Annals of Mathematics and Philosophy
***vol.* 3, *no.* 1**, 2025

$M \times \Phi$

Human mathematics in the age of reasoning machines

Akshay Venkatesh

Abstract: This essay intertwines reflection on current mathematical practice with discussion of how it may be reshaped by automation. I speculate that the conceptual language of mathematics might undergo drastic rewritings, and look to historical examples for guidance.

Keywords: Automated reasoning, mathematical concepts, cryptomorphism, mathematical psychology, mathematical modernism

§ 1. — Introduction.

Mechanical reasoning will change not only how we *do* mathematics, but what it *is*; this must be renegotiated amongst its practitioners and with society. To examine this, I prefer to focus on humans rather than technology, and to try to understand mathematics in terms of the way we think about it, rather than its symbolic trappings.

In this broad spirit I shall discuss a few topics related to automation in mathematics: in §2, some discontents of mechanization and formalization; in §3 how the conceptual language of mathematics might be changed by reasoning machines; in §4 some examples of prior shifts in this conceptual language; and finally in §5 a few thoughts about the relationship of mathematics and society.

This essay is an expansion of my first Ahlfors lecture at Harvard University, entitled "(Re)imagining mathematics in an age of reasoning machines," and some of the terminology reflects that audience: "mathematics" means solely *pure* mathematics, and the pronoun "we" refers to researchers and students in this field.

§ 2. — The ghost in the machine.

Formalism and the foundational crisis. Postulational analysis. Psychological foundations of mathematics. The second life of postulational analysis.

To think about our future, we must understand why we do what we do; and for this we must engage more deeply with our own history.

The late nineteenth and early twentieth century were a period of broad disquiet in mathematics (see Gray's article [27] for a discussion of this climate). The discovery of non–Euclidean geometry, the failure of our intuition to anticipate various classes of pathological functions, the paradoxes arising from infinite sets – all these suggested that something was, perhaps, very wrong in the subject. The response to these concerns – the "foundational crisis" – shaped modern mathematics. In a manner of speaking, mathematics suffered an anxiety attack, and responded by trying to mechanize itself.

2.1. Formalism and the foundational crisis. Hilbert's 1899 text *Grundlagen der Geometrie*, an axiomatization of Euclidean geometry, greatly raised the profile of the formal-axiomatic method as an approach to foundational and metamathematical questions. A flippant phrase attributed to Hilbert by Blumenthal:

> in place of point, line, plane we must be able to say table, chair, beer glass.

captures some of its spirit, and to an even greater extent[(1)] captures the spirit of some of the work that it would inspire (see §2.2).

Thus, if our loose thinking about geometry led us into error, we could set ourselves aright by severing mathematics from that dangerous geometric intuition. In practice, this severance was to be carried out by forced externalization[(2)] of our thought process: replacing the intuitive objects by written ones that can be manipulated according to prescribed rules. Mathematics thus realized has a mechanical character; in his review [42, 44] of Hilbert's book, Poincaré already imagined putting the axioms into a "logical machine," for the idea of an automaton that would carry out tasks of mathematical reasoning was old even in 1900.[(3)]

Yet there is a deep tension here; if we became more machine-like, this machine remains haunted by the conflicting aspirations of its human creators. To illustrate this, I will look at two of the responses to Hilbert's book.

2.2. Postulational analysis. It is a slightly awkward fact that I do not really know the axiomatic definitions of group, ring, ideal, field and so on. (Should I require a left inverse, a right inverse or both? Do they have to be the same?) At some point when teaching a course one is supposed to give such a definition; my usual response is to imagine a few examples and counterexamples, and keep writing down properties until the boundary between them is firmly

(1) Hilbert's own views around this were nuanced. See [16] for a deeper discussion.

(2) The extended mind thesis of Clark and Chambers [12] gives an interesting philosophical viewpoint on externalization.

(3) Poincaré refers to the "logical piano" of S. Jevons, a machine for solving logical puzzle built in the 1870s; Babbage built his difference engine in 1820s, and *Gulliver's Travels*, written in the 17th century, already envisions a machine by means of which "the most ignorant person, at a reasonable charge, and with a little bodily labor, might write books in philosophy, poetry, politics, laws, mathematics, and theology, without the least assistance from genius or study..."

established. The result can be slightly different each time; there are, after all, different ways to axiomatize the same structure.

Hilbert's book triggered a systematic study, in the United States, of precisely this issue – "the systematic investigation of axiomatic systems for geometry, algebra, arithmetic and even mechanics," as Van Vleck was to describe it, or "postulational analysis" as it was frequently called. Thus, for example, in 1902 Edward Huntington[(4)] offers a three-axiom presentation of group, which he shortly followed with a four-axiom presentation; a little later Eliakam Moore gives a five-axiom version "very desirable from the group theoretic standpoint," and in 1905 Leonard Dickson offers a different four-axiom version. In each case, the authors painstakingly verify that each axiom is independent of the remaining ones. Such investigations were carried out for a variety of other mathematical structures too, and involved many mathematicians, including well-known names such as Theodor Hildebrandt, Oswald Veblen, R. L. Moore and (later) George Birkhoff and Norbert Wiener. See [5, 46].

Postulational analysis displays, on its surface, features that are often absorbed into the mathematical subconscious. For example, Huntington uses symbols $\oplus, \leqslant, \odot$ in his axiomatization of a Boolean algebra, in place of the more usual $+, <, \cdot$. Why so?

> On account of the circles around them they are sufficiently unfamiliar to remind us of their true character as undefined symbols which have no properties not expressly stated in the postulates; while the $+, \cdot$ and $<$ within the circles enable us to adopt, with the least mental effort, the interpretation which is likely to be the most useful. [32, p. 292]

This dual purpose notation reflects an essential tension. Those exact same mental processes that cause us to fall into error are also those that enable us to think efficiently; and, correspondingly, mathematicians have sought to live in a strange limbo between the intuitive and formal worlds.

Huntington's description [33] of postulational analysis for an audience of nonmathematicians is particularly revealing. He

[(4)] Huntington's name is perhaps not well-known to modern mathematicians. He spent his career as a teaching professor of engineering at Harvard University, and also served as president of the Mathematical Association of America. One of his mathematical contributions has had a great impact: the current apportionment of political representation used in the United States Congress is based on a system devised by Huntington and Joseph Hill.

formulates clearly where the postulates end and the human component begins:

> Theorem 18, to which I have just referred is an illustration. In the universe of discourse which we were there considering, the basic symbols within the class K were only X and $'$ but this theorem contains a new symbol, $\vee$, which came into the system by way of definition, namely: $a \vee b = (a'b')'$. The question immediately arises: Why did anyone think of introducing this particular definition? Why was this particular combination of basic symbol $(a'b')'$ regarded as of such special interest as to justify giving it a separate name? Mathematics as such gives no answer to this question, which properly belongs in philosophy, because in the last analysis it must be recognized that the construction of any abstract deductive theory is the work of some active human agent.

This human element enters not only into the definitions, but into the questions:

> For example, in Theorem 18, when once we have asked the question: "What is $a(b \vee c)$ equal to"? the postulates prohibit us from giving any other answer than "$ab \vee ac$." But there is nothing in the postulates which requires us to ask the question. The origin of the question itself must be sought in a realm far deeper than the postulates themselves, namely in the realm of human volition.

and into the choice of postulates themselves:

> The postulates adopted as the basis of any system constitute the definition of that system, within its universe of discourse; and the selection of one definition rather than another as the subject for discussion is again a matter of human volition.

Said differently, externalization does not eliminate the human element, but simply puts it out of sight and out of mind; its study, according to Huntington, "properly properly belongs in philosophy."

Certainly, in the modern era – by which I shall mean mathematics subsequent to the crisis of foundations – discussions among mathematicians about this human aspect are largely carried out in private and out of print. But such discussions have never been absent, and

become more visible in moments of tension;[(5)] the crisis of foundations was no exception.

2.3. Psychological foundations of mathematics. I have already mentioned Poincaré's review of Hilbert and its invocation of logical machines. Poincaré appreciated the significance of Hilbert's achievement, but, at the same time, expresses a sentiment closely related to Huntington's:

> Being given a sequence of propositions, he finds that all follow logically from the first. With the foundation of this first proposition, with its psychological origin, he does not concern himself. [44, p. 22]

We might imagine replacing points by chairs, but to actually do so would be ridiculous; we would never understand geometry thus expressed. The language of points, lines and planes may be formally equivalent to a language of tables, chairs and glasses, but the two are certainly not *psychologically* equivalent.

