SMALL DOUBLING IN ORDERED SEMIGROUPS

SALVATORE TRINGALI

ABSTRACT. Let $\mathbb{A} = (A, \cdot)$ be a semigroup. We generalize some recent results by G. Freiman, M. Herzog and coauthors on the structure theory of set addition from the context of linearly orderable groups to linearly orderable semigroups, where we say that $\mathbb{A}$ is linearly orderable if there exists a total order $\le$ on A such that $xz < yz$ and $zx < zy$ for all $x, y, z \in A$ with $x < y$.

In particular, we find that if S is a finite subset of A generating a non-abelian subsemigroup of $\mathbb{A}$, then $|S^2| \ge 3|S| - 2$. On the road to this goal, we also prove a number of subsidiary results, and most notably that for S a finite subset of A the commutator and the normalizer of S are equal to each other.

1. INTRODUCTION

Semigroups are ubiquitous in mathematics. Apart from being a subject of continuous interest to algebraists, they provide a natural framework for introducing several broadly-scoped concepts and developing large parts of theories traditionally presented in much less general contexts. While on the one hand this makes it possible to use methods and results otherwise restricted to "richer settings" for larger classes of problems, on the other hand it can suggest new directions of research and shed light on classical questions, say, with a primary focus on groups.

Through the present paper, a semigroup is, as usual, a pair $\mathbb{A} = (A, \cdot)$ consisting of a set A, called the carrier of $\mathbb{A}$, and an associative binary operation $\cdot$ on A (unless otherwise specified, all semigroups considered below are written multiplicatively). Then, for $S \subseteq A$ we write $\langle S \rangle_{\mathbb{A}}$ for the smallest subsemigroup of $\mathbb{A}$ containing S, which is simply denoted by $\langle S \rangle$ if $\mathbb{A}$ is implied from the context.

2010 *Mathematics Subject Classification.* Primary 06A07; Secondary 06F05, 06F15, 20F60, 20M10.

Key words and phrases. Centralizer, Freiman's structure theory, linearly ordered semigroups and semirings, matrix semirings, Minkowski sums, normalizer, product sets, semigroup semirings, small doubling, strict total orders, sumsets.

This research is partially supported by the French ANR Project No. ANR-12-BS01-0011 (project CAESAR). Some fundamental aspects of the work were developed while the author was funded from the European Community's 7th Framework Programme (FP7/2007-2013) under Grant Agreement No. 276487 (project ApProCEM).

We let an *ordered semigroup* be a triple $(A, \cdot, \leq)$, where $(A, \cdot)$ is a semigroup, $\leq$ is an order on A (notice that, in this work, the term "order" always means "total order"; see also Section 2), and the following holds:

$$\forall a, b, c \in A : a < b \quad \Longrightarrow \quad ac \leq bc \text{ and } ca \leq cb. \tag{1}$$

If each of the symbols "$\leq$" in (1) is replaced with the symbol "$<$", then $(A, \cdot, \leq)$ is called a *linearly ordered semigroup*; see, e.g., [10].

Accordingly, we say that a semigroup $\mathbb{A} = (A, \cdot)$ is [*linearly*] *orderable* if there exists an order $\leq$ on A such that $(A, \cdot, \leq)$ is a [linearly] ordered semigroup. Then, we may also say that $\mathbb{A}$ is [linearly] ordered by $\leq$.

All of the above notions and terminology are adapted to monoids (that is, unital semigroups) and groups in the obvious way.

Our interest in semigroups is related here to the structure theory of groups and its generalizations; this is an active area of research, which has drawn a constantly increasing attention in the last two decades, and has led to significant progress in several fields, from algebra [5] to number theory and combinatorics [15, 18, 19].

The present paper fits into this context. Our primary goal is, in fact, to extend some recent results by G. A. Freiman, M. Herzog and coauthors from the setting of linearly orderable groups [4] to linearly orderable *semi*groups.

Specifically, assume for the remainder of this section that $\mathbb{A} = (A, \cdot)$ is a fixed semigroup (unless a statement to the contrary is made). Then, the main contribution of this work is the following generalization of [4, Theorem 1.2] (if S is a set, we use $|S|$ for its cardinality):

Theorem 1. *Let $\mathbb{A}$ be a linearly orderable semigroup and S a finite subset of A such that $|S^2| \leq 3|S| - 3$. Then $\langle S \rangle$ is abelian.*

This counts as a genuine generalization of [4, Theorem 1.2] because, if $\mathbb{A}$ is a group and S is a non-empty subset of A such that the smallest sub*semigroup* of $\mathbb{A}$ containing S is abelian, then also the sub*group* of $\mathbb{A}$ generated by S is abelian.

Our proof of Theorem 1 basically follows the same broad scheme as the proof of [4, Theorem 1.2], but there are significant differences in the details. As expected, the increased generality implied by the switching to semigroups - and especially the fact that inverses are no longer available - presents, in practice, a number of challenges and requires something more than a mere adjustment of terminology (in some cases, for instance, it is not even clear *how* a certain statement on linearly ordered groups should be rephrased in the language of semigroups).

In particular, we will look for an extension of several classical results, such as the following lemma (here and later, the lower case Latin letters i, m and n shall denote positive integers unless otherwise noted):

Lemma 1. *Let $\mathbb{A}$ be a linearly orderable semigroup and pick $a, b \in A$. If $a^n b = ba^n$ for some n, then $ab = ba$.*

This is, in fact, a generalization of an old lemma by N. H. Neumann [16] on commutators of linearly ordered groups, appearing as Lemma 2.2 in [4].

