Notre Dame Journal of Formal Logic
Volume 56, Number 3, 2015

Ordinal Exponentiations of Sets

Laurence Kirby

Abstract The "high school algebra" laws of exponentiation fail in the ordinal arithmetic of sets that generalizes the arithmetic of the von Neumann ordinals. The situation can be remedied by using an alternative arithmetic of sets, based on the Zermelo ordinals, where the high school laws hold. In fact the Zermelo arithmetic of sets is uniquely characterized by its satisfying the high school laws together with basic properties of addition and multiplication. We also show how in both arithmetics the behavior of exponentiation depends on whether the empty set is an element of the base.

1 Introduction

In the 1950s Tarski [7] generalized to all sets the addition operator on the von Neumann ordinals in set theory by defining

$$x + y = x \cup \{x + r \mid r \in y\}.$$

Dana Scott (unpublished) followed with definitions of multiplication and exponentiation:

$$x \cdot y = \{x \cdot q + r \mid q \in y \wedge r \in x\},$$
$$x^0 = 1, \qquad x^y = \{x^p \cdot q + r \mid p \in y \wedge q \in x \wedge r \in x^p\} \quad \text{if } y \neq 0.$$

(Here and throughout $0, 1, 2, \ldots$ are the usual von Neumann ordinals, so 0 is the empty set.) Scott did not publish these definitions, but in [5] I studied the addition and multiplication operators. This paper examines exponentiation.

But von Neumann's ordinal arithmetic is not the only possible one. We shall also consider an alternative arithmetic of ordinals and its extension to sets: the *Zermelo arithmetic* (see Kirby [6]). (For clarity, we shall sometimes call the original arithmetic of sets the *von Neumann arithmetic*.) We shall explore the similarities between these two arithmetics of sets, and also some differences which emerge at the level of exponentiation.

Received February 11, 2013; accepted March 30, 2013
2010 Mathematics Subject Classification: Primary 03E10, 03E20
Keywords: set theory, ordinal arithmetic, exponentiation
 10.1215/00294527-3132806

By the "high school algebra" laws of exponentiation I mean the universal closures of

$$a^{b+c} = a^b \cdot a^c \qquad \text{and} \qquad a^{b\cdot c} = (a^b)^c.$$

(I exclude from consideration the third law of exponentiation commonly learned in high school, $(a \cdot b)^c = a^c \cdot b^c$, because our operations are noncommutative, even for finite sets, which makes this law unlikely on the face of it and, in fact, easily shown to be false in the arithmetics discussed here.)

Theorem 1.1 *The high school algebra laws of exponentiation are true in the Zermelo arithmetic of sets but not in the von Neumann arithmetic of sets.*

Further, we shall see that the Zermelo arithmetic is the *only* arithmetic of sets possessing the high school laws along with basic properties of addition and multiplication (see Theorem 6.4).

We also establish many algebraic properties that the two arithmetics have in common, including the rather unexpected way that when the empty set is an element of the base a, the value of a^x depends only upon $\rho(x)$, the rank of x in the cumulative hierarchy.

Theorem 1.2 *In both the von Neumann and Zermelo arithmetics of sets, if* $0 \in a$, *then* $\forall x\, (a^x = a^{\rho(x)})$.

The simplified behavior of exponentiation in this case means that the von Neumann arithmetic does have the high school laws for such bases (see Corollary 4.6).

Even within the von Neumann arithmetic, other exponentiations are possible. Garcia [1] used the Tarski–Scott sum and product but defined an exponentiation similar but not identical to Scott's.[1] For this exponentiation he stated many basic arithmetical properties including Lemma 3.5 and Corollary 4.6 below.

The rest of this paper is organized as follows.

Section 2 is an account of the Zermelo ordinals and the Zermelo arithmetic of sets. The Zermelo sum and product were introduced in [6]. Now we include exponentiation.

Section 3 presents a common core of basic properties that hold in both arithmetics of sets and uses them to obtain the properties of multiplication that the arithmetics share.

Section 4 extends this to exponentiation, proving Theorem 1.2. Also, we show for both arithmetics the existence, for certain sets, of the Cantorian decomposition to a given base (see Proposition 4.7). However, it is unique only when the empty set is not an element of the base (see Theorem 4.8).

Section 5 gives examples showing the failure of the high school laws in the von Neumann arithmetic. Section 6 proves them for the Zermelo arithmetic and shows that indeed the Zermelo arithmetic is the only arithmetic that has these laws along with the common basic properties of Section 3.

2 The Zermelo Ordinals and the Zermelo Arithmetic of Sets

How to represent the natural numbers, or more generally the Cantorian ordinals (well-ordered order types), in the universe of sets? Besides the canonical way, the von Neumann ordinals, there is a more parsimonious way. The *Zermelo ordinal* α_z defined for each ordinal[2] α by $0_z = 0$, $(\alpha + 1)_z = \{\alpha_z\}$, with unions at limit stages

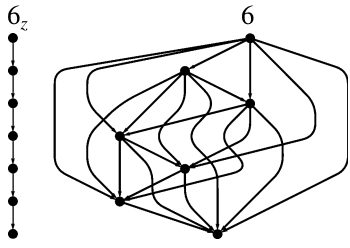

Figure 1 The ordinal 6 in the Zermelo arithmetic (left) and in the von Neuman arithmetic (right).

