"`There is no ontology here': visual and structural geometry in today's Arithmetic,"

in press for Paolo Mancosu ed. *The Philosophy of Mathematical Practice*, Oxford University Press, 2008.

“THERE IS NO ONTOLOGY HERE”: VISUAL AND STRUCTURAL GEOMETRY IN ARITHMETIC

COLIN MCLARTY

> In Diophantine geometry one looks for solutions of polynomial equations which lie either in the integers, or in the rationals, or in their analogues for number fields. Such polynomial equations $\{F_i(T_1,\dots\ T_n)\}$ define a subscheme of affine space $\mathbb{A}^n$ over the integers which can have points in an arbitrary commutative ring R. (Faltings, 2001, 449)

Structuralists in philosophy of mathematics can learn from the current heritage of the ancient arithmetician Diophantus. A list of polynomial equations defines a kind of geometric space called a *scheme*. By one definition these schemes are countable sets built from integers in very much the way that Leopold Kronecker approached pure arithmetic. In another version every scheme is a functor as big as the universe of sets. The two versions are often mixed together because they give precisely the same structural relations between schemes. The practice was vividly put by André Joyal in conversation: “There is no ontology here.” Mathematicians work rigorously with relations among schemes without choosing between the definitions. The tools which enable this in principle and require it in practice grew from topology.

The three great projects for 20th century mathematics were to absorb Richard Dedekind’s and David Hilbert’s algebra, to absorb Henri Poincaré’s and Luitzen Brouwer’s topology, and to create functional analysis.[1] Algebra and topology made explosive advances when Emmy Noether initiated a series of ever-deeper structural unifications. Her group theory became the method of *homology* of spaces. When abstract algebra spread from advanced number theory into basic topology it became a contender for organizing all of mathematics, as Noether intended. Her protégé Bartel van der Waerden advanced the new hegemony in his *Moderne Algebra* (1930). Bourbaki based their encyclopedic work on van der Waerden’s text (Corry, 1996, pp. 309ff.). This “structural” mathematics was the research norm by the 1950s and the textbook norm by the 1960s. Homology itself continues expanding and linking Dedekind and Poincaré to the latest Fields Medals.[2]

This case study looks at *schemes*, which arose largely in pursuit of a single problem, namely the *Weil conjectures*, a series of elegant conjectures on counting the solutions to certain arithmetic equations (Weil, 1949).[3] Weil sketched a fascinating strategy for a proof if only the *Lefschetz fixed point theorem* from topology would apply in arithmetic. It was a brilliant idea with repercussions all across mathematics but only a handful of leading mathematicians thought it could possibly work.

[1]Functional analysis also joined the structural unification (Dieudonné, 1981). Leading workers in all three projects contributed to mathematical logic.

[2]See notably Mumford and Tate (1978); Lafforgue (2003); Soulé (2003).

[3]Chapters 7–11 of Ireland and Rosen (1992) introduce the arithmetic aspect of the conjectures.

Philosophical ideas of "structuralism" in and out of mathematics could go deeper than they have before by absorbing some general features of scheme theory, the proof of the Weil conjectures, and much other 20th century mathematics:

- Structuralist tools are the feasible method of highlighting intuitive and relevant information on each structure as against technical nuts and bolts.
- Single structures matter less than the *maps* or *morphisms* between them.
- Maps and structures are often best understood by placing them in higher level structures: "Patterns themselves are *positionalized* by being identified with positions of another pattern" (Resnik, 1997, p. 218).
- Maps are often richer and more flexible than functions. In set theoretic terms they are often more complicated than functions while in structural terms they often form simpler more comprehensible patterns.

Intuition develops as knowledge does. The *Chinese remainder theorem* is an accessible example from number theory. Logicians use it in arithmetizing syntax (Gödel, 1967, p. 611). Georg Kreisel saw its "mathematical core in the combinatorial or constructive aspect of its proof" which suits its role in proving Gödel's incompleteness theorem but he added:

> I realize that there are other points of view. E.g. a purely abstract point of view: Jean-Pierre Serre once told me that he saw the mathematical core of the Chinese remainder theorem in a certain result of cohomology theory. (Kreisel, 1958, p. 158)

We will see, though, that cohomology is not "abstract." It is geometrical.

Section 1 sketches Kronecker's and Noether's arithmetic. Section 2 shows how Noether's algebra organized Poincaré's topology and illustrates the centrality of maps. Poincaré emphasized single spaces. Noether emphasized the pattern of spaces and maps which was soon captured as the category **Top** of topological spaces which in turn became one object in the pattern of categories and functors i.e. the category **CAT** of categories. Homology today uses patterns where each single position is a functor from one category to another and the maps are *natural transformations* (Mac Lane, 1986, p. 390). The rising levels are sketched in Sections 2.2 and 2.4 while section 2.3 illustrates the Lefschetz fixed point theorem. Sections 3 and 4 introduce schemes and give the Chinese remainder theorem in classical and cohomological forms.

The final section focusses on three points that philosophy of mathematics ought to learn from the past century's practice: first the rising levels of structure directly aid intuition; second practice relies on the generality of categorical morphisms as against the set theoretic functions favored by most philosophers of mathematics today; and third the interplay of levels raises conceptual questions on identity. In particular categorists currently debate the importance of equality versus isomorphism, as discussed in Sections 5.3–5.5.

1. Diophantine equations

1.1. **Kronecker's treatment of irrationals.** Diophantus sought positive integer and rational solutions to arithmetic equations. Sometimes he would explore a problem far enough to show in our terms that the solution (or its square) is negative. Then he says there is no solution. When a problem leads towards a positive irrational solution "he retraces his steps and shows how by altering the equation he can get a new one that has rational roots" (Kline, 1972, p. 143). Perhaps he rejected irrationals although they had been studied for centuries before him (Fowler, 1999). Perhaps he just enjoyed rational arithmetic. Perhaps he was like modern mathematicians who appreciate the irrational solutions to $X^n + Y^n = Z^n$ but also worked for centuries to see if it has non-zero rational ones. His motives are as hard to tell today as the date of his life, which is only known to lie between 150BC and 350AD (Knorr and Mancosu, 1988).

His book *Arithmetica* was cutting edge mathematics in 1650, though, as Fermat worked from it and sparked a rebirth of Diophantine arithmetic. Today this uses irrational and complex numbers in two different ways. The subject called *analytic number theory* uses complex function theory. Even now it is mysterious why deep theorems of calculus should reveal so much arithmetic, although the formal techniques are well understood.[4] The other use of irrational and complex numbers, *algebraic number theory*, was unmysterious by the mid-19th century. Or, better, it was no more mysterious than arithmetic itself. It only added algebra.

For an infamously seductive example let ω be a complex cube root of 1 so that $1 + \omega + \omega^2 = 0$.[5] The degree 3 Fermat equation $X^3 + Y^3 = Z^3$ factors as:

$$(X + Y)(X + Y\omega)(X + Y\omega^2) \quad = \quad Z^3$$

Just multiply out the left hand side and use the equation on ω. In fact prime factorization holds for numbers of the form $a_0 + a_1\omega$ with ordinary integers a_0, a_1 and this helps to prove that the degree 3 Fermat equation has no non-trivial solutions. Prime factorization fails for the numbers formed using some primes p in place of 3 so this reasoning cannot prove Fermat's Last Theorem. But the method made great advances on Fermat and many other problems (Kline, 1972, p. 819f.).

Kronecker would replace ω with the arithmetic of polynomials

$$P(X) \;=\; a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + a_nX^n$$

where $a_0 \ldots a_n$ are ordinary integers; and X is merely a variable. We say polynomials $P(X)$ and $Q(X)$ are congruent *modulo* $1 + X + X^2$, and we write

$$P(X) \equiv Q(X) \pmod{1 + X + X^2}$$

if and only if the difference $Q(X) - P(X)$ is divisible by $1 + X + X^2$. In particular

$$X \not\equiv 1 \pmod{1 + X + X^2}$$

since clearly $1 - X$ is not divisible by $1 + X + X^2$. And yet

$$X^3 \equiv 1 \pmod{1 + X + X^2} \qquad \text{because} \qquad 1 - X^3 = (1 - X)(1 + X + X^2)$$

This arithmetic reproduces the algebra of ω only writing X for ω and congruence modulo $1 + X + X^2$ for $=$. Of course the complex number ω also fits into an analytic theory of the whole complex number plane. This analytic context is lost, as Kronecker intended, when we restrict attention to integer polynomials.

As another example the *Gaussian integers* are complex numbers $a_0 + a_1 i$ where a_0, a_1 are ordinary integers. Replace them with polynomials modulo $1+X^2$, writing

$$P(X) \equiv Q(X) \pmod{1 + X^2}$$

---

[4] Mazur conveys the depth of both mystery and knowledge in one famous case (1991).

[5] Cube roots of 1 are the roots of $1 - X^3$ which factors as $(1 - X)(1 + X + X^2)$. So 1 is a cube root of itself, and the two complex cube roots satisfy $1 + \omega + \omega^2 = 0$. The quadratic formula shows the complex roots are $\omega = (-1 \pm \sqrt{-3})/2$.

if and only if $Q(X) - P(X)$ is divisible by $1 + X^2$. In particular

$$X^2 \equiv -1 \pmod{1 + X^2}$$

Other congruence relations give all the *number fields* mentioned in Faltings' quote above. Kronecker would even banish negative numbers by replacing -1 with a variable Y modulo the positive polynomial $1 + Y$ (Kronecker, 1887*a*,*b*).

1.2. **The theology of numbers.** It is worth a moment to put Kronecker's famous saying in context:

> Many will recall his saying, in an address to the 1886 Berliner Naturforscher-Versammlung, that "the whole numbers were made by dear God (*der liebe Gott*), the rest is the work of man." (Weber, 1893, p. 15)

Kronecker elsewhere reversed this to say we make the whole numbers and not the rest. He endorsed Gauss in print:

> The principal difference between geometry and mechanics on one hand, and the other mathematical disciplines we comprehend under the name of "arithmetic," consists according to Gauss in this: the object of the latter, number, is a *pure* product of our mind, while space as well as time has reality also *outside* of our mind which we cannot fully prescribe a priori. (Kronecker, 1887*b*, p. 339)

The late Walter Felscher has pointed out that:

> "lieber Gott" is a colloquial phrase usually used only when speaking to children or illiterati.[6] Addressing grown-ups with it contains a taste of being unserious, if not condescending. . . ; no priest, pastor, theologian or philosopher would use it when expressing himself seriously. There is the well known joke of Helmut Hasse who, having quoted Kronecker's dictum on page 1 of his yellow *Vorlesungen über Zahlentheorie* (1950), added to the index of names at the book's end under the letter L the entry "Lieber Gott p. 1." (26 May 1999 post to the list *HistoriaMatematica* archived at mathforum.org.)

