

# SET THEORY FOR GROTHENDIECK'S NUMBER THEORY

COLIN MCLARTY

Draft of January 26, 2011

At a time when mathematical fashion despises generality (seen as gratuitous “generalities”, i.e. vacuities) 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)

Grothendieck preempted set theoretic issues in cohomology by positing that every set is an element of some “universe, which is a set ‘large enough’ that the habitual operations of set theory do not go outside it” (SGA 1 VI.1 p. 146). What looks like a proper class in a universe is a set when seen from outside it. His universes model Zermelo-Fraenkel set theory with choice (ZFC), so ZFC cannot prove they exist. We show the weak fragment of ZFC called *Mac Lane set theory* (MC) suffices for existing applications. It has the proof theoretic strength of simple type theory. Adding Mac Lane’s axiom of one universe gives MC+U, weaker than the ZFC theory of  $V_{\omega,3}$  yet sufficient for the whole SGA.

The message for number theory is that the SGA essentially as published can use standard set theory. The logical point is that cohomology uses unity more than generality. A functor from ‘all’ modules on a scheme to ‘all’ Abelian groups displays unity and generality. But cohomology can have that unity without the sweeping generality of strong set theory.

**Outline.** Sections 1–2 compare MC and MC+U to Zermelo set theory with choice (ZC). They define the sets which are *U-correspondents* of proper classes and remark that MC+U is weaker than MC plus countable replacement. Sections 3–5 get much of the SGA in MC. Number theorists remark how close cohomology is to explicit calculation. Logicians remark how much category theory is constructive (McLarty, 2006). The weak MC provides space enough for these explicit constructions with proofs little changed from the published forms—except for the very existence of cohomology groups, which is recast in Section 4.2.

Sections 6–8 use a universe to formalize the large structure tools of the SGA and the unified theorems they make possible. We use a naive definition of *U*-category which SGA 4 I.1.1 (p. 5) rejected. We cannot go theorem by theorem through 1500 pages of SGA 4 let alone all the SGA and EGA. Most of that is commutative algebra elementary in logical strength. Section 8 focuses on key, interrelated themes: cohomology, duality and derived categories, and fibred categories. Section 9 describes prospects for yet weaker foundations for cohomological number theory.

We need no arithmetic or deep algebra because Grothendieck kept them out of the basics. For example, Serre (1955) based his cohomology on his proof that affine

varieties have vanishing higher Čech cohomology. Grothendieck built on Serre's ideas but insisted "it is important for technical reasons not to take as *definition* of cohomology the Čech cohomology" (Grothendieck, 1958, p. 108, emphasis in the original). He defined cohomology by functorial trivialities. The enduring standard (Hartshorne, 1977) shows the success of this strategy. Hartshorne defines cohomology functorially on p. 204 and reaches Čech cohomology 15 pages later.

## 1. MAC LANE SET THEORY

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  $\phi(x)$  of (first order) set theory there is a set  $B$  of all elements of  $A$  which have  $\phi$ :

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

As an example of how this matters, the relation of a natural number  $n$  to the  $n$ -th transfinite cardinal  $\aleph_n$  is first order expressible, so replacement in ZFC proves there is a set of all these cardinals:

$$\{\aleph_i \mid i \in \mathbb{N}\}$$

That proof fails in ZC for lack of any set  $A$  provably containing all  $\aleph_i$  and this cannot be evaded. The ZFC set  $V_{\omega+\omega}$  models ZC, and  $\{\aleph_i \mid i \in \mathbb{N}\}$  is not in it.

Mac Lane set theory (MC) is ZC with bounded separation, that is separation only using formulas  $\phi(x)$  with all quantifiers bounded ( $\Delta_0$ ). So MC is finitely axiomatizable just as Gödel-Bernays set theory is. So ZC proves the consistency of MC. In terms of Mathias (2001, 107), MC is ZBQC omitting the axiom of foundation so it is **Mac** omitting foundation and transitive containment.

Mathias (2001) gives the key contrast to ZC: ZC proves the quantified statement " $\forall n \in \mathbb{N}$  there exists  $\aleph_n$ ." See the technical note on cardinalities at the end of this section. MC says  $\aleph_0$  exists; and it proves if  $\aleph_n$  exists then so does  $\aleph_{n+1}$  since  $\aleph_{n+1}$  can be bounded by the powerset of  $\aleph_n$ . So MC proves each finitely iterated case, say  $\aleph_5$ . But the formula "there exist  $n$  successive transfinite cardinals" with variable  $n$  escapes any bound by a stated iteration of powerset. MC cannot prove the formula defines a subset of  $\mathbb{N}$  and so cannot apply induction to it. Mathias shows indeed " $\forall n \in \mathbb{N}$  there exists  $\aleph_n$ " is unprovable in MC.

Contrast the real coordinate spaces  $\mathbb{R}^n$ . Each  $n \in \mathbb{N}$  determines  $\mathbb{R}^n$  by a definable relation, so replacement gives a set of all these spaces:

$$\{\mathbb{R}^n \mid n \in \mathbb{N}\}$$

But we can bound these sets. Define  $\mathbb{R}^n$  as the set of functions from  $\{0, \dots, n-1\}$  to  $\mathbb{R}$ . Then ZC proves the set of all  $\mathbb{R}^n$  exists as a subset of  $\mathcal{P}^2(\mathbb{N} \times \mathbb{R})$ . The  $\mathbb{R}^n$  are those  $V \in \mathcal{P}^2(\mathbb{N} \times \mathbb{R})$  meeting this  $\Delta_0$  condition:

$$\exists n \in \mathbb{N}, \forall y \in \mathcal{P}(\mathbb{N} \times \mathbb{R})$$

$$(y \in V \text{ iff } y \text{ is a function from } \{x \in \mathbb{N} \mid x < n\} \text{ to } \mathbb{R})$$

So MC proves there is a set  $\{\mathbb{R}^n \mid n \in \mathbb{N}\}$ .

To bound sets of sets explicitly, we define an *I-indexed* set of sets as a function  $f: A \rightarrow I$ . For each index  $i \in I$  the set  $A_i$  is the preimage:

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

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

**1.1. Classes, proper classes, and  $U$ -correspondents.** For us reference to a class  $\{x|\phi(x)\}$  is shorthand for talk about sets which satisfy the formula  $\phi(x)$  in first order set theory. A *proper class* is a class which does not define a set. This is just as Kunen (1983, p. 24) treats classes in ZFC: “Formally, proper classes do not exist. . . there is, in fact no formal distinction between a class and a formula.”

Given a universe  $U$ , the  $U$ -*correspondent* of a class  $\{x|\phi(x)\}$  is defined by  $\phi_U(x)$ , the formula  $\phi(x)$  with all variables relativized to  $U$ . By bounded separation every  $U$ -correspondent is a set, specifically a subset of  $U$ .

$$\{x \in U \mid \phi_U(x)\} \subseteq U$$

**1.2. Technical note on cardinalities in ZC and MC.** Neither MC nor ZC offers canonical representatives  $\aleph_\alpha$  for cardinalities. In these set theories, to say  $\aleph_n$  exists is shorthand for saying there is a set  $S$  with a sequence of subsets

$$s_0 \subset s_1 \subset, \dots, \subset s_n = S$$

where  $s_0 \cong \omega$  and each  $s_{k+1}$  has larger cardinality than  $s_k$  with no subsets intermediate in size. To say  $\{\aleph_i \mid i \in \mathbb{N}\}$  exists means some set  $S$  is the union of an infinite sequence of successively larger subsets with  $s_0 = \omega$ .