As this and other writings make clear, Poincaré did not believe that psychological considerations should be exiled, and he was not alone. Felix Klein ran an entire seminar on the psychological foundations of mathematical thought in 1912, and the intuitionism of L. E. J. Brouwer (who also coined "formalism") reflected a deep concern with its origin in human experience and judgement:

> ... the formalist wishes to leave to the psychologist the task of selecting the "truly mathematical" language from among the many symbolic languages that may be consistently developed... Not to the mathematician, but to the psychologist, belongs the task of explaining ... why we are averse to the so-called contradictory systems in which the negative as well as the positive of certain propositions are valid. [11, p 56, 58]

In his 1912 ICM address, Enriques sought to situate the foundational crisis as just the latest stage in a long history of critique of mathematical principles. About it he writes:

> If this is the conclusion that emerges from a historical view of science and criticism, logical mathematical pragmatism, far from opening an era of fantastic constructions multiplying

[(5)] Recent examples include an issue [50] of the Bulletin of the American Mathematical Society devoted to questions around machine mathematics, and Thurston's essay [48], which was written in the context of some of the challenges posed by physically inspired mathematics.

> to infinity almost for fun or whim, will have given research a higher awareness of its aims; and on the other hand, by purifying Logic, it will have demonstrated its insufficiency and the need to deepen the other psychological elements that give meaning and value to mathematical construction. ([24, Section IX]; translation by Google Translate).

This mismatch between formal language and mathematical practice – for example, that I don't actually know the exact axioms for practically any object that I work with – has been a cause of disquiet for mathematicians; the search for alternative foundations continues to this day. This search reflects, I would say, our desire for a formal language whose structure aligns with subjective human experience. For example, we might seek a language where the number of instances of the symbol Q in a given argument indicates faithfully how difficult that argument is for a human to understand. It seems to me that, in producing a formal language that could truly track mathematical thinking, we would in effect be producing a formal model of some part of our brains; understanding such a language would be tantamount to understanding our own mental processes.

2.4. The second life of postulational analysis. Postulational analysis in the spirit of Huntington's work – the study of specific axiom systems for specific structures – seems to have faded by around 1930. Broader theories of axiomatic structures, on the other hand, were very much taken up by the mathematical mainstream, for example in model theory and logic; and related ideas played a crucial role in the intellectual foundations of computer science. So it is fitting that, two decades later, the appearance of electronic computers led to a resurgence in the field that continues to the present day.(6) For, by their very design, the questions of postulational analysis were better adapted to machines than humans.

Indeed, if postulational analysis was to be done by machine, why not adapt the methodology – the rules of inference by which we are permitted to pass from one line to the next – to machines, too? This point was made in an important paper of John Robinson (1965):

(6) Indeed, there are perhaps many interesting comparisons to be drawn between postulational analysis and present trends in mathematical formalization. See, for example, Avigad's survey [3] on the "formal turn", and Macbeth's discussion [38] of stylistic differences between "traditional" and formalized mathematics. I thank Alex Kontorovich for illuminating discussions about this and pointers to the literature.

> Traditionally, a single step in a deduction has been required, for pragmatic and psychological reasons, to be simple enough, broadly speaking, to be apprehended as correct by a human being in a single intellectual act. [...] When the agent carrying out the application of an inference principle is a modern computing machine, the traditional limitation on the complexity of inference principles is no longer very appropriate. [45, p 23]

Robinson was closely affiliated with a decades-long project at Argonne National Laboratories to produce theorem-proving software, and his "machine-oriented logic" played an important role in its development;[(7)] but it came at a cost. `OTTER`, a software package developed at Argonne, was used by McCune to prove, for example, the following statement [41, Theorem 1]:

> A binary operation $x \cdot y$ and a unary operation $x \mapsto x^{-1}$ such that
>
> $$x \cdot (y \cdot (((z \cdot z^{-1}) \cdot (u \cdot y)^{-1}) \cdot x))^{-1} = u \qquad (1)$$
>
> are the multiplication and inverse operations of a group structure.

This is a *one-axiom* definition of group![(8)]. Now, here are the first three lines of the approximately thirty line mechanical proof of (1): can you figure out how to get from each line to the next?

$$\begin{gathered} x \cdot (y \cdot (((z \cdot z^{-1}) \cdot (u.y)^{-1}) \cdot x))^{-1} = u \\ \Longrightarrow\ x \cdot ((((y \cdot y^{-1}) \cdot (z \cdot u)^{-1}) \cdot (v \cdot v^{-1})) \cdot (z \cdot x))^{-1} = u. \\ \Longrightarrow (x \cdot ((y \cdot (z \cdot z^{-1})) \cdot (u \cdot x))^{-1}) = (((v \cdot v^{-1}) \cdot (y \cdot u)^{-1}) \cdot (w \cdot w^{-1})) \\ \Longrightarrow\ \cdots \end{gathered}$$

I could never use this definition in my course. Other examples of the same type abound. Such proofs can be broken into smaller

(7) Larry Wos, a pioneer of automatic theorem proving, and for a long time the director of this project, wrote in an unpublished column "... Willam F. Miller, Director of the Applied Mathematics Division at Argonne National Laboratory, invited John Alan Robinson. Miller introduced Robinson to Larry Wos and to Dan Carson, an introduction that had unbelievable consequences for the field that would eventually be called automated reasoning. While Robinson was visiting Argonne, he introduced his new inference rule that he called binary resolution. The introduction of the inference rule binary resolution changed the course of history for automated reasoning forever."

(8) It is not the first; Higman and Neumann had already provided in 1952, without computer, a one-axiom characterization of the binary operation $x, y \mapsto xy^{-1}$ associated to a group. For a full list see McCune's review [41].

steps, individually more comprehensible, but this creates a different issue, that of unmanageable length.

What we see from this is that the psychological aspects of the matter were by no means exiled by mechanical proof. For, if a machine is to provide proofs that we can understand, or be interested in, it is – whether by design or some other means – reflecting those psychological aspects that, as Enriques said, "give meaning and value" to mathematics.

§ 3. — The conceptual basis of mathematics.

The concept of a concept. How humans and machines might make different use of concepts. Concepts and economy of thought. Concepts and communication. Concepts in the age of machines.

Formal descriptions of mathematics are – partly by design, as we saw – very hard to parse. We narrate mathematics, instead, in a dialect intermediate between natural language and formal language, whose vocabulary consists of specialized terms that I will informally call concepts:

> smooth function, differentiation, modular arithmetic, group, vector space, Hilbert space, manifold, metric, Lie group, homotopy, Sobolev space, non-Riemannian hypersquare, etc.

Concepts have both a communicative and a cognitive function. They are an abridged way of recording and expressing our thought process, but they are also part of our thought process itself. Like Huntington's "combinations of symbols," what is and is not a concept is very much a matter of human choice. How might these choices change in the future?

3.1. The concept of a concept. In the end, my purpose in discussing concepts is to probe our psychological representation of mathematics. As touched on in §2.3, this is a very complicated matter, which perhaps cannot be effectively represented in any human-comprehensible way, and correspondingly I will have to leave the exact meaning of "concept" embarrassingly vague – proceeding by example rather than trying to pin down a definition

and without making sharp distinctions between (e.g) differentiation, modular arithmetic and group despite the fact that the first is a process, the second a theory, and the third an axiomatically defined mathematical entity. (Compare Wilder [55, p 425]).

Nonetheless, a few words of orientation – not to be taken too literally or formally – might help to clarify what I have in mind. We might imagine concepts to be something like nodes of a tree by which we collectively organize mathematical ideas. (Bourbaki advances a related picture [10] in relation to the organization and relationship of mathematical theories.) The uppermost levels of this tree live in the world of natural language. Concepts at lower levels are defined by reference to higher ones, and are meaningful to smaller and smaller communities. Thus, for example, an integer modulo m is "an infinite arithmetic progression with common difference m," or a Hilbert space is "a real or complex vector space V and a bilinear function on V such that..." Here "arithmetic progression", "vector space", "bilinear function" are less specialized concepts, living higher on the tree, and at least "arithmetic progression" could then be elaborated in terms comprehensible to a primary schooler.