Kronecker was not serious about the theology of numbers. He was serious about replacing irrational numbers with the "pure" arithmetic of integer polynomials.

1.3. **One Diophantine equation.** Consider this Diophantine equation

$$Y^2 = 3X + 2 \tag{1}$$

Calculation modulo 3 will show it has no integer solutions. Say that integers a, b are congruent modulo 3, and write

$$a \equiv b \pmod 3$$

if and only if the difference $a - b$ is divisible by 3. The key here is that congruent numbers have congruent sums and products.

Theorem 1. *Suppose* $a \equiv b$ *and* $c \equiv d \pmod 3$. *Then*

$$(a + c) \equiv (b + d) \quad \textit{and} \quad (a \cdot c) \equiv (b \cdot d) \pmod 3$$

[6] The phrase is famous in classical music but searches of WorldCat confirm that "lieber Gott" in 19th century prose was generally folkloric or aimed at children.

Proof. Suppose 3 divides both $a-b$ and $c-d$. The claim follows because

$$(a+c)-(b+d) \;=\; (a-b)+(c-d)$$
$$(a\cdot c)-(b\cdot d) \;=\; (a-b)\cdot c \;+\; b\cdot(c-d) \qquad \square$$

If Equation 1 had an integer solution $X=a,\ Y=b$ then the sides would also be congruent modulo 3

$$b^2 \equiv 3a+2 \equiv 2 \pmod 3$$

But b is congruent to one of $\{0,1,2\}$ modulo 3. By Theorem 1 the square b^2 is congruent to the square of one of these. And none of these squares is 2 modulo 3:

$$0^2 \equiv 0 \qquad 1^2 \equiv 1 \qquad 2^2 \equiv 4 \equiv 1 \pmod 3$$

So a,b cannot be an integer solution to Equation 1.

For future reference notice Equation 1 does have solutions modulo other integers. For example $X=2,\ Y=1$ is a solution modulo 7 since

$$1^2 \;\equiv\; 1 \equiv\; 8 \equiv\; 3\cdot 2+2 \qquad \pmod 7$$

And the equation has solutions of other forms. For example, in numbers of the form $a+b\sqrt{2}$ with ordinary integers a,b there is a solution $X=0,\ Y=\sqrt{2}$ since

$$(\sqrt{2})^2 = 3\cdot 0+2$$

1.4. **Arithmetic via morphisms.** This reasoning can be organized in the ring $\mathbb{Z}/(3)$, the *quotient ring* of $\mathbb{Z}$ by 3, which is the set $\{0,1,2\}$ with addition and multiplication by casting out 3's:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Construing Equation 1 in $\mathbb{Z}/(3)$ makes 3=0 and so gives $Y^2=2$. The multiplication table shows $0,1$ are the only squares in $\mathbb{Z}/(3)$. So Equation 1 has no solutions in $\mathbb{Z}/(3)$. Next, consider the function $r\colon\mathbb{Z}\to\mathbb{Z}/(3)$ taking each integer to its remainder on division by 3. So

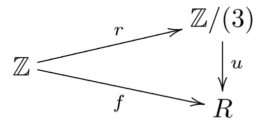
$$r(0)=r(3)=0 \qquad r(2)=r(8)=2 \qquad \text{and so on}$$

By Theorem 1, this preserves addition and multiplication. So it would take any integer solution to any polynomial equation over to a solution for that same equation in $\mathbb{Z}(3)$. Since Equation 1 has no solutions in $\mathbb{Z}(3)$, it cannot have any in $\mathbb{Z}$ either.

The watershed in "modern algebra" came when Noether reversed the order of argument. Instead of beginning with arithmetic she would deduce the arithmetic from purely structural descriptions of structures like $\mathbb{Z}/(3)$ (Noether, 1926). In the case of $\mathbb{Z}/(3)$ this meant looking at arbitrary rings and ring morphisms: A ring R is any set with selected elements 0,1 and operations of addition, subtraction and multiplication satisfying the familiar associative, distributive, and commutative laws.[7] A *ring morphism* $f\colon R\to R'$ is a function preserving $0,1$ addition and multiplication. Noether would rely on the following:

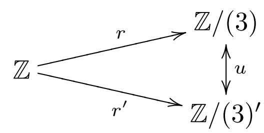
[7]See Mac Lane (1986, pp. 39, 98) or any algebra text. All rings in this paper are commutative.

Fact on $\mathbb{Z}/(3)$**.** *The ring morphism* $r\colon\mathbb{Z}\to\mathbb{Z}/(3)$ *has* $r(3)=0$ *and: For any ring* R *and ring morphism* $f\colon\mathbb{Z}\to R$ *with* $f(3)=0$ *there is a unique morphism* $u\colon\mathbb{Z}/(3)\to R$ *with* $ur=f$*.*



This Fact in no way *identifies* the elements of $\mathbb{Z}/(3)$. It says how $\mathbb{Z}/(3)$ fits into the pattern of rings and ring morphisms. It implies there are exactly three elements and they have specific algebraic relations to each other. It does not say what the elements are. Noether's school specified them in various ways: as the integers 0,1,2, or else as congruence classes of integers, or else as integers taken with congruence modulo 3 as a new equality relation. Saunders Mac Lane contrasted those last two approaches.[8] Noether could have defined $\mathbb{Z}/(3)$ in some such way and proved the Fact from the definition; but in practice the Fact was her working definition. She knew it characterized $\mathbb{Z}/(3)$ up to isomorphism:

Theorem 2. *Suppose a ring* $\mathbb{Z}/(3)$ *and morphism* r *satisfy the Fact on* $\mathbb{Z}/(3)$*, as do another* $\mathbb{Z}/(3)'$ *and* r'*. Then there is a unique ring isomorphism* $u\colon\mathbb{Z}/(3)\to\mathbb{Z}/(3)'$ *such that* $ur=r'$*.*



Proof. Since $r'(3)=0$, the assumption on $\mathbb{Z}/(3)$ and r says there is a unique morphism u with $ur=r'$. Since $r(3)=0$, the assumption on $\mathbb{Z}/(3)'$ and r' says there is a unique $v\colon\mathbb{Z}/(3)'\to\mathbb{Z}/(3)$ with $vr'=r$. The composite vu is a ring morphism with $vur=vr'=r$. In other words, $vur=1_{\mathbb{Z}/(3)}r$, so uniqueness implies $vu=1_{\mathbb{Z}/(3)}$. Similarly $uv=1_{\mathbb{Z}/(3)'}$. □

She took the Fact as a case of the *homomorphism theorem*: a theorem or family of theorems on quotient structures which she was rapidly expanding through the ten years up to her death.[9] From the homomorphism theorem she deduced *isomorphism theorems* very much the way we deduced Theorem 2. She recast problems of arithmetic as problems about morphisms, as for example problems of arithmetic modulo 3 became problems about morphisms between $\mathbb{Z}/(3)$ and related structures.

Equation 1 has solutions in other rings such as the quotient $\mathbb{Z}/(7)$ or the ring $\mathbb{Z}[\sqrt{2}]$ of numbers of the form $a+b\sqrt{2}$ with a,b ordinary integers. Kronecker's way of eliminating the irrational $\sqrt{2}$ amounts to treating $\mathbb{Z}[\sqrt{2}]$ as a quotient of the ring $\mathbb{Z}[X]$ of integer polynomials in one variable X.

$$r_{2-X^2}:\mathbb{Z}[X]\longrightarrow\mathbb{Z}[X]/(2-X^2)\cong\mathbb{Z}[\sqrt{2}]$$

Noether's homomorphism and isomorphism theorems describe this and all quotients up to isomorphism by their places in the pattern of ring morphisms. That means arbitrary commutative rings as in the epigraph from Faltings. Restricting attention

[8]See (Noether, 1927, note 6) and discussion in McLarty (2007*a*, Section 5).

[9]She knew she had not yet measured the scope of this theorem (McLarty, 2006, Section 4). We could call the present paper a case study of Noether's homomorphism theorem.

to "the rings that occur in practice" would be pointless and unworkable. Just stating the restriction would mean focussing on details irrelevant to most proofs. Plus, too many rings of too many kinds are already in use and more are constantly brought in. Important results often refer to specific rings, notably the integers $\mathbb{Z}$ and rationals $\mathbb{Q}$, but no such focus fits into the basic theorems or definitions.

2. The Homology of Topological Spaces

2.1. **The sphere and the torus.** Homology theory began pictorially enough. Compare the sphere S^2, i.e. the surface of a ball, to the torus T, i.e. the surface of a doughnut. A small circle on either one can bound a patch of it:

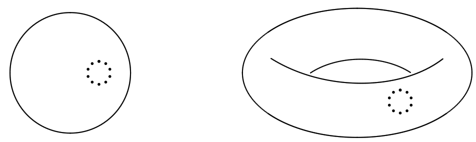


Figure 1

The difference is that every circle on the sphere bounds a region but not all circles on the torus do. Draw a vertical circle around the small circumference of the torus, another larger horizontal circle around the top of the torus, and a diagonal circle that spirals around in both ways:

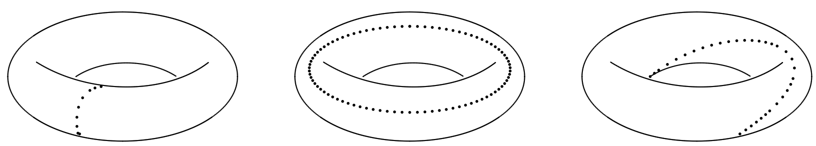


Figure 2

Intuitively the vertical circle on the left is not wrapped around any region on the surface because it is wrapped around the "hole" that runs through the interior of the torus. The larger horizontal circle wraps around the hole through the center of the torus. The spiraling circle wraps around both holes.

A hole is called 1-dimensional if a circle can wrap around it. The hole inside the sphere is not 1-dimensional since any circle on the sphere can slip off to one side and (for example) shrink down to the small bounding circle in Figure 1. That hole is 2-dimensional as the sphere surface wraps around it. The holes in each dimension say a great deal about a topological space (Atiyah, 1976).

To organize this information, Henri Poincaré called a circle C on a surface *homologous to* 0 if it bounds a region, and then wrote $C \sim 0$ (Sarkaria, 1999). The two small circles in Figure 1 are both homologous to 0, while none of the three on the torus in Figure 2 are. Name those three C_1, C_2, C_3 respectively. Together they do bound a region.[10] Poincaré says their sum is homologous to 0:

$$C_1 + C_2 + C_3 \sim 0$$

He would use the usual rules of arithmetic to rewrite this as

$$C_3 \sim -C_1 - C_2$$

[10]Cut the torus along the small circle C_1 to form a cylinder, and then along the horizontal circle C_2 to get a flat rectangle with the spiral circle C_3 as diagonal. Either triangular half of the rectangle is bounded by one vertical side, one horizontal, and the diagonal.

