Small doubling in ordered semigroups

Salvatore Tringali

SMALL DOUBLING IN ORDERED SEMIGROUPS

SALVATORE TRINGALI

Abstract. We generalize recent results by G.A. Freiman, M. Herzog and coauthors on the structure theory of product-sets from the context of linearly (i.e., strictly and totally) ordered groups to linearly ordered semigroups. In particular, we find that if S is a finite subset of a linearly ordered semigroup generating a nonabelian subsemigroup, then $|S^2| \geq 3\,|S| - 2$. On the road to this goal, we also prove a number of subsidiary results, and notably that the commutator and the normalizer of a finite subset of a linearly ordered semigroup are equal to each other. The whole is accompanied by several examples, including a proof that the multiplicative semigroup of 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 [8], have been successfully applied for decades to the study of partial [5] and stochastic [16] 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 coauthors on the structure theory of product-sets in the (nonabelian) setting of linearly (i.e., strictly and totally) ordered groups [6]. This is an active area of research, with notable applications, e.g., to additive combinatorics [15], Freiman's structure theory [14], invariant measures [1], and spectral gaps [2]. The present work fits into this background; it is basically a collection of miscellaneous results, serving as a preliminary to further study and future developments and aiming to be a contribute to the efforts of extending some parts of the theory from groups to the scenery of semigroups (and magmas). Specifically, our main result is the following generalization of [6, Theorem 1.2]:

Theorem 1. *Let S be a finite subset of a linearly ordered semigroup (written multiplicatively), which generates a nonabelian subsemigroup. Then, $|S^2| \geq 3\,|S| - 2$.*

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

Key words and phrases. Freiman's theory, ordered magmas, ordered semigroups, product-sets, small doubling, sum-sets, torsion-free semigroups.

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

Net of a number of (minor) simplifications, our proof of Theorem 1 basically follows the same broad scheme as the proof of [6, Theorem 1.2]. However, the increased generality implied by the switching to the setting of linearly ordered semigroups raises a number of challenges and requires more than a mere adjustment of terminology, and especially the refinement of several classical results on linearly orderable groups, such as the following:

Corollary 2. *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 2 is actually a generalization of an old lemma by N.H. Neumann [13] on commutators of linearly ordered groups, appearing as Lemma 2.2 in [6]; we prove it in Section 2.3.

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

Proposition 9. *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 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 9 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 two simple applications of Proposition 9, none of them covered by less general formulations of the same result such as the (classical) one reported in [6] for linearly ordered groups: The second one 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 Proposition 1. In this respect, we raise the question, at present 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.

Then, we combine Proposition 9 with other basic properties to establish the following:

Proposition 10. *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, and pick $y \in \mathfrak{A} \setminus \mathrm{C}_{\mathfrak{A}}(S)$. Then $|yS \cup Sy| \ge m+1$, so in particular there exist $a, b \in S$ such that $ya \notin Sy$ and $by \notin yS$.*

Proposition 10 is a generalization of [6, Proposition 2.4]. We prove it in Section 3, along with the following interesting result, which in turn generalizes [6, Corollary 1.5].

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

The whole is accompanied by a significant number of examples, mostly finalized to explore conditions under which some special classes of semigroups (or more sophisticated structures as semirings) are linearly orderable. In particular, we show by Proposition 6 that every abelian torsion-free cancellative semigroup is linearly orderable, so extending a similar 1913 result of F.W. Levi on abelian torsion-free groups.

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 4, 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 reference for terms not given here or in a later section is [9]; in particular, for order-theoretic concepts the reader should consult [9, §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 $a \neq b$. 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. If S is a subset of A and S is closed under $\star$, i.e. $a \star b \in S$ for all $a, b \in S$, we say that $(S, \star)$ is a submagma of $\mathfrak{A}$.

Note that [9, §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 $(\mathfrak{A}, \preceq)$, where (i) $\mathfrak{A} = (A, \star)$ is a magma, (ii) $\preceq$ is an order on A, and (iii) $a \star c \preceq b \star c$ and $c \star a \preceq c \star b$ for all $a, b, c \in A$ with $a \preceq b$; this will be equivalently represented by the triple $(A, \star, \preceq)$. 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 strictly and totally ordered. Accordingly, $\mathfrak{A}$ is totally orderable in the first case, strictly orderable in the second, and linearly orderable in the latter, and we say respectively that $\mathfrak{A}$ is totally, strictly, and linearly ordered by $\preceq$.

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 $a \preceq b$.

Totally ordered semigroups are considered, for instance, by A.H. Clifford in his 1958 survey on the subject [3], where they are simply referred to as ordered semigroups. Note that, in spite of its title, Clifford's work deals with totally ordered semigroups both in the abelian and nonabelian setting; however, the manuscript is not really focused on linearly ordered semigroups as here defined (these are only mentioned in the introduction, but not further considered).

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. The notion of orderable magma is somewhat vacuous since every magma $\mathfrak{A}$ is ordered by the trivial order $\preceq$, defined for $a, b \in \mathfrak{A}$ by taking $a \preceq b$ if and only if $a = b$.

Remark 2. If $(A, \star, \preceq)$ is an ordered, totally ordered, or strictly ordered magma, then the same is also true for $(A, \star, \preceq_{\rm op})$, $(A, \star_{\rm op}, \preceq)$ and $(A, \star_{\rm op}, \preceq_{\rm op})$, where $\preceq_{\rm op}$ is the dual order of $\preceq$ and $\star_{\rm op}$ the dual product of $\star$, i.e. the binary operation $A \times A \to A : (a, b) \mapsto b \star a$.

Remark 3. Every submagma of a linearly orderable magma is linearly orderable.

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 id_A is the map $A \to A : a \to a$, and $\mathcal{P}_{n+1} := \mathcal{P}^{\rm L}_{n+1} \cup \mathcal{P}^{\rm R}_{n+1}$, where

(i) $P^{\rm L}_{n+1}$ 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 $a_1 \star f(a_2, a_3, \ldots, a_{n+1})$.

