An Invitation to Power Semigroups

Salvatore Tringali

School of Mathematical Sciences, Hebei Normal University

Ring Theory Seminar (online)

DMSC, University of Graz · Graz, Austria · Dec 5, 2024

Outline

What is a semigroup?

A semigroup (shortly, sgrp) is an ordered pair $(S, \otimes)$ consisting of a (possibly empty) set S, called the underlying set of the sgrp, and an associative (binary) operation $\otimes$ on S, meaning that $\otimes$ is a function (shortly, fnc) $S \times S \to S$ s.t.[1]

$$x \otimes (y \otimes z) = (x \otimes y) \otimes z, \qquad \text{for all } x, y, z \in S. \tag{1}$$

Eq. (1) is referred to as the associativity law (for the operation $\otimes$) and allows for the *unambiguous* usage of "long expressions" of the form $x_1 \otimes \cdots \otimes x_n$, where n is a positive integer and $(x_1, \ldots, x_n)$ is an n-tuple of elements of S.

There are two standard notations commonly used for the operation of a sgrp (unless a different symbol is explicitly required):

- the multiplicative notation, where the sgrp operation is called multiplication and denoted by a centered dot $\cdot$ (with or without subscripts or superscripts);
- the additive notation, where the sgrp operation is called addition and denoted by a plus sign $+$ (with or without subscripts or superscripts).

NOTE. Later on, we will typically identify a sgrp with its underlying set (especially if there is no serious risk of confusion), denote the sgrp operation multiplicatively, and write xy in place of $x \cdot y$.

[1] Here as usual, we define $u \otimes v := \otimes(u, v)$ for every $u, v \in S$.

Examples and non-examples of semigroups

We denote by $\mathbb{N}^+$ the (set of) positive int[eger]s, by $\mathbb{N}$ the non-negative ints, by $\mathbb{Z}$ the ints, by $\mathbb{Q}$ the rationals, by $\mathbb{R}$ the reals, and by $\mathbb{C}$ the complex numbers.

(1) Let $\otimes$ be the (binary) operation of exponentiation $(a, b) \mapsto a^b$ on $\mathbb{N}^+$. The pair $(\mathbb{N}^+, \otimes)$ is *not* a sgrp: $\otimes$ is not associative, since $(2 \otimes 2) \otimes 3 = 2^6 \neq 2^8 = 2 \otimes (2 \otimes 3)$.

(2) The set of *odd* ints does not form a sgrp under the (usual) operation of addition inherited from $\mathbb{Z}$: the sum of two odd ints is even.

(3) For all $a, b \in \mathbb{N}$ s.t. $b^2 \equiv b \bmod a$, the set $\{ak + b \colon k \in \mathbb{N}\} \subseteq \mathbb{N}$ is a sgrp under the (usual) operation of multiplication inherited from $\mathbb{N}$.

(4) Let $\mathbb{H} \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. For all $n \in \mathbb{N}^+$ and $a_1, \ldots, a_n \in \mathbb{H}$, the set

$$\{a_1 x_1 + \cdots + a_n x_n \colon x_1, \ldots, x_n \in \mathbb{N}\} \subseteq \mathbb{H}$$

is a sgrp under the (usual) operation of addition inherited from $\mathbb{H}$.

(5) Given $n \in \mathbb{N}^+$, the set of n-by-n singular matrices A with entries in a commutative ring R forms a sgrp under the (usual) operation of row-by-column multiplication. (We call the matrix A singular if its determinant is a zero divisor of R.)

(6) The non-empty finite tuples with components in a set X form a sgrp, called the free sgrp over X and denoted by $\mathscr{F}^+(X)$, under the (binary) operation $*$ of concatenation:

$$(x_1, \ldots, x_m) * (y_1, \ldots, y_n) := (x_1, \ldots, x_m, y_1, \ldots, y_n),$$

for all $m, n \in \mathbb{N}^+$ and $x_1, \ldots, x_m, y_1, \ldots, y_n \in X$.

Monoids and groups

A sgrp $(S, \otimes)$ is a monoid if there exists a (provably unique) element $e \in S$, called *the* identity [element] or neutral element (of the monoid itself), s.t.

$$x \otimes e = x = e \otimes x, \qquad \text{for every } x \in S.$$

A unit (or invertible element) of a monoid $\mathbb{S} = (S, \otimes)$ with neutral element e is then an element $u \in S$ for which there is a (provably unique) element $v \in S$, accordingly called *the* inverse of u (wrt to $\otimes$), s.t.

$$u \otimes v = e = v \otimes u.$$

We denote the set of units of $\mathbb{S}$ by $\mathbb{S}^\times$ and call $\mathbb{S}$ a group if $\mathbb{S}^\times = S$. Properties:

- The neutral element is a unit, and its inverse is itself.
- $u \in S$ is a unit iff the inverse of u is a unit.
- If $u, v \in \mathbb{S}^\times$, then $u \otimes v \in \mathbb{S}^\times$.

A couple of remarks about the notation:

- In a multiplicatively written monoid H, the neutral element is commonly denoted by 1_H (also without the subscript 'H') and the inverse of a unit u is denoted by u^{-1}.
- In an additively written monoid K, the neutral element is commonly denoted by 0_K (also without the subscript 'K') and the inverse of a unit u is denoted by $-u$.

Examples and non-examples of monoids

(1) Endowed with the (usual) operation of multiplication inherited from $\mathbb{Z}$, the *even* ints form a semigroup but not a monoid: there is no even integer e s.t. $2e = 2$.

(2) Example (5) on Slide 4 is a monoid iff R is a zero ring (i.e., R has one element), or $n = 1$ and R is a domain (i.e., R has no zero divisors apart from the zero element).

(3) The elements of a *unital* ring R form a monoid under the operation of multiplication of the ring itself, accordingly called the multiplicative monoid of R.

(4) Example (4) on Slide 4 is a monoid for any choice of $\mathbb{H}$, n, and $a_1, \ldots, a_n$.

(5) Every semigroup $(S, \otimes)$ can be (canonically) made into a monoid as follows:

- If the semigroup has already a neutral element, we have nothing to do.
- Otherwise, we adjoin a *new* element e to S and extend $\otimes$ to a (binary) operation on $S \cup \{e\}$ by taking $x \otimes e := x =: e \otimes x$ for every $x \in S \cup \{e\}$.

The monoid obtained in this way is called a (conditional) unitization of $(S, \otimes)$.

(6) The unitization of the free sgrp $\mathscr{F}^+(X)$ over a set X (Example (6) on Slide 4) is named the free monoid over X and denoted by $\mathfrak{F}(X)$. The elements of $\mathscr{F}(X)$ are referred to as X-words, and the neutral element as the empty X-word. If the set X is clear from the context, we just say "word" instead of "X-word".

(7) A group is, by def., a monoid in which every element is a unit. It follows from the basic properties of units on Slide 5 that, under the operation inherited from H, the units of a monoid H form a group, accordingly called the group of units of H.

