Some questions in combinatorial and elementary number theory

Salvatore Tringali

Thèse de l'Université de Lyon

présentée

à l'Université Jean MONNET de Saint-Étienne

École Doctorale Sciences, Ingéniérie, Santé ED SIS 488

par

Salvatore Tringali

sous la direction de François Hennecart et Alain Plagne

pour obtenir le grade de

Docteur

Specialité : Mathématiques Pures

Quelques questions de théories combinatoire et élémentaire des nombres

(Some Questions in Combinatorial and Elementary Number Theory)

Après avis de

Alfred Geroldinger, Professeur	Karl-Franzens-Universität Graz	Rapporteur
Gilles Zémor, Professeur	Université Bordeaux 1	Rapporteur

Devant la commission d'examen formée de

Éric Balandraud, Maître de conférences	Université Pierre et Marie Curie	Examinateur
Georges Grekos, Maître de conférences	Université de Saint-Étienne	Examinateur
Laurent Habsieger, Directeur de recherche	UMI-CRM, CNRS	Examinateur
François Hennecart, Professeur	Université de Saint-Étienne	Directeur
Federico Pellarin, Professeur	Université de Saint-Étienne	Examinateur
Alain Plagne, Chercheur	École polytechnique	Directeur

Résumé

Cette thèse consiste essentiellement en la concaténation de contributions variées à la théorie additive des structures algébriques comme les groupes, les anneaux et leurs généralisations, d'une part, et à la théorie élémentaire des nombres, d'autre part. En conséquence, la présentation sera divisée en deux parties, partie I et partie II, qui sont indépendantes l'une de l'autre et se composent, respectivement, de trois et deux chapitres.

Dans la première partie, nous prouvons un certain nombre de résultats concernant la théorie additive des groupes (pas nécessairement commutatifs), mais nous le faisons dans le cadre plus large et abstrait des semi-groupes (éventuellement non-commutatifs). Notre philosophie à cet égard peut être résumée dans le méta-principe suivant : plus faibles sont les hypothèses structurelles, plus grand est le nombre de problèmes que nous pouvons espérer résoudre, tout en essayant d'arriver à une meilleure compréhension de leur nature intime.

Les sommes d'ensembles, principalement dans le cadre des groupes commutatifs, ont été intensivement étudiés depuis plusieurs années (voir [Ru] pour un survol récent). Également des résultats intéressants ont été obtenus pour le cas des monoïdes commutatifs et cancellatifs par A. Geroldinger et ses coauteurs ; voir, par exemple, [G] et les références citées là (en notation additive, "cancellatif" veut dire que $a + c = b + c$ ou $c + a = c + b$ impliquent $a = b$). Mais presque rien n'est connu sur la théorie additive des semi-groupes, et l'un des objectifs du présent travail est de contribuer à l'exploration de cette théorie et de convaincre, nous l'espérons, le lecteur que le sujet est plus intéressant que l'on pourrait peut-être le suspecter.

Une première motivation naturelle pour s'intéresser aux semi-groupes vient de l'observation que l'ensemble des éléments non nuls d'un anneau à unité non-trivial (commutatif ou non) n'est pas, en

général, cancellatif (sauf si l'anneau est sans diviseurs de zéro), et par conséquent n'est même pas fermé pour la multiplication. Une autre motivation est liée au fait que, même si $\mathbb{A} = (A, +)$ est un groupe, les sous-ensembles non vides de A, munis de l'opération binaire qui envoie une paire (X, Y) sur la somme $X + Y$, ne forment en général rien de plus qu'un monoïde non cancellatif (par exemple, quand $\mathbb{A}$ est $(\mathbb{Z}, +)$, la structure correspondante sur les parties de A a été étudiée par J. Cilleruello, Y. ould Hamidoune et O. Serra [CHS]).

A cet égard, il semble utile de mentionner une chose. Bien que chaque semi-groupe commutatif et cancellatif puisse être immergé dans un groupe (comme il résulte de la construction standard du groupe de fractions d'un monoïde ; voir [B1, chapitre I, section 2.4]), rien de semblable n'est vrai dans le cas non-commutatif, pas même dans le cas de type fini. Ceci est lié à une question bien connue en théorie des semi-groupes, d'abord résolue par A. I. Mal'cev dans [Ma]. Ce résultat est d'une importance fondamentale pour notre travail sur ce point dans la mesure où il démontre que l'étude des sommes d'ensembles dans les semi-groupes ne peut pas être systématiquement réduite, en l'absence de commutativité, au cas des groupes (en tout cas, pas de façon évidente). En fait, l'exemple de Mal'cev est basé sur le quotient du semi-groupe libre sur huit lettres par une congruence appropriée, et le semi-groupe correspondant est non seulement de type fini, mais aussi linéairement (c'est-à-dire, strictement et totalement) ordonnable.

La Partie I se compose de trois chapitres (chapitres 1, 2 et 3). Dans le premier chapitre, qui est basé sur un article par l'auteur [Tr1] publié dans *Uniform Distribution Theory*, on généralise la transformée de Davenport [V] et on l'utilise pour prouver que, si $\mathbb{A} = (A, +)$ est un semi-groupe cancellatif (éventuellement non-commutatif) et X, Y sont des sous-ensembles non vides de A tels

que le sous-semi-groupe engendré par Y est commutatif, on a

$$|X+Y| \geq \min(\gamma(Y), |X|+|Y|-1),$$

où $\gamma(Y)$, qu'on appelle la constante de Cauchy-Davenport de Y relative au semi-groupe $\mathbb{A}$, est définie par

$$\gamma(Y) := \sup_{y_0 \in Y^\times} \inf_{y_0 \neq y \in Y} \mathrm{ord}(y - y_0).$$

Cela généralise le théorème classique de Cauchy-Davenport [C] [D1] [D2] au cadre plus large des semi-groupes, avec comme cas particuliers une extension des théorèmes de I. Chowla [Ch] et S. S. Pillai [Pi] pour les groupes cycliques et une version plus forte d'une autre généralisation du même théorème de Cauchy-Davenport pour les groupes commutatifs, où dans la formule ci-dessus $\gamma(Y)$ est remplacé par l'infimum des ordres d'un sous-semi-groupe non trivial de l'unitarisation de $\mathbb{A}$. Ce dernier résultat a été prouvé par G. Károlyi dans le cas des groupes finis, grâce au théorème de Feit-Thompson ; puis par Hamidoune pour un groupe arbitraire. L'approche d'Hamidoune passe par sa généralisation d'un théorème additif de L. Shatrowsky et il est en définitive construit sur sa méthode isopérimétrique.

Dans le deuxième chapitre, qui s'appuie sur un papier par l'auteur [Tr2] soumis pour publication, on fait une étude plus approfondie des propriétés de la constante de Cauchy-Davenport (introduite dans le chapitre précédent) pour montrer l'extension supplémentaire suivante du théorème de Cauchy-Davenport : si $(A, +)$ est un semi-groupe cancellatif et si $X, Y \subseteq A$, alors

$$|X+Y| \geq \min(\gamma(X+Y), |X|+|Y|-1).$$

Cela implique une généralisation de l'inégalité de Kemperman pour les groupes sans torsion [Ke] et aussi une version plus forte du théorème d'Hamidoune-Károlyi mentionné ci-dessus. Ici, on donne une preuve indépendante et totalement combinatoire du cas général de ce résultat, qui ne dépend ni du théorème de Feit-Thompson ni de la méthode isopérimétrique. Enfin, on se penche sur certains aspects d'une conjecture qui, si elle était vraie, pourrait fournir une formulation unifiée de beaucoup de théorèmes de type Cauchy-Davenport, y compris ceux-là déjà prouvés dans le chapitre 1.

Enfin, le troisième chapitre généralise des résultats par G. A. Freĭman, M. Herzog et leurs coauteurs sur la théorie structurelle des sommes d'ensembles dans les groupes ordonnés [FHLM] au cas plus général des semi-groupes ordonnés. En particulier, on prouve que, si $(A, \cdot, \preceq)$ est un semi-groupe linéairement ordonné et S est un sous-ensemble fini de A engendrant un sous-semi-groupe non-abélien, alors $|S^2| \geq 3|S|-2$. Au cours de la preuve, on obtient également un grand nombre de résultats secondaires, et notamment que le commutateur et le normalisateur d'un sous-ensemble fini d'un semi-groupe linéairement ordonné coïncident. Ce chapitre est basé sur un article par l'auteur [Tr3] soumis pour publication.

La deuxième partie de la thèse traite de questions de théorie élémentaire des nombres, avec un accent particulier sur les congruences, les nombres premiers et la divisibilité. Cette partie est composée de deux chapitres (chapitres 4 et 5).

Dans le chapitre 4, on prouve des résultats liés à une conjecture par K. Győry et C. Smyth [GS] sur la finitude des ensembles $R_k^{\pm}(a, b)$ de tous les entiers n tels que n^k divide $a^n \pm b^n$ pour des entiers fixés a, b et k avec $k \geq 3$, $|ab| \geq 2$ et $\gcd(a, b) = 1$: en particulier, on démontre que les ensembles $R_k^{\pm}(a, b)$ sont finis si $k \geq \max(|a|, |b|)$. Le chapitre s'appuie sur un article par l'auteur [Tr4] publié dans *Integers*.

Enfin, dans le chapitre 5, nous considérons une question de divisibilité dans l'anneau des entiers, en quelque sorte liée au problème de Znám et à la conjecture Agoh-Giuga. Plus précisément, étant donné un entier $n \geq 3$, soient $u_1, \ldots, u_n$ des entiers premiers entre eux deux à deux pour lesquels $2 \leq u_1 < \cdots < u_n$, soit $\mathcal{D}$ une famille de sous-ensembles propres et non vides de $\{1, \ldots, n\}$ qui contient un nombre "suffisant" d'éléments, et soit ε une fonction $\mathcal{D} \to \{\pm 1\}$. Existe-t-il au moins un nombre premier q tel que q divise $\prod_{i \in I} u_i - \varepsilon(I)$ pour un certain $I \in \mathcal{D}$, mais ne divise pas $u_1 \cdots u_n$? Nous donnons une réponse positive à cette question dans le cas où les u_i sont des puissances de nombres premiers si on impose certaines restrictions sur ε et $\mathcal{D}$. Nous utilisons ce résultat pour prouver que, si $\varepsilon_0 \in \{\pm 1\}$ et si A est un ensemble de trois ou plus nombres premiers qui contient les diviseurs premiers des tous les nombres de la forme $\prod_{p \in B} p - \varepsilon_0$ pour lesquels B est un sous-ensemble propre, fini et non vide de A, alors A contient tous les nombres premiers. Le chapitre est basé sur un article par Paolo Leonetti et l'auteur [Tr5] accepté pour publication au *Journal de Théorie des Nombres de Bordeaux*.

This page intentionally left blank

Abstract

The present thesis is basically a recollection of several sparse contributions to the additive theory of group-like and ring-like structures, on the one hand, and to the elementary theory of numbers, on the other hand. Accordingly, the presentation will be subdivided into two parts, namely Part I and Part II, which are essentially independent from each other and consist, respectively, of three and two chapters.

In the first part, we prove a number of results concerning the additive theory of (possibly non-commutative) groups, but we do it in the broader and more abstract setting of (possibly non-commutative) semigroups. Our philosophy in this respect can be summarized in the following meta-principle: The weaker are the structural assumptions, the larger is the class of problems that we can hope to solve, while trying to get a deeper understanding.

Sumsets in (mostly commutative) groups have been intensively investigated for several years (see [Ru] for a recent survey), and interesting results have been also obtained in the case of commutative and cancellative monoids by A. Geroldinger and coauthors; see, e.g., [G] and references therein (in additive notation, "cancellative" means that $a + c = b + c$ or $c + a = c + b$ imply $a = b$). But almost nothing is known on the additive theory of semigroups, and one of the goals of the present work is to contribute to the investigation of the theory and to convince the reader, we hope, that the subject is more interesting than one would possibly suspect.

A natural motivation in this sense comes from considering that the non-zero elements of a non-trivial unital ring, either commutative or not, are not, in general, cancellative (unless the ring is a domain), and hence not even closed under multiplication. Another motivation relies on the fact that, even when $\mathbb{A} = (A, +)$ is a group, the non-empty subsets of A, endowed with the binary op-

eration taking a pair (X, Y) to the sumset $X+Y$, is, in general, nothing more than a non-cancellative monoid (e.g., when $\mathbb{A}$ is $(\mathbb{Z}, +)$, the corresponding structure on the powerset of A has been studied by J. Cilleruello, Y. ould Hamidoune and O. Serra [CHS]).

In this respect, one thing seems worth mentioning. While 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 [B1, Chapter I, Section 2.4]), nothing similar is true in the non-commutative case, not even if the ambient semigroup is finitely generated. This is related to a well-known question in the theory of semigroups, first answered by A. I. Mal'cev in [Ma], and is of fundamental importance for our work here, in that it shows that the study of sumsets in cancellative semigroups cannot be systematically reduced, in the absence of commutativity, to the case of groups (at the very least, not in any obvious way). In fact, Mal'cev's example involves the quotient of the free semigroup over eight letters by a suitable congruence, and it is not only finitely generated, but even linearly orderable (here, a semigroup $(A, +)$ is called linearly orderable if there exists a total order $\preceq$ on A such that $x+z \prec y+z$ and $z+x \prec z+y$ for all $x, y, z \in A$ with $x \prec y$).

Part I consists of three chapters, namely Chapters 1, 2 and 3. In the first chapter, based on a paper by the author [Tr1] published in *Uniform Distribution Theory*, we generalize the Davenport transform [V] and use it to prove that, for a (possibly non-commutative) cancellative semigroup $\mathbb{A} = (A, +)$ and non-empty subsets X, Y of A such that the subsemigroup generated by Y is commutative, we have

$$|X + Y| \geq \min(\gamma(Y), |X| + |Y| - 1),$$

where

$$\gamma(Y) := \sup_{y_0 \in Y^\times} \inf_{y_0 \neq y \in Y} \mathrm{ord}(y - y_0)$$

is what we call the Cauchy-Davenport constant of Y (relative to $\mathbb{A}$). This generalizes the classical Cauchy-Davenport theorem [C] [D1] [D2] to the setting of semigroups, and it implies, in particular, an extension of I. Chowla's [Ch] and S. S. Pillai's [Pi] theorems for cyclic groups, as well as a strengthening of another generalization of the same Cauchy-Davenport theorem to the case of commutative groups, where $\gamma(Y)$ in the above formula is replaced by the infimum of the order of the non-trivial subsemigroups of the (conditional) unitization of $\mathbb{A}$. In fact, a proof of this latter result was first given by G. Károlyi in 2005 for the special case of finite groups [Ka], based on the structure theory of group extensions, by reduction to finite solvable groups in the light of the Feit-Thompson theorem. Then, a more "elementary" proof of the general statement (for an arbitrary group) was communicated to Károlyi by Hamidoune during the peer-review process of Károlyi's paper and included in the final version of the manuscript [Ka]. Hamidoune's approach depends on a generalization of an addition theorem by L. Shatrowsky and is ultimately built upon the isoperimetric method.

In the second chapter, which is founded on a paper by the author [Tr2] submitted for publication, we further investigate the properties of the Cauchy-Davenport constant and use them to prove the following: If $\mathbb{A}$ is cancellative and $X, Y \subseteq A$, then

$$|X + Y| \geq \min(\gamma(X + Y), |X| + |Y| - 1).$$

This implies at once a generalization of Kemperman's inequality for torsion-free groups [Ke] and a strengthening of the Hamidoune-Károlyi theorem mentioned in the above. Our proof of this is

basically a transformation proof; in particular, it is self-contained and does not depend on either the Feit-Thompson theorem or the isoperimetric method. In addition, we present and discuss aspects of a conjecture which, if true, would further improve most of the results in the chapter and provide a unified picture of many more theorems of Cauchy-Davenport type, including the ones proved in Chapter 1.

Finally, Chapter 3 generalizes results by G. A. Freĭman, M. Herzog and coauthors on the structure theory of set addition from the context of linearly ordered groups [FHLM] to linearly ordered semigroups. In particular, we find that, if $(A, \cdot, \preceq)$ is a linearly ordered semigroup and S is a finite subset of A generating a non-abelian subsemigroup, then $|S^2| \geq 3|S| - 2$. On the road to this goal, we also prove a number of subsidiary results, and most notably that the commutator and the normalizer of a finite subset of a linearly ordered semigroup are equal to each other. The chapter is based on a paper by the author [Tr3] submitted for publication.

The second part of the thesis, on the other hand, deals with questions from the elementary theory of numbers, with a focus on congruences, prime numbers and divisibility in the integers.

Part II is composed of two chapters, namely Chapters 4 and 5. In Chapter 4 we prove a result related to a difficult conjecture by K. Győry and C. Smyth [GS] about the finiteness of the sets $R_k^{\pm}(a, b)$ of all positive integers n such that n^k divides $a^n \pm b^n$ for fixed integers a, b and k with $k \geq 3$, $|ab| \geq 2$ and $\gcd(a, b) = 1$: Specifically, we show that $R_k^{\pm}(a, b)$ are finite sets if $k \geq \max(|a|, |b|)$. The chapter relies on a paper by the author [Tr4] published in *Integers*.

Finally, in Chapter 5 we consider a question in the study of primes and divisibility in the ring of integers, somehow related to Znám's problem and the Agoh-Giuga conjecture. Specifically, given an integer $n \geq 3$, let $u_1, \ldots, u_n$ be pairwise coprime integers for which $2 \leq u_1 < \cdots < u_n$, and let $\mathcal{D}$ be a family of nonempty proper subsets of $\{1, \ldots, n\}$ with "enough" elements and ε a map

$\mathcal{D} \to \{\pm 1\}$. It is then natural to ask whether there exist at least one prime q such that q divides $\prod_{i\in I} u_i - \varepsilon(I)$ for some $I \in \mathcal{D}$, but it does not divide $u_1 \cdots u_n$. In fact, we answer this in the positive in the case where the integers u_i are prime powers and some restrictions hold on ε and $\mathcal{D}$. We use the result to prove that, if $\varepsilon_0 \in \{\pm 1\}$ and A is a set of three or more primes that contains all prime divisors of any number of the form $\prod_{p\in B} p - \varepsilon_0$ for which B is a finite nonempty proper subset of A, then A contains all the primes. The chapter is based on a paper by the author [Tr5] (joint work with Paolo Leonetti) accepted for publication in *Journal de Théorie des Nombres de Bordeaux*.

This page intentionally left blank

Table des matières

This page intentionally left blank

This page intentionally left blank

Dédicace

À ma famille. À mes parents : pour le bien que vous me voulez. Pour le bien que je vous veux. Parce que sans vous, je ne serais rien. À ma sœur : pour me rappeler toujours que tout est, en principe, une question de confiance. À mes grands-mères et à mes grands-pères : à ceux qui sont encore en vie et à ceux qui ne sont plus là. Pour m'avoir donné une plage pour écouter la mer et un petit bois pour courir le vent.

À tous ceux que j'ai perdus dans la rue du monde. Je suis heureux de vous avoir connus. Pour ce que vous avez simplement signifié. Pour les sourires soudains que le passant ne comprendra jamais. Et même pour la mélancolie que je porte dans les poches du cœur, avec les souvenirs dont la mémoire ne se souvient plus.

À mes amis, et à Giovanni d'une façon particulière. S'ils ne sont pas nombreux, ils me sont en revanche très chers sans que cela ne coûte rien.

Aux artistes. Parce qu'ils me rendent le monde des hommes plus beau. Aux musiciens : pour la musique. Aux écrivains : pour les romans. Aux poètes : pour la joie et la tristesse de la parole. Aux chanteurs : pour les chansons. Et aux jardiniers : pour les roses dans les jardins de la ville.

Aux personnes généreuses. À ceux qui regardent les autres pour ce qu'ils sont, sans a priori. À ceux qui sont grands sans être arrogants. À ceux qui sont extraordinaires parce que, personnes simples, ils font des choses parfois très compliquées. Cette thèse n'a été possible que parce que j'ai eu la chance d'en rencontrer beaucoup.

Aux rêveurs. Pour être ce qu'ils sont, malgré celui qui leur a dit que les rêves sont aujourd'hui démodés. Pour être déraisonnables, têtus, téméraires et fous. Et à moi même, enfin. Pour être un peu tout cela. Sans doute.

Remerciements

Merci à mes directeurs de thèse, François Hennecart et Alain Plagne : rien de tout cela n'aurait été possible sans leur confiance et leur soutien, moral et matériel. Et un remerciement particulier à Alain : son écoute, ses conseils et son amitié m'ont été precieux durant ces longs mois, aussi bien que la chanson française, dont j'apprends de jour en jour, grâce à lui, à apprécier la beauté, la poésie et l'humanité.

Merci également à tous ceux qui ont contribué à l'aboutissement de cette thèse. Merci tout spécialement aux rapporteurs, Alfred Geroldinger et Gilles Zémor, pour leur généreuse appréciation de mon travail, et aux membres du jury, Eric Balandraud, Georges Grekos, Laurent Habsieger et Federico Pellarin, pour avoir accepté d'en faire partie. Une pensée spéciale pour Éric et Georges, avec qui j'ai eu la chance d'avoir des échanges concrets à l'occasion de la préparation de cette thèse et qui m'ont toujours encouragé.

This page intentionally left blank

This page intentionally left blank

Cualquier destino, por largo y complicado que sea, consta en realidad de un solo momento: el momento en que el hombre sabe para siempre quién es.

— Jorge Luis Borges, *El Aleph*

0

General formalities

Resumé. Le but de ce bref chapitre est de rappeler les définitions de base et de fixer les notations et la terminologie générales. Nous faisons tout d'abord une courte digression sur la théorie des ensembles, qui pour pédante qu'elle puisse sembler aux praticiens, se révèle nécessaire au vu des développements à venir.

Abstract. The purpose of this brief chapter is to review basic definitions and fix some general terminology and notation. We make first a short digression into set theory, which may sound pedantic to practitioners, but is necessary in view of certain developments, on which we hope to work in the future.

0.1 Preliminaries and general notation

We use as a foundation the Tarski-Grothendieck set theory, shortly TG. Alternatives are possible, but this issue exceeds the scope of the thesis, and we can pass over it. We just mention that we choose to work in TG, rather than, say, in ZFC (the classical Zermelo-Fraenkel set theory with the axiom of choice), motivated by the fact that we will hopefully be concerned, in a sequel of this work, with objects like the "class of all structures of a certain type", which would make no sense in ZFC, essentially because the latter does not allow for anything like the "class of all sets". With this in mind, we fix once and for all an uncountable Grothendieck universe Ω, and refer to the elements of Ω as Ω-sets, or simply sets, and to an *arbitrary* set in the ontology of TG as a class, a family, or a collection.

We write $\mathbb{Z}$ for the integers, $\mathbb{N}^+$ for the positive integers, $\mathbb{Q}$ for the rationals, $\mathbb{R}$ for the real numbers, and $\mathbb{R}^+$ for the positive real numbers. Then, we let $\mathbb{N} := \{0\} \cup \mathbb{N}^+$ and $\mathbb{R}_0^+ := \{0\} \cup \mathbb{R}^+$. Each of these sets is regarded as a subset of $\mathbb{R}$ and endowed with its usual addition $+$, multiplication $\cdot$, absolute value $|\cdot|_\infty$ and order $\leq$ (as customary, we write $\geq$ for the dual of $\leq$, and $<$ and $>$, respectively, for the strict orders induced by $\leq$ and $\geq$). Moreover, we denote by $\mathbb{P}$ the set $\{2, 3, \ldots\}$ of all (positive rational) primes, and for $m \in \mathbb{N}^+$ we write $\mathbb{Z}/m\mathbb{Z}$ for the integers modulo m, equipped with the usual addition $+_m$ and multiplication $\cdot_m$ (we omit the subscript 'm' if there is no danger of confusion).

We extend the operations and the order of $\mathbb{R}$ to $\mathbb{R} \cup \{\infty\}$, by adjoining a "point at infinity", viz an element $\infty \notin \mathbb{R}$ (in fact, we may assume $\infty := \mathbb{R}$), and by taking $a + \infty := \infty + a := \infty$ and $a \leq \infty$ for $a \in \mathbb{R} \cup \{\infty\}$, as well as $a \cdot \infty := \infty \cdot a := \infty$ if $a \neq 0$ and $0 \cdot \infty := \infty \cdot 0 := 0$. Accordingly, we set $\frac{1}{0} := \infty$ and $\frac{0}{0} := 0 \cdot \frac{1}{0} = 0 \cdot \infty = 0$.

We use capital blackboard letters such as $\mathbb{A}$ and $\mathbb{B}$, with or without subscripts or superscripts, to denote *structured classes* (or simply *structures*), by which we mean here any tuple consisting of one class, referred to as the carrier of the structure, and a finite number of operations or relations of finite ariety on the same class such as $(A, +)$, $(B, \perp)$, or $(C, +, \cdot, 0, \preceq)$. Accordingly, if $\mathbb{A}$ is a structure and A its carrier, we write $a \in \mathbb{A}$ to mean on the one hand that a is an element of A, and on the other to emphasize that, in the context of the discourse, any statement involving the element a should be interpreted, in the presence of ambiguity, with respect to the structure of $\mathbb{A}$ (this is typically the case where, by an abuse of notation, operations or relations of different structures are

denoted by the same symbol). The same principle applies to subclasses, so that we may occasionally write $S \subseteq \mathbb{A}$ in place of $S \subseteq A$. Since every class can be viewed as a "vacuous structure", the above is perfectly consistent with the fact that we are using blackboard letters like $\mathbb{N}$, $\mathbb{Z}$, etc. to refer to some special sets of numbers.

We write $|X|$ for the counting measure of a set X (this is just the number of elements of X when X is finite), by interpreting $|\cdot|$ as a map from Ω to $\mathbb{N} \cup \{\infty\}$.

At several points throughout the thesis, we will use without explicit mention the elementary fact that if $A \subseteq B \subseteq \mathbb{R}_0^+ \cup \{\infty\}$ then $\inf(B) \leq \inf(A)$ and $\sup(A) \leq \sup(B)$, with the convention that the supremum and the infimum of an empty subset of $\mathbb{R}_0^+ \cup \{\infty\}$ are, respectively, 0 and ∞. Note that, here and later, infima and suprema of subsets of $\mathbb{R}_0^+ \cup \{\infty\}$, as well as minima and maxima (when defined) are always taken with respect to (the appropriate restriction of) the order $\leq$.

Given $a, b \in \mathbb{Z}$ with $a^2 + b^2 \neq 0$ we use $\gcd(a, b)$ for the greatest common divisor of a and b. Also, for $c \in \mathbb{Z} \setminus \{0\}$ and $p \in \mathbb{P}$, we write $e_p(c)$ for the p-adic valuation of c, namely the greatest exponent $k \in \mathbb{N}$ such that $p^k \mid c$, and we extend this to $\mathbb{Z}$ by $e_p(0) := \infty$. Finally, for $m \in \mathbb{N}^+$ and $x \in \mathbb{Z}/m\mathbb{Z}$ we let $\gcd(m, x) := \gcd(m, \bar{x})$, where $\bar{x}$ is the smallest non-negative integer in x.

Unless otherwise specified, we refer to N. Bourbaki, *Théorie des ensembles*, Éléments de mathématique I, Springer-Verlag, Berlin, 2006 (reprint ed.) and N. Bourbaki, *Algèbre, Chapitres 1 à 3*, Éléments de mathématique II, Springer-Verlag, Berlin, 2006 (2nd revised ed.), respectively, for standard notations and definitions from set theory and abstract algebra.

In all what follows, the lowercase Latin letters h and k shall denote integers, while i, j, ℓ, m and n stand for positive integers, unless a statement to the contrary is made.