In the same spirit, we will also need to extend [4, Proposition 2.4]. To this end, we shall use $\mathrm{C}_{\mathbb{A}}(S)$ for the centralizer of S (relative to $\mathbb{A}$), viz the set of all $a \in A$ such that $ay = ya$ for every $y \in S$, and $\mathrm{N}_{\mathbb{A}}(S)$ for the normalizer of S (relative to $\mathbb{A}$), namely the set $\{a \in A : aS = Sa\}$. These are written as $\mathrm{C}_{\mathbb{A}}(a)$ and $\mathrm{N}_{\mathbb{A}}(a)$, respectively, if $S = \{a\}$ for some a and there is no ambiguity. Then we have:

Lemma 2. *Let $\mathbb{A}$ be a linearly orderable semigroup and S a non-empty finite subset of A, and pick $y \in A \setminus \mathrm{C}_{\mathbb{A}}(S)$. Then $|yS \cup Sy| \geq |S| + 1$, that is $yS \neq Sy$.*

Lemma 2 is proved in Section 3, along with the following generalization of [4, Corollary 1.5], which may perhaps be interesting *per se*:

Theorem 2. *Let S be a finite subset of A and assume that $\mathbb{A}$ is a linearly orderable semigroup. Then $\mathrm{N}_{\mathbb{A}}(S) = \mathrm{C}_{\mathbb{A}}(S)$.*

We conclude the paper with a number of examples (Appendix A), mostly finalized to explore conditions under which certain semigroups (or related structures as semirings) are linearly orderable. This is mainly to show that the class of linearly orderable semigroups is not, in some sense, trivial.

In particular, we prove (Theorem 3) that, for each n, the subsemigroup of $\mathrm{GL}_n(\mathbb{R})$, the general linear group of degree n over the real field, consisting of all upper (respectively, lower) triangular matrices with positive entries on or above (respectively, below) the main diagonal is linearly orderable.

Then, we raise the question (to which we do not have an answer) whether or not the same conclusion holds for the subsemigroup of $\mathrm{GL}_n(\mathbb{R})$ consisting of those matrices which can be written as a (finite) product of upper or lower triangular matrices of the same type as above.

2. General notation and definitions

We refer to [2], [1], and [9], respectively, for notation and terminology from set theory, algebra, and semigroup theory used but not defined here.

An order on a set A is a binary relation $\leq$ on A which is reflexive, antisymmetric, transitive, and *total*, in the sense that for all $a, b \in A$ we have either $a \leq b$ or $b < a$, where $<$ is used for the strict order induced on A by $\leq$. We write $\geq$ and $>$, respectively, for the dual order of $\leq$ and $<$, as usual.

If $\mathbb{A} = (A, \cdot)$ is a semigroup and $S_1, \ldots, S_n$ are subsets of A, we let $S_1 \cdots S_n$ denote the *product set*, relative to $\mathbb{A}$, of the n-tuple $(S_1, \ldots, S_n)$, namely the set

$$\{a_1 \cdots a_n : a_1 \in S_1, \ldots, a_n \in S_n\},$$

and we write it as S^n when the S_i are all equal to the same S. In particular, if $a \in A$, $T \subseteq A$ and no confusion can arise, we use aT for $\{a\}T$ and Ta for $T\{a\}$.

3. Preliminaries

In what follows, unless otherwise specified, $\mathbb{A} = (A, \cdot)$ is a fixed semigroup and $\leq$ is an order on A for which $\mathbb{A}_\sharp = (A, \cdot, \leq)$ is an ordered semigroup.

In this section, we collect some results that will be essential, later in Section 4, to prove the main contributions of the paper. Some are quite elementary, and their group analogues are part of the folklore; however, we do not have a reference to something similar for semigroups, and thus we include them here for the sake of exposition. In particular, the proof (by induction) of the proposition below is straightforward from the definitions, and we may omit the details.

Proposition 3.1. *The following holds:*

(i) *If $a_1, b_1, \ldots, a_n, b_n \in A$ and $a_1 \leq b_1$, …, $a_n \leq b_n$, then $a_1 \cdots a_n \leq b_1 \cdots b_n$; also, $a_1 \cdots a_n < b_1 \cdots b_n$ if $\mathbb{A}_\sharp$ is linearly ordered and $a_i < b_i$ for each i.*

(ii) *If $a, b \in A$ and $a \leq b$, then $a^n \leq b^n$ for all n, and in fact $a^n < b^n$ if $\mathbb{A}_\sharp$ is linearly ordered and $a < b$.*

(iii) *If $a \in A$ is such that $a^2 \leq a$, then $a^n \leq a^m$ for $m \leq n$; moreover, $a^n < a^m$ if $\mathbb{A}_\sharp$ is linearly ordered, $a^2 < a$ and $m < n$.*

Pick an element $a \in A$. We say that a is cancellable (in $\mathbb{A}$) if both of the maps $A \to A : x \mapsto ax$ and $A \to A : x \mapsto xa$ are one-to-one. The semigroup $\mathbb{A}$ is then cancellative if each element of A is cancellable.

Remark 1. A cancellative semigroup is linearly orderable if and only if it is totally orderable. Furthermore, any linearly orderable semigroup is cancellative.

Thus, one thing seems worth mentioning before proceeding: While, on the one hand, every commutative cancellative semigroup embeds as a subsemigroup into a group (as it follows from the standard construction of the group of fractions of a commutative monoid; see [1, Chapter I, Section 2.4]), nothing similar is true, on the other hand, in the non-commutative case, no matter if we restrict to linearly orderable finitely generated semigroups, as first noticed by R. E. Johnson [11] on the basis of an example by A. Malcev [13].

This is of fundamental importance here, as it shows that the study of sumsets in linearly ordered semigroups cannot be systematically reduced, in the absence of commutativity, to the case of groups (at least, not in any obvious way).

On another hand, $a \in A$ is said to be periodic (in $\mathbb{A}$) if there exist positive integers n and p such that $a^n = a^{n+p}$; we then refer to the smallest n with this property as the index of a (in $\mathbb{A}$) and to the smallest p relative to such an n as the period of a (in $\mathbb{A}$); see, e.g., [9, p. 10]. In particular, a is called idempotent (in $\mathbb{A}$) if it has period and index equal to 1, namely $a = a^2$, and we say that $\mathbb{A}$ is torsion-free if its only periodic elements are idempotent.

Remark 2. The unique idempotent element of a cancellative monoid is the identity, so that torsion-free groups are definitely a special type of torsion-free semigroups; cf. Example A.2. Moreover, if $\mathbb{A}$ is cancellative and $a \in A$ is idempotent, then $\mathbb{A}$ is unital (which applies especially to linearly orderable semigroups, in view of Remark 1): For, $a^2 = a$ implies $a^2b = ab$ and $ba^2 = ba$ for every $b \in A$, hence $ab = ba = b$. This ultimately proves that a serves as the identity of $\mathbb{A}$.