Homomorphisms

A sgrp homomorphism (shortly, hom) is a triple $(\mathbb{S}, \mathbb{T}, \phi)$, where $\mathbb{S} = (S, \otimes)$ and $\mathbb{T} = (T, \odot)$ are sgrps (called the domain and the codomain of the hom, resp.), and ϕ is the graph of a fnc from S to T s.t.

$$\phi(x \otimes y) = \phi(x) \odot \phi(y), \qquad \text{for all } x, y \in S. \tag{2}$$

We will typically denote a sgrp hom $(\mathbb{S}, \mathbb{T}, \phi)$ by the arrow notation $\phi \colon \mathbb{S} \to \mathbb{T}$ and say that ϕ is a *sgrp hom from* $\mathbb{S}$ *to* $\mathbb{T}$. Accordingly, we refer to ϕ as

- a monomorphism (or a monic or injective hom) if ϕ is an injective fnc;
- an epimorphism (or an epic or surjective hom) if ϕ is a surjective fnc;
- an isomorphism if ϕ is both injective and surjective (i.e., a bijection);
- an endomorphism (of $\mathbb{S}$) if domain and codomain coincide (i.e., $\mathbb{S} = \mathbb{T}$);
- an automorphism (of $\mathbb{S}$) if ϕ is both an isomorphism and an endomorphism;
- a monoid hom if $\mathbb{S}$ and $\mathbb{T}$ are both monoids, and ϕ maps the neutral/identity element of $\mathbb{S}$ to the neutral/identity element of $\mathbb{T}$.

In particular, we say that $\mathbb{S}$ is (sgrp-)isomorphic to $\mathbb{T}$, written $\mathbb{S} \simeq \mathbb{T}$, if there is an isomorphism from $\mathbb{S}$ to $\mathbb{T}$.

NOTE. A sgrp hom from a monoid to a monoid need not be a monoid hom (e.g., consider the integers under multiplication and the fnc $\mathbb{Z} \to \mathbb{Z} \colon x \mapsto 0$).

Substructures

A subsemigroup (shortly, subsgrp) of a sgrp $\mathbb{S} = (S, \otimes)$ is a set $T \subseteq S$ that is closed (and hence becomes itself a sgrp) under the operation inherited from $\mathbb{S}$:

$$x \otimes y \in T, \qquad \text{for all } x, y \in T. \tag{3}$$

It is easily checked that the following hold for a sgrp hom $f\colon \mathbb{H} \to \mathbb{K}$:

- If T is a subsgrp of $\mathbb{S}$, then $f[T] := \{f(x)\colon x \in T\}$ is a subsgrp of $\mathbb{K}$.
- If T is a subsgrp of $\mathbb{K}$, then $f^{-1}[T] := \{x \in H\colon f(x) \in T\}$ is a subsgrp of $\mathbb{H}$.

In a similar vein, a submonoid (resp., a subgroup) of $\mathbb{S}$ is a (necessarily non-empty) subsgrp T of $\mathbb{S}$ s.t. the pair $(T, \otimes_T)$ is a monoid (resp., a group) in its own right, where $\otimes_T$ is the binary operation $(x, y) \mapsto x \otimes y$ on T (which is a well-defined fnc $T \times T \to T$ as we are supposing that Eq. (3) holds).

In general, a submonoid/subgroup K of a monoid $\mathbb{H}$ need *not* contain the neutral element e of $\mathbb{H}$ (e.g., the singleton $\{0\} \subseteq \mathbb{Z}$ is a subgroup of the multiplicative monoid of the ring of integers, and the neutral element of the latter is the integer 1). If, on the other hand, K contains e, then e is a fortiori the neutral element of K, and we call K a unital submonoid/subgroup of $\mathbb{H}$.

Most notably, the set of units, $\mathbb{H}^\times$, of a monoid $\mathbb{H}$ is a unital subgroup of $\mathbb{H}$, accordingly called the group of units of H.

Composing homomorphisms

The (functional) composition of a sgrp hom $f\colon \mathbb{H} \to \mathbb{K}$ *with* a sgrp hom $\mathbb{K} \to \mathbb{L}$ is the triple $(\mathbb{H}, \mathbb{L}, g \circ f)$, where $g \circ f$ (read "g after f") is the function

$$H \to L\colon x \mapsto g(f(x)),$$

where H and L are the underlying sets of $\mathbb{H}$ and $\mathbb{L}$, resp.

Assuming for ease of notation that $\mathbb{H}$, $\mathbb{K}$, and $\mathbb{L}$ are all written multiplicatively, and considering that both f and g satisfy Eq. (2), we find that, for all $x, y \in H$,

$$g \circ f(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f(x))(g \circ f(y)).$$

That is, $g \circ f$ is a sgrp hom from $\mathbb{H}$ to $\mathbb{L}$.

It follows that, under the operation of composition, the endomorphisms of a sgrp $\mathbb{S} = (S, \otimes)$ form a *monoid*, herein denoted by $\mathrm{End}(\mathbb{S})$, whose neutral element is the identity fnc id_S on the set S (i.e., the fnc $S \to S\colon x \mapsto x$).

The units of $\mathrm{End}(\mathbb{S})$ are then the endomorphisms ϕ of $\mathbb{S}$ s.t. $\phi \circ \phi' = \phi' \circ \phi = \mathrm{id}_S$ for some $\phi' \in \mathrm{End}(\mathbb{S})$, namely, the automorphisms of $\mathbb{S}$.

So, under the operation of composition, the automorphisms of $\mathbb{S}$ form a group, henceforth called the automorphism group of $\mathbb{S}$ and denoted by $\mathrm{Aut}(\mathbb{S})$.

Congruences and quotients

A (sgrp) congruence on a sgrp $\mathbb{S} = (S, \otimes)$ is an equivalence relation $\sim$ on the set S with the additional property that

$$\text{if } u \sim v \text{ and } x \sim y, \text{ then } u \otimes x \sim v \otimes y.$$

An equivalence class in the quotient (set) of S by $\sim$ is then referred to as a congruence class modulo $\sim$. In particular, we write $[x]_\sim$ for the congruence class modulo $\sim$ represented by an element $x \in S$, that is, we set

$$[x]_\sim := \{y \in S \colon x \sim y\}.$$

The quotient of S by $\sim$ is in fact a sgrp under the binary operation that maps a pair $(\mathfrak{u}, \mathfrak{v})$ of equivalence classes in the quotient to the equivalence class of the element $u \otimes v$, where $u \in \mathfrak{u}$ and $v \in \mathfrak{v}$ (it is routine to check that this definition does not depend on the choice of the representatives u and v).

The sgrp obtained in this way is the quotient (or factor) sgrp of $\mathbb{S}$ by $\sim$, and it is denoted by $\mathbb{S}/\sim$. Accordingly, (the graph of) the fnc

$$\pi \colon S \to S/\sim \colon x \mapsto [x]_\sim$$

is a sgrp hom $\mathbb{S} \to \mathbb{S}/\sim$, named the canonical projection of $\mathbb{S}$ onto $\mathbb{S}/\sim$.

Outline

Power semigroups

From now on, all sgrps are written multiplicatively unless stated otherwise

The large power sgrp of a sgrp S is the sgrp $\mathcal{P}(S)$ obtained by endowing the *non-empty* subsets of S with the (provably associative) operation

$$(X, Y) \mapsto XY := \{xy \colon x \in X,\, y \in Y\}.$$

Loosely speaking, a power sgrp is any of a variety of sgrps that sit between a sgrp and its large power sgrp (no precise definition). For instance:

(1) The non-empty *finite* subsets of S form a subsgrp of $\mathcal{P}(S)$, herein denoted by $\mathcal{P}_{\text{fin}}(S)$ and called the finitary power sgrp of S.