This page intentionally left blank

Part I

Additive Semigroup Theory

This page intentionally left blank

Il mare è senza strade, il mare è senza spiegazioni.
Se lo guardi non te ne accorgi: di quanto rumore faccia.

— Alessandro Baricco, *Oceano Mare*

1

Cauchy-Davenport type theorems, I

Resumé. On généralise la transformée de Davenport et on l'utilise pour prouver que, si $\mathbb{A} = (A, +)$ est un semi-groupe cancellatif (éventuellement non-commutatif) et X, Y sont des sous-ensembles non vides de A tels que le sous-semi-groupe engendré par Y est commutatif, on a $|X + Y| \geq \min(\gamma(Y), |X| + |Y| - 1)$, où $\gamma(Y)$, qu'on appelle la constante de Cauchy-Davenport de Y relative au semi-groupe $\mathbb{A}$, est définie par

$$\gamma(Y) := \sup_{y_0 \in A^\times} \inf_{y_0 \neq y \in Y} \mathrm{ord}(y - y_0).$$

Cela généralise le théorème classique de Cauchy-Davenport au cadre plus large des semi-groupes, avec comme cas particuliers une extension des théorèmes de I. Chowla et S. S. Pillai pour les groupes cycliques et une version plus forte d'une autre généralisation du théorème de Cauchy-Davenport pour les groupes commutatifs, où dans la formule ci-dessus $\gamma(Y)$ est remplacé par l'infimum de $|S|$

sur les sous-semigroupes S non triviaux de l'unitarisation de $\mathbb{A}$. Ce dernier résultat a été prouvé par G. Károlyi dans le cas des groupes finis, grâce au théorème de Feit-Thompson ; puis par Hamidoune pour un groupe arbitraire grâce à sa méthode isopérimétrique. Le chapitre est basé sur un papier par l'auteur [Tr1] publié dans *Uniform Distribution Theory*.

Abstract. We generalize the Davenport transform and use it to prove that, for a (possibly non-commutative) cancellative semigroup $\mathbb{A} = (A, +)$ and non-empty subsets X, Y of A such that the subsemigroup generated by Y is commutative, we have $|X+Y| \geq \min(\gamma(Y), |X| + |Y| - 1)$, where

$$\gamma(Y) := \sup_{y_0 \in A^\times} \inf_{y_0 \neq y \in Y} \mathrm{ord}(y - y_0).$$

This carries over the Cauchy-Davenport theorem to the broader setting of semigroups, and it implies, in particular, an extension of I. Chowla's and S. S. Pillai's theorems for cyclic groups and a strengthening of another generalization of the same Cauchy-Davenport theorem to commutative groups, where $\gamma(Y)$ in the above is replaced by the infimum of $|S|$ as S ranges over the non-trivial subsemigroups of the (conditional) unitization of $\mathbb{A}$. This latter result was first proved by G. Károlyi in 2005 for the special case of finite groups [Ka], by reduction to simple groups by the Feit-Thompson theorem, and later by Y. O. Hamidoune for an arbitrary group, building upon the isoperimetric method. The chapter is based on a paper by the author [Tr1] published in *Uniform Distribution Theory*.

1.1 Introduction

Semigroups are a natural framework for developing large parts of theories traditionally presented in less general contexts. Not only this can suggest new directions of research and shed light on questions primarily focused on groups, but it also makes methods and results otherwise restricted to "richer settings" applicable, at least in principle, to larger classes of problems.

Here and later, a *semigroup* is a structure $\mathbb{A} = (A, +)$ consisting of a (possibly empty) set A and an associative binary operation $+$ on A. Given subsets X and Y of A, we define the sumset, relative

to $\mathbb{A}$, of the pair (X, Y) as the set

$$X + Y := \{x + y : x \in X, y \in Y\},$$

which is written as $x + Y$ if $X = \{x\}$ (respectively, as $X + y$ if $Y = \{y\}$). Furthermore, we extend the notion of difference set by

$$X - Y := \{z \in A : (z + Y) \cap X \neq \emptyset\} \tag{1.1}$$

and

$$-X + Y := \{z \in A : (X + z) \cap Y \neq \emptyset\}. \tag{1.2}$$

Expressions involving one or more summands of the form $Z_1 + \cdots + Z_n$ or $\sum_{i=1}^{n} Z_i$, as well as expressions of the form $-x + Y$ and $X - y$ for $x, y \in A$ are defined in a similar way (we may omit the details); in particular, we use nZ for $Z_1 + \cdots + Z_n$ if the Z_i are all equal to the same set Z, and we possibly refer to nZ as the n-fold sum of Z.

We say that $\mathbb{A}$ is unital, or a *monoid*, if there exists $0 \in A$ such that $z + 0 = 0 + z = z$ for all z; when this is the case, 0 is unique and called *the* identity of $\mathbb{A}$. Then, we let $\mathbb{A}^\times$ be the set of units of $\mathbb{A}$, so that $\mathbb{A}^\times = \emptyset$ if $\mathbb{A}$ is not a monoid. In this respect, we recall that, if $\mathbb{A}$ is unital with identity 0, a *unit* of $\mathbb{A}$ is an element z for which there exists a provably unique element $\tilde{z} \in A$ such that $z + \tilde{z} = \tilde{z} + z = 0$; this $\tilde{z}$ is then called *the* inverse of z in $\mathbb{A}$ and denoted by $(-z)_{\mathbb{A}}$, or simply by $-z$ if no ambiguity can arise.

Given $Z \subseteq A$, we write $Z^\times$ in place of $Z \cap \mathbb{A}^\times$ (if there is no likelihood of confusion) and $\langle Z \rangle_{\mathbb{A}}$ for the smallest sub*semigroup* of $\mathbb{A}$ containing Z. Note that $\mathbb{A}$ is a group if and only if $A^\times = A$. Then, if $Z = \{z\}$, we use $\langle z \rangle_{\mathbb{A}}$ instead of $\langle \{z\} \rangle_{\mathbb{A}}$ and $\mathrm{ord}_{\mathbb{A}}(z)$ for the *order* of z (in $\mathbb{A}$), that is we let $\mathrm{ord}_{\mathbb{A}}(z) := |\langle z \rangle_{\mathbb{A}}|$, so generalizing the notion of order for the elements of a group. Here and later, the subscript '$\mathbb{A}$' may be omitted from the notation if $\mathbb{A}$ is clear from the context. Finally, an element $z \in A$ is called cancellable (in $\mathbb{A}$) if $x + z = y + z$ or $z + x = z + y$ for $x, y \in A$ implies $x = y$ (see [B1, Section I.2.2]), and $\mathbb{A}$ is said cancellative if any element of A is cancellable.

On another hand, we define the *conditional unitization* of $\mathbb{A}$, herein denoted by $\mathbb{A}^{(0)}$ and simply referred to as the unitization of $\mathbb{A}$, as follows: If $\mathbb{A}$ is *not* unital, $\mathbb{A}^{(0)}$ is the pair $(A \cup \{A\}, +)$, where $+$ is, by an abuse of notation, the unique extension of $+$ to a binary operation on $A \cup \{A\}$ for which

A serves as an identity (note that $A \notin A$, so loosely speaking we are just adjoining a distinguished element to A and extending the structure of $\mathbb{A}$ in such a way that the outcome is a monoid whose identity is the adjoined element); otherwise $\mathbb{A}^{(0)} := \mathbb{A}$ (cf. [Ho, p. 2]). Then, for a subset S of A we write $\mathfrak{p}_{\mathbb{A}}(S)$ for $\inf_{z \in S \setminus \{0\}} \mathrm{ord}_{\mathbb{A}^{(0)}}(z)$, namely the infimum of the order of the non-trivial subsemigroups of $\mathbb{A}^{(0)}$, which is simply denoted by $\mathfrak{p}(S)$ if there is no ambiguity.

Remark 1.1. In the case of a multiplicatively written semigroup $\mathbb{B} = (B, \cdot)$, the "sumset" of two subsets X and Y of B, relative to $\mathbb{B}$, is more properly called the product set of the pair (X, Y) and possibly denoted by XY, while the analogues of the difference sets defined by (1.1) and (1.2) are written as XY^{-1} and $X^{-1}Y$, respectively. Accordingly, given $Z \subseteq B$ we use Z^n for the product set of n copies of Z and call it the n-fold product of Z. Further, we write the unitization of $\mathbb{B}$ as $\mathbb{B}^{(1)}$ rather than as $\mathbb{B}^{(0)}$. However, note that, if we are talking of a semigroup and it is not clear from the context whether this is written either additively or not, the term "sumset" will be preferred. For the rest, everything works as expected.

Sumsets in (mostly commutative) groups have been intensively investigated for several years (see [Ru] for a recent survey), and interesting results have been also obtained in the case of commutative cancellative monoids (see [G] and references therein, where these structures are simply called "monoids"). The chapter aims to extend aspects of the theory to the more general setting of possibly *non-commutative* semigroups.

A natural motivation in this sense comes from considering that the non-zero elements of a non-trivial unital ring, either commutative or not, are not, in general, cancellative (unless the ring is a domain), and hence not even closed under multiplication. Another motivation relies on the fact that, even when $\mathbb{A} = (A, +)$ is a group, the non-empty subsets of A, endowed with the binary operation taking a pair (X, Y) to the sumset $X + Y$, is, in general, nothing more than a non-cancellative monoid (e.g., when $\mathbb{A}$ is $(\mathbb{Z}, +)$, the corresponding structure on the powerset of A has been studied by J. Cilleruello, Y. O. Hamidoune and O. Serra [CHS]; see the discussion at the end of the section for details on this).

Historically, one of the first significant achievements in the field is probably the Cauchy-Davenport theorem, originally established by A.-L. Cauchy [C] in 1813, and independently rediscovered more than a century later by H. Davenport [D1] [D2]:

Theorem 1.2 (Cauchy-Davenport theorem). *Let $(A, +)$ be a group of prime order p and X, Y non-empty subsets of A. Then, $|X + Y| \geq \min(p, |X| + |Y| - 1)$.*

The result has been the subject of numerous papers, and received many different proofs, each favoring alternative points of view and eventually leading to progress on a number of related questions. In fact, the main contribution here is an extension of Theorem 1.2 to cancellative semigroups (this is stated in Section 1.2).

The Cauchy-Davenport theorem applies especially to the additive group of the integers modulo a prime. Extensions to composite moduli have been given by several authors, and notably by I. Chowla [Ch] and S. S. Pillai [Pi]. These results, reported below for the sake of exposition and used by Chowla and Pillai in relation to Waring's problem, are further strengthened, in Section 1.2, by Corollary 1.17, which can be viewed as a common generalization of both of them, and whose proof is sensibly shorter than each of the proofs appearing in [Ch] and [Pi] (not to mention that it comes as a by-product of a deeper result).

Theorem 1.3 (Chowla's theorem). *If X, Y are non-empty subsets of $\mathbb{Z}/m\mathbb{Z}$ such that $0 \in Y$ and $\gcd(m, y) = 1$ for each $y \in Y \setminus \{0\}$, then*

$$|X + Y| \geq \min(m, |X| + |Y| - 1).$$

Theorem 1.4 (Pillai's theorem). *Pick non-empty subsets X and Y of $\mathbb{Z}/m\mathbb{Z}$. Let δ be the maximum of $\gcd(m, y - y_0)$ for distinct $y, y_0 \in Y$ if $|Y| \geq 2$, and set $\delta := 1$ otherwise. Then,*

$$|X + Y| \geq \min(\delta^{-1}m, |X| + |Y| - 1).$$

A partial account of further results in the same spirit can be found in [N, Section 2.3], along with an entire chapter dedicated to Kneser's theorem [N, Chapter 4], which, among the other things, implies Theorem 1.3 (and then also Theorem 1.2); see [N, Section 4.6, Exercises 5 and 6]. Generalizations of the Cauchy-Davenport theorem of a somewhat different flavor have been furnished, still in recent years, by several authors.

Specifically, assume for the rest of the chapter that $\mathbb{A} = (A, +)$ is a fixed, arbitrary semigroup (unless differently specified), and let 0 be the identity of the unitization, $\mathbb{A}^{(0)}$, of $\mathbb{A}$. Then we have:

Theorem 1.5 (folklore)**.** *If $\mathbb{A}$ is a commutative group and X, Y are non-empty subsets of A, then*

$$|X+Y| \geq \min(\mathfrak{p}(\mathbb{A}), |X|+|Y|-1).$$

Theorem 1.5 is another (straightforward) consequence of Kneser's theorem. While it applies to both finite and infinite *commutative* groups, an analogous result holds for all groups:

Theorem 1.6 (Hamidoune-Károlyi theorem)**.** *If $\mathbb{A}$ is a group and X, Y are non-empty subsets of A, then $|X+Y| \geq \min(\mathfrak{p}(\mathbb{A}), |X|+|Y|-1)$.*

This was first proved by G. Károlyi in the case of finite groups, relying on the structure theory of group extensions, by reduction to finite solvable groups in the light of the Feit-Thompson theorem, and then by Hamidoune in the general case, based on the isoperimetric method. In fact, we will give an elementary proof of the Hamidoune-Károlyi theorem in the next chapter, which the reader is referred to for more details on the history of the result.

A further result from the literature that is significant in relation to the subject matter is due to J. H. B. Kemperman [Ke], and reads as follows:

Theorem 1.7 (Kemperman's inequality)**.** *Let $\mathbb{A}$ be a group, and let X, Y be non-empty subsets of A. Suppose that every non-zero element of A has order $\geq |X|+|Y|-1$. Then, $|X+Y| \geq |X|+|Y|-1$.*

Remarkably, [Ke] is focused on *cancellative* semigroups (there simply called semigroups), and it is precisely in this framework that Kemperman establishes a series of results, related to the number of different representations of an element in a sumset, that eventually lead to Theorem 1.7, a weakened version of which will be obtained in Section 1.5 as a corollary (namely, Corollary 1.15) of our main theorem.

As for the rest, Cilleruello, Hamidoune and Serra, see [CHS, Theorem 3], have proved a Cauchy-Davenport theorem for *acyclic* monoids (these are termed acyclic *semigroups* in [CHS], but they are, in fact, *monoids* in our terminology), and it would be interesting to find a common pattern among their result and the ones in the present chapter. Unluckily, we do not have much on this for the moment (in particular, note that acyclic semigroups in [CHS] are not cancellative semigroups), but will come back to the question with some thoughts in the next chapter.

Organization.

In Section 1.2, we define the Cauchy-Davenport constant and state our main results. In Section 1.3, we establish a few basic lemmas. Section 1.4 is devoted to generalized Davenport transforms and their fundamental properties. We demonstrate the central theorem of the chapter (Theorem 1.9) in Section 1.5 and give a couple of applications in Section 1.6.

1.2 The statement of the main results

Keeping all of the above in mind, we can now proceed to the heart of the chapter.

Definition 1.8. For an arbitrary subset X of A, we let

$$\gamma_{\mathbb{A}}(X) := \sup_{x_0 \in X^\times} \inf_{x_0 \neq x \in X} \operatorname{ord}(x - x_0)$$

Then, given $X_1, \dots, X_n \subseteq A$ we define

$$\gamma_{\mathbb{A}}(X_1, \dots, X_n) := \max_{1 \leq i \leq n} \gamma_{\mathbb{A}}(X_i)$$

and call $\gamma_{\mathbb{A}}(X_1, \dots, X_n)$ the Cauchy-Davenport constant of $(X_1, \dots, X_n)$ relative to $\mathbb{A}$ (again, the subscript '$\mathbb{A}$' may be omitted from the notation if there is no likelihood of confusion).

Any pair of subsets of A has a well-defined Cauchy-Davenport constant (relative to $\mathbb{A}$). In particular, $\gamma(Z)$ is zero for $Z \subseteq A$ if $A^\times = \emptyset$. However, this is not the case, for instance, when $Z \neq \emptyset$ and $\mathbb{A}$ is a group, which serves as a "moral base" for the following non-trivial bound:

Theorem 1.9. *Suppose $\mathbb{A}$ is cancellative and let X, Y be non-empty subsets of A such that $\langle Y \rangle$ is commutative. Then, $|X + Y| \geq \min(\gamma(Y), |X| + |Y| - 1)$.*

Theorem 1.9 represents the central contribution of the chapter. Not only it extends the Cauchy-Davenport theorem to the broader setting of semigroups (see Section 1.6), but it also provides a strengthening and a generalization of Theorem 1.5, as is shown below. Any pair of subsets of A has, in fact, a well-defined Cauchy-Davenport constant (relative to $\mathbb{A}$), and it is interesting to compare it with other "structural parameters", as in the following:

Lemma 1.10. *Let X, Y be subsets of A and assume that $\mathbb{A}$ is cancellative and $X^\times + Y^\times$ is non-empty. Then, $\gamma(X,Y) \geq \min(\gamma(X), \gamma(Y)) \geq \gamma(X+Y) \geq \mathfrak{p}(A)$.*

The proof of Lemma 1.10 is deferred to the end of Section 2.3. Note that the result applies, on the level of groups, to *any* pair of non-empty subsets. On the other hand, the following basic example suggests that the lemma is quite pessimistic, insofar as there are some relevant cases where each of the '$\geq$' in its statement can actually be replaced with a "much greater than":

Example 1.11. Let $m \geq 2$ and pick prime numbers p and q with $m < p < q$. Then, set

$$X := \{mk \bmod n : k = 0, \dots, p-1\} \quad \text{and} \quad Y := \{mk \bmod n : k = 1, \dots, p\},$$

where $n := m \cdot p \cdot q$. We have $|X+Y| = 2p$, $\gamma(X) = \gamma(Y) = p \cdot q$ and $\gamma(X+Y) = q$, while $\mathfrak{p}(\mathbb{Z}/n\mathbb{Z})$ is the smallest prime divisor of m, with the result that

$$\mathfrak{p}(\mathbb{Z}/n\mathbb{Z}) < \gamma(X+Y) < \min(\gamma(X), \gamma(Y)) = \gamma(X,Y),$$

and indeed $\mathfrak{p}(\mathbb{Z}/n\mathbb{Z})$ is "much" smaller than $\gamma(X+Y)$ if q is "much" larger than m, and similarly $\gamma(X+Y)$ is "much" smaller than $\gamma(X,Y)$ if p is "much" larger than 2.

Theorem 1.9 can be "symmetrized" and further strengthened when each summand generates a commutative subsemigroup. This leads to the following corollaries, whose proofs are straightforward, by duality (see Proposition 2.8 in Section 2.3), in the light of Definition 1.8:

Corollary 1.12. *Assume $\mathbb{A}$ is cancellative and let X, Y be non-empty subsets of A such that $\langle X \rangle$ is commutative. Then, $|X+Y| \geq \min(\gamma(X), |X| + |Y| - 1)$.*

Corollary 1.13. *If $\mathbb{A}$ is cancellative and X, Y are non-empty subsets of A such that both of $\langle X \rangle$ and $\langle Y \rangle$ are commutative, then $|X+Y| \geq \gamma(X,Y)$.*

Moreover, the result specializes to groups as follows:

Corollary 1.14. *If $\mathbb{A}$ is a group and X, Y are non-empty subsets of A such that $\langle Y \rangle$ is commutative, then $|X+Y| \geq \min(\tilde{\gamma}(Y), |X| + |Y| - 1)$, where now*

$$\tilde{\gamma}(Y) = \sup_{y_0 \in Y} \inf_{y_0 \neq y \in Y} \mathrm{ord}(y - y_0),$$

and indeed $\tilde{\gamma}(Y) = \max_{y_0 \in Y} \inf_{y_0 \neq y \in Y} \mathrm{ord}(y - y_0)$ *if* Y *is finite.*

Proof. Immediate by Theorem 1.9, for on the one hand $\mathbb{A}$ being a group implies $Y = Y^{\times}$, and on the other, a supremum over a non-empty finite set is a maximum. □

The next corollary is now a *partial* generalization of Theorem 1.7 to cancellative semigroups: its proof is straightforward by Corollary 1.13 and Lemma 1.10. Here, we say that $\mathbb{A}$ is torsion-free if $\mathfrak{p}(\mathbb{A})$ is infinite (in fact, this is an abstraction of the classical definition for groups).

Corollary 1.15. *If* $\mathbb{A}$ *is cancellative, and if* X, Y *are non-empty subsets of* $\mathbb{A}$ *such that every element of* $A \setminus \{0\}$ *has order* $\geq |X| + |Y| - 1$ *(this is especially the case when* $\mathbb{A}$ *is torsion-free) and either of* $\langle X \rangle$ *and* $\langle Y \rangle$ *is abelian, then* $|X + Y| \geq |X| + |Y| - 1$.

Theorem 1.9 is proved in Section 1.5. The argument is inspired by the transformation proof originally used for Theorem 1.2 by Davenport in [D1]. This leads us to the definition of what we call a *generalized Davenport transform*. The author is not aware of any earlier use of the same technique in the literature, all the more in relation to semigroups. With few exceptions, remarkably including [HR] and A. G. Vosper's original proof of his famous theorem on critical pairs [V], even the "classical" Davenport transform has not been greatly considered by practitioners in the area, especially in comparison with similar "technology" such as the Dyson transform [N, p. 42].

Remark 1.16. A couple of things are worth mentioning before proceeding. While 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 [B1, Chapter I, Section 2.4]), nothing similar is true in the non-commutative case, not even if the ambient is finitely generated. This is related to a well-known question in the theory of semigroups, first answered by A. I. Mal'cev in [Ma], and is of fundamental importance for our work here, in that it shows that the study of sumsets in cancellative semigroups cannot be systematically reduced, in the absence of commutativity, to the case of groups (at the very least, not in any obvious way). In fact, Mal'cev's example involves the quotient of the free semigroup over eight letters by a suitable congruence, and it is not only finitely generated, but even linearly orderable (see Section 3.2 for the terminology and cf. Remark 3.6).

On the other hand, it is true that every cancellative semigroup can be embedded into a cancellative monoid, so that, for the *specific purposes of the chapter*, we could have assumed almost everywhere that the "ambient" is a monoid (rather than a semigroup), but we did differently because, first, the assumption is not really necessary, and second, it seems more appropriate to develop *as much as possible* of the material with no regard to the presence of an identity (e.g., since this is better suited for the kind of generalizations outlined above). We will see, however, that certain parts take a simpler form when an identity is made available somehow, as in the case of various lemmas in Section 1.3 or in the proof of Theorem 1.9.

We provide two applications of Theorem 1.9 in Section 1.6 (hopefully, others will be investigated in future work): The first is a generalization of Theorem 1.3, the second is an improvement on a previous result by Ø. J. Rødseth [R, Section 6] based on Hall's "marriage theorem". As for the former (which is stated below), we will use the following specific notation: Given a non-empty $Z \subseteq \mathbb{Z}/m\mathbb{Z}$, we let

$$\delta_Z := \min_{z_0 \in Z} \max_{z_0 \neq z \in Z} \gcd(m, z - z_0) \tag{1.3}$$

if $|Z| \geq 2$, and $\delta_Z := 1$ otherwise. With this in hand, we have:

Corollary 1.17. *Let X and Y be non-empty subsets of $\mathbb{Z}/m\mathbb{Z}$ and define $\delta := \min(\delta_X, \delta_Y)$. Then,*

$$|X + Y| \geq \min(\delta^{-1}m, |X| + |Y| - 1).$$

In particular, $|X + Y| \geq \min(m, |X| + |Y| - 1)$ if there exists $y_0 \in Y$ such that $\gcd(m, y - y_0) = 1$ for each $y \in Y \setminus \{y_0\}$ (or dually with X in place of Y).

In fact, Corollary 1.17 contains Chowla's theorem (Theorem 1.3) as a special case: With the same notation as above, it is enough to assume that at least one unit of $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ belongs to Y and $\gcd(m, y) = 1$ for each non-zero $y \in Y$ (or dually with X in place of Y). Also, it is clear from (1.3) that the result is a strengthening of Pillai's theorem (Theorem 1.4).

Many questions arise. Most notably: Is it possible to further extend Corollary 1.13 in such a way to get rid of the assumption that summands generate commutative subsemigroups? Partial answers in this sense will be provided in the next chapter, leading to what we refer to as the Cauchy-Davenport conjecture (namely, Conjecture 2.1).

1.3 Preliminaries

This short section collects basic results used later to introduce the generalized Davenport transforms and prove Theorem 1.9. Some proofs are direct and standard (and thus omitted without further explanation), but we have no reference to anything similar in the context of semigroups, so we include them here for completeness.

Proposition 1.18. *Pick subsets $X_1, Y_1, \dots, X_n, Y_n$ of A such that $X_i \subseteq Y_i$ for each i. Then, $\sum_{i=1}^n X_i \subseteq \sum_{i=1}^n Y_i$ and $\left|\sum_{i=1}^n X_i\right| \leq \left|\sum_{i=1}^n Y_i\right|$.*

Proposition 1.19. *Assume that $\mathbb{A}$ is cancellative, let $n \geq 2$, and pick non-empty $X_1, \dots, X_n \subseteq A$. Then, $\left|\sum_{i=2}^n X_i\right| \leq \left|\sum_{i=1}^n X_i\right|$ and $\left|\sum_{i=1}^{n-1} X_i\right| \leq \left|\sum_{i=1}^n X_i\right|$.*

In spite of being trivial, the next estimate is often useful (cf. [TV, Lemma 2.1, p. 54]).

Proposition 1.20. *Given $X_1, \dots, X_n \subseteq A$, it holds $\left|\sum_{i=1}^n X_i\right| \leq \prod_{i=1}^n |X_i|$.*

Let $X, Y \subseteq A$. No matter whether or not $\mathbb{A}$ is cancellative, nothing similar to Proposition 1.20 applies, in general, to the difference set $X - Y$, which can be infinite even if both of X and Y are not. On another hand, it follows from the same proposition that, in the presence of cancellativity, the cardinality of $X + Y$ is preserved under translation, namely $|z + X + Y| = |X + Y + z| = |X + Y|$ for every $z \in A$.

This is a point in common with the case of groups, but a significant difference is that, in the context of semigroups (even when unital), the above invariance property cannot be used, at least in general, to "normalize" either of X and Y in such a way as to contain some distinguished element of A. However, we will see in a while that things continue to work properly when $\mathbb{A}$ is a monoid and sets are shifted by units.

Lemma 1.21. *Let X and Y be subsets of A. The following are equivalent:*

(i) $X + 2Y \subseteq X + Y$.

(ii) $X + nY \subseteq X + Y$ *for all* n.

(iii) $X + \langle Y \rangle = X + Y$.

Proof. Points (ii) and (iii) are clearly equivalent, as $X + \langle Y \rangle = \bigcup_{n=1}^{\infty} (X + nY)$, and (i) is obviously implied by (ii). Thus, we are left to prove that (ii) follows from (i), which is immediate (by induction) using that, if $X + nY \subseteq X + Y$ for some n, then we have $X + (n+1)Y = (X + nY) + Y \subseteq (X + Y) + Y = X + 2Y \subseteq X + Y$. □

The above result is as elementary as central in the plan of the chapter, as the applicability of the generalized Davenport transform (introduced in Section 1.5) to the proof of Theorem 1.9 depend on it in a critical way. On another hand, the following lemma shows that, in reference to Theorem 1.9, there is no loss of generality in assuming that the ambient semigroup is unital, for any semigroup embeds as a subsemigroup into its unitization (recall Remark 1.16).

Lemma 1.22. *Let $\mathbb{B} = (B, \star)$ be a semigroup, ϕ a semigroup monomorphism $\mathbb{A} \to \mathbb{B}$, i.e. an injective function from A to B such that $\phi(z_1 + z_2) = \phi(z_1) \star \phi(z_2)$ for all $z_1, z_2 \in A$, and $X_1, \ldots, X_n \subseteq A$. Then, $|X_1 + \cdots + X_n| = |\phi(X_1) \star \cdots \star \phi(X_n)|$.*

We close the section with a few properties of units. Here and later, given $X \subseteq A$ we use $\mathrm{C}_{\mathbb{A}}(X)$ for the centralizer of X in $\mathbb{A}$, namely the set of all $z \in A$ such that $z + x = x + z$ for every $x \in X$.

