AUBRY Mathieu

Metaphors in Mathematics

Electronic copy available at: http://ssrn.com/abstract=1478871

Abstract:

Analogies play an essential role in Mathematics. George Lakoff and Rafael E. Núñez have shown in *Where Mathematics Comes From* that our understanding of basic mathematics is deeply linked to our experience of the world. They claim that we understand mathematics throught Conceptual Metaphors between source domains (for example spatial relationships between objects) and target domains (abstract Mathematics). These metaphors are supposed to map certain basic schemata of thought, namely, cross-modal organizational structures. In fact the use of conceptual metaphor is a more general cognitive process, used not only in other sciences (as in physics [6], or Cell Biology and Ecology [7]) but also in every aspect of our understanding of the world, for example in philosophy [8] and ethics [1].

In this report, I am going to deal with specific cases of metaphors in advanced and abstract mathematics linked to our conception of space. The goal is both to show that conceptual metaphor theory continues to apply with great success in these areas, and to try to understand the theory more deeply.

Introduction:

Les Analogies ont un rôle essentiel en mathématiques. George Lakoff et Rafael E. Núñez ont montré dans *Where Mathematics Comes From* que notre compréhension des mathématiques élémentaires était profondément liée à notre expérience du monde. Ils affirment que nous comprenons les mathématiques grâce à un ensemble de Métaphores Conceptuelles entre des domaines sources (par exemple des relations spatiales entre objets) et des domaines cibles (des structures mathématiques abstraites). Ces métaphores conserveraient certains schémas élémentaires de pensée, appellés structures organisationnelles cross-modales. En fait, l'utilisation de métaphores conceptuelles est un processus cognitif général, utilisé non seulement dans d'autres sciences (comme en physique [6] ou en biologie et en écologie [7]) mais encore dans toute notre compréhension du monde, par exemple en philosophie [8] et dans le domaine moral [1].

Ce rapport présente une étude de cas particuliers de métaphores en mathématiques, liées à la conception de l'espace. Le but est à la fois de montrer que la théorie de la métaphore conceptuelle est toujours valable dans ce domaine et d'essayer de la comprendre plus précisément.

Electronic copy available at: http://ssrn.com/abstract=1478871

Contents

Part I

Introduction to the embodied theory of Mathematics

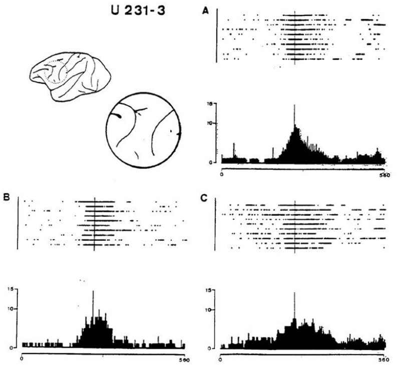

Figure 1: Experiment done by Rizzolatti et al. in 1988 showing the same activity of the same neurons in area F5 of the pre-motor cortex when a monkey is grasping an object with its mouth (A) or with one of its hands (B and C)

1 The conceptual Metaphor theory

1.1 Introduction

Conceptual metaphor theory is an attempt to understand how we think. It is part of a general theory of the mind. At its origin is the claim that our mind is embodied, and that what we think comes from our brain, which is shaped by our experiences in the world. In this theory, what we think can be inferred from the firing of neurons, and we understand it because this firing is similar to the firing corresponding to a perception. Thus, we do not understand abstract concepts, such as freedom or love, directly, but only through a metaphorical understanding. The theory also claims that our understanding rests on two things:

- a structured multi-modal knowledge of some basic concepts in Cross-modal OrGanizational structures (or COGs), which have a kind of universality
- some frames about situations or events which depend on culture and experience.

Both categories will be developed in the next paragraphs.

These claims are based on the biological structure of the brain, and on discoveries in neuroscience. In particular, the discovery of mirror neurons and the work which followed in the 1980s supports the idea of Cross-modal OrGanizational structures. Mirror neurons are neurons, especially in the pre-motor cortex and in the inferior parietal cortex, which are firing when any action corresponding to the same concept (for example grasping, cf. fig.1) is performed, seen, or imagined, even with different conditions. The other crucial idea from neuroscience in the conceptual theory of metaphors is recruitment learning: links between domains which are simultaneously activated become more important, thus creating a binding between the two domains. Most of the ideas developed in this paragraph are thought to arise through recruitment learning.

This theory is also supported by many computational ideas. For example the NTL project tries to show that the definitions of frames and schemata allow for good analysis of language (and also as a consequence, good generation of sentences). In this theory, each concept is defined by a control node which regulates the activation of other nodes, and is related to other parts of the brain by a linking circuitry. Concepts are described using a formalism which we will develop in the case of functions (cf. annex 2) and which can be implemented with different kind of "nodes". Two examples will be developed in the next paragraphs: the works of Terry Regier and Srini Narayanan on Image-schemata and X-schemata .

1.2 Cross-modal OrGanizational Structures

It may perhaps seem strange to separate COGs into different kinds when they structure all our experiences and are cross-modal. But this division arises for historical reasons, and, for example, image-schemas like the container schema can occur in non-visual experiences.

1.2.1 Image-schema

In the mid-1970s, Len Talmy and Ron Langacker were working separately on terms describing spatial relations. They discovered that despite the important variation in spatial-relation terms between languages, all of them can be expressed using a few universal primary relations. These relations are the image-schemata. The most important of them are the spatial relation schemata (like the ”above”, ”contact”, ”magnitude” schemata), the ”container” schema and the ”Source-Path-Goal” schema. These primary image-schemata can be combined to form more complex schemata, which depend on culture. For example the English schema ”into” is a composition of a Source-Path-Goal (SPG) schema and a container schema, with the constraints that the Source of the SPG schema is the exterior of the container schema, and the goal of the SPG schema is the interior of the container schema. (this example is developed in Lakoff [1])

The work of Terry Regier [2] in 1996 gives a deeper plausibility to the idea of universal image-schemata, by showing that a connectionist network with a specific structure and specific input (he called this method constrained connectionism), similar to the visual system structure, can learn (using a set of examples, and assuming negative evidence) the lexicon of spatial relations from different languages. The network is even able to learn words for movement, while differentiating between the moving object, the trajector, and the spatial reference, the landmark. To achieve this, he especially makes use of center-surround receptive and orientation-sensitive neurons, the layer organization of the visual areas and the separation between what-and where-pathways. One of the main achievements of this work is that it ”emphasizes the reliance of linguistic semantic content on nonlinguistic perceptual structure.”

This was in fact not the first work on this kind: in 1969, Berlin and Kay explained a kind of universality in color terms (loci in the spectrum described as ”best example” of a specific color in different languages) by the neurophysiology of the human visual system. Regier’s model is differing from this work in two ways: first what it describes are more complex concepts, including several perceptions, and second his model is not a direct image of the neural network, but is only motivated by it and is shaped by learning methods.

Nevertheless, the fact that Regier’s model allows one to describe the emergence of schemata like the container schema and complex relations such as the trajector-landmark relation using well-known characteristics of the visual system, remains an important argument in favor of the existence of image-schemata.

Image-schemata and mathematics: The image schemata and the deep intuition they contain are essential to Mathematics. In [3], Lakoff shows that the container schema is the source of the basic operations of arithmetic (the 4Gs) and of the whole logic of the set theory. The spatial relations schemata are of course central in our intuition of space, and we will see that the SPG schema has also an important role in our understanding of functions and linear applications.

Image-schematic transformations: There are several transformations we perform very easily with image-schemata. This is obvious in linguistics, because the words of the source domain of the transformation can also be used in the target domain, and the very same process occur in mathematics. In [1], Lakoff identifies several of these transformations:

- *path focus ↔ end point focus:* a word can describe either an action or its end, for example: ”He goes through the doorway / The room is through the doorway”. In mathematics, we use such a transformation about space: we focus either on a point or on the vector, which can be understood as the path from the origin to the point.

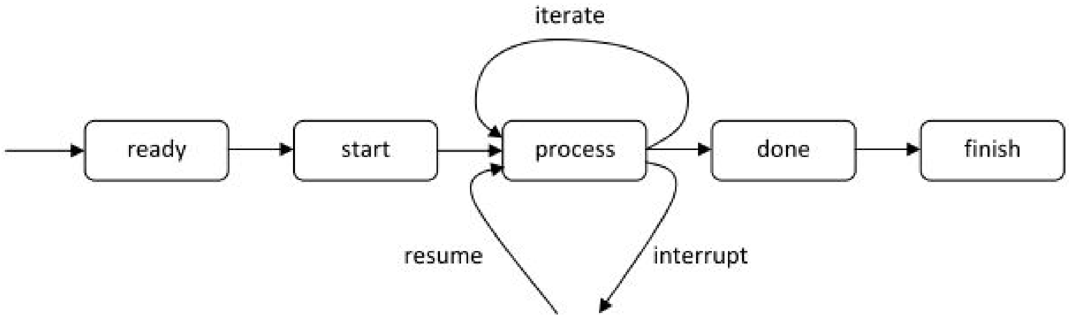

Figure 2: The structure of an X-schema

- *Multiplex* ↔ *Mass*: You can focus on a group of individuals in two different ways. You can either see all the individuals in the group, or see the group as a whole. An example in English is "All men are mortal/All gold is yellow". We also use this kind of transformation while speaking about arithmetic, and consider sets of sets (we will call them k-containers).
- *Zero-dimensional trajectors* ↔ *One-dimensional trajectors :* We are able to imagine the result of the continuous movement of a zero-dimensional trajector, that is a one dimensional trajector. Thus the words which can be applied to the zero-dimensional trajector can often be applied to the one-dimensional trajector : "He went through the forest / The road goes through the forest". This transformation can for example allow us to change our representation of a function.
- *Non-reflexive trajectors* ↔ *Reflexive trajectors*: given a relationship between a trajector and a landmark, you can imagine the same relation between different parts of the same entity, or the same entity at different moment of time. In the last case, this is in fact the result of a binding between two situations at different times.

1.2.2 X-schema

The idea of X-schema comes from the work of David Bailey [4] and Srini Narayanan [5] in the 1990s, who were working on motor control. Narayanan tried to build a computational model that could represent the way our brain understands and plans actions. He points out that there exists a universal structure for all actions which he called executive schemata (or in short X-schemata). This structure is presented in the figure 2. With this structure Narayanan was able to model dozens of basic body movements.

X-schema are important in cognitive linguistics because they allow one to explain certain facts about grammar, especially the aspects of verbs. In Mathematics, we will see that the proofs and the algorithms have exactly an X-schematic structure. Thus, we can suppose that the same part of the brain allows us to plan actions and proofs, and that our ability to reason relies on spatial reasoning.

1.2.3 Force-dynamic-schema

Force-dynamic-schemata were introduced by Len Talmy. They are for example "supporting", "resisting", "blocking". The notion of cause seems to rest on force-dynamic-schemata. There are a lot of examples of metaphorical use of force-dynamic terms in the language : "I refrained from responding", " he resisted the pressure of the crowd", he was forced to resign"... They are also useful in mathematics, for example for understanding reductio ad absurdum, or the fact that one parameter is overpowering another.

1.2.4 The entity-schema

The entity-schema is also especially important. It seems to organize our entire conception of the world. In the computational theory of metaphor it is linked to a Gestalt node. This structure would also arise through recruitment learning, generalizing our experience from the objects of the world. Here is its structure, presented with the NTL formalism : (the Neural Theory of Language group is a joint project from UC Berkeley computer science and linguistic department which try to develop a biologically plausible computational model for language, including his understanding)

```
Schema Entity
    Roles
        Referent
        Category
        Modifier
        Prototype (Type, Schema)
    Parameters
        Individuation (Individual, Plurality, Group)
        Objectification (Object, Substance)
        Quantification (Amount, Proportion)
        Specification (Definite, Indefinite, Generic)
        Deixis (Center; NonCenter; SpeakerLocation,OtherLocation)
```

1.3 Frame

Unlike COGs, frames are not based only on our perception and are not necessary cross-modal (although often multimodal) but come from our repeated experience. For this reason they are very dependent on culture. For example, we have a frame for commercial events, which includes a buyer, a seller, goods etc. In mathematics, mathematicians have frames for reasoning and thinking about objects. For example, in [3] Lakof and Núñez developed the ”epsilon-disc” frame, which allows us to think about continuity. Algebraic structures can also be considered as frames.

1.4 The classic theory of Metaphor

A metaphor is the link we naturally make between two domains: one source domain, usually more concrete, and a target domain, usually more abstract. This allows us to better understand and think about the target domain. For example, we have a ”love is a journey” metaphor. This metaphor really modifies our notion of love (or at least is the manifestation of our specific cultural notion of love), it implies for example the existence of plans, goals, which in fact do not necessarily have anything to do with the concept of love.

Most of the metaphors we have and we use everyday are unconscious, and pointing them out can thus help us to understand the way we think, and to evaluate their scope. We will also argue that metaphors are a source of creativity by pointing out that progress in the understanding of (mathematical) objects can often be grounded in the development of new metaphors. A simple example is the plane metaphor for the complex numbers: they were used long before, for example to solve equations of the third degree, but their actual existence only became accepted through Gauss' introduction of this metaphor. One can argue that meatphors are also a source of creativity in other sciences, as Nersessian does in [6] for physics, and Brown does in [7] for chemistry, biology and ecology. One can also argue that they also ground of philosophy, as Lakoff and Johnson do in [8].