(ii) $P^{\rm R}_{n+1}$ 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 $(a_1 \star a_2 \star \cdots \star a_n)_{\rm P}$ in place of $\mathrm{P}(a_1, a_2, \ldots, a_n)$ and, whenever $S_1, S_2, \ldots, S_n$ are subsets of A, we let

$$(S_1 \star S_2 \star \cdots \star S_n)_{\rm P} := \{(a_1 \star a_2 \star \cdots \star a_n)_{\rm P} : a_1 \in S_1, a_2 \in S_2, \ldots, a_n \in S_n\} \tag{2}$$

if S_i is nonempty for each $i = 1, 2, \ldots, n$, while taking $(S_1 \star S_2 \star \cdots \star S_n)_{\rm P} := \emptyset$ otherwise. If $\mathfrak{A}$ is a semigroup or $n \le 2$, then $(a_1 \star a_2 \star \cdots \star a_n)_{\rm P}$ 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 serious sdanger 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 write $\langle S \rangle_{\mathfrak{A}}$ for the submagma of $\mathfrak{A}$ generated by S, i.e. the smallest submagma of $\mathfrak{A}$ containing S (which is clearly a semigroup if the magma operation is associative); cf. [9, §1.2]. Also, 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 $\{a \in \mathfrak{A} : a \star S = S \star a\}$. In particular, these are written as $\mathrm{C}_{\mathfrak{A}}(a)$ and $\mathrm{N}_{\mathfrak{A}}(S)$, respectively, if $S = \{a\}$ for some $a \in \mathfrak{A}$.

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 [9, 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 $|A| \ge 2$.

Example 2. A notable example of linearly ordered groups is provided by abelian torsion-free groups, as first proved by F.W. Levi in [11], and we show in Section 2.3 that Levi's result can be,

in fact, extended to abelian cancellative torsion-free semigroups (see Proposition 6). In the same lines, K. Iwasawa [10], A.I. Mal'cev [12] and B.H. Neumann [13] established, independently from each other, that the class of torsion-free nilpotent groups is contained in the class of linearly orderable groups. These are already reported in [6], along with further references to existing literature on the subject.

Example 3. As for linearly ordered monoids which are not linearly ordered groups, one can consider, for instance, the free monoid on an alphabet X together with the "shortlex ordering": Words are primarily sorted by length, with the shortest ones first, and words of the same length are then sorted into lexicographical order. On the other hand, the positive integers divisible only for the members of a given subset S of (natural) primes, endowed with the usual multiplication, provides the example of a linearly orderable semigroup which is not even a monoid unless $S = \emptyset$.

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 nonabelian 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 linearly ordered semigroups which are neither abelian 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 linearly 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 (cf. [7, Ch. II]). A semiring is similar to a ring, save that elements in semirings do not necessarily have an inverse for the addition. We denote by $\mathfrak{A}_0$ the set of zero divisors of $\mathfrak{A}$, i.e. the non-zero elements $a \in A$ such that $a \cdot b = 0$ or $b \cdot a = 0$ for some $b \in A \setminus \{0\}$; $\mathfrak{A}$ has no zero divisors if $\mathfrak{A}_0 = \emptyset$.

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:

(iv) $(A, +, \preceq)$ is a strictly ordered semigroup;
(v) $(A \setminus \{0\}, \cdot, \preceq)$ is a strictly ordered semigroup,

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 notion of orderable semiring is basically vacuous, insomuch as every semiring is ordered by the trivial order (cf. Remark 1). Also, a semiring is strictly orderable only if it has no zero

divisors. 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 integers.

Based on these premises, assume in what follows 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 $\mathfrak{A}$ (here respectively denoted, as is usual, by the same symbols as the addition and multiplication of this latter), $\mathcal{M}_n(A)$ becomes a semiring in its own right, referred to as the semiring of the n-by-n matrices over $\mathfrak{A}$ and indicated throughout 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.

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

Proof. Set $I_n := \{1, 2, \ldots, n\}$, $\Xi_n := \{(i, j) \in I_n \times I_n : i \le j\}$ and define a binary relation $\le_n$ on Ξ_n by letting $(i_1, j_1) \le_n (i_2, j_2)$ 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 $\le_n$ is a total order, and indeed a well-order as Ξ_n is finite. This allows us define a binary relation $\preceq_n^{\mathrm{U}}$ on $\mathrm{U}_n(\mathfrak{A}^+)$ by taking, for $\alpha = (a_{i,j})_{i,j=1}^n$ and $\beta = (b_{i,j})_{i,j=1}^n$ in $\mathrm{U}_n(\mathfrak{A}^+)$, $\alpha \preceq_n^{\mathrm{U}} \beta$ 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 an order. To see that it is total: Pick $\alpha = (a_{i,j})_{i,j=1}^n$ and $\beta = (b_{i,j})_{i,j=1}^n$ in $\mathrm{U}_n(\mathfrak{A}^+)$ with $\alpha \ne \beta$. There then exists $(i_0, j_0) \in \Xi_n$ such that $a_{i_0,j_0} \ne b_{i_0,j_0}$ and, using that $\le_n$ is a well-order, (i_0, j_0) can be chosen in such a way that $a_{i,j} = b_{i,j}$ for every $(i, j) \le_n (i_0, j_0)$. Thus, as $\preceq$ is total, either $\alpha \prec_n^{\mathrm{U}} \beta$ if $a_{i_0,j_0} \prec b_{i_0,j_0}$ or $\beta \prec_n^{\mathrm{U}} \alpha$ otherwise.

It remains to prove that $\mathrm{U}_n(\mathfrak{A}^+)$ is linearly ordered by $\preceq_n^{\mathrm{U}}$. For let α, β and γ 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 consequence, $a_{i,k}c_{k,j} \preceq b_{i,k}c_{k,j}$ 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 $(i, k) \le_n (i_0, j_0)$ and $(k, j) \le_n (k, j_0)$, 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 $(i, j) \le_n (i_0, j_0)$,

$$\sum_{k=1}^n a_{i,k}c_{k,j} = \sum_{k=i}^j a_{i,k}c_{k,j} \preceq_n^{\mathrm{U}} \sum_{k=i}^j b_{i,k}c_{k,j} = \sum_{k=1}^n b_{i,k}c_{k,j} \tag{3}$$

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 ultimately shows that $\alpha \cdot \gamma \prec_n \beta \cdot \gamma$ and $\gamma \cdot \alpha \prec_n \gamma \cdot \beta$, and our proof is complete. ∎

We refer to the order $\preceq_n^{\mathrm{U}}$ defined in the proof of Proposition 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 linearly ordered semiring of all nonnegative real numbers (with their standard structure) and take α as the n-by-n matrix whose entries are all equal to 1 and β 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 constructions reported below.

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

$$A \times A \to A : (f, g) \mapsto \Big(I \to \textstyle\bigcup_{i\in I} A_i : i \mapsto f(i) \star_i g(i)\Big), \tag{4}$$

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 lexicographical 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 $\star$, 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 $i \in I$.