(2) If κ is an idempotent cardinal number (i.e., $\kappa = 0$, $\kappa = 1$, or κ is infinite), then the family of all non-empty sets $X \subseteq S$ such that $|X| < \kappa$ (resp., $|X| \le \kappa$) is a subsgrp of $\mathcal{P}(S)$, hereafter denoted by $\mathcal{P}_{<\kappa}(S)$ (resp., by $\mathcal{P}_{\le\kappa}(S)$). In particular, $\mathcal{P}_{\text{fin}}(S) = \mathcal{P}_{<|\mathbb{N}|}(S)$.

A couple of remarks:

- $\mathcal{P}_{\le 1}(S)$ is sgrp-isomorphic to S via the fnc $S \to \mathcal{P}(S) \colon x \mapsto \{x\}$ (corestricted to its own image), i.e., $\mathcal{P}(S)$ contains an isomorphic copy of S.
- If S is a monoid with neutral element 1_S, then $\mathcal{P}(S)$ is a monoid with neutral element $\{1_S\}$ and $\mathcal{P}_{\text{fin}}(S)$ is a unital submonoid of $\mathcal{P}(S)$. Accordingly, we call $\mathcal{P}(S)$ and $\mathcal{P}_{\text{fin}}(S)$ the large power monoid and the finitary power monoid of S, resp.

Older literature and origins

To my knowledge, power sgrps made their first *explicit* appearance in a 1953 paper by Dubreil and later on in Lyapin's influential book on sgrp theory[(2)]. They were studied quite intensively in the 1980s and 1990s[(3)].

In fact, $\mathcal{P}(S)$ was first *systematically* tackled by Tamura & Shafer[(4)] in 1967, while being a special case of the general notion of power algebra[(5)].

Tamura & Shafer were especially interested in the following problem:

Problem 1.

Given a class $\mathcal{O}$ of sgrps, prove/disprove that $\mathcal{P}(H) \simeq \mathcal{P}(K)$, for some $H, K \in \mathcal{O}$, iff $H \simeq K$. (Here and later, $\simeq$ means "is sgrp-isomorphic to".)

The heart of the problem lies in the "only if" direction, for every (sgrp) isomorphism $H \to K$ lifts to a global isomorphism $H \to K$ (that is, to an isomorphism $\mathcal{P}(H) \to \mathcal{P}(K)$) via the mapping $X \mapsto f[X] := \{f(x) \colon x \in X\}$.

---

(2) Their definition is however *implicit* to the early work on additive combinatorics, including Cauchy's 1813 paper containing the first-known proof of the Cauchy-Davenport inequality.

(3) Almeida, Semigroup Forum **64** (2002), 159–179.

(4) Tamura & Shafer, Math. Japon. **12** (1967), 25–32.

(5) Sect. 2 in Brink, Algebra Universalis **30** (1993), 177–216.

Partial history of a problem

The Tamura–Shafer problem was quickly answered in the negative for *arbitrary* sgrps[(6)], but has a positive answer in many cases (the list is *not* complete):

- *finite* groups and *finite* chains, see Theorems 5.8 and 5.9 in [Tamura & Shafer, Math. Japon. **12** (1967), 25–32].
- groups [Shafer, Math. Japon. **12** (1967), 32].
- *unital* semilattices, chains, and lattices, see Theorems 1.3, 1.4, and 2.2 in [Gould, Iskra, & Tsinakis, Algebra Univ. **19** (1984), 137–141].
- *finite* simple sgrps and *finite* semilattices of torsion groups, see Theorems 3.3 and 2.2 in [Gould & Iskra, Semigroup Forum **28** (1984), 1–11].
- semilattices, see p. 218 in [Kobayashi, Semigroup Forum **29** (1984), 217–222].
- completely 0-simple sgrps and completely simple sgrps, see Theorems 5.9 and 6.8 in [Tamura, J. Algebra **98** (1986), 319–361].
- Clifford sgrps, see Theorem 4.7 in [Gan & Zhao, J. Aust. Math. Soc. **97** (2014), 63–77].

The problem is open, e.g., for *finite* sgrps and *cancellative*[(7)] sgrps, but was solved in the cancellative *commutative* setting, both in its original form and in the variant for *finitary* power sgrps [T., 2024]. The latter result has been further generalized to the cancellative *duo* setting [Li & T., work in progress].

---

(6) See Mogiljanskaja, Semigroup Forum **6** (1973), 330–333.

(7) A sgrp S is cancellative if $x \mapsto ax$ and $x \mapsto xa$ are injective fncs on S for every $a \in S$.

Categories go on stage

The Tamura–Shafer problem and its variants are in fact a special instance of a much more general problem, whose formulation is categorial in nature[8]:

Functorial isomorphism problem

Given a functor $F\colon \mathcal{C} \to \mathcal{D}$ and a class $\mathcal{O} \subseteq \mathrm{Ob}(\mathcal{C})$ that is closed under isos, prove/disprove that $F(A) \simeq_{\mathcal{D}} F(B)$, for some $A, B \in \mathcal{O}$, iff $A \simeq_{\mathcal{C}} B$.

Of course, the answer is generally in the negative, and the only interesting part of the problem lies in the "only if" clause.

The Tamura–Shafer problem is in particular the special case where F is the endofunctor of the (usual) category Sgrp of sgrps and sgrp homs, hereinafter referred to as the large power functor of Sgrp, that maps

- a sgrp S to its large power semigroup $\mathcal{P}(S)$, and
- a sgrp hom $f\colon S \to T$ to its augmentation $f^*\colon \mathcal{P}(S) \to \mathcal{P}(T)\colon X \mapsto f[X]$.

Reframing the problem in the language of categories doesn't (seem to) make it easier, but it helps to place it in the 'right perspective' and provides a unifying approach to the formulation of many analogous problems.

[8]We write $\mathrm{Ob}(\mathcal{Q})$ for the object class of a category $\mathcal{Q}$, and we write $X \simeq_{\mathcal{Q}} Y$ to mean that X and Y are isomorphic objects in $\mathcal{Q}$.

Recent literature and popularization

Power sgrps went dormant for about 20 years, until Yushuang Fan and I (unaware of any previous literature!) rediscovered them in 2018:

- Fan & T., J. Algebra **512** (2018), 252–294.

The paper brought new life to the topic and has been followed by a few more:

- Antoniou & T., Pacific J. Math. **312** (2021), No. 2, 279–308.
- Sect. 4.2 in T., J. Algebra **602** (July 2022), 352–380.
- pp. 101–102 in Geroldinger & Khadam, Ark. Mat. **60** (2022), 67–106.
- Bienvenu & Geroldinger, Israel J. Math. (2024). DOI: 10.1007/s11856-024-2683-0
- Example 4.5(3) and Remark 5.5 in Cossu & T., J. Algebra **630** (2023), 128–161.
- T. & Yan, Proc. Amer. Math. Soc., to appear (arXiv:2310.17713).
- Gonzalez et al., Intl. J. Algebra Comput. (2024). DOI: 10.1142/S0218196724500565
- T. & Yan, J. Comb. Theory Ser. A **209** (2025), #105961, 16 pp.
- [Preprints] Cossu & T., under review (soon on arXiv).

