Congruence Preservation, Lattices and Recognizability

Patrick Cégielski[1,3]   Serge Grigorieff[2,3]   Irène Guessarian[2,3,4]

December 14, 2017

To Yuri, on his 70th birthday, with gratitude for sharing with us his beautiful mathematical ideas during our long friendship

Abstract

Looking at some monoids and (semi)rings (natural numbers, integers and p-adic integers), and more generally, residually finite algebras (in a strong sense), we prove the equivalence of two ways for a function on such an algebra to behave like the operations of the algebra. The first way is to preserve congruences or stable preorders. The second way is to demand that preimages of recognizable sets belong to the lattice or the Boolean algebra generated by the preimages of recognizable sets by "derived unary operations" of the algebra (such as translations, quotients,...).

Contents

[1]LACL, EA 4219, Université Paris-Est Créteil, IUT Sénart-Fontainebleau, France `cegielski@u-pec.fr`

[2]IRIF, UMR 8243, Université Paris 7 Denis Diderot, France `FirstName.LastName@irif.fr`

[4]Emeritus at UPMC Université Paris 6

1 Motivation and overview of the paper

In [2], we proved that if $f : \mathbb{N} \longrightarrow \mathbb{N}$ is non decreasing then conditions (1) and (2) are equivalent

(1) (a) for all $a, b \in \mathbb{N}$, $a - b$ divides $f(a) - f(b)$, and

    (b) for all $a \in \mathbb{N}$, $f(a) \geq a$,

(2) every lattice $\mathcal{L}$ of regular subsets of $\mathbb{N}$ which is closed under $x \mapsto x - 1$, i.e., $L \in \mathcal{L}$ implies $\{n \mid n + 1 \in L\} \in \mathcal{L}$, is also closed under f^{-1}, i.e., for every $L \in \mathcal{L}$, $f^{-1}(L) = \{n \in \mathbb{N} \mid f(n) \in L\} \in \mathcal{L}$.

    For which (semi)rings does this property hold? For instance, does it hold for the ring of integers $\mathbb{Z}$ or the rings of p-adic integers $\mathbb{Z}_p$? To extend this property to diverse structures, we begin by rewriting the two conditions (1) and (2) in more algebraic terms.

    Observing that condition (1) is equivalent to the notion of "congruence preservation" (Section 3.3 Theorem 3.12) in the case of $\mathbb{N}$, we will use the latter notion of congruence preservation instead of condition (1). The general notion of congruence preservation is defined in Definition 2.5 for arbitrary algebras. This will allow to consider general algebras in the sense of universal algebra instead of just (semi)rings.

    Moreover, as regular subsets coincide with recognizable subsets for $\mathbb{N}$ (Remark 2.19), we will use "recognizable" subsets in condition **(2)** (see Section 2.3) instead of regular subsets, again leading to an algebraic statement also suitable for general algebras.

    The above equivalence can thus be restated for the original case $\langle \mathbb{N}; +, \times \rangle$ as

Theorem 1.1. *If $f : \mathbb{N} \longrightarrow \mathbb{N}$ is non decreasing then conditions (1) and (2) below are equivalent*

(1) *f is congruence preserving on $\langle \mathbb{N}; +, \times \rangle$ and, for all $a \in \mathbb{N}$, $f(a) \geq a$*

(2) *for every recognizable subset L of $\langle \mathbb{N}; +, \times \rangle$ the smallest lattice of subsets of $\mathbb{N}$ containing L and closed under $x \mapsto x - 1$ is also closed under f^{-1}.*

In the present paper, we try and generalize Theorem 1.1 as much as possible: i.e., for which classes of algebras does a similar Theorem hold? We investigate in a general framework the relationships between congruence preservation, recognizability and lattices or Boolean algebras of recognizable sets.

Formal definitions are recalled in Section 2. Besides the usual universal algebra notion of congruence preservation, we consider a similar notion of stable preorder preservation. We also extend to general algebras the notions of recognizability, syntactic preorder and syntactic congruence from language theory.

In Section 3, we prove Theorem 1.1 (cf. Theorem 3.22 in Section 3.5). To this end, using the characterization of congruences on $\langle \mathbb{N}; + \rangle$ (Sections 3.1 and 3.2) we prove that congruence preserving functions on $\langle \mathbb{N}; + \rangle$ are exactly those satisfying conditions **(1) (a)** and **(b)** supra, a result interesting per se (Theorem 3.12, Section 3.3). Functions satisfying condition **(1) (a)** on $\langle \mathbb{N}; + \rangle$ have been characterized in [3]. They can be very complex, for instance $x \mapsto$ if $x = 0$ then 1 else $\lfloor ex! \rfloor$ satisfies conditions **(1) (a)** and **(b)**. In Section 3.4 we prove that stable preorder preserving functions on $\langle \mathbb{N}; + \rangle$ are exactly the non decreasing congruence preserving functions (Theorem 3.20). All these results on $\langle \mathbb{N}; + \rangle$ hold on $\langle \mathbb{N}; +, \times \rangle$. In Section 3.6, we generalize Theorem 1.1 to the monoid $\langle \mathbb{N}; \times \rangle$. Moreover, we give a very simple characterization of the corresponding subclass of congruence preserving functions: this subclass consists of all monomial functions $x \mapsto kx^n$ (Theorem 3.23).

We prove our main results in Section 4. We consider variants of Theorem 1.1 for algebras as general as possible and a version of condition **(2)** of Theorem 1.1 involving the lattices $\mathcal{L}_{\mathcal{A}}(L)$ and the Boolean algebras $\mathcal{B}_{\mathcal{A}}(L)$ of preimages of a recognizable set L by derived unary operations of the algebra (such as translations, quotients,..., cf. Definition 2.21). Our results show that congruence preservation of a function f is related to the condition that $f^{-1}(L)$ belongs to the Boolean algebra $\mathcal{B}_{\mathcal{A}}(L)$ for all recognizable L whereas stable preorder preservation is related to the condition that $f^{-1}(L)$ belongs to the lattice $\mathcal{L}_{\mathcal{A}}(L)$. Theorem 4.3 is a general wild version of Theorem 1.1 relating stable preorder preserving functions to the condition $f^{-1}(L)$ belongs to the complete lattice variant of $\mathcal{L}_{\mathcal{A}}(L)$ for all sets L. Theorem 4.11 in section 4.3 shows that, on any algebra, stable preorder preserving functions satisfy $f^{-1}(L) \in \mathcal{L}_{\mathcal{A}}(L)$ for recognizable L. The reciprocal is true for sp-residually finite algebras (a strong variant of residual finiteness, cf. Definition 4.6). Avatars with congruence preservation and the Boolean algebra $\mathcal{B}_{\mathcal{A}}(L)$ are stated in Theorems 4.5 and 4.13. In case the algebra contains a group operation and satisfies a strong form of residual finiteness it turns out that all the conditions considered in the paper are equivalent.

Section 5 is devoted to $\langle \mathbb{Z}; +, \times \rangle$ to which Theorem 4.11 applies, giving Theorem 5.10 in Section 5.5. Though the congruence preserving functions can be very intricate [4], for instance,

$$f(n) = \begin{cases} \sqrt{\dfrac{e}{\pi}} \times \dfrac{\Gamma(1/2)}{2 \times 4^n \times n!} \displaystyle\int_1^\infty e^{-t/2}(t^2 - 1)^n dt & \text{for } n \geq 0 \\ -f(|n| - 1) & \text{for } n < 0 \end{cases},$$

the lattices $\mathcal{L}_{\langle \mathbb{Z}; +, \times \rangle}(L)$ for L recognizable are very simple, cf. Lemma 5.8 in Section 5.4.

In Section 6, congruence preservation for the rings of p-adic integers is treated similarly (Proposition 6.10, section 6.4).

2 Preliminary definitions

We here recall the useful definitions, notations and prove basic results.

2.1 Stable relations and congruences on an algebra

Definition 2.1. An algebra $\mathcal{A} = \langle A; \Xi \rangle$ consists of a nonempty carrier set A together with a set of operations Ξ, each $\xi \in \Xi$ is a mapping $\xi \colon A^{ar(\xi)} \to A$ where $ar(\xi) \in \mathbb{N}$ is the arity of ξ.

Definition 2.2. Let A be a set and let f be a function $f \colon A^p \longrightarrow A$. A binary relation ρ on A is said to be compatible with f if and only if, for all elements $x_1, \ldots, x_p, y_1, \ldots, y_p$ in A

$$(x_1 \rho\, y_1 \ \wedge \cdots \wedge \ x_p \rho\, y_p) \quad \Longrightarrow \quad f(x_1, \ldots, x_p) \, \rho \, f(y_1, \ldots, y_p) \tag{1}$$

Definition 2.3. A binary relation ρ on A is said to be stable on the algebra $\mathcal{A} = \langle A; \Xi \rangle$ if it is compatible with each operation $\xi \in \Xi$, i.e., if ξ is n-ary then, for all $x_1, \ldots, x_n, y_1, \ldots, y_n$ in A

$$(x_1 \rho\, y_1 \ \wedge \cdots \wedge \ x_n \rho\, y_n) \quad \Longrightarrow \quad \xi(x_1, \ldots, x_n) \, \rho \, \xi(y_1, \ldots, y_n) \tag{2}$$

Definition 2.4. A stable equivalence relation on $\mathcal{A}$ is called an $\mathcal{A}$-congruence. If there are finitely many equivalence classes, it is said to be a finite index congruence.

2.2 Congruence and stable (pre)order preservation

2.2.1 Definitions

The substitution property, introduced by Grätzer in [7] page 44, has since been renamed congruence preservation in the literature. We shall also use an extension dealing with (pre)orders instead of congruences.

Definition 2.5. Let $\mathcal{A} = \langle A; \Xi \rangle$ be an algebra.

1) A function $f \colon A^p \longrightarrow A$ is $\underline{\mathcal{A}\text{-congruence preserving}}$ if all $\mathcal{A}$-congruences are compatible with f, i.e., for every congruence $\sim$ on $\mathcal{A}$ and all elements $x_1, \ldots, x_p$, $y_1, \ldots, y_p$ in A

$$(x_1 \sim y_1 \ \wedge \cdots \wedge \ x_p \sim y_p) \quad \Longrightarrow \quad f(x_1, \ldots, x_p) \sim f(y_1, \ldots, y_p). \qquad (3)$$

2) A function $f \colon A^p \longrightarrow A$ is $\underline{\mathcal{A}\text{-stable (pre)order preserving}}$ if all $\mathcal{A}$-stable (pre)orders are compatible with f, i.e., for every stable (pre)order $\preceq$ on $\mathcal{A}$ and all elements $x_1, \ldots, x_p, y_1, \ldots, y_p$ in A

$$(x_1 \preceq y_1 \ \wedge \cdots \wedge \ x_p \preceq y_p) \quad \Longrightarrow \quad f(x_1, \ldots, x_p) \preceq f(y_1, \ldots, y_p). \qquad (4)$$

When the algebra $\mathcal{A}$ is clear from the context, f is simply said to be $\underline{\text{congruence preserving}}$ (resp. $\underline{\text{stable (pre)order preserving}}$).

Congruences and congruence preservation can also be defined in terms of morphisms.

Definition 2.6. For $f \colon A \to B$, the kernel $Ker(f)$ of f is defined by $Ker(f) = \{(x, y) \mid f(x) = f(y)\}$.

Lemma 2.7. *1) A binary relation on $\mathcal{A}$ is a congruence if and only if it is the $\underline{kernel}$ $Ker(\varphi) = \{(x, y) \mid \varphi(x) = \varphi(y)\}$ of some homomorphism $\varphi \colon A \to B$ onto some algebra $\mathcal{B}$.*

2) $f \colon A \to A$ is congruence preserving if and only if, for every homomorphism $\varphi \colon A \to B$, $Ker(\varphi) \subseteq Ker(\varphi \circ f)$.

The next result shows that congruence preserving functions somehow extend operations of the algebra.

Proposition 2.8. *Let $\mathcal{A} = \langle A; \Xi \rangle$ be an algebra and let $f : A^n \to A$ with $n \geq 1$. The following conditions are equivalent:*

 (i) *f is $\mathcal{A}$-congruence preserving,*

 (ii) *For every algebra $\mathcal{B} = \langle B; \Theta \rangle$ having the same signature as $\mathcal{A}$ and every surjective morphism $\varphi \colon A \to B$ there exists a unique function $f_\varphi \colon B^n \to B$ such that $\varphi(f(x_1, \ldots, x_n)) = f_\varphi(\varphi(x_1), \ldots, \varphi(x_n))$, (i.e., φ is also a morphism between the algebras $\langle A; \Xi \cup \{f\} \rangle$ and $\langle B; \Theta \cup \{f_\varphi\} \rangle$, namely the diagram of Figure 1 is commutative).*

Proof. $(i) \Longrightarrow (ii)$ Assume (i). As φ is a morphism, $Ker(\varphi)$ is the congruence: $x \sim y$ if and only if $\varphi(x) = \varphi(y)$; as f is congruence preserving, $\varphi(x_i) = \varphi(y_i)$ for $1 \leq i \leq n$ implies $\varphi(f(x_1, \ldots, x_n)) = \varphi(f(y_1, \ldots, y_n))$ hence f_φ is well defined and equal to the common value of all the $\varphi(f(y_1, \ldots, y_n))$ for y_i's such that $\varphi(y_i) = \varphi(x_i)$.

$(ii) \Longrightarrow (i)$ Assume (ii). Let $\sim$ be a congruence on A and let $\mathcal{B} = \langle A/\sim; \Xi/\sim \rangle$ be the quotient algebra. The canonical quotient map $\varphi \colon A \to A/\sim$ is a surjective

$$\begin{array}{ccc} A^n & \xrightarrow{\quad f \quad} & A \\ {\scriptstyle(\varphi,\ldots,\varphi)}\big\downarrow & & \big\downarrow{\scriptstyle\varphi} \\ B^n & \xrightarrow{\quad f_\varphi \quad} & B \end{array}$$

Figure 1: From $f \colon A^n \to A$ to $f_\varphi \colon B^n \to B$

morphism. By (ii), f factors through $A/\sim$ to f_φ. In particular, if $y_i \sim x_i$ for $1 \leq i \leq n$ then $\varphi(y_i) = \varphi(x_i)$ hence $f_\varphi(\varphi(y_1), \ldots, \varphi(y_n)) = f_\varphi(\varphi(x_1), \ldots, \varphi(x_n))$. Using (ii), we get $\varphi(f(y_1, \ldots, y_n)) = \varphi(f(x_1, \ldots, x_n))$, i.e., $f(y_1, \ldots, y_n) \sim f(x_1, \ldots, x_n)$. Hence f preserves congruences. $\qquad\square$

2.2.2 Reduction from arity n to arity one

Congruence preservation of a function of arbitrary arity can be characterized via congruence preservation of its restrictions to unary functions. This enables us to simplify some proofs.

Reducing to unary functions is also a key point in the definition of recognizability, syntactic congruences and syntactic preorders for general algebras.

Definition 2.9. Given $n \geq 2$, a n-ary $f : A^n \to A$, an index $i \in \{1, \ldots, n\}$, and $\vec{c} = (c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n) \in A^{n-1}$, we denote by $f_i^{\vec{c}}$ the unary function $A \to A$ (called the <u>frozen function</u> of f relative to $i, \vec{c}$) obtained by fixing all arguments to $\vec{c}$ except the i-th one. In other words,

$$f_i^{\vec{c}}(x) = f(c_1, \ldots, c_{i-1}, x, c_{i+1}, \ldots, c_n).$$

Lemma 2.10. *1) An equivalence relation (resp. (pre)order) is compatible with an n-ary function $f \colon A^n \longrightarrow A$ if and only if for all $i \in \{1, \ldots, n\}$, for all $\vec{c} = (c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n) \in A^{n-1}$, it is compatible with the unary function $f_i^{\vec{c}}$.*

2) Given an algebra $\mathcal{A} = \langle A; \Xi \rangle$, a n-ary function $f \colon A^n \longrightarrow A$ is $\mathcal{A}$-congruence preserving (resp. $\mathcal{A}$-stable (pre)order preserving) if and only if for all $i \in \{1, \ldots, n\}$, for all $\vec{c} = (c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n) \in A^{n-1}$, the unary function $f_i^{\vec{c}}$ is $\mathcal{A}$-congruence preserving (resp. $\mathcal{A}$-stable (pre)order preserving).

Proof. We prove 1) for an equivalence $\sim$, the case of preorders is similar, and 2) is an immediate consequence of 1). The left to right implication in 1) is clear. For the converse implication, use the transitivity of $\sim$, e.g., assuming $n = 2$, if $\sim$ is compatible with $f_1^{a_1}$ and $f_2^{b_2}$, then $a_1 \sim b_1$ and $a_2 \sim b_2$ imply $f(a_1, a_2) \sim f(a_1, b_2)$ and $f(a_1, b_2) \sim f(b_1, b_2)$, hence $f(a_1, a_2) \sim f(b_1, b_2)$. $\qquad\square$

2.2.3 Syntactic congruence and preorder

To every subset of the carrier set of an algebra are associated a <u>syntactic congruence</u> and a <u>syntactic preorder</u>. Let us first define the notion of <u>derived unary operation</u>.

6

Definition 2.11. [Derived Unary Operations] Given $\mathcal{A} = \langle A; \Xi \rangle$, we denote by $DUO(\mathcal{A})$ the set of unary functions γ defined by composing frozen functions of the operations in Ξ, i.e., $\gamma = \xi_{1,j_1}^{\vec{c_1}} \circ \cdots \circ \xi_{n,j_n}^{\vec{c_n}}$ where $n \in \mathbb{N} \setminus \{0\}$, $i = 1, \ldots, n$, $\xi_i \in \Xi$, $1 \leq j_i \leq ar(\xi_i)$, and $\vec{c_i} \in A^{ar(\xi_i)-1}$. For $n = 0$, γ is the identity on A.

Example 2.12. 1) For $\mathcal{A} = \langle \mathbb{N}; + \rangle$, $DUO(\mathcal{A})$ is the set of translations $x \mapsto x + a$, for $a \in \mathbb{N}$.

2) For $\mathcal{A} = \langle \mathbb{N} \setminus \{0\}; \times \rangle$ (resp. $\mathcal{A} = \langle \mathbb{N}; \times \rangle$), $DUO(\mathcal{A})$ is the set of homotheties $x \mapsto ax$, with $a \geq 1$ (resp. $a \in \mathbb{N}$).

