A FINITE ORDER ARITHMETIC FOUNDATION FOR COHOMOLOGY

COLIN MCLARTY

> I affirm the principal force in all my work has been the quest for the "general." In truth I prefer to accent "unity" rather than "generality." But for me these are two aspects of one quest. Unity represents the profound aspect, and generality the superficial aspect. (Grothendieck, 87, p. PU 25)

Abstract: Large-structure tools like toposes and derived categories in cohomology never go far from arithmetic in practice, yet existing formalizations are stronger than ZFC. We formalize the practical insight by grounding the entire toolkit of EGA and SGA at the level of finite order arithmetic.

Grothendieck pre-empted many set theoretic issues in cohomology by positing a *universe*: "a set 'large enough' that the habitual operations of set theory do not go outside it" (SGA 1 VI.1 p. 146). His universes prove Zermelo-Fraenkel set theory with choice (ZFC) is consistent, so ZFC cannot prove they exist. This paper founds the EGA and SGA on axioms with the proof theoretic strength of finite order arithmetic. Even Zermelo set theory (Z) proves these axioms consistent. So functors from all modules on a scheme to all Abelian groups achieve unity by generality indeed, but with little generality in the set theoretic sense.

Outline. Section 1 introduces the issues by formalizing EGA and SGA with weaker universes within ZFC. Section 2 opens the serious reduction to Mac Lane set theory (MC) a fragment of ZFC with the strength of finite order arithmetic. Section 3 develops category theory in MC, with special care for injective resolutions. Section 4 gives a conservative extension of MC with classes and collections of classes so Sections 5–6 can develop large-scale structures of cohomology at the strength of finite order arithmetic.

We use a simple notion of $\mathcal{U}$-category which Grothendieck rejected at SGA 4 I.1.2 (p. 5). We cannot go through all the SGA and EGA. Most of that is commutative algebra elementary in logical strength. We focus on cohomology, geometric morphisms, duality and derived categories, and fibred categories. This supports the entire EGA and SGA. Section 7 relates this to prospects for proving Fermat's Last Theorem (FLT) in Peano Arithmetic.

1. Replacement, separation, and the quick route to ZFC

We can formalize EGA and SGA verbatim within ZFC by using a weaker definition of universe. We only modify the proof that cohomology groups exist.

Zermelo set theory with choice (ZC) is ZFC without foundation or replacement but with the separation axiom scheme. This says for any set A and formula $\Psi(x)$

of set theory there is a set B of all elements of A which have Ψ:

$$B = \{x \in A \mid \Psi(x)\}$$

For example, the n-th iterated powerset of the natural numbers $\mathcal{P}^n(\mathbb{N})$ is definable in terms of n, so replacement in ZFC proves there is a set $\{\mathcal{P}^i(\mathbb{N}) \mid i \in \mathbb{N}\}$. That proof fails in ZC for lack of any set A provably containing all $\mathcal{P}^n(\mathbb{N})$ and this cannot be evaded. The ZFC set $V_{\omega+\omega}$ of all sets with rank below $\omega+\omega$ models ZC, and $\{\mathcal{P}^i(\mathbb{N}) \mid i \in \mathbb{N}\}$ is not in it since it has rank $\omega+\omega$.

A *ZC universe* is a transitive set U modelling ZC with every subset $B \subseteq A \in U$ of an element of U also an element $B \in U$. ZFC proves these are the sets $U = V_\alpha$ for limit ordinals $\alpha > \omega$ so they exist and each is an element of a larger one.

Grothendieck's approach performs each geometric construction in some universe. No proof in EGA or SGA uses replacement, so all can be done in any ZC universe. But the whole rests on cohomology groups, whose existence follows from a theorem cited without proof in SGA: every module over a ring R embeds in an *injective* R-module. The category of R-modules has *enough injectives.*

Baer (1940) proved this for modules in sets by using replacement in the form of transfinite recursion. Then Eckmann and Schopf (1953) showed without replacement that every Abelian group embeds in a injective, and the result extends to modules. Rather than use the Eckmann-Schopf proof, Grothendieck (1957a) lifted Baer's transfinite recursion to a categorical context including categories of modules in any Grothendieck topos (albeit toposes were undreamt of at that time).

In hindsight Grothendieck had a reason not to use Eckmann-Schopf. The proof that ordinary Abelian groups embed in injectives requires the axiom of choice (Blass, 1979). So it will not lift to every Grothendieck topos. Barr (1974) overcame this by showing every Grothendieck topos E is covered by one that satisfies choice called a *Barr cover* of E. This first step works in a Barr cover of E, and the result descends from the cover to E (Johnstone, 1977, p. 261). Compare van Osdol (1975).

The descent uses a formal triviality first made explicit by Maranda (1964, p. 108) and Verdier in (Artin et al., 1964, §V lemma 0.2):

Lemma 1.1. *If a functor $\mathcal{F}\colon\mathcal{B}\to\mathcal{A}$ has a left exact left adjoint $\mathcal{G}\colon\mathcal{A}\to\mathcal{B}$ with monic unit and $\mathcal{B}$ has enough injectives then so has $\mathcal{A}$.*

Proof. Since units are monic, every monic $\mathcal{G}(A)\rightarrowtail B$ has monic adjunct $A\rightarrowtail\mathcal{F}(B)$. Since $\mathcal{G}$ preserves monics, $\mathcal{F}$ preserves injectives. If object A in $\mathcal{A}$ has a monic $\mathcal{G}(A)\rightarrowtail I$ to an injective in $\mathcal{B}$, the adjunct $A\rightarrowtail\mathcal{F}(I)$ is monic. □

Take the category of Abelian groups in any Grothendieck topos as $\mathcal{A}$, while $\mathcal{B}$ is the category of Abelian groups in a Barr cover of it. Thus $\mathcal{A}$ has enough injectives.

Next, apply the same triviality to the functor taking each Abelian group A to the R-module $Hom_{\mathbb{Z}}(R, A)$ of additive functions from R to A, with scalar multiplication:

$$(r \cdot f)(x) = f(r \cdot x)$$

This functor is defined in any elementary topos with natural numbers. The underlying Abelian group functor on R-modules is left adjoint, and is left exact as it is right adjoint to tensor with R. The unit $\eta\colon A\rightarrowtail Hom_{\mathbb{Z}}(R, A)$ takes each $a \in A$ to the function $r \mapsto r \cdot a$, so is monic. The category of R-modules has enough injectives. Section 3.6.1 revisits this with more care and weaker set theory.

Thus ZFC can formalize the EGA and SGA entire, and all existing proofs in cohomological number theory. But it is visibly vastly stronger than needed.

2. Mac Lane set theory

Mac Lane set theory (MC) is ZC with bounded separation, that is separation only using formulas $\Psi(x)$ with only bounded (Δ_0) quantifiers. In terms of Mathias (2001, 107), MC is ZBQC omitting foundation or **Mac** omitting foundation and transitive containment. It is finitely axiomatizable like Gödel-Bernays set theory, so ZC proves it consistent. It has the proof theoretic strength of finite order arithmetic, in the sense of the simple theory of types with infinity (see Takeuti (1987, Part II)).

Mathias (2001) makes the contrast to ZC: ZC proves "$\forall n \in \mathbb{N}$ there exists an n-th iterated powerset $\mathcal{P}^n(\mathbb{N})$." MC says $\mathbb{N} = \mathcal{P}^0(\mathbb{N})$ exists; and it proves if $\mathcal{P}^n(\mathbb{N})$ exists then so does $\mathcal{P}^{(n+1)}(\mathbb{N})$ since MC has powersets. So MC proves each finitely iterated case, say $\mathcal{P}^5(\mathbb{N})$. But the formula "there exist n successively iterated powersets of $\mathbb{N}$" with variable n escapes any fixed bound on the powersets, so MC cannot prove the formula defines a subset of $\mathbb{N}$ and cannot apply induction to it. Mathias shows MC indeed cannot prove "$\forall n \in \mathbb{N}$ there exists $\mathcal{P}^n(\mathbb{N})$."