It is possible to differentiate between two kinds of metaphors:

- the grounding metaphors or primary metaphors are directly linked with experience. For example, the metaphor ”knowing is seeing”, or the metaphor ”goals are destinations” arise directly from our experience of the world, because we first learn by seeing things, and because the firsts kind of goals are destinations. In primary metaphors both the source domain and the target domain are concrete.

- complex metaphors are more elaborate and are the result of linking metaphors between schemas, frames and folk theories from different domains

An important point about metaphors is that they can be learned easily, but are not always easy to find. Thus, we are able to understand a piece of poetry immediately, and students are able to learn in a few years metaphors which scientists took centuries to find.

1.5 Neural binding

All this theory of structures and association is not enough to explain the way we think. Indeed, we do not think the different concepts separately. For example if you think of a blue square, you do not understand blue and square separately, but you imagine a blue square. This phenomenon is called neuro-binding. These bindings can already be present in the brain structure (for example if I ask you to imagine grass, you imagine it green, and if I ask you to imagine an apple, you will not imagine it blue) or depend on the context. The important question of the physical expression of neuro-binding has unfortunately not been solved. It can be considered as the main element of the gap which remains between the theory of the brain network and our experience of thought in this theory.

1.6 Mental spaces and conceptual blending

Fauconnier and Turner introduced the idea of conceptual blending. Fauconnier and Turner view metaphors as a specific case of conceptual blending which they consider as a basic mental operation, whereas Lakoff would argue that conceptual blending does not correspond to any structure of the brain, but is just a composition of metaphors and bindings. This question is not central here, and we will use one point of view or the other, depending on the aspect we want to emphasize. In particular, Fauconnier's and Turner's point of view allows one to emphasize the importance of compression and blending in our thought, and the way emergent structure can arise through blending.

A mental space is an idealized cognitive model of a possible situation, ”a small conceptual packet assembled for purposes of thought and action” [36]. It is structured by frames. Mental spaces can be connected through a mental space network. ”In blending, structure from input mental spaces is projected to a separate, blended mental space.” [11] This projection is made following some rules and allow a vital relation from the outer space (the original space) to become a vital relation from the inner space (the blended space). These vital relations are for example change, analogy, disanalogy, part-whole, cause-effect...

Blending allows us to compress a complicated situation (e.g. dinosaurs which evolved into birds) into a more simple situation (e.g. a single dinosaur which become a bird). According to Fauconnier and Turner this compression is essential to our understanding, since we are only able to understand situations with very few actors and simple relations.

The most interesting case of blending is the case of double scope integration. In this situation, the inner space has inputs from several spaces, which have different and often clashing frames. This situation is especially important for creativity, since the inner space often has properties which differ from the outer space.

1.7 Categorization

How do concepts arise? How are objects, sounds, gestures differentiated? Tomasello points out that apes already have these kinds of capacities for example to differentiate sounds like ”ba” and ”pa”. It is interesting to point out that our language abilities rest on pre-existing capacities. Nevertheless, these basic capacities are not enough to explain how concepts can be learned.

The basic idea of the theory of categorization is the following: for each property (e.g. being a bird) you have a prototype, and evaluate things as being more or less close to it (a robin is a better example of a bird than a chicken). This prototype effect is clearly proved by reaction-time experiments, experiments on priming by super-ordinates, production of examples... Experiments show that the prototypes are not only the most common items, but are chosen because they share many properties with the other members of the category, and not with the nonmember, thus implying a contrast set. Nevertheless a ”best example” is not enough to represent a category. The fact that we can recognize schematic representation of members of categories shows that we make some abstraction and pay more importance to some features. That allows us to make inferences and generalizations. But that does not mean that our categories can be defined by abstract definition, because they are linked to our knowledge of the world. For example the word ”bachelor” means something only relative to our frame of a ”standard life”, which includes marriage. Thus we would hardly apply it to a priest, a homosexual, or an old man. Finally categories typically include a prototype, conventionalized extensions of it which are linked with our knowledge of the world, and a set of examples.

2 Basic Metaphors in Mathematics

2.1 Intuitive Mathematics

In [3] Lakoff and Johnson present a broad range of evidence that children have an intuitive notion of Mathematics, and can for example note the difference between two and three. Stanislas Dehaene in [10] provides even evidence that this capacity is not only linked to our visual system, but that children are able to do some abstraction in their first year of life. For example, he describes an experiment where children’s attention is attracted by a ”magic” situations (where the number of objects change), and another where the interest of four-day-old children is increased by a change in the number of syllables which they which they hear while sucking a nipple. Moreover, the analysis of the primary visual cortex (V1 area) shows that our brain has for example an embodied ability to detect continuous and straight lines. These primary notions are important for grounding Mathematics, but some people will argue that because they are not clearly identified they are not part of real Mathematics.

2.2 Mathematics

Lakoff and Núñez present in [3] some characteristics of mathematical ideas: they are precise, consistent, stable across time and communities, understandable across cultures, symbolizable, calculable, generalizable and effective for describing the world in the way we see it. This could ground the idea that mathematics comes from the world. On the contrary, the idea I want to present here is that mathematical objects and properties come from image-schemata, embodied in our mind, via grounding metaphors. Nevertheless, to reason mathematically and to create new interesting mathematical concepts, you cannot stop at these grounding image-schemata, but you have to find linking metaphors and bindings, even if all these metaphors can be understood in terms of cross-modal structures. This view, which explains why mathematics fits the world without seeing anything transcendental in it, is one of the great successes of Lakoff and Núñez in [3] : Mathematics fits the way we see the world, because they come from image schemata and metaphors. The following examples show that some abstract concepts can be introduced by new metaphors in a very intuitive way, preserving some image-schematic properties. We will even see that often mathematicians justify their work through use of analogies.

2.2.1 Mathematical objects and their properties

The first capacity you need to begin to do real mathematics is to be able to think about abstract mathematical objects. This is possible using what we presented as an ”entity-schema”.

The second thing you need is to be able to describe their properties and relations. That means that from a large set of objects you can sort objects with respect to a property. In general cognitive science, this is explained by categorization theory. On the one hand, this kind of categorization cannot work as a basis for Mathematics, because it is too loose (some objects are not in a well defined category, for example it is not clear if a phone is a piece of furniture). On the other hand, it is too strict: if you have apples on a table, you want to be able to count either the apples or the masses of apples. Thus, the mathematical properties cannot be seen just as the usual properties, but both have to be clearly defined and to be able to fit the world in different ways. For this reason, mathematical properties are grounded in the general structures of intuition, or Cross-modal OrGanisational Structures. These structures are general, but not abstract; on the contrary they are deeply embodied and linked with our experience of the world.

Since mathematics deals with abstract relations (formalized in the axioms, using COG relations, especially image-schematic relations) between abstract objects (entity-schemata), a large part of the phenomena from the world can be described using a mathematical formalism. Nethertheless, some phenomena can seem not to be coherent with our axioms, and thus give mathematics the idea of new axioms, or give them more importance. The basic case of this kind is of course general relativity and non-Euclidean geometry (cf. part III). This point of view can induce us to ”conceive of an axiom system as a logical mold (« Leerform ») of possible science.” [9]

2.2.2 Mathematical language

To speak about these objects and properties, you need also a language which is not defined with categorization, but a well-defined mathematical language, also defined using the image-schematic relations described in the axioms.

The objects designated by this language are purely mathematical and abstract, but we understand them only via metaphors whose source domains motivate us to define the relation in the way we did it. Most of mathematical objects are not only understood via a single metaphor, but many. The richness of mathematical constructions comes from this wealth of metaphors, which allow us to recognize some structures from one domain in another one. Thus, via a repeated metaphorical process, mathematics creates very rich structures, and points out some of their complex properties. Using the metaphors we can compress our understanding of it and some expressions can be transfered. For example, you can speak of a symetric linear application, or of the image of a matrix (cf. part IV).

This kind of matching, if it concerns only mathematical structures and is systematic, was named and its importance recognized long ago in mathematics: it is an isomorphism. In an isomorphism, two sets of elements are mapped one to one such that their relations (for example operations) are also be mapped. One of the most important ideas of this report is that this mapping does not have to be systematic,that it does not have to map objects but can only map image-schematic properties, and in this case some structure will also be mapped.

2.2.3 Mathematical algorithm

A mathematical proof can be conceptualized with X-schema and force dynamics schema. In the following text most of the proofs will be given in diagrams with an X-schematic structure. This comes from a usual metaphor which makes it seems natural for us to conceptualize a proof as an action: PROOF IS MOTION TO A RESULT. We find some evidence of this metaphor in the usual language about proofs: ”achieve a result”, ”start from an assumption”, ”get around a difficulty from a proof”, ”take another way”... We can check that in most cases a mathematical proof has the following structure, exactly like the structure of motor-control programs as described by Bailey [4] and Narayanan in [5] :

- Readiness: having the previous results and axioms needed.
- Starting up: define objects, and prove their elementary properties.
- The main process: the main step of the proof.
- Possible interruption and resumption: you may try different hypotheses which are not correct (reductio ad absurdum or if you separate different cases)
- Iteration (or continuing): iterate a process, for example in a mathematical induction
- Purpose: check if the different goals of the proof are really achieved.
- Completion: end of the proof.
- Final state: what you have shown.

These similarities allow us to suppose that proofs are conceptualized via a metaphor ”proofs are actions”. In fact the previous schema works very well, and on its own seems to be good enough for ”direct” proofs and constructive proofs (the name itself refers to a human concrete action).

For a mathematical induction, you need also what Lakoff and Núñez call in [3] the BASIC METAPHOR OF INFINITY. It is a mapping between completed iterative processes, and iterative processes that never stop (both conceptualized with X-schema). The resultant state of the completed process is mapped with the resultant state of the infinite process. This mapping allows us to conceptualize clearly the mathematical induction with an X-schematic structure.

Reductio ad absurdum needs also another metaphor. It is a force-dynamic metaphor, which with the PROOF IS MOTION TO A RESULT metaphor allows the following complex metaphor.

Force dynamic interaction	*Proof*
possible movements	*possible hypotheses*
a force which impedes movement	*a contradiction following from an hypothesis*
the only possible movements	*the non-contradictory hypotheses*

The fact that we need more metaphors to conceptualize mathematical induction and reductio ad absurdum could explain why these proof methods are discussed and sometimes challenged by mathematicians: some of them work on theories without axioms allowing this kinds of proof (for example non-standard analysis for mathematical induction, and intuitionist logic for reductio ad absurdum).

We can have with mathematical constructions of objects the same mapping with the X-schemata, perhaps because we have the same metaphorical understanding of this process as a ”construction”. The metaphor can also be extended with the BASIC METAPHOR OF INFINITY, and an example is given in Fig. 4.

2.2.4 A method of abstraction: the equivalence relations

I will now present a useful mathematical process which allows us to use a metaphor to separate objects in different groups and to reason about this groups. In mathematics, separating objects using a property (for example the multiple of 2) is referred to as identifying equivalence relations, and equivalence classes. This ability is image-schematic. It is the fact of ”matching collections of objects”

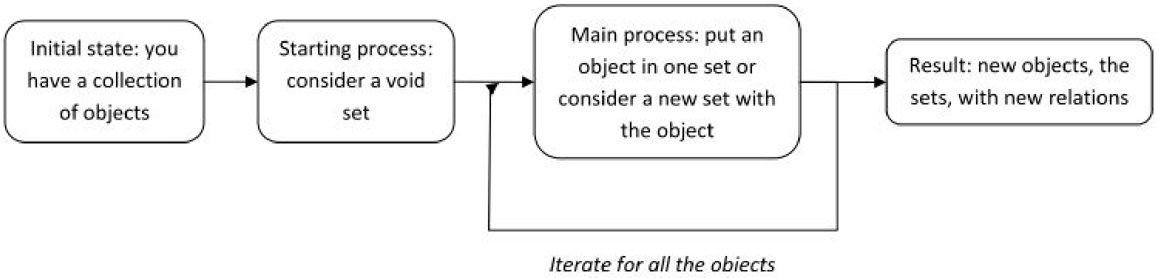
Initial state: you have a collection of objects
Starting process: consider a void set
Main process: put an object in one set or consider a new set with the object
Result: new objects, the sets, with new relations
Iterate for all the obiects

Figure 3: The construction of new object using the construction of equivalence classes

Merging objects	*Drawing Equivalence Relations*
objects	*objects*
splitting of the objects in different collections using a specific criterion	*definition of equivalence classes*
each collection of objects	*equivalence class*
to be in the same class	*be related by the equivalence relation*
property : *→ ”be in the same class” is a relation reflexive, transitive and symmetric.* *→ Given a reflexive, transitive and symmetric relation ” $\sim$ ” between objects, you can sort them in classes by the property :”* *”objects a and b are in the same class if and only if $a \sim b$”*	***definition :*** *→ an equivalence relation is a relation which is reflexive, transitive and symmetric.*
see each collection as an object, using multiplex to mass transformation	*abstract object*
transformation on an objects from which the results’ collections depend only from the initial objects collection	*operations on abstract objects*

This metaphor is important both to be able to draw general properties from our experience of the world, and in mathematics, because applying it to mathematical objects allows us to create new objects, with new relations, as shown in figure 3.

