the transitivity of $\preceq$ implies the claim by induction. ∎

**Corollary 1.** *Let $\mathfrak{A} = (A, \cdot, \preceq)$ be a linearly ordered semigroup and $a, b \in \mathfrak{A}$. If $a^n b = ba^n$ for some $n \in \mathbb{N}^+$, then $ab = ba$.*

*Proof.* It is an immediate consequence of Theorem 4 and the fact that, in virtue of Remark 1, one can assume without loss of generality that $ab \preceq ba$. ∎

## 3. The main results

First, we extend [6, Theorem 1.1] to the setting of linearly ordered magmas. As with the previous section, all magmas here are written multiplicatively.

**Theorem 5.** *Suppose that $\mathfrak{A} = (A, \cdot, \preceq)$ is a linearly ordered magma and let $S$ and $T$ be nonempty finite subsets of $\mathfrak{A}$. Then, $|ST| \geq |S| + |T| - 1$.*

*Proof.* Denote $m$ the size of $S$ and $n$ the size of $T$, and let $a_1, a_2, \ldots, a_m$ be a one-to-one enumeration of $S$ and $b_1, b_2, \ldots, b_n$ a one-to-one enumeration of $T$. Without loss of generality, we can assume that $a_1 \prec a_2 \prec \ldots \prec a_m$ and $b_1 \prec b_2 \prec \ldots \prec b_n$. Since $\mathfrak{A}$ is linearly ordered by $\preceq$, then $a_1 b_1 \prec a_2 b_1 \prec \ldots \prec a_m b_1 \prec a_m b_2 \prec \ldots \prec a_m b_n$, whence $|ST| \geq m + n - 1$. ∎

**Proposition 1.** *Suppose that $\mathfrak{A} = (A, \cdot)$ is a linearly ordered magma. Pick $n \in \mathbb{N}^+$ and let $S_1, S_2, \ldots, S_n$ be nonempty finite subsets of $\mathfrak{A}$. Then*

$$|(S_1 S_2 \cdots S_n)_{\mathrm{P}}| \geq 1 - n + \textstyle\sum_{i=1}^{n} |S_i| \tag{6}$$

*for any given parenthetization $\mathrm{P}$ of $\mathfrak{A}$ of length $n$.*

*Proof.* The claim is obvious if $n = 1$ and it reduces to Theorem 5 when $n = 2$, while for $n \geq 3$ it follows by induction from the fact that there exists a $(n-1)$-parenthetization $\mathrm{Q}$ of $\mathfrak{A}$ such that $(S_1 S_2 \cdots S_n)_{\mathrm{P}} = S_1 \cdot (S_2 \cdots S_n)_{\mathrm{Q}}$ or $(S_1 S_2 \cdots S_n)_{\mathrm{P}} = (S_1 \cdots S_{n-1})_{\mathrm{Q}} \cdot S_n$. ∎

**Corollary 2.** *Pick $m \in \mathbb{N}^+$ and let $\mathfrak{A} = (A, \cdot)$ be a linearly ordered magma and $S$ a finite subset of $A$ of size $m$. Then, for every $n \in \mathbb{N}^+$ and every $n$-parenthetization $\mathrm{P}$ of $\mathfrak{A}$, one has*

$$|(S^n)_{\mathrm{P}}| \geq (m-1)n + 1, \tag{7}$$

*where $(S^n)_{\mathrm{P}} := \{(a_1 a_2 \ldots a_n)_{\mathrm{P}} : a_1, a_2, \ldots, a_n \in S\}$. In addition to this, if $\mathfrak{A}$ is associative and there exists at least one element $a \in \mathfrak{A}$ which is not idempotent, then (7) is a sharp inequality, the lower bound being attained, for all $n \in \mathbb{N}^+$, by taking $S = \{a^i : i = 1, 2, \ldots, m\}$.*

*Proof.* The first part of the claim is obvious if $m = 0$, while it follows from Proposition 1 if $m \neq 0$. As for the second part, assume that $\mathfrak{A}$ is associative and $a \in \mathfrak{A}$ is not idempotent. Then, point (iii) of Theorem 2 implies that $a^i \neq a^j$ for all $i, j \in \mathbb{N}^+$ with $i \neq j$, to the effect that $T = \{a^i : i = 1, 2, \ldots, m\}$ is a set of size $m$ and $|T^n| = (m-1)n + 1$ for every $n \in \mathbb{N}^+$. ■

We give two applications of these results. The first one being based on Example 4; while on the one hand this is not much more than a curiosity, on the other it serves as an instance of a simply-stated problem which cannot be solved by relying on less general formulations of Corollary 2 such as the classical one presented in [6] and already mentioned in the introduction.