λ: $\lambda_z = \bigcup_{\gamma<\lambda} \gamma_z = \{\gamma_z \mid \gamma < \lambda\}$, the first equality by definition, the second by ordinal induction.

Zermelo ordinals are named for Ernst Zermelo whose 1908 statement of the axiom of infinity posits a set containing 0 and closed under the Zermelo successor. He deduces the existence of the intersection of all such sets, which he calls Z_0, and is identical with our ω_z. He calls it "the *number sequence* ... the simplest example of a denumerably infinite set" [8, p. 205].

The relative simplicity of the Zermelo successor, as contrasted with the von Neumann successor $\alpha + 1 = \alpha \cup \{\alpha\}$, is evident in graph representations [6] of the two arithmetics: compare for example the graphs of 6_z and 6 (see Figure 1).

The graph of n_z has n edges, while that of n has $n(n+1)/2$ edges. This quadratic increase in complexity (as measured by number of edges) arguably makes no difference for infinite sets, but on the finite sets it raises questions of relative feasibility of the two representations.

We have used the scaffolding of the von Neumann ordinals to construct the Zermelo ordinals; we could instead define the Zermelo ordinals from scratch and use α_z as our representative of the well-ordered order type normally represented by α.

This comes at a price, because the order of the von Neumann ordinals is the restriction to them of, simultaneously, three relations on sets: the membership relation $\in$, the relation $<$ given by

$$x < y \longleftrightarrow x \in TC(y),$$

where $TC(y)$ is the transitive closure of y, and the proper subset relation $\subset$. This gives elegance and flexibility to the use of ordinals. The order of the Zermelo ordinals, on the other hand, is the restriction only of $<$. Thus α_z does a clumsy job of representing its order type, because it is $\langle TC(\alpha_z), <\rangle$ that has order type α, not $\langle \alpha_z, \in\rangle$.

Extending the Zermelo ordinals to the infinite makes them even worse as yardsticks for well-orderings. The infinite Zermelo ordinals are not even closed under addition (see [6]). They can be used to develop the theory of infinite well-orderings, but only at the cost of circumlocutions.

Ironically, Zermelo himself also (in unpublished work) anticipated von Neumann's canonical 1923 definition of the ordinals, as did Dmitry Mirimanoff.[3]

In [6] I defined the *Zermelo addition and multiplication* of sets, extending the arithmetic of the Zermelo ordinals:

$$x +_z 0 = x, \qquad x +_z y = \{x +_z r \mid r \in y\} \quad \text{if } y \neq 0,$$
$$x \cdot_z y = \{x \cdot_z q +_z r \mid q \in y \wedge r \in x\}.$$

As with multiplication, *Zermelo exponentiation* x_z^y is defined in exact analogy with Scott's definition of exponentiation:

$$x_z^0 = 1, \qquad x_z^y = \{x_z^p \cdot_z q +_z r \mid p \in y \wedge q \in x \wedge r \in x_z^p\} \quad \text{if } y \neq 0.$$

When restricted to the finite ordinals, the Zermelo arithmetic of sets and the von Neumann arithmetic of sets agree with each other and with the standard ordinal operations, so that for example $m_z +_z n_z = (m + n)_z$. But this is no longer true in the infinite case: $1_z +_z \omega_z \neq \omega_z$, although their transitive closures have the same order type.

As with the ordinals, each of the two arithmetics of sets has advantages. The von Neumann arithmetic of sets retains the von Neumann ordinals' good fit with the theory of well-orderings, especially in the infinite case. On the other hand, the Zermelo operations are simpler and have more natural graph interpretations; we can add to these the advantage conferred by Theorem 1.1.

3 Arithmetics of Sets

In order to develop some of the basic properties that the von Neumann and Zermelo arithmetics of sets have in common, and to examine where they differ, it will be convenient to isolate some key properties by defining what it means to be an *arithmetic of sets*.

To abate a proliferation of subscripts, I adopt the following notational convention. Let $\mathcal{L}$ be a first-order language with equality and symbols that have standard interpretations on sets: for example $\in$, $<$, the binary *arithmetical* operators of addition, multiplication, and exponentiation (interpreted on sets by their Tarski–Scott definitions), ordinals, and even the informal set-builder notation. If $s = t$ is an equation in $\mathcal{L}$, let $s =_z t$ be the equation obtained by inserting the subscript z in each occurrence of the arithmetical operators and ordinals. We shall sometimes express $s =_z t$ by saying that $s = t$ is *true in the Zermelo arithmetic (of sets)*, and by way of contrast $s = t$ may be said to be *true in the von Neumann arithmetic*. Furthermore, we do the same for any relation and thus for any formula of $\mathcal{L}$. So for example $a + b <_z c + d$ means $a +_z b < c +_z d$.

In the same way, suppose that $+_*$ is a binary operation on sets. The Scott definitions give an associated multiplication $\cdot_*$ and exponentiation x_*^y. A $*$-arithmetic of sets follows in the same way as the Zermelo arithmetic, indicated either by the subscript $*$ or by declaring that a formula is to be construed in the $*$-arithmetic.