The following proposition generalizes properties mentioned in [4, Section 2].

Proposition 3.2. *Let $\mathbb{A}_\sharp$ be a linearly ordered semigroup. We have:*

(i) *If $a \in A$ and $a^2 < a$, then $ab < b$ and $aba < b$ for all $b \in A$.*
(ii) *If $aba = b$ for $a, b \in A$, then $\mathbb{A}$ is unital and a is the identity of $\mathbb{A}$.*
(iii) *None of the elements of A has finite period unless $\mathbb{A}$ is unital and such an element is the identity. In particular, $\mathbb{A}$ is torsion-free.*

Proof. (i) Pick $a, b \in A$ with $a^2 < a$. Then $a^2b < ab$, whence $ab < b$ by the totality of $\leq$ and Remark 1. It follows from Proposition 3.1 that $aba^2 < ba$; thus, $aba < b$ by the same arguments as above.

(ii) Let $a, b \in A$ be such that $aba = b$. By duality, we may suppose that $a^2 \leq a$. If $a^2 < a$, then $aba < b$ by the previous point (i). Therefore, we must have $a^2 = a$, which implies the claim by Remark 2.

(iii) This is immediate from the above (we leave the details to the reader). □

The next proposition, of which we omit the proof, is in turn an extension of an elementary property of the integers; see, for instance, [18, Exercise 1, p. 93] and contrast with [4, Theorem 1.1].

Proposition 3.3. *Assume $\mathbb{A}_\sharp$ is a linearly ordered semigroup and let $S_1, \ldots, S_n$ be non-empty finite subsets of A. Then*

$$|S_1 \cdots S_n| \geq 1 - n + \textstyle\sum_{i=1}^{n} |S_i|. \tag{2}$$

Moreover, (2) is sharp, the lower bound being attained, e.g., by picking $a \in A$ and letting S_i be, for each i, of the form $\{a, \ldots, a^{s_i}\}$ for some positive integer s_i.

In particular, the second part of Proposition 3.3 follows from considering that, if $\mathbb{A}$ is a linearly orderable non-trivial non-empty semigroup, point (iii) of Proposition 3.2 provides at least one element $a \in A$ such that $a^{j_1} \neq a^{j_2}$ for all distinct integers $j_1, j_2 \geq 1$.

Now we prove the generalizations of [4, Lemma 2.2] and [4, Proposition 2.4] alluded to in the introduction, while noticing that, if $\mathbb{A}$ is a group with identity 1 and $a, b \in A$, then $[a^n, b] = 1$, for some n, if and only if $a^n b = ab^n$ (the square brackets denote a commutator).

Proposition 3.4. *Let $\mathbb{A}_\sharp$ be a linearly ordered semigroup and pick $a, b \in A$. If $ab < ba$ then for every n we have*

$$a^n b < a^{n-1}ba < \cdots < aba^{n-1} < ba^n. \tag{3}$$

Proof. Assume that equation (3) is true for some n. Then, multiplying by a on the left gives $a^{n+1}b < a^n ba < \cdots < a^2 ba^{n-1} < aba^n$, while multiplying by a on the right yields $aba^n < ba^{n+1}$. Since $ab < ba$, the transitivity of $\leq$ implies the claim by induction. □

The proof of Lemma 1 is now an immediate consequence of Proposition 3.4 (by duality, if $\mathbb{A}_\sharp$ is a linearly ordered semigroup and $a, b \in A$ then we may assume $ab \leq ba$ without loss of generality), so we come to Lemma 2.

Proof of Lemma 2. Assume to the contrary that $yS = Sy$. Since $y \notin \mathrm{C}_{\mathbb{A}}(S)$, we can find an element $a_1 \in S$ such that $a_1 y \neq y a_1$, which in turn implies that there exists $a_2 \in S \setminus \{a_1\}$ such that $y a_1 = a_2 y$. Then, using that S is a finite set, we get a maximum integer $k \geq 2$ and elements $a_1, \ldots, a_k \in S$ such that

(i) $y a_i = a_{i+1} y$ for $i = 1, \ldots, k-1$;
(ii) the a_i are pairwise distinct for $i = 1, \ldots, k$.

Hence, the maximality of k and $yS = Sy$ imply $y a_k = a_h y$ for some $h = 1, \ldots, k$, with the result that $y^{i+1} a_k = a_{h+i} y^{i+1}$ for every $i = 0, \ldots, k-h$ (by induction). In particular, it holds $y^{k-h+1} a_k = a_k y^{k-h+1}$. Therefore, $y a_k = a_k y$ (by Lemma 1), and in fact $y a_k = y a_{k-1}$ (since $a_k y = y a_{k-1}$, by construction).

So, Remark 1 yields $a_k = a_{k-1}$, which is however absurd because $a_i \neq a_j$ for all $i, j = 1, \ldots, k$ with $i \neq j$. The proof is thus complete. □

We conclude the section with the following:

Proof of Theorem 2. The claim is obvious if S is empty, so assume $S \neq \emptyset$. Given $y \in \mathrm{N}_{\mathbb{A}}(S)$ we have $yS = Sy$, and Lemma 2 implies $y \in \mathrm{C}_{\mathbb{A}}(S)$, whence we get $\mathrm{N}_{\mathbb{A}}(S) \subseteq \mathrm{C}_{\mathbb{A}}(S)$. The other inclusion is straightforward. □

4. The main result

Throughout, $\mathbb{A} = (A, \cdot)$ denotes a fixed semigroup (unless otherwise specified). We start with a series of three lemmas: The two first apply to cancellative semigroups in general, while the latter is specific to linearly orderable semigroups.

Lemma 3. *Let $\mathbb{A}$ be a cancellative semigroup and S a finite subset of A such that $\langle S\rangle$ is abelian. If $y \in A \setminus \mathrm{C}_{\mathbb{A}}(S)$, then S^2 is disjoint from $yS \cup Sy$.*

Proof. Pick $y \in A \setminus \mathrm{C}_{\mathbb{A}}(S)$ and assume for the sake of contradiction that S^2 is not disjoint from $yS \cup Sy$. Without loss of generality, there then exist $a, b, c \in S$ such that $ab = cy$. Since $\langle S\rangle$ is abelian, this gives that $cyc = abc = cab$, whence $ab = yc$ (using that $\mathbb{A}$ is cancellative), and finally $cy = yc$.

