I.8 Translation and interpretation

The English differs from the French in some significant ways. In particular, in trying to establish an English edition I have followed the usual conventions for published mathematics. Thus, for example, italics are used where the manuscript has underlined words; italics are used (in most places—though not in Dossier 15) for the statements of propositions, theorems, lemmas, and the like; punctuation is corrected and modernised. Most, but not quite all, of the crossed-out material is incorporated into the translation. This was done mainly in the hope that some readers might find it useful, partly to help the English and French run properly in tandem on opposite pages. I can only hope that it does not make difficulties for those readers who want just the main text.

Generally I have tried to produce a rather literal translation, so as to give a fair idea in English of what Galois actually wrote. The reader will therefore find some artificial phrases and some sentences which could be re-cast into more agreeable form. Reading Galois is not difficult. He writes a legible and (mostly) pleasant hand. Understanding what he is saying is not difficult either (except where, in the polemical passages, his writing becomes unsympathetic and idiomatic). Translating, however, is harder. Many words and phrases, both in French and in English, have changed their usage and/or their meaning over these last 200 years. I can only hope that, having the original side by side with the translation, the reader will be able to make the comparisons which should lead to a good understanding of what Galois was trying to explain.

One example should give an idea of what I mean by the difference between understanding and translation. Near the beginning of the *Lettre testamentaire* (see p. 84) there is the sentence

> Le premier [mémoire] est écrit, et malgré ce qu'en a dit Poisson, je le maintiens avec les corrections que j'y ai faites.

The mention of Poisson refers to the report he made to the Académie des Sciences on 4 July 1831 (see Ch. IV, Note 2, p. 146). Although it is quite clear what Galois meant, finding a good English equivalent for his word *maintiens* presents difficulties. Dictionaries variously give 'maintain', 'keep', 'sustain', 'endorse', 'uphold', 'support', for the transitive French verb *maintenir*. But in this context none of these sounds quite right to my ear. My own translation is

> The first is written, and in spite of what Poisson has said about it I stand by it with the corrections that I have made in it.

In [Weisner (1929), p. 278] it is rendered as

> The first is written, and, despite what Poisson has said of it, I am keeping it, with the corrections I have made.

I find this an agreeable translation except that 'I am keeping it' does not quite fit the context. [Fauvel & Gray (1987), p. 503, § 15D1]—quoted in [Wardhaugh (2010), p. 21], where, however, it is mis-attributed to Weisner in [Smith (1929)]—offers

> The first is written, and despite what Poisson has said about it, I hold it aloft with the corrections that I have made.

Although 'hold it aloft' could be a version of 'uphold', this does not, I feel, present quite the picture that Galois would have had in mind. Perhaps the fact that Chevalier mistranscribed it as *soutiens* is an indication that the word *maintiens* is not particularly natural in this context.

Technical terms are a particular problem because translation involves judgments of meaning, so that translation and interpretation have to go together. Here are some notes on some of the more important words.

I.8.1 The words *analyste* and *géomètre*

The two words *analyste* and *géomètre* are fine illustrations of the problem with meanings. Their natural translations into modern English are of course 'analyst' and 'geometer' respectively (though a brass plate on an office door announcing *M. Pierre Lemesurier, Géomètre* says that Mr Pierre Lemesurier is a surveyor). In 1830, however, the two words both had two main meanings: on the one hand they were both used to mean 'pure mathematician' generically, though the former had overtones of 'algebraist'; on the other hand they indicated practitioners of the main subdivisions of pure mathematics.

They derive of course from the nouns *analyse* and *géométrie*. These were parts of *mathématiques* or *sciences mathématiques*, a broad area that included both pure and applied mathematics and more besides. Thus, for example, Vol. 21 (1830/31) of Gergonne's *Annales de mathématiques pures et appliquées* organised the material under 12 headings:

- *Analyse Algébrique;*
- *Analyse Appliquée;*
- *Analyse Élémentaire;*
- *Analyse Indéterminée;*
- *Analyse Transcendante;*
- *Arithmétique;*
- *Arithmétique Sociale;*
- *Géométrie Analytique;*
- *Géométrie des Courbes;*
- *Géométrie Élémentaire;*
- *Géométrie Transcendante;*
- *Philosophie Mathématique*.

Other volumes have similar lists, and whereas topics like *arithmétique, arithmétique sociale, astronomie, dynamique, hydrodynamique, hydrostatique, météorologie, philosophie mathématique, optique* come and go, various branches of *analyse* and *géométrie* always appear. Roughly speaking *analyse* covered algebra, number theory and calculus while *géométrie* covered spatial matters.

If the above paragraph gives an impression that *analyste* and *géomètre* were more or less synonymous then it is wrong. For one thing, as was indicated above, the former carries the suggestion of 'algebraist', if in a broad sense. For another, although pure mathematics was pretty much covered (with some overlap) by *analyse* and *géométrie*, the latter was the broader term. From 1820 to 1835, of the eleven sections of the Académie des Sciences, there was only one—as one sees when one reads the published minutes, the *Procès-Verbaux de l'Académie des Sciences de l'Institut de France*—that naturally covered pure mathematics and that was the *section de géométrie*. There were members of the *sections d'astronomie, de mécanique, de physique générale*, and perhaps even of other sections, who wrote articles that we might naturally classify as pure mathematics. These would then, however, be thought of as contributions to *géométrie*. There was no *section de mathématiques*.

During the first half of the 19th century the word *mathématiques* occurred quite rarely—hardly more than in the title of Gergonne's *Annales*, the title of Liouville's *Journal*, and in the context of the Academy prizes (*prix de mathématiques*, *grand prix de mathématiques*). Thus in the language of the Academy the word *géomètre* was used in the same way as we might use 'pure mathematician'. Abel, for example, contributed much more to *analyse* than to *géométrie*, but could nevertheless be referred to by Galois as a *géomètre* (see, for example, Section VI.5), meaning simply 'mathematician'. And the 1984 French postage stamp portraying Galois and describing him as '*révolutionnaire et géomètre*' is saying that he was a revolutionary and a mathematician—he was, after all, very much an algebraist and analyst, rather than a geometer in the familiar modern senses of these words.

I.8.2 The phrases *équation algébrique* and *équation numérique*

The phrases *équation algébrique* and *équation numérique* also require some thought. Their natural literal translations are 'algebraic equation' and 'numerical equation', meaning equations with literal or numerical coefficients, respectively. In almost all contexts in 18th- and 19th-century writings, however, the adjective does not in fact qualify the noun equation. It refers instead to what the writer has in mind as a strategy for solution. The former refers to the search for a formula, the latter to iterative numerical methods. Thus Lagrange's great works [Lagrange (1767)], [Lagrange (1798)], with titles involving *la résolution des équations numériques* have the adjective numerical qualifying the plural noun equations, and yet their subject is numerical methods for finding accurate approximations to the roots of polynomial equations.

A paragraph in Poinsot's preface to the 1826 edition of [Lagrange (1798)] (originally a review of the 1808 edition published in the *Magasin Encyclopédique* in 1808) explains well:

> D'abord si l'on jette un coup d'oeil général sur l'Algèbre, on voit que cette science, abstraction faite des opérations ordinaires (au nombre desquelles on peut compter l'élimination), se partage naturellement en trois articles principaux. 1°. La théorie générale des équations, c'est-à-dire l'ensemble des propriétés qui leur sont communes à toutes. 2°. Leur résolution générale, qui consiste à trouver une expression composée des coefficiens de la proposée, et qui, mise au lieu de l'inconnue, satisfasse identiquement à cette équation, en sorte que tout s'y détruise par la seule opposition des signes. 3°. La résolution des équations numériques, où il s'agit de trouver des valeurs particulières qui satisfassent d'une manière aussi approchée qu'on le voudra, à une équation dont tous les coefficiens sont actuellement connus et donnés en nombres.
>
> [If one casts a general glance over algebra, one sees first that, setting aside ordinary operations (numbered among which one can include elimination), this science is divided naturally into three principal parts. 1st. The general theory of equations, that is to say, the collection of properties which are common to all of them. 2nd. Their general solution, which consists in finding an expression composed of the coefficients of the given equation, and which, replacing the unknown, satisfies this equation identically, so that everything vanishes simply through cancellation. 3rd. The solution of numerical equations, where what matters is to find particular values which satisfy an equation, all of whose coefficients are actually known and given as numbers, to as close an approximation as is desired.]

The term *équation algébrique* has *équation littérale* ('literal equation' or 'letter equation') and *équation générale* ('general equation') as common variants. Galois used all three terms, and used them synonymously.

I.8.3 The words *permutation* and *substitution*

The words *permutation* and *substitution* are of course translated as 'permutation' and 'substitution' respectively. Straightforward and natural though that is, it involves pitfalls for the unwary modern reader.