2.3 Definition of natural Integers, N

An extensive explanation of the metaphors and image-schemata used in basic arithmetic is given in [3], which especially developed the two metaphors `ARITHMETIC IS OBJECT COLLECTION` and `ARITHMETIC IS MOTION ALONG A PATH`. What I give in this paragraph is just a summary, to ground the metaphors which will be developed later.

2.3.1 Intuitive definition with the equivalence relation in collections of objects :

We can associate to every set of objects seen as a whole (via a *multiplex* → *mass* transformation) any other set which has the same number of items. The ”same number” just means that we can superimpose, or match any item from each set with one item from the other set. We say that two collections which have the same number of items are in the same equivalence class. I will not check that the operations I define do not depend on classes. You can either consider that it comes from a pure intuition on the container schema or from a mathematical point of view, that it comes from axioms (which reflect the properties of the container-schema).

This intuition allows Cantor to ground the notion of cardinal in his set theory: two sets have the same cardinal if they can be put in one to one correspondence. This relation between two sets is called equinumerosity.

Equivalence classes of collections	*Integers*
equivalence classes from collections obtained with the relation ”objects from both collections can be matched one to one”	*Integers*
the class c which contains the merging of two collections from classes a and b	*the operation ”+”, a+b=c*
class of collections without objects inside	*0*
the class of collections with a single element	*1*
the class c (if it exists) in which you are if you split a collection of class a into a collection of class b and another collection	*the operation ”-”, a-b=c*
the relation between a class a and classes b such that you can split a collection from the class a into a collection from the class b and another collection	*the relation* $a \geq b$
the class c in which you are if you iterate the process : for each element of a collection in class a you merge a collection of class b with the previous result, beginning with a collection without objects	*the operation ”×” ,* $a \times b = c$
the class c (if it exists) in which you are if you iterate the process: you begin with a collection in class a and until you have no more objects in this class you split it into a collection from class b and another and each time you merge a collection with a single element with the previous result, beginning with a collection without objects	*the operation ”÷” ,* $a \div b = c$

This definition seems perhaps too hard, because of the use of the equivalence classes. But if we examine how we understand the `integers are objects collection` metaphor, the first thing we do is to say that any object you consider ”is the same”, is an indivisible whole, without asking about its size or color or any other characteristic : you just focus on the fact that it can be represented by an entity-schema. This idea was used by Carnap to define the notion of cardinal number. The difficulty from a mathematical point of view is to access the ”essence” of a class corresponding to the cognitive idea of the number. Carnap used the concept of ε-operator, introduced by Hilbert. The idea of the ε-operator is that if F is a predicate which some object can satisfy F, then $\varepsilon_x F(x)$ is an ideal object and denotes the most salient object that satisfies F. Carnap defined the cardinal of a set x, x as $\varepsilon_y F(x, y)$, where $F(x, y)$ is the predicate ”x and y are equipotent”.

A definition of substraction and division as the reciprocal operations of additions and multiplication may also seems clearer (the result of $a - b$ resp. $a \div b$ is the collection x such as $x + b = a$, resp. $x \times b = a$), but if the reciprocal operations are good definitions, it is not the way substraction and division are imagined.

2.3.2 Intuitive definition with the straight line metaphor

It is somewhat intuitive to compare lengths as we compared the size of sets of objects and to put measuring sticks one after the other as we merged sets. For this reason, we have a metaphor between the integers and a collection of points on a line.

Imagine a straight line with a specific location (point) on it. Lets decide that this point is the origin, from which we count distances: it will represent ”0”. If you have an object with a specific length, you can put it near the point and decide that the other endpoint will be ”1” and iterate the process in the same direction (e.g. right) to build other Integers. The number of times you repeat the process corresponds to the number of items in each collection from a class in the previous metaphor. In this new metaphor, adding one number to another is going to the right for a specific distance, and subtracting is going to the left.

Before going further, we have to check that we have an intuitive understanding of lines, straight lines, intersections and points. Indeed, we can show that parallel connections in the V1 area of the neural system, allow us to detect limits between objects, and especially straight lines: to know what a line is you have just to look at the angle of your table if you are far enough from it. We are also able to detect intersections, and then to understand what a point is. (cf. [13])

I want also to point out that this metaphor is not only a possible representation, but is very deeply embodied. Stanislas Dehaene presents some evidence of this for example in [10]. By measuring reaction times in the comparison of numbers, he makes several points. Firstly, that the brain ”transforms [two-digit numerals] mentally into an internal quantity or magnitude”. Thus we do not stop at an abstract representation of numbers, and for example apply a comparison algorithm concerning only the first digit if it is possible. Secondly, by comparing the reaction times using the right or left hand to decide if a number is greater or smaller than another, he demonstrates the existence of what he calls the SNARC effect (Spatial-Numerical Association of Response Code). The subjects clearly answer faster if they have to decide that a number is bigger with their right hand, and smaller with their left hand. He also shows that this spatial association depends only on the relative sizes of the numbers. Lastly, he shows that this association of right with greater, although deeply embodied, is a cultural one by testing people who learned to write from right to left.

Another question thus arises, which at the beginning could seem surprising: do numbers have color? Indeed, as pointed out by Riemann, color and space seems to be the only two examples of continuous manifolds we see in our everyday life. Why would we not understand numbers as colors? Stanislas Dehaene shows in [10] that for some people (perhaps 10 % of the population) numbers have colors : ”Most people associate black and white with 0 and 1 or 8 and 10 ; yellow, red, and blue with small numbers such as 2,3, and 4 ; and brown, purple, and gray with larger numbers such as 6,7, and 8. ” It is very interesting to see that primary colors are associated with small numbers and that larger numbers are associated with more complex colors. Stanislas Dehaene suggests the following explanation for that association: ”Because the number of neurons remains constant, the growth of the numerical network must occur at the expense of the surrounding cortical maps, including those coding for color, form, and location. In some children, perhaps the shrinkage of non-numerical areas may not reach its fullest term. In this case, some overlap between the cortical areas coding for numbers, space and color may remain.” There are perhaps other mappings between color and space, such as a mapping between left and bright colors and between right and dark colors, but they seem not to have been already studied. An interesting question arises from the observation that space, color, and numbers (when we develop our knowledge of them) are the main continuous manifolds we experience: is this common characteristic the reason why the cerebral maps are near each other, perhaps having evolved from the same one?

2.3.3 Von Neumann’s mathematical definition

With the two metaphors we have presented, we have a notion of what integers are , because we defined relations between them, but they come only via these metaphors. To have well-defined mathematical objects, you have to build them in Mathematics with as few materials (axioms) as possible. Finding ”good” axioms is a very important issue in Mathematics: they have to allow you to build well-defined mathematical objects with image-schematic relations, but if they are too restrictive, you will not be able to build any interesting objects. A well-known example is Euclid’s axiom : ”from a specific point, you can draw one and only one straight line parallel to another one”. If you take this axiom (which seems very intuitive in geometry) you cannot build non-Euclidean geometries, which are very interesting and for example important in general relativity.

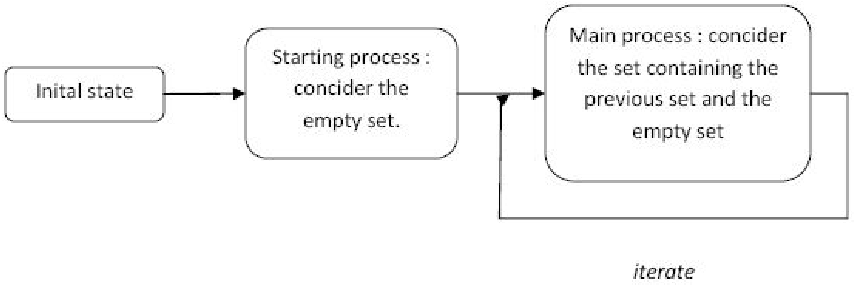
Inital state
Starting process : concider the empty set.
Main process : concider the set containing the previous set and the empty set
iterate

Figure 4: Von Neuman's X-schematic construction of natural integers

To build integers, you can use the set theory axioms (developed in [3]) and consider the objects $\emptyset$ (empty set, a set without elements, considered as the basic example of an entity), $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$... and match them as in `INTEGERS ARE OBJECTS COLLECTIONS` with 0,1,2,3...

This process is X-schematic and can be summarized in the schema of figure 4, and seems to us very intuitive. Nevertheless, as Poincaré pointed out, it is not a very good definition from a logical point of view. The fact that there is iteration in the process leads to an impredicativity problem: an integer is 0 (the void set) or a successor of an integer in our construction process, and thus the definition of the set relies on the set itself. This kind of process can lead to paradoxes such as Russel's paradox (does the set of all sets which do not contain themselves contain itself?). For this reason some mathematicians adopt a predicativist position and reject all impredicative constructions except the one for the integers.

2.4 First extensions of the Integers

2.4.1 The Relative Integers, Z

With the metaphor `INTEGERS ARE POINTS ON A STRAIGHT LINE`, we see that there is no reason to stop at the zero on the left and we can consider negative numbers. The relations between relative integers are clearly given by this metaphor, and you can easily build them in a mathematical way, once you have natural integers.

It is interesting to notice that the negative numbers are not easy to conceptualize via an understanding of sets, although the definition of integers via set theory seems to be clearer. We see here for the first time that to have different metaphors and different understandings of a single notion, even if one seems better from a logical point of view, allow us to extend the notion in interesting ways.

2.4.2 The rationals, Q:

There is also no reason to consider only the points corresponding to integers. If we take another object, say half as long, we have a new point "a" which is such that $2 \times a = 1$. So you can write a=1/2, and so on. In this way, you will define rationals. Once again, after having this idea, it is easy to define rationals via set theory with the idea of object collections and equivalence classes. But the idea is much easier to introduce with the idea of proportion and the straight line metaphor.

A better mathematical definition can be made using equivalence classes on sets of two integers, the second being nonzero . The equivalence relation says that $(A, B) \sim (A', B')$ if $AB' = A'B$, and the operations are the natural operations for quotients.

Part II
Mixing arithmetic and analysis : the origin of Algebraic Geometry

3 Arithmetic

3.1 Divisibility and Prime numbers

The previous metaphors, especially the container metaphor, allow us to see the integers in a more general context, and as example of more general structures. We will now focus on relations between the integers.

An integer A is said to be divisible by another B, if a collection with A items can be split into B collections with the same number of items. Another way to understand this is to build a rectangle with A elements and a side with B elements. (With this metaphor, it is obvious that multiplication is commutative, and even associative if you see the multiplication of three numbers as building a rectangular parallelepiped.)

An integer A is prime if it cannot be split into several collections of the same size, unless it is "split" into a single collection with of A elements or into A single-element collections. You can also understand the primeness of A as the impossibility of building a rectangle with A elements. In other words, A is only divisible by one and itself.

3.1.1 The division algorithm

A collection of size A cannot always be split into collections of size B, but you can always form as many collections of size B as possible, and have B or fewer elements left over. The number of collections of size B is called the quotient of the division, and the number of elements left over, the remainder. This algorithm is of course image schematic and very useful when dealing with arithmetic. We can have another image-schematic representation of this division process with the number-line metaphor for integers: you can use a stick B units long to try to measure A units, and then find the remainder.

It is easy to see that if a collection divides two others, it will divide the remainder of their division. The iterated application of this algorithm thus allows us to calculate the greatest common divisor of two numbers. (It is the last nonzero remainder). This property allowed the Greeks to prove the existence of certain irrational numbers. It seems that they had a spatial understanding of this fact. The corresponding notion of irrationality is then incommensurability. The earliest recorded proof of this is the one by Euclid which appears in the Elements. In fact, the second proposition of book X gives a general way to prove that two lengths are incommensurable: if you can always subtract the smaller from the greater without ever having two lines of the same length, then the two first lines are incommensurable. Indeed, imagine that a length l can be used to measure two lengths, a and b ($a > b$), then it can also be used to measure $a - b$ and b etc. If you iterate this process and never produce two equals numbers, you will have lengths smaller than l, and that is not possible. This method of proof, proving a property for ever smaller quantities, is called an infinite descent.

An easy geometrical proof using the same idea can be done in the case of $\sqrt{2}$. If some length l divides a and $a\sqrt{2}$, it also divides $a\sqrt{2} - a$ and $2a - a\sqrt{2}$. But we can see in figure 5 that $a\sqrt{2} - a$ and $2a - a\sqrt{2}$ are also the lengths of the sides of an isosceles right triangle. Thus, we can iterate this process without end, and show that l divides a length smaller than l, and that is impossible.