In fact he would consider all the circles C on the torus.[11] He called any formal sum

$$a_jC_j + a_kC_k + \cdots + a_nC_n$$

of circles C_i on the torus with integer coefficients a_i a *1-cycle*. If those circles with those multiplicities form the boundary of some sum of regions then the 1-cycle is homologous to 0:

$$a_jC_j + a_kC_k + \cdots + a_nC_n \sim 0$$

A pair of 1-cycles are homologous to each other

$$a_iC_i + \cdots + a_kC_k \sim a_nC_n + \cdots + a_pC_p$$

if and only if their formal difference is homologous to 0:

$$a_iC_i + \cdots + a_kC_k - a_nC_n - \cdots - a_pC_p \sim 0$$

The key to the homology of the torus is that every 1-cycle on the torus is homologous to a unique sum of C_1 and C_2:

$$a_jC_j + a_kC_k + \cdots + a_nC_n \sim a_1C_1 + a_2C_2$$

for some unique $a_1, a_2 \in \mathbb{Z}$. The pair $\{C_2, C_3\}$ serves as well

$$a_jC_j + a_kC_k + \cdots + a_nC_n \sim a_2C_2 + a_3C_3$$

for some unique $a_2, a_3 \in \mathbb{Z}$. The pair $\{C_1, C_3\}$ also serves as do infinitely many others. No single cycle will do. So the *first Betti number* of the torus is 2. The first Betti number of the sphere S^2 is 0, since all 1-cycles on it are homologous to 0.

Higher Betti numbers are defined using higher dimensional figures in place of circles. A good n-dimensional space M has an i-th Betti number, counting the i-dimensional holes in M, for every i from 0 to n. The Betti numbers of a space say much about its topology but, in fact, Poincaré and all topologists of the time knew that the numbers alone omit important relations between cycles.

2.2. **Brouwer to Noether to functors.** By 1910 the standard method in topology was algebraic calculation with cycles (Herreman, 2000). Everyone from Poincaré on knew the cycles formed groups. The 1-cycles on the torus add and subtract and they satisfy all the axioms for an Abelian group, when the relation $\sim$ is taken as equality. The same holds for the i-dimensional cycles on any n-dimensional space M, for each $0 \leq i \leq n$. Only no one wanted to use group theoretic language in topology. Brouwer would not even calculate with cycles. But he was a friend of Noether's and they shared some students.

As Noether emphasized morphisms in algebra, so Brouwer organized his topology around *maps* or continuous functions $f: M \to N$ between topological spaces (van Dalen, 1999). His most famous theorem, the *fixed point theorem*, says: Let D^n be the n-dimensional solid disk, that is all points on or inside the unit sphere in n-dimensional space R^n, then every map $f: D^n \to D^n$ has a fixed point, a point x such that $f(x) = x$. Many of his theorems are explicitly about maps, and essentially all of his proofs are based on finding suitable maps.

Noether's homomorphism and isomorphism theorems unified her viewpoint with Brouwer's. Given any topological space M, she would explicitly form the group $Z_i(M)$ of i-cycles on M, as the formal sums of circles shown above form the group $Z_1(T)$ of 1-cycles on the torus. Then she would form the subgroup $B_i(M) \subseteq Z_i(M)$

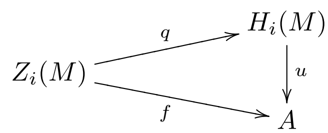
[11] Here a "circle" in any space M is any continuous map $C: S^1 \to M$ from the isolated circle or *1-sphere* S^1 to M. It may be quite twisted and run many times around M in many ways.

of *i-boundaries* on M, in other words the i-cycles which bound $(i+1)$-dimensional regions in M. She formed the *i-th homology group* as the quotient:

$$H_i(M) \cong Z_i(M)/B_i(M)$$

Intuitively $H_i(M)$ counts the i-cycles on M, but counting a cycle as 0 if it bounds a region. In effect it counts the cycles that surround holes and thus counts the i-dimensional holes in M. Her whole approach to algebra led her to focus on:

Fact on $H_i(M)$. *There is a group morphism $q: Z_i(M) \to H_i(M)$ which kills boundaries in the sense that $q(\beta) = 0$ for every $\beta \in B_i(M)$ and: For any Abelian group A and $f: Z_i(M) \to A$ which kills boundaries there is a unique $u: H_i(M) \to A$ with $uq = f$.*



This defines $H_i(M)$ up to Abelian group isomorphism just as the Fact on $\mathbb{Z}/(3)$ defined $\mathbb{Z}/(3)$ up to ring isomorphism in Section 1.4.

Crucially, the Fact specifies group morphisms from $H_i(M)$. With some trivial facts of topology[12] it implies that each map $f: M \to N$ induces morphisms

$$H_i(f): H_i(M) \to H_i(N)$$

It articulates what had been ad hoc and implicit before: While a map f carries points of M to points of N, the morphism $H_i(f)$ carries i-dimensional holes in M to i-dimensional holes in N and preserves intricate relations between them. This works in every dimension i relevant to the spaces M and N. Paul Alexandroff, Noether's student and also Brouwer's, seized on this.

When Hilbert published his lectures on intuitive geometry he asked Alexandroff for a section on topology. Finally the section did not appear in (Hilbert and Cohn-Vossen, 1932) but became the brilliant 50 page (Alexandroff, 1932) which has never gone out of print. It does topology with thoroughly group theoretic tools and may be the only mathematics text ever dedicated jointly to Hilbert and Brouwer. Alexandroff and Hopf (1935) became the standard topology textbook for the next 20 years and has also never been out of print.

The explicit correlation of maps to group morphisms immediately proved new topological theorems. But it also simplified the creation of new homology theories using new technical definitions of *cycle* and *boundary*. So it brought new complexities and some disorder over the next 20 years until topologists found a way to organize the subject by bypassing all the nuts and bolts:

> In order that these algebraic techniques not remain a special craft, the private reserve of a few virtuosos, it was necessary to put them in a broad, coherent, and supple conceptual setting. This was accomplished in the 1940's and 1950's through the efforts of many mathematicians, notably Samuel Eilenberg at Columbia University, Saunders Mac Lane of the University of Chicago, the late Norman Steenrod, and Henri Cartan. (Bass, 1978, p. 505).

[12]Each map $f: M \to N$ takes M-cycles to N-cycles, and M-boundaries to N-boundaries.

They axiomatized homology as a correlation between patterns of continuous maps and patterns of group morphisms. For each dimension i, the i-dimensional homology group became a functor H_i. This means:

- Homology preserves domain and codomain.

$$f : M \to N \quad \text{gives} \quad H_i(f) : H_i(M) \to H_i(N)$$

- Each identity map $1_M : M \to M$ (which, intuitively, does not affect the holes of M) has identity homology.

$$1_M : M \to M \quad \text{gives} \quad 1_{H_i(M)} : H_i(M) \to H_i(M)$$

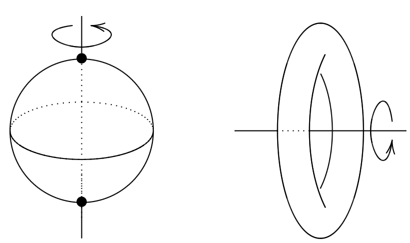
- The homology of a composite gf is the composite of the homologies.

$$\begin{array}{ccc} & T' & \\ {\scriptstyle f}\nearrow & & \searrow{\scriptstyle g} \\ T & \xrightarrow[gf]{} & T'' \end{array} \quad \text{gives} \quad \begin{array}{ccc} & H_i(T') & \\ {\scriptstyle H_i(f)}\nearrow & & \searrow{\scriptstyle H_i(g)} \\ H_i(T) & \xrightarrow[H_i(gf)]{} & H_i(T'') \end{array}$$

The axioms require more which we will not go into.[13]

The structuralist point is that all the groups and morphisms are defined only up to isomorphism. Topologists still use nuts-and-bolts descriptions of cycles and boundaries but textbooks use the axioms to define homology. The axioms make it easier to focus on geometry and they show how different nuts and bolts all yield the same calculations.

2.3. **The Lefschetz fixed point theorem.** The *Lefschetz fixed point theorem* applies to especially nice spaces M, the *orientable topological manifolds*, where each small enough region of M looks like a continuous piece of some Euclidean coordinate space $\mathbb{R}^n$ as for example small regions of a sphere or torus look like pieces of the plane $\mathbb{R}^2$. A sphere can turn on an axis the way the earth does. A torus can turn around a central axis the way a bicycle tire turns around its axle:



A rotating sphere has two fixed points, call them the North and South poles. The rotating torus has none—obviously because the axis passes through a hole. Of course the matter is more complex with general continuous functions rather than just rigid rotations. It is more complex yet for manifolds with more holes or in higher dimensions. In general the theorem relates fixed points of a map $f : M \to M$ to the way f acts on holes in all dimensions, that is to the morphisms $H_i(f)$.

On its face the fixed point theorem counts fixed points, which are solutions to equations of the form $f(x) = x$. Weil saw that if he could apply it to suitable arithmetic spaces then he could use this plus Galois theory to count solutions to

[13] See (Eilenberg and Steenrod, 1945), (Hocking and Young, 1961, Chapter 7).

his polynomials. There was one crying problem: it was nearly inconceivable that arithmetic spaces could be defined so as to support such a topological theorem.

2.4. **Cohomology.** The route to scheme theory ran through a variant of homology called *cohomology* and the key to schemes is that they admit *coverings* analogous to the topological case. For example, the torus can be covered by overlapping cylindrical sleeves, U_1, U_2, U_3, drawn here in solid outline:

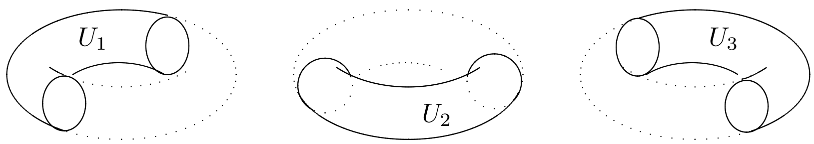


Figure 3

The route from U_1 to U_2 to U_3 travels around the hole in the center of the torus. The hole is revealed, very roughly, by the fact that every two components of this cover have non-empty intersection

$$U_{12} = U_1 \cap U_2 \qquad U_{23} = U_2 \cap U_3 \qquad U_{31} = U_3 \cap U_1$$

while the triple intersection is empty:

$$U_{123} = U_1 \cap U_2 \cap U_3 = \emptyset$$

There is no point in the center where the components would all overlap. In the center is a hole. The precise relation between holes and covers is complex. For example the cover $\{U_1, U_2, U_3\}$ does not reveal the hole inside the torus, which is hidden inside each sleeve. Other covers reveal that one. Cohomology summarizes covers of a space M to produce cohomology groups $H^n(M)$ which are close kin to the homology groups $H_n(M)$. The standard tool for it is *sheaves*.