3) For $\mathcal{S} = \langle \Sigma^*; \cdot \rangle$, the algebra of words with concatenation, $DUO(\mathcal{A})$ is the set of left and right multiplications by words $x \mapsto w \cdot x \cdot w'$ for $w, w' \in \Sigma^*$.

Using the notion of Derived Unary Operations, we can define the syntactic preorder and syntactic congruence associated with L.

Definition-Lemma 2.13. *For $L \subseteq A$, the relation $\leq_L$ defined by*

$$x \leq_L y \quad \text{if and only if} \quad \forall \gamma \in DUO(\mathcal{A}) \quad \big(\gamma(y) \in L \Longrightarrow \gamma(x) \in L\big) \qquad (5)$$

is a stable preorder. It is called the syntactic preorder associated with L.
   The relation $\sim_L$ defined by

$$x \sim_L y \quad \text{if and only if} \quad \forall \gamma \in DUO(\mathcal{A}) \quad \big(\gamma(x) \in L \Longleftrightarrow \gamma(y) \in L\big) \qquad (6)$$

is the congruence associated with the preorder $\leq_L$. It is called the syntactic congruence associated with L.

Proof. It is clear that $\leq_L$ is reflexive and transitive. Also, if $x \leq_L y$ and $\delta \in DUO(\mathcal{A})$ then equation (5) (applied with the composition $\gamma \circ \delta$) insures that for all $\gamma \in DUO(\mathcal{A})$ we have $\gamma(\delta(x)) \in L \iff \gamma(\delta(x)) \in L$; hence $\delta(x) \leq_L \delta(y)$. Applying Lemma 2.10, we see that $\leq_L$ is a stable preorder.

Clearly, $\sim_L$ is reflexive, symmetric and transitive, and it is the equivalence associated with $\leq_L$. By equation (6), we see that for all $\xi \in \Xi$, for $1 \leq i \leq ar(\xi)$ and $\vec{c} \in A^{ar(\xi)-1}$, $\xi_i^{\vec{c}}$ is compatible with $\sim_L$, hence Lemma 2.10 implies that for all $\xi \in \Xi$, ξ is compatible with $\sim_L$, i.e., $\sim_L$ is a congruence on $\langle A; \Xi \rangle$. $\qquad \square$

Remark 2.14. Recall, that in the algebra of words Σ^* with concatenation, (1) the frozen unary operations consist in adding a fixed prefix or suffix, (2) the family DUO consists of operations $x \mapsto uxv$ for fixed $u, v \in \Sigma^*$. if $L \subseteq \Sigma^*$ is a language then its syntactic congruence $x \sim_L y$ is defined by the condition $\forall u, v \in \Sigma^*$ ($uxv \in L \Leftrightarrow uyv \in L$). Our notion of syntactic congruence thus generalizes the usual notion of syntactic congruence in language theory.

Definition 2.15. A set is said to be saturated with respect to an equivalence if is is a union of equivalence classes.

Proposition 2.16 states some properties of syntactic congruences and preorders.

Proposition 2.16. *Let L be a subset of an algebra $\mathcal{A}$.*

1) If L is saturated for a congruence $\equiv$ of $\mathcal{A}$ then $\equiv$ refines the syntactic congruence $\sim_L$ of L, i.e., $x \equiv y$ implies $x \sim_L y$.

2) If L is an initial segment of a stable preorder $\preceq$ of $\mathcal{A}$ (i.e., if $b \in L$ and $x \preceq b$ then $x \in L$), then $\preceq$ refines the syntactic congruence $\leq_L$ of L, i.e., $x \preceq y$ implies $x \leq_L y$.

Proof. Assume $x \equiv y$. Since $\equiv$ is a congruence we have $\gamma(x) \equiv \gamma(y)$ for all $\gamma \in DUO(\mathcal{A})$. If L is saturated for $\equiv$ we then have $\gamma(x) \in L \Leftrightarrow \gamma(y) \in L$ hence $x \sim_L y$. Similar proof with a stable preorder. $\qquad\square$

2.3 Recognizability

Definition 2.17 (Recognizability)**.** Given $\mathcal{A} = \langle A; \Xi \rangle$ an algebra, a subset B of A is said to be Ξ-recognizable (or $\mathcal{A}$-recognizable) if there exists a finite algebra $\mathcal{M} = \langle M; \Theta \rangle$ with the same signature as $\mathcal{A}$ and a surjective morphism $\varphi : \mathcal{A} \to \mathcal{M}$ such that such that $B = \varphi^{-1}(\varphi(B))$, i.e., $B = \varphi^{-1}(T)$ for some subset T of M.

Recognizability can also be stated in terms of congruences.

Lemma 2.18. *Let B be a subset of A. The following are equivalent*
1) B is $\mathcal{A}$-recognizable,
2) B is saturated with respect to some finite index congruence of $\mathcal{A}$,
3) the syntactic congruence $\sim_B^s$ of B has finite index.

Proof. 1) $\Leftrightarrow$ 2). Let B be saturated with respect to some congruence defined by $Ker(\varphi)$ (cf. Lemma 2.7), then $B = \varphi^{-1}(\varphi(B))$. As $Ker(\varphi)$ has finite index, $M = \varphi(A)$ is finite and B is recognizable. Conversely, if B is recognizable, $B = \varphi^{-1}(\varphi(B))$ is saturated with respect to the congruence $Ker(\varphi)$. As $\varphi : \mathcal{A} \to \mathcal{M}$ with M finite, this congruence has a finite number of classes hence a finite index.

2) $\Rightarrow$ 3). Assume B is saturated for the finite index congruence $\equiv$. By Proposition 2.16, $\equiv$ refines $\sim_B^s$ hence $\sim_B^s$ also has finite index.

3) $\Rightarrow$ 2). Follows from the fact that B is saturated with respect to $\sim_B^s$. $\qquad\square$

Remark 2.19. Recall the difference between the notions of *recognizable* and *regular* subsets for a monoid X: a subset L of X is regular if it can be generated from finite subsets of X by unions, products and stars. It happens that the two notions coincide, e.g., in $\langle \mathbb{N}; + \rangle$ or in the free monoids.

2.4 Lattices and Boolean algebras of subsets closed under preimage

We denote by $\mathcal{P}(X)$ the class of subsets of X.

Definition 2.20. 1. A lattice (resp. complete lattice) $\mathcal{L}$ of subsets of a set E is a family of subsets of E such that $L \cap M$ and $L \cup M$ are in $\mathcal{L}$ whenever $L, M \in \mathcal{L}$ (resp. such that any nonempty but possibly infinite) union or intersection of subsets in $\mathcal{L}$ is in $\mathcal{L}$.

$\mathcal{L}$ is a <u>Boolean algebra</u> (resp. <u>complete Boolean algebra</u>) if it is a lattice (resp. complete lattice) also closed under complementation.

2. For $f : E \to E$, a lattice $\mathcal{L}$ of subsets of E is <u>closed under</u> f^{-1} if $f^{-1}(L) \in \mathcal{L}$ whenever $L \in \mathcal{L}$.

Definition 2.21. For $\mathcal{A} = \langle A; \Xi \rangle$ an algebra and $L \subseteq A$, we denote by $\mathcal{L}_{\mathcal{A}}(L)$ (resp. $\mathcal{L}_{\mathcal{A}}^{\infty}(L)$) the smallest sublattice (resp. complete sublattice) $\mathcal{L}$ of $\mathcal{P}(A)$ containing L and closed under the inverses of the *DUO*s: i.e., $\gamma^{-1}(Z) \in \mathcal{L}$, for all $Z \in \mathcal{L}$, for all $\gamma \in DUO$.

We denote by $\mathcal{B}_{\mathcal{A}}(L)$ (resp. $\mathcal{B}_{\mathcal{A}}^{\infty}(L)$) the Boolean algebra (resp. complete Boolean algebra) similarly defined.

Example 2.22. 1) If $\mathcal{A} = \langle \mathbb{N}; Suc \rangle$, $\mathcal{L}_{\mathcal{A}}(L)$ is the smallest lattice containing L and closed under $(x \mapsto x + 1)^{-1}$, i.e., closed under decrement where $(L - 1) = \{n - 1 \mid n \in L, n - 1 \geq 0\} \in \mathcal{L}$, e.g., $\{0, 3, 7\} - 1 = \{2, 6\}$.

2) If $\mathcal{A}' = \langle \mathbb{N}; + \rangle$, $\mathcal{L}_{\mathcal{A}'}(L)$ is the smallest lattice containing L and closed under $(x \mapsto x + a)^{-1}$ for all $a \in \mathbb{N}$. Since this last closure amounts to closure under decrement, we have $\mathcal{L}_{\mathcal{A}}(L) = \mathcal{L}_{\mathcal{A}'}(L)$.

3) If $\mathcal{A}'' = \langle \mathbb{N}; \times \rangle$, $\mathcal{L}_{\mathcal{A}''}(L)$ is the smallest lattice containing L and closed under $(x \mapsto ax)^{-1}$, i.e., the set $L/a = \{n \mid an \in L\} \in \mathcal{L}$. For instance $\{0, 3, 7\}/3 = \{0, 1\}$.

4) If $\mathcal{S} = \langle \Sigma^*; \cdot \rangle$, $\mathcal{L}_{\mathcal{S}}(L)$ is the smallest lattice containing L and closed under $(x \mapsto w \cdot x \cdot w')^{-1}$ for $w, w' \in \Sigma^*$, i.e., the set $w^{-1} L w'^{-1} = \{x \mid w \cdot x \cdot w' \in L\} \in \mathcal{L}$.

Lemma 2.23 (Disjunctive Normal Form)**.** *1) Every set in $\mathcal{L}_{\mathcal{A}}^{\infty}(L)$ $\bigl(resp.\ \mathcal{L}_{\mathcal{A}}(L)\bigr)$ is of the form $\cup_{i \in I}\bigl(\cap_{\gamma \in \Gamma_i} \gamma^{-1}(L)\bigr)$ where the Γ_i's are subsets of DUO $\bigl(resp.\ with\ I$ and the Γ_i's finite$\bigr)$.*

2) Every set in $\mathcal{B}_{\mathcal{A}}^{\infty}(L)$ $\bigl(resp.\ \mathcal{B}_{\mathcal{A}}(L)\bigr)$ is of the form $\cup_{i \in I}\bigl(\cap_{\gamma \in \Gamma_i} \gamma^{-1}(L_{i,\gamma})\bigr)$ where $L_{i,\gamma}$ is either L or its complement $A \setminus L$, and the Γ_i's are as above.

Proof. 1) As $\cap$ and $\cup$ distribute over each other, and $\gamma^{-1}(\cup_{i \in I} L_i) = \cup_{i \in I} \gamma^{-1}(L_i)$, and similarly for $\cap$, every arbitrary (resp. finite) $\cap, \cup$ combination of the $\gamma^{-1}(L)$'s, $\gamma \in DUO$, can be put in a disjunctive normal form of the mentioned type. A similar argument proves 2). $\qquad\square$

Lemma 2.24. *Let $\mathcal{A}$ be an algebra and L be a subset of $\mathcal{A}$.*

1) Let $\sim$ be an $\mathcal{A}$-congruence. If L is $\sim$-saturated then so is every set in $\mathcal{B}_{\mathcal{A}}^{\infty}(L)$.

2) Let $\leq$ be an $\mathcal{A}$-stable preorder. If L is a $\leq$-initial segment then so is every set in $\mathcal{L}_{\mathcal{A}}^{\infty}(L)$.

Proof. 1) Since $\sim$ is an $\mathcal{A}$-congruence, if $x \sim y$ then $\gamma(x) \sim \gamma(y)$ for every $\gamma \in DUO$. In particular, if L is $\sim$-saturated then so is $\gamma^{-1}(L)$. Since $\sim$-saturation is closed under finite or infinite Boolean operations we conclude that all sets in $\mathcal{B}_{\mathcal{A}}^{\infty}(L)$ are $\sim$-saturated.

2) Argue similarly, observing that the family of initial segments is closed under finite or infinite union and intersection. $\qquad\square$

Lemma 2.25. *Let L be a subset of an algebra $\mathcal{A}$.*
1. The boolean algebra $\mathcal{B}_{\mathcal{A}}^{\infty}(L)$ is the family of subsets of A which are saturated for the syntactic congruence $\sim_L$ of L.
2. The lattice $\mathcal{L}_{\mathcal{A}}^{\infty}(L)$ is the family of subsets of A which are initial segments for the syntactic preorder $\leq_L$ of L.

Proof. 1) As L is $\sim_L$-saturated, Lemma 2.24 insures that every set in $\mathcal{B}_L^{\infty}(L)$ is also $\sim_L$-saturated. Conversely, for every element $x \in A$ the $\sim_L$-congruence class of x belongs to $\mathcal{B}_{\mathcal{A}}(L)$ since it is equal to

$$\{y \mid \forall \gamma \in DUO(\mathcal{A}) \ (\gamma(x) \in L \Leftrightarrow \gamma(y) \in L)\}$$
$$= \bigcap_{\gamma \in DUO(\mathcal{A})} \text{If } \gamma(x) \in L \text{ then } \gamma^{-1}(L) \text{ else } A \setminus \gamma^{-1}(L)$$

Finally, a $\sim_L$-saturated set is a union of $\sim_L$-congruence classes, hence also belongs to $\mathcal{B}_{\mathcal{A}}(L)$.

2) As L is a $\leq_L$-initial segment, Lemma 2.24 insures that every set in $\mathcal{L}_L^{\infty}(L)$ is also a $\leq_L$-initial segment. Conversely, for every element $x \in A$ the $\leq_L$-initial segment $I_x = \{y \mid y \leq_L x\}$ belongs to $\mathcal{L}_{\mathcal{A}}(L)$ since it is equal to

$$\{y \mid \forall \gamma \in DUO(\mathcal{A}) \ (\gamma(x) \in L \Rightarrow \gamma(y) \in L)\} = \bigcap_{\gamma \in DUO(\mathcal{A}), \ \gamma(x) \in L} \gamma^{-1}(L)$$

Finally, a $\leq_L$-initial segment X is the union of the I_x's for $x \in X$ hence also belongs to $\mathcal{L}_{\mathcal{A}}(L)$. □

Lemma 2.26. *If L is a recognizable subset of $\mathcal{A}$ then $\mathcal{L}_{\mathcal{A}}(L)$ and $\mathcal{B}_{\mathcal{A}}(L)$ are finite hence $\mathcal{L}_{\mathcal{A}}^{\infty}(L) = \mathcal{L}_{\mathcal{A}}(L)$ and $\mathcal{B}_{\mathcal{A}}^{\infty}(L) = \mathcal{B}_{\mathcal{A}}(L)$.*

Proof. If L is recognizable, then $\sim_L$ has a finite index k, there are k congruence classes and, as each $\gamma^{-1}(L)$ and each $A \setminus \gamma^{-1}(L)$, for $\gamma \in DUO(\mathcal{A})$, is a union of congruence classes of $\sim_L$ (cf. Lemma 2.13), there are at most 2^k sets $\gamma^{-1}(L)$ and $A \setminus \gamma^{-1}(L)$. Thus, the Boolean algebra $\mathcal{B}_{\mathcal{A}}(L)$ is finite hence it is complete and equal to $\mathcal{B}_{\mathcal{A}}^{\infty}(L)$. A fortiori, the lattice $\mathcal{L}_{\mathcal{A}}(L)$ is finite hence it is complete and equal to $\mathcal{L}_{\mathcal{A}}^{\infty}(L)$. □

Proposition 2.27. *If a lattice $\mathcal{L}$ of subsets of E is closed under f^{-1} then so is the Boolean algebra $\mathcal{B}$ of subsets of E generated by $\mathcal{L}$.*

As a consequence, in subsequent sections, every result of the form "$\mathcal{L}_{\mathcal{A}}(L)$ (resp. $\mathcal{L}_{\mathcal{A}}^{\infty}(L)$) is closed under f^{-1}" implies its twin statement "$\mathcal{B}_{\mathcal{A}}(L)$ (resp. $\mathcal{B}_{\mathcal{A}}^{\infty}(L)$) is closed under f^{-1}".

2.5 Generated sets

A convenient generalization of condition $f(a) \geq a$ in (1) of Theorem 1.1 to arbitrary algebras, consists in assuming that f is such that, for each $a \in A$, $f(a)$ is in the set $gen(a)$ generated by $\{a\}$ using all functions in $DUO(\mathcal{A})$ (cf. Definition 2.11).

Definition 2.28. [Generated set] For $\mathcal{A} = \langle A; \Xi \rangle$ an algebra and $a \in A$, let $gen(a)$ be the subset of A defined by $gen(a) = \{\gamma(a) \mid \gamma \in DUO(\mathcal{A})\}$.

Example 2.29. 1) For $\mathcal{A} = \langle \mathbb{N}; Suc \rangle$ and $\mathcal{A}' = \langle \mathbb{N}; + \rangle$, we have $gen(a) = \{b \mid b \geq a\} = a + \mathbb{N}$. Hence $b \in gen(a)$ if and only if $b \geq a$. In particular, $f(a) \in gen(a)$ is equivalent to $f(a) \geq a$.

2) If $\mathcal{A}'' = \langle \mathbb{N}; \times \rangle$, we have $gen(a) = \{b \mid a \text{ divides } b\} = a\mathbb{N}$. Thus $b \in gen(a)$ if and only if a divides b. In particular, $f(a) \in gen(a)$ is equivalent to a divides $f(a)$.

3) For $\mathcal{S} = \langle \Sigma^*; \cdot \rangle$, the algebra of words with concatenation, $gen(a) = \{w \cdot a \cdot w' \mid w, w' \in \Sigma^*\}$. In particular, $f(a) \in gen(a)$ is equivalent to a is a factor of $f(a)$.

Remark 2.30. The failure of the extension of Theorem 1.1 to some simple algebras can be related to the failure of the hypothesis $f(a) \in gen(a)$ for every $a \in A$. Consider the algebra $\mathcal{A} = \langle \{a, b\}; Id \rangle$ and f such that $f(a) = b$ and $f(b) = a$. On the one hand, the sole congruences on $\mathcal{A}$ are the two trivial ones and f is trivially congruence preserving, even though f fails the condition $f(x) \in gen(x)$ as $f(a) = b \notin gen(a) = \{a\}$. On the other hand, letting $L = \{a\}$, the set $f^{-1}(L) = \{b\}$ is not in the lattice $\mathcal{L}_{\mathcal{A}}(L) = \mathcal{L}_{\mathcal{A}}^{\infty}(L) = \{\{a\}\}$.