3.1.2 The fundamental theorem of arithmetic

We will give in this paragraph a proof of the fact that a number can be written in only one way as a product of primes, and show how it grounds a new metaphor for numbers. This view of integers is very important in arithmetic, as Hensel underlines in the introduction to [20]: "In der elementaren Arithmetik, wie sie in de "disquisitiones

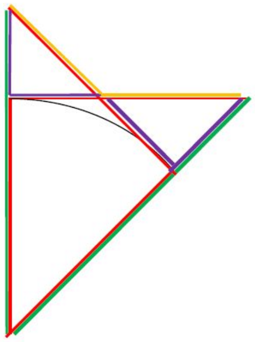

Figure 5: Irrationality of $\sqrt{2}$. In red, the sides from length a, in green $a\sqrt{2}$, in violet $a\sqrt{2}-a$, and in orange $2a-a\sqrt{2}$

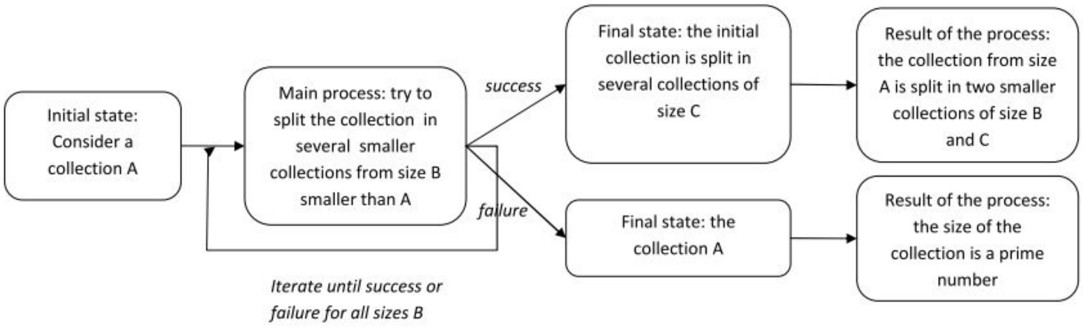
Initial state: Consider a collection A
Main process: try to split the collection in several smaller collections from size B smaller than A
success
failure
Final state: the initial collection is split in several collections of size C
Final state: the collection A
Result of the process: the collection from size A is split in two smaller collections of size B and C
Result of the process: the size of the collection is a prime number
Iterate until success or failure for all sizes B

Figure 6: Process to break down a number

arithmeticae" von Gauss erst im Anfang des vorigen Jahrunderts systematisiert und zu Range einer Wissenschaft erhoben worden ist, tritt als Hauptpunkt die Tatsache der Existenz der rationalen Primzahlen und *der Satz in den Vordergrund, dass jede rationale Zahl auf eine einzige Weise als Produkt von Primzahlen dargestellt werden kann*"

Proof of existence of product It is clear that any integer can be broken down into a product of primes, that is, that it can be seen as the result of iterated addition, in such a way that every iteration is done a prime number of times. Indeed, the process described in figure 6 shows that every number is prime or can be split into a product of two smaller numbers. The process has to finish because the collections become smaller at each iteration.

Consider now that (prime) numbers are kinds. Each collection can be seen as the result of multiplication (that is iterated addition) of these kinds. We also consider numbers as collections of kinds in a container we will call a kind-container, or k-container, to differentiate it from the containers which represent numbers as the sum of the objects in a collection (in the definition of integers, we used this sort of containers, with each entity representing 1), which we will call elementary containers or e-containers. Thus, a k-container can be seen as containing e-containers. An example of this process is shown on figure 7. To understand the meaning of a k-container in terms of e-containers, you have to iterate addition on its e-containers. These two metaphors for number can be mixed to form a complex representation, as explained in the following table.

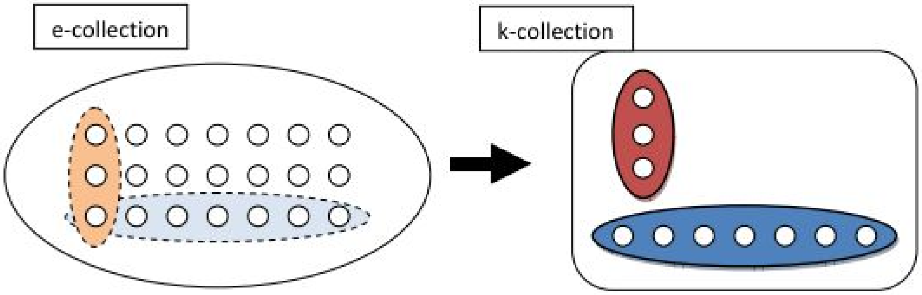

Figure 7: Process to see an e-container an a k-container

number	*e-collections*	*k-collections*
1	*an e-collection with a single object*	*a void k-collection*
a number A	*an e-collection containing A elementary objects*	*a k-collection corresponding to a prime decomposition of A*
the product k_1k_2	*the iterated merging of k_1 collections of k_2 elements*	*a k-collection containing the kinds k_1 and k_2*
the sum of A and B	*an e-collection containing the merging of two e-collections of size A and B*	*an e-collection containing the kinds corresponding to a prime decomposition of A+B*

This mapping allows us to see k-containers as e-containers when needed.

Proof of uniqueness with the division algorithm: We will show that it is also true that every number can be written in only one way as a product of primes. We will therefore use the following lemma.

lemma: if m and n are relatively prime, a is an integer and $m|an$, then m divides a.

proof of the lemma: Consider two relatively prime numbers m and n. Their greatest common divisor is 1. We saw that with the division algorithm, the greatest common divisor can be written as iterated differences of the original two numbers. You can thus write $1 = xm + yn$ (with x and y integers), and $a = (an)y + m(xa)$. Because m divides both terms on the right side, it also divides a.

Consider now two ways of writing a number as product of primes $p_1p_2...p_n = q_1q_2...q_n$. Because p_1 is prime, it is relatively prime to all q_i to which it is not equal. Thus it divides (by the lemma) one of them, and is necessarily equal to it. Dividing the previous equality by p_1, and iterating the process, you see that you have the same prime numbers with the same multiplicity on both sides. This concludes the proof.

Proof of uniqueness with container schema: Another proof of the uniqueness is possible. It is a little more difficult, but I give it here because it uses only a direct application of the container schema.

We will suppose that a number can be split in two ways into a product of prime numbers and we will show that a smaller number exists with the same property. This is of course impossible. We have already seen a proof using this idea, an infinite descent. Because of the complex mapping presented in the previous table, when needed, we

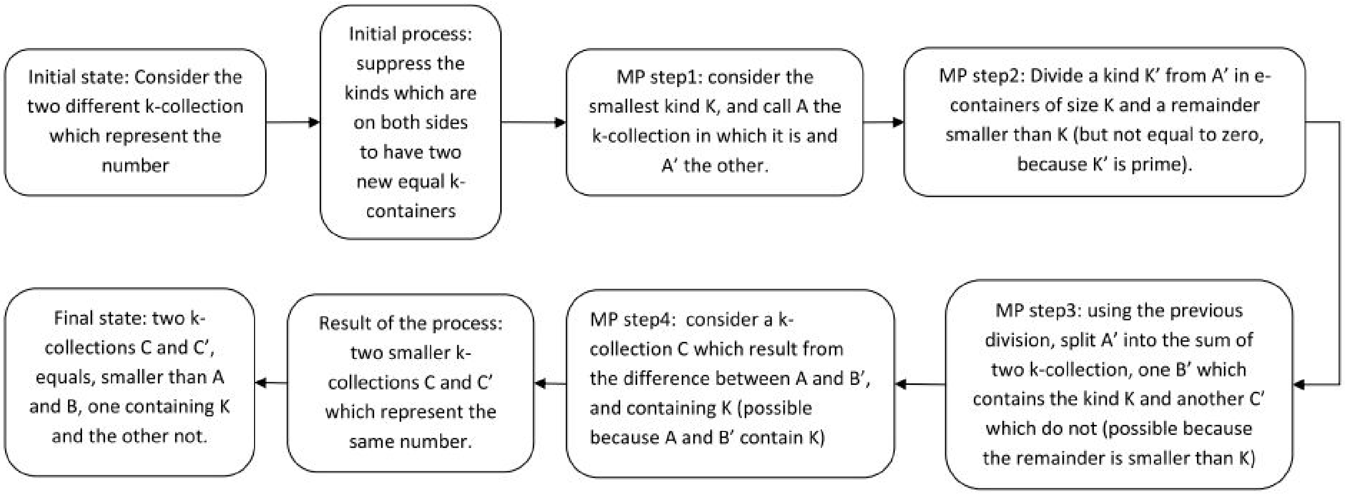
Initial state: Consider the two different k-collection which represent the number
Initial process: suppress the kinds which are on both sides to have two new equal k-containers
MP step1: consider the smallest kind K, and call A the k-collection in which it is and A' the other.
MP step2: Divide a kind K' from A' in e-containers of size K and a remainder smaller than K (but not equal to zero, because K' is prime).
MP step3: using the previous division, split A' into the sum of two k-collection, one B' which contains the kind K and another C' which do not (possible because the remainder is smaller than K)
MP step4: consider a k-collection C which result from the difference between A and B', and containing K (possible because A and B' contain K)
Result of the process: two smaller k-collections C and C' which represent the same number.
Final state: two k-collections C and C', equals, smaller than A and B, one containing K and the other not.

Figure 8: Process to find a smaller number which can be written as two different k-containers

will consider a k-container as an e-container, or an e-container as a k-container. The X-schematic structure of the proof is given in figure 8, which may be better understood by following the example represented in figure 9.

example: In this example, K=3 and is in orange, K'=7 and is in violet, A is on the left, A' on the right. The numbers are represented as e-containers or k-containers. The elliptical containers symbolize addition or difference of the numbers which are inside (as the e-containers) and the rectangular containers, multiplication of the numbers inside (as k-containers).

3.2 Fundamental metaphor of arithmetic

The fundamental theorem of arithmetic allows a one-to-one mapping which is very efficient for capturing many arithmetic properties, which we will refer later as the FUNDAMENTAL METAPHOR OF ARITHMETIC:

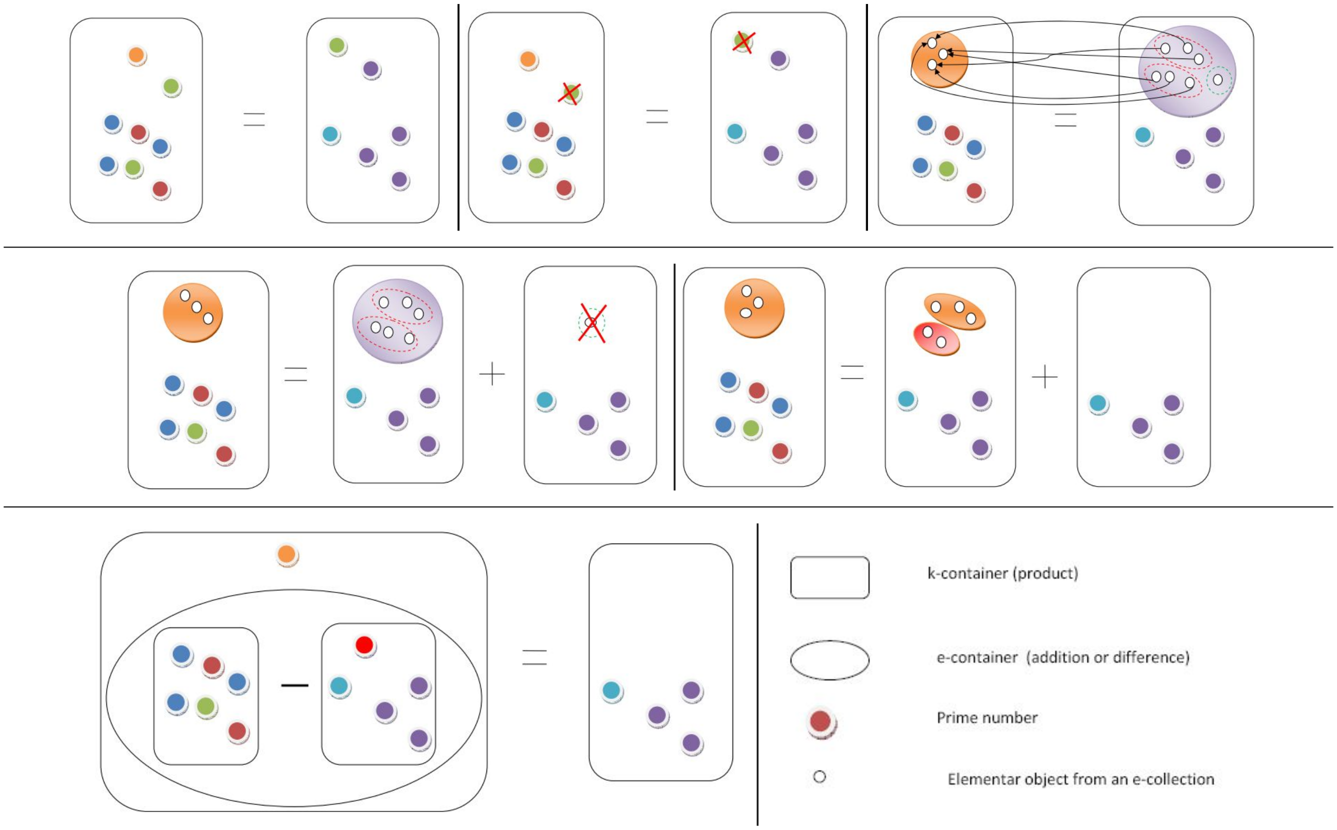
k-container (product)
e-container (addition or difference)
Prime number
Elementar object from an e-collection

Figure 9: example of the descent:
- on the top initial state; initial process; Main process, step 2;
- in the middle: Main process, step 3 ; Main process, step 3
- on the bottom: Main process, step 4

k-containers	*positive integers*
the empty k-container	*1*
an object of a specific kind in a k-container	*a prime number in a decomposition*
a k-container P with a single object	*a prime number P*
several objects (possibly of the same kind) in a k-container A	*a composite number A*
the merger of two k-containers	*the product of two numbers*
all the objects in a k-container A can be mapped one-to-one to objects of the same kind in a k-container B	*A divides B ($A\|B$)*
for each object in a k-container A removing one object of the same kind in the k-container B until the container A is empty	*divide B by A*
two k-containers A and B have no objects of the same kind in common	*A and B are relatively prime*
a k-container with all the objects that A and B have in common, taking multiplicity into account	*the greatest common divisor of A and B*

PROPERTIES

Fundamental theorem of arithmetic

a k-container can be decomposed into k-containers, each containing a single object,in only one way	*each number can be written in one and only one way as a product of primes*

Euclid's lemma

if an object P is in the merger of two collections A and B, it is in at least one of them	*if P is prime and $P\|AB$ then $P\|A$ or $P\|B$*
if k-containers A and B have no object in common, and all objects in A can be mapped one-to-one to the merger of B and C then the objects in A can be mapped one-to-one to the objects in C	*if A and B are relatively prime and $A\|BC$, then $A\|C$*

example: With this metaphor many properties become straightforward, such as the irrationality of the square roots of integers which are not squares of integers. Suppose you have $\sqrt{x} = \frac{a}{b}$, with x, a and b integers, $x = \frac{a^2}{b^2}$. As multiplication is the merging of k-containers, a square contains each e-container an even number of times, so a^2 and b^2 contain each e-container an even number of times. As division is the removal of the e-containers of the divisor from the dividend k-container, $\frac{a^2}{b^2}$ also contains each e-container an even number of times and so is a square.