Lemma 1.23. *Let $\mathbb{A}$ be a monoid, X a subset of A, and z a unit of $\mathbb{A}$ with inverse $\tilde{z}$. Then:*

(i) *$X - z = X + \tilde{z}$ and $-z + X = \tilde{z} + X$, but also $|-z + X| = |X - z| = |X|$.*

(ii) *If $z \in \mathrm{C}_{\mathbb{A}}(X)$ then $\tilde{z} \in \mathrm{C}_{\mathbb{A}}(X)$; in addition to this, $\langle X - z \rangle$ and $\langle -z + X \rangle$ are commutative if $\langle X \rangle$ is commutative.*

Proof. (i) By duality, it suffices to prove that $X - z = X + \tilde{z}$ and $|X - z| = |X|$. As for the first identity, it holds $w \in X - z$ if and only if there exists $x \in X$ such that $w + z = x$, which in turn is equivalent to $x + \tilde{z} = (w + z) + \tilde{z} = w$, namely $w \in X + \tilde{z}$. In order to conclude, it is then sufficient to observe that the function $A \to A : \xi \mapsto \xi + \tilde{z}$ is a bijection.

(ii) Pick $z \in \mathrm{C}_{\mathbb{A}}(X)$ and $x \in X$. It is clear that $x + \tilde{z} = \tilde{z} + x$ if and only if $x = (x + \tilde{z}) + z = \tilde{z} + x + z$, and this is certainly verified as our standing assumptions imply $\tilde{z} + x + z = \tilde{z} + z + x = x$. It follows that $\tilde{z} \in \mathrm{C}_{\mathbb{A}}(X)$.

Suppose now that $\langle X \rangle$ is a commutative semigroup and let $v, w \in \langle X - z \rangle$. By point (i) above, there exist $x_1, \ldots, x_\ell, y_1, \ldots, y_m \in X$ such that $v = \sum_{i=1}^{\ell} (x_i + \tilde{z})$ and $w = \sum_{i=1}^{m} (y_i + \tilde{z})$, thus

$v + w = w + v$ by induction on $\ell + m$ and the observation that for all $u_1, u_2 \in X$ it holds

$$(u_1 + \tilde{z}) + (u_2 + \tilde{z}) = u_1 + u_2 + 2\tilde{z} = u_2 + u_1 + 2\tilde{z} = (u_2 + \tilde{z}) + (u_1 + \tilde{z}),$$

where we use that $\tilde{z} \in \mathrm{C}_{\mathbb{A}}(X)$, as proved above, and $\langle X \rangle$ is commutative. Hence, $\langle X - z \rangle$ is commutative too, which completes the proof by duality. □

Remark 1.24. Considering that units are cancellable elements, point (i) in Lemma 1.23 can be (partially) generalized as follows: If $X \subseteq A$ and $z \in A$ is cancellable, then $|z + X| = |X + z| = |X|$ (this is straightforward, because both of the functions $A \to A : x \mapsto x + z$ and $A \to A : x \mapsto z + x$ are bijective).

Remark 1.25. There is a subtleness in Definition 1.8 and Lemma 1.23 that we have so far (intentionally) overlooked, but should be remarked. For, suppose that $\mathbb{A}$ is a monoid and pick $x, y \in A$. In principle, $x - y$ and $-y + x$ are not elements of A: In fact, they are difference sets, namely subsets of A, and no other interpretation is possible a priori. However, if y is a unit of $\mathbb{A}$ and $\tilde{y}$ is the inverse of y, then $x - y = \{x + \tilde{y}\}$ and $-y + x = \{\tilde{y} + x\}$ by point (i) of Lemma 1.23, and we are allowed to identify $x - y$ with $x + \tilde{y}$ and $-y + x$ with $\tilde{y} + x$, which is useful in many ways.

1.4 The Davenport transform revisited

As mentioned in Section 1.2, Davenport's proof [D1, Statement A] of Theorem 1.2 is a transformation proof. For $\mathbb{A}$ a *commutative group*, the idea is to map a pair (X, Y) of non-empty subsets of A to a new pair (X, Y_D), which is smaller than (X, Y) in an appropriate sense, and specifically such that

$$|Y_D| < |Y|, \quad |X + Y_D| + |Y| \leq |X + Y| + |Y_D|.$$

We then refer to (X, Y_D) as a Davenport transform of (X, Y); see, for instance, [HR]. For this to be possible, the classical approach requires that $X + 2Y \not\subseteq X + Y$ and $0 \in Y$, so that $|Y| \geq 2$.

As expected, many difficulties arise when attempting to adapt the same approach to semigroups, all the more if these are non-commutative. Even the possibility of embedding a semigroup into a monoid does not resolve anything, since the fundamental problem is that, contrary to the case of groups, cardinality is not preserved "under subtraction". Namely, if $\mathbb{A}$ is an arbitrary monoid with

identity 0 (as intended for the remainder of the section), X is a subset of A, and $z \in A$, then $|X|$, $|X-z|$ and $|-z+X|$ can be greatly different from each other, even in the case that $\mathbb{A}$ is cancellative; cf. point (i) of Lemma 1.23. Thus, unless $\mathbb{A}$ is a group or, more generally, embeds as a submonoid into a group, we are not allowed to assume, for instance, that $0 \in Y$ by picking an arbitrary element $y_0 \in Y$ and replacing (X, Y) with the "shifted" pair $(X + y_0, -y_0 + Y)$; cf. the comments following Proposition 1.20.

In fact, the primary goal of this section is to show that, in spite of these issues, Davenport's original ideas can be extended and used for a proof of Theorem 1.9.

To start with, let X and Y be subsets of A such that $mX + 2Y \not\subseteq X + Y$ for some (positive integer) m. For the sake of brevity, define

$$Z := (mX + 2Y) \setminus (X + Y).$$

Our assumptions give $Z \neq \emptyset$. Thus fix $z \in Z$, and take $x_z \in (m-1)X$ and $y_z \in Y$ for which $z \in x_z + X + Y + y_z$, where $0X := \{0\}$. Finally, set

$$\tilde{Y}_z := \{y \in Y : z \in x_z + X + Y + y\} \quad \text{and} \quad Y_z := Y \setminus \tilde{Y}_z. \tag{1.4}$$

We refer to (X, Y_z) as a *generalized* Davenport transform of (X, Y) (relative to z), and based on this notation we have:

Proposition 1.26. *If $Y_z \neq \emptyset$, then the triple $(X, Y_z, \tilde{Y}_z)$ satisfies the following:*

(i) *Y_z and $\tilde{Y}_z$ are non-empty disjoint proper subsets of Y, and $\tilde{Y}_z = Y \setminus Y_z$.*

(ii) *If $\mathbb{A}$ is cancellative, then $(x_z + X + Y_z) \cup (z - \tilde{Y}_z) \subseteq x_z + X + Y$.*

(iii) *If $\langle Y \rangle$ is commutative, then $(x_z + X + Y_z) \cap (z - \tilde{Y}_z) = \emptyset$.*

(iv) *If $\mathbb{A}$ is cancellative, then $|z - \tilde{Y}_z| \geq |\tilde{Y}_z|$.*

(v) *If $\mathbb{A}$ is cancellative and $\langle Y \rangle$ is commutative, then $|X + Y| + |Y_z| \geq |X + Y_z| + |Y|$.*

Proof. (i) Y_z is non-empty by hypothesis, while $\tilde{Y}_z$ is non-empty since $y_z \in \tilde{Y}_z$ by construction. Also, (1.4) gives $Y_z, \tilde{Y}_z \subseteq Y$ and $Y_z \cap \tilde{Y}_z = \emptyset$, so that $Y \setminus Y_z = Y \setminus (Y \setminus \tilde{Y}_z) = \tilde{Y}_z$ and $Y_z, \tilde{Y}_z \subsetneq Y$.

(ii) Since $Y_z \subseteq Y$ by point (i) above, $x_z + X + Y_z \subseteq x_z + X + Y$ by Proposition 1.19. On the other hand, if $w \in z - \tilde{Y}_z$ then there exists $y \in \tilde{Y}_z$ such that $z = w + y$. But $y \in \tilde{Y}_z$ implies by (1.4) that $z = \tilde{w} + y$ for some $\tilde{w} \in x_z + X + Y$, whence $w = \tilde{w}$ by cancellativity, namely $w \in x_z + X + Y$.

(iii) Assume the contrary and let $w \in (x_z + X + Y_z) \cap (z - \tilde{Y}_z)$. There then exist $x \in X, y_1 \in Y_z$ and $y_2 \in \tilde{Y}_z$ such that $w = x_z + x + y_1$ and $z = w + y_2$. Using that $\langle Y \rangle$ is commutative, it follows that $z = x_z + x + y_1 + y_2 = x_z + x + y_2 + y_1$, which in turn implies $y_1 \in \tilde{Y}_z$ by (1.4), since $Y_z, \tilde{Y}_z \subseteq Y$ by point (i). This is, however, absurd as $Y_z \cap \tilde{Y}_z = \emptyset$, by the same point (i).

(iv) We have from (1.4) that for each $y \in \tilde{Y}_z$ there exists $w \in x_z + X + Y$ such that $z = w + y$, and hence $w \in z - \tilde{Y}_z$. On the other hand, since $\mathbb{A}$ is cancellative, we cannot have $w + y_1 = w + y_2$ for some $w \in A$ and distinct $y_1, y_2 \in \tilde{Y}_z$. Thus, $\tilde{Y}_z$ embeds as a set into $z - \tilde{Y}_z$, with the result that $|z - \tilde{Y}_z| \geq |\tilde{Y}_z|$.

(v) Since $\mathbb{A}$ is cancellative and $X \neq \emptyset$ (otherwise $Z = \emptyset$), we have $|X + Y| \geq \max(|X|, |Y|)$ by Propositions 2.8 and 1.19. This implies the claim if Y is infinite, since then either $|X + Y| > |Y|$, and hence

$$|X + Y| + |Y_z| = |X| = |X + Y_z| + |Y|,$$

or $|X + Y| = |Y|$, and accordingly

$$|X + Y_z| + |Y_z| = |Y| = |X + Y_z| + |Y|.$$

So we are left with the case when Y is finite, for which the inclusion-exclusion principle, points (ii)-(iv) and Proposition 1.19 give, by symmetry, that

$$\begin{aligned} |X + Y| = |x_z + X + Y| \geq |x_z + X + Y_z| + |z - \tilde{Y}_z| = \\ = |X + Y_z| + |z - \tilde{Y}_z| \geq |X + Y_z| + |\tilde{Y}_z|. \end{aligned}$$

But $\tilde{Y}_z = Y \setminus Y_z$ and $Y_z \subseteq Y$ by point (i) above, so at the end we have $|X+Y| \geq |X+Y_z|+|Y|-|Y_z|$, and the proof is complete. □

Remark 1.27. To apply the generalized Davenport transform to Theorem 1.9, it will be enough to consider the case where $m = 1$, for which it is easily seen that $0 \in Y_z$ if $0 \in Y$ (we continue with the notation from above), as otherwise $z \in X + Y$, contradicting the fact that $z \in (X + 2Y) \setminus (X + Y)$. However, it seems intriguing that the same machinery can be used, at least in principle, even if

$m \geq 2$ in so far as there is a way to prove that Y_z is non-empty.

1.5 The proof of the main theorem

Lemma 1.26 is used here to establish the main contribution of the chapter.

Proof of Theorem 1.9. Since every semigroup embeds as a subsemigroup into its unitization, and the unitization of a cancellative semigroup is cancellative in its own right, Lemma 1.22 and Definition 1.8 imply that there is no loss of generality in assuming, as we do, that $\mathbb{A}$ is unital.

Thus, suppose by contradiction that the theorem is false. There then exists a pair (X, Y) of subsets of A for which $\langle Y \rangle$ is abelian and $|X + Y| < \min(\gamma(Y), |X| + |Y| - 1)$. Then,

$$2 \leq |X|, |Y| < \infty. \tag{1.5}$$

In fact, if either of X and Y is a singleton or infinite then $|X + Y| = |X| + |Y| - 1$, contradicting the standing assumptions. It follows from (1.5) that

$$|X + Y| < \sup_{y_0 \in Y^\times} \inf_{y_0 \neq y \in Y} \operatorname{ord}(y - y_0) \quad \text{and} \quad |X + Y| \leq |X| + |Y| - 2. \tag{1.6}$$

Again without loss of generality, we also take $|X| + |Y|$ to be minimal over the pairs of subsets of A for which, in particular, (1.5) and (1.6) are assumed to hold.

Now, since $|X + Y|$ is finite, thanks to (1.5) and Proposition 1.20, we get by (1.6) and the same equation (1.5) that there exists $\tilde{y}_0 \in Y^\times$ such that

$$|X + Y| < \inf_{\tilde{y}_0 \neq y \in Y} \operatorname{ord}(y - \tilde{y}_0) = \min_{\tilde{y}_0 \neq y \in Y} \operatorname{ord}(y - \tilde{y}_0). \tag{1.7}$$

So letting $W_0 := Y - \tilde{y}_0$ implies

$$|X + W_0| < \min_{0 \neq w \in W_0} \operatorname{ord}(w) \quad \text{and} \quad |X + W_0| \leq |X| + |W_0| - 2 \tag{1.8}$$

in view of (1.6) and (1.7). In fact, on the one hand $|Y - \tilde{y}_0| = |Y|$ and $|X + Y - \tilde{y}_0| = |X + Y|$ by point (i) of Lemma 1.23, and on the other, $y \in Y \setminus \{\tilde{y}_0\}$ only if $y - \tilde{y}_0 \in (Y - \tilde{y}_0) \setminus \{0\}$, but also

$w \in (Y - \tilde{y}_0) \setminus \{0\}$ only if $w + \tilde{y}_0 \in Y \setminus \{\tilde{y}_0\}$ (see also Remark 1.25). We claim that

$$Z := (X + 2W_0) \setminus (X + W_0) \neq \emptyset. \tag{1.9}$$

For, suppose the contrary. Then, $X + W_0 = X + \langle W_0 \rangle$ by Lemma 1.21, so that

$$|X + W_0| = |X + \langle W_0 \rangle| \geq |\langle W_0 \rangle| \geq \max_{w \in W_0} \mathrm{ord}(w) \geq \min_{0 \neq w \in W_0} \mathrm{ord}(w),$$

where we use, in particular, Proposition 1.19 for the first inequality and the fact that $|W_0| \geq 2$ for the last one. But this contradicts (1.8), so (1.9) is proved.

Pick $z \in Z$ and let $(X, \bar{W}_0)$ be a generalized Davenport transform of (X, W_0) relative to z. Since $\langle Y \rangle$ is a commutative subsemigroup of $\mathbb{A}$ (by hypothesis), the same is true for $\langle W_0 \rangle$, by point (ii) of Lemma 1.23. Moreover, $0 \in W_0$, and thus

$$0 \in \bar{W}_0 \neq \emptyset \quad \text{and} \quad \bar{W}_0 \subsetneq W_0, \tag{1.10}$$

when taking into account Remark 1.27 and point (i) of Proposition 1.26. As a consequence, point (v) of the same Proposition 1.26 yields, together with (1.8), that

$$|X + \bar{W}_0| + |W_0| \leq |X + W_0| + |\bar{W}_0| \leq |X| + |W_0| - 2 + |\bar{W}_0|,$$

which means, since $|W_0| = |Y - \tilde{y}_0| = |Y| < \infty$ by (1.5) and the above, that

$$|X + \bar{W}_0| \leq |X| + |\bar{W}_0| - 2. \tag{1.11}$$

It follows from (1.10) that $1 \leq |\bar{W}_0| < |W_0|$, and in fact $|\bar{W}_0| \geq 2$, as otherwise we would have $|X| = |X + \bar{W}_0| \leq |X| - 1$ by (1.11), in contrast to the fact that $|X| < \infty$ by (1.5). To summarize, we have found that

$$2 \leq |\bar{W}_0| < |W_0| < \infty. \tag{1.12}$$

Furthermore, (1.8) and (1.10) entail that

$$|X + \bar{W}_0| \leq |X + W_0| < \min_{0 \neq w \in \bar{W}_0} \mathrm{ord}(w). \tag{1.13}$$

Thus, since $0 \in \bar{W}_0^\times$, we get by (1.13) that

$$|X + \bar{W}_0| < \sup_{w_0 \in \bar{W}_0^\times} \min_{w_0 \neq w \in \bar{W}_0} \mathrm{ord}(w), \tag{1.14}$$

which is however in contradiction, due to (1.5), (1.11) and (1.12), with the minimality of $|X|+|Y|$, for $|\bar{W}_0| < |W_0| = |Y|$, and hence $|X| + |\bar{W}_0| < |X| + |Y|$. □

1.6 A couple of applications

First, we show how to use Theorem 1.9 to prove the extension of Chowla's theorem for composite moduli mentioned in Section 1.2.

Proof of Corollary 1.17. The claim is trivial if X or Y is a singleton. Otherwise, since $\mathbb{Z}/m\mathbb{Z}$ is a commutative finite group and $\mathrm{ord}(z - z_0) = m/\gcd(m, z - z_0)$ for all $z, z_0 \in \mathbb{Z}/m\mathbb{Z}$, we get by Corollary 1.14 that $|X + Y| \geq \min(\tilde{\gamma}(Y), |X| + |Y| - 1)$, where

$$\tilde{\gamma}(Y) = \max_{y_0 \in Y} \min_{y_0 \neq y \in Y} \mathrm{ord}(y - y_0) = m \cdot \max_{y_0 \in Y} \min_{y_0 \neq y \in Y} \frac{1}{\gcd(m, y - y_0)} = \delta_Y^{-1} m.$$

Now in an entirely similar way, it is found, in view of Corollary 1.12, that

$$|X + Y| \geq \min(\delta_X^{-1} m, |X| + |Y| - 1).$$

This concludes the proof, considering that $\delta_Y = 1$ if there exists $y_0 \in Y$ such that $\gcd(m, y - y_0) = 1$ for every $y \in Y \setminus \{y_0\}$ (and dually with X). □

We now use P. Hall's theorem on distinct representatives [H] to say something on the "localization" of elements in a sumset.

Theorem 1.28 (Hall's theorem)**.** *Let $S_1, \ldots, S_n$ be sets. There then exist (pairwise) distinct elements $s_1 \in S_1, \ldots, s_n \in S_n$ if and only if for each $k = 1, \ldots, n$ the union of any k of $S_1, \ldots, S_n$ contains at least k elements.*

More precisely, suppose $\mathbb{A}$ is a cancellative semigroup and let X, Y be non-empty finite subsets of A such that $|X + Y| < \gamma(Y)$. Clearly, this implies $Y^\times \neq \emptyset$. Define $k := |X|$ and $\ell := |Y|$, and let

$x_1, \dots, x_k$ be a numbering of X and $y_1, \dots, y_\ell$ a numbering of Y. Then consider the k-by-ℓ matrix, say $a(X, Y)$, whose entry in the i-th row and j-th column is $x_i + y_j$. Any element of $X + Y$ appears in $a(X, Y)$, and viceversa any entry of $a(X, Y)$ is an element of $X + Y$. Also, Theorem 1.9 and our hypotheses give $|X+Y| \geq k+\ell-1$. So it is natural to try to get some information about where in the matrix $a(X, Y)$ it is possible to find $k+\ell-1$ distinct elements of $X+Y$. In this respect we have the following proposition, whose proof is quite similar to the one of a weaker result in [R, Section 6], which is, in turn, focused on the less general case of a group of prime order:

Proposition 1.29. *Assume that $\langle Y \rangle$ is commutative and let Z be any subset of $X + Y$ of size $\ell - 1$, for instance $Z = x_1 + \{y_1, \dots, y_{\ell-1}\}$. Then we can choose one element from each row of $a(X, Y)$ in such a way that Z and these elements form a subset of $X + Y$ of size $k + \ell - 1$.*

Proof. For each $i = 1, \dots, k$ let $Z_i := (x_i + Y) \setminus Z$ and note that Z_i is a subset of the i-th row of $a(X, Y)$. Thus, $Z_{i_1} \cup \cdots \cup Z_{i_h} = (\{x_{i_1}, \dots, x_{i_h}\} + Y) \setminus Z$ for any positive $h \leq k$ and all distinct $i_1, \dots, i_h \in \{1, \dots, k\}$. It follows that

$$|Z_{i_1} \cup \cdots \cup Z_{i_h}| \geq |\{x_{i_1}, \dots, x_{i_h}\} + Y| - |Z| \geq h + \ell - 1 - (\ell - 1) = h,$$

where we combine Theorem 1.9 with the fact that

$$|\{x_{i_1}, \dots, x_{i_h}\} + Y| \leq |X + Y| < \gamma(Y),$$

as is implied by Proposition 1.18 and the assumption that $|X+Y| < \gamma(Y)$. Then, as a consequence of Hall's theorem, we can find k distinct elements $z_1 \in Z_1, \dots, z_k \in Z_k$, and these, together with the $\ell - 1$ elements of Z, provide a total of $k + \ell - 1$ distinct elements of $X + Y$, since $Z \cap Z_1 = \cdots = Z \cap Z_k = \emptyset$ (by construction). □

References

[B1] N. Bourbaki, *Algèbre, Chapitres 1 à 3*, Éléments de mathématique II, Springer-Verlag, Berlin, 2006, 2nd revised ed.

[C] A.-L. Cauchy, *Recherches sur les nombres*, J. École Polytech. **9** (1813), 99–116 (reproduced in *Oeuvres*, Série 2, Tome 1, 39–63).

[CHS] A. L. Cilleruelo, Y. O. Hamidoune and O. Serra, 'Addition theorems in acyclic semigroups', in: *Additive number theory* (Springer, 2010), 99–104.

[Ch] I. Chowla, *A theorem on the addition of residue classes: Application to the number* $\Gamma(k)$ *in Waring's problems*, Proc. Indian Acad. Sc. (A) **2** (1935), 242–243.

[CP] A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups, Vols. I and II*, Mathematical Surveys **7** (American Mathematical Society, 1964, 2nd ed.).

[D1] H. Davenport, *On the addition of residue classes*, J. Lond. Math. Soc. **10** (1935), 30–32.

[D2] H. Davenport, *A historical note*, J. Lond. Math. Soc. **22** (1947), 100–101.

[G] A. Geroldinger, 'Additive Group Theory and Non-unique Factorizations', in: *Combinatorial Number Theory and Additive Group Theory* (Springer, 2009), 1–86.

[H] P. Hall, *On representatives of subsets*, J. Lond. Math. Soc. **10** (1935), 26–30.

[HR] Y. O. Hamidoune and Ø. J. Rødseth, *An inverse theorem mod p*, Acta Arith. **92** (2000), 251–262.

[Ho] J. M. Howie, *Fundamentals of semigroup theory* (Clarendon Press, 1995).

[Ka] G. Károlyi, *The Cauchy-Davenport theorem in group extensions*, Enseign. Math. **51** (2005), 239–254.

[Ke] J. H. B. Kemperman, *On complexes in a semigroup*, Indag. Math. **18** (1956), 247–254.

[Ma] A. I. Mal'cev, *On the immersion of an algebraic ring into a field*, Math. Annalen (1)**113** (1937), 686–691.

[N] M. B. Nathanson, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets*, GTM **165** (Springer, 1996).

[Pi] S. S. Pillai, *Generalization of a theorem of Davenport on the addition of residue classes*, Proc. Indian Acad. Sc. (A) (3)**6** (1937), 179–180.

[R] Ø. J. Rødseth, *Sumsets mod p*, Skr. K. Nor. Vidensk. Selsk. (Trans. R. Norw. Soc. Sci. Lett.), **4** (2006), 1–10.

[Ru] I. Z. Ruzsa, 'Sumsets and structure', in: *Combinatorial Number Theory and Additive Group Theory* (Springer, 2009), 87–210.

[Tr1] S. Tringali, *A Cauchy-Davenport theorem for semigroups,* Uniform Distribution Theory, Vol. 9, No. 1 (2014), 27–42.

[V] A. G. Vosper, *The critical pairs of subsets of a group of prime order*, J. Lond. Math. Soc. **31** (1956), 200–205.

This page intentionally left blank

On ne voit bien qu'avec le cœur.
L'essentiel est invisible pour les yeux.

— Antoine de Saint Exupéry, *Le Petit Prince*

2

Cauchy-Davenport type theorems, II

Resumé. On fait une étude plus approfondie des propriétés de la constante de Cauchy-Davenport (introduite dans le chapitre 1) pour montrer l'extension supplémentaire suivante du théorème de Cauchy-Davenport : si $(A, +)$ est un semi-groupe cancellatif et si $X, Y \subseteq A$, alors

$$|X + Y| \geq \min(\gamma(X + Y), |X| + |Y| - 1).$$

Cela implique une généralisation de l'inégalité de Kemperman pour les groupes sans torsion [Ke] et aussi une version plus forte du théorème d'Hamidoune-Károlyi mentionné précédemment. Ici, on donne une preuve indépendante et totalement combinatoire du cas général de ce résultat, qui ne dépend ni du théorème de Feit-Thompson ni de la méthode isopérimétrique. Enfin, on se penche sur certains aspects d'une conjecture qui, si elle était vraie, pourrait fournir une formulation unifiée de beaucoup de théorémes de type Cauchy-Davenport, y compris ceux déjà prouvés

dans le chapitre précédent. Le contenu ci-après est basé sur un papier par l'auteur [Tr2] soumis pour publication.

Abstract. Based on a paper by the author [Tr2] which is still under review, we further investigate the properties of the Cauchy-Davenport constant (introduced in Chapter 1) and use them to prove the following: If $\mathbb{A}$ is a cancellative semigroup (either commutative or not) and $X, Y \subseteq A$, then

$$|X + Y| \geq \min(\gamma(X + Y), |X| + |Y| - 1).$$

This implies at once a generalization of Kemperman's inequality for torsion-free groups [Ke] and a strengthening of the Hamidoune-Károlyi theorem. Our proof of the latter is basically a transformation proof; in particular, it is self-contained and does not depend on either the Feit-Thompson theorem or the isoperimetric method. In addition, we discuss aspects of a conjecture that, if true, would further improve most of the results in the chapter, generalize a greater number of Cauchy-Davenport type theorems (including those proved in the previous chapter), and hopefully provide a deeper understanding on this kind of inequalities.

2.1 Introduction

The weaker are the structural assumptions, the larger is, in principle, the number of problems that we can hope to solve, while trying to arrive at a better understanding of their "real nature": This is, in essence, the philosophy at the heart of the present thesis. Building on these ideas, we aim here to further extend some aspects of the theory developed in the previous chapter, particularly in the direction of the study of non-commutative or non-cancellative semigroups.

A natural motivation for this comes from considering that the non-zero elements of a non-trivial unital ring, either commutative or not, are not, in general, cancellative (and hence not even closed) under multiplication (unless the ring is a domain). Another motivation is the fact that, even when $\mathbb{A}$ is a commutative group, the non-empty subsets of A, endowed with the binary operation taking a pair (X, Y) to the sum-set $X+Y$, is, in general, nothing more than a non-cancellative monoid (e.g., when $\mathbb{A}$ is the additive group of the ring of integers, the corresponding structure on the powerset of A has been studied by J. Cilleruello, Y. O. Hamidoune and O. Serra; see [CHS] and references

therein).

