ELSEVIER Journal of Pure and Applied Algebra 154 (2000) 295–298

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Objective number theory and the retract chain condition

Stephen H. Schanuel *

SUNY at Buffalo, 106 Diefendorf Hall, Buffalo, NY 14214-3093, USA

Communicated by M. Tierney

To Bill Lawvere

Abstract

In an extensive category satisfying a mild chain condition, the arithmetic of multiplication and addition (cartesian product and coproduct) of objects is shown to be very close to that of natural numbers. Examples of such categories abound, e.g. in algebraic geometry. © 2000 Elsevier Science B.V. All rights reserved.

MSC: 11A99; 18A99

0. Dedication and introduction

As one might imagine, the opportunity to discuss mathematics with Bill Lawvere for 25 years has been a constant joy for which I cannot adequately express my gratitude. Recently, these conversations have turned with increasing frequency to questions about finite sums and products, and I think that we have both been pleasantly surprised to see how much follows from the most elementary considerations. Bill and I plan a short book on this subject, of which this talk outlines one corner, the initial consequences of a weak finiteness condition.

1. Arithmetic of objects and the extensive law

Objective number theory is the study of addition and multiplication (and eventually exponentiation) of objects in suitable categories. An abstract set does not come equipped with preferred algebraic operations, but a category is often more obliging:

* Tel.: 1-716-829-2144; fax: 1-716-829-2299.

E-mail address: schanuel@buffalo.edu (S.H. Schanuel).

PII: S0022-4049(99)00185-1

cartesian products and coproducts are uniquely determined, if they exist. Also, in any category with finite coproducts and finite products, most of the usual laws of arithmetic are automatic: the commutative, associative, and identity laws for addition and multiplication of isomorphism classes of objects are forced by the universal properties characterizing sum and product; but the distributive law is not, since it involves a relation between limits and colimits. A category with finite products and coproducts is said to be *distributive* if the canonical maps

$$\sum_{i=1}^{n}(A_i \times B) \to \left(\sum_{i=1}^{n} A_i\right) \times B$$

are isomorphisms; here $n \geq 0$, but the case $n = 2$ suffices, as Robin Cockett observed. (The analogous notion in algebra is *rig*, a set with two commutative monoid structures 0, $+$ and 1, $\times$, satisfying

$$\sum_{i=1}^{n}(a_i \times b) = \left(\sum_{i=1}^{n} a_i\right) \times b,$$

but in algebra both $n = 0$ and $n = 2$ are needed.)

Often a category is distributive because one of the two operations, plus or times, is so friendly that the other is perforce compatible with it. For multiplication: if the functor ‘multiplication by a fixed object’ has a right adjoint (i.e. if function spaces exist in the category) then this multiplication preserves whatever colimits exist, in particular sums, so the category is distributive. For addition: if sums resemble disjoint unions, the distributive law is again forced. More precisely, call a category $\boldsymbol{E}$ *extensive* if it has finite coproducts (sums) and for each pair A, B of objects the obvious functor

$$\boldsymbol{E}/A \times \boldsymbol{E}/B \to \boldsymbol{E}/(A+B)$$

is an equivalence; if $\boldsymbol{E}$ has also finite products, this extensive law implies the distributive law. The current consensus calls an extensive category with finite products a *prextensive* category, and an extensive category which is lex (has all finite limits) a *lextensive* category.

Our subject will be prextensive categories $\boldsymbol{E}$, and our question is: “To what extent does the number theory of $\boldsymbol{E}$ resemble the number theory of the category of finite sets?” We can interpret ‘number theory’ narrowly as the algebra of the set of isomorphism classes equipped with 0, 1, $+$, and $\times$, so that the number theory of the category of finite sets is exactly the rig of natural numbers (but see Section 3 for an additional family of algebraic operations.) Sometimes we take it more broadly, so that our question becomes: “To what extent does the category $\boldsymbol{E}$ resemble the category $\boldsymbol{S}$ of finite sets?”; that is, we can take ‘number theory’ in the classical case to include much of finite combinatorics, as did our ancestors when they spoke of ‘square numbers’, ‘triangular numbers’, etc.

2. Examples of extensivity

Any topos is extensive, but extensivity is far more pervasive. If $\boldsymbol{E}$ is extensive or lextensive, so is $\boldsymbol{E}/B$ for any object B of $\boldsymbol{E}$ and so is $\boldsymbol{E}^{\boldsymbol{C}^{\mathrm{op}}}$ for any small category $\boldsymbol{C}$. If $\boldsymbol{E}$ is extensive, any full subcategory closed under sums and summands is extensive. A rule of thumb is that any 'category of space' is extensive, e.g. all the standard examples of categories of analytic spaces, algebraic spaces, piecewise linear spaces, topological spaces, or spaces with action of a group G. Two special examples motivated much of our work: From algebraic geometry $(k\text{-}Alg)^{\mathrm{op}}$, the opposite of the category of finitely generated commutative k-algebras for a commutative Noetherian base ring k, and from combinatorics the category *Graph* of finite directed graphs, i.e. the presheaf category $\boldsymbol{S}^{\boldsymbol{C}^{\mathrm{op}}}$, where $\boldsymbol{S}$ is the category of finite sets and $\boldsymbol{C}$ has only two objects A and D and only two non-identity maps, 'source' and 'target', both from D to A. Typically, facts were rather evident in the latter example, and to us less so in the former (sometimes requiring the assistance of Don Schack and Shuen Yuan). The desire to unite these extremes led eventually to simple hypotheses and the resulting almost trivial proofs.