Contrast the real coordinate spaces $\mathbb{R}^n$. Each $n \in \mathbb{N}$ determines $\mathbb{R}^n$ by a definable relation, but furthermore each $\mathbb{R}^n$ is an element of $\mathcal{P}^2(\mathbb{N}\times\mathbb{R})$, and the set of all is defined by a Δ_0 condition with free variable V:

$$\exists n \in \mathbb{N}\ \forall y \in \mathcal{P}(\mathbb{N}\times\mathbb{R})\ (y \in V \text{ iff } y \text{ is a function from } \{x \in \mathbb{N} | x < n\} \text{ to } \mathbb{R})$$

So MC proves there is a set $\{\mathbb{R}^n | n \in \mathbb{N}\}$. Most constructions in mathematics are naturally bounded like this. In particular the site constructions in the Barr covering theorem are bounded and work in MC (Mac Lane and Moerdijk, 1992, p. 511).

As a useful way of bounding sets we define an *I-indexed* set of sets as a function $f : A \to I$. Each set A_i is the preimage of $i \in I$:

$$A_i = \{x \in A | f(x) = i\ \}$$

It is a set of *disjoint* sets with disjoint union A.

3. Category theory in MC

Category theory in MC must avoid replacement and unbounded separation. We also avoid "classes" or "locally small categories" until Section 4 makes them precise.

3.1. **Small categories.** A *small category* $\mathcal{C}$ is a set C_0 called the objects and a set C_1 called the arrows with domain and codomain functions d_0, d_1 and composition m satisfying the category axioms. A *functor* $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ of small categories is an *object part* $F_0 : C_0 \to D_0$ and *arrow part* $F_1 : C_1 \to D_1$ commuting with composition and identity arrows in the standard way. In fact $\mathcal{F}$ is fully determined by its arrow part F_1, because F_0 is determined by the effect of F_1 on identity arrows.

For any small categories $\mathcal{B}, \mathcal{C}$ there is a small category $\mathcal{B}^{\mathcal{C}}$ of all functors $\mathcal{C} \to \mathcal{B}$, with natural transformations as arrows (Mac Lane, 1998, pp. 40–42). The functors can be represented by suitable functions $C_1 \to B_1$ between the sets of arrows, so the set of all functors appears as a subset of the function set $B_1^{C_1}$. Natural transformations are certain functions $C_0 \to B_1$ from objects of $\mathcal{C}$ to arrows of $\mathcal{B}$, so the set of them appears as a subset of the function set $B_1^{C_0}$. The defining conditions of these subsets are equations between given objects and arrows and thus are Δ_0.

3.2. **Presheaves.** A *presheaf* F on a small category $\mathcal{C}$ is a contravariant functor from $\mathcal{C}$ to sets. But sets do not form a small category so the above definition of functors does not apply. And in the absence of replacement, a rule associating a set $F(A)$ to each object $A \in C_0$ of $\mathcal{C}$ might give no set containing all the values $F(A)$.

So we define a presheaf F on $\mathcal{C}$ as a C_0-indexed set of sets $\gamma_0 : F_0 \to C_0$ with an action e_F as follows. For each $A \in C_0$ the value $F(A)$ is:

$$F(A) = \{s \in F_0 \mid \gamma_0(s) = A\}$$

The action is a function $e_F : F_1 \to F_0$ where F_1 is the set

$$F_1 = \{\langle s, f\rangle \in F_0 \times C_1 \mid \gamma_0(s) = d_1(f)\}$$

The elements of F_1 are $\langle s, f\rangle$ where $s \in F(d_1(f))$. And we require these Δ_0 conditions: for all arrows $g : B \to A$ and $h : C \to B$ in $\mathcal{C}$, and all $s \in F(A)$

(1) $e_F\langle s, g\rangle \in F(B)$.
(2) $e_F\langle s, gh\rangle = e_F\langle e_F\langle s, g\rangle, h\rangle$.
(3) $e_F\langle s, 1_A\rangle = s$ for the identity arrow 1_A.

Clause 1 says we can define $F(g) : F(A) \to F(B)$ by $(F(g))(s) = e_F\langle s, g\rangle$. Clauses 2–3 express functoriality for composition and identity arrows.

A *natural transformation* $\eta : F \to G$ of presheaves is a function over C_0

$$\begin{tikzcd} F_0 \arrow[rr, "\eta"] \arrow[dr, "\gamma_0"'] & & G_0 \arrow[dl, "\gamma_0'"] \\ & C_0 & \end{tikzcd} \qquad \gamma_0 = \gamma_0'\eta$$

which commutes with the actions e_F and e_G in the obvious way.

Any set of presheaves has a set of all transformations between them. Precisely, an *I-indexed set* of presheaves on a small category $\mathcal{C}$ is a $C_0 \times I$-indexed set of sets $\gamma_0 : F_0 \to C_0 \times I$ with an I-indexed action $e_F : F_1 \to F_0$ where now

$$F_1 = \{\langle s, f, i\rangle \in F_0 \times C_1 \times I \mid \gamma_0(s) = \langle d_1(f), i\rangle\}$$

Each $A \in \mathcal{C}$ and $i \in I$ determine a set $F(A, i)$. The action must satisfy equations saying for each arrow $g : B \to A$ in $\mathcal{C}$ and index i it induces a function $F(g, i) : F(A, i) \to F(B, i)$ and is functorial. For any $i, j \in I$ a natural transformation $F(\_, i) \to F(\_, j)$ is a subset of $F_0 \times F_0$. So all these transformations form a subset of the powerset $\mathcal{P}(F_0 \times F_0)$, with defining conditions bounded by F_1.

Given parallel natural transformations $\eta, \iota : F \to G$ of presheaves the usual construction of a coequalizer works in MC (Mac Lane, 1998, p. 115). And every indexed set $\gamma_0 : F_0 \to C_0 \times I$ of presheaves has a coproduct $\coprod F$ given by projection to C_0:

$$\coprod F \xrightarrow{\coprod \gamma_0} C_0 \qquad = \qquad F_0 \xrightarrow{\gamma_0} C_0 \times I \xrightarrow{p_0} C_0$$

For any object A the value $\coprod F(A)$ is the disjoint union of the values $F(A, i)$ for $i \in I$. Because $\coprod F = F_0$ as sets, the action $e_F : F_1 \to F_0$ is also the action for $\coprod F$.

3.3. **The Yoneda lemma.** Each object B of a small category $\mathcal{C}$ *represents* a presheaf R_B assigning to each object A of $\mathcal{C}$ the set

$$R_B(A) = \mathrm{Hom}_{\mathcal{C}}(A, B)$$

of all arrows from A to B. Each $\mathcal{C}$ arrow $f : A' \to A$ gives a function

$$R_B(f) : \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{C}}(A', B)$$

defined by composition, so $R_B(f)(g) = gf$.

Formally R_B is the domain function $d_0 : C_1 \to C_0$ restricted to arrows with codomain B, and action by composition with all arrows. The C_0-indexed family of all functors R_B, each indexed by its object B, is the set C_1 with the domain and codomain functions:

$$C_1 \xrightarrow{\langle d_0, d_1 \rangle} C_0 \times C_0$$

Any arrow $h : B \to D$ of $\mathcal{C}$ induces a natural transformation of presheaves in the same direction, defined in the natural way:

$$R_h : R_B \to R_D \qquad R_h(g) = hg \quad \text{for all } g \in R_B$$

This operation is functorial in that $R_h R_k = R_{hk}$ and $R_{(1_B)} = 1_{(R_B)}$.