Figure 10 gives a summary of the understanding I presented of the basic metaphors of arithmetic. The caption that is included with the figure will be systematically used in the rest of this report for similar figures.

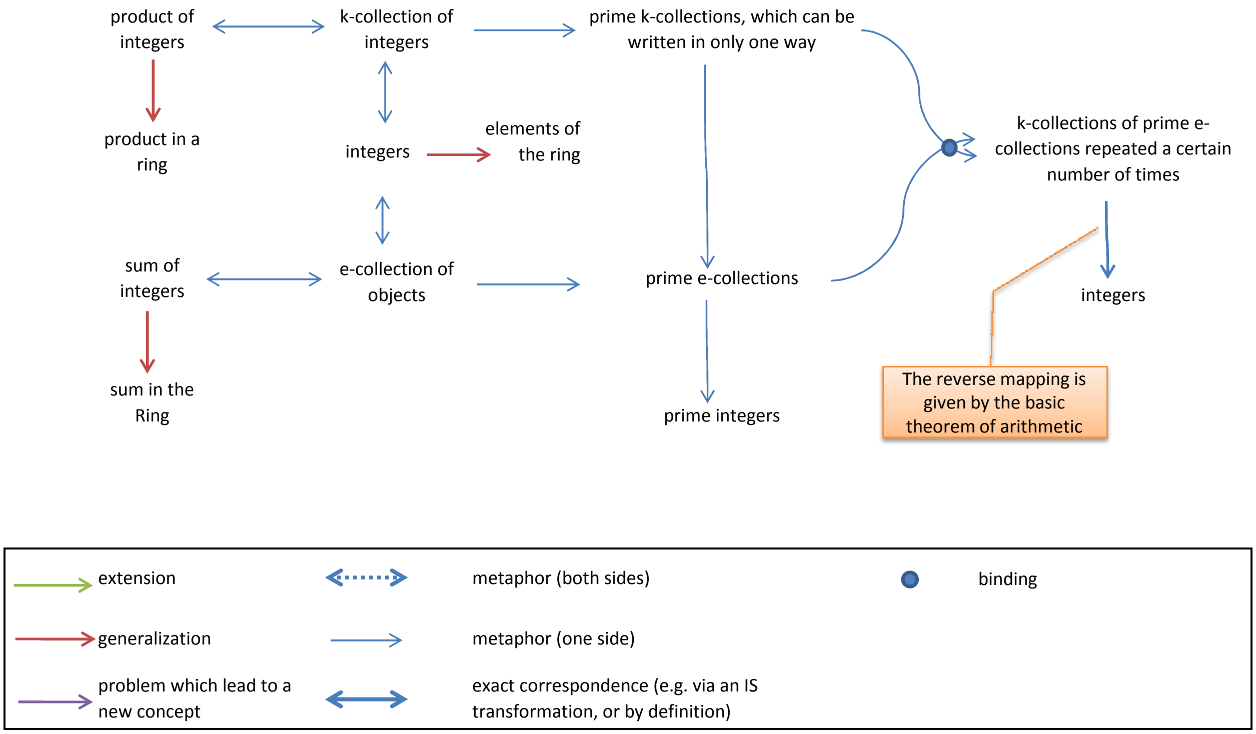
product of integers
k-collection of integers
prime k-collections, which can be written in only one way
product in a ring
integers
elements of the ring
k-collections of prime e-collections repeated a certain number of times
sum of integers
e-collection of objects
prime e-collections
integers
sum in the Ring
prime integers
The reverse mapping is given by the basic theorem of arithmetic
extension
metaphor (both sides)
binding
generalization
metaphor (one side)
problem which lead to a new concept
exact correspondence (e.g. via an IS transformation, or by definition)

Figure 10: The fundamental metaphor of arithmetic

3.3 Finite sets

Thanks to the notion of equivalence relation, we will be able to build finite rings in an intuitive and rigorous way (Rings are systems in which you can add, subtract, and multiply the elements. For a better definition and another interpretation see annex I). Recall that the remainder of the division of A by B is the number of objects you have left if you form as many collections of B elements as possible from a coolection of size A. Consider an integer n. "Have the same remainder by the division by n" is an equivalence relation. The equivalence classes are called classes modulo n. The class of the sum or the product of two elements depends only on the classes of these elements. There are n equivalence classes, the equivalence classes of 0,1,...,n-1. The equivalence classes with addition and multiplication form a ring called $\mathbf{Z/nZ}$. They can also be viewed using different spatial metaphors:

- view numbers as points on a line. Color each equivalence class with a specific color. You can perform operations on numbers as with the usual metaphor where numbers are point on a line, but you care only about the color of the result. We will see that this metaphor can be extended in the plane for complex numbers.

- they can also be interpreted as points on a circle: take a straight line with numbers as points on it, and wrap the line around a circle of radius $\frac{pn}{2\pi}$. Adding numbers becomes adding angles, and any time you make a complete revolution you come back at the same point.

3.4 Polynomials and rational fractions

Polynomials: A polynomial is an expression from the form: $P(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ where the a_i are in a specific ring A. The set of all polynomials is called A[X]. Here we will consider polynomials with coefficients in $\mathbb{C}$ (A definition and interpretation of the complex numbers is given in **??**). We can multiply integral powers of X, $X^a \times X^b = X^{a+b}$ and thus we can extend the addition, subtraction, and multiplication to $\mathbb{C}$[X]. How are polynomials understood? A first way to see them is just as abstract expressions, the sequence of their coefficients, and that is the view we will develop here. Another point of view is to consider the functions associated with the polynomials, and we will come back to this later.

It is possible to transfer arithmetic on $\mathbb{C}$[X] by matching polynomials with integers and there is a precise analogue of the fundamental theorem of arithmetic. Units are the polynomials which can be inverted, and by considering degrees (i.e. the largest exponent of X), one can see that these are exactly the polynomials of degree zero, i.e., the nonzero constants. You can also map the division algorithm, by asking that the remainder shall be of smaller degree than the divisor. As in arithmetic, a polynomial is called prime if it cannot be written as the product of two non constant polynomials. The primes in $\mathbb{C}$[X] are the polynomials $X - a$, with $a \in \mathbb{C}$. Indeed, if you view polynomials as functions (cf. annex II), you can prove that all complex nonconstant polynomials have a zero in $\mathbb{C}$ (the proof of this fact called the basic theorem of algebra is given in **??**). If P is a polynomial and a is a zero of P, then by applying the division algorithm to P divided by $X - a$, you see that the remainder must be zero, so that $X - a$ divide P. On the other hand, it is easy to see that any polynomial of degree one is prime. This fact shows that we can map the fundamental theorem of arithmetic: any polynomial can be written in one and only one way as a product of prime polynomials (and a unit)

Simon Stevin (1548-1620) was the first to discover that this mapping was possible, and Gauss carried over to polynomials the theory of congruence and proved the fundamental theorem of algebra, and we will see how Dedekind and Weber went further with this analogy.

integers	*complex polynomials*
an integer	*a polynomial*
the size of the integer	*the size of the highest exponent of the polynomial*
the unit 1	*the units, the nonzero constant polynomials*
the division algorithm: *for a given B, all A can be written A=BQ+R with R<B*	*the division algorithm:* *for a given B, all A can be written A=BQ+R with R<B*
The prime integers $\wp$	*The prime polynomials* $\{X - a,\ with\ a \in R\}$
The fundamental theorem of arithmetic: *any number can be written in one and only one way* *as a product of primes*	***The fundamental theorem of algebra:*** *any polynomial from degree n can be written* *in one and only one way as the product* *of a unit and n polynomials of the form X-a.*

Rational functions: Just as we have extended the integers to the rationals, we can extend the set of polynomials to the set of rational functions. Intuitively, a rational function is just the division of one polynomial by a non-zero polynomial. For a better mathematical definition, we can once again use equivalence classes on pairs of polynomials, the second being nonzero. The equivalence relation says that $(P, Q) \sim (R, S)$ if $PS = RQ$, and the operations are the natural operations for quotients of polynomials.

3.5 Diophantine equations

The subject of Diophantine equations is a very old one in mathematics. It consists of looking for the integer solutions of equations of the form $P(X, Y...) = 0$, with $P \in \mathbb{Z}[\mathrm{X}]$. It has been proved that there is no general way to solve these equations. Thus, there are a lot of specific methods. We will be interested in two aspects of this problem. Firstly, mapping the properties of arithmetic with certain complex numbers allows one to solve some cases of Fermat last theorem: the equation $X^n + Y^n + Z^n = 0$ has no nonzero solutions for $n \geq 3$. Secondly, mapping arithmetic with certain functions allows one to sort these equations in different classes for which we may have a method for finding solutions.

4 Analogy between arithmetic, analysis and geometry

Thanks to the BASIC METAPHOR OF ARITHMETICS, we have an intuitive notion of divisibility and decomposition of an integer into a product of primes. The idea that it could help to understand the structure of other systems to view them, to think of them as integers: that is, to build efficient metaphors between these other systems and the integers which preserve this property of decomposition, and thus our image-schematic understanding of it; this idea becomes, in Mathematics, according to Weil in [21] "*un principe de transport*, par le moyen duquel tout théorème concernant l'algèbre d'une variété algébrique peut être traduit en un théorème d'arithmétique sur la même variété".

4.1 Extension of the notions of rational and integer in numbers

The first step is to extend these notions to algebraic numbers, which seem similar to rationals numbers. This section uses the concept of complex numbers which is introduced in **??**.

4.1.1 First Intuitive matching

Rational numbers	*Algebraic numbers*
rationals, $\boldsymbol{Q}$ *solution of* $az + b = 0$ *with* $a, b \in \boldsymbol{Z}$	*algebraic rationals* $\bar{Q}$ *solutions of* $a_n z^n + a_{n-1} z^{n-1} + ... + a_o$ *with* $\forall i\ a_i \in \boldsymbol{Z}$
rational integers, $\boldsymbol{Z}$ *solution of* $z + a = 0$ *with* $a \in \boldsymbol{Z}$	*algebraic integers* $\bar{Z}$ *solutions of* $z^n + a_{n-1} z^{n-1} + ... + a_o$ *with* $\forall i\ a_i \in \boldsymbol{Z}$
$\boldsymbol{Z}$ *is a ring in the field* $\boldsymbol{Q}$	$\bar{Z}$ *a ring in the field of* $\bar{Q}$
if $a, b \in \boldsymbol{Z}$, $a\|b$ *(i.e. a divides b) if* $\{\exists c \in \boldsymbol{Z}$ / $b{=}ac\}$	*if* $a, b \in \bar{Z}$, $a\|b$ *if* $\{\exists c \in \bar{Z}$ / $b = ac\ \}$
1 ***property*** *if* $a \in \boldsymbol{Z}$ *and* $\forall b \in \boldsymbol{Z}$ $a\|b$ *then a=1*	*unit* ***definition*** *if* $a \in \bar{Z}$ *and* $\forall b \in \bar{Z}$ $a\|b$ *then a is called a unit*
prime integers, $\wp$ *p is called a prime integer if* $p \in \boldsymbol{Z}$ *and* $\{x{,}y \in \boldsymbol{Z}$ *and* $xy = p \Rightarrow x{=}1$ *or* $y{=}1\ \}$	*prime algebraic integers,* $\wp$ *p is called a prime integer if* $p \in \bar{Z}$ *and* $\{x{,}y \in \bar{Z}$ *and* $xy = p \Rightarrow$ *x is a unit or y is a unit* $\}$

$\Longrightarrow$ *issue with mapping with this definition of prime algebraic integer,*
none of the algebraic integers are prime: we need a more specific mapping.

example: All $\sqrt[n]{m}$ of an integer m are algebraic integers, because they are zeros of $X^n - m$, so $\sqrt{5} = \sqrt[4]{5}^2 = \sqrt[8]{5}^4 ...$

4.1.2 Kummer and Ideal numbers

As we have just seen, to match rationals and algebraic numbers and retain a good notion of prime number seems impossible, because each number can be written as a product of non-units. Nevertheless, Ernst Edouard Kummer (1810-1893) was the first to succeed in creating such a matching. First, he reduced the problem by considering only the algebraic numbers generated by the zeros of $X^n - 1$, and then he showed that there is a good matching for these numbers if we consider ”ideal” prime numbers (which are not actual numbers, but are introduced to be able to decompose numbers which appear to be prime according to our previous definition, but do not behave like prime numbers). What does all of this mean? To understand it you use the basic metaphor of arithmetic. You postulate that all numbers can be written as k-containers in one and only one way. The problem is that some numbers which appear to be prime (they cannot be written as products without units) do not behave like primes because the decomposition of these numbers into products is not unique. Kummer’s hypothesis is that they are in fact composed of several kinds, but that the k-containers with only one kind are not ”real” numbers. Thus he introduced the notion of an ideal prime number, and as a a result some of the false prime numbers could then be written as products of these ideal primes.