3 Case of natural integers

We now reinterpret Theorem 1.1 using the notions introduced in Section 2. Let us first recall "folk" results about congruences and recognizable sets of $\langle \mathbb{N}; + \rangle$.

3.1 Congruences on $\langle \mathbb{N}; + \rangle$ and $\langle \mathbb{N}; +, \times \rangle$

Lemma 3.1. *A congruence $\sim$ on $\langle \mathbb{N}; Suc \rangle$ or on $\langle \mathbb{N}; + \rangle$ is either equality, or $\sim_{a,k}$ for some $a, k \in \mathbb{N}$, $k \geq 1$ where $\sim_{a,k}$ is defined by*

$$x \sim_{a,k} y \text{ if and only if } \begin{cases} either \ x = y \\ or \ a \leq x \ , \ a \leq y \ and \ x \equiv y \pmod{k} \end{cases} . \quad (7)$$

The congruence $\sim_{a,k}$ has finite index $a + k$. It is cancellable if and only if $a = 0$.

Proof. Let $\equiv$ be a congruence on $\langle \mathbb{N}; + \rangle$ (or on $\langle \mathbb{N}; Suc \rangle$) which is not the identity: there are a and $k > 0$ such that $a \equiv a + k$. Choose the least (in lexicographic order) such a, k; then for all j, $(a + j) \equiv (a + j + k)$, hence $x \sim_{a,k} y$ implies $x \equiv y$.

Moreover, all elements in $\{0, \ldots, a + k - 1\}$ are pairwise nonequivalent modulo $\equiv$. First, if $0 \leq x < a$ and $x < y$, then x and y cannot be equivalent modulo $\equiv$ as a is the least one such that $a \equiv (a + k)$ for some k. Finally, we show that if $a \leq x < y < a + k$, then we also have $x \not\equiv y$. Indeed, assume by contradiction that $x \equiv y$ and let $h = x - a$ and $\ell = y - x$. We then have $0 \leq h < h + \ell < k$, $\ell > 0$ and $a + h = x \equiv y = a + h + \ell < a + k$. As $\equiv$ is a +-congruence, we have $a + h + j \equiv a + h + \ell + j$ for all j. Letting $j = k - (h + \ell)$ yields $a + h + j \equiv a + h + \ell + j = a + k$,

hence, as $a \equiv a + k$, by transitivity of $\equiv$, we get $a \equiv a + h + j$. As $h + j = k - \ell < k$, this contradicts the minimality of k.

If $a = 0$ then $\sim_{0,k}$ is the usual congruence modulo k hence it is cancellable. If $a \geq 1$ then $a - 1 + k \sim_{a,k} a - 1 + 2k$ but $a - 1 \not\sim_{a,k} a - 1 + k$ hence $\sim_{a,k}$ is not cancellable. □

A priori, congruences, recognizability strongly depend upon the signature. However, due to the properties of addition and multiplication on the integers in $\mathbb{N}$ we have

Corollary 3.2. *The three structures $\langle \mathbb{N}; +, \times \rangle$, $\langle \mathbb{N}; + \rangle$ and $\langle \mathbb{N}; Suc \rangle$ yield the same notions of congruence (namely, equality and the $\sim_{a,k}$'s), congruence preserving function $\mathbb{N} \to \mathbb{N}$ and recognizable subset of $\mathbb{N}$.*

Proof. Every congruence for $\langle \mathbb{N}; +, \times \rangle$ is a fortiori a congruence for $\langle \mathbb{N}; + \rangle$. Conversely, observe that the $\sim_{a,k}$'s are stable under multiplication, a straightforward property of modular congruences. Using Lemma 3.1, this shows that every +-congruence is also a ×-congruence. The assertion about congruence preservation is a trivial consequence. For that about recognizability, use Lemma 2.18. □

For morphisms the situation is more complex, as shown by the next Remark.

Remark 3.3. Homotheties $x \mapsto kx$ for $k \geq 2$ are +-morphisms which are not ×-morphism as $k(x \times y) \neq kx \times ky$.

3.2 The "frying pan" monoids and semirings

We define canonical representations of the quotient monoids and semirings $\mathbb{N}/\sim_{a,k}$.

Definition 3.4. Let $a, k \in \mathbb{N}$ such that $k \geq 1$.

1) We denote by $M_{a,k} = \{0, \ldots, a + k - 1\}$ the set of minimum representatives of the equivalence classes of $\sim_{a,k}$ and by $\varphi_{a,k} : \mathbb{N} \to M_{a,k}$ the map such that

$$\varphi_{a,k}(x) = \textit{IF } x < a \textit{ THEN } x \textit{ ELSE } a + ((x - a) \pmod{k})$$

which can be identified to the canonical surjection $\mathbb{N} \to \mathbb{N}/\sim_{a,k}$.

2) To any n-ary operation $\xi : \mathbb{N}^n \to \mathbb{N}$ on $\mathbb{N}$ corresponds a unique operation $\xi_{a,k} : M_{a,k}^n \to M_{a,k}$ making $\varphi_{a,k}$ a morphism $\langle \mathbb{N}; \xi \rangle \to \langle M_{a,k}; \xi_{a,k} \rangle$; it is defined by $\xi_{a,k}(x_1, \ldots, x_n) = \varphi_{a,k}(\xi(x_1, \ldots, x_n))$. In this way, we shall consider the arithmetic operations $Suc_{a,k}$, $+_{a,k}$ and $\times_{a,k}$ on $M_{a,k}$.

Definition 3.5. A monoid $\langle M; \oplus \rangle$ with unit 0 is monogenic if there exists $g \in M$ such that every element of $M \setminus \{0\}$ is a sum of some nonempty finite set of copies of g. Such an element g is called a <u>generator</u>.
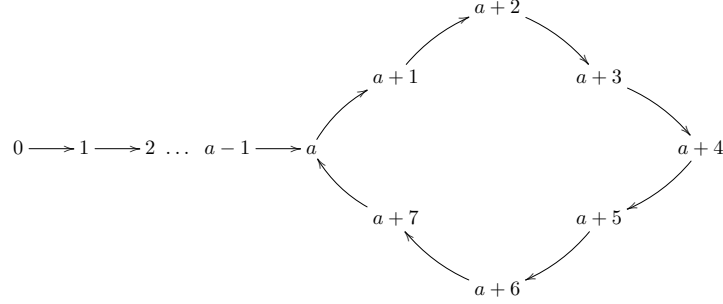
Figure 2: "Frying pan" monoid $M_{a,k}$, $k = 8$, where $Suc_{a,k}$ is represented by arrow.

Lemma 3.6. *1)* $\langle M_{a,k}; +_{a,k} \rangle$ *is a monogenic commutative monoid (called "frying pan" monoid, cf. Figure 2) with* 0 *as unit.*

2) Every finite monogenic monoid $\langle M; \oplus \rangle$ *is isomorphic to the monoid* $\langle M_{a,k}; +_{a,k} \rangle$ *for some* a, k.

3) For every surjective morphism $\psi : \langle \mathbb{N}; + \rangle \to \langle M; \oplus \rangle$ *onto a finite monoid* $\langle M; \oplus \rangle$, *there exists* a, k *and an isomorphism* $\theta : \langle M_{a,k}; +_{a,k} \rangle \to \langle M; \oplus \rangle$ *such that* $\psi = \theta \circ \varphi_{a,k}$.

Proof. We recall the argument of the classical proof of 2) which is also used for Lemma 3.7. Let g be a generator of M. Consider the relation on $\mathbb{N}$ such that $\ell \equiv n$ if the sums in $\langle M; \oplus \rangle$ of ℓ copies of g and that of n copies of g are equal. This relation $\equiv$ is a congruence on $\langle \mathbb{N}; + \rangle$ and it has finite index since M is finite. Thus, it is equal to $\sim_{a,k}$ for some a, k. The wanted isomorphism $\theta : \langle M_{a,k}; +_{a,k} \rangle \to \langle M; \oplus \rangle$ maps $x \in M_{a,k}$ onto the sum in M of x copies of g. To get 3) observe that $\langle M; \oplus \rangle$ is necessarily monogenic as so is $\langle \mathbb{N}; + \rangle$, and that the image $g = \psi(1)$ of the generator 1 of $\langle \mathbb{N}; + \rangle$ is a generator of $\langle M; \oplus \rangle$, then use the above isomorphism θ. $\square$

Lemma 3.7. *The generators of the monogenic monoid* $\langle M_{a,k}; +_{a,k} \rangle$ *are as follows:*

- *If* $a \geq 2$ *then* 1 *is the unique generator,*

- *If* $a \in \{0, 1\}$ *the generators are the elements of* $\{1, \ldots, a + k - 1\}$ *which are coprime with* k.

Proof. Obviously, 1 is a generator in all cases. Let g be a generator. Necessarily $g \neq 0$. If $a \geq 2$ since any $+_{a,k}$ sum of copies of an element ≥ 2 is also ≥ 2, the sole way to obtain 1 as a $+_{a,k}$ sum of copies of g is that $g = 1$. If $a = 0$ then the set of $+_{0,k}$ sums of nonempty finite sets of copies of g is equal to $\{ng \pmod{k} \mid n \geq 1\} = \{ng \pmod{k} \mid n = 1, \ldots, k\}$ and contains $M_{0,k} \setminus \{0\}$ if and only if g is coprime with k. If $a = 1$ then, for $g \geq 1$, the set of $+_{1,k}$ sums of nonempty finite sets of copies of g is equal to $\{1 + (ng - 1 \pmod{k}) \mid n \geq 1)\} = \{1 + (ng - 1 \pmod{k}) \mid n = 1, \ldots, k\}$ and contains $M_{a,k} \setminus \{0\}$ if and only if g is coprime with k. $\square$

13

Lemma 3.8. *There is a bijective correspondence between the generators of a finite monogenic monoid $\langle M; \oplus \rangle$ and the surjective morphisms $\langle \mathbb{N}; + \rangle \to \langle M; \oplus \rangle$, defined by*

$$g \quad \leadsto \quad \text{the unique morphism } \psi_g : \langle \mathbb{N}; + \rangle \to \langle M; \oplus \rangle \text{ such that } \psi_g(1) = g \quad (8)$$

Proof. Given a generator g of M, let ψ_g be defined by condition (8) together with $\psi_g(0) = 0_M$ and, for $n \geq 1$, $\psi_g(n) = \overbrace{g \oplus \cdots \oplus g}^{n \text{ times}}$; ψ_g defines a surjective morphism. Conversely, as 1 is a generator of $\langle \mathbb{N}; + \rangle$, if $\psi : \langle \mathbb{N}; + \rangle \to \langle M; \oplus \rangle$ is a surjective morphism, then $\psi(1)$ is a generator of M. $\qquad \square$

Corollary 3.9. *If $a \geq 2$ or $(a, k) \in \{(0, 1), (0, 2), (1, 1), (1, 2)\}$ then $\varphi_{a,k}$ is the unique surjective morphism $\langle \mathbb{N}; + \rangle \to \langle M_{a,k}, +_{a,k} \rangle$. If $a \in \{0, 1\}$ and $k \geq 3$, then there are $\phi(k)$ distinct surjective morphisms $\langle \mathbb{N}; + \rangle \to \langle M_{a,k}; +_{a,k} \rangle$, where $\phi \colon \mathbb{N} \to \mathbb{N}$ is Euler totient function mapping x to the number of integers $\leq x$ which are coprime with x.*

Proof. It follows from Lemma 3.7. $\qquad \square$

Definition 3.10. A <u>semiring</u> is a set R equipped with two binary operations $\oplus$ and $\otimes$ such that
- $\langle R, \oplus \rangle$ is a commutative monoid with an identity element, say 0,
- $\langle R, \otimes \rangle$ is a monoid with an identity element,
- Multiplication by 0 annihilates R: $0 \otimes a = a \otimes 0 = 0$ for all a,
- Multiplication left and right distributes over addition: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ and $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$ for all a, b, c.

We use the arithmetic operations defined on $M_{a,k}$, cf. Definition 3.4.

Lemma 3.11. *The algebra $\langle M_{a,k}; +_{a,k}, \times_{a,k} \rangle$ is a semiring, called the "(a,k) frying pan semiring", and $\varphi_{a,k}$ is a morphism $\langle \mathbb{N}; +, \times \rangle \to \langle M_{a,k}; +_{a,k}, \times_{a,k} \rangle$.*

3.3 Congruence preservation and divisibility

Congruence preservation on $\langle \mathbb{N}; + \rangle$ can be characterized as follows

Theorem 3.12. *For a map $f : \mathbb{N} \to \mathbb{N}$, the following conditions are equivalent*

(1) $f : \mathbb{N} \to \mathbb{N}$ is congruence preserving on the algebra $\langle \mathbb{N}; + \rangle$,

(2) $\begin{cases} \text{(i)} & (x - y) \text{ divides } (f(x) - f(y)) \text{ for all } x, y \in \mathbb{N}, \text{ and} \\ \text{(ii)} & \text{either } f \text{ is constant or } f(x) \geq x \text{ for all } x. \end{cases}$

Proof. $(1) \Rightarrow (2)$. Suppose f is congruence preserving. Let $x < y$ and consider the congruence modulo $y - x$. As $y \equiv x \bmod y - x$ we have $f(y) \equiv f(x) \bmod y - x$ hence $y - x$ divides $f(y) - f(x)$. This proves (i). To prove (ii), we show that if condition $f(x) \geq x$ is not satisfied then f is constant. Let a be least such that
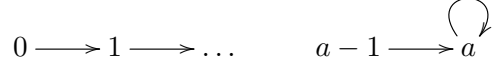
Figure 3: $M_{a,1}$

$f(a) < a$. Consider the frying pan $M_{a,1}$ (depicted in Figure 3) and the congruence $\sim_{a,1}$. We have $a \sim_{a,1} y$ for all $y \geq a$ hence $f(a) \sim_{a,1} f(y)$. As $f(a) < a$ this implies $f(a) = f(y)$. Thus, $f(a) = f(y)$ for all $y \geq a$. Let $z < a$. By condition (i) (already proved) we know that p divides $f(z) - f(z + p)$ for all p. Now, $f(z + p) = f(a)$ when $z + p \geq a$. Thus, $f(z) - f(a)$ is divisible by all $p \geq a - z$. This shows that $f(z) = f(a)$. Summing up, we have proved that f is constant with value $f(a)$.

(2) $\Rightarrow$ (1). Constant functions are trivially congruence preserving. We thus assume that f is not constant, hence f satisfies condition (i) and $f(x) \geq x$ for all x. Consider a congruence $\sim$ and suppose $x \sim y$. If $\sim$ is the identity relation then $x = y$ hence $f(x) = f(y)$. Else, by Lemma 3.1 the congruence $\sim$ is $\sim_{a,k}$ with $a \in \mathbb{N}$ and $k \geq 1$. In case $y < a$ then condition $x \sim_{a,k} y$ implies $x = y$ hence $f(x) = f(y)$ and $f(x) \sim f(y)$. In case $y \geq a$ then condition $x \sim_{a,k} y$ implies $x \geq a$ and $x \equiv y \bmod k$, hence k divides $y - x$. Condition (i) insures that $y - x$ divides $f(y) - f(x)$ hence k also divides $f(y) - f(x)$. Also, our hypothesis yields $f(x) \geq x$ and $f(y) \geq y$. As $x, y \geq a$ we get $f(x), f(y) \geq a$. Since k divides $f(y) - f(x)$ we conclude that $f(x) \sim_{a,k} f(y)$, whence (1). $\qquad\square$

Remark 3.13. We cannot withdraw the over-linearity condition $f(x) \geq x$ in Theorem 3.12. We proved in [5] that any function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ satisfying $(2)(i)$ can be lifted to a function $F : \mathbb{N} \to \mathbb{N}$ such that F satisfies $(2)(i)$ and for $x \leq n - 1$, $F(x) = f(x)$. Consider the function $f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ such that $f(0) = f(1) = 0 < 1$, $f(2) = 2$; F is non constant, satisfies $(2)(i)$ but is not congruence preserving as $F(1) < 1$ (using Theorem 3.12). In fact we can directly see that F is not congruence preserving using the congruence $\sim_{1,1}$: indeed $1 \sim_{1,1} 2$ but $F(1) \not\sim_{1,1} F(2)$.

Using Lemma 2.10, we immediately deduce from Theorem 3.12

Corollary 3.14. *Function $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ is congruence preserving if and only if condition (2) of Theorem 3.12 holds for all the unary frozen functions $f_i^{\vec{a}}$, $1 \leq i \leq n$ and $\vec{a} \in \mathbb{N}^{n-1}$.*

3.4   Congruence/(pre)orders preservation and monotonicity

Theorem 3.12 may induce the hope that congruence preserving functions over $\langle \mathbb{N}; + \rangle$ are monotone, but this is not the case. Counterexamples can be obtained using the following Propostition 3.15 (Theorem 3.15 in [3]).

Proposition 3.15 ([3]). *For every $f : \mathbb{N} \to \mathbb{N}$ there exists a function $g : \mathbb{N} \to \mathbb{Z}$ such that, letting $lcm(x)$ be the least common multiple of $1, \ldots, x$,*

i) *$x - y$ divides $g(x) - g(y)$ for all $x, y \in \mathbb{N}$,*

ii) $f(x) - 2^x lcm(x) \le g(x) \le f(x)$.

Proposition 3.16. *There exists a non monotone function $g : \mathbb{N} \to \mathbb{N}$ which is $\langle \mathbb{N}; + \rangle$-congruence preserving.*

Proof. Let $f(x) = \sum_{0 \le y \le x, y \ even} 2^{y+2} lcm(y+2) - \sum_{1 \le z \le x, z \ odd} 2^z lcm(z)$ and let g be as in Proposition 3.15. We first prove that g maps $\mathbb{N}$ into $\mathbb{N}$. A simple computation shows that $f(x) > 3 \left(2^x\right) lcm(x)$ for all $x \in \mathbb{N}$, hence $g(x) \ge f(x) - 2^x lcm(x) > 2^{x+1} lcm(x)$. This proves that $g(x) \in \mathbb{N}$ and moreover $g(x) > x$ for all x.