We claim that $xy = yx$ for all $x \in S$. For, let $x \in S$. On the one hand, we have $abx = cyx = ycx = yxc$ (as we have just seen that $cy = yc$). On the other hand, $xab = xcy = xyc$. But $abx = xab$ (again, by the commutativity of $\langle S\rangle$). So, in the end, $yxc = xyc$, and hence $yx = xy$ (by the cancellativity of c). It follows that $y \in \mathrm{C}_{\mathbb{A}}(S)$, which is absurd. □

Lemma 4. *Let $\mathbb{A}$ be a cancellative semigroup and pick elements $a, b, x, y, z \in A$ such that $x, y, z \in \mathrm{C}_{\mathbb{A}}(b)$ and $xy = az$ (respectively, $xy = za$). Then $ab = ba$.*

Proof. By duality, we just consider the case when $xy = az$. On the one hand, $xyb = azb = abz$ since $zb = bz$; on the other hand, $baz = bxy = xyb$ since $x, y \in \mathrm{C}_{\mathbb{A}}(b)$. Hence $abz = baz$, that is $ab = ba$ (by the cancellativity of z). □

Now, assume for the remainder of the section that $\mathbb{A}$ is turned into an ordered semigroup by a certain order $\leq$, and set $\mathbb{A}_\sharp = (A, \cdot, \leq)$ for brevity.

Lemma 5. *Let $\mathbb{A}_\sharp$ be linearly ordered, and let S be a non-empty finite subset of A. Pick $y \in A \setminus \mathrm{C}_{\mathbb{A}}(S)$. If $\langle S\rangle$ is abelian, then*

$$|S^2 \cup yS \cup Sy| \geq 3|S|.$$

Proof. The inclusion-exclusion principle, Remark 1 and Lemma 3 give

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

which is enough to complete the proof on account of the fact that $|S^2| \geq 2|S| - 1$, by Proposition 3.3, and $|yS \cup Sy| \geq |S| + 1$, by Lemma 2. □

So at long last we are ready to prove the main theorem of the paper.

Proof of Theorem 1. Write I_m for $\{1, \ldots, m\}$, where $m = |S|$, and let $a_1, \ldots, a_m$ be a numbering of S for which $a_1 < \cdots < a_m$. It is evident that $m \geq 2$. If $m = 2$ then $|S^2| \leq 3$, and in fact $|S^2| = 3$ by Proposition 3.3. Since $a_1^2 < a_1a_2 < a_2^2$ and

$a_1^2 < a_2a_1 < a_2^2$, it follows that $S^2 = \{a_1^2, a_1a_2, a_2^2\}$ and $a_1a_2 = a_2a_1$, which implies that $\langle S\rangle$ is abelian, as desired.

So, in what follows, let $m \geq 3$ and suppose that $\langle B\rangle$ is abelian for every subset B of A for which $2 \leq |B| < m$ and $|B^2| \leq 3|B| - 3$. Furthermore, assume by contradiction that $\langle S\rangle$ is *not* abelian, and accordingly denote by i the maximum integer in I_m such that $\langle T\rangle$ is abelian for $T = \{a_1, \ldots, a_i\}$. Then $1 \leq i < m$ and $a_{i+1} \notin \mathrm{C}_{\mathbb{A}}(T)$, so on the one hand

$$T^2 \cap (a_{i+1}T \cup Ta_{i+1}) = \emptyset, \tag{4}$$

thanks to Remark 1 and Lemma 3, and on the other hand

$$|T^2 \cup a_{i+1}T \cup Ta_{i+1}| \geq 3i, \tag{5}$$

by virtue of Lemma 5. Also, there exists a positive integer $j \leq i$ such that

$$a_{i+1}a_j \neq a_ja_{i+1}, \tag{6}$$

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

$$xa_{i+1} = a_{i+1}x \text{ for every } x \in T \text{ with } a_j < x. \tag{7}$$

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

$$V^2 \cap (T^2 \cup a_{i+1}T \cup Ta_{i+1}) = \emptyset \tag{8}$$

since $a_ha_k < a_{i+1}^2 \leq a_ra_s$ for all indices $h, k, r, s \in I_m$ with $h + k \leq 2i + 1$ and $i + 1 \leq \min(r, s)$. Then the inclusion-exclusion principle, together with (5) and the standing assumptions, gives that

$$|V^2| \leq |S^2| - |T^2 \cup a_{i+1}T \cup Ta_{i+1}| \leq 3m - 3 - 3i = 3|V| - 3.$$

Thus $2 \leq |V| < m$, and $\langle V\rangle$ is abelian (by the inductive hypothesis). Then

$$V^2 \cap (a_jV \cup Va_j) = \emptyset, \tag{9}$$

in view of Remark 1, Lemma 3 and the fact that $a_j \notin \mathrm{C}_{\mathbb{A}}(V)$. We claim

$$T^2 \cap (a_jV \cup Va_j) = \emptyset. \tag{10}$$

For, assume to the contrary, with no loss of generality, that $T^2 \cap a_jV \neq \emptyset$, namely $xy = a_jz$ for some $x, y \in T$ and $z \in V$. Using that $y < z$, this yields $a_j < x$, and similarly $a_j < y$ as $\langle T\rangle$ is abelian (so that $xy = yx$, and hence $yx = a_jz$). It then follows from (7) and the commutativity of $\langle V\rangle$ that $x, y, z \in \mathrm{C}_{\mathbb{A}}(a_{i+1})$. Thus, we get $a_{i+1}a_j = a_ja_{i+1}$ by Lemma 4, which however contradicts (6) and implies (10).