4.1.3 Matching with Ideals

In 1876 Richard Dedekind understood that the most important aspect of Kummer’s theory was not the notion of an ideal prime number, but the systems of numbers which could be divided by each prime number (ideal or real). We have already introduced this system with the notion of module in the case of the integers, but the process here is exactly the same. Dedekind thus introduced with the notion of ideals a powerful metaphor. To understand why he considered these ideals, we will first introduce a little more arithmetic in **Z**

Mapping with ideals We consider now $P(X) \in \mathbf{Q}[\mathrm{X}]$, $P(X) = X^n + b_{n-1} X^{n-1} + ... + b_0$, such that P is irreducible in $\mathbf{Q}[\mathrm{X}]$ and $\theta \in \mathbf{C}$ such that $\mathrm{P}(\theta) = 0$.

Rational numbers	*Algebraic number field*
rational numbers, $\boldsymbol{Q}$	*field of algebraic rationals,* Ω= $\{\phi(\theta)/\phi \in \boldsymbol{Q}[X]\}$
rational integers, $\boldsymbol{Z}$	$\diamond$=$\{\phi(\theta)/\phi \in \boldsymbol{Q}[X] and\ \phi(\theta) \in \bar{Z}\}$
$\boldsymbol{Z}$ *is a ring in the field* $\boldsymbol{Q}$	$\diamond$ *a ring in the field* Ω
$\boldsymbol{Z}$ *principal ideals* $n\boldsymbol{Z} = \{x \in \boldsymbol{Z}/\ n \mid x\}$	$\diamond$ *principal ideals* $\alpha\diamond = \{x \in\ \omega/\alpha \mid x\}$
if $a, b \in \boldsymbol{Z}$, $a \mid b$ *(i.e. a divides b) if* $\{\exists c \in \boldsymbol{Z}\ /\ b{=}ac\}$	*if* $a, b \in \diamond$, $a \mid b$ *if* $\{\exists c \in \diamond\ /\ b = ac\ \}$
$\boldsymbol{Z}$ *ideals,* $\Im$ ***property****: if* $A \subset \boldsymbol{Z}$, $\{\exists n \in \boldsymbol{Z}/A = n\boldsymbol{Z}\} \Leftrightarrow$ $\{\forall a, b \in A, \forall x \in \boldsymbol{Z}, ax \in A, a + b \in A\ \}$	$\diamond$ *ideals,* $\Im$ ***definition:*** *if* $A \subset \diamond$, *A is an ideal* $\Leftrightarrow$ $\{\ \forall a, b \in A, \forall x \in \diamond, ax \in A, a + b \in A\ \}$
ideal multiplication *AB*=$\{ab\ /\ a \in A, b \in B\}$ $\Leftrightarrow p\boldsymbol{Z}q\boldsymbol{Z} = pq\boldsymbol{Z}$	*ideal multiplication* *AB*=$\{ab\ /\ a \in A, b \in B\}$
divisibility in $\Im$ *if* $a\boldsymbol{Z}, b\boldsymbol{Z} \in \Im$, $a\boldsymbol{Z} \mid b\boldsymbol{Z}$ *if* $\{\exists c \in \boldsymbol{Z}\ /\ b\boldsymbol{Z}{=}a\boldsymbol{Z}c\boldsymbol{Z}\}$	*divisibility in* $\Im$ *if* $A, B \in \Im$, $A \mid B$ *if* $\{\exists C \in \Im\ /\ B = AC\ \}$
unit, 1$\boldsymbol{Z}$=$\boldsymbol{Z}$	*unit* $\diamond$
prime ideals *P is called a prime ideal if* $P \in \Im$ *and* $\{X, Y \in \Im$ *and* $XY = P \Rightarrow X{=}\boldsymbol{Z}$ *or* $Y{=}\boldsymbol{Z}\ \}$ $\Leftrightarrow \{P = p\boldsymbol{Z} with p \in \wp\ \}$	*prime ideals* *P is called a prime ideal if* $P \in \Im$ *and* $\{X, Y \in \Im$ *and* $XY = P \Rightarrow X{=}\boldsymbol{Z}$ *or* $Y{=}\boldsymbol{Z}\ \}$

$\Longrightarrow$ *good mapping, for both sides we have the property* $\forall\ A \in \Im\ \exists! v_1, v_2 .../$
$A = \prod_{P_i\ prime\ ideals} P_i^{v_i}$

example: The first of the following two figures shows the algebraic integers of the field $\mathbf{Q}[\sqrt{-3}]$ along with its units, and the second figure shows the primes in this field. We have succeeeded in mapping the basic property of arithmetic onto algebraic number fields, and we have shown that this property is image-schematic. We can thus map the image-schematic representation we had for integers onto algebraic number field ideals. Particularly, we can speak of two integers as being congruent modulo another integer.

4.1.4 Solution of Fermat's last theorem for the exponent n=3

The problem is to prove that, aside from the solution $X = Y = Z = 0$, there are no other solutions in $\mathbb{Z}$ to the equation

$$X^3 + Y^3 + Z^3 = 0. \tag{1}$$

There are two classic proofs for this case of Fermat's theorem. The two proofs use infinite descent (they prove that given a solution there is a smaller one, and then contradict the fact that there should be a smallest solution if there are any), but the first one, due to Euler, uses integers of the form $a^2 + 3b^2$ and the second one, due to Gauss, uses integers of the form $a + b\zeta$, where $\zeta = \dfrac{-1 + i\sqrt{3}}{2} = e^{\dfrac{2i\pi}{3}}$. We will focus on the second method, because it is more general and directly linked to what we have done. Indeed, the integers of the form $a + b\zeta$ are exactly the integers of the field $\mathbf{Q}[\sqrt{-3}]$, which is also the field generated by $X^2 - X + 1$. In fact this proof appeared before the work of Kummer and Dedekind, but this work generalized Gauss' ideas and Kummer's main theorem generalized this proof to a large class of prime integers.

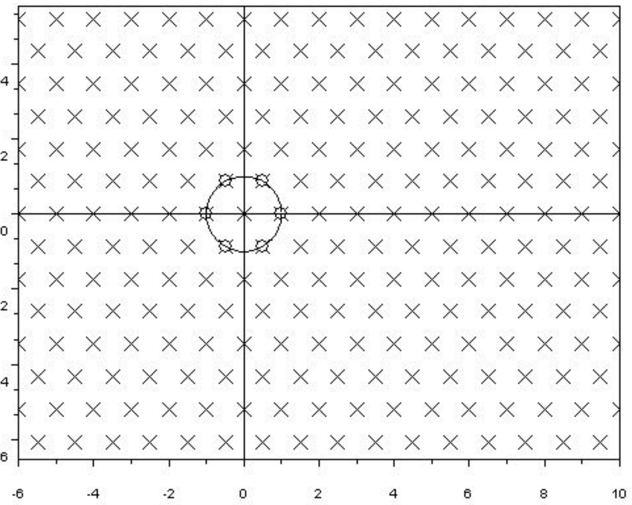

Figure 11: The integers and units of $\mathbf{Q}[\sqrt{-3}]$

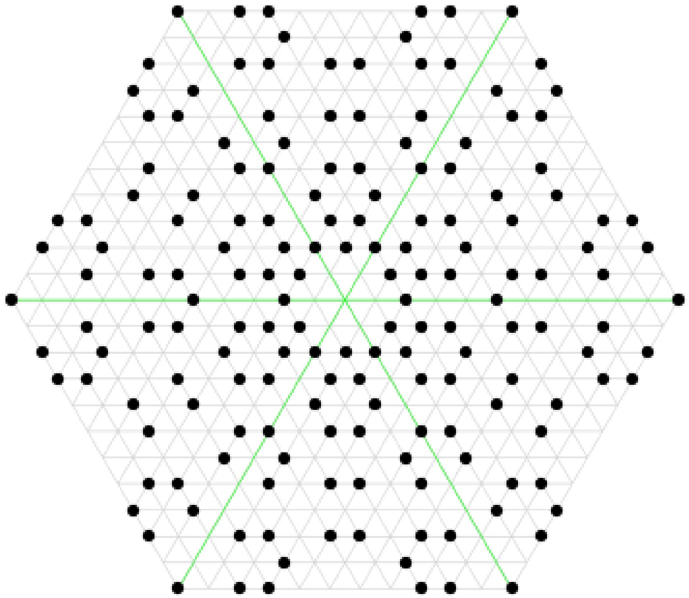

Figure 12: The prime numbers among the integers of $\mathbf{Q}[\sqrt{-3}]$

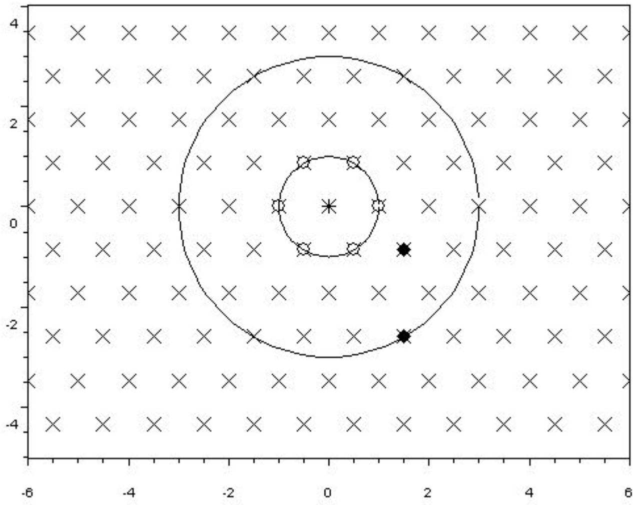

Figure 13: $\lambda = 1 - \zeta$, λ^2, in the ring A, with circles of size 1 and 3

We consider a solution (α,β,γ) of the equation. The idea of the proof is to use arithmetic properties of this solution to build a new and smaller solution. Because we saw that the metaphor for arithmetic works better for products, we will try to rewrite the equation as an equality of products. This is not possible in **R**, but it is in **C**. Indeed, $1+\zeta+\zeta^2 = 0$, and so $(-\gamma)^3 = \alpha^3+\beta^3 = (\alpha+\beta)(\alpha+\zeta\beta)(\alpha+\zeta^2\beta)$. More interestingly, $\alpha+\beta \equiv \alpha+\zeta\beta \equiv \alpha+\zeta^2\beta \; mod[\lambda]$, where $\lambda = 1-\zeta$, because $1 \equiv \zeta \equiv \zeta^2 \; mod[\lambda]$. Thus, $\alpha^3+\beta^3$ can be written as a cube of a number depending of α and β modulo lambda, and the process is reversible.

Indeed, because $1+\zeta+\zeta^2 = 0, 0 = (\alpha+\beta)+\zeta(\alpha+\zeta\beta)+\zeta^2(\alpha+\zeta^2\beta)$. For this reason, we will work in the ring A of the integers of $\mathbf{Q}[\sqrt{-3}]$. This is a ring with nice properties; the basic metaphor for arithmetic applies exactly, and, moreover, each ideal is principal (i.e., is generated by a single number). For this reason, we will be able to think of numbers as ideals. We will write $a \sim b$ if there is a unit ε such that $a = b\varepsilon$ (this means they generate the same ideal).