We next prove that g is non monotone. Condition $ii)$ of Proposition 3.15 implies

$$(f(x) - 2^x lcm(x)) - f(x-1) \le g(x) - g(x-1) \le f(x) - (f(x-1) - 2^{x-1} lcm(x-1)) \quad (9)$$

Computing the lower and upper bounds in (9) shows that: for x even, $g(x) - g(x - 1) \ge (f(x) - f(x-1)) - 2^x lcm(x) = 2^{x+2} lcm(x+2) - 2^x lcm(x) > 0$, while for x odd, $g(x) - g(x-1) \le f(x) - f(x-1) + 2^{x-1} lcm(x-1)) = -2^x lcm(x) + 2^{x-1} lcm(x-1) < 0$. Thus, g is a zig zag function hence non monotone.

Finally, as $g(x) > x$ for all x and $x - y$ divides $g(x) - g(y)$ for all $x, y \in \mathbb{N}$ (by condition $i)$ of Proposition 3.15, both conditions (i) and (ii) of Theorem 3.12 *(2)* hold and g is congruence preserving. $\square$

The existence of a stable total order has a nice consequence.

Proposition 3.17. *Let $\mathcal{A} = \langle A; \Xi \rangle$ be an algebra. Assume there is a total order on A which is $\mathcal{A}$-stable. Then a function $f : A \to A$ is $\mathcal{A}$-stable preorder preserving if and only if it is $\mathcal{A}$-stable order preserving.*

Proof. One implication is trivial. We show that if f preserves all $\mathcal{A}$-stable orders then it also preserves all $\mathcal{A}$-stable preorders. Let $\le$ be a total $\mathcal{A}$-stable order on A and $\preceq$ be an $\mathcal{A}$-stable preorder on A. Then $\le \cap \preceq$ and $\ge \cap \preceq$ are $\mathcal{A}$-stable orders on A. Indeed, as reflexivity and transitivity go through intersection, the intersection of two preorders is a preorder. Also, the antisymmetry property of an order (namely, $x \le y \le x$ implies $x = y$) still holds for the intersection with any relation. Finally, the intersection of two $\mathcal{A}$-stable relations is $\mathcal{A}$-stable.

Suppose now that $x \preceq y$. As $\le$ is total, either $x \le y$ or $y \le x$. Assume $x \le y$. As f preserves the $\mathcal{A}$-stable order $\le \cap \preceq$ and $x(\le \cap \preceq)y$ we have $f(x)(\le \cap \preceq)f(y)$ and a fortiori $f(x) \preceq f(y)$. Same argument if $y \le x$ using the order $\ge \cap \preceq$. $\square$

Remark 3.18. In particular, considering the usual total order on $\mathbb{R}$, the above result applies for the algebras $\langle \mathbb{R}; + \rangle$ and $\langle [0, +\infty[; +, \times \rangle$ and their subalgebras, e.g., $\langle \mathbb{N}; + \rangle$ and $\langle \mathbb{N}; +, \times \rangle$. It also applies to products of these algebras (consider the stable lexicographic product of the usual order).

We now show what monotonicity adds to congruence preservation in $\langle \mathbb{N}; + \rangle$ and $\langle \mathbb{N}; +, \times \rangle$. First, a simple observation.

Definition-Lemma 3.19. *Let $\preceq$ be a stable order on $\langle \mathbb{N}; + \rangle$ and, for $a \in \mathbb{N}$, let $M_a^+ = \{x \mid a \preceq a + x\}$ and $M_a^- = \{x \mid a + x \preceq a\}$.*
  1) M_a^+ and M_a^- are submonoids of $\langle \mathbb{N}; + \rangle$.
  2) If $a \le b$ then $M_a^+ \subseteq M_b^+$ and $M_a^- \subseteq M_b^-$.

Proof. 1) Clearly, $0 \in M_a^+$. Suppose $a \preceq a + x$ and $a \preceq a + y$. By stability the first inequality yields $a + y \preceq a + x + y$ and, by transitivity, the second inequality gives $a \preceq a + x + y$. Thus, M_a^+ is a submonoid. Idem with M_a^-.

2) If $a \preceq a + x$ then by stability $a + (b - a) \preceq a + x + (b - a)$, i.e. $b \preceq b + x$. Thus, $M_a^+ \subseteq M_b^+$. Similarly, $M_a^- \subseteq M_b^-$. $\qquad\qquad\square$

Theorem 3.20. *Relative to the algebras $\langle \mathbb{N}; + \rangle$ and $\langle \mathbb{N}; +, \times \rangle$, a function $f : \mathbb{N} \to \mathbb{N}$ is stable preorder preserving if and only if it is monotone non decreasing and congruence preserving.*

Proof. If f is stable preorder preserving then it is a fortiori congruence preserving. As the usual order on $\mathbb{N}$ is stable, it is preserved by f hence f is monotone non decreasing.

Assume f is congruence preserving and monotone nondecreasing. We prove that f preserves stable preorders. The case f is constant is trivial. We now suppose f is not constant hence f satisfies conditions (i) and (ii) in Theorem 3.12. Since the usual order on $\mathbb{N}$ is stable, using Lemma 3.19 it suffices to show that f preserves every stable order $\preceq$. Let $\sim$ be the congruence associated with $\preceq$. Suppose $a \preceq b$, then

- either $a \le b$ hence $b - a \in M_a^+ = \{x \mid a \preceq a + x\}$. By condition (i) we know that $b - a$ divides $f(b) - f(a)$. As M_a^+ is a monoid, $f(b) - f(a)$ is also in M_a^+. Condition (ii) insures that $f(a) \ge a$ hence, by Lemma 3.19, $M_a^+ \subseteq M_{f(a)}^+$. Thus, $f(b) - f(a)$ is in $M_{f(a)}^+$ implying $f(a) \preceq f(b)$.

- or $b \le a$, the proof is similar, by noting that $a - b \in M_b^- = \{x \mid b + x \preceq b\}$. $\quad\square$

3.5   Recognizable subsets of $\langle \mathbb{N}; + \rangle$ and $\langle \mathbb{N}; +, \times \rangle$

We recall the classical characterization of recognizability in $\langle \mathbb{N}; + \rangle$ and $\langle \mathbb{N}; +, \times \rangle$.

Proposition 3.21. *Let L be a subset of $\mathbb{N}$. The following conditions are equivalent.*

(1) L is $\langle \mathbb{N}; + \rangle$-recognizable

(2) L is $\langle \mathbb{N}; +, \times \rangle$-recognizable

(3) L is of the form $L = F \cup (R + k\mathbb{N})$ with $1 \le k$, $F \subseteq \{x \mid 0 \le x < a\}$, and $R \subseteq \{x \mid a \le x < a + k\}$ (possibly empty in which case L is finite).

Proof. $(1) \Leftrightarrow (2)$. By Corollary 3.2.

$(1) \Leftrightarrow (3)$. By definition, a subset L of $\mathbb{N}$ is $\langle \mathbb{N}; + \rangle$-recognizable if it is of the form $L = \psi^{-1}(U)$ for some surjective morphism $\psi : \langle \mathbb{N}; + \rangle \to \langle M; \oplus \rangle$ onto a finite monoid and some $U \subset M$. Using Lemma 3.6 3), we reduce to the case $M = M_{a,k}$ and $\psi = \varphi_{a,k}$ for some a, k. Letting $F = U \cap \{0, \ldots, a-1\}$ and $Y = \{x \in \{0, \ldots, k-1\} \mid a + x \in U\}$, we have $U = F \cup (a+Y)$ and $\varphi_{a,k}^{-1}(F) = F$ and $\varphi_{a,k}^{-1}(a+Y) = a+Y+k\mathbb{N} = R + k\mathbb{N}$ hence $\varphi_{a,k}^{-1}(U) = F \cup (R + k\mathbb{N})$. □

In [2] we proved a connection between recognizable subsets and functions satisfying conditions *(2) (i)* and *(2) (ii)* of Theorem 3.12. Using the equivalence given by Theorem 3.12 we now can reformulate the result of [2] as the following version of Theorem 1.1.

Theorem 3.22. *Let $f : \mathbb{N} \longrightarrow \mathbb{N}$ be a non decreasing function, the following conditions are equivalent:*

$(1)_{\mathbb{N}}$ *The function f is $\langle \mathbb{N}; + \rangle$-congruence preserving on $\mathbb{N}$ and $f(x) \geq x$ for all x.*

$(2)_{\mathbb{N}}$ *For every finite subset L of $\mathbb{N}$, the lattice $\mathcal{L}_{\langle \mathbb{N}; + \rangle}(L)$ is closed under f^{-1}.*

$(3)_{\mathbb{N}}$ *For every recognizable subset L of $\langle \mathbb{N}; + \rangle$, the lattice $\mathcal{L}_{\langle \mathbb{N}; + \rangle}(L)$ is closed under f^{-1}.*

3.6 Case of $\langle \mathbb{N}; \times \rangle$

We here extend Proposition 3.22 to congruence preserving function on $\langle \mathbb{N}; \times \rangle$ and explicitly characterize these functions in Theorem 3.23 *(ii)*. We have seen that congruences and morphisms of $\langle \mathbb{N}; + \rangle$ coincide with congruences and morphisms of $\langle \mathbb{N}; +, \times \rangle$. The situation changes radically when considering the algebra $\langle \mathbb{N}; \times \rangle$.

Theorem 3.23. *For $f : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{N} \setminus \{0\}$ the following conditions are equivalent:*

(i) For every recognizable subset L of $\langle \mathbb{N} \setminus \{0\}; \times \rangle$ the lattice $\mathcal{L}_{\times}(L)$ is closed under f^{-1}.

(ii) The function f is of the form $f(x) = f(1) \times x^n$ for some fixed $n \in \mathbb{N}$.

(iii) The function f is $\langle \mathbb{N} \setminus \{0\}; \times \rangle$-congruence preserving and x divides $f(x)$ for all x.

It appears that a sharp difference between Theorem 3.23 and Proposition3.22 is the richness of the family of involved functions. For instance on $\langle \mathbb{N}; + \rangle$ this family contains non polynomial functions. This can be explained by the fact that there are many more congruences on $\langle \mathbb{N} \setminus \{0\}; \times \rangle$ than $\langle \mathbb{N}; + \rangle$. See Example 3.25.

Definition 3.24. Let P be the set of prime numbers. For $p \in P$, the p-valuation of x denoted $Val(x, p)$ is the highest exponent n of p such that p^n divides x.

Example 3.25. 1) There are strictly more congruences on $\langle \mathbb{N} \setminus \{0\}; \times \rangle$ than on $\langle \mathbb{N}; + \rangle$. Let $Q \neq P$ be a nonempty set of prime numbers. The relation $\sim_Q$ such that $x \sim_Q y$ if for all $p \in Q$, $Val(x, p) = Val(y, p)$ is a congruence for $\langle \mathbb{N} \setminus \{0\}; \times \rangle$ but not for $\langle \mathbb{N}; + \rangle$. For instance for $Q = \{2, 5\}$, $2 \sim_Q 6$, but $4 = 2 + 2 \not\sim_Q 6 + 2 = 8$. In particular, there are uncountably many $\langle \mathbb{N} \setminus \{0\}; \times \rangle$-congruences whereas there are only countably many $\langle \mathbb{N}; + \rangle$-congruences.

2) The same phenomenon occurs for maorphisms. Let $\varphi_Q \colon \mathbb{N} \to \mathbb{N}$ be such that $\varphi_Q(x) = \prod_{p \in Q} p^{Val(x, p)}$. This map is a $\langle \mathbb{N} \setminus \{0\}; \times \rangle$-morphism. There are thus uncountably many $\langle \mathbb{N} \setminus \{0\}; \times \rangle$-morphisms whereas there are only countably many $\langle \mathbb{N}; + \rangle$-morphisms.

2) Another example: the relation $\sim$ such that $x \sim y$ if $x = y$ or both x, y are powers of 2 is a congruence for $\langle \mathbb{N}; \times \rangle$ but not for $\langle \mathbb{N}; + \rangle$ since $2 \sim 4$ and $4 \sim 4$ but $2 + 4 = 6 \not\sim 4 + 4 = 8$. This stems from the fact that a mapping $\varphi \colon \langle \mathbb{N}; +, \times \rangle \to \langle M; \oplus, \otimes \rangle$ can be a $\times$-morphism without being a $+$morphism and vice versa.

2) Let $\varphi \colon \langle \mathbb{N}; +, \times \rangle \to \langle \mathbb{Z}/2\mathbb{Z}; +, \times \rangle$ be defined by: $\varphi(x) = 1$ if and only if $x = 2^n$ for some $n \in \mathbb{N}$ and $\varphi(x) = 0$ otherwise; φ is a $\times$-morphism but not a $+$-morphism because $\varphi(6 + 1) = 0 \neq 0 + 1 = \varphi(6) + \varphi(1)$.

Before proving Theorem 3.23, let us introduce some simple notation and obervationss.

Notation 3.26. If L is a subset of $\mathbb{N}$, and $a \in \mathbb{N}$, L/a denotes the set of exact quotients of elements of L by a, $L/a = \{x \mid x \in \mathbb{N} \text{ and } ax \in L\}$.

Lemma 3.27. *1) $DUO(\langle \mathbb{N}; \times \rangle) = \{x \mapsto ax \mid a \in \mathbb{N}^*\}$ is the set of homotheties.*

2) For $L \subseteq \mathbb{N} \setminus \{0\}$, $\mathcal{L}_\times(L) = \mathcal{L}_{\langle \mathbb{N}; \times \rangle}(L)$ is the smallest sublattice $\mathcal{L}$ of $\mathcal{P}(\mathbb{N})$ containing L and closed under exact division of sets where $L/a = \{x \mid x \in \mathbb{N} \text{ and } ax \in L\}$. In particular, for a singleton set $L = \{c\}$, all sets in $\mathcal{L}_\times(L)$ are sets of divisors of c.

Example 3.28. 1) For $L = \{2^n 5^p \mid n, p \in \mathbb{N}\}$, we have $\mathcal{L}_\times(L) = \{\emptyset, L\}$.

2) For $L = \{2^n 5^p \mid n \leq 2, p \leq 1\} = \{1, 2, 4, 5, 10, 20\}$, the set $\mathcal{L}_\times(L)$ is
$$\{\emptyset, \{1\}, \{1, 2\}, \{1, 5\}, \{1, 2, 4\}, \{1, 2, 5\}, \{1, 2, 4, 5\}, \{1, 2, 5, 10\}, \{1, 2, 4, 5, 10, 20\}\}$$
since the sets L/n are given by the following table:

a	1	2	4	5	10	20	$\notin L$
L/a	$\{1, 2, 4, 5, 10, 20\}$	$\{1, 2, 5, 10\}$	$\{1, 5\}$	$\{1, 2, 4\}$	$\{1, 2\}$	$\{1\}$	$\emptyset$

Proof of Theorem 3.23. $(i) \implies (ii)$ If f is constant, then (ii) holds with $n = 0$. Let us assume from now on that f is non constant.

Fact 1. We first prove that (i) implies: x divides $f(x)$ for all x. First, observe that any finite set L is $\times$-recognizable. Indeed, letting $L \subseteq \{0, \ldots, a - 1\}$ and considering the map $\varphi_{a,1}$, we have $L = \varphi_{a,1}^{-1}(L)$. As Lemma 3.11 insures that $\varphi_{a,1}$ is a $\times$-morphism, we conclude that L is $\times$-recognizable.

19

Let $L = \{f(a)\}$, then (by lemma 3.27) every set in $\mathcal{L}_\times(L)$ is a set of divisors of $f(a)$. As $a \in f^{-1}(L) \in \mathcal{L}_\times(L)$, we conclude that a is a divisor of $f(a)$.

Fact 2. We next prove that (i) implies: <u>if b divides a then $f(a) = f(b) \times (a/b)^n$</u> <u>for some $n \in \mathbb{N}$</u>. The case $b = a$ being trivial we suppose $b < a$. Let q be the integer $q = a/b$ and set $L = \mathbb{N} \cap \{f(a)/(q^j) \mid j \in \mathbb{N}\}$. This set is finite: if $f(a)/(q^j) \in \mathbb{N}$ then $q^j \leq f(a)$ hence $j \leq \lfloor \log(f(a)/\log(q) \rfloor$. Being finite L is recognizable and condition (i) insures that $f^{-1}(L) \in \mathcal{L}_\times(L)$. Letting $j = 0$ we see that $f(a) \in L$ hence $a \in f^{-1}(L)$. We prove that b is also in $f^{-1}(L)$. Being in $\mathcal{L}_\times(L)$, the set $f^{-1}(L)$ is of the form $\bigcup_{s \in S} \bigcap_{i \in S_s} L/i$ for some finite family S of finite subsets $S_i \subset \mathbb{N}$, $i \in S$ (cf. Lemmas 2.23 & 3.27) hence $a \in \bigcap_{i \in S_s} L/i$ for some s. In particular, to prove $b \in f^{-1}(L)$ it suffices to prove that $a \in L/i \Rightarrow b \in L/i$ for all $i \geq 1$. If $a \in L/i$ then for some ℓ we have $a = f(a)/(i \times q^\ell)$ Thus, $f(a)/(a \times q^\ell) = i$ is an integer. As $q = a/b$ we have $f(a)/(q^{\ell+1}) = b \times f(a)/(a \times q^\ell) = b \times i$. Thus, $f(a)/(q^{\ell+1})$ is also an integer hence $f(a)/(q^{\ell+1}) \in L$. Now, $f(a)/(i \times q^{\ell+1}) = (f(a)/(i \times q^\ell)) \times (b/a) = a \times (b/a) = b$ is an integer hence $b = f(a)/(i \times q^{\ell+1}) \in L/i$. This proves that b is in $f^{-1}(L)$ hence $f(b) \in L$, i.e. $f(b) = f(a)/(q^j)$ for some j hence $f(a) = f(b) \times q^j = f(b) \times (a/b)^j$. This finishes the proof of Fact 2.

We finally prove that (i) implies: <u>f is of the form $f(x) = f(1) \times x^n$ for some</u> <u>fixed $n \in \mathbb{N}$</u>, i.e., $(i) \Rightarrow (ii)$. We apply Fact 2 with various pairs (a, b) and write $n(a, b)$ for the exponent such that $f(a) = f(b)(a/b)^{n(a,b)}$. Let u and v be coprime.

$$f(uv) = f(1)(uv)^{n(uv,1)} \qquad\qquad (a,b) = (uv, 1) \qquad (10)$$

$$f(u) = f(1) x^{n(u,1)} \qquad\qquad (a,b) = (u, 1) \qquad (11)$$

$$f(uv) = f(u) v^{n(uv,u)} \qquad\qquad (a,b) = (uv, u) \qquad (12)$$

$$f(uv) = f(1) u^{n(u,1)} v^{n(uv,1)} \qquad (\text{combine (12) and (11)}) \qquad (13)$$

As u and v are coprime, comparing the exponents of u in (10) and (13), we conclude that $n(uv, 1) = n(u, 1)$, for all coprime u, v. Exchanging the roles of u and u we get $n(uv, 1) = n(v, 1)$. Thus, if u, v are coprime then $n(u, 1) = n(v, 1)$. Now, for every $x, y \geq 1$ there exists z coprime to both x and y. We then have $n(x, 1) = n(z, 1)$ and $n(y, 1) = n(z, 1)$. Thus, $n(x, 1) = n(y, 1)$. Let k be the common value of the $n(x, 1)$'s. Equation (11) insures that $f(x) = f(1)x^n$ for every $x \geq 1$.