With that said, let $x \in T$ and $y \in V$ be such that $xa_{i+1} = a_jy$. Since $a_{i+1} \leq y$, it is clear that $a_j \leq x$. Suppose for the sake of contradiction that $a_j < x$. Then we get from (7) and the commutativity of $\langle V\rangle$ that $x, a_{i+1}, y \in \mathrm{C}_{\mathbb{A}}(a_{i+1})$, with the

result that $a_j a_{i+1} = a_{i+1} a_j$ (by Lemma 4). But this is in open contrast with (6), and it is enough to argue that

$$Ta_{i+1} \cap a_j V = \{a_j a_{i+1}\}.$$

Thus, the inclusion-exclusion principle gives that

$$|Ta_{i+1} \cup a_j V| = |Ta_{i+1}| + |a_j V| - |Ta_{i+1} \cap a_j V| = m - 1, \tag{11}$$

which in turn implies, together with (4), (8), (9) and (10), that

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

It follows from Proposition 3.3 and (11) that

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

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

$$S^2 = T^2 \cup V^2 \cup Ta_{i+1} \cup a_j V. \tag{12}$$

So to conclude, let us define $a = a_{i+1} a_j$. By (4) and (8), it is straightforward that $a \notin T^2 \cup V^2$, and we want to show that $a \notin Ta_{i+1} \cup a_j V$ to reach a contradiction. For, observe that, by (6) and Lemma 2, there exist $x \in T$ and $y \in V$ such that

$$a_{i+1} x \notin Ta_{i+1}, \quad ya_j \notin a_j V. \tag{13}$$

Since $a_{i+1} x, ya_j \notin T^2 \cup V^2$ by (4), (8), (9) and (10), it then follows from (12) that $a_{i+1} x \in a_j V$ and $ya_j \in Ta_{i+1}$, so we find $b \in V$ and $c \in T$ such that

$$a_j b = a_{i+1} x, \quad ya_j = ca_{i+1}. \tag{14}$$

Suppose that $a \in Ta_{i+1}$, i.e. there exists $z \in T$ for which $za_{i+1} = a_{i+1} a_j$.

We get from (6) that $z \neq a_j$. If $a_j < z$ then (7) yields $z \in \mathrm{C}_{\mathbb{A}}(a_{i+1})$, and Lemma 4 implies $a_{i+1} a_j = a_j a_{i+1}$, again in contradiction to (6). Thus $z < a_j$.

In addition, $x \leq a_j$, since otherwise $a_{i+1} x = x a_{i+1} \in Ta_{i+1}$ in view of (7), in contradiction to (13). Considering that $\langle T \rangle$ is abelian, it follows from (14) that

$$a_j b a_j = a_{i+1} x a_j = a_{i+1} a_j x.$$

But $a_{i+1} a_j = za_{i+1}$, so at the end $a_j b a_j = za_{i+1} x$. Hence, $ba_j < a_{i+1} x$ as $z < a_j$, which is absurd as $a_{i+1} \leq b$ and $x \leq a_j$, viz $a_{i+1} x \leq ba_j$. This gives $a \notin Ta_{i+1}$.

Finally, assume that $a \in a_j V$, i.e. there exists $w \in V$ such that $a_{i+1} a_j = a_j w$. By construction of V, we have $a_{i+1} \leq w$, and in fact $a_{i+1} < w$ by (6). We want to show that $c \leq a_j$. For, suppose to the contrary that $a_j < c$. The commutativity of $\langle V \rangle$, together with (7), then yields that $c, a_{i+1}, y \in \mathrm{C}_{\mathbb{A}}(a_{i+1})$, so $a_{i+1} a_j = a_j a_{i+1}$ by (14) and Lemma 4; this contradicts (6), and hence $c \leq a_j$. Using once more that $\langle V \rangle$ is abelian, it is then immediate from (14) that

$$a_{i+1} c a_{i+1} = a_{i+1} y a_j = y a_{i+1} a_j,$$

so $a_{i+1}ca_{i+1} = ya_jw$ since $a_{i+1}a_j = a_jw$. But, as argued before, $a_{i+1} < w$, whence it is seen that $ya_j < a_{i+1}c$, which is absurd because $a_{i+1} \leq y$, by construction of V, and $c \leq a_j$, as proved above. Therefore, we get that $a \notin a_jV$.

Putting all together, it follows that $a \notin T^2 \cup V^2 \cup Ta_{i+1} \cup a_jV$, which is however in contradiction to (12), as a is obviously an element of S^2. Thus, $\langle S \rangle$ is abelian, and we are done. □

In some sense, Theorem 1 is best possible. More precisely, [4, Section 3] provides the example of a subset S of the carrier of a linearly ordered group generating a non-abelian subgroup and such that $|S^2| = 3|S| - 2$.

Corollary 1. *Assume $\mathbb{A}_\sharp$ is a linearly orderable semigroup and let S be a finite subset of A generating a non-abelian subsemigroup of $\mathbb{A}$. Then $|S^2| \geq 3|S| - 2$.*

Proof. It is just a trivial restatement of Theorem 1. □

We have not found so far an appropriate way to extend Proposition 3.1 in [4] from finite subsets of linearly ordered groups, generating abelian subgroups, to finite subsets of linearly ordered semigroups, generating abelian subsemigroups, so we raise the following:

Question 1. Assume that $\mathbb{A}$ is a linearly orderable semigroup. Let S be a finite subset of A, set $s = |S|$ and $t = |S^2|$ for the sake of notation, and suppose that $t \leq 3s - 4$ and $\langle S \rangle$ is abelian. Is it then possible to find $a, b \in A$ such that $ab = ba$ and S is a subset of the progression $a, ab, \ldots, ab^{t-s}$?

Appendix A. Examples

We conclude the paper with a few examples. As mentioned in the introduction, the basic goal is to show that [linearly] orderable semigroups and related structures are far from being "exotic".

We start with an orderable semigroup which is not linearly orderable. Next, we mention some notable classes of linearly orderable groups and a linearly orderable monoid which is not a linearly orderable group (we do not know if it embeds into a linearly ordered semigroup).

Example A.1. Every set A can be turned into a semigroup by the operation $\cdot : A \times A \to A : (a, b) \to a$; see, for instance, [9, p. 3]. Trivially, if $\leq$ is a total order on A then $(A, \cdot, \leq)$ is a totally ordered semigroup. However, $(A, \cdot)$ is not linearly orderable for $|A| \geq 2$ (e.g., because it is not cancellative).

Example A.2. An interesting variety of linearly orderable groups is provided by abelian torsion-free groups, as first proved by F. W. Levi in [12], and the result can be, in fact, extended to abelian cancellative torsion-free semigroups with no

substantial modification; see the comments following Remark 1 in Section 3 and Corollary 3.4 in R. Gilmer's book on commutative semigroup rings [6].