The simplest *Yoneda lemma* says for any presheaf F on $\mathcal{C}$ and object B of $\mathcal{C}$, natural transformations $R_B \to F$ correspond naturally to the elements of $F(B)$. Mac Lane (1998, p. 59) has a proof suitable for MC. So the representables are *generators*: any two distinct natural transformations of presheaves $\eta \neq \theta : F \to G$ are distinguished by some natural transformation $\nu : R_B \to F$ from a representable.

$$\begin{tikzcd} R_B \arrow[r, "\nu"] & F \arrow[r, shift left, "\eta"] \arrow[r, shift right, "\theta"'] & G \end{tikzcd} \qquad \eta\nu \neq \theta\nu$$

A stronger Yoneda lemma says every presheaf is a colimit of presheaves R_B. The proof by Johnstone (1977, p. 51) works in any elementary topos so it can be read as specifying bounds for a proof in MC.

3.4. **Topologies.** A *Grothendieck topology* J on a small category $\mathcal{C}$ assigns each object A of $\mathcal{C}$ a set of sets of arrows to A called the set of *covers* of A. So it is a C_0-indexed set of sets of arrows subject to familiar conditions all bounded by C_1 and its powerset. Thus there is a set of all topologies on $\mathcal{C}$.

A *J-sheaf* on $\langle \mathcal{C}, J \rangle$ is a presheaf meeting a Δ_0 compatibility condition: for every J-covering family $\{f_i : A_i \to A | i \in I\}$ the value $F(A)$ is an equalizer

$$\begin{tikzcd} F(A) \arrow[r, "\nu"] & \prod_i F(A_i) \arrow[r, shift left, "\eta"] \arrow[r, shift right, "\theta"'] & \prod_{i,j} F(A_i \times_A A_j) \end{tikzcd}$$

So every sheaf is a set.

The usual proofs work in MC to show every presheaf F on a site $\langle \mathcal{C}, J \rangle$ has an *associated sheaf* $\mathbf{a}F$ and natural transformation $i : F \to \mathbf{a}F$ such that every natural transformation $\eta : F \to S$ to a J-sheaf S factors uniquely through this one:

$$\begin{tikzcd} F \arrow[r, "i"] \arrow[dr, "\eta"'] & \mathbf{a}F \arrow[d, "u"] \\ & S \end{tikzcd} \qquad \eta = ui$$

This universal property shows each natural transformation of presheaves $\theta : F \to G$ induces a natural transformation of the J-sheaves $\mathbf{a}\theta : \mathbf{a}F \to \mathbf{a}G$.

3.4.1. *Technical note.* Most textbooks and published proofs make number theoretic sites proper classes. Making them small is not trivial. Grothendieck SGA 4 VII.3.3 uses the comparison lemma, our Theorem 6.1, to show a scheme site can be replaced by a small subsite if it has a refinement by affine maps of finite type.

The issue is not *gros* versus *petit* sites. Those do not differ in set theoretic size but in the geometric "size" of fibers. Fibers may have any dimension in a gros site but are 0-dimensional in a petit site.

A general issue is that publications often use scheme sites local on the fiber so the site is closed under all set-sized disjoint unions $\coprod_i Y_i \to X$, making it a proper class. In practice we can require the maps to be *quasi-compact* so only finite unions arise. See EGA I 6.3.1 or Tamme (1994, p. 90). Without an exhaustive literature survey, I rely on experts saying all sites in use can be handled in such ways.

3.5. **Étale fundamental groups.** A topological space X has *covering spaces* as e.g. a helix covers a circle. The symmetries of a cover of X are like a Galois group, revealing much about X. The *finite étale covers* of a scheme X and the corresponding étale fundamental group give uncannily good analogues to topological covering spaces and include Galois groups as special cases (Grothendieck, 1971).

The theory of finite étale covers is elementary algebra as in EGA IV. We do need a category of all étale covers of a scheme X, and this is not small by the common definition. But the finite étale covers are given by finitely generated extensions of coordinate rings on X. MC proves any set of rings has a set of all finite extensions generated by any fixed set G of generators. So there is a set containing at least one representative (up to isomorphism) of every finite étale cover of X.

3.6. **Injectives and cohomology groups.** Section 1 gave a proof which works in MC that every sheaf of modules M on any small site embeds in an injective, and thus has injective resolutions of any given finite length. More care shows in MC each sheaf has an infinite resolution:

$$M \rightarrowtail I_1 \longrightarrow \ldots \longrightarrow I_i \longrightarrow \ldots$$

The usual construction of a homotopy between any two resolutions of M works in MC to show cohomology groups are unique up to isomorphism.

Further, we can specify a preferred $H^n(E, M)$. Mac Lane and Moerdijk (1992, p. 511) specify a Barr cover for any site by bounded constructions. Given an Abelian group in any topos with natural number object Section 3.6.1 specifies a divisible Abelian group embedding it. Thus we specify embeddings $M \rightarrowtail I$ and groups $H^n(E, M)$. We only use choice in Barr covers to verify their properties.

The usual proofs show cohomology groups are functorial, exact, and effaceable. They give all the usual exact sequences. Standard results on Čech cohomology and spectral sequences Also follow. These would suffice for published applications in number theory with routine re-working to remove large-structure apparatus. But we can formalize the large-structure apparatus at the same logical strength.

3.6.1. *Injective resolutions in MC.* MC proves every module or sheaf of modules has an infinite injective resolution by fixing set bounds on the construction.

For any ordinary ring R and R-module M specify an embedding in two steps:

(1) For F the free Abelian group on the set of elements of M, use the free presentation of M and tensor with $\mathbb{Q}$ to embed M in a divisible group M_d.

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r] \arrow[d, "="'] & F \arrow[r] \arrow[d, tail] & M \arrow[r] \arrow[d, tail] & 0 \\
0 \arrow[r] & K \arrow[r] & F \otimes_{\mathbb{Z}} \mathbb{Q} \arrow[r] & M_d \arrow[r] & 0
\end{tikzcd}$$

The middle vertical is monic since F is free. Since the lefthand vertical is an isomorphism the righthand one is monic.

(2) The R-module $I_0 = Hom_{\mathbb{Z}}(R, M_d)$ of additive functions $R \to M_d$ is injective by Lemma 1.1, with monic homomorphism $M \rightarrowtail Hom_{\mathbb{Z}}(R, M_d)$ taking each $m \in M$ to the function $r \mapsto r \cdot m$.

Next we want an injective embedding of the quotient $I_0/M \rightarrowtail I_1$. Skip step 1 since injective modules and their quotients are already divisible groups. Step 2 forms $I_1 = Hom_{\mathbb{Z}}(R, I_0/M)$. Repeat this for all following I_i.

Theorem 3.1. *For any R-module M in sets, take the set $R^{\mathbb{N}}$ of infinite sequences in R and define S_n as the set of all partial functions $R^{\mathbb{N}} \rightharpoonup M_d$ which are defined for all and only those sequences $s \in R^{\mathbb{N}}$ with $s(i) = 0$ for all $i > n$. For each $i \in \mathbb{N}$ there is a subset $J_i \subseteq S_i$ and an equivalence relation $E_i \subseteq J_i \times J_i$ such that the quotients $I_i = J_i/E_i$ are R-modules giving an infinite injective resolution of M.*

$$M \rightarrowtail I_0 \longrightarrow \cdots \longrightarrow I_n \longrightarrow \cdots$$

Proof. Up to isomorphism S_n is the set of all functions from R^{n+1} to M_d. The subset of addition-preserving functions in S_0 is the module $I_0 = Hom_{\mathbb{Z}}(R, M_d)$ of step 2. That subset is our J_0 with its identity relation as E_0.

