NOTES ON RIEG THEORY: SEMIRING WITH EXPONENTIALS IN LOGIC, PROFINITE ARITHMETIC, ENUMERATIVE COMBINATORICS, AND CATEGORY THEORY

RYUYA HORA

Abstract. In this paper, we introduce the notion of a *rieg*, that is, a semiring equipped with a binary operation called exponentiation, and present its basic theory along with numerous examples. We begin by reviewing the classification of quotient riegs over $\mathbb{N}$ given by Burris and Lee. Then, through concrete examples, we propose how riegs can appear in (pro)finite arithmetic, category theory, enumerative combinatorics, and logic. Typical examples of a rieg include the rieg of natural numbers $\mathbb{N}$, the five cyclic models ($\mathbb{N}_{1,1}, \mathbb{N}_{1,2}, \mathbb{N}_{1,6}, \mathbb{N}_{1,42}$, and $\mathbb{N}_{1,1806}$), other quotient riegs of $\mathbb{N}$ (= modulo arithmetic with exponentials), the canonical profinite rieg $\mathbb{N} \sqcup \widehat{\mathbb{Z}}$, the topological rieg of 10-adic natural numbers $\mathbb{N}_{\infty,10^\infty} = \mathbb{N} \sqcup (\mathbb{Z}_2 \times \mathbb{Z}_5)$ (which does not work for the 5-adic natural numbers $\mathbb{N} \sqcup \mathbb{Z}_5$), the cardinal arithmetic like $2^{\aleph_0}$, the rieg of truth values $\{\bot, \top\}$ with $p^q := (q \to p)$, Heyting algebras including the set of open subsets $\mathcal{O}(X)$ of a topological space X, the rieg of finite directed graphs, the Burnside rieg of a finite group, the rieg of rooted trees, the rieg of isomorphism classes of finite groups, and other decategorified topoi.

Contents

1. Introduction 2
2. Riegs 2
2.1. Preliminaries: rigs 2
2.2. Definition 3
2.3. Digression: Why rigs, not rings? 5
3. Example 1: Riegs in finite and profinite arithmetic 5
3.1. Rieg theoretic phenomena 5
3.2. Finite arithmetic: the Burris-Lee theorem 8
3.3. Profinite arithmetic: a total exponentiation 11
4. Example 2: Riegs in category theory and combinatorics 16
4.1. Burnside rieg of CCC with finite coproducts (and a topos) 17
4.2. Riegs of functions $\mathfrak{B}(\mathbf{FinSet}^{\to})$: List of numbers and Liouville's divisor theorem 18
4.3. Rieg of finite groups 20
5. Example 3: Riegs in logic 22
5.1. Riegs in which $1 + 1 = 1$ 23
5.2. Riegs that are lattices 23
5.3. Heyting algebras are riegs 24
Appendix A. Preliminaries on equational theory and profinite topology 25
A.1. Categorical properties of riegs (and general $\mathbb{T}$-algebras) 25
A.2. Topological $\mathbb{T}$-algebras and their profinite completion 25
Appendix B. Other (counter)examples 26

2020 *Mathematics Subject Classification.* 16Y60, 03G10, 11D61, 20E18, 18D15, 18B25.

Key words and phrases. Semiring, rig, exponential, profinite set, Tarski highschool problem, objective number theory, cartesian closed category, topos, Burnside rig, Heyting algebra, equational theory.

B.1. Basic examples 26
B.2. Riegs of three elements 28
References 29

1. Introduction

The aim of the present paper is to popularise an algebraic structure, which we will call *riegs*, by providing several theorems and examples. As a *rig* defined as a "ri**n**g without **n**egatives" ([Sch90]) a *rieg* is a "rig with **e**xponentials." In other words, a rieg is a ring-like structure that has $0, 1, +, \times$, and a binary operation $\uparrow$ (Definition 2.2.1). The prototypical example of a rieg is the rieg of natural numbers.

Of course, the idea of considering ring-like structures with exponentials is not new.

In the context of category theory, [Bir42]

> [Sch00a] Objective number theory is the study of addition and multiplication (and eventually exponentiation) of objects in suitable categories.

Fiore [FDB06]

To the best of the author's knowledge, the field in which rigs with (binary) exponentiation have been most actively studied is (finite) model theory. The Tarski High School problem concerns the theory of the positive integers with addition, multiplication, and exponentiation. Even after this problem was resolved, research on small models continued to progress. The story until 2005 is summarized in [BY05].

Acknowledgement. The author would like to thank his supervisor Ryu Hasegawa for helpful discussions and suggestions. He was supported by JSPS KAKENHI Grant Number JP24KJ0837 and FoPM, WINGS Program, the University of Tokyo. He is also grateful to Ivan Di Liberti for pointing out Remark 2.3.3.

Survey.

1942 One can see the idea of an algebra of structures, with exponential in [Bir42].
1980s Wilkie gives a solution to Tarski's high school algebra problem, circulated as a preprint and published in 2000 [Wil00].
1992 [BL92] (and its summary [BL93]) give what we call *the Burris-Lee theorem*
2000 Schanuel publishes papers on objective number theory [Sch00a][Sch00b]
2005 The survey paper [BY05] was published.
2006 Fiore, Cosmo, and Balat give a type-theoretic view on this structure, with 0 [FDB06].

Notation 1.0.1. We adopt the following notations:

- $\mathbb{N}$ denotes the set of all non-negative integers. Sometimes, we regard it as a poset with the natural ordering.
- $\mathbb{N}^*$ denotes the set of all positive integers. We may regard it as a poset with the divisibility order.

2. Riegs

2.1. **Preliminaries: rigs.** Since our theory of riegs is based on the theory of rigs (= semirings), we start by recalling the notion of rigs. (The word "rig" comes from "ri**n**g without **n**egatives" [Sch90].) We only need the definition and a few examples.

Definition 2.1.1 (Rig)**.** A (possibly non-commutative) *rig* is a set R equipped with

- two constants (= nullary operations) $0, 1 \in R$ and
- two binary operations, $+, \times \colon R \times R \to R$

such that the following equations hold for all $x, y, z \in R$:

(1) $0 + x = x$,

(2) $(x+y)+z = x+(y+z)$,
(3) $x+y = y+x$,
(4) $1 \times x = x$,
(5) $x \times 1 = x$,
(6) $(x \times y) \times z = x \times (y \times z)$,
(7) $x \times 0 = 0$,
(8) $x \times (y+z) = (x \times y) + (x \times z)$,
(9) $0 \times x = 0$, and
(10) $(x+y) \times z = (x \times z) + (y \times z)$.

If R satisfies an additional equation

(11) $x \times y = y \times x$,

we call it a *commutative rig*. A *rig homomorphism* is a function that preserves the four operations $0, 1, +, \times$. The category of rigs and rig homomorphisms is denoted by **Rigs**.

For the sake of simplicity, we may write xy for $x \times y$. Let us provide three examples, each of which plays a specific role in what follows.

Example 2.1.2 (Rings)**.** Of course, every ring is a rig; the theory of rigs is obtained from that of rings by dropping the axiom that every element has an additive inverse. However, rings will play only a marginal role in this paper: we will see that the only rieg whose underlying rig is a ring is the degenerate one (Proposition 2.3.2).

Example 2.1.3 (Rig of natural numbers)**.** The rig of natural numbers (with the usual addition and multiplication) $\mathbb{N}$ is the initial object of the category **Rigs**. Its quotients will be the main subject of Section 3.

Example 2.1.4 (Rig of endohomomorphisms on a commutative monoid)**.** For a commutative monoid $(A, e, *)$, the set of monoid endohomomorphisms $\mathrm{End}(A, e, *)$ admits a rig structure as follows:

- The element $0 \in \mathrm{End}(A, e, *)$ is the constant function to the neutral element $A \to A\colon a \mapsto e$.
- The element $1 \in \mathrm{End}(A, e, *)$ is the identity function $\mathrm{id}_A\colon A \to A$.
- The sum $f + g$ of two elements $f, g \in \mathrm{End}(A, e, *)$ is given by $(f+g)(a) \coloneqq f(a) * g(a)$. (Here, we use the commutativity of $*$.)
- The product $f \times g$ of two elements $f, g \in \mathrm{End}(A, e, *)$ is given by the composite $f \circ g$.

For the additive monoid $(\mathbb{N}, 0, +)$, the rig $\mathrm{End}(\mathbb{N}, 0, +)$ is isomorphic to the rig of natural numbers $(\mathbb{N}, 0, 1, +, \times)$. A rig of endohomomorphisms is, however, typically non-commutative; for the additive group $(\mathbb{Z}^2, 0, +)$, the rig $\mathrm{End}(\mathbb{Z}^2, 0, +)$ is isomorphic to the ring $M_2(\mathbb{Z})$ of 2×2 matrices over $\mathbb{Z}$, which is not commutative. This is the example that we will use to define riegs (Definition 2.2.1).

2.2. **Definition.** This subsection aims to introduce the notion of riegs. Although it is possible to define riegs by familiar but numerous equations (Proposition 2.2.2), we adopt another definition, which turns out to be surprisingly simple. Note that $\mathrm{End}(R, 1, \times)$ in the definition below is the rig explained in Example 2.1.4 obtained from the multiplicative commutative monoid $(R, 1, \times)$.

Definition 2.2.1 (Rieg)**.** A *rieg* is a commutative rig $(R, 0, 1, +, \times)$ equipped with a rig homomorphism $R \to \mathrm{End}(R, 1, \times)$.

At first glance, this definition may not seem to have anything to do with exponents. So let us unpack the definition into a sequence of equalities. The rig homomorphism $R \to \mathrm{End}(R, 1, \times)$ sends an element $x \in R$ to a (commutative) monoid homomorphism, which will be denoted by

$$-^x\colon (R, 1, \times) \to (R, 1, \times).$$

The condition that $-^x\colon R \to R$ is a monoid homomorphism is equivalent to the familiar equations

- $1^x = 1$, and
- $(yz)^x = y^x z^x$.

For the function $R \to \mathrm{End}(R, 1, \times)$ to be a rig homomorphism, it must preserve 0, 1, $+$, and $\times$. Preservation of each operation corresponds to the equation listed in Table 1.

Preserved rig structure	The required equation
0	$x^0 = 1$
1	$x^1 = x$
$+$	$x^{y+z} = x^y x^z$
$\times$	$x^{yz} = (x^z)^y$

TABLE 1. Four of the rieg equations

Summarising the above observations, we obtain an equational definition of the notion of riegs. While it is longer than Definition 2.2.1, it consists only of familiar conditions.

Proposition 2.2.2 (Equational definition of riegs)**.** *The definition of riegs (Definition 2.2.1) can be rephrased by the five operations:*

- *two constants (= nullary operations),* $0, 1 \in R$*, and*
- *three binary operations,* $+, \times, \uparrow \colon R \times R \to R$*,*

and fourteen equations:

(1) $0 + x = x$
(2) $(x + y) + z = x + (y + z)$
(3) $x + y = y + x$
(4) $1x = x$
(5) $(xy)z = x(yz)$
(6) $xy = yx$
(7) $x0 = 0$
(8) $x(y + z) = xy + xz$
(9) $1^x = 1$
(10) $(yz)^x = y^x z^x$.
(11) $x^0 = 1$
(12) $x^1 = x$
(13) $x^{y+z} = x^y x^z$
(14) $x^{yz} = (x^z)^y$,

where xy *denotes* $x \times y$*, and* x^y *denotes* $x \uparrow y$ *as usual.*

If we forget the constant 0, these are exactly the eleven "high school identities" of Tarski [BY05]. The other three equations, $0 + x = x$, $x \times 0 = 0$, and $x^0 = 1$, are the ones that involve 0.

Remark 2.2.3. As a special case of the equation $x^0 = 1$, we have $0^0 = 1$. This convention will be repeatedly interpreted in many ways in this paper.

From this equational (or algebraic) definition, we can define the notion of rieg homomorphisms in the usual way.

Definition 2.2.4. A *rieg homomorphism* is a function that preserves all (five) operations $0, 1, +, \times, \uparrow$. We write **Riegs** for the category of riegs.

As we will see numerous examples later, for now, we introduce only two trivial (but important!) examples of riegs: the initial object and the terminal object in the category of riegs.

Example 2.2.5 (The initial rieg: natural numbers)**.** The set of all natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$ equipped with the usual zero 0, one 1, addition $+$, multiplication $\times$, and exponentiation $\uparrow$, forms the rieg of natural numbers $\mathbb{N}$. Here are a few remarks about this example:

- This rieg $\mathbb{N}$ is an initial object in the category **Riegs**. Indeed, for a rieg R, the unique rig homomorphism $\phi\colon \mathbb{N} \to R$ automatically preserves $\uparrow$: for $n, m \in \mathbb{N}$, the equations $x^{y+z} = x^y x^z$, $x^1 = x$, and $x^0 = 1$ give $\phi(n)^{\phi(m)} = \phi(n)^{1+\cdots+1} = \phi(n) \cdots \phi(n) = \phi(n^m)$, where both products have m factors.
- This is the unique rieg structure on the rig of natural numbers, since $\mathbb{N}$ is the initial rig (Example 2.1.3) and a rieg structure is given by a rig homomorphism $\mathbb{N} \to \mathrm{End}(\mathbb{N}, 1, \times)$.
- We adopt the convention that $0^0 = 1$ (see Remark 2.2.3).

Example 2.2.6 (The degenerate rieg)**.** A singleton $\{*\}$ admits exactly one rieg structure, which we call the *degenerate rieg* **1**. The degenerate rieg is a terminal object of the category **Riegs**.

2.3. **Digression: Why rigs, not rings?** The reader may wonder: why do we develop our theory using rigs, even though rings are so famous and successful? There are several possible answers, but perhaps the simplest is that subtraction and exponentiation are fundamentally incompatible—if we have subtraction, then we have to give a meaning to 0^{-1}!