The point I want to suggest is that this tree, like natural language, is a living organism, adapting to time and circumstance and culture.

3.2. How humans and machines might make different use of concepts. Recently DeepMind's *AlphaProof* [31] software generated a solution to the following question:

> Find all positive integers a, b such that the greatest common divisor of $a^n + b$ and $b^n + a$ is independent of n, for big enough n.

The answer is that it is only possible for $a = b = 1$. Let me contrast (without giving details) my approach to this problem with *AlphaProof*'s.

When I see such a problem, my training predisposes me to deploy a general-purpose strategy in number theory: replace arithmetic of integers by the arithmetic of integers modulo a prime. In the case above, I consider a, b with the stated property, fix a prime p, and look at the equations

$$a^n \equiv -b \text{ and } b^n \equiv -a \text{ modulo a prime number } p \qquad (2)$$

in arithmetic modulo p. When n solves these equations, then p divides $\gcd(a^n + b, b^n + a)$. So, if a, b have the desired property,

then (2) is either valid for all large enough n, or invalid for all large enough n. Now, the advantage of arithmetic modulo p is that many tools of ordinary high school algebra apply; in this case, I analyzed (2) by taking logarithms, followed by some algebraic manipulation. This suggested to me that there would be a problem in the case that ab is equal to -1 modulo p[9] , that is, when p divides $ab + 1$. Analyzing that case quickly leads to a contradiction, at least for p odd. Thus $ab + 1$ must be a power of 2, and I ruled this out by an argument modulo 4.

What about AlphaProof? AlphaProof directly guesses that it is useful to consider arithmetic modulo $ab + 1$. Who knows why? Perhaps it, in effect, tried reduction modulo many different moduli, to see which simplified the problem – I do not know, and perhaps it is unproductive to apply the metaphors of human thought to it. Now, doing arithmetic modulo a product $pqr\ldots$ of primes is in essence equivalent to doing separately arithmetic modulo p, modulo q, modulo r, etc.; and so, by working modulo $ab + 1$, AlphaProof is in effect doing arithmetic modulo all prime divisors of $ab + 1$ at the same time. Thus, in a sense, AlphaProof has collected arguments that I do in parallel (an analysis for each p separately) and collated them into one. For a trained number theorist it is not hard to go between the two points of view; but there is, again, enough psychological distance between them that the difference is worth exploring.

3.3. Concepts and economy of thought. It is by now a reflex for me, faced with a new question, to replace arithmetic of integers by the arithmetic of integers modulo a prime p, or to "reduce modulo p" in the jargon of number theorists. This process is mentally efficient, saving me time and memory space. It is usable across a large range of problems in number theory, so I don't need to remember a variety of domain-specific techniques; and doing arithmetic modulo prime numbers is greatly facilitated by the fact that I can recycle

[9] To see why this case is significant, write α, β, π for the discrete logarithms of $a, b, -1$. The equations become $n\alpha = \beta + \pi$ and $n\beta = \alpha + \pi$; multiplying the first equation by β and the second by α we find $\beta^2 + \pi\beta = \alpha^2 + \pi\alpha$. Thus the quadratic $x^2 + \pi x$ takes the same value as α, β; now, the symmetry in the graph of a quadratic shows that this will certainly happen if $\alpha + \beta = -\pi$, that is when ab is equal to -1 modulo p.

intellectual constructs familiar from early schooling such as addition, multiplication, subtraction, division and logarithms, as well as associated intuitions.

AlphaProof's limitations regarding mental space and time are very different to mine, and there is no particular reason that reduction modulo a prime should be well adapted to those limitations. It *did* use modular arithmetic, but to what is usually a composite modulus, namely, $ab + 1$. When one works in arithmetic to a composite modulus, some ordinary arithmetic carries over (addition, multiplication) but some does not (division or logarithms).[(10)] This causes a certain amount of mental stress for me, a notion whose analogue for AlphaProof remains to be investigated.

Thus seen, the concept of arithmetic modulo a prime p, or said differently the finite field with p elements, stands out to us as a feature of the mathematical universe because of its adaption to human psychology. That modular arithmetic makes effective use of analogy with an existing mental structure was already noted by Gauss, who introduced the $\equiv$ sign as a perturbation of the $=$ sign:

> We have adopted this symbol because of the analogy between equality and congruence. For the same reason Legendre, in the treatise which we shall often have occasion to cite, used the same sign for equality and congruence. To avoid ambiguity we have made a distinction. [25, §1]

Compare with Huntington's $\oplus$ notation; an extra circle, or a horizontal stroke, is all that separates the formal from the intuitive.

I offer another example to underline the role of analogy in our concepts. It is common to use Hilbert spaces of functions in analysis, for example, $L^2(\boldsymbol{R})$, or perhaps more exotic Sobolev spaces. Thus we may find an argument of the following type:

> Suppose that $\|f - g\|_{L^2} \leqslant 1$ and $\|g - h\|_{L^2} \leqslant 1$. Then $\|f - h\|_{L^2} \leqslant 2$, and if equality holds, then $g = \frac{f+h}{2}$.

You could, of course, give this argument simply by writing out all the definitions and wading through the inequalities. It would not be so hard. But the Hilbert space packages the notion of closeness in such a way that we do not have to write out the definitions

(10) Indeed, in my initial version of the argument, I made an error exactly related to this point: the proof involves working modulo p and modulo $p - 1$, and, conflating the two in my mind, I used division modulo $p - 1$ when it was not justified. So, as with other examples we have discussed, what makes modular arithmetic intuitive also makes it dangerous; and I did not even notice the mistake until I wrote it down for this essay.

every time, and it does so in a way that almost perfectly aligns with our geometric intuition about points in space, so that the last conclusion ("... then $g = \frac{f+h}{2}$") becomes obvious rather than a struggle with integrals. Thus we find our psychology, our spatial intuition, reflected in the concepts by which we encode rather sophisticated mathematics – even types of mathematics, such as the inequalities above, that do not seem on their face to be geometric in nature.

3.4. Concepts and communication. Concepts are indispensable not only for thinking, but also for sharing those thoughts – a point enunciated beautifully by Waldhausen:

> The first part of the paper, on which everything depends, may perhaps look a little frightening because of the abstract language that it uses throughout. This is unfortunate, but there is no way out. It is not the purpose of the abstract language to strive for great generality. The purpose is to simplify proofs, and indeed to make some proofs understandable at all. The reader is invited to run the following test: take theorem 2.2.1 (this is about the worst case), translate the complete proof into not using the abstract language, and then try to communicate it to someone else. [52, p. 318]

The communication of mathematics requires the creation of a peculiarly rigid shared mental image. (This can even be taken as a defining characteristic of the subject, see §5.1.) A concept well-suited to this process may not be well-adapted to thought, or vice versa; and a concept that works for one audience might fall flat with another.

For example, one of the key concepts in my recent paper [7] is that of "hyperspherical variety," which we introduce by means of five axioms. The precise definition doesn't matter here; what is relevant is that we managed to work out quite a large part of the theory before we had these axioms. What we had, in their place, was a large supply of examples of "hyperspherical varieties," a collection of operations that we could perform to produce new examples, and a list of properties that any example should have. This proved to be perfectly effective for working out a theory. [(11)] This jumble of examples, operations and properties defined, as far as our thinking

[(11)] It is by no means anomalous that a concept can exist in an informal version for a long time. Assessing the history of finite-dimensional vector spaces, Gray writes: "It is possible that the concept of a vector space is one of many which mathematicians have found they have been using for many years without knowing

was concerned, a usable concept. We could have turned it into a formal definition; but it would have been difficult to convey this definition to an outsider who did not share our mathematical context. The abstract five-axiom conception is less intuitive, but more suited to communicating with an anonymous reader.

Similar comments apply to the discussion of §2.2. I think of a group by means of a muddle of examples and properties and pictures, rather than axioms. However effective the muddle is as a thinking tool, I am unable to communicate it in a clear way. The axioms, on the other hand, can be explained, in entirety, to an undergraduate with a very limited mathematical background in a few minutes. These axioms are a spore, compact and self-contained and complete but also lifeless, vivified only through the mental effort of the listener.