In 2023, power sgrps were the subject of a CrowdMath project led by F. Gotti:

`https://artofproblemsolving.com/polymath/mitprimes2023`

Why caring?

1) A leading example in the development of a *unifying theory of factorization*:

- T., J. Algebra **602** (July 2022), 352–380.
- Cossu & T., Israel J. Math. **263** (2024), 349–395.
- Cossu & T., J. Algebra **630** (2023), 128–161.
- T., Math. Proc. Cambridge Philos. Soc. **175** (2023), 459-465.
- Cossu & T., Ark. Mat. **62** (2024), No. 1, 21–38.
- Casabella, García-Sánchez, & D'Anna, Mediterr. J. Math. **21** (2024), #7, 28 pp.
- García-Sánchez, Semigroup Forum **108** (2024), 365–376.
- [Preprints] Ajran & Gotti (`arXiv:2305.00413`) and Cossu & T. (soon on arXiv).

2) A natural algebraic framework for arithmetic combinatorics:

- **Sárközy's conjecture**[(9)]**.** For all but finitely many primes p, the set of [non-zero] quadratic residues mod p is an atom in the finitary power sgrp of $(\mathbb{Z}/p\mathbb{Z}, +)$.
- **Ostmann's conjecture**[(10)]**.** Every set of integers that differ from the set of primes by finitely many elements is an atom in the large power sgrp of $(\mathbb{Z}, +)$.

3) A key role in the study of formal languages and automata[(11)].

---

(9) Conjecture 1.6 in Sárközy, Acta Arith. **155** (2012), No. 1, 41–51.
(10) Elsholtz, Mathematika **48** (2001), Nos. 1–2, 151–158.
(11) See (the refs in) Auinger & Steinberg, Theoret. Comput. Sci. **341** (2005), 1–21.

Age of Ultron

In the 1980s and early 1990s, semigroup theorists, computer scientists, and model theorists worked on the "block groups = power groups" conjecture.

A pseudovariety (of semigroups) is a class of *finite* semigroups that is closed under taking homomorphic images, subsemigroups, and finite (direct) products.

Denote by $\mathcal{B}$G the pseudovariety generated by the *finite monoids* all of whose *regular*(12) one-sided principal ideals(13) are Brandt(14), and by $\mathcal{P}$G the pseudovariety generated by the power monoids of the *finite groups*.

In 1984, S. W. Margolis and J.-E. Pin proved that $\mathcal{P}$G $\subseteq$ $\mathcal{B}$G, but whether the opposite inclusion is true remained open for many years.

Settled (in the positive) by K. Henckell and J. Rhodes in ["The theorem of Knast, the $PG = BG$ and Type II Conjectures", pp. in 453–463 in J. Rhodes (ed.), *Monoids and Semigroups with Applications*, Word Scientific, 1991].

(12) The one-sided ideals of M are subsemigroups of M, and a semigroup S is regular if, for each $a \in S$, there exists $x \in S$, called a (von Neumann) inverse of a, such that $a = axa$.

(13) The one-sided principal ideals of a semigroup S are the sets of the form $\{a\} \cup aS$ or $\{a\} \cup Sa$ with $a \in S$. They are also known in semigroup theory as $\mathcal{D}$-classes.

(14) A sgrp S is Brandt if it is an inverse sgrp (i.e., a regular sgrp where each element has a *unique* inverse) without *non-trivial* (2-sided) ideals, the trivial ideals being S and $\varnothing$.

Outline

Global closedness

It was mentioned on Slide 14 that, back in 1967, Shafer proved (in a half-a-page note) that the class $\mathcal{O}$ of groups is globally determined, meaning that the Tamura–Shafer problem (Slide 13) has a positive answer for $\mathcal{O}$.

However, the answer to the following question was unknown until recently:

Problem 2.

If a group G is globally isomorphic to a sgrp S, then is S necessarily a group?

This is a special case of a broader and more general problem, which is, once again, most naturally formulated in the language of categories (cf. Slide 15):

Functorial closure problem

Given a functor $F\colon \mathcal{C} \to \mathcal{D}$ and a class $\mathcal{O} \subseteq \mathrm{Ob}(\mathcal{C})$, prove/disprove that if $F(A) \simeq_{\mathcal{D}} F(B)$ for some $A \in \mathcal{O}$ and $B \in \mathrm{Ob}(\mathcal{C})$, then $B \in \mathcal{O}$.

If the answer to the last question is positive, we say that the class $\mathcal{O}$ is F-closed. In particular, a class of sgrps is called globally closed if it is $\mathcal{P}$-closed, where $\mathcal{P}$ is the large power sgrp functor from Slide 15.

Unit-invariance

For instance, the following classes of sgrps are globally closed:

(1) The class of all sgrps (obvious and uninteresting).

(2) Finite sgrps (if two sgrps are globally iso, then their power sets are equipotent).

(3) Commutative sgrps (a simple exercise).

(4) Monoids (Lemma 1.1 in [Gould, Iskra, & Tsinakis, Algebra Universalis **19** (1984), 137–141]).

We will show that groups are also globally closed (**it is open** whether the same is true of *cancellative* sgrps). Crucial to the proof is the following:

Definition.

Given a monoid M, we say that an element $x \in M$ is unit-invariant if $ux = x = xu$ for all $u \in M^\times$ (where $M^\times$ is the group of units of M).

Every element of a monoid *with trivial group of units* is unit-invariant (this is not an issue), and the following lemma is straightforward from the definitions:

Lemma.

A sgrp isomorphism from a monoid H to a monoid K maps unit-invariant elements of H to unit-invariant elements of K.

Groups are globally closed

In hindsight, proving that groups are globally closed is not at all difficult. One key observation is that the units of the large power monoid $\mathcal{P}(M)$ of a monoid M are precisely the singletons $\{u\}$ with $u \in M^\times$, which implies in turn that

$X \in \mathcal{P}(M)$ is unit-invariant iff $XM^\times = M^\times X = X$.

This leads to the following:

Theorem.

If f is a global iso from a monoid H to a monoid K, then f maps $H^\times$ to $K^\times$ and hence restricts to a global isomorphism from $H^\times$ to $K^\times$.

From here, it is quite easy to conclude:

Proof that groups are globally closed.

Let f be a global iso from a group G to a sgrp H. By Lemma 1.1 in [Gould et al., 1984] (see Slide 21), H is a monoid. So, f restricts to a global iso from $G^\times$ to $H^\times$ (by the above theorem) and is therefore an iso $\mathcal{P}(G) \to \mathcal{P}(H^\times)$. Since $\mathcal{P}(H^\times)$ is contained in $\mathcal{P}(H)$ and, by hp, f is also an iso $\mathcal{P}(G) \to \mathcal{P}(H)$, this is only possible if $H^\times = H$. ■

Outline

Focus on power monoids

A closer look at the refs on the previous slides will reveal that most of the *recent* work on power sgrps has in fact focused on power monoids (PMs), where the "ground sgrp" has a neutral element (i.e., is a monoid).

One reason is that PMs are usually much tamer that arbitrary power sgrps, which is partly reflected in the richness of the lattice of their subsgrps.

Throughout, M is a multiplicative[ly written] monoid and we denote by $M^\times$ its group of units (note that M need not be commutative, cancellative, etc.)