Claim 2.3.1. *If a rieg R contains an additive inverse -1 of 1, then it is degenerate, that is, $R \cong \mathbf{1}$ (cf. Example 2.2.6).*

Proof. We have the equation $1 = 0^0 = 0^{1+(-1)} = 0^1 \times 0^{-1} = 0 \times 0^{-1} = 0$. This implies that every element $r \in R$ is equal to 0, since $r = r \times 1 = r \times 0 = 0$. □

Proposition 2.3.2 (No rieg is a ring)**.** *If a rieg R is a ring, then it is degenerate, that is, $R \cong \mathbf{1}$.*

Proof. A ring contains an additive inverse of 1, so Claim 2.3.1 applies. □

Remark 2.3.3. A similar problem appears for division, and there we have a solution. A *meadow* is a commutative ring with a total inverse operation, and its axioms imply $0^{-1} = 0$ [BHT09]. So we may hope to do the same thing here, that is, to choose a value of 0^{-1}. This does not work. Whatever the value of 0^{-1} is, we have $0 \times 0^{-1} = 0$, and the proof of Claim 2.3.1 still gives $1 = 0$.

For example, exponentiation can be defined on the rig $\mathbb{N}$, but it is impossible on the ring $\mathbb{Z}$ (Proposition 2.3.2). To the best of the author's understanding, one reason why exponential structures—despite being present in many mathematical objects—have not received the attention they perhaps deserve is that the process of decategorification often involves introducing formal subtraction. For example, the ring of integers $\mathbb{Z}$ is obtained by introducing a formal subtraction to $\mathbb{N}$, which inherently admits the exponential structure of the cartesian closed category **FinSet** (Section 4). This subtraction does help clarify theories (sometimes by reducing the amount of information), but at the same time, it forces us to entirely forget the exponential structure.

3. Example 1: Riegs in finite and profinite arithmetic

3.1. **Rieg theoretic phenomena.** Before delving into the technical details, let us first take a look at a few phenomena that will be studied in the rest of this section.

3.1.1. *Phenomenon 1: modular arithmetic with exponentials.* Let us consider the following high school level problem from elementary number theory, which involves exponentiation.

Puzzle 3.1.1. Find all pairs of natural numbers (n, m) such that

$$2^n + 5 = m^2.$$

Answer. *Consider the equation modulo* 8*. If* $n \geq 3$*, the equation is simplified to*

$$5 \equiv m^2 \mod 8.$$

However, since the quadratic residues modulo 8 *are* 0*,* 1*, and* 4*, it is impossible. Therefore, we only need to check* $n = 0$*,* 1*, and* 2*. We conclude that the only solution is* $(n, m) = (2, 3)$*.*

In this example, when considering exponentiation modulo 8, we have to set aside the "first exceptions", namely the three numbers $n = 0, 1, 2$.

3.1.2. *Phenomenon 2: Profinite dynamical systems with exponentials.* Let us consider the following puzzle.

Puzzle 3.1.2 (A puzzle provided by J.Koizumi)**.** Find a four-digit natural number n such that the last four digits of 3^n are equal to n.

There is a surprisingly simple way to obtain the solution — namely, iteration! First, take an arbitrary natural number n, say $n = 2024$. Then, repeatedly replace n by the last four digits of 3^n[1].

- $3^{2024} \equiv 6481$
- $3^{6481} \equiv 6803$
- $3^{6803} \equiv 2027$
- $3^{2027} \equiv 4987$
- $3^{4987} \equiv 9387$
- $3^{9387} \equiv 5387$
- $3^{5387} \equiv 5387$

We obtain an answer $n = 5387$.

Answer. $n = 5387$ *is the only answer.*

Then, it is natural to ask whether we can go farther:

Question 3.1.3. *Is there an infinite sequence of decimal digits*

$$\dots a_4 a_3 a_2 a_1$$

such that, for every integer $k \geq 1$*, the truncation* $n_k := \sum_{i=1}^{k} a_i 10^{i-1}$ *satisfies the congruence*

$$3^{n_k} \equiv n_k \pmod{10^k}?$$

The answer is Yes! (See Figure 1)

Remark 3.1.4 (Attribution)**.** The affirmative answer is not new. It is a special case of a theorem of Jiménez Urroz and Yebra [JY09, Theorem 3]: for every *valid base* b (an integer such that $q \mid b$ for every prime $p \mid b$ and every prime $q \mid p - 1$) and every integer a not divisible by the squarefree part of b, there is a unique such digit sequence for the congruences $a^x \equiv x \pmod{b^n}$ for all sufficiently large n. The base $b = 10$ is valid, and our digit sequence is recorded as [OEIa], known there as the final digits of Graham's number; the truncations displayed in Figure 1 form [OEIb]. What rieg theory adds is not the statement but a conceptual proof: the sequence is the unique fixed point of the contraction 3^x (Proposition 3.3.12).

[1]Thanks to the repeated squaring algorithm, a computer can conduct this calculation in a short time.

$$
\begin{aligned}
3^{87} &\equiv 87 \mod 100\\
3^{387} &\equiv 387 \mod 1000\\
3^{5387} &\equiv 5387 \mod 10000\\
3^{95387} &\equiv 95387 \mod 100000\\
3^{195387} &\equiv 195387 \mod 1000000\\
3^{4195387} &\equiv 4195387 \mod 10000000\\
3^{64195387} &\equiv 64195387 \mod 100000000\\
3^{464195387} &\equiv 464195387 \mod 1000000000\\
&\vdots
\end{aligned}
$$

FIGURE 1. The unique solution of $3^n = n \mod 10^k$ for each $k \geq 2$

This phenomenon is reminiscent of p-adic integers. Indeed, the stabilization of the digits of an iterated exponential (or *tower*) modulo a fixed number is classically known, and is even used as a computational tool [Hit20]. However, in this case, the exponential operation is involved not only as an iteration of a fixed function but as a binary operation on the number system itself.

In this section, we will construct profinite systems of numbers, which can be regarded as p-adic number systems with exponentials. Using that structure, we will be able to answer the above question easily.

The rough sketch of our proof is as follows:

Answer (Rough sketch)**.** *In a topological rieg $\mathbb{N}_{\infty,10^\infty}$ (Definition 3.3.6), we can take the limit α of the sequence*

$$3, 3^3, 3^{3^3}, 3^{3^{3^3}}, 3^{3^{3^{3^3}}} \cdots \to \alpha.$$

By the continuity of $3^x \colon \mathbb{N}_{\infty,10^\infty} \to \mathbb{N}_{\infty,10^\infty}$, we have $3^\alpha = \alpha$.

Furthermore, the fixed point α turns out to be unique, which explains why the iteration in the above puzzle reaches the same answer regardless of the starting value: we will later regard 3^x as a contraction with respect to a natural metric and apply the Banach fixed-point theorem (Proposition 3.3.12).

3.1.3. *Phenomenon 3: Well-defined modulo exponentials.* Let us conclude this subsection by introducing the fact that first attracted the author to riegs. As far as the author knows, it was originally proven by Burris and Lee [BL92; BL93].

It is well-known that the addition and multiplications of natural numbers (or even of integers) are well-defined modulo n, for any positive integer $n \in \mathbb{N}$. It is just saying that $\mathbb{Z}/n\mathbb{Z}$ is a well-defined ring. But how about exponentials?

Puzzle 3.1.5. Find all positive integer $n > 0$ such that, for any positive integers a, b, a', b', we have

$$(a \equiv a' \mod n) \wedge (b \equiv b' \mod n) \implies (a^b \equiv a'^{b'} \mod n).$$

For the obvious reason, $n = 1$ satisfies the condition. Since a (positive) power of an odd (resp. even) number is odd (resp. even), $n = 2$ also satisfies the condition. However, $n = 3$ does not, since we have a counter example $2^1 \equiv 2 \not\equiv 1 \equiv 2^{1+3}$.

Answer (A special case of [BL92; BL93])**.** *There are exactly* 5 *possibilities:* $n = 1, 2, 6, 42, 1806$

3.2. **Finite arithmetic: the Burris-Lee theorem.** Ordinary modular arithmetic remembers only a residue. Exponentiation also needs a finite initial part in which small exponents remain distinct. The result is a finite arithmetic with a tail followed by a cycle.

3.2.1. *The Burris–Lee classification.*

Definition 3.2.1 ($\mathbb{N}_{a,b}$)**.** For a natural number $a \geq 0$ and a positive integer $b > 0$, let $\mathbb{N}_{a,b}$ be the $(a+b)$-element quotient $\mathbb{N}/\!\sim_{a,b}$, where

$$n \sim_{a,b} m \iff (n = m) \vee ((n, m \geq a) \wedge (n \equiv m \mod b)).$$

Thus the numbers below a form the initial exceptional part, and the numbers from a onward repeat with period b.

Figure 2 shows this tail–cycle picture for $\mathbb{N}_{3,4}$.

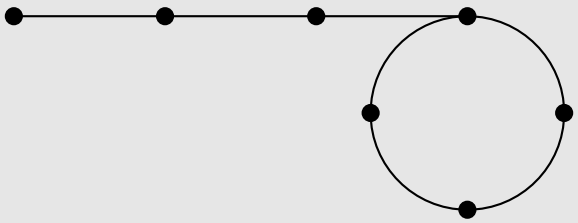


FIGURE 2. $\mathbb{N}_{3,4}$

By [BL92, Proposition 3.6], every finite quotient of the positive integers has this tail–cycle form. The same paper determines exactly when exponentiation descends to it.

Theorem 3.2.2 (Burris–Lee [BL92, Theorem 3.12])**.** *For $a \geq 0$ and $b > 0$, the canonical operations descend from $\mathbb{N}$ to $\mathbb{N}_{a,b}$ if and only if, for every prime p and every positive integer e,*

$$p^e \mid b \Longrightarrow e \leq a, \qquad p \mid b \Longrightarrow p - 1 \mid b.$$

Burris and Lee work with the positive integers and the language $\{+, \times, \uparrow, 1\}$.[2]

3.2.2. *Examples and the five cyclic models.*

Example 3.2.3 (The rieg of truth values)**.** The quotient $\mathbb{N}_{1,1}$ is the rieg of truth values $\mathbf{2} = \{\bot, \top\}$ from Section 5.

Example 3.2.4 (Parity rieg)**.** The quotient $\mathbb{N}_{1,2}$ is

$$\{0,\ \text{positive odd},\ \text{positive even}\},$$

which we call the *parity rieg*. Keeping 0 separate is essential: exponentiation does not descend to $\mathbb{Z}/2\mathbb{Z}$, since 2^0 is odd but 2^2 is even.

Example 3.2.5 (Overflow riegs)**.** For $n \geq 0$, the quotient $\mathbb{N}_{n,1}$ is the *overflow rieg with threshold* n, denoted by $\mathrm{OverFlow}_n$. Its elements are $0, 1, \ldots, n-1, \star$, where every natural number at least n is sent to $\star$.