On one definition, a sheaf on a space M is another space with a map $S \to M$ where S is a union of partially overlapping partial covers of M, which may (or may not) patch together in many different ways to form many covers.[14] Another definition says a sheaf $\mathcal{F}$ on M assigns a set $\mathcal{F}(U)$ to each open subset $U \subseteq M$, thought of heuristically as a set of "patches" covering U. There are compatibility conditions among the sets over different open subsets of M which we will not detail. If the sets $\mathcal{F}(U)$ are Abelian groups in a compatible way then $\mathcal{F}$ is an *Abelian sheaf.*

The cohomology of a space M became an infinite series $H^1, H^2, \ldots$ of functors from the category $\mathbf{Ab}_M$ of Abelian sheaves on M to the category $\mathbf{Ab}$ of ordinary Abelian groups. Then the entire series $H^1, H^2, \ldots$ was conceived as a single object called a *δ-functor*, which can be defined (up to isomorphism) by its place within a category of series of functors $\mathbf{Ab}_M \to \mathbf{Ab}$. Today's tools were introduced in one of the most cited papers in mathematics (Grothendieck, 1957). In topology or complex analysis the functorial patterns are always invoked although lower-level constructions are often taken as defining cohomology. Textbooks on cohomological number theory take the functorial pattern as definition. Of course the theory of derived functors was developed to get at geometry, arithmetic, et c. and not to call attention to itself. So for example Washington on Galois cohomology never

[14]See the light introduction in (Mac Lane, 1986, pp. 252–6, 351–5).

mentions derived functors. But each time he writes "for proof see. . . ," the reference uses them.[15]

3. Arithmetic Schemes

3.1. **Geometry over the integers.** Classical algebraic geometry looked at real and complex number solutions to lists of polynomials. Around 1940 though André Weil took up Kronecker's vision of arithmetic and called for "algebraic geometry over the integers," which Grothendieck achieved by the theory of *schemes* (Weil, 1979, vol.1, p. 576). So now, for example, Faltings in the epigraph writes of "affine space over the integers", written $\mathbb{A}^n_{\mathbb{Z}}$ to make the integers explicit. What is it?

Classical real affine n-space $\mathbb{R}^n$, or $\mathbb{A}^n_{\mathbb{R}}$, is the space of n-tuples $\langle x_1, \ldots x_n\rangle$ of real numbers.[16] But the set $\mathbb{Z}^n$ of n-tuples of integers captures little arithmetic. Recalling Section 1.3, the equation

$$Y^2 = 3X + 2 \tag{1}$$

defines the empty subset of $\mathbb{Z}^2$ the same as, say,

$$1 = 0$$

But Equation 1 is not arithmetically trivial while $1 = 0$ is. Equation 1 has solutions in many rings including paradigmatically arithmetic examples like $\mathbb{Z}/(7)$ and $\mathbb{Z}[\sqrt{2}]$ as in Sections 1.3–1.4. The affine space $\mathbb{A}^2_{\mathbb{Z}}$ is more subtle than $\mathbb{Z}^2$, so that Equation 1 can define a subscheme of it containing these solutions, while 1=0 defines the empty subscheme. There are two basic approaches.

3.2. **Schemes as variable sets of solutions.** Consider the equation

$$X^2 + Y^2 = 1 \tag{2}$$

It has four integer solutions

$$X = \pm 1 \text{ while } Y = 0\text{; or else } X = 0 \text{ while } Y = \pm 1$$

Clearly the equation points towards a circle but these four solutions do little to show it. So the idea is to look not only at integer solutions. The equation has infinitely many rational solutions. Each rational number q gives a rational solution

$$X = \frac{q^2 - 1}{q^2 + 1} \qquad Y = \frac{2q}{q^2 + 1}$$

as straightforward calculation shows. Every real number θ gives a real solution

$$X = \cos(\theta) \qquad Y = \sin(\theta)$$

The ring $\mathbb{Z}/(7)$ of integers modulo 7 has eight solutions, including $X = 2, Y = 5$:

$$2^2 + 5^2 \ = \ 29 \ \equiv \ 1 \pmod 7$$

So the equation has not one set of solutions, but for each ring R it has a set of solutions in R which we call $V_{S^1}(R)$. Here "V" recalls the classical geometer's term, the *variety* of points defined by an equation, while the subscript is to suggest that this is the equation of the circle S^1. Ring morphisms preserve solutions.

[15]See Huybrechts (2005) on complex geometry, Hartshorne (1977) and Milne (1980) on number theory. Compare Washington (1997, pp. 102, 104, 105, 107, 108, 118, 120).

[16]This usage contrasts affine spaces to projective spaces, not to vector spaces.

Given any ring morphism $f\colon R \to R'$ and any solution $a, b \in R$ to Equation 2 then $f(a), f(b) \in R'$ is also a solution since by definition of morphism

$$f(a)^2 + f(b)^2 \;=\; f(a^2 + b^2) \;=\; f(1) \;=\; 1$$

So V_{S^1} is a *variable set*, specifically a functor $V_{S^1}\colon \mathbf{Ring} \to \mathbf{Set}$ from the category of rings to the category of sets. It takes each ring R to the set $V_{S^1}(R)$, and each ring morphism $f\colon R \to R'$ to the corresponding function. It preserves identities:

$$1_R\colon R \to R \quad \text{gives} \quad 1_{V_{S^1}(R)}\colon V_{S^1}(R) \to V_{S^1}(R)$$

And it preserves composition:

$$\begin{array}{ccc} & R' & \\ {\scriptstyle f}\nearrow & & \searrow{\scriptstyle g} \\ R & \xrightarrow[gf]{} & R'' \end{array} \qquad \text{gives} \qquad \begin{array}{ccc} & V_{S^1}(R') & \\ {\scriptstyle V_{S^1}(f)}\nearrow & & \searrow{\scriptstyle V_{S^1}(g)} \\ V_{S^1}(R) & \xrightarrow[V_{S^1}(gf)]{} & V_{S^1}(R'') \end{array}$$

Call V_{S^1} the *affine scheme* of the Equation 2. From this viewpoint the affine n-space $\mathbb{A}^n_{\mathbb{Z}}$ is the functor corresponding to n variables and the trivial equation 1=1. Any list of equations on n variables defines a similar functor, a *subscheme* of $\mathbb{A}^n_{\mathbb{Z}}$. An equation may have no variables, as for example the equation 7=0 gives subschemes expressing arithmetic modulo 7. An *arithmetic scheme* is any functor $\mathbf{Ring} \to \mathbf{Set}$ which contains suitably overlapping parts, where each part is isomorphic to the affine scheme of some finite list of integer polynomials. In general there are many ways to choose these parts and no one covering is intrinsic to the scheme.

A *scheme map*, on this approach, is simply any natural transformation between the functors. This is the start of many pay-offs as geometrically important ideas find quite direct functorial expression. It may not even seem plausible that such an abstract definition of maps could have geometric content, until you have seen it work as we have not got space to show here. In fact, though, it gives exactly the same patterns of maps as the more evidently geometrical definition in the following section. The functorial apparatus looked heavy to some algebraic geometers but it merely made a central fact of algebra explicit: Every integer polynomial has a (possibly empty) set of solutions in every commutative ring, and every ring morphism preserves solutions. The techniques spread as geometers learned the practical value of using arbitrary commutative rings to prove theorems on the ring $\mathbb{Z}$ of integers.

Grothendieck and Dieudonné (1971) used this version of schemes in the introduction. Such a scheme is "basically a structured set" (Mumford, 1988, p. 113) but strictly it is a structured proper class. There are technical means to avoid proper classes—by specific tricks in specific situations, or generally by adding *Grothendieck universes* to set theory (Artin *et al.*, 1972, pp. 185ff.). But standard textbook presentations use functors on all commutative rings and these are proper classes in either ZF or categorical set theory.

3.3. **Schemes as Kroneckerian spaces.** The other approach to schemes constructs a space from the data. If the equation

$$X^2 + Y^2 = 1 \tag{2}$$

is to define a space then intuitively a *coordinate function* on that space should be given by a polynomial in X and Y, while two polynomials $P(X, Y), Q(X, Y)$ give the same function if they agree all over the space. To a first approximation we would say $P(X,Y)$ and $Q(X,Y)$ give the same function on this space if

$$P(a,b) \;=\; Q(a,b) \qquad \text{for all } \langle a,b\rangle \in \mathbb{Z}^2 \text{ with } a^2+b^2-1=0$$

But this puts too much stress on integer solutions. In the case of equations with no integer solutions this poor definition would make every two polynomials give the same function trivially. So we actually use a stronger condition taken from the defining polynomial: Polynomials $P(X,Y)$ and $Q(X,Y)$ are called congruent modulo X^2+Y^2-1, written

$$P(X,Y) \equiv Q(X,Y) \pmod{X^2+Y^2-1}$$

if and only if

$$Q(X,Y)-P(X,Y) \quad \text{is divisible by} \quad X^2+Y^2-1$$

A coordinate function on the space is a congruence class of polynomials. For example X^2Y defines a coordinate function on this space, the same function as $Y-Y^3$, since light calculation shows

$$(X^2Y)-(Y-Y^3) \;=\; Y.(X^2+Y^2-1)$$

Altogether the ring of coordinate functions is the ring of integer polynomials in two variables, $\mathbb{Z}[X,Y]$, modulo X^2+Y^2-1. I.e. it is the quotient ring

$$\mathbb{Z}[X,Y]/(X^2+Y^2-1)$$

These "functions" are constructed from integer polynomials just as Kronecker would construct irrationals as in Section 1.1.

The next step is to use the functions to define points of this space. The motivation is that each point p should have a set of functions

$$\mathfrak{p} \;\subseteq\; \mathbb{Z}[X,Y]/(X^2+Y^2-1)$$

which take value 0 at p. This set should be an *ideal*, closed under addition and under multiplication by arbitrary functions. That is, if the functions $P_1(X,Y)$ and $P_2(X,Y)$ are both construed as taking value 0 at p then $P_1(X,Y)+P_2(X,Y)$ must also be; and so must the product $R(X,Y)\cdot P_1(X,Y)$ for any polynomial $R(X,Y)$. Further, the ideal $\mathfrak{p}$ should be *prime*, in the sense that whenever a product lies in $\mathfrak{p}$ then at least one factor already lies in it.[17] More formally:

$$\text{If } P_1(X,Y)\cdot P_2(X,Y)\in\mathfrak{p} \text{ then either } P_1(X,Y)\in\mathfrak{p} \text{ or } \; P_2(X,Y)\in\mathfrak{p}.$$

Scheme theory demands no more than that for a point. It says there is a point for each prime ideal. Textbooks say the points *are* the prime ideals. So our space has a point for each integer solution $a,b\in\mathbb{Z}$ to Equation 2, but also a point for the mod 7 solution $2,5\in\mathbb{Z}/(7)$. It has one point combining the two real algebraic solutions

$$\sqrt{2}/2,\sqrt{2}/2\in\mathbb{R} \quad \text{and} \quad -\sqrt{2}/2,-\sqrt{2}/2\in\mathbb{R}$$

and another point combining these two[18]

$$\sqrt{2}/2,-\sqrt{2}/2\in\mathbb{R} \quad \text{and} \quad -\sqrt{2}/2,\sqrt{2}/2\in\mathbb{R}$$

[17] This expresses the idea that if a product is 0 then at least one factor must be—which *does not* hold in every ring—but this definition makes it hold for function values at points of a scheme.

