François Viète, between analysis and cryptanalysis

Marco Panza

François Viète

Between Analysis and Cryptanalysis

Marco Panza

CNRS, Paris,

Équipe REHSEIS (UMR 7596, CNRS and Univ. of Paris 7);

e-mail: Marco.Panza@paris7.jussieu.fr

June 12, 2005

François Viète (1540-1603) was certainly one of the figures who mainly inspired the emergence of a new way to do mathematics in early modern age. He was also a statesman and an adviser of the French King Henry IV, who employed him, during his confrontation with the Holy League, to decrypt the coded messages of the Spaniards and the Italians and appointed him to the title of *déchiffreur du roi*. He has been often considered the "father of mod-

ern algebra" and, more recently, P. Pesic called him "the father of modern cryptanalysis"[1].

The first judgement could be based on the consideration of different parts of Viète's *oeuvre*, according to the different senses that could be attributed to the term "algebra"[2], but is usually justified by relying on the symbolic formalism that Viète used both in the *In artem analyticem isagoge* and in the *Zeteticorum Libri*[3], where capital consonants and vowels are employed to denote known and unknown quantities, respectively.

The second judgement has been justified, instead, by relying on the consideration of two short memoirs that remained unpublished for a long time[4]. The first of them was written by Viète himself on his deathbed and addressed to the duke of Sully, in order to expose his techniques for codebreaking. The second, probably written sometimes after Viète's death, is a more general description of the same techniques[5]. Pesic has translated them into English and published them[6].

In another paper of his, Pesic argued for the existence of a "close rapport" between Viète's methods in cryptanalysis and "the innovations he introduced in the conceptual foundations of mathematics", by maintaining that "the basic concepts of his 'new algebra' parallel those employed in his art

of decryption[7]." This is the thesis I would like to discuss here and partially question.

1

Pesic begins[8] by mentioning the "disclosure of secrets" as being "a central theme in the development of modern science" and contrasting Aristotle's rational optimism, according to which "nature is fundamentally open to common human understanding", and esoteric mysticism, according to which only few elects, who have been initiated to it, have access—and yet, a very partial access—to these secrets. Provided that Viète's decryption of coded messages is understood as a disclosure of secrets, his attitude with respect to these secrets was certainly closer to Aristotle's rational optimism than to cabalistic, or Hermetic habits, and it contrasts under this respect with the attitude of other codebreakers, as Blaise de Vigenère[9]: in the memoir addressed to the duke of Sully, he lists some relevant features of Spanish and Italian ciphers, then proposes some tricks to be used to decrypt the first ones by exploiting the clumsiness of their authors (which, though utilising "subtle" ciphers, used them often in a "crude" way[10]), and finally suggests a "general method

for success" in their complete decryption and an "infallible rule" to be applied when "the ciphers are simple", that "can be [also] extended to double ciphers"[11].

To illustrate Aristotle's attitude, Pesic refers to *Physics* I.1[12]. Let me also start with this fundamental text. Here is an excerpt of it in R. P. Hardie's and R. K. Gaye's translation, with some local modifications added in brackets, that, according to my suggestion, should replace the parts included between backslashes[13]:

> [...] we do not think that we know a thing until we are acquainted with its primary causes or first principles, \and have carried our analysis as far as its elements\ [and have arrived at the elements].
>
> [...] The natural way of doing this is to start from the things which are more knowable and clear to us and proceed towards those which are clearer and more knowable by nature; for the same things are not knowable relatively to us and knowable without qualification.
>
> [...] what is to us \plain\ [manifest] and clear at first \is rather confused masses\ [is rather what is more confused, or the whole], \the elements and principles of which\ [and from it the ele-

> ments and principles] become known to us later by \analysis\ [division]. Thus we must advance from \universals\ [general] to \particulars\ [particular]; for [...] \a universal\ [the general] is a kind of whole, comprehending many things within it, like parts.

Only two of the corrections I have proposed are relevant. I refer to the replacement of the phrase "and have carried our analysis as far as its elements" with the phrase "and have arrived at the elements", and of the term "analysis" with the term "division". The first correction is motivated by the fact that in Aristotle's text ["*καὶ μέχρι τῶν στοιχείων*"] there is no term that one can reasonably translate with "analysis", while the second is motivated by the fact that Aristotle's term is not "*ἀνάλῠσις*", but "*διαίρεσις*", a Platonic term that one could also translate in different contexts with "dialectic". Yet, the translation of "*διαίρεσις*" with "analysis" is far from being a mistake. It is rather quite a usual habit which depends on a very old tradition.

I have discussed this issue elsewhere[14]. Here, I confine myself to observe that such a translation aims to emphasise the Aristotelian root of two sharply different, though connected, notions that nowadays are usually designated with the same term, that is, "analysis". I'll argue that Viète's method for

decrypting coded messages is concerned with analysis in one of these senses, while Viète's algebra is concerned with analysis in the other one: Viète's method for decrypting coded messages is concerned with analysis as long as this term translates "*διαίρεσις*" in *Physics* I.1, whereas Viète's algebra is concerned with analysis as long as this term translates "*ἀνάλῠσις*" in other parts of the Aristotelian and more generally the Greek corpus, specially the Greek mathematical corpus[15]. Hence, my first task consists in making clear the distinction between the meaning of the terms "*ἀνάλῠσις*" and "*διαίρεσις*".

2

I begin with the term "*ἀνάλῠσις*".

A comparison of the relevant passages from Aristotle's corpus[16] suggests that he understood analysis as the typical pattern of an argument or, more generally, as a piece of reasoning which[17]:

i) starts from the (hypothetical) assumption that something that is not actually given or established—and whose obtainment or establishment is aimed—is rather given or established;

ii) leads to the obtainment or establishment of something that is actually given or established, through an argumentative procedure;

iii) because of that, suggests a way for actually obtaining or establishing what was aimed to be obtained or established.

Thus, an analysis, in the sense of "*ἀνάλυσις*", occurs, according to Aristotle, when an aim has been fixed, but it is not able, as such, to lead to the attainment of this aim. It rather appeals to a second and conclusive argument or procedure that is suggested by it.

It is quite natural for us to term "synthesis" this second argument. But, as a matter of fact, it is far from clear whether the corresponding Greek term—that is, "*σύνθεσις*"—was used at the time of Aristotle to designate in general the argument or procedure suggested by an analysis (in the sense of "*ἀνάλυσις*"), following it, and finally leading to the attainment of the aim. The available evidence seems to indicate only that this term was used, particularly by Aristotle, Apollonius and Archimedes[18], to designate the procedure following a geometric analysis and leading to the construction of a certain geometric object and thus to the solution of a given problem. This is quite natural, since a geometric construction in the Euclidean sense merely consists in putting together (as the term "*σύνθεσις*" suggests, as long as it derives

from the prefix "$\sigma\acute{\upsilon}\nu$" and the verb "$\tau\acute{\iota}\theta\eta\mu\iota$") some objects which are either given or constructed step by step according to some fixed clauses, the principals of which are established by the first three postulates of the first book of the *Elements*.

I shall come back later onto geometric analysis applied to the solution of problems, that is, geometric problematic analysis, as Pappus will term it. To better understand Aristotle's general notion of $\grave{\alpha}\nu\acute{\alpha}\lambda\breve{\upsilon}\sigma\iota\varsigma$, let me consider firstly the example of "deliberation [$\beta o\acute{\upsilon}\lambda\varepsilon\upsilon\sigma\iota\varsigma$]", that is, Aristotle's argument of *Nicomachean Ethics*, III, 3-5[19].

A deliberation is not concerned with the determination of an aim, but only with the means that are supposed to be employed to attain an already fixed aim. It is the act of a human subject which has the (practical) power to attain this aim and consists in establishing a chain of simple acts that have to be accomplished in order to do that. Notice that a deliberation is nothing but an intellectual act, it is a piece of reasoning whose conclusion is the establishment of such a chain. It does not have as such the power to change the relevant situation for the attainment of the aim, whereas the simple acts that compose this chain are supposed to operate on such a situation and modify it to attain the aim. Thus, a deliberation is the first stage of a

twofold process whose second stage is essentially different from the first. Its very name suggests that its prototype is the act of a civic council, a "$\beta o \upsilon \lambda \acute{\eta}$", that occurs when the problem arises to pick out a procedure or a strategy for getting a certain result.

