用什么来证明 Fermat 大定理？ Grothendieck 与数论的逻辑

Colin McLarty

摘要 本文探究现已发表的 Fermat (费马) 大定理证明中所使用到的集合论假设，这些假设怎样出现在 Wiles (怀尔斯) 使用的方法中，以及目前所知道的使用更弱假设的证明的前景.

Fermat 大定理 (简记为 FLT) 的证明是否超出了 Zermelo-Fraenkel (策梅洛–弗伦克尔) 集合论 (简记为 ZFC)? 或者，它是否仅仅使用了 Peano (佩亚诺) 算术 (简记为 PA) 或其某个较弱的部分？这些问题的答案依赖于什么叫 "证明" 和 "使用"，而答案目前还不完全清楚. 本文对这些问题的现状进行评述，并概述目前证明中使用的 上同调数论 (*cohomological number theory*) 方法.

FLT 的现有证明为 Wiles [1995] 以及一些不改变其特征的改进. 这些文献远不是自我包含的，其中大量所需背景知识只是在 [Cornell et al., 1997] 这本厚达 500 页的书中才得以引进. 我们把 Wiles 在其证明中作为步骤明确引用的这些假设称为 "事实上在已发表的证明中使用到的". 现在不知道哪些假设是 "原理上使用到的"，即对于 FLT 的证明从理论上说是必不可少的. 当然，在原理上使用到的比 ZFC 要少得多，大概没有超出 PA，也许比 PA 少得多.

容易引起莫名争议的问题是 全域 (*universe*)，也经常被称为 *Grothendieck* (格罗滕迪克) 全域.[1] 在 ZFC 的基础上，全域是一个不可数的传递集合 U，使得 $\langle U, \in\rangle$ 以最好的方式满足 ZFC 公理：它包含每个元素的幂集 (powerset)，且对于任何从 U 的一个元素到 U 的函数，其值域仍是 U 的一个元素. 这就比仅仅说 $\langle U, \in\rangle$ 满足 ZFC 公理强得多. 我们不是仅说当所有量词 (quantifier) 为相对 U 时幂集公理 "每个集合有幂集" 为真. 而是要求 "对每个集合 $x \in U$, x 的幂集仍在 U 中"，在这里 x 的幂集的定义中没有一个量词是相对于 U 的. 看起来像 x 在 U 内部的幂集的东西必须 是 在更大的集合环境中看起来是 x 的幂集. 类似地，关于函数的像集的条件也比 $\langle U, \in\rangle$ 满足相对于 U 的替代公理范式 (replacement axiom scheme) 更强. 这一条件说任何从 U 的一个元素到 U 的函数，如果在更大的集合环境领域中存在，则它本身是 U 的一个元素. 这个附加的强度保证了应用于 U 中的集合的任何集合论构造，无论它是在 U 的内部还是在更大的集合论域中，都将

译自： The Bulletin of Symbolic Logic, Vol.16 (2010), No.3, p.359–377, What does it take to prove Fermat's last theorem? Grothendieck and the logic of Number theory, Colin McLarty.

Colin McLarty 是美国 Case Western Reserve 大学的哲学系和数学系教授. 他的邮箱地址是 colin.mclarty@case.edu.

1) 参阅 Grothendieck [1971] 以及更完整的叙述 Artin et al. [1972, vol. I, p. 185–217]. 我们把这些书分别简写为 SGA 1 和 SGA 4.—— 原注

给出同样的结果. 全域的使用常常依赖于此.

Grothendieck 证明了一个集合论学家已经知道的结果: 在 ZFC 中全域的定义和以下说法是一样的: 对某个不可数的强不可达 (strongly inaccessible) 基数 α, U 是所有秩低于 α 的集合的集合 V_α[Artin et al., 1972, vol. I, p. 196]. 因为每个全域是 ZFC 的一个模型, 全域或不可数强不可达基数的存在性在 ZFC 中是不可证明的. Grothendieck 自己的全域公理设想每个集合包含在某个全域中, 根据替代公理, 这蕴含了真类多个 (proper-class many) 与逐次增大的不可达基数相对应的逐次增大的 (successively larger) 全域. 我们记 ZFC+U 为下面这个稍弱一些的理论. 即 ZFC+U 由 ZFC 加上存在一个全域的假设 (或等价地, 存在一个不可数的强不可达基数的假设) 组成.

所以, ZFC+U 肯定蕴含比单独的 ZFC 更多的算术命题.[1] 以下事实由 Gödel (哥德尔) 观察得到: 任何蕴含 ZFC 相容性的公理必定蕴含 ZFC 不能推出的算术命题, 这是因为 ZFC 的相容性可以表示为一个不能由 ZFC 推出的算术命题. 这就使得一个全域的假设与连续统假设, 或其他不需要增加相容性强度或蕴含任何新算术的扩张 ZFC 的公理, 相当地不同. 但是我们将看到这个 Gödel 现象对 FLT 不会产生影响.

本文的目的是解释以下 3 个事实怎样共存以及为什么共存:

1. 全域对那些用于证明 FLT 或其他数论问题的相当明确的算术计算提供了一个环境.

2. 尽管从未这样做过, 通过已知手段, 全域可用 ZFC 代替 (这仍比 PA 强得多).

3. 上同调数论中一些杰出的证明, 如 Wiles [1995] 或 Deligne (德利涅) [1974], 或 Faltings (法尔廷斯) [1983], 事实上使用了全域.

Grothendieck 对这类大基数既不感兴趣也不认为其成问题. 本文也采用了他的观点. 对他来说这些基数只不过是得到其它结论的合理手段. 他想将明确的可以计算的算术以一个对几何概念的排序来进行排列. 他发现了在 上同调 中进行上述构造的方法并使用它们来进行计算, 从而逃离了所有顶尖数学家们研究 Weil (韦依) 猜想的年代 [Osserman (奥瑟曼), 2008]. 他因而提供了大部分当前代数几何的基础而不仅仅是承担算术的那些部分. 他的上同调虽基于全域, 但在不考虑某些所需的对概念的排序时, 稍弱的基础也足以应付.

§1 给出 Wiles 关于 FLT 证明中全域的一个主要使用的具体例子. §2 介绍在 PA 或较弱算术中证明 FLT 的可能性. §3—4 概述上同调数论和 Grothendieck 的策略. 大结构问题占据了 §5—7, 包括 §5 末对 ZFC 3 种逐次增强的扩张的比较. 我们引用 Deligne [1977, 1998] 来证明寻找原理上非必须的全域和实际上有用的全域没有矛盾. 二者均为真. 否认其中一个会引起认知上的缺失. 在 §7 末, 我们描述目前所知的关于在没有全域的 ZFC 中表达上同调的证明的情况. 这一表达肯定能在失去理论上某些系统性的情况下做到, 而我们给出一种猜想中的损失不大的方式. §8 重新审视如何使 Wiles 的证明更接近 PA 的问题. 认真看过 Wiles 证明的人, 没有谁会怀疑完全按照例行的做法, 这个证明能在 PA

1) 在本文, "算术" 始终是指 1 阶算术, 即用 PA 的语言表述或在 ZFC 说明的 PA 上的命题.—— 原注

一个相当高阶 (例如 8 阶) 非保守的 (non-conservative) 扩张中展开，尽管这会对理论的系统性产生巨大损失. 另有证据表明，算术中大量非常规的进展能够在 PA 一个保守的高阶扩张中 (因而在 PA 中是能行的) 提供一个证明. 对于算术中目前还不可预见的进展能使证明简化到怎样的程度，我们还看不到任何限制. §9 提出关于数学基础的结论.