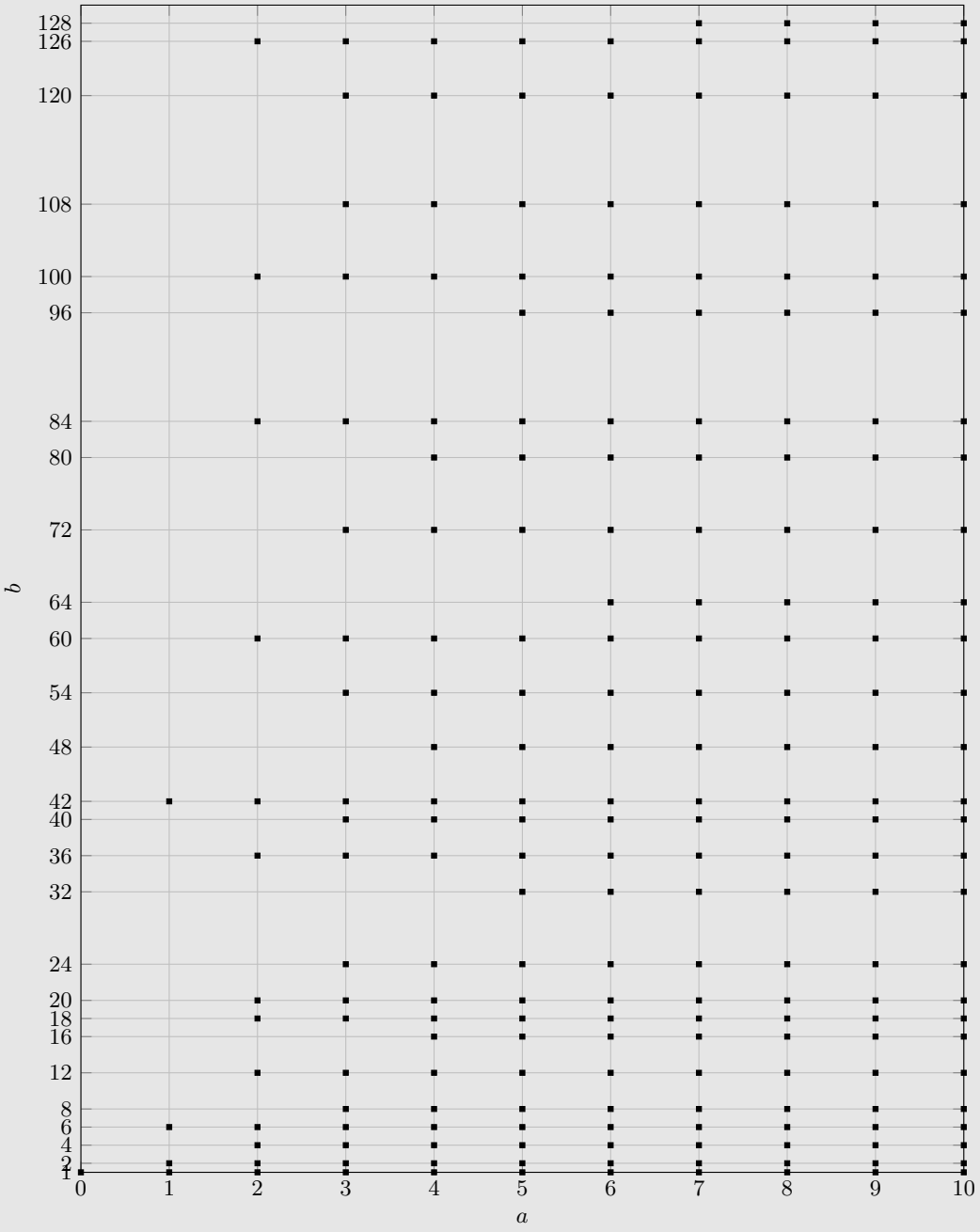


FIGURE 3. Finite quotient riegs of $\mathbb{N}$ for small a and b

$$
\begin{aligned}
a = 0 &: \ \mathbb{N}_{0,1} \\
a = 1 &: \ \mathbb{N}_{1,1}, \mathbb{N}_{1,2}, \mathbb{N}_{1,6}, \mathbb{N}_{1,42}, \mathbb{N}_{1,1806} \\
a = 2 &: \ \mathbb{N}_{2,1}, \mathbb{N}_{2,2}, \mathbb{N}_{2,4}, \mathbb{N}_{2,6}, \mathbb{N}_{2,12}, \mathbb{N}_{2,18}, \mathbb{N}_{2,20}, \mathbb{N}_{2,36}, \mathbb{N}_{2,42}, \mathbb{N}_{2,60}, \mathbb{N}_{2,84}, \dots \\
a = 3 &: \ \mathbb{N}_{3,1}, \mathbb{N}_{3,2}, \mathbb{N}_{3,4}, \mathbb{N}_{3,6}, \mathbb{N}_{3,8}, \mathbb{N}_{3,12}, \mathbb{N}_{3,18}, \mathbb{N}_{3,20}, \mathbb{N}_{3,24}, \mathbb{N}_{3,36}, \mathbb{N}_{3,40}, \dots \\
a = 4 &: \ \mathbb{N}_{4,1}, \mathbb{N}_{4,2}, \mathbb{N}_{4,4}, \mathbb{N}_{4,6}, \mathbb{N}_{4,8}, \mathbb{N}_{4,12}, \mathbb{N}_{4,16}, \mathbb{N}_{4,18}, \mathbb{N}_{4,20}, \mathbb{N}_{4,24}, \mathbb{N}_{4,36}, \dots \\
&\ \ \vdots \\
\text{“}a = \infty\text{”} &: \ \mathbb{N}
\end{aligned}
$$

FIGURE 4. Finite quotient riegs of $\mathbb{N}$, arranged by a

The theorem gives all finite quotient riegs at once. Figures 3 and 4 keep their distribution visible.

When $a = 1$, the positive part has no tail: its successor operation is a single cycle. Following [AJ25], we call such positive algebras *cyclic models*. There are surprisingly few of them.

Corollary 3.2.6 ([BL92, Corollary 3.14], attributed there to D. Higgs)**.** *The only finite quotient riegs of* $\mathbb{N}$ *with cyclic positive part are*

$$\mathbb{N}_{1,1}, \quad \mathbb{N}_{1,2}, \quad \mathbb{N}_{1,6}, \quad \mathbb{N}_{1,42}, \quad \mathbb{N}_{1,1806}.$$

Equivalently, if a rieg R has a least positive integer n such that

$$1 = 1 + \underbrace{1 + \cdots + 1}_{n},$$

then n is one of $1, 2, 6, 42, 1806$. This is precisely the puzzle in Section 3.1.3; no separate calculation is needed here.

Example 3.2.7. The number $8 = 2^3$ satisfies both conditions in Theorem 3.2.2 with $a = 3$. Hence $\mathbb{N}_{3,8}$ is a rieg. This is exactly the finite arithmetic used in the high-school calculation of Section 3.1.1.

Example 3.2.8. The number 10 fails the second Burris–Lee condition, since $5 \mid 10$ but $4 \nmid 10$. For every $n \geq 2$, however, $10^n = 2^n 5^n$ and $4 \mid 10^n$, so $\mathbb{N}_{n,10^n}$ is a rieg. These riegs form the finite inverse system used below to construct the topological rieg of 10-adic natural numbers (Definition 3.3.6).

3.2.3. *Characteristics of riegs.* Recall that the characteristic of a ring R is the smallest positive integer n such that $0 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$, if such an n exists; otherwise, the characteristic is defined to be 0. For quotient rigs and riegs, we need to record both the beginning of the cycle and its period. We order $\mathbb{N} \times \mathbb{N}^*$ by

$$(a, b) \leq (a', b') \quad \Longleftrightarrow \quad a \leq a' \text{ and } b \mid b'.$$

Definition 3.2.9 (Characteristic)**.** The *characteristic* of a rig or rieg R, denoted by $\mathrm{char}R$, is the minimum pair $(a, b) \in \mathbb{N} \times \mathbb{N}^*$ such that

$$\underbrace{1 + \cdots + 1}_{a \text{ times}} = \underbrace{1 + \cdots + 1}_{a \text{ times}} + \underbrace{1 + \cdots + 1}_{b \text{ times}},$$

if it exists. Otherwise, we put $\mathrm{char}R = (\infty, 0)$, where $(\infty, 0)$ is a formal maximum element.

[2]For $a \geq 1$, their algebra $N_{a,b}$ is the positive part of $\mathbb{N}_{a,b}$. Adjoining a distinct 0 adds only the forced rules for 0, so it adds no new condition. For $a = 0$, the displayed conditions force $b = 1$, which gives the degenerate rieg.

Corollary 3.2.10 (Burris–Lee theorem in terms of rieg characteristics [BL92; BL93])**.** *A pair* $(a, b) \in \mathbb{N} \times \mathbb{N}^*$ *is the characteristic of a rieg if and only if*

$$p^e \mid b \Longrightarrow e \leq a, \qquad p \mid b \Longrightarrow p - 1 \mid b$$

for every prime p *and every positive integer* e*.*

Remark 3.2.11 (Why this definition is natural)**.** Let R be a rig or rieg. Factor the unique homomorphism from the initial object as

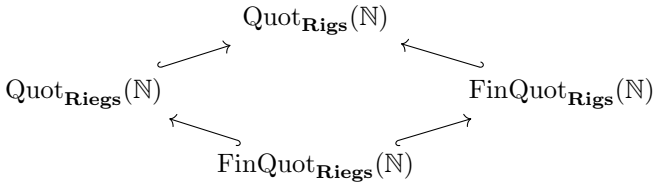
$$\mathbb{N} \twoheadrightarrow \mathrm{Im}(\mathbb{N} \to R) \rightarrowtail R.$$

If this image is finite, then it is $\mathbb{N}_{a,b}$ and $\mathrm{char}R = (a, b)$. If the map $\mathbb{N} \to R$ is injective, then $\mathrm{char}R = (\infty, 0)$. The usual definition for rings cannot be used directly: if a positive integer n satisfies $n = 0$ in a rieg, then $n - 1$ is an additive inverse of 1, and the rieg is degenerate by Claim 2.3.1.

This viewpoint makes sense for any equational theory: for an algebra R, the image of the canonical map from the initial algebra is a quotient of the initial algebra, and this quotient deserves to be called the *characteristic* of R in general. For rings, the initial algebra is $\mathbb{Z}$, the image is $\mathbb{Z}/n\mathbb{Z}$, and we recover the usual characteristic n. For riegs, the image is $\mathbb{N}_{a,b}$, and $\mathrm{char}R = (a, b)$ is just a name for this quotient.

3.3. **Profinite arithmetic: a total exponentiation.** In this subsection, we take the profinite completion of the initial rieg $\mathbb{N}$ and describe it explicitly. Its underlying set turns out to be $\mathbb{N} \sqcup \widehat{\mathbb{Z}}$. The main point is not that the exponentiation is total—this holds in every rieg by definition—but where it is total: although no non-degenerate ring admits a rieg structure (Proposition 2.3.2), the completion contains the profinite ring $\widehat{\mathbb{Z}}$, and the exponentiation x^y is still defined for all pairs.

3.3.1. *Profinite natural numbers with total exponentiation.* For $\mathcal{C} = \mathbf{Rigs}$ or $\mathbf{Riegs}$, let $\mathrm{Quot}_{\mathcal{C}}(\mathbb{N})$ denote the poset of quotient $\mathcal{C}$-algebras of $\mathbb{N}$. We put $Q \leq Q'$ if there is a quotient map $Q' \twoheadrightarrow Q$ compatible with the maps from $\mathbb{N}$. Let $\mathrm{FinQuot}_{\mathcal{C}}(\mathbb{N})$ denote its subposet of finite quotients. Thus we use four notations, which form a square of subposets of $\mathrm{Quot}_{\mathbf{Rigs}}(\mathbb{N})$:



Going down-left in the square imposes the arithmetic condition of Theorem 3.2.2 (admitting a rieg structure); going down-right imposes finiteness. The smallest poset $\mathrm{FinQuot}_{\mathbf{Riegs}}(\mathbb{N})$, placed at the bottom, satisfies both conditions. Every finite quotient rig is of the form $\mathbb{N}_{a,b}$. The finite quotient riegs are the ones that satisfy Theorem 3.2.2, and $\mathbb{N}$ is the maximum element of each full quotient poset. For two finite quotients, the order is

$$\mathbb{N}_{a,b} \leq \mathbb{N}_{a',b'} \quad \Longleftrightarrow \quad a \leq a' \text{ and } b \mid b'.$$

Recall that the profinite completion of an algebraic structure is the limit of its finite quotient algebras (Section A.2).

Definition 3.3.1. The *rieg of profinite natural numbers* $\widehat{\mathbb{N}}$ is the profinite completion of the initial rieg $\mathbb{N}$.

Thus

$$\widehat{\mathbb{N}} := \lim \left(\mathrm{FinQuot}_{\mathbf{Riegs}}(\mathbb{N})^{\mathrm{op}} \to \mathbf{Riegs} \right).$$

Lemma 3.3.2. *The quotient rieg $\mathbb{N}_{n,n!}$ exists for every $n \in \mathbb{N}$. Moreover, the family*

$$\{\mathbb{N}_{n,n!} \mid n \in \mathbb{N}\}$$

is cofinal in $\mathrm{FinQuot}_{\mathbf{Riegs}}(\mathbb{N})$.

Proof. Suppose that p is prime and that $p^e \mid n!$, where e is maximal. Counting the factors divisible by p^k gives

$$e = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \leq \sum_{k=1}^{\infty} \frac{n}{p^k} = \frac{n}{p-1} \leq n.$$

Moreover, if $p \mid n!$, then $p \leq n$, so $p-1$ divides $n!$. Thus $\mathbb{N}_{n,n!}$ is a rieg by Theorem 3.2.2.

Now let $\mathbb{N}_{a,b}$ be a finite quotient rieg and take $n = \max(a,b)$. Then $a \leq n$ and $b \mid n!$, so

$$\mathbb{N}_{a,b} \leq \mathbb{N}_{n,n!}.$$

This proves cofinality. □

Proposition 3.3.3. *The profinite rieg $\widehat{\mathbb{N}}$ is the limit of the following diagram.*

$$\cdots \xrightarrow{\pi_4} \mathbb{N}_{3,3!} \xrightarrow{\pi_3} \mathbb{N}_{2,2!} \xrightarrow{\pi_2} \mathbb{N}_{1,1!} \xrightarrow{\pi_1} \mathbb{N}_{0,0!}$$

Proof. By Lemma 3.3.2, the order-preserving functor

$$\mathbb{N} \longrightarrow \mathrm{FinQuot}_{\mathbf{Riegs}}(\mathbb{N}), \qquad n \longmapsto \mathbb{N}_{n,n!},$$

is final. Therefore, it gives the same limit. □

Theorem 3.3.4 (The underlying set of $\widehat{\mathbb{N}}$)**.** *The underlying set of $\widehat{\mathbb{N}}$ is*

$$\widehat{\mathbb{N}} = \mathbb{N} \sqcup \widehat{\mathbb{Z}},$$

where $\widehat{\mathbb{Z}}$ denotes the usual set of profinite integers. The canonical projection $\pi_{a,b} \colon \widehat{\mathbb{N}} \to \mathbb{N}_{a,b}$ restricts to the canonical maps

$$\mathbb{N} \twoheadrightarrow \mathbb{N}_{a,b}$$

and

$$\widehat{\mathbb{Z}} \twoheadrightarrow \mathbb{Z}/b\mathbb{Z} \rightarrowtail \mathbb{N}_{a,b}.$$

Proof. By Proposition 3.3.3 and lemma A.2.1, an element of $\widehat{\mathbb{N}}$ is a compatible sequence

$$(x_n \in \mathbb{N}_{n,n!})_{n \geq 0}.$$

Suppose that one coordinate is an exceptional element $k < n$. Compatibility then gives

$$x_m = \begin{cases} k & (m > k), \\ [k] & (m \leq k). \end{cases}$$

Hence the sequence comes from the natural number k. Otherwise, every coordinate belongs to the modular part $\mathbb{Z}/n!\mathbb{Z} \subset \mathbb{N}_{n,n!}$, so the sequence is an element of

$$\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n!\mathbb{Z}.$$

Conversely, every element of $\mathbb{N}$ and every element of $\widehat{\mathbb{Z}}$ gives a compatible sequence of the indicated form. □

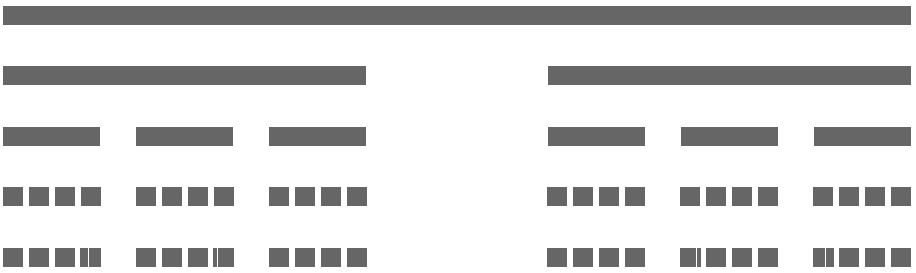


FIGURE 5. $\widehat{\mathbb{Z}}$ as limits of $\mathbb{Z}/n!\mathbb{Z}$

Corollary 3.3.5 (The unique continuous extension of exponentiation)**.** *The exponentiation of* $\mathbb{N}$ *extends to a continuous operation*

$$(-)^{(-)} \colon \widehat{\mathbb{N}} \times \widehat{\mathbb{N}} \longrightarrow \widehat{\mathbb{N}}$$

defined for all pairs of elements, and such a continuous extension is unique.