The word *permutation* is ambiguous in French, as it is in English. In English school syllabuses the word 'permutation' in the phrase 'permutations and combinations' refers to an arrangement of symbols. In undergraduate mathematics it acquires a second (and perhaps more usual) meaning as a bijection of a set to itself. Thus it is used to mean a (static) arrangement, and also to mean an act of (dynamic) rearrangement. Lagrange in [Lagrange (1770/71)] and [Lagrange (1798), 2nd or 3rd ed., Note XIII] used the word in both senses, but more usually dynamically (in the phrase *faire une permutation*). Cauchy in [Cauchy (1815a)] used the word *permute*

as a verb in the title of his article, but used the noun *permutation* in the static sense of an arrangement in the body of his text.

The word *substitution*, on the other hand, is quite unambiguous. It always means the act of rearranging, that is to say, in modern terms a bijective mapping. This is how Cauchy defined it quite precisely in his 1815 paper cited above. Thus, referring to a function K of several variables, he wrote

> Pour indiquer cette substitution, j'écrirai les deux permutations entre parenthèses en plaçant la première au-dessus de la seconde; ainsi, par exemple, la substitution
>
> $$\begin{pmatrix} 1.2.4.3 \\ 2.4.3.1 \end{pmatrix}$$
>
> indiquera que l'on doit substituer, dans K, l'indice 2 à l'indice 1, l'indice 4 à l'indice 2, l'indice 3 à l'indice 4 et l'indice 1 à l'indice 3.
>
> [To indicate this substitution I write the two permutations between parentheses, placing the first above the second; thus, for example, the substitution
>
> $$\begin{pmatrix} 1.2.4.3 \\ 2.4.3.1 \end{pmatrix}$$
>
> will indicate that one must substitute the index 2 for the index 1, the index 4 for the index 3, the index 3 for the index 4 and the index 1 for the index 3 in K.]

In this context it should be noted that when Cauchy returned to substitutions in 1845, and wrote his many *Compte rendus* papers, of which [Cauchy (1845a)] is (or are) the first, and his long memoir [Cauchy (1845b)] (the title of which includes an interesting use of the words *arrangements*, *permutations*, and *substitutions*), he turned his two-line notation the other way up. Thus in the works of 1845 (see [Neumann (1989)] for an account of the dating of these works) we must read $\begin{pmatrix} B \\ A \end{pmatrix}$ as the substitution in which the arrangement B replaces the arrangement A.

Galois sometimes used the verb *permuter*, 'to permute' in the sense of 'to rearrange'; see, for example, Lemma II and the proofs of Lemmas III and IV of the First Memoir. Mostly, however, he used noun-forms and followed Cauchy's 1815 language, using *permutation* to mean 'arrangement' (static) and *substitution* to mean 'substitution' or 'act of rearrangement' (dynamic). Unfortunately, however, he did not use the words consistently. Sometimes he used *permutation* where he meant *substitution*—moreover, he caught himself doing this from time to time, and changed the former to the latter. The reader must be aware of the ambiguity and, where it is not immediately clear, infer the meaning from the context.

I.8.4 The word *groupe*

The word *groupe* is of course translated as 'group'. Note, however, that in the writings of Galois a group is always a group of permutations or a group of substitutions. These are not the same.

In Galois' writings a group of substitutions is a collection (non-empty goes without saying) of substitutions that is closed under composition. Since these are always substitutions of a finite number of 'letters' (the roots of a polynomial equation), closure under composition automatically implies that the identity lies in the collection and that the collection is closed under formation of inverses. Thus a *groupe de substitutions* is what we know as a group of (confusingly) permutations, a subgroup of the relevant symmetric group.

Galois also has *groupes de permutations*. A *groupe de permutations* is a collection of arrangements with the property that the collection of substitutions that change any one to any other of them is closed under composition, that is to say, is a group of substitutions. Originally these were the fundamental tools that he invented for Proposition I of the First Memoir. Gradually, though, as his thinking developed (as seen in the First Memoir, then the Second Memoir, and finally the Testamentary Letter), we see groups of substitutions becoming the principal objects of study.

Unfortunately, Galois often used the word *groupe* without specifying which kind of group he had in mind. Usually the context gives a clear indication whether the group in question is a group of permutations (arrangements) or a group of substitutions; sometimes the reader has to work quite hard to discover what was intended; and sometimes (though rarely), of course, it does not much matter.

At first Galois used the word *groupe* as an ordinary French noun meaning 'group', 'set', 'collection'. It acquired a technical meaning only through repeated use. When the academy referees read his *Premier Mémoire* they would have had to infer any special meaning of the word from the proof of Proposition I, from the first scholium (see p. 116) that follows it, and (if they were not already stymied) from the regular use of it later in the paper. At that time Galois had not explained its meaning. It was only at the final revision on the eve of the fatal duel that he added his famous explicit definition (**f.3b**, p. 114):

> Les substitutions sont le passage d'une permutation à l'autre.
>
> La permutation d'où l'on part pour indiquer les substitutions est toute arbitraire [...]
>
> [...]
>
> Donc si dans un pareil groupe on a les substitutions S et T, on est sûr d'avoir la substitution ST.

> [Substitutions are the passage from one permutation to another.
>
> The permutation from which one starts in order to indicate substitutions is completely arbitrary [...]
>
> [...]

Therefore, if in such a group one has the substitutions S and T, one is sure to have the substitution ST.]

He added this in the margin alongside Proposition I of the *Premier Mémoire*, with the instruction to print it in the introductory section, which is where it correctly appears in all editions previous to this one.

The point made in the foregoing paragraph is illustrated by comparison with the word *ensemble* ('set', 'collection'). Galois used this word, but it did not acquire a technical meaning in his writings. It remained an informal word. Compare the words *groupe* and *ensemble* in passages where they occur together: in the deleted sentence before the last paragraph of the definition of *groupe* in the *Premier Mémoire* (**f.3b**, p. 114), in Dossier 15, **f.82a**, **f.83b** and **f.84a**, and in the first example to Proposition I of the *Premier Mémoire* (**f.3b**, p. 114, **f.54b** in Dossier 6, and **f.87a**, **f.88a** in Dossier 16).

It has been suggested to me that Galois may have acquired his word *groupe* from the lovely preface by Poinsot to the 1826 edition of Lagrange's treatise on numerical solution of equations (cited above, p. 20). Poinsot used the word informally at first, and although, as he continued to develop the ideas he was expounding there, it gradually acquired some of the characteristics of a technical term, the context is rather different from that of Galois. Poinsot's are groups of roots of an equation, not of permutations or substitutions of roots. In modern terms we can recognise them as being akin to blocks of imprimitivity of a transitive permutation group acting on the set of roots; indeed, in anachronistic terms, once the relevant Galois theory is in place, that is precisely what they are. That this is where Galois got the word is certainly a possibility. I am inclined to doubt it, though. And I doubt very much that it is where he got his concept—there is nothing like his notions of *groupe* in Poinsot's preface. Reading what Galois wrote I get a strong impression that, as I have explained above, he began by simply using the word *groupe* as an ordinary and convenient noun. He could as well have chosen some other collective noun, except that *groupe* is simple and direct and has the associated verb *grouper*. It seems extremely unlikely that he owed it to Poinsot.

I.8.5 The word *semblable*

The word *semblable* is naturally translated as 'similar'. At many points it has a technical meaning. Most often it occurs in plural form as an adjective qualifying *groupes*. Thus for example, in the discussion following the statement of Proposition VII of the First Memoir, and in **f.84a** (Dossier 15), if Γ is a group of permutations (arrangements) and S is a substitution, then ΓS is a group of permutations and Γ, ΓS are *groupes semblables*. (I have distorted the notation here, using Γ where Galois used G, because I want to emphasize the distinction between a group of permutations and a group of substitutions. Note that if G is the group of substitutions corresponding to the group Γ of permutations then the group of substitutions corresponding to ΓS is $S^{-1}GS$.)

There are a few points where the adjectival phrase *semblables et identiques* is used to qualify *groupes*. This should be understood as follows: there is a group Γ of permutations (arrangements) with group G of substitutions; this contains a group Δ of permutations with group H of substitutions; what is meant is that H is a normal subgroup of G. The point is this. Let $S_1, S_2, \ldots, S_m$ be right coset representatives for H in G, so that $G = HS_1 \cup HS_2 \cup \cdots \cup HS_m$ (a disjoint union). Then $\Gamma = \Delta S_1 \cup \Delta S_2 \cup \cdots \cup \Delta S_m$, a union of *groupes semblables*. The group ΔS_i of permutations (arrangements) corresponds to the group $S_i^{-1} H S_i$ of substitutions. Given that H is a normal subgroup of G these are identical; hence *semblables et identiques*, 'similar and identical'. The groups of permutations are similar, their groups of substitutions are identical. That this reading is likely to be robust is confirmed by a passage on **f.55b** (Dossier 7), where Galois changed

> Il faut donc que le groupe G se partage en p groupes H semblables et identiques
>
> [It is therefore necessary that the group G be partitioned into p similar and identical groups H.

to

> Il faut donc que le groupe G se partage en p groupes H semblables et dont les substitutions soient les mêmes
>
> [It is therefore necessary that the group G be partitioned into p groups H that are similar and of which the substitutions are the same]

The *décomposition propre* of the *Lettre testamentaire*, **f.8a** is the same thing. Also, in the Second Memoir, for example in **f.37b**, **f.39a**, **f.39b**, Galois used *groupes conjugués* ('conjugate groups') in what appears (from the context) to be a similar sense, that is to say, for groups of permutations contained in a larger group and such that their groups of substitutions are all equal and form a normal subgroup of the group of substitutions of the large one.