Here, more specifically, the main contribution is an extension (Theorem 2.3) of the (classical) Cauchy-Davenport theorem (Theorem 1.2) to the setting of cancellative, but possibly non-commutative semigroups (see comments at the end of Section 2.2), whence we derive as an almost immediate consequence a stronger and more abstract version (Corollary 2.4) of the Hamidoune-Károlyi theorem (Theorem 1.6). In fact, a proof of this latter result was first published by Károlyi in 2005 for the special case of finite groups [Ka], based on the structure theory of group extensions, by reduction to finite solvable groups in the light of the Feit-Thompson theorem. In the same paper (p. 242), Károlyi reports a more elementary proof of the general statement (for an arbitrary group), which was apparently communicated to him by Hamidoune during the peer-review process of [Ka]. Hamidoune's approach depends on a generalization of an addition theorem by L. Shatrowsky and is ultimately built upon the isoperimetric method (see [Ha] and references therein). However, Károlyi himself has pointed out to the author, as recently as July 2013, that an alternative and even "simpler" approach comes from a Kneser-type result due to J. E. Olson [O, Theorem 2], based on Kemperman's transform. Yet another argument along the same lines was suggested by I. Ruzsa in a private communication in mid-June 2013.

On these premises, we remark from the outset that also our proof of Theorem 2.3, and consequently of Corollary 2.4, is basically a transformation proof, close in the spirit to Olson's approach and as elementary as other combinatorial proofs in the literature (in particular, it is self-contained and does not depend at all on the Feit-Thompson theorem or Hamidoune's isoperimetric method).

In addition to the above, we present and discuss aspects of a conjecture (Conjecture 2.1) which, if true, would further improve most of the results in the paper and include as a special case a greater number of Cauchy-Davenport type theorems, and particularly those proved in the previous chapter. In all of this, a key role is played by certain invariance properties of the Cauchy-Davenport constant (Definition 1.8), which are also investigated in this work.

Organization.

In Section 2.2 we give an overview, complementary to the one of the previous chapter, of the literature on theorems of Cauchy-Davenport type (with a particular emphasis on those that we are going to strengthen or generalize), and state our main results and a related conjecture (Conjec-

ture 2.1). Section 2.3 contains intermediate results on the invariance of the Cauchy-Davenport constant under suitable transformations. Finally, in Section 2.4 we prove the principal theorem (namely, Theorem 2.3).

2.2 Cauchy-Davenport type theorems

As already emphasized in the previous chapter, the Cauchy-Davenport theorem is probably the first significant achievement in the field of additive theory, dating back to work by A.-L. Cauchy in 1813 [C]. The result has many generalizations. E.g., we have seen that extensions to composite moduli (the theorem applies especially to the additive group of the integers modulo a prime) have been given by I. Chowla [Ch, Theorem 1] and S. S. Pillai [Pi]. These latter results have been sharpened and further generalized by Corollary 1.17 in the previous chapter, where they appear as Theorems 1.3 and 1.4, respectively. The whole thing comes as an almost immediate consequence of Theorem 1.9, and leads us here to the following:

Conjecture 2.1. *Let n be a positive integer and $X_1, \dots, X_n$ non-empty subsets of A. If $\mathbb{A}$ is cancellative, then $|X_1 + \cdots + X_n| \geq \min(\gamma(X_1, \dots, X_n), |X_1| + \cdots + |X_n| + 1 - n)$.*

Unluckily, we do not have a proof of the conjecture (not even for two summands), which can however be confirmed in some special case (see, in particular, Corollary 2.5 below, or consider Corollary 1.13 when $\mathbb{A}$ is commutative) and would provide, if it were true, a comprehensive generalization of about all the extensions of the Cauchy-Davenport theorem reported in this thesis. Incidentally, the next example shows that the assumption of cancellativity, or a surrogate of it, is critical and somewhat necessary:

Example 2.2. Let X and Y be non-empty disjoint sets with $|X| < \infty$ and denote by $(F_X, \cdot_X)$ and $(F_Y, \cdot_Y)$, respectively, the free abelian groups on X and Y. For a fixed element $e \notin F_X \cup F_Y$, we define a binary operation $\cdot$ on $F := F_X \cup F_Y \cup \{e\}$ by taking $u \cdot v := u \cdot_X v$ for $u, v \in F_X$, $u \cdot v := u \cdot_Y v$ for $u, v \in F_Y$ and $u \cdot v := e$ otherwise. It is routine to check that $\cdot$ is associative, so we write $\mathbb{F}$ for the unitization of $(F, \cdot)$ and 1 for the identity of $\mathbb{F}$. Then, taking $Z := Y \cup \{1\}$ gives $\gamma_{\mathbb{F}}(Z) = \infty$ and $X \cdot Z := \{x \cdot z : x \in X, z \in Z\} = X \cup \{e\}$, so that $|X \cdot Z| < |X| + |Z| - 1 \leq \gamma_{\mathbb{F}}(X, Z)$, namely $|X \cdot Z| < \min(\gamma_{\mathbb{F}}(X, Z), |X| + |Z| - 1)$, and the right-hand side can be made arbitrarily larger than the left-hand side.

Nevertheless, we can prove the following inequality, which in fact represents the main contribution of the present chapter:

Theorem 2.3. *Let X, Y be subsets of A and suppose that $\mathbb{A}$ is cancellative. Then, $|X+Y| \geq \min(\gamma(X+Y), |X| + |Y| - 1)$.*

At this point, it is worth comparing Theorems 1.9 and 2.3. On the one hand, the latter is "much stronger" than the former, for it does no longer depend on commutativity (which, by the way, leads to a perfectly symmetric statement). Yet on the other hand, the former is "much stronger" than the latter, since for subsets X and Y of A we are now replacing $\gamma(X, Y)$ in Theorem 1.9 with $\gamma(X + Y)$, and it has been already observed (Example 1.11) that this means, in general, a weaker bound.

The above seems to suggest that a common generalization of the two theorems should be possible, and gives another (indirect) motivation to believe that Conjecture 2.1 can be true. Let it be as it may, Theorem 2.3 is already strong enough to allow for a strengthening of the Hamidoune-Kàrolyi theorem (Theorem 1.6 in Chapter 1), as implied by Lemma 1.10 and Example 1.11. As pointed out before, the theorem was first proved by Károlyi in [Ka] in the particular case of finite groups, based on the Feit-Thompson theorem. The full theorem was then established by Hamidoune through the isoperimetric method [Ka, p. 242].

In contrast, our proof of Theorem 1.6 is purely combinatorial, and it comes as a trivial consequence of Theorem 2.3 in view of Lemma 1.10. Specifically, we have the following:

Corollary 2.4. *Pick $n \in \mathbb{N}^+$ and subsets $X_1, \ldots, X_n$ of A such that $X_1^\times + \cdots + X_n^\times \neq \emptyset$. If $\mathbb{A}$ is cancellative, then $|X_1 + \cdots + X_n| \geq \min(\mathfrak{p}(A), |X_1| + \cdots + |X_n| + 1 - n)$.*

Theorem 2.3 and Corollary 2.4 are proved in Section 2.4. Another result from the literature that is meaningful in relation to the present chapter is Kemperman's inequality, to wit Theorem 1.7. In fact, the result is generalized by the following, whose proof is straightforward in the light of Corollary 2.4 (we may omit the details).

Corollary 2.5. *Given $n \in \mathbb{N}^+$, let $X_1, \ldots, X_n$ be subsets of A such that $X_1^\times + \cdots + X_n^\times \neq \emptyset$. Define $\kappa := |X_1| + \cdots + |X_n| + 1 - n$ and assume $\mathrm{ord}(x) \geq \kappa$ for every $x \in A \setminus \{0\}$. If $\mathbb{A}$ is cancellative, then $|X_1 + \cdots + X_n| \geq \kappa$.*

For the rest, it was already mentioned in the introduction that earlier contributions by other authors to the additive theory of semigroups are due, e.g., to Cilleruelo, Hamidoune and Serra,

who in particular proved in [CHS] a Cauchy-Davenport theorem for *acyclic* monoids (these are termed acyclic *semigroups* in [CHS], but they are, in fact, *monoids* in our terminology), and it could be quite interesting to find a common pattern among their result and the ones in this chapter. The same question was raised at the end of Section 1.1, where it was also observed that one of the main difficulties with this idea is actually represented by the fact that acyclic monoids in [CHS] are *not* cancellative, which has served as a basic motivation for making the results of Section 2.3 mostly independent from the assumption of cancellativity.

Remark 2.6. Incidentally, we point out that condition M1 in the definition of an acyclic semigroup $\mathbb{M} = (M, \cdot)$ in [CHS], to wit "$y \cdot x = x$ implies $y = 1$, for every $x \in M$" (we write 1 for the identity of $\mathbb{M}$), is to be fixed in some way, since otherwise taking $\mathbb{M}$ to be the unitization of a non-empty left-zero semigroup $(N, \cdot)$, where $x \cdot y := x$ for all $x, y \in N$, yields a counterexample to the statement that "If $\mathbb{M}$ is an acyclic semigroup and $1 \in S$", where S is a finite subset of M, "then the only finite directed cycles in the Cayley graph $\mathrm{Cay}(\mathbb{M}, S)$ are the loops": This is first mentioned in the second paragraph of Section 2 in the cited paper (p. 100), and is fundamental for most of its results. At first, we thought of a typo and tried to substitute condition M1 with its "dual", namely "$x \cdot y = x$ implies $y = 1$, for every $x \in M$." In fact, this is enough to fix the issue with the Cayley graphs of $\mathbb{M}$, but Lemma 1 in the same paper, which is equally essential in many proofs, breaks down completely (for a concrete counterexample, consider the monoid obtained by reversing the multiplication of $(N, \cdot)$ in the previous counterexample).

However, there are at least two possible workarounds: The first is to assume that $\mathbb{M}$ is commutative, the second to turn condition M1 into a "self-dual" axiom, namely to replace it with "$x \cdot y = x$ or $y \cdot x = x$ implies $y = 1$, for every $x \in M$."

2.3 Preparations

Throughout, we collect basic results to be used later in Section 2.4 to prove Theorem 2.3 and Corollary 2.4. Some proofs are quite simple (and thus omitted without further explanation), but we have no standard reference to anything similar in the context of semigroups, so we include them here for completeness.

Notice that, even though Theorem 2.3, say, refers to *cancellative* semigroups, most of the results presented in the section do not depend on the cancellativity of the "ambient". While this makes no

serious difference from the point of view of readability, it seems interesting in itself, and our hope is that the material can help to find a proof of Conjecture 2.1 (or to further refine it).

Lemma 2.7. *Suppose $\mathbb{A}$ is a monoid. Pick $n \in \mathbb{N}^+$ and $z_0, \dots, z_n \in A^\times$, and let $X_1, \dots, X_n$ be subsets of A. Then, $\left|\sum_{i=1}^n X_i\right| = \left|\sum_{i=1}^n (z_{i-1} + X_i - z_i)\right|$.*

Proof. Let $\tilde{z}_i$ be, for $i = 0, \dots, n$, the inverse of z_i in $\mathbb{A}$, and set $X := \sum_{i=1}^n X_i$ for economy of notation. Lemma 1.23 gives $\sum_{i=1}^n (z_{i-1} + X_i - z_i) = \sum_{i=1}^n (z_{i-1} + X_i + \tilde{z}_i) = z_0 + X + z_n$, and then another application of the same proposition yields $|X| = |z_0 + X + z_n|$. □

In all what follows, we let $\mathbb{A}^{\mathrm{op}}$ be the dual (or opposite) semigroup of $\mathbb{A}$, namely the pair $(A, +_{\mathrm{op}})$ where $+_{\mathrm{op}}$ is the binary operation $A \times A \to A : (z_1, z_2) \mapsto z_2 + z_1$; cf. [B1, Section I.1.1, Definition 2].

Proposition 2.8. *Given $n \in \mathbb{N}^+$, let X and $X_1, \dots, X_n$ be subsets of A, and pick $z \in A$. Then, $X_1 + \cdots + X_n = X_n +_{\mathrm{op}} \cdots +_{\mathrm{op}} X_1$ and $\mathrm{ord}(z) = \mathrm{ord}_{\mathbb{A}^{\mathrm{op}}}(z)$.*

Here and later, to express that a statement follows as a more or less direct consequence of Proposition 2.8, we will simply say that it is true "by duality". This is useful for it often allows, for instance, to simplify a proof to the extent of cutting by half its length, as in the following lemma, which generalizes an analogous, well-known property of groups:

Lemma 2.9. *Pick $x, y \in A$ and suppose that at least one of x or y is cancellable. Then, $\mathrm{ord}(x + y) = \mathrm{ord}(y + x)$.*

Proof. By duality, there is no loss of generality in assuming, as we do, that y is cancellable. Further, it suffices to prove that $\mathrm{ord}(x + y) \leq \mathrm{ord}(y + x)$, since then the desired conclusion will follow from the fact that, on the one hand,

$$\begin{aligned}\mathrm{ord}(y + x) = \mathrm{ord}(x +_{\mathrm{op}} y) = \mathrm{ord}_{\mathbb{A}^{\mathrm{op}}}(x +_{\mathrm{op}} y) \leq \\ \mathrm{ord}_{\mathbb{A}^{\mathrm{op}}}(y +_{\mathrm{op}} x) = \mathrm{ord}(y +_{\mathrm{op}} x) = \mathrm{ord}(x + y),\end{aligned}$$

and on the other hand, y is cancellable in $\mathbb{A}$ if and only if it is cancellable in $\mathbb{A}^{\mathrm{op}}$. Now, the claimed inequality is obvious if $\mathrm{ord}(y + x)$ is infinite. Otherwise, there exist $n, k \in \mathbb{N}^+$ with $k < n$ such

that $\operatorname{ord}(y+x) = n$ and

$$\underbrace{(y+x)+\cdots+(y+x)}_{k \text{ times}} = \underbrace{(y+x)+\cdots+(y+x)}_{n+1 \text{ times}}.$$

So, by adding y to the right of both sides and using associativity to rearrange how the terms in the resulting expression are grouped we get

$$y+\underbrace{(x+y)+\cdots+(x+y)}_{k \text{ times}} = y+\underbrace{(x+y)+\cdots+(x+y)}_{n+1 \text{ times}},$$

Since y is cancellable, it then follows that

$$\underbrace{(x+y)+\cdots+(x+y)}_{k \text{ times}} = \underbrace{(x+y)+\cdots+(x+y)}_{n+1 \text{ times}},$$

which ultimately gives $\operatorname{ord}(x+y) \leq n = \operatorname{ord}(y+x)$. □

Proposition 2.10. *Let X be a subset of A. Then, $\gamma(X) = \gamma_{\mathbb{A}^{\mathrm{op}}}(X)$.*

Proof. Let $\mathfrak{i}$ be the map $\mathbb{A}^\times \to \mathbb{A}^\times$ sending a unit of $\mathbb{A}$ to its inverse, and define $\mathfrak{i}_{\mathrm{op}}$ in a similar way by replacing $\mathbb{A}$ with its dual. An element $x_0 \in A$ is a unit in $\mathbb{A}$ if and only if it is also a unit in $\mathbb{A}^{\mathrm{op}}$, and $\tilde{x}_0 \in A$ is the inverse of x_0 in $\mathbb{A}$ if and only if it is also the inverse of x_0 in $\mathbb{A}^{\mathrm{op}}$. Thus, $\mathbb{A}^\times = (\mathbb{A}^{\mathrm{op}})^\times$, $X \cap \mathbb{A}^\times = X \cap (\mathbb{A}^{\mathrm{op}})^\times$ and $\mathfrak{i} = \mathfrak{i}_{\mathrm{op}}$, with the result that

$$\gamma(X) = \sup_{x_0 \in X^\times} \inf_{x_0 \neq x \in X} \operatorname{ord}(x + \mathfrak{i}(x_0))$$

and

$$\gamma_{\mathbb{A}^{\mathrm{op}}}(X) = \sup_{x_0 \in X^\times} \inf_{x_0 \neq x \in X} \operatorname{ord}_{\mathbb{A}^{\mathrm{op}}}(\mathfrak{i}(x_0) + x),$$

where we use Lemma 1.23 to express the Cauchy-Davenport constant of X relative to either of $\mathbb{A}$ and $\mathbb{A}^{\mathrm{op}}$ only in the terms of $\mathfrak{i}$. But any unit in a monoid is cancellable, so for all $x_0 \in X^\times$ and $x \in A$

we get, again by Proposition 2.8 and in the light of Lemma 2.9, that

$$\begin{aligned}\mathrm{ord}_{\mathbb{A}^{\mathrm{op}}}(\mathfrak{i}(x_0)+x) &= |\langle \mathfrak{i}(x_0)+x\rangle_{\mathbb{A}^{\mathrm{op}}}| = |\langle \mathfrak{i}(x_0)+x\rangle| = \\ &= \mathrm{ord}(\mathfrak{i}(x_0)+x) = \mathrm{ord}(x+\mathfrak{i}(x_0)).\end{aligned}$$

And this, together with the above, is enough to conclude. □

We define an *invariant n-transform of* $\mathbb{A}$, here simply called an invariant n-transform if no confusion can arise, to be any tuple $\mathbf{T} = (T_1, \ldots, T_n)$ of functions on the powerset of A, herein denoted by $\mathcal{P}(A)$, with the property that, for all non-empty $X_1, \ldots, X_n \in \mathcal{P}(A)$,

1. $\left|\sum_{i=1}^n T_i(X_i)\right| = \left|\sum_{i=1}^n X_i\right|$ and $\sum_{i=1}^n |X_i| = \sum_{i=1}^n |T_i(X_i)|$;
2. $\gamma(X_1 + \cdots + X_n) = \gamma(T_1(X_1) + \cdots + T_n(X_n))$.

An interesting case is when each of the T_i is a *unital shift*, namely a function of the form

$$\mathcal{P}(A) \to \mathcal{P}(A) : X \to z_l + X + z_r$$

such that z_l and z_r are units of $\mathbb{A}$. This is implied by the following results, for which we use, among the other things, that if $\mathbb{A}$ is a monoid and $z \in A^\times$ then, by Lemma 1.23, we have

$$(X+Y) - z = X + (Y - z) \text{ and } (-z+X) + Y = -z + (X+Y)$$

for all $X, Y \subseteq A$, so that we can drop the parentheses without worrying and write, e.g., $X + Y - z$ for $(X+Y) - z$ and $-z + X + Y$ in place of $(-z+X) + Y$.

Lemma 2.11. *If $n \in \mathbb{N}^+$ and $X_1, \ldots, X_n \subseteq A$, then $X_1^\times + \cdots + X_n^\times \subseteq (X_1 + \cdots + X_n)^\times$, and the inclusion is, in fact, an equality if $\mathbb{A}$ is cancellative.*

Proof. The assertion is obvious for $n = 1$, so it is enough to prove it for $n = 2$, since then the conclusion follows by induction. For, let X, Y be subsets of A.

Suppose first that $z \in X^\times + Y^\times$ (which means, in particular, that $\mathbb{A}$ is a monoid), i.e. there exist $x \in X^\times$ and $y \in Y^\times$ such that $z = x + y$. If $\tilde{x}$ is the inverse of x (in $\mathbb{A}$) and $\tilde{y}$ is the inverse of y, then

it is immediate to see that $\tilde{y}+\tilde{x}$ is the inverse of $x+y$, and hence $x+y \in (X+Y)^\times$. It follows that $X^\times + Y^\times \subseteq (X+Y)^\times$.

As for the other inclusion, assume that $\mathbb{A}$ is cancellative and pick $z \in (X+Y)^\times$. We have to show that $z \in X^\times + Y^\times$. For, let $\tilde{z}$ be the inverse of z, and pick $x \in X$ and $y \in Y$ such that $z = x+y$. We define $\tilde{x} := y+\tilde{z}$ and $\tilde{y} := \tilde{z}+x$. It is straightforward to check that $x+\tilde{x} = (x+y)+\tilde{z} = 0$ and $\tilde{y}+y = \tilde{z}+(x+y) = 0$. Also, $(\tilde{x}+x)+y = y+\tilde{z}+(x+y) = y$ and $x+(y+\tilde{y}) = (x+y)+\tilde{z}+x = x$, from which we get, by cancellativity, $\tilde{x}+x = y+\tilde{y} = 0$. This implies that z belongs to $X^\times + Y^\times$, and so we are done. □

Remark 2.12. As a byproduct of the proof of Lemma 2.11, we get the following: If $x_1, \ldots, x_n \in A^\times$ ($n \in \mathbb{N}^+$) and $\tilde{x}_i$ is the inverse of x_i, then $\tilde{x}_n + \cdots + \tilde{x}_1$ is the inverse of $x_1 + \cdots + x_n$. This is a standard fact about groups, which goes through verbatim for monoids; see [B1, Section I.2.4, Corollary 1]. We mention it here because it is used below.

Lemma 2.13. *Let $\mathbb{A}$ be a monoid, and pick $z \in A^\times$ and $X \subseteq A$. Then, $\gamma(X) \leq \gamma(X+z)$.*

Proof. By Lemma 2.11, we have $X^\times + z \subseteq (X+z)^\times$, and thus

$$\gamma(X+z) = \sup_{w_0 \in (X+z)^\times} \inf_{w_0 \neq w \in X+z} \mathrm{ord}(w-w_0) \geq \sup_{w_0 \in X^\times + z} \inf_{w_0 \neq w \in X+z} \mathrm{ord}(w-w_0). \tag{2.1}$$

But $w \in X+z$ if and only if there exists $x \in X$ such that $w = x+z$, and in particular $w \in X^\times + z$ if and only if $x \in X^\times$. Also, given $x_0 \in X^\times$ and $x \in X$, it holds $x+z = x_0+z$ if and only if $x = x_0$. As a consequence, it is immediate from (2.1) and Remark 2.12 that

$$\gamma(X+z) \geq \sup_{x_0 \in X^\times} \inf_{x_0+z \neq w \in X+z} \mathrm{ord}(w+\tilde{z}-x_0) = \sup_{x_0 \in X^\times} \inf_{x_0 \neq x \in X} \mathrm{ord}(x-x_0) = \gamma(X),$$

where $\tilde{z}$ is the inverse of z in $\mathbb{A}$. Thus, our proof is complete. □

Now, the following proposition shows that the Cauchy-Davenport constant of a set is invariant under translation by units. While fundamental for the proof of our main result, this may be of independent interest in view of Conjecture 2.1.

Proposition 2.14. *Suppose that $\mathbb{A}$ is a monoid and pick $z \in A^\times$ and $X \subseteq A$. Then, we have*

$$\gamma(X) = \gamma(X+z) = \gamma(z+X).$$

Proof. Let $\tilde{z}$ denote the inverse of z in $\mathbb{A}$. Lemma 2.13 yields

$$\gamma(X) \leq \gamma(X+z) \leq \gamma((X+z)+\tilde{z}),$$

whence $\gamma(X) = \gamma(X+z)$. Then, we observe that, on the one hand, Proposition 2.10, together with the fact that $\mathbb{A}$ is the dual of $\mathbb{A}^{\mathrm{op}}$, implies $\gamma(X) = \gamma_{\mathbb{A}^{\mathrm{op}}}(X)$ and $\gamma_{\mathbb{A}^{\mathrm{op}}}(X+_{\mathrm{op}} z) = \gamma(X+_{\mathrm{op}} z) = \gamma(z+X)$, and on the other hand, it follows from the above that $\gamma_{\mathbb{A}^{\mathrm{op}}}(X) = \gamma_{\mathbb{A}^{\mathrm{op}}}(X+_{\mathrm{op}} z)$. This gives $\gamma(X) = \gamma(z+X)$ and completes our proof. □

Corollary 2.15. *Let $\mathbb{A}$ be a monoid, and for a fixed integer $n \geq 1$ pick $X_1, \ldots, X_n \subseteq A$ and $z_0, \ldots, z_n \in A^\times$. For each $i = 1, \ldots, n$ denote by T_i the map*

$$\mathcal{P}(A) \to \mathcal{P}(A) : X \to z_{i-1} + X - z_i.$$

Then, $(T_1, \ldots, T_n)$ is an invariant n-transform and $\gamma(T_i(X_i)) = \gamma(X_i)$ for each i.

Proof. By construction, it holds $\sum_{i=1}^n T_i(X_i) = z_0 + (X_1 + \cdots + X_n) + z_n$. Then, we get by Lemma 2.7 that

$$|X_1| = |T_1(X_1)|, \ldots, |X_n| = |T_n(X_n)| \text{ and } \left|\sum_{i=1}^n X_i\right| = \left|\sum_{i=1}^n T_i(X_i)\right|,$$

while Proposition 2.14 implies $\gamma(X_i) = \gamma(T_i(X_i))$ for each i and $\gamma(X_1 + \cdots + X_n) = \gamma(T_1(X_1) + \cdots + T_n(X_n))$. By putting all together, the claim follows immediately. □

Corollary 2.16. *Suppose $\mathbb{A}$ is a monoid, fix an integer $n \geq 1$ and let $X_1, \ldots, X_n$ be subsets of A such that $X_1^\times + \cdots + X_n^\times \neq \emptyset$. There then exists an invariant n-transform $\mathbf{T} = (T_1, \ldots, T_n)$ such that $0 \in \bigcap_{i=1}^n T_i(X_i)$. Moreover, if $\mathbb{A}$ is cancellative and $X_1^\times + \cdots + X_n^\times$ is finite, then $\mathbf{T}$ can be chosen in such a way that*

$$\gamma(T_1(X_1) + \cdots + T_n(X_n)) = \min_{0 \neq w \in T_1(X_1) + \cdots + T_n(X_n)} \mathrm{ord}(w). \tag{2.2}$$

Proof. For each $i = 1, \ldots, n$ pick $x_i \in X_i^\times$, using that $X_1^\times + \cdots + X_n^\times$ is non-empty (and hence

$X_i^\times \neq \emptyset$), and let T_i be the function

$$\mathcal{P}(A) \to \mathcal{P}(A) : X \mapsto z_{i-1} + X - z_i,$$

where $z_0 := 0$ and $z_i := x_1 + \cdots + x_i = z_{i-1} + x_i$. Then clearly $0 \in \bigcap_{i=1}^n T_i(X_i)$, while Corollary 2.15 entails that $(T_1, \ldots, T_n)$ is an invariant n-transform. Thus, the first part of the claim is proved.