An *additive arithmetic of sets* is a binary operation $+_*$ on sets satisfying the universal closures of the following five properties:

(i) $0 + x =_* x + 0 =_* x$;
(ii) $+_*$ is associative;
(iii) left cancellation: $a + x =_* a + y \longrightarrow x = y$;
(iv) $a + b =_* c + d \longrightarrow \exists e\,(a + e =_* c \vee c + e =_* a)$;
(v) $x <_* a + b \longleftrightarrow x < a \vee \exists y < b\,(x =_* a + y)$.

If $+_*$ satisfies (i)–(v), define

$$x \cdot y =_* \{x \cdot q + r \mid q \in y \wedge r \in x\},$$

$$x^0 =_* 1, \qquad x^y =_* \{x^p \cdot q + r \mid p \in y \wedge q \in x \wedge r \in x^p\} \quad \text{if } y \neq 0.$$

We say that $+_*$ is a *multiplicative arithmetic of sets* if (i)–(v) hold and also:

(vi) Multiplication is left distributive over addition: $a \cdot (b + c) =_* a \cdot b + a \cdot c$,

and an *exponential arithmetic of sets* if, in addition, the first high school law of exponentiation holds:

(vii) $a^{b+c} =_* a^b \cdot a^c$.

Some comments about these properties. None of them mentions $\in$. All except (v) are purely arithmetical properties, expressed in the language with only 0, equality, and the three arithmetical operations. Property (iv) is a finite version of Tarski's directed refinement postulate (see [7, p. 8]) and together with (ii) is part of his theory of concatenation.[4]

Property (v) is not purely arithmetical, stating the compatibility of $+_*$ with $<$ and harnessing the latter's well-foundedness; (v) implies that $x \leq_* x + y$. There is a natural arithmetical partial order $\trianglelefteq_*$ on sets defined by $a \trianglelefteq_* b \longleftrightarrow \exists x\,(a + x =_* b)$ (see [5]), and (v) tells us that $a \trianglelefteq_* b \longrightarrow a \leq b$.

Properties (i)–(vi) are among the properties of the von Neumann arithmetic shown in [5], and so we have the following.

Lemma 3.1 *The von Neumann sum is a multiplicative arithmetic of sets.*

The proofs of (i)–(vi) for the Zermelo case are similar to the von Neumann case. Less formally, these properties of the Zermelo arithmetic are also easy to see using the graph interpretations of [6], so we have the following.

Lemma 3.2 *The Zermelo sum is a multiplicative arithmetic of sets.*

Later we shall improve this in Theorems 6.2 and 6.3 by showing that both high school laws hold in the Zermelo arithmetic, so that the Zermelo sum is an exponential arithmetic of sets and is in fact (see Theorem 6.4) the unique exponential arithmetic of sets.

Our strategy now is to show that many arithmetical facts follow from the above assumptions. This will enable us to prove arithmetical properties which the von Neumann and Zermelo arithmetics have in common. For example, both additions preserve ranks.

Lemma 3.3 *If $+_*$ is an additive arithmetic of sets, then $\rho(a +_* b) = \rho(a) + \rho(b)$.*

Proof A simple $\in$-induction on b. (Note that the $*$ subscript in the statement and proof of this lemma applies *only* to the $+$ to which it is attached. The notational convention introduced at the start of this section only applies when the subscript is attached to the relation or "main verb.") We have

$$\begin{aligned}\rho(a +_* b) &= \sup\{\rho(a +_* p) + 1 \mid p \in b\} \quad \text{using (v)}\\ &= \sup\{\rho(a) + \rho(p) + 1 \mid p \in b\} \quad \text{by inductive hypothesis}\\ &= \rho(a) + \rho(b),\end{aligned}$$

since b contains elements p of maximal rank if $\rho(b)$ is a successor ordinal, and of rank cofinal in $\rho(b)$ if it is a limit. □

In fact, the properties (i)–(iv) of addition alone are enough to prove many properties of addition shown for the von Neumann case in [5], such as the fact that any set is uniquely decomposed into a sum of additively irreducible sets, which falls out of Tarski's more general ordinal algebra of order types in [7].

In additive arithmetics we can also prove that multiplication and exponentiation preserve ranks.

Lemma 3.4 *If $+_*$ is an additive arithmetic of sets, then $\rho(a \cdot_* b) = \rho(a) \cdot \rho(b)$.*

Lemma 3.5 *If $+_*$ is an additive arithmetic of sets, then $\rho(a_*^b) = \rho(a)^{\rho(b)}$.*

Proof We prove Lemma 3.5; the proof of Lemma 3.4 is similar. By $\in$-induction on b,

$$\begin{aligned}\rho(a_*^b) &= \sup\{\rho(a_*^p \cdot_* q +_* r) + 1 \mid p \in b \wedge q \in a \wedge r \in a_*^p\} \\ &= \sup\{\rho(a)^{\rho(p)} \cdot \rho(q) + \rho(r) + 1 \mid p \in b \wedge q \in a \wedge r \in a_*^p\},\end{aligned}$$

by inductive hypothesis, Lemma 3.3, and Lemma 3.4. But this last ordinal equals $\rho(a)^{\rho(b)}$. □

In additive arithmetics we have some basic arithmetical properties of the product.

Lemma 3.6 *If $+_*$ is an additive arithmetic of sets, then*

$$x <_* a \cdot b \longleftrightarrow \exists q < b\ \exists r < a\ (x =_* a \cdot q + r).$$

Furthermore, such q, r are unique.