Aristotle argues that in order to do it, one should feign or suppose that the aim has already been attained, and come back in thought from the imaginary situation that would then occur until the real or actual situation, through a sequence of intermediary situations every one of which could be made actual starting from the next one, provided that a certain simple act is accomplished. This intellectual exercise establishes a sequence of connected situations—let us say $\{s_0, s_1, s_2, \ldots, s_n\}$—where the last one ($s_n$) is the actual situation, whereas the other ones are imaginary situations, the first one of which (s_0) is the situation which would be actual if the aim had been attained. To attain the aim, one has thus to accomplish the simple acts that are supposed to lead from any situation s_i to the precedent situation s_{i-1} ($i = n, n-1, \ldots, 1$) following an inverse order with respect to the order established in the deliberation. This means to start from the actual situation s_n and then pass through the intermediary situations $s_{n-1}, s_{n-2}, \ldots, s_1$ until one reaches the situation s_0 and thus attains the aim. As Aristotle notices, a deliberation

is thus a sort of analysis, and the accomplishment of this sequence of simple acts is the procedure that follows it and leads to the attainment of the aim. The term he uses in this case is of course "*ἀνάλυσις*". Here is what he writes, quoted in Apostle's translation (again with some local modifications added in brackets, that, according to my suggestion, should replace the parts included between backslashes)[20]:

> For the man who deliberates resembles the man who \inquires\ [researches] and analyses, in the way stated, as in the case of a geometric diagram. It appears, however, that not all \inquiry\ [research] is a process of deliberation, e.g., mathematical inquiry is not a process of deliberation; but every process of deliberation is \inquiry\ [research], and the last step in the analysis is the first step \in the coming to be of an end\ [in generation].

This example should make clear that for Aristotle an analysis, in the sense of "*ἀνάλυσις*", starts with something that is not actual and ends with something that is actual, instead. I use here the adjective "actual" in a very general sense. The specific sense that has to be attributed to such an adjective depends on the particular sort of analysis that is considered. In the case of deliberation, "actual" means "real" or "present", whereas "non

actual" means "imaginary": the starting point of analysis is an imaginary situation and its final point is the real situation, the present situation in which the subject of the analysis is. When geometric analysis is considered, this sense changes slightly.

The previous quotation shows that geometric analysis is for Aristotle the prototype of analysis. Unfortunately, we do not have at our disposal a general characterisation of it due to Aristotle or to someone of his contemporaries. Apart from a paraphrase by al-Nayrïzï of a definition contained in Heron's commentary of book II of the *Elements* and a definition presented in an interpolation at the book XIII of the same *Elements*, probably due to the same Heron[21], the first general characterisation we know is due to Pappus which exposes it in the very beginning of the book VII of his *Mathematical Collection*[22].

According to Pappus, geometric analysis is the first stage of the method of analysis and synthesis[23]. This method would have been applied by Greek mathematicians both to prove their theorems and to solve their problems, though they would have hidden the analytic part of their arguments: they would have reasoned by analysis in order to conceive another argument able to prove a theorem or to solve a problem; in the first case the analysis is said

"theorematic", in the second it is said "problematic". Some historians have denied the legitimacy of Pappus' application of the notion of analysis to the proof of theorems[24], or argued that Pappus was in fact "not concerned with synthesis", but rather with "the field of analysis and its role in mathematics[25]." I will not enter these questions here and confine myself to Pappus' problematic analysis, since this is the only one which is relevant for Viète.

Both in classical and in early modern mathematics, to solve a geometric problem meant to construct a geometric object which satisfied a certain condition that the terms of the problem established. Such a construction started with some objects that were taken as given and applied a number of fixed clauses. In Pappus's version, when concerned with the solution of a geometric problem, the method of analysis and synthesis included the following stages[26]:

i) the sought-for object was supposed to be given—that is, it was supposed to have been already constructed—and it was represented by means of a diagram where the objects that were actually given were also represented;

ii) by reasoning on this diagram—and eventually by extending it through auxiliary constructions (without replacing it with another one)—a sub-

diagram was isolated, where the object that was sought for was shown to be related to some of the given objects by a certain constructive relation;

iii) the objects entering such a sub-diagram were actually constructed step by step according to the constructive clauses, starting from those which were given and ending with that which was sought for.

Stages (*i*) and (*ii*) belong to the analysis; stage (*iii*) constitutes the synthesis.

It should then be clear that in the case of Pappusian problematic geometric analysis, the adjective "actual" has to be taken as meaning "given" or "already constructed", whereas "non actual" means "non actually constructed": the starting point of a Pappusian problematic geometric analysis is an object that is not given (an object that has not been constructed, yet), which is taken as it were given or constructed, whereas its final point is a certain configuration where this objects is shown to be constructively connected with some objects that are given or already constructed.

Once the adjective "actual" is understood in this way, it becomes very natural to wonder: for whom is the starting point of analysis not actual? and for whom is its final point actual? In case of Pappusian problematic geometric analysis this means to wonder: for whom is the starting point of analysis not

given? and for whom is its final point given? The answer seems to me very clear: an analysis, in the sense of "*ἀνάλυσις*", starts from something that is not actual for—or, more specifically, in the case of a Pappusian problematic geometric analysis, with something that is not given to—the human subjects that are the actors of the analysis itself; and it leads to something that is actual for—or given to—these same actors. An analysis in this sense, is thus a top-down argument from the point of view of the human subjects that are producing this very argument.

* * *

At this point the difference between an analysis, in the sense of "*ἀνάλυσις*", and an analysis, in the sense of "*διαίρεσις* ", should be quite clear.

The previous quotation from *Physics* I.1 contains the prototypical characterisation of analysis in the second sense and it makes evident that this is an argument or a piece of reasoning that goes "from the things which are more knowable and clear to us [...] towards those which are clearer and more knowable by nature". As it is also clearly explained in such a quotation, the former are the empirical diversity of the natural word as it appears at a first

and quite naive human view, whereas the latter are the elements we can discern in such a diversity at the end of an intellectual process that is just the analysis itself. Though it makes certainly sense to say that these elements are the first ones, they are so according to something as the natural order that is unveiled only at the end of the analysis. With respect to the process of our—that is, human—knowledge, these elements are rather the last ones.

Thus, the starting point of an analysis, in the sense of "$\delta\iota\alpha\acute{\iota}\rho\varepsilon\sigma\iota\varsigma$", is something that is actual for the human subjects that are the actors of the analysis itself, that is, something that is immediately given to them, whereas its final point is something that, when the analysis starts, is not actual for them, is not given to them yet. An analysis in this sense is thus a bottom-up argument from the point of view of the human subject that is producing this very argument. To maintain that it could also be understood as a top-down argument, since it goes from the last to the first, one should consider the first and the last from the point of view of the intrinsic organisation of nature, or, if you prefer, from God's point of view. And there is no reason to maintain that an analysis in this sense starts from something that is not given or not actual.

With respect to their logical order, an analysis in the sense of "$\grave{\alpha}\nu\acute{\alpha}\lambda\breve{\upsilon}\sigma\iota\varsigma$"

and an analysis in the sense of "$\delta\iota\alpha\acute{\iota}\rho\varepsilon\sigma\iota\varsigma$" are thus two quite opposite pieces of reasoning: the order of the latter is the opposite than the order of the former. To identify these two forms of reasoning or to consider that they are equivalent, means thus, among other things, to conflate the points of view with respect to which their logical order is deemed, to conflate the epistemological with the ontological points of view. Hence, the difference between $\grave{\alpha}\nu\acute{\alpha}\lambda\breve{\upsilon}\sigma\iota\varsigma$ and $\delta\iota\alpha\acute{\iota}\rho\varepsilon\sigma\iota\varsigma$ is radical.

* * *

One could then wonder how happened that the same term—that is, "analysis" or its equivalents in other vernacular languages—were used later to translate both "$\grave{\alpha}\nu\acute{\alpha}\lambda\breve{\upsilon}\sigma\iota\varsigma$" and "$\delta\iota\alpha\acute{\iota}\rho\varepsilon\sigma\iota\varsigma$". This is a very interesting issue that would deserve a deep study. But I cannot consider it here. I confine myself to guess that, passing through the Latin translation "*resolutio*" and in concomitance with the "Platonisation" or "Neo-platonisation" of Aristotle's system, the term "$\grave{\alpha}\nu\acute{\alpha}\lambda\breve{\upsilon}\sigma\iota\varsigma$" acquired in the middle age a new sense, namely an ontological sense, according to which the concept of being given—which was surreptitiously replaced by the concept of being given firstly—was understood from the point of view of the intrinsic order of nature, or the point

of view of God.