As for the rest, assume in what follows that $\mathbb{A}$ is cancellative and $X_1^\times + \cdots + X_n^\times$ is finite. Then, letting $Z := X_1 + \cdots + X_n$ for brevity yields, by Proposition 2.11, that $X_1^\times + \cdots + X_n^\times = Z^\times$, so there exist $\bar{x}_1 \in X_1, \ldots, \bar{x}_n \in X_n$ such that

$$\gamma(Z) = \min_{\bar{z} \neq z \in Z} \operatorname{ord}(z - \bar{z}), \tag{2.3}$$

where $\bar{z} := \bar{x}_1 + \cdots + \bar{x}_n$ and we are using that a supremum taken over a non-empty finite set is, in fact, a maximum. It follows from the above that we can build an invariant n-transform $\bar{\mathbf{T}} = (\bar{T}_1, \ldots, \bar{T}_n)$ such that $0 \in \bigcap_{i=1}^n \bar{T}_i(X_i)$ and $\sum_{i=1}^n \bar{T}_i(X_i) = Z - \bar{z}$, with the result that

$$\gamma(Z) = \gamma(Z - \bar{z}) \geq \min_{0 \neq w \in Z - \bar{z}} \operatorname{ord}(w) = \min_{\bar{z} \neq z \in Z} \operatorname{ord}(z - \bar{z}),$$

by the invariance of $\bar{\mathbf{T}}$ and the fact that, on the one hand, $0 \in Z - \bar{z}$ and, on the other hand, $w \in Z - \bar{z}$ if and only if $w = z - \bar{z}$ for some $z \in Z$. Together with (2.3), this ultimately leads to $\gamma(Z - \bar{z}) = \min_{0 \neq w \in Z - \bar{z}} \operatorname{ord}(w)$, and thus to (2.2). □

We conclude the section with a proof of Lemma 1.10:

Proof of Lemma 1.10. By duality, it is enough to prove that $\gamma(Y) \geq \gamma(X + Y) \geq \mathfrak{p}(A)$, since all the rest is more or less trivial from our definitions. For, pick $z_0 \in (X + Y)^\times$ using that, on the one hand, $(X + Y)^\times = X^\times + Y^\times$ by Proposition 2.11 and the cancellativity of $\mathbb{A}$, and on the other hand, $X^\times + Y^\times$ is non-empty by the standing assumptions. There then exist $x_0 \in X^\times$ and $y_0 \in Y^\times$ such that $z_0 = x_0 + y_0$, and it is immediate from Remark 2.12 that, for all $y \in A$,

$$\langle x_0 + y - z_0 \rangle = x_0 + \langle y - y_0 \rangle - x_0,$$

which, together with Lemma 2.7, gives $\operatorname{ord}(y - y_0) = \operatorname{ord}(x_0 + y - z_0)$. Thus, considering that,

for $y \in A$, it holds $x_0 + y = z_0$ if and only if $y = y_0$, it follows that

$$\inf_{y_0 \neq y \in Y} \operatorname{ord}(y - y_0) = \inf_{y_0 \neq y \in Y} \operatorname{ord}(x_0 + y - z_0) \geq \inf_{z_0 \neq z \in X+Y} \operatorname{ord}(z - z_0) \geq \mathfrak{p}(A),$$

and this in turn implies the claim by taking the supremum over the units of $X + Y$. □

2.4 The proof of the main theorem

At long last, we are ready to prove the central contributions of the chapter. We start with the following:

Proof of Theorem 2.3. The claim is obvious if $(X + Y)^\times = \emptyset$, so suppose for the remainder of the proof that $(X + Y)^\times$ is non-empty (which, among the other things, implies that $\mathbb{A}$ is a monoid), and set $\kappa := |X + Y|$, while noticing that, by Lemma 2.11, both of $X^\times$ and $Y^\times$ are non-empty, and so, by Proposition 1.18 and Lemma 1.23, we have

$$\kappa \geq \max(|X|, |Y|) \geq \min(|X|, |Y|) \geq 1. \tag{2.4}$$

The statement is still trivial if $\kappa = \infty$ (respectively, $\kappa = 1$), since then either of X and Y is infinite (respectively, both of X and Y are singletons), and hence $|X+Y| = |X|+|Y|-1$ by (2.4). Thus, we assume in what follows that κ is a positive integer and argue by strong induction on κ, supposing by contradiction that $\kappa < \min(\gamma(X + Y), |X| + |Y| - 1)$. Based on the above, this ultimately means that

$$2 \leq \kappa < \infty, \;\; 2 \leq |X|, |Y| < \infty, \;\; \kappa < \gamma(X + Y), \;\; \text{and} \;\; \kappa \leq |X| + |Y| - 2. \tag{2.5}$$

More specifically, there is no loss of generality in assuming, as we do, that (X, Y) is a "minimax counterexample" to the claim, by which we mean that, if $(\bar{X}, \bar{Y})$ is another pair of subsets of A with $\bar{X}^\times + \bar{Y}^\times \neq \emptyset$ and $|\bar{X} + \bar{Y}| < \min(\gamma(\bar{X} + \bar{Y}), |\bar{X}| + |\bar{Y}| - 1)$, then either $\kappa = |\bar{X} + \bar{Y}|$ and at least one of the following conditions holds:

$$\text{(i) } |\bar{X}| + |\bar{Y}| < |X| + |Y|; \qquad \text{(ii) } |\bar{X}| + |\bar{Y}| = |X| + |Y| \text{ and } |\bar{X}| \leq |X|, \tag{2.6}$$

or $\kappa < |\bar{X} + \bar{Y}|$. This makes sense because if $\bar{X}, \bar{Y} \subseteq A$, $\bar{X}^\times + \bar{Y}^\times \neq \emptyset$ and $\kappa = |\bar{X} + \bar{Y}|$ then $\bar{X}^\times$

and $\bar{Y}^\times$ are non-empty, so we get, as before with (2.4), that

$$|\bar{X}| \leq |\bar{X}| + |\bar{Y}| \leq 2 \cdot \max(|\bar{X}|, |\bar{Y}|) \leq 2 \cdot |\bar{X} + \bar{Y}| = 2\kappa < \infty.$$

Finally, in the light of Corollary 2.16, we may also assume without restriction of generality, up to an invariant 2-transform, that

$$0 \in X \cap Y \text{ and } \gamma(X+Y) = \min_{0 \neq z \in X+Y} \operatorname{ord}(z). \tag{2.7}$$

Then, both of X and Y are subsets of $X+Y$, and by the inclusion-exclusion principle we have $\kappa \geq |X| + |Y| - |X \cap Y|$, which gives, together with (2.5), that $X \cap Y$ has at least one element different from 0, i.e. $|X \cap Y| \geq 2$. On these premises, we prove the following intermediate claim (from here on, we set $Z := X \cap Y$ for notational convenience):

Claim. *There exists n such that $X + nZ + Y \not\subseteq X + Y$, but $X + kZ + Y \subseteq X + Y$ for each $k = 0, \ldots, n-1$, with the convention that $0Z := \{0\}$.*

Proof of the claim. Assume by contradiction that $X + nZ + Y \subseteq X + Y$ for all n. Then, we get from $\langle Z \rangle = \bigcup_{n=1}^{\infty} nZ$ that $X + \langle Z \rangle + Y \subseteq X + Y$, which implies by (2.7) that $\langle Z \rangle = 0 + \langle Z \rangle + 0 \subseteq X + Y$. Then, using that $|Z| \geq 2$ to guarantee that $\{0\} \subsetneq Z \subseteq X + Y$, it follows from Proposition 1.18 and the same equation (2.7) that

$$\kappa \geq |\langle Z \rangle| \geq \max_{0 \neq z \in Z} \operatorname{ord}(z) \geq \min_{0 \neq z \in Z} \operatorname{ord}(z) \geq \min_{0 \neq z \in X+Y} \operatorname{ord}(z) = \gamma(X+Y).$$

This is, however, absurd, for it is in contradiction to (2.5), and we are done. □

So, let n be as in the above claim and fix, for the remainder of the proof, an element $\bar{z} \in nZ$ such that $X + \bar{z} + Y \not\subseteq X + Y$ (this exists by construction since otherwise we would have $X + nZ + Y \subseteq X + Y$, which is a contradiction). Consequently, observe that

$$(X + \bar{z}) \cup (\bar{z} + Y) \subseteq X + Y. \tag{2.8}$$

In fact, $\bar{z}$ being an element of nZ entails that there exist $z_1, \ldots, z_n \in Z$ such that $\bar{z} = z_1 + \cdots + z_n$, whence we get that both of $X + \bar{z}$ and $\bar{z} + Y$ are contained in $X + (n-1)Z + Y$. But $X + (n-1)Z + Y$ is,

again by construction, a subset of $X+Y$, so (2.8) is proved. With this in hand, let us now introduce the sets

$$X_0 := \{x \in X : x + \bar{z} + Y \not\subseteq X + Y\}$$

and

$$Y_0 := \{y \in Y : X + \bar{z} + y \not\subseteq X + Y\}.$$

It is then clear that X (respectively, Y) is disjoint from $X_0 + \bar{z}$ (respectively, from $\bar{z} + Y_0$). In addition, since $X + \bar{z} + Y \not\subseteq X + Y$, it is also immediate that X_0 and Y_0 are both non-empty. Finally, it follows from (2.8) that 0 is not an element of either X_0 or Y_0. To sum it up,

$$X_0 \neq \emptyset \neq Y_0, \;\; 0 \notin X_0 \cup Y_0 \;\text{ and }\; (X_0 + \bar{z}) \cap X = (\bar{z} + Y_0) \cap Y = \emptyset. \tag{2.9}$$

Now, let $n_X := |X_0|$ and $n_Y := |Y_0|$. By Remark 1.24 and the cancellativity of $\mathbb{A}$, we have

$$|X_0 + \bar{z}| = |X_0| = n_X \;\text{ and }\; |\bar{z} + Y_0| = |Y_0| = n_Y, \tag{2.10}$$

which naturally leads to distinguish between the following two cases:

Case 1 $n_X \geq n_Y$. We form $\bar{X}$ as the union of X and $X_0 + \bar{z}$ and $\bar{Y}$ as the relative complement of Y_0 in Y. First, note that $0 \in \bar{X}^\times \cap \bar{Y}^\times$ by (2.9). Secondly, pick $\bar{x} \in \bar{X}$ and $\bar{y} \in \bar{Y}$ and set $z := \bar{x} + \bar{y}$. If $\bar{x} \in X$, then obviously $z \in X + Y$; otherwise, by the construction of $\bar{X}$ and $\bar{Y}$, we get $\bar{x} \in X_0 + \bar{z} \subseteq X + \bar{z}$ and $\bar{y} \notin Y_0$, so that $\bar{x} + \bar{y} \in X + Y$. Therefore, we see that $\bar{X} + \bar{Y}$ is a non-empty subset of $X + Y$ with $0 \in \bar{X} + \bar{Y}$, so on the one hand $|\bar{X} + \bar{Y}| \leq \kappa$ and on the other hand we have by (2.7) that

$$\gamma(X + Y) \leq \inf_{0 \neq z \in \bar{X} + \bar{Y}} \mathrm{ord}(z) \leq \gamma(\bar{X} + \bar{Y}).$$

Furthermore, (2.9) and (2.10) give that $|\bar{X}| = |X| + |X_0 + \bar{z}| = |X| + n_X > |X|$ and $|\bar{Y}| = |Y| - |Y_0| = |Y| - n_Y$, so $|\bar{X}| + |\bar{Y}| = |X| + |Y| + n_X - n_Y \geq |X| + |Y|$.

Case 2 $n_X < n_Y$. We set $\bar{X} := X \setminus X_0$ and $\bar{Y} := (\bar{z} + Y_0) \cup Y$. Then, by repeating (except for obvious modifications) the same reasoning as in the previous case, we get again that $0 \in \bar{X}^\times \cap \bar{Y}^\times$ and $\bar{X} + \bar{Y} \subseteq X + Y$, with the result that $|\bar{X} + \bar{Y}| \leq \kappa$ and $\gamma(X + Y) \leq \gamma(\bar{X} + \bar{Y})$. In

addition, it follows from (2.9) and (2.10) that $|\bar{X}| = |X| - |X_0| = |X| - n_X$ and $|\bar{Y}| = |Y| + |\bar{z} + Y_0| = |Y| + n_Y$, whence $|\bar{X}| + |\bar{Y}| = |X| + |Y| + n_Y - n_X > |X| + |Y|$.

So in both cases, we end up with an absurd, for we find subsets $\bar{X}$ and $\bar{Y}$ of A that contradict the "minimaximality" of (X, Y) as it is expressed by (2.6). □

Remarkably, several pieces of the above proof of Theorem 2.3 do *not* critically depend on the cancellativity of the ambient, while others can be adapted to the case where $\gamma(X + Y)$ is replaced by $\gamma(X, Y)$, which is one of our strongest motivations for believing that Conjecture 2.1 should be ultimately true.

Proof of Corollary 2.4. The claim is obvious if $n = 1$. Thus, assume in what follows that n is ≥ 2 and the assertion is true for all sumsets of the form $Y_1 + \cdots + Y_{n-1}$ with $Y_1^\times + \cdots + Y_{n-1}^\times \neq \emptyset$. Based on these premises, we get by Theorem 2.3 that

$$|X_1 + \cdots + X_n| \geq \min(\gamma(X_1 + \cdots + X_n), |X_1 + \cdots + X_{n-1}| + |X_n| - 1),$$

which in turn implies, by Lemma 1.10, that

$$|X_1 + \cdots + X_n| \geq \min(\mathfrak{p}(A), |X_1 + \cdots + X_{n-1}| + |X_n| - 1). \tag{2.11}$$

But we know from Proposition 2.11 that $X_1^\times + \cdots + X_{n-1}^\times \neq \emptyset$, so the inductive hypothesis gives

$$|X_1 + \cdots + X_{n-1}| \geq \min(\mathfrak{p}(A), |X_1| + \cdots + |X_{n-1}| + 2 - n),$$

which, together with (2.11), yields the desired conclusion by induction. □

References

[B1] N. Bourbaki, *Algèbre, Chapitres 1 à 3*, Éléments de mathématique II (Springer-Verlag, Berlin, 2006, 2nd revised ed).

[C] A.-L. Cauchy, *Recherches sur les nombres*, J. École Polytech. **9** (1813), 99–116 (reproduced in *Oeuvres*, Série 2, Tome 1, 39–63).

[CHS] A. L. Cilleruelo, Y. O. Hamidoune and O. Serra, 'Addition theorems in acyclic semigroups', in *Additive number theory* (Springer, 2010), 99–104.

[Ch] I. Chowla, *A theorem on the addition of residue classes: Application to the number* $\Gamma(k)$ *in Waring's problems*, Proc. Indian Acad. Sc. (A) **2** (1935), 242–243.

[D1] H. Davenport, *On the addition of residue classes*, J. London Math. Soc. **10** (1935), 30–32.

[D2] _____, *A historical note*, J. London Math. Soc. **22** (1947), 100–101.

[Ha] Y. O. Hamidoune, *A Generalization of an Addition Theorem of Shatrowsky*, Europ. J. Combmatorics **13** (1992), 249–255.

[Ho] J. M. Howie, *Fundamentals of semigroup theory* (Clarendon Press, 1995).

[Ka] G. Károlyi, *The Cauchy-Davenport theorem in group extensions*, Enseign. Math. **51** (2005), 239–254.

[Ke] J. H. B. Kemperman, *On complexes in a semigroup*, Indag. Math. **18** (1956), 247–254.

[Ma] A. I. Mal'cev, *On the immersion of an algebraic ring into a field*, Math. Annalen (1) **113** (1937), 686–691.

[O] J. E. Olson, *On the Sum of Two Sets in a Group*, J. Number Th. **18** (1984), 110–120.

[Pi] S. S. Pillai, *Generalization of a theorem of Davenport on the addition of residue classes*, Proc. Indian Acad. Sc. (A) (3) **6** (1937) 179–180.

[TV] T. Tao and V. H. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics **105** (Cambridge University Press, Cambridge, 2009).

[Tr2] S. Tringali, *Cauchy-Davenport type theorems for semigroups*, submitted (preprint: arXiv/1307.8396).

This page intentionally left blank

This page intentionally left blank

If you can make one heap of all your winnings
And risk it on one turn of pitch-and-toss,
And lose, and start again at your beginnings
And never breathe a word about your loss.

— Joseph R. Kipling, *If*

3

Small doubling in ordered semigroups

Resumé. On généralise des résultats par G. A. Freĭman, M. Herzog et leurs coauteurs sur la théorie structurelle des sommes d'ensembles dans les groupes linéairement ordonnés au cas plus général des semi-groupes linéairement ordonnés. En particulier, on prouve que, si $(A, \cdot, \preceq)$ est un semi-groupe linéairement ordonné et S est un sous-ensemble fini de A engendrant un sous-semi-groupe non-abélien, alors $|S^2| \geq 3|S|-2$. Au cours de la preuve, on obtient également un grand nombre de résultats secondaires, et notamment que le commutateur et le normalisateur d'un sous-ensemble fini d'un semi-groupe linéairement ordonné coïncident. Ce chapitre est basé sur un article par l'auteur [Tr3] soumis pour publication.

Abstract. Let $\mathbb{A} = (A, \cdot)$ be a semigroup. We generalize results by G. A. Freĭman, M. Herzog and coauthors on the structure theory of set addition from the context of linearly ordered groups to linearly ordered semigroups, where we say that $\mathbb{A}$ is linearly orderable if there exists a total order

$\preceq$ on A such that $xz \prec yz$ and $zx \prec zy$ for all $x, y, z \in A$ with $x \prec y$. In particular, we find that if S is a finite subset of A generating a non-abelian subsemigroup of $\mathbb{A}$, then $|S^2| \geq 3|S| - 2$. 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. The chapter is based on a paper by the author [Tr3] submitted for publication.

3.1 Introduction

Semigroups are ubiquitous in mathematics. Apart from being a subject of continuous interest to algebraists, they are, as already remarked in the previous chapters, a natural framework for introducing several broadly-scoped concepts and developing large parts of theories traditionally presented in much less general contexts.

Our interest in semigroups is related here to Freĭman's structure theory of set addition and its generalizations; this is a very active area of research, which has drawn a constantly increasing attention in the last decade, and has led to significant progress in several fields, from algebra [Ge] to additive number theory and combinatorics [Na, R, TV].

The primary goal of the chapter is, in fact, to extend recent results by G. A. Freĭman, M. Herzog and coauthors from the setting of linearly ordered groups [FHLM] to linearly ordered semigroups (see Section 3.2 for definitions). 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). The main contribution here is then represented by the following generalization of [FHLM, Theorem 1.2]:

Theorem 3.1. *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.*

Our proof of Theorem 3.1 basically follows the same broad scheme as the proof of [FHLM, 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 result known to hold for linearly ordered groups should be reformulated in the language of semigroups). In particular, we will look for an extension of several classical results, such as the following:

Lemma 3.2. *Let $\mathbb{A}$ be a linearly orderable semigroup and pick $a, b \in A$. If $a^n b = b a^n$ for some n, then $ab = ba$.*

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

In the same spirit, we will also need to extend [FHLM, Proposition 2.4]. For, we 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. Building on these premises, we have:

Lemma 3.3. *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, $|yS \cup Sy| \geq |S| + 1$, i.e. there are $a, b \in S$ with $ya \notin Sy$ and $by \notin yS$.*

Lemma 3.3 is proved in Section 3.2, along with the following generalization of [FHLM, Corollary 1.5], which may perhaps be interesting *per se*:

Theorem 3.4. *If $\mathbb{A}$ is a linearly orderable semigroup and S a finite subset of A, then $\mathrm{N}_{\mathbb{A}}(S) = \mathrm{C}_{\mathbb{A}}(S)$.*

We conclude the chapter with a number of examples (Appendix 3.5), 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 3.21) 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, subsequently raising the question (to which we do not have an answer) whether the same conclusion holds for the subsemigroup of all matrices which can be written as a (finite) product of upper or lower triangular matrices of the same kind as above.

3.2 Notation and definitions

Throughout, an order on a set A is a binary relation $\preceq$ on A which is reflexive, antisymmetric, transitive, and total, in the sense that for all $a, b \in A$ we have either $a \preceq b$ or $b \prec a$, where $\prec$ is used for the strict order induced on A by $\preceq$.

Accordingly, we let an ordered semigroup be a triple $(A, \cdot, \preceq)$, where $(A, \cdot)$ is a semigroup, $\preceq$ is an order on A, and the following holds:

$$\forall a, b, c \in A : a \prec b \quad \Longrightarrow \quad a \cdot c \preceq b \cdot c \text{ and } c \cdot a \preceq c \cdot b. \tag{3.1}$$

If each of the signs "$\preceq$" in (3.1) is replaced with the sign "$\prec$", then $(A, \cdot, \preceq)$ is called a *linearly ordered semigroup*; see, e.g., [Iw].

Conversely, we say that a semigroup $\mathbb{A} = (A, \cdot)$ is *[linearly] orderable* if there exists an order $\preceq$ on A such that $(A, \cdot, \preceq)$ is a [linearly] ordered semigroup.

All of the above notions and terminology are now extended in the obvious way to monoids and groups (so we have, for instance, ordered monoids and linearly orderable groups).

3.3 Preliminaries

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

In this section, we collect some results that will be essential to prove the main contributions of the paper, later in Section 3.4. 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 our definitions, and we may omit the details.

Proposition 3.5. *The following holds:*

(i) *For all $a_1, \dots, a_n, b_1, \dots, b_n \in A$ with $a_1 \preceq b_1, \dots, a_n \preceq b_n$ we have $a_1 \cdots a_n \preceq b_1 \cdots b_n$, and indeed $a_1 \cdots a_n \prec b_1 \cdots b_n$ if $\mathbb{A}_\sharp$ is linearly ordered and $a_i \prec b_i$ for each i.*

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

(iii) *If $a \in A$ is such that $a^2 \preceq a$, then $a^n \preceq a^m$ for $m \leq n$, and indeed $a^n \prec a^m$ if $\mathbb{A}_\sharp$ is linearly ordered, $a^2 \prec a$ 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 3.6. 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 already mentioned in Remark 1.16, nothing similar is true, on the other hand, in the non-commutative case, no matter if the ambient is linearly orderable and finitely generated, as first noticed by R. E. Johnson [J] on the basis of Mal'cev's construction [M1]. Again, 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 n and $p \in \mathbb{N}^+$ 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, for instance, [Ho, 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 3.7. The unique idempotent element of a cancellative monoid is the identity, so that torsion-free groups are definitely a special kind of torsion-free semigroups; cf. Example 3.17. 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 3.6): 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 next proposition generalizes properties mentioned in [FHLM, Section 2].

Proposition 3.8. *Let $\mathbb{A}_\sharp$ be a linearly ordered semigroup. We have:*

(i) *If $a \in A$ and $a^2 \prec a$, then $ab \prec b$ and $aba \prec b$ 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 $a^2 \prec a$. Then $a^2 b \prec ab$, whence $ab \prec b$ by totality of $\preceq$ and Remark 3.6. It follows from Proposition 3.5 that $aba^2 \prec ba$; thus, $aba \prec b$ by the same arguments as above.

(ii) Let $a, b \in A$ be such that $aba = b$. By duality, we may suppose that $a^2 \preceq a$, which implies the claim by Remark 3.7 and the previous point (i).

(iii) is trivial from the above, and we may omit the details. □

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

Proposition 3.9. *Suppose that $\mathbb{A}_\sharp$ is a linearly ordered semigroup and let $S_1, \ldots, S_n$ be non-empty finite subsets of A. Then,*

$$|S_1 \cdots S_n| \geq 1 - n + \sum_{i=1}^{n} |S_i|. \tag{3.2}$$

Also, (3.2) is sharp, the lower bound being attained, for instance, by picking $a \in A$ and letting S_i be, for each i, of the form $\{a, \ldots, a^{s_i}\}$ for some $s_i \in \mathbb{N}^+$.

In particular, the second part of Proposition 3.9 follows from considering that, given a linearly orderable non-trivial non-empty semigroup $\mathbb{A}$, point (iii) of Proposition 3.8 provides at least one element $a \in A$ such that $a^{j_1} \neq a^{j_2}$ for all distinct $j_1, j_2 \in \mathbb{N}^+$.

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

Proposition 3.10. *Let $\mathbb{A}_\sharp$ be a linearly ordered semigroup and pick $a, b \in A$. If $ab \prec ba$ then for all n we have*

$$a^n b \prec a^{n-1} ba \prec \cdots \prec aba^{n-1} \prec ba^n. \tag{3.3}$$

Proof. Assume that (3.3) holds true for some 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. □

The proof of Lemma 3.2 is now an immediate consequence of Proposition 3.10 (by duality, if $\mathbb{A}_\sharp$ is a linearly ordered semigroup and $a, b \in A$ then we may assume $ab \preceq ba$ without loss of generality).

Proof of Lemma 3.3. 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) $a_i = a_j$ for $i, j = 1, \ldots, k$ only if $i = j$.

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 3.2), and indeed $y a_k = y a_{k-1}$ (as $a_k y = y a_{k-1}$, by construction). So, Remark 3.6 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. □

Proof of Theorem 3.4. The claim is obvious if $S = \emptyset$, so assume that S is non-empty. For $y \in \mathrm{N}_{\mathbb{A}}(S)$ we have $yS = Sy$, and Lemma 3.3 implies $y \in \mathrm{C}_{\mathbb{A}}(S)$, from which it follows $\mathrm{N}_{\mathbb{A}}(S) \subseteq \mathrm{C}_{\mathbb{A}}(S)$. The other inclusion is obvious. □

3.4 The main result

Throughout, $\mathbb{A} = (A, \cdot)$ denotes a fixed semigroup (unless differently 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 ordered semigroups.

Lemma 3.11. *Let $\mathbb{A}$ be a cancellative semigroup and S a finite subset of A such that $\langle S \rangle$ is an abelian subsemigroup. 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 by contradiction that $S^2 \cap (yS \cup Sy)$ is non-empty. Then, without loss of generality, there 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 abelianity of $\langle S \rangle$). So, at the end of the day, $yxc = xyc$, and hence $yx = xy$ (by cancellativity of c). It follows that $y \in \mathrm{C}_{\mathbb{A}}(S)$, which is absurd. □

Lemma 3.12. *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, $baz = bxy = xyb$ since $x, y \in \mathrm{C}_{\mathbb{A}}(b)$. Hence $abz = baz$, that is $ab = ba$ (by cancellativity of z). □

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

Lemma 3.13. *Let $\mathbb{A}_\sharp$ be linearly ordered, and let S be a non-empty finite subset of A, and 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 3.6 and Lemma 3.11 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 3.9, and $|yS \cup Sy| \geq |S| + 1$, by Lemma 3.3. □

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

Proof of Theorem 3.1. Write I_m for $\{1, \ldots, m\}$, where $m := |S|$, and let $a_1, \ldots, a_m$ be a numbering of S for which $a_1 \prec \cdots \prec a_m$. It is clear that $m \geq 2$. If $m = 2$ then $|S^2| \leq 3$, and indeed $|S^2| = 3$ by Proposition 3.9. Since $a_1^2 \prec a_1a_2 \prec a_2^2$ 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 $\langle S \rangle$ is abelian, as was desired.

So, in what follows, let $m \geq 3$ and suppose that $\langle B \rangle$ is abelian for every subset B of A satisfying $2 \leq |B| < m$ and $|B^2| \leq 3|B| - 3$. Furthermore, assume for the sake of 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

$$T^2 \cap (a_{i+1}T \cup Ta_{i+1}) = \emptyset, \tag{3.4}$$

thanks to Remark 3.6 and Lemma 3.11, and on the other hand

$$|T^2 \cup a_{i+1}T \cup Ta_{i+1}| \geq 3i, \tag{3.5}$$

by virtue of Lemma 3.13. Also, there exists a positive integer $j \leq i$ such that

$$a_{i+1}a_j \neq a_j a_{i+1}, \tag{3.6}$$

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

$$xa_{i+1} = a_{i+1}x \quad \text{for every } x \in T \text{ with } a_j \prec x. \tag{3.7}$$

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

$$V^2 \cap (T^2 \cup a_{i+1}T \cup Ta_{i+1}) = \emptyset \tag{3.8}$$

since $a_h a_k \prec a_{i+1}^2 \preceq a_r a_s$ for all $h, k, r, s \in I_m$ with $h + k \leq 2i + 1$ and $i + 1 \leq \min(r, s)$. Then, the inclusion-exclusion principle, together with (3.5) 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,

$$V^2 \cap (a_j V \cup Va_j) = \emptyset \tag{3.9}$$

in view of Remark 3.6, Lemma 3.11 and the fact that $a_j \notin \mathrm{C}_{\mathbb{A}}(V)$. We claim

$$T^2 \cap (a_j V \cup Va_j) = \emptyset. \tag{3.10}$$

For, assume to the contrary, with no loss of generality, that $T^2 \cap a_j V \neq \emptyset$, namely $xy = a_j z$ for some $x, y \in T$ and $z \in V$. Using that $y \prec z$, this yields $a_j \prec x$, and similarly $a_j \prec y$ as $\langle T \rangle$ is abelian (so that $xy = yx$, and hence $yx = a_j z$). It then follows from (3.7) and the abelianity of $\langle V \rangle$ that $x, y, z \in \mathrm{C}_{\mathbb{A}}(a_{i+1})$. Thus, we get $a_{i+1}a_j = a_j a_{i+1}$ by Lemma 3.12, which however contradicts (3.6) and implies (3.10).

That said, let $x \in T$ and $y \in V$ be such that $xa_{i+1} = a_j y$. 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 (3.7) and the abelianity 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 3.12).