I.8.6 The word *primitif*

The word *primitif* is naturally translated as 'primitive'. It is a technical term for which Galois gave a definition in his 'Analyse d'un Mémoire' published in Férussac's *Bulletin*, April 1830, in **f.8b** of the *Lettre testamentaire*, and at one or two other points (sometimes implicitly). The paper [Neumann (2006)] devotes some 50 printed pages to the word. I do not propose to enter into such detail here. It must suffice to remind the reader that in this context a *groupe primitif* should usually be thought of in modern terms as a quasi-primitive permutation group, that is to say, a permutation group with the property that every non-trivial normal subgroup is transitive; an *équation primitive* is then an equation or polynomial whose Galois group is quasi-primitive in its action on the set of roots.

I.8.7 Other words and phrases

In addition to (semi-)technical terms discussed above there are other words and constructions that Galois used which are not easy to translate. It is easy enough to see what he meant, but finding a way of saying it in English using similar words and constructions is not easy. Here are some common examples:

- I have chosen to translate *ensemble* as 'collection' because 'set' has a modern technical meaning, and Galois used the word as an ordinary noun, not as a technical term.
- I have chosen to translate *équation proposée* literally as 'proposed equation'. Nowadays we would more naturally write 'given equation' but most writers of the time used *équation proposée*, in preference to *équation donnée* (which, however, one does see from time to time).
- Galois made extensive use of the construction *x étant*. Mostly I have used the ugly literal translation '*x* being', but more common (and more agreeable) English usage is 'where *x* is'.
- Constructions such as *Remarquons que*, *Prenons*, etc., might be translated literally as 'We note that', 'We take', etc. In French however, they indicate an imperative, and so they should be translated into the imperative mood 'Note that', 'Take', etc., that is common also in mathematical English.
- Constructions such as *on obtient* are often translated into the passive rather than 'one obtains'.
- The word *caractère* should naturally mean 'character' or 'characteristic', but Galois often used it to mean 'property' or 'condition'.

I.8.8 Glossary

For the convenience of the reader I summarise here some of the discussion above, and add a few further words to the dictionary.

Analyse is naturally translated as 'analysis', but with a meaning that is close to algebra in our context.

Analyste is naturally translated as 'analyst', but the meaning is closer to 'algebraist' or 'pure mathematician' (compare *géomètre*).

Équation is naturally translated as 'equation', but very often is used where we would use 'polynomial'.

Degré is naturally translated as 'degree'. Mostly Galois used it in exactly the same way as it is used nowadays as in degree of an equation or a polynomial, degree

of a radical (or algebraic number), degree of a substitution group (as the number n such that the group is a subgroup of $\mathrm{Sym}(n)$), degree of an algebraic surface. Note, however, that in [Cauchy (1815a), p. 13] *le degré* [*d'une*] *substitution* is defined to be what we would call its order: the degree of S is the least m such that S^m is the identity. There are a few passages where Galois seems to have this usage, or something similar to it, in mind—see **f.84b** and **f.91a**, for example (pp. 290, 314)—but there are discrepancies in that Galois could there be intending the number of letters permuted.

Géomètre is naturally translated as 'geometer', but the meaning is closer to 'pure mathematician' (compare *analyste*).

Groupe, sometimes groups of permutations (static arrangements), sometimes groups of substitutions.

Groupe partiel, is naturally translated as 'partial group'. Think of the modern terms 'subgroup' and 'coset'. In some contexts one is appropriate, in others the other.

Groupe sousmultiple, naturally translated as 'submultiple group', to be thought of as 'subgroup'. Galois also used the word *diviseur* 'divisor'.

Mémoire is naturally translated as 'memoir'. This works well in 19th century English, though 'article' or 'paper' would be more common now.

Ordre is naturally translated as 'order'. Note, however, that in the context 'la substitution sera de l'ordre p' it usually means the number of letters moved by the substitution.

Période is naturally translated as 'period'. Note, however, that in the context 'substitution dont la période sera de p termes' it means what is now called order—the substitution will have order p.

Permutation is naturally translated as 'permutation' but with the meaning of an arrangement (static).

Substitution is naturally translated as 'substitution', meaning an act of rearranging (dynamic); unfortunately, nowadays we use the word 'permutation'.

Substitution circulaire is naturally translated as 'circular substitution'. It would be very dangerous to follow one's instinct and use 'cyclic substitution' (or 'cyclic permutation') because that is not what it appears to mean. In the First Memoir, in passages about equations of prime degree p, the term refers to the whole cyclic group generated by a p-cycle. In the Second Memoir it is less clear what is meant, but at one point (see p. 178) Galois used the term to refer to the substitutions of prime order that lie in the (unique, as it happens) normal abelian subgroup of his primitive permutation group of prime-squared degree. At that point these have p p-cycles.

The usage of this term by Galois seem to differ considerably from the meaning carefully defined by Cauchy in [Cauchy (1815a), p. 17], where a *substitution circulaire* is very clearly defined as a cyclic substitution of the indices (letters, points) that it does not fix.

Transformer is translated as 'to transform'. It occurs a few times in the Second Memoir, where its meaning is what I can best describe in modern language as 'transform by conjugation'.

I.9 A 'warts and all' transcription

As has been indicated above, the French is intended as a 'warts-and-all' transcription. What this means is that I have sought to reproduce the manuscript as accurately as possible in print, with all its crossings-out, emendations, additions and quirks of writing. In particular, the crossed-out material, except where it consists of no more than one or two illegible letters, has been included in its proper place. (Most, but not all, of this was transcribed by Robert Bourgne and appears on the left hand pages of [B & A (1962)].) Some of the crossed-out material was simply abandoned as Galois proceeded to his next phrase or sentence. But sometimes a word or two here and there was retained and re-used. Thus, for example, near the bottom of **f.39a** in the Second Memoir there was a passage that might have read

> [...]. Ce n'est point $p^2 - p$, puisque le groupe G serait non primitif.
> Mais il faut que les substitutions [...]

Then three words from the beginning of the second paragraph were deleted, the words 'que les' were retained and incorporated into the revised text, the word 'substitutions' was changed to 'permutations', and new text was inserted at the end of the previous paragraph, so as to read

> [...]. Ce n'est point $p^2 - p$, puisque le groupe G serait non primitif. Si donc dans le groupe G on ne considère que les permutations [...]

without a paragraph break. Independently of all this the words 'dans ce cas' were inserted so that the final text reads

> [...]. Ce n'est point $p^2 - p$, puisque dans ce cas le groupe G serait non primitif. Si donc dans le groupe G on ne considère que les permutations [...]

It should be noted also that there was a false start, immediately broken off, to the second paragraph. Also, it is quite possible that at the first pass Galois stopped after 'Mais il faut'.

The following notes are intended to make the phrase 'a warts and all transcription' a little more precise.

- Misprints, mis-spellings and infelicities of punctuation have been retained; note that mis-spellings include unconventional use or non-use of diacritical marks. Often accents, especially acute accents are missing; where ‘é’ follows ‘t’, however, the accent could be swallowed up in the crossbar of the ‘t’ and where it is unclear I have assumed that it is there. Some of these may be not so much mis-spellings as dated usage, such as ‘tems’ for ‘temps’. Others may be not so much mis-spellings as haste—a circumflex accent might easily emerge like a grave accent late on a pre-duel evening.