本文中将会提到两种十分不同的尺度. 我们称一个集合或结构是 "大" 的，意味着它至少像某个全域那么大. 我们称之为 "很小" 的结构则是最多像连续统那样的尺度. 几乎每个我们所谈论的特定结构在这个意义下，或者是大的，或者是很小的.

§1. 全域的运用

Harvey Friedman (弗里德曼) 提出了一个清晰而简单的断言："我听说在 Wiles 论文的正文中用到的文献中绝对不能回溯到全域."[1] 但我们很快将看到，Wiles 证明中的一篇关键文献直接回溯到了 Grothendieck 和全域.

同样是 Friedman 或另一个未提及名字的专家排除了任何全域的实际作用："任何理解这些证明的人都自始至终考虑很小的结构."[2] 在大多数情形，这是正确的，而且对上同调数论是重要的. Grothendieck 创造了十分灵活的大的上同调结构，人们可以十分顺利地通过它们来得到算术而同时几乎不考虑这些结构.

当一个数论学家开始进行活跃研究时，他也许被好意地劝告，首先从 SGA 4 及相关文献去熟悉研究大结构的定理，特别是算术和几何，而不是长时间徘徊在这些定理的证明中 —— 直到他需要证明其中一个定理的修正形式. Barry Mazur (马祖尔) 向我指出了这种策略，他强调，任何一个实际带有这些想法工作的人，随着时间的推移，将修改许多一般性的结果，从而需要熟练掌握大结构定理和大量小结构的算术. 事实上，能够理解证明的人只是常规地引用已发表的大结构定理，而很少有人修改证明使之包含新的情形.

Wiles 解释，他对证明的探索曾经怎样被一个特殊的算术问题所打断. 他说，当这种探索把他引向两种上同调不变量时，"此处的转折点，实际上也是整个证明的转折点来到了","我意识到，由 Tate (泰特) 关于 Grothendieck 对完全交的对偶理论的说明，这两种不变量是相等的" [Wiles, 1995, p. 451]. 证明的主要部分 (p. 486—487) 引述了来源：

"当前用到的对偶性叙述的概要，参阅 [Mazur, 1977, §II.3] . . . . 要详细证明这种约简，见 [Mazur, 1977, §II.3] 中的论证."

Mazur 并没有提供完全的证明，但是引用了 Grothendieck 与 Dieudonné (迪厄多内) [1961], 我们将它简记为 EGA III, 以及 Deligne 与 Rapoport [1973], 后者引用了 EGA III 的同样部分. Grothendieck 和 Dieudonné 用了局部小范畴之间的函子范畴 (p. 349). 从 ZFC 的观点来看，这些局部小范畴是真类. 真类之间的一个函数是一个真类，所以两个

1) 引自 FOM 电子邮件列表，Friedman 题为 "来自专家的报告" 的邮件，1999 年 4 月 6 日星期二. cs.nyu.edu/pipermail/fom.—— 原注 (FOM 是美国的一个内部网站，列出讨论数学基础的一些自动化电子邮件.—— 译注)

2) 引自 FOM 电子邮件列表，Friedman 题为 "利用全域？专家再次评述" 的邮件，1999 年 4 月 8 日星期四. cs.nyu.edu/pipermail/fom.—— 原注

真类之间的函数的任何 "集合" 是一族真类. 我们称这样的一个族 (collection) 为一个 *超类* (*superclass*).

如果我们考虑使得秩的增加尽可能小, 则选取适当的细节, 我们可以说, 在 ZFC+U 中, 局部小范畴有和全域 U 有相同的秩, 而它们之间的函子范畴是秩高出 1 的超类.[1] 在 ZFC+U 中以这种方式尽量限制秩的提升实际上是没有意义的, 这是由于 ZFC+U 中对每个序数 β 都有比 U 的秩高出 β 的集合; 但如果我们想考虑 ZFC 较弱扩张的话 (只增加真类和其上高出一个限定数量下的秩), 这将是非常关键的. 无论如何, 这不是我们增加秩的终点, 因为这些超类范畴的范畴运算意味着将它们置于更高秩的范畴中. Grothendieck 的基本原理, 正如他在以书的形式出版的 EGA [Grothendieck and Dieudonné, 1971, p. 19] 第 0 章 p.1 所说, 就是全域.

Wiles [1995] 和 Mazur [1977] 把注意力集中在很小的结构上. 这些结构是有限的, 可数的, 或最多是连续统尺度的. 但他们用了 Grothendieck 和 Dieudonné [1961] 把那些很小的结构置于大结构内部而证明的一般定理. 这些定理至今仍被广泛征引, 而且还被 Lipman 和 Hashimoto [2009, p. 160, 287] 利用全域证明.

Deligne 和 Rapoport 在表达和证明他们的结果 (p. 151) 时解释说, "这些技巧提供了系统性的手段". 包括 Grothendieck 和 Dieudonné 在内的所有作者都知道, 可以使用与具体应用相关的技术性细节和累赘论述, 来替代系统性证明, 从而使得这些定理中对算术中任何给定的应用都已足够的那些部分可以在 ZFC 内部叙述. 作者们更喜欢系统性的手段, 因为现有材料已经够长了.

§2. 较弱证明的前景

Angus Macintyre [即将发表 (已在 2011 年发表, 见参考文献.—— 译注)] 设计了一个程序来将对于 Wiles [1995] 极为重要的模块性论点 (MT) 表示为算术的一个 Π^0_1 命题, 并论证它在 PA 中是可证明的. 这个程序可以导出 MT 的一个 PA 证明, 而且还有可能导出一个不用 MT 的 FLT 证明. 它需要算术中大量的新工作. 虽然它紧密地依赖于 Wiles [1995], 但不是能仅靠例行的改写原证明得出.

Macintyre 指出, Wiles 的证明中引入的如 p 进数, 实数, 以及复数这样的分析或拓扑结构, 是经由对整数环或有理数域这类结构进行完备化得到的. 这一过程可在 PA 中说明. Macintyre 概述了怎样用 PA 中的有限逼近来代替证明中许多完备化的运用. 他证明了怎样应用算术和模型论中的大量已知结果产生来得到适用于特定情形的逼近. 他还明确提出了另外一些需要目前尚未知的数值界的情形. 这种类型的定理可能极难. 他注意到, 甚至连常规情形也可能需要大量工作以至于 "持有某些元定理 (metatheorem) 是有用的" (p. 14). 这个规划的工作量极大. 如果用元定理能够达成目标, 则沿同一方向的进一步发展也许能但也许不能使我们最终用 PA 中的一个清晰证明来替代这些元定理.