Example 7. Let $\mathfrak{A} = (A, \star)$ and $\mathfrak{B} = (B, \cdot)$ be magmas and $\phi : \mathfrak{A} \to \mathfrak{B}$ a magma monomorphism, i.e. an injective function $A \to B$ with $\phi(a_1 \star a_2) = \phi(a_1) \cdot \phi(a_2)$ for all $a_1, a_2 \in A$. If $\mathfrak{B}$ is linearly ordered by some total order $\preceq_B$ and $\preceq_A$ is the binary relation on A defined for $a_1, a_2 \in A$ by taking $a_1 \preceq_A a_2$ if (and only if) $\phi(a_1) \preceq_B \phi(a_2)$, it is routine to verify that $\preceq_A$ is a total order, and indeed $(\mathfrak{A}, \preceq_A)$ is a linearly ordered magma: In particular, if $a_1, a_2, c \in \mathfrak{A}$ and $a_1 \prec_B a_2$, then $\phi(a_1) \prec_B \phi(a_2)$, from which it follows that

$$\phi(a_1 \star c) = \phi(a_1) \cdot \phi(c) \prec_B \phi(a_2) \cdot \phi(c) = \phi(a_2 \star c) \tag{5}$$

and similarly $\phi(c \star a_1) \prec_A \phi(c \star a_2)$, since ϕ is a magma monomorphism. Thus, $a_1 \star c \prec_A a_2 \star c$ and $c \star a_1 \prec_A c \star a_2$, by definition of $\preceq_A$. For future reference we summarize the result in the following proposition:

Proposition 2. *Let $\mathfrak{A}$ and $\mathfrak{B}$ be magmas and suppose that $\mathfrak{A}$ embeds in $\mathfrak{B}$, that is, there exists a magma monomorphism $\phi : \mathfrak{A} \to \mathfrak{B}$. Then, $\mathfrak{A}$ is totally (respectively, linearly) orderable if and only if the same holds true for $\phi(\mathfrak{A})$.*

Example 8. This example deals with polynomials. We start by recalling some basic definitions, to fix notation and terminology. Let $\mathfrak{X} = (X, \preceq_X)$ be a well-ordered nonempty set (which can be interpreted as a set of distinct labelled variables) and $\mathfrak{A} = (A, +, \cdot, 0)$ a semiring (see Example 5). Writing $\mathcal{F}_c(X, \mathbb{N})$ for the set of all functions $\phi : X \to \mathbb{N}$ with $|\{x \in X : \phi(x) \neq 0\}| < \infty$, we take a polynomial variable with $\mathfrak{X}$ over (the ground semiring) $\mathfrak{A}$ to be any function $f : \mathcal{F}_c(X, \mathbb{N}) \to \mathfrak{A}$

such that $f(\phi) \neq 0$ for finitely many ϕ (here, $\mathbb{N}$ includes 0). We use $A[\mathfrak{X}]$ for the set of all such functions and endow it with binary operations of addition and multiplication defined as follows (we denote them, each in turn, by the same symbols as the addition and multiplication of $\mathfrak{A}$): For all $f, g \in A[\mathfrak{X}]$, $f + g$ is the pointwise sum of f and g, i.e. the mapping

$$\mathcal{F}_c(X, \mathbb{N}) \to \mathfrak{A} : \phi \mapsto f(\phi) + g(\phi), \tag{6}$$

and fg the Cauchy product of f by g, i.e. the function

$$\mathcal{F}_c(X, \mathbb{N}) \to \mathfrak{A} : \phi \mapsto \textstyle\sum_{(\alpha,\beta)\in\Pi(\phi)} f(\alpha) \cdot g(\beta), \tag{7}$$

Here, given $\phi \in \mathcal{F}_c(X, \mathbb{N})$, $\Pi(\phi)$ means the set of all pairs $(\alpha, \beta) \in \mathcal{F}_c(X, \mathbb{N}) \times \mathcal{F}_c(X, \mathbb{N})$ such that $\alpha \oplus \beta = \phi$, where $\alpha \oplus \beta$ is the function $X \to \mathbb{N} : x \mapsto \alpha(x) + \beta(x)$. For what it is worth, note that the summation in (7) involves only a finite number of non-zero terms for every ϕ, which makes the Cauchy product well-defined even if $\mathfrak{X}$ is infinite.

It is routine to check that $(A[\mathfrak{X}], +, \cdot, 0)$ is a semiring, with 0 the function $\mathcal{F}_c(X, \mathbb{N}) \to \mathfrak{A} : \phi \mapsto 0$. We call it the semiring of polynomials over $\mathfrak{A}$ with variables in $\mathfrak{X}$. This is denoted, in general, by $\mathfrak{A}[\mathfrak{X}]$, and indeed by $\mathfrak{A}[x_1, x_2, \ldots, x_k]$ in the case where $\mathfrak{X}$ is finite of size k and $x_1, x_2, \ldots, x_k$ is the unique enumeration of the elements of $\mathfrak{X}$ with $x_1 \prec_X x_2 \prec_X \cdots \prec_X x_k$. Here, we focus on this latter case, by systematically identifying the elements of $\mathfrak{A}[x_1, x_2, \ldots, x_k]$ with the functions $f : \mathbb{N}^k \to \mathfrak{A}$ such that $\mathbb{N}^k \setminus f^{-1}(0)$ is finite. Especially, we have the following:

Proposition 3. *If $\mathfrak{A}$ is a linearly orderable semiring, then the same is true for $\mathfrak{A}[x_1, x_2, \ldots, x_k]$.*

Proof. It is well-known (cf. [7, Remark 1.10]) that, for $k \geq 2$, $\mathfrak{A}[x_1, x_2, \ldots, x_k]$ is canonically isomorphic to $\mathfrak{A}'[x_k]$, where $\mathfrak{A}' := \mathfrak{A}[x_1, x_2, \ldots, x_{k-1}]$. By induction and Proposition 2, it is then enough to show that $\mathfrak{A}[x_1, x_2, \ldots, x_k]$ is a linearly orderable semiring for $k = 1$.

So write x in place of x_1, for notational simplicity, and assume that $\mathfrak{A}$ is linearly ordered, as a semiring, by a certain order $\preceq$ (see Example 5). Accordingly, define a binary relation $\preceq_{\text{poly}}$ on $\mathfrak{A}[x]$ by taking, for $f, g \in \mathfrak{A}[x]$, $f \preceq_{\text{poly}} g$ if and only if either (i) $f = g$ or (ii) there exists $i_0 \in \mathbb{N}$ such that (ii.1) $f(i_0) \prec g(i_0)$ and (ii.2) $f(i) = g(i)$ for all $i \in \mathbb{N}$ with $i < i_0$.

It is easily recognized that $\preceq_{\text{poly}}$ is an order. To see that $\preceq_{\text{poly}}$ is total: Pick $f, g \in \mathfrak{A}[x]$ with $f \neq g$. Then, there exists $i_0 \in \mathbb{N}$ such that $f(i_0) \neq g(i_0)$. In particular, as $\leq$ is a well-order, i_0 can be chosen in such a way that $f(i) = g(i)$ for every $i < i_0$. Thus, since $\mathfrak{A}$ is totally ordered by $\preceq$, either $f \prec_{\text{poly}} g$ if $f(i_0) \prec g(i_0)$ or $g \prec_{\text{poly}} f$ otherwise.