Proof. The limit defining $\widehat{\mathbb{N}}$ is taken in the category of topological riegs. Hence its operations, including exponentiation, are defined coordinatewise and are continuous by Lemma A.2.1.

For the uniqueness, it suffices to show that the image of $\mathbb{N}$ is dense in $\widehat{\mathbb{N}}$: then $\mathbb{N}\times\mathbb{N}$ has dense image in $\widehat{\mathbb{N}}\times\widehat{\mathbb{N}}$, and two continuous maps into the Hausdorff space $\widehat{\mathbb{N}}$ that agree on a dense subset must coincide. By Proposition 3.3.3, every non-empty basic open subset of $\widehat{\mathbb{N}}$ is the preimage of a non-empty subset $S \subseteq \mathbb{N}_{n,n!}$ under the projection $\widehat{\mathbb{N}} \to \mathbb{N}_{n,n!}$ for some $n \in \mathbb{N}$. Since the composite $\mathbb{N} \twoheadrightarrow \mathbb{N}_{n,n!}$ is surjective, this preimage contains an element of $\mathbb{N}$. □

This is different from the usual p-adic exponentiation, which is not defined on all pairs in $\mathbb{Z}_p \times \mathbb{Z}_p$. In fact, a non-degenerate ring cannot be a rieg by Proposition 2.3.2. The summand $\mathbb{N}$ in Theorem 3.3.4 is what makes $\widehat{\mathbb{N}}$ different from a ring.

By using a smaller diagram of finite quotient riegs, we obtain variants of $\widehat{\mathbb{N}}$. The following one appeared in Phenomenon 2 (Section 3.1.2).

Definition 3.3.6 (The topological rieg of 10-adic natural numbers)**.** The *topological rieg of* 10*-adic natural numbers* $\mathbb{N}_{\infty,10^\infty}$ is the limit of the following diagram in the category of topological riegs:

$$\cdots \twoheadrightarrow \mathbb{N}_{4,10^4} \twoheadrightarrow \mathbb{N}_{3,10^3} \twoheadrightarrow \mathbb{N}_{2,10^2}.$$

By Example 3.2.8, each $\mathbb{N}_{n,10^n}$ is a rieg for $n \geq 2$.

By the same argument as in Theorem 3.3.4, the underlying set of $\mathbb{N}_{\infty,10^\infty}$ is given by

$$\mathbb{N}_{\infty,10^\infty} = \mathbb{N} \sqcup \mathbb{Z}_{10} = \mathbb{N} \sqcup (\mathbb{Z}_2 \times \mathbb{Z}_5),$$

where $\mathbb{Z}_{10} \coloneqq \lim_n(\mathbb{Z}/10^n\mathbb{Z}) \cong \mathbb{Z}_2 \times \mathbb{Z}_5$ denotes the set of 10-adic integers.

Remark 3.3.7 (No 5-adic analogue)**.** This construction does not work for the powers of a single odd prime, say 5: since $5 \mid 5^n$ but $4 = 5 - 1 \nmid 5^n$, the second condition in Theorem 3.2.2 fails. Hence the rig $\mathbb{N}_{a,5^n}$ admits no rieg structure for any a. In this sense, there is no topological rieg of "5-adic natural numbers" $\mathbb{N} \sqcup \mathbb{Z}_5$ obtained in this way.

3.3.2. *Contractive exponential dynamics.*

Definition 3.3.8 (Carmichael function [Car10])**.** For a positive integer n, the *Carmichael function* $\lambda(n)$ is the least positive integer d such that

$$u^d \equiv 1 \pmod{n}$$

for every $u \in (\mathbb{Z}/n\mathbb{Z})^\times$. Equivalently, $\lambda(n)$ is the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^\times$.

Remark 3.3.9 (The jump function)**.** With respect to the divisibility order, the Carmichael function has a right adjoint $\lambda^*\colon \mathbb{N}^* \to \mathbb{N}^*$, whose notation λ^* we borrow from [CP09, Theorem 5.2(b)]. Thus

$$\lambda(b') \mid b \quad \Longleftrightarrow \quad b' \mid \lambda^*(b).$$

Therefore, $\lambda^*(b)$ records the possible next periods b' for which exponentiation raises the precision.

Lemma 3.3.10 (A metric for an inverse sequence)**.** *Let*

$$X = \lim(\cdots \twoheadrightarrow X_2 \twoheadrightarrow X_1 \twoheadrightarrow X_0)$$

be an inverse limit of non-empty finite sets and surjective maps, where X_0 has one element. Write $\pi_n\colon X \to X_n$ for the projections. For distinct $x, y \in X$, let

$$\nu(x,y) = \max\{n \in \mathbb{N} \mid \pi_i(x) = \pi_i(y) \text{ for every } i \le n\},$$

and put

$$d(x,y) = 2^{-\nu(x,y)}, \qquad d(x,x) = 0.$$

Then (X,d) is a complete ultrametric space.

Suppose that a map $F\colon X \to X$ satisfies

$$\pi_n(x) = \pi_n(y) \quad \Longrightarrow \quad \pi_{n+1}(F(x)) = \pi_{n+1}(F(y))$$

for every $n \ge 0$. Then F is a contraction with Lipschitz constant $\frac{1}{2}$.

Proof. The ultrametric inequality follows because two elements that agree with a third element through level n also agree with each other through level n. A Cauchy sequence stabilizes at every finite level. These stable coordinates form an element of X, so the metric is complete.

If x and y agree through level n, then $F(x)$ and $F(y)$ agree through level $n+1$. Hence

$$d(F(x),F(y)) \le \frac{1}{2} d(x,y).$$

□

We now use another inverse sequence for the same topological rieg:

$$\cdots \twoheadrightarrow \mathbb{N}_{4,10^4} \twoheadrightarrow \mathbb{N}_{3,10^3} \twoheadrightarrow \mathbb{N}_{2,100} \twoheadrightarrow \mathbb{N}_{2,20} \twoheadrightarrow \mathbb{N}_{2,4} \twoheadrightarrow \mathbb{N}_{2,2} \twoheadrightarrow \mathbb{N}_{2,1}.$$

All the displayed objects are quotient riegs by Theorem 3.2.2. Adding the last four quotients does not change the limit in Definition 3.3.6. The periods in this sequence are

$$1 \mid 2 \mid 4 \mid 20 \mid 100 \mid 1000 \mid 10^4 \mid \cdots.$$

The standard formula for the Carmichael function [Car10] gives

$$\lambda(2) = 1, \quad \lambda(4) = 2, \quad \lambda(20) = 4, \quad \lambda(100) = 20,$$

and

$$\lambda(10^{k+1}) \mid 10^k \qquad (k \ge 2).$$

The modular parts of this inverse sequence have limit

$$\mathbb{Z}_{10} = \mathbb{Z}_2 \times \mathbb{Z}_5.$$

We equip this limit with the metric in Lemma 3.3.10. Since $\mathbb{N}_{\infty,10^\infty}$ is a topological rieg, its total exponentiation defines a map

$$T\colon \mathbb{N}_{\infty,10^\infty} \longrightarrow \mathbb{N}_{\infty,10^\infty}, \qquad T(x) = 3^x.$$

This map preserves the modular part: at each finite quotient, a modular exponent can be represented by an integer m above the tail, and 3^m is again above the tail. If two elements of the modular part agree modulo a period b, then their images agree modulo the next period b': indeed, $\lambda(b') \mid b$ and 3 is invertible modulo b'. Therefore, T raises the agreement by one level. By Lemma 3.3.10, the restriction

$$T\colon \mathbb{Z}_2 \times \mathbb{Z}_5 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_5$$

is a contraction with Lipschitz constant $\frac{1}{2}$.

Lemma 3.3.11 (Stabilization of the last two digits)**.** *For every element ξ of the modular part $\mathbb{Z}/10^2\mathbb{Z} \subset \mathbb{N}_{2,10^2}$, we have $T^4(\xi) = [87]$.*

Proof. The first four transitions of the above sequence give

$$T(\xi) \equiv 1 \pmod 2, \qquad T^2(\xi) \equiv 3 \pmod 4,$$

and then

$$T^3(\xi) \equiv 3^3 \equiv 7 \pmod{20}, \qquad T^4(\xi) \equiv 3^7 \equiv 87 \pmod{100}.$$

□

Proposition 3.3.12 (The unique fixed point of 3^x)**.** *The function $T(x) = 3^x$ on $\mathbb{N}_{\infty,10^\infty}$ has a unique fixed point α, which belongs to $\mathbb{Z}_2 \times \mathbb{Z}_5$, and every iteration sequence $x, T(x), T^2(x), \dots$ starting from $x \in \mathbb{Z}_2 \times \mathbb{Z}_5$ converges to α. Furthermore, for each $k \geq 2$, the reduction of α is the unique solution of $3^x = x$ in $\mathbb{Z}/10^k\mathbb{Z} \subset \mathbb{N}_{k,10^k}$ (cf. Figure 1).*

Proof. There is no fixed point in the natural-number part, since $3^n > n$ for every $n \in \mathbb{N}$. On the modular part, the map T is a contraction on a non-empty complete metric space. The Banach fixed-point theorem gives a unique fixed point $\alpha \in \mathbb{Z}_2 \times \mathbb{Z}_5$, and every iteration sequence in the modular part converges to α.

It remains to prove the statement at each finite level. If $r \in \mathbb{Z}/10^2\mathbb{Z}$ satisfies $3^r = r$, then

$$r = T^4(r) = [87]$$

by Lemma 3.3.11. Suppose that the solution is unique modulo 10^k, and let r and r' be solutions modulo 10^{k+1}. Their reductions modulo 10^k coincide. Since $\lambda(10^{k+1}) \mid 10^k$, we obtain

$$r = 3^r \equiv 3^{r'} = r' \pmod{10^{k+1}}.$$

Hence the solution is unique at every level. The reduction of α gives its existence. □

We close this subsection by determining the solutions of another exponential equation, $x^x = x$, in the same topological rieg.

Proposition 3.3.13 (The solutions of $x^x = x$)**.** *In $\mathbb{N}_{\infty,10^\infty} = \mathbb{N} \sqcup (\mathbb{Z}_2 \times \mathbb{Z}_5)$, the equation $x^x = x$ has exactly 11 solutions: the element 1 of the summand $\mathbb{N}$, and the ten elements*

$$(0,0),\ (0,1), \qquad (1,0),\ (1,1),\ (1,i),\ (1,-1),\ (1,-i), \qquad (-1,0),\ (-1,1),\ (-1,-1)$$

of $\mathbb{Z}_2 \times \mathbb{Z}_5$, where $\mu_4 = \{1, i, -1, -i\}$ denotes the group of fourth roots of unity in ${\mathbb{Z}_5}^\times$.

Proof. In the summand $\mathbb{N}$, we have $0^0 = 1 \neq 0$, $1^1 = 1$, and $n^n > n$ for $n \geq 2$, so 1 is the only solution there.

Let x belong to the modular part $\mathbb{Z}_2 \times \mathbb{Z}_5$, let $k \geq 2$, and choose an integer $n \geq k$ with $n \equiv x \pmod{10^k}$. Since $\mathbb{N}_{k,10^k}$ is a rieg (Example 3.2.8), the reduction of x^x to $\mathbb{Z}/10^k\mathbb{Z}$ is $[n^n]$. Therefore,

$$(*) \qquad x^x = x \iff n^n \equiv n \pmod{10^k} \text{ for every } k \geq 2.$$

Below, v_p denotes the p-adic valuation and p ranges over $\{2, 5\}$.

First, suppose $1 \leq v_p(x) < \infty$ and put $a \coloneqq v_p(x)$. Taking $k > a$ in $(*)$, we have $v_p(n) = a$, and $n^n - n = n(n^{n-1} - 1)$ with $p \mid n$ and $n - 1 \geq 1$, so $p \nmid n^{n-1} - 1$ and

$$v_p(n^n - n) = a < k,$$

contradicting $(*)$. Hence each of the two coordinates of $x \in \mathbb{Z}_2 \times \mathbb{Z}_5$ is either 0 or a unit.

Next, suppose that the p-coordinate u of x is a unit. Then $(*)$ modulo p^k reads $n^{n-1} \equiv 1 \pmod{p^k}$, i.e., the order of u in $(\mathbb{Z}/p^k\mathbb{Z})^\times$ divides $n - 1$. If $u = 1$, it is a torsion element of ${\mathbb{Z}_p}^\times$; assume $u \neq 1$ and put $s \coloneqq v_p(u - 1) < \infty$. Once $k > s$, we have $v_p(n - 1) = s$. For $p = 2$, the order of u is a power of 2 dividing $n - 1$, hence divides 2^s. For $p = 5$, the order divides $4 \cdot 5^{k-1}$; its 5-part divides $n - 1$, hence divides 5^s, while its prime-to-5 part divides 4. In both cases the orders are bounded independently of k, so u is a torsion element of ${\mathbb{Z}_p}^\times$. The torsion subgroup of ${\mathbb{Z}_2}^\times$ is $\{\pm 1\}$, and that of ${\mathbb{Z}_5}^\times$ is μ_4.