## 2. UNIVERSES FOR MC

Mac Lane set theory with a universe (MC+U) is MC plus an axiom U positing a universe  $U$  such that:

- (U 1) The pair  $\langle U, \in \rangle$  models the axioms of pair set, powerset, union, and infinity using the ambient membership relation  $\in$ .
- (U 2) If  $x \in U$  and  $y \in x$  or  $y \subseteq x$ , then  $y \in U$ .

This implies  $\langle U, \in \rangle$  models the axioms of extensionality, empty set, choice, and unbounded separation since  $U$  bounds all constructions in  $U$ . So  $U$  provably satisfies the ZC axioms plus all arithmetic statements provable in MC+U notably including Con(ZC). Each theory here proves consistency of the one before:

$$\text{MC, ZC, ZC+Con(ZC), MC+U, ZC+U}$$

MC+U proves  $\aleph_n$  exists for every  $n \in \mathbb{N}$  but also  $\aleph_n \in U$ . So unlike ZC it proves there is a set  $\{\aleph_n \mid n \in \mathbb{N}\}$ , bounded by the powerset  $\mathcal{P}(U)$ . In terms of ZFC, the ZFC set  $V_{\omega.3}$  models MC+U with  $U = V_{\omega.2}$ .

For future reference: MC plus countable replacement implies uncountably many successively larger universes. The union of the class  $\{\mathcal{P}^n(\omega) \mid n \in \mathbb{N}\}$  of all finitely iterated powersets of  $\omega$ , if it exists, is a universe. Any universe in place of  $\omega$  gives a larger one. And by countable replacement any countable sequence of universes has a universe as supremum.

**2.1. Fullness.** To say  $\langle U, \in \rangle$  models the powerset axiom means for every  $x \in U$  there is a set in  $U$  containing all and only the subsets of  $x$  that are in  $U$ . Condition U 2 says further every subset of  $x$  must be in  $U$ . We say  $U$  is *full on subsets*. This implies  $f \in U$  for every function  $f: x \rightarrow y$  between  $x, y \in U$ . And it implies arithmetic and analysis in  $U$  agree with the ambient. What looks like a standard model of Peano Arithmetic in  $U$  is a standard model in the ambient, and what looks like a powerset in  $U$  is a powerset in the ambient.

**2.2. Universes in categorical set theory.** The Elementary Theory of the Category of Sets (ETCS) can define a universe as a set of sets such that all the functions between them form an elementary topos with natural number object. ETCS implies this topos is well pointed and satisfies the axiom of choice, so it models ETCS and is full. These universes are very like MC universes. However, on categorical foundations the purposes of universes are less well served by adding a universe to ETCS than by positing a model of ETCS as a universe in the category of categories.

### 3. CATEGORY THEORY IN MC

This section uses MC as set theory.

**3.1. Small and locally small categories.** A *small category*  $\mathcal{C}$  is a set  $C_0$  of objects and a set  $C_1$  of arrows with domain and codomain functions  $d_0, d_1$  and composition satisfying the category axioms. A *functor*  $\mathcal{F}: \mathcal{C} \rightarrow \mathcal{D}$  of small categories is an *object part*  $F_0: C_0 \rightarrow D_0$  and *arrow part*  $F_1: C_1 \rightarrow D_1$  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  $\mathcal{C} \rightarrow \mathcal{B}$ , with natural transformations as arrows (Mac Lane, 1998, pp. 40–42). The functors can be represented by suitable functions  $C_1 \rightarrow B_1$  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  $C_0 \rightarrow B_1$  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  $\Delta_0$ .

A *locally small category* is commonly defined as any class of objects and any class of arrows with any rule for composition that satisfies the category axioms, only requiring that any two objects  $A, B$  of  $\mathcal{C}$  have a set  $\text{Hom}_{\mathcal{C}}(A, B)$  of all arrows  $A \rightarrow B$ . That definition is unusable without the axiom scheme of replacement. The correct requirement in our context is that each set of objects have a set of all arrows between them.

**3.2. Presheaves.** A *presheaf*  $F$  on a small category  $\mathcal{C}$  is a contravariant functor from  $\mathcal{C}$  to the category of all sets. But the latter is not small so the definition of functors between small categories 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 single set containing all the values  $F(A)$ .

So we define a presheaf  $F$  on  $\mathcal{C}$  as a  $C_0$ -indexed set of sets  $\gamma_0: F_0 \rightarrow C_0$  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  $e_F: F_1 \rightarrow F_0$  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  $\Delta_0$  conditions: for all arrows  $g: B \rightarrow A$  and  $h: C \rightarrow B$  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  $F(g): F(A) \rightarrow F(B)$  by  $(F(g))(s) = e_F \langle s, g \rangle$ . Clauses 2–3 express functoriality for composition and identity arrows.

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

$$\begin{array}{ccc} F_0 & \xrightarrow{\eta} & G_0 \\ \gamma_0 \searrow & & \swarrow \gamma'_0 \\ & C_0 & \end{array} \quad \gamma_0 = \gamma'_0 \eta$$

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

Each single presheaf on a (non-small) locally small category is a proper class and thus not easy to handle in MC. The right definition in our context is to say a presheaf  $F$  on a locally small category  $C$  is an assignment of presheaves to each small subcategory of  $C$  so that they agree wherever they overlap. For some purposes we might require “agreement” only up to compatible isomorphisms but for present purposes there is no problem with requiring agreement to be identity. This strict requirement has the convenience that makes a presheaf on a small category  $C$  the same thing as a presheaf on  $C$  taken as merely locally small.

The category of presheaves on a small category  $C$  is locally small. An *I-indexed set* of presheaves on a small category  $C$  is a  $C_0 \times I$ -indexed set of sets  $\gamma_0: F_0 \rightarrow C_0 \times I$  with an  $I$ -indexed action  $e_F: F_1 \rightarrow F_0$  where now

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

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

The category of presheaves is cocomplete: it has coequalizers and every indexed set of presheaves has a coproduct. The usual construction of coequalizers in functor categories obviously suits MC (Mac Lane, 1998, p. 115). The coproduct  $\coprod F$  of an indexed set  $\gamma_0: F_0 \rightarrow C_0 \times I$  of presheaves is the projection to  $C_0$ :

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

The value  $\coprod F(A)$  for any object  $A$  of  $C$  is the disjoint union of the values  $F(A, i)$  for  $i \in I$ . Because  $\coprod F = F_0$  as sets, the action  $e_F: F_1 \rightarrow F_0$  is also the action for  $\coprod F$ . The coproduct property follows trivially.

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

$$R_B(A) = \text{Hom}_C(A, B)$$

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

$$R_B(f): \text{Hom}_C(A, B) \rightarrow \text{Hom}_C(A', B)$$

defined by composition, so  $R_B(f)(g) = gf$ . As an explicit  $C_0$ -indexed set,  $R_B$  is just the domain function  $d_0: C_1 \rightarrow C_0$  restricted to arrows with codomain  $B$ , and action by composition with all arrows. A presheaf on  $C$  is *representable* if it is isomorphic (in the category of presheaves on  $C$ ) to  $R_B$  for some object  $B$  of  $C$ .