Proof This was shown for the von Neumann arithmetic in [5, Section 4], and once again the Zermelo form is easy to see from the graph interpretation, but let us sketch the proof with an eye to its reliance only on the properties (i)–(v) together with the inductive definition of multiplication.

Work by induction on b. To prove the left-to-right implication, suppose $x <_* a \cdot b$. Then for some $s \in b$ and $t \in a$, $x \leq_* a \cdot s + t$, and the interesting case is $x <_* a \cdot s + t$. By (v), either $x <_* a \cdot s$, in which case apply the inductive hypothesis to obtain q and r, or $x =_* a \cdot s + y$ with $y < t \in a$.

Conversely, consider $x =_* a \cdot q + r$ with $r < a$ and $q < b$. Choose t with $r \leq t \in a$. If $q \in b$, then, using (v), $x \leq_* a \cdot q + t \in_* a \cdot b$. Otherwise choose s with $q < s \in b$, so that by inductive hypothesis $x <_* a \cdot s \leq_* a \cdot s + t \in_* a \cdot b$.

For uniqueness, prove by induction on q that $a \cdot q + r =_* a \cdot s + t$ with $r, t < a$ implies that $q = s$ and $r = t$. By (iv) take e such that $a \cdot q + e =_* a \cdot s$ (or symmetrically). By left cancellation, $e + t =_* r$, so by (v), $e \leq r$; hence $e < a$ and $\rho(e) < \rho(a)$. Now by Lemmas 3.3 and 3.4,

$$\rho(a) \cdot \rho(q) + \rho(e) = \rho(a) \cdot \rho(s),$$

so by the usual (von Neumann) ordinal arithmetic $\rho(e) = 0$, hence $e = 0$, $a \cdot q =_* a \cdot s$, and using left cancellation $r = t$.

To show that $q = s$, suppose $u \in q$, and pick $v \in a$ since we may assume $a \neq 0$. Then $a \cdot u + v \in_* a \cdot q =_* a \cdot s$ so $a \cdot u + v =_* a \cdot w + x$ for some $w \in s$, $x \in a$. By inductive hypothesis $u = w$ so $u \in s$. It follows that $q \subseteq s$. By a symmetrical argument $s \subseteq q$ and hence $q = s$. □

A corollary of the uniqueness is that in any additive arithmetic of sets, the product preserves cardinalities.

Corollary 3.7 *If $+_*$ is an additive arithmetic of sets, then $|x \cdot_* y| = |x| \cdot |y|$. (The product on the right-hand side of this equation is the cardinal product.)*

This was shown for the von Neumann arithmetic in [5, Theorem 4.14]. Likewise the product of an additive arithmetic preserves the function $|TC(x)|$.[5] But other basic properties of the product need left distributivity.

Lemma 3.8 *In any multiplicative arithmetic of sets, multiplication is associative.*

Proof We show that $(a \cdot b) \cdot c =_* a \cdot (b \cdot c)$ by induction on c. Using the property (vi) and the inductive hypothesis, we obtain

$$\begin{aligned} x \in_* a \cdot (b \cdot c) &\longleftrightarrow \exists q \in c\, \exists s \in b\, \exists t \in a \left(x =_* a \cdot (b \cdot q + s) + t\right) \\ &\longleftrightarrow \exists q \in c\, \exists s \in b\, \exists t \in a \left(x =_* (a \cdot b) \cdot q + a \cdot s + t\right) \\ &\longleftrightarrow x \in_* (a \cdot b) \cdot c. \end{aligned}$$

□

Before turning our attention to exponentiation, we mention without details an example (which will not be needed in the sequel) showing that (vi) is independent of (i)–(v).

Example 3.9 Define a binary operation $+_t$ on sets by

$$x +_t 0 = x, \qquad x +_t y = TC(x) \cup \{x +_t r \mid r \in y\} \quad \text{if } y \neq 0.$$

Then $+_t$ is an additive arithmetic of sets but not a multiplicative arithmetic of sets. In fact, $\{1\} \cdot 2 \neq_t \{1\} + \{1\}$. Also, multiplication in this arithmetic is not associative: $\{1\} \cdot (\{1\} \cdot \{1\}) \neq_t (\{1\} \cdot \{1\}) \cdot \{1\}$.

4 Exponentiations of Sets

In the first part of this section we prove Theorem 1.2. After that we develop, in any additive arithmetic, the expansion to a given base.

We start with some general lemmas. The first follows directly from the definition of the product and uses (i).

Lemma 4.1 *Let $+_*$ be an additive arithmetic of sets. If $0 \in a$, then $\forall x\, (x \subseteq_* x \cdot a)$.*

Lemma 4.2 *Let $+_*$ be an additive arithmetic of sets. If $0 \in a$, then*

$$\forall xy\, (x \leq y \longrightarrow a^x \subseteq_* a^y).$$

Proof Working in the $*$-arithmetic, we show by induction on y that $\forall x \leq y\, (a^x \subseteq a^y)$. If $x < y$, choose w such that $x \leq w \in y$. Then

$$a^x \subseteq a^w \subseteq a^w \cdot a \subseteq \bigcup_{p \in y} (a^p \cdot a) = a^y,$$

the first subset relation by inductive hypothesis, the second by Lemma 4.1. □

Lemma 4.3 *Let $+_*$ be an additive arithmetic of sets. If $0 \in a$, then*

$$\forall xy\, (x < y \to a^x \cdot a \subseteq_* a^y \cdot a).$$

Proof Working in the $*$-arithmetic, choose v with $x \in v \leq y$. Then

$$a^x \cdot a \subseteq a^v \subseteq a^y \subseteq a^y \cdot a,$$

using the definition of exponentiation, Lemma 4.2, and Lemma 4.1. □

To prove Theorem 1.2, we need some particular properties of the Zermelo and von Neumann arithmetics.