In a similar vein, K. Iwasawa [10], Malcev [14] and B. H. Neumann [16] established independently that torsion-free nilpotent groups are linearly orderable.

Save for the semigroup analogue of Levi's result, all of the above is already mentioned in [4], where the interested reader can find further references to existing literature on the subject. Two more examples (of linearly orderable groups) which are *not* included in [4] are *pure* braid groups [17] and free groups [10].

Example A.3. As for linearly orderable monoids which are not linearly orderable groups, consider, for instance, the free monoid [9, Section 1.6] on a well-ordered alphabet $(X, \leq)$ 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.

The next example seems interesting *per se*. Not only it gives a family of linearly ordered semigroups which are neither abelian nor groups (at least in general); it also shows that, for each n, certain subsemigroups of $\mathrm{GL}_n(\mathbb{R})$ consisting of triangular matrices are linearly orderable.

Example A.4. We let a semiring be a triple $(A, +, \cdot)$ consisting of a set A and associative operations $+$ and $\cdot$ from $A \times A$ to A (referred to, respectively, as the semiring addition and multiplication) such that

1. $(A, +)$ is an abelian monoid, whose identity we denote by 0;
2. 0 annihilates A, that is $0 \cdot a = a \cdot 0 = 0$ for every $a \in A$;
3. multiplication distributes over addition, that is $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in A$.

(In other words, a semiring is just a ring where elements do not need have an additive inverse.) We call $(A, +)$ and $(A, \cdot)$, respectively, the additive monoid and the multiplicative semigroup of $(A, +, \cdot)$, which in turn is termed a unital semiring if $(A, \cdot)$ is a monoid too; see [8, Ch. II] and [7, Ch. 1, p. 1].

A semiring $(A, +, \cdot)$ is said to be orderable if there exists a (total) order $\leq$ on A such that $(A, +, \leq)$ and $(A, \cdot, \leq)$ are ordered semigroups, in which case $(A, +, \cdot, \leq)$ is referred to as an ordered semiring. If, on the other hand, the following hold:

4. $(A, +, \leq)$ is a linearly ordered monoid;
5. $ac < bc$ and $ca < cb$ for all $a, b, c \in A$ with $a < b$ and $0 < c$,

then $(A, +, \cdot)$ is said to be linearly orderable and $(A, +, \cdot, \leq)$ is called a linearly ordered semiring; cf. [7, Ch. 20]. Common examples of linearly ordered semirings are the [non-negative] integers, the [non-negative] rational numbers, and the [non-negative] reals with their usual addition, multiplication, and order.

With that said, let $\mathbb{A} = (A, +, \cdot)$ be a fixed semiring. We write $\mathcal{M}_n(A)$ for the set of n-by-n matrices with entries in A. Endowed with the usual operations of entry-wise addition and row-by-column multiplication induced by the structure of $\mathbb{A}$, here respectively denoted by the same symbols as the addition and multiplication of the latter, $\mathcal{M}_n(A)$ becomes itself a semiring, which we call the semiring of n-by-n matrices over $\mathbb{A}$ and write as $\mathcal{M}_n(\mathbb{A})$; see [7, Ch. 3].

Suppose now that $\mathbb{A}$ is linearly ordered by a certain order $\leq$, in such a way that $\mathbb{A}_\sharp = (A, +, \cdot, \leq)$ is a linearly ordered semiring, and denote by $\mathrm{U}_n(\mathbb{A}_\sharp^+)$ the subsemigroup of the multiplicative semigroup of $\mathcal{M}_n(\mathbb{A})$ consisting of all upper triangular matrices whose entries on or above the main diagonal belong to

$$\mathbb{A}_\sharp^+ = \{a \in A : a > 0\}.$$

We observe that $\mathrm{U}_n(\mathbb{A}_\sharp^+)$ is not a group (and not even a monoid) for $n \geq 2$. But what is perhaps more interesting is the following:

Theorem 3. $\mathrm{U}_n(\mathbb{A}_\sharp^+)$ *is a linearly orderable semigroup.*

Proof. Set $I_n = \{1, 2, \ldots, n\}$, $\Xi_n = \{(i, j) \in I_n \times I_n : i \leq j\}$ and define a binary relation $\leq_n$ on Ξ_n by $(i_1, j_1) \leq_n (i_2, j_2)$ 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 seen that $\leq_n$ is a well-order, so we can define a binary relation $\leq_{n,\mathrm{U}}$ on $\mathrm{U}_n(\mathbb{A}_\sharp^+)$ by taking, for $\alpha = (a_{i,j})_{i,j=1}^n$ and $\beta = (b_{i,j})_{i,j=1}^n$ in $\mathrm{U}_n(\mathbb{A}_\sharp^+)$, $\alpha \leq_{n,\mathrm{U}} \beta$ if and only if (i) $\alpha = \beta$ or (ii) there exists $(i_0, j_0) \in \Xi_n$ such that $a_{i_0,j_0} < b_{i_0,j_0}$ and $a_{i,j} = b_{i,j}$ for all $(i, j) \in \Xi_n$ with $(i, j) <_n (i_0, j_0)$.

It is straightforward that $\leq_{n,\mathrm{U}}$ is an order. To see, in particular, that it is total: Pick $\alpha = (a_{i,j})_{i,j=1}^n$ and $\beta = (b_{i,j})_{i,j=1}^n$ in $\mathrm{U}_n(\mathbb{A}_\sharp^+)$ with $\alpha \neq \beta$. There then exists $(i_0, j_0) \in \Xi_n$ such that $a_{i_0,j_0} \neq b_{i_0,j_0}$, where (i_0, j_0) is chosen in such a way that $a_{i,j} = b_{i,j}$ for every $(i, j) \leq_n (i_0, j_0)$. Since $\leq$ is total, we have that either $\alpha <_{n,\mathrm{U}} \beta$ if $a_{i_0,j_0} < b_{i_0,j_0}$ or $\beta <_{n,\mathrm{U}} \alpha$ otherwise, and we are done.