Finally, we determine which of the remaining 3×5 combinations satisfy $(*)$; note that the same representative n serves both coordinates. If the 2-coordinate is 0, then $4 \mid n$, so $n - 1$ is odd, and the order of the 5-coordinate must be odd: the 5-coordinate is 0 or 1. If the 2-coordinate is 1, then $2^k \mid n - 1$, so every order in $\{1, 2, 4\}$ divides $n - 1$: the 5-coordinate can be any element of $\{0\} \cup \mu_4$. If the 2-coordinate is -1, then $n \equiv 3 \pmod 4$, so $v_2(n - 1) = 1$: the order 2 divides $n - 1$ but 4 does not, and the 5-coordinate lies in $\{0, 1, -1\}$. This yields the $2 + 5 + 3 = 10$ listed elements. Conversely, each listed element satisfies $(*)$: a coordinate 0 gives $v_p(n) \geq k$, hence $n^n \equiv 0 \equiv n \pmod{p^k}$, and the case analysis above shows precisely that the order of each torsion coordinate divides $n - 1$. □

Remark 3.3.14 (The levelwise counts diverge)**.** Contrast Proposition 3.3.13 with Proposition 3.3.12, where every level has a unique solution. The numbers of solutions of $x^x = x$ in $\mathbb{Z}/10^k\mathbb{Z} \subset \mathbb{N}_{k,10^k}$ for $k = 2, 3, \ldots, 7$ are

$$22,\ 38,\ 196,\ 196,\ 1412,\ 1412,$$

and they are unbounded, even though the limit has only 11 points: for a unit $u \equiv 1 \pmod 4$ with $s \coloneqq v_2(u - 1)$, one has $v_2(u^{2^s} - 1) = 2s$, so u solves the 2-adic part of the equation modulo 2^k precisely when $k \leq 2s$. Pairing such u with the 5-coordinate 0 produces, for $k \geq 4$, at least $2^{\lfloor k/2 \rfloor}$ solutions at level k, almost all of which die at a later level. Note also that 0 is a solution in the summand $\mathbb{Z}_2 \times \mathbb{Z}_5$ but not in the summand $\mathbb{N}$: modulo 10^k, the class $[0]$ is represented by 10^k, and $(10^k)^{10^k} \equiv 0$. This illustrates the splitting $\mathbb{N} \sqcup \mathbb{Z}_{10}$ of Definition 3.3.6.

4. Example 2: Riegs in category theory and combinatorics

In this section, we consider the rieg structures obtained through decategorification. Since many of these are defined via universality, the verification of the rieg structure follows from abstract nonsense. However, when one tries to write them down explicitly, it looks non-trivial that all fourteen axioms of a rieg are satisfied.

For example, from abstract nonsense, it follows immediately that the set of all isomorphism classes of finite directed graphs admits a natural rieg structure. But can you imagine what the exponentiation looks like? For instance, consider a single edge $\to$, and then consider taking the exponential of that edge with itself, denoted $\to^{\to}$. The resulting graph is depicted in Figure 6: its four vertices are the four functions from the vertex set $\{0, 1\}$ of $\to$ to itself (the two constant functions c_0, c_1, the identity id, and the transposition swap), and it has exactly four edges, one of which is a loop. Notice that the vertex swap is isolated.

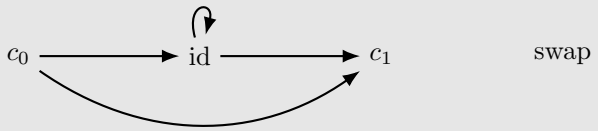


FIGURE 6. The exponential graph $\to^{\to}$

Regarding the decategorified semiring structure, numerous studies have been conducted under the name *Burnside rig*. However, to the author's knowledge, research on its exponential structure has been very limited. Despite the exponential structure satisfying numerous equations in the definition of rieg, these have been left unused. See [Sch00b]

4.1. **Burnside rieg of CCC with finite coproducts (and a topos).**

4.1.1. *The Burnside rieg functor* $\mathfrak{B}$.

Definition 4.1.1. The (1-)category **CCCc** is defined as follows:

- Its objects are small categories that are cartesian closed and have finite coproducts.
- Its morphisms are functors between these categories that preserve finite products, finite coproducts, and exponentials, where we consider functors up to natural isomorphism[3].

Proposition 4.1.2. *For a cartesian closed category $\mathcal{C}$ with finite coproducts, the set of isomorphism classes of $\mathcal{C}$ forms a rieg with the categorical initial object, the binary coproducts, the terminal object, the binary products, and the exponentials.*

Proof. All of the fourteen axioms are implied by the universalities. □

Remark 4.1.3 (Symmetric monoidal closed categories)**.** This construction does not work for a symmetric monoidal closed category with finite coproducts, since we use the fact that the product $A \times B$ is a categorical product to prove some axioms including $(x \times y)^z = x^z \times y^z$.

We borrow the following notation from [Men17] (and from [Sch90]).

Definition 4.1.4. The *Burnside rieg functor* $\mathfrak{B}\colon \mathbf{CCCc} \to \mathbf{Riegs}$ sends an object $\mathcal{C}$ of the category **CCCc** to the rieg induced by $\mathcal{C}$ (Proposition 4.1.2), and a functor in **CCCc** to the induced rieg homomorphisms.

Proposition 4.1.5 (Topos to rieg functor)**.** *For a locally cartesian closed small category $\mathcal{C}$ with finite coproduct (in particular, an elementary topos $\mathcal{C}$), the correspondence*

$$\mathrm{ob}(\mathcal{C}) \ni c \mapsto \mathfrak{B}(\mathcal{C}/c) \in \mathbf{Riegs}$$

defines a contravariant functor

$$\mathfrak{B}(\mathcal{C}/-)\colon \mathcal{C}^{\mathrm{op}} \to \mathbf{Riegs}.$$

Example 4.1.6 (Finite sets to natural numbers)**.** The Burnside rieg of finite sets is isomorphic to the rieg of natural numbers

$$\mathfrak{B}(\mathbf{FinSet}) \cong \mathbb{N}.$$

[3]The author admits that it is more natural to consider this category as a 2-category.

Example 4.1.7 (Infinite sets to cardinal arithmetic)**.** Let κ be an infinite cardinal and $\mathbf{Set}_{<\kappa}$ be the (essentially small) category of sets with cardinality less than κ. The category $\mathbf{Set}_{<\kappa}$ is a topos if and only if it is cartesian closed if and only if κ is a strong limit cardinal. Therefore, if κ is a strong limit cardinal, then we obtain the induced rieg $\mathfrak{B}(\mathbf{Set}_{<\kappa})$, which is the (small) rieg of cardinal arithmetic.

Obviously, the structure of this rieg is interconnected with set theory, especially continuum hypothesis. With the generalized continuum hypothesis, $\mathfrak{B}(\mathbf{Set}_{<\beth_\omega})$ is a countable rieg with $2^{\aleph_0} = \aleph_1$. However, without the GCH, there are many other possibilities of this rieg structure.

Example 4.1.8 (Finite presheaf topos)**.** For any small category $\mathcal{C}$, $\mathbf{FinSet}^{\mathcal{C}}$ has all finite limits and colimits. Therefore, if $\mathbf{FinSet}^{\mathcal{C}}$ is cartesian closed, we obtain a rieg $\mathfrak{B}(\mathbf{FinSet}^{\mathcal{C}})$. For example, if $\mathcal{C}$ is a finite category or a (possibly infinite) group, then $\mathbf{FinSet}^{\mathcal{C}}$ is known to be cartesian closed (and a topos).

- The category of finite functions $[\to, \mathbf{FinSet}]$ forms a rieg of multisets of natural numbers (or Dirichlet polynomials [SM23]).
- More generally, for any finite category $\mathcal{C}$, its finite (co)presheaf category $[\mathcal{C}, \mathbf{FinSet}]$ forms a rieg. Examples include the category of finite graphs $[\rightrightarrows, \mathbf{FinSet}]$ and the category of rooted forests $[\omega^{\mathrm{op}}, \mathbf{FinSet}]$.
- For any (possibly infinite) group G, the category of its finite actions $[G, \mathbf{FinSet}]$ forms the *Burnside rig* of the group G. Examples include the category of sets with involution $[\mathbb{Z}/2\mathbb{Z}, \mathbf{FinSet}]$ and the category of finite loops $[\mathbb{Z}, \mathbf{FinSet}]$.

On the other hand, the category of finite discrete dynamical systems $[\mathbb{N}, \mathbf{FinSet}]$ is not cartesian closed.

Question 4.1.9. *When is a finite presheaf category* $[\mathcal{C}^{\mathrm{op}}, \mathbf{FinSet}]$ *cartesian closed? The author is also interested in the closely related question: when is a finite presheaf category a topos?*

Example 4.1.10. HeyAlg Every Heyting algebra H is a cartesian closed poset with finite coproducts, and thus a rieg.

4.1.2. *Enumerations.* In many cases, to utilize the Burnside rieg $\mathfrak{B}(\mathcal{C})$ to enumerate something, we consider a *enumeration function* $|-| : \mathfrak{B}(\mathcal{C}) \to \mathbb{N}$, which is typically a rig homomorphism. There are several ways to choose such enumeration function.

Example 4.1.11 (Global sections for a connected topos)**.** For example, for a locally finite topos $\mathcal{C}$ we have the global section functor $\Gamma = \mathcal{C}(1, -) \colon \mathcal{C} \to \mathbf{FinSet}$, which preserves products, but not necessarily coproducts. If the topos $\mathcal{C}$ is connected (i.e., if Γ preserves finite coproduct), then the functor $\Gamma \colon \mathcal{C} \to \mathbf{FinSet}$ induces the rig homomorphism $|-|_\Gamma : \mathfrak{B}(\mathcal{C}) \to \mathbb{N}$ that counts the number of global sections.

Example 4.1.12 (Connected components for a stably locally connected topos)**.** If a topos $\mathcal{C}$ admits an adjoint triple $\pi_0 \dashv \Delta \dashv \Gamma \colon \mathcal{C} \to \mathbf{FinSet}$ such that π_0 preserves finite products (see *stable local connectedness* in [Joh11]), then the functor π_0 induces a rig homomorphism $|-|_{\pi_0} : \mathfrak{B}(\mathcal{C}) \to \mathbb{N}$.

Example 4.1.13 (Enumeration with a torsion-free atom.)**.** Let $\mathcal{E}$ be a small topos. Due to Proposition 4.1.5, every object $X \in \mathrm{ob}(\mathcal{E})$ induces a rieg homomorphism $\mathfrak{B}(\mathcal{E}) \xrightarrow{\mathfrak{B}(X \to 1)} \mathfrak{B}(\mathcal{E}/X)$. Therefore, if $\mathcal{E}/X \simeq \mathbf{FinSet}$, then we obtain a rieg homomorphism $\mathfrak{B}(\mathcal{E}) \to \mathbb{N}$. According to the terminology in [KM91], we call such an object X a *torsion-free atom*[4].

4.2. Riegs of functions $\mathfrak{B}(\mathbf{FinSet}^{\to})$: List of numbers and Liouville's divisor theorem.

[4]An object X of a topos $\mathcal{E}$ is an *atom* if it has exactly two subobjects. Following [KM91, Definitions 1.1 and 1.9], an object X of a topos with a geometric morphism $\gamma \colon \mathcal{E} \to \mathbf{FinSet}$ is *torsion-free* if every map with codomain X is locally monic relative to γ; in the topos of finite G-sets, for instance, this means that every G-orbit of X is free. If $\mathcal{E}/X \simeq \mathbf{FinSet}$, then X is a torsion-free atom in this sense.

4.2.1. *The Burnside rieg of functions* $\mathfrak{B}(\mathbf{FinSet}^{\to})$. Our first example is the Burnside rieg of the topos $\mathbf{FinSet}^{\to}$, which is called the topos of (finite) fucntions or the (finite) Sierpinski topos. An object of the topos is a function $p\colon A \to B$.

Since a function $f\colon A \to B$ can be regarded as a family of sets $\{f^{-1}(b)\}_{b\in B}$, the isomorphism classes of the topos $\mathbf{FinSet}^{\to}$ are in bijective correspondence with the finite multiset of natural numbers. Let $\mathrm{mult}(\mathbb{N})$ denote the set of all multisets of natural numbers. Each multiset will be denoted as a list of natural numbers $(), (3,1,4), (1,2,3,1,1,0,0) \in \mathrm{mult}(\mathbb{N})$, and rearranged lists are identified $(1,2,3,1,1,0,0) = (0,0,1,1,1,2,3) \in \mathrm{mult}(\mathbb{N})$.

The addition is given by a concatenation of lists, and the product is given by the list of all ccomponent-wise products.

$$(3,1,4) + (1,2,7,0) = (3,1,4,1,2,7,0)$$
$$(3,1,4) \times (1,2,7,0) = (3,6,21,0,1,2,7,0,4,8,28,0)$$

[SM23] explains that this rig structure is isomorphic to the rig of (formal) Dirichlet polynomials

$$\mathrm{mult}(\mathbb{N}) \cong \mathbb{N}\left[0^{-x}, 1^{-x}, 2^{-x}, \dots\right] \text{ in } \mathbf{Rigs}.$$

However, exponentials are different:

$$(n_1, \dots, n_k)^{(m)} = ({n_1}^m, \dots, {n_k}^m).$$

There is a unique extension of this exponential to all exponentials. For example,

$$\begin{aligned}(3,1,4)^{(2,0)} &= (3,1,4)^{(2)}(3,1,4)^{(0)}\\ &= (9,1,16)(1,1,1)\\ &= (9,9,9,1,1,1,16,16,16).\end{aligned}$$

Remark 4.2.1 ($\mathrm{mult}(R)$ and Artin gluing)**.**

4.2.2. *Liouville's theorem.* The equation

$$(1+2+3+\cdots+n)^2 = 1^3+2^3+\cdots+n^3$$

is well-known. As studied in [BS13], there are so many similar equations including

- $(1+2+2+4)^2 = 1^3+2^3+2^3+4^3$,
- $(1+2+2+3+5)^2 = 169 = 1^3+2^3+2^3+3^3+5^3$, and
- $(1+2+2+3+4+6)^2 = 1^3+2^3+2^3+3^3+4^3+6^3$.