But this is in open contrast with (3.6), 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

$$|Ta_{i+1} \cup a_j V| = |Ta_{i+1}| + |a_j V| - |Ta_{i+1} \cap a_j V| = m - 1, \tag{3.11}$$

which in turn implies, together with (3.4), (3.8), (3.9) and (3.10), 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 3.9 and (3.11) 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

$$S^2 = T^2 \cup V^2 \cup Ta_{i+1} \cup a_j V. \tag{3.12}$$

So to conclude, let us define $a := a_{i+1}a_j$. By (3.4) and (3.8), it is straightforward to see 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. To this aim, observe first that, by (3.6) and Lemma 3.3, there exist $x \in T$ and $y \in V$ such that

$$a_{i+1}x \notin Ta_{i+1}, \quad ya_j \notin a_j V. \tag{3.13}$$

Since $a_{i+1}x, ya_j \notin T^2 \cup V^2$ by (3.4), (3.8), (3.9) and (3.10), it follows from (3.12) 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

$$a_j b = a_{i+1}x, \quad ya_j = c\,a_{i+1}. \tag{3.14}$$

Suppose that $a \in Ta_{i+1}$, that is there exists $z \in T$ for which $za_{i+1} = a_{i+1}a_j$, and in fact $z \neq a_j$ by (3.6). If $a_j \prec z$ then $z \in \mathrm{C}_{\mathbb{A}}(a_{i+1})$ by (3.7), so $a_{i+1}a_j = a_j a_{i+1}$ by Lemma 3.12, again in

contradiction to (3.6). Thus $z \prec a_j$, and in addition $x \preceq a_j$, as otherwise $a_{i+1}x = xa_{i+1} \in Ta_{i+1}$ in view of (3.7), in contradiction to (3.13). Considering that $\langle T \rangle$ is abelian, it follows from (3.14) that $a_j b a_j = a_{i+1} x a_j = a_{i+1} a_j x$. However $a_{i+1}a_j = z a_{i+1}$, so at the end $a_j b a_j = z a_{i+1} x$. Hence, $b a_j \prec a_{i+1} x$ as $z \prec a_j$, which is absurd since $a_{i+1} \preceq b$ and $x \preceq a_j$, viz $a_{i+1}x \preceq b a_j$. This implies $a \notin Ta_{i+1}$.

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 $a_{i+1} \preceq w$, and indeed $a_{i+1} \prec w$ by (3.6). We want to show that $c \preceq a_j$. For, suppose to the contrary that $a_j \prec c$. The abelianity of $\langle V \rangle$, together with (3.7), 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 (3.14) and Lemma 3.12; this contradicts (3.6), and hence $c \preceq a_j$. Using once more that $\langle V \rangle$ is abelian, it is then immediate from (3.14) that $a_{i+1}ca_{i+1} = a_{i+1}ya_j = ya_{i+1}a_j$, so $a_{i+1}ca_{i+1} = ya_j w$ since $a_{i+1}a_j = a_j w$. But, as argued before, $a_{i+1} \prec w$, whence it is seen that $ya_j \prec a_{i+1}c$, which is absurd because $a_{i+1} \preceq y$, by construction of V, and $c \preceq a_j$, as proved above. Thus, we get that $a \notin a_j V$.

Putting all together, it follows that $a \notin T^2 \cup V^2 \cup Ta_{i+1} \cup a_j V$, which is however in contradiction to (3.12), as a is obviously an element of S^2. Therefore, $\langle S \rangle$ is abelian. □

In some sense, Theorem 3.1 is best possible; specifically, [FHLM, Section 3] provides the example of a subset S of a linearly ordered group generating a non-abelian subgroup and such that $|S^2| = 3|S| - 2$.

Corollary 3.14. *Let S be a finite subset of a linearly orderable semigroup $(A, \cdot)$, which generates a non-abelian subsemigroup. Then $|S^2| \geq 3|S| - 2$.*

Proof. It is just a trivial restatement of Theorem 3.1. □

We have not found so far an appropriate way to extend Proposition 3.1 in [FHLM] 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 3.15. *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 convenience 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 geometric progression $a, ab, \ldots, ab^{t-s}$?*

3.5 Appendix: 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. Then, we mention some classes of linearly orderable groups and some linearly orderable monoids (respectively, semigroups) which are not groups (respectively, monoids).

Example 3.16. 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, [Ho, p. 3]. Trivially, if $\preceq$ is a total order on A then $(A, \cdot, \preceq)$ is a totally ordered semigroup. However, $(A, \cdot)$ is not linearly orderable for $|A| \geq 2$.

Example 3.17. An interesting variety of linearly ordered groups is provided by abelian torsion-free groups, as first proved by F. W. Levi in [Le], and the result can be, in fact, extended to abelian cancellative torsion-free semigroups with no substantial modification; see the comments following Remark 3.6 in Section 3.2 and Corollary 3.4 in R. Gilmer's book on commutative semigroup rings [Gi]. In a similar vein, K. Iwasawa [Iw], A. I. Mal'cev [M2] and B. H. Neumann [Ne] established independently that all torsion-free nilpotent groups are linearly orderable.

Save for the semigroup analogue of Levi's result, all of the above is already mentioned in [FHLM], where the interested reader can find further references to existing literature on the subject. However, there are other interesting examples of linearly ordered groups which are *not* included in [FHLM], and remarkably *pure* braid groups [RZ] and free groups [Iw].

Example 3.18. As for linearly ordered monoids which are not linearly ordered groups, consider, for instance, the free monoid [Ho, Section 1.6] on a totally ordered alphabet $(X, \preceq)$ 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 primes, endowed with the usual multiplication, provide the example of a linearly orderable semigroup which is not even a monoid unless $S = \emptyset$.

Example 3.19. Let $\mathbb{A} = (A, \cdot)$ and $\mathbb{B} = (B, \diamond)$ be semigroups and $\varphi : \mathbb{A} \to \mathbb{B}$ a semigroup monomorphism, i.e. an injective function $A \to B$ such that $\varphi(a_1 \cdot a_2) = \varphi(a_1) \diamond \varphi(a_2)$ for all

$a_1, a_2 \in A$. If $\mathbb{B}$ is linearly ordered by a certain order $\preceq_B$ and $\preceq_A$ is the binary relation on A defined by taking $a_1 \preceq_A a_2$ if and only if $\varphi(a_1) \preceq_B \varphi(a_2)$, it is routine to check that $\preceq_A$ is a total order, and indeed $(A, \cdot, \preceq_A)$ is a linearly ordered semigroup.

The next example is potentially 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 3.20. 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 $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(a+b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in A$.

(In other words, a semiring is 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 [He, Ch. II] and [Go, Ch. 1, p. 1].

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

4. $(A, +, \preceq)$ is a linearly ordered monoid;
5. $a \cdot c \prec b \cdot c$ and $c \cdot a \prec c \cdot b$ for all $a, b, c \in A$ with $a \prec b$ and $0 \prec c$,

then $(A, +, \cdot)$ is said to be linearly orderable and $(A, +, \cdot, \preceq)$ is called a linearly ordered semiring; cf. [Go, Ch. 20]. Notable examples of linearly ordered semirings are $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}_0^+$, and $\mathbb{R}$ with their usual structure.

On these premises, 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 implied 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 a semiring *per se*, called the semiring of n-by-n matrices over $\mathbb{A}$ and written as $\mathcal{M}_n(\mathbb{A})$; see [Go, Ch. 3].

Now, suppose $\mathbb{A}$ is linearly ordered by a certain order $\preceq$, so that $\mathbb{A}_\sharp := (A, +, \cdot, \preceq)$ 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 $\mathbb{A}_\sharp^+ := \{a \in A : 0 \prec a\}$. Observe that $\mathrm{U}_n(\mathbb{A}_\sharp^+)$ is not, in general, a group (for instance, the inverse of a regular 2-by-2 matrix with positive real entries has not positive real entries), and not even a monoid for $n \geq 2$. Perhaps more interestingly, we have the following:

Theorem 3.21. *$\mathrm{U}_n(\mathbb{A}_\sharp^+)$ 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 $\preceq_{n,\mathrm{U}}$ 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 $\mathrm{U}_n(\mathbb{A}_\sharp^+)$, $\alpha \preceq_{n,\mathrm{U}} \beta$ 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 $(i, j) \in \Xi_n$ with $(i, j) <_n (i_0, j_0)$.

It is straightforward that $\preceq_{n,\mathrm{U}}$ 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 $\preceq$ is total, we have that 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, and we are done.

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

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

and, similarly, $\sum_{k=1}^n c_{i,k}a_{k,j} \preceq \sum_{k=1}^n c_{i,k}b_{k,j}$. In particular, these majorizations are equalities for

$(i,j) <_n (i_0,j_0)$ and strict inequalities if $(i,j) = (i_0,j_0)$. So $\alpha \cdot \gamma \prec_{n,\mathrm{U}} \beta \cdot \gamma$ and $\gamma \cdot \alpha \prec_{n,\mathrm{U}} \gamma \cdot \beta$, and the proof is complete. □

We refer to the order $\preceq_{n,\mathrm{U}}$ defined in the proof of Theorem 3.21 as the *zig-zag order* on $\mathrm{U}_n(\mathbb{A}_\sharp^+)$. If $\mathrm{L}_n(\mathbb{A}_\sharp^+)$ stands for 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 straightforward to see that $\mathrm{L}_n(\mathbb{A}_\sharp^+)$ is itself linearly orderable: It is, in fact, linearly ordered by the binary relation $\preceq_{n,\mathrm{L}}$ defined by taking $\alpha \preceq_{n,\mathrm{L}} \beta$ if and only if $\alpha^\top \preceq_{n,\mathrm{U}} \beta^\top$, where the superscript '$\top$' means 'transpose'. Provided that $\mathrm{T}_n(\mathbb{A}_\sharp^+)$ 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 3.22. *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 $\mathbb{A}$ be the real field 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 (real) entries each of whose columns sums up 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 [Go, Example 20.60].

Example 3.23. In what follows, we let $\mathbb{K} = (K,+,\cdot)$ be a semiring (see Example 3.20 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 $f(a) \neq 0_K$ for finitely many $a \in A$, 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 multiplication of $\mathbb{K}$, respectively). We have the following:

Theorem 3.24. *Suppose that* $\mathbb{K}$ *is a linearly orderable semiring and* $\mathbb{A}$ *a linearly orderable semigroup. Then* $\mathbb{K}[\mathbb{A}]$ *is itself a linearly orderable semiring.*

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

Then, given $a \in A$ and $f \in K[A]$ we let $f_{\downarrow a}$ (respectively, $f_{\uparrow a}$) be the function $A \to K$ taking a to $f(a)$ if $a \prec_A a$ (respectively, $a \preceq_A a$), and to 0_K otherwise, in such a way that $f = f_{\downarrow a} + f_{\uparrow a}$. 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 $\preceq_A$, and it exists by consequence of the definition itself of $K[A]$), and to A otherwise.

We define a binary relation $\preceq$ on $K[A]$ by letting $f \preceq g$ if and only if either $f = g$ or $f \neq g$ and $f(\mu(f,g)) \prec_K f(\mu(f,g))$. It is clear that $\preceq$ 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 $\preceq$.

For, pick $f, g, h \in K[A]$ with $f \prec g$. Since the additive monoid of $\mathbb{K}$ is linearly ordered by $\preceq_K$, we have $\mu(f,g) = \mu(f+h, g+h)$, and thus $f + h \prec g + h$. That is, $(K[A], +, \preceq)$ is a linearly ordered monoid in its own right. On another hand, assume $\Theta \prec h$, 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 $f \cdot h \prec g \cdot h$ if and only if $f_{\uparrow\alpha} \cdot h_{\uparrow\beta} \prec g_{\uparrow\alpha} \cdot h_{\uparrow\beta}$, and the latter inequality is certainly true, since on the one side $f_{\uparrow\alpha} \cdot h_{\uparrow\beta}(a) = g_{\uparrow\alpha} \cdot h_{\uparrow\beta}(a) = 0_K$ for $a \prec_A \alpha \diamond \beta$, and on the other

$$f_{\uparrow\alpha} \cdot h_{\uparrow\beta}(\alpha \diamond \beta) = f_{\uparrow\alpha}(\alpha) \cdot h_{\uparrow\beta}(\beta) \prec_K g_{\uparrow\alpha}(\alpha) \cdot h_{\uparrow\beta}(\beta) = g_{\uparrow\alpha} \cdot h_{\uparrow\beta}(\alpha \diamond \beta).$$

In a similar way, it is seen that $h \cdot f \prec h \cdot g$. So, by the arbitrariness of f, g, and h, we get that $(K[A], +, \cdot, \preceq)$ 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 3.17), we have the following:

Corollary 3.25. *The semiring $\mathbb{K}$ is linearly orderable if and only if it goes the same with the semiring of polynomials with coefficients in $\mathbb{K}$ depending on a given set of pairwise commuting (respectively, non-commuting) variables.*

References

[B1] N. Bourbaki, *Algèbre, Chapitres 1 à 3*, Éléments de mathématique II (Springer-Verlag, Berlin, 2006, 2nd revised ed.).

[B2] N. Bourbaki, *Théorie des ensembles*, Éléments de mathématique I (Springer-Verlag, Berlin, 2006, reprint ed.).

[FHLM] G. Freĭman, M. Herzog, P. Longobardi, and M. Maj, *Small doubling in ordered groups*, J. Austral. Math. Soc., to appear.

[Ge] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations: Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics 278 (Chapman & Hall/CRC, 2006).

[Gi] R. Gilmer, *Commutative Semigroup Rings* (University Of Chicago, Chicago, 1984).

[Go] J. S. Golan, *Semirings and their Applications* (Kluwer Academic Publishers, Dordrecht, 1999).

[He] U. Hebisch and H. J. Weinert, *Semirings: Algebraic Theory and Applications in Computer Science*, Algebra 5 (World Scientific, 1998).

[Ho] J. M. Howie, *Fundamentals of semigroup theory* (Clarendon Press, Oxford, 2003, reprint ed.).

[Iw] K. Iwasawa, *On linearly ordered groups*, J. Math. Soc. Japan **1** (1948), 1–9.

[J] R. E. Johnson, *Extended Malcev Domains*, Proc. Amer. Math. Soc. (1) **21** (Apr., 1969), 211–213.

[Le] F. W. Levi, *Arithmetische Gesetze im Gebiete diskreter Gruppen*, Rend. Circ. Mat. Palermo **35** (1913), 225–236.

[M1] A. I. Mal'cev, *On the immersion of an algebraic ring into a field*, Math. Annalen (1)**113** (1937), 686–691.

[M2] ———, *On ordered groups*, Izv. Akad. Nauk. SSSR Ser. Mat. **13** (1948), 473–482.

[Na] M. B. Nathanson, *Additive Number Theory: Inverse Problems and Geometry of Sumsets*, Graduate Texts in Mathematics 165 (Springer-Verlag, New York, 1996).

[Ne] B. H. Neumann, *On ordered groups*, Amer. J. Math. **71** (1949), 1–18.

[RZ] D. Rolfsen and J. Zhu, *Braids, orderings and zero divisors*, J. Knot Theory Ramifications (6)**7** (1998), 837–841.

[R] I. Z. Ruzsa, 'Sumsets and structure', in: *Combinatorial Number Theory and Additive Group Theory* (Birkhäuser Verlag, Basel, 2009), 87–210.

[Tr3] S. Tringali, *Small doubling in ordered semigroups*, submitted (preprint: arXiv/1208.3233).

[TV] T. Tao and V. H. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics 105 (Cambridge University Press, Cambridge, 2009).

This page intentionally left blank

This page intentionally left blank

Part II

Elementary Number Theory

This page intentionally left blank

Amo como ama o amor. Não conheço nenhuma outra razão para amar senão amar. Que queres que te diga, além de que te amo, se o que quero dizer-te é que te amo?

— Fernando A. N. Pessoa, *Primeiro Fausto*

4

On a conjecture of Győry and Smyth

Resumé. Nous déterminons tous les triplets (a, b, n) d'entiers positifs tels que a et b sont premiers entre eux et n^k divise $a^n + b^n$ (respectivement, $a^n - b^n$), lorsque k est le maximum de a et b (en fait, nous répondons à une question un peu plus générale). Comme sous-produit, il est obtenu que, pour $m, n \in \mathbb{N}^+$ et $n \geq 2$, n^m divise $m^n + 1$ si et seulement si $(m, n) = (2, 3)$ ou $(1, 2)$. Les résultats sont liés à une conjecture par K. Győry et C. Smyth sur la finitude des ensembles $R_k^{\pm}(a, b) := \{n \in \mathbb{N}^+ : n^k \mid a^n \pm b^n\}$, où a, b, k sont des entiers fixes avec $k \geq 3$, $\gcd(a, b) = 1$ et $|ab| \geq 2$; en particulier, ce résultat implique que la conjecture est vraie pour $k \geq \max(|a|, |b|)$. Ce chapitre est basé sur un papier par l'auteur [Tr4] publié sur *Integers*.

Abstract. We determine all triples (a, b, n) of positive integers such that a and b are relatively prime and n^k divides $a^n + b^n$ (respectively, $a^n - b^n$), when k is the maximum of a and b (in fact, we answer a slightly more general question). As a by-product, it is found that, for $m, n \in \mathbb{N}^+$ with

$n \geq 2$, n^m divides $m^n + 1$ if and only if $(m, n) = (2, 3)$ or $(1, 2)$, which generalizes problems from the 1990 and 1999 editions of the International Mathematical Olympiad. The results are related to a conjecture by K. Győry and C. Smyth on the finiteness of the sets $R_k^{\pm}(a, b) := \{n \in \mathbb{N}^+ : n^k \mid a^n \pm b^n\}$, where a, b, k are fixed integers with $k \geq 3$, $\gcd(a, b) = 1$ and $|ab| \geq 2$; in particular, we find that the conjecture is true for $k \geq \max(|a|, |b|)$. The chapter is based on a paper by the author [Tr4] published in *Integers*.

4.1 Introduction

It is a problem from the 1990 edition of the International Mathematical Olympiad (shortly, IMO) to find all integers $n \geq 2$ such that $n^2 \mid 2^n + 1$. This is reported as Problem 7.1.15 (p. 147) in [AA], together with a solution by the authors (p. 323), which shows that the only possible n is 3. On another hand, Problem 4 in the 1999 IMO asks for all pairs (n, p) of positive integers such that p is a (positive rational) prime, $n \leq 2p$ and $n^{p-1} \mid (p-1)^n + 1$. This is Problem 5.1.3 (p. 105) in the same book as above, whose solution by the authors (p. 105) is concluded with the remark that "With a little bit more work, we can even erase the condition $n \leq 2p$." Specifically, it is found that the required pairs are $(1, p)$, $(2, 2)$ and $(3, 3)$, where p is an arbitrary prime. (For notation and terminology herein used without definition, as well as for material concerning classical topics in number theory, the reader should refer to [HW].)

It is now fairly natural to ask whether similar conclusions can be drawn in relation to the more general problem of determining all pairs (m, n) of positive integers for which $n^m \mid m^n + 1$. In fact, the question is answered in the positive, and even in a stronger form, by Theorem 4.1 below, where the following observations are taken into account to rule out from the analysis a few trivial cases: Given $a, b \in \mathbb{Z}$ and $n, k \in \mathbb{N}^+$, we have that $1^k \mid a^n \pm b^n$ and $n^k \mid a^n - a^n$. Furthermore, $n^k \mid a^n \pm b^n$ if and only if $n^k \mid b^n \pm a^n$, and also if and only if $n^k \mid (-a)^n \pm (-b)^n$. Finally, $n^k \mid a^n + (-a)^n$ for n odd and $n^k \mid a^n - (-a)^n$ for n even.

Theorem 4.1. *Let a, b, n be integers such that $n \geq 2$, $a \geq \max(1, |b|)$ and $b \geq 0$ for n even, and set $\delta := \gcd(a, b)$, $\alpha := \delta^{-1}a$ and $\beta := \delta^{-1}b$.*

(i) *Assume that $\beta \neq -\alpha$ when n is odd. Then, $n^\alpha \mid a^n + b^n$ and $n^\alpha \mid a^n + \beta^n$ if and only if $(a, b, n) = (2, 1, 3)$ or $(2^c, 2^c, 2)$ for $c \in \{0, 1, 2\}$.*

(ii) *Assume* $\beta \neq a$. *Then,* $n^a \mid a^n - b^n$ *and* $n^a \mid a^n - \beta^n$ *if and only if* $(a, b, n) = (3, 1, 2)$ *or* $(2, -1, 3)$.

The theorem will be proved in Section 4.2. In fact, our proof is just the result of a meticulous refinement of the solutions already known for the IMO problems mentioned in the preamble. Thus, our only possible merit, if any at all, has been that of bringing into focus a clearer picture of (some of) their essential features.

Some comments are in order before proceeding. First, it would be interesting to extend Theorem 4.1, possibly at the expense of some extra solutions, by removing the assumption that $n^a \mid (a^n + \beta^n)$ or $n^a \mid (a^n - \beta^n)$ (the notation is the same as in the statement of the result), but at present we do not have great ideas for this. Secondly, three out of the six triples obtained by the present formulation of the theorem come from the identity $2^3 + 1^3 = 3^2$. Lastly, the result yields a solution of the problems which have originally stimulated this work, as we have the following corollary (of which we omit the obvious proof):

Corollary 4.2. *Let* $m, n \in \mathbb{N}^+$. *Then* $n^m \mid m^n + 1$ *if and only if either* $(m, n) = (2, 3)$, $(m, n) = (1, 2)$, *or* $n = 1$ *and* m *is arbitrary.*

We will make use at some point of the following lemma, which belongs to the folklore and is typically attributed to É. Lucas [Lu] and R. D. Carmichael [Car] (the latter having fixed an error in Lucas' original work in the 2-adic case).

Lemma 4.3 (Lifting-the-exponent lemma)**.** *For all* $x, y \in \mathbb{Z}$, $\ell \in \mathbb{N}^+$ *and* $p \in \mathbb{P}$ *such that* $p \nmid xy$ *and* $p \mid x - y$, *the following conditions are satisfied:*

(i) *If* $p \geq 3$, ℓ *is odd, or* $4 \mid x - y$, *then* $e_p(x^\ell - y^\ell) = e_p(x - y) + e_p(\ell)$.

(ii) *If* $p = 2$, ℓ *is even and* $e_2(x - y) = 1$, *then* $e_2(x^\ell - y^\ell) = e_2(x + y) + e_2(\ell)$.

The study of the congruences $a^n \pm b^n \equiv 0 \bmod n^k$ has a very long history, dating back at least to Euler, who proved that, for all relatively prime integers a, b with $a > b \geq 1$, every primitive prime divisor of $a^n - b^n$ is congruent to 1 modulo n; see [BV, Theorem I] for a proof (a prime divisor p of $a^n - b^n$ is said to be primitive if there does not exist any $k \in \mathbb{N}^+$ with $k < n$ such that $p \nmid a^k - b^k$). However, since there are so many results related to the question, instead of trying to

summarize them here, we just refer the interested reader to the paper [GS], whose authors provide an account of the existing literature on the topic and characterize, for $a, b \in \mathbb{Z}$ and $k \in \mathbb{N}^+$, the set $R_k^+(a,b)$, respectively $R_k^-(a,b)$, of all positive integers n such that n^k divides $a^n + b^n$, respectively $a^n - b^n$ (note that no assumption is made about the coprimality of a and b), while addressing the problem of finding the exceptional cases when $R_1^-(a,b)$ and $R_2^-(a,b)$ are finite; see, in particular, [GS, Theorems 1–2 and 18]. Nevertheless, the related question of determining, given $a, b \in \mathbb{Z}$ with $\gcd(a,b) = 1$, all positive integers n such that n^k divides $a^n + b^n$ (respectively, $a^n - b^n$), when k is the maximum of $|a|$ and $|b|$, does not appear to be considered neither in [GS] nor in the references therein.

On another hand, it is suggested in [GS] that $R_k^+(a,b)$ and $R_k^-(a,b)$ are both finite provided that a, b, k are fixed integers with $k \geq 3$, $\gcd(a,b) = 1$ and $|ab| \geq 2$ (the authors point out that the question is probably a difficult one, even assuming the ABC conjecture). Although far from being an answer to this, Theorem 4.1 below implies that, under the same assumptions as above, $R_k^+(a,b)$ and $R_k^-(a,b)$ are finite for $k \geq \max(|a|, |b|)$.

4.2 Proofs

First, for the sake of exposition, we give a couple of lemmas.

Lemma 4.4. *Let $x, y, z \in \mathbb{Z}$ and $\ell \in \mathbb{N}^+$ such that $\gcd(x,y) = 1$ and $z \mid x^\ell + y^\ell$. Then xy and z are relatively prime, $q \nmid x^\ell - y^\ell$ for every integer $q \geq 3$ for which $q \mid z$, and $4 \nmid z$ provided that ℓ is even. Moreover, if there exists an odd prime divisor p of z and ℓ such that $\gcd(\ell, p-1) = 1$, then $p \mid x + y$, ℓ is odd and $e_p(z) \leq e_p(x+y) + e_p(\ell)$.*

Proof. The first part is routine (we omit the details). As for the second, let p be an odd prime dividing both z and ℓ with $\gcd(\ell, p-1) = 1$. Also, considering that z and xy are relatively prime (by the above), denote by y^{-1} an inverse of y modulo p and by ω the order of xy^{-1} modulo p, viz the smallest $k \in \mathbb{N}^+$ such that $(xy^{-1})^k \equiv 1 \bmod p$; cf. [HW, Section 6.8]. Since $(xy^{-1})^{2\ell} \equiv 1 \bmod p$, we have $\omega \mid 2\ell$. It follows from Fermat's little theorem and [HW, Theorem 88] that ω divides $\gcd(2\ell, p-1)$, whence we get $\omega \mid 2$, using that $\gcd(\ell, p-1) = 1$. This in turn implies that $p \mid x^2 - y^2$, and hence either $p \mid x - y$ or $p \mid x + y$. But $p \mid x - y$ would give that $p \mid x^\ell - y^\ell$, which is impossible by the first part of the claim (since $p \geq 3$). So $p \mid x + y$, with the result that

ℓ is odd: For, if $2 \mid \ell$, then $p \mid 2x^\ell$ (because $p \mid z \mid x^\ell + y^\ell$ and $y \equiv -x \bmod p$), which would lead to $\gcd(x, y) \geq p$ (again, using that p is odd), viz to a contradiction. The rest is an immediate application of Lemma 4.3. □

Lemma 4.5. *Let $x, y, z \in \mathbb{Z}$ such that x, y are odd and $x, y \geq 0$. Then $x^2 - y^2 = 2^z$ if and only if $z \geq 3$, $x = 2^{z-2} + 1$ and $y = 2^{z-2} - 1$.*

Proof. Since x and y are odd, $x^2 - y^2$ is divisible by 8, namely $z \geq 3$, and there exist $i, j \in \mathbb{N}^+$ such that $i + j = z$, $x - y = 2^i$ and $x + y = 2^j$. It follows that $x = 2^{j-1} + 2^{i-1}$ and $y = 2^{j-1} - 2^{i-1}$, and then $j > i$ and $i = 1$ (otherwise x and y would be even). The rest is straightforward. □

Now, we are ready to write down the proof of the main result.