It remains to prove that $\mathrm{U}_n(\mathbb{A}_\sharp^+)$ is linearly ordered by $\leq_{n,\mathrm{U}}$. For, let α and β be as above and suppose $\alpha <_{n,\mathrm{U}} \beta$, viz there exists $(i_0, j_0) \in \Xi_n$ with $a_{i_0,j_0} < b_{i_0,j_0}$ and $a_{i,j} = b_{i,j}$ for all $(i, j) \in \Xi_n$ with $(i, j) <_n (i_0, j_0)$. Given $\gamma = (c_{i,j})_{i,j=1}^n$ in $\mathrm{U}_n(\mathbb{A}_\sharp^+)$ we then have $a_{i,k}c_{k,j} \leq b_{i,k}c_{k,j}$ and $c_{i,k}a_{k,j} \leq c_{i,k}b_{k,j}$ 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 in fact $a_{i_0,j_0}c_{j_0,j_0} < b_{i_0,j_0}c_{j_0,j_0}$ and $c_{i_0,i_0}a_{i_0,j_0} < c_{i_0,i_0}b_{i_0,j_0}$ since $(A, +, \cdot, \leq)$ is a linearly ordered semiring. It follows that, for all $(i, j) \in \Xi_n$ with $(i, j) \leq_n (i_0, j_0)$,

$$\textstyle\sum_{k=1}^n a_{i,k}c_{k,j} = \sum_{k=i}^j a_{i,k}c_{k,j} \leq \sum_{k=i}^j b_{i,k}c_{k,j} = \sum_{k=1}^n b_{i,k}c_{k,j}$$

and, similarly, $\sum_{k=1}^n c_{i,k}a_{k,j} \leq \sum_{k=1}^n c_{i,k}b_{k,j}$. In particular, these majorations are equalities for $(i, j) <_n (i_0, j_0)$ and strict inequalities if $(i, j) = (i_0, j_0)$. So $\alpha\gamma <_{n,\mathrm{U}} \beta\gamma$ and $\gamma\alpha <_{n,\mathrm{U}} \gamma\beta$, and the proof is complete. □

We refer to the order $\leq_{n,\mathrm{U}}$ defined in the proof of Theorem 3 as the *zig-zag order* on $\mathrm{U}_n(\mathbb{A}_\sharp^+)$. If $\mathrm{L}_n(\mathbb{A}_\sharp^+)$ is the subsemigroup of the multiplicative semigroup of $\mathcal{M}_n(\mathbb{A})$ consisting of all *lower* triangular matrices whose entries on or below the main diagonal are in $\mathbb{A}_\sharp^+$, it is then easy to see that $\mathrm{L}_n(\mathbb{A}_\sharp^+)$ is itself linearly orderable: It is, in fact, linearly ordered by the binary relation $\leq_{n,\mathrm{L}}$ defined by taking $\alpha \leq_{n,\mathrm{L}} \beta$ if and only if $\alpha^\top \leq_{n,\mathrm{U}} \beta^\top$, where the superscript '$\top$' stands for 'transpose'. If $\mathrm{T}_n(\mathbb{A}_\sharp^+)$ is the subsemigroup of $(\mathcal{M}_n(A), \cdot)$ generated by $\mathrm{U}_n(\mathbb{A}_\sharp^+)$ and $\mathrm{L}_n(\mathbb{A}_\sharp^+)$, it is hence natural to ask the following:

Question 2. Is $\mathrm{T}_n(\mathbb{A}_\sharp^+)$ a linearly orderable semigroup?

While at present we do not have an answer to this, it was remarked by Carlo Pagano (Università di Roma Tor Vergata, Italy) in a private communication that $\mathcal{M}_n(\mathbb{A}_\sharp^+)$, namely the subsemigroup of $(\mathcal{M}_n(A), \cdot)$ consisting of *all* matrices with entries in $\mathbb{A}_\sharp^+$, is not in general linearly orderable: For a specific counterexample, let $\mathbb{A}_\sharp$ be the real field together with its usual order, and take as α the n-by-n real matrix whose entries are all equal to 1 and as β *any* n-by-n matrix with positive real entries each of whose columns has sum equal to n. Then $\alpha^2 = \alpha\beta$.

Apparently, the question has not been addressed before by other authors, although the ordering of $\mathcal{M}_n(\mathbb{A})$, in the case where $\mathbb{A}$ is a *partially* orderable semiring, is considered in [7, Example 20.60].

Example A.5. In what follows, we let $\mathbb{K} = (K, +, \cdot)$ be a semiring (see Example A.4 for the terminology) and $\mathbb{A} = (A, \diamond)$ a semigroup, and use $K[A]$ for the set of all functions $f : A \to K$ such that f is finitely supported in $\mathbb{K}$, namely $f^{-1}(0_K)$ is a finite subset of A, where 0_K is the additive identity of $\mathbb{K}$.

In fact, $K[A]$ can be turned into a semiring, here written as $\mathbb{K}[\mathbb{A}]$, by endowing it with the operations of pointwise addition and Cauchy product induced by the structure of $\mathbb{A}$ and $\mathbb{K}$ (these operations are denoted below with the same symbols as the addition and the multiplication of $\mathbb{K}$, respectively). We have:

Theorem 4. *Suppose $\mathbb{K}$ is a linearly orderable semiring and $\mathbb{A}$ is a linearly orderable semigroup. Then $\mathbb{K}[\mathbb{A}]$ is a linearly orderable semiring too.*

Proof. The claim is obvious if $A = \emptyset$, so assume that A is non-empty, and let $\leq_K$ and $\leq_A$ be, respectively, orders on A and K for which $(K, +, \cdot, \leq_K)$ is a linearly ordered semiring and $(A, \diamond, \leq_A)$ a linearly ordered semigroup.

Then, given $\alpha \in A$ and $f \in K[A]$, we let $f_{\downarrow\alpha}$ (respectively, $f_{\uparrow\alpha}$) be the function $A \to K$ taking a to $f(a)$ if $a <_A \alpha$ (respectively, $\alpha \leq_A a$), and to 0_K otherwise, in such a way that $f = f_{\downarrow\alpha} + f_{\uparrow\alpha}$. Also, we denote by μ the map $K[A] \times K[A] \to A \cup \{A\}$ sending a pair (f, g) to $\min\{a \in A : f(a) \neq g(a)\}$ if $f \neq g$ (the minimum is taken with respect to $\leq_A$, and it exists by consequence of the definition itself of $K[A]$), and to A otherwise.

