The philosophy of dynamical algebra

The title is an allusion to the book Philosophie de l'algèbre by Jules Vuillemin of the 60s. It deals e.g. with the meaning of solving a polynomial equation. Dynamical algebra is also about this, but let us speak about this later. There are three words in the title; I don't feel the need to speak about the last one, « algebra », because it is not really fundamental here, it is just the domain I shall speak about; but there is something I wish to stress: as algebra is about solving equations, it is natural to imagine it as a concrete business that deals with algorithms — so it is surprising that algebra has become so abstract (abstract structures, abstract level of discourse) and so noneffective (proving existence without effective access to the solution because one in fact proves the absurdity of non-existence; using noneffective procedures, i.e procedure that we cannot effectively apply, prominently an infinity of choices, but also to distinguish indiscernibles). The core of this course will deal with the epithet « dynamical », so please wait. I presently feel the urge of justifying the word « philosophy ». In my opinion, philosophy need not be a discourse about algebra, I rather call for a philosophy of algebra as a specific component of algebra. But which component is it? In order to state my point, let me use the words of this school: « proof » and « computation ». In French, « calcul » is used only for computing the date of Easter, and for this you combine certain data of the ephemerids: the date of the equinox, the date of full moon, and you get a certain result. So to compute is just to follow certain rules that transform certain data into other data. There are also interesting reflections to be had here, but let us presume that this is perfectly clear to us, and consider computation as formal. But how do we know what the computation is about? One way of knowing is to spell out what the result of the computation is supposed to provide and to prove that the computation is actually providing

it. (One speaks about showing the correction of an algorithm.) In doing so, one is in a specific mindset of transporting the truth of the initial data through every step seen as a kind of dangerous jump in which evidence must be preserved by convincing ourselves that what ought to be preserved is actually preserved. How does philosophy step in here? I don't believe that there can be an exhaustive answer to this question, so I will just try to collect a few occurrences: ① what is the computation actually about? Is it possible to clarify how the object of the actual discourse is replaced by another one, by a different kind of dangerous jump in which the transport ought to be provided in both directions? This jump is most prominently the «abstractions» in which a certain structure is considered to allow certain objects to be freed from certain contingencies and the relationships between them to be revealed. In a nutshell, philosophy can be about the ontology of mathematical objects. ② What is the computation actually doing? What meaning do the images that we rely on for this understanding actually have? There are spatial images, temporal processes, graph-like structures, most prominently diagrams, combinatorics of signs. How do they acquire their meaning? There is practice, which is in some sense an adequation of the mental structure of the mathematician with the structure under study. ③ Philosophy can also be about the nature of this relationship and especially about keeping alive, i.e. in process, in change, in becoming, thus about the position and nature of the mathematician.

All that has been addressed has actually also become part of mathematics itself in a process that has been called reflection: our own way of understanding is meaningful to us and leads to elaborating specific mathematics that express this meaning. Thus, to do philosophy of algebra, of mathematics, is about being a mathematician in the search of understanding his own activity, and this is mathematically fruitful; it is at least a way of approaching the progress of mathematics, and also a way of empowerment of the mathematician.

Ideal objects

Dynamical algebra arises as a reflection on the computational content of ideal objects. There is a huge philosophical reflection on ideal objects that I do not wish to enter. I rather see this course as a particularly perspicuous analysis of two ideal objects that should trigger people to think about their conception of ideal objects in general. The very reason for this is again philosophical: it is a matter of fact that people have very different views on the principle of mathematics, i.e. on their beginnings, roots in our understanding of things. For me they are rooted in life itself, and for me it is important that these roots themselves are alive, that the fluids necessary for blooming are circulating from them and back to them. But there are much more pragmatic views. The question is how much of a private issue this is, and how much one ought to speak about it or rather mute it out. For me, to speak about it is definitely part of the mathematical business, and it is a part I like to call philosophy and of which I wish to stress the proficiency.