Lemma 4.4 *For any sets a and x, $a^{x+1} =_z a^x \cdot a$.*

Proof This follows directly from the definitions of the Zermelo operations. (Of course this lemma is a special case of the first high school law, which we shall later prove in full for the Zermelo arithmetic.) □

Lemma 4.5 *In the von Neumann arithmetic, if $0 \in a$, then $\forall x\ (a^{x+1} = a^x \cdot a)$.*

Proof $a^{x+1} = a^x \cup (a^x \cdot a)$ from the definitions of the von Neumann operations. But by Lemma 4.1, $a^x \subseteq a^x \cdot a$. □

Proof of Theorem 1.2 We work in the von Neumann arithmetic, indicating where the proof in the Zermelo case differs. Use induction on x for fixed a. If $\rho(x)$ is a successor ordinal, $\gamma + 1$, say, choose $v \in x$ with $\rho(v) = \gamma$. Then for any $p \in x$, $\rho(p) \leq \gamma$, so by Lemma 4.3, $a^{\rho(p)} \cdot a \subseteq a^\gamma \cdot a$.

Since $a^x = \bigcup_{p\in x}(a^p \cdot a) = \bigcup_{p\in x}(a^{\rho(p)} \cdot a)$ by inductive hypothesis, it follows that $a^x = a^\gamma \cdot a = a^{\gamma+1}$ by Lemma 4.5 (or, in the Zermelo case, by Lemma 4.4).

If $\rho(x)$ is a limit ordinal, the induction step follows from

$$a^x = \bigcup_{p\in x}(a^{\rho(p)} \cdot a) = \bigcup_{p\in x} a^{\rho(p)+1},$$

Lemma 4.2, and the fact that ranks of elements of x are cofinal in $\rho(x)$. □

The simplified behavior when 0 is in the base given by Theorem 1.2 means that the high school laws hold for such bases in the von Neumann arithmetic, as was hinted at in Lemma 4.5.

Corollary 4.6 *If $0 \in a$, then $a^{b+c} = a^b \cdot a^c$ and $a^{b\cdot c} = (a^b)^c$ for all b and c.*

Proof Prove the first law by induction on the rank of c. If $\rho(c) = \gamma + 1$, then using successively Theorem 1.2, Lemma 3.3, Lemma 4.5, the inductive hypothesis, and Lemma 3.8,

$$\begin{aligned} a^{b+c} &= a^{\rho(b+c)} = a^{\rho(b)+\rho(c)} = a^{\rho(b)+\gamma+1} \\ &= a^{\rho(b)+\gamma} \cdot a = a^{\rho(b)} \cdot a^\gamma \cdot a = a^{\rho(b)} \cdot a^{\gamma+1} \\ &= a^b \cdot a^c. \end{aligned}$$

The proof when c has limit rank is similar.

Having established the first law, we prove the second law by induction on c. Suppose that $\rho(c) = \gamma + 1$. From Lemma 4.2 it follows that $0 \in a^b$, so we can apply Theorem 1.2 and Lemma 4.5 to give

$$(a^b)^c = (a^b)^{\rho(c)} = (a^b)^\gamma \cdot a^b.$$

By the inductive hypothesis this last set is equal to

$$a^{b\cdot\gamma} \cdot a^b = a^{b\cdot\gamma+b} = a^{b\cdot(\gamma+1)} = a^{\rho(b\cdot(\gamma+1))} = a^{\rho(b\cdot c)} = a^{b\cdot c}.$$

Again the proof can be adapted to the limit case. □

On the other hand, Theorem 1.2 means that exponentiation fails rather badly to be one-to-one in the exponent when 0 is an element of the base. Theorem 4.8 below will show that this situation is remedied when 0 is not in the base. To that end, we now work toward establishing the base-a expansion of a set in any additive arithmetic, first noting the following.

Proposition 4.7 *Suppose that $a > 1$ and $b \neq 0$. Then in any additive arithmetic of sets,*

$$x < a^b \longleftrightarrow \exists p < b\, \exists q < a\, \exists r < a^p\, (x = a^p \cdot q + r).$$

Proof Work in an additive arithmetic of sets. We have

$$TC(a^b) = TC \bigcup_{p \in b} (a^p \cdot a) = \bigcup_{p \in b} TC(a^p \cdot a).$$

It follows that

$$\begin{aligned} x < a^b &\longleftrightarrow \exists p \in b\, (x < a^p \cdot a) \\ &\longleftrightarrow \exists p \in b\, \exists u < a\, \exists v < a^p\, (x = a^p \cdot u + v) \quad \text{by Lemma 3.6.} \end{aligned} \tag{1}$$

This shows that if $x < a^b$, we may in fact take the p in the right-hand side of the proposition to be an element of b. On the other hand, by induction on b we can show that the right-hand side of the proposition implies $x < a^b$: if the right-hand side holds and $p \notin b$, choose e such that $p < e \in b$. By inductive hypothesis, $x < a^e = a^e \cdot 1 + 0 < a^b$ by (1). □

So, unlike the situation for ordinals, for a given base $a > 1$, not every set x can be expanded as in Proposition 4.7—only those x which are in the transitive closure of some power of a. When $0 \in a$ the expansion is not unique, by Theorem 1.2. However, we do have uniqueness (so long, of course, as we stipulate $q \neq 0$) when 0 is not an element of the base.