It remains to prove that $(\mathfrak{A}[x], \preceq_{\text{poly}})$ is a linearly ordered semiring. For pick $f, g, h \in \mathfrak{A}[x]$ with $f \prec_{\text{poly}} g$ and $h \neq 0$. By condition (ii), there exists $i_1 \in \mathbb{N}$ such that $f(i_1) < g(i_1)$ and $f(i) = g(i)$ for all $i < i_1$; furthermore, there exists $i_2 \in \mathbb{N}$ such that $h(i_2) \neq 0$ and $h(i) = 0$ for all $i < i_2$. Now, take $i \in \mathbb{N}$ with $i \leq i_0 := i_1 + i_2$. It is immediate from (7) that

$$(fh)(i) = \textstyle\sum_{(a,b)\in\Pi_0(i)} f(a)h(b), \quad (gh)(i) = \sum_{(a,b)\in\Pi_0(i)} g(a)h(b), \tag{8}$$

where $\Pi_0(i) := \{(a, b) \in \mathbb{N}^2 : a + b = i \text{ and } i_2 \leq b\}$, to the effect that $(fh)(i) = (gh)(i)$ if $i < i_0$. Hence, assume $i_0 \leq i$. It is then easy to check that $a \leq i_1$ for every $(a, b) \in \Pi_0(i)$, and indeed $a < i_1$ unless $i = i_0$, $a = i_1$ and $b = i_2$. It follows from here that $(fh)(i) = (gh)(i)$ for every $i < i_0$ and $(fh)(i_0) \prec (gh)(i_0)$, whence $fh \prec_{\text{poly}} gh$. On the other hand, similar arguments show that $hf \prec_{\text{poly}} hg$. And this completes our proof on account of the fact that it is actually a trivial task to check that $(A[x], +, \preceq_{\text{poly}})$ is a linearly ordered monoid. ∎

We could not figure out how to extend the proof of Proposition 3 in such a way to cover the case of polynomials depending on infinitely many variables. Hence, we conclude this section by raising the following question (up to date, open to us):

Question 2. If $\mathfrak{A}$ is a linearly orderable semiring and $\mathfrak{X}$ a well-ordered nonempty set, is $\mathfrak{A}[\mathfrak{X}]$ a linearly orderable semiring in its own right regardless of the finiteness of $\mathfrak{X}$?

2.3. **A few useful properties.** Here, we aim to derive a few elementary properties of ordered semigroups and magmas, which are basically a generalization of some elementary properties reported in [6, §2] in reference to linearly ordered groups; with the exception of Proposition 6 and Corollary 1 (which are somewhat subsidiary to the main purpose of the paper), these properties will be essential to prove the main results of the paper, in Section 4. Most of them are straightforward, and their group analogues are very well-known; however, since we have no explicit references to similar results in the context of ordered semigroups (and magmas), we prove them here for the sake of completeness and exposition.

All magmas in this section are written multiplicatively (unless an explicit statement to the contrary); 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 n-parenthetization of $\mathfrak{A}$, we use $(a^n)_{\mathrm{P}}$ for the n-fold product $\mathrm{P}(a, a, \dots, a)$.

Proposition 4. *Let $\mathfrak{A} = (A, \cdot, \preceq)$ be an ordered magma. The following holds:*

(i) *If $n \in \mathbb{N}^+$ and 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 $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n \in \mathfrak{A}$ 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 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 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 $c_1, c_2, \dots, c_n \in \mathfrak{A}$, 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, $a^n \preceq \cdots \preceq a^2 \preceq a$ for all $n \in \mathbb{N}^+$, and indeed $a^n \prec \cdots \prec a^2 \prec a$ 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 4. A cancellative magma is linearly orderable if and only if it is totally orderable, as is immediate to check; conversely, every linearly orderable magma is cancellative.

Remark 5. The unique idempotent element of a cancellative unital magma is the identity, so that torsion-free groups are definitely a special kind of torsion-free semigroups. Furthermore,

a cancellative semigroup $\mathfrak{A}$ with an idempotent element a is unital (which applies especially to linearly ordered semigroups, as implied by Remark 4). In fact, $a^2 = a$ entails that $a^2b = ab$ and $ba^2 = ba$ for every $b \in \mathfrak{A}$; then $ab = ba = b$ (by cancellativity of a), which ultimately proves that a serves as an identity for $\mathfrak{A}$.

The next proposition 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.

Proposition 5. *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 $aba = b$ for some $a, b \in \mathfrak{A}$, then $\mathfrak{A}$ is unital and a is the identity of $\mathfrak{A}$.*
(iii) *None of the elements of $\mathfrak{A}$ has finite period unless $\mathfrak{A}$ is unital and such an element is the identity. In particular, $\mathfrak{A}$ is torsion-free.*

Proof. (i) Pick $a, b \in \mathfrak{A}$ with $a^2 \prec a$. Then $a^2b \prec ab$, whence $ab \prec b$ by totality of $\preceq$ and Remark 4. It follows from Proposition 4 that $aba^2 \prec ba$; thus, $aba \prec b$ by the same arguments as before.

(ii) Let $a, b \in \mathfrak{A}$ be such that $aba = b$. Due to Remark 2, we can suppose without loss of generality that $a^2 \preceq a$, which implies the claim by Remark 5 and the previous point (i).

(iii) It is straightforward from Remark 2, point (iii) of Proposition 4 and Remark 5. ∎

Based on point (iii) of Proposition 5 and the work of F.W. Levi on abelian torsion-free groups already mentioned in Example 2, it is somewhat natural to ask whether every abelian torsion-free cancellative semigroup is linearly orderable. This is answered in the positive by the following proposition, which is in fact an extension of Levi's result:

Proposition 6. *Every abelian torsion-free cancellative semigroup is linearly orderable.*

Proof. Let $\mathfrak{A} = (A, \cdot)$ be a semigroup and denote by $\mathfrak{A}^{(1)}$ the canonical unitization of $\mathfrak{A}$ as given in [9, p. 2], where $\mathfrak{A}^{(1)}$ is described as "the monoid obtained from $\mathfrak{A}$ by adjoining an identity if necessary." In fact, $\mathfrak{A}^{(1)}$ is an abelian torsion-free cancellative monoid if and only if $\mathfrak{A}$ is abelian, torsion-free and cancellative as a semigroup. Furthermore, $\mathfrak{A}$ embeds in $\mathfrak{A}^{(1)}$ as a subsemigroup, so $\mathfrak{A}$ is linearly orderable if this is the case with $\mathfrak{A}^{(1)}$, by Remark 3 and Proposition 2.