  The lists below are unlikely to be complete—I did not start compiling them until well into the work. I hope, however, that they may give the reader some idea of the problem. Now that images of the manuscripts have (from June 2011) become available through web-publication in digitised form (see [Galois (2011)], p. 392), these and other infelicities are capable of being checked. I believe that the reader will find

  – ‘a’ for à’,
  – ‘algèbrique’ or ‘algebrique’ for ‘algébrique’,
  – ‘appêllerons’ for ‘appellerons’,
  – ‘appèle’ for ‘appelle’,
  – ‘arrèter’ for ‘arrêter’,
  – ‘bientòt’ for ‘bientôt’,
  – ‘celà’ for ‘cela’,
  – ‘complementaire’ for ‘complémentaire’,
  – ‘completer’ for ‘compléter’,
  – ‘connait’ for ‘connaît’,
  – ‘consequent’ for ‘conséquent’,
  – ‘coté’ for ‘côté’,
  – ‘dégré’ for ‘degré’,
  – ‘doît’ for ‘doit’,
  – ‘dù’ for ‘dû’,
  – ‘ecrire’ for ‘écrire’,
  – ‘equation’ for ‘équation’,
  – ‘ètre’ or ‘etre’ for ‘être’,
  – ‘eùt’ for ‘eût’,
  – ‘evidemment’ for ‘évidemment’,
  – ‘éxemple’ for ‘exemple’,
  – ‘éxige’ for ‘exige’,

  - ‘frequent’ for ‘fréquent’,
  - ‘gachis’ for ‘gâchis’,
  - ‘general’ for ‘général’,
  - ‘geometre’ for ‘géomètre’,
  - ‘guere’ for ‘guère’,
  - ‘intéret’ for ‘intérêt’,
  - ‘meme’ or ‘mème’ for ‘même’,
  - ‘numeriques’ for ‘numériques’,
  - ‘ou’ for ‘où’,
  - ‘paraitrait’ for ‘paraîtrait’,
  - ‘partageàt’ for ‘partageât’,
  - ‘periode’ for ‘période’,
  - ‘plutot’ for ‘plutôt’,
  - ‘précedemmant’ for ‘précédemmant’,
  - ‘premiérement’ for ‘premièrement’,
  - ‘prevoir’ for ‘prévoir’,
  - ‘pùt’ for ‘pût’,
  - ‘rebùte’ for ‘rebute’,
  - ‘reconnaitre’ for ‘reconnaître’,
  - ‘regles’ for ‘règles’,
  - ‘remplacant’ for ‘remplaçant’,
  - ‘reponde’ for ‘réponde’ and ‘repondre’ for ‘répondre’,
  - ‘resolues’ for ‘résolues’,
  - ‘resultat’ for ‘résultat’ (and in plural),
  - ‘siécle’ or ‘siecle’ for ‘siècle’,
  - ‘symmétrique’, ‘symmetrique’ or ‘symmettrique’ for ‘symétrique’,
  - ‘tems’ for ‘temps’ [but perhaps this is simply a case of old spelling],
  - ‘tète’ for ‘tête’,
  - ‘théoreme’ for ‘théorème’;

  note also that there is little consistency here;

- inconsistencies in hyphenation, such as

  - ‘c’est à dire’ *v.* ‘c’est-à-dire’.

  - ‘non-primitif’ *v.* ‘non primitif’,
  - ‘peut être’ *v.* ‘peut-être’.

- Unconventional but consistent usages, such as ‘de suite’ for ‘tout de suite’, have been retained.

- Often Galois clearly ran two words together, as in ‘àmoins’, ‘cequi’, ‘delà’, ‘demême’, ‘deplus’, ‘enaura’, ‘enfonction’, ‘ensorte’, ‘entout’, ‘entant’, ‘desuite’ (as in ‘ainsi desuite’), ‘lemoyen’, ‘oubien’, ‘parconséquent’, ‘quelque’ for ‘quel que’ (though of course ‘quelque’ also exists as a genuine word), ‘yavait’;

- contrariwise sometimes Galois clearly would split a word, as in ‘la quelle’ for ‘laquelle’ or ‘les quelles’ for ‘lesquelles’, ‘en suite’ for ‘ensuite’, ‘puis que’ for ‘puisque’, ‘si non’ for ‘sinon’;

Some of these infelicities are sporadic, some are more systematic, none are greatly disturbing.

The notation that Galois used was generally clear and conventional, though the Second Memoir and a few other manuscripts have some unconventional usages:

- In the Second Memoir Galois used a clearly and carefully written . (rather than ,) to separate indices, as in $a_{1.0}$, etc.; moreover, within the text a dot often stands for a comma—but this usage has not been retained as it would be too confusing, especially since the manuscripts also contain a number of random and otiose non-punctuating dots which, one may conjecture, Galois may have made by touching the paper lightly with his pen on finishing a word or formula;

- In the Second Memoir (and several other places) Galois almost always, with just a very few exceptions, wrote his 2nd order inferiors directly below the 1st order inferiors as in $a_{\substack{k \\ 1}}$, etc.;

- Galois used four or more dots $\cdot\cdot\cdot\cdot$ for ellipsis.

In the manuscripts such labels as ‘Lemme’, ‘Théorème’, ‘Démonstration’ are written in the same style as the main text, as are the statements that they label. In his copy Chevalier doubly underlined them; Liouville used SMALL CAPITALS for the main labels and *italics* for subsidiary ones; Bourgne & Azra used SMALL CAPITALS. Liouville used quotation marks to indicate the status of statements of theorems, lemmas, etc., Picard italicised them in the conventional way, Bourgne & Azra followed Galois in not distinguishing. For the present warts-and-all edition I have chosen to follow Galois in the French, but to use modern conventions in the English.

In some of his writings Galois indented the first lines of his paragraphs, in others he did not. I have not studied the phenomenon carefully, but I have an impression that it is the later writings that have indentations. If so, and if this is systematic, then it could help to date the various items. Where paragraphs are not indented

their beginnings can usually be deduced from the fact that the previous line is not full and that there is sometimes a very thin space between paragraphs. The English translation, which does have paragraph indentations, should help to clarify what is going on in the French.

Often Galois used a thin horizontal line to indicate that he had come to a full cadence or finished a passage of writing. Many of these seem to me to be significant, and I have tried to reproduce them as faithfully as possible in the transcription.

I.10 The transcription: editorial conventions

In physical descriptions of the manuscripts a cm $\times$ b cm gives width (East–West, direction of lines of writing) first, then depth (North–South). In his emendations and other adjustments to his writings Galois made heavy use of the two-dimensional nature of a page. In my transcriptions I have tried to produce something that reflects the order and the disorder of the manuscripts. The linearity of print makes that well-nigh impossible of course. There are, however, some techniques that help. The following conventions differ from, but are similar in concept to, some of those used by Bourgne & Azra (see [B & A (1962), p. xxxiii]):

- brackets ^text^ indicate emendations or afterthoughts inserted above the line;
- brackets ˬtextˬ indicate emendations or afterthoughts inserted below the line;
- brackets ⌜text⌝ indicate afterthoughts inserted on the line of text;
- asterisks used as brackets *text* indicate afterthoughts written into the margin (the left margin—there is no right margin).

Note that Galois himself used asterisks to indicate footnotes and also some of his marginal additions. These are here rendered as * or * .

It has been impossible to mimic the deletions in the manuscript as closely as I would have liked. Although many of them are done with a single line, sometimes Galois used a very heavy line, sometimes a wavy line, sometimes he cross-hatched. Two lines ~~thus~~ simply indicate heavier crossing-out than one ~~thus~~. Where something is crossed out and replaced (usually with a word or two above the line) it is rendered without a space thus: ~~rendered~~^transcribed^. A space, small though it may be, as in ~~rendered~~ ^A space^, indicates that the insertion was not a replacement for the deleted material. Or at least, that that is my belief.

Where I have been unable to decipher a word I have used [?], [??], [???] or [????], the number of question marks indicating the probable number of illegible syllables.

Most, but not quite all, of the crossed out material has been translated. This is partly as a service to the reader, partly to help keep the English running properly in tandem with the French on the opposite page.

Just as it is impossible to make a perfect translation, so it is impossible to transcribe a manuscript into print entirely faithfully. Choices have had to be made. I have sought to get as close to the original as I could, but it would not have been helpful, even had it been possible, to reproduce in type the exact layout on the page, such as line-breaks or replacement above (and sometimes below) the line, or in the margin, of crossed-out words and phrases. Nevertheless, I hope that this transcription will be found to be satisfactorily close to the original. If nothing else, the retention of infelicities of spelling and grammar, and the many indications of emendations and afterthoughts, should keep at the front of our mind the fact that we are dealing here with mainly unpolished manuscripts by an untrained young genius of another age.

Chapter II
The published articles

The five mathematical articles (there was also a non-mathematical article in the form of a 'letter to the editor' [Galois (1831)], reprinted in [Dalmas (1956/82), pp. 96–99], in [B & A (1962), pp. 20–25], and in [APMEP (1982), p. 16]) published in Galois' lifetime are:

(1) Démonstration d'un Théorème sur les Fractions Continues Périodiques (1829)

(2) Analyse d'un Mémoire sur la résolution algébrique des Équations (1830)

(3) Note sur la résolution des équations numériques (1830)

(4) Sur la théorie des nombres (1830)

(5) Note sur quelques points d'analyse (1830)

Galois was just seventeen years old when (1) was published, eighteen when the next three came out, and nineteen when (5) was published.

They appeared in two journals of the day. The first was *Annales de Mathématiques pures et appliquées*. Its title-page describes it as "Recueil périodique, rédigé et publié Par J. D. Gergonne, professeur à la faculté des sciences de Montpellier, membre de plusieurs sociétés savantes." [A periodic collection edited and published by J. D. Gergonne, professor at the faculty of science of Montpellier, member of several learned societies.] It appeared in monthly issues of 30–40 pages from 1801 to 1832, and was devoted to the publication of original mathematics. It was succeeded by Liouville's *Journal de Mathématiques pures et appliquées* (see the editorial by Liouville in the first issue of his journal), which started publication in 1835 and is still going strong.