我们熟知这样的情形: 更初等的证明通常需要更精妙的计算. 这些计算常常揭示出

1) 定义范畴为一个箭头的类上的合成算子. 如果把范畴定义为一类箭头和它上面的合成算子的 Kuratowski (库拉托夫斯基) 有序对, 则局部小范畴的秩比 U 高出 2.—— 原注

更多信息. 这个证明往往也更长. 即使在得到显式证明是一种无效劳动的情形下, 通过证明它的存在, 我们也能获得很多. 对于 FLT 来说, 困难在于目前已知证明的规模. Wiles [1995] 给出 84 篇参考文献. 其中许多是 Wiles 必需的步骤. 它们自身大多数都不短. 而且它们也依赖于其他相当高级的文献.

Harvey Friedman 猜测 FLT 在指数函数算术 (简记为 EFA) 中是可证明的. 参阅 Avigad [2003].[1] 目前还没有独立的证明策略. 也许最有希望的是从 Macintyre 的程序开始, 只要在一定程度上它是成功的, 就试着将其也应用于 EFA.

比起 PA, 对于 EFA 来说, 我们的上述论点更加成立, 这是因为从证明论的角度来说, EFA 要弱得多. 我们可以将其用 Avigad 的话来说 [2003, p. 270]: 某人某日可能在还不能给出任何独立的 "在 EFA 中定理证明的非形式化描述" 时, 却能 "非形式化地证明在 EFA 的某保守扩张中存在形式化的定理证明的." 用我们自己的话来描述这一情形: 保守扩张是事实上用到的, 而 EFA 是原则上用到的. 我们可能终将知道 FLT 的 EFA 证明存在, 尽管这一理解依赖于实际上在保守扩张中描述的证明.

有些人把我看成是 Grothendieck 方法的 "支持者", 并得出结论说我反对从较弱的原理来寻找证明. 这个前提大体上是对的, 结论却是荒谬的. 我不反对寻求任何证明. 但下列事实是改变不了的: Wiles 给出了 FLT 的第 1 个且是 15 年来唯一知道的证明, 而这一证明引用并依赖已发表的明确使用全域的论证. Macintyre 也没有以任何方式反对这个证明! 在 Macintyre 的程序和 Grothendieck 的方法之间存在共鸣, 而不是对抗. Macintyre [2003] 反复鼓励模型论专家多去注意那些方法.[2]

寻找最弱的足以用之证明 FLT 的分离和归纳原理是非常美妙的, 但数论研究生的讨论班上甚至不会教到这些原理. 以数学史为鉴, 我们可以肯定, 随着时间的推移, FLT 的证明会被大大简化, 但这不等于寻求所需的最弱的逻辑原理. 在可预见的将来, 对任何 FLT 的使用较弱算术理论的证明, 最可能发生的情况是, 首先我们发现了一个新证明, 之后通过对这一使用较强逻辑的较短证明应用元定理并加以修改, 我们将这一新证明变为所求的使用较弱理论的证明. 可以说在这个意义下, Wiles [1995] 是一个短的证明.

§3. 上同调数论的思想

在过去的 50 年间, 利用某些称为 *概型* (*scheme*) 的空间, 数论以 *算术代数几何* 的形式取得了巨大的进步. 这要追溯到 Riemann (黎曼), Dedekind (戴德金), 和 Kronecker (克罗内克) 把代数数理解为 Riemann 曲面上的函数, 但它依赖于 Serre (塞尔) 和 Grothendieck 在 1950 年代创建的上同调工具. 从集合论角度来说, 定义概型并不比定义诸如微分流形或 Riemann 曲面的其他类型的空间更难, 但我们这里将跳过所有细节.[3]

任何一组有限个多变量的 Diophantine (丢番图) 方程定义一个概型, 实际上是称为

1) EFA 是只允许没有量词的归纳法, 取后继运算, 加法, 乘法, 以及求幂作为二元算子的 1 阶算术. —— 原注

2) 例如, topos theory on p. 197 及 Grothendieck's Standard Conjectures on p. 211.—— 原注

3) Ellenberg [2008] 作了简单介绍. McLarty [2008] 比较了概型的两个分别利用函子或拓扑空间给出的集合论定义.—— 原注

谱 (*spectrum*) 的一种特殊情形，而一般概型是把相容的谱放在一起修补而得到，正如一个微分流形把 n 维实坐标空间 $\mathbb{R}^n$ 的一些部分修补而成一样. 当一个概型 X 由一个拓扑空间加上某个代数结构表示时，它的点对应于特定形式的 X 的方程. 显然，如果给出整系数多项式方程，则概型在有理数上建立相应的方程，以及对每个素数 p, 相应的模 p 的方程. X 的代数和拓扑表达了这些方程包括它们的解的全部信息 —— 用上同调完美显示的一种形式.[1)]

对概型最简单有用的上同调依赖于概型 X 上 *模的凝聚层* $\mathcal{F}$ 的概念. 将一个层 $\mathcal{F}$ 考虑为一个整个 X 上的算术问题. 最简单的问题是 "选择一个数", 我们这样理解，在 X 的某些点上，"数" 可以是指一个有理数，但在其他点上，它可以指的是一个模 p 的整数，对某个依赖于这个点的素数 p.

我们在这个简单粗略的例子停留片刻，令 $x \in X$ 为一个点，其中 "数" 是一个有理数，$y \in X$ 是附近的一个点，其中 "数" 是模 7 的一个整数. 注意有理数 n/m 有一个合理定义的模 7 整数值，只要表为既约形式的分母 m 不被 7 整除. 我们问题的一个 *局部解* 是在某个区域 $U \subseteq X$ 中每个点有一个 "数" 的相容选择，其中相容性的一个典型要求是：如果在点 x 选取有理数 n/m, 则这个有理数 n/m 模 7 的值必须是在点 y 的选择. 在这个意义下，我们必须在点 x 和 y 选择 "同样的" 解，尽管一个是有理数而另一个是模 7 的整数.

如果把任何层 $\mathcal{F}$ 考虑为放在整个 X 上的一个问题，则 $\mathcal{F}$ 的一个 *局部瓣* 就是在某个区域 $U \subseteq X$ 每个点相容的解的一个选择，而 $\mathcal{F}$ 的一个 *整体瓣* 是在整个 X 上变化着相容性的一个解. 换句话说，整体瓣是 $U = X$ 为整个概型的特殊情形的一个局部瓣. 相对地说，在小区域中做某个问题比较容易，而重要的是在整体上做.

上同调起初是描述拓扑空间 (例如 Riemann 曲面) 的洞 [Totaro, 2008, p. 389–391]. 一个 Riemann 曲面 S 的 1 阶上同调群 $H^1(S)$ 就是用度量 S 上一个形式沿着不同路径的积分有多大差别的方法，来计算 S 中洞的个数. 如果一个 *全纯 1-形式* α 沿 S 中一条路径的积分与同一个形式沿同样端点的另一条路径的积分不同，这两条路径必定包围至少一个洞. 知道了单个全纯 1-形式 α 在 S 上沿不同路径积分可以得到多少个不同结果，就告诉我们有多少个洞. 曲面 S 的这个特征通过深刻的定理，如 Riemann-Roch (罗赫) 定理，控制着 S 上大量复分析问题.