As a consequence, assume in the sequel, without loss of generality, that $\mathfrak{A}$ is an abelian cancellative monoid with identity 1 and denote by $\mathcal{R}$ the binary relation on $A \times A$ defined, for $a_1, a_2, b_1, b_2 \in A$, by taking $(a_1, a_2)\,\mathcal{R}\,(b_1, b_2)$ if and only if $a_1 \cdot b_2 = a_2 \cdot b_1$. It is easily seen that $\mathcal{R}$ is an equivalence and $\cdot$ is compatible with $\mathcal{R}$, in the sense that, for $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathfrak{A}$, $(a_1, a_2)\,\mathcal{R}\,(b_1, b_2)$ implies that $(a_1 \cdot c_1, a_2 \cdot c_2)\,\mathcal{R}\,(b_1 \cdot c_1, b_2 \cdot c_2)$. If $A/_{\mathcal{R}}$ is now the quotient set of A by $\mathcal{R}$ and, for $(a, b) \in A \times A$, we write $[(a, b)]_{\mathcal{R}}$ for the equivalence class of (a, b), then $A/_{\mathcal{R}}$ becomes an abelian group with the binary operation

$$A/_{\mathcal{R}} \times A/_{\mathcal{R}} \to A/_{\mathcal{R}} : ([(a_1, a_2)]_{\mathcal{R}}, [(b_1, b_2)]_{\mathcal{R}}) \mapsto [(a_1 + a_2, b_1 + b_2)]_{\mathcal{R}}, \tag{9}$$

which we still denote by the same symbol as the product of $\mathfrak{A}$. Indeed, the pair $(A/_{\mathcal{R}}, \cdot)$ is the Grothendieck group of $\mathfrak{A}$ and we indicate it by $\mathfrak{A}_{\mathcal{G}}$; its construction is simplified here by the assumed cancellativity of $\mathfrak{A}$, which entails as well that $\mathfrak{A}$ embeds as a submonoid in $\mathfrak{A}_{\mathcal{G}}$. Now, since, on the one hand, $\mathfrak{A}$ is torsion-free if and only if the same holds true for $\mathfrak{A}_{\mathcal{G}}$ and, on the other, every abelian torsion-free group is linearly orderable by Levi's original result [11], our proof is complete, again by virtue of Proposition 2. ∎

As a minor remark, observe that not every abelian torsion-free monoid is linearly orderable, as recognized by adjoining an extra element, say ∞, to the set $\mathbb{Z}$ of all integers and considering the monoid $(\mathbb{Z} \cup \{\infty\}, +)$, where $+$ is the usual addition of integers when it is restricted to $\mathbb{Z}$ and $a + \infty := \infty + a := \infty$ for all $a \in \mathbb{Z} \cup \{\infty\}$. This monoid has two idempotent elements, namely 0 and ∞, so it cannot be linearly orderable by point (iii) of Proposition 5.

Another consequence of Proposition 5 is the following:

Corollary 1. *Let $\mathfrak{A} = (A, \cdot)$ be a semigroup and denote by $\mathfrak{A}^{(1)}$ its canonical unitization. Then, $\mathfrak{A}$ is linearly orderable if and only if the same holds true with $\mathfrak{A}^{(1)}$.*

Proof. Since $\mathfrak{A}$ canonically embeds in $\mathfrak{A}^{(1)}$, the right-to-left implication is trivial by Remark 3 and Proposition 2. As for the converse, assume that $\mathfrak{A} = (A, \cdot)$ is linearly ordered by a certain total order $\preceq$. If $\mathfrak{A}$ is unital, there is nothing to prove. So, suppose that $\mathfrak{A}$ is not unital and set

$$\mathfrak{A}^- := \{a \in \mathfrak{A} : a^2 \prec a\}, \quad \mathfrak{A}^+ := \{a \in \mathfrak{A} : a \prec a^2\}. \tag{10}$$

Also, denote by 1 the identity of $\mathfrak{A}^{(1)}$. Since $\preceq$ is total, we have by point (iii) of Proposition 5 that $\{\{1\}, \mathfrak{A}^{-1}, \mathfrak{A}^+\}$ is a partition of $\mathfrak{A}^{(1)}$. Accordingly, we define a binary relation $\preceq^{(1)}$ on $\mathfrak{A}^{(1)}$ by taking $a \preceq^{(1)} b$ if and only if either (i) $a, b \in \mathfrak{A}$ and $a \preceq b$, (ii) $a \in \mathfrak{A}^-$ and $b = 1$, (iii) $a = 1$ and $b \in \mathfrak{A}^+$, or (iv) $a = b = 1$. It is routine to check that $\preceq^{(1)}$ is a total order. Furthermore, if $a, b \in \mathfrak{A}^{(1)}$ and $a \prec^{(1)} 1$, then by construction $a^2 \prec a$; hence, we get from Remark 2 and point (i) of Proposition 5 that $ab \prec b$ and $ba \prec b$, with the result that $ab \prec^{(1)} b$ and $ba \prec^{(1)} b$. Similarly, $b \prec^{(1)} ab$ and $b \prec^{(1)} ba$ if $a, b \in \mathfrak{A}$ and $1 \prec^{(1)} a$. The claim follows. ∎

We conclude the section with the generalization of Neumann's lemma already mentioned in the introduction (cf. Lemma 2.2 in [6]): The basic observation is that, if $\mathfrak{A}$ is a group with identity 1 and $a, b \in \mathfrak{A}$ are such that $[a^n, b] = 1$ for some $n \in \mathbb{N}^+$, then $a^n b = ab^n$ (the square brackets denote a commutator, as is expected).

Proposition 7. *Let $\mathfrak{A} = (A, \cdot, \preceq)$ be a linearly ordered semigroup and pick $a, b \in \mathfrak{A}$. If $ab \prec ba$, then $a^n b \prec a^{n-1}ba \prec \cdots \prec aba^{n-1} \prec ba^n$ for all $n \in \mathbb{N}^+$.*

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

Corollary 2. *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 Proposition 7 and the fact that, in virtue of Remark 2, one can assume without loss of generality that $ab \preceq ba$. ∎

3. Finite subsets of linearly ordered semigroups

The present section is concerned with various lower bounds on the size of the product-set of two or more finite subsets of linearly ordered magmas or semigroups (here again written multiplicatively, as in the previous section). First, we extend [6, Theorem 1.1] to the setting of linearly ordered magmas and derive a number of related results.