$(ii) \implies (iii)$. Straightforward.

$(ii) \implies (i)$. If f is of the form given in (ii), then $f^{-1}(L) = \sqrt[n]{L/f(1)}$ with $n \in \mathbb{N}$. We proved (Theorem 2.2 in [2]) that any lattice closed by division is also closed by nth root. As $\mathcal{L}_\times(L)$ is the smallest lattice containing L and closed under division, it is also closed by nth root; this implies that $\mathcal{L}_\times$ is closed under f^{-1}.

$(iii) \implies (ii)$. For $x \in \mathbb{N}$, let $P(x)$ be the set of primes dividing x. Recall that $Val(x, p)$ denotes the highest exponent n of p such that p^n divides x.

If p is prime then the relation $\sim_p$ defined by $x \sim_p y$ if and only if $Val(x, p) = Val(y, p)$ is a congruence on $\langle \mathbb{N} \setminus \{0\}; \times \rangle$. As f is congruence preserving, we see

that $Val(x,p) = Val(y,p)$ implies $Val(f(x),p) = Val(f(y),p)$. In other words, the p-valuation of $f(x)$ depends only on that of x. Thus, there is function $\theta_p : \mathbb{N} \to \mathbb{N}$ such that $Val(f(x),p) = \theta_p(Val(x,p))$.

Consider now the $\times$-congruence defined by $x \sim_{p,q} y$ if and only if $Val(x,p) + Val(x,q) = Val(y,p) + Val(y,q)$. Clearly $p \sim_{p,q} q$ and $p^k \sim_{p,q} p^{k-1}q$ for all $k \geq 1$, hence $f(p) \sim_{p,q} f(q)$ and $f(p^k) \sim_{p,q} f(p^{k-1}q)$. Thus, $Val(f(p),p) + Val(f(p),q) = Val(f(q),p) + Val(f(q),q)$ and $Val(f(p^k),p) + Val(f(p^k),q) = Val(f(p^{k-1}q),p) + Val(f(p^{k-1}q),q)$, hence

$$\theta_p(1) + \theta_q(0) = \theta_p(0) + \theta_q(1) \tag{14}$$
$$\theta_p(k) = \theta_p(k-1) + \theta_q(1) - \theta_q(0) \qquad \text{for } k \geq 1$$
$$\text{this yields} \quad \theta_p(k) = \theta_p(0) + k\,n \qquad \text{for all } k \in \mathbb{N} \tag{15}$$

where n is the common value of the $\theta_p(1) - \theta_p(0)$'s for prime p, a property insured by equation (14).

Let F be the finite set of primes which divide $f(1)$. This set is also the set of primes p such that $\theta_p(0) \neq 0$. Using (15) we see that $Val(f(x),p) = \theta_p(Val(x,p)) = \theta_p(0) + Val(x,p)\,n$ for every prime p. In particular, $Val(f(x),p) = 0$ if $p \notin F \cup P(x)$. Thus,

$$f(x) = \prod_{p \in F \cup P(x)} p^{\theta_p(0) + Val(x,p)\,n}$$

$$= \prod_{p \in F \cup P(x)} p^{\theta_p(0)} \times \prod_{p \in P(x) \cup F} p^{Val(x,p)\,n} \tag{16}$$

$$= \prod_{p \in F} p^{\theta_p(0)} \times \prod_{p \in P(x)} p^{Val(x,p)\,n} \tag{17}$$

$$= f(1)\,x^n \tag{18}$$

where the passage from (16) to (17) is justified as follows:
  - for $p \notin P(x)$ we have $Val(x,p) = 0$ hence $p^{Val(x,p)} = 1$,
  - for $p \notin F$ we have $\theta_p(0) = 0$ hence $p^{\theta_p(0)} = 1$.
Equation (18) is the wanted condition (ii). □

4 Lattices and preservation of stable preorders or congruences

We prove a variant of Theorem 1.1 for general algebras, where congruence preservation is replaced by the stronger condition of stable preorder preservation (Section 4.1). We also extend the stronger version of Theorem 1.1 with the weaker condition (2) to residually finite algebras (in a strong sense) admitting a group operation.

4.1 Stable preorder preservation and complete lattices

We prove Theorem 4.3, a variant of Theorem 1.1, where stable preorder preservation, complete lattices and arbitrary subsets replace congruences, lattices and recognizable subsets respectively.

Lemma 4.1. *Let $\mathcal{A} = \langle A; \Xi \rangle$. Given a subset $L \subseteq A$, if $f : A \to A$ preserves the syntactic preorder $\leq_L$ then we have*

$$f^{-1}(L) = \bigcup_{a \in f^{-1}(L)} \left(\bigcap_{\{\gamma \in DUO(\mathcal{A}) | \gamma(a) \in L\}} \gamma^{-1}(L) \right). \tag{19}$$

Thus $f^{-1}(L) \in \mathcal{L}_{\mathcal{A}}^{\infty}(L)$.

Proof. Let $I_a = \bigcap_{\{\gamma \in DUO(\mathcal{A}) | \gamma(a) \in L\}} \gamma^{-1}(L)$. Observe that $c \in I_a$ if and only if, for all $\gamma \in DUO(\mathcal{A})$, we have $\gamma(a) \in L \Rightarrow \gamma(c) \in L$. Thus, by definition of the syntactic preorder $\leq_L$, we have $I_a = \{c \mid c \leq_L a\}$. Since $a \leq_L a$ we have $a \in I_a$ hence $f^{-1}(L) \subseteq \bigcup_{a \in f^{-1}(L)} I_a$. Conversely, for every $c \in I_a$ we have $c \leq_L a$ and, as f preserves $\leq_L$, we also have $f(c) \leq_L f(a)$ hence if $f(a) \in L$ then $f(c) \in L$. Thus, $\bigcup_{a \in f^{-1}(L)} I_a \subseteq f^{-1}(L)$. This proves (19). $\qquad\square$

Remark 4.2. For $\mathbb{N}$ with operations Suc, $+$ or $\times$, equation (19) can be simplified due to the associativity and commutativity of the operations.

- For $\langle \mathbb{N}; Suc \rangle$ or $\langle \mathbb{N}; + \rangle$, equation (19) reduces to

  $$f^{-1}(L) = \cup_{a \in f^{-1}(L)} \left(\cap_{\{n \in L-a\}} L - n \right), \text{ where } L - a = \{x \mid x + a \in L\}.$$

- For $\langle \mathbb{N}; \times \rangle$, equation (19) becomes

  $$f^{-1}(L) = \cup_{a \in f^{-1}(L)} \left(\cap_{\{n \in L/a\}} L/n \right), \text{ where } L/n = \{x \mid nx \in L\}.$$

- For the free monoid $\langle \Sigma^*; \cdot \rangle$, equation (19) becomes

  $$f^{-1}(L) = \cup_{a \in f^{-1}(L)} \left(\cap_{\{(x,y) | xay \in L\}} x^{-1}Ly^{-1} \right), \text{ where } x^{-1}Ly^{-1} = \{z \mid xzy \in L\}.$$

Theorem 4.3. *[Stable preorder preservation and lattices] Let $\mathcal{A} = \langle A; \Xi \rangle$ be an algebra and f be a mapping $f \colon A \to A$.*

1) Conditions (i) and (ii) are equivalent and when they are satisfied, $f(a) \in gen(a)$ for every $a \in A$.

(i) f is stable preorder preserving.

(ii) for every subset $L \subseteq A$, $f^{-1}(L)$ is in the complete lattice $\mathcal{L}_{\mathcal{A}}^{\infty}(L)$.

2) Conditions (i') and (ii') are equivalent

(i') *f preserves the stable preorders which have finite index.*

(ii') *for every $\mathcal{A}$-recognizable subset $L \subseteq A$, $f^{-1}(L)$ is in the finite lattice $\mathcal{L}_\mathcal{A}(L)$.*

Proof. 1) $(i) \Longrightarrow (ii)$: follows from Lemma 4.1.

$(ii) \Longrightarrow (i)$: Assume that $f^{-1}(L)$ is in $\mathcal{L}_\mathcal{A}^\infty(L)$ for all L. Let $\leq$ be an $\mathcal{A}$-stable preorder and $x \in A$ and consider the $\leq$-initial segment $L = \{z \mid z \leq f(x)\}$. The assumed condition insures that $f^{-1}(L)$ is in $\mathcal{L}_\mathcal{A}^\infty(L)$. Since L is a $\leq$-initial segment so is also every set in $\mathcal{L}_\mathcal{A}^\infty(L)$ (by Lemma 2.24). In particular, $f^{-1}(L)$ is a $\leq$-initial segment. Observing that $x \in f^{-1}(L)$ (since $f(x) \leq f(x)$), we deduce that if $y \leq x$ then $y \in f^{-1}(L)$ hence $f(y) \in L$ and therefore $f(y) \leq f(x)$. This shows that f preserves the stable preorder $\leq$.

In order to see that $f(a) \in gen(a)$, it suffices to apply (ii) to $L = \{f(a)\}$: applying Lemma 4.1, we have $a \in f^{-1}(L) = \cup_{i \in I}\left(\cap_{\gamma \in \Gamma_i} \gamma^{-1}(L)\right)$ hence, for some $\gamma \in DUO(\mathcal{A})$, we have $a \in \gamma^{-1}(L) = \gamma^{-1}(\{f(a)\})$ and therefore $\gamma(a) = f(a)$.

2) $(i') \Longrightarrow (ii')$ follows from Lemma 4.1 and Lemma 2.26.

$(ii') \Longrightarrow (i')$. Let $\leq$ be a stable preorder with finite index associated congruence. Observe that the initial segment $L = \{z \mid z \leq f(a)\}$ is $\mathcal{A}$-recognizable. Indeed, L is saturated for the congruence $\sim$ associated to $\leq$ and, as $\sim$ has finite index, we can apply Lemma 2.18. Thus, using again Lemma 2.26, we can follow the proof given for item 1). $\square$

The weak version Theorem 4.3 differs in three ways from Theorem 1.1: 1) the set L is arbitrary, 2) the lattice $\mathcal{L}_\mathcal{A}^\infty(L)$ is complete, 3) the function is stable prorder preserving. In the next subsections, we will get a result closer to Theorem 1.1 by assuming that

(1) The algebra satisfies a convenient residual finiteness property (Definition 4.6), in which case we can restrict ourselves to considering finite index preorders, congruences, recognizable sets, and lattices (instead of arbitrary congruences, sets and complete lattices).

(2) The algebra has a group operation; by Corollary 4.18 1), finite index congruence preservation is equivalent to finite index stable order preservation.

4.2 Congruence preservation and (complete) boolean algebras of subsets

Congruence preservation for arbitrary algebras can be characterized using boolean algebras instead of lattices.

Lemma 4.4. *Let $\mathcal{A} = \langle A; \Xi \rangle$, let L be a subset of A and $f : A \to A$. If f preserves the syntactic congruence $\sim_L$ then $f^{-1}(L) \in \mathcal{B}_\mathcal{A}^\infty(L)$. More precisely,*

$$f^{-1}(L) = \bigcup_{a \in f^{-1}(L)} \bigcap_{\gamma \in DUO(\mathcal{A})} If \gamma(a) \in L \text{ then } \gamma^{-1}(L) \text{ else } A \setminus \gamma^{-1}(L)) \qquad (20)$$

Proof. Letting $I_a = \bigcap\limits_{\gamma \in DUO(\mathcal{A})}$ If $\gamma(a) \in L$ then $\gamma^{-1}(L)$ else $A \setminus \gamma^{-1}(L))$, we argue as in the proof of Lemma 4.1. Observe that $c \in I_a$ if and only if, for all $\gamma \in DUO(\mathcal{A})$, we have $\gamma(a) \in L \Leftrightarrow \gamma(c) \in L$. Thus, by definition of the syntactic congruence $\sim_L$, we have $I_a = \{c \mid c \sim_L a\}$. Since $a \sim_L a$ we have $a \in I_a$ hence $f^{-1}(L) \subseteq \bigcup_{a \in f^{-1}(L)} I_a$. Conversely, for every $c \in I_a$ we have $c \sim_L a$ and, as f preserves $\sim_L$, we also have $f(c) \sim_L f(a)$ hence if $f(a) \in L$ then $f(c) \in L$. Thus, $\bigcup_{a \in f^{-1}(L)} I_a \subseteq f^{-1}(L)$. This proves (20). $\qquad \square$

Theorem 4.5. *[Congruence preservation and Boolean algebras] Let $\mathcal{A}$ be an algebra and $f \colon A \to A$.*

   1) Conditions (i) and (ii) are equivalent

  (i) f is $\mathcal{A}$-congruence preserving.

  (ii) for every subset $L \subseteq A$, $f^{-1}(L)$ is in the complete Boolean algebra $\mathcal{B}_{\mathcal{A}}^{\infty}(L)$.

   2) Conditions (i') and (ii') are equivalent

  (i') f preserves the $\mathcal{A}$-congruences which have finite index.

  (ii') for every $\mathcal{A}$-recognizable subset $L \subseteq A$, $f^{-1}(L)$ is in the finite Boolean algebra $\mathcal{B}_{\mathcal{A}}(L)$.

Proof. 1) $(i) \Longrightarrow (ii)$: follows from Lemma 4.4.

   $(ii) \Longrightarrow (i)$. Assume that $f^{-1}(L)$ is in $\mathcal{B}_{\mathcal{A}}^{\infty}(L)$ for all L. Let $\sim$ be an $\mathcal{A}$-congruence and $x \in A$ and consider the $\sim$-class L of $f(x)$. The assumed condition insures that $f^{-1}(L)$ is in $\mathcal{B}_{\mathcal{A}}^{\infty}(L)$. Since L is $\sim$-saturated so is also every set in $\mathcal{B}_{\mathcal{A}}^{\infty}(L)$ (by Lemma 2.24). In particular, $f^{-1}(L)$ is $\sim$-saturated. Observing that $x \in f^{-1}(L)$ (since L is the class of $f(x)$), we deduce that if $x \sim y$ then $y \in f^{-1}(L)$ hence $f(y) \in L$ and therefore $f(y) \sim f(x)$ (again because L is the class of $f(x)$). This shows that f preserves the congruence $\sim$.

2) $(i') \Longrightarrow (ii')$. If L is recognizable then $\sim_L$ has finite index and hypothesis (i') insures that f preserves $\sim_L$. Applying Lemma 4.4 and Lemma 2.26 we see that $f^{-1}(L) \in \mathcal{B}_{\mathcal{A}}(L)$.

   $(ii') \Longrightarrow (i')$. Let $\sim$ be a congruence with finite index, let $x \in A$ and consider the $\sim$-class L of $f(x)$. By Lemma 2.18 the set L is $\mathcal{A}$-recognizable. The assumed condition (ii') insures that $f^{-1}(L)$ is in $\mathcal{B}_{\mathcal{A}}(L)$. Since L is $\sim$-saturated so is also every set in $\mathcal{B}_{\mathcal{A}}(L)$ (by Lemma 2.24). In particular, $f^{-1}(L)$ is $\sim$-saturated. We conclude as in the proof given for item 1). $\qquad \square$

4.3   Residually finite algebras, recognizability and lattices

In the vein of [8] (page 102), we define notions of residual finiteness stronger than the classical ones for congruences, preorders and algebras tailored to fit in our framework.

Definition 4.6. 1) A congruence on an algebra $\mathcal{A}$ is c-residually finite if it is the intersection of a family of finite index congruences.

2) A stable preorder on an algebra $\mathcal{A}$ is sp-residually finite if it is the intersection of a family of stable preorders all of which have finite index associated congruences.

3) An algebra $\mathcal{A}$ is said to be c-residually finite if all congruences on $\mathcal{A}$ are c-residually finite. $\mathcal{A}$ is said to be sp-residually finite if all stable preorders on $\mathcal{A}$ are sp-residually finite.

Remark 4.7. The usual notion of residually finite group, ring or module requires that morphisms into finite algebras separate points, i.e., if $x \neq y$ there exists a morphism φ into a finite algebra such that $\varphi(x) \neq \varphi(y)$. This notion is equivalent to the c-residual finiteness of a single congruence, the trivial identity congruence, hence it is weaker than that of c-residually finite algebra.

Every congruence being a preorder, Definition 4.6 gives a priori two notions of residual finiteness for a congruence. In fact, both notions are proven to coincide below.

Lemma 4.8. *1) If a stable preorder $\preceq$ is sp-residually finite then its associated congruence $\sim$ is c-residually finite.*

2) A congruence is c-residually finite if and only if, as a preorder, it is sp-residually finite.

3) A sp-residually finite algebra is also c-residually finite.

Proof. 1) Let $(\preceq_i)_{i \in I}$ be a family of stable preorders such that $\preceq = \bigcap_{i \in I} \preceq_i$. Let $\sim_i$ be the congruence associated to $\preceq_i$. We show that $\sim = \bigcap_{i \in I} \sim_i$. As $\sim_i$ is included in $\preceq_i$ we have $(\bigcap_{i \in I} \sim_i) \subseteq (\bigcap_{i \in I} \preceq_i) = \preceq$. As $\bigcap_{i \in I} \sim_i$ is a congruence, the last inclusion yields $(\bigcap_{i \in I} \sim_i) \subseteq \sim$. The inclusion of the congruence $\sim$ in the preorder $\preceq$ together with the inclusion $\preceq \subseteq \preceq_i$ imply the inclusion $\sim \subseteq \preceq_i$. As $\sim$ is a congruence, this last inclusion yields $\sim \subseteq \sim_i$. Thus, $\sim \subseteq (\bigcap_{i \in I} \sim_i)$.

2) If a congruence $\sim$ is c-residually finite and $\sim = \bigcap_{i \in I} \sim_i$ then the congruences $\sim_i$'s, being also preorders, witness that $\sim$ is sp-residually finite. Conversely, applying 1) to a congruence $\sim$, we see that if $\sim$ is sp-residually finite then it is also c-residually finite.