Notably, there is a  $C_0$ -indexed family of all functors  $R_B$  each indexed by its object  $B$ , using the set  $C_1$  of all  $\mathcal{C}$  arrows and the domain and codomain functions:

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

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

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

This operation is functorial in that

$$R_h R_k = R_{hk} \quad \text{and} \quad R_{(1_B)} = 1_{(R_B)}$$

The operation  $R_{(\cdot)}$  is called the *Yoneda embedding* and is so to speak a functor from  $\mathcal{C}$  to the locally small category of presheaves on  $\mathcal{C}$  which is called  $\widehat{\mathcal{C}}$ . But locally small categories formally do not exist.

The locally small category  $\widehat{\mathcal{C}}$  of presheaves on  $\mathcal{C}$  appears throughout topos theory. Its theory is organized around several theorems called the *Yoneda lemma*. The simplest version says for any presheaf  $F$  on  $\mathcal{C}$  and object  $B$  of  $\mathcal{C}$ , natural transformations  $R_B \rightarrow F$  correspond naturally to the elements of  $F(B)$ . So to speak, the functorial operation  $R_{(\cdot)}$  is full and faithful. Mac Lane (1998, p. 59) has a proof suitable for MC. The strongest version is Corollary 2.22 of Johnstone (1977, p. 51) which says, among other things, every presheaf is a colimit of presheaves  $R_B$ . Johnstone's diagrammatic proof works in any elementary topos, and so can be read as specifying bounds for a proof in MC.

A key aspect of Yoneda is that representable presheaves on a small category  $\mathcal{C}$  are *generators* for the category of presheaves  $\widehat{\mathcal{C}}$ . That is, distinct natural transformations  $\eta \neq \theta: F \rightarrow G$  are distinguished by some natural transformation  $\nu: R_B \rightarrow F$  from a representable:

$$R_B \xrightarrow{\nu} F \begin{array}{c} \xrightarrow{\eta} \\ \xrightarrow{\theta} \end{array} G \quad \eta\nu \neq \theta\nu$$

So the representables  $R_B$  give a  $C_0$ -indexed set of generators for the presheaf category (Mac Lane, 1998, p. 59). Notice this quantifies over small natural transformations in a locally small category of presheaves.

#### 4. COHOMOLOGY IN MC

**4.1. Topologies and toposes.** A *Grothendieck topology*  $J$  on a category  $\mathcal{C}$  assigns each object  $A$  of  $\mathcal{C}$  a set of *covers*, where each cover is a set of arrows to  $A$ . See any of our references on toposes. So a Grothendieck topology is a  $C_0$ -indexed set of sets of arrows subject to familiar conditions which are all bounded by the set  $C_1$  of arrows and its powerset. Thus each topology on  $\mathcal{C}$  is small as is the set of all topologies on  $\mathcal{C}$ .

A *site*  $\langle \mathcal{C}, J \rangle$  is a topology  $J$  on a small category  $\mathcal{C}$ . A  *$J$ -sheaf* on  $\langle \mathcal{C}, J \rangle$  is a presheaf on  $\mathcal{C}$  which meets this compatibility condition for  $J$ -covers: for each object  $A$  of  $\mathcal{C}$  and  $J$ -covering family  $\{f_i: A_i \rightarrow A \mid i \in I\}$  the value  $F(A)$  is an equalizer

$$F(A) \xrightarrow{\nu} \prod_i F(A_i) \begin{array}{c} \xrightarrow{\eta} \\ \xrightarrow{\theta} \end{array} \prod_{i,j} F(A_i \times_A A_j)$$

The condition is  $\Delta_0$  so every sheaf is a set.

When the site  $\langle \mathcal{C}, J \rangle$  is clear from context we speak of sheaves to mean  $J$ -sheaves. Notice a sheaf is a presheaf, meeting a condition. The category of  $J$ -sheaves has all  $J$ -sheaves as objects and all natural transformations between them as arrows.

As above,  $\widehat{\mathcal{C}}$  is the category of presheaves on  $\langle \mathcal{C}, J \rangle$ . The category of sheaves is called  $\widetilde{\mathcal{C}}_J$ . A Grothendieck topos is any category equivalent to  $\widetilde{\mathcal{C}}_J$  for some small site. It is locally small since an equivalence functor preserves the size of arrow sets. But it is not small. MC can prove elementary facts on categories of sheaves on a specified site as a shorthand for talk about all the sheaves on that site. But MC is poorly equipped to deal with locally small categories defined up to equivalence, since they are proper classes with their objects and arrows not individually specified.

Every presheaf  $F$  on a site  $\langle \mathcal{C}, J \rangle$  has an *associated sheaf*, that is a natural transformation  $i: F \rightarrow \mathbf{a}F$  to a  $J$ -sheaf  $\mathbf{a}F$  such that every natural transformation  $\eta: F \rightarrow S$  to a  $J$ -sheaf  $S$  factors uniquely through this one:

$$\begin{array}{ccc}
 F & \xrightarrow{i} & \mathbf{a}F \\
 & \searrow \eta & \downarrow u \\
 & & S
 \end{array}
 \quad \eta = ui$$

The usual argument from a universal property shows each natural transformation of presheaves  $\theta: F \rightarrow G$  induces a natural transformation of the associated  $J$ -sheaves  $\mathbf{a}\theta: \mathbf{a}F \rightarrow \mathbf{a}G$ . The definition of  $i: F \rightarrow \mathbf{a}F$  essentially says the associated sheaf operator is left adjoint to the inclusion of the category of  $J$ -sheaves into the category of presheaves on the site. The proofs in SGA 4 II and (Mac Lane and Moerdijk, 1992, pp. 227ff.) work in MC, and show that the associated sheaf operator preserves finite limits.

The Giraud theorem in Section 7 uses the fact that the associated  $J$ -sheaves of the representable presheaves on a site  $\langle \mathcal{C}, J \rangle$  give a  $C_0$ -indexed set of generators for the sheaf category. This follows from the universal property of the transformations  $i: R_B \rightarrow \mathbf{a}R_B$  for each object  $B$  of  $\mathcal{C}$ .

We have defined an associated sheaf for each presheaf by a functorial operation that preserves limits. But we define no associated sheaf *functor*. The locally small categories of presheaves and sheaves formally do not exist.

**4.2. Injectives and derived functors.** The definition of cohomology groups relies on the fact that every module over any ring  $R$  embeds in an *injective*  $R$ -module. We say the category of  $R$ -modules has *enough injectives*. Baer (1940) proved this for rings and modules in sets. Grothendieck's methods use the result for rings and modules in any Grothendieck topos. Grothendieck (1957a) lifted Baer's transfinite induction to a categorical context including Grothendieck toposes (albeit toposes were undreamt of at that time). But Baer's proof was soon simplified into two steps avoiding transfinite induction: First, every Abelian group embeds in a injective then extend the result to modules. See Blass (1979) for logical analysis and Eisenbud (1995, pp. 620f.) for a proof in sets.

The first step uses the axiom of choice so it will not lift into every Grothendieck topos. But Barr (1974) showed (in any set theory including choice) 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).