We define a binary relation $\leq$ on $K[A]$ by letting $f \leq g$ if and only if either $f = g$ or $f \neq g$ and $f(\mu(f,g)) <_K f(\mu(f,g))$. It is clear that $\leq$ is a total order on $K[A]$, and we want to prove that it is also compatible with the algebraic structure of $\mathbb{K}[\mathbb{A}]$, in the sense that $\mathbb{K}[\mathbb{A}]$ is linearly ordered by $\leq$.

For, pick $f, g, h \in K[A]$ with $f < g$. Since the additive monoid of $\mathbb{K}$ is linearly ordered by $\leq_K$, we have $\mu(f,g) = \mu(f+h, g+h)$, and thus $f + h < g + h$. That is, $(K[A], +, \leq)$ is a linearly ordered monoid in its own right. On another hand, assume $\Theta < h$, where Θ is the function $A \to K : a \mapsto 0_K$, and set $\alpha = \mu(f,g)$ and $\beta = \mu(\Theta, h)$. We have $f_{\downarrow\alpha} = g_{\downarrow\alpha}$ and $h = h_{\uparrow\beta}$, with the result that $fh < gh$ if and only if $f_{\uparrow\alpha}h_{\uparrow\beta} < g_{\uparrow\alpha}h_{\uparrow\beta}$, and the latter inequality is certainly true, since on the one side $f_{\uparrow\alpha}h_{\uparrow\beta}(a) = g_{\uparrow\alpha}h_{\uparrow\beta}(a) = 0_K$ for $a <_A \alpha \diamond \beta$, and on the other side

$$f_{\uparrow\alpha}h_{\uparrow\beta}(\alpha \diamond \beta) = f_{\uparrow\alpha}(\alpha)h_{\uparrow\beta}(\beta) <_K g_{\uparrow\alpha}(\alpha)h_{\uparrow\beta}(\beta) = g_{\uparrow\alpha}h_{\uparrow\beta}(\alpha \diamond \beta).$$

In a similar way, it is seen that $hf < hg$. So, by the arbitrariness of f, g, and h, we get that $(K[A], +, \cdot, \leq)$ is a linearly ordered semiring. □

So taking $\mathbb{A}$ to be the free commutative monoid (respectively, the free monoid) on a certain set and recalling that free groups (and hence free monoids) are linearly orderable (Example A.2), we have:

Corollary 2. *The semiring $\mathbb{K}$ is linearly orderable if and only if the same is true for the semiring of polynomials over $\mathbb{K}$ depending on a given set of pairwise commuting (respectively, non-commuting) variables.*

Acknowledgments

The author is indebted with Martino Garonzi (Università di Padova, Italy) for having attracted his attention to the work of G. A. Freiman, M. Herzog and coauthors by which this research was inspired. Also, he is grateful to Alain Plagne (CMLS, École polytechnique, France) for uncountably many suggestions and to Carlo Sanna (Università di Torino, Italy) for an accurate check of the proof of Theorem 1. Last but not least, he would like to thank the anonymous referees for valuable comments which improved the quality of the paper (most notably, this is the case with Theorem 4, initially stated and proved by the author in a less general form).

References

[1] N. Bourbaki, *Algèbre, Chapitres 1 à 3*, Éléments de mathématique II (Springer-Verlag, Berlin, 2006, 2nd revised ed.).

[2] ———, *Théorie des ensembles*, Éléments de mathématique I (Springer-Verlag, Berlin, 2006, reprint ed.).

[3] A. H. Clifford, 'Totally ordered commutative semigroups', *Bull. Amer. Math. Soc.* (6) **64** (1958), 305–316.
[4] G. Freiman, M. Herzog, P. Longobardi, and M. Maj, 'Small doubling in ordered groups', *J. Austral. Math. Soc.*, to appear.
[5] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations: Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics **278** (Chapman & Hall/CRC, 2006).
[6] R. Gilmer, *Commutative Semigroup Rings* (University Of Chicago, Chicago, 1984).
[7] J. S. Golan, *Semirings and their Applications* (Kluwer Academic Publishers, Dordrecht, 1999).
[8] U. Hebisch and H. J. Weinert, *Semirings: Algebraic Theory and Applications in Computer Science*, Series in Algebra **5** (World Scientific, 1998).
[9] J. M. Howie, *Fundamentals of semigroup theory* (Clarendon Press, Oxford, 2003, reprint ed.).
[10] K. Iwasawa, 'On linearly ordered groups', *J. Math. Soc. Japan* **1** (1948), 1–9.
[11] R. E. Johnson, 'Extended Malcev Domains', *Proc. Amer. Math. Soc.* (1) **21** (Apr., 1969), 211–213.
[12] F. W. Levi, 'Arithmetische Gesetze im Gebiete diskreter Gruppen', *Rend. Circ. Mat. Palermo* **35** (1913), 225–236.
[13] A. Malcev, 'On the immersion of an algebraic ring into a field', *Math. Ann.* (1) **113** (1937), 686–691.
[14] ———, 'On ordered groups', *Izv. Akad. Nauk. SSSR Ser. Mat.* **13** (1948), 473–482.
[15] M. B. Nathanson, *Additive Number Theory: Inverse Problems and Geometry of Sumsets*, Graduate Texts in Mathematics **165** (Springer-Verlag, New York, 1996).
[16] B. H. Neumann, 'On ordered groups', *Amer. J. Math.* **71** (1949), 1–18.
[17] D. Rolfsen and J. Zhu, 'Braids, orderings and zero divisors', *J. Knot Theory Ramifications* (6) **7** (1998), 837–841.
[18] I. Z. Ruzsa, 'Sumsets and structure', in: *Combinatorial Number Theory and Additive Group Theory* (Birkhäuser Verlag, Basel, 2009), 87–210.
[19] T. Tao and V. H. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics **105** (Cambridge University Press, Cambridge, 2009).

CMLS, École polytechnique - 91128 Palaiseau cedex, France
Web site: http://www.math.polytechnique.fr/~tringali/
E-mail address: salvatore.tringali@cmls.polytechnique.fr