By contrast, the back-and-forth of *dialogue* enables speaker and listener to converge to a shared mental picture even when the individual utterances are rather ambiguous. This sometimes permits the use of concepts that track our thought process much more closely. In this, as in other respects, the difference between the oral and written culture of mathematics is vast, and worthy of more careful examination.

3.5. Concepts and machines. Stephanie Dick has studied how mathematicians interacted with AURA (a predecessor of OTTER that was mentioned in §2.4):

> In a sense, the Argonne team used AURA to produce the preliminary "scratch work" that traditional mathematicians often use to approach a new problem. They try several cases, construct examples, and search for patterns or useful analogies in order to guide their approach to a proof. However offloading that part of the work to AURA fundamentally changed the type of insight garnered by the humans. The resulting human insights were not about the mathematical problem at hand, but about the behavior of the computer program. [22, p.502]

Interaction with machines, then, changes how *we* think and act. How might it affect our choice of concepts, in future?

Concepts package together a collection of mathematical ideas, in a way that we can absorb them or transmit them as a single chunk, frequently repurposing to that end existing intuitions and mental

it, or, perhaps one should say, needing to know it. Other examples taken at random are semigroups, long used in the theory of integral equations and even groups. "

capabilities. In this way they enable us to fit big arguments into our small minds; they reduce cognitive load, or, in the older language of Mach, they achieve *economy of thought*.

But machines, too – and even machines that are not particularly smart – can help us achieve economy of thought. Machines and concepts thereby compete for a similar function, and the availability of one will alter the use of the other. The need to reduce modulo primes, or to transport geometric intuition into functional analysis, may diminish when machines can carry out routine proofs in number theory or analysis.

It is worthy of note that mathematicians already use the word "machinery" to describe a certain class of concepts; frequently, these structure a collection of long but routine computations,[12] and are used without knowledge of all internal details. (Marquis [39] compares such machinery with the use of technology in other sciences, a parallel surely worthy of further study.) Outsourcing such computations to a machine will affect not only this "machinery," but also the various secondary concepts that interact with it, and so on. As a personal example, the appendix to my paper [1] set up an elaborate conceptual infrastructure to determine whether a single sign was positive or negative; I like the infrastructure, but if a machine could have done it, we would not have made the effort.

Concepts will still help us talk with each other. But, in the future, they may also help us talk to machines, and this will surely affect how we value them. Just as we spend our time engineering prompts and optimizing search queries in an attempt to interface with a mechanical process, so also we can expect concepts, too, to be re-engineered and optimized.

It seems possible to me that mechanical reasoning will trigger such a complete rewriting of our mathematical language and conceptual system that a current mathematician and one of the nearby future might find one another almost mutually unintelligible, at

[12] For example, Frank Adams, writing in 1971, offers the following definition at the start of a Chapter entitled "Machinery" [2, Chapter 2]: "The object of this chapter is to survey in somewhat greater detail the project mentioned in §1.7 [...] The apparatus of definitions, theorems and proofs needed to carry out this programme in detail demands a capital investment of intellectual work which may seem daunting to those not directly concerned; many readers may be able to remember feeling the same way about spectral sequences, sheaf theory or whatever is now their favorite tool; let us be glad we don't work in algebraic geometry. Topologists commonly refer to this apparatus as "machinery." "

least without a great effort. Such rewritings have already occurred many times, as I now discuss.

§ 4. — Cryptomorphism.

Rewritings of algebra in the 20th century. Weber's modular functions. Pure and applied linear algebra. Computations, concepts, and the hypergeometric function. The unreasonable effectiveness of mathematics in mathematics.

I have suggested in the previous section that machines may lead to a rewriting of our conceptual system of mathematics. Many such examples exist: Just as the same story may be differently told through the eyes of different characters, two descriptions of the same mathematics can be formally equivalent but psychologically utterly distinct, This is sometimes called "cryptomorphism," a term originally coined by Birkhoff [6, VI §11] in relation to the phenomenon, already mentioned in §2.2, that there are multiple ways to axiomatize the same structure.(13)

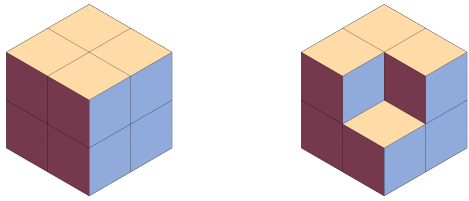
Although Birkhoff offers a formal definition, I wish to interpret cryptomorphism more flexibly to mean a translation betwen two valid classes of mathematical statements whose mental representations are distinct. As a test of distinction, we might seek problems that can be formulated in either of the "languages," but for which the different languages suggest different solutions; or we might more loosely ask whether the problems which seem natural in one language also seem natural when translated into the other.

Some cryptomorphisms can be captured in mathematical language – for example duality in projective geometry, or any interesting equivalence of categories. But my primary interest is, rather, in

(13) Birkhoff was interested in classifying algebraic structures, which he axiomatizes as sets S together with a collection of operations $f_i : S^{n_i} \to S$ for various integers n_i. When are two such "the same?" While there is an obvious notion of equivalence, this itself is not wholly satisfactory; a group, for instance, can be axiomatized by means of a binary operation $x, y \mapsto xy^{-1}$ and a unary operation $x \mapsto x^{-1}$, or equally well by means of a single operation $x, y \mapsto xy^{-1}$, or in many other ways. As Birkhoff expresses it, "a much more serious complication is associated with the fact that the *same* abstract algebra can often be defined in several nonpolyisomorphic ways." Birkhoff then says that $(S, f_1, \ldots, f_k)$ and $(S, g_1, \ldots, g_m)$ are *cryptomorphic* if, informally speaking, each f can be expressed in terms of the gs, and each g can be expressed in terms of the fs.

cryptomorphisms less amenable to simple mathematical formulations, wherein, for example, some statements have no translations, and others may have more than one.

Before considering examples taken from research mathematics, it may be helpful to illustrate this concept in a more down-to-earth and visual context. Consider the following picture –



which we may interpret either as (i) stacks of cubes or (ii) tilings of a hexagon by twelve diamonds (which come in three orientations, differentiated by shading). It is then not difficult to make a translation between a certain class of mathematical statements about tilings and a certain class of mathematical statements about stacks of cubes. But it is also evident that the mental representations are very distinct, and suggest different classes of natural questions and different approaches to their solution. Unsurprisingly, given the striking nature of the transition, this example has been extensively studied in the mathematical literature, e.g. [17, 49].

I will look at four examples in this section. They are not intended to say anything directly about machines doing mathematics; rather they serve to suggest that mutual unintelligibility is a real possibility, and to promote cryptomorphism as an interesting topic in the philosophy of mathematics.

This section assumes rather more mathematics of the reader than the others, but I hope that the general gist can be grasped without technical background.

4.1. Rewritings of algebra in the 20th century. Successive rewritings were the norm in 20th century algebra, along with the adjacent field of algebraic geometry. The viewpoint of Weber and Gordan emphasized the algorithmic and equational aspects of algebra – to a point where Weber included the theory of elliptic functions in his *Lehrbuch der Algebra*, to which we will return in §4.2. [(14)] This vision of algebra was replaced by the structural viewpoint of Noether,

[(14)] For further discussion of algebra as presented in the *Lehrbuch*, see the article [15] of Corry.

which in turn gave way to further rewritings under the successive influences of Bourbaki, Eilenberg–MacLane, and Grothendieck. In modern times the higher categorical language is again reshaping part of the field.