The descent uses a formal triviality known to Verdier (1972, p. 3):

**Lemma 4.1.** *If a functor  $\mathcal{F}:\mathcal{B}\rightarrow\mathcal{A}$  has a left exact left adjoint  $\mathcal{G}:\mathcal{A}\rightarrow\mathcal{B}$  with monic unit and  $\mathcal{B}$  has enough injectives then so has  $\mathcal{A}$ .*

*Proof.* Right adjoints preserve monics so a monic unit implies every monic  $G(A)\rightarrow I$  has monic adjunct  $A\rightarrow F(I)$ . Any left exact  $G$  preserves monics. These imply  $F$  preserves injectives. If object  $A$  in  $\mathcal{A}$  has a monic  $G(A)\rightarrow I$  to an injective in  $\mathcal{B}$ , the adjunct  $A\rightarrow F(I)$  is monic in  $\mathcal{A}$ .  $\square$

The descent takes  $\mathcal{A}$  be the category of Abelian groups in any Grothendieck topos and  $\mathcal{B}$  the category of Abelian groups in any Barr cover of it.

The second step applies 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  $A$ . Scalar multiplication  $r \cdot f$  in this module is defined by

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

This functor is defined in any elementary topos with natural numbers. The underlying Abelian group functor from  $R$ -modules is left adjoint to this, since each Abelian group  $A$  has a homomorphism  $\eta_A:A\rightarrow Hom_{\mathbb{Z}}(R, A)$  defined by

$$\eta_A(a)(r) = r \cdot a$$

which trivially has the unit property. It is monic. The underlying group functor is also left exact as it is right adjoint to tensor with  $R$  over  $\mathbb{Z}$ . The category of  $R$ -modules has enough injectives.

This implies every module  $M$  over any ring  $R$  in any definable Grothendieck topos  $E$  has injective resolutions of any given finite length  $n$ :

$$M \twoheadrightarrow I_1 \twoheadrightarrow \dots \twoheadrightarrow I_n$$

The usual proof of uniqueness of cohomology (up to isomorphism) is explicit calculation, so  $M$  has a unique (up to isomorphism)  $n$ -th cohomology group  $H^n(E, M)$  for any given finite  $n$ . The stronger set theory ZC proves the quantified statement

$$\forall n \in \mathbb{N} \text{ there exists } H^n(E, M)$$

There is no apparent proof that modules have infinite resolutions even in ZC. That requires the axiom of choice, and ZC apparently provides no sufficient sets of modules in which to apply choice.

For any explicitly defined left exact functor  $F$  from  $R$ -modules in  $E$  to ordinary Abelson groups, MC can define *right derived functors*

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

up to any given  $n$ . These have the usual properties of derived functors (Hartshorne, 1977, p. 204), except that we deal with exact sequences of any specified finite length  $n$  rather than infinite exact sequences. Čech cohomology is primarily a calculating tool, often used with spectral sequences. Most uses involve finitely many cohomology groups of a few explicitly defined modules and finite parts of spectral sequences. MC proves those exist.

In MC all this is shorthand for talk about small sites and sheaves, and explicit constructions of sites from sites or sheaves from sheaves. Mac Lane and Moerdijk (1992, pp. 511–13) construct a site for a Barr cover of the topos of sheaves on any site  $\langle \mathcal{C}, J \rangle$ , bounded in terms of  $\langle \mathcal{C}, J \rangle$ . To say the underlying Abelian group functor is left adjoint to  $Hom_{\mathbb{Z}}(R, \_)$  just means for each Abelian group  $A$  the homomorphism  $\eta$  explicitly defined above has the universal property of a unit.

**4.3. Grothendieck duality and change of base.** The pursuit of Fermat's Last Theorem (FLT) led Wiles to a family of problems each in elementary arithmetic but he needed a systematic solution. "The turning point in this, and indeed in the whole proof came" when he found one using "Tate's account of Grothendieck duality theory" (Wiles, 1995, p. 451). Wiles (p. 486) mentions Altman and Kleiman (1970) but for his specific claims he cites Mazur (1977). Mazur cites Deligne and Rapoport (1973) for the theorem. They cite Hartshorne (1966) for the proof.

Wiles uses a few cohomology groups for specified curves, and this is all polynomial algebra over countable rings closely related to the natural numbers. Specifically for each prime  $p$  it uses the finite field  $\mathbf{F}_p$  of integers modulo  $p$ , the ring of  $p$ -adic integers  $\mathbf{Z}_p$ , and the field of  $p$ -adic numbers  $\mathbf{Q}_p$ . Wiles identifies the tangent spaces on certain  $p$ -adic curves  $J_1(N, p)_{/\mathbf{Q}_p}$  with certain first cohomology groups. By Grothendieck duality he concludes related tangent spaces to curves over  $\mathbf{F}_p$  are isomorphic to the duals of related zero-th cohomology groups:

$$H^1(M_1(N, p)_{/\mathbf{Z}_p}, \mathcal{O}_{M_1(N, p)}) \quad H^0(X_1(N, p)_{/\mathbf{F}_p}, \Omega)$$

The relation is set up the same way for every case and it gets along well with mappings of curves and groups.

Altman and Kleiman's proof works in MC. It quantifies over sheaves and modules, not categories or functors. It uses only finite segments of cohomology, plus elementary algebra from EGA. The constructions are explicit and Wiles' cases are definable. This form is weaker than the theorem for  $U$ -categories in MC+U. And in any set theory, Altman and Kleiman's version applies to fewer schemes  $X$  than other versions. It suffices for Wiles's use and any equally explicit applications to suitably non-singular schemes. Section 8.2 below returns to Hartshorne (1966).

Wiles uses the *base change theorem for proper morphisms* (the point for which he cites Mazur). The logical picture is as for duality. The treatment at SGA 4 XII and XIII quantifies over schemes, morphisms, sheaves, and finite segments of cohomology. It uses much elementary algebra. It works for locally small categories in MC, while it has greater reach for  $U$ -categories in MC+U.

On this level, Grothendieck duality has small connection to Poincaré duality in étale cohomology. Étale Poincaré duality in (Deligne, 1977a) is easily cast in MC subject to the usual limitations on its scope.

**4.4. Étale fundamental groups.** A topological space  $X$  has *covering spaces* over it the way a helix can be stacked smoothly over a circle. The group of symmetries of such a cover of  $X$  is like a Galois group in algebra revealing much about the base  $X$ . The fundamental group of  $X$  summarizes all these groups in one. 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. Its use in cohomology can be stated with the finite segments of cohomology. The literature most often relates the étale fundamental group of a scheme  $X$  only to first étale cohomology groups  $H^1(X_{et}, M)$  for trivially definable sheaves of modules  $M$  on  $X$ .

We only need to show the category of finite étale covers of a scheme  $X$  is a set in MC. This is false using the common definition of étale covers up to isomorphism. Each isomorphism class is a proper class. But a finite étale cover of  $X$  is given by finitely generated extensions of the coordinate rings on Zariski open subsets of  $X$ .

So fix one countable set  $G$  of elements to be considered “generators.” MC proves any set of rings has a set of all finite extensions generated by elements of  $G$ . This set includes representatives (not unique) of every isomorphism class of finite extensions of those rings. So there is a set of all finite étale covers of  $X$  up to isomorphism.

## 5. FORMALIZING THE APPLICATIONS IN MC

The SGA and other literature often use universes to talk about actual categories and functors as in Lemma 4.1, in cases where schemes such as Theorem Scheme 5.1 below suffice for current applications. All the published applications of cohomological number theory can be formalized in MC using theorem schemes to handle specified, definable instances (possibly with parameters). See the technical note on sites at the end of this section. This shows the proofs have at most the proof theoretic strength of simple type theory though in fact the current uses surely have less strength yet. The published proofs invoke results genuinely quantifying over categories and functors that MC cannot define (McLarty, 2010). But those theorems can be circumvented by theorem schemes.