Let us get back to ideal objects. The most simple object that has come to my mind is the following: the minimal element of a set of integers (≥ 0). Why is it ideal? In the sense that there is no effective way of getting it if I am given a set of integers that is infinite. One may think that this means that it is meaningless, just by expressing that a meaning is a way of effectively accessing it. Are there weaker forms of meaning than this one? The one we shall be particularly interested in is that we know how to disprove that an element is minimal: by exhibiting a still smaller one. The dynamical point of view is then to make sense out of a potentially minimal element, i.e. an element that is regarded as minimal not in an effective way (with a proof that all elements are bigger than this one) but in a provisional way (with an expression of the situation in which it is considered as minimal and with an expression of the situation in which it turns out that it is not minimal, or an expression of how our previous knowledge is affected by the discovery of a still smaller element).

I have said enough to ring many bells in the head of certain people present here, and these bells have names like Kripke semantics, backtracking, game semantics, sheaf semantics, toposes. Those people are able to spell out everything I say in such terms, and it is the ambition of note to come to do that, but it is not the aim of this course, which tries to put in motion philosophical reflections about simple historically relevant situation. Before doing so, I want to give an application of this simplest example, well known to many. You may have seen the definition of the gcd of the integers a and b as the minimal element >0 among those that have the form $ua+vb$ with u and v integers, and here there is about an effective way of getting it, because the plain meaning of this is to consider the element >0 among $a, b, a+b, a-b, -a+b, -a-b, 2a, 2b, -2a, -2b, 2a+b, a+2b, 2a-b, a-2b, -2a+b, -a+2b, -2a-b, -a-2b$, etc. and to pretend that one of those is d minimal. Let us look at the proof that d is a gcd: suppose that d does not divide a: then the remainder of the euclidean division of a by d has the form $a-qd$, i.e. $a-q(ua+bv)$, i.e. $(1-qu)a-qvb$, and is smaller than d. The same argument works if d does not divide b. We have here an example of a typical scheme: the use of an ideal object in an argument by contradiction. The ideality of the element is spelled out by the argument by contradiction; its feature is that its ideality makes it win beforehand against every competitor. The dynamical counterpart to this ideal object is to start with any $d>0$ of the form $ua+vb$, e.g. b. If it divides a and b, we are done because every divisor of both a and b divides d. Otherwise, the argument above shows how to obtain a new d which is smaller than the former one, which is still of the form $ua+vb$. This change of d can only happen a finite number of time because a decreasing sequence of integers stops. This means that one gets a', d' such that $d' \mid a$; $d' \mid b$; $d' = ua+vb$. Some more reflections on the proof: it is a remarkable fact to have found the form $ua+vb$ as the important invariant when turning from a provisional minimum to a new provisional minimum. This is in fact the main point in the ideal object we have considered, and the dynamical method explains its relevance and connects it with the proof of correction of the algorithm.

The philosophy of dynamical algebra: day 1

I wish to state more precisely certain points of my course of day 1.

- My vocabulary does not try to introduce what I consider technical distinctions: I am using different words to express the same thing because sometimes this is useful to approach it.
  - I have used the expression of ideal object for a concept of which we might know many concrete instances, but for which in itself there is a problem of effectiveness. I might have (or used) other words: existence, constructiveness, access, clarity/obscurity, computability. Each of these words refers to something different, or to a different aspect of the problem. Some words have the advantage of having an unambiguous meaning, but it is also good to use the more ambiguous ones because their ambiguity expresses by itself aspects of the problem.

- When I address mathematics, I think that there is one and only mathematics, the one at the highest level of discourse, sometimes called the metalevel, or metamathematical level. The specificity there is that (by definition) we are outside any kind of formal structure, axiomatic system, and that only our intimate conviction secures what is going on, together with our intersubjective sharing of this experience. We are often led to postulating certain things and more generally to put up formal structures, axiomatic systems, calculuses, and then our conviction is about them like about any mathematical object, and we also take up the burden of justifying these objects, i.e. of explaining their meaning.

Let us give again the ingredients of the classical proof that the module generated by integers a and b is principal and gives a dynamical analysis.

Let d be the minimum of the set of the $ua+vb>0$. Then every element of this form is a multiple of d, for the euclidean division of a multiple of d by d gives a positive remainder $<d$, also of the form $ua+vb$.

Let d be a provisional minimum of the $ua+vb$, e.g. a. If d does not divide a and b, then the remainder of the euclidean division by d gives a better provisional minimum, affect it to d. Repeat this step. It can happen only a finite number of times because a decreasing sequence of integers stops. We obtain thus a common divisor d of a and b of the form $ua+vb$, and therefore every element of this form is a multiple of d (and obviously reversely).