Theorem 4.8 *In any additive arithmetic of sets, if $0 \notin a$ and $a \neq 0$, then for any p, q, r, s, t, u,*

$$\begin{aligned} &0 < q < a \wedge 0 < t < a \wedge r < a^p \wedge u < a^s \wedge a^p \cdot q + r = a^s \cdot t + u \\ &\quad \longrightarrow p = s \wedge q = t \wedge r = u. \end{aligned}$$

Proof Working in an additive $*$-arithmetic, we show for fixed a by $\in$-induction on p that the theorem holds for any s and for any q, r, t, u as hypothesized. Suppose that

$$a^p \cdot q + r = a^s \cdot t + u.$$

By the property (iv), there is an e such that $a^p \cdot q + e = a^s \cdot t$ (or, symmetrically, $a^s \cdot t + e = a^p \cdot q$). By left cancellation $e + u = r$, hence $e \leq r < a^p$, using Lemma 3.6. Since the arithmetical operations preserve ranks, we move into the von Neumann arithmetic to say that $\rho(e) < \rho(a)^{\rho(p)}$ and

$$\rho(a)^{\rho(p)} \cdot \rho(q) + \rho(e) = \rho(a)^{\rho(s)} \cdot \rho(t).$$

By the uniqueness of the base-$\rho(a)$ expansion for ordinals, $\rho(e) = 0$ so $e = 0$ and $r = u$. Moving back to the $*$-arithmetic, we now know that $a^p \cdot q = a^s \cdot t$.

Let $q' \leq q$ be $<$-minimal such that $0 < q'$ and $\exists t' < a\ (a^p \cdot q' = a^s \cdot t')$. Suppose that q' has an element $q'' > 0$. Pick an element r'' of a^p. Then $a^p \cdot q'' + r'' \in a^p \cdot q' = a^s \cdot t'$, so for some $t'' \in t'$ and $u'' \in a^s$, $a^p \cdot q'' + r'' = a^s \cdot$

$t'' + u''$. Repeating the argument in the previous paragraph, it follows that $a^p \cdot q'' = a^s \cdot t''$, contradicting the minimality of q'. Thus $q' = 1$ and $a^p = a^s \cdot t'$. Hence, in another temporary move to the von Neumann arithmetic,

$$\rho(a)^{\rho(p)} = \rho(a)^{\rho(s)} \cdot \rho(t'), \quad \text{with } \rho(t') < \rho(a).$$

Ordinal arithmetic gives $\rho(t') = 1$, that is, $t' = 1$, so back in the $*$-arithmetic $a^p = a^s$. By left cancellation of multiplication (which follows from Lemma 3.6), we have $q = t$. It remains to prove that $p = s$.

To show $p \subseteq s$, we may assume $p \neq 0$. Let v be any element of p, and choose $w \in a$ and $x \in a^v$. Then $a^v \cdot w + x \in a^p = a^s$, so for some $c \in s$, $d \in a$, and $e \in a^c$, $a^v \cdot w + x = a^c \cdot d + e$. This is where we use the assumption that $0 \notin a$: it implies that $d \neq 0$ and $w \neq 0$ so we can apply the inductive hypothesis to deduce that $v = c$ and hence $v \in s$. Thus $p \subseteq s$. A symmetrical argument shows that $s \subseteq p$ and hence $p = s$. □

Proposition 4.7 and Theorem 4.8 iterate as usual to a full base-a expansion.

Theorem 4.9 *In any additive arithmetic of sets, if $a > 1$, $b \neq 0$, and $0 < x < a^b$, then there exist $n \in \omega$, $b > p_1 > p_2 > \cdots > p_n$, and $0 < q_i < a$ for $1 \leq i \leq n$ such that*

$$x = a^{p_1} \cdot q_1 + \cdots + a^{p_n} \cdot q_n.$$

If $0 \notin a$, this expansion is unique.

5 Von Neumann Exponentiation

Here are the simplest examples of the failure of the high school laws in the von Neumann arithmetic of sets.

Example 5.1 $\{1\}^2 \neq \{1\} \cdot \{1\}$.

To verify this inequality, let $\gamma = \{\{1, \{1\}\}\} = \{\{1\} + 1\} = \{1\} \cdot \{1\} = \{1\}^{\{1\}}$. From the definition of exponentiation, $\{1\}^2 = \{1, \{1\} + 1\} \neq \gamma$. The graph representations of the two sets $\{1\}^2$ and $\{1\} \cdot \{1\}$ are shown in Figure 2.

Example 5.2 $\{1\}^{\{1\}\cdot\{1\}} \neq (\{1\}^{\{1\}})^{\{1\}}$.

Figure 3 gives the graph representations of these two sets.