We will try to use congruences in A, and we will be especially interested in the congruence of x^3 given the congruence of x. Because $(a+b)^3 = a^3+b^3+3(a^2b+b^2a)$, we see we will be interested in congruences modulo λ such that $3 \equiv 0 \; mod[\lambda]$ and even $3 \equiv 0 \; mod[\lambda^2]$. 3 is not a prime number, indeed, $3 \sim (1-\zeta)^2$ and $(1-\zeta)$ is a prime number as shown in fig.13 So it will be easier to consider the congruence modulo $\lambda = 1-\zeta$. To begin, we can look at the equivalence classes modulo λ in fig. 14. There are three of them, the equivalence classes of 0, 1 and -1. Because $\lambda^2 \sim 3$ we have the following property:” if $x \equiv y \; mod[\lambda]$ then $x^3 \equiv y^3 mod[\lambda^3]$”. We have also the following lemma: if $x \in A$ and $\lambda \nmid x$ then $x^3 \equiv \pm 1 \; mod[\lambda^4]$.
To prove this lemma, you just need to write it. Any equality is easy to see straightforward with metaphors, but because you have to look at a lot of cases, in fact 6 of the congruences modulo 9, for which it is true for different reasons, the general equality is not straightforward.

proof: We suppose that α, β and γ are solutions of (1) in A. We can assume that α, β and γ are relatively prime (no prime or kind is in the three of them, and thus in two of them because of the equality)and hence that $\lambda \nmid \alpha$ and $\lambda \nmid \beta$. (it is clearly possible if you look at the ideals as containers schema: λ can be in only one of them)

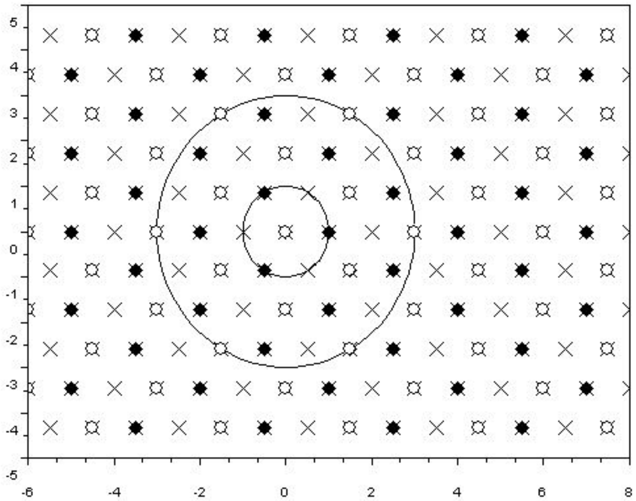

Figure 14: The equivalence classes modulo λ

case 1: $\lambda \nmid \gamma$ We have

$$0 = \alpha^3 + \beta^3 + \gamma^3 \equiv \pm 1 \pm 1 \pm 1 \; mod[\lambda^3]$$

which is false. (To see this, you just have to look at the equivalence classes, and because $|\lambda^3| = 3\sqrt{3}$, two elements in the same equivalence class are at least at a distance of $3\sqrt{3} > 3$ apart this comes directly from the plane metaphor for multiplication in **C**.)

case 2: $\lambda | \gamma$ In this case, we will isolate the powers of λ in γ, and then write $\gamma = \lambda^n \delta$ where $\lambda \nmid \delta$. To come back to the first case, we will consider the property

(P_n) *There exist* α, β, $\gamma \in A$ *such that* $\lambda \nmid \alpha$, $\lambda \nmid \beta$, $\lambda \nmid \gamma$, α, β *and* γ *are relatively prime and solution of* $X^3 + Y^3 + \omega\lambda^{3n} Z^3 = 0$ *where* ω *is a unit*, and prove that if it is true for n, it is for n-1.

If P_n is satisfied, then $n \geq 2$: From the lemma we have

$$\alpha^3 + \beta^3 \equiv \pm 1 \pm 1 \equiv -\omega\lambda^{3n}\delta^3 \; mod[\lambda^4]$$

Since $\lambda \nmid \pm 2$ the $3 + \beta^3 = 0 \; mod[\lambda^4]$ and then $3n \geq 4$ and $n \geq 2$.

If P_n is satisfied, then P_{n-1} is satisfied: $-\omega\lambda^{3n}\delta^3 = \alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \zeta\beta)(\alpha + \zeta^2\beta)$. Since $\alpha + \beta \equiv \alpha + \zeta\beta \equiv \alpha + \zeta^2\beta \; mod[\lambda]$, we see with the BASIC METAPHOR OF ARITHMETICS that

$$\frac{\alpha + \beta}{\lambda}, \frac{\alpha + \zeta\beta}{\lambda}, \frac{\alpha + \zeta^2\beta}{\lambda} \in A$$

With the BASIC METAPHOR OF ARITHMETICS, because α and β are relatively prime, we see that $\frac{\alpha+\beta}{\lambda}$, $\frac{\alpha+\zeta\beta}{\lambda}$ and $\frac{\alpha+\zeta^2\beta}{\lambda}$ are relatively prime. Then λ divides one and only one of these numbers and each can be writing as a cube times a unit $\omega_{01}\phi_1^3, \omega_{02}\phi_2^3$ and $\omega_{03}\phi_3^3$.

From $0 = (\alpha+\beta) + \zeta(\alpha+\zeta\beta) + \zeta^2(\alpha+\zeta^2\beta)$, it follows that $\phi_1^3 + \omega_1\phi_2^3 + \omega_2\lambda^{3(n-1)}\phi_3^3 = 0$ where ω_1 and ω_2 are units. By considerations modulo λ^4 we can show that $\omega_1 = \pm 1$, concluding the proof.

4.2 Mapping with other kinds of objects

Once we have the powerful notion of ideals, developed with the algebraic numbers, in precise analogy with the rational numbers, we can use it to map the properties of numbers onto very different objects, for example functions, or points. Some basic facts about functions are presented in Annex 2.

4.2.1 Algebraic numbers and algebraic functions

The first mapping we will introduce was made by Dedekind and Weber in 1882, and allowed for the development of algebraic geometry (the study of algebraic varieties, i.e. the surface defined by the zeros of a polynomial); and in turn, as we shall see, progress with certain algebraic questions. We present this analogy just as Dedekind and Weber did in their article.

We always consider $P(X) \in \mathbf{Q}[X]$, $P(X) = X^n + b_{n-1}X^{n-1} + ... + b_0$, such that P is irreducible in $\mathbf{Q}[X]$ and $\theta \in \mathbf{C}$ such that P(θ)=0. We also consider $P'(X) \in \mathbf{Q}[x][X]$, $P'(X) = X^n + c_{n-1}X^{n-1} + ... + c_0$ (the c_i are in $\mathbf{Q}(x)$, such that P’ is irreducible in $\mathbf{Q}(x)[X]$) and θ' is a function of x such as P(θ’)=0.

Algebraic number field	*Algebraic function field*
algebraic rationals (usually called “algebraic numbers”) $\bar{Q}$ *solutions* $z \in \boldsymbol{C}$ *of* $a_nz^n + a_{n-1}z^{n-1} + ... + a_o$ *with* $\forall \boldsymbol{i}\ a_i \in \boldsymbol{Z}$	*algebraic functions* *solutions* $z \in \boldsymbol{F}(x)$ *of* $a_nz^n + a_{n-1}z^{n-1} + ... + a_o$ *with* $\forall \boldsymbol{i}\ a_i \in \boldsymbol{C}[x]$
algebraic integers $\bar{Z}$ *solutions* $z \in \boldsymbol{C}$ *of* $z^n + a_{n-1}z^{n-1} + ... + a_o$ *with* $\forall \boldsymbol{i}\ a_i \in \boldsymbol{Z}$	*regular functions* *solutions* $z \in \boldsymbol{F}(x)$ *of* $z^n + a_{n-1}z^{n-1} + ... + a_o$ *with* $\forall \boldsymbol{i}\ a_i \in \boldsymbol{C}[x]$
$\bar{Z}$ *a ring in the field of* $\bar{Q}$	*regular functions are a ring in the field of algebraic functions*
algebraic number field, $\Omega = \{\phi(\theta)/\phi \in \boldsymbol{Q}[X]\}$	*algebraic function field,* $\Omega = \{\phi(\theta')/\phi \in \boldsymbol{Q}[X]\}$
$\diamond = \{\phi(\theta)/\phi \in \boldsymbol{Q}[X]$ *and* $\phi(\theta) \in \bar{Z}\}$	$\diamond = \{\phi(\theta')/\phi \in \boldsymbol{Q}[X]$ *and* $\phi(\theta')$ *regular function* $\}$
$\boldsymbol{Z}$ *is a ring in the field* $\boldsymbol{Q}$	$\diamond$ *a ring in the field* Ω
if $a, b \in \diamond,\ a\vert b$ *if* $\{\exists c \in \diamond\ /\ b = ac\ \}$	*if* $a, b \in \diamond,\ a\vert b$ *if* $\{\exists c \in \diamond\ /\ b = ac\ \}$
$\diamond$ *ideals,* $\Im$ *if* $A \in \diamond$, A *is an ideal*$\Leftrightarrow$ $\{\ \forall a, b \in \diamond, \forall x \in \diamond, ax \in \diamond, a+b \in \diamond, a-b \in \diamond\ \}$	$\diamond$ *ideals,* $\Im$ *if* $A \in \diamond$, A *is an ideal*$\Leftrightarrow$ $\{\ \forall a, b \in \diamond, \forall x \in \diamond, ax \in \diamond, a+b \in \diamond, a-b \in \diamond\ \}$
ideal multiplication	*ideal multiplication*
divisibility in $\Im$	*divisibility in* $\Im$
prime ideals	*prime ideals*

$\Longrightarrow$ *good mapping, for both sides we have the property* $\forall\ A \in \Im\ \exists! v_1, v_2 .../$
$A = \prod_{P_i\ prime\ ideals} \boldsymbol{P}_i^{v_i}$

4.2.2 Algebraic functions and points on a Riemann surface

In the same article, Dedekind and Weber presented a second mapping, which allowed them to give a new proof of the Riemann-Roch theorem from algebraic geometry. This was due to the fact that the prime ideals of regular functions are exactly the regular functions which vanish at a specific point.

Functions and points This part of the analogy is quite important because it shows that it is not only formal, but that even properties of functions (their values, and not only their formal description) can be interpreted and transmitted with our metaphor. We now consider an algebraic function field Ω.
First, we have to give a definition of a point on a Riemann surface. From the point of view of the field Ω, two points A and B are different if there is a function which has different values at A and B. That's why Dedekind says that a point on the Riemann surface is by definition a specific valuation on the functions of Ω. Two points are distinct if and only if two functions from Ω have different values on this point. It seems of course impossible to have this idea for a definition without the space metaphor, but once it is given, we no longer need this metaphor to reason about points on a Riemann surface, which could possibly have other properties than actual points in space. Dedekind presents this process in [14] §14: ”Eine Geometrische Versinnlichung des ”Punktes” ist übrigens keineswegs notwendig (...) . Es genügt das Wort ”Punkt” als einen kurzen und bequem Ausdruck für die beschriebene Wert-Koexistenz zu betrachten”

Points and fields of functions on the plane	*Points on a Riemann surface and Ω*
property: *→ if A and B are two distinct points, there is a function f such as $f(A) \neq f(B)$ (except if all functions in the field are constant)* *→ At each specific point we can associate a value for each function*	***definition:*** *To each valuation on the functions of Ω we associate an object A called a point.*

Points and ideal We can prove that if B is a point on a Riemann surface and z is a finite variable in B, any regular function of z is finite in B. Now, if f, g are two functions in $\diamond$ such that $f(B) = g(B) = 0$, then for all functions h in $\diamond$ $fh(B) = 0$ and $f + g = 0$. Thus the set of all functions that vanish at B is an ideal. In fact, one can prove that it is a prime ideal.

One can now further associate to every set of points $B_1, B_2, ...$, called a polygon, the ideal that is the product of the ideals generated by $B_1, B_2...$ An interesting question is the meaning of expressions like B^2 in terms of functions. Dedekind and Weber give an answer in §15 of [14] by defining the order of a function $f \in \Omega$ at a point B. If we take the set S of all the functions of Ω which vanish at B, we say that f is of order 1 (respectively, of order r), or 0^1 (resp 0^r), if for all $g \in S$, $\frac{g}{f}$ (resp. $\frac{g^r}{f}$) is finite.

Point on Riemann surface	*Ideals of $\diamond$*
a point	*a prime ideal*
a polygon (i.e. a set of points)	*an ideal*
the number of times a point is in a polygon	*the minimal order of the function in the ideal*

This mapping between ideals and points has important consequences in algebraic geometry. Indeed, each time you have a ring A, you can associate to it a geometric construction in the following way: view the set of all prime ideals of A, also called the spectrum of A, as a space by considering each prime ideal as a point.
Another really interesting thing about this mapping, is that it allows us immediately to map the BASIC METAPHOR OF ARITHMETIC and to define and understand the product or the greatest common divisor of two polygons with this metaphor.

k-container	*Ideals of* $\diamond$	*set of points on the Riemann surface*
a kind	*a prime ideal*	*a point*
a collection of kind	*an ideal*	*a polygon*
the merging of two k-containers	*the product of two ideals*	*the merging of two polygons*
the smallest k-container containing the kinds of two others	*the least common multiple of two ideals*	*the smallest polygon containing two others*
the set of the kinds in two k-containers	*the greatest common divisor of two ideals*	*the intersection of two polygons*

From Points to Riemann surface: We have already defined points by using arithmetic considerations, but can there be another and more geometric representation of them? The answer is yes: Dedekind and Weber explain in §16 of [14] "Will man von dieser Definition der "absoluten" Riemannschen Fläche, welche ein zu ein Körper $\mathbf{\Omega}$ gehöriger invarianter Begriff ist, zu der bekannten Riemannschen Vorstellung übergehen, so hat man sich die Fläche in einer z-Ebene ausgebreitet zu denken, welche sie dann überall mit Ausnahme der Verzweigungspunkte n-fach bedeckt" In fact they give even a way to "draw" it. Indeed it is possible to show that, if z is in $\mathbf{\Omega}$, n is the degree of the polynomial we used to define $\mathbf{\Omega}$ and c is a constant, the principal ideal $\diamond(z-c)$ can be written as a product of n prime ideals. Now imagine the complex plane, and to each point c associate the n points of the previous decomposition. Except in a finite number of cases, the n points are different, so the surface can be locally viewed as the superposition of n graphs of a continuous function. Only for a few points, the ramifications points, several prime ideals are the same.
In this way, you can associate to each function in $\mathbf{\Omega}$ a Riemann surface, and the polygon of the ramifications points (with their multiplicity).