The explicitly numerical calculations in cohomological number theory are clearly within MC. We have just seen MC proves for any explicitly given Grothendieck topos  $E$  every definable module  $M$  has an  $n$ -th cohomology group  $H^n(E, M)$  for any given finite  $n$ . We cannot genuinely quantify over locally small categories or form sets of them, but we can specify them by formulas for their objects and arrows.

MC can quantify over parameters in a parametrized family of locally small categories such as “the locally small category  $\tilde{\mathcal{C}}_J$  of sheaves on a small site  $\langle \mathcal{C}, J \rangle$ .” Here  $\mathcal{C}$  is a variable which the formula says stands for a category, and  $J$  a variable which the formula says stands for a topology on  $\mathcal{C}$ .

The relations between toposes and topological spaces in SGA 4 IV, for example, are partly expressible this way. To express “every topological space  $X$  has a topos of sheaves  $Top(X)$ ,” we define sheaves and sheaf morphisms on  $X$  and prove (in MC) the category axioms as stated for these sheaves and morphisms. We say loosely “the sheaves and morphisms form a category” but formally they do not form one entity at all. We can prove in MC the sheaves and morphism on any space  $X$  satisfy the conditions of the Giraud Theorem, 7.4 below. Yet these sheaves and morphisms are not a *model* of any category or topos axioms, since they cannot be collected into one set.

To express “every continuous function  $f: X \rightarrow X'$  induces a geometric morphism  $f^*, f_*: Top(X) \rightarrow Top(X')$ ,” we define the direct image (resp. inverse image) along  $f$  of any sheaf on  $X$  (resp. on  $X'$ ) and show MC proves these definitions satisfy the conditions for a geometric morphism. We cannot say “every topos with such and so properties is equivalent to  $Top(X)$  for some topological space  $X$ ,” let alone “every geometric morphism  $Top(X) \rightarrow Top(X')$  corresponds to some function  $X \rightarrow X'$ .” Those statements genuinely quantify over toposes and their morphisms. We can only express definable cases.

Formally a locally small category  $\mathcal{A}$  is three formulas of set theory which we abbreviate and interpret as follows:

- $Ob_{\mathcal{A}}(x)$ :  $X$  is an object of  $\mathcal{A}$ .
- $Ar_{\mathcal{A}}(f, x, y)$ :  $f$  is an arrow of  $\mathcal{A}$  with domain  $x$  and codomain  $y$ .
- $Comp_{\mathcal{A}}(x, y, z)$ :  $x$  and  $y$  are arrows of  $\mathcal{A}$  with composite  $z$ .

Of course the category axioms as stated using these formulas must be theorems of MC. And MC must prove for any set  $S$  of objects satisfying  $Ob_{\mathcal{A}}(x)$  there is a set of all  $f$  satisfying  $Ar_{\mathcal{A}}(f, x, y)$  as  $x$  and  $y$  range over  $S$ . For the locally small category **AbGrp** of all Abelian groups and group homomorphisms,  $Ob_{\mathbf{AbGrp}}(x)$  would be the usual formula of set theory saying  $X$  is an Abelian group. The usual formula saying  $f$  is a homomorphism from group  $x$  to group  $y$  would be  $Ar_{\mathbf{AbGrp}}(f, x, y)$ .

The formulas may have other free variables which we regard as parameters. To talk about the locally small category  $\widehat{\mathcal{C}}$  of all presheaves on any small category  $\mathcal{C}$  we use formulas as listed here, involving an undisplayed free variable to be assigned the value  $\mathcal{C}$ .

A functor  $G: \mathcal{A} \rightarrow \mathcal{X}$  between locally small categories is two formulas:

- $Ob_G(x, y)$ :  $X$  is an object of  $\mathcal{A}$  and  $y$  an object of  $\mathcal{X}$  and  $y = G(x)$ .
- $Ar_G(x, y)$ :  $X$  is an arrow of  $\mathcal{A}$  and  $y$  an arrow of  $\mathcal{G}$  and  $y = G(x)$ .

The conditions of functoriality stated using these formulas and the formulas for  $\mathcal{A}$  and  $\mathcal{X}$  must be theorems of MC.

Given parallel functors  $F, G: \mathcal{B} \rightarrow \mathcal{D}$  between locally small categories, a natural transformation  $\eta: F \rightarrow G$  is a formula:

- $Trans_{\eta}(x, h)$ :  $X$  is an object of  $\mathcal{A}$  and  $h$  an arrow of  $\mathcal{X}$  and  $h = \eta_x$ .

This formula and the formulas for  $F$  and  $G$  must together satisfy the conditions of a natural transformation.

As a crucial example, we cannot define an adjunction between locally small categories as a pair of functors “for which there exists” some suitable natural transformation as unit. That would quantify over locally small transformations. But if we can specify an explicit unit  $\eta$  for a specified pair of functors  $F, G$  then we can specify an adjunction by a quintuple

$$\mathcal{A} \quad \mathcal{X} \quad F: \mathcal{X} \rightarrow \mathcal{A} \quad G: \mathcal{A} \rightarrow \mathcal{X} \quad \eta: 1_{\mathcal{X}} \rightarrow GF$$

meeting the usual conditions. Formally this adjunction is a way of invoking eleven formulas in the language of set theory.

We can formalize Lemma 4.1 in MC this way:

**Theorem Scheme 5.1.** *Take any formulas with free variables as shown*

$$\begin{array}{cccccc} Ob_{\mathcal{C}}(x) & Ar_{\mathcal{C}}(f, x, y) & Comp_{\mathcal{C}}(x, y, ) & Ob_{\mathcal{C}'}(x) & Ar_{\mathcal{C}'}(f, x, y) & \\ Comp_{\mathcal{C}'}(x, y, z) & Ob_F(x, y) & Ar_F(x, y) & Ob_G(x, y) & Ar_G(x, y) & \\ & & Trans_{\eta}(x, h) & & & \end{array}$$

*Suppose MC proves the formulas written with these which say they define locally small categories  $\mathcal{C}, \mathcal{C}'$  and functors  $F: \mathcal{C} \rightarrow \mathcal{C}'$  and  $G: \mathcal{C}' \rightarrow \mathcal{C}$  which are adjoint with unit  $\eta: 1_{\mathcal{C}} \rightarrow GF$ . Further suppose it proves for every  $x$  if  $Trans_{\eta}(x, h)$  then  $h$  is monic, and that every object of  $\mathcal{C}$  has a monic arrow to an injective. Then MC also proves every object of  $\mathcal{C}'$  has a monic arrow to an injective.*

Section 4.2 used two cases of this scheme. In the first use, the formulas  $Ob_{\mathcal{A}}(x)$  and  $Ob_{\mathcal{B}}(x)$  respectively say “ $x$  is a sheaf on a site  $\mathcal{C}$ ” and “ $x$  is a sheaf on the Barr cover of site  $\mathcal{C}$ ” where the Barr cover of site  $\mathcal{C}$  is explicitly defined in terms of  $\mathcal{C}$ . That section gave explicit descriptions of the other relevant formulas. The second use dealt with formulas defining groups and modules of sheaves over a site.

We can use the formulas expressing a locally small category  $\mathcal{A}$  to produce a formula saying every set of objects in  $\mathcal{A}$  has a coproduct in  $\mathcal{A}$ . Another formula

says every parallel pair of arrows in  $\mathcal{A}$  has a coequalizer. The conjunction of these says  $\mathcal{A}$  is cocomplete, there is a colimit for every set-sized diagram in  $\mathcal{A}$ . We have already proved these formulas stated for the locally small category of presheaves on a small category and we could do it as well for sheaves.