Each of the following is a *unital* submonoid of $\mathcal{P}(M)$:

- $\mathcal{P}_\times(M) := \{X \in \mathcal{P}(M) \colon X \cap M^\times \neq \varnothing\}$, the restricted large PM of M.
- $\mathcal{P}_1(M) := \{X \in \mathcal{P}(M) \colon 1_M \in X\}$, the reduced large PM of M.
- $\mathcal{P}_{\mathrm{fin}}(M) = \{X \in \mathcal{P}(M) \colon |X| < \infty\}$, the finitary PM of M.
- $\mathcal{P}_{\mathrm{fin},\times}(M) := \mathcal{P}_{\mathrm{fin}}(M) \cap \mathcal{P}_\times(M)$, the restricted finitary PM of M.
- $\mathcal{P}_{\mathrm{fin},1}(M) := \mathcal{P}_{\mathrm{fin}}(M) \cap \mathcal{P}_1(M)$, the reduced finitary PM of M.

Follow the arrows

In the diagram below, a "hooked arrow" $P \hookrightarrow Q$ means the inclusion map from P to Q and a "tailed arrow" $P \rightarrowtail Q$ means the embedding $P \to Q\colon x \mapsto \{x\}$:

$$\begin{array}{ccccc}
\{1_M\} & \hookrightarrow & M^\times & \hookrightarrow & M \\
\downarrow\!\!\!\!\curlyvee & & \downarrow\!\!\!\!\curlyvee & & \downarrow\!\!\!\!\curlyvee \\
\mathcal{P}_{\mathrm{fin},1}(M) & \hookrightarrow & \mathcal{P}_{\mathrm{fin},\times}(M) & \hookrightarrow & \mathcal{P}_{\mathrm{fin}}(M) \\
\big\downarrow & & \big\downarrow & & \big\downarrow \\
\mathcal{P}_1(M) & \hookrightarrow & \mathcal{P}_\times(M) & \hookrightarrow & \mathcal{P}(M)
\end{array}$$

There are many objective reasons why PMs are "smoother" than power sgrps:

- If M is cancellative, then $\mathcal{P}_{\mathrm{fin}}(M)$ is divisor-closed[15] in $\mathcal{P}(M)$.
- If M is Dedekind-finite (that is, $xy = 1_M$ iff $yx = 1_M$), then (i) $\mathcal{P}_\times(M)$ is divisor-closed in $\mathcal{P}(M)$, and so is $\mathcal{P}_{\mathrm{fin},\times}(M)$ in $\mathcal{P}_{\mathrm{fin}}(M)$; (ii) $\mathcal{P}_{\mathrm{fin},1}(M)$ and $\mathcal{P}_{\mathrm{fin},\times}(M)$ have, in a way, the same arithmetic[16], and so do $\mathcal{P}_1(M)$ and $\mathcal{P}_\times(M)$.
- $\mathcal{P}_{\mathrm{fin},1}(N)$ is divisor-closed in $\mathcal{P}_{\mathrm{fin},1}(M)$ for *every* submonoid N of M[17].

---

(15) A submonoid K of a monoid H is divisor-closed if "$x \in H$ and $y \in K \cap HxH$" $\Rightarrow x \in K$.
(16) Propositions 3.5 and 4.10 in [Antoniou & T., 2021].
(17) Proposition 3.2(iii) in [Antoniou & T., 2021].

Pivots

It follows from the facts on the previous slide that, to some extent, we can[18] focus our attention on the reduced finitary PMs of $(\mathbb{N}, +)$ and $(\mathbb{Z}/n\mathbb{Z}, +)$, herein denoted by $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ and $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$, resp., and written additively:

- The arithmetic of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ is the object of Sect. 4 in [Fan & T., 2018].
- The arithmetic of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$ for an *odd* modulus n is the object of Sect. 5 in [Antoniou & T., 2021] (see also Sect. 4.2 in [T., 2022]).
- Bienvenu & Geroldinger have addressed algebraic and (sort of) analytic properties of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ and closely related structures (see the next slide).

In this regard, a major open problem is the following conjecture:

Sect. 5 of [Fan & T., 2018]

Every non-empty *finite* $L \subseteq \mathbb{N}_{\ge 2}$ is the length set of a set $X \in \mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$, i.e., L is the set of all $k \in \mathbb{N}$ s.t. X is a sum of k atoms[a] of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$.

[a] In a monoid, an atom is a non-unit that does not factor as a product of two non-units.

Propositions 4.8–4.10 in [Fan & T., 2018] show that, for all $n \ge 2$, each of $\{n\}$, $\{2, n\}$, and $[\![2, n]\!]$ can be realized as the length set of a set in $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$.

[18] When M is cancellative, there are no other monogenic submonoids (up to iso).

The Bienvenu–Geroldinger conjecture

True or not, Fan & T.'s conjecture has spurred a new wave of questions.

Most notably, let S be a numerical monoid, i.e., a submonoid of $(\mathbb{N}, +)$ with finite complement in $\mathbb{N}$. Bienvenu & Geroldinger have

- obtained quantitative results on the "density" of the atoms of the reduced finitary PM of S, herein denoted by $\mathcal{P}_{\mathrm{fin},0}(S)$ and written additively;
- started a foray into the ideal theory of $\mathcal{P}_{\mathrm{fin},0}(S)$, with emphasis on prime ideals.

Moreover, they have formulated (and proved special cases of) the following:

The Bienvenu–Geroldinger conjecture

The reduced finitary PM of a numerical monoid S_1 is isomorphic to the reduced finitary PM of a numerical monoid S_2 iff $S_1 = S_2$.

A couple of remarks:

i) The Bienvenu–Geroldinger conjecture is ultimately asking to show that, in a certain class of multiplicative monoids, $\mathcal{P}_{\mathrm{fin},1}(H) \simeq \mathcal{P}_{\mathrm{fin},1}(K)$ iff $H \simeq K$, as it is folklore that two numerical monoids are isomorphic iff they are equal[19].

ii) The equivalence i) is false for arbitrary monoids — if H is an idempotent (multiplicative) monoid with two elements, then $H \simeq \mathcal{P}_{\mathrm{fin},1}(H) \simeq \mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/2\mathbb{Z}) \not\simeq (\mathbb{Z}/2\mathbb{Z}, +)$.

[19] See, e.g., Theorem 3 in Higgins, Bull. Austral. Math. Soc. **1** (1969), 115–125.

Sketch of proof

The Bienvenu–Geroldinger conjecture was recently settled by Weihao Yan and myself in a 7-page note (to appear in Proc. AMS). *In hindsight*, the proof is rather simple — the most advanced technology we use is a classic[20]:

Nathanson's Theorem (or Fundamental Theorem of Additive NT)

Given $A \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ with $\gcd A = 1$, there exist $b, c \in \mathbb{N}$, $B \subseteq [\![0, b-2]\!]$, and $C \subseteq [\![0, c-2]\!]$ s.t., for all large $k \in \mathbb{N}$,

$$kA = B \cup [\![b, ka - c]\!] \cup (ka - C),$$

where $a := \max A$ and $kA := A + \cdots + A$ (k times).