So the question is: for a given finite list of natural numbers $(a_1, \dots a_n)$, does the equation

$$\left(\sum_{i=1}^{n} a_1\right)^2 = \sum_{i=1}^{n} a_i^3. \tag{1}$$

holds?

Writing $d(n)$ for the number of divisors of a positive integer n, Liouville's theorem states that

$$\left(\sum_{m|n} d(m)\right)^2 = \sum_{m|n} d(m)^3.$$

For example, in the case of $n = 10$, we obtain the equation

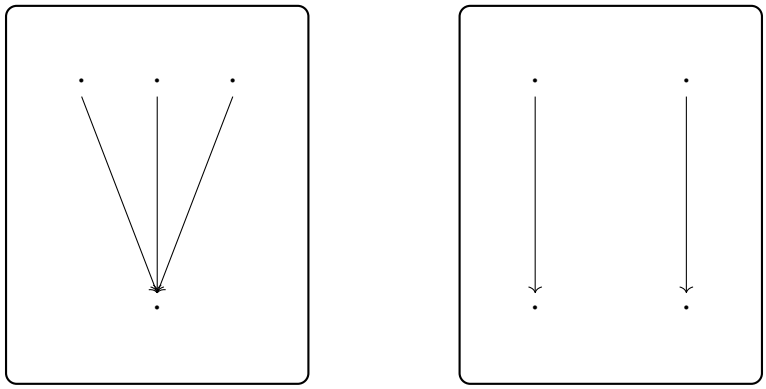
$$(d(1)+d(2)+d(5)+d(10))^2 = d(1)^3+d(2)^3+d(5)^3+d(10)^3.$$

The proof of this theorem is not difficult, and is just a highschool level problem. Given the equation $(1+2+3+\cdots+n)^2 = 1^3+2^3+\cdots+n^3$, it suffices to prove that the problem can be reduced to the case of $m = p^e$ for some prime number p. In other words, the only non-trivial part is to prove that if two sequence $(a_1,\dots,a_n)$ and $(b_1,\dots,b_m)$ satisfies the equation, so does their "product sequence" $(a_1\cdot b_1, a_1\cdot b_2,\dots,a_1\cdot b_m, a_2\cdot b_1,\dots,a_n\cdot b_m)$.

Here is a categorified (or Burnside) point of view. Consider the Burnside rieg $\mathfrak{B}(\mathbf{FinSet}^{\to})$ of the topos of functions between finite sets. We obtain the equivalence

$$\text{a list } C=(a_1,\dots a_n) \text{ satisfies Equation (1)} \iff \#\mathrm{Hom}(A,C) = \#\mathrm{Hom}(B,C),$$

where $A, B \in \mathbf{FinSet}^{\to}$ are given in Figure 7.



$A=(3)$ $\qquad$ $B=(1,1)$

FIGURE 7. The representing object of sum-of-cubes and square-of-sum in $\mathbf{FinSet}^{\to}$

4.3. **Rieg of finite groups.**

Counting problems. We will give a rieg-theoretic method to answer the following undergraduate-level counting problems.

Question 4.3.1. *For a finite group G, let n_G denote the number of subgroups whose index (= the number of cosets) is 2. Write $n_{G\times H}$ using n_G and n_H.*

Question 4.3.2. *Count the number of group homomorphisms from D_6 to itself. (Hint: D_6 is the dihedral group of order 12, and $D_6 \cong S_3\times C_2$.)*

Notice that all operations $0,1,+,\times,\uparrow$ of the cartesian closed category of finite groupoids $\mathrm{Groupoid}_{\mathrm{fin}}$ are well-defined up to equivalence. Therefore, (as a 2-categorical analogy of Proposition 4.1.2), the equivalence classes of finite groupoids, which are the formal sums of finite groups, form a rieg! The aim of this section is to concretely describe the rieg structure.

Definition 4.3.3. We definite *the rig of finite groups* $\mathcal{G}$ as follows:

- The underlying additive commutative monoid is the free commutative monoid of the set of isomorphism classes of finite groups, which is given by the finite formal sum.

$$\mathcal{G} := \bigoplus_{[G]:\ \text{iso.class}} \mathbb{N}$$

- The multiplication is given by the unique extension of
$$[G] \times [H] \coloneqq [G \times H].$$

Hereafter, the isomorphism class of a group G will be simply referred to as G.

Notation 4.3.4. The (isomorphism class of) the cyclic group $\mathbb{Z}/n\mathbb{Z}$ is denoted by C_n.

Example 4.3.5. Some examples of calculations include:

- $C_{12} = C_3 \times C_4$
- $D_6 = S_3 \times C_2$
- $(S_3 + C_2)^2 = {S_3}^2 + 2(S_3 \times C_2) + {C_2}^2 = {S_3}^2 + 2D_6 + {C_2}^2$

Definition 4.3.6 (Conjgacy classes of homomorphism)**.** Let G and H be finite groups.

- Two homomorphisms $\phi, \psi \colon G \to H$ are *conjugate* if there exists $h \in H$ such that $\phi = h\psi h^{-1}$ holds.
- The automorphism group (or the stabilizer) of a homomorphism $\phi \colon G \to H$ is the subgroup of H, defined by $\mathrm{Aut}(\phi) \coloneqq \{h \in H \mid h\phi h^{-1} = \phi\}$.

Theorem 4.3.7. *The rig of finite groups $\mathcal{G}$ admits the following rieg structure:*

- *For two finite groups G and H, its exponential H^G is defined by*
$$H^G \coloneqq \sum_{[\phi]:conj.class} \mathrm{Aut}(\phi)$$
- *In general, the exponential is defined by*
$$\left(\sum_j H_j\right)^{\left(\sum_i G_i\right)} \coloneqq \prod_i \sum_j \left({H_j}^{G_i}\right),$$
for any two families of finite groups $(G_i)_i$ and $(H_j)_j$.

Proof. This is the rieg of equivalent classes of finite groupoids, explained at the beginning of this section. □

Example 4.3.8. Let's try to calculate ${D_6}^{D_6}$. In order to utilize the exponential rules, we first calculate smaller parts:

- ${C_2}^{C_2} = 2 \cdot C_2$
- ${C_2}^{S_3} = 2 \cdot C_2$
- ${S_3}^{C_2} = C_2 + S_3$
- ${S_3}^{S_3} = 1 + C_2 + S_3$

Then we obtain
$${D_6}^{D_6} = \left({S_3}^{S_3}\right)^{C_2} \cdot \left({C_2}^{S_3}\right)^{C_2} = (1 + C_2 + S_3)^{C_2} \cdot (2 \cdot C_2)^{C_2} = (1 + 3 \cdot C_2 + S_3) \cdot (4 \cdot C_2) = 4 \cdot C_2 + 12 \cdot {C_2}^2 + 4 \cdot D_6.$$

Some properties of finite groups, like being abelian, are characterized in terms of this rieg structure.

Proposition 4.3.9. *For a finite group A,*

- *if A is abelian, then we have $A^G = \#\mathrm{Hom}(G, A) \cdot A$.*
- *conversely, if A^G is a sum of A for any G, then A is abelian.*

Proof. The former statement is immediate from the definition. If A^G is a sum of A for any G, then A^A is a sum of A. Especially, we have $\mathrm{Aut}(\mathrm{id}_A) = A$ and A is abelian. □

Now we can answer the first problem, Question 4.3.1!

Answer (to Question 4.3.1)**.** *Since* ${C_2}^G = (n_G+1)\cdot C_2$*, we have*

$$(n_{G\times H}+1)\cdot C_2 = {C_2}^{G\times H} = \left({C_2}^G\right)^H = (n_G+1)\cdot {C_2}^H = (n_G+1)\cdot(n_H+1)\cdot C_2.$$

This proves $n_{G\times H} = n_G\cdot n_H + n_G + n_H$*.*

Remark 4.3.10. For a limit cardinal κ, one can consider a rieg of larger groups, in which we can similarly consider representations of product groups, like ${\mathbb{C}\mathbf{Vect}_{\text{f.d.iso.}}}^{G\times H} = \left(\sum_{k=0}^{\infty}\mathrm{GL}_k(\mathbb{C})\right)^{G\times H}$.

4.3.1. *Groupoid cardinality.* In order to utilize riegs for counting something, the basic rieg theoretic method is to consider a **rig** homomorphism from a given rieg to the rig of numbers, like $\mathbb{N},\mathbb{Z},\mathbb{Q}$.

For the rieg of finite groups $\mathcal{G}$, the notion of *groupoid cardinality*, introduced in [BD01], is useful. We can utilize it to obtain rational numbers from elements of $\mathcal{G}$.

Definition 4.3.11. For $x=\sum_i G_i\in\mathcal{G}$, its *groupoid cardinality* $|x|\in\mathbb{Q}$ is defined by

$$|x| \coloneqq \sum_i \frac{1}{\#G_i}.$$

Proposition 4.3.12. *The groupoid cardinality function* $|-|:\mathcal{G}\to\mathbb{Q}$ *is a rig homomorphism. Furthermore, for finite groups* G *and* H*, we have*

$$\left|G^H\right| = \frac{\#\mathrm{Hom}(H,G)}{\#G}.$$

Proof. For sums and products, the proof is easy. Regarding exponentials, one can use the orbit-stabilizer theorem for the conjugate action of G on $\mathrm{Hom}(H,G)$. □

Exercise 4.3.13. Check that Proposition 4.3.12 is compatible with Proposition 4.3.9.

Let us finish this introductory note by giving the answer to Question 4.3.2!

Answer (to Question 4.3.2)**.** *In Example 4.3.8, we obtained* ${D_6}^{D_6} = 4\cdot C_2 + 12\cdot {C_2}^2 + 4\cdot D_6$*. By taking the groupoid cardinality, we obtain*

$$\frac{\#\mathrm{Hom}(D_6,D_6)}{12} = \frac{4}{2}+\frac{12}{4}+\frac{4}{12}.$$

This proves that $\#\mathrm{Hom}(D_6,D_6)=64$*.*

5. Example 3: Riegs in logic

In this subsection, we investigate the riegs that consist of "propositions." The motivating examples are the rieg of truth values and the rieg of subsets:

Example 5.0.1 (Rieg of truth values)**.** The set of truth values $\mathbf{2}=\{\bot,\top\}$ has a natural rieg structure, as $(\mathbf{2},\bot,\top,\vee,\wedge,\leftarrow)$. This is isomorphic to the overflow rieg with threshold 1 and $\mathbb{N}_{1,1}$.

Example 5.0.2 (Powerset)**.** For any set X, its powerset $\mathcal{P}(X)$ has a rieg structure with $(\mathcal{P}(X),\emptyset,X,\cup,\cap,\leftarrow)$, where $A\leftarrow B$ is defined to be $A\cup B^c$. More generally, every Heyting algebra[5] is a rieg.

When $X=\emptyset$, its powerset rieg is the degenerate rieg. When X is a singleton, its power rieg is the rieg of truth values.

The above riegs have special properties:

- $1+1=1$
- The underlying rig is a lattice

[5] or CCC

- They are Heyting algebras.

For each property, we have a class of riegs. We will study them one by one.

5.1. **Riegs in which $1+1=1$.**

Proposition 5.1.1. *For a rieg R, the followings are equivalent:*

(1) $1+1=1$
(2) $\mathrm{char}R=(0,1)$ *or* $(1,1)$
(3) There is a rieg homomorphism from the rieg of truth values $\mathbf{2}=\{\bot,\top\}$
(4) The addition is idempotent. (i.e., for any $x\in R$, $x+x=x$*)*
(5) Both addition and multiplication are idempotent. (i.e, for any $x\in R$, $x+x=x\times x=x$*)*

Proof. The equivalence between 1, 2 and 3 follows from the definition of characteristics. By multiplying x, we have 1 $\implies$ 4. To prove 5 from 1, we can use

$$x\times x=x^{1+1}=x^1=x.$$

The remaining implications are trivial.

□

Example 5.1.2 (Max-plus is not a rieg)**.** The max-plus algebra $(\mathbb{R}\cup\{-\infty\},-\infty,\oplus,0,\otimes)$ admits no rieg structures. If it admits a rieg structure, since $1\oplus 1=\max(1,1)=1$, the multiplication $\otimes$, (which is the addition in the usual sense) should also be idempotent. However, $1\otimes 1=1+1=2\neq 1$, contradiction.

Definition 5.1.3. A rieg R is said to be *idempotent*, if it satisfies the conditions of Proposition 5.1.1.

Remark 5.1.4. (Multiplicatively idempotent riegs) Even if a rieg R is multiplicatively idempotent, it might not be additively idempotent. For example, the parity rieg Example 3.2.4 is multiplicatively idempotent but not additively idempotent.

However, there is a strong restriction on the characteristics. For a multiplicatively idempotent rieg R, its characteristics $\mathrm{char}R$ should be less than $(2,2)$ since $2=2\times 2=4$. Therefore, there are only finitely many possible characteristics, namely

$$\mathrm{char}R=(0,1),(1,1),(1,2),(2,1),\text{or }(2,2).$$

And all of them are possible, since $\mathbb{N}_{0,1},\mathbb{N}_{1,1},\mathbb{N}_{1,2},\mathbb{N}_{2,1},$ and $\mathbb{N}_{2,2}$ are multiplicatively idempotent.