一个概型 X 的上同调可以度量从局部解过渡到整体解的障碍. 依赖于以 X 上的层 $\mathcal{F}$ 的形式提出的 "问题" 的选择，可以有不同方法把 $\mathcal{F}$ 在 X 的两个重叠小区域上的局部解修补在一起，它们在任何 3 个互相重叠的小区域上相容，但它们以不同路径围绕 X 游走时却给出不同的累积结果 —— 所以它们并非在整个 X 上同时相容 —— 就像把一个型 α 在 Riemann 曲面 S 上两个端点之间沿不同路径积分方法的不同可以给出不同的结果. 这样的修补给出局部解，而不是整体解. 1 阶上同调群 $H^1(X, \mathcal{F})$ 就是度量在空间 X 上解问题 $\mathcal{F}$ 时这种情形有多少不同的方式发生，从而以表示出 X 上大量算术的方式，

1) 概型创造出来是为了与上同调一起工作 [McLarty, 2007]. —— 原注

对 X 的 "形态" 给出某种度量. 更高阶的上同调群把这更加精细化.

这听起来可能有点奇怪, 但它的确给出了通往具体情形下的算术信息的一条条理清楚的途径. Wiles 通过凝聚上同调以及其他下面要涉及的更复杂的上同调, 得到了他的通道. 使人感兴趣的层和上同调群通常很小. 它们最多是连续统尺度的, 但却包含了相当复杂的信息. 甚至在转向曲线或高维空间之前, 0 维单个点的算术概型的上同调就已经包括了所有代数数域的 Galois (伽罗瓦) 理论.

§4. Grothendieck 的策略

"我们将不理会任何集合论的困难. 通过使用全域的标准论证, 这些困难总是能被克服." [Fantechi et al., 2005, p. 10]

逻辑学家抱怨人们草率地诉诸集合论的威力, 例如援引选择公理来说明有理数域有代数闭包. 它需要用选择来证明所有域都有代数闭包. 好, 严格地说, 相对于 ZF, 它 *想要* 的是比选择公理弱的 Boole (布尔) 素理想定理. 代数教科书很少说得那么精细. 无论如何, 对于可数的域如有理数域, 整件事没有必要这样复杂.

对逻辑学家, 自然要质疑: 代数几何需要多大的集合. 也许, 这些理论被构建为包括任意大但实际并不感兴趣的概型?[1] 但不, 那不是理由. 甚至小概型和层也引入大的集合, 这是因为下面这个逻辑学家应当感兴趣的观点: Grothendieck 对处理极其复杂的算术数据的策略是在之前从未见过的尺度下创造精确的梳理工具 —— 或, 更准确地, 除了梳理集合整体全域的集合论和范畴论中, 甚至对非常小的概型, Grothendieck 也用我们将要描述的方式把它放进巧妙选择的大环境中. 并不是所有数论学家都喜欢这种观点, 或是愿意思考这个问题. 那些数论学家只是使用他和他的学派的定理.

Grothendieck 定义概型 X 上任何模的层 $\mathcal{F}$ 的上同调使用的并不是 $\mathcal{F}$ 内部细节, 而是 $\mathcal{F}$ 对 X 上所有其他层的关系. 只有当被特定的运算需要时才会用到细节. 用 Grothendieck 自己的话来说, 他处理了 X 上的层的 "巨大的兵器库", 即 "它那 '就在你眼前' 那样显而易见的结构, 也就是 '范畴' 的结构" [Grothendieck, 1985, p. P38]. 他在 [Grothendieck, 1957] 中就已这样做了, 那是数学中被引用最广的文章之一. 给定了一个空间 X, 他选取相关空间和空间上层的一系列范畴, 作为他的简单而清晰地组织起来的用以引导关于 X 证明的工作区域.

他将 "从一个 '单纯的' (naïve) 观点来接近这些范畴, 如同处理集合那样" [Grothendieck and Dieudonné, 1971, p. 19]. 他的目标不是探寻强的集合论公理. 相反, Grothendieck 的目的是使他的几何保持如他所说 "幼稚的 ... 无法矫正的纯真 (naïveté)" [1985, p. P32]. 但在 Bourbaki (布尔巴基) 的集合论上初步工作后, Dieudonné 和 Grothendieck 两人都知道这些范畴在朴素的 ZFC 基本原理下是真类, 而且他们也都知道 Tarski (塔斯基) 的不可达基数. 所以 Grothendieck 决定: "为了避免某些逻辑困难, 我们将接受大全域 (Universe, 首字母大写) 的概念, 它是一个 '足够大的' 集合, 使得其中的惯常集合论的运算不能超出

1) 有些人想弄清这是不是 Hartshorne 用 "极度一般性" [1977, p. xiv] 的意思. 事实上, 他指的是放弃对 Noether (诺特) 环的限制, 这一限制与尺度没有太多关系. Noether 环可以是任何尺度的, 而非 Noether 环可以是任何无限尺度的.—— 原注

它" [Grothendieck, 1971, p. 146].

§5. 超出 ZFC 的第一步

没有人会在不精通标准的研究生教科书 [Hartshorne, 1977] 的情况下，去尝试理解 Wiles [1995]. 作为 Hartshorne 书的中心，第 III 章在上同调上花了 80 页，这些将用来证明该书其余部分的所有几何结果. 他假设通常同调代数的基本定理在研究生教材中没有被证明，并且适于他的目的，他同样也不加以证明 (p. 203). 唯一一个他列出的证明的来源是 Freyd 的书《阿贝尔范畴 (Abelian Categories)》，该书含糊地描述了其基础为 "一种集合论的语言，例如" Morse-Kelley (莫尔斯－凯利) 集合论 (MK), 但该书也在至少一种情形超出这个范围 [Freyd, 1964, p. 14 and 131]. 下面的 §5.1 会对理论 NGB, MK 和 ZFC+U 进行比较.

根据 Grothendieck 的策略，Hartshorne (p. 207) 利用 *整体辫函子* 的导出函子，定义了 X 上模的层 $\mathcal{F}$ 的上同调群无限序列

$$H^0(X,\mathcal{F}),\ H^1(X,\mathcal{F}),\ \ldots,\ H^n(X,\mathcal{F}),\ \ldots.$$

整体辫函子 Γ 从 X 上模的层范畴 $\mathfrak{Mod}(X)$ 映到阿贝尔群的范畴

$$\mathfrak{Mod}(X) \xrightarrow{\Gamma} \mathfrak{Ab}.$$

它把 X 上模的层 $\mathcal{F}$ 映为其整体辫群 $\Gamma(\mathcal{F})$.