Proof of Theorem 4.1. (i) Assume that $n^a \mid a^n + b^n$, $n^a \mid a^n + \beta^n$, and $\beta \neq -a$ when n is odd. Since a and β are coprime (by construction), it holds that $\beta \neq 0$, for otherwise $n \mid a^n + \beta^n$ and $n \geq 2$ would give $\gcd(a, \beta) \geq 2$. Also, $a = |\beta|$ if and only if $a = \beta = 1$ and $n = 2$ (as $\beta \geq 0$ for n even), and thus 2^δ divides $2\delta^2$, which is possible if and only if $\delta \in \{1, 2, 4\}$ and gives $(a, b, n) = (1, 1, 2)$, $(2, 2, 2)$, or $(4, 4, 2)$. So, we are left with the case when

$$a \geq 2 \quad \text{and} \quad a > |\beta| \geq 1, \tag{4.1}$$

since $a \geq \max(1, |\beta|)$. Considering that $4 \mid n^2$ for n even, it follows from Lemma 4.4 that n is odd and $\gcd(a\beta, n) = 1$. Denote by p the smallest prime divisor of n. Again by Lemma 4.4, it is then found that p divides $a + \beta$ and

$$a - 1 \leq (a - 1) \cdot e_p(n) \leq e_p(a + \beta). \tag{4.2}$$

Furthermore, $a + \beta \geq 1$ by equation (4.1), whence

$$a + \beta = p^r s, \quad \text{with } r, s \in \mathbb{N}^+ \text{ and } p \nmid s. \tag{4.3}$$

Therefore, equations (4.1) and (4.3) yield that $2a \geq p^r s + 1$. This implies by equation (4.2), since $r = e_p(a + \beta)$, that $3^r s \leq p^r s \leq 2r + 1$, which is possible only if $p = 3$ and $r = s = 1$. Thus, by

equations (4.2) and (4.3), we get $\alpha + \beta = 3$ and $\alpha = 2$, namely $(\alpha, \beta) = (2, 1)$. Also, $e_3(n) = 1$, and hence $n = 3t$ for some $t \in \mathbb{N}^+$ with $\gcd(6, t) = 1$. It follows that $t^2 \mid \gamma^t + 1$ for $\gamma = 2^3$.

So suppose, for the sake of contradiction, that $t \geq 2$ and let q be the least prime divisor of t. Then, another application of Lemma 4.4 gives $2e_q(t) \leq e_q(\gamma + 1) + e_q(t)$, and accordingly $1 \leq e_q(t) \leq e_q(\gamma + 1) = e_q(3^2)$, which is however absurd, due to the fact that $\gcd(3, t) = 1$. Hence $t = 1$, i.e. $n = 3$, and putting everything together completes the proof, because $2^3 + 1^3 = 3^2$ and $3^{2\delta} \mid \delta^2 \cdot (2^3 + 1^3)$ only if $\delta = 1$.

(ii) Assume that $n^a \mid a^n - b^n$, $n^a \mid \alpha^n - \beta^n$, and $\beta \neq \alpha$. Since $\gcd(\alpha, \beta) = 1$, we get as in the proof of point (i) that $\beta \neq 0$, while $\alpha = |\beta|$ only if $\alpha = 1$, $\beta = -1$, and n is odd (again, $\beta \geq 0$ for n even), which is however impossible, because it would give that $n \mid 2$ with $n \geq 3$. So, we can suppose from now on that α and β satisfy the same conditions as in equation (4.1), and write n as $2^r s$, where $r \in \mathbb{N}$, $s \in \mathbb{N}^+$ and $\gcd(2, s) = 1$. We have the following:

Case 1: $r = 0$, i.e. $n = s$. Then, n is odd, so that $n^a \mid a^n + (-b)^n$ and $n^a \mid \alpha^n + (-\beta)^n$, so by point (i) we get $(a, b, n) = (2, -1, 3)$.

Case 2: $r \geq 1$. Since n is even and $\gcd(\alpha, \beta) = 1$, both α and β are odd, that is $8 \mid \alpha^2 - \beta^2$. It follows from point (i) of Lemma 4.3 that

$$e_2(\alpha^n - \beta^n) = e_2(\alpha^2 - \beta^2) + e_2(2^{r-1}s) = e_2(\alpha^2 - \beta^2) + r - 1. \tag{4.4}$$

(With the same notation as in its statement, we apply Lemma 4.3 with $x = \alpha^2$, $y = \beta^2$, $\ell = 2^{r-1}s$, and $p = 2$.) Also, $2^{r\alpha} \mid \alpha^n - \beta^n$, so equation (4.4) yields

$$(\alpha - 1) \cdot r \leq e_2(\alpha^2 - \beta^2) - 1. \tag{4.5}$$

There now exist $u, v \in \mathbb{N}^+$ with $u \geq 2$ and $\gcd(2, v) = 1$ such that $\alpha^2 - \beta^2 = 2^{u+1}v$, with the result that $\alpha > 2^{u/2}\sqrt{v}$. Hence, taking also into account that $2^x \geq x + 1$ for every $x \in \mathbb{R}$ with $x \geq 1$, we get by equation (4.5) that

$$\left(\frac{u}{2} + 1\right)\sqrt{v} \leq 2^{u/2}\sqrt{v} < \frac{u}{r} + 1, \tag{4.6}$$

which is possible only if $r = 1$ and $\sqrt{v} < 2$. Then $2^{u/2}\sqrt{v} < u + 1$, in such a way that

$2 \leq u \leq 5$ and $v = 1$ (using that v is odd). In consequence of Lemma 4.5, all of this implies, at the end of the day, that $a = 2^z + 1$, $b = 2^z - 1$ and $n = 2s$ (recall that we want the conditions in equation (4.1) to be satisfied and $\beta \geq 0$ for n even), where z is an integer between 1 and 4. But we need $2^z \leq z + 1$ by equation (4.5), so necessarily $z = 1$, i.e. $a = 3$ and $\beta = 1$. Finally, we check that $(2s)^3 \mid 3^{2s} - 1^{2s}$ if and only if $s = 1$: For, if $s \geq 2$ and q is the smallest prime divisor of s, then $0 < 3e_q(s) \leq e_q(3^2 - 1)$ by Lemma 4.4, which is absurd since $\gcd(2, s) = 1$. This gives $(a, b, n) = (3, 1, 2)$, while it is trivially seen that $2^{3\delta} \mid \delta^2 \cdot (3^2 - 1^2)$ if and only if $\delta = 1$.

Putting all the pieces together, the proof is thus complete. □

References

[AA] T. Andreescu and D. Andrica, *Number Theory - Structures, Examples, and Problems* (Birkhäuser, 2009, 1st ed.).

[BV] G. D. Birkhoff and H. S. Vandiver, *On the Integral Divisors of $a^n - b^n$*, Ann. of Math. (4) **5** (Jul., 1904), 173–180.

[Car] R. D. Carmichael, *On the Numerical Factors of Certain Arithmetic Forms*, Amer. Math. Monthly (10) **16** (1909), 153–159.

[GS] K. Győry and C. Smyth, *The divisibility of $a^n - b^n$ by powers of n*, Integers (3) **10** (Jul., 2010), 319–334.

[HW] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Oxford University Press, 2008, 6th ed., revised by D. R. Heath-Brown and J. H. Silverman).

[Lu] É. Lucas, *Théorie des Fonctions Numériques Simplement Periodiques*, Amer. J. Math. **1** (1878), 184–196, 197-240, 289–321.

[Tr4] S. Tringali, *On the divisibility of $a^n \pm b^n$ by powers of n,* Integers, Vol. 13, No. A071 (Nov. 2013).

This page intentionally left blank

This page intentionally left blank

Ithaca has given you the beautiful voyage.
Without her you would not have set out on the road.
Nothing more does she have to give you.

— Konstantinos Petrou Kavafis, *Ithaca*

5

On a system of equations with primes

Resumé. Étant donné un entier $n \geq 3$, soient $u_1, \dots, u_n$ des entiers premiers entre eux deux à deux pour lesquels $2 \leq u_1 < \cdots < u_n$, soit $\mathcal{D}$ une famille de sous-ensembles propres et non vides de $\{1, \dots, n\}$ qui contient un nombre "suffisant" d'éléments, et soit ε une fonction $\mathcal{D} \to \{\pm 1\}$. Existe-t-il au moins un nombre premier q tel que q divise $\prod_{i \in I} u_i - \varepsilon(I)$ pour un certain $I \in \mathcal{D}$, mais ne divise pas $u_1 \cdots u_n$? Nous donnons une réponse positive à cette question dans le cas où les u_i sont des puissances de nombres premiers si on impose certaines restrictions sur ε et $\mathcal{D}$. Nous utilisons ce résultat pour prouver que, si $\varepsilon_0 \in \{\pm 1\}$ et si A est un ensemble de trois ou plus nombres premiers qui contient les diviseurs premiers de tous les nombres de la forme $\prod_{p \in B} p - \varepsilon_0$ pour lesquels B est un sous-ensemble propre, fini et non vide de A, alors A contient tous les nombres premiers. Ce chapitre est basé sur un article par Paolo Leonetti et l'auteur [Tr5] accepté pour publication au *Journal de Théorie des Nombres de Bordeaux*.

Abstract. Given an integer $n \geq 3$, let $u_1, \dots, u_n$ be pairwise coprime integers for which $2 \leq u_1 < \cdots < u_n$, and let $\mathcal{D}$ be a family of nonempty proper subsets of $\{1, \dots, n\}$ with "enough" elements and ε a map $\mathcal{D} \to \{\pm 1\}$. Does there exist at least one prime q such that q divides $\prod_{i \in I} u_i - \varepsilon(I)$ for some $I \in \mathcal{D}$, but it does not divide $u_1 \cdots u_n$? We answer this question in the positive in the case where the integers u_i are prime powers and some restrictions hold on ε and $\mathcal{D}$. We use the result to prove that, if $\varepsilon_0 \in \{\pm 1\}$ and A is a set of three or more primes that contains all prime divisors of any number of the form $\prod_{p \in B} p - \varepsilon_0$ for which B is a finite nonempty proper subset of A, then A contains all the primes. The chapter is based on a paper by the author [Tr5] (joint work with Paolo Leonetti) accepted for publication on *Journal de Théorie des Nombres de Bordeaux*.

5.1 Introduction

There are several proofs of the fact that $\mathbb{P}$ is infinite: Some are elementary, others come as a byproduct of deeper results. E.g., six of them, including Euclid's classical proof, are given by M. Aigner and G. M. Ziegler in the first chapter of their lovely *Proofs from THE BOOK* [AZ]. Although not really focused on the infinity of primes, this chapter is inspired by Euclid's original work on the subject, concerned as it is with the factorization of numbers of the form $a_1 \cdots a_n \pm 1$, where $a_1, \dots, a_n$ are coprime positive integers, and in fact prime powers (we do not consider 1 as a prime power).

To be more specific, we need first some notation. Given a set A, we denote by $\mathcal{P}_\star(A)$ the family of all finite nonempty *proper* subsets of A, in such a way that $A \notin \mathcal{P}_\star(A)$. Furthermore, for an integer $n \geq 1$ we set $S_n := \{1, \dots, n\}$ and let $\mathcal{P}_n(A)$ be the collection of all subsets B of A with $|B| = n$. For more notation and terminology used here without explanation, as well as for material concerning classical topics in number theory, the reader should refer to [HW]. With this in mind, we can state the basic question addressed below:

Question 5.1. *Given an integer $n \geq 3$, pick exponents $v_1, \dots, v_n \in \mathbb{N}^+$ and primes $p_1, \dots, p_n \in \mathbb{P}$ such that $p_1 < \cdots < p_n$, and let $\mathcal{D}$ be a nonempty subfamily of $\mathcal{P}_\star(S_n)$ with "enough" elements and ε a map $\mathcal{D} \to \{\pm 1\}$. Does there exist at least one prime $q \in \mathbb{P} \setminus \{p_1, \dots, p_n\}$ such that q divides $\prod_{i \in I} p_i^{v_i} - \varepsilon(I)$ for some $I \in \mathcal{D}$?*

At present, we have no formal definition of what should be meant by the word "enough" in the

previous statement: this is part of the question. With the notation from above it is rather clear, for instance, that the answer to Question 5.1 is no, at least in general, if $|\mathcal{D}|$ is "small" with respect to n, as shown by the following:

Example 5.2. Given an integer $k \geq 3$, (pairwise) distinct primes $q_1, \dots, q_k$ and positive integers $e_1, \dots, e_k$, let q be the greatest prime dividing at least one of the numbers of the form $\prod_{i \in I} q_i^{e_i} \pm 1$ for $I \in \mathcal{P}_\star(S_k)$. Then, we get a negative answer to Question 5.1 by extending $q_1, \dots, q_k$ to a sequence $q_1, \dots, q_\ell$ containing all the primes $\leq q$ (note that $\ell \geq k+1$), by taking a nonempty $\mathcal{E} \subseteq \mathcal{P}_\star(S_k)$ and arbitrary $e_{k+1}, \dots, e_\ell \in \mathbb{N}^+$, and by setting $n := \ell$, $p_i := q_i$, $v_i := e_i$ and $\mathcal{D} := \mathcal{E}$.

Thus, to rule out such trivial cases, one shall suppose, e.g., that $|\mathcal{D}| \geq n\kappa$ or, in alternative, $|\mathcal{D}| \geq n^\kappa$ for some absolute constant $\kappa > 0$.

That said, we concentrate here on the case where $\mathcal{D}$ contains at least all subsets of S_n of size 1, $n-2$, or $n-1$, and the function ε is constant when restricted to these (see Theorem 5.5 below), while collecting a series of intermediate results that could be useful, in future research, to try to draw broader conclusions. In particular, Question 5.1 can be naturally "generalized" as follows:

Question 5.3. *Given an integer $n \geq 3$ and pairwise relatively prime integers $u_1, \dots, u_n$ such that $2 \leq u_1 < \cdots < u_n$, let $\mathcal{D}$ be a nonempty subcollection of $\mathcal{P}_\star(S_n)$ for which $\mathcal{D}$ has "enough" elements and ε a function $\mathcal{D} \to \{\pm 1\}$. Does there exist at least one $q \in \mathbb{P}$ such that q divides $\prod_{i \in I} u_i - \varepsilon(I)$ for some $I \in \mathcal{D}$ and $q \nmid u_1 \cdots u_n$?*

Note that Question 5.3 is not really a generalization of Question 5.1, in the sense that the former can be stated in the terms of the latter by replacing, with the same notation as above, n with the total number d of the prime divisors of $u_1 \cdots u_n$ and $\mathcal{D}$ with a suitable subfamily of $\mathcal{P}_\star(S_d)$.

Questions 5.1 and 5.3 are somewhat reminiscent of cyclic systems of simultaneous congruences, studied by several authors, and still in recent years, for their connection with some long-standing questions in the theory of numbers, and especially Znám's problem and the Agoh-Giuga conjecture (see [BV] and [La], respectively, and references therein). Our initial motivation has been, however, of a completely different sort, and in fact related to the following:

Question 5.4. *Let A be a subset of $\mathbb{P}$, having at least three elements, and such that for any $B \in \mathcal{P}_\star(A)$ all prime divisors of $\prod_{p \in B} p - 1$ belong to A. Then $A = \mathbb{P}$.*

This served as a problem in the 4th grade of the 2003 Romanian IMO Team Selection Test, and it appears (up to minor notational differences) as Problem 10 in [BAB, p. 53]. The solution provided in the book (p. 62) consists of two parts. In the first one, the authors aim to show that A is infinite, but their argument is seen to be at least incomplete. Specifically, they argue as follows (we use the notation from above): After having proved that 2 is in A, they suppose by contradiction that A is a finite set of size k (where $k \geq 3$) and let $p_1, \ldots, p_k$ be a numbering of A such that $2 = p_1 < \cdots < p_k$. Then, they derive from the standing assumptions on A that

$$p_2^a + 1 = 2^{\beta+1} p_2^\gamma + 2$$

for some $a, \beta, \gamma \in \mathbb{N}$. But this does not imply $1 \equiv 2 \bmod p_2$ (as is stated in the book) unless $\gamma \neq 0$, which is nowhere proved and has no obvious reason to hold.

The problem *per se* is not, however, difficult, and it was used also for the 2004 France IMO Team Selection Test (we are not aware of any official solution published by the organizers of the competition).

Questions somewhat similar to those above have been considered by other authors, even though under different assumptions, and mostly focused on the properties of the prime factorization of very particular numerical sequences $a_0, a_1, \ldots$ recursively defined, e.g., by formulas of the form $a_{n+1} = 1 + a_0 \cdots a_n$; see [Na, Section 1.1.2] and the references therein for an account (for all practical purposes, we report that one of the questions raised by A. A. Mullin in [Mu] and mentioned by W. Narkiewicz on page 2 of his book has been recently answered by [Bo]).

Now, we have not been able to work out a complete solution of Question 5.1, whatever this may be. Instead, we solve it in some special cases. In fact, our main result here is as follows:

Theorem 5.5. *Given an integer $n \geq 3$, pick distinct primes $p_1, \ldots, p_n$, exponents $v_1, \ldots, v_n \in \mathbb{N}^+$ and a subcollection $\mathcal{D}$ of $\mathcal{P}_\star(S_n)$ such that*

$$\mathcal{D}_0 \subseteq \mathcal{D}, \quad \text{with } \mathcal{D}_0 := \mathcal{P}_1(S_n) \cup \mathcal{P}_{n-2}(S_n) \cup \mathcal{P}_{n-1}(S_n).$$

Then, for every function $\varepsilon : \mathcal{D} \to \{\pm 1\}$ such that the restriction of ε to $\mathcal{D}_0$ is constant, there exists at least one $q \in \mathbb{P} \setminus \{p_1, \ldots, p_n\}$ such that q divides $\prod_{i \in I} p_i^{v_i} - \varepsilon(I)$ for some $I \in \mathcal{D}$.

The proof of Theorem 5.5, as presented in Section 5.3, requires a number of preliminary lemmas,

which are stated and proved under assumptions much weaker than those in the above statement. In particular, we will make use at some point of the following (well-known) result [Zs]:

Theorem 5.6 (Zsigmondy's theorem). *Pick $a, b \in \mathbb{N}^+$ and an integer $n \geq 2$ such that (i) $a > b$ and (ii) neither $(a, b, n) = (2, 1, 6)$ nor $a + b$ is a power of 2 and $n = 2$. Then, there exists $p \in \mathbb{P}$ such that $p \mid a^n - b^n$ and $p \nmid a^k - b^k$ for each positive integer $k < n$.*

Theorem 5.5 can be used to solve a generalization of Question 5.4. Specifically, we say that a set A of integers is *fine* if either A is finite or for every $p \in \mathbb{P}$ there exist infinitely many $a \in A$ such that $p \nmid a$. On the other hand, for $B, C \subseteq \mathbb{Z}$ we write $B \perp C$ if for every $b \in B$ there exists $c \in C$ such that $b \mid c$; this simplifies to $b \perp C$ when $B = \{b\}$. Clearly, $B \perp C$ if and only if $b \perp C$ for all $b \in B$. Based on these premises, we then prove the following:

Theorem 5.7. *Pick $\varepsilon_0 \in \{\pm 1\}$ and let A be a fine set of prime powers with the property that $|A| \geq 3$ and $q \perp A$ whenever q is a prime dividing $\prod_{a \in B} a - \varepsilon_0$ for some $B \in \mathcal{P}_\star(A)$. Then $|A| = \infty$, and in particular $A = \mathbb{P}$ if $A \subseteq \mathbb{P}$ and $\mathbb{P} \perp A$ if $\varepsilon_0 = 1$.*

Theorem 5.7 is proved in Section 5.4. With the notation from above, the assumption that A is fine is somehow necessary, as we show in Example 5.19. Incidentally, the result gives a solution of Question 5.4 in the special case where $\varepsilon_0 = 1$ and $A \subseteq \mathbb{P}$, while providing another proof, although overcomplicated, of the infinitude of primes. One related question is as follows:

Question 5.8. *Pick $n \in \mathbb{N}^+$ and distinct primes $q_1, \ldots, q_n$. Does there always exist a nonempty set of prime powers, say A, such that $\mathbb{P} \setminus \{q_1, \ldots, q_n\}$ is precisely the set of all prime divisors of the numbers $\prod_{a \in B} a + 1$ for which B is a finite nonempty subset of A?*

This is completely open to us. An easier question is answered in Example 5.20.

5.2 Preparations

Here below, we fix some more notation and prove a few preliminary lemmas related to the original version of Question 5.1 (that is, not only to the special cases covered by Theorem 5.5). For any purpose it may serve, we recall that, in our notation, $0 \in \mathbb{N}$ and $\emptyset, S_n \notin \mathcal{P}_\star(S_n)$.

In the remainder of this section, we suppose that there exist an integer $n \geq 3$, a set $\mathfrak{P} = \{p_1, \ldots, p_n\}$ of n primes, integral exponents $v_1, \ldots, v_n \in \mathbb{N}^+$, a nonempty subfamily $\mathcal{D}$ of $\mathcal{P}_\star(S_n)$,

and a function $\varepsilon : \mathcal{D} \to \{\pm 1\}$ such that $p_1 < \cdots < p_n$ and $q \in \mathfrak{P}$ whenever $q \in \mathbb{P}$ and q divides $\prod_{i\in I} p_i^{v_i} - \varepsilon_I$ for some $I \in \mathcal{D}$, where $\varepsilon_I := \varepsilon(I)$ for economy of notation. Accordingly, we show that these assumptions lead to a contradiction if $\mathcal{D}$ contains some distinguished subsets of S_n and the restriction of ε to the subcollection of these sets, herein denoted by $\mathcal{D}_0$, is constant: This is especially the case when $\mathcal{D}_0 = \mathcal{P}_1(S_n) \cup \mathcal{P}_{n-2}(S_n) \cup \mathcal{P}_{n-1}(S_n)$.

We let $P := \prod_{i=1}^n p_i^{v_i}$ and $\mathcal{D}^{\mathrm{op}} := \{S_n \setminus I : I \in \mathcal{D}\}$, and then we define

$$P_I := \prod_{i\in I} p_i^{v_i} \quad \text{and} \quad P_{-I} := P_{S_n\setminus I}$$

for $I \in \mathcal{P}_\star(S_n)$ (note that $P = P_I \cdot P_{-I}$), and $\varepsilon_{-I} := \varepsilon_{S_n\setminus I}$ for $I \in \mathcal{D}^{\mathrm{op}}$. In particular, given $i \in S_n$ we write P_i in place of $P_{\{i\}}$ and P_{-i} for $P_{-\{i\}}$, but also ε_i instead of $\varepsilon_{\{i\}}$ and ε_{-i} for $\varepsilon_{-\{i\}}$ (whenever this makes sense). It then follows from our assumptions that there are maps $a_1, \ldots, a_n : \mathcal{D}^{\mathrm{op}} \to \mathbb{N}$ such that

$$\forall I \in \mathcal{D}^{\mathrm{op}} : P_{-I} = \varepsilon_{-I} + \prod_{i\in I} p_i^{a_{i,I}}, \tag{5.1}$$

where $a_{i,I} := a_i(I)$. In particular, if there exists $i \in S_n$ such that $\{i\} \in \mathcal{D}^{\mathrm{op}}$ then

$$P_{-i} = p_i^{a_i} + \varepsilon_{-i}, \quad \text{with} \quad a_i := a_{i,\{i\}} \in \mathbb{N}^+ \tag{5.2}$$

(of course, $a_i \geq 1$ since $P_{-i} - \varepsilon_{-i} \geq 2 \cdot 3 - 1$). This in turn implies that

$$\forall I_1, I_2 \in \mathcal{D}^{\mathrm{op}} : P = P_{I_1} \cdot \left(\varepsilon_{-I_1} + \prod_{i\in I_1} p_i^{a_{i,I_1}}\right) = P_{I_2} \cdot \left(\varepsilon_{-I_2} + \prod_{i\in I_2} p_i^{a_{i,I_2}}\right), \tag{5.3}$$

which specializes to

$$P = p_{i_1}^{v_{i_1}} \cdot \left(p_{i_1}^{a_{i_1}} + \varepsilon_{-i_1}\right) = p_{i_2}^{v_{i_2}} \cdot \left(p_{i_2}^{a_{i_2}} + \varepsilon_{-i_2}\right) \tag{5.4}$$

for all $i_1, i_2 \in S_n$ such that $\{i_1\}, \{i_2\} \in \mathcal{D}^{\mathrm{op}}$. We mention in this respect that, for any fixed integer $b \neq 0$ and any finite subset $\mathcal{S}$ of $\mathbb{P}$, the diophantine equation

$$A \cdot (a^{x_1} - a^{x_2}) = B \cdot (b^{y_1} - b^{y_2}) \tag{5.5}$$

has only finitely many solutions in *positive* integers $a, A, B, x_1, x_2, y_1, y_2$ for which a is a prime,

$\gcd(Aa, Bb) = 1$, $x_1 \neq x_2$ and all the prime factors of AB belong to $\mathcal{S}$; see [BL] and the references therein. It follows that our equation (5.4) has only finitely many possible scenarios for ε taking the constant value -1 in $\mathcal{D}$. However, the methods used in [BL] are not effective and, as far as we can tell, a list of all the solutions to equation (5.5) is not known, not even in the special case when $A = B = 1$ and $b = 2$. Furthermore, there doesn't seem to be any obvious way to adapt the proof of the main result in [BL] to cover all of the cases resulting from equation (5.4).

With this in mind, and based on (5.1), our main hypothesis can be now restated as

$$\text{“}q \text{ divides } P_{-I} - \varepsilon_{-I} \text{ for some } q \in \mathbb{P} \text{ and } I \in \mathcal{D}^{\text{op}} \text{ only if } q \in \mathfrak{P}\text{.”} \tag{5.6}$$

In addition, we can easily derive, using (5.3) and unique factorization, that

$$\text{“}q \text{ divides } \varepsilon_{-I} + \textstyle\prod_{i\in I} p_i^{a_{i,I}} \text{ for some } q \in \mathbb{P} \text{ and } I \in \mathcal{D}^{\text{op}} \text{ only if } q \in \mathfrak{P}\text{.”} \tag{5.7}$$

Both of (5.6) and (5.7) will be often referred to throughout the article. Lastly, we say that ε is *k-symmetric* for a certain $k \in \mathbb{N}^+$ if both of the following conditions hold:

$$\text{(i) } I \in \mathcal{D} \cap \mathcal{P}_k(S_n) \text{ only if } I \in \mathcal{D}^{\text{op}}; \quad \text{(ii) } \varepsilon_I = \varepsilon_{-I} \text{ for all } I \in \mathcal{D} \cap \mathcal{P}_k(S_n).$$

With all this in hand, we are finally ready to prove a few preliminary results that will be used later, in Section 5.3, to establish our main theorem.

5.2.1 Preliminaries

The material is intentionally organized into a list of lemmas, each one based on “local”, rather than “global”, hypotheses. This is motivated by the idea of highlighting which is used for which purpose, while looking for an approach to solve Question 5.1 in a broader generality. In particular, the first half of Theorem 5.5 (the one relating to the case $\varepsilon_0 = 1$) will follow as a corollary of Lemma 5.14 below, while the second needs more work.

In what follows, given $a \in \mathbb{Z}$ and $m \in \mathbb{N}^+$ such that $\gcd(a, m) = 1$, we denote by $\operatorname{ord}_m(a)$ the smallest $k \in \mathbb{N}^+$ such that $a^k \equiv 1 \bmod m$, namely the order of a in the group of units of $\mathbb{Z}/m\mathbb{Z}$.

Lemma 5.9. *If $p_i = 3$ for some $i \in S_n$ and there exists $j \in S_n \setminus \{i\}$ such that $\{j\} \in \mathcal{D}^{\text{op}}$, then one,*

and only one, of the following conditions holds:

1. $\varepsilon_{-j} = -1$ *and* a_j *is even.*
2. $\varepsilon_{-j} = -1$, a_j *is odd and* $p_j \equiv 1 \bmod 6$.
3. $\varepsilon_{-j} = 1$, a_j *is odd and* $p_j \equiv 2 \bmod 3$.