[18] Notice the first two solutions also satisfy $2XY=1$. The second two satisfy $2XY=-1$.

It has one point for each pair of conjugate complex algebraic solutions such as

$$2, \pm\sqrt{-3} \in \mathbb{C}$$

It has no points for real or complex transcendental solutions. This elegant algebraic definition gives our space points for precisely those solutions to Equation 2 given by roots of integer polynomials (possibly modulo some prime number) and it distinguishes only those points given by roots of distinct polynomials.

Intuitively a *closed set* should be the set of all points where some function is 0, or where some list of functions are all 0. Formally, an affine scheme has a *closed set* for each ideal of coordinate functions on it, and in the case of arithmetic schemes each ideal is defined by a finite list of polynomial equations:

$$P_1(X,Y) = 0 \quad \ldots \quad P_k(X,Y) = 0$$

Then we name the space after its coordinate ring, calling it

$$\mathrm{Spec}(\mathbb{Z}[X,Y]/(X^2 + Y^2 - 1))$$

or the *spectrum* of the ring $\mathbb{Z}[X,Y]/(X^2 + Y^2 - 1)$.

Every commutative ring R has a spectrum $\mathrm{Spec}(R)$. The coordinate function ring on $\mathrm{Spec}(R)$ is just the ring R. So again the "functions" are generally not functions in the set-theoretic sense. They are any elements of any ring. The points are the prime ideals of R. The spectrum has a topology where closed sets correspond to ideals. The spectra of rings are the *affine* schemes. Notably, the affine n-space $\mathbb{A}^n_{\mathbb{Z}}$ is the spectrum of the integer polynomial ring in n variables $\mathbb{Z}[X_1, \ldots X_n]$ subject to no equation or, if you prefer, the trivially true equation 1=1.

$$\mathbb{A}^n_{\mathbb{Z}} = \mathrm{Spec}(\mathbb{Z}[X_1, \ldots X_n])$$

A scheme is patched together from affine schemes. More fully, a *scheme* is a topological space X together with a sheaf of rings $\mathcal{O}_X$ called the *structure sheaf* of the scheme. This sheaf assigns a ring $\mathcal{O}_X(U)$ of "coordinate functions" to each open subset $U \subseteq X$, and to each inclusion of open subsets $U \subseteq V$ of X a ring morphism

$$r_{U,V} : \mathcal{O}_X(V) \to \mathcal{O}_X(U)$$

The whole must be made of parts isomorphic to the spectra $\mathrm{Spec}(R)$ of rings R with their coordinate functions. A scheme map

$$f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$$

consists of a continuous function $f : X \to Y$ in the ordinary sense plus a great many ring morphisms in the opposite direction: By continuity of f, each open subset $V \subset Y$ has inverse image $f^{-1}(V)$ open in X, and the scheme map includes a suitable ring morphism

$$\mathcal{O}_Y(V) \to \mathcal{O}_X(f^{-1}(V))$$

for each open $V \subset Y$, showing how $f^{-1}(V)$ maps algebraically into V. This version of schemes dominates Grothendieck and Dieudonné (1971) and Hartshorne (1977) though Grothendieck favored the functorial version in his work.

An arithmetic scheme is a scheme pasted from finitely many parts defined by finite lists of integer polynomials. Each integer polynomial ring $\mathbb{Z}[X_1, \ldots X_n]$ is countable. Since each of its ideals is generated by a finite list of polynomials there are only countably many, thus countably many points and closed sets and functions on them. Altogether the Kroneckerian version of any arithmetic scheme is countable.

3.4. **Scheme cohomology.** Schemes were born for cohomology. In fact they were born and re-born for it. Jean-Pierre Serre introduced structure sheaves into algebraic geometry so as to produce the cohomology theory today called *coherent cohomology*. These structure sheaves were "the principle of the right definition" of schemes (Grothendieck, 1958, p. 106). Then Serre took the first step towards the sought-after "Weil cohomology." Using ideas from differential geometry he defined covers and he proved they gave good 1-dimensional Weil cohomology groups $H^1(M)$ for algebraic spaces M. Notably, Serre proved his groups gave the first non-trivial step in the infinite series of a δ-functor as in our Section 2.4.[19]

For Grothendieck the functorial pattern was decisive. An idea that gave the *first* step had to give *every* step. He made it work by producing the general theory of schemes and lightly altering Serre's covers into a frankly astonishing theory of *étale* maps. The purely algebraic definition of a *finite étale* map $X \to S$ between schemes does a brilliant job of saying the space X lies smoothly stacked over S even when there is no very natural geometric picture of X or S alone. Working with Serre, Pierre Deligne, and others over several years Grothendieck proved that these étale covers yield a cohomology theory, called étale cohomology, satisfying enough classical topological theorems for the Weil conjectures and much more.

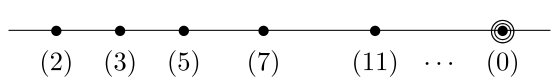
4. An Example

4.1. **Integers as coordinate functions.** The arithmetic scheme Spec($\mathbb{Z}$), the affine scheme of the ring of integers $\mathbb{Z}$, is given by the trivially true equation 1=1 in no variables. There is exactly one "solution" to 1=1—and that is to say it is *true*—and indeed the equation remains true in any ring R. As a variable set this scheme is the functor $\mathrm{Spec}(\mathbb{Z}) = V_{1=1}$ where for each ring R the set of solutions $V_{1=1}(R)$ is a singleton which we may think of as:

$$V_{1=1}(R) = \{true\} \qquad \text{for every ring } R$$

This is perfectly simple and even too simple. It does nothing to reveal the arithmetic of the integers. But that is because we have looked at this scheme in isolation. Looking at its maps to and from other schemes we find it is *terminal* in the category of schemes: Every scheme has exactly one scheme map to Spec($\mathbb{Z}$). This is a very simple specification of the place of Spec($\mathbb{Z}$) in the pattern or category of all schemes but it does invoke the pattern or category of all schemes, and that very large pattern reveals all of the arithmetic of the integers! The arithmetic of any ring R does not lie *inside* Spec(R) but in the pattern of all scheme maps *to* Spec(R).

On the other hand, look at Spec($\mathbb{Z}$) as a space. The points are the prime ideals and these are of two kinds: The singleton 0 is a prime ideal $\{0\} \subseteq \mathbb{Z}$ and for each prime number $p \in \mathbb{Z}$ the set of all integer multiples of p is a prime ideal usually written as $(p) \subseteq \mathbb{Z}$. We may also write $\{0\} = (0)$ since 0 is indeed the only multiple of 0. Algebraic geometers often draw these points as a kind of line



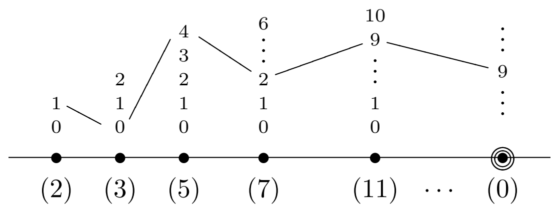
Then the idea is to think of each integer $m \in \mathbb{Z}$ as a function defined on this line. For very good reasons, the values of the function over the point (0) are rational

[19](Serre, 1958, esp. §1.2 and §3.6)

numbers while the values over any point (p) are integers modulo p. The integer $m \in \mathbb{Z}$ is a function whose value at the point (0) is m and value at each point (p) is m modulo p. For example the integer 9 has

$$9 \equiv 1 \pmod 2 \qquad 9 \equiv 0 \pmod 3$$
$$9 \equiv 4 \pmod 5 \qquad 9 \equiv 2 \pmod 7$$

and we can graph 9 as a function this way:



The spatial structure of $\mathrm{Spec}(\mathbb{Z})$ is determined by the "coordinate functions" on it—namely by the integers! But the picture is only suggestive. Rigorous proofs show schemes have structural relations parallel to those in geometry and these relations return major new arithmetic theorems. We sketch one simple example.

4.2. **The Chinese remainder theorem.** Consider congruences modulo 4 and 6:

$$a \equiv 2 \pmod 4 \quad \text{and} \quad a \equiv 1 \pmod 6$$

These two have no solution since the first implies a is even and the second implies it is odd. On the other hand consider

$$a \equiv 1 \pmod 4 \quad \text{and} \quad a \equiv 3 \pmod 6$$

These agree modulo 2, as both say a is odd, and clearly $a = 9$ is a solution. Then too $a = 21$ is a solution. Adding any multiple of 12 will give another solution since 12 is the smallest common multiple of 4 and 6. One classical statement of the Chinese remainder theorem is:

Theorem. *Take any integer moduli m_1, m_2. Then for any integer remainders r_1, r_2 consider the congruences on an unknown integer a*

$$a \equiv r_1 \pmod{m_1} \quad \textit{and} \quad a \equiv r_2 \pmod{m_2}$$

There are solutions a if and only if

$$r_1 \equiv r_2 \pmod{\mathrm{GCD}(m_1, m_2)}$$

where $\mathrm{GCD}(m_1, m_2)$ is the greatest common divisor of m_1 and m_2. And in that case the solution is unique modulo $\mathrm{LCM}(m_1, m_2)$, the least common multiple of m_1 and m_2. In a formula, if a and b are both solutions then

$$a \equiv b \pmod{\mathrm{LCM}(m_1, m_2)}$$

Note that $2 = \mathrm{GCD}(4, 6)$ and $12 = \mathrm{LCM}(4, 6)$ in the examples above.