Assume the result holds as far as S_n. Since S_{n+1} is up to isomorphism the set of all functions $R \to S_n$, let J_{n+1} be the subset of those mapping R into J_n and additive up to the equivalence relation E_n, i.e. those inducing Abelian group homomorphisms $R \to I_n$. Let E_{n+1} relate all those inducing the same homomorphism $R \to I_n$. Step 2 shows the R-module $I_{i+1} = S_{i+1}/E_{i+1}$ extends the resolution to

$$M \rightarrowtail I_0 \longrightarrow \cdots \longrightarrow I_n \longrightarrow I_{n+1}$$

This construction is bounded by the set of partial functions $R^{\mathbb{N}} \rightharpoonup M_d$ plus a few of its powersets to define the module structures on the sets I_i and the morphisms $I_i \to I_{i+1}$. These bounds prove the infinite injective resolution is a set in MC. □

Theorem 3.2. *For any sheaf of rings R on any site, every sheaf of R-modules M has an infinite injective sheaf resolution.*

$$M \rightarrowtail I_0 \longrightarrow \cdots \longrightarrow I_n \longrightarrow \cdots$$

Proof. The proof of Theorem 3.1 holds over any site whose sheaves satisfy choice, including any Barr cover of $\langle \mathcal{C}, J \rangle$. The following lemma shows the direct image functor of the cover is exact on modules. We can pull M back to the cover, find an infinite resolution there, and push the whole down to a resolution over $\langle \mathcal{C}, J \rangle$. □

Lemma 3.3. *For any elementary topos $\mathcal{E}$ and geometric morphism $f^* \dashv f_* : \mathcal{B} \to \mathcal{E}$ where $\mathcal{B}$ satisfies axiom of choice, the direct image f_* preserves module quotients.*

Proof. In the choice topos $\mathcal{B}$ every quotient homomorphism $q : M \twoheadrightarrow M/J$ has a right inverse function $M/J \to M$ (generally not a homomorphism), so $f_*(q)$ also does. So $f_*(q)$ is onto and thus is a quotient. □

4. Classes and collections: Mac Lane type theory

Take the sets of MC as one type and add classes of sets as a higher type and collections of classes as another. We indicate sets by italics x, A, classes by calligraphic $\mathcal{A}, \mathcal{B}$, and collections by fraktur $\mathfrak{A}, \mathfrak{B}$. As above, $x \in B$ or $A \in B$ say a set x or A is in set B. Use $A \in_1 \mathcal{A}$ to say set A is in class $\mathcal{A}$, and $\mathcal{A} \in_2 \mathfrak{B}$ to say class $\mathcal{A}$ is in collection $\mathfrak{B}$. The MC axioms for sets plus the higher type axioms and inference rules below give *Mac Lane Type Theory* (MTT), a conservative extension of MC. Adding all finite types above MC would still be a conservative extension, as Takeuti (1978, pp. 77f.) shows for Peano Arithmetic. But we do not need that.

So MTT has the same proof theoretic strength as MC, the strength of finite order arithmetic. Indeed as a conservative extension MTT proves nothing in the language of MC that is not already provable in MC. It can, and does, allow levels of organization inexpressible in MC.

A *set theoretic fomula* is a formula which may include variables over classes and collections but has quantifiers only over sets. So class inclusion is set theoretic:

$$\mathcal{A} \subseteq \mathcal{B} \;\leftrightarrow\; \forall x\,(x \in_1 \mathcal{A} \rightarrow x \in_1 \mathcal{B})$$

Inclusion of collections is well defined, expressed by a formula of MTT

$$\mathfrak{A} \subseteq \mathfrak{B} \;\leftrightarrow\; \forall \mathcal{X}\,(\mathcal{X} \in_2 \mathfrak{A} \rightarrow \mathcal{X} \in_2 \mathfrak{B})$$

But it is not a *set theoretic* formula as it quantifies over classes $\mathcal{X}$.

The key device is *set theoretic abstracts* by which set theoretic formulas define classes and collections. For any set theoretic formula $\Psi(X)$ with variable X of set type, $\{X|\Psi(X)\}$ is a class abstract indicating the class of all sets with property Ψ.

For example a function between classes $\mathcal{F}\colon\mathcal{A}\rightarrow\mathcal{B}$ is naturally a class of ordered pairs of sets taken from $\mathcal{A}$ and $\mathcal{B}$. The cartesian product of classes $\mathcal{A}\times\mathcal{B}$ is a class of ordered pairs of sets. And so for any classes $\mathcal{A},\mathcal{B}$ an abstract describes the collection $\mathcal{B}^{\mathcal{A}}$ of all functions $\mathcal{F}\colon\mathcal{A}\rightarrow\mathcal{B}$. The natural definition is set theoretic:

$$\mathcal{B}^{\mathcal{A}} = \{\mathcal{F} \mid \mathcal{F} \subset \mathcal{A}\times\mathcal{B} \;\&\; (\forall A \in_1 \mathcal{A})(\exists! B \in_1 \mathcal{B})\ \langle A, B\rangle \in_1 \mathcal{F}\}$$

Another example is the abstract for the class of all small categories:

$$\{\langle C_0, C_1, d_0, d_1, m\rangle|\ Cat(C_0, C_1, , d_0, d_1, m)\}$$

Here Cat is a formula saying d_0, d_1 are functions between the sets $C_1 \rightarrow C_0$ and m is a partially defined function $C_1 \times C_1 \rightarrow C_1$ fulfilling the category axioms.

A 5-tuple of sets $\langle C_0, C_1, d_0, d_1, m\rangle$ is a set. But we also want a collection of all class-sized categories while a 5-tuple of classes is not naturally a class. So we take n-tuples of classes as primitive. There is an abstract

$$\{\langle \mathcal{C}_0, \mathcal{C}_1, \mathcal{D}_0, \mathcal{D}_1, \mathcal{M}\rangle|\ Cat(\mathcal{C}_0, \mathcal{C}_1, \mathcal{D}_0, \mathcal{D}_1, \mathcal{M}))\}$$

saying the classes $\mathcal{C}_0, \mathcal{C}_1, \mathcal{D}_0, \mathcal{D}_1, \mathcal{M}$ fulfill the category axioms. It indicates the 5-tuple collection of all class categories.

We adapt rules from Takeuti (1978, p. 77–80). Our basic types are *Set*, *Class* (of sets), and *Collection* (of classes). For any types τ_1, τ_2 there is a product type $\tau_1 \times \tau_2$. Abstracts are as defined here:

6. If $\Psi(v_1, \ldots, v_n)$ is a set theoretic formula with variables $v_1, \ldots, v_n$ of types $\tau_1, \ldots, \tau_n$ then
$$\{\langle v_1, \ldots, v_n\rangle|\Psi(v_1, \ldots, v_n)\}$$
is an abstract of type $\tau_1\times\ldots\times\tau_n$. The indicated variables need not actually occur in Ψ, and other free variables of any type may occur.

6′. Given abstracts $A_1, \ldots, A_n$ of types $\tau_1, \ldots, \tau_n$ respectively, and abstract $\{\langle v_1, \ldots, v_n\rangle|\Psi(v_1, \ldots, v_n)\}$ with variables of the same types, the expression $\langle A_1, \ldots, A_n\rangle \in \{\langle v_1, \ldots, v_n\rangle|\Psi(v_1, \ldots, v_n)\}$ is equivalent to $\Psi(A_1, \ldots, A_n)$.

7. If α is a free variable of type $\tau_1 \times \ldots \times \tau_n$ and $A_1, \ldots, A_n$ are abstracts of types $\tau_1, \ldots, \tau_n$ then $\langle A_1, \ldots, A_n \rangle \in \alpha$ is a formula.