Proposition 8. *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 $a_1, a_2, \dots, a_m$ be a one-to-one enumeration of S and $b_1, b_2, \dots, b_n$ a one-to-one enumeration of T. Without loss of generality, we can assume that $a_1 \prec a_2 \prec \cdots \prec a_m$ and $b_1 \prec b_2 \prec \cdots \prec b_n$. Since $\mathfrak{A}$ is linearly ordered by $\preceq$, then $a_1b_1 \prec a_2b_1 \prec \cdots \prec a_mb_1 \prec a_mb_2 \prec \cdots \prec a_mb_n$, whence $|ST| \ge m + n - 1$. ■

Proposition 9. *Suppose that $\mathfrak{A} = (A, \cdot)$ is a linearly ordered magma. Pick $n \in \mathbb{N}^+$ and let $S_1, S_2, \dots, S_n$ be nonempty finite subsets of $\mathfrak{A}$. Then*

$$|(S_1S_2 \cdots S_n)_{\mathrm{P}}| \ge 1 - n + \textstyle\sum_{i=1}^{n} |S_i| \tag{11}$$

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

Proof. The claim is obvious if $n = 1$ and it reduces to Proposition 8 when $n = 2$, while for $n \ge 3$ it follows by induction from the fact that there exists a $(n-1)$-parenthetization Q of $\mathfrak{A}$ such that $(S_1S_2 \cdots S_n)_{\mathrm{P}} = S_1 \cdot (S_2 \cdots S_n)_{\mathrm{Q}}$ or $(S_1S_2 \cdots S_n)_{\mathrm{P}} = (S_1 \cdots S_{n-1})_{\mathrm{Q}} \cdot S_n$. ■

Corollary 3. *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 P of $\mathfrak{A}$, one has*

$$|(S^n)_{\mathrm{P}}| \ge (m-1)n + 1, \tag{12}$$

where $(S^n)_{\mathrm{P}} := \{(a_1a_2 \cdots a_n)_{\mathrm{P}} : a_1, a_2, \dots, a_n \in S\}$. 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 (12) is a sharp inequality, the lower bound being attained, for all $n \in \mathbb{N}^+$, by taking $S = \{a^i : i = 1, 2, \dots, m\}$.

Proof. The first part of the claim is obvious if $m = 0$, while it follows from Proposition 9 if $m \ne 0$. As for the second part, assume that $\mathfrak{A}$ is associative and $a \in \mathfrak{A}$ is not idempotent. Then, point (iii) of Proposition 4 implies that $a^i \ne a^j$ for all $i, j \in \mathbb{N}^+$ with $i \ne j$, to the effect that $T = \{a^i : i = 1, 2, \dots, m\}$ 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 3 such as the classical one reported in [6] and already mentioned in the introduction.

Example 9. 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 $\le$ 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 $a \ne b$. 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 $|(S^n)|_{\mathrm{P}} \ge (m-1)n + 1$. If $m = 1$ or $1 \notin S$, the claim follows from Corollary 3 in the light of Example 4. Otherwise, let $\tilde{S} := S \setminus \{1\}$ and denote by a the minimum of $\tilde{S}$ in $(A, \le)$. Then, by the same reasoning as before,

$$|(S^n)_{\mathrm{P}}| \ge |(\tilde{S}^n)_{\mathrm{P}}| + |T| \ge (m-2)n + 1 + |T|, \tag{13}$$

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 $|T| \ge n$ as

$$1 = \mathrm{P}(1, 1, \dots, 1) < a = \mathrm{P}(a, 1, \dots, 1) < \cdots < \mathrm{P}(a, a, \dots, a) = (a^n)_{\mathrm{P}}. \tag{14}$$

Example 10. 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 $S_1, S_2, \dots, S_k$ are nonempty finite subsets of $\mathfrak{A}$, then Propositions 1 and 9 yield that $|S_1S_2 \cdots S_k| \ge 1 - k + \sum_{i=1}^{k} |S_i|$.

Proposition 10. *Let $\mathfrak{A} = (A, \cdot, \preceq)$ be a linearly ordered semigroup and S a nonempty finite subset of $\mathfrak{A}$ of size m, and pick $y \in \mathfrak{A} \setminus \mathrm{C}_{\mathfrak{A}}(S)$. Then $|yS \cup Sy| \geq m+1$, so in particular there exist $a, b \in S$ such that $ya \notin Sy$ and $by \notin yS$.*

Proof. Assume to the contrary 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 2), and indeed $y a_k = y a_{k-1}$ (as $a_k y = y a_{k-1}$, by design). Therefore, Remark 4 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 4. *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 10 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. The main results

In this section we prove our main results and some corollaries. We start with a series of lemmas: The two first of these apply to cancellative semigroups in general, while the others, more restrictively, to linearly ordered semigroups. All semigroups here are written multiplicatively.

Lemma 1. *Let $\mathfrak{A}$ be a cancellative semigroup and S a finite subset of $\mathfrak{A}$ such that $\langle S \rangle_{\mathfrak{A}}$ is abelian. If $y \in \mathfrak{A} \setminus \mathrm{C}_{\mathfrak{A}}(S)$, then $S^2 \cap (yS \cup Sy) = \emptyset$.*

Proof. Pick $y \in \mathfrak{A} \setminus \mathrm{C}_{\mathfrak{A}}(S)$ and suppose for the sake of contradiction that $S^2 \cap (yS \cup Sy) \neq \emptyset$. Then, without loss of generality, there exist $a, b, c \in A$ such that $ab = cy$. As $\langle S \rangle_{\mathfrak{A}}$ is abelian, this gives that $cyc = abc = cab$, whence $ab = yc$ since $\mathfrak{A}$ is cancellative, and finally $cy = yc$.

We claim that $xy = yx$ for all $x \in S$. Indeed, let $x \in S$. Then, on the one hand, $abx = cyx = ycx = yxc$ (as we have just seen that $cy = yc$); on the other, $xab = xcy = xyc$. But $abx = xab$ (again by the abelianity of $\langle S \rangle_{\mathfrak{A}}$), so in the end $yxc = xyc$, and hence $yx = xy$ (by cancellativity of c). It follows that $y \notin \mathrm{C}_{\mathfrak{A}}(S)$, which is absurd. ∎

Lemma 2. *Let $\mathfrak{A}$ be a cancellative semigroup and pick $a, b, x, y, z \in \mathfrak{A}$ such that $x, y, z \in \mathrm{C}_{\mathfrak{A}}(b)$ and $xy = az$ (respectively, $xy = za$). Then $ab = ba$.*

Proof. On the one hand, $xyb = azb = abz$ since $zb = bz$; on the other hand, $baz = bxy = xyb$ as $x, y \in \mathrm{C}_{\mathfrak{A}}(b)$. Then $abz = baz$, from which $ab = ba$ (by cancellativity of z). The dual case where $xy = za$ is now immediate by Remark 2. ∎

Lemma 3. *Let $\mathfrak{A} = (A, \cdot, \preceq)$ be a linearly ordered semigroup and S a nonempty finite subset of $\mathfrak{A}$ of size m, and pick $y \in \mathfrak{A} \setminus \mathrm{C}_{\mathfrak{A}}(S)$. If $\langle S \rangle_{\mathfrak{A}}$ is abelian, then $|S^2 \cup yS \cup Sy| \geq 3m$.*

Proof. Since every linearly ordered semigroup is cancellative (Remark 4), the inclusion-exclusion principle, in combination with Lemma 1, implies that

$$|S^2 \cup yS \cup Sy| = |S^2| + |yS \cup Sy| - |S^2 \cap (yS \cup Sy)| = |S^2| + |yS \cup Sy|, \tag{15}$$

which is enough to complete the proof on account of the fact that $|S^2| \geq 2m - 1$ by Corollary 3 and $|yS \cup Sy| \geq m + 1$ by Proposition 10. ∎

At long last, we are ready to prove the main theorems of the paper.