To see that these two sets are different without completing the tedious computations of both, note that for any x,

$$x^{\{y\}} = x^y \cdot x, \tag{2}$$

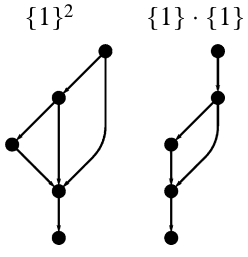

Figure 2 The failure of the first high school law in the von Newmann arithmetic.

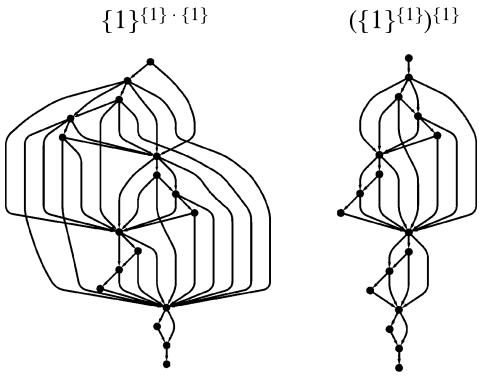

Figure 3 The failure of the second high school law in the von Newmann arithmetic.

and in particular $x^{\{1\}} = x \cdot x$. Further, the von Neumann product preserves cardinalities (see Corollary 3.7). It follows that $(\{1\}^{\{1\}})^{\{1\}} = \{1\} \cdot \{1\} \cdot \{1\} \cdot \{1\}$ has just one element. On the other hand, $\{1\}^{\{1,\{1\}\}}$ has two elements, namely, $\{1\} + 1$ and $\gamma + \{1\} + 1$, so $\{1\}^{\gamma} = \{1\}^{\{1,\{1\}\}} \cdot \{1\}$ must also have two elements.

The reader may care to contrast the graphs of these terms in the von Neumann arithmetic with the much simpler graph of $\{1\}^{\{1\}\cdot\{1\}} =_z (\{1\}^{\{1\}})^{\{1\}} =_z 16$ in the Zermelo arithmetic.

An odd sort of hybrid arithmetic falls out of (2): it says that in the von Neumann arithmetic, a^{n_z} equals the product of n copies of a.

I conclude this section by noting that the von Neumann arithmetic does have a modified form of the first high school law, which can be proved by adapting the proof of Theorem 6.2 below.

Proposition 5.3 *For any sets a, b, and c,* $a^{b+c} = a^b \cup (a^b \cdot a^c)$.

6 Zermelo Exponentiation

Now we complete the proof of Theorem 1.1 by deriving the high school laws in the Zermelo arithmetic.

Lemma 6.1 *In any multiplicative arithmetic of sets,*

$$a^b \cdot a^c = \{a^b \cdot a^p \cdot q + r \mid p \in c \wedge q \in a \wedge r \in a^b \cdot a^p\}.$$

Proof Work in a multiplicative $*$-arithmetic of sets. We have

$$\begin{aligned} a^b \cdot a^c &=_* \left\{a^b \cdot (a^p \cdot q + s) + t \;\middle|\; p \in c \wedge q \in a \wedge s \in a^p \wedge t \in a^b\right\} \\ &=_* \{a^b \cdot a^p \cdot q + a^b \cdot s + t \mid p \in c \wedge q \in a \wedge s \in a^p \wedge t \in a^b\} \\ &=_* \{a^b \cdot a^p \cdot q + r \mid p \in c \wedge q \in a \wedge r \in a^b \cdot a^p\}, \end{aligned}$$

noting uses of left distributivity (see property (vi)) and associativity of multiplication (see Lemma 3.8). □

Theorem 6.2 *For any sets a, b, and c,* $a^{b+c} =_z a^b \cdot a^c$.

Proof By $\in$-induction on c for fixed a, b, and using the definition of the Zermelo sum,

$$\begin{aligned} a^{b+c} &=_z \{a^{b+p}\cdot q + r \mid p \in c \wedge q \in a \wedge r \in a^{b+p}\} \\ &=_z \{a^b \cdot a^p \cdot q + r \mid p \in c \wedge q \in a \wedge r \in a^b \cdot a^p\} \quad \text{by inductive hypothesis} \\ &=_z a^b \cdot a^c \quad \text{by Lemma 6.1;} \end{aligned}$$

note that the first equality fails in the von Neumann arithmetic. □

Theorem 6.3 *For any sets a, b, and c, $a^{b\cdot c} =_z (a^b)^c$.*

Proof By induction on c:

$$\begin{aligned} a^{b\cdot c} &=_z \{a^{b\cdot q+r}\cdot v + w \mid q \in c \wedge r \in b \wedge v \in a \wedge w \in a^{b\cdot q+r}\} \\ &=_z \{a^{b\cdot q}\cdot a^r \cdot v + w \mid q \in c \wedge r \in b \wedge v \in a \wedge w \in a^{b\cdot q}\cdot a^r\} \\ &\quad \text{by Theorem 6.2} \\ &=_z \{a^{b\cdot q}\cdot a^r \cdot v + a^{b\cdot q}\cdot s + u \mid q \in c \wedge r \in b \wedge v \in a \wedge s \in a^r \wedge u \in a^{b\cdot q}\} \\ &=_z \left\{a^{b\cdot q}\cdot (a^r \cdot v + s) + u \;\middle|\; q \in c \wedge r \in b \wedge v \in a \wedge s \in a^r \wedge u \in a^{b\cdot q}\right\} \\ &=_z \left\{(a^b)^q \cdot t + u \;\middle|\; q \in c \wedge t \in a^b \wedge u \in (a^b)^q\right\} \quad \text{by inductive hypothesis} \\ &=_z (a^b)^c. \end{aligned}$$

□

So the Zermelo sum is an exponential arithmetic of sets. Our final result says that it is the only exponential arithmetic of sets: obeying the high school laws makes the Zermelo arithmetic of sets unique among the class of multiplicative arithmetics of sets.