**Example 7.** Let $A$ be the interval $[1, +\infty[$ of the real line and $\star$ the binary operation $A \times A \to A : (a, b) \mapsto a^b$. As a magma, $(A, \star)$ is totally ordered by the standard ordering $\leq$ of the real field, but it is not linearly orderable, since $1 \star a = 1 \star b$ for $a, b \in A$ regardless as to whether $a \neq b$. With this in mind, let $n$ be a positive integer, $S$ a finite subset of $A$ of size $m$ and P a parenthetization of $\mathfrak{A}$ of length $n$. We want to prove that $|(S^n)_{\mathrm{P}}| \geq (m-1)n + 1$. If $m = 1$ or $1 \notin S$, the claim follows from Corollary 2 in the light of Example 4. Otherwise, let $\tilde{S} := S \setminus \{1\}$ and denote by $a$ the minimum of $\tilde{S}$ in $(A, \leq)$. Then, by the same reasoning as before,

$$|(S^n)_{\mathrm{P}}| \geq |(\tilde{S}^n)_{\mathrm{P}}| + |T| \geq (m-2)n + 1 + |T|, \tag{8}$$

where $T$ is the set of the elements of $(S^n)_{\mathrm{P}}$ which are smaller than $(a^n)_{\mathrm{P}}$. This is enough to complete our proof when considering that $|T| \geq n$ as $1 = \mathrm{P}(1, 1, \ldots, 1) < a = \mathrm{P}(a, 1, \ldots, 1) < \ldots < \mathrm{P}(a, a, \ldots, a) = (a^n)_{\mathrm{P}}$.

**Example 8.** Let $n$ be a positive integer and $\mathfrak{A}$ a subsemigroup of the (unital) semigroup of all $n$-by-$n$ upper (respectively, lower) triangular matrices with positive real entries equipped with the usual row-by-column multiplication. If $k \in \mathbb{N}^+$ and $S_1, S_2, \ldots, S_k$ are nonempty finite subsets of $\mathfrak{A}$, then Theorem 1 and Proposition 1 yield that $|S_1 S_2 \ldots S_k| \geq 1 - k + \sum_{i=1}^{k} |S_i|$.

Finally, we are ready to prove our main result.

**Proposition 2.** *Let $\mathfrak{A} = (A, \cdot, \preceq)$ be a linearly ordered semigroup and $S$ a nonempty finite subset of $\mathfrak{A}$ of size $m$. If $y \in \mathfrak{A} \setminus \mathrm{C}_{\mathfrak{A}}(S)$, then*

$$|yS \cup Sy| \geq m + 1. \tag{9}$$

*In particular, there exist $a, b \in S$ such that $ya \notin Sy$ and $by \notin yS$.*

*Proof.* Pick $y \in \mathfrak{A} \setminus \mathrm{C}_{\mathfrak{A}}(S)$ and suppose by contradiction that $yS = Sy$. Since $y \notin \mathrm{C}_{\mathfrak{A}}(S)$, there exists $a_1 \in S$ such that $a_1 y \neq y a_1$, which in turn implies, as $y \in \mathrm{N}_{\mathfrak{A}}(S)$, that there exists an element $a_2 \in S$ such that $y a_1 = a_2 y$. Hence, by the finiteness of $S$, it is possible to find a maximum integer $k \geq 2$ such that i) $y a_i = a_{i+1} y$ for every $i = 1, 2, \ldots, k-1$ and ii) $a_i = a_j$ for $i, j = 1, 2, \ldots, k$ only if $i = j$. From the maximality of $k$ and, again, the fact that $yS = Sy$, it follows that $y a_k = a_h y$ for some $h = 1, 2, \ldots, k$. Then, by induction, $y^{i+1} a_k = a_{h+i} y^{i+1}$ for every $i = 0, 1, \ldots, k-h$. In particular, $y^{k-h+1} a_k = a_k y^{k-h+1}$, whence $y a_k = a_k y$ (due to Corollary 1), and indeed $y a_k = y a_{k-1}$ (as $y a_k = y a_{k-1}$, by design). Therefore, Remark 2 yields that $a_k = a_{k-1}$, which is absurd since $a_i \neq a_j$ for all $i, j = 1, 2, \ldots, k$ with $i \neq j$. ■