3. Separable, connected

Two classes of objects play a role in analyzing a prextensive category. In any category $\boldsymbol{E}$ with finite coproducts, an object C is *connected* if the functor $\boldsymbol{E}(C,-)$ to sets preserves these; for an extensive category this is equivalent to: $C \neq 0$ and if $C = A + B$ then $A = 0$ or $B = 0$. (In particular, this is the standard notion in topology and in algebraic geometry.) If $\boldsymbol{E}$ is extensive, it turns out that a complementary summand for a subobject is unique (as subobject, not merely as object) if it exists. In particular, if the diagonal map $S \to S \times S$ has has a complement, we say that S is *separable* and denote the complement by $S^{\downarrow 2}$, called the 'second *falling power*' and thought of as the 'object of distinct pairs'. (More precisely, it is the object of *disjoint* pairs, i.e. represents the functor assigning to each X the set of pairs of maps $X \to S$ with equalizer 0.) For separable S, the higher falling powers $S^{\downarrow n}$ are easily defined and exist automatically. With some license one can write $S^{\downarrow n} = S(S-1)\dots(S-(n-1))$; to prove the formulas (e.g. for $(S_1 + S_2)^{\downarrow n}$) suggested by this license is not difficult. A typical example is

$$S^n = \sum S^{\downarrow (n/\sim)}$$

with the sum over all equivalence relations on n, splitting the object of n-tuples into terms according to which components are equal. If $S^{\downarrow n} = 0$ for some natural number n, we say that S is *falling nilpotent*.

A consequence of the extensive law is that for any map f with codomain a sum, the pullbacks of f along the inclusions of the summands exist and f is the sum of these. In particular, with C connected and S separable, any two maps $C \to S$ together yield a map $C \to S^2 = S + S^{\downarrow 2}$, giving a (necessarily trivial) decomposition of C, and we get: the maps are either equal or disjoint, i.e. have equalizer 0. Likewise,

$$\boldsymbol{E}(C, S^{\downarrow n}) = \boldsymbol{E}(C, S)^{\downarrow n},$$

i.e. a map $C \to S^{\downarrow n}$ is a distinct n-tuple of maps $C \to S$, so that for points with connected domain, $S^{\downarrow n}$ represents merely distinct n-tuples.

4. The retract chain condition and algebraic objects

We say that a category $\boldsymbol{E}$ has the *retract chain condition* (RCC) if for any infinite chain

$$X_0 \underset{s_1}{\overset{r_1}{\rightleftarrows}} X_1 \underset{s_2}{\overset{r_2}{\rightleftarrows}} X_2 \underset{s_3}{\overset{r_3}{\rightleftarrows}} X_3 \underset{s_4}{\overset{r_4}{\rightleftarrows}}$$

with $r_i s_i = 1$ for all i, it follows that some $s_n r_n = 1$. This condition is self dual, and easily seen to be true for commutative Noetherian rings, hence for our basic example from algebraic geometry (and even more trivially for any category with all homsets finite, e.g. *Graph*). If $\boldsymbol{E}$ is extensive with RCC, it follows that every object is (uniquely) a finite sum of connected objects, since if A were not, one could construct an infinite chain of retracts starting with $A+A$. By the *spectrum* of an object X is meant the set of cardinalities $\#\boldsymbol{E}(C,X)$ for connected C; if these cardinalities are bounded by some natural number, we say that *X has bounded spectrum.*

For the rest of this section, $\boldsymbol{E}$ is prextensive with RCC.

Theorem. *For $X \in \boldsymbol{E}$, the following are equivalent*:
(1) *X is algebraic*, i.e. *there exist $p(T) \neq q(T) \in \mathbb{N}[T]$ with $p(X) \cong q(X)$.*
(2) *X has bounded spectrum.*
(3) *X is separable and falling nilpotent.*
(4) *Only finitely many connected objects are summands of powers of X.*

The proof actually makes things more explicit; e.g. if X has bounded spectrum, then two polynomials agree at X if and only if they agree on the spectrum. Note that since every object is uniquely a finite sum of connected objects, the rig of isomorphism classes is additively free, so it maps injectively to the associated ring; it is now literally correct to write $X^{\downarrow 2} = X(X-1)$, etc., and to rewrite $p(X) = q(X)$ as an equation $f(X) = 0$ where $f(T) \in \mathbb{Z}[T]$. The implication (1) $\Rightarrow$ (3) now says that if X satisfies *any* equation, then X is also 'separable over $\mathbb{N}$', i.e. satisfies a monic equation $X(X-1)\cdots(X-k) = 0$ with distinct natural number roots.

The analogy between algebraic objects and algebraic numbers extends quite far. Given finitely many algebraic objects in a prextensive $\boldsymbol{E}$ with RCC, the smallest full subcategory containing these and closed under products, sums, and summands, is again prextensive with RCC; but now every object is algebraic and there are only finitely many connected objects. Conversely, if $\boldsymbol{E}$ is prextensive with RCC and only finitely many connected objects, then all objects are algebraic, and we may think of $\boldsymbol{E}$ as a partial analog of the ring of algebraic integers in a finite extension of the field of rational numbers.