What in any case is important here is that this new sense did not replace the old one. It was merely added to it. And in mathematical language and contexts, the old sense was preserved. Hence, when in early modern mathematical texts the Latin or vernacular versions of the term "$\grave{\alpha}\nu\acute{\alpha}\lambda\breve{\upsilon}\sigma\iota\varsigma$"[27] occurred, the reference was not Aristotle's notion of $\delta\iota\alpha\acute{\iota}\rho\varepsilon\sigma\iota\varsigma$, but his notion of $\grave{\alpha}\nu\acute{\alpha}\lambda\breve{\upsilon}\sigma\iota\varsigma$, or better Pappus' notion of geometric analysis. This is not of course the same as arguing that this notions were preserved as unchanged. We shall see on the contrary that Viète's conception significantly differed from Pappus' and that this difference does not only depend on the fact that for Viète the method of analysis and synthesis was not only a geometric method—being rather a method that could be applied to the solution of problems relying on geometric quantities as well as on numbers—but also to other reasons. Nevertheless, these changes did not concern the aspects of Aristotle's notion of $\grave{\alpha}\nu\acute{\alpha}\lambda\breve{\upsilon}\sigma\iota\varsigma$ that makes it radically differs from his notion of $\delta\iota\alpha\acute{\iota}\rho\varepsilon\sigma\iota\varsigma$[28].

3

We can now go back to Pesic's thesis. It concerns a "parallel" between Viète's "art of decryption" and his "new algebra".

The first difficulty with this thesis pertains to the exact identification of the matter that is supposed to be designed by the term "new algebra". This term enters the title of a collection of treatises constituting the most part of Viète's mathematical *œuvre* and forming a coherent mathematical system: *Opus restitutæ mathematicæ analyseos, seu Algebrâ novâ.* Such a title appears in the *title-page* of a very short pamphlet containing the introduction to such a collection—the famous and already mentioned *In artem analyticem isagoge*—published in 1591[29], together with the list of the treatises that were supposed to form this collection and that were published successively, partially during Viète's life-time and partially after his death. Quite ironically, neither the term "new algebra", nor the simple term "algebra" enter these treatises in any significant way, however. Hence—though, starting from the third decade of 17$^{\text{th}}$ century, it became very common to speak about Viète's algebra[30]—the exact meaning of this term remains unclear.

The most natural candidates for being the referent of this term are Viète's analysis—that is, the first stage of Viète's version of the method of analysis

and synthesis—and Viète's *logistica speciosa*. Though often conflated, these are two essentially different things: in modern terms, we could say that the latter is the symbolic formalism that is supposed to be used in the former. If I understand well Pesic's thesis, it refers more to the latter than to the former, since it insists on the fact that "the cipher stands for the plain text" as "the algebraic symbol stands for its implicit value[31]." However, the nature of Viète's formalism strongly depends on the features of his analysis. To evaluate this thesis, is thus necessary to make clear what Viète's analysis is.

Here is how Viète describes his method of analysis and synthesis in the begging of the *Isagoge*, in J. W. Smith's English translation[32]:

> In mathematics there is a certain way of seeking the truth [...] which was called "analysis" [...] and was defined [...] as [...] "taking the thing sought as granted and proceeding by means of what follows to a truth that is uncontested"; so, on the other hand, "synthesis" is "taking the thing that is granted and proceeding by means of what follows to the conclusion and comprehension of the thing sought." And although the ancients set forth a twofold analysis [...], it is nevertheless fitting that there be established also a third kind [...], so that there is a zetetic

> art by which is found the equation or proportion between the magnitude that is being sought and those that are given, a poristic art by which from the equation or proportion the truth of the theorem set up is investigated, and an exegetic art by which from the equation set up or the proportion there is produced the magnitude itself which is being sought.

Viète's distinction between zetetic, poristic and exegetic has been understood in different ways. My opinion is that—despite the letter of Viète's text, but accordingly to his mathematical practice—we should consider them as three sequential stages of the method of analysis and synthesis. On this view:

- Zetetic would consist in expressing any given problem by means of one or more equations or proportions, and in solving or transforming them, that is, in transforming the configuration of given and sought-for quantities corresponding to the statement of the problem in a new configuration that is supposed to be equivalent to the first one, but also to be such that, starting from it, the determination or construction of the sought-for quantities is easier;

- Poristic consists in proving that the new configuration obtained by

means of zetetic is actually equivalent to the original one;

- Exegetic consists in the determination or construction of the sought-for quantities.

Zetetic and exegetic would thus constitute analysis and synthesis, respectively, whereas poristic is a sort of confirmation of analysis.

Let us concentrate on zetetic. Suppose that a problem is advanced. Viète proposes:

- To assume that the sought-for quantities were already given and to indicate them with certain alphabetic letters, namely capital vowels;

- To indicate the given quantities by other alphabetic letters, namely capital consonants, and to express the conditions of the problem by means of a system of equations or proportions;

- To operate on these equations or proportions by means of an established formalism—that is just the *logistica speciosa*—in order to transform them in a system of equalities or new proportions which directly suggests the procedure to be followed in order to determine the sought-for quantities.

Let's take a simple example, namely a particular case of the problem II.1 of Viète's *Zeteticorum libri*[33]: to construct two segments whose ratio is equal to the ratio between two other given segments and such that the rectangle constructed on them is equal to a given square. Let us call the sought-for segments "A" and "E", the given segments "B" and "C" and the side of the the given square "D". The conditions of the problem may thus be expressed by the proportions:

$$A : E = B : C \qquad ; \qquad A : D = D : E \tag{1}$$

According to the formalism of the *logistica speciosa*, from them it follows

$$A = \frac{EB}{C} = \frac{D^2}{E} \quad ; \quad \frac{D^2}{E}C = EB \quad ; \quad \frac{D^2C}{B} = E^2 \tag{2}$$

and thus:

$$E = D\sqrt{\frac{C}{B}} \qquad \text{or} \qquad B : C = D^2 : E^2 \tag{3}$$

$$A = D\sqrt{\frac{B}{C}} \qquad \text{or} \qquad C : B = D^2 = A^2 \tag{4}$$

This is the conclusion of zetetic[34], but it is not the solution of the problem, yet. To solve it, one has still to construct the sought-for segments A and E starting from the given ones, B, C and D. This is the aim of exegetic. But to do that, exegetic can follow the suggestions, or better the instructions

provided by zetetic and expressed in the equations or proportions (3) and (4).

Thus, as in Aristotle's conception, analysis operates on something that is not actual—namely on quantities that are not given, but sought-for, the unknown segments A and E—and does not solve the problem, limiting itself to suggest the solution. Nevertheless, Viète's analysis is, for other reasons, very different from Pappus'.

The most important difference concerns the kind of problems it applies to. These problems are, as it were, purely quantitative. They do not rely on the respective positions of a number of geometric objects, but only on the relations that certain objects have as long as they are quantities, that is, on their purely quantitative relations. Consider the proposition I.1 of Euclide's *Elements*. It asks for the construction of an equilateral rectangle on a given segment. Its solution depends on the determination of the position that a certain point must take with respect to the position of the given segment. Viète's method cannot solve a similar problem, since no equality or proportion can be used to express the construction that has to be realised to fix such a position. The solution of the previous particular case of the problem II.1 of Viète's *Zeteticorum libri* depends instead only on the determination of

two segments that, though supposed to be able to form a rectangle satisfying a certain condition, can be constructed as such in any position of the plane where the given segments lay. This is because, once one knows that two rectangles $R(a, b)$ and $R(\alpha, \beta)$ are equal if and only if their sides a, b, α, and β satisfy the proportion $a : \alpha = \beta : b$, the problem of establishing two segments such that the rectangle constructed on them is equal to a given square reduces to the problem of establishing two segments that satisfy a certain proportion.

This makes it possible to express the conditions of the problem by means of a number of formulas belonging to a certain codified language, where both the given and the sought-for objects are, in turn, expressed by means of suitable proper names, constituted by suitable alphabetic letters. By contrast, in Pappus's method of analysis and synthesis, the conditions of the problem are rather represented by a certain diagram. While Pappusian analysis consists in reasoning on such a diagram, eventually extending it by means of auxiliary constructions, Viète's analysis consists in transforming these formulas in other formulas of the same language according to a certain fixed formalism.

The diagram works in Pappus's analysis as a fixed configuration, while the systems of equations or proportions works in Viète's analysis as a chang-

ing configuration: Pappus' analysis is intra-configurational; Viète's is trans-configurational. The former relies on the constructive clauses of Euclide's geometry, whereas the latter relies on a suitable formalism[35] formed by a language, consisting both of symbols for (known and unknown) quantities and of symbols for operational relations between these quantities, plus a number of rules of transformations of the formulas written in this language. The establishment of such a formalism is the main aim of Viète's *Isagoge*.