5.2. **Riegs that are lattices.** Next, we will study when (the underlying rig of) a rieg is a lattice. The necessary condition is being idempotent (Definition 5.1.3). However, this is not sufficient:

Example 5.2.1 (Idempotent rieg that is not a lattice)**.** In Example B.1.9, we observed that $\mathbb{N}[x]$ with exponential

$$f(x)^{g(x)}=f(x)^{g(0)}=\underbrace{f(x)\times\cdots\times f(x)}_{g(0)\text{ times}}$$

is a rieg.

Dividing $\mathbb{N}[x]$ into 4 groups

$$\begin{aligned}\mathrm{ZC}&=\{f(x)\in\mathbb{N}[x]\mid f(0)=0\text{ and }f\text{: constant}\}=\{0\}\\ \mathrm{ZI}&=\{f(x)\in\mathbb{N}[x]\mid f(0)=0\text{ and }f\text{: increasing}\}\\ \mathrm{PC}&=\{f(x)\in\mathbb{N}[x]\mid f(0)>0\text{ and }f\text{: constant}\}\\ \mathrm{PI}&=\{f(x)\in\mathbb{N}[x]\mid f(0)>0\text{ and }f\text{: increasing}\},\end{aligned}$$

we obtain a 4-element rieg $\{\mathrm{ZC},\mathrm{ZI},\mathrm{PC},\mathrm{PI}\}$ as a quotient rieg. Indeed, the group to which f belongs is determined by the pair of data (whether $f(0)=0$ or $f(0)>0$; whether f is constant or increasing), and this pair for $f+g$ and

for $f \times g$ is determined by the pairs for f and g (for the multiplication, note that $\mathrm{ZC} = \{0\}$ consists of the single element 0). For the exponential, observe that $f^g = f^{g(0)}$ is equal to $1 \in \mathrm{PC}$ if $g(0) = 0$, and belongs to the same group as f if $g(0) > 0$; in both cases, the group of f^g depends only on the groups of f and g.

The underlying rig of this quotient is the rig presented by a single generator x and two equations $1 + 1 = 1$ and $x^2 = x$. (The additive idempotency follows from $1 + 1 = 1$ via $f + f = f \times (1 + 1) = f$; hence the presented rig consists of the four elements $0, 1, x$, and $1 + x$, corresponding to $\mathrm{ZC}, \mathrm{PC}, \mathrm{ZI}$, and PI, respectively.) This rieg satisfies $1 + 1 = 1$, but the underlying rig is not a lattice since $1 + x \neq 1$.

Proposition 5.2.2 (Rieg and Lattice)**.** *For a rieg R, the following conditions are equivalent:*

(1) The underlying rig is a (bounded) lattice.
(2) For any $x \in R$, $1 + x = 1$.

Proof. The implication 1 $\implies$ 2 follows from the fact that 1 is the maximum element in a lattice.

We prove 1 from 2. Substituting x with 1, we obtain $1 + 1 = 1$, i.e., this rieg is idempotent (Definition 5.1.3). Now it is enough to prove the absorption laws

$$x + xy = x$$
$$x(x + y) = x.$$

It is proven as $x(x + y) = x^2 + xy = x + xy = x(1 + y) = x1 = x$. □

5.3. **Heyting algebras are riegs.** A Heyting algebra is not just related but is a rieg satisfying additional equations.

Proposition 5.3.1. *Every Heyting algebra $(H, 0, 1, \vee, \wedge, \leftarrow)$ is a rieg.*

Proof. We can directly prove this. Alternatively, this is also an immediate corollary of Proposition 4.1.2, since a Heyting algebra is a bicartesian closed category whose underlying category is a poset. □

Example 5.3.2 (A rieg that is a lattice but not a Heyting algebra)**.** Let $\mathcal{P}(X)$ be the power set of a non-empty set X, equipped with a rig structure given by $\emptyset, X, \cup$ and $\cap$. We consider a rieg structure on $\mathcal{P}(X)$ that is different from Example 5.0.2.

First, fix an arbitrary element $x \in X$ and define the exponential as

$$A^B \coloneqq \begin{cases} A & (x \in B) \\ X & (x \notin B). \end{cases}$$

This rieg structure is given by the composition of two rig homomorphisms. The first one is a rig homomorphism to the rig of truth value $\mathbf{2} = \{\bot, \top\}$ defined as

$$\mathcal{P}(X) \to \mathbf{2} \colon A \mapsto \text{“}x \in X\text{”}.$$

The other is the unique rig homomorphism

$$\mathbf{2} \to \mathrm{End}(\mathcal{P}(X), X, \cap),$$

which sends $0 \in \mathbf{2}$ to the constant funciton $\mathrm{const}_X \colon \mathcal{P}(X) \to \mathcal{P}(X)$ and $1 \in \mathbf{2}$ to the identity function $\mathrm{id}_X \colon \mathcal{P}(X) \to \mathcal{P}(X)$.

Remark 5.3.3 (Riegs from ultrafilters)**.** Rig homomorphisms $\mathcal{P}(X) \to \mathbf{2}$ correspond exactly to ultrafilters on X. For each ultrafilter $\mathcal{U}$ on X, the same construction equips the rig $\mathcal{P}(X)$ with a rieg structure: the exponentiation is given by $A^B = A$ if $B \in \mathcal{U}$, and $A^B = X$ otherwise. The example above is the special case where $\mathcal{U}$ is the principal ultrafilter generated by $x \in X$.

If X has at least two elements, this rieg is not a Heyting algebra, because

$$\{x\}^{\{x\}} = \{x\} \neq X.$$

Proposition 5.3.4. *A rieg R is a Heyting algebra, if and only if it satisfies the following additional equations:*

- $1 + x = 1$
- $x^x = 1$
- $xy^x = xy$

Corollary 5.3.5. *The category of Heyting algebras* HeyAlg *is a reflective full subcategory of the category of riegs* **Riegs**.

$$\text{HeyAlg} \hookleftarrow \textbf{Riegs}$$

The construction of the left adjoint is the usual one: quotient by new equations. For example, the associated Heyting algebra of $\mathbb{N}$ is the Heyting algebra of truth values $\{\bot, \top\}$.[6]

The relation between Heyting algebras and riegs is not an addition of structures, but an addition of properties. In this respect, it is closer to the relationship between abelian groups and groups rather than to the relationship between rings and groups.

Appendix A. Preliminaries on equational theory and profinite topology

In this section, let $\mathbb{T}$ be a (finite arity single-sorted) algebraic theory. We are especially interested in the case $T =$ (the theory of riegs). The category of $\mathbb{T}$-algebras is denoted by $\text{Alg}_{\mathbb{T}}$.

A.1. Categorical properties of riegs (and general $\mathbb{T}$-algebras).

Remark A.1.1 (Categorical properties of riegs)**.** Several category-theoretic properties of **Riegs** immediately follow from the mere existence of an equational definition by the theory of categorical universal algebra. Some of them are noted below.

- The category of riegs **Riegs** has all small limits and colimits.
- Furthermore, the forgetful functor $U\colon \textbf{Riegs} \to \textbf{Set}$ (preserves and) creates all limits.
- The forgetful functor $U\colon \textbf{Riegs} \to \textbf{Set}$ has a left adjoint $F\colon \textbf{Set} \to \textbf{Riegs}$
- Every rieg homomorphism $f\colon R \to S$ is uniquely (up to the canonical isomorphism) decomposed into the composition of a surjective homomorphism followed by an injective homomorphism $R \twoheadrightarrow \text{Im}(f) \rightarrowtail S$.

This means we can construct arbitrary small limits using limits in **Set**. For a given family of riegs $\{R_\lambda\}_{\lambda\in\Lambda}$, its categorical product is given by the product set $\prod_{\lambda\in\lambda} R_\lambda$ with the index-wise operations.

An element of the free rieg $F(\{x\})$ looks like

$$(3^x + x^{x^x})^{x^{2^x}+5^{x+0^x}+1} + 0^x x.$$

A.2. Topological $\mathbb{T}$-algebras and their profinite completion.

A *topological $\mathbb{T}$-algebra* is a model of $\mathbb{T}$ in the category Top, that is, a $\mathbb{T}$-algebra equipped with a topology such that all operations of $\mathbb{T}$ are continuous. Morphisms of topological $\mathbb{T}$-algebras are continuous $\mathbb{T}$-algebra homomorphisms. The category of topological $\mathbb{T}$-algebras is denoted by $\text{TopAlg}_{\mathbb{T}}$.

It is straightforward to verify the next lemma.

Lemma A.2.1 (Limits in the topological $\mathbb{T}$-algebras)**.** $\text{TopAlg}_{\mathbb{T}}$ *admits all small limits, which are preserved by the two forgetful functors* $\text{TopAlg}_{\mathbb{T}} \to \text{Alg}_{\mathbb{T}}$ *and* $\text{TopAlg}_{\mathbb{T}} \to \text{Top}$.

[6] This particular example is a trivial case, since a left adjoint preserves colimits.

In otherwords, a small limit in $\mathrm{TopAlg}_{\mathbb{T}}$ is just the limit at the underlying set level equipped with the canonical $\mathbb{T}$-algebra structure and the initial topology.

For a given $\mathbb{T}$-algebra R, a *quotient* $\mathbb{T}$-algebra is a surjective $\mathbb{T}$-algebra homomorphism $R \twoheadrightarrow Q$, up to the canonical isomorphisms. The quotients form a complete lattice $\mathrm{Quot}_{\mathbb{T}}(R)$. We put $Q \leq Q'$ if there exists a homomorphism $Q' \twoheadrightarrow Q$ that commutes with the quotient maps from R. Let $\mathrm{FinQuot}_{\mathbb{T}}(R)$ denote the subposet of finite quotient $\mathbb{T}$-algebras.

Definition A.2.2 (Profinite completion of a $\mathbb{T}$-algebra)**.** For a $\mathbb{T}$-algebra R, its *profinite completion* $\widehat{R}$ is the limit of all finite quotients of R. In other words, $\widehat{R}$ is the limit of the following diagram:

$$\mathrm{FinQuot}_{\mathbb{T}}(R)^{\mathrm{op}} \to \mathrm{Alg}_{\mathbb{T}} \xrightarrow{\text{discrete}} \mathrm{TopAlg}_{\mathbb{T}}.$$

Remark A.2.3 (As a codensity monad)**.** It is much more natural to define the profinite completion as an endofunctor on the category $\mathrm{TopAlg}_{\mathbb{T}}$ although we will not need it in the present paper. The category of finite (and discrete) $\mathbb{T}$-algebras $\mathrm{finAlg}_{\mathbb{T}}$ is a full subcategory of the category $\mathrm{TopAlg}_{\mathbb{T}}$, and the codensity monad of the embedding $\mathrm{finAlg}_{\mathbb{T}} \hookrightarrow \mathrm{TopAlg}_{\mathbb{T}}$ is the profinite completion.

Appendix B. Other (counter)examples

B.1. **Basic examples.**

Example B.1.1 (Non-negative real numbers)**.** The set of non-negative real numbers $[0, \infty)$ has the natural rieg structure, defining

$$0^x = \begin{cases} 1 & (x = 0) \\ 0 & (x > 0). \end{cases}$$

The rieg of natural numbers is a subrieg of this rieg. However, the subset of all non-negative rational numbers is not subrieg, since it is not closed under exponentials.

Proposition B.1.2 (J. Koizumi, personal communication)**.** *Let $f\colon (0,\infty) \to (0,\infty)$ preserve the exponentiation, i.e. satisfy*

$$f(x^y) = f(x)^{f(y)} \qquad (x, y > 0).$$

Then f is either the constant function 1 or the identity function.

Proof. Putting $x = y = 1$, the value $a \coloneqq f(1)$ satisfies $a = a^a$, hence $(a-1)\log a = 0$ and $a = 1$. Applying f to $x^{yz} = (x^y)^z$ gives

$$f(x)^{f(yz)} = f(x^y)^{f(z)} = f(x)^{f(y)f(z)} \qquad (x, y, z > 0).$$

Assume f is not constantly 1, and fix x_0 with $f(x_0) \neq 1$; then $f(yz) = f(y)f(z)$, i.e. f is multiplicative. Put $\varphi(u) \coloneqq \log f(e^u)$ for $u \in \mathbb{R}$. Multiplicativity gives $\varphi(u+v) = \varphi(u) + \varphi(v)$, while the original equation with $x = e^u$ gives $\varphi(yu) = f(y)\varphi(u)$ for all $u \in \mathbb{R}$ and $y > 0$. Fixing u_0 with $\varphi(u_0) \neq 0$, we obtain $f(y) = \varphi(yu_0)/\varphi(u_0)$, so additivity of φ makes f additive: $f(y+y') = f(y) + f(y')$. An additive function with positive values is strictly increasing, and $f(1) = 1$ forces $f(q) = q$ for every positive rational q; being increasing and agreeing with the identity on a dense subset, $f = \mathrm{id}$. Conversely, both functions do satisfy the equation. □

Remark B.1.3. The hypothesis has to be $f(x^y) = f(x)^{f(y)}$, that is, f is an endomorphism of the binary operation $\uparrow$. Under the weaker reading $f(x^y) = f(x)^y$ the statement is false, since $f(x) = x^c$ satisfies $(x^y)^c = (x^c)^y$ for every $c > 0$. Note also that $(0,\infty)$ is not a rieg, having no 0; it is a model of the eleven high school identities, so the correct reading of Proposition B.1.2 is a rigidity statement about $\uparrow$-endomorphisms.

Remark B.1.4 (The rig $[0,\infty]$ is not a rieg)**.** It is natural to ask whether this rieg structure can be extended to the rig $[0,\infty]$. The answer is no. The rig $[0,\infty]$ cannot have a rieg structure. Suppose that there is an extension to a rieg structure. First, since $2^\infty = 2^{\infty+1} = 2^\infty \times 2$, we have $2^\infty \in \{0,\infty\}$. And, since $2^\infty (0.5)^\infty = 1^\infty = 1$, we have $2^\infty \in (0,\infty)$, contradiction.