As quantifier rules:

$$\forall \alpha \Psi(\alpha) \text{ implies } \Psi(A)$$

for any formula $\Psi(\alpha)$ and abstract A of the same type as variable α. And given any proof of $\Psi(\alpha)$, with variable α not in any assumption, conclude $\forall \alpha \Psi(\alpha)$. Define $\exists \alpha \Psi(\alpha)$ as $\neg \forall \alpha \neg \Psi(\alpha)$. This gives class and collection comprehension: For each arithmetical formula $\Psi(v)$ with variable v of set or class type, the equivalence

$$\Psi(v) \leftrightarrow v \in_i \{v | \Psi(v)\} \quad \text{implies} \quad \exists \psi \forall v (\Psi(v) \leftrightarrow v \in_i \psi) \quad \text{for } i = 1, 2$$

The identity axiom connects classes to sets:

$$\forall \mathcal{A} \forall x \forall y \, (\, (x = y \,\&\, x \in_1 \mathcal{A}) \rightarrow y \in_1 \mathcal{A} \,)$$

A class $\mathcal{A}$ might be a set in the sense of having the same elements as some set

$$\exists A \forall x (x \in A \leftrightarrow x \in_1 \mathcal{A})$$

We express this set theoretic formula informally by saying $\mathcal{A}$ is small or is a set. The set A is uniquely determined and we can work with $\mathcal{A}$ by working with A,

MTT has no identity relation for classes or collections. This follows Takeuti (1978) where the absence of higher-type identity facilitates the conservative extension proof. And it suits categorical practice where large-structure categories like toposes are often defined up to equivalence rather than on-the-nose.

5. Category theory in MTT

The class $\mathcal{U}$ of all sets serves as *universe*. With the class of all functions between sets it provides a class category $\mathcal{SET}$. A $\mathcal{U}$-category, also called a *locally small category* is a category with a class of objects and and a class of arrows such that every set of objects has a set of all arrows between them. In the absence of replacement this is stronger than requiring every pair of objects A, B have a set of all arrows $Hom_{\mathcal{C}}(A, B) \in \mathcal{U}$.[1] Obviously $\mathcal{SET}$ is a $\mathcal{U}$-category.

There is a class category $\mathcal{CAT}$ of all small categories using the abstract in Section 4 for the class $\mathcal{CAT}_0$ of all small categories. Analoguous abstracts give the class $\mathcal{CAT}_1$ of all small functors and the class graphs of the domain, codomain, and composition functions. Section 3.1 shows it is locally small.

A class category is a 5-tuple of classes $\langle \mathcal{C}_0, \mathcal{C}_1, \mathcal{D}_0, \mathcal{D}_1, \mathcal{M} \rangle$ satisfying the axioms. Elements of $\mathcal{C}_0$ and $\mathcal{C}_1$ are sets so the axioms are set theoretic and there is a collection category $\mathfrak{CAT}$ of all class categories. The abstract in Section 4 gives the collection $\mathfrak{CAT}_0$ of all class categories. Similar ones work for all functors, and so on.

5.1. **Sheaf and presheaf toposes.** Section 3.2 proved the category of presheaves on a small category $\mathcal{C}$ is locally small. Call that category of presheaves $\widehat{\mathcal{C}}$. It is indicated by a 5-tuple of classes:

$$\{ \langle \mathcal{F}_{\mathcal{C}0}, \mathcal{F}_{\mathcal{C}1}, \mathcal{D}_0, \mathcal{D}_1, \mathcal{M} \rangle | \begin{cases} F \in_1 \mathcal{F}_{\mathcal{C}0} \text{ iff } F \text{ is a presheaf on } \mathcal{C} \\ \eta \in_1 \mathcal{F}_{\mathcal{C}1} \text{ iff } \eta \text{ is a presheaf transform on } \mathcal{C} \\ \text{etc.} \end{cases} \quad \}$$

[1] Grothendieck and Verdier (1972, p. 5) reject this definition because presheaf categories should be $\mathcal{U}$-categories while their definition at the time made presheaves too big to be in $\mathcal{U}$. Our Section 3.2 uses the later *Grothendieck construction* so presheaves are indexed sets.

All these formulas are set theoretic as in MC. Here $\mathcal{C}$ abbreviates a 5-tuple $\langle C_0, C_1, d_0, d_1, m\rangle$ of free variables of set type and conditions saying they form a small category, so the abstract indicates a variable presheaf category $\widehat{\mathcal{C}}$ depending on $\mathcal{C}$. We can also abstract over all these variables at once to form

$$\{\langle C_0, C_1, d_0, d_1, m, \mathcal{F}_{\mathcal{C}0}, \mathcal{F}_{\mathcal{C}1}, \mathcal{D}_0, \mathcal{D}_1, \mathcal{M}\ \rangle \mid \\ \langle \mathcal{F}_{\mathcal{C}0}, \mathcal{F}_{\mathcal{C}1}, \mathcal{D}_0, \mathcal{D}_1, \mathcal{M}\rangle \text{ is the presheaf category on } \langle C_0, C_1, d_0, d_1, m\rangle\}$$

indicating the class of all pairs of a small category $\mathcal{C}$ and its presheaf category $\widehat{\mathcal{C}}$.

In MTT, for each small category $\mathcal{C}$, the Yoneda operation $R_{(\_)}$ is an actual functor $R_{(\_)}\colon \mathcal{C} \to \widehat{\mathcal{C}}$ called the *Yoneda embedding*. Compare Section 3.3. We use the obvious definition of a functor from a small category to a class category.

For any small site $\langle \mathcal{C}, J\rangle$ MTT provides a category of sheaves called $\widetilde{\mathcal{C}}_J$. As a full subcategory of a presheaf category it is locally small. The definition of the associated sheaf $i\colon F \to \mathbf{a}F$ in Section 3.4 says sheafification $\mathbf{a}\colon \widehat{\mathcal{C}} \to \widetilde{\mathcal{C}}_J$ is left adjoint to the inclusion $\widetilde{\mathcal{C}}_J \rightarrowtail \widehat{\mathcal{C}}$. Proofs in SGA 4 II and (Mac Lane and Moerdijk, 1992, pp. 227ff.) work in MC and show sheafification preserves finite limits.

A Grothendieck topos in MTT is any class category equivalent to $\widetilde{\mathcal{C}}_J$ for some small site. It is locally small since equivalence preserves the size of arrow sets.

Theorem 5.1. *Every theorem of elementary topos theory holds for class Grothendieck toposes in MTT. See (Johnstone, 1977).*

Proof. The elementary topos axioms are easily verified as they involve only bounded constructions on objects and arrows. In any class category these are sets. Proofs in the elementary theory quantify only over objects and arrows of the toposes. $\square$

5.2. **Cohomology in MTT.** A sheaf of modules over a sheaf of rings on any small site $\langle \mathcal{C}, J\rangle$ is just a module M on a ring R in the sheaf topos $\widetilde{\mathcal{C}}_J$. All commutative algebra that does not use excluded middle or the axiom of choice holds in every Grothendieck topos by Thm. 5.1.

For any ring R in any sheaf topos $\widetilde{\mathcal{C}}_J$, MTT gives a $\mathcal{U}$-category $\mathcal{MOD}_R$ of all R-modules. The usual constructions of biproducts, kernels, and cokernels are bounded so they work in MC, so they show in MTT that $\mathcal{MOD}_R$ is an Abelian category.

Section 3.6 defined cohomology groups $H^n(E, M)$ in MC. In MTT we define cohomology functors $H^n\colon \mathcal{MOD}_R \to \mathcal{AB}$ from sheaves of modules to ordinary Abelian groups. The construction in Section 3.6 was explicit (not using choice) and set theoretic so MTT can express it by a class abstract.