This very formalism is responsible of another difference between Pappus' and Viète's methods. To simplify the matter, I have just considered a particular case of a problem of Viète's: I have supposed that both the given and the sought-for quantities were segments, and thus that the particular nature of these quantities was known. In Pappusian analysis, a similar supposition is essential: how can one represent a quantity whose particular nature is not known by means of a diagram? But in Viète's analysis this is not needed. And in fact Viète's original problem asks rather for the determination of two quantities of any sort whose product and ratio are both given. Nevertheless, it is easy to understand that the analysis of this general problem goes exactly like the analysis of the previous particular problem, since it consists of nothing but the stages (1)-(4). This is possible because the formalism that is used

in Viète's analysis is not defined on specific kinds of quantities, but rather on quantities taken in general. Such a definition depends on an axiomatic characterisation of the operational relations between these quantities that is advanced in chapter II of the *Isagoge*.

This is, I think, the most valuable innovation of Viète's mathematics.

What is more important here, however, is not to insist on this novelty, but to observe that, while in Viète's analysis there is no need to know the particular nature of the quantities we are working on, in Viète's exegetic or synthesis (as well as in his poristic) this is required indeed. If it were not known, the quantities A and E could not be constructed according to the indications contained in the formulas (3) and (4). The reason is clear: though the operational relations that subsist separately between numbers, segments, polygons, solids, angles, times, or any other sort of quantities have the same mutual properties, these different sorts of quantities do not add, subtract, multiply, or divide each other in the same way. To take only an example: to add two integer numbers means to count, starting from the first one, as many units as those which are contained in the second one; to add two segments means to juxtapose them by means of a geometric construction. Thus, in order to solve a problem with Viète's method of analysis and synthesis one

needs to know which sort of quantities this problem is concerned with. This essential information is nevertheless hidden in Viète's analysis. If, on the one hand, this is the force of it, on the other, it is its essential weakness.

4

It is the time now to consider the second horn of Pesic's parallel.

As Pesic notices[36], the term "cryptanalysis" does not come from Viète, being rather introduced in 20th-century. Thus, the fact that it is composed by "analysis" is not a reason to expect that this parallel subsists (and Pesic does not rely on it, indeed), since it would be far from unlikely that "analysis" is used with two quite different meanings when it occurs in this term and when it refers to the first stage of Viète's method of analysis and synthesis.

The aim of Viète's cryptanalysis is actually the disclosure of secrets. Nevertheless a distinction is required. Modern age, as well as Renaissance, were concerned at least with three different sorts of secrets: those that were hidden in the Book of Nature; those that were hidden in the Book of (the Holy) Scriptures; those that were hidden in coded messages. Of course, there are analogies among these cases. Yet, we could say that modern science and

modern cryptanalysis were born when a distinction was made respectively between the first case and the second, and between this case and the third. I do not want to suggest that the interpretation of the Book of Scriptures was stranger to modern science. The example of Newton is only one among many others that could be mentioned to deny it: not only he was convinced that the reading and interpretation of the Holy Scriptures was an essential task; he also believed that both this reading and the study of Hermetic tradition could give important information about the hidden content of the Book of Nature[37]. Yet, taken as such, the Book of Nature and the Book of Scriptures should not be read in the same way. And this is so because, among other reasons, they were written in different languages. And the language of coded messages too was different.

Although it seems that this last difference was not commonly grasped at Viète's time, it certainly was by him, who clearly conceived a cipher as a human convention. Here is what he writes in the memoir addressed to the duke of Sully[38]:

> The Spaniard is quite subtle in the composition of his ciphers but crude in using them. The Italian is very subtle in his composition and very subtle in his usage. Once the composition [of

> these ciphers] has been understood in one instance, solution is not difficult.

But to conceive secret ciphers as human conventions is not as such a good reason to be optimistic about the possibility of breaking them, and even less about the possibility of a general method to break them. Yet, human conventions follow a human logic that has to be transmitted (for, otherwise, no coded message could be deciphered by its addressees), and this logic should always be reconstructible with human capacities: this seems to be the reason of Viète's optimism in codebreaking. Though he speaks, as I have previously noticed, of a "general method for success" and of an "infallible rule", the procedures he proposes to follow in order to break Spanish and Italian codes intimately depends both on the particular nature of these codes and on the way in which they were used.

The codes that Viète had to break consisted in transformations by substitution. In the simplest version, this kind of codes relied on the substitution of numerals (written in the Arabic habitual decimal notation), or some other stable character, for the letters of the alphabet in which the original message was written. Of course, when a single character is associated to a single letter according to an injective application from letters to characters the decryp-

tion is relatively easy. Thus, both Spaniards and Italians had complicated their codes in different ways that are described in both memoirs considered by Pesic. Any letter was for example associated to different characters to be used indifferently in place of this letter, mute characters were introduced, sometimes a character was used to replace a syllable or a group of letters rather than a single letter (so that the same word could be coded in different ways), and moreover a number of frequent words or proper names were associated to elementary characters or fixed composition of them.

Viète does not say how he succeed in discovering that Spanish and Italian codes were composed according to the general standards he describes. This was a common habit at his times and probably he simply begun his work as a codebreaker in supposing that it was so, being then confirmed in this by his own success. What it is sure in any case, is that the procedures he proposes do not apply to any sort of codes, being rather appropriate just for such a sort of codes and even for the particular way they were used.

The first three suggestions that Viète makes to break Spaniard's codes just depend on their "crude" use of them[39].

He firstly observes that when Spanish ambassadors wrote to their king, they sent the same letter several times, coded in different ways, according to

the same cipher. This made sometimes possible to compare different coded messages corresponding to the same original text, and, Viète adds, this shed "a great light on the abbreviations and the form of disguises of the same word and the diversity of figures for the expression of the same term or syllable[40]."

Then Viète suggests to pay attention to what he calls "*chiffre essentiel*"[41]. They are numerals that, because of the value of the corresponding numbers, were probably used not as characters for letters, syllables or words, but just as usual numerals. Thus it was probable that numerals such as "4000", "500" or "100.000" were used to denote the corresponding numbers, and were thus probably followed in the original message by words like "infantrymen", "horses" or "ducats", respectively.

Finally, Viète remarks that the position of certain characters within a coded message can reveal the possible words they stand for. For example, a copy of an already sent message cannot but begin with the words "copy of ...". When this is the case, it is thus easy to associate to certain characters the letters, syllable or words they replace.

Though they are certainly clever, these suggestions can only help in decrypting certain parts of certain coded messages and thus in starting the cryptanalytic work. To complete it, a more extensive method is needed. In

the two memoirs considered by Pesic, this method is not clearly described. As I have already noticed[42], the part of the first memoir concerned with Spanish ciphers closes with the exposition of a "general method for success", while the part of this same memoir concerned with Italian ciphers consists for its main part of the presentation of a "infallible rule" to be used "when the ciphers are simple" but also extendible to "double" or more generally "composite" ciphers. However, these are both quite obscure, and the same is the case for the description of Viète's "rules for deciphering all sorts of ciphers" contained in the second memoir[43].

What is clear is that these methods or rules relied on looking for the frequency of characters though not reduced to the quite obvious procedure consisting in comparing the frequency of single elementary characters with that of single letters in a text written in Spanish (that, because of the complex nature of Spaniard's codes, would have been quite useless).

When in the coded message word divisions were made clear, the idea was that of considering the characters used to represent the final and initial letters of any word, or those that formed pairs of equal characters repeated one after the other (as it is the case for the double letters both in Spanish and Italian), in order to identify characters for vowels and characters for

consonants[44].

But, when word divisions were occulted, a similar procedure was not available and the identification of characters for vowels and characters for consonants called for a different technique. This certainly relied on the consideration and comparisons of dyads and triads of successive characters that were supposed (thanks to a previous frequency tally)[45] to represent a single letter, together with the remark that both in Spanish and Italian the most frequent dyads and triads of sequential letters contain at least a vowel. Based on Pesic's interpretation of Viète's method[46], Delahaye has proposed that this method worked as follows.

Starting from the beginning of a sequence of characters that are supposed to represent a single letter, one lists successively the triads of characters composing this sequence that do not contain any character occurring in the triads already listed. In Delahaye's example, the coded message (where any letter is represented by one and only one other letter and the original message is written in French) begins as follows:

$$tyenlpyenlqwqyfyklmlqtyhgmjwnkkyj.$$

This sequence contains 33 characters and 31 triads, that is:

$$tye \quad ; \quad yen \quad ; \quad enl \quad ; \ldots ; \quad kky \quad ; \quad kyj,$$

but among them, only the four triads

$$tye \quad ; \quad nlp \quad ; \quad qwq \quad ; \quad hgm$$

do not contain any character occurring in the preceding ones, since both *yen* and *enl* contain *y* or *e* that are already contained in *tye*, while *lpy*, *pye*, *yen*, *enl*, *nlq*, *lqw* contain *l*, *p*, *y*, *e*, *n*, that are already contained in *tye* and *nlp*, and so on. If one continues to consider the remaining part of Delahaye's coded message, one does not find any new triad of characters satisfying the same condition. Thus, these four triads are all the triads that have to be listed according to the method.