It is perhaps no longer clear how disorienting these changes were, or that they were in significant part rewritings of what had gone before. A few quotes from our predecessors may illustrate this. In his 1944 introduction to "Foundations of algebraic geometry," Weil writes [54]: [(15)]

> Of course every mathematician has a right to his own language – at the risk of not being understood; and the use sometimes made of this right by our contemporaries almost suggests that the same fate is being prepared for mathematics that once befell, at Babel, another of man's great achievements.

and Mattuck, reviewing in 1957 Chevalley's text on algebra, was even sharper –

> It is downright unfair for an older generation which learned these ideas in an intuitive fashion in which they were well-adapted for thought to foist off on a younger one, in the name of rigorous thinking and without any further explanation, such a construction ... [40, p. 416]

Mumford, whose advisor Zariski belonged to the generation immediately before Grothendieck, reminisced about another transition:

> One of the remarkable things is to see how various theorems were re-expressed in each new generation in different languages. Zariski and Serre were really in fact doing the same thing, but they had a totally different language for it. [43, p 103]

And the continuing need of translation, long after these developments, remains; here it is forcefully stated by my Stanford colleague Brian Conrad:

> With all due respect to the role of Andre Weil in the development of algebraic geometry, nobody should ever again have to read Weil's "Foundations of algebraic geometry": EGA must

[(15)] The quote from Weil is very curious, given the context: his book, after all, is itself a rewriting of the language of algebraic geometry, about which Oscar Zariski states that "The author justifies his procedure by an argument of historical continuity... But it is very unlikely that our predecessors will recognize in Weil's book their own familiar edifice, however improved and completed. "

> be an adequate logical starting point for the subject. Hence, if there is an important, interesting, or useful theorem whose published proofs use pre-Grothendieck methods in such an essential way so as to render them impenetrable to later generations (or to me?), and if I have a need to understand why the theorem is true and consequently I figure out a scheme-theoretic proof, then I'll try to write it up. [13]

4.2. Modular functions. As mentioned, the third volume of Weber's *Lehrbuch der Algebra* [53] happens to be devoted to the theory of elliptic functions. These are richly connected, in various ways, to algebraic topics; a general quintic equation cannot be solved by means of radicals, but *can* be solved by means of elliptic functions.

An *elliptic modular function* can be defined as a Laurent series

$$\sum_{m=m_0}^{\infty} a_m q^m \tag{3}$$

that is convergent for $0 < |q| < 1$; and, when expressed in coordinates $q = e^{2\pi i z}$, is symmetric by $z \mapsto -1/z$. In fact, all such functions can be expressed as rational functions of one particularly important example, universally denoted j, whose series expansion starts

$$j = q^{-1} + 744 + 196884q + \dots$$

While j is standard in most modern presentations, Weber puts surprising little emphasis on it. Rather, he frequently uses an arcane set of "level 2" functions f, f_1, f_2, which are specified up to finite ambiguity by j – indeed, $f^8, -f_1^8, -f_2^8$ are the roots of

$$\left(\frac{x^3 - 16}{x}\right)^3 = j. \tag{4}$$

This forces the validity of a number of other identities, for example:

$$f_0 f_1 f_2 = \sqrt{2}, f^8 = f_1^8 + f_2^8. \tag{5}$$

One can write every elliptic modular function in terms of the fs, but the fs themselves are not strictly modular functions as defined above; their transformation laws are somewhat more complicated. The function j thus provides a more elegant basis for the theory of elliptic modular functions. Why then does Weber use a more elaborate – and redundant – basis?

One of the many algebraic miracles within this theory is that, if Φ is any elliptic modular function for which the a_m from (3) are rational, then Φ takes algebraic values on any quadratic irrational z, that is, any z of the form $z = a + i\sqrt{b}$ with a, b rational. This is the theory of complex multiplication, one of the jewels of 19th century mathematics, and, perhaps, the reason that I went into number theory. The same statement is valid for the fs; but the f-values are frequently much simpler than the j-values. For example, Weber offers the following table: the values of f at $\sqrt{-11}, \sqrt{-19}, \sqrt{-43}, \sqrt{-67}, \sqrt{-163}$ are the roots of, respectively,

$$x^3-2x^2+2x-2, x^3-2x-2, x^3-2x^2-2, x^3-2x^2-2x-2, x^3-6x^2+4x-2. \quad (6)$$

This table is astounding in its simplicity to any modern number theorist who is only familiar with evaluations of j; for example, the value of j in the first case of $\sqrt{-11}$ is a root of

$$x^3 - 1122662608x^2 + 270413882112x - 653249011576832 = 0,$$

and it gets worse from there. This distinction is of little value if you have a modern computer, but for Weber, who did extensive hand computations, the advantage of the fs over j should be evident.

The translation from statements formulated in terms of j to statements formulated in terms of the fs might seem to be such a small step that it does not deserve the name of cryptomorphism. But it played a key role in the development of number theory. In 1952 Kurt Heegner, a high school teacher, solved the class number one problem of Gauss, which amounts, in the present language, to finding all quadratic irrationals z such that $j(z)$ is actually a rational number. Heegner makes full use of Weber's functions; he exploits the tension between the fact that $f(z)^2$ must satisfy a simple cubic equation, similar to (6), and that it must satisfy a second equation derived from (4).[16] At least from my point of view, the spirit of this approach is very much in line with Weber: rather than focus on the single invariant j, study the richer collection of fs and exploit the interrelationships between them. The modern theory of "Heegner points" can be seen as an outgrowth of this viewpoint [8, §3, §4].

Heegner's proof was disregarded by mathematicians until after his death; it was only after other proofs of the same result were

[16] Heegner asserts that $f(z)^2$ satisfies a cubic equation of the form $y^3 + 2Ay^2 + 2By = 2$ for certain integers A, B, and comparing with (4) he concludes that $(B - 2A^2)^2 = 2A(A^3 + 1)$. The only solutions for (A, B) are are $(0,0), (1,0), (-1,2), (2,2), (1,4), (2,14)$.

discovered that his arguments were found to be essentially valid. Imprecisions in Weber's work played a role in the dismissal of Heegner, as well as Heegner's status as outsider; but perhaps it was also relevant that Weber's explicit style had gone out of fashion. Yet it is precisely Weber's explicit style that led him to use the fs, whose interrelationships were so effectively exploited by Heegner.

4.3. Pure and applied linear algebra. Strolling on the sunny Stanford campus, I once had the following conversation with my colleague Jack Poulson, an expert in numerical linear algebra.

> "Say," he said, "I don't like how you pure mathematicians teach eigenvalues."
>
> "What's wrong with it?"
>
> "Well, it's just silly to say that you find eigenvalues by finding roots of the characteristic polynomial. If you give me a polynomial and asked me to find its roots, I would set up a matrix with that characteristic polynomial and apply the QR algorithm !"

Jack's comment illustrates the different approaches to linear algebra within different communities. The QR algorithm takes its name from a *matrix decomposition*: a way of writing a general square matrix A as a product

$$A = QR \tag{7}$$

where Q is orthogonal, and R is upper triangular. There is a variety of such matrix decompositions, and they give tools to solve many problems of linear algebra.

Matrix decompositions were not part of my education in linear algebra – at least, not in any systematic way; in general, pure mathematicians put relatively little emphasis on them. However, most of the standard matrix decompositions are equivalent to some phenomena or theorem that I encountered in linear algebra, but under a different guise. For example, I learned (7) as part of the mathematics surrounding the concept of orthonormal basis:

> Gram–Schmidt orthonormalization theorem: Given a basis $e_1, \ldots, e_n$ for the real Hilbert space V, there exists an orthonormal basis $q_1, \ldots, q_n$ for V such that the span of $e_1, \ldots, e_j$ and $q_1, \ldots, q_j$ coincide for each j. (In particular, there exists an orthonormal basis of V.)

This is equivalent to the QR decomposition: if we take $V = \boldsymbol{R}^n$ with the dot product, and collect $e_1, \ldots, e_n$ as the columns of a matrix A,

and similarly $q_1, \ldots, q_n$ into a matrix Q, then $A = QR$ for some upper triangular R.

With experience, the translation between (7) and Gram-Schmidt orthonormalization does not take too long; yet the statements have different emphases and suggest different lines of thought. The QR algorithm itself is an illustration: it amounts to iterating the process $A = QR \to A' = RQ$. Miraculously, under this iteration, A (under a genericity hypothesis) converges to an upper triangular form, whose diagonal entries give the eigenvalues of A. This is an absolutely fundamental fact of numerical analysis, for it gives a numerically stable method of computing eigenvalues, which, as Jack observed, can be used for many other problems too. The QR algorithm is *also*, from my point of view, a remarkable piece of pure mathematics; it has a rich internal algebraic structure and, for example, it is closely connected to the Toda integrable system [47]. But pure mathematicians did not discover the QR algorithm, and, at least in my informal polling, it is known to very few of us. The way we set up linear algebra makes it distinctly harder for pure mathematicians to even think of it or about it: we represent the QR matrix factorization in terms of existence theorems and constructions with bases, and the iteration $QR \to RQ$ makes little sense in this language.