导出函子有几个等价的定义，Hartshorne 在联系到特殊问题以及为理论目的时将它们结合起来使用. 最简明的定义是说导出函子是一个 *通用 δ-函子* (universai δ-functor) [Hartshorne, 1977, p. 206]. 对我们不太重要的特殊情况有以下形式：

1. $\mathfrak{Mod}(X)$ 上一个 δ-函子 T^* 是一个无限通常函子序列 $T^i : \mathfrak{Mod}(X) \to \mathfrak{Ab}$ 的，$i \in N$, 加上与 $\mathfrak{Mod}(X)$ 中正合序列有某种关系的自然变换 δ^i.

2. 一个态射 $\eta^* : T^* \to S^*$, 其中 S^* 是 $\mathfrak{Mod}(X)$ 上另一个 δ-函子，是一个适当的自然变换的无限序列 $\eta^i : T^i \to S^i$.

3. 称 $\mathfrak{Mod}(X)$ 上一个 δ-函子 U^* 是 *通用的*, 当对任意 δ-函子 T^*, 每个通常函子的自然变换 $\eta^0 : U^0 \to T^0$ 恰能扩张到一个 δ-函子的态射 $\eta^* : U^* \to T^*$.

在 ZFC 中，范畴 $\mathfrak{Mod}(X)$ 和 $\mathfrak{Ab}$ 以及它们之间的函子都是真类. 上面的这些定义需要量词取遍所有函子. 也许，在 [Hartshorne, 1977] 中的每件事情都能在 NGB 中被形式化，尽管像将在下面的小节 5.1 中指出的那样，NGB 对诸如数学归纳法等熟悉的思想设置了限制. 除了那些限制，在 NGB 中把这些数学形式化还需要围绕某些关于自然的真类族的赘述.

通用 δ-函子的这个刻画显然定义了一个范畴，其对象是 $\mathfrak{Mod}(X)$ 上的 δ-函子，而态射是它们之间的箭头. 事实上，通用 δ-函子被称为 *通用的*, 因为它们是以 δ-函子为定义域的范畴的某个函子的通用对象. 也就是说，这个函子把每个 δ-函子 T^* 映为它的零部分 T^0. 这是这一学科中考虑问题的通常方式. 但 δ-函子和态射的范畴是一个超类，它的每个对象和箭头都是真类. 这样的超类范畴在教科书中通常是隐藏在文字中而从不明确提出的. 这就是我说赘述的意思.

超类范畴在更高级的 Hartshorne [1966] 中被明确提出. 该书用 导出范畴 定义了 δ-函子性, 其中导出范畴的每一单个的态射是一个真类.[1]Hartshorne 对这些超类使用量词, 而同时理所当然地完全隐藏了集合论.

关于 δ-函子范畴的思想是那么明显, 毫无疑问, 它能安全地被隐含保留. 每个 δ-函子范畴仍是真类的一个超类. Hartshorne 的教科书合理地省略了这样一些议题. 该书明确使用的语言只是超出 ZFC 一些, 即 ZFC 的保守扩张 NGB. 如果一旦全域变得不那么令人担心, 也许在研究中用到的组织得更有条理的函子工具将更容易被学生们接受.

§5.1. ZFC 扩张之比较

由于假设一个包含所有集合的类 U 的存在, NGB 和 MK 都扩张了 ZFC. 于是, U 自身不是一个集合; 设想 U 有许多子类, 这些子类作为集合也 "太大", 因而被称为 *真类* (*proper class*). 真类的元素是集合, 而且没有一个真类是 NGB 或 MK 中任何一个族的元素. 重要区别是 NGB 在定义一个类时只允许对集合使用量词, 而 MK 还可以对类使用量词来定义一个类.

ZFC 的任何模型 $\mathcal{M}$ 有一个到 NGB 的极小扩张模型 $\mathcal{M}'$. 在模型 $\mathcal{M}$ 外工作, 我们可以构造一个族 $|\mathcal{M}'|$, 其由所有 $|\mathcal{M}|$ 的在 ZFC 语言中用 $\mathcal{M}$ 中参数可定义的子集组成. 当然, $|\mathcal{M}|$ 中的每个集合 α 由公式 $x_1 \in \alpha$ 定义了它自身, 所以 $|\mathcal{M}| \subsetneq |\mathcal{M}'|$. 以这个较大的域和自然的成员关系, 建立一个模型 $|\mathcal{M}'|$. 所有那些在 $\mathcal{M}$ 中不存在的可定义子集成为 $\mathcal{M}'$ 中的真类. 由于真类不能用于指定 NGB 中任何集合或类, 因此 $\mathcal{M}'$ 已是 NGB 的一个模型, 而不需要再重复扩张. 集合之间的关系在此过程中未作改变, 所以任何在 ZFC 的模型 $\mathcal{M}$ 中关于集合的为真的叙述, 在 NGB 相应的模型 $\mathcal{M}'$ 仍为真.

于是, NGB 是 ZFC 一个保守扩张, 故不能证明 ZFC 的相容性. Mostowski [1950, p. 113] 精确地描述了关键的事实: NGB 可以用所有集合构成的类 U 来表达对 ZFC 公示的 Gödel 编码的真值谓词, 但这一谓词使用了一个对类的 (存在) 量词. 所以在 NGB 中, 这个谓词不能定义一个由 "真实" 公式的 Gödel 编码构成的集合或类. 由于利用这个谓词的公式不能在 NGB 中定义集合或类, 数学归纳法也不能应用于它们, 所以 NGB 用这个谓词几乎做不了什么, 而且它显然不能用来证明 ZFC 的相容性. 而 MK 公理允许类的非直谓定义, 因而能用这个真值谓词来证明 ZFC 的相容性.

ZFC+U 这个扩张则要强得多, 因为它使全域 U 成为一个集合, 其有幂集 $\mathcal{P}(U)$, 这个幂集又有相应的幂集 $\mathcal{P}^2(U)$, 等等, 对每个序数 β, 可以得到更高秩的 $\mathcal{P}^\beta(U)$, 通常写为 $V_\beta(U)$. 根据定义, U 是 ZFC 的模型, 而且可以直接验证幂集 $\mathcal{P}(U)$ 是 MK 的一个模型. U 中秩低于 U 的子集事实上是 U 的所有元素, 且在 MK 的这个模型中作为集合出现, 而与 U 有相同秩的子集则作为真类出现.

§6. Grothendieck 全域

我们已经看到一本标准的教科书利用了 NGB 并暗示了真类构成的超类. 在应用中

1) Carter [2008] 对她的工作给出一个哲学说明, 其使用了同一个 分式范畴 的技巧处理一个从集合论来说较小的几何问题.—— 原注

引用的高级结果利用了类的非直谓定义，这意味着 MK，而不是 NGB. 其他标准文献利用了超类的一种非直谓理论. 这还是比 ZFC+U 弱得多，但是能弱多少则没有可确定的限制，而且也确实没有理由去记录它. 任何试图把数论的逻辑假设极小化的人，原则上都可以用比 ZFC 少得多的东西. 走到 ZFC 之外的理由是，对已发表的证明提供一个安全简单的基础.