Then one lists the different characters contained in these triads and guesses that among these characters there are those that represent the five vowels *a*, *e*, *i*, *o*, *u*. In this case, these characters are 11: *t*, *y*, *e*, *n*, *l*, *p*, *q*, *w*, *h*, *g* and *m*.

Finally, one considers any triad of characters in the coded message that contains only one among the characters that are selected in this way. The obvious conclusion is that this character represents a vowel. This is, for

example, the case of the triad fyk, so that the character y should represent a vowel. The same procedure leads to identify the other characters representing a vowel.

Pesic adds that when the original message is supposed to be written in Spanish or Italian, a similar argument can be also applied to dyads of characters, so that the triads and the dyads selected in this way could be compared.

5

Finally, let's turn to Pesic's arguments in favour of the parallel between Viète's cryptanalysis and Viète's algebra.

There is of course a general analogy between the procedures that Viète suggests must be followed in decrypting coded messages and those that enter the first stage of his method of analysis and synthesis. As Pesic argues, both are formal procedures that result from systematic techniques concerned with the manipulation of elementary symbols combined according to given rules[47]. Moreover, though in both procedures these symbols are considered expressions or representations of something else (that is, letters, groups of

letters or words in the case of cryptanalysis, and quantities or operations with them in the case of algebraic formalism), they are *prima facie* treated as elements of certain systems of relations or even as pieces of a formal game[48]. But there is also an evident difference between these procedures. The former consists of remarking certain internal features of the system of symbols that is given, by studying the mutual positions, the distributions, the frequencies of elementary symbols or of appropriate combinations of them with the aim of disclosing a structure that this system would share with a text written in a certain natural language. The latter consists in transforming symbolic formulae (that is, certain well formed sequences of elementary symbols) in other symbolic formulae with the aim of obtaining formulae that could be understood as a prescription for certain other procedures (normally geometric constructions or numerical calculations). In the first case, the elementary symbols are characters forming the words of an unknown language, and the problem consists in identifying these words and establishing their meaning. In the second case, these symbols are terms having an already fixed meaning and entering a formal deduction that has to be performed according to a certain aim.

However, it is not simply because of the existence of this difference that

I question Pesic's thesis. After all, this thesis is about parallelism and not perfect equivalence. I rather argue that the analogy I have just admitted depends on similarities that, when compared with the difference between the intrinsic logical natures of the two procedures, appear to be quite general and extrinsic, and thus, in a sense, only superficial. Besides, I think that the other similarities that Pesic points out do not actually subsist.

I shall come back later to what I hold to be the essential difference between Viète's algebra and his cryptanalysis. Let us firstly consider these other supposed similarities.

To stress one of them, Pesic[49] insists on the fact that in his activity as a cryptanalyst, Viète "rested on the application of general procedures and rules rather than haphazard search for probable words or mere trial and error", being "more interested in the 'infallible rule' on which he can rely when inspired guesswork fails", than in looking for ingenious gambles. Then he remarks that the same is true for his "algebraic work", whose ambition is the famous one that is proclaimed at the end of the *Isagoge*: to solve the "problem of problems, that is: to leave no problem unsolved."

If there is an apparent analogy here, it is because of Viète's rhetoric over-estimation of the power of his owns techniques. As his "general method for

success" and his "infallible rule" for cryptanalysis are far from being actually general and infallible[50], being applicable only to certain sorts of coded messages that they may enable to decrypt with the help of appropriate conjectures[51] and by trial and error[52] only, his method of analysis and synthesis too only applies to purely quantitative problems and is far from guaranteeing that any problem of this sort will be actually solved.

Another of Pesic's arguments relies on Viète's use of the French term "*chiffre essentiel*"[53]. By using this term, Viète would "direct[...] our attention to the double meaning of *chiffres*, which refers both to ordinary numbers and to ciphers" and would make clear that for him a "letter sign or species is in essence a cipher, joining 'the general character of being a number'[54] with the particular numbers that satisfy the given stipulations." Thus, for Viète "an equation [would be][...] like enciphered text" and then "algebraic solution [would be][...] analogous to solving a cipher[55]." This argument is flawed, however. First of all, the French term "chiffres", just as well as all the corresponding terms in other languages, does not refer, and did never refer, to numbers, but to (elementary) symbols for numbers. Secondly, as long as it is a symbol and the term "cipher" is correctly understood, one can certainly maintain that in Viète's algebraic formalism a letter sign is a

cipher, but this does not depend on the fact that it stands for a number. This is simply because it does not stand for a number but for a quantity of any sort, as I have previously made clear[56]. Thirdly, when one argues that, in this sense, an equation is like an enciphered text, one simply maintains that it is a symbolic formula. Thus, there is no room to argue from here that an algebraic solution is analogous to a solution of a cipher (or coded message).

The last argument[57] goes as follows[58]:

> The stance of the cryptanalyst toward an unknown cipher is exactly the analytical attitude of the problem solver, rather than the ancient mathematical attitude of the contemplative geometer that is expressed in the synthetic proof of theorems. The aggressive analysis that Viète directed at his ciphers parallels his desire to "leave no problem unsolved" in algebra. He was doubtless encouraged in this ambition by his express belief that the ancients had intentionally concealed in their synthetic mathematics a hidden analytical art that he understood himself to be reviving. Thus he held that the ancient mathematical writers wrote in a kind of code that concealed under its synthetic exterior an esoteric, analytic art. Viète solves these ancient texts [...].

Apart from the fact that ancient mathematicians were perfectly able both of a "contemplative" attitude in proving their theorems and of a seeking attitude in solving their problems, there are two major confusions here.

The most evident one concerns the logical nature of the argument. Though one admitted that, by concealing the analytic part of their method, "the ancient mathematical writers wrote in a kind of code" that Viète would have decrypted by showing what they were hiding, or, better, in reviving their "analytic art", it would not follow that this same art is analogous to the art of decrypting coded texts. To pretend that it is so would be pretending that any message that has been decrypted starting from its coded form is in itself an exposition of a cryptanalytic technique.

The second confusion concerns my main point, that is, the difference between Viète's algebra and his cryptanalysis that I consider to be essential: in this quotation the term "analysis" occurs with two quite different meanings. Viète certainly directed at his ciphers an "aggressive analysis". But this analysis was not one in the sense of "*ἀνάλῠσις*", being rather one in the sense of "*διαίρεσις*". Hence, it was essentially different from the analysis which the first part of his method of analysis and synthesis consists of. And this difference is responsible, I think, of a deep—that is, structural or

logical—difference between his cryptanalysis and his algebra: while the latter is a technique, or a formalism, used in performing an analysis in the sense of "*ἀνάλῠσις*", the former was a form of analysis in the sense of "*διαίρεσις*".

To substantiate this thesis, I have presently only to justify the interpretation of Viète's cryptanalysis as a form of analysis in the sense of "*διαίρεσις*". This is my final task.

As long as Viète's cryptanalysis was part of his job as *déchiffreur du roi* it was concerned with discovering what the characters composing the coded messages stood for. It was starting from a given system of characters and was looking for the hidden logic of the internal organisation of this system. If these characters were combined as they were, it was because of the fact that they denoted certain letters, groups of letters and words and that these letters, groups of letters and words were used to compose a message in a certain natural language. Thus, to unveil the logic of the internal organisation of the system was the same as decrypting the coded message. But, in Aristotle's terms, to unveil the logic of the internal organisation of a system is also the same as starting "from the things which are more knowable and clear to us and proceed towards those which are clearer and more knowable by nature[59]". And when the system is a coded message, that

is, an apparently arbitrary sequence of characters or an apparently confused assemblage of signs, the equivalence is even more vivid, since this is also the form of the empirical diversity of the natural world as it appears at a first and naive human view, while the plain text, once unveiled, shows the elements that are hidden in such a diversity and that have been discerned at the end of an intellectual process.

The decryption of a coded message is thus, in a sense, a prototype of an analysis in the sense of "*διαίρεσις*", since it is a sort of distilled form of the process of acquirement of knowledge—the process the Aristotle wanted to describe in the beginning of the *Physics*, but certainly not in *Nicomachean Ethics*, III.3-5.