In the table that follows, I list a few other standard matrix decompositions, and the contexts where I have encountered them. Except for the first, I encountered each one implicitly in a linear algebra course, and explicitly in either the theory of Lie groups or the theory of algebraic groups – not as features of matrices, but rather as properties of reductive Lie groups or reductive algebraic groups.

	matrix decomposition	**linear algebra**	**Lie groups/algebraic groups**
i.	$A = X\Lambda X^{-1}$, Λ diagonal A symmetric, X orthogonal	existence of orthonormal eigenvector basis	conjugacy of maximal tori
ii.	$A = QR$ R triangular	implicitly, Gram-Schmidt orthogonalization	Iwasawa decomposition
iii.	SVD: $A = U\Sigma V$ U, V orthogonal, Σ diag.	implicitly, simult. diag. of quadratic forms	Cartan decomposition
iv.	$PA = LU$, P permutation, L lower, U upper	implicitly row reduction	theory of algebraic groups Bruhat decomposition

Expositions of linear algebra aimed at pure mathematicians tend to put less emphasis on matrix decompositions than expositions aimed at, say, numerical analysts. The two fields have made

differing choices about the appropriate level of generality and applicability. The pure mathematician's approach to linear algebra is concerned with operations that make sense over any field, that is, any notion of scalars that admit addition, multiplication, subtraction and division. An idea in linear algebra that is specific to *real scalars* may be considered overly specialized for this context, and might then be transferred to a different one – for example, the theory of real Lie groups. A numerical analyst is, by contrast, primarily concerned with operations that make sense for real scalars, and moreover those operations that are numerically stable; thus they will, typically, emphasize the singular value decomposition over the eigenvalue decomposition. It is easy to imagine both fields making different choices, which, likely, would have led to different conceptualizations of linear algebra.[17]

4.4. Computations, concepts, and the hypergeometric function. An even more essential difference between the pure and applied approach to linear algebra lies in the fact that, in the former approach, matrices are not a primary object at all, but a computational tool. The more fundamental object, in the pure mathematician's presentation, is much more abstract: a linear transformation between vector spaces. A matrix is "just" a representation of that object. This replacement of an algorithmic concept by a more abstract one is a characteristic feature of modern mathematics.

Yet the language of finite-dimensional vector spaces, a conceptual repackaging of the more algorithmic language of matrices and vectors, has largely failed to find purchase outside of pure mathematics. And, more generally, whatever the elegance of abstract concepts, the algorithmic form sometimes proves more organic and more durable - a point eloquently formulated by Demazure in relation to elimination theory,

> But *the objects are stubborn* and explicit methods do not stop resurfacing. A calculation is always more general than the theoretical framework in which it is confined at a given period. The resolution of the second-degree equation, originating with Babylonian tablets (and introducing the first discriminant of History), reappears in the decomposition into squares of

[17] For example, the pure mathematician might have been concerned with operations that make sense over general rings or skew-fields, and the applied mathematician might have sought operations that are stable not against small perturbation of the entries, but against perturbation of a small number of entries (as is indeed done in computer science).

> quadratic forms, in the Legendre-Gauss least-squares method, in Gram-Schmidt orthonormalization ... [21, p. 336] [(18)]

Intricate calculations at times feel to be a form of manual work: the hand and the paper carries out the thought, and not the mind. The replacement of this process by a conceptual infrastructure is an attempt to *internalize* the process, to render this manual computation cognizable and communicable. Yet this is exactly the opposite of the impulse animating formalism, which seeks to *externalize*, to pass mathematical thought from mind to paper or machine. This is a curious tension. Put it in a different way: a computational presentation of a result is already a formalist account of it, that is, a step-by-step processing according to defined inferential rules. Mathematicians frequently chose a more elaborate encoding, where the computational account was first replaced by a conceptual one, and then the conceptual one recast in an axiomatic framework.

Special functions offer an interesting example of the replacement of computations by abstractions. In pure mathematics, at least, they have largely been pushed to the margins; yet their shadows can be glimpsed in many contemporary theories. To illustrate this, let us look at the miraculous *hypergeometric function* of Euler and Gauss:

$$ {}_2F_1(a,b;c;z) = \sum \frac{(a)_n (b)_n}{(c)_n n!} z^n \quad (a)_n = a(a+1)\dots(a+n-1) $$

It participates in a dazzling array of beautiful identities, some of which I list below. These identities are rarely taught nowadays; certainly I never encountered them in any course (and what a loss!) But thse identities are nonetheless captured in different ways by topics that *are* still taught, because:

(a) in representation theory, the ${}_2F_1$ give an explicit way of writing irreducible representations of the group $\mathrm{SL}_2(\boldsymbol{R})$ in coordinates, a special case of a point of view advocated by Vilenkin [51].

[(18)] I thank James Parson for bringing Demazure's paper to my attention. In the original it reads: "Mais *les objets sont têtus* et les méthodes explicites ne cessent de ressurgir. Un calcul est toujours plus général que le cadre théorique dans lequel on l'enferme à une periode donnée. La résolution de l'équation du second degré, provenant des tablettes babyloniennes (et introduisant le premier discriminant de l'Histoire), repararaît dans la décomposition en carrés des formes quadratiques, dans la méthode des moindres carrés de Legendre-Gauss, dans l'orthonormalisation de Gram-Schmidt..."

(b) the differential equation satisfied by ${}_2F_1$ only involves polynomials in z and $\frac{d}{dz}$, and this gives a sense in which ${}_2F_1$ can be imported into pure algebra. This gives rise to the theory of hypergeometric D-modules and its even more algebraic incarnation, hypergeometric sheaves, as studied in great depth by Katz [34].

I set myself an exercise analogous to that of §4.3, of going through a list of standard identities for ${}_2F_1$ and trying to translate them into the much more abstracted languages (a) and (b). One finds that indeed (a) and (b) give natural and transparent explanations of *some* of the formulas; but – reflecting Demazure's comments – neither one gives *all* of them. In fact, some of the formulas do not really fit inside either framework.

A ?? in table 1 below means that I don't see immediately a "natural" way of deriving the specified formula from the given point of view. Perhaps the most interesting entry of this table is the last one. It was discovered by Heine and others that the entire theory of hypergeometric series admits a q-deformation: a systematic way of altering the terms to involve an additional parameter q in such a way that many of the identities remain valid. The same deformation was discovered much later in the representation-theory context (quantum groups) and seems to still not be entirely clear in the algebro-geometric context (it is presumably related to the q-deformed de Rham cohomology). In both cases, these are topics that touch the deepest parts of the modern theory, and yet they exhibit a deep parallel to symbolic identities that predate modern mathematics entirely.

4.5. The unreasonable effectiveness of mathematics in mathematics. A new set of concepts can evolve out of another, but the example we have just discussed illustrates a yet more remarkable phenomenon. Time and time again, the stories that mathematicians tell have unexpectedly collided with one another, which David Corfield has dubbed "the unreasonable effectiveness of mathematics in mathematics" [14].

[1]Katz describes the translation process, in relation to this example: "Our key observation is that formally, this integral is the additive convolution of $f(x) := x^{a-c}(1-x)^{c-b-1}$ and $g(x) := x^{-a}$. We then view $f(x)$ as incarnating a rigid local system, and $g(x)$ as incarnating a Kummer sheaf on $\mathbb{G}_m$, and think about forming the additive convolution of two such objects. In some sense, our entire book consists of first making sense of this, and then exploiting it."

property of ${}_2F_1(a,b;c,z)$	representation theory	algebraic geometry
at $z=1$ equals $\frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)}$	asymptotics of matrix coefficients	??
functional equations under $a,b,c \leftarrow a\pm 1, b\pm 1, c\pm 1$	translation functors	rigidity of underlying local system
$= \int_0^1 t^{b-1}(1-t)^{c-b-1}(1-zt)^{-a}$	(simple) computation	(middle) convolution [1]
$= \int \frac{\Gamma(a+s)\Gamma(b+s)\Gamma(-s)}{\Gamma(c+s)} \frac{z^s}{2\pi i}$ (Mellin–Barnes)	duality	??
continued fraction	??	??
Clausen: ${}_2F_1^2 = {}_3F_2$	??	symmetric square of local system
algebraic transformation in z	??	Belyi maps
$z(1-z)F'' + (c-(a+b+1)z)F' = -abF$	Casimir operator	flat connection
q-deformation ${}_2\varphi_1$	quantum groups	q-deformed de Rham cohomology (?)