MTT can give the usual definition of a universal δ-functor (Hartshorne, 1977, p. 204). Every left exact functor $F\colon \mathcal{MOD}_R \to \mathcal{AB}$ has *right derived functors*

$$F \cong R^0F,\ R^1F,\ \ldots,\ R^nF,\ \ldots$$

defined up to isomorphism either as a universal δ-functor over F, or as an effaceable δ-functor over F. See (Grothendieck, 1957a, p. 141).

The cohomology functors $H^i, i \le n$ are derived functors of the global section functor $\Gamma\colon \mathcal{MOD}_R \to \mathcal{AB}$ which takes each module to its group of global sections.

6. Large-structure tools

6.1. **Geometric morphisms.** A *geometric morphism* of toposes is an adjoint pair of functors $f^* \dashv f_*\colon \mathcal{E} \to \mathcal{E}'$ where the left adjoint $f^*\colon \mathcal{E}' \to \mathcal{E}$ is also left exact. Then

$f_*:\mathcal{E}\to\mathcal{E}'$ is called the *direct image* functor, and f^* the *inverse image* functor. The standard, published theory of geometric morphisms among Grothendieck toposes largely applies. The objects and arrows of any Grothendieck topos are sets, and most standard constructions are all bounded. For example, each Grothendieck topos $\mathcal{E}$ has a geometric morphism $\Delta\dashv\Gamma:\mathcal{E}\to\mathcal{SET}$ with the *global section functor* Γ taking each object $A\in\mathcal{E}$ to the set of arrows $1\to A$. The usual argument shows this is up to equivalence the only geometric morphism from $\mathcal{E}$ to $\mathcal{SET}$.

For other examples, MC proves any continuous function $f: X\to X'$ between topological spaces induces suitable operations on sheaves and their transforms on those spaces. So MTT proves f induces a geometric morphism $f^*, f_*: Top(X)\to Top(X')$ between the sheaf toposes, and given suitable separation conditions on the spaces every geometric morphism arises from a unique continuous function Mac Lane and Moerdijk (1992, p. 348).

Grothendieck toposes are defined in MTT but the definition quantifies over functors of class type, saying a category is a Grothendieck topos if there exists a functor equivalence beween it and some sheaf topos. So MTT cannot prove there is a collection of all Grothendieck toposes. It can prove there is a collection $\mathfrak{Top}_0$ of all sheaf toposes, and thus all Grothendieck toposes up to equivalence. This has abstract

$$\{\langle\mathcal{S}_0,\mathcal{S}_1,d_0,d_1,m\rangle|\ \exists\text{ a small site }\langle\mathcal{C},J\rangle\ \begin{cases} X\in_1\mathcal{S}_0\leftrightarrow X\text{ is a sheaf on }\langle\mathcal{C},J\rangle\\ f\in_1\mathcal{S}_1\leftrightarrow f\text{ is a sheaf transform}\\ \textit{etc.}\end{cases}\}$$

Similar abstracts give a collection $\mathfrak{Top}_1$ of all geometric morphisms between sheaf toposes, and a collection of all natural transformations between these morphisms. These form a 2-category $\mathfrak{Top}$ of Grothendieck toposes. Cf. (Johnstone, 1977, p. 26).

The standard theorems on $\mathfrak{Top}$ follow in MTT. They make elementary use of classes, and work seriously with sheaves, transforms, and other sets.

6.2. **Sites.** A presheaf on a $\mathcal{U}$-category $\mathcal{C}$ is a $\mathcal{C}_0$ indexed class $\gamma_0: F_0\to C_0$ with action $e_{\mathcal{F}}$ analogously to Section 3.2. A $\mathcal{U}$-preasheaf or *locally small presheaf* on $\mathcal{C}$ is a presheaf whose values are all sets, that is such that the restriction to any small subcategory $\mathcal{C}'\subseteq\mathcal{C}$ is small.

A $\mathcal{U}$-site, or *locally small site* $\langle\mathcal{C},J\rangle$, is a site with locally small $\mathcal{C}$. A $\mathcal{U}$-sheaf is a locally small presheaf with the sheaf property. Local smallness only quantifies over sets: every set of objects in a class categoryhas a set of values. So MTT can invoke local smallness in abstracts. thus every $\mathcal{U}$-site $\langle\mathcal{C},J\rangle$ has a class category $\widetilde{\mathcal{C}}_J$ of all $\mathcal{U}$-sheaves. A *class topos* is any class category equivalent to $\widetilde{\mathcal{C}}_J$ for some $\mathcal{U}$-site. For suitably bounded U-sites, these are Grothendieck toposes:

Theorem 6.1 (Comparison lemma)**.** *Let U-site $\langle\mathcal{C}',J'\rangle$ have a full and faithful functor $u:\mathcal{C}\to\mathcal{C}'$ from a small category $\mathcal{C}$ where every object of $\mathcal{C}'$ has at least one J'-cover by objects $u(A)$ for objects A of $\mathcal{C}$. Then J' induces a topology J on $\mathcal{C}$ making $\widetilde{\mathcal{C}}_J$ and $\widetilde{\mathcal{C}}'_{J'}$ equivalent categories.*

Proof. This is case i)⇒ii) of SGA 4 III.4.1 (p. 288). Verdier's small categories are sets for us, as are his functors $u_!, u^*, u_*$. The constructions are bounded. The proof by Mac Lane and Moerdijk (1992, p. 588) also adapts to MTT. □

Corollary 6.2. *Any U-category $\mathcal{E}$ with a set of generators $\{G_i|i\in I\}\in U$ and with every U-sheaf for the canonical topology representable, is a Grothendieck topos.*

Proof. See the canonical topology in any topos theory text. The representability assumption says $\mathcal{E}$ is equivalent to the category of canonical U-sheaves. Apply the theorem to $\mathcal{C}' = \mathcal{E}$ and $\mathcal{C}$ the full subcategory of objects in G. □

Theorem 6.3. *For any small site $\langle \mathcal{C}, J\rangle$ the sheaf topos $\widetilde{\mathcal{C}}_J$ has:*

a) *a limit for every finite diagram.*
b) *a coproduct for each set of sheaves, and these are stable disjoint unions.*
c) *a stable quotient for every equivalence relation.*
d) *a set $\{G_i | i \in I\}$ of generators.*

Proof. Section 3.2 proved most of this for presheaf categories. The sheaf case follows from sheafification described in Section 3.4. See SGA 4 II.4 (p. 235) and SGA 4 IV.1.1.2 (p. 302); or see Mac Lane and Moerdijk (1992, pp. 24ff.). □

In fact $\widetilde{\mathcal{C}}_J$ has limits for every small diagram, but Theorem 6.4 below refers to this list as given. The list amounts to saying $\widetilde{\mathcal{C}}$ is an elementary topos with small coproducts and a small generator (Mac Lane and Moerdijk, 1992, pp. 591).

Theorem 6.4 (Giraud theorem)**.** *Any U-category $\mathcal{E}$ with the properties listed in Theorem 6.3 is a Grothendieck topos.*

Proof. The proof by Mac Lane and Moerdijk (1992, pp. 578ff.) is easily cast in MTT. As they do, define $\mathcal{C}$ to be the full subcategory of $\mathcal{E}$ on the set of generators. It is small since $\mathcal{E}$ is locally small. Take their functors $(\mathrm{Hom}_{\mathcal{E}}) \dashv (\_ \otimes_{\mathcal{C}} A) \colon \mathcal{SET}^{\mathcal{C}^{op}} \to \mathcal{E}$ as class functors between class categories. □

Corollary 6.5. *Every Grothendieck topos is equivalent to some sheaf topos on a subcanonical site with all finite limits.*

Proof. After Mac Lane and Moerdijk (1992, pp. 578ff.), it remains to prove in MTT that every small category $\mathcal{C}$ has a small full subcategory $\mathcal{C}' \subseteq \widehat{\mathcal{C}}$ of presheaves containing the representables and closed under finite limits. Since $\widehat{\mathcal{C}}$ is locally small it suffices to find a set of presheaves including the representables and closed under finite limits. Limits of presheaves are computed pointwise (Mac Lane, 1998, p. 116), and a product of equalizers is an equalizer. So we must show for each set of sets there is a set of all finite products of those sets, which follows if we know for each single set A there is a set of all finite powers A^n. To prove that, code an n-tuple of elements of A as a partial function $\mathbb{N} \to A$ defined for $0 \leq i < n$. □

SGA 4 often invokes successive universes $U \in V$ where our weak logic of classes and collections suffices with some care. See e.g. SGA 4 IV.1.2 on the Giraud theorem, and SGA 4 IV.10 on multilinear algebra in toposes.