This theorem supports thinking of integers as functions on the scheme $\mathrm{Spec}(\mathbb{Z})$. Compare this familiar fact about the real line $\mathbb{R}$:

Theorem. *Take any intervals on the line, say $[0, 2] \subseteq \mathbb{R}$ and $[1, 3] \subseteq \mathbb{R}$. Then for any continuous functions f_1 and f_2 consider these conditions on an unknown continuous function a:*

$$a(x) = f_1(x) \textit{ for all } x \in [0, 2] \quad \textit{and} \quad a(x) = f_2(x) \textit{ for all } x \in [1, 3]$$

There are solutions a if and only if the functions f_1 and f_2 agree on the intersection of the intervals:

$$f_1(x) = f_2(x) \quad \textit{for all } x \in [1, 2]$$

And in that case the solution is unique over the union of the intervals: if a and b are both solutions then

$$a(x) = b(x) \quad \textit{for all } x \in [0, 3]$$

In the Chinese remainder theorem the given numbers r_1 and r_2 and the sought number a are taken as functions on the line $\mathrm{Spec}(\mathbb{Z})$. The equation

$$a \equiv r_1 \pmod{m_1}$$

says that a must agree with r_1 not necessarily over the whole line but at least at all points (p) of the line corresponding to prime factors p of m_1.[20] The other equation

$$a \equiv r_2 \pmod{m_2}$$

says a must agree with r_2 at all points (p) corresponding to prime factors p of m_2. The necessary condition is that r_1 and r_2 must agree at all points (p) where p divides both m_1 and m_2. But p divides both m_1 and m_2 if and only if it divides their greatest common divisor so this condition can be expressed in an equation:

$$r_1 \equiv r_2 \pmod{\mathrm{GCD}(m_1, m_2)}$$

The proof shows this condition is also sufficient. And the function a is uniquely determined at all points (p) where p divides either one of m_1 and m_2. But those are the prime factors of $\mathrm{LCM}(m_1, m_2)$ so the unique determinacy says any two solutions a, b have

$$a \equiv b \pmod{\mathrm{LCM}(m_1, m_2)}$$

The Chinese remainder theorem patches part of one function r_1 with part of another r_2 to get a single function a on $\mathrm{Spec}(\mathbb{Z})$ just as you can patch parts of continuous functions f_1, f_2 into a single continuous function a on the real line $\mathbb{R}$. But the Chinese remainder theorem only deals with parts given by finite numbers of primes. It follows from a more general result with a very similar proof: for every ring R you can patch compatible partial functions on the affine scheme $X = \mathrm{Spec}(R)$. In technical terms: every structure sheaf $\mathcal{O}_X$ is actually a sheaf, so it agrees with its own 0-dimensional Čech cohomology.[21]

The point is simple. Many arithmetic problems are easily solved "locally" in some sense, while we want "global" solutions. In the Chinese remainder theorem the list of congruences is easily solved "locally at each prime" and the trick is to patch together one solution on the whole line.[22] Cohomology is all about patching.

5. The Philosophy of Structure

5.1. **Understanding sheaves and schemes.** Intuitive ideas available in some way to some experts often become explicit and publicly available by passing to higher levels of structure, and they often grow further in the passage. Section 2.2 gave homology group morphisms and homology theories as two examples. For another, there was a serious problem in the early 1950s of how to understand sheaves

[20] For each prime power p^n that divides m_1, the functions a and r_1 must agree on the n-th order infinitesimal neighborhood of the point (p), or in other words $a \equiv r_1 \pmod{p^n}$.

[21] Compare (Hartshorne, 1977, Proposition II.2.2) and (Tamme, 1994, p. 41).

[22] Eisenbud (1995, Exercise 2.6) gives a basically homological proof.

and work with them. Several nuts-and-bolts definitions were known but none were as simple as the ideas seemed to be. And the specialists seeking a Weil cohomology to prove the Weil conjectures saw that none of these definitions was vaguely suitable for that. One thing was clear. People who worked with sheaves would draw vast commutative diagrams "full of arrows covering the whole blackboard" dumfounding the student Grothendieck (Grothendieck, 1985–87, p. 19). The vertices were Abelian sheaves and the arrows were sheaf morphisms between them. One key to getting the diagrams right was to think of them as diagrams of ordinary Abelian groups and group morphisms. Abelian sheaves were a lot like Abelian groups.

Grothendieck followed his constant belief that the simplest most unified account of the intuition would itself provide the needed generality.[23] Rather than focus on individual sheaves he would describe the "vast arsenal" of sheaves on a given space:

> We consider this "set" or "arsenal" as equipped with its most evident structure, the way it appears so to speak "right in front of your nose"; that is what we call the structure of a "category." (Grothendieck, 1985–87, p. P38)

The diagrams do not *stand for* some *other* information about sheaves. They *are* the *relevant, categorical* information. They are the information used in practice. So Grothendieck extended ideas from Mac Lane to produce a short list of axioms. A category satisfying these axioms is called an *Abelian category*:

(1) The category **Ab** of Abelian groups is an Abelian category, as is the category $\mathbf{Ab}_M$ of Abelian sheaves on any space M. So are many categories used in other cohomology theories apparently quite unlike these. This was promising for a Weil cohomology and later did work for étale cohomology.
(2) The Abelian category axioms themselves suffice to define cohomology in terms of derived functors and prove the general theorems on cohomology (Grothendieck, 1957).

The axioms explicated how Abelian sheaves are like Abelian groups. They quickly entered textbooks as the easiest way to work with sheaves. And they opened the way to an even more intuitive understanding as they led Grothendieck to analogous axioms for the category $\mathbf{Sh}_M$ of all sheaves on M.

He produced new axioms on a category, and called any category which satisfies them a *topos* (Artin *et al.*, 1972, pp. 322ff.):

(1) The category **Set** of all sets is a topos, as is the category $\mathbf{Sh}_M$ of all sheaves on any space M.
(2) We can interpret mathematics inside any topos very much the way we do in sets. The "Abelian groups" in the topos $\mathbf{Sh}_M$ of sheaves on any space M turn out to be just the Abelian sheaves on M. The "Abelian groups" in other toposes play similar roles in other cohomology theories.

In short the objets of any topos are *continuously variable sets* as for example the topos $\mathbf{Sh}_M$ contains the sets varying continuously over the space M.[24] Mathematics in a topos is like classical mathematics with some differences reflecting the variation. Specifically mathematics in $\mathbf{Sh}_M$ differs from classical by reflecting the topology of M. The cohomology of M measures the difference between classical Abelian groups

---

[23]For more detail see McLarty (2007*b*).

[24]William Lawvere has made this much more explicit but Grothendieck already found each topos is "like" the universe of sets (McLarty, 1990, p. 358).

and Abelian groups varying continuously over M. This measure also works in other toposes to give other cohomology theories and it was the key to producing étale cohomology. For one expert view of how far toposes can be eliminated from étale cohomology, and yet how they help in understanding it, see Deligne (1977, 1998).

Categorical thinking is also central to understanding schemes. At the basic level of the spaces to be studied, on either definition of schemes, the geometry of a scheme is poorly revealed by looking at it as a set of points with geometric relations among them. It may even be "bizarre" on that level:

> [In many schemes] the points ... have no ready to hand geometric sense.... When one needs to construct a scheme one generally does not begin by constructing the set of points.... [While] the decision to let every commutative ring define a scheme gives standing to bizarre *schemes*, allowing it gives a *category of* schemes with nice properties. (Deligne, 1998, pp. 12–13)

One generally constructs a scheme from its relations to other schemes. The relations are geometrically meaningful. The category of schemes captures those relations and incorporates Noether's insight that the simplest arithmetic definitions often relate a desired ring to arbitrary commutative rings as in Section 1.4.

5.2. **Several reasons morphisms are not functions.** Functions are examples of morphisms, but overreliance on this example has been a major obstacle to understanding category theory (McLarty, 1990, §7). Indeed schemes typify the failure of Bourbaki's structure theory based on structure preserving functions and so they witness the inadequacy of current philosophical theories of "structure." It is not a problem with set theory. Set theory handles schemes easily enough. We handle schemes set-theoretically here. But even on set theoretic foundations scheme maps are not "structure preserving functions" in the set theoretic sense—that is in Bourbaki's sense or in the closely related sense of the model-theoretic structuralist philosophies of mathematics.[25]

In the plainest technical sense neither of our definitions of schemes has set theoretic functions as maps. On the structure sheaf definition a map from $(X, \mathcal{O}_X)$ to $(Y, \mathcal{O}_Y)$ consists of a continuous function $f : X \to Y$ plus many ring morphisms in the opposite direction (in general, infinitely many). For the variable set definition each map is a natural transformation and thus a structure preserving proper class of functions. Either way a map is more complex than a set theoretic function.

Topology gives another kind of morphism more complex than functions. Continuous functions $f, g : S \to S'$ between topological spaces are called *homotopic* if each one can be continuously deformed into the other (Mac Lane, 1986, p. 323). Write $\overline{f}$ for the homotopy class of f, that is the set of functions $S \to S'$ homotopic to f. The *homotopy category* **Toph** has topological spaces S as objects, and homotopy classes $\overline{f} : S \to S'$ as morphisms. The morphisms of **Toph** are not functions but equivalence classes of functions. By the global axiom of choice we can select one representative function from each class. But there is provably no way to select representatives so that the composite of every pair of selected representatives is also selected. The categorical structure of **Toph** cannot be defined by composition of functions but requires composition of equivalence classes of functions (Freyd, 1970).

[25]Bourbaki (1958); Hellman (1989); Shapiro (1997).

A case study by Leng (2002) includes an example from functional analysis. C^*-algebras originated in quantum mechanics and the paradigms are algebras of operators on function spaces. The mathematician George Elliott sought a theorem characterizing certain ones. The theorem used *inductive limits*, where the inductive limit of an infinite sequence of C^*-algebras and morphisms

$$A_1 \longrightarrow A_2 \longrightarrow \cdots \longrightarrow A_n \longrightarrow \cdots$$

is a single C^*-algebra A_∞ combining all of the A_n in a way compatible with the morphisms. The inductive limit is an actual C^*-algebra. On the way to the theorem, though, Elliott first treated each infinite sequence of C^*-algebras as a single new object, and defined morphisms between sequences in just such a way as to make the sequences act like their own inductive limits.[26] As Leng says: "Defining the morphisms between these sequences turned out to require some ingenuity" (2002, p. 21). But it worked. Elliott's formal inductive limits supported the proofs needed to imply the theorem for the actual C^*-algebra inductive limits. It would be triply useless to think of the ingeniously defined morphisms of sequences as "structure preserving functions" in the logician's or Bourbaki's sense. They are technically more complex than functions, the properties desired of them were categorical rather than set theoretic, and it was far from clear what structure they should preserve.

Carter (Forthcoming) gives a similar example in geometry, and urges a modal logic interpretation of it. Examples from analysis and geometry influenced the founders of category theory (McLarty, 2007*a*, §2).

Technicalities aside, it is a bad idea to think of scheme maps just one way. We have two fundamentally different definitions. This is quite different from cases familiar to philosophers such as the two definitions of real numbers from the rationals by Cauchy sequences and by Dedekind cuts. Neither one of those definitions is much used in practice.[27] Both definitions of scheme maps are used. Intuition draws on both and must hang on neither. Each is fitted to some proofs or calculations and clumsy for others. There is no ontology here.