Proof. Under the assumptions of the claim, (5.4) gives that $3 \mid p_j^{a_j} + \varepsilon_{-j}$, which is possible only if one, and only one, of the desired conditions is satisfied. □

The next lemma, as trivial as it is, furnishes a sufficient condition under which $2 \in \mathfrak{P}$. Indeed, having a way to show that 2 and 3 are in $\mathfrak{P}$ looks like a key aspect of the problem in its full generality.

Lemma 5.10. *If there exists* $I \in \mathcal{D}$ *such that* $1 \notin I$ *then* $p_1 = 2$*; also,* $a_1 \geq 4$ *if, in addition to the other assumptions,* $I \in \mathcal{P}_{n-1}(S_n)$.

Proof. Clearly, p_i is odd for each $i \in I$, which means that $P_I - \varepsilon_I$ is even, and hence $p_1 = 2$ by (5.6) and the assumed ordering of the primes p_i. Thus, it follows from (5.2) that if $I \in \mathcal{P}_{n-1}$ then $2^{a_1} = P_{-1} - \varepsilon_{-1} \geq 3 \cdot 5 - 1$, to the effect that $a_1 \geq 4$. □

The following two lemmas prove that, in the case of a 1-symmetric ε, reasonable (and not-so-restrictive) assumptions imply that 3 belongs to $\mathfrak{P}$.

Lemma 5.11. *Suppose that* ε *is* 1*-symmetric and pick a prime* $q \notin \mathfrak{P}$*. Then, there doesn't exist any* $i \in S_n$ *such that* $\{i\} \in \mathcal{D}$ *and* $p_i \equiv 1 \bmod q$.

Proof. Assume by contradiction that there exists $i_0 \in S_n$ such that $\{i_0\} \in \mathcal{D}$ and $p_{i_0} \equiv 1 \bmod q$. Then, since ε is 1-symmetric, we get by (5.1) and (5.2) that

$$1 - \varepsilon_0 \equiv p_{i_0}^{v_{i_0}} - \varepsilon_0 \equiv \prod_{i \in I_0} p_i^{a_{i,I_0}} \bmod q \quad \text{and} \quad P_{I_0} \equiv p_{i_0}^{a_{i_0}} + \varepsilon_0 \equiv 1 + \varepsilon_0 \bmod q,$$

where $I_0 := S_n \setminus \{i_0\}$. But $q \notin \mathfrak{P}$ implies $q \nmid p_{i_0}^{v_{i_0}} - \varepsilon_0$ by (5.6), with the result that $\varepsilon_0 = -1$ (from the above), and then $q \mid P_{I_0}$. By unique factorization, this is however in contradiction to the fact that q is not in $\mathfrak{P}$. □

Lemma 5.12. *Suppose that ε is 1-symmetric and there exists $J \in \mathcal{P}_\star(S_n)$ such that $S_n \setminus J$ has an even number of elements, $\mathcal{D}_0 := \mathcal{P}_1(S_n) \cup \{S_n \setminus J\} \subseteq \mathcal{D}$, and the restriction of ε to $\mathcal{D}_0$ is constant. Then $p_2 = 3$ and $a_2 \geq \frac{1}{2}(5 - \varepsilon_0)$.*

Proof. Let ε take the constant value ε_0 when restricted to $\mathcal{D}_0$ and assume by contradiction that $3 \notin \mathfrak{P}$. Then, Lemma 5.11 entails that $p_i \equiv -1 \bmod 3$ for all $i \in S_n$, while taking $I = S_n \setminus \{i\}$ in (5.1) and working modulo 3 yield by (5.6) that

$$p_i^{v_i} - \varepsilon_0 \equiv \prod_{j \in I} p_j^{a_{j,I}} \not\equiv 0 \bmod 3,$$

to the effect that v_i is odd if $\varepsilon_0 = 1$ and even otherwise (here, we are using that $\mathcal{P}_1(S_n) \in \mathcal{D}$ and ε is 1-symmetric, in such a way that $\mathcal{P}_{n-1}(S_n) \in \mathcal{D}$ too). Now, since $S_n \setminus J \in \mathcal{D}$, the very same kind of reasoning also implies that

$$1 - \varepsilon_0 \equiv P_{-J} - \varepsilon_0 \equiv \prod_{j \in J} p_j^{a_{j,J}} \bmod 3,$$

with the result that if $\varepsilon_0 = 1$ then $3 \in \mathfrak{P}$ by (5.6), as follows from the fact that $S_n \setminus J$ has an even number of elements and v_i is odd for each $i \in J$ (which was proved before). This is however a contradiction.

Thus, we are left with the case $\varepsilon_0 = -1$. Since -1 is not a quadratic residue modulo a prime $p \equiv -1 \bmod 4$, we get by the above and (5.2) that $p_i \equiv 1 \bmod 4$ for each $i = 2, 3, \ldots, n$. Then, (5.1) gives, together with Lemma 5.10, that $P_{-1} + 1 = 2^{a_1}$ with $a_1 \geq 2$, which is again a contradiction as it means that $2 \equiv 0 \bmod 4$. The whole proves that $p_2 = 3$, which implies from (5.2) that $3^{a_2} = P_{-2} - \varepsilon_{-2} \geq 2 \cdot 5 - \varepsilon_0$, and hence $a_2 \geq \frac{1}{2}(5 - \varepsilon_0)$. □

Now, we show that, if $\mathcal{D}$ contains at least some distinguished subsets of S_n and $\varepsilon_{\pm i} = 1$ for some admissible $i \in S_n \setminus \{1\}$, then p_i has to be a Fermat prime.

Lemma 5.13. *Assume $\mathcal{P}_1(S_n \setminus \{1\}) \subseteq \mathcal{D}^{\mathrm{op}}$ and suppose there exists $i \in S_n \setminus \{1\}$ for which $\{i\} \in \mathcal{D}$ and $\varepsilon_{\pm i} = 1$. Then, p_i is a Fermat prime.*

Proof. It is clear from Lemma 5.10 that $p_1 = 2$. Suppose by contradiction that there exists an odd prime q such that $q \mid p_i - 1$ (note that $p_i \geq 3$), and hence $q \mid p_i^{v_i} - \varepsilon_i$. Then, taking $I = \{i\}$ in

(5.6) gives that $q = p_j$ for some $j \in S_n \setminus \{1, i\}$. Considering that $\mathcal{P}_1(S_n \setminus \{1\}) \subseteq \mathcal{D}^{\mathrm{op}}$, it follows from (5.4) that

$$p_j^{v_j}(p_j^{a_j} + \varepsilon_{-j}) = p_i^{v_i}(p_i^{a_i} + 1),$$

where we use that $\varepsilon_{-i} = 1$. This is however a contradiction, because it implies that $0 \equiv 2 \bmod p_j$ (with $p_j \geq 3$). So, p_i is a Fermat prime by [HW, Theorem 17]. □

Lemma 5.14. *Suppose that $p_i = 3$ for some $i \in S_n$, $\mathcal{P}_1(S_n) \subseteq \mathcal{D}^{\mathrm{op}}$, and there exists $j \in S_n \setminus \{1, i\}$ such that $\{j\} \in \mathcal{D}$ and $\varepsilon_{\pm j} = 1$. Then $i = 2$, $p_1 = 2$, and $\varepsilon_{-1} = -1$.*

Proof. First, we have by Lemma 5.10 that $p_1 = 2$, and hence $i = 2$. Also, p_j is a Fermat prime by Lemma 5.13 (and clearly $p_j \geq 5$). So suppose by contradiction that $\varepsilon_{-1} = 1$. Then, Lemma 5.9 and (5.2) imply that $p_j \mid P_{-1} = 2^{a_1} + 1$ with a_1 odd, to the effect that $2 \leq \mathrm{ord}_{p_j}(2) \leq \gcd(2a, p_j - 1) = 2$. It follows that $5 \leq p_j \leq 2^2 - 1$, which is obviously impossible. □

The proof of the next lemma depends on Zsigmondy's theorem. Although not strictly related to the statement and the assumptions of Theorem 5.5, it will be of crucial importance later on.

Lemma 5.15. *Pick $p, q \in \mathbb{P}$ and assume that there exist $x, y, z \in \mathbb{N}$ for which $x \neq 0$, $y \geq 2$, $p \mid q+1$ and $q^x - 1 = p^y(q^z - 1)$. Then $x = 2$, $z = 1$, $p = 2$, $y \in \mathbb{P}$, and $q = 2^y - 1$.*

Proof. Since $x \neq 0$, it is clear that $q^x - 1 \neq 0$, with the result that $z \neq 0$ and $q^z - 1 \neq 0$ too. Therefore, using also that $y \neq 0$, one has that

$$p^y = (q^x - 1)/(q^z - 1) > 1, \tag{5.8}$$

which is obviously possible only if

$$x > z \geq 1. \tag{5.9}$$

We claim that $x \leq 2$. For suppose to the contrary that $x > 2$. Then by Zsigmondy's theorem, there must exist at least one $r \in \mathbb{P}$ such that $r \mid q^x - 1$ and

$$r \nmid q^k - 1 \text{ for each positive integer } k < x.$$

In particular, (5.8) yields that $r = p$ (by unique factorization), which is a contradiction since $p \mid$

$q^2 - 1$. Thus, we get from (5.9) that $x = 2$ and $z = 1$. Then, $p^y = q + 1$, that is $p^y - 1 \in \mathbb{P}$, and this is absurd unless $p = 2$ and $y \in \mathbb{P}$. The claim follows. □

This completes the series of our preliminary lemmas; we can now proceed to the proof of the main result.

5.3 Proof of Theorem 5.5

Throughout we use the same notation and assumptions as in Section 5.2, but we specialize to the case where

$$\mathcal{D}_0 := \mathcal{P}_1(S_n) \cup \mathcal{P}_{n-2}(S_n) \cup \mathcal{P}_{n-1}(S_n) \subseteq \mathcal{D}$$

and ε takes the constant value ε_0 when restricted to $\mathcal{D}_0$ (as in the statement of Theorem 5.5).

Proof of Theorem 5.5. At least one of $n-2$ or $n-1$ is even, so we have by Lemmas 5.10 and 5.12 that $p_1 = 2$, $p_2 = 3$ and $v_2 \geq 2$. There is, in consequence, no loss of generality in assuming, as we do, that $\varepsilon_0 = -1$, since the other case is impossible by Lemma 5.14. Thus, pick $i_0 \in S_n$ such that $3 \mid p_{i_0} + 1$. It follows from (5.3) and our hypotheses that there exist $\beta_{i_0}, \gamma_{i_0} \in \mathbb{N}$ such that

$$P = 3^{v_2}(3^{a_2} - 1) = p_{i_0}^{v_{i_0}} \cdot \left(p_{i_0}^{a_{i_0}} - 1\right) = 3^{v_2} p_{i_0}^{v_{i_0}} \cdot \left(3^{\beta_{i_0}} p_{i_0}^{\gamma_{i_0}} - 1\right),$$

to the effect that, on the one hand,

$$p_{i_0}^{a_{i_0}} - 1 = 3^{v_2} \cdot \left(3^{\beta_{i_0}} p_{i_0}^{\gamma_{i_0}} - 1\right), \tag{5.10}$$

and on the other hand,

$$3^{a_2} - 1 = p_{i_0}^{v_{i_0}} \cdot \left(3^{\beta_{i_0}} p_{i_0}^{\gamma_{i_0}} - 1\right). \tag{5.11}$$

Then, since $v_2 \geq 2$ and $a_{i_0} \neq 0$, we see by (5.10) and Lemma 5.15 that $\beta_{i_0} \geq 1$. It is then found from (5.11) that $-1 \equiv (-1)^{v_{i_0}+1} \bmod 3$, i.e. v_{i_0} is even. To wit, we have proved that

$$\forall i \in S_n : p_i \equiv -1 \bmod 3 \implies v_i \text{ is even and } p_i^{v_i} \equiv 1 \bmod 3. \tag{5.12}$$

But every prime $\neq 3$ is congruent to ± 1 modulo 3. Thus, we get from (5.2) and (5.12) that

$$2 \equiv \prod_{i \in S_n \setminus \{2\}} p_i^{\nu_i} + 1 \equiv 3^{a_2} \equiv 0 \bmod 3,$$

which is obviously a contradiction and completes the proof. □

5.4 Proof of Theorem 5.7

In the present section, unless differently specified, we use the same notation and assumptions of Theorem 5.7, whose proof is organized into three lemmas, one for each aspect of the claim.

Lemma 5.16. *A is an infinite set.*

Proof. Suppose for the sake of contradiction that A is finite and let $n := |A|$. Since A is a set of prime powers, there then exist $p_1, \dots, p_n \in \mathbb{P}$ and $\nu_1, \dots, \nu_n \in \mathbb{N}^+$ such that $p_1 \leq \cdots \leq p_n$ and $A = \{p_1^{\nu_1}, \dots, p_n^{\nu_n}\}$, and our assumptions give that

$$\text{“}q \text{ divides } \textstyle\prod_{i \in I} p_i^{\nu_i} - \varepsilon_0 \text{ for some } I \in \mathcal{P}_\star(S_n) \text{ only if } q \in \{p_1, \dots, p_n\}.\text{”} \tag{5.13}$$

This clearly implies that $p_1 < \cdots < p_n$. In fact, if $p_{i_1} = p_{i_2}$ for distinct $i_1, i_2 \in S_n$, then it is found from (5.13) and unique factorization that

$$p_{i_1}^k = \prod_{i \in S_n \setminus \{i_1\}} p_i^{\nu_i} - \varepsilon_0$$

for a certain $k \in \mathbb{N}^+$, which is impossible when reduced modulo p_{i_1}. Thus, using that $n \geq 3$, it follows from Theorem 5.5 that there also exists $q \in \mathbb{P} \setminus \{p_1, \dots, p_n\}$ such that q divides $\prod_{i \in I} p_i^{\nu_i} - \varepsilon_0$ for some $I \in \mathcal{P}_\star(S_n)$. This is, however, in contradiction with (5.13), and the proof is complete. □

Lemma 5.17. *If $\varepsilon_0 = 1$, then $\mathbb{P} \perp A$. In particular, $A = \mathbb{P}$ if $A \subseteq \mathbb{P}$.*

Proof. Suppose for the sake of contradiction that there exists $p \in \mathbb{P}$ such that p does not divide any element of A. Then, since A is fine and $|A| = \infty$ (by Lemma 5.16), there are infinitely many $a \in A$

such that $p \nmid a$. By the pigeonhole principle, this yields that, for a certain $r \in \{1, \dots, p-1\}$, the set $A_r := \{a \in A : a \equiv r \bmod p\}$ is infinite, and we have that

$$\forall B \in \mathcal{P}_\star(A_r) : \prod_{a \in B} a \equiv \prod_{a \in B} r \equiv r^{|B|} \bmod p. \tag{5.14}$$

As it is now possible to choose $B_0 \in \mathcal{P}_\star(A_r)$ in such a way that $|B_0|$ is a multiple of $p-1$, one gets from (5.14) and Fermat's little theorem that p divides $\prod_{a \in B} a - 1$ for some $B \in \mathcal{P}_\star(A)$, and hence $p \mid a_0$ for some $a_0 \in A$ (by the assumptions of Theorem 5.7). This is, however, absurd, because by construction no element of A is divisible by p. It follows that $\mathbb{P} \perp A$. The rest is trivial. □

In the next lemma, we let $\omega(n)$ denote the number of distinct prime factors of n, in such a way that, e.g., $\omega(1) = 0$ and $\omega(12) = 2$. Moreover, we let an empty sum be equal to 0 and an empty product be equal to 1, as usual.

Lemma 5.18. *If $\varepsilon_0 = -1$ and $A \subseteq \mathbb{P}$, then $A = \mathbb{P}$.*

Proof. Suppose to the contrary that $A \neq \mathbb{P}$, i.e. there exists $p \in \mathbb{P}$ such that $p \nmid A$, and for each $r \in S_{p-1}$, let $A_r := \{a \in A : a \equiv r \bmod p\}$. Then, $p \nmid A$ yields that

$$A = A_1 \cup \dots \cup A_{p-1}. \tag{5.15}$$

In addition, set $\Gamma_{\text{fin}} := \{r \in S_{p-1} : |A_r| < \infty\}$ and $\Gamma_{\text{inf}} := S_{p-1} \setminus \Gamma_{\text{fin}}$, and then

$$A_{\text{fin}} := \{a \in A : a \in A_r \text{ for some } r \in \Gamma_{\text{fin}}\} \quad \text{and} \quad A_{\text{inf}} := A \setminus A_{\text{fin}}.$$

It is clear from (5.15) that A_{inf} is infinite, because A_{fin} is finite, $\{A_{\text{fin}}, A_{\text{inf}}\}$ is a partition of A, and $|A| = \infty$ by Lemma 5.16. Thus, we define $\xi_0 := \prod_{a \in A_{\text{fin}}} a$, and we claim that there exists a sequence $\varrho_0, \varrho_1, \dots$ of positive integers such that ϱ_n is, for each $n \in \mathbb{N}$, a nonempty product (of a finite number) of distinct elements of A with the property that

$$\xi_0 \mid \varrho_n \quad \text{and} \quad 1 + \varrho_n \equiv \sum_{i=0}^{n+1} \varrho_0^i \bmod p. \tag{5.16}$$

Proof of the claim. We construct the sequence $\varrho_0, \varrho_1, \dots$ in a recursive way. To start with, pick an

arbitrary $a_0 \in A_{\text{inf}}$ and define $\varrho_0 := a_0 \cdot \xi_0$, where the factor a_0 accounts for the possibility that $\Gamma_{\text{fin}} = \emptyset$. By construction, ϱ_0 is a nonempty product of distinct elements of A, and (5.16) is satisfied in the base case $n = 0$.

Now fix $n \in \mathbb{N}$ and suppose that we have already found $\varrho_n \in \mathbb{N}^+$ such that ϱ_n is a product of distinct elements of A and (5.16) holds true with ϱ_0 and ϱ_n. By unique factorization, we then get from the assumptions on A that there exist $s_1, \ldots, s_k \in \mathbb{N}^+$ and distinct primes $p_1, \ldots, p_k \in \mathbb{P}$ such that $p_i \perp A$ for each i and

$$\xi_0 \mid \varrho_n \quad \text{and} \quad 1 + \varrho_n = \prod_{i=1}^{k} p_i^{s_i}, \tag{5.17}$$

where $k := \omega(\varrho_n) \geq 1$. Since A is a subset of $\mathbb{P}$, then $p_i \perp A$ implies $p_i \in A$, and indeed $p_i \in A_{\text{inf}}$, because every element of A_{fin}, if any exists, is a divisor of ξ_0, and $\xi_0 \mid \varrho_n$ by (5.17). Using that A_r is infinite for every $r \in \Gamma_{\text{inf}}$ and $A_{\text{inf}} = \bigcup_{r \in \Gamma_{\text{inf}}} A_r$, we get from here that there exist elements $a_1, \ldots, a_h \in A_{\text{inf}}$ such that, on the one hand,

$$\varrho_0 < a_1 < \cdots < a_h, \tag{5.18}$$

and on the other hand,

$$\forall i \in S_k : p_i \equiv a_{1+t_i} \equiv \cdots \equiv a_{s_i+t_i} \bmod p, \tag{5.19}$$

where $h := \sum_{i=1}^{k} s_i$ and $t_i := \sum_{j=1}^{i-1} s_j$ for each i. It follows from (5.17) and (5.19) that

$$1 + \varrho_n \equiv \prod_{i=1}^{k} p_i^{s_i} \equiv \prod_{i=1}^{h} a_i \bmod p.$$

So, for the assumptions on ϱ_n and the above considerations, we see that

$$1 + \varrho_0 \cdot (1 + \varrho_n) \equiv 1 + \varrho_0 \cdot \sum_{i=0}^{n+1} \varrho_0^i \equiv \sum_{i=0}^{n+2} \varrho_0^i \bmod p.$$

Our claim is hence proved, by recurrence, by taking $\varrho_{n+1} := \varrho_0 \cdot (1 + \varrho_n)$, because $\xi_0 \mid \varrho_0 \mid \varrho_{n+1}$

and ϱ_{n+1} is, by virtue of (5.18), a nonempty product of distinct elements of A. □

Thus, letting $n = p(p-1) - 2$ in (5.16) and considering that $p \nmid \varrho_0$, as $p \nmid A$ and ϱ_0 is, by construction, a product of elements of A, gives that $1 + \varrho_n \equiv 0 \bmod p$, with the result that $p \in A$ by the assumed properties of A. This is, however, a contradiction, and the proof is complete. □

Finally, we have all the ingredients to cook the following:

Proof of Theorem 5.7. Just put together Lemmas 5.16, 5.17 and 5.18. □

One obvious question arises: Can we prove Theorem 5.7 without assuming that A is a fine subset of $\mathbb{Z}$? That the answer is not unconditionally affirmative is implied by the following:

Example 5.19. Pick distinct primes $q_1, q_2, \dots, q_\ell \geq 3$ and, in view of [HW, Theorem 110], let g_i be a primitive root modulo q_i. A standard argument based on the Chinese remainder theorem then shows that there also exists an integer g such that g is a primitive root modulo q_i for each i, and by Dirichlet's theorem on arithmetic progressions we can choose g to be prime. Now, define

$$A := \begin{cases} \bigcup_{i=1}^{\ell} \{g^{(q_i-1)n} : n \in \mathbb{N}^+\} & \text{if } \varepsilon_0 = 1 \\ \\ \bigcup_{i=1}^{\ell} \{g^{\frac{1}{2}(q_i-1)(2n+1)} : n \in \mathbb{N}\} & \text{if } \varepsilon_0 = -1. \end{cases}$$

If $\mathfrak{P}$ is the set of all primes q such that q divides $\prod_{a\in B} a - \varepsilon_0$ for some $B \in \mathcal{P}_\star(A)$, then on the one hand, $q_i \subseteq \mathfrak{P}$ for each i (essentially by construction), and on the other hand, $q_i \nmid A$ because $\gcd(q_i, g) = 1$. Note that this is possible, by virtue of Theorem 5.7, only because A is not fine.

We conclude the section with another example, that provides evidence of a substantial difference between Lemmas 5.17 and 5.18, and is potentially of interest in relation to Question 5.8.

Example 5.20. Given odd primes $q_1, \dots, q_\ell$, let $k := \operatorname{lcm}(q_1 - 1, \dots, q_\ell - 1)$ and $A := \{p^{nk} : p \in \mathbb{P}, n \in \mathbb{N}^+\}$. We denote by $\mathfrak{P}$ the set of all primes q for which there exists $B \in \mathcal{P}_\star(A)$ such that q divides $\prod_{a\in B} a + 1$. It is then easily seen that $\mathfrak{P} \subseteq \mathbb{P} \setminus \{q_1, \dots, q_\ell\}$, since $\prod_{a\in B} a + 1 \equiv 2 \not\equiv 0 \bmod q_i$ for each $i = 1, 2, \dots, \ell$.

5.5 Closing remarks

Many natural questions related arise (in addition to the ones already raised in the previous sections), and perhaps it can be interesting to find them an answer.

Some examples: Is it possible to prove Theorem 5.5 under the weaker assumption that $\mathcal{D}_0$, as there defined, is $\mathcal{P}_1(S_n) \cup \mathcal{P}_{n-1}(S_n)$ instead of $\mathcal{P}_1(S_n) \cup \mathcal{P}_{n-2}(S_n) \cup \mathcal{P}_{n-1}(S_n)$? This is clearly the case if $n = 3$, but what about $n \geq 4$? And what if n is sufficiently large and $\mathcal{D}_0 = \mathcal{P}_k(S_n)$ for some $k \in S_n$? The answer to the latter is negative for $k = 1$ (to see this, take $p_1, \ldots, p_n$ to be the n smallest primes and let $v_1 = \cdots = v_n = \varepsilon_0 = 1$, then observe that, for each $i \in S_n$, the greatest prime divisor of $p_i^{v_i} - \varepsilon_0$ is $\leq p_i - 1$). But what if $k \geq 2$?

Furthermore: To what degree can the results in Section 5.2 be extended in the direction of Question 5.3? It seems worth mentioning in this respect that Question 5.3 has the following abstract formulation in the setting of integral domains (we refer to [Mo, Ch. 1] for background on divisibility and related topics in the general theory of rings):

Question 5.21. *Given an integral domain $\mathbb{F} = (F, +, \cdot)$ and an integer $n \geq 3$, pick pairwise coprime non-units $u_1, \ldots, u_n \in \mathbb{F}$ (assuming that this is actually possible), and let $\mathcal{D}$ be a nonempty subfamily of $\mathcal{P}_\star(S_n)$ with "enough" elements. Does there exist at least one irreducible $q \in \mathbb{F}$ such that q divides $\prod_{i \in I} u_i - 1$ for some $I \in \mathcal{D}$ and $q \nmid u_1 \cdots u_n$?*

In the above, the condition that $u_1, \ldots, u_n$ are non-units is needed to ensure that, for each $I \in \mathcal{D}$, the number $\prod_{i \in I} u_i - 1$ is non-zero, which would, in some sense, trivialize the question. On another hand, one may want to assume that $\mathbb{F}$ is a UFD, in such a way that an element is irreducible if and only if it is prime [Mo, Theorems 1.1 and 1.2]. In particular, it seems interesting to try to answer Question 5.21 in the special case where $\mathbb{F}$ is the ring of integers of a quadratic extension of $\mathbb{Q}$ with the property of unique factorization, and $u_1, \ldots, u_n$ are primes in $\mathbb{F}$. This will be, in fact, the subject of future work.

References

[AZ] M. Aigner and G. M. Ziegler, *Proofs from THE BOOK* (Springer, 2010, 4th ed.).

[BAB] M. Becheanu, M. Andronache, M. Bălună, R. Gologan, D. Şerbănescu, and V. Vornicu, *Romanian Mathematical Competitions 2003* (Societatea de Ştiinţe Matematice din România, 2003).

[Bo] A. Booker, *On Mullin's second sequence of primes*, Integers (6) **12** (2012), 1167–1177.

[BBB] D. Borwein, J. M. Borwein, P. B. Borwein, and R. Girgensohn, *Giuga's conjecture on primality*, Amer. Math. Monthly **103** (1996), 40–50.

[BV] L. Brenton and A. Vasiliu, *Znám's problem*, Math. Magazine (1) **75** (2002), 3–11.

[BL] Y. Bugeaud and F. Luca, *On Pillai's Diophantine equation*, New York J. Math. **12** (2006), 193–217.

[Ca] R. D. Carmichael, *On the Numerical Factors of Certain Arithmetic Forms*, American Math. Monthly (10) **16** (1909), 153–159.

[HW] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Oxford University Press, 2008, 6th ed., revised by D.R. Heath-Brown and J.H. Silverman).

[La] J. C. Lagarias, *Cyclic systems of simultaneous congruences*, Int. J. Number Theory (2) **6** (2010), 219–245.

[L] F. Luca, *On the diophantine equation* $p^{x_1} - p^{x_2} = q^{y_1} - q^{y_2}$, Indag. Mathem. N. S. (2) **14** (2003), 207–222.

[Lu] É. Lucas, *Théorie des Fonctions Numériques Simplement Periodiques*, Amer. J. Math. **1** (1878), 184–196, 197–240, 289–321.

[Mo] R. A. Mollin, *Algebraic Number Theory*, Discrete Mathematics and Its Applications (Chapman and Hall/CRC, 2011, 2nd ed.).

[Mu] A. A. Mullin, *Recursive function theory (a modern look at a Euclidean idea)*, Bull. Amer. Math. Soc. **69** (1963), 737.

[Na] W. Narkiewicz, *The Development of Prime Number Theory* (Springer-Verlag, 2000).

[Tr5] P. Leonetti and Salvatore Tringali, *On a system of equations with primes*, to appear in Journal de Théorie des Nombres de Bordeaux (preprint: arXiv/1212.0802).

[Zs] K. Zsigmondy, *Zur Theorie der Potenzreste*, Journal Monatshefte für Mathematik **3** (1892), 265–284.