The second is the *Bulletin des Sciences Mathématiques, Physiques et Chimiques* (originally the *Bulletin des Sciences Mathématiques, Astronomiques, Physiques et Chimiques*), an approximation to the title-page of which is shown overleaf. It was known familiarly as Férrusac's *Bulletin* and was very different from Gergonne's *Annales*. It was not the sort of journal in which one might nowadays expect a technical paper to appear. The great majority of its content consisted of reviews of books and articles published elsewhere. Little of what it contained was original. The note 'Sur la théorie des nombres' by Galois was one of the few exceptions. The paper [Taton (1947b)] gives a valuable account of Férussac's *Bulletin* and the mathematics it contained.

I have tried to copy the originals as faithfully as possible, bating the differences between the typography of 1830 and our time. They contain a number of misprints and other slips, some of them surely not the fault of the printer. We do not have the original manuscripts however, so although editors and compositors have intervened, these come as close as we can get to what Galois originally wrote.

The title-page of Férussac's *Bulletin*:

BULLETIN
DES SCIENCES MATHÉMATIQUES,
PHYSIQUES ET CHIMIQUES,
RÉDIGÉ PAR MM. STURM ET GAULTIER DE CLAUBRY.

1re SECTION DU BULLETIN UNIVERSEL,
PUBLIÉ
PAR LA SOCIÉTÉ
POUR LA
PROPAGATION DES CONNAISSANCES
SCIENTIFIQUES ET INDUSTRIELLES,
ET SOUS LA DIRECTION
DE M. LE BARON DE FÉRUSSAC.

TOME TREIZIÈME.

A PARIS,
. . . . .
1830

The five papers are very different and appear to have triggered very different responses. The first, on continued fractions, had a friendly review in Férussac's *Bulletin*, 11, pp. 254–255. It has been cited even relatively recently by Davenport, who, however, comments that its main result was 'implicit in earlier work of Lagrange' (see [Davenport (1962), p. 100]). The second, which is an abstract of what the *Second Mémoire* was probably intended to become, is an announcement containing remarkable insights, but is, unfortunately, not entirely correct, and seems to have been ignored both by mathematicians—except, perhaps, Camille Jordan (but this must be the subject of a separate article at another time)—and by historians. The third also seems to have had little impact. It has been carefully treated in [Galuzzi (2001)]. The fourth was described in the *Lettre testamentaire* as being no more than a lemma for the work in the *Second Mémoire* (see p. 86) but is a work of immense independent interest, containing, as it does, most of the salient facts in the elementary part of the theory of what are now known as finite fields. The two items in the fifth were reviewed briefly in Férussac's *Bulletin*, 15, p. 15, but seem to have had no impact and are (in my view) of little interest, except insofar as they are comparable with the essays in Dossiers 21 and 22, which seem to me to be broadly similar in scope and character if not in subject-matter.

II.1 A theorem on continued fractions

This paper was published in Gergonne's *Annales de Mathématiques Pures et Appliquées*, 19, 294–301 (April 1829), when Galois was still a pupil at the Collège Louis-le-Grand. It was reprinted in [Liouville (1846), pp. 385–392], in [Picard (1897), pp. 1–8], and in [B & A (1962), pp. 364–377]. The concluding footnote is not by Galois; it is an addition by the editor J. D. Gergonne.

The edition by Liouville in 1846 has some modifications to punctuation and typography. In particular, continued fractions are rendered there in the form

$$\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\ddots}}}}}.$$

Picard's reprint of 1897 is more or less the same (though there are a few changes of punctuation), except at one point where the clause *écrite dans un ordre inverse*, echoing the statement of the main theorem, is added. The version in [B & A (1962)] is pretty faithful to the 1829 original.

The reference to Lagrange in the opening sentence of the paper is almost certainly to passages in the third edition [Lagrange (1826)] of his great work *Traité de la Résolution des équations numériques de tous les degrés*, 'Treatise on the solution of numerical equations of all degrees' (or 'Treatise on the numerical solution of equations of any degree' — see Subsection I.8.2 above). Continued fractions appeared in his approach to the numerical solution of equations already in [Lagrange (1767)], but I doubt that Galois would have read that article; [Lagrange (1798)], which is the foundation for [Lagrange (1826)], is heavily based on that earlier work. Continued fractions are introduced in § 22 of the 1826 edition and are developed throughout the book. In [Lagrange (1826), Ch. VI, pp. 47–73], §§ 45–64 are devoted to periodic continued fractions and irrational roots of quadratic equations — § 59 is of particular historical interest for its reference to earlier work of Euler in this area. It seems a fair conjecture that this long and careful treatment is what Galois had in mind.

p. 294

Démonstration d'un théorème sur les fractions continues périodiques;

par M. Evariste GALOIS, élève au Collége de Louis-le-Grand.

Spelling corrected in BA1962 to 'Collège'; Liouville has 'Collége' in a footnote, corrected to 'Collège' in P1897.

On sait que si, par la méthode de Lagrange, on développe en fraction continue une des racines d'une équation du second degré, cette fraction continue sera périodique, et qu'il en sera encore de même de l'une des racines d'une équation de degré quelconque, si cette racine est racine d'un facteur rationnel du second degré du premier membre de la proposée, auquel cas cette équation aura, tout au moins, une autre racine qui sera également périodique. Dans l'un et dans l'autre cas, la fraction continue pourra d'ailleurs être immédiatement périodique ou ne l'être pas immédiatement, mais, lorsque cette dernière circonstance aura lieu, il y aura du moins une des transformées dont une des racines sera immédiatement périodique.

Punctuation after 'immédiatement' changed in L1846 to semicolon.

Or, lorsqu'une équation a deux racines périodiques, répondant à un même facteur rationnel du second degré, et que l'une d'elles est immédiatement périodique, il existe entre ces deux racines une relation assez singulière qui paraît n'avoir pas encore été remarquée, et qui peut être exprimée par le théorème suivant:

THÉORÈME. Si une des racines d'une équation de degré quelconque est une fraction continue immédiatement périodique, cette équation aura nécessairement une autre racine également périodique

p. 295

que l'on obtiendra en divisant l'unité négative par cette même fraction continue périodique, écrite dans un ordre inverse.

Démonstration. Pour fixer les idées, ne prenons que des périodes de quatre termes; car la marche uniforme du calcul prouve qu'il en serait de même si nous en admettions un plus grand nombre. Soit une des racines d'une équation de degré quelconque exprimée comme il suit

$$x = a + \frac{1}{b + \frac{1}{c + \frac{1}{d + \frac{1}{a + \frac{1}{b + \frac{1}{c + \frac{1}{d + \text{.....}}}}}}}};$$

l'équation du second degré, à laquelle appartiendra cette racine et qui contiendra conséquemment sa corrélative, sera

$$x = a + \frac{1}{b + \frac{1}{c + \frac{1}{d + \frac{1}{x}}}};$$

Proof of a theorem on periodic continued fractions

by Mr Evariste GALOIS, Pupil at the College of Louis-le-Grand.

It is known that if one of the roots of an equation of the second degree is developed by the method of Lagrange as a continued fraction, this continued fraction will be periodic, and the same will be true of one of the roots of an equation of arbitrary degree if this root is a root of a rational factor of the second degree of the first member of the proposed equation, in which case this equation will have at least one other root which will equally be periodic. Furthermore, in either case the continued fraction could be periodic immediately or not immediately. But when the latter happens there will be at least one transformed equation, of which one of the roots will be immediately periodic.

Now when an equation has two periodic roots, corresponding to a rational factor of the second degree, if one of them is immediately periodic there exists a quite singular relationship between these two roots which appears not to have been noticed yet, and which may be expressed by the following theorem:

THEOREM. *If one of the roots of an equation of arbitrary degree is an immediately periodic continued fraction, the equation will necessarily have another root that is likewise periodic*

that is obtained by dividing negative unity by this same periodic continued fraction written in the reverse order.

Proof. To fix ideas, let us take only periods of four terms because the uniform progression of the calculation proves that it will be the same if we were to allow a greater number. Let one of the roots of an equation of arbitrary degree be expressed as follows:

$$x = a + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} + \frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} + \text{.....}\ .$$

The equation of the second degree to which this root belongs, and which therefore contains its co-relative, will be

$$x = a + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} + \frac{1}{x}\ .$$

or, on tire de là successivement

$$a - x = -\frac{1}{b} + \frac{1}{c} + \frac{1}{d} + \frac{1}{x}\ , \qquad \frac{1}{a-x} = -(b + \frac{1}{c} + \frac{1}{d} + \frac{1}{x}\ ,$$

$$b + \frac{1}{a-x} = -\frac{1}{c} + \frac{1}{d} + \frac{1}{x}\ , \qquad \frac{1}{b} + \frac{1}{a-x}\ , = -(c + \frac{1}{d} + \frac{1}{x}\ ,$$

$$c + \frac{1}{b} + \frac{1}{a-x} = -\frac{1}{d} + \frac{1}{x}\ , \qquad \frac{1}{c} + \frac{1}{b} + \frac{1}{a-x} = -(d + \frac{1}{x}\ ,$$

p. 296

$$d + \frac{1}{c} + \frac{1}{b} + \frac{1}{a-x} = -\frac{1}{x}\ , \qquad \frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a-x} = -x\ ,$$

c'est-à-dire,

$$x = -\frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a-x}\ ;$$

c'est donc toujours là l'équation du second degré qui donne les deux racines dont il s'agit; mais en mettant continuellement pour x, dans son second membre, ce même second membre qui en est, en effet la valeur, elle donne

$$x = -\frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a} + \frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a} + \text{.....}\ ;$$

c'est donc là l'autre valeur de x, donnée par cette équation; valeur qui, comme l'on voit, est égale à -1 divisé par la première.