**Corollary 3.** *If $S$ is a finite subset of a linearly ordered semigroup $\mathfrak{A}$, then $\mathrm{N}_{\mathfrak{A}}(S) = \mathrm{C}_{\mathfrak{A}}(S)$.*

*Proof.* If $S = \emptyset$, the claim is obvious, so assume that $S$ is nonempty. If $y \in \mathrm{N}_{\mathfrak{A}}(S)$, then $yS = Sy$, and Proposition 2 implies that $y \in \mathrm{C}_{\mathfrak{A}}(S)$, whence follows that $\mathrm{N}_{\mathfrak{A}}(S) \subseteq \mathrm{C}_{\mathfrak{A}}(S)$. On the other hand, it is trivial that $\mathrm{C}_{\mathfrak{A}}(S) \subseteq \mathrm{N}_{\mathfrak{A}}(S)$. ■

## 4. Acknowledgements

I am grateful to Martino Garonzi (Università di Padova) for attracting my attention to the work of G.A. Freiman and M. Herzog which inspired this research.

## References

[1] N. Bourbaki, *Algébre: Chapitres 1 á 3,* Springer-Verlag, 2007 (reprint of the 1970 original).
[2] J. Bourgain, A. Furman, E. Lindenstrauss, and S. Mozes, *Invariant measures and stiffness for non-abelian groups of toral automorphisms,* C. R. Math. Acad. Sci. Paris, Vol. 344 (2007), No. 12, pp. 737–742.
[3] J. Bourgain and A. Gamburd, *On the spectral gap for finitely-generated subgroups of SU(2),* Invent. Math., Vol. 171 (2008), No. 1, pp. 83–121.
[4] S. Eliahou and M. Kervaire, *Some extensions of the Cauchy-Davenport theorem,* Electronic Notes in Discrete Mathematics, Vol. 28 (2007), pp. 557–564.
[5] K.-J. Engel and R. Nagel, *A Short Course on Operator Semigroups,* Springer, 2006.
[6] G. Freiman, M. Herzog, P. Longobardi, and M. Maj, *Small doubling in ordered groups,* J. Austral. Math. Soc., to appear.
[7] E. Hille and R.S. Phillips, *Functional analysis and semi-groups,* AMS, 1996 (revised edition).
[8] J.M. Howie, *Fundamentals of semigroup theory,* Clarendon Press, 1995.
[9] K. Iwasawa, *On linearly ordered groups,* J. Math. Soc. Japan, Vol. 1 (1948), pp. 1–9.
[10] F.W. Levi, *Arithmetische Gesetze im Gebiete diskreter Gruppen,* Rend. Circ. Mat. Palermo, Vol. 35 (1913), pp. 225-236.
[11] A.I. Mal'cev, *On ordered groups,* Izv. Akad. Nauk. SSSR Ser. Mat., Vol. 13 (1948), pp. 473–482.
[12] B.H. Neumann, *On ordered groups,* Amer. J. Math., Vol. 71 (1949), pp. 1–18.
[13] I.Z. Ruzsa. "Sumsets and structure." In *Combinatorial Number Theory and Additive Group Theory,* Springer, 2009.
[14] T.C. Tao, *Product set estimates for non-commutative groups,* Combinatorica, Vol. 28 (2008), No. 5, pp. 547–594.
[15] J.A. van Casteren, *Markov Processes, Feller Semigroups and Evolution Equations,* Series on Concrete and Applicable Mathematics, 2010.

Laboratoire Jacques-Louis Lions, Université Pierre et Marie Curie, 4 place Jussieu, 75005 Paris.
*E-mail address*: tringali@ann.jussieu.fr