The proof breaks down to the following steps:

1) Show by Nathanson's theorem that, given $A \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$, we have $(k+1)A = kA + B$ for all large $k \in \mathbb{N}$ and every $B \subseteq A$ with $\{0, \max A\} \subseteq B$.
2) Use 1) to prove that, if S_1 and S_2 are numerical monoids and $\phi\colon \mathcal{P}_{\text{fin},0}(S_1) \to \mathcal{P}_{\text{fin},0}(S_2)$ is an iso, then ϕ sends 2-element sets to 2-element sets.
3) Use 2) to show that, if $\phi(\{0, a_1\}) = \{0, b_1\}$ and $\phi(\{0, a_2\}) = \{0, b_2\}$ for some $a_1, a_2 \in S_1$, then $\phi(\{0, a_1 + a_2\}) = \{0, b_1 + b_2\}$.

[20] See Nathanson, Amer. Math. Monthly **79** (1972), No. 9, 1010–1012.

A good question fights back

End of the story? Let a Puiseux monoid H be a submonoid of $(\mathbb{R}_{\geq 0}, +)$. We denote the reduced finitary PM of H by $\mathcal{P}_{\mathrm{fin},0}(H)$, write it additively, and say that H is a rational Puiseux monoid[(21)] if $H \subseteq \mathbb{Q}_{\geq 0}$.

Nathanson's theorem has a natural extension to (non-empty, finite) sets of rationals, so the proof outlined on the previous slide can be adapted to show:

Theorem (T. & Yan · PAMS, 202*)

$\mathcal{P}_{\mathrm{fin},0}(H) \simeq \mathcal{P}_{\mathrm{fin},0}(K)$, for rational Puiseux monoids H and K, iff $H \simeq K$.

No analogue of Nathanson's theorem is available for (finite) subsets of $\mathbb{R}$, and the question arises whether rationality is really necessary. More generally, the following is another instance of the Functorial Isomorphism Problem (Slide 15).

Problem 3.

Given a class $\mathcal{O}$ of monoids, prove/disprove that $\mathcal{P}_{\mathrm{fin},1}(H) \simeq \mathcal{P}_{\mathrm{fin},1}(K)$, for some $H, K \in \mathcal{O}$, iff $H \simeq K$.

I conjecture a "Yes!" for cancellative monoids (cf. the remarks on Slide 27).

[(21)] Rational Puiseux monoids have been intensively studied by F. Gotti since 2018. They are indeed much older, but Gotti's work has bolstered a revival of the topic.

Outline

Be transformed!

The previous problems motivate the study of morphisms between power sgrps. In particular, Weihao Yan and I have posed the following:

Problem 4.

Given a monoid M, "determine" the (sgrp) automorphisms of $\mathcal{P}_{\mathrm{fin},1}(M)$.

To set the stage, let $\mathrm{Aut}(N)$ be the automorphism group of a monoid N. It is not difficult to show that, for each $f \in \mathrm{Aut}(M)$, the function

$$\mathcal{P}_{\mathrm{fin},1}(M) \to \mathcal{P}_{\mathrm{fin},1}(M) \colon X \mapsto f[X]$$

is an automorphism of $\mathcal{P}_{\mathrm{fin},1}(M)$, herein called the (reduced finitary) augmentation of f. We say that an automorphism of $\mathcal{P}_{\mathrm{fin},1}(M)$ is inner if it is the augmentation of an automorphism of M. So, we have a well-defined map

$$\Phi \colon \mathrm{Aut}(M) \to \mathrm{Aut}(\mathcal{P}_{\mathrm{fin},1}(M))$$

sending an automorphism of M to its augmentation. In fact, Φ is an *injective* (*group*) *homomorphism* from $\mathrm{Aut}(M)$ to $\mathrm{Aut}(\mathcal{P}_{\mathrm{fin},1}(M))$.

The question becomes whether Φ is also *surjective* and hence an isomorphism.

Place your bets, ladies and gents

Unsurprisingly, the answer is that, in general, Φ (as defined on Slide 31) is not surjective. This is already so in the fundamental case of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$:

The only automorphism of a numerical monoid is the identity. Yet, the automorphism group of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is non-trivial, because it contains the reversion map $\text{rev}\colon \mathcal{P}_{\text{fin},0}(\mathbb{N}) \to \mathcal{P}_{\text{fin},0}(\mathbb{N})\colon X \mapsto \max X - X$.

What may be, however, surprising is that $\text{Aut}(\mathcal{P}_{\text{fin},0}(\mathbb{N}))$ is... small:

Theorem (T. & Yan · JCTA, 2025)

The only non-trivial automorphism of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is the reversion map.

Somehow, this hints that homomorphisms are not the "right morphisms" when it comes, say, to additive problems in the integers[22]. Moreover:

Conjecture

If H is a numerical monoid $\neq \mathbb{N}$, then $\text{Aut}(\mathcal{P}_{\text{fin},0}(H))$ is trivial.

---

[22] A better alternative is offered by Freiman homomorphisms (see, e.g., Sects. 2.8, 3.1, and 4.5 and Chap. 20 in D. Grynkiewicz, *Structural Additive Theory*, Springer, 2013.

A characterization

In fact, things are even more surprising if we consider the next:

Theorem (T. & Yan · JCTA, 2025)

The following are equivalent for an endomorphism f of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$:

(a) f is injective and $f(\{0,1\}) = \{0,1\}$.

(b) f is surjective.

(c) f is an automorphism.

One simple consequence of the previous theorem is the following:

Corollary (T. & Yan · JCTA, 2025)

If f is an automorphism of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$, then the following hold:

(i) $\max X = \max f(X)$ for every $X \in \mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$.

(ii) $\{0,k\}$ and $[\![0,k]\!]$ are fixed points of f for all $k \in \mathbb{N}$.

(iii) Either $f(\{0,2,3\}) = \{0,1,3\}$ or $f(\{0,2,3\}) = \{0,2,3\}$.

Hidden symmetries

In turn, one consequence of the corollary on the previous slide is that every automorphism f of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ gives rise to a well-defined function

$$f^*\colon \mathcal{P}_{\text{fin},0}(\mathbb{N}) \to \mathcal{P}_{\text{fin},0}(\mathbb{N})\colon\ \max X - f(X),$$

henceforth referred to as the reversal of f.

Interestingly enough, f^* is something more than just a function (which reveals the existence of a "hidden symmetry" in the problem):

Lemma

The reversal of an automorphism of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is itself an automorphism.

In particular, the reversion map (Slide 32) is the reversal of the identity.

It follows that the automorphism group of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is determined by those automorphisms that fix the set $\{0, 2, 3\}$.

Thus, we are *naturally* led to consider the behavior of the automorphisms of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ w.r.t. the sets of the form $\{0, a, a+1\}$ with $a \in \mathbb{N}$.

A non-standard induction

Based on the previous slides, proving that the only non-trivial automorphism of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is the reversion map comes down to showing that, if $\{0,2,3\}$ is a fixed point of an automorphism f of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$, then f is the identity.

The proof is essentially an induction on the boxing dimension of X, where we let the boxing dimension $\text{b.dim}(S)$ of a set $S \subseteq \mathbb{Z}$ be the smallest integer $k \ge 0$ for which there exist k (discrete) intervals whose union is S, with the understanding that if no such k exists then $\text{b.dim}(S) := \infty$.