Finally, categorical axioms patently ignore ontology. When the leader of a graduate student session on spectral sequences says "Let **A** be your favorite Abelian category...," then all we know of **A** is what kind of patterns its morphisms can form. In some useful Abelian categories the morphisms are structure preserving functions, in others they are more complex, in others the morphisms are finite arrays of numbers (Mac Lane, 1998, p. 11). It cannot matter which they are since we do not know which example anyone prefers. When Lang (1993) proves a theorem for all Abelian categories it does not matter what the morphisms *are*. And when Lawvere poses axioms for a category of categories as foundation (1963) or a category of sets as a foundation (1965) then the morphisms are what the axioms say they are—they are not "functions" defined in any prior set theory.

5.3. **"The" category of schemes.** Section 3 gave two definitions of schemes, and so two definitions of the category of schemes. A structuralist might hope these would be isomorphic categories but the truth is more interesting. They are *equivalent*. Roughly speaking, equivalent categories contain the same structures in

---

[26]Compare Grothendieck's *ind-objects* and *pro-objects* in (Artin *et al.*, 1972, Exposé I).

[27]Practice usually defines the real numbers up to isomorphism by their algebra and the least upper bound property (Rudin, 1953, p. 8).

the sense that they contain all the same patterns of objects and arrows—but they may have different numbers of copies of each pattern (Mac Lane, 1998, §IV.4).

Let $\mathbf{Scheme}_{\mathcal{O}}$ be the category of schemes $X, \mathcal{O}_X$ as point sets with sheaves of rings and call these *ringed space schemes*. Let $\mathbf{Scheme}_V$ be the category of schemes as functors, and call these *functor schemes*. There is a functor

$$h : \mathbf{Scheme}_{\mathcal{O}} \to \mathbf{Scheme}_V$$

with two nice properties (Mumford, 1988, §. II.6).[28]

(1) The scheme maps from any $X, \mathcal{O}_X$ to any $Y, \mathcal{O}_Y$ in $\mathbf{Scheme}_{\mathcal{O}}$ correspond exactly to the scheme maps $h(X) \to h(Y)$ in $\mathbf{Scheme}_V$.
(2) Every functor scheme is isomorphic to the image $h(X)$ of at least one ringed space scheme $X, \mathcal{O}_X$.

We say that a functor scheme V *corresponds* to the ringed space scheme X if V is isomorphic to $h(X)$. But then V also corresponds to every ringed space scheme isomorphic to X. The key to working this way is that all the ringed space schemes corresponding to X are already isomorphic (as ringed space schemes). For many purposes you need not decide which category you are in. You can go back and forth by the functor h. As one germane application this passage preserves cohomology. Cohomology of schemes can be defined purely in terms of categorical relations between schemes. Exactly the same relations exist in the category of ringed space schemes and the category of functor schemes. Many calculations of cohomology, and applications of cohomology, work identically verbatim in the two categories.

5.4. **Isomorphism versus equivalence.** Like the two definitions of the category of schemes, so the two definitions in Section 2.4 of the category of sheaves on a space M agree only up to equivalence. Equivalence is isomorphism *of* categories up to isomorphism *in* the categories.

Isomorphism is defined the same way for categories as for any kind of structure: A functor $\mathbf{F} : \mathbf{C} \to \mathbf{D}$ is an isomorphism if it has an inverse, namely a functor $\mathbf{G} : \mathbf{D} \to \mathbf{C}$ composing with $\mathbf{F}$ to give the identity functors $\mathbf{GF} = 1_{\mathbf{C}}$ and $\mathbf{FG} = 1_{\mathbf{D}}$. In other words, for all objects C of $\mathbf{C}$, and D of $\mathbf{D}$:

$$\mathbf{GF}(C) = C \qquad\qquad \mathbf{FG}(D) = D$$

and the same for morphisms. Categories are isomorphic if there is an isomorphism between them.

A functor $\mathbf{F} : \mathbf{C} \to \mathbf{D}$ is an *equivalence* if it has a quasi-inverse, a functor $\mathbf{G}$ with composites isomorphic to identity functors: $\mathbf{GF} \cong 1_{\mathbf{C}}$ and $\mathbf{FG} \cong 1_{\mathbf{D}}$. In other words for all objects C of $\mathbf{C}$ and D of $\mathbf{D}$ there are isomorphisms

$$\mathbf{GF}(C) \cong C \qquad\qquad \mathbf{FG}(D) \cong D$$

in a way compatible with morphisms. Categories are *equivalent* if there is an equivalence between them. Gelfand and Manin overstate an important insight when they call isomorphism "useless" compared to equivalence:

> Contrary to expectations [isomorphism of categories] appears to be more or less useless, the main reason being that neither of the requirements $\mathbf{GF} = 1_{\mathbf{C}}$ and $\mathbf{FG} = 1_{\mathbf{D}}$ is realistic. When we apply two natural constructions to an object, the most we can ask for is to get a new object which is canonically isomorphic to the old one;

[28] These imply equivalence as defined in the next section, given a suitable axiom of choice.

> it would be too much to hope for the new object to be identical to the old one. (Gelfand and Manin, 1996, p. 71)

This is actually not true even in Gelfand and Manin's book. Their central construction is the *derived category* $D(\mathbf{A})$ of any Abelian category $\mathbf{A}$. Given $\mathbf{A}$, they define $D(\mathbf{A})$ up to a unique isomorphism (1996, §III.2). They use the uniqueness up to isomorphism repeatedly. The notion of isomorphic categories remains central. Yet for many purposes equivalence is enough.[29] The next section returns to it.

5.5. **Philosophical open problems.** We have seen structuralist ideas grow dramatically from Noether through Eilenberg and Mac Lane to Grothendieck. We have alluded to Lawvere's elementary category theory unifying and generalizing the key ideas and to many advances in functorial geometry and number theory. Most of that is quite pure mathematics but there is physics as well. Sir Michael Atiyah has made functorial tools standard in theoretical particle physics and influential in the search for a general relativistic quantum theory (Atiyah, 2006). Among Lawvere's goals throughout his career has been simpler and yet less idealized continuum mechanics (Lawvere and Schanuel, 1986; Lawvere, 2002). An obvious project for philosophers is to apply the agile morphism-based notion of structure in other fields as, for example, Corfield (2006) looks at cognitive linguistics. That article also describes how categorical foundations put foundations into a wider perspective: We now know that very many widely different formalisms are adequate to interpret mathematics while highlighting many different aspects of practice.

Let us close with the philosophical question of how mathematical objects are identified. On one Zermelo-Fraenkel-based story the set of real numbers $\mathbb{R}$ is identified by choosing specific ZF sets for the natural numbers, for ordered pairs, and so on through, say, Cauchy sequences of rational numbers. Perhaps

$$0 = \phi,\ 1 = \{\phi\},\ \ldots$$
$$\langle x, y\rangle = \{x, \{x, y\}\}$$

But mathematicians rarely make such choices and often contradict the choices they seem to make. Textbooks routinely define a complex number $\langle x_0, x_1\rangle \in \mathbb{C}$ as an ordered pair of real numbers $x_0, x_1 \in \mathbb{R}$ and yet equate each real number x with a complex number, $x = \langle x, 0\rangle$, which is false on any ZF definition of ordered pair I have ever seen in print.[30] Few textbooks define ordered pairs at all.

To be very clear: these facts of practice do not deny the formal adequacy of ZF to reconstruct much mathematics. They show that ZF reconstructions differ from practice on the question of how to identify mathematical objects. The difference is already clear in textbooks while it is greatest in the most highly structured mathematics with the greatest need for rigor.

In practice most structures are defined only up to isomorphism by their morphisms to and from similar structures. Section 1.4 did this for quotient rings like $\mathbb{Z}/(3)$. Section 2.2 sketched how this way of defining homology groups $H_i(M)$ not only works "in principle" but is precisely adapted to the key use of homology which is defining homology morphisms $H_i(f)\colon H_i(M) \to H_i(N)$ for each topological map

[29] Krömer (Forthcoming, Chapter 5) discusses Gelfand and Manin's view conceptually but without close comparison to the mathematics in their book. And see (Marquis, Forthcoming)

[30] It is at once easy and pointless to gerrymander a ZF definition with $x = \langle x, 0\rangle$ for all $x \in \mathbb{R}$. It would only generate other anomalies in other textbook practices.

$f: M \to N$. The morphism-based methods of working up to isomorphism are entirely standard today. Less standardized today, and less thoroughly conceptualized, are the methods of working across many levels of structures-of-structures with the corresponding levels of isomorphism-up-to-isomorphism. These occur in practice and rigorous methods are known but no unified choice of methods is yet standard. The conceptual and foundational issues around them are still debated.[31]

One view of identity has the provocative slogan that "Every interesting equation is a lie," or more moderately "behind every interesting equation there lies a richer story of isomorphism or equivalence" (Corfield, 2005, p. 74). An equation between numbers is often an isomorphism between sets. As a trivial example suppose there are as many dogs in a certain sheep pen as there are rams. The equation expresses an isomorphism of sets

$$\begin{aligned} \#(\text{dogs in this sheep pen}) &= \#(\text{rams}) \\ \{\text{dogs in this sheep pen}\} &\cong \{\text{rams}\} \end{aligned}$$

and the real interest is the specific correspondence: at this moment my dogs are facing one ram each and that is all the rams. Corfield gives practically important examples from combinatorics and topology, as our Sections 2.1 and 2.2 raised equations of Betti numbers into isomorphisms of homology groups. Turning every equation into an isomorphism is just the same thing as turning every isomorphism into an equivalence—an "isomorphism up to isomorphism." It is not clear how far this can be taken. We have seen that mathematicians cannot entirely dispense with isomorphism in favor of equivalence and so cannot entirely dispense with equality in favor of isomorphism. On the other hand, as Corfield says, philosophers have missed the real importance of equivalence as a kind of sameness of structure (2005, p. 76). Mathematical physicist John Baez has taken this viewpoint very far, originally using *n-categories* or *higher dimensional algebra* as a revealing approach to quantum gravity, but also looking at it conceptually all across mathematics (Baez and Dolan, 2001).

Philosophers are right that structural mathematics raises issues such as: how are purely structural definitions possible? and what is the role of identity versus structural isomorphism? But let us take Resnik's point that "mathematicians have emphasized that mathematics is concerned with structures involving mathematical objects and not with the 'internal' nature of the objects themselves" (Resnik, 1981, p. 529). This is already the rigorous practice of mathematics. That practice offers working answers with powerful and beautiful results.

Acknowledgements

I thank Karine Chemla, José Ferreirós, and Jeremy Gray for discussions of the topics here, and William Lawvere for extensive critique of the article.

References

Alexandroff, Paul (1932), *Einfachste Grundbegriffe der Topologie* (Berlin: Julius Springer). Translated as *Elementary Concepts of Topology.* New York: Dover, 1962.

---

[31]See fibred categories versus indexed categories in (Johnstone, 2002) and references there. Bénabou (1985) makes pointed and far-reaching claims for fibred categories.