3) Trivial consequence of 2). $\qquad\qquad\square$

Example 4.9. 1) Integer (semi)-groups $\langle \mathbb{N}; + \rangle$ and $\langle \mathbb{Z}; + \rangle$ are c-residually finite as every non trivial congruence is of finite index (cf. Lemmata 3.1 and 5.2) and the identity congruence is the intersection of all non trivial congruences. They are also sp-residually finite. Let for instance, $\preceq$ be a stable preorder on $\langle \mathbb{N}; + \rangle$. For $i \in \mathbb{N}$ the relation $\preceq_i$ defined by $x \preceq_i y$ if and only if

- either $x < i$ or $y < i$ and $x \preceq y$,
- or $x \geq i$ and $y \geq i$,

is a stable preorder. The congruence $\sim_i$ associated to $\preceq_i$ identifies all elements larger than i, thus $\sim_i$ has finite index. It is easy to see that $\preceq = \bigcap_{i \in \mathbb{N}} \preceq_i$, hence $\preceq$ is residually finite and $\langle \mathbb{N}; + \rangle$ is sp-residually finite.

2) Contrary to the previous example, for $k \geq 2$, the algebra $\langle \mathbb{N}^k; + \rangle$ admits c-residually finite congruences having infinite index, e.g., the congruence $\vec{x} \sim \vec{y} \Leftrightarrow x_1 = y_1$. It is residually finite because $x_1 = y_1$ if and only if $x_1 \equiv y_1 \pmod{n}$, for all n.

3) On the algebra of integers with multiplication $\langle \mathbb{N}; \times \rangle$, there exist residually finite non trivial congruences with infinite index. For instance consider on $\langle \mathbb{N}; \times \rangle$ the congruence $x \sim y$ if and only if x and y have the same set of primes divisors: $\sim$ does not have a finite index. For each prime number p let $\sim_p$ be the congruence $x \sim_p y$ if and only if p divides both x, y or neither of them. Each $\sim_p$ has finite index 2 and $\sim = \cap_{p \in \mathbb{P}} \sim_p$.

Lemma 4.10. *Let $\mathcal{A} = \langle A; \Xi \rangle$ be an algebra and $f : A \to A$.*

1) If $\mathcal{A}$ is sp-residually finite then f is stable preorder preserving if and only if f preserves all stable preorders having finite index associated congruences

2) If $\mathcal{A}$ is c-residually finite then f is congruence preserving if and only if f preserves all finite index congruences.

Proof. 1) Let $\leq$ be a stable preorder. The hypothesis of sp-residual finiteness of $\mathcal{A}$ insures that $\preceq$ is sp-residually finite: there exists a family of stable preorders $(\preceq_i)_{i \in I}$ with associated congruences having finite indexes, such that $\preceq = \cap_{i \in I} \preceq_i$. Thus, $a \preceq b$ if and only if, for all $i \in I$, $a \preceq_i b$. The hypothesis insures that f preserves the $\preceq_i$'s hence $f(a) \preceq_i f(b)$ for all $i \in I$. This yields $f(a) \preceq_i f(b)$.

The proof of 2) is similar. $\qquad\square$

The next theorem improves item 2 of Theorem 4.3 for sp-residually finite algebras.

Theorem 4.11. *Let $\mathcal{A} = \langle A; \Xi \rangle$ be an algebra.*

1) If $f : A \to A$ is stable preorder preserving then $f^{-1}(L)$ is in the lattice $\mathcal{L}_\mathcal{A}(L)$ for every $\mathcal{A}$-recognizable $L \subseteq A$.

2) Assume $\mathcal{A}$ is a sp-residually finite algebra. If $f : A \to A$ is such that $f^{-1}(L)$ is in the lattice $\mathcal{L}_\mathcal{A}(L)$ for every $\mathcal{A}$-recognizable $L \subseteq A$ then f is stable preorder preserving.

Proof. 1) Apply implication $(i) \Rightarrow (ii)$ of Theorem 4.3 and then Lemma 2.26.

2) Applying implication $(ii') \Rightarrow (i')$ of Theorem 4.3, we already know that f preserves stable preorders with finite index associated congruences. To conclude apply Lemma 4.10. $\qquad\square$

Remark 4.12. If $\mathcal{A}$ is sp-residually finite, Theorem 4.11 states the equivalence: $f : A \to A$ is stable preorder preserving if and only if $f^{-1}(L)$ is in the lattice $\mathcal{L}_\mathcal{A}(L)$ for every $\mathcal{A}$-recognizable $L \subseteq A$. An instance of Theorem 4.11 for the sp-residually finite algebra $\mathcal{N} = \langle \mathbb{N}; +, \times \rangle$ is the characterization of congruence preservation given in Theorem 1.1. Indeed, Proposition 3.20, shows that on $\mathcal{N}$ a function f is stable preorder preserving if and only if it is monotone non decreasing and congruence preserving. Theorem 3.12 shows that a non constant congruence preserving f satisfies

$f(x) \geq x$ for all x. Thus on $\mathcal{N}$, Theorem 1.1 becomes a consequence of Theorem 4.11.

The next theorem improves item 2 of Theorem 4.5 for c-residually finite algebras.

Theorem 4.13. *Let $\mathcal{A} = \langle A; \Xi \rangle$ be an algebra.*

1) If $f \colon A \to A$ is congruence preserving then $f^{-1}(L)$ is in the Boolean algebra $\mathcal{B}_{\mathcal{A}}(L)$ for every $\mathcal{A}$-recognizable $L \subseteq A$.

2) Assume $\mathcal{A}$ is a c-residually finite algebra. If $f \colon A \to A$ is such that $f^{-1}(L)$ is in the Boolean algebra $\mathcal{B}_{\mathcal{A}}(L)$ for every $\mathcal{A}$-recognizable $L \subseteq A$ then f is congruence preserving.

Proof. 1) Apply implication $(i) \Rightarrow (ii)$ of Theorem 4.5 and then Lemma 2.26.

2) Applying implication $(ii') \Rightarrow (i')$ of Theorem 4.5, we already know that f preserves finite index congruences. To conclude apply Lemma 4.10. □

4.4 Stable preorders become congruences when there is a group operation

In some frameworks the requirement that a preorder be stable is quite a strong requirement as shown by Corollary 4.18 below. Recall first the notion of cancellability.

Definition 4.14. 1) A semigroup S is said to be cancellable if $xz = yz$ implies $x = y$ and $zx = zy$ implies $x = y$.

2) A stable preorder $\preceq$ on S is said to be cancellable if $xz \preceq yz$ implies $x \preceq y$ and $zx \preceq zy$ implies $x \preceq y$.

Lemma 4.15. *The only stable order of a finite group G is the identity relation.*

Proof. Assuming $x \preceq y$ we prove $x = y$. Let e be the unit of G. Stability under left product by x^{-1} and $(x^{-1}y)^n$ successively yield $e \preceq x^{-1}y$ and then $(x^{-1}y)^n \preceq (x^{-1}y)^{n+1}$ for all $n \geq 1$. By transitivity, $e \preceq x^{-1}y \preceq (x^{-1}y)^n$. As the group is finite there exists k and $n \geq 1$ such that $(x^{-1}y)^{k+n} = (x^{-1}y)^k$ hence $(x^{-1}y)^n = e$; thus $e \preceq x^{-1}y \preceq e$ and by antisymmetry $e = x^{-1}y$ and $x = y$. □

Lemma 4.16. *Any finite cancellable semigroup is a group.*

Proof. Cancellability insures that, for every $a \in S$, the maps $x \mapsto ax$ and $x \mapsto xa$ are injective hence are bijections $S \to S$ because S is finite. In particular, for all $a \in S$ there exist e'_a, e''_a such that $ae'_a = a$ and $e''_a a = a$. For $a, b \in S$ we then have $ae'_a b = ab = ae''_b b$ and by cancellability $e'_a = e''_b$, proving that e'_a and e''_a do not depend on a and are equal. Thus, the common value e of the e'_a's and e''_a's is a unit of S. Also, for $a \in S$ there exists a', a'' such that $aa' = a''a = e$. Then Then $a' = ea' = (a''a)a' = a''(aa') = a''e = a''$, proving that a' is an inverse of a. □

Proposition 4.17. *Let $\mathcal{A} = \langle A; \Xi \rangle$ be an algebra such that Ξ contains a semigroup operation. Every cancellable stable preorder $\preceq$ of $\mathcal{A}$ such that the associated congruence $\sim$ has finite index is equal to its associated congruence $\sim$.*

Proof. The semigroup operation on $\mathcal{A}$ induces a semigroup operation on the quotient algebra $\mathcal{G} = \mathcal{A}/\sim$ with carrier set $A/\sim$. The cancellability property of the congruence $\sim$ yields the cancellability property of the semigroup operation on G. Indeed, suppose $X, Y, Z \in G$ satisfy $XZ = YZ$ and let $x, y, z \in A$ be representatives of the classes X, Y, Z. Then we have $xz \sim yz$ and cancellability yields $x \sim y$ hence $X = Y$. Idem if $ZX = ZY$. As $\sim$ has finite index, G is finite and Lemma 4.16 insures that the semigroup operation on G is a group operation. As $\sim$ is the congruence associated to the stable preorder $\preceq$, it induces a quotient stable order $\preceq /\sim$ on the finite quotient algebra $\mathcal{G}$. As $\mathcal{G}$ is an expansion of a finite group, Lemma 4.15 insures that $\preceq /\sim$ is the identity relation on G hence $\preceq$ coincides with $\sim$ and is therefore a congruence on $\mathcal{A}$. $\qquad\square$

Corollary 4.18. *Let $\mathcal{A} = \langle A; \Xi \rangle$ be an algebra such that Ξ contains a group operation.*

1) Every stable preorder with finite index associated congruence is a congruence.

2) Every sp-residually finite preorder is a c-residually finite congruence.

3) If $\mathcal{A}$ is c-residually finite then it is also sp-residually finite.

Proof. Observe that stability of $\preceq$ implies its cancellability: if $xz \preceq yz$ then $xzz^{-1} \preceq yzz^{-1}$ hence $x \preceq y$. Idem if $zx \preceq zy$. Then apply Proposition 4.17. $\qquad\square$

Corollary 4.19. *Let $\mathcal{A} = \langle A; \Xi \rangle$ be an algebra such that Ξ contains a group operation. If $L \subseteq A$ is recognizable then its syntactic preorder is equal to its syntactic congruence.*

Proof. Recall that the syntactic congruence of a recognizable set has finite index and apply Corollary 4.18. $\qquad\square$

4.5 Congruence preservation when there is a group operation

When there is a group operation in a c-residually finite algebra, Theorem 4.3 can be given a more interesting variant form by replacing stable preorder preservation by congruence preservation, complete lattices by lattices and subsets by recognizable subsets.

In case the algebra has a group operation and is c-residually finite, there is a collapse of the diverse conditions involving congruence preservation, stable preorder preservation, inverse images of recognizable sets, lattices and Boolean algebras.

Theorem 4.20. *Let $\mathcal{A} = \langle A; \Xi \rangle$ be a c-residually finite algebra such that Ξ contains a group operation. Let $f \colon A \to A$. The following conditions are equivalent*

  (i) f is stable preorder preserving,

 (ii) f preserves stable preorder having finite index associated congruences,

(iii) f is congruence preserving,

(iv) f is preserves finite index congruences,

(v) $f^{-1}(L)$ is in the lattice $\mathcal{L}_\mathcal{A}(L)$ for every $\mathcal{A}$-recognizable $L \subseteq A$.

(vi) $f^{-1}(L)$ is in the Boolean algebra $\mathcal{B}_\mathcal{A}(L)$ for every $\mathcal{A}$-recognizable $L \subseteq A$.

Proof. Item 3 of Corollary 4.18 insures that $\mathcal{A}$ is also sp-residually finite. Thus, equivalences $(i) \Leftrightarrow (ii)$ and $(iii) \Leftrightarrow (iv)$ are given by Lemma 4.10.

Item 1) of Corollary 4.18 yields the equivalence $(ii) \Leftrightarrow (iv)$.

Equivalences $(i) \Leftrightarrow (v)$ and $(iii) \Leftrightarrow (vi)$ are given by Theorems 4.11 and 4.13.

Summing up, we have $(v) \Leftrightarrow (i) \Leftrightarrow (ii) \Leftrightarrow (iv) \Leftrightarrow (iii) \Leftrightarrow (vi)$. $\square$

In Section 5 we will apply Theorem 4.20 to $\langle \mathbb{Z}, + \rangle$.

5 Case of integers $\langle \mathbb{Z}; + \rangle$ and $\langle \mathbb{Z}; +, \times \rangle$

In this section we look for an extension of Theorem 3.22 to functions $\mathbb{Z} \to \mathbb{Z}$, for the structures $\mathcal{Z} = \langle \mathbb{Z}; + \rangle$ and $\mathcal{Z}' = \langle \mathbb{Z}; +, \times \rangle$.

5.1 Congruences on $\langle \mathbb{Z}; + \rangle$ and $\langle \mathbb{Z}; +, \times \rangle$

Recall that the congruences of $\langle \mathbb{Z}; + \rangle$ are the equality relation and the modular congruences $x \equiv y \pmod{k}$ for $k \geq 1$. These $\langle \mathbb{Z}; + \rangle$-congruences are also $\langle \mathbb{Z}; +, \times \rangle$-congruences. Thus, applying item 2 of Definition 3.4, we have the following $\mathbb{Z}$ avatar of Corollary 3.2 about $\mathbb{N}$.

Lemma 5.1. *The two structures $\langle \mathbb{Z}; +, \times \rangle$ and $\langle \mathbb{Z}; + \rangle$ yield the same notions of congruence (namely, equality and the modular congruences), congruence preserving function $\mathbb{Z} \to \mathbb{Z}$, morphism $\mathbb{Z} \to \mathbb{Z}$ and recognizable subset of $\mathbb{Z}$.*

Hence on $\mathbb{Z}$, the study of congruence-preservation and recognizability w.r.t. to the signature $+$ supersedes the study w.r.t. the signature $+, \times$. However congruence-preservation and recognizability w.r.t. to the signature $\times$ yield no consequence for congruence-preservation and recognizability w.r.t. to the signature $+$ as not every $\langle \mathbb{Z}; \times \rangle$-morphism (resp. congruence, recognizable set) is a $\langle \mathbb{Z}; + \rangle$-morphism (resp. congruence, recognizable set).

In general, congruences are kernels of morphisms into possibly infinite algebras. However, for the ring of integers (cf. Lemma 5.2), non trivial congruences coincide with kernels of morphisms onto finite structures, exactly as for with the semiring of natural numbers. This allows to consider only congruences having finite index.

5.2 Congruence preservation on principal commutative rings

More generally than $\langle \mathbb{Z}; +, \times \rangle$, we characterize congruence preservation for commutative principal rings with the signature $\Xi = \{+, \times\}$.

Lemma 5.2. *If $\mathcal{A}$ is a principal commutative ring (i.e., every ideal is principal), then*
(i) any congruence $\sim$ is of the form $\sim_k = \{(u, v) \mid u - v \in k\,A\}$ for some $k \in A$.
(ii) a function $f : A \to A$ is congruence preserving if and only if it satisfies

$$x - y \text{ divides } f(x) - f(y) \text{ for all } x, y \in X \tag{21}$$

Proof. The hypothesis that $\mathcal{A}$ is principal yields condition (i).

(ii) Assume f is congruence preserving. For $x, y \in A$, let $\sim = \{(u, v) \mid u - v \in (x-y)\,A\}$ be the congruence generated by the ideal $(x-y)A$. Since $x \sim y$, congruence preservation insures that $f(x) \sim f(y)$ hence $x - y$ divides $f(x) - f(y)$.

Conversely, assume (21) holds and let $\sim$ be a congruence, which is of the form $\sim_k$ because of principality. If $x \sim_k y$ then k divides $x - y$ and, by transitivity of divisibility, (21) insures that k divides $f(x) - f(y)$, i.e., $f(x) \sim_k f(y)$. $\qquad\square$

Remark 5.3. Otherwise stated, for principal commutative rings, congruence preservation is equivalent to condition $(2)(i)$ of Theorem 3.12 and the over-linearity condition $(2)(ii)$ of Theorem 3.12 is not needed.

5.3 Recognizability in $\langle \mathbb{Z}; + \rangle$ and $\langle \mathbb{Z}; +, \times \rangle$

Recall first a folk Proposition.

Proposition 5.4. *Let $X \subseteq \mathbb{Z}$. The following conditions are equivalent:*

(i) X is $\langle \mathbb{Z}; + \rangle$-recognizable,

(ii) X is $\langle \mathbb{Z}; +, \times \rangle$-recognizable,

(iii) X is of the form $X = F + k\mathbb{Z}$ with $k \in \mathbb{N} \setminus \{0\}$ and $F \subseteq \{0, \ldots, k-1\}$.

Proof. $(i) \Rightarrow (ii)$. Assume (i) and let $\varphi : \langle \mathbb{Z}; + \rangle \to \langle M; \oplus \rangle$ be a surjective morphism where M has k elements. Since $\langle \mathbb{Z}; + \rangle$ is a monogeneous group so is $\langle M; \oplus \rangle$ which is therefore isomorphic to $\mathbb{Z}/k\mathbb{Z}$. Also, the morphism φ is the modular projection $x \mapsto x \pmod{k}$. To conclude that (ii) is true, recall that the modular projection is also a ring morphism $\langle \mathbb{Z}; +, \times \rangle \to \langle \mathbb{Z}/k\mathbb{Z}; +, \times \rangle$.

$(ii) \Rightarrow (iii)$. Assume (ii) and let $X = \varphi^{-1}(F)$ with M finite, $F \subseteq M$, φ a surjective morphism $(\mathbb{Z}, +, \times) \to \langle M; \oplus, \otimes \rangle$. We know (from the proof of $(i) \Rightarrow (ii)$) that, up to an isomorphism, $\langle M; \oplus, \otimes \rangle$ is the ring $\mathbb{Z}/k\mathbb{Z}$ for some $k \in \mathbb{N} \setminus \{0\}$ and $\varphi : \mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ is the modular projection. Thus, $X = \varphi^{-1}(F) = F + k\mathbb{Z}$.