In P1897, though not in L1846, "écrite dans un ordre inverse" is supplied after "la première".

Dans ce qui précède nous avons supposé que la racine proposée était plus grande que l'unité; mais, si l'on avait

$$x = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} + \frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} + \text{.....}\ ,$$

on en conclurait, pour une des valeurs de $\frac{1}{x}$,

Now from that one derives successively

$$a - x = -\frac{1}{b} + \frac{1}{c} + \frac{1}{d} + \frac{1}{x}\,, \qquad \frac{1}{a-x} = -(b + \frac{1}{c} + \frac{1}{d} + \frac{1}{x}\,,$$

$$b + \frac{1}{a-x} = -\frac{1}{c} + \frac{1}{d} + \frac{1}{x}\,, \qquad \frac{1}{b} + \frac{1}{a-x}\,, = -(c + \frac{1}{d} + \frac{1}{x}\,,$$

$$c + \frac{1}{b} + \frac{1}{a-x} = -\frac{1}{d} + \frac{1}{x}\,, \qquad \frac{1}{c} + \frac{1}{b} + \frac{1}{a-x} = -(d + \frac{1}{x}\,,$$

$$d + \frac{1}{c} + \frac{1}{b} + \frac{1}{a-x} = -\frac{1}{x}\,, \qquad \frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a-x} = -x\,,$$

that is to say,

$$x = -\frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a-x}\,.$$

This therefore is always the equation of the second degree which gives the two roots in question. But, continually putting for [in place of] x in its second member this same second member, which is, in fact its value, it gives

$$x = -\frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a} + \frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a} + \text{.....}\,.$$

This is therefore the other value of x given by the equation, a value which, as can be seen, is equal to -1 divided by the first [written in the reverse order].

In what precedes we have supposed that the given root was greater than unity, but if one had

$$x = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} + \frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} + \text{.....}\,,$$

One would conclude, for one of the values of $\frac{1}{x}$, that

p. 297

$$\frac{1}{x} = a + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} + \frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} + \text{..... ,}$$

l'autre valeur de $\frac{1}{x}$ serait donc, par ce qui précède,

$$\frac{1}{x} = -\frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a} + \frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a} + \text{..... ,}$$

d'où l'on conclurait, pour l'autre valeur de x,

$$x = -(d + \frac{1}{c} + \frac{1}{b} + \frac{1}{a} + \frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a} + \text{.....,}$$

ou

$$x = -\cfrac{1}{\frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a} + \frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a}} ;$$

ce qui rentre exactement dans notre théorème.

Soit A une fraction continue, immédiatement périodique quelconque, et soit B la fraction continue qu'on en déduit en renversant la période; on voit que, si l'une des racines d'une équa-

p. 298

tion est $x = A$, elle aura nécessairement une autre racine $x = -\frac{1}{B}$; or, si A est un nombre positif plus grand que l'unité, $-\frac{1}{B}$ sera négatif et compris entre 0 et -1; et, à l'inverse, si A est un nombre négatif compris entre 0 et -1, $-\frac{1}{B}$ sera un nombre positif plus grand que l'unité. Ainsi, lorsque l'une des racines d'une équation du second degré est une fraction continue immédiatement périodique, plus grande que l'unité, l'autre est nécessairement comprise entre 0 et -1, et réciproquement si

$$\frac{1}{x} = a + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} + \frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} + \text{.....}\ .$$

The other value of $\frac{1}{x}$ would therefore, by what precedes, be

$$\frac{1}{x} = -\frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a} + \frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a} + \text{.....}\ ,$$

from which one would conclude for the other value of x that

$$x = -(d + \frac{1}{c} + \frac{1}{b} + \frac{1}{a} + \frac{1}{d} + \frac{1}{c} + \frac{1}{b} + \frac{1}{a} + \text{.....},$$

or

$$x = -\cfrac{1}{\cfrac{1}{d} + \cfrac{1}{c} + \cfrac{1}{b} + \cfrac{1}{a} + \cfrac{1}{d} + \cfrac{1}{c} + \cfrac{1}{b} + \cfrac{1}{a}}\ ;$$

which is exactly what enters into our theorem.

Let A be an arbitrary immediately periodic continued fraction, and let B be the continued fraction that one deduces from it by reversing the period. One sees that if one of the roots of an equation

is $x = A$ it will necessarily have another root $x = -\frac{1}{B}$. Now if A is a positive number greater than unity, $-\frac{1}{B}$ will be negative and contained between 0 and -1; and conversely, if A is a negative number contained between 0 and -1, $-\frac{1}{B}$ will be a positive number greater than unity. Thus when one of the roots of an equation of the second degree is an immediately periodic continued fraction greater than unity, the other is necessarily contained between 0 and -1, and conversely, if

l'une d'elles est comprise entre 0 et -1, l'autre sera nécessairement positive et plus grande que l'unité.

On peut prouver que, réciproquement, si l'une des deux racines d'une équation du second degré est positive, est plus grande que l'unité, et que l'autre soit comprise entre 0 et -1, ces racines seront exprimables en fractions continues immédiatement périodiques. En effet, soit toujours A une fraction continue immédiatement périodique quelconque, positive et plus grande que l'unité, et B la fraction continue immédiatement périodique qu'on en déduit, en renversant la période, laquelle sera aussi, comme elle, positive et plus grande que l'unité. La première des racines de la proposée ne pourra être de la forme $x = p + \frac{1}{A}$, car alors, en vertu de notre théorème, la seconde devrait être $x = a + \frac{1}{-\frac{1}{B}} = a - B$; or, $a - B$ ne saurait être compris entre 0 et -1 qu'autant que la partie entière de B serait égale à p; auquel cas, la première valeur serait immédiatement périodique. On ne pourrait avoir davantage, pour la première valeur de x, $x = p + \frac{1}{q} + \frac{1}{A}$, car alors l'autre serait $x = p + \frac{1}{q - B}$ ou $x = p - \frac{1}{B - q}$; or, pour que cette

Corrected in L1846, BA1962 to "positive, et"; P1897 has "positive et".

Misprinted as "entre **0** et **1**" in L1846, P1897.

p. 299

valeur fût comprise entre 0 et -1, il faudrait d'abord que $\frac{1}{B - q}$ fût égal à p plus une fraction; il faudrait donc que $B - q$ fût plus petit que l'unité, ce qui exigerait que B fût égal à q, plus une fraction; d'où l'on voit que q et p devraient être respectivement égaux aux deux premiers termes de la période qui répond à B ou aux deux derniers de la période qui répond à A; de sorte que, contrairement à l'hypothèse, la valeur $x = p + \frac{1}{q} + \frac{1}{A}$ serait immédiatement périodique. On prouverait, par un raisonnement analogue, que les périodes ne sauraient être précédées d'un plus grand nombre de termes n'en faisant pas partie.

Lors donc qu'on traitera une équation numérique par la méthode de Lagrange, on sera sûr qu'il n'y a point de racines périodiques à espérer tant qu'on ne rencontrera pas une transformée ayant au moins une racine positive plus grande que l'unité, et une autre comprise entre 0 et -1; et si, en effet, la racine que l'on poursuit doit être périodique, ce sera tout au plus à cette transformée que les périodes commenceront.

Si l'une des racines d'une équation du second degré est non seulement immédiatement périodique mais encore symétrique, c'est-à-dire, si les termes de la période sont égaux à égale distance des extrêmes, on aura $B = A$; de sorte que ces deux racines seront A et $-\frac{1}{A}$; l'équation sera donc

$$Ax^2 - (A^2 - 1)x - A = 0\,.$$

one of them is contained between 0 and -1, the other will necessarily be positive and greater than unity.