B.1.1. *Numbers with Infinites.*

Example B.1.5 (Complemented natural numbers)**.** $\mathbb{N} \cup \{\infty\}$ has a canonical rieg structure, which is obtained as the limit of the overflow riegs

$$\dots \longrightarrow \mathrm{OverFlow}_2 \longrightarrow \mathrm{OverFlow}_1 \longrightarrow \mathrm{OverFlow}_0.$$

In this sense, this rieg is the overflow rieg with threshold ∞. Notice that this construction is similar to the construction of p-adic integers.

B.1.2. *Rig with many rieg structures.*

Example B.1.6 (Rieg of dual numbers constructed by Yuhi Kamio)**.** Recall that a dual number is a number plus an "infinitesimal number"

$$a + b\varepsilon \ (a, b \in \mathbb{R})$$

The ring of infinitesimal numbers is denoted by $\mathbb{R}[\varepsilon]$ and algebraically defined as $\mathbb{R}[\varepsilon] = \mathbb{R}[x]/(x^2)$.

There is a similar rieg, which we call the *dual number rieg.*

Definition B.1.7 (Dual numbers, concrete definition)**.** The dual number rieg $\mathbb{N}[\varepsilon]$ has $\mathbb{N} \times \mathbb{Z}$ as the underlying set and its element (n, m) is denoted by $n + m\epsilon$. Three operations are defined as follows:

(1) $(n + m\varepsilon) + (n' + m'\varepsilon) = (n + n') + (m + m')\varepsilon$
(2) $(n + m\varepsilon) \times (n' + m'\varepsilon) = (nn') + (nm' + n'm)\varepsilon$
(3) The exponential depends only on the natural-number part n' of the exponent:

$$(n + m\varepsilon) \uparrow (n' + m'\varepsilon) = \underbrace{(n + m\varepsilon) \times \cdots \times (n + m\varepsilon)}_{n' \text{times}} = \begin{cases} 1 & (n' = 0), \\ n^{n'} + n' n^{n'-1} m\varepsilon & (n' > 0). \end{cases}$$

This definition has a more conceptual paraphrase, with which we can easily prove that it's actually a rieg. First notice that the projection

$$\mathbb{N}[\varepsilon] \to \mathbb{N} \colon n + m\varepsilon \mapsto n$$

is a rig homomorphism to the initial rig $\mathbb{N}$. Thus we have the composite rig homomorphism

$$\mathbb{N}[\varepsilon] \to \mathbb{N} \to \mathrm{End}(\mathbb{N}[\varepsilon], \times, 1),$$

and this gives the exponential structure of the dual number rieg.

More generally, we have the following proposition.

Proposition B.1.8 (Rieg structure by a natural number evaluation)**.** *For a commutative rig R and a rig homomorphism (or say, "natural number evaluation")*

$$v \colon R \to \mathbb{N},$$

R admits an induced rieg structure

$$R \to \mathbb{N} \to \mathrm{End}(R, \times, 1).$$

In other words, the exponential is given by

$$x^y = \underbrace{x \times \cdots \times x}_{v(y) \text{ times}}.$$

For example, we can replace the additive group $\mathbb{Z}\varepsilon$ in the definition of the dual number rieg with an arbitrary commutative monoid.

Example B.1.9. In Proposition B.1.8, letting $v\colon R \to \mathbb{N}$ be the evaluation function

$$\mathrm{ev}_0\colon \mathbb{N}[x] \to \mathbb{N}\colon x \mapsto 0,$$

we have a rieg structure on $\mathbb{N}[x]$ with

$$f(x)^{g(x)} = f(x)^{g(0)} = \underbrace{f(x) \times \cdots \times f(x)}_{g(0) \text{ times}}.$$

Example B.1.10 (Rieg of polynomials)**.** Is it possible to have more than one rieg structure on a single rig? The answer is (not at all surprisingly) yes. A typical example is the rig of polynomials $\mathbb{N}[x]$. Since $\mathbb{N}[x]$ is the free rig with a generator x, rieg structures on $\mathbb{N}[x]$

$$\mathbb{N}[x] \to \mathrm{End}(\mathbb{N}[x], \times, 1)$$

bijectively correspond to the elements of $\mathrm{End}(\mathbb{N}[x], \times, 1)$.

B.2. **Riegs of three elements.** The degenerate rieg **1** is the unique 1-element rieg. The rieg of truth values **2** is the unique 2-element rieg. This subsection aims to provide all 3-element riegs.

Proposition B.2.1 (3-element riegs)**.** *There are* 8 *isomorphism classes of* 3*-element riegs.*

Let R be a 3-element rieg. There are three possible characteristics $\mathrm{char}(R) = (1,1), (1,2), (2,1)$.
Case 1: $\mathrm{char}(R) = (1,2), (2,1)$. If $\mathrm{char}(R) = (1,2), (2,1)$, then R is the parity rieg (Example 3.2.4) or the overflow rieg with the threshold 2 (Example 3.2.5).
Case 2: $\mathrm{char}(R) = (1,1)$. So we need to classify all 3-element riegs with characteristics $\mathrm{char}(R) = (1,1)$.

Let $R = \{0, 1, a\}$. We distinguish cases based on the value of $1 + a$.
- Case 2.1: $\mathrm{char}(R) = (1,1)$ **and** $1 + a = 1$. If $1 + a = 1$, then the rieg R satisfies the equation $1 + x = 1$, which means that the underlying rig of R is the lattice $(\{0 < a < 1\}, 0, \vee, 1, \wedge)$ (Proposition 5.2.2). This rig $0 < a < 1$ is isomorphic to the rig

$$R \cong \langle a \mid 1 + 1 = 1, 1 + a = 1, a^2 = a \rangle \text{ in } \mathbf{Rigs}$$

Therefore, the rieg structures $R \to \mathrm{End}(R, 1, \wedge)$ on the rig R are in bijective correspondence with the monoid homomorphisms $\phi\colon (R, 1, \wedge) \to (R, 1, \wedge)$, which correspond to the exponentiation function $-^a\colon R \to R$, that satisfy

- $x \wedge x = x$, which always holds,
- $x \wedge \phi(x) = x$, and
- $\phi^2(x) = \phi(x)$.

In other words, the rieg structures on the rig $(\{0 < a < 1\}, 0, \vee, 1, \wedge)$ are in bijective correspondence with the idempotent $\wedge$-semilattice homomorphisms $-^a = \phi\colon (R, 1, \wedge) \to (R, 1, \wedge)$ with $\phi(x) \geq x$. One can show that there are exactly 4 rieg structures on the rig $(\{0 < a < 1\}, 0, \vee, 1, \wedge)$, which are visualized in Figure 8.

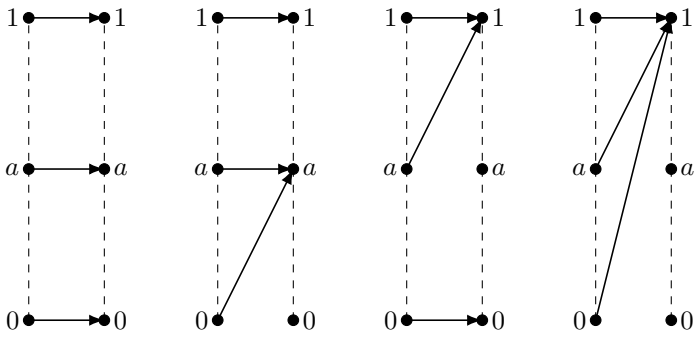


FIGURE 8. The four possible exponentiations $x \mapsto x^a$

- Case 2.2: $\mathrm{char}(R) = (1,1)$ **and** $1 + a = a$. The only remaining case is $1 + a = a$, since $1 + a = 0$ is impossible (Claim 2.3.1). Since R is idempotent (Definition 5.1.3), the underlying rig structure is determined:

$$R \cong \langle a \mid 1 + 1 = 1, 1 + a = a, a^2 = a \rangle \text{ in } \mathbf{Rigs}$$

Therefore, the rieg structures on R are in bijective correspondence with monoid homomorphisms $\phi\colon (R, 1, \times) \to (R, 1, \times)$ with

- $x \times x = x$, which always holds
- $x \times \phi(x) = \phi(x)$, and
- $\phi^2(x) = \phi(x)$.

There are two such morphisms visualized in Figure 9.

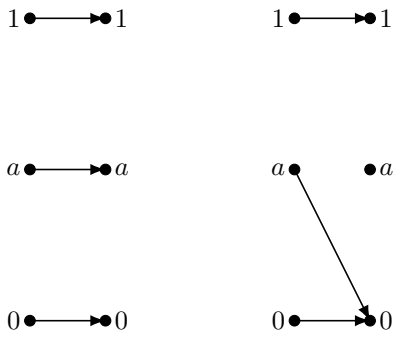


FIGURE 9. The two possible exponentiations $x \mapsto x^a$

REFERENCES

[AJ25] Tumadhir Alsulami and Marcel Jackson. "Cyclic arithmetic and combinatorial operations". *The American Mathematical Monthly* 132.4 (2025), pp. 316–332. DOI: 10.1080/00029890.2024.2439803.

[BD01] John C. Baez and James Dolan. "From finite sets to Feynman diagrams". *Mathematics unlimited—2001 and beyond* (2001), pp. 29–50.

[BS13] Edward Barbeau and Samer Seraj. "Sum of cubes is square of sum". *Notes on Number Theory and Discrete Mathematics* 19.1 (2013), pp. 1–13.

[BHT09] Jan A. Bergstra, Yoram Hirshfeld, and John V. Tucker. "Meadows and the equational specification of division". *Theoretical Computer Science* 410.12–13 (2009), pp. 1261–1271. DOI: 10.1016/j.tcs.2008.12.015.

[Bir42] Garrett Birkhoff. "Generalized arithmetic". *Duke Math. J.* 9.1 (1942), pp. 283–302.

[BL92] Stanley Burris and Simon Lee. "Small models of the high school identities". *International Journal of Algebra and Computation* 2.02 (1992), pp. 139–178. DOI: 10.1142/S0218196792000104.

[BL93] Stanley Burris and Simon Lee. "Tarski's high school identities". *The American Mathematical Monthly* 100.3 (1993), pp. 231–236.

[BY05] Stanley N. Burris and Karen A. Yeats. "The saga of the High School Identities". *Algebra Universalis* 52.2–3 (2005), pp. 325–342. DOI: 10.1007/s00012-004-1900-2.

[CP09] Peter J. Cameron and Donald A. Preece. *Notes on primitive lambda-roots*. Unpublished notes. 2009. URL: http://www.maths.qmul.ac.uk/~pjc/csgnotes/lambda.pdf.

[Car10] Robert D. Carmichael. "Note on a new number theory function". *Bulletin of the American Mathematical Society* 16.5 (1910), pp. 232–238. DOI: 10.1090/S0002-9904-1910-01892-9.

[FDB06] Marcelo Fiore, Roberto Di Cosmo, and Vincent Balat. "Remarks on isomorphisms in typed lambda calculi with empty and sum types". *Annals of Pure and Applied Logic* 141.1-2 (2006), pp. 35–50.

[Hit20] Markus Hittmeir. "A reduction of integer factorization to modular tetration". *International Journal of Foundations of Computer Science* 31.4 (2020), pp. 461–481. DOI: 10.1142/S0129054120500197.

[JY09] Jorge Jiménez Urroz and José Luis Andrés Yebra. "On the equation $a^x \equiv x \pmod{b^n}$". *Journal of Integer Sequences* 12.8 (2009). Article 09.8.8. URL: https://cs.uwaterloo.ca/journals/JIS/VOL12/Yebra/yebra4.html.

[Joh11] Peter T. Johnstone. "Remarks on punctual local connectedness". *Theory Appl. Categ* 25.3 (2011), pp. 51–63.

[KM91] Anders Kock and Ieke Moerdijk. "Presentations of étendues". *Cahiers de topologie et géométrie différentielle catégoriques* 32.2 (1991), pp. 145–164.

[Men17] Matías Menni. "Every rig with a one-variable fixed point presentation is the burnside rig of a prextensive category". *Applied Categorical Structures* 25 (2017), pp. 663–707.

[OEIa] OEIS Foundation Inc. *Sequence A133613: Decimal digits such that for all $k \geq 1$, the number $A(k) := \sum_{n=0}^{k-1} a(n) \cdot 10^n$ satisfies the congruence $3^{A(k)} \equiv A(k) \pmod{10^k}$*. The On-Line Encyclopedia of Integer Sequences. URL: https://oeis.org/A133613.

[OEIb] OEIS Foundation Inc. *Sequence A183613: $a(n) = 3 \uparrow\uparrow (n+1)$ modulo 10^n*. The On-Line Encyclopedia of Integer Sequences. URL: https://oeis.org/A183613.

[Sch90] Stephen H. Schanuel. "Negative sets have Euler characteristic and dimension". *Category Theory: Proceedings of the International Conference held in Como, Italy, July 22–28, 1990*. Springer. 1990, pp. 379–385.

[Sch00a] Stephen H. Schanuel. "Objective number theory and the retract chain condition". *Journal of Pure and Applied Algebra* 154.1-3 (2000), pp. 295–298.

[Sch00b] Stephen H. Schanuel. *Transcendence in objective number theory*. 2000.

[SM23] David I. Spivak and David Jaz Myers. "Dirichlet polynomials form a topos". *The Graduate Journal of Mathematics* 8.2 (2023), pp. 73–87.

[Wil00] Alex J. Wilkie. "On exponentiation—a solution to Tarski's high school algebra problem". *Connections between Model Theory and Algebraic and Analytic Geometry*. Ed. by Angus Macintyre. Vol. 6. Quaderni di Matematica. Circulated as an Oxford University preprint in the early 1980s. Rome: Aracne, 2000, pp. 107–129.

ZEN University, Tokyo, Japan
Email address: ryuya_hora@zen.ac.jp