6.3. Duality and derived categories.

> The chief ideas of [Grothendieck duality] were known to me since 1959, but the lack of adequate foundations for homological algebra prevented me attempting a comprehensive revision. This gap in foundations is about to be filled by Verdier's dissertation, making a satisfactory presentation possible in principle. (Grothendieck quoted by Hartshorne, 1966, p. III)

Grothendieck (1957b) finds his duality theorem too limited. It was essentially as in Altman and Kleiman (1970): certain cohomology groups (and related groups) of nonsingular projective schemes are isomorphic in a natural way. The proof invokes proper class categories but really only quantifies over sheaves and modules. It can be given in MC. Wiles (1995, p. 486) calls it "explicit duality over fields."

Grothendieck (1958, pp. 112–15) explains why duality can and should reach farther. By 1959 he believed the most unified and general tool is *derived categories*, now standard for Grothendieck duality. "Miraculously, the same formalism applies in étale cohomology, with quite different proofs" (Deligne, 1998, p. 17). Delignes uses them for étale Poincaré duality in SGA 4 XVII, XVIII and (Deligne, 1977).

Cohomology takes a module M on a scheme X and deletes nearly all its structure, highlighting just a little of it in the groups $H^n(X, M)$. The *derived category* $D(X)$ of modules on X deletes much of the same information but not all. Some manipulations work at this level which are obscured by excess detail at the level of modules and are impossible for lack of detail at the level of cohomology.

Notably, a scheme map $f : X \to Y$ sets up complicated relations between cohomology over X and Y. The successive effect on cohomology of f and a further $g : Y \to Z$ is not fully determined by the separate effects of f and g (those determine it only up to a spectral sequence). Yet a functor $Rf_* : D(X) \to D(Y)$ between derived categories approximates the effect of f on cohomology so that the approximation of successive effects is (up to isomorphism) the composite of the approximations:

$$\begin{tikzcd} & Y \arrow[dr, "g"] & \\ X \arrow[ur, "f"] \arrow[rr, "gf"'] & & Z \end{tikzcd} \qquad \begin{tikzcd} & D(Y) \arrow[dr, "Rg_*"] & \\ D(X) \arrow[ur, "Rf_*"] \arrow[rr, "R(gf)_* \cong\ Rg_* Rf_*"'] & & DZ) \end{tikzcd}$$

All variants of Grothendieck duality being developed today say the functor Rf_* has a right adjoint $Rf^! : D(Y) \to D(X)$, with some further properties under some conditions on f. The adjunction contains very much information.

The set theoretic issue is to form certain *categories of fractions*. In any small or class category $\mathcal{C}$ each suitable class Σ of arrows has a category of fractions $\mathcal{C}[\Sigma^{-1}]$ inverting each arrow in Σ. It has the same objects, while an arrow $A \to B$ in $\mathcal{C}[\Sigma^{-1}]$ is represented by a pair of arrows in $\mathcal{C}$:

$$A \xleftarrow{\ s\ } C \xrightarrow{\quad f \quad} B \qquad\qquad s \in \Sigma$$

We define an equivalence relation on these pairs, and a composition rule so a pair $\langle s, f\rangle$ acts like a composite $fs^{-1} : A \to B$ even if s has no inverse in $\mathcal{C}$.

The derived category $D(X)$ starts with the category $\mathcal{K}(X)$ whose objects are complexes of quasi-coherent sheaves of modules over a scheme X

$$\cdots \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow M_{i+1} \longrightarrow M_{i+2} \longrightarrow \cdots$$

and arrows are *homotopy classes* of maps between complexes. Quasi-coherent sheaves are those closest to the geometry of a scheme, but this sets no bound on cardinality and does not affect the set theory involved. Complexes and homotopy classes are sets, provably existing in MC. The derived category $D(X)$ is a certain calculus of fractions on $\mathcal{K}(X)$ (Eisenbud, 1995, pp. 678ff.).

Weibel (1994, p. 386) shows how to cut the equivalence classes of fractions down to sets for many cases of interest including modules on schemes. But he uses countable replacement (so that sequences of cardinals have suprema). This is far stronger than ZC as it implies existence of uncountably many ZC universes. By using MTT instead we avoid all replacement and use no special facts about schemes.

Here the class category $\mathcal{C}$ is the category of complexes and maps of complexes, and Σ is the class of *quasi-isomorphisms* meaning those maps of complexes which induce isomorphisms in all degrees of cohomology. For fixed A, B the relevant pairs

$$A \xleftarrow{s} C \xrightarrow{\quad f \quad} B \qquad\qquad s \in \Sigma$$

are those with s any quasi-isomorphic. Even a single equivalence class in $\mathcal{C}[\Sigma^{-1}]$ will involve a proper class of pairs with different complexes C. The collection $D(X)_1$ of arrows of the derived category $D(X)$ is the collection of these equivalence classes, while there is a class of objects namely the class $D(X)_0 = \mathcal{K}(X)_0$ of complexes.

The key point conceptually and for MTT is that the definition of $D(X)_1$ depends on (infinitely many) complexes of modules making (infinitely many) finite diagrams commute. It is expressed by a set theoretic abstract. The graphs of domain, codomain, and composition are similar. MTT proves there is a derived category $D(X)$, with a class of objects and collection of arrows.

So current work on Grothendieck duality is formalizable in MTT. For lively debate over mathematical strategies (not foundations) see Conrad (2000, preface), Lipman in (Lipman and Hashimoto, 2009, pp. 7–9), and Neeman (2010, pp. 294–300). Hartshorne (1966, pp. 1–13) notes many issues, describes an "ideal form" of the theorem, and among other ideas offers: "Perhaps some day this type of construction will be done more elegantly using the language of fibred categories and results of Giraud's thesis" (p. 16).

6.4. **Fibred categories.** Universes first appeared in print in SGA 1 VI on fibred categories. They are a way to treat a class or category of categories as a single category. So SGA 4 VI calculates limits of families of Grothendieck toposes by using fibred toposes. In much of SGA 4 fibred toposes are presented by fibred sites. The logical issues are essentially the same as in Section 6.2 above. Many applications can be cast in MC by talking about sites, while the general facts are clearer and more concise in MTT explicitly quantifying over toposes and fibred families of them. The latter requires no stronger logical foundation than the former, only a foundation that can talk about classes satisfying very weak axioms. Currently fibred categories occur in the literature more as a research topic than a tool.

7. A proof of FLT in PA?

We have given foundations for cohomology rather than for individual arithmetic theorems. For example we use the axiom of choice to provide cohomology groups though it is eliminable from the proof of any arithmetic theorem. MC suffices for the existing applications. MTT founds the whole SGA for arbitrary sites, meaning any small site existing in the set theory MC.

Number theory, of course, does not use arbitrary sites or unbounded degrees of cohomology. It uses relatively low degree cohomology of very small sites close to arithmetic. By detailed attention to cardinal bounds we can expect to found arithmetic cohomology on n-order arithmetic for relatively low n which depends on the site and on the highest degree of cohomology needed. The promising approach is to use ZFC- which is Zermelo Fraenkel with choice (and replacement) but without the powerset axiom. That theory, plus the assumption of n successive powersets of the set of natural numbers, is equivalent to n-th order arithmetic.