Theorem 1. *Let $\mathfrak{A}$ be a linearly ordered semigroup and S a finite subset of $\mathfrak{A}$ of size m such that $|S^2| \le 3m-3$. Then $\langle S\rangle_{\mathfrak{A}}$ is abelian.*

Proof. Write I_m for the set $\{1, 2, \dots, m\}$ and let $a_1, a_2, \dots, a_m$ be a one-to-one enumeration of S, assuming, without loss of generality, that $a_1 \prec a_2 \prec \cdots \prec a_m$. Clearly, $m \ge 2$. If $m = 2$ then $|S^2| \le 3$, and indeed $|S^2| = 3$ by Corollary 3; as $a_1^2 \prec a_1a_2 \prec a_2^2$ and $a_1^2 \prec a_2a_1 \prec a_2^2$, it follows that $S^2 = \{a_1^2, a_1a_2, a_2^2\}$ and $a_1a_2 = a_2a_1$, which implies that $\langle S\rangle_{\mathfrak{A}}$ is abelian, as required.

So, in what follows, let $m \ge 3$ and suppose that $\langle B\rangle_{\mathfrak{A}}$ is abelian for every subset B of $\mathfrak{A}$ satisfying $2 \le |B| < m$ and $|B^2| \le 3|B| - 3$. Furthermore, assume for the sake of contradiction that $\langle S\rangle_{\mathfrak{A}}$ is not abelian and accordingly denote by i the maximum integer in I_m such that $\langle T\rangle_{\mathfrak{A}}$ is abelian for $T := \{a_1, a_2, \dots, a_i\}$. Then $1 \le i < m$ and $a_{i+1} \notin \mathrm{C}_{\mathfrak{A}}(T)$, so in particular

$$T^2 \cap (a_{i+1}T \cup Ta_{i+1}) = \emptyset, \tag{16}$$

thanks to Remark 4 and Lemma 1, and

$$|T^2 \cup a_{i+1}T \cup Ta_{i+1}| \ge 3i, \tag{17}$$

by virtue of Lemma 3. Also, there exists a positive integer $j \le m$ such that

$$a_{i+1}a_j \ne a_ja_{i+1}, \tag{18}$$

which is chosen here to be as great as possible, in such a way that

$$xa_{i+1} = a_{i+1}x \quad \text{for every } x \in \mathfrak{A} \text{ with } a_j \prec x. \tag{19}$$

We have that $a_j \notin \mathrm{C}_{\mathfrak{A}}(V)$, where $V := S \setminus T = \{a_{i+1}, a_{i+2}, \dots, a_m\}$, and

$$V^2 \cap (T^2 \cup a_{i+1}T \cup Ta_{i+1}) = \emptyset \tag{20}$$

since $a_ha_k \prec a_{i+1}^2 \preceq a_ra_s$ for all $h, k, r, s \in I_m$ with $h + k \le 2i + 1$ and $i + 1 \le \min(r, s)$. Then, the inclusion-exclusion principle, together with (17) and our hypotheses, gives that

$$|V^2| \le |S^2| - |T^2 \cup a_{i+1}T \cup Ta_{i+1}| \le 3m - 3 - 3i = 3(m-i) - 3 = 3|V| - 3. \tag{21}$$

It follows that $2 \le |V| < m$, and the inductive hypothesis yields that $\langle V\rangle_{\mathfrak{A}}$ is abelian. Thus,

$$V^2 \cap (a_jV \cup Va_j) = \emptyset \tag{22}$$

in view of Remark 4, Lemma 1 and the fact that $a_j \notin \mathrm{C}_{\mathfrak{A}}(V)$. We want to prove that

$$T^2 \cap (a_jV \cup Va_j) = \emptyset. \tag{23}$$

Indeed, assume to the contrary, without loss of generality, that $T^2 \cap a_jV \ne \emptyset$, i.e. $xy = a_jz$ for some $x, y \in T$ and $z \in V$. Since $y \prec z$, this yields that $a_j \prec x$; similarly, $a_j \prec y$ as $\langle T\rangle_{\mathfrak{A}}$ is abelian (to the effect that $xy = yx$, and hence $yx = a_jz$). It then follows from (19) and the abelianity of $\langle V\rangle_{\mathfrak{A}}$ that $x, y, z \in \mathrm{C}_{\mathfrak{A}}(a_{i+1})$. Hence, Lemma 2 entails that $a_{i+1}a_j = a_ja_{i+1}$, which contradicts (18) and implies (23).

That said, let $x \in T$ and $y \in V$ be such that $xa_{i+1} = a_jy$. Since $a_{i+1} \preceq y$, it is apparent that $a_j \preceq x$. Suppose for the sake of contradiction that $a_j \prec x$. Then, we get from (19) and the abelianity of $\langle V\rangle_{\mathfrak{A}}$ that $x, a_{i+1}, y \in \mathrm{C}_{\mathfrak{A}}(a_{i+1})$, to the effect that $a_ja_{i+1} = a_{i+1}a_j$ (by Lemma 2). But this is in open contrast with (18), and it is enough to deduce that

$$Ta_{i+1} \cap a_jV = \{a_ja_{i+1}\}. \tag{24}$$

Thus, the inclusion-exclusion principle gives that

$$|Ta_{i+1} \cup a_jV| = |Ta_{i+1}| + |a_jV| - |Ta_{i+1} \cap a_jV| = i + (m-i) - 1 = m - 1, \tag{25}$$

which in turn implies, together with (16), (20), (22) and (23), that

$$|T^2 \cup V^2 \cup Ta_{i+1} \cup a_jV| = |T^2| + |V^2| + |Ta_{i+1} \cup a_jV|. \tag{26}$$