和 Grothendieck 一起，我们将全域作为把所有感兴趣的范畴当做集合来处理的一种单纯的方法.[1] 我们避开作为 NGB 和 MK 核心的关于集合和真类的区别，更不用说只差 1 阶的超类和真类的区别. 我们避免讨论可定义性，它们被援引来说明什么时候超类变量可用真类上的明确构造来代替. 可定义性问题对某些问题可能是极有价值的，但我们可以只看那些有价值的情况，而不是把可定义性放进基本原理中. 我们的基本原理 ZFC+U 只是说有一个集合 U，带有一些自然的闭性.

Grothendieck 最喜欢宣称的使用全域的理由是函子范畴.[2] 对范畴 $\boldsymbol{AA}$ 和 $\boldsymbol{B}$，他构建所有从 $\boldsymbol{A}$ 到 $\boldsymbol{B}$ 的函子的范畴 $\boldsymbol{B^A}$. 我们已经看到它们在 EGA III 中的使用隐藏于 Wiles [1995, p. 486–487] 一个关键步骤之后. 依赖于我们怎样用集合来定义范畴，在集合论的意义下，其任何使用都是在比 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 高 1 或几个秩. 不过，当接下来我们对另一个函子范畴 $\boldsymbol{C^{(B^A)}}$ 时，可能还需要更高的秩. Grothendieck 倾向于把所有这些都作为集合来处理. 而全域 U 使他能够这样做. 只要初始范畴不比 U 大 (从 ZFC 的观点，它们不比真类大)，则所有有限次迭加的函子范畴都将是 ZFC+U 中的集合.

集合论意义下大的 *场所* (*site*) 处于在原始的算术应用和一般理论的交接点上. 拓扑空间的上同调利用 T 的所有开子集的集合 $\mathrm{Ouv}(T)$ 处理任何拓扑空间 T，这些构成那个上同调的 *场所*. 它们构成一个不大于 T 的点集的幂集的集合. 如同上述 §3—5 描述 Hartshorne [1977] 所做的那样，Wiles [1995] 在这个框架内工作. 但 Mumford (芒福德) 和 Tate [1978] 给出一个优美的简要说明，即原始的算术应用怎样运用一个概型 X 的 *艾达尔* (*étale*) *上同调*，它用 *艾达尔映射* $X' \to X$ 代替 X 的开子集. 它们共同构成对 X *微小的* (*petit*) *艾达尔场所*. 这里的单词 "petit" 是针对 *重大的* (*gros*) 和 *微小的* 艾达尔场所之间的代数 – 几何区别. 它不是基于集合论的尺度来考虑的. 从 ZFC 的观点，一个概型的微小艾达尔场所不是一个集合，而是一个真类. Grothendieck 提到几个技术性的诀窍来避免这些真类，也提到这些诀窍在实践中的不方便，并断言这个集合论的大场所是适合于艾达尔上同调的 (SGA 4, p. 307).

集合论的大场所的运用以真类代替了 §3—5 描述的许多集合，因此以超类代替了这几节中的大多数真类. 它以 ZFC 上的你可以任意命名的高于 ZFC3 秩的超类族代替了我们谈到的所有超类. 像之前一样，如果目的是寻找在原理上足以给出算术证明的最弱逻

1) 关于采用全域的最近一次数学讨论，参阅 Lurie [2009, p. 50f.]，并注意许多全域是作为强不可达基数而存在. Lurie 遵循通常的做法，只假设 "足够多的" 逐次大的全域，而不去跟踪想要多少.—— 原注

2) Grothendieck [1971, p. 146f.] 机敏地承诺 Claude Chevalley 和 Pierre Gabriel 将在 2000 年给出一个最终处理. 在那之前，他提供了自己的 [1957] 作为替代，他也注意到即使对于他的目的，这也是非常不完全的.—— 原注

辑，则这些都是不必要的．在此我们有不同的目的，即把证明形式化为它们发表时的那样．当你已经越过 ZFC 时，就没有理由因不使用全域而止步．

§7. Deligne 和 SGA $4\frac{1}{2}$

Deligne [1977] 对艾达尔上同调提供了一种专家级的介绍，从而鲜少提到高级技巧．奇怪的是，有些人认为这本书使 Deligne 关于 Weil 最后猜想的证明独立于全域，也独立于别的 SGA．

该书明显地用了集合论大场所 [1977, p. 23]，也以其他方式隐含地用到了全域．其目的是 "比 SGA 4 更清楚 ... 但并不断言给出一个完全的证明" (p. 2)．对诸如 Poincaré (庞加莱) 对偶性和迹公式这样的必要步骤的证明，Deligne 引用了他自己在 SGA 4 中的论文，其中明显地用到了全域．该书意在对 Deligne 关于 Weil 最后猜想的证明给出一个充分的工作背景，其仅仅包含基于拓扑空间的某种上同调加上 "一些信念" (un peu de foi) (p. 1)．但 Deligne 从未暗示过信念最终会代替证明．

虽然 Deligne 经常使用全域，他在交谈时强调它们只是便利的工具，在技术上是可以用 ZFC 代替而消除的．在实践中用到的一般定理总是可用小场所上的独特的层给出 (其中 "小" 是指在 ZFC 中证明性地存在)，甚至不用去看整个层的范畴，更不用说它们的范畴的范畴，等等．这是一种从数论或其他任何地方中的 Grothendieck 上同调把全域的使用消除的诀窍．尽管在实践中很明显可以做到这一点，在文献中却没有这样做过，而且这些从来没有被陈述为一个精细的元定理．任何对此感兴趣的人应该尝试一下给出这个元定理．

利用这样的手段，杰出的上同调证明如 Deligne [1974]，或 Faltings [1983]，或 Wiles [1995] 都不需要走出 ZFC．但事实上已经完成并发表的这三者都用了 Grothendieck 的工具．他们或者引用了 EGA 和 SGA 中利用全域的证明，或者引用了采用这些证明的原始资料．

关键在于数学不仅仅是技巧性的．Deligne [1998] 解释了 Grothendieck 高水平系统性的实际价值，特别是拓扑斯 (toposes) 的价值．他解释说，Grothendieck 不会去描述单个的结构，而是去描述一个范畴，它构成围绕所有单一结构的工作场所．Grothendieck 不仅对每个非常小的在几何或算术上合理定义的交换环定义了概型，而且对所有交换环定义了概型：

"如果让每个交换环定义一个概型的决定会引起各种怪诞的 概型，那么允许这样做就提供了具有良好性质的一个概型的 范畴." [Deligne, 1998, p. 13]

这一范畴是一个容易且自然的研究概型的手段．而 Grothendieck 不仅仅在一个给定概型上非常小的在几何或算术上合理的层上工作，而且在这个概型上所有层的拓扑斯上工作，因为这导向上同调作为一个 δ-函子的正确而自然的定义：

"Grothendieck 已经证明，给定层的一个范畴,[1] 就产生了上同调群的概念." [Deligne, 1998, p. 16]

1) 即一个 Grothendieck 拓扑斯.—— 原注

在最近一次谈话中, Deligne 对母题 (motives) 给出了同样的观点: Grothendieck 并不寻求用内部细节来定义母题, 而是用它们在母题的范畴中的内在关系来定义. 参阅 [Deligne, 2009, minute 5].