If that works it might be a good context for hard analysis of individual proofs as Macintyre (2011) begins for (Wiles, 1995) on FLT. Starting in ZFC-, detailed numerical estimates might bound each use of induction and comprehension within a conservative n-th order extension of PA as in (Takeuti, 1978). This would show FLT is provable in PA by essentially the existing proof, and might help further reduce it to Exponential Function Arithmetic (EFA) as in (Friedman, 2010). In any context, the estimates will be difficult. This is no end run around hard arithmetic.

Not motivated by concern with logic, Kisin (2009b) extends and simplifies (Wiles, 1995), generally using geometry less than commutative algebra, visibly reducing the demands on set theory. And Kisin (2009a) completes a different proof of FLT by a strategy of Serre advanced by Khare and Wintenberger.

Acknowledgments

It is a pleasure to thank people who contributed ideas to this work, which does not mean any of them shares any given viewpoint here. I thank especially Jeremy Avigad, Steve Awodey, John Baldwin, Brian Conrad, Pierre Deligne, Adam Epstein, Thomas Forster, Harvey Friedman, Sy David Friedman, Steve Gubkin, Michael Harris, Wiliam Lawvere, Angus Macintyre, Barry Mazur, Michael Shulman, Jean-Pierre Serre, and Robert Solovay.

References

The abbreviation SGA 1 refers to Grothendieck (1971) and SGA 4 is Artin et al. (1972). EGA I and IV are respectively Grothendieck and Dieudonné (1971) and Grothendieck and Dieudonné (1964).

Altman, A. and Kleiman, S. (1970). *An Introduction to Grothendieck Duality Theory.* Springer Lecture Notes in Mathematics no. 146. Springer-Verlag, New York.

Artin, M., Grothendieck, A., and Verdier, J.-L. (1964). *Cohomologie Etale des Schémas*, volume 1 of *Séminaire de géométrie algébrique 1963–64.* Institut des Hautes Études Scientifiques. Mimeographed reports of the seminar later published in greatly expanded form as SGA 4.

Artin, M., Grothendieck, A., and Verdier, J.-L. (1972). *Théorie des Topos et Cohomologie Etale des Schémas.* Séminaire de géométrie algébrique du Bois-Marie, 4. Springer-Verlag. Three volumes, cited as SGA 4.

Baer, R. (1940). Abelian groups that are direct summands of every containing abelian group. *Bulletin of the American Mathematical Society*, 46:800–06.

Barr, M. (1974). Toposes without points. *Journal of Pure and Applied Algebra*, 5:265–80.

Blass, A. (1979). Injectivity, projectivity, and the axiom of choice. *Transactions of the American Mathematical Society*, 255:31–59.

Conrad, B. (2000). *Grothendieck duality and base charge.* Number 1750 in Lecture Notes in Mathematics. Springer-Verlag, New York.

Deligne, P. (1977). Cohomologie étale: les points de départ. In Deligne, P., editor, *Cohomologie Étale*, pages 4–75. Springer-Verlag.

Deligne, P. (1998). Quelques idées maîtresses de l'œuvre de A. Grothendieck. In *Matériaux pour l'Histoire des Mathématiques au XX^e Siècle (Nice, 1996)*, pages 11–19. Soc. Math. France.

Eckmann, B. and Schopf, A. (1953). über injektive Moduln. *Archiv der Mathematik*, 4(2):75–78.

Eisenbud, D. (1995). *Commutative Algebra*. Springer-Verlag.

Friedman, H. (2010). Concrete mathematical incompleteness. On-line at www.math.ohio-state.edu/ friedman/. Lecture at University of Cambridge, UK.

Grothendieck, A. (1957a). Sur quelques points d'algèbre homologique. *Tôhoku Mathematical Journal*, 9:119–221.

Grothendieck, A. (1957b). Théorèmes de dualité pour les faisceaux algébriques cohérents, exposé 149. In *Séminaire Bourbaki*. Secrétariat mathématique, Université Paris, Paris.

Grothendieck, A. (1958). The cohomology theory of abstract algebraic varieties. In *Proceedings of the International Congress of Mathematicians, 1958*, pages 103–18. Cambridge University Press.

Grothendieck, A. (1971). *Revêtements Étales et Groupe Fondamental*. Séminaire de géométrie algébrique du Bois-Marie, 1. Springer-Verlag. Cited as SGA 1.

Grothendieck, A. (1985–87). *Récoltes et Semailles*. Université des Sciences et Techniques du Languedoc, Montpellier. Published in several successive volumes.

Grothendieck, A. and Dieudonné, J. (1964). *Éléments de Géométrie Algébrique IV: Étude locale des schémas et des morphismes de schémas, Première partie*. Number 20 in Publications Mathématiques. Institut des Hautes Études Scientifiques, Paris.

Grothendieck, A. and Dieudonné, J. (1971). *Éléments de Géométrie Algébrique I*. Springer-Verlag.

Grothendieck, A. and Verdier, J.-L. (1972). Préfaisceaux. In Artin, M., Grothendieck, A., and Verdier, J.-L., editors, *Théorie des Topos et Cohomologie Etale des Schémas*, volume 1 of *Séminaire de géométrie algébrique du Bois-Marie, 4*, pages 1–218. Springer-Verlag.

Hartshorne, R. (1966). *Residues and Duality, Lecture Notes of a Seminar on the Work of A. Grothendieck given at Harvard 1963–64*. Number 20 in Lecture Notes in Mathematics. Springer-Verlag, New York.

Hartshorne, R. (1977). *Algebraic Geometry*. Springer-Verlag.

Johnstone, P. (1977). *Topos Theory*. Academic Press.

Kisin, M. (2009a). Modularity of 2-adic Barsotti-Tate representations. *Inventiones Mathematicae*, 178(3):587–634.

Kisin, M. (2009b). Moduli of finite flat group schemes, and modularity. *Annals of Mathematics*, 170(3):1085–1180.

Lipman, J. and Hashimoto, M. (2009). *Foundations of Grothendieck Duality for Diagrams of Schemes*. Springer-Verlag.

Mac Lane, S. (1998). *Categories for the Working Mathematician*. Springer-Verlag, New York, 2nd edition.

Mac Lane, S. and Moerdijk, I. (1992). *Sheaves in Geometry and Logic*. Springer-Verlag.

Macintyre, A. (2011). The impact of Gödel's incompleteness theorems on mathematics. In *Kurt Gödel and the Foundations of Mathematics: Horizons of Truth*, pages 3–25. Proceedings of Gödel Centenary, Vienna, 2006.

Maranda, J.-M. (1964). Injective structures. *Transactions of the American Mathematical Society*, 110:98–135.

Mathias, A. R. D. (2001). The strength of Mac Lane set theory. *Annals of Pure and Applied Logic*, 110:107–234.

Neeman, A. (2010). Derived categories and Grothendieck duality. In Holm, T., Jørgensen, P., and Rouquier, R., editors, *Triangulated categories*, pages 290–350. Cambridge University Press.

Takeuti, G. (1978). A conservative extension of Peano Arithmetic. In *Two Applications of Logic to Mathematics*, pages 77–135. Princeton University Press.

Takeuti, G. (1987). *Proof Theory*. Elsevier Science Ltd, 2nd edition.

Tamme, G. (1994). *Introduction to Etale Cohomology*. Springer-Verlag.

van Osdol, D. (1975). Homological algebra in topoi. *Proceedings of the American Mathematical Society*, 50:52–54.

Weibel, C. (1994). *An introduction to homological algebra*. Cambridge University Press.

Wiles, A. (1995). Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics*, 141:443–551.