Ideals of $\diamond$	*Riemann surface view in space*
a prime ideal	*a point*
an ideal $\diamond(z-c)$	*the set of points above the point c in the complex plane*
the ideals $\diamond(z-c)$ *whose decompositions contain the same ideal several times*	*a point c from the complex plane above which there is a ramification point*

Polygon and function The notion of order of a function allow us to make a mapping between the function of ω and a quotient of polygons. Indeed, as we define positive order for a function equal to zero at a point, we can define a negative order for a function which is infinite at a point. Dedekind and Weber show in §17 of [14] that if you know the order of a function on all points (and there are only a finite number of points where it is not zero), you almost know the function, except for multiplication by a constant. Thus, you can represent a function as the quotient of the two polynomials containing the points (with their multiplicity) where the function is infinitely small or big. The fact that two polygons represent a function in $\mathbf{\Omega}$ is an equivalence relation, as is shown in §18.

4.3 Reverse mapping, from function to numbers

4.3.1 p-adic numbers

Hensel introduction of p-adic integers: In 1897, Kurt Hensel introduced the reverse mapping. In fact he realized that we are able to understand analytical functions quite well because we are able to write them $f(z) = \sum_{i=0}^{\infty} a_i(z-a)^i$ for different points a, which we cannot do with numbers. Because of the deep analogy between the factors $(z-a)$ and the prime numbers, which can both be considered as elementary kinds, he introduced the notion of p-adic numbers, $\sum_{i=0}^{\infty} a_i p^i$. On these numbers, we can easily define the addition, subtraction and multiplication. Hensel really wanted to draw an efficient analogy between functions and numbers, with the goal of using the methods of function theory in the study of numbers, as Dedekind and Weber had introduced the methods of number theory in function theory [20]: "Seit meiner erste Beschäftigung mit den Fragen der höheren Zahlentheorie glaubte ich, dass die Methodes de Funktionentheorie auch auf dieses Gebiet anwendbach sein müssten". The set of p-adic integers is written $\mathbb{Z}_p$.

p-adic integers as a projective limit of Z/p^nZ: Knowing the projection of a number in Z/p^nZ give us quite a good understanding of this number, especially as n grows. In other words if we know the sequence of the projections of a number in Z/p^nZ for all n in $\mathbb{N}$, we know the number. Conversely, to any sequence of numbers z_n in Z/p^nZ such that $z_n = \pi(z_{n+1})$, we could associate a number z (where π is the natural projection from $Z/(p+1)Z$ in Z/pZ). This number is a p-adic integer. Hensel himself presents this point of view in [20] where he defined the number $\bar{A}$ as the limit $lim_{k=\infty}\bar{A}_k$ with $\bar{A}_k \equiv \bar{A}_{k+1}$ $(mod\ p^k)$. In this introduction we see that the analogy between polynomials and integers is present, and is even a little deeper, with an analogy between polynomials of degree n and Z/p^nZ. Indeed, the analytical functions in a can be seen as the projective limit of the polynomials of degree n in $(z-a)$.

The general p-adic numbers: Contemplating the nature of the inverse of a p-adic integer lead Hensel to consider numbers of the form $\sum_{i=\nu}^{\infty} a_i p^i$, where ν is a (possibly negative) integer, with an immediate analogy with meromorphic functions. The p-adic numbers thus introduced form a field (addition, multiplication subtraction and division are possible) written $\mathbb{Q}_p$.

Size of a p-adic number: Hensel realized that it is awkward to speak of the value of $\sum_{i=\nu}^{\infty} a_i p^i$ since the size of the integers p^i is increasing. To have a reasonable notion of convergence, he introduced a new notion of size, again using the analogy with functions. If you are near a point a, the size of the function $f(x) = \sum_{i=\nu}^{\infty} a_i(x-a)^i$ is approximately $(x-a)^\nu$. Thus, using the analogy between primes and factors $(x-a)$ in the decomposition of a polynomial, one can define the p-adic size of $z = \sum_{i=\nu}^{\infty} a_i p^i$ as $|z|_p = p^{-\nu}$. This is a well-behaved notion of size in the sense that $|a.b|_p = |a|_p.|b|_p$ and $|a+b|_p \leqslant ||a|_p + |b|_p$ (and even $|a+b|_p \leqslant \max(|a|_p, |b|_p)$).

Links with the rationals: It is clear that every integer is a p-adic number. Indeed, any positive integer can be written $a_0 + a_1 p + ... + a_n p^n + 0 \times p^{n+1} + ...$ and $-1 = (p-1) + (p-1)p + ... + (p-1)p^k + ...$ It is also clear from the fact that the p-adic integers are the projective limit from Z/p^nZ. We thus have a standard inclusion of Z in the p-adic numbers, which can be easily extended to an inclusion of $\mathbb{Q}$ in the p-adic numbers (in fact, the rational numbers correspond to p-adic numbers whose sequences are periodic). Thus we can consider that $\mathbb{Q} \subset \mathbb{Q}_p$. The analogy with the reals and the rationals (which can be seen as infinite sequences of bits and infinite periodic sequences of bits, respectively) leads to the idea that the p-adic numbers can also be built as a completion of the rationals, not with the usual idea of size, but with the p-adic one. This is indeed the case.

Ostrowski's theorem: This construction of $\mathbb{Q}_p$ as a completion of $\mathbb{Q}$ using a specific notion of distance leads to the question of whether there are other possible distances on $\mathbb{Q}$ and what structures could be built from $\mathbb{Q}$ using these other notions of distance. The theorem of Ostrowski tells us that there are in fact no other possibilities for $\mathbb{Q}$ (in fact that for any absolute value on $\mathbb{Q}$ "$|.|$" there exist a real positive number α and a prime number p such that $|.| = |.|_p{}^\alpha$ or $|.| = |.|_\infty{}^\alpha$, where "$|.|_\infty$" is the usual absolute value) and thus that there is not any other completion of $\mathbb{Q}$ than the $\mathbb{Q}_p$ and $\mathbb{R}$, also written $\mathbb{Q}_\infty$

local point of view for functions	*p-adic numbers*
approximation of a function in $\mathbb{C}_n\,[X]$ $f(x) = \sum_{i=\nu}^{n-1} a_i(x-a)^i + o((x-a)^n) \text{ with } a_\nu \neq 0 \text{ and } \forall i,\ a_i \in \mathbb{C}$	*approximation of a number in* Z/p^nZ $\sum_{i=\nu}^{n-1} a_i p^i + o(p^{-n}) \text{ with } a_\nu \neq 0 \text{ and } \forall i,\ a_i \in \{0, 1, ..., p-1\}$
a meromophic function in a $f(x) = \sum_{i=\nu}^{\infty} a_i(x-a)^i \text{ with } a_\nu \neq 0 \text{ and } \forall i,\ a_i \in \mathbb{C}$	*a p-adic number* $\sum_{i=\nu}^{\infty} a_i p^i \text{ with } a_\nu \neq 0 \text{ and } \forall i,\ a_i \in \{0, 1, ..., p-1\}$
develloppement of function near a point at the order n	*representation of a number in* Z/p^nZ
size of f in x near a, $\lvert f\rvert \sim \lvert x-a\rvert^\nu$	*size of z,* $\lvert z\rvert = p^{-\nu}$
projective limit of polynomials of degree n *analytic functions* $f(x) = \sum_{i=0}^{\infty} a_i(x-a)^i \text{ with } \forall i,\ a_i \in \mathbb{C}$	*projective limit of* Z/p^nZ *p-adic integers* $\sum_{i=0}^{\infty} a_i p^i \text{ with } \forall i,\ a_i \in \{0, 1, ..., p-1\}$

4.3.2 From local to global in Diophantine equations, Minkowski-Hasse theorem

The local-global principle: Because $\mathbb{Q} \subset \mathbb{Q}_p$ for any prime $p \leqslant \infty$ ($\mathbb{Q}_\infty = \mathbb{R}$), if an equation has a solution in $\mathbb{Q}$, it has also a solution in $\mathbb{Q}_p$. Conversely, we can ask if an equation that has a solution in $\mathbb{Q}_p$ for every p also has a solution in $\mathbb{Q}$. More generally, the local-global principle is to look at the local fields $\mathbb{Q}_p$ and at $\mathbb{R}$ to obtain information about $\mathbb{Q}$. This is natural in the sense that they are all the completions of $\mathbb{Q}$ (Ostrowski theorem), and because of the analogy with functions, which says that the p-adic numbers give us local information "near" a prime number p: if we have local information at every "location," we may have a global information as well.

Square root extraction in $\mathbb{Q}_p$: Because of prime decomposition, we have a link between all the distances on $\mathbb{Q}$. Indeed, for any rational r, $\prod_{p \leqslant \infty} \lvert r\rvert_p = 1$. Thus, if an equation $X^2 = a$ with $a \in \mathbb{Q}$ has a solution in $\mathbb{Q}_p$ for any $p < \infty$, there is a solution in $\mathbb{Q}$ (using the fact that $\lvert a^2\rvert = \lvert a\rvert^2$).

Theorem of Hasse-Minkowski: This theorem generalizes the previous property. A quadratic form has a nonzero solution in $\mathbb{Q}$ if and only if it has a nonzero solution in $\mathbb{Q}_p$ for any $p \leqslant \infty$.

Limit to the principle: The local-global principle is nevertheless not always true. For example, the Fermat equation has a solution in the field $\mathbb{Q}_p$ for any p and any $n > 2$, but not in $\mathbb{Q}$ for $n > 2$.

References

[1] Georges Lakoff *Women, Fire, and Dangerous Things: What Categories Reveal About the Mind*, The university of Chicago Press, 1987

[2] Terry Regier, *The Human Semantic potential*, MIT Press, 1996

[3] George Lakoff, Rafael E. Núñez , *Where Mathematics come from?*, Basic Books, 2000

[4] David Bailey *A computationnal model of embodiemment in the acquisition of action Verbs*PhD UCB 1997

[5] Srini Narayanan *Embodiement in language understanding : Sensory-motor representation for Metaphoric reasonning about event description* PhD UCB 1997

[6] Nancy Nersessian , *Creating Scientific Concepts*

[7] Theodore L. Brown , *Making Truth: Metaphors in Science*

[8] George Lakoff, *Philosophy in the flesh : The Embodied Mind and Its Challenge to Western Thought*

[9] Hermann Weyl, Philosophy of Mathematics and Natural Science.

[10] Stanislas Dehaene, *The Number Sense*, 1997

[11] Gilles Fauconnier and Mark Turner, *Conceptual Integration Networks* , Cognitive Science, Vol. 22, 1998

[12] Richard Dedekind *Was sind und was sollen die Zahlen*

[13] Jean Petitot *Neurogéomètrie de la vision*

[14] Richard Dedekind and Carl Weber, *Theorie der Algebraischen funktionnen einer Veränderlichen*

[15] Isabella Bashmakova and Galina Smirnova *The beginning and Evolution of Algebre*

[16] Gauss, *Untersuchungen über höhere Arithmetik*, Berlin, 1889

[17] Ernst Kummer *Zur Theorie der complexen Zahlen*, J. für Math., 1847

[18] Ernst Kummer *Uber die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren*, J. für Math., 1847

[19] Richard Dedekind, Xth Supplement to the second edition of Dirichlet's *Lectures on the number Theory,*

[20] Kurt Hensel, *Theorie der Algebraischen Zahlen*, 1908

[21] André Weil, *Arithmétique et géomètrie sur les variètés algébriques*, 1935

[22] Bernardh Riemann On the Hypotheses That Lie at the Foundation of Geometry 1854

[23] Piero Della Francesca De prospettiva pingendi

[24] Patrizi De spacio physico et mathematico 1587

[25] Euclide, Les Elements

[26] Max Jammer, Concepts of space: The History of Theories of Space in Physics

[27] Platon, Timée, Les Belles Lettres, 1956

[28] George Johnston Allman, Greek Geometry from Thales to Euclide, 1889.

[29] Nancy Neressian, Creating Scientific Concepts

[30] Hermann Weyl, The Continuum

[31] René Descartes, Géométrie

[32] Peter Pesic, Beyond Gemoetry, Classic papers from Riemann to Einstein, 2006

[33] Martin Väth, Nonstandard Analysis, 2000

[34] Henri Poincaré, Des fondements de la géométrie

[35] Gilles Fauconnier and Mark Turner, The Way We Think: Conceptual Blending and the Mind's Hidden Complexities,2002

websites :

[36] `http://markturner.org/blending.html` : Gilles Fauconnier and Mark Turner website on conceptual blending, including a presentation of the theory and a lot of references.

[37] `http://www.icsi.berkeley.edu/NTL/` The NTL group website. A software using their formalism to analyse sentences is available on `http://www.icsi.berkeley.edu/ lucag/`