One can prove that conversely, if one of the two roots of an equation of the second degree is positive and greater than unity, and if the other is contained between 0 and -1, the roots will be expressible as immediately periodic continued fractions. Indeed, let A always be an immediately periodic continued fraction, positive and greater than unity, and B the immediately periodic continued fraction that one deduces from it by reversing the period, which will likewise be positive and greater than unity. The first of the roots of the proposed equation could not be of the form $x = p + \dfrac{1}{A}$, for then, in virtue of our theorem, the second would have to be $x = a + \dfrac{1}{-\dfrac{1}{B}} = a - B$; however, $a - B$ could not be contained between 0 and -1 unless the integer part of B was equal to p; in which case the first value would be immediately periodic. Further, for the first value of x one could not have $x = p + \dfrac{1}{q + \dfrac{1}{A}}$, for then the other would be $x = p + \dfrac{1}{q - B}$ or $x = p - \dfrac{1}{B - q}$; however, in order that this value should be contained between 0 and -1 it would first be necessary that $\dfrac{1}{B - q}$ was equal to p plus a fraction; then it would be necessary that $B - q$ was smaller than unity, which requires that B was equal to q plus a fraction; from which it may be seen that q and p would have to be equal respectively to the first two terms of the period corresponding to B, or to the last two of the period corresponding to A; so that, contrary to hypothesis, the value $x = p + \dfrac{1}{q + \dfrac{1}{A}}$ would be immediately periodic. It may be proved by analogous reasoning that the periods cannot be preceded by a greater number of terms not forming a part of it.

Therefore when one treats a numerical equation by the method of Lagrange one will be sure that one cannot hope for any periodic roots as long as one does not come across a transformed equation having at least one root positive and greater than unity and another contained between 0 and -1; and if, indeed, the root one is seeking should be periodic it will be at most at this transformed one that the periods will begin.

If one of the roots of an equation of the second degree is not only immediately periodic but also symmetric, that is to say, if the terms of the period are equal at equal distances from the extremes, one will have $B = A$, so that these two roots will be A and $-\dfrac{1}{A}$. The equation will therefore be

$$Ax^2 - (A^2 - 1)x - A = 0\,.$$

Réciproquement, toute équation du second degré de la forme

$$ax^2 - bx - a = 0\,,$$

aura ses racines à la fois immédiatement périodiques et symétriques. En effet, en mettant tour à tour pour x l'infini et -1, on

p. 300

obtient des résultats positifs, tandis qu'en faisant $x = 1$ et $x = 0$, on obtient des résultats négatifs; d'où l'on voit d'abord que cette équation a une racine positive plus grande que l'unité et une racine négative comprise entre 0 et -1, et qu'ainsi ces racines sont immédiatement périodiques; de plus, cette équation ne change pas en y changeant x en $-\frac{1}{x}$; d'où il suit que si A est une de ses racines l'autre sera $-\frac{1}{A}$, et qu'ainsi, dans ce cas, $B = A$.

Appliquons ces généralités à l'équation du second degré

$$3x^2 - 16x + 18 = 0\,;$$

on lui trouve d'abord une racine positive comprise entre 3 et 4; en posant

Corrected by Liouville to $x = 3 + \frac{1}{y}$.

$$x = 3x + \frac{1}{y}$$

on obtient la transformée

$$3y^2 - 2y - 3 = 0\,,$$

dont la forme nous apprend que les valeurs de y sont à la fois immédiatement périodiques et symétriques; en effet, en posant, tour à tour,

$$y = 1 + \frac{1}{z}\,, \qquad z = 1 + \frac{1}{t}\,, \qquad t = 1 + \frac{1}{u}\,,$$

on obtient les transformées

$$2z^2 - 4z - 3 = 0\,,$$
$$3t^2 - 4t - 2 = 0\,,$$
$$3u^2 - 2u - 3 = 0\,,$$

p. 301

l'identité entre les équations en u et en y prouve que la valeur positive de y est

Misprint corrected in L1846: the minus sign is removed.

$$y = -\frac{1}{2} + \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \text{.....}$$

Conversely, every equation of the second degree of the form

$$ax^2 - bx - a = 0\,,$$

will have its roots both immediately periodic and symmetric. Indeed, setting in turn x to be infinity and -1, one

gets positive results, while putting $x = 1$ and $x = 0$ one obtains negative results, from which one sees straightaway that this equation has a root that is positive and greater than unity and a root that is negative and contained between 0 and -1, and that therefore these roots are immediately periodic; moreover, this equation is not changed on changing x to $-\dfrac{1}{x}$, from which it follows that if A is one of its roots the other will be $-\dfrac{1}{A}$, and that therefore in this case $B = A$.

Let us apply these generalities to the equation of the second degree

$$3x^2 - 16x + 18 = 0\,.$$

One first finds a positive root of it contained between 3 and 4. On setting

$$x = 3 + \frac{1}{y}$$

one obtains the transformed equation

$$3y^2 - 2y - 3 = 0$$

whose form tells us that the values of y are both immediately periodic and symmetric. Indeed, setting in turn

$$y = 1 + \frac{1}{z}\,, \qquad z = 1 + \frac{1}{t}\,, \qquad t = 1 + \frac{1}{u}\,,$$

one gets the transformed equations

$$\begin{aligned} 2z^2 - 4z - 3 &= 0\,,\\ 3t^2 - 4t - 2 &= 0\,,\\ 3u^2 - 2u - 3 &= 0\,. \end{aligned}$$

The identity of the equations in u and in y proves that the positive value of y is

$$y = \frac{1}{2} + \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \ldots\ldots$$

sa valeur négative sera donc

$$y = -\frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \ldots\ldots$$

les deux valeurs de x seront donc

$$x = 3 + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \ldots.$$

$$x = 3 - \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \ldots\ldots$$

dont la dernière, en vertu de la formule connue

$$p - \frac{1}{q} = p - 1 + \frac{1}{1} + \frac{1}{q-1},$$

devient

$$x = 1 + \frac{1}{1} + \frac{1}{1} + \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \ldots \quad (*)$$

(*) On trouve diverses recherches sur le même sujet, dans le présent recueil, tom. IX, pag. 261, tom. XIV, pag. 324 et 337.

J. D. G.

Its negative value will therefore be

$$y = -\frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \ldots\ldots$$

The two values of x will therefore be

$$x = 3 + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \ldots.$$

$$x = 3 - \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \ldots\ldots$$

of which the latter, in virtue of the known formula

$$p - \frac{1}{q} = p - 1 + \frac{1}{1} + \frac{1}{q-1},$$

becomes

$$x = 1 + \frac{1}{1} + \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \ldots \quad (*)$$

(*) Several researches on the same subject may be found in the present collection Vol. IX, p. 261, Vol. XIV, pp. 324 and 337.

J. D. G.

II.2 Abstract of an article on the algebraic solution of equations

The note 'Analyse d'un Mémoire sur la résolution algébrique des équations' is extracted from *Bulletin des Sciences Mathématiques, Physiques et Chimiques* (Férussac's *Bulletin*), Vol. 13, pp. 271–272 (April 1830). It is reprinted in [Liouville (1846), pp. 395–396], in [Picard (1897), pp. 11–12], and in [B & A (1962), pp. 162–165]. A manuscript which is very probably a first draft of the first half survives as **f.94a** in Dossier 18 (see p. 323 below).

In this paper Galois announced results, some of which are treated in the *Second Mémoire*, some in the *Lettre testamentaire*. For a detailed analysis of the meaning of the word *primitif* and of the reference to Gauss see [Neumann (2006)]. The first and second assertions of the note are famous theorems of Galois; the third is wrong, as Galois himself recognised when he wrote in the *Lettre testamentaire* (**f.9a**, p. 88 below):

> La condition que j'ai indiquée dans le bulletin ferussac pour que l'équation soit soluble par radicaux est trop restreinte. Il y a peu d'exceptions, mais il y en a.
>
> [The condition that I indicated in Férussac's *Bulletin* for the equation to be soluble by radicals is too restrictive. There are few exceptions, but there are some.]

In fact it is very far from correct—the claim that there are only few exceptions does not bear close examination. I believe, however, that it was an inspiration to Camille Jordan in the 1860s—but this is the subject of a planned article that I hope to write if and when time permits.

The last paragraph of the note is expanded, corrected and explained in the *Lettre testamentaire*, **f.9b**, pp. 88, 90 below.

It was tempting to replace such notation as $a = b \pmod{c}$ with $a \equiv b \pmod{c}$ for the English version. Following the advice of a referee, I have not done so. Although the former is unusual nowadays, it is perfectly clear what it means.

p. 271

138. Analyse d'un Mémoire sur la résolution algébrique des équations; par M. E. Galois.

On appelle équations non-primitives les équations qui étant, par exemple, du degré $m\,n$, se décomposent en m facteurs du degré n, au moyen d'une seule équation du degré m. Ce sont les équations de M. Gauss. Les équations primitives sont celles qui ne jouissent pas d'une pareille simplification. Je suis, à l'égard des équations primitives, parvenu aux résultats suivans.

1° Pour qu'une équation de degré premier soit résoluble par radicaux, il faut et il suffit que deux quelconques de ses racines étant connues, les autres s'en déduisent rationnellement.

2° Pour qu'une équation primitive du degré m soit résoluble par radicaux, il faut que $m = p^\nu$, p étant un nombre premier.