$(iii) \Rightarrow (i)$. Observe that $X = F + k\mathbb{Z} = \varphi^{-1}(F)$ where $\varphi : \mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ is the modular projection. $\qquad\square$

In $\langle \mathbb{N}; + \rangle$ recognizable subsets cioncide with regular subsets. In $\langle \mathbb{Z}; + \rangle$ this is no longer true. A subset $L \subseteq \mathbb{Z}$ is regular if it is of the form $L = L^+ \cup (-L^-)$ where L^+, L^- are regular subsets of $\mathbb{N}$, i.e., $L = -(d + S + d\mathbb{N}) \cup F \cup (d + R + d\mathbb{N})$ with $d \geq 1$, $R, S \subseteq \{x \mid 0 \leq x < d\}$, $F \subseteq \{x \mid -d < x < d\}$ (possibly empty). See [1].

Corollary 5.5. *Both $\langle \mathbb{Z}; + \rangle$ and $\langle \mathbb{Z}; +, \times \rangle$ are c-residually finite.*

Remark 5.6. The only finite $\langle \mathbb{Z}; + \rangle$-recognizable set is the emptyset.

5.4 Lattices in $\langle \mathbb{Z}; + \rangle$ and $\langle \mathbb{Z}; +, \times \rangle$

Definition 5.7. Let $\mathcal{R}$ be a unit (semi)ring $\langle R; +, \times \rangle$, with $0, 1$ as distinct identities for $+$ and $\times$.

- $\mathcal{L}_{\langle R; + \rangle}(L)$ is the smallest sublattice of $\mathcal{P}(R)$ containing L and closed under $(x \mapsto x + a)^{-1}$ for all $a \in R$ (closed under <u>translations</u>).

- $\mathcal{L}_{\langle R; +, \times \rangle}(L)$ (resp. $\mathcal{L}^{\infty}_{\langle R; +, \times \rangle}(L)$)

is the smallest (resp. complete) sublattice of $\mathcal{P}(R)$ containing L and closed under both translations and <u>divisions</u> (i.e., $(x \mapsto ax)^{-1}$ for all $a \in R$).

By Lemma 5.1, congruence preservation (resp. recognizability) w.r.t. $\langle \mathbb{Z}; + \rangle$ and $\langle \mathbb{Z}; +, \times \rangle$ are equivalent. The next Lemma shows that this goes on with lattices, i.e., the lattices $\mathcal{L}_{\langle \mathbb{Z}; + \rangle}(L)$ and $\mathcal{L}_{\langle \mathbb{Z}; +, \times \rangle}(L)$ coincide for any recognizable L.

Lemma 5.8 (Characterization of the lattice generated by a recognizable subset and closed by translations)**.** *Let $L \subseteq \mathbb{Z}$ be a nontrivial (i.e., different from $\mathbb{Z}$ and $\emptyset$) recognizable subset of $\langle \mathbb{Z}; + \rangle$. Let $k \geq 1$ be smallest such that $L = F + k\mathbb{Z}$ with $F \subset \{0, \ldots, k-1\}$. Then*

$$\mathcal{L}_{\langle \mathbb{Z}; + \rangle}(L) = \mathcal{L}_{\langle \mathbb{Z}; +, \times \rangle}(L) = \{G + k\mathbb{Z} \mid G \subseteq \{0, \ldots, k-1\}\}.$$

If $L = \emptyset$ or $L = \mathbb{Z}$ (i.e. $k = 0$ or $k = 1$) then these three lattices coincide with $\{L\}$.

Proof. We first prove that $\mathcal{L}_{\langle \mathbb{Z}; + \rangle}(L) \supseteq \{G + k\mathbb{Z} \mid k \in \mathbb{N} \text{ and } G \subseteq \{0, \ldots, k-1\}\}$. Let $k \geq 1$ and F be a nonempty subset of $\{0, \ldots, k-1\}$, i.e., $F = \{z_1, \ldots, z_n\}$ with $n \geq 1$ and $0 \leq z_1 < \ldots < z_n < k$. For $i = 1, \ldots, n$ consider the set $A_i = \{z_j - z_i \pmod{k} \mid j = 1, \ldots, n\} \subseteq \{0, \ldots, k-1\}$. Clearly, 0 is in each A_i. We claim that $\bigcap_{i=1}^{i=n} A_i = \{0\}$. If $k = 1$ this is clear since then every A_i is $\{0\}$. We now assume $k \geq 2$ and $\bigcap_{i=1}^{i=n} A_i \neq \{0\}$. Let $a \in \bigcap_{i=1}^{i=n} A_i$ with $a \neq 0$. Then, there exists $\theta : \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that $z_{\theta(i)} - z_i \equiv a \pmod{k}$ for $i = 1, \ldots, n$; hence $z_i + a \in z_{\theta(i)} + k\mathbb{Z} \subseteq F + k\mathbb{Z}$. Since $F = \{z_1, \ldots, z_n\}$ we get $F + a \subseteq F + k\mathbb{Z}$, and by induction, for all $n \in \mathbb{N}$, $F + na \subseteq F + k\mathbb{Z}$. Indeed $F + na = F + (n-1)a + a \subseteq F + k\mathbb{Z} + a = F + a + k\mathbb{Z} \subseteq F + k\mathbb{Z} + k\mathbb{Z} = F + k\mathbb{Z}$. Let $d = \gcd(k, a)$. Using Bézout identity, there are $p, q \in \mathbb{Z}$, $p > 0 > q$ such that $pa + qk = d$ and $p', q' \in \mathbb{Z}$, $p' < 0 < q'$ such that $p'a + q'k = d$. Inclusion $F + pa \subseteq F + k\mathbb{Z}$ yields $F + d = F + pa + qk \subseteq F + k\mathbb{Z}$ hence (again by induction) $F + d\mathbb{N} \subseteq F + k\mathbb{Z}$. In the same way, using p', q' we get $F - d\mathbb{N} \subseteq F + k\mathbb{Z}$. Thus, $F + d\mathbb{Z} \subseteq F + k\mathbb{Z}$. As d divides k we also have $F + k\mathbb{Z} \subseteq F + d\mathbb{Z}$. Thus, $F + d\mathbb{Z} = F + k\mathbb{Z} = L$ and since $0 < d < k$ (recall $0 < a < k$ and d divides a) this contradicts the minimality of k.

Equality $\bigcap_{i=1}^{i=n} A_i = \{0\}$ implies that

$$\bigcap_{i=1}^{i=n} L - z_i \;\; = \;\; \bigcap_{i=1}^{i=n} \left(\{z_j - z_i \mid j = 1, \ldots, n\} + k\mathbb{Z} \right) = \bigcap_{i=1}^{i=n} \left(\{A_i\} + k\mathbb{Z} \right)$$

31

$$= \ \Big(\bigcap_{i=1}^{i=n} A_i \Big) + k\mathbb{Z} = \{0\} + k\mathbb{Z} \ = \ k\mathbb{Z}.$$

Thus, for all $b \in \{0, \ldots, k-1\}$, $b + k\mathbb{Z} = \bigcap_{i=1}^{i=n} \big(L - z_i + b \big)$ belongs to $\mathcal{L}_{\langle \mathbb{Z};+\rangle}(L)$. All finite unions and intersections of such $b + k\mathbb{Z}$ also belongs to $\mathcal{L}_{\langle \mathbb{Z};+\rangle}(L)$ proving that for all $G \subseteq \{0, \ldots, k-1\}$, $\{G + k\mathbb{Z}\}$ is in $\mathcal{L}_{\langle \mathbb{Z};+\rangle}(L)$.

The converse inclusion is straightforward.

Finally, as $\mathcal{L}_{\langle \mathbb{Z};+,\times\rangle}(L)$ is the smallest lattice closed by translations and divisions containing L, it suffices to prove that $\{G + k\mathbb{Z} \mid G \subseteq \{0, \ldots, k-1\}\}$ is closed by divisions to conclude. Recall that $L = F + k\mathbb{Z}$ with $F \subseteq \{0, \ldots, k-1\}$. For $d \in \mathbb{Z}$ $L/d = \{b \mid bd \in L\}$. Set $G = L/d \cap \{0, \ldots, k-1\}$, we show that $L/d = G + k\mathbb{Z}$. Clearly $(G + k\mathbb{Z})d \subseteq dG + dk\mathbb{Z} \subseteq L + k\mathbb{Z} = L$, hence $G + k\mathbb{Z} \subseteq L/d$. Conversely, if $b \in L/d$, then $bd = f + kz \in L$, $f \in F$; letting $a = b \pmod{k} \in \{0, \ldots, k-1\}$, we have $ad = (b + kz')d = f + k(z + dz') \in L$ hence $a \in L/d \cap \{0, \ldots, k-1\}$. Thus $b \in G + k\mathbb{Z}$, this shows that $L/d \subseteq G + k\mathbb{Z}$. Hence $L/d = G + k\mathbb{Z}$.

Finally, the last assertion about the cases $L = \emptyset$ and $L = \mathbb{Z}$ is straightforward. $\square$

Remark 5.9. Note the following immediate consequence of Lemma 5.8. For every $L \neq \emptyset$ we have $\mathbb{Z} \in \mathcal{L}_{\langle \mathbb{Z};+\rangle}(L)$ as $\mathbb{Z} = \{0, \ldots, k-1\} + k\mathbb{Z}$. This is different from the case of $\mathbb{N}$ where $\mathbb{N}$ does not necessarily belong to $\mathcal{L}_{\mathbb{N}}(L)$, for instance when L is finite (hence recognizable in $\langle \mathbb{N};+\rangle$) all sets in $\mathcal{L}_{\langle \mathbb{N};+\rangle}(L)$ are finite.

5.5   Characterizing congruence preserving functions on $\langle \mathbb{Z};+\rangle$

Theorem 4.20 for residually finite algebras immediately yields the following consequence, even though we also can give a direct proof without using residual finiteness.

Theorem 5.10. *Function $f : \mathbb{Z} \to \mathbb{Z}$ is $+$-congruence preserving if and only if for every recognizable subset L of $\mathbb{Z}$ the lattice $\mathcal{L}_{\langle \mathbb{Z};+\rangle}(L)$ is closed under f^{-1}.*

Proof. For any $a \in \mathbb{Z}$, in the algebra $\mathcal{Z}$, $gen(a) = \{c + a \mid c \in \mathbb{Z}\} = \mathbb{Z}$. Hence for any function $f \colon \mathbb{Z} \to \mathbb{Z}$, for any a, condition $f(a) \in gen(a)$ trivially holds. Thus by Theorem 4.20, f is $\mathcal{Z}$-congruence preserving if and only if for every $\mathcal{Z}$-recognizable subset L of $\mathbb{Z}$ the lattice $\mathcal{L}_{\mathcal{Z}}(L)$ is closed under f^{-1}. $\square$

Remark 5.11. 1) The previous result shows that conditions $(1)_{\mathbb{N}}$ and $(3)_{\mathbb{N}}$ of Theorem 3.22 can be extended when substituting $\langle \mathbb{Z};+\rangle$ for $\langle \mathbb{N};+\rangle$. However, conditions $(2)_{\mathbb{N}}$ and $(3)_{\mathbb{N}}$ of Theorem 3.22 are no longer equivalent when substituting $\langle \mathbb{Z};+\rangle$ for $\langle \mathbb{N};+\rangle$ as shown by the counterexample exhibited in 2).

2) It is straightforward to see that, for any L finite, $\mathcal{L}_{\mathcal{Z}}(L)$ is the set of all finite subsets of $\mathbb{Z}$. Consider $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(k) = 2^k$ for $k \in \mathbb{N}$ and $f(x) = x$ if $x < 0$. As $f^{-1}(a)$ is finite for every a, the inverse image of any finite subset is a finite subset, and $\mathcal{L}_{\mathcal{Z}}(L)$ is closed under f^{-1}. However f is not congruence preserving: for instance, $2 - 0 = 2$ does not divide $f(2) - f(0) = 2^2 - 2^0 = 3$.

3) Example 5.12 shows that in Theorem 5.10 "regular" cannot be substituted for "recognizable".

Example 5.12. Theorem 5.10 does not hold if we substitute "regular" for "recognizable". In [1] it is shown that a regular subset L of $\mathbb{Z}$ is of the form $L = L^+ \cup (-L^-)$ where L^+, L^- are regular subsets of $\mathbb{N}$, i.e., $L = -(d + S + d\mathbb{N}) \cup F \cup (d + R + d\mathbb{N})$ with $d \geq 1$, $R, S \subseteq \{x \mid 0 \leq x < d\}$, and $F \subseteq \{x \mid -d < x < d\}$ (possibly empty). Consider the regular set $L = 6 + 10\mathbb{N}$; function f defined by $f(x) = x^2$ is congruence preserving by Lemma 5.2. The set $f^{-1}(L) = (\{4, 6\} + 10\mathbb{N}) \cup -(\{4, 6\} + 10\mathbb{N})$ contains infinitely many negative numbers. Each set $L - t$ (for $t \in \mathbb{Z}$) contains only finitely many negative numbers and the same is true for any finite union of finite intersections of $L - t$'s, and, in particular, for any set in $\mathcal{L}_{\mathcal{Z}}(L)$. Thus, $f^{-1}(L)$ is not in $\mathcal{L}_{\mathcal{Z}}(L)$.

6 Case of rings of p-adic integers

For rings $\mathbb{Z}_p$ of p-adic integers, the results are similar to those for the ring $\mathbb{Z}$.

Representation of p-adic integers. Let us recall some basic facts about p-adic integers. The set $\mathbb{Z}_p$ of p-adic integers is the projective limit $\varprojlim \langle \mathbb{Z}/p^n\mathbb{Z}; +, \times \rangle$ relative to the projections $\pi_{p^n, p^m} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ with $n \geq m$, such that $\pi_{p^n, p^m}(x) = x$ (mod $p)^m$ for $x = 0, \ldots, 2^n - 1$. Every p-adic integer can be represented as an infinite sum $\sum_{n=0}^{\infty} a_n p^n$ with $a_n \in \{0, \ldots, p-1\}$. Addition is performed with carries as in the finite case (except that it goes from left to right). Elements of $\mathbb{N}$ are represented in $\mathbb{Z}_p$ by sums with an infinite tail of 0's. Elements of $\mathbb{Z} \setminus \mathbb{N}$ correspond in $\mathbb{Z}_p$ to base p representations with an infinite tail of digits all equal to $p - 1$. For instance, (writing a^ω for an infinite tail of digits all equal to a) we have $100110^\omega + (p-1)(p-1)(p-1)(p-2)(p-2)(p-1)^\omega = 0^\omega$.

6.1 About saturation and congruence preservation

We first show that p-adic integers come in naturally for congruence preservation reasons, more precisely we study the extension of congruence preserving functions $\mathbb{N} \to \mathbb{Z}$ into congruence preserving function $\mathbb{Z} \to A$. Example 6.1 below shows that, if we want to extend all congruence preserving functions $\mathbb{N} \to \mathbb{Z}$ into congruence preserving functions $\mathbb{Z} \to A$, the carrier set A of the extended algebra cannot be reduced to $\mathbb{Z}$ and it must be "saturated" in the sense of p-adic analysis (different from Definition 2.15).

Example 6.1. On $\langle \mathbb{N}; + \rangle$ we can define by induction a congruence preserving function $F: \mathbb{N} \to \mathbb{N}$ such that $F(0) = 0$, $F(1) = F(2) = 2$ and for all $n > 1$, $F(2^n - 1) \equiv 0$ (mod 2^n). See the Appendix for the inductive proof.

We now show that F cannot be extended into a congruence preserving function $F_{\mathbb{Z}}$ on $\mathbb{Z}$. Indeed, $F_{\mathbb{Z}}(-1)$ ought to satisfy the following conditions

- $F_{\mathbb{Z}}(-1) \equiv F_{\mathbb{Z}}(2) = 2$ (mod 3), hence $F_{\mathbb{Z}}(-1) \neq 0$

- $F_{\mathbb{Z}}(-1) \equiv 0$ (mod 2^n) for all n (if $F_{\mathbb{Z}}$ is congruence preserving then 2^n divides $F_{\mathbb{Z}}(2^n - 1) - F_{\mathbb{Z}}(-1)$, and it already divides $F_{\mathbb{Z}}(2^n - 1) = F(2^n - 1)$)

hence $|F_{\mathbb{Z}}(-1)| \geq 2^n$ for all n and that is impossible in $\mathbb{Z}$.

Saturation. Let $f : \mathbb{N} \to \mathbb{N}$ be a congruence preserving function. In order to extend f into a congruence preserving function in -1, letting $a = f(-1)$, we must have: 2 divides $a - f(1)$, 3 divides $a - f(2)$, 4 divides $a - f(3)$, ... Hence infinitely many conditions must hold. For every finite subset of this set of conditions, there exists such an a in $\mathbb{Z}$ (and also in $\mathbb{N}$) as proved in Example 6.1. Unfortunately, an a satisfying <u>all</u> the conditions in the infinite set of conditions does not exist in $\mathbb{N}$, or $\mathbb{Z}$, because neither $\mathbb{N}$, nor $\mathbb{Z}$ are "saturated"(in the logical sense). Saturated sets containing $\mathbb{Z}$ are the sets of p-adic integers.

6.2 Residual finiteness of rings of p-adic integers

Definition 6.2. The <u>p-adic valuation</u> of $x \in \mathbb{Z}_p$ is the maximum k such that p^k divides x, i.e., the number of heading zeroes in the p-adic representation of x.

Remark 6.3. The set U of invertible elements of $\mathbb{Z}_p$ consists of all elements with null p-adic valuation, i.e., those with p-adic representation $(a_n)_{n \in \mathbb{N}}$ such that $a_0 \neq 0$. Thus, every element x of $\mathbb{Z}_p$ can be written $x = p^n u$ where $n \in \mathbb{N}$ and $u \in U$.

Lemma 6.4 (cf. Lenstra [10]). *$\mathbb{Z}_p$ is a principal ring, and all ideals of $\mathbb{Z}_p$ are of the form $\mathcal{I}_n = p^n \mathbb{Z}_p$, with $n \in \mathbb{N}$, or $\mathcal{I} = \{0\}$*

Proof. Let us recall the simple proof. If a is an element with minimum valuation in an ideal I then $a = p^n u$ for some inversible u and also $I \subseteq p^n \mathbb{Z}_p$. Let v be an inverse of u. Then I contains $av\mathbb{Z}_p = p^n uv\mathbb{Z}_p = p^n \mathbb{Z}_p$. □

Corollary 6.5. *The ring $\langle \mathbb{Z}_p; +, \times \rangle$ is residually finite.*

Proof. By Lemma 5.2 and Lemma 6.4 a non trivial congruence on $\mathbb{Z}_p$ is of the form

$$x \sim_n y \text{ iff } x - y \in p^n \mathbb{Z}_p.$$

There thus are p^n equivalence classes $a + p^n \mathbb{Z}_p$ with $a \in \{0, \ldots, p^n - 1\}$.