就是这一策略造就了当代的上同调数论. 目的根本不是定位大范畴. 而是定位适当的范畴, 从而可以像处理集合那样来处理它们. 目前已知的唯一简单的概念上的方法就是利用全域 —— 从原理上这是可以消除的, 要付出的代价是使工作复杂化.

§7.1. 一个对元定理的可能策略

也许, 用 "小全域" 代替全域, Grothendieck 上同调理论的总体性质可以在 ZFC 内部保留. 小全域是指集合 V_β, 其中 β 是在 ZFC 中可证明存在的极限序数. 它们可以作为除去替代公理范式外的 ZFC 的模型. 但为了可以开展工作, 这个极限序数 β 必须大到足以包括所有超限归纳法所需要的范围, 尤其在证明中某些范畴有 "足够多的内射模" 时 [Grothendieck, 1957]. 如果能在 ZFC 中证明, 对于任意给定的场所, 某个极限序数 β 足以界定对那个场所的上同调所需要的所有归纳法, 则利用替代公理, 存在适当的 β, 对任何场所集合都适用. 而上同调数论中每一单个的证明最多只用到一个场所集合. 所以, 如果这个困难能被克服, 则这些证明中的每一个都可在 ZFC 内部给出, 而不会对证明在理论上的系统性造成任何感觉得到的损害.

§8. 函子性和弱证明

任何人都愿意尽其所能地来精简数论 (或任何数学) 中的任何证明. 对许多数论学家来说, 这包括了弃用函子工具. 所有数论学家都参与了 Lenstra 解方程的目标, 但许多人并没有分享他的乐趣:

"Hendrik Lenstra 在会议演讲中再次说明, 他在 20 年前坚定地认为他 *确实* 想解 Diophantine 方程, 但他 *确实不* 想表示函子 —— 而现在他为发现自己为了解 Diophantine 方程而表示函子感到很开心 !" [Mazur, 1997, p. 245, 原文中强调] [1)]

有趣的东西是真实的. 函子使算术变得容易就是证据. 事实上, 从现在来看, 是函子使得 Wiles 的证明变得可能.

在 Wiles 的证明以及大量其他数论问题中的主要函子工具是 *群的上同调*.[2)] 它对每个群 G 以及带 G 作用的阿贝尔群 A, 指定了上同调群的一个无限序列

$$H^0(G,A),\ \ H^1(G,A),\ \ H^2(G,A),\ \ \ldots$$

Washington [1997, p. 103] 解释了 Wiles 的证明怎样主要用了前 3 项 H^0—H^2, 描述了它们具体的算术意义. 同时, 他解释了这些群怎样作为一个无限函子序列 H^n 中函子 H^0, H^1, H^2 的值而出现, 与拓扑上同调极其相似.

看过证明的人都不怀疑这个上同调, 和 Wiles [1995] 的其余部分, 当在比自然数秩大出约为 7 或 8 的集合上工作时, 可以常规地展开. 虽然同时它会对理论系统性产生目前未知的损害. 这一过程不需要解决任何新的算术问题, 而只需消除上同调中目前还未

1) 引文有误, 原文为 "..., and that he DID NOT wish to represent functors..." —— 校注

2) 关于这个上同调的起源, 参阅 [Mac Lane, 1988] 以及更多历史细节 Basbois [2009]. —— 原注

知的大量的一般定义 (当然, 它们互相嵌套而出现), 并替代为适用于算术中特定应用的形式. 这种常规的消除比 Macintyre 的规划弱得多, 因为它用了强得多的逻辑. 它对每个秩都假设完全分离, 并对归纳法中使用的公式不加限制.

Macintyre 给出下列强得多的关于上同调的论断 "根本没有证据显示基的改变或迹公式有任何本质上高阶的内容" 时 [即将发表, MS p. 14–15].[1] 这些定理每一次的使用都代表了算术中一次相当明确的计算. 这些使用很可能要么在 PA 自身中展开, 要么能在 PA 的一个高阶的保守扩张中被证明, 此时这一扩张中对归纳法和分离公理确有类似 [Takeuti, 1978] 的限制. 这就解决了 Macintyre 的关于 FLT 和 Gödel 现象无关的断言 —— 即其与任何需要比 PA 更强公理才能得出的算术事实无关.

Macintyre 提出了证据, 而且说明他的断言如何需要用算术中大量进一步的工作来验证. 这个工作可以是非常有启发性的, 而且很可能是不容易的. 除了对使用全域的一般定理以外, 最具体的对群上同调的需求出现在当它们面对高于自然数集几个秩的集合时. H^1 的一个具体版本是从一个 Galois 群到它的数域的交叉同态的等价类的群. 在 PA 或到 PA 的一个高阶保守扩张中得到关于这个群的必要事实将不是常规的练习. 它将要求严肃的新算术.

§9. 基本原理

"基本原理的意义不是为了任意地限制探究, 而是要提供一个框架, 从而我们可在其中合理地执行那些从数学上说是有趣和有用的构造和运算."

——Herrlich and Strecker [1973, p. 331]

"真正有趣的基本问题是在整数中寻找大全域的真不可移除性 (genuine unremovability). 事实上, 目前我们还未能找到关于有限秩集合的任何陈述, 使得其导出大全域的真不可移除性! 这是因为, 例如关于实数投影集合的正规性质要么能在 ZFC 中证明, 要么需要远在大全域之外的大基数."

——Friedman post Apr 8, 1999 on FOM[2]

Wiles [1995] 中的大量注释和索引在某一天可能不再受重视, 而以 PA 更直接的使用来代替. 这将极不容易, 而且我们不可能知道离这一天还有多远. 同时, 将有关函子的内容变得更灵活和更容易被接受 —— 用 Grothendieck 的术语, 更 "单纯"—— 的进程将会继续. 这也一样极不容易, 而且我们同样不可能知道离这些还有多远. 不论逻辑学家怎样考虑它们, 这两个计划将继续进行, 就如它们正在进行的那样. 它们都将推动算术的发展.

虽然如此, 目前来说, 我们还是必须求助于高水平的系统性, 就像 Wiles 所做的那样, 因为他需要用之完成证明. 我们被引向 EGA III, SGA 1 和 SGA 4, 因为它们是 Wiles 证明的源头. 我们抵达了全域.

我们想就基本原理再多说一点. 我们研究了什么逻辑在数学中是合理的. 我们试图证明或驳倒关于有限秩集合的陈述的各种强集合论公理的真不可移除性. 我没有打算为

1) 已在 2011 年发表, 见参考文献.—— 译注

2) 引自 FOM 电子邮件列表, Friedman 题为 "利用全域? 专家再次评述" 的邮件, 1999 年 4 月 8 日星期四 cs.nyu.edu/pipermail/fom.—— 原注

Friedman 关于这一点的笼统断言辩护，但我完全同意上同调数论并没有提供全域的这种不可移除性. 我怀疑任何对这个学科有兴趣的人会认为这可能发生. 然而这一数论利用全域提供了大量合理的，有趣的和有用的构造和运算 —— 如果我们同意 Wiles [1995] 事实上所用的一切都是合理的，有趣的和有用的.