Misprint 'ci-dessus' corrected to 'ci-dessous' in L1846 (misquoted as 'au-dessous' in BA1962).

3° A part les cas mentionnés ci-dessus, pour qu'une équation primitive du degré p^ν soit résoluble par radicaux, il faut que deux quelconques de ses racines étant connues, les autres s'en déduisent rationnellement.

A la règle précédente échappent les cas très-particuliers qui suivent:

1° le cas de $m = p^\nu = 9, = 25$.

2° le cas de $m = p^\nu = 4$, et généralement celui où a^α étant un diviseur de $\dfrac{p^\nu - 1}{p-1}$ on aurait, a premier et

p. 272

$$\frac{p^\nu - 1}{a^\alpha (p-1)}\, \nu = p. \qquad (\text{mod. } a^\alpha).$$

Ces cas s'écartent toutefois fort peu de la règle générale.

Quand $m = 9, = 25$, l'équation devra être du genre de celles qui déterminent la trisection et la quintisection des fonctions elliptiques.

Dans le second cas, il faudra toujours que deux des racines étant connues, les autres s'en déduisent, du moins au moyen d'un nombre de radicaux du degré p, égal au nombre des diviseurs a^α de $\dfrac{p^\nu - 1}{p-1}$ qui sont tels que

$$\frac{p^\nu - 1}{a^\alpha (p-1)}\, \nu = p \qquad (\text{mod. } a^\alpha) \qquad a \text{ premier.}$$

Toutes ces propositions ont été déduites de la théorie des permutations

Voici d'autres résultats qui découlent de ma théorie.

Analysis of a Memoir on the algebraic solution of equations; by Mr E. Galois.

Those equations which, being, for example of degree mn, decompose into m factors of degree n by means of a single equation of degree m, are called non-primitive equations. These are the equations of Mr Gauss. The primitive equations are those which do not enjoy such a simplification. With regard to primitive equations I have been led to the following results.

1. In order that an equation of prime degree should be soluble by radicals it is necessary and sufficient that, given any two of its roots, the others may be deduced rationally from them.

2. In order that a primitive equation of degree m be soluble by radicals, it is necessary that $m = p^\nu$, p being a prime number.

3. Apart from the cases mentioned below, in order that a primitive equation of degree p^ν be soluble by radicals, it is necessary that, given any two of its roots, the others may be deduced rationally from them.

Misprint 'above' corrected to 'below'.

The following very special cases escape from the preceding rule:

1. the case of $m = p^\nu = 9,\ = 25$.

2. the case of $m = p^\nu = 4$, and generally that where, a^α being a divisor of $\dfrac{p^\nu - 1}{p - 1}$, one has a prime and

$$\frac{p^\nu - 1}{a^\alpha (p-1)} \nu = p \ (\mathrm{mod}\, a^\alpha)\,.$$

These cases deviate rather little from the general rule however.

When $m = 9,\ = 25$, the equation must be of the kind of those which determine the trisection and the quintisection of elliptic functions.

In the second case, it is still necessary that, given any two of the roots, the others may be deduced rationally from them, at least by means of a number of radicals of degree p equal to the number of divisors a^α of $\dfrac{p^\nu - 1}{p - 1}$ which are such that

$$\frac{p^\nu - 1}{a^\alpha (p-1)} \nu = p \ (\mathrm{mod}\, a^\alpha), \qquad a \text{ prime.}$$

All these propositions have been deduced from the theory of permutations.

Here are some other results which may be derived from my theory.

1° Soit k le module d'une fonction elliptique, p un nombre premier donné > 3; pour que l'équation du degré $p + 1$ qui donne les divers modules des fonctions transformées relativement au nombre p, soit résoluble par radicaux, *il faut* de deux choses l'une, ou bien qu'une des racines soit rationnellement connue, ou bien que toutes soient des fonctions rationnelles les unes des autres. Il ne s'agit ici, bien entendu, que des valeurs particulières du module k. Il est évident que la chose n'a pas lieu en général. Cette règle n'a pas lieu pour $p = 5$.

2° Il est remarquable que l'équation modulaire générale du 6e degré, correspondant au nombre 5, peut s'abaisser à une du 5e degré dont elle est la réduite. Au contraire, pour des degrés supérieurs, les équations modulaires ne peuvent s'abaisser.

1. Let k be the modulus of an elliptic function, p a given prime number > 3; in order that the equation of degree $p + 1$ which gives the various moduli of the transformed functions relative to the number p should be soluble by radicals, one of two things is *necessary*: either that one of the roots should be rationally known, or that all should be rational functions of each other. Of course we are concerned here only with special values of the modulus k. It is clear that the fact does not hold in general. The rule does not hold for $p = 5$

2. It is worthy of note that the general modular equation of degree 6, corresponding to the number 5, can be reduced to one of the 5^{th} degree of which it is the reduced equation. By contrast, for higher degrees the modular equations cannot be reduced.

II.3 A note on the numerical solution of equations

We present here the original version of this note extracted from *Bulletin des Sciences Mathématiques, Physiques et Chimiques* (Férussac's *Bulletin*), Vol. 13, pp. 428–435 (June 1830). It was reprinted in [Liouville (1846), pp. 397–398], [Picard (1897), pp. 13–14], and in [B & A (1962), pp. 378–381]. One typographical idiosyncracy of the *Bulletin* that I have been unable to reproduce is the use of the letter V turned 90° one way or the other to stand for $<$ or $>$. Curiously, this was not universal. The printer had perfectly good $<$ and $>$ symbols that he used most of the time.

The reference to Legendre with which the article opens is identified by Massimo Galuzzi (see [Galuzzi (2001)]) as being to the third chapter of the supplement [Legendre (1816)] to the second edition (1808) of Legendre's great *Essai sur la théorie des nombres*. But then the first paragraph of Galois' article is pretty unfair on his readers. The only direct contact with Legendre's exposition is that his *fonction omale*, which he defines as a monotonic function, increasing or decreasing, is what for Galois is a *fonction de x qui croît constamment en même temps que x*, a function of x that grows constantly as x does. Beyond that the connections have to be made through a considerable amount of interpretation. Legendre, for example, did not put his equations into such a simple form as $\varphi x = x$. Nevertheless, Galuzzi makes a good and convincing case—and I am most grateful to him for drawing my attention to it.

In a private communication Professor Galuzzi suggests that Galois may have come across the approximation method in Cauchy's *Cours d'Analyse* rather than, or as well as, in [Legendre (1816)]. In [Cauchy (1821), Note III, p. 464*ff*] (see also [B & S (2009), p. 312*ff*]), there is a modification of Legendre's method for finding approximations to the roots of an equation $f(x) = 0$. In effect it requires writing $f(x) = \varphi(x) - \chi(x)$, where both φ, χ are continuous and monotonic increasing, and then using an iterative method to seek solutions of the equation $\varphi(x) = \chi(x)$. It seems likely that Galois had read this exposition by Cauchy at some time. But the 1816 supplement to Legendre (1808) was reprinted with only minimal changes as the first section, Articles (1)–(41), of the appendix to [Legendre (1830)], and although I have not been able to track down the exact publication date, it was early enough in 1830 that a substantial review could appear in the August issue of Férussac's *Bulletin*, 14 (1830), pp. 90–93. Thus, even although he may well have considered the matter at some earlier time, it seems a good possibility that Galois was stimulated to write his note by seeing this new edition of Legendre's book.

p. 413

216. Note sur la résolution des équations numériques; par M. E. Galois.

M. Legendre a le premier remarqué que, lorsqu'une équation algébrique était mise sous la forme

$$\varphi x = x$$

où φx est une fonction de x qui croît constamment en même temps que x, il était facile de trouver la racine de cette équation immédiatement plus petite qu'un nombre donné a, si $\varphi a < a$, et la racine immédiatement plus grande que a, si $\varphi a > a$.

Pour le démontrer, on construit la courbe $y = \varphi x$ et la droite $y = x$. Soit prise une abscisse $= a$, et supposons, pour fixer les idées, $\varphi a > a$, je dis qu'il sera aisé d'obtenir la racine immédiatement supérieure à a. En effet, les racines de l'équation $\varphi x = x$ ne sont que les abscisses des points d'intersection de la droite et de la courbe, et il est clair que l'on s'approchera du point le plus voisin d'intersection, en substituant à l'abscisse a l'abscisse φa. On aura une valeur plus approchée encore en prenant $\varphi\varphi a$, puis $\varphi\varphi\varphi a$, et ainsi de suite.

Soit $\mathrm{F}x = o$ une équation donnée du degré n, et $\mathrm{F}x = \mathrm{X} - \mathrm{Y}$, X et Y n'ayant que des termes positifs. M. Legendre met successivement l'équation sous ces deux formes

$$x = \varphi x = \sqrt[n]{\frac{\mathrm{X}}{\left(\frac{\mathrm{Y}}{x^n}\right)}} \qquad x = \psi x = \sqrt[n]