The difference between Viète's cryptanalysis and Viète's analysis becomes even more manifest when one notices that in decrypting a coded message according to Viète's suggestions there is absolutely no need to take something that is not actual as if it were so. At the end of a long research, one may surmise that certain characters represent a certain letter, group of letters or word. But this is just a guess, and is thus quite different from the assumption that something that is not actually given or established is rather so, which constitutes the starting point of an analysis in the sense of "*ἀνάλῠσις*"[60].

Besides, before this stage, the characters that form the coded message are treated, as Pesic himself notices, just as symbols having the mutual relations that this message explicitly shows.

Moreover, these symbols denote things whose nature is perfectly known: they denote alphabetic letters or sequences of them. And they do it by composing each other according to rules that are, at the contrary, unknown. Contrariwise, as long as they are used in the first stage of Viète's method of analysis and synthesis, algebraic symbols denote quantities whose nature was not known, but they do it by composing them according to rules that are perfectly known. Also from this point of view the logical nature of Viète's cryptanalysis is thus opposite to the logical nature of Viète's analysis.

* * *

In insisting on this disanalogy I have of course no intention to deny or diminish Viète's scientific merits. The methodological, or even logical unity of an intellectual enterprise is often considered as being a quality in itself. And it is thus searched for, behind apparent differences. I think, on the contrary, that the first quality of a scientist is to be able to distinguish the different methods that need be applied in the different domains of his research, and

to separate these domains from each other. It seems to me that this is the essential methodological feature of modern science.

Acknowledgements. The present paper is drawn from a lecture given at the conference *Communication and Dissimulation in Seventeenth Century Europe* organised by the UCLA Center of 17th and 18th-Century Studies, the *Centro Interdipartimentale di Studi su Descartes e il Seicento* of the Lecce University, and the *Ecole Pratique de Hautes Etudes de Paris*, and hold in Los Angeles, at the Clark Library, on February 6-7, 2004. I thank the organisers of the conference for having invited me and left me free to submit my paper for an independent publication. I also thank Andrew Arana, Jean Robert Armogathe, Giulia Belgioioso, Annalisa Coliva, Massimo Galuzzi, Daniel Garber, Niccolò Guicciardini, Antoni Malet, Sébastien Maronne, Gianni Micheli, Massimiliano Savini, and two anonymous referees for valuable comments on my talk, and previous versions of my paper.

Notes

1. Cf. Pesic (1997a), p. 1. This judgement has been repeated in Delahaye (2003).

2. I have discussed some of these senses in my Panza (fc).

3. Cf. Viete (1591a) and Viete (1591b).

4. Both memoirs are mentioned in Ritters's classic biography: cf. Ritter (1895), pp. 257-258.

5. Two transcriptions of these memoirs by F. Ritter are included in a large manuscript intellectual biography of Viète, composed by Ritter himself and forming four manuscript volumes conserved at the *Bibliothèque de l'Institut de France* [Ms. 2009-2012 respectively : *François Viète, inventeur de l'Algèbre moderne. Sa vie. Son temps. Son Œuvre* ; the transcriptions of the two memoirs I refer to occurs in Ms. 2009, ff. 187-194 and 185-187, respectively ; other five volumes—namely Ms 2004-2008—contain a French translation of Viète's mathematical works]. Ritter says there to have Viète's autograph of the first memoirs "*sous les yeux*" but gives no other indication about his sources, that are presently lost. No other copy of the fist

memoirs has been localised up to now, while an older copy of the second is conserved at the *Bibliothèque National de France*, in Paris [cf. Ms Dupuy 661, ff. 219r-220r].

6. Cf. Pesic (1997a), pp. 22-27 and 27-29, respectively. Pesic's paper also contains a large amount of information concerned with the context in which these memoirs were probably written and the transmission of their manuscript copies.

7. Cf. Pesic (1997b), p. 675. Cf also p. 677: "[. . .] my argument points toward parallels between developments in algebra and in decryption rather than unequivocal influences."

8. Cf. Pesic (1997b), p. 674.

9. Cf. Pesic (1997b), 680 and Kahn (1996), 146.

10. Cf. Pesic(1997a), p. 23[V]. I shall quote Viète's passage in full in the section 4: cf. the footnote (38). The letter "V" added between brackets after a page number referred to Pesic's first paper indicates that the quotation refers to his translation of the mentioned memoirs, rather than to his own considerations.

11. Cf. Pesic (1997a), p. 25[V] and 26-27[V], and Ms. 2009, *Bibliothèque de l'Institut de France*, Paris, f. 191 ("Quand il n'y aura lieu a aucune des observations precedentes, le descouvrement sera plus difficile Mais voici la methode generale pour y parvenir") and 193 ("Regle infallible quand les chiffres sont simples [...][qui] se peut estendre aux chiffres doubles").

12. Especially 184a, 12-26.

13. Cf. Aristotele (CWAB), vol I, 315.

14. Cf. Panza (1997).

15. Notice that I'm far from claiming either that Viète's method for decrypting coded messages and Viète's algebra can be seen as mere applications of the (general) procedures that Aristotle designed with the terms "*διαίρεσις*" and "*ἀνάλῠσις*", respectively, or that it is enough to understand Aristotle's related notions to understand Viète's practices. Viète's algebra comes particularly together with a new understanding of the classical notion of *ἀνάλῠσις* and with the introduction of a quite new terminology that was just intended to emphasise it. The novelties involved in Viète's "analytic art" have been described in several occasions. I have tried to account for them in section VII of my Panza(1997) (pp. 402-405), in the introduction of

Panza (2005) (pp. 16-23), and in Panza (fc), and I shall come back briefly on the topic in section 3, below. Still, I maintain that Viète's art includes, as its essential part, a procedure that can be understood as a particular example of ἀνάλῠσις in Aristotelian sense. This is all what I take to be relevant for my present purpose.

16. Cf. *Prior Analytics*, 51*a* 18-19; *Posterior Analytics*, 78*a* 6-8, 84*a* 8, 88*b* 15-20; *Metaphysics* , 1005*b*, 4; and *Nicomachean Ethics,* 1112*b* 20-24.

17. I refer, for a detailed justification of this conclusion, to Panza (1997).

18. Cf. *On Sophistical Refutations*, 175*a* 26-28; *Cutting-off of a Ratio*, prop. II; and *On the Sphere and Cylinder,* props. 1 and 3-7.

19. Especially 1112*b* 20-24, [cf. the previous footnote (16)]. For a reconstruction of Aristotle's argument, cf. Joachim (1951), pp. 101-102.

20. Cf. Aristotle (NEA), p. 41.

21. Cf. Euclid (OOH), vol of supplements, p. 89 and vol. IV, pp. 364, respectively. Cf. also Heiberg(1903), p. 58, for the attribution of the interpolation to Heron. According to another conjecture, first advanced by Bretschneider [cf. Bretschneider (1870), p. 168], this interpolation has in-

stead an older (and in fact pre-Euclidean) origin, being a survival of Eudoxus' work (this is also Mahoney's view [cf. Mahoney (1968-1969), p. 321]). For a discussion of these different hypothesis, cf. Euclid (EH), vol. I, p. 137, and vol. III, p. 442.

22. Cf. Pappus (CH) and Pappus (CM7J).

23. Among many other discussions of Pappus' definition and many reconstructions of the classical geometric method of analysis and synthesis, cf. those that are contained in Mahoney (1968-1969), Hintikka & Remes (1974), Knorr (1986), and Bos (2001).

24. Cf. for example Knorr (1986), p. 358 and Bos (2001), pp. 96-97.

25. Cf. Mahoney (1968-1969), p. 325. To substantiate his claim, Mahoney argues that Pappus' text, as it has been established by Hultsch [cf. Pappus(CH), vol. II, pp. 634-636], is corrupt because of the introduction of later interpolations aiming to provide a definition of synthesis, together with an alternative definition of analysis with respect to Pappus' original one (which would only consist of the lines 634, 11-13 of Hultsch's text).

26. I have justified this reconstruction of Pappus' characterisation of

problematic analysis in Panza(fc).

27. Notice that often—and specially in Viète's texts—the Latin literal translation of "*ἀνάλῠσις*", that is, "*resolutio*", was replaced by a simple Latinisation of the Greek term, that is "*analysis*", and that this was the origin of the corresponding vernacular terms.