参考文献

[1972] M. Artin, A. Grothendieck, and J.-L. Verdier, Théorie des topos et cohomologie etale des schémas, Séminaire de Géométrie Algébrique du Bois-Marie, 4, Springer-Verlag, 1972, three volumes, generally cited as SGA 4.

[2003] J. Avigad, Number theory and elementary arithmetic, Philosophia Mathematica, vol. 11 (2003), pp. 257–284.

[2009] N. Basbois, La naissance de la cohomologie des groupes, Ph.D. thesis, Université de Nice Sophia-Antipolis, 2009.

[2008] J. Carter, Categories for the working mathematician: Making the impossible possible, Synthese, vol. 162 (2008), pp. 1–13.

[1997] G. Cornell, J. Silverman, and G. Stevens (editors), Modular forms and Fermat's Last Theorem, Springer-Verlag, 1997.

[1974] P. Deligne, La conjecture de Weil I, Publications Mathématiques. Institut de Hautes Études Scientifiques, (1974), no. 43, pp. 273–307.

[1977] P. Deligne (editor), Cohomologie étale, 1977, 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.

[1998] _____, Quelques idées maîtresses de l'œuvre de A. Grothendieck, Matériaux pour l'histoire des mathématiques au XX^e siècle (Nice, 1996), Société Mathématique de France, 1998, pp. 11–19.

[2009] _____, Colloque Grothendieck, Pierre Deligne, vidéo by IHES Science, on-line at www. dailymotion.com/us, 2009.

[1973] P. Deligne and M. Rapoport, Les schémas de modules de courbes elliptiques, Modular functions of one variable, II, Lecture Notes in Mathematics, vol. 349, Springer-Verlag, New York, 1973, pp. 143–316.

[2008] J. Ellenberg, Arithmetic geometry, Princeton companion to mathematics (T. Gowers, J. Barrow-Green, and I. Leader, editors), Princeton University Press, 2008, pp. 372–383.

[1983] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Inventiones Mathematicae, vol. 73 (1983), pp. 349–366.

[2005] B. Fantechi, A. Vistoli, L. Gottsche, S. L. Kleiman, L. Illusie, and N. Nitsure, Fundamental algebraic geometry: Grothendieck's FGA explained, Mathematical Surveys and Monographs, vol. 123, American Mathematical Society, Providence, 2005.

[1964] P. Freyd, Abelian categories: An introduction to the theory of functors, Harper and Row, 1964, reprinted with author commentary in: Reprints in Theory and Applications of Categories, (2003), no. 3, pp. 25–164, available on-line at www.emis.de/journals/TAC/reprints/articles/3/tr3abs.html.

[1957] A. Grothendieck, Sur quelques points d'algèbre homologique, Tôhoku Mathematical Journal, vol. 9 (1957), pp. 119–221.

[1971] _____, Revêtements étales et groupe fondamental, Séminaire de Géométrie Algébrique du Bois-Marie, 1, Springer-Verlag, 1971, generally cited as SGA1.

[1985] _____, Récoltes et semailles, Université des Sciences et Techniques du Languedoc, Montpellier, 1985, published in several successive volumes.

[1961] A. Grothendieck and J. Dieudonné, Éléments de géométrie algébrique III: Étude cohomologique des faisceaux cohérents, Publications Mathématiques. Institut des Hautes Études Scientifiques, Paris, (1961), no. 11.
[1971] _____, Éléments de géométrie algébrique I, Springer-Verlag, 1971.
[1966] R. Hartshorne, Residues and duality, lecture notes of a seminar on the work of A. Grothendieck given at Harvard 1963–64, Lecture Notes in Mathematics, no. 20, Springer-Verlag, New York, 1966.
[1977] _____, Algebraic geometry, Springer-Verlag, 1977.
[1973] H. Herrlich and G. Strecker, Category theory, Allyn and Bacon, Boston, 1973.
[2009] J. Lipman and M. Hashimoto, Foundations of Grothendieck duality for diagrams of schemes, Springer-Verlag, 2009.
[2009] J. Lurie, Higher topos theory, Annals of Mathematics Studies, no. 170, Princeton University Press, Princeton, 2009.
[1988] S. Mac Lane, Group extensions for 45 years, Mathematical Intelligencer, vol. 10 (1988), no. 2, pp. 29–35.
[2003] A. Macintyre, Model theory: Geometrical and set-theoretic aspects and prospects, this Bulletin, vol. 9 (2003), no. 2, pp. 197–212.
[forthcoming] _____, The impact of Gödel's incompleteness theorems on mathematics, Horizons of truth: Proceedings of Gödel's centenary, Vienna, 2006, forthcoming.[1)]
[1977] B. Mazur, Modular curves and the Eisenstein ideal, Publications Mathématiques. Institut des Hautes Études Scientifiques, vol. 47 (1977), pp. 133–186.
[1997] _____, Introduction to the deformation theory of Galois representations, Modular forms and Fermat's Last Theorem (G. Cornell, J. Silverman, and S. Stevens, editors), Springer-Verlag, 1997, pp. 243–312.
[2007] C. McLarty, The rising sea: Grothendieck on simplicity and generality I, Episodes in the history of recent algebra (J. Gray and K. Parshall, editors), American Mathematical Society, 2007, pp. 301–326.
[2008] _____, "There is no ontology here": visual and structural geometry in arithmetic, The philosophy of mathematical practice (P. Mancosu, editor), Oxford University Press, 2008, pp. 370–406.
[1950] A. Mostowski, Some impredicative definitions in the axiomatic set theory, Fundamenta Mathematicae, vol. 37 (1950), pp. 111–124.
[1978] D. Mumford and J. Tate, Fields Medals IV. An instinct for the key idea, Science, vol. 202 (1978), pp. 737–739.
[2008] B. Osserman, The Weil conjectures, Princeton companion to mathematics (T. Gowers, J. Barrow-Green, and I. Leader, editors), Princeton University Press, 2008, pp. 729–732.
[1978] G. Takeuti, A conservative extension of Peano Arithmetic, Two applications of logic to mathematics, Princeton University Press, 1978, pp. 77–135.
[2008] B. Totaro, Algebraic topology, Princeton companion to mathematics (T. Gowers, J. Barrow-Green, and I. Leader, editors), Princeton University Press, 2008, pp. 383–396.
[1997] L. Washington, Galois cohomology, Modular forms and Fermat's Last Theorem (G. Cornell, J. Silverman, and S. Stevens, editors), Springer-Verlag, 1997, pp. 101–120.
[1995] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, Annals of Mathematics, vol. 141 (1995), pp. 443–551.

(李福安 译　　吴刘臻 校)

1) 该文已发表：A. Macintyre, The impact of Gödel's incompleteness theorems on mathematics, Kurt Gödel and the foundations of mathematics, 3–25, Cambridge Univ. Press, Cambridge, 2011.——译注