Finally, the trivial congruence $x \sim y$ iff $x = y$ is equal to the intersection of all non trivial congruences. □

Lemmata 5.2 and 6.4 imply the following

Proposition 6.6. *A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is congruence preserving on $\langle \mathbb{Z}_p; +, \times \rangle$ if and only if it is satisfies the divisibility condition (21).*

Let us recall a result proved in [5] (Theorem 24) for functions satisfying condition (21), hence by Corollary 6.6 for congruence preserving functions.

Proposition 6.7. *Every $\langle +, \times \rangle$-congruence preserving function $f : \mathbb{N} \to \mathbb{Z}$ extends to unique $\langle +, \times \rangle$-congruence preserving function $\widehat{f} : \mathbb{Z}_p \to \mathbb{Z}_p$.*

In particular, this answers the problem raised in section 6.1 and Example 6.1.

Corollary 6.8. *Every $\langle +, \times \rangle$-congruence preserving function $f : \mathbb{N} \to \mathbb{Z}$ extends to unique $\langle +, \times \rangle$-congruence preserving functions $\widehat{f_{\mathbb{Z}}} : \mathbb{Z} \to \mathbb{Z}_p$.*

However, for $x \in \mathbb{Z}$, $\widehat{f_{\mathbb{Z}}}(x)$ is not necessarily in $\mathbb{Z}$ but in $\mathbb{Z}_p$, cf. Example 6.1.

6.3 Recognizability in $\langle \mathbb{Z}_p; +, \times \rangle$

We here give a simple characterization of recognizable subsets.

Proposition 6.9. *Let X be a subset of $\mathbb{Z}_p$. The following conditions are equivalent:*

(i) X is a recognizable subset of the ring $\langle \mathbb{Z}_p; +, \times \rangle$.

(ii) X is of the form $X = F + p^n \mathbb{Z}_p$ for some $n \in \mathbb{N}$ and some finite subset of $\{0, \ldots, p^n - 1\}$.

Proof. $(i) \Rightarrow (ii)$. Assume (i) and let $\varphi : \mathbb{Z}_p \to M$ be a surjective $\{+, \times\}$-morphism with M finite. Since $\mathbb{Z}_p$ is a ring so is $M = \varphi(\mathbb{Z}_p)$. Let $K = \varphi^{-1}(0_M)$ be the kernel of φ. The kernel K of φ is not reduced to $\{0\}$, otherwise φ would be injective and M infinite. Let n be the smallest among the p-adic valuations of the elements of K. Then $K \subseteq p^n \mathbb{Z}_p$. Let $z \in K$ have this smallest p-adic valuation: $z = p^n u$ with $u \in U$. We have for all $v \in \mathbb{Z}_p$, $p^n v = p^n u \times u^{-1} v = z \times u^{-1} v$, hence, as K is an ideal and $z \in K$, we have $K \supseteq p^n \mathbb{Z}_p$, whence $K = p^n \mathbb{Z}_p$. As $\varphi^{-1}(\varphi(x)) = x + K$, we get $\varphi^{-1}(\varphi(x)) = x + p^n \mathbb{Z}_p$. As M is finite, any $T \subset M$ is a finite union $T = \cup_{i=1,\ldots,k} \{\varphi(x_i)\}$. Any $\{+, \times\}$-recognizable subset Z of $\mathbb{Z}_p$ is thus a finite union of such $\varphi^{-1}(\varphi(x_i))$, $i = 1, \ldots, k$, i.e., $Z = \bigcup_{i=1}^{i=k} (x_i + p^n \mathbb{Z}_p) = F + p^n \mathbb{Z}_p)$ where $F = \{x_1, \ldots, x_k\}$. This proves condition (ii).

$(ii) \Rightarrow (i)$. It suffices to consider $M = \mathbb{Z}/p^n\mathbb{Z}$ and φ the modular projection $(a_k)_{k \in \mathbb{N}} \mapsto (a_0, \ldots, a_{n-1}, 0, 0, \ldots)$. $\qquad \square$

6.4 Congruence preserving functions and lattices

Theorem 4.20 allows to extend Theorem 5.10 to the ring $\mathbb{Z}_p$.

Proposition 6.10. *A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is $\langle \mathbb{Z}_p; +, \times \rangle$-congruence preserving if and only if for every recognizable subset L of $\mathbb{Z}_p$, the lattice $\mathcal{L}_{\langle \mathbb{Z}_p; +, \times \rangle}(L)$ is closed under f^{-1}.*

Proof. By Corollary 6.5 and Theorem 4.20, noting that the condition $f(a) \in gen(a)$ holds because, $\mathbb{Z}_p$ being a group, for any $a \in \mathbb{Z}_p$ we have $gen(a) = \mathbb{Z}_p$. $\qquad \square$

Remark 6.11. We do not know whether Proposition 6.10 extends to the ring of profinite integers $\widehat{\mathbb{Z}}$. As there is no simple characterization of the ideals of $\widehat{\mathbb{Z}}$ [10], our proofs of Corollary 6.6 and Proposition 6.9 do not hold for $\widehat{\mathbb{Z}}$. We nevertheless conjecture that these results hold on $\widehat{\mathbb{Z}}$.

7 Conclusion

We studied the relationships between lattices generated by recognizable sets of some algebras and congruence preserving functions. For quite a few usual algebras (in particular those with carriers $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_p$), we showed that congruence preserving

functions somehow correspond to functions which can be added to the algebra with no modification of the lattices generated by recognizable set and closed under the inverses of the "generating operations" of the algebra.

References

[1] M. Benois, <u>Parties Rationnelles du Groupe Libre</u>, C. R. Acad. Sci. Paris Série A, 269, pp 1188-1190, 1969.

[2] P. Cégielski, S. Grigorieff, I. Guessarian, <u>On Lattices of Regular Sets of Natural Integers Closed under Decrementation</u>, Information Processing Letters 114(4): 197-202, 2014.

[3] P. Cégielski, S. Grigorieff, I. Guessarian, <u>Newton expansion of functions over natural integers having integral difference ratios</u>, Int. J. Number Theory, Int. J. Number Theory, Vol. 11 No 7 (2015), p. 2109-2139.

[4] P. Cégielski, S. Grigorieff, I. Guessarian, <u>Integral Difference Ratio Functions on Integers</u>, LNCS 8808, 2014, 277-291.

[5] P. Cégielski, S. Grigorieff, I. Guessarian, <u>Arithmetical Congruence Preservation: From Finite to Infinite</u>, LNCS 9300, 2015, 210-225.

[6] G Grätzer, <u>Universal Algebra</u>, 2dn edition, Springer Verlag, 1979.

[7] K. Kaarli, A.F. Pixley, <u>Polynomial completeness in algebraic systems</u>, Chapman & Hall/CRC, 2001.

[8] S. Lang, <u>Algebra</u>, 3rd ed., Springer, 2002.

[9] H.W. Lenstra, <u>Profinite number theory</u>, `http://www.euro-math-soc.eu/system/files/news/Hendrik%20Lenstra_Profinite%20number%20theory.pdf`

8 Appendix

Proof of Example 6.1. We can define, by induction on $x \in \mathbb{N}$, a congruence preserving function $F \colon \mathbb{N} \to \mathbb{N}$ such that: $F(\mathbb{N}) \subseteq \mathbb{N}$, $F(0) = 0$, $F(1) = F(2) = 2$ and for all $n > 1$, $F(2^n - 1) \equiv 0 \pmod{2^n}$. Note that F is congruence preserving both as a mapping $\mathbb{N} \to \mathbb{N}$, and as a mapping $\mathbb{N} \to \mathbb{Z}$. Basis: for $x = 3$ ($n = 2$), $F(3) = 12$ is suitable

Induction: assume $F(y)$ has been defined for $y < x$ and define $F(x)$; $F(x)$ must satisfy

$$F(x) \equiv F(0) \pmod{2^n} \qquad \text{if } x = 2^n - 1 \tag{22a}$$

$$F(x) \equiv F(0) \pmod{x} \tag{22b}$$

$$F(x) \equiv F(1) \pmod{(x-1)}$$

$$\vdots$$

$$F(x) \equiv F(i) \pmod{(x-i)} \tag{22c}$$

$$\vdots$$

$$F(x) \equiv F(x-2) \pmod{2} \tag{22d}$$

36

Otherwise stated, assuming for all $n < x$, $F(n)$ satisfying (22) has been defined, we define $F(x)$ satisfying all of the equivalences in (22).

As for q_1, q_2 coprime, $a \equiv b \pmod{q_1 \times q_2}$ if and only if $a \equiv b \pmod{q_1}$ and $a \equiv b \pmod{q_2}$, we can transform the above system of equivalences (22) so that all equivalences are modulo a power of a prime number. For any n and any prime $p < n$, let $\alpha_{n,p}$ be the exponent of the largest power of p dividing n (i.e., $\alpha_{n,p} = \lfloor \log_p n \rfloor$). Then system (22) is equivalent to system (23) below

$$F(x) \equiv F(0) \pmod{2^n} \qquad \text{if } x = 2^n - 1 \quad \text{and } p = 2 \qquad \text{(23a)}$$
$$F(x) \equiv F(0) \pmod{p^{\alpha_{x,p}}} \qquad \text{for all } p \text{ dividing } x \qquad \text{(23b)}$$
$$F(x) \equiv F(1) \pmod{p^{\alpha_{(x-1),p}}} \qquad \text{for all } p \text{ dividing } x - 1 \qquad \text{(23c)}$$
$$\vdots$$
$$F(x) \equiv F(i) \pmod{p^{\alpha_{(x-i),p}}} \qquad \text{for all } p \text{ dividing } x - i \qquad \text{(23d)}$$
$$\vdots$$
$$F(x) \equiv F(x-2) \pmod{2} \qquad \text{for all } p \text{ dividing } 2 \qquad \text{(23e)}$$

The next Fact allows us to simplify system (23) in such a way that each prime p occurs in at most one equivalence.

Fact 8.1. *Let F satisfy system (22) for all $y < x$. Let $p \le x$ be a prime. Let $\alpha_p = \max \{ \alpha_{i,p} \mid i = 2, \dots, x \}$. Let (24) be the subsystem of (23) consisting only of equivalences modulo a power of the chosen prime p*

$$F(x) \equiv F(0) \pmod{2^n} \text{ if } x = 2^n - 1 \quad \text{and } p = 2 \qquad \text{(24a)}$$
$$F(x) \equiv F(0) \pmod{p^{\alpha_{x,p}}} \text{ if } p \text{ divides } x \qquad \text{(24b)}$$
$$\vdots$$
$$F(x) \equiv F(j) \pmod{p^{\alpha_{(x-j),p}}} \text{ if } p \text{ divides } x - j \qquad \text{(24c)}$$
$$\vdots$$
$$F(x) \equiv F(i) \pmod{p^{\alpha_{(x-i),p}}} \text{ if } p \text{ divides } x - i \qquad \text{(24d)}$$
$$\vdots$$
$$F(x) \equiv F(x-2) \pmod{p^{\alpha_{2,p}}} \text{ if } p \text{ divides } 2 \qquad \text{(24e)}$$

The system (24) of equivalences reduces to a <u>single equivalence</u> (25) of the form

$$\text{either} \quad F(x) \equiv F(i) \pmod{p^{\alpha_p}} \quad \text{if } x \ne 2^n - 1 \text{ or } p \ne 2 \qquad \text{(25a)}$$
$$\text{or} \quad F(x) \equiv F(0) \pmod{2^n} \quad \text{if } x = 2^n - 1 \text{ and } p = 2 \qquad \text{(25b)}$$

Proof. Clearly, if all equivalences (24) hold then equivalence (25) holds. Let us prove the converse:

- assume first $x \neq 2^n - 1$ or $p \neq 2$, then equation (24a) is out of the picture and system (24) is equivalent to equation (25a). If $\alpha_p = \alpha_{(x-i),p} = \alpha_{(x-j),p}$, arbitrarily choose one of the equivalences (24c) or (24d) for (25). We prove that equivalences (24c) hold for all $j \in \{2, \ldots, x\} \setminus \{i\}$. Let j be given, note that $p^{\alpha_{(x-j),p}}$ divides $p^{\alpha_{(x-i),p}}$

  - assume e.g. $i > j$. Then $p^{\alpha_{(x-j),p}}$ divides both $x - i$ and $x - j$, hence it divides $(x - j) - (x - i) = i - j$, and by the induction hypothesis, equivalences (22) hold for i, thus $F(i) \equiv F(j) \pmod{p^{\alpha_{(x-j),p}}}$
  - (25a) and $p^{\alpha_{(x-j),p}}$ divides $p^{\alpha_{(x-i),p}}$ imply that $F(x) \equiv F(i) \pmod{p^{\alpha_{(x-j),p}}}$

  hence (24c) by transitivity.

- assume now $x = 2^n - 1$. For $p \neq 2$ the proof is the same as above. If $p = 2$, then equation (24a) gets into the picture and more care is needed. The largest power of 2 dividing the $(x - i)$'s is 2^{n-1} and it is reached for $i = 2^{n-1} - 1$ as $x - i = 2^n - 1 - 2^{n-1} - 1 = 2^{n-1}$.

  - By the induction hypothesis on F, we have $F(2^{n-1} - 1) \equiv 0 \pmod{2^{n-1}}$
  - As $F(0) = 0$, equation (25b) implies that $F(x) \equiv 0 \pmod{2^n}$

  Hence $F(x) \equiv F(2^{n-1} - 1) \pmod{2^{n-1}}$ by transitivity of $\equiv$ and, by the proof of the previous case, this implies that all equations (24b) to (24e) hold. $\qquad\square$

We now use the above Fact 8.1 to simplify system (23) so that there is at most one equivalence for each prime p; the Chinese remainder theorem shows that this last system has at least a solution $F(x) = y_0$; as F is congruence preserving both $2^n - 1$ and 2^n divide $F(2^n - 1)$. $\qquad\square$

Profinite integers

Recall some classical equivalent approaches to the topological rings of p-adic integers integers, cf. Lenstra [10] and Lang [9].

Proposition 8.2. *Let p be prime. The three following approaches lead to isomorphic structures, called the topological ring $\mathbb{Z}_p$ of p-adic integers.*

- *The ring $\mathbb{Z}_p$ is the inverse limit of the following inverse system:*

  - *the family of rings $\mathbb{Z}/p^n\mathbb{Z}$ for $n \in \mathbb{N}$, endowed with the discrete topology,*
  - *the family of surjective morphisms $\pi_{p^n, p^m} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ for $0 \leq n \geq m$.*

- *The ring $\mathbb{Z}_p$ is the set of infinite sequences $\{0, \ldots, p - 1\}^{\mathbb{N}}$ endowed with the Cantor topology and addition and multiplication which extend the usual way to perform addition and multiplication on base p representations of natural integers.*

- *The ring $\mathbb{Z}_p$ is the Cauchy completion of the metric topological ring $(\mathbb{N}, +, \times)$ relative to the following ultrametric: $d(x,x) = 0$ and for $x \neq y$, $d(x,y) = 2^{-n}$ where n is the p-valuation of $|x - y|$, i.e., the maximum k such that p^k divides $x - y$.*

Proposition 8.3. *The topological group $\mathbb{Z}_p$ is compact and has a basis of clopen sets (sets which are both open and closed) of the form $\prod_{i=0}^{n} G_i \times \prod_{i=n+1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}$, with G_i a subset of $\{0, \ldots, p - 1\}$.*
Any clopen set of $\mathbb{Z}_p$ is of the form $G_n + p^n\mathbb{Z}_p$, with $G_n \subseteq \{0, 1, \ldots, p^n - 1\}$.

Proof. The topology on $\mathbb{Z}_p$ is the product topology (coarsest such that the projections $\pi_i \colon \mathbb{Z}_p \to \mathbb{Z}$ defined by $\pi_i(a_0, a_1, \ldots) = a_i$ are continuous); as $\mathbb{Z}/p^i\mathbb{Z}$ has the discrete topology, any $G_i \subseteq \mathbb{Z}/p^i\mathbb{Z}$ is both open and closed; hence any set $\pi_i^{-1}(G_i) = \prod_{i=0}^{n-1} \mathbb{Z}/p^i\mathbb{Z} \times G_i \times \prod_{i=n+1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}$ is clopen, and so is also any finite intersection of such sets, $\prod_{i=0}^{n} G_i \times \prod_{i=n+1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}$. It is easy to see that these clopens form a basis of the open sets of $\mathcal{O}$.

$\mathbb{Z}_p$ is compact: by the theorem of Tychonoff the product of compact topological spaces is itself compact. $\mathbb{Z}_p$ is an intersection of closed subsets: $\mathbb{Z}_p = \cap_{n=0}^{\infty} C_n$, where $C_n = \prod_{i=0}^{n-2} \mathbb{Z}/p^i\mathbb{Z} \times G_n \times \prod_{i=n+1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}$ where $G_n = \{(a_{n-1}, a_n) \mid \pi_{n-1}(a_n) = a_{n-1}\} \subset \mathbb{Z}/p^{n-1}Z \times \mathbb{Z}/p^n\mathbb{Z}$; G_n is closed as it is a finite subset of the product of two finite sets with discrete topology, the complement $\overline{G_n}$ of G_n is thus open and so is the complement $\overline{C_n}$ of C_n; thus C_n is closed in $\prod_{i=0}^{\infty} \mathbb{Z}/p^i\mathbb{Z}$; $\mathbb{Z}_p$ is therefore closed as intersection of closed subset, hence compact.

Finally, all clopens of $\mathbb{Z}_p$ are of the form $\prod_{i=0}^{n} G_i \times \prod_{i=n+1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}$, with G_i a subset of $\{0, \ldots, p - 1\}$: any clopen set L is a union $\cup_{i\in I} C_i$ of such clopens of the basis; L being a closed subset of a compact space is compact, hence a finite union $\cup_{i\in\{i,\ldots,i_k\}} C_i$ of these clopens covers L, and as $L = \cup_{i\in I} C_i$, we also have $L = \cup_{i\in\{i,\ldots,i_k\}} C_i$. It is then easy to see that L is in the form $G_n + p^n\mathbb{Z}_p$, with $G_n \subseteq \{0, 1, \ldots, p^n - 1\}$. $\qquad\square$