It is obvious that, for all $X, Y \subseteq \mathbb{Z}$,

$$\text{b.dim}(X \cup Y) \le \text{b.dim}(X) + \text{b.dim}(Y), \tag{4}$$

a property we refer to as *subadditivity*.

The induction basis comes down to the observation that the boxing dimension of a set $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ is 1 iff X is an interval (and we already know from item (ii) of the corollary on Slide 33 that intervals are fixed by *any* automorphism).

We then prove certain identities on sumsets which, when combined with Eq. (4), make it possible to perform the inductive step and complete the proof.

Outline

Semigroups of ideals

A *non-empty* subset I of a sgrp S is called

- an ideal (of S) if $IS \subseteq I$ and $SI \subseteq I$;
- a finitely generated (shortly, f.g.) ideal if $I = \widehat{S}X\widehat{S}$ for some $X \in \mathcal{P}_{\rm fin}(S)$, where $\widehat{S}$ denotes a (conditional) unitization of S (i.e., we add an identity only if necessary).
- a principal ideal if $I = \widehat{S}a\widehat{S}$ for some $a \in S$.

Each of the following is a subsgrp of the large power sgrp $\mathcal{P}(S)$ of S:

- $\mathfrak{I}(S) := \{I \in \mathcal{P}(S) \colon I \text{ is an ideal}\}$, the ideal semigroup of S.
- $\mathfrak{I}_{\rm fin}(S) := \text{Sgrp}\langle\{I \in \mathfrak{I}(S) \colon I \text{ is f.g.}\}\rangle_{\mathcal{P}(S)}$, the finitary ideal semigroup of S.
- $\mathfrak{P}(S) := \text{Sgrp}\langle\{I \in \mathfrak{I}(S) \colon I \text{ is principal}\}\rangle_{\mathcal{P}(S)}$, the principal ideal semigroup of S.

Some remarks:

- The setwise product of two f.g. (resp., principal) ideals need not be f.g. (resp., principal).
- $\mathfrak{P}(S)$ is a subsemigroup of $\mathfrak{I}_{\rm fin}(S)$, and $\mathfrak{I}_{\rm fin}(S)$ is a subsemigroup of $\mathfrak{I}(S)$.
- If S is a monoid, then each of $\mathfrak{I}(S)$, $\mathfrak{I}_{\rm fin}(S)$, and $\mathfrak{P}(S)$ is a submonoid of $\mathcal{P}(S)$ whose neutral element is S (hence not a *unital* submonoid unless S is trivial).

Problems and troubles

In the spirit of the Tamura–Shafer problem (Slide 13), we have the following:

Problem 5 (tentative).

Find sufficient/necessary conditions on the sgrps H and K so that

1. $\mathfrak{I}(H) \simeq \mathfrak{I}(K)$ iff $H \simeq K$, or
2. $\mathfrak{I}_{\rm fin}(H) \simeq \mathfrak{I}_{\rm fin}(K)$ iff $H \simeq K$.

The "if" condition is trivial: given a (sgrp) isomorphism $f \colon H \to K$,

$$\bar{f} \colon \mathcal{P}(H) \to \mathcal{P}(K) \colon X \mapsto f[X] := \{f(x) \colon x \in X\}$$

is itself an isomorphism, with the additional property that

$$\bar{f}[\mathfrak{I}(H)] = \mathfrak{I}(K), \quad \bar{f}[\mathfrak{I}_{\rm fin}(H)] = \mathfrak{I}_{\rm fin}(K), \quad \text{and} \quad \bar{f}[\mathfrak{P}(H)] = \mathfrak{P}(K).$$

The "only if" condition is troubles: groups have *one* non-empty ideal, which implies that there are trivial obstructions to a positive answer to Problem 5.

What to do? One possible approach is to relax the "only if" condition and require that H and K be isomorphic modulo a (natural) congruence.

Same up to associates

Denote by S_{red} the reduced quotient of S, i.e., the factor sgrp given by the quotient of S by the smallest (sgrp) congruence containing all pairs $(x, y) \in S \times S$ s.t. $\widehat{S}x\widehat{S} = \widehat{S}y\widehat{S}$ (associated elements or associates).

In a cancellative[(23)] commutative monoid H, x and y are associated iff $xH^\times = yH^\times$; and in some situations[(24)], it is natural to identify H with the quotient $H/H^\times$. So we are led to the following:

Problem 6 (García–Sánchez & T. · PAMS, 202*).

Find sufficient/necessary conditions on the sgrps H and K so that

1. $\mathfrak{I}(H) \simeq \mathfrak{I}(K) \implies H_{\text{red}} \simeq K_{\text{red}}$.
2. $\mathfrak{I}_{\text{fin}}(H) \simeq \mathfrak{I}_{\text{fin}}(K) \implies H_{\text{red}} \simeq K_{\text{red}}$.

The problem is already challenging in the cancellative commutative setting, and almost nothing appears to be known[(25)].

(23) Recall that S is cancellative if $ax \neq ay$ and $xa \neq ya$ for all $a, x, y \in S$ with $x \neq y$.
(24) E.g., in the study of the arithmetic of commutative monoids/(unital) rings.
(25) There are a couple of results where the isomorphism $\mathfrak{I}(H) \to \mathfrak{I}(K)$ is assumed to be isotone wrt the inclusion order, see, e.g., [Kuroki, Proc. Japan Acad. **47**, 1971].

The beginning and the end

Our original goal. Solve Problem 6 in the case where H and K are numerical monoids, i.e., submonoids of $(\mathbb{N}, +)$ with finite complement in $\mathbb{N}$.

Numerical monoids are cancellative commutative monoids. Moreover, they are [strongly] Archimedean, where the sgrp S is

- Archimedean if, for all $a, b \in S$ with $b \notin \widehat{S}^\times$, there exists $k \in \mathbb{N}^+$ with $b^k \in \widehat{S}a\widehat{S}$;
- strongly Archimedean if, for each non-unit $a \in \widehat{S}$, there exists $k \in \mathbb{N}^+$ s.t. any product of any k non-units of $\widehat{S}$ lies in $\widehat{S}a\widehat{S}$.

This prompted us to tackle a more general case:

How it ended. Give a positive solution to Problem 2.1 in the case where H and K are strongly Archimedean, cancellative, duo monoids; and to Problem 2.2 in the case where H and K are Archimedean, cancellative, duo monoids.

Recall that the sgrp S is duo if $aS = Sa$ for all $a \in S$.

Question. Trivially enough, groups are strongly Archimedean, cancellative, and duo. Any non-trivial non-commutative examples? Yes, see the next slide!

Strolling through the skew fields

Let R be a right discrete valuation domain, i.e., a domain with a non-unit $p \in R$ s.t. every non-zero element $a \in R$ can be written in the form $p^n u$, where n is a non-negative integer and $u \in R^\times$ (= the group of units of R).

If, in addition, $aR^\times = R^\times a$ for every $a \in R$, then $R^\bullet := R \setminus \{0_R\}$ is a strongly Archimedean, cancellative, duo monoid.

Special case: Let R be the ring of formal power series in one variable x over a skew field F, with multiplication twisted by a (ring) automorphism σ of F in such a way that $ax = x\sigma(a)$ for every $a \in F$.