**5.1. Technical note on sites.** In saying MC can formalize all published applications I have not searched the entire literature. The key is to show small sites suffice, albeit most published proofs use locally small sites. Grothendieck at SGA 4 VII.3.3 (p. 350) shows any scheme site where all objects have covers by affine maps of finite type can be replaced by a small subsite. He uses the comparison lemma, our Theorem 7.1, which is formally inexpressible in MC. But the idea adapts to Zariski, étale, and flat sites in MC and these sites make up nearly all current applications. Compare Section 4.4 above and Milne (1980, p. 57). I rely on experts saying all sites in use can be handled this way.

The issue is not *gros* versus *petit* sites. Those do not differ in set theoretic size but in the geometric “size” of fibers, which roughly speaking may have any dimension in a gros site but must be 0-dimensional in a petit site. For scheme sites the issue is whether the finiteness conditions on maps  $Y \rightarrow X$  are local on the base or in the fibers. Local character on the base is essential and is no problem. But publications often use finiteness conditions local on the fiber. Then for any set  $Y_i \rightarrow X$  of maps in the site the union  $\coprod_i Y_i \rightarrow X$  is also in the site. This conveniently allows us to combine every cover into a cover by one map. But it makes the site a proper class, and it makes no difference to the sheaves. For the sites used in practice we can require that maps be *quasi-compact*, so that roughly speaking only finite coproducts  $\coprod_i Y_i \rightarrow X$  arise, See EGAI 6.3.1 (p. 304) or Tamme (1994, p. 90).

## 6. $U$ -CATEGORIES

We now work in MC+U positing a universe  $U$ .

A  $U$ -category is the  $U$ -correspondent of any locally small category. In other words it has subsets  $C_0, C_1$  of the universe  $U$  as sets of objects and arrows, and any composition rule satisfying the category axioms, only requiring that for every set of objects  $S \subseteq C_0$  with  $S \in U$  the set of arrows is in  $U$ :

$$\{f \in C_1 \mid d_0(f) \in S \text{ and } d_1(f) \in S\} \in U$$

The sets in  $U$  and the functions between them form a  $U$ -category  $\mathcal{SET}_U$ . It is  $U$ -correspondent to the locally small category of all sets and functions.

Since  $U$ -categories and functors between them are all small, MC+U handles them freely. In particular, if  $\mathcal{A}, \mathcal{B}$  are  $U$ -categories then the functor category  $\mathcal{B}^{\mathcal{A}}$  may not be a  $U$ -category but it is small and can be used to form further small functor categories in turn.

Grothendieck and Verdier (1972, p. 5) reject this definition of  $U$ -category because of a problem with set-valued functors. Section 3.2 solves the problem like everyone in the field today by using the *Grothendieck construction* of a presheaf on a small category  $\mathcal{C}$  as a  $C_0$ -indexed set  $\gamma_0$  with an action  $e_F$ . This way each presheaf is an element of  $U$ , and the category of all of them is a  $U$ -category by our definitions.

## 7. TOPOSES OVER A UNIVERSE

This section uses MC+U. Remarks after Theorem 7.1 typify the relation of results here to Section 5.

A  $U$ -presheaf on a  $U$ -category  $\mathcal{C}$  is the  $U$ -correspondent of a presheaf on a locally small category. So it is a presheaf  $\gamma_0: F_0 \rightarrow C_0$  such that every restriction to a subcategory  $\mathcal{C}' \subseteq \mathcal{C}$  with  $\mathcal{C} \in U$  is a presheaf in  $U$ . If  $\mathcal{C} \in U$  this is just a presheaf in  $U$ . A  $U$ -sheaf is a  $U$ -presheaf with the sheaf property. A  $U$ -site is a site  $\langle \mathcal{C}, J \rangle$  with a  $U$ -category  $\mathcal{C}$ . The categories of presheaves and sheaves on a  $U$ -site are small, but are not  $U$ -categories unless  $\mathcal{C} \in U$ .

If  $\mathcal{C} \in U$  then  $J \in U$  for every topology  $J$  on  $\mathcal{C}$ . Then the category  $\widehat{\mathcal{C}}_U$  of  $U$ -presheaves and the category  $\widetilde{\mathcal{C}}_{JU}$  of  $U$ -sheaves for  $J$  are  $U$ -categories. They are the  $U$ -correspondents of the locally small categories of presheaves or sheaves. We may omit any subscript on  $\widehat{\mathcal{C}}_U$  and  $\widetilde{\mathcal{C}}_{JU}$  which is clear from context.

A  $U$ -topos is any  $U$ -category equivalent to  $\widetilde{\mathcal{C}}_{JU}$  for some site  $\langle \mathcal{C}, J \rangle \in U$ . A Grothendieck topos is any small category equivalent to a  $U$ -topos. Sheaf categories on suitably bounded  $U$ -sites are Grothendieck toposes, by a theorem with many other uses:

**Theorem 7.1** (Comparison lemma). *Let  $U$ -site  $\langle \mathcal{C}', J' \rangle$  have a full and faithful functor  $u: \mathcal{C} \rightarrow \mathcal{C}'$  from a category  $\mathcal{C} \in U$  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  $\widetilde{\mathcal{C}}_{JU}$  and  $\widetilde{\mathcal{C}}'_{J'U}$  equivalent categories.*

*Proof.* This is case i)  $\Rightarrow$  ii) of SGA 4 III.4.1 (p. 288). Verdier's small categories are elements of  $U$  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 MC.  $\square$

This can be unwound to some extent to work without a universe for explicitly defined instances as in Section 5. But that would not just eliminate  $\mathcal{C}'$  in favor of its objects and arrows. Worse, it would only handle definable sheaves  $F$  on  $\mathcal{C}'$ , using defined values  $F(A)$ . The equivalence claim would be inexpressible since each single sheaf on  $\mathcal{C}'$  is a proper class and we cannot quantify over them.

**Corollary 7.2.** *If a  $U$ -category  $\mathcal{E}$  has a set of generators  $\{G_i | i \in I\} \in U$  and every  $U$ -sheaf for the canonical topology on  $\mathcal{E}$  is representable then  $\mathcal{E}$  is a  $U$ -topos.*

*Proof.* See the canonical topology in any reference on topos theory. The representability assumption implies  $\mathcal{E}$  is equivalent to the category of canonical  $U$ -sheaves  $\widetilde{\mathcal{E}}_{cU}$ . Apply the theorem to  $\mathcal{C}' = \mathcal{E}$  with its canonical topology and  $\mathcal{C}$  the full subcategory of objects in  $G$ . The local smallness condition on  $U$ -categories says  $\mathcal{C} \in U$ .  $\square$

**Theorem 7.3.** *For any site  $\langle \mathcal{C}, J \rangle \in U$ , the sheaf topos  $\widetilde{\mathcal{C}}_{JU}$  has:*

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

*Proof.* This is immediate by sheafification from the same properties of the presheaf category  $\widehat{\mathcal{C}}$ . See SGA 4 II.4 (p. 235). References to proofs for the presheaf case are collected at SGA 4 IV.1.1.2 (p. 302). Proofs are also in Mac Lane and Moerdijk (1992, pp. 24ff.). Their  $\mathcal{SET}$  is our  $\mathcal{SET}_U$  so they use explicit bounded constructions in small categories.  $\square$

In fact  $\tilde{\mathcal{C}}$  has limits for every diagram  $D \in U$ , but Theorem 7.4 below refers to this list as given. The list amounts to saying  $\tilde{\mathcal{C}}$  is an elementary topos with  $U$ -small coproducts (Mac Lane and Moerdijk, 1992, pp. 591).