Remarks: There are no new ingredients in the dynamical analysis, but they are reorganised. It is worthwhile to recognise which ingredient is more what with respect to the presentations of algorithms today.

(A) Mathematics is common sense.
(B) Do not ask whether a statement is true until you know what it means.
(C) A proof is any completely convincing argument.
(D) Meaningful distinctions deserve to be maintained.

P. Halmos, Schizophrenia in contemporary mathematics, 1973

Krull's fundamental satz for integral domains.

Let I be an integral domain, K its field of fractions, $G = K^*$ the multiplicative group.

Think of $I = \mathbb{Z}$, $K = \mathbb{Q}$, $G = \mathbb{Q}^*$. The main question is: when is $\alpha \in G$ divisible by $\beta \in G$, i.e. $\alpha \cdot \beta^{-1} \in I$?

For $\mathbb{Z}$ we have the answer that this holds iff for every prime number p the value of α at p is at least as great as that of β, where the value is the exponent of p in the prime factor decomposition.

Valuations[1] and valuation rings[2] are the concepts ideated by Krull to play the role of prime numbers for general I.

Characterization: A proper subring B of K is a valuation ring if its noninvertible elements form an ideal (i.e. it is a local ring) such that every proper supering B' (i.e. $B \subsetneq B' \subseteq K$) contains the inverse of a noninvertible of B. What is hoped for is that I is the intersection of all valuation rings containing I

- For $\mathbb{Z}$, the valuation ring corresponding to the prime number p is the ring of those fractions that can be written with a denominator not divisible by p.
- In general this intersection is greater* Krull's fundamental satz states that it is equal to I if and only if I is integrally closed. This means that every element $a \in K$ satisfying the relation $a^n + a_1 a^{n-1} + \dots + a_n = 0$ with $a_i \in I$ (of integral dependence) is actually in I. This follows from:

  * a valuation ring is integrally closed: the supering of integrally dependent elements must coincide with the valuation ring because if it did contain the inverse of an element a of B, we would have $a^{-n} + a_1 a^{-n+1} + \dots + a_n = 0$ and $a(-a_1 - a_2 a - \dots - a_n a^{n-1}) = 1$ and a would be invertible in B.

  ** if $a \in G \setminus I$ with I integrally closed, then a^{-1} is a noninvertible of $I[a^{-1}]$. By Zorn's lemma, consider a maximal subring B of K containing $I[a^{-1}]$ but not a. This is a valuation ring.

In Louveau 1950, he proposes the following new construction: We ask ourselves under what circumstances $a \in B$ holds for every valuation supering B of I. For arbitrary $z \in G$ and any valuation supering B of I, it always holds that $z \in B$ or $z^{-1} \in B$. Therefore, whenever $a \in I[z]$ or $a \in I[z^{-1}]$ holds, so does $a \in B$. Likewise follows: if there are elements $z_1, \dots, z_n \in G$ for which $a \in I[z_1^{\pm 1}, \dots, z_n^{\pm 1}]$ holds for each of the 2^n combinations of signs, then, for every valuation supering B of I, it holds that $a \in B$. The condition is also necessary. Namely, if it is not fulfilled for any $z_1, \dots, z_n$, then a simple well-ordering argument shows that there is a maximal supering $\bar{I}$ of I with the property that, for all $z_1, \dots, z_n$, $a \notin \bar{I}[z_1^{\pm 1}, \dots, z_n^{\pm 1}]$ holds for at least one combination of signs. Therefore in particular $a \notin \bar{I}$. If this $\bar{I}$ were not a valuation ring, then there would be a $z \in G$ with $z \notin \bar{I}$ and $z^{-1} \notin \bar{I}$, therefore there would be elements $x_1, \dots, x_m, y_1, \dots, y_n$ with $a \in \bar{I}[z][x_1^{\pm 1}, \dots, x_m^{\pm 1}]$, $a \in \bar{I}[z^{-1}][y_1^{\pm 1}, \dots, y_n^{\pm 1}]$ for each combination of signs. But from this, $a \in \bar{I}[z^{\pm 1}, x_1^{\pm 1}, \dots, x_m^{\pm 1}, y_1^{\pm 1}, \dots, y_n^{\pm 1}]$ would follow, i.e. a contradiction. Therefore $\bar{I}$ is a valuation ring.