28. Cf. the previous footnote 15.

29. Cf. Viete(1591a).

30. This was also due to the title chosen by Vasset et Vaulézard for their two 1630 French translations of the *Isagoge* and the *Zeteticorum libri*: cf. Viete (1630a) (containing both the *Isagoge* and the *Zeteticorum libri*) and Viete (1630b) (containing only the *Isagoge*; for Vaulézard's translation of the *Zeteticorum libri*, cf. instead Viete (1630c).

31. Cf. Pesic (1997b), p. 682. Remark however that according to Pesic, Viète's " 'infallible rule' of decryption manifests the same ambitious methodicalness as the 'analytic art, or new algebra' " [cf. Pesic (1997a), p. 21]. In the same vein, Ritter had identified Viète's "new algebra" with his "analytic art", but argued that Viète "créa l'Algèbre nouvelle, en représentant tous les

éléments d'une question, connus ou inconnus, par des lettres de l'alphabet, les opérations à effectuer sur elles par des signes et enfin le résultat par une formule, dans laquelle il suffisait, si la même question était posée avec des donnés différentes, de les substituer pour obtenir immédiatement le nouveau résultat demandé." [cf. Ritter (1895), pp. 255-256 and 373].

32. Cf. Viete (1591a), p. 1 and Klein (1968), 320-321. For an alternative translation by T. R. Witmer, cf. Viete (AAW), pp. 11-12.

33. Below, I shall consider this problem in all its generality.

34. According to my interpretation of poristic (that I take from Mahoney (1994), p. 34), to complete it, one should then prove that the proportions (1) hold, providing that the squares $Q(D)$, $Q(A)$ and $Q(E)$, respectively constructed on D, A, and E, are such that $B : C = Q(D) : Q(E)$ and $C : B = Q(D) : Q(A)$. Notice that another interpretation of poristic (and consequently of zetetic) is possible [cf. for example Freguglia (1999), 121-126 and Bos (2001), pp. 146-147]. This comes back to argue that zetetic only consists in the translation of the (conditions of the) problem in a system of equations, while poristic transforms such a system in a suitable system of proportions to be stated under the form of a theorem expressing the relation

between the givens and the unknowns of the problem. According to this interpretation, poristic ends, in the case under consideration, with the statement of proportions (3) and (4), while zetetic consists in the transformation of proportions (1) in the equations $AC = EB$ and $AE = D^2$.

35. As I have argued in Panza (fc), I think that neither the availability of a similar formalism is a necessary condition for performing a trans-configurational analysis nor Viète's analysis in the first example of trans-configurational analysis in the history of mathematics. However, I do not enter this question here, confining myself to notice the differences between Pappus' and Viète's analysis.

36. Cf. Pesic (1997a), p. 2 and Pesic (1997b), p. 681.

37. The literature about Newton's science and its relation with theology and alchemy is immense. I have given an account and an assessment of it in Panza (2003).

38. Cf. Pesic (1997a), 23[V] and Ms. 2009, *Bibliothèque de l'Institut de France*, Paris, f. 189 : "L'Espagnol est assez subtile en la composition de ses chiffres, Mais fort grossier en l'usage. L'Italien est tres subtil en la composition et tres subtil en l'usage. Quant la composition est une fois

entendue La resolution n'est pas difficile."

39. Viète remarks that Spaniard's coded messages "would be difficult to decipher if they [the Spaniards] were as fine and nimble in the usage of their ciphers as they are in composing them" [cf. Pesic (1997a), p. 24[V] and Ms. 2009, *Bibliothèque de l'Institut de France*, Paris, f. 190 : "Or y aurait bien peine à les descouvrer s'ils estoient fins et deliés en l'usage de leurs chiffres comme les sont a les composer."].

40. Cf. Pesic (1997a), p. 24[V] and Ms. 2009, *Bibliothèque de l'Institut de France*, Paris, f. 190 : "une grande lumière a voir l'abbrevrature et la forme des desguisements d'un mesme mot et la diversité des figures a l'expression du mesme terme ou syllabe."

41. Cf. Ms. 2009, *Bibliothèque de l'Institut de France*, Paris, f. 190.

42. Cf. p. 4, above.

43. Cf. Pesic (1997a), p. 27[V] and Ms Dupuy 661, *Bibliothèque Nationale de France*, Paris, f. 219r : "Mons. Viette avait des regles pour deschiffrer toute sorte de chiffres[...]."

44. This is made clear in the second memoir written after Viète's death:

cf. Pesic (1997a), pp. 27-28[V].

45. Cf. Pesic (1997a), p. 13.

46. Cf. Pesic (1997a), pp. 13-14.

47. Cf. Pesic (1997b), p. 682: "In the present instance, there are obvious connections: the articulation of a new kind of symbolic calculus in which the cipher stands for the plain text (or the algebraic symbol stands for its implicit values); and the search for the solution to the cipher (or for the unknown quantity), undertaken through a specific series of systematic manipulations."

48. Cf. Pesic (1997b), p. 684: "Viète treats both ciphers and algebraic symbols as systems of relations, rather than as objects. In neither case is there a direct correspondence between symbols and signified. Both ciphers and algebraic variables represent a whole range of possible values, not just one, and both must be manipulated with full generality in order to reveal whatever solution is possible."

49. Cf. Pesic (1997b), p. 683.

50. In the second memoir considered by Pesic, Viète's rules are indeed presented as being "so sure that they were almost infallible" [cf. Pesic

(1997a), p. 27[V] and Ms Dupuy 661, *Bibliothèque Nationale de France*, Paris, f. 219r: "si asseurées, qu'elles estoient presque infallibles"], what is quite different than arguing that they constitute a general and infallible method.

51. The term "conjecture" occurs explicitly in the second memoir: "In the end he attempted his conjectures on one of the copies of the cipher [...]" [cf. Pesic (1997a), p. 28[V] and Ms Dupuy 661, *Bibliothèque Nationale de France*, Paris, f. 219r: "Après il esseyoit ses conjectures sur une des copies de son chiffre [...]."]

52. Among a number of other documents and pieces of information that F. Ritter inserted in the part of his large unpublished intellectual biography of Viète [cf. the previous footnote (5)] concerned with Viète's cryptographic activity [cf. Ms. 2009, ff. 181-209], there are the transcription of two fragments of two coded messages decrypted by Viète, together with his respective solutions (that Ritter says [cf. *ibid*, f. 194] to have copied from a "volume, qui fait partie, dans la section des manuscrits de la Bibliothèque Nationale, de la collection dite 'Les cinq cents de Colbert' K. 33). The first fragment [*ibid*, f. 205-206] applies a simple code composed by 89 characters each of which either is a null or represents a single letter. In spite of the fact that each

vowel is represented by several characters [6 for "i" or "j", 5 for "u" or "v", and 4 for "a", "e" and "o"], it seems that Viète could have decrypted a similar code using his "infallible rule", as it has been interpreted in the previous section. This does not seem to be the case of the code applied in the second fragment [*ibid*, f. 206-208], instead. According to Ritter, it is composed by at least 200 characters (generally formed by Arabic numbers with two or three digits) representing either "syllabic combination" or words. If one can suppose that a similar code could have been solved by Viète quite easily, it is because, some exception apart, any syllabic combination that occurs in it, is represented by the ordinal number that designates its place in the list of all the syllabic combinations ordered according to the alphabetic order of their first letters (so that any combination begging with "a" is represented by a number smaller than the number which represents any combination begging with "b" and so on : "do" is for example represented by "21", "di" by "22", "de" by "23", "das" by "24", then "se" by "91", "sin" or "si" by "92", "so" by "93" and so on). A similar performance certainly testifies Viète's sagacity but it is not a proof of the generality and infallibility of his rules or methods.

53. Cf. p. 31, above.

54. Pesic is here quoting J. Klein: cf. Klein (1968), p. 174.

55. Cf. Pesic (1997b), p. 684.

56. Cf. p. 25, above.

57. Pesic also remarks that Viète's use of vowels and consonants to denote respectively unknown and known quantities in his algebraic formalism depends on his "cryptologic experience" [cf. Pesic (1997b), pp. 684-685]. This is quite possible, but certainly not significant for arguing in favour of the parallel I'm discussing.