Theorem 6.4 *If $+_*$ is an exponential arithmetic of sets, then $+_*$ is identical with $+_z$.*

Proof Suppose that $+_*$ satisfies the properties (i)–(vi) and differs from $+_z$: we shall show that (vii) fails in the $*$-arithmetic. Take b, c such that $b +_* c \neq b +_z c$. For this b, we may assume that c is $\in$-minimal with this property.

The first case is when there is x such that $x \in b +_* c$ but $x \notin b +_z c$. So for any $p \in c$, $x \neq b +_z p = b +_* p$.

Pick any nonempty a with $0 \notin a$. Also pick any $u \in a$ (so u will be nonempty) and $v \in a^x$. Then

$$a^x \cdot u + v \in_* a^{b+c},$$

since $x \in_* b + c$. On the other hand,

$$a^x \cdot u + v \notin_* a^b \cdot a^c,$$

for suppose otherwise. Using the minimality of c, we can mimic the reasoning in the proof of Theorem 6.2 to show by induction on p that $p < c \longrightarrow a^{b+p} =_* a^b \cdot a^p$. So by Lemma 6.1, for these values of a, b, and c:

$$a^b \cdot a^c =_* \{a^{b+p}\cdot q + r \mid p \in c \wedge q \in a \wedge r \in a^{b+p}\}.$$

By our supposition, $a^x \cdot u + v =_* a^{b+p}\cdot q + r$ for some such p, q, r. By Theorem 4.8, $x =_* b + p$, which is a contradiction.

Thus $a^{b+c} \neq_* a^b \cdot a^c$.

In the second case, there is an x with $x \in b +_z c$ and $x \notin b +_* c$. So there is an element p of c such that $b + p \notin_* b + c$. Picking suitable a, q, and r, and $*$-characterizing $a^b \cdot a^c$ as above, we have $a^{b+p} \cdot q + r \in_* a^b \cdot a^c$. On the other hand, we can conclude from another appeal to Theorem 4.8 that $a^{b+p} \cdot q + r \notin_* a^{b+c}$, so again $a^{b+c} \neq_* a^b \cdot a^c$. □

Notes

1. Later, Garcia [2] used the same exponentiation again and also four alternative definitions of exponentiation, only two of which are equivalent, and none of which agrees with Scott's.

2. Following normal usage, by "ordinal" *tout court*, I mean von Neumann ordinal.

3. See Kanamori [4, p. 25].

4. See Grzegorczyk [3] for an account.

5. On the other hand, exponentiation fails to preserve cardinalities in any of the arithmetics considered here. This failure, well known in the usual ordinal arithmetic for infinite ordinals, occurs here even for finite sets.

References

[1] Garcia, N., "Operating on the universe," *Archive for Mathematical Logic*, vol. 27 (1988), pp. 61–8. Zbl 0633.03045. MR 0955312. DOI 10.1007/BF01625835. 450

[2] Garcia, N., "A theory of operations on the universe, I: The theory of iteration and F-ordinals," *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, vol. 37 (1991), pp. 385–92. MR 1270182. DOI 10.1002/malq.19910372502. 461

[3] Grzegorczyk, A., "Undecidability without arithmetization," *Studia Logica*, vol. 79 (2005), pp. 163–230. Zbl 1080.03004. MR 2135033. DOI 10.1007/s11225-005-2976-1. 461

[4] Kanamori, A., "The mathematical development of set theory from Cantor to Cohen," *Bulletin of Symbolic Logic*, vol. 2 (1996), pp. 1–71. Zbl 0851.04001. MR 1380824. DOI 10.2307/421046. 461

[5] Kirby, L., "Addition and multiplication of sets," *Mathematical Logic Quarterly*, vol. 53 (2007), pp. 52–65. Zbl 1110.03034. MR 2288890. DOI 10.1002/malq.200610026. 449, 453, 454, 455

[6] Kirby, L., "Ordinal operations on graph representations of sets," *Mathematical Logic Quarterly*, vol. 59 (2013), pp. 19–26. Zbl 1275.03138. MR 3032422. DOI 10.1002/malq.201100082. 449, 450, 451, 452, 453

[7] Tarski, A., "The notion of rank in axiomatic set theory and some of its applications," *Bulletin of the American Mathematical Society*, vol. 61 (1955), p. 443. 449, 453, 454

[8] Zermelo, E., "Investigations in the foundations of set theory, I" pp. 199–215 in *From Frege to Gödel*: *A Source Book in Mathematical Logic, 1879–1931*, edited by Jean van Heijenoort, Harvard University Press, Cambridge, Mass., 2002. 451

Department of Mathematics
Baruch College
City University of New York
New York, New York 10010
USA
laurence.kirby@baruch.cuny.edu
http://faculty.baruch.cuny.edu/lkirby/