**Theorem 7.4** (Giraud theorem). *Any  $U$ -category  $\mathcal{E}$  with the properties listed in Theorem 7.3 is a  $U$ -topos, and has a left exact subcanonical site.*

*Proof.* The first claim is case ii)  $\Rightarrow$  iii) of SGA 4 IV.1.2 (p. 303) plus our Corollary 7.2. The second is case iii)  $\Rightarrow$  i'). To show ii)  $\Rightarrow$  iii) we construct a site  $(\mathcal{C}, J) \in U$  with  $\mathcal{C}$  the full subcategory of  $\mathcal{E}$  with objects  $G_i$  and with  $\mathcal{E}$  equivalent to  $\tilde{\mathcal{C}}_{\mathcal{J}U}$ . The proof at SGA 4 IV.1.2 (pp. 305f.) uses a universe  $V$  with  $U \in V$  and the category  $\tilde{\mathcal{E}}_{cV}$  of  $V$ -sheaves on  $\mathcal{E}$  for the canonical topology. Instead of  $\tilde{\mathcal{E}}_{cV}$  we use the locally small category of all sheaves on  $\mathcal{E}$  for the canonical topology. This category is not a set but each sheaf is, and there is a set of all transformations among any set of them. Fortunately the proof uses explicit constructions quantifying only over sets of these sheaves and sets of transformations among them so it works in MC+U. The same adaptation works for the proof of iii)  $\Rightarrow$  i') on p. 304, using choice to select one limit for each diagram. The proof by Mac Lane and Moerdijk (1992, pp. 577ff.) in effect uses one universe plus locally small categories and also adapts to MC+U.  $\square$

## 8. LARGE-STRUCTURE TOOLS

This section uses MC+U so the intuitions behind the theorem schemes of Section 5 are formalized as plain theorems.

**8.1. Topos cohomology.** Given a universe, the  $n$ -th cohomology group  $H^n(\mathcal{E}, F)$  is not just an operator applicable to definable  $R$ -modules  $F$  on definable toposes  $\mathcal{E}$ , and functorial on them. It is actually a functor from the category of  $R$ -modules in any  $U$ -topos  $\mathcal{E}$  to the category of Abelian groups, whether  $R$  or  $\mathcal{E}$  are definable or not. These are small categories and in fact  $U$ -categories. We omit the generalization to all Grothendieck toposes.

Standard accounts of derived functor cohomology work in MC+U. Many, like Hartshorne (1977) and Tamme (1994), elide set theoretic questions. We read their functors to sets as functors to  $\mathcal{SET}_U$ , and their functors to Abelian groups as functors to the category  $\mathcal{AB}_U$  of Abelian groups and group morphisms in  $\mathcal{SET}_U$ . All of these are  $U$ -categories, and thus small:

- Every  $U$ -topos  $\mathcal{E}$ , including  $\mathcal{SET}_U$ .
- The category  $\mathcal{AB}_{\mathcal{E}}$  of Abelian groups and homomorphisms in any  $U$ -topos  $\mathcal{E}$ , including  $\mathcal{AB}_U$ .
- For every ring  $R$  in any  $U$ -topos  $\mathcal{E}$  the category  $R\text{-MOD}_{\mathcal{E}}$  of  $R$ -modules and homomorphisms in  $\mathcal{E}$ , including for all rings  $R$  in  $\mathcal{SET}_U$ .

The standard, published theory of geometric morphisms among these toposes applies. The toposes are all sets, and the standard constructions are all bounded. In particular each  $U$ -topos  $\mathcal{E}$  has a global section functor  $\Gamma$  to  $\mathcal{SET}_U$  with left exact left adjoint  $\Delta$  the constant sheaf functor.

$$\mathcal{E} \xrightarrow{\Gamma} \mathcal{SET}_U \quad \text{with left exact left adjoint} \quad \mathcal{SET}_U \xrightarrow{\Delta} \mathcal{E}$$

For any ring  $R$  in  $\mathcal{E}$  the global section functor takes  $R$ -modules to Abelian groups. Indeed it takes them to modules over the ring  $\Gamma(R)$  but we focus on the Abelian

group valued functor:

$$R\text{-MOD}_{\mathcal{E}} \xrightarrow{\Gamma} \mathcal{AB}_U$$

This has a series of right derived functors  $R^n\Gamma$  which define the cohomology groups  $H^n(\mathcal{E}, M)$  of each  $R$ -module  $M$ :

$$H^n(\mathcal{E}, \_) = R^n\Gamma(\_) : R\text{-MOD}_{\mathcal{E}} \longrightarrow \mathcal{AB}_U$$

These functors are defined up to isomorphism by either of two equivalent functorial characterizations (Grothendieck, 1957a, p. 141):

- (1) The functors  $H^n(\mathcal{E}, \_)$  form a universal  $\delta$ -functor over  $\Gamma$ .
- (2) The functors  $H^n(\mathcal{E}, \_)$  form an effaceable  $\delta$ -functor over  $\Gamma$ .

These statements are formalized in MC+U in the natural way, using the category of  $\delta$ -functors on  $R\text{-MOD}_{\mathcal{E}}$ . See set theoretic discussion in McLarty (2010, pp. 368f.). In the context of MC+U the category of  $\delta$ -functors on  $R\text{-MOD}_{\mathcal{E}}$  is provably small, and thus a legitimate entity, though it is not provably a  $U$ -category.

The existence of the derived functors follows Section 4.2 but with stronger statements. MC+U proves the quantified statement that for every  $U$ -topos  $\mathcal{E}$  and every  $R$ -module  $M$  in  $\mathcal{E}$  there is an infinite injective resolution:

$$M \rightrightarrows I_1 \rightrightarrows \dots \rightrightarrows I_n \rightrightarrows \dots$$

Čech cohomology provides calculating tools which work essentially as in Section 4.2 but more systemically. All the relevant categories are small and we do not face the limits on mathematical induction that MC by itself does.

SGA 4 often invokes successively larger universes  $U \in V$  where we can use  $U$  plus  $U$ -categories, as SGA 4 IV.10 does as a context for multilinear algebra in toposes. All this is easily handled in MC+U since  $U$ -categories are small.

## 8.2. 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 proved by Altman and Kleiman (1970): certain cohomology groups (and more general groups) of nonsingular projective schemes are isomorphic in a natural way. Grothendieck (1958, pp. 112–15) explains why it should allow singularities and why that will require a more sophisticated approach. By 1959 he believed the right approach would use *derived categories* which would allow a considerably more general theorem with a more systematic statement and proof.

Hartshorne (1966) uses derived categories, which are now standard for theoretical work on 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 and XVIII and (Deligne, 1977b), while he has always been clear that large-structure tools are dispensable in principle.

Cohomology takes a module  $M$  on a scheme  $X$  and deletes nearly all the detailed 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.