58. Cf. Pesic (1997b), pp. 683.

59. Clearly "the things which are more knowable and clear for us" are here the characters which enter the coded message together with their mutual relations depending on the way they are combined, while "those which are clearer and more knowable by nature" are the plain texts that result after decryption, and that had been originally coded. Of course, there is an obvious sense in which these latter texts are for us more knowable and clearer than any coded message, providing that a cipher text is, for the great majority of us, *prima facie* incomprehensible. This has, nevertheless, little to do with my

point, since what is *prima facie* incomprehensible in a cipher text is not the text as such—that is, the sequence of the symbols it is composed of—, but rather its meaning, and this meaning is just what the decoded text expresses. Hence, though there is no doubt that an uncoded message would be easier to read for us, this cannot be in this case but the result of the process of decryption, and cannot thus but appear to us at the end, like the laws of nature appear at the end of a scientific enquiry (though being in a sense "more knowable and clear for us" than the empirical data that constitute the starting point of this enquiry). A more appropriate objection would consist in remarking that in decrypting a coded message following Viète's suggestions, one is guided not only by the regularities of the given system of characters (that is, the coded message itself) but also by the cogency of the plain text that is gradually unveiled and by some supposed regularities that such a text should satisfy. This is certainly true: the techniques relying on "essential ciphers" or on the position of words provide quite evident examples of it. Still this also happens, *mutatis mutandis*, in a scientific enquiry aiming to unveil the laws of nature starting from the "what is more confused, or the whole", which is the prototypical case of $\delta\iota\alpha\acute{\iota}\rho\varepsilon\sigma\iota\varsigma$ for Aristotle.

60. Notice that I'm not claiming that guesswork has nothing to do

with analysis or cannot enter it. One could mention different situations in which an analysis involves some sorts of guesses. This is for example the case of a locus problem, providing that analysis starts not only with the supposition that the sought-for curve is given, but also that it belongs to a certain class, which was quite usual in early modern geometric practice. A different (though, in a sense, correlative) example concerns the problem of looking for the compact form of a given polynomial, that was often solved starting with the supposition that this form was given and satisfied certain supplementary conditions. Finally, one could argue that theorematic analysis cannot but start with the guess that a certain proposition is a theorem.

References

Aristotele (CWAB). The complete works of Aristotle. The revised Oxford translation', edited by J.Barnes. Princeton: Princeton University Press, 1984.

Aristotle (NEA). The Nicomachean Etichs', translated with commentaries and glossary by H. G. Apostle. Dordrecht, Boston: Reidel publishing Company, 1975.

Bos, H. J. M. (2001). Redefining Geometrical Exactness. Descartes' Transformation of the Early Modern Concept of Construction. New York, Berlin, etc.: Springer.

Bretschneider, C. A. (1870). Die Geometrie und die Geometer vor Euklides [...]. Leipzig: B. G. Teubner.

Delahaye, J. P. (2003). "Viète, inventeur de la cryptanalyse mathématique". Pour la science, 313, November, 2003, 90-95.

Euclid (EH). Euclid's Elements, translated with introduction and commentary by Sir T. Heath (2nd). Cambridge: Cambridge Univ. Press, 1926 (2 vols.).

Euclid (OOH). Opera Omnia, editerunt I. L. Heiberg et H. Menge. New York, Heidelberg:Teubner, 1883-1889 (8 vols. + 1 vol. supl.).

Freguglia, P. (1999). La geometria fra tradizione e innovazione [...]. Torino: Bollati Boringhieri.

Heiberg, J. L. (1903). "Paralipomena zu Euklid". Hermes, 38, 46-74, 161-201, 321-356.

Hintikka, J. & Remes, U. (1974). The Method of Analysis. Its Geometrical Origin and Its General Significance. Dordrecht: Reidel.

Joachim, H. H. (1951). The Nicomachean Etichs. Oxford: Clarendon Press.

Kahn, D. (1996). The Codebreakers (2nd ed.). New York: Scribner (1st ed.: New York, Macmillan, 1967.

Klein, J. (1934-1936). "Die griechischte Logistik und die Entstehung der Algebra". Quellen und Studien zur Geschichte der Mathematik, Astronomie und Physik; Abteilung B : Studien, 3, 18-105 (n. 1, 1934), and 122-235 (n. 3, 1933).

Klein, J. (1968). Greek Mathematical Thought and the Origins of Algebra. Cambridge (Mass.): M.I.T. Press (English translation by E. Brann of Klein (1934-1936), with an Appendix containing Viète's Isagoge translated by J. W. Smith (pp. 313-353).

Knorr. W. (1986). The Ancient Tradition of Geometric Problems. Boston,

Basel, Stuttgart: Birkhäuser.

Mahoney, L. S. (1968-1969). "Another Look at Greek Geometrical Analysis". Archive for History of Exact Sciences, 5, 318-348.

Mahoney M. S. (1994). The Mathematical Career of Pierre de Fermat (2nd ed.). Princeton: Princeton Univ. Press (First edition, 1973).

Otte, M. & Panza, M. (1997). Analysis and Synthesis in Mathematics. History and Philosophy. Dordrecht: Kluwer A. P.

Panza, M. (1997). "Classical Sources for the Concepts of Analysis and Synthesis". In Otte & Panza (1997), 365-414.

Panza, M. (2003). Netwon. Paris: Les Belles Lettres.

Panza, M. (2005). Netwon et les origines de l'*analyse*: 1664-1666. Paris: Blanchard.

Panza, M. (fc). "On the notion of algebra in early modern mathematics and its relations with analysis: Some reflections on Bos' definitions". Submitted to the Revue d'histoire des mathématiques.

Pappus (CM7J).Book 7 of the Collection [of] Pappus of Alexandria, edited with English translation and commentary by A. Jones. Leipzig: Springer-Verlag, 1986.

Pappus (CH). Pappi Alexandrini Collectionis [...], edited with Latin trans-

lation and commentary by F. Hultsch. Berolini: Weidmann, 1876-1878 (3 vols.).

Pesic, P. (1997a). "François Viète, Father of Modern Cryptanalysis. Two New Manuscripts". Cryptologia, 21, n. 1, 1-29.

Pesic, P. (1997b). "Secret, symbols, and systems. Parallel between cryptoanalys and algebra, 1580-1700". Isis, 88, 674-692.

Ritter, F. (1895). "François Viète, inventeur de l'algèbre moderne, 1540-1603. Essai sur sa vie et son œuvre". Revue Occidentale, 10, 234-274 and 354-415.

Viète, F. (1591a). In artem analiticem isagoge. Turonis: Apud J. Mettayer (in Viète (OPvS), 1-12).

Viète, F. (1591b). Zeteticorum libri quinque[...]'. Turonis: Apud J. Mettayer (in Viète (OPvS), 42-81).

Viète, F. (OPvS). Francisci Vietæ Opera Mathematica, In unum Volumen congesta, ac recognita, Operâ atque studio Francisci à Schooten Leydensis [...]. Lugduni Batavorum: B. & A. Elzeriorum, 1646.

Viète, F. (1630a). Introduction en l'art analytic, ou Nouvelle algèbre [...], traduict en nostre langue et commenté et illustré d'exemples par I.-L. Sieur de Vav-Lezard [...]. Paris: J. Jacquin (new edition in: La nouvelle algèbre de

M. Viète. Paris: Fayard, 1986.

Viète, F. (1630b). Les Cinq livres des zététiques de François Viette mis en françois, commentez et augmentez des exemples [...]. Par I.-L. Sieur de Vav-Lezard [...]. Paris: J. Jacquin (new edition in: La nouvelle algèbre de M. Viète. Paris: Fayard, 1986.

Viète, F. (1630c). L'algèbre nouvelle de Mr Viète [...] trad. en françois par A. Vasset. Paris: Chez Pierre Rocolet.

Viète, F. (AAW). The analytic art. Nine studies in algebra, geometry and trigonometry from the Opus Restituitæ Mathematicæ Analyseos, seu algebrâ novâ, translated by R. T. Witmer. Kent (Ohio): The Kent State Univ. Press, 1983.

Abstract

François Viète is considered the father both of modern algebra and of modern cryptanalysis. The paper outlines Viète's major contributions in these two mathematical fields and argues that, despite an obvious parallel between them, there is an essential difference. Viète's "new algebra" relies on his reform of the classical method of analysis and synthesis, in particular on a new conception of analysis and the introduction of a new formalism. The procedures he suggests to decrypt coded messages are particular forms of analysis based on the use of formal methods. However, Viète's algebraic analysis is not an analysis in the same sense as his cryptanalysis is. In Aristotelian terms, the first is a form of $\grave{\alpha}\nu\acute{\alpha}\lambda\breve{\upsilon}\sigma\iota\varsigma$, while the second is a form of $\delta\iota\alpha\acute{\iota}\rho\varepsilon\sigma\iota\varsigma$. While the first is a top-down argument from the point of view of the human subject, since it is an argument going from what is not actual to what is actual for such a subject, the second one is a bottom-up argument from this same point of view, since it starts from what is first for us and proceed towards what is first by nature.

Keywords: Analysis, Cryptanalysis, Algebra, Aristotle, Viète.