TABLE 1.

There are too many such examples to readily enumerate here, but I list a few that are near to my heart: Dedekind and Weber [19] found the language of ideals and ring extensions an appropriate tool with which to recast the theory of Riemann surfaces; the collaboration of Eilenberg and Maclane was triggered [23] by a coincidence between computations in algebra and topology; that compact connected Lie groups come in pairs was discovered

independently by mathematicians [36] and physicists [26] – two occurrences in vastly separated fields that were later found [35] to be related. About yet another recent convergence, that of higher category theory and topology, John Baez memorably writes:

> It's sort of like climbing a mountain, surmounting steep cliffs with the help of ropes and other equipment, and then finding a Holiday Inn on top and realizing there was a 4-lane highway going up the other side. [4]

What are we to make of these coincidences, which verge on the miraculous? Do they tell us about the unity of the world, the interconnectedness of mathematical culture, or the limitations of our own minds? I prefer to take away the following message: part of the essence of doing mathematics is to tell the same story a thousand times in a thousand tongues.

§ 5. — Looking out.

Davis–Hersh thesis. Valuing communication.

There are many possible visions for the conceptual landscape of mathematics in the world of automated reasoning. Which one we choose depends very much on what we want mathematics to be.

It is often implicitly supposed that we all agree on the answer to this. I do not think this is the case, and even if it were, the question must be considered afresh by each generation. But mathematicians cannot consider it in isolation; we must engage, and indeed re-engage, with the world around us. I will conclude with some reflections related to this.

5.1. The Davis–Hersh thesis. In thinking about the human role of mathematics, I find the following thesis formulated by Davis and Hersh very useful:

> The study of mental objects with reproducible properties is called mathematics. [18, p. 399]

Of course, similar ideas have been put forward by others; Davis and Hersh provide us with a particularly pithy formulation.

What does this mean? A story changes from person to person; the words mean slightly different things for different people, and

alter with each passage. The communication of mathematics is far less subject to this type of alteration. If I describe the concept of "right angle" you may forget it, but you are unlikely to remember it in a slightly incorrect way; the concept of right angle is a rigid one. For a wonderful discussion of mathematics centered around this thesis, see Borovik [9].

One can quibble in many ways. "Mental objects" do not adequately account for the role of externalized thinking, such as written calculations, and they fail to shed light on the phenomenon of cryptomorphism, which amounts to surprising relations between different reproducible mental objects. Reproducibility comes in shades; activities such as music and poetry too have strong reproducible characteristics. And we cannot forget that there is an enormous cultural influence on what constitutes a reproducible mental object– consider the staggering effort required to condition our minds to use the letters and numbers upon which our mathematics rests.

But the Davis–Hersh thesis has two essential features that make it uniquely suited to our present purpose: it situates mathematics as a *human* activity ("mental objects") and as a *social* activity ("reproducible properties"). This makes it a convenient framework for understanding the role of mathematics in human culture. Reproducible mental structures provide psychological certainty and aesthetic satisfaction; they support precise communication and scientific understanding; and they mediate agreement – all of these are functions that are likely to persist even in an era of ubiquitous and intelligent machines.

Thus, for example, if science is the study of reproducible properties of nature, it is only natural, if somewhat glib, to conclude that a mental model of science must be inevitably be a reproducible cognitive object, and thereby, from this point of view, tautologically mathematical. It is similarly evident that mental reproducibility should be relevant to mediating, and to some extent forcing, agreement; such agreement can be seen as the basis for the widespread mathematization of knowledge in modern culture. For the facts of arithmetic are facts we must all agree on, without necessarily knowing about their interpretation; we all agree Mount Everest is the tallest mountain in the world because its height is greater than

the heights of all other mountains, but we tend not to inquire what precisely the height of a mountain actually measures. [19]

5.2. Valuing communication. Thus mathematics in the broad sense plays fundamental human roles. But the more advanced the mathematics, the more tenuous its link to these human functions.

The concepts mentioned in §3, such as Hilbert spaces and rings, indeed possess the character of mental replicability – but their replication takes great effort. It takes place only within the massive infrastructure of training and education bridging the gap between natural language and the modern language of pure mathematics, and the continued existence of that infrastructure cannot be taken for granted.

The separation of mathematical from natural language is part of a broader theme, the separation of mathematics as an intellectual tradition from the broader academic and cultural discourse. This is part of what the historian Jeremy Gray has called the "modernist transformation" of mathematics:

> Here, modernism is defined as an autonomous body of ideas, having little or no outward reference, placing considerable emphasis on formal aspects of the work and maintaining a complicated—indeed, anxious—rather than a naïve relationship with the day-to-day world... [28, §1.1.1]

The development of mathematics as an autonomous research field enabled us to probe structures of profound complexity, to a depth that could never have been matched were we constantly called to account by the society around us. But this came at a very high cost. As we forgot more and more about the rest of human thought – and here I include humanities and the arts as much as the sciences – we also developed a creeping amnesia about ourselves; we lost the narratives that help us understand the "value and meaning" of what it is that we are doing.

Of course, most mathematicians would agree there is *something* very special about doing mathematics, or we would not do it; we experience it as an activity with intrinsic meaning, one that requires little external validation. But our ability to share this experience outside the narrowest circle of peers has become diminished, and the loss is ours, too.

[19] The relationship between mathematics and consensus runs both ways. Lloyd [37, Chapter 3] discusses the relationship, in Ancient Greece, between the concept of proof, and the need of persuasion in politics and law.

Despite this gulf, our mathematics remains, in the final analysis, a servant of the broader culture around us. It is a tool for individual and collective thought and will only survive to the extent that it remains useful as such. And while our relationship to knowledge and scholarship will surely be transformed by artificial reasoning, just as it was transformed long ago by writing, the need for thought, alone and together, remains undiminished. Mathematics surely has its role to play in this, but we cannot take for granted that this role looks the same as it did in the past.

Thus, as mathematicians consider our future, our thinking about how the field should evolve cannot stop at our doors. Rather, we need to engage in a much more serious dialogue with the intellectual world outside our borders; and for this we need to recenter *communication* in our conception of mathematics. As is so eloquently expressed by Davis and Hersh, communicability is not an afterthought to mathematics, but part of its very definition.

§ 6. — Acknowledgements.

I thank the Harvard mathematics department for its kind hospitality, and the attendees of my lecture for generously engaging with my eccentric choice of topic.

I would also like to thank Stephanie Dick for interesting conversations about the history of automation and mathematics, and Michael Harris for tirelessly advocating for a deeper engagement between mathematics and the humanistic disciplines. And I am deeply grateful to my colleagues Jeremy Avigad, Aravind Asok, Mathilde Gerbelli-Gauthier, Diana Gillooly, Alex Kontorovich, Pat Shafto, and Jesse Wolfson, and no less to the two anonymous referees. Their careful reading and criticisms of this essay sharpened my thinking and reshaped its final form.

§ — Bibliography.

[1] **A. Abdurrahman** and **Akshay Venkatesh**, *Symplectic L-functions and symplectic Reidemeister torsion* (*mod squares*). Invent. Math. 241, (2025), 717–839.

[2] **J. F. Adams**, *Infinite Loop Spaces*, Annals of Mathematics Studies, 90, Princeton University Press, 1978.

[3] **J. Avigad**, *Mathematics and the formal turn*, Bulletin of the AMS, 61 (2), (2024), pp. 225–240.

[4] **J. Baez**, *This week's finds in mathematical physics* (*week 233*), https://math.ucr.edu/home/baez/week223.html

[5] **J.H. Barnett**, *An American Postulate Theorist: Edward V. Huntington.* In: Zack, M., Landry, E. (eds) Research in History and Philosophy of Mathematics. Proceedings of the Canadian Society for History and Philosophy of Mathematics/La Société Canadienne d'Histoire et de Philosophie des Mathématiques. Birkhäuser (2016).