As a central example, a scheme map  $f: A \rightarrow B$  sets up complicated relations between cohomology over  $A$  and  $B$ . These relations are tightly summed up in a single functor  $Rf_*: D(A) \rightarrow D(B)$  between derived categories. The successive effect on cohomology of two maps cannot be fully determined merely from the two separate effects on cohomology (it is only determined up to a spectral sequence by those). Yet the derived functorial summary of the successive effects is (up to isomorphism) precisely the composite of the individual functorial summaries:

$$\begin{array}{ccc} & A & \\ f \nearrow & & \searrow g \\ B & \xrightarrow{gf} & C \end{array} \qquad \begin{array}{ccc} & D(A) & \\ Rf_* \nearrow & & \searrow Rg_* \\ D(B) & \xrightarrow{R(gf)_* \cong (Rg_* Rf_*)} & D(C) \end{array}$$

All the various forms of Grothendieck duality in research today say the functor  $Rf_*$  has a right adjoint  $Rf^!: D(B) \rightarrow D(A)$ , with some further properties and under some conditions on  $f$ . The adjunction contains very much information and allows generality of a kind important in practice.

The set theoretic issue is to form certain *categories of fractions*. Weibel (1994) gives a careful treatment in ZFC with universes. For a suitable class  $\Sigma$  of arrows in a category  $\mathcal{C}$  there is a category of fractions  $\mathcal{C}[\Sigma^{-1}]$  with the same objects, while an arrow  $A \rightarrow B$  in  $\mathcal{C}[\Sigma^{-1}]$  is represented by a pair of arrows in  $\mathcal{C}$ :

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

We define an equivalence relation on these pairs with the crucial feature that many different objects  $C$  may figure in one equivalence class. And we define a composition rule so a pair  $\langle s, f \rangle$  acts like a composite  $s^{-1}f$ . This gives the effect of an inverse to  $s$  even if  $s$  has no inverse in  $\mathcal{C}$ .

That equivalence relation is no problem if  $\mathcal{C}$  is small. Then there is a set  $C_1$  of all arrows of  $\mathcal{C}$ , and so a set of all pairs of arrows, and so  $\mathcal{C}[\Sigma^{-1}]$  is also small. In MC+U all the cases we want are small.

The equivalence relation can be a problem for a locally small category  $\mathcal{C}$ . Then one arrow may be a proper class, as it may be an equivalence class involving proper class many different objects  $C$  of  $\mathcal{C}$ . Weibel (1994, p. 386) gives a set theoretic fix which works for most cases of interest but in no way eliminates our universes. It uses countable replacement to show sequences of cardinals have suprema. Section 2 shows countable replacement in MC implies uncountably many universes (in our sense, not Grothendieck's original sense).

Current work on Grothendieck duality is formalizable in MC+U. For lively differences over mathematical strategies (not over 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).

**8.3. Fibred categories.** Universes first appeared in print in SGA 1 VI on fibred categories. Everything there could be formalized in MC in terms of small categories and no universes, but the motivating examples use universes.

Fibred categories 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, and definable cases can be unwound into theorem schemes as in Section 5 with the usual loss of scope and unity. More often though, the literature avoids them except as a research topic—as in the Hartshorne quote ending Section 8.2

## 9. FURTHER PROSPECTS

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. MC+U founds the whole SGA for arbitrary sites, meaning any small site existing in the set theory ZC and bit more than that. Even on the level of these tools weaker foundations may be possible. Sites and modules in arithmetic are generally countable. Cardinal bounds plus ideas from elementary topos theory might be able to found arithmetic cohomology on some full  $n$ -order arithmetic with a universe a few ranks above  $\mathbb{N}$ .

If that works it might be a good context for hard analysis of individual proofs as Macintyre (Forthcoming) begins for (Wiles, 1995) on FLT. Currently known proofs would fit into  $n$ -th order arithmetic. Detailed estimates might bound each use of induction and comprehension to fit into 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.

There is recent progress quite apart from logic. Kisin (2009a) extends and radically simplifies (Wiles, 1995). He eliminates appeal to Grothendieck duality and generally uses less geometry than commutative algebra. Still cohomological, the proof uses visibly less set theory than Wiles's did. At the same time Kisin (2009b) completes a different proof of FLT by a strategy of Jean-Pierre Serre advanced by Chandrasekhar Khare and Jean-Pierre Wintenberger.

## ACKNOWLEDGMENTS

It is a pleasure to thank the people whose generous advice and suggestions made this work possible, 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, Steve Gubkin, Michael Harris, William Lawvere, Angus Macintyre, Barry Mazur, 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). A citation SGA 4 III.1.2 means SGA 4 exposé III section 1 paragraph 2.

- Altman, A. and Kleiman, S. (1970). *An Introduction to Grothendieck Duality Theory*, volume 146 of *Springer Lecture Notes in Mathematics*. Springer-Verlag, New York.
- Artin, M., Grothendieck, A., and Verdier, J.-L. (1972). *Théorie des Topos et Cohomologie Étale 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 change*. Number 1750 in *Lecture Notes in Mathematics*. Springer-Verlag, New York.
- Deligne, P., editor (1977a). *Cohomologie Étale*. Séminaire de géométrie algébrique du Bois-Marie; SGA 4 1/2. Springer-Verlag. Generally cited as SGA 4 1/2, this is not strictly a report on Grothendieck’s Seminar.
- Deligne, P. (1977b). 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<sup>e</sup> Siècle (Nice, 1996)*, pages 11–19. Soc. Math. France.
- Deligne, P. and Rapoport, M. (1973). Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II*, volume 349 of *Lecture Notes in Mathematics*, pages 143–316. Springer-Verlag, New York.
- Eisenbud, D. (1995). *Commutative Algebra*. Springer-Verlag.
- Friedman, H. (2010). Concrete mathematical incompleteness. On-line at [www.math.ohio-state.edu/~friedman/](http://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 Étale*

- 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). Moduli of finite flat group schemes, and modularity. *Annals of Mathematics*, 170(3):1085–1180.
- Kisin, M. (2009b). Modularity of 2-adic Barsotti-Tate representations. *Inventiones Mathematicae*, 178(3):587–634.
- Kunen, K. (1983). *Set Theory: An Introduction to Independence Proofs*. North-Holland.
- 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. (Forthcoming). The impact of Gödel's incompleteness theorems on mathematics. In *Horizons of Truth: Proceedings of Gödel Centenary, Vienna, 2006*.
- Mathias, A. R. D. (2001). The strength of Mac Lane set theory. *Annals of Pure and Applied Logic*, 110:107–234.
- Mazur, B. (1977). Modular curves and the Eisenstein ideal. *Publ. Math. IHES*, 47:133–86.
- McLarty, C. (2006). Two aspects of constructivism in category theory. *Philosophia Scientiae, Cahier Spécial* 6:95–114.
- McLarty, C. (2010). What does it take to prove Fermat's Last Theorem? *Bulletin of Symbolic Logic*, 16:359–77.
- Milne, J. (1980). *Étale Cohomology*. Princeton University Press.
- 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.
- Serre, J.-P. (1955). Faisceaux algébriques cohérents. *Annals of Mathematics*, 61:197–277.
- Takeuti, G. (1978). A conservative extension of Peano Arithmetic. In *Two Applications of Logic to Mathematics*, pages 77–135. Princeton University Press.
- Tamme, G. (1994). *Introduction to Étale Cohomology*. Springer-Verlag.
- Verdier, J.-L. (1972). Cohomologie dans les topos. In Artin, M., Grothendieck, A., and Verdier, J.-L., editors, *Théorie des Topos et Cohomologie Étale des Schémas*, volume 2 of *Séminaire de géométrie algébrique du Bois-Marie, 4*, pages 1–82. Springer-Verlag.
- 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.