Hence, it follows from Theorem 3 and (25) that

$$|T^2 \cup V^2 \cup Ta_{i+1} \cup a_jV| \geq (2i-1) + (2m-2i-1) + (m-1) = 3m - 3. \tag{27}$$

As $|S^2| \leq 3m-3$ and $T^2 \cup V^2 \cup Ta_{i+1} \cup a_jV \subseteq S^2$, it is then established that

$$S^2 = T^2 \cup V^2 \cup Ta_{i+1} \cup a_jV. \tag{28}$$

So to conclude our proof, let us define $a := a_{i+1}a_j$. By (16) and (20), it is immediate that $a \notin A^2 \cup V^2$, and we want to show that $a \notin Ta_{i+1} \cup a_jV$ to reach a contradiction. To this aim, observe first that, by (18) and Proposition 10, there exist $\tilde{x} \in T$ and $\tilde{y} \in V$ such that

$$a_{i+1}\tilde{x} \notin Ta_{i+1}, \quad \tilde{y}a_j \notin a_jV. \tag{29}$$

Since $a_{i+1}\tilde{x}, \tilde{y}a_j \notin T^2 \cup V^2$ by (16), (20), (22) and (23), it follows from (28) that $a_{i+1}\tilde{x} \in a_jV$ and $\tilde{y}a_j \in Ta_{i+1}$, with the result that it is possible to find $b \in V$ and $c \in T$ such that

$$a_jb = a_{i+1}\tilde{x}, \quad \tilde{y}a_j = ca_{i+1}. \tag{30}$$

Based on this, suppose first that $a \in Ta_{i+1}$, i.e. there exists $z \in T$ such that $za_{i+1} = a_{i+1}a_j$, and indeed $z \neq a_j$ by (18). If $a_j \prec z$, then $z \in \mathrm{C}_{\mathfrak{A}}(a_{i+1})$ by (19), and hence $a_{i+1}a_j = a_ja_{i+1}$ by Lemma 2, again in contradiction to (18). Thus, $z \prec a_j$. Furthermore, $\tilde{x} \preceq a_j$, as otherwise $a_{i+1}\tilde{x} = \tilde{x}a_{i+1} \in Ta_{i+1}$ by (19), in contradiction to (29). Using that $\langle T \rangle_{\mathfrak{A}}$ is abelian, it follows from (30) that $a_jba_j = a_{i+1}\tilde{x}a_j = a_{i+1}a_j\tilde{x}$. But $a_{i+1}a_j = za_{i+1}$, so in the end $a_jba_j = za_{i+1}\tilde{x}$. Therefore, $ba_j \prec a_{i+1}\tilde{x}$ as $z \prec a_j$, which is absurd since $a_{i+1} \preceq b$ and $\tilde{x} \preceq a_j$, to the effect that $a_{i+1}\tilde{x} \preceq ba_j$. This implies, in the end, that $a \notin Ta_{i+1}$.

Finally, assume that $a \in a_jV$, viz there exists $w \in V$ such that $a_{i+1}a_j = a_jw$. By construction of V, $a_{i+1} \preceq w$, and indeed $a_{i+1} \prec w$ by (18). We want to show that $c \preceq a_j$. For this purpose, suppose to the contrary that $a_j \prec c$. The abelianity of $\langle V \rangle_{\mathfrak{A}}$, together with (19), then yields that $c, a_{i+1}, \tilde{y} \in \mathrm{C}_{\mathfrak{A}}(a_{i+1})$, so $a_{i+1}a_j = a_ja_{i+1}$ by (30) and Lemma 2; this contradicts (18), and hence $c \preceq a_j$. Using once more that $\langle V \rangle_{\mathfrak{A}}$ is abelian, it is then immediate from (30) that $a_{i+1}ca_{i+1} = a_{i+1}\tilde{y}a_j = \tilde{y}a_{i+1}a_j$, so that $a_{i+1}ca_{i+1} = \tilde{y}a_jw$ since $a_{i+1}a_j = a_jw$. But, as argued before, $a_{i+1} \prec w$, whence it is seen that $\tilde{y}a_j \prec a_{i+1}c$, which in turn is absurd because $a_{i+1} \preceq \tilde{y}$, by construction of V, and $c \preceq a_j$, as proved above. Thus, we get that $a \notin a_jV$.

Putting all pieces together, it follows that $a \notin T^2 \cup V^2 \cup Ta_{i+1} \cup a_jV$, which is however in contradiction to (28), as a is obviously an element of S^2. Therefore, $\langle S \rangle_{\mathfrak{A}}$ is abelian. ∎

In some sense, Theorem 1 is best possible; specifically, [6, §3] provides the example of a subset S of linearly ordered group generating a nonabelian subgroup and such that $|S^2| = 3|S| - 2$.

Corollary 5. *Let S be a finite subset of a linearly ordered semigroup, which generates a nonabelian subsemigroup. Then, $|S^2| \geq 3|S| - 2$.*

Proof. Nothing to check here; it is just a trivially equivalent formulation of Theorem 1. ∎

5. Acknowledgements

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

References

[1] J. Bourgain, A. Furman, E. Lindenstrauss, and S. Mozes, *Invariant measures and stiffness for nonabelian groups of toral automorphisms,* C. R. Math. Acad. Sci. Paris, Vol. 344 (2007), No. 12, pp. 737–742.
[2] 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.
[3] A.H. Clifford, *Totally ordered commutative semigroups,* Bull. Amer. Math. Soc., Vol. 64, No. 6 (1958), pp. 305–316.
[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] H. Hebisch and Weinert, *Semirings: Algebraic Theory and Applications in Computer Science,* World Scientific, 1998.
[8] E. Hille and R.S. Phillips, *Functional analysis and semi-groups,* AMS, 1996 (revised edition).
[9] J.M. Howie, *Fundamentals of semigroup theory,* Clarendon Press, 1995.
[10] K. Iwasawa, *On linearly ordered groups,* J. Math. Soc. Japan, Vol. 1 (1948), pp. 1–9.
[11] F.W. Levi, *Arithmetische Gesetze im Gebiete diskreter Gruppen,* Rend. Circ. Mat. Palermo, Vol. 35 (1913), pp. 225-236.
[12] A.I. Mal'cev, *On ordered groups,* Izv. Akad. Nauk. SSSR Ser. Mat., Vol. 13 (1948), pp. 473–482.
[13] B.H. Neumann, *On ordered groups,* Amer. J. Math., Vol. 71 (1949), pp. 1–18.
[14] I.Z. Ruzsa, "Sumsets and structure." In *Combinatorial Number Theory and Additive Group Theory,* Springer, 2009.
[15] T.C. Tao, *Product set estimates for non-commutative groups,* Combinatorica, Vol. 28 (2008), No. 5, pp. 547–594.
[16] 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