[6] **G. Birkhoff**, *Lattice theory*. 3rd edition. American Mathematical Society Colloquium Publications, Vol. 25, American Mathematical Society, 1967.

[7] **D. Ben-Zvi, Y. Sakellaridis** and **Akshay Venkatesh**, *Relative Langlands duality*, https://arxiv.org/abs/2409.04677.

[8] **B. Birch**, *Heegner Points: The Beginnings*, in Heegner Points and Rankin L-Series, Mathematical Sciences Research Institute Publications 49. Cambridge University Press, 2004.

[9] **A. Borovik**, *Mathematics under the Microscope: Notes on Cognitive Aspects of Mathematical Practice.* American Mathematical Society, 2010.

[10] **N. Bourbaki**, *The Architecture of Mathematics*. The American Mathematical Monthly, 57(4), (1950), pp. 221-232.

[11] **L.E.J. Brouwer**, *Intuitionism and formalism* (translated by Arnold Dresden), Bull. Amer. Math. Soc. 20 (1913), 81–96.

[12] **A. Clark** and **D. Chambers**, Analysis, *The extended mind analysis,* Analysis, 58(1), (1998), 7-19.

[13] **B. Conrad**, https://math.stanford.edu/~conrad/, point 2 of "Notes."

[14] **D. Corfield**, *Towards a Philosophy of Real Mathematics*. Cambridge University Press, 2003.

[15] **L. Corry**, *Heinrich Weber, Lehrbuch der Algebra* (*1895–1896*), in *Landmark Writings in Western Mathematics, 1640–1940*, I. Grattan-Guinness (Editor), Elsevier 2005.

[16] **L. Corry**, *The Origin of Hilbert's Axiomatic Method*. In: Jürgen Renn et al (eds.) *The Genesis of General Relativity, Vol. 4: Theories of Gravitation in the Twilight of Classical Physics: The Promise of Mathematics and the Dream of a Unified Theory,* New York, Springer (2006), 139-236.

[17] **G. R. David** and **C. Tomei**, The problem of the calissons, Amer. Math. Monthly, 96(5), (1989), 429–431.

[18] **P. Davis** and **R. Hersh**, *The Mathematical Experience*, Birkhaüser Boston, 1981.

[19] **R. Dedekind** and **H. Weber**, *Theorie der algebraischen Funktionen einer Veränderlichen*, Journal für die reine und angewandte Mathematik 92 (1882), pp. 181–290.

[20] **P. Deift, L. C. Li, C. Tomei**. *Matrix factorizations and integrable systems*, Communications on Pure and Applied Mathematics 42(4), (1989), pp. 443-521.

[21] **M. Demazure**, *Résultant, discriminant.* Enseign. Math. 58(3–4), (2012), pp. 333–373.

[22] **S. Dick**, *AfterMath: The Work of Proof in the Age of Human–Machine Collaboration*, Isis 102(3), (2011), pp. 494–505.

[23] **S. Eilenberg**, and **S. MacLane**, *Samuel Eilenberg and Categories*. Journal of Pure and Applied Algebra 168, (2002), pp 127–131.

[24] **F. Enriques**, *Il significato della critica dei principii nello sviluppo delle matematiche*. Proceedings of the International Congress of Mathematicians, Cambridge University Press, volume 1, (1913), pp 68–79.

[25] **K.F. Gauss**, *Disquisitiones Arithmeticae*, translated by Arthur A. Clarke. Springer–Verlag, 1986.

[26] **P. Goddard, J. Nuyrs** and **D. Olive**, *Gauge theories and magnetic charge*. Nuclear Physics B, 125(1), (1977), pp. 1–28.

[27] **J. Gray**, *Anxiety and abstraction in Nineteenth-Century Mathematics.* Science in Context, 17(2) (2004), pp. 23–47.

[28] **J. Gray**, *Plato's Ghost: The Modernist Transformation of Mathematics.* Princeton University Press, 2008.

[29] **I. Hacking**, *Why Is There Philosophy of Mathematics At All?*, Cambridge University Press, 2014.

[30] **M. Harris**, *Silicon Reckoner*, https://siliconreckoner.substack.com/.

[31] **Hubert, T., Mehta, R., Sartran, L.** et al. Olympiad-level formal mathematical reasoning with reinforcement learning. Nature (2025).

[32] **E. Huntington**, *Sets of Independent Postulates for the Algebra of Logic*, Transactions of the American Mathematical Society, 5(3), (1904), pp. 288-309.

[33] **E. Huntington**, *The method of postulates*, Philosophy of Science 4(4), (1937), pp. 482-495.

[34] **N. Katz**, *Rigid local systems*. Annals of Mathematics Studies, 139 (1996). Princeton University Press.

[35] **A. Kapustin** and **E. Witten**, *Electric-Magnetic Duality And The Geometric Langlands Program*. Communications in number theory and physics, 1(1), (2007), pp. 1–236.

[36] **R. Langlands**, *Letter to A. Weil*, https://publications.ias.edu/rpl/paper/43, 1967.

[37] **G. E. R. Lloyd**, *Demystifying Mentalities*, Cambridge University Press, 1990.

[38] **H. MacBeth**, *Algorithm and abstraction in formal mathematics.* In: Buzzard, K., Dickenstein, A., Eick, B., Leykin, A., Ren, Y. (eds) *Mathematical Software – ICMS 2024.* Lecture Notes in Computer Science, 14749 (2024), pp. 12-25.

[39] **Jean-Pierre Marquis**, "A Path to the Epistemology of Mathematics: Homotopy Theory," in *The Architecture of Modern Mathematics: Essays in History and Philosophy*, ed. José Ferreirós and Jeremy J. Gray, Oxford University Press, 2006, pp. 239–260.

[40] **A. Mattuck**, *Review: Claude Chevalley, Fundamental concepts of algebra*, Bull. Amer. Math. Soc. 63(6), (1957), pp. 412-417.

[41] **W. McCune**, *Single axioms for groups and Abelian groups with various operations.* Studies In Automated Reasoning, 10, (1993), pp 1.-13.

[42] **C. McLarty**, *Poincaré on the value of reasoning machines.* Bulletin of the AMS 61(3), (2024), pp. 411–422.

[43] **C. Parikh**, *The Unreal Life of Oscar Zariski*, Springer, 2009.

[44] **H. Poincaré**, (translated by Arnold Dresden): *Poincaré's review of Hilbert's Foundations of Geometry*. Bull. Amer. Math. Soc. 10(1), (1903), pp. 1-23.

[45] **J.A. Robinson**, *A Machine-Oriented Logic Based on the Resolution Principle*. Journal of the ACM, 12(1), (1965), pp. 23–41.

[46] **M. Scanlan**, *Who were the American postulate theorists?* The Journal of Symbolic Logic, 56(3), (1991), pp. 981-1002.

[47] **W. W Symes**, *The QR algorithm and scattering for the finite non-periodic Toda lattice*, Physica D, 4(2), (1982), pp. 275–280.

[48] **W. Thurston**, *On proof and progress in mathematics*, Bull. Amer. Math. Soc. (new series) 30(2), (1994), pp 161–177.

[49] **W. P. Thurston**, Conway's tiling groups, Amer. Math. Monthly 97(8), (1990), pp. 757–773.

[50] **M. Fraser, A. Granville, M. Harris, C. McLarty, E. Riehl, Akshay Venkatesh**, *Will machines change mathematics?* Bulletin of the American Mathematical Society 61 (2), (2024), pp. 201–202.

[51] **N. Ja. Vilenkin**, *Special Functions and the Theory of Group Representations*. Translations of Mathematical Monographs, volume 22, American Mathematical Society, 1968.

[52] **F. Waldhausen**, *Algebraic K-theory of spaces*, Springer Lectures Notes in Mathematics 1126, (1985), pp. 318–419.

[53] **H. Weber**, *Lehrbuch der Algebra, vol 3: Elliptische funktionen und algebraische Zahlen*, Braunschweig F. Vieweg, 1908.

[54] **A. Weil**, *Foundations of Algebraic Geometry,* American Mathematical Society Colloquium Publications, vol. 29, American Mathematical Society, 1946.

[55] **R. Wilder**, *The origin and growth of mathematical concepts*, Bull. Amer. Math. Soc. 59 (5), (1953), pp. 423–448.

Akshay Venkatesh
Institute for Advanced Study