By Exercise 19.7 in [Lam, *Exercises in Classical Ring Theory*, Springer-Verlag, 2003 (2nd ed.)], R is a right discrete valuation domain.

On the other hand, a formal power series $f = \sum_{k \in \mathbb{N}} a_k x^k \in R$ is a unit iff a_0 is not the zero element 0_F of F. It follows that

$$xR^\times = R^\times x,$$

which implies in turn that $gR^\times = R^\times g$ for every $g \in R$.

Therefore, $R^\bullet$ is a strongly Archimedean, cancellative, duo monoid; and it is commutative iff σ is the trivial automorphism.

The strongly Archimedean case

The key step is provided by the following theorem, along with the fact that if S is a duo semigroup, then $S_{\mathrm{red}} \simeq \mathfrak{P}(S)$ ($=$ the principal ideal sgrp of H).

Theorem (García–Sánchez & T. · PAMS, 202*).

If H and K are strongly Archimedean, cancellative, duo monoids, then every isomorphism $\mathfrak{I}(H) \to \mathfrak{I}(K)$ restricts to an isomorphism $\mathfrak{P}(H) \to \mathfrak{P}(K)$.

This, in turn, descends from a characterization of strongly Archimedean monoids in terms of a structural property of their ideal semigroup:

Proposition

The following conditions are equivalent for a duo monoid H:

(a) H is strongly Archimedean.

(b) Any non-trivial divisor-closed subsemigroup of $\mathfrak{I}(H)$ contains $\mathfrak{P}(H)$.

Here, we say that a subsemigroup T of the semigroup S is divisor-closed if

$$(a \in T \quad \text{and} \quad b \in \widehat{S} a \widehat{S}) \implies b \in T.$$

The Archimedean case

We use the same approach, but are forced to restrict to f.g. ideals:

Theorem (García–Sánchez & T. · PAMS, 202*).

If H and K are Archimedean, cancellative, duo monoids, then every isomorphism $\mathfrak{I}_{\rm fin}(H) \to \mathfrak{I}_{\rm fin}(K)$ restricts to an isomorphism $\mathfrak{P}(H) \to \mathfrak{P}(K)$.

Similarly as in the strongly Archimedean case, the proof is ultimately based on a characterization of Archimedean monoids in terms of a structural property of their *finitary* ideal semigroup:

Proposition

The following are equivalent for a *cancellative*, duo monoid H:

(a) H is Archimedean.

(b) Every non-trivial divisor-closed submonoid of $\mathfrak{I}_{\rm fin}(H)$ contains $\mathfrak{P}(H)$.

A remarkable difference between these results and their strongly Archimedean analogues (Slide 42) is that, in the proof of the latter, we can do *without* cancellativity. **It is open** whether the same is possible in the Archimedean case.

Keep It Simple 'n Sweet

The following results are straightforward from the previous theorems.

Corollary 1.

If H and K are numerical monoids with $\mathfrak{I}(H) \simeq \mathfrak{I}(K)$, then $H = K$.

Proof.

Every numerical monoid is strongly Archimedean. Thus, $H_{\mathrm{red}} \simeq K_{\mathrm{red}}$ by the results of Slide 42. It follows that $H \simeq K$, because for a cancellative, commutative, monoid M with trivial group of units (e.g., a numerical monoid) the canonical projection $M \to M_{\mathrm{red}}$ is an isomorphism (the congruence classes are singletons). This finishes the proof, for two numerical monoids are isomorphic iff they are equal (as already noted on Slide 27). ■

Recall from Slide 29 that a rational Puiseux monoid is a submonoid of $(\mathbb{Q}_{\geq 0}, +)$. These monoids are cancellative, commutative, and Archimedean, but need not be strongly Archimedean.

Corollary 2.

If H and K are rational Puiseux monoids with $\mathfrak{I}_{\mathrm{fin}}(H) \simeq \mathfrak{I}_{\mathrm{fin}}(K)$, then $H \simeq K$.

Back again to the origin

The last result provides a positive answer to the Tamura–Shafer problem for a new, albeit rather special, class of *cancellative* semigroups.

The result is a complement to Theorem 1 of [T., 2025] (`arXiv:2402.11475`), which solves a stronger version of the Tamura–Shafer problem[26] in the positive for the class of cancellative *commutative* semigroups.

Theorem (García–Sánchez & T. · PAMS, 202*).

If H and K are strongly Archimedean, cancellative, duo monoids and either of them has a trivial group of units, then every isomorphism $\mathcal{P}(H) \to \mathcal{P}(K)$ restricts to an isomorphism $\mathfrak{I}(H) \to \mathfrak{I}(K)$, whence $\mathcal{P}(H) \simeq \mathcal{P}(K)$ iff $H \simeq K$.

Notice that a strongly Archimedean, cancellative, duo monoid with trivial group of units need not be commutative:

- The non-units of a *cancellative* duo monoid form a duo (sub)sgrp. It follows that any unitization of the non-units of a strongly Archimedean, cancellative, duo monoid is a strongly Archimedean, cancellative, duo monoid with trivial group of units; and it only remains to use the construction (with formal power series) from Slide 41.

[26] Kobayashi's problem (1984): Prove or disprove that, for any two sgrps H and K in a certain class $\mathcal{O}$, every isomorphism $\mathcal{P}(H) \to \mathcal{P}(K)$ maps singletons to singletons.

Outline

References

- A. A. Antoniou & S. Tringali, *On the Arithmetic of Power Monoids and Sumsets in Cyclic Groups*, Pacific J. Math. **312** (2021), No. 2, 279–308 (arXiv:1804.10913).
- P.-Y. Bienvenu & A. Geroldinger, *On algebraic properties of power monoids of numerical monoids*, Israel J. Math. (2025). DOI: 10.1007/s11856-024-2683-0 (arXiv:2205.00982).
- L. Cossu & S. Tringali, *Abstract Factorization Theorems with Applications to Idempotent Factorizations*, Israel J. Math **263** (2024), 349–395 (arXiv:2108.12379).
- L. Cossu & S. Tringali, *Factorization under local finiteness conditions*, J. Algebra **630** (Sep 2023), 128–161 (arXiv:2208.05869).
- Y. Fan & S. Tringali, *Power monoids: A bridge between Factorization Theory and Arithmetic Combinatorics*, J. Algebra **512** (2018), 252–294 (arXiv:1701.09152).
- P. A. García-Sánchez & S. Tringali, *Semigroups of ideals and isomorphism problems*, Proc. Amer. Math. Soc., to appear (arXiv: 2410.15622).
- S. Tringali, *An abstract factorization theorem and some applications*, J. Algebra **602** (July 2022), 352–380 (arXiv:2102.01598).
- S. Tringali, "On the isomorphism problem for power semigroups", to appear in M. Brešar, A. Geroldinger, B. Olberding, and D. Smertnig (eds.), *Recent Progress in Ring and Factorization Theory*, Springer Proc. Math. Stat. **477**, Springer, 2025 (arXiv: 2402.11475).
- S. Tringali & W. Yan, *A conjecture by Bienvenu and Geroldinger on power monoids*, Proc. Amer. Math. Soc., to appear (arXiv:2310.17713).
- S. Tringali & W. Yan, *On power monoids and their automorphisms*, J. Comb. Theory Ser. A **209** (2025), #105961, 16 pp. (arXiv:2312.04439).