Krull's fundamental theorem becomes a characterisation of an intersection of valuation rings as an integral domain in which behaving as if it were linearly preordered, i.e. assuming that certain pairs of elements $\{a_1, a'_1\}, \dots, \{a_i, a'_i\}$ enjoy a relation of divisibility ~~between~~ and add new relations of divisibility. His formulation of this "as if" goes as follows: it is the simultaneous consideration of 2^i different relations of divisibility among i pairs of elements

(1) a valuation w of K is defined as a function of G into an abelian linearly preordered group Γ

(2) such that it is multiplicative and $w(a+b) \geq \min(w(a), w(b))$. The corresponding valuation ring is the ring formed by 0 together with the elements that have valuation ≥ 0. A valuation ring is characterised by the fact that its field of fractions is K and that it is linearly ordered by divisibility. One has for every $z \in G$ $w(z) \geqslant 0$ $z \in B$ or $w(z) \leq 0$ $z^{-1} \in B$

of K, each generating the integral domain in which these relations are forced, and the statement that the intersection of these integral domains coincides with the integral domain we have started with.

A citation from Blaise Pascal's Thoughts (1623–1730) by Lorenten in 1962:

« Thus we see that all sciences are infinite in the range of their researches, for who can doubt that mathematics, for instance, has an infinity of infinities of propositions to be proved? They are infinite also in the multiplicity and subtlety of their principles, for anyone can see that those which are supposed to be ultimate do not stand by themselves, but depend on others again, and thus never allow any finality. »

The philosophy of dynamical algebra: days 2 and 3

We have had a thorough look into Krull's theory of valuations and Lorenzen's analysis of it. Lorenzen shows that

$a \in B$ for every valuation ring $B \supseteq I$ $\iff$ there are $z_1, \dots, z_n \in G$ such that $a \in I[z_1^{\pm 1}, \dots, z_n^{\pm 1}]$ for each choice of signs

$\iff$ a is integrally dependent on I

Note also the following: if a is integrally dependent on $I[z]$ and $I[z^{-1}]$, then a is integrally dependent on I: one has $1 \in \langle \vec{a}^1, \vec{a}^2 z, \dots, \vec{a}^{\nu} z^{\nu} \rangle_{I[a^{-1}]}$ and $1 \in \langle \vec{a}^1, \vec{a}^1 z^{-1}, \dots, \vec{a}^{\nu} z^{-\nu} \rangle_{I[a^{-1}]}$; i.e. $\vec{a} z^{-\nu}, \dots, \vec{a}^0, \dots, \vec{a}^{\nu} z^{\nu} \rangle_{I[a^{-1}]} \ni z^k$ for $k = -\nu, \dots, \nu$, i.e. there is a matrix with coefficients in $I[a^{-1}]$ such that $M \begin{pmatrix} z^{-\nu} \\ \vdots \\ z^{\nu} \end{pmatrix} = \begin{pmatrix} z^{-\nu} \\ \vdots \\ z^{\nu} \end{pmatrix}$, i.e. $(\mathrm{Id} - M) \begin{pmatrix} z^{-\nu} \\ \vdots \\ z^{\nu} \end{pmatrix} = 0$. Multiply $\mathrm{Id} - M$ by the matrix of its cofactors and expand: you get 0, i.e. a relation of integral dependence for a ("déterminantielle"). $1 \in a^{-1} I[a^{-1}]$, i.e. a

What do these two results mean?

The first means that the computational content of being in the intersection of valuation superrings of I is exactly that one can do as if it was linearly ordered: you can at any point for any given pair of elements u, v of G make the case distinction $u \le v$ / $v \le u$; if you obtain a conclusion in each case, it will hold altogether. This "as if" not only targets that it is not really linearly ordered; it targets also that you are not really making case distinctions: the second result shows how the case distinction may be removed by gluing together computations made in each case into a computation without case distinction.

The dynamical method in algebra proposes to make this precise by a description of the computations, so that the nature of the theory, typically its being geometric, grants the possibility of case distinctions and of gluing the computations made in each case together. Lorenzen's analysis does all this by hand and arrives at an exposition of the theory of divisibility without valuations: in this sense, it goes further than dynamical algebra, which gives a constructive meaning to classical reasoning and has the aim of revealing the constructive nature of classical algebra.