Alexandroff, Paul and Hopf, Heinz (1935), *Topologie* (Berlin: Julius Springer). Reprinted 1965, New York: Chelsea Publishing.

Artin, Michael, Grothendieck, Alexander, and Verdier, Jean-Louis (1972), *Théorie des Topos et Cohomologie Etale des Schémas I*, Séminaire de géométrie algébrique du Bois-Marie, 4 (Springer-Verlag). Generally cited as SGA4.

Atiyah, Michael (1976), 'Bakerian Lecture, 1975: Global geometry', *Proceedings of the Royal Society of London Series A*, 347(1650), 291–99.

——— (2006), 'The interaction between geometry and physics', in Pavel Etingof, Vladimir Retakh, and I.M. Singer (eds.), *The Unity of Mathematics*, number 244 in Progress in Mathematics, 1–15 (Boston: Birkhäuser).

Baez, John and Dolan, J. (2001), 'From Finite Sets to Feynman Diagrams', in Björn Engquist and Wilfried Schmid (eds.), *Mathematics Unlimited: 2001 and Beyond*, 29–50 (Springer-Verlag).

Bass, Hyman (1978), 'The Fields Medals II: Solving Geometry Problems with Algebra', *Science*, 202, 505–6.

Bénabou, Jean (1985), 'Fibered categories and the foundations of naive category theory', *Journal of Symbolic Logic*, 50, 10–37.

Bourbaki, N. (1958), *Théorie des Ensembles* (Hermann), 3rd edition.

Carter, Jessica (Forthcoming), 'Categories for the Working Mathematician: Making the Impossible Possible', *Synthese*.

Corfield, David (2005), 'Categorification as a Heuristic Device', in D. Gillies and C. Cellucci (eds.), *Mathematical Reasoning and Heuristics*, 71–86 (London: King's College Publications).

——— (2006), 'Some Implications of the Adoption of Category Theory for Philosophy', in Giandomenico Sica (ed.), *What is category theory?*, 75–93 (Milan: Polimetrica).

Corry, Leo (1996), *Modern Algebra and the Rise of Mathematical Structures* (Birkhäuser).

Deligne, Pierre (ed.) (1977), *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 the Seminar.

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

Dieudonné, Jean (1981), *History of Functional Analysis* (Amsterdam: North-Holland).

Eilenberg, Samuel and Steenrod, Norman (1945), 'Axiomatic approach to homology theory', *Proceedings of the National Academy of Science*, 31, 117–20.

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

Eisenbud, David and Harris, Joe (1992), *Schemes: The Language of Modern Algebraic Geometry* (Wadsworth).

Faltings, Gerd (2001), 'Diophantine equations', in Björn Engquist and Wilfried Schmid (eds.), *Mathematics Unlimited: 2001 and Beyond*, 449–54 (Springer-Verlag).

Fowler, David (1999), *The Mathematics of Plato's Academy* (Oxford University Press).

Freyd, Peter (1970), 'Homotopy is not concrete', in F. Peterson (ed.), *The Steenrod Algebra and its Applications*, 25–34 (Springer-Verlag).

Gelfand, Sergei and Manin, Yuri (1996), *Methods of Homological Algebra* (Springer-Verlag).

Gödel, Kurt (1967), 'On formally undecidable propositions (excerpts)', in J. van Heijenoort (ed.), *From Frege to Gödel*, 592–617 (Cambridge: Harvard University Press).

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

——— (1958), 'The cohomology theory of abstract algebraic varieties', in *Proceedings of the International Congress of Mathematicians, 1958*, 103–18 (Cambridge University Press).

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

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

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

Hasse, Helmut (1950), *Vorlesungen über Zahlentheorie* (Springer-Verlag).

Hellman, Geoffrey (1989), *Mathematics Without Numbers* (Oxford University Press).

Herreman, Alain (2000), *La topologie et ses signes: Éléments pour une histoire sémiotique des mathématiques* (Paris: L'Harmattan).

Hilbert, David and Cohn-Vossen, S. (1932), *Anschauliche Geometrie* (Berlin: Julius Springer). Translated to English as *Geometry and the Imagination*, New York: Chelsea Publishing, 1952.

Hocking, John and Young, Gail (1961), *Topology* (Addison-Wesley).

Huybrechts, Daniel (2005), *Complex Geometry* (Berlin: Springer-Verlag).

Ireland, Kenneth and Rosen, Michael (1992), *A Classical Introduction to Modern Number Theory* (Springer-Verlag).

Jacobson, Nathan (ed.) (1983), *E. Noether: Gesammelte Abhandlungen* (Springer Verlag).

Johnstone, Peter (2002), *Sketches of an Elephant: a Topos Theory Compendium* (Oxford University Press). To be finished as three volumes.

Kline, Morris (1972), *Mathematical Thought from Ancient to Modern Times* (Oxford University Press).

Knorr, Wilber and Mancosu, Paolo (1988), 'Diophantus', in *Great Lives from History*, 632–37 (San Diego, California: Salem Press).

Kreisel, Georg (1958), 'Review of *Wittgenstein's Remarks on the Foundations of Mathematics*, (Basil Blackwell, Oxford, 1956)', *British Journal for the Philosophy of Science*, 9(34), 135–58.

Krömer, Ralf (Forthcoming), *Tool and Object: A History and Philosophy of Category Theory* (Birkhäuser).

Kronecker, Leopold (1887*a*), 'Ein Fundamentalsatz der allgemeinen Arithmetik', *Crelle, Journal für die reine und angewandte Mathematik*, 100, 209–40.

——— (1887*b*), 'Über den Zahlbegriff', *Crelle, Journal für die reine und angewandte Mathematik*, 101, 337–55.

Lafforgue, Laurent (2003), 'Chtoucas de Drinfeld, Formule des Traces d'Arthur-Selberg et Correspondance de Langlands', in Li Tatsien (ed.), *Proceedings of the International Congress of Mathematicians, Beijing 2002*, volume 1, 383–400 (World Scientific Publishers).

LANG, Serge (1993), *Algebra* (Addison-Wesley).

LAWVERE, F. William (1963), *Functorial Semantics of Algebraic Theories*, Ph.D. thesis, Columbia University. Republished with commentary by the author in: *Reprints in Theory and Applications of Categories*, No. 5 (2004) pp. 1–121, available on-line at http://138.73.27.39/tac/reprints/articles/5/tr5abs.html.

——— (1965), 'An elementary theory of the category of sets', Lecture notes of the Department of Mathematics, University of Chicago. Republished with commentary by the author and Colin McLarty in: *Reprints in Theory and Applications of Categories*, No. 11 (2005) pp. 1–35, available on-line at http://138.73.27.39/tac/reprints/articles/11/tr11abs.html.

——— (2002), 'Categorical algebra for continuum micro physics', *Journal of Pure and Applied Algebra*, 175, 267–287.

LAWVERE, F. William and SCHANUEL, S. (eds.) (1986), *Categories in Continuum Physics. Proceedings of a Workshop held at SUNY, Buffalo, N.Y., May 1982*, number 1174 in Lecture Notes in Mathematics (Springer-Verlag).

LENG, Mary (2002), 'Phenomenology and Mathematical Practice', *Philosophia Mathematica*, 10(1), 3–25.

MAC LANE, Saunders (1986), *Mathematics: Form and Function* (Springer-Verlag).

——— (1998), *Categories for the Working Mathematician* (New York: Springer-Verlag), 2nd edition.

MARQUIS, Jean-Pierre (Forthcoming), *From a Geometrical Point of View: The Categorical Perspective on Mathematics and its Foundations* (Kluwer).

MAZUR, Barry (1991), 'Number theory as gadfly', *American Mathematical Monthly*, 98, 593–610.

MCLARTY, Colin (1990), 'The uses and abuses of the history of topos theory', *British Journal for the Philosophy of Science*, 41, 351–75.

——— (2006), 'Emmy Noether's 'Set Theoretic' Topology: From Dedekind to the rise of functors', in Jeremy Gray and José Ferreirós (eds.), *The Architecture of Modern Mathematics: Essays in History and Philosophy*, 211–35 (Oxford University Press).

——— (2007*a*), 'The last mathematician from Hilbert's Göttingen: Saunders Mac Lane as a philosopher of mathematics', *British Journal for the Philosophy of Science*, 58, 77–112.

——— (2007*b*), 'The Rising Sea: Grothendieck on simplicity and generality I', in Jeremy Gray and Karen Parshall (eds.), *Episodes in the History of Recent Algebra*, ??–?? (American Mathematical Society).

MILNE, James (1980), *Étale Cohomology* (Princeton University Press).

MUMFORD, David (1988), *The Red Book of Varieties and Schemes* (Springer-Verlag).

MUMFORD, David and TATE, John (1978), 'Fields Medals IV. An instinct for the key idea', *Science*, 202, 737–739.

NOETHER, Emmy (1926), 'Abstract', *Jahresbericht DMV*, 34, 104.

——— (1927), 'Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern', *Mathematische Annalen*, 96, 26–91. I cite this from Jacobson (1983). 493-528.

RESNIK, Michael (1981), 'Mathematics as a Science of Patterns: Ontology and Reference', *Noûs*, 15, 529–50.

Resnik, Michael (1997), *Mathematics as a Science of Patterns* (Oxford University Press).

Rudin, Walter (1953), *Principles of Mathematical Analysis* (New York: McGraw-Hill).

Sarkaria, K. (1999), 'The topological work of Henri Poincaré', in I. James (ed.), *History of Topology*, 123–68 (Elsevier).

Serre, Jean-Pierre (1958), 'Espaces fibrés algébriques', in *Séminaire Chevalley*, chapter exposé no. 1 (Secrétariat Mathématique, Institut Henri Poincaré).

Shapiro, Stewart (1997), *Philosophy of Mathematics: Structure and Ontology* (Oxford University Press).

Soulé, Christophe (2003), 'The work of Vladimir Voevodsky', in Li Tatsien (ed.), *Proceedings of the International Congress of Mathematicians, Beijing 2002*, volume 1, 99–104 (World Scientific Publishers).

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

van Dalen, Dirk (1999), 'Luitzen Egbertus Jan Brouwer', in I. James (ed.), *History of Topology*, 947–64 (Elsevier).

van der Waerden, Bartel L. (1930), *Moderne Algebra* (Berlin: J. Springer).

Washington, L. (1997), 'Galois cohomology', in G. Cornell, J. Silverman, and S. Stevens (eds.), *Modular Forms and Fermat's Last Theorem*, 101–120 (Springer-Verlag).

Weber, Heinrich (1893), 'Leopold Kronecker', *Jahresberichte Deutsche Mathematiker Vereinigung*, 2, 5–31.

Weil, André (1949), 'Number of solutions of equations in finite fields', *Bulletin of the American Mathematical Society*, 55, 487–95.

——— (1979), *Oeuvres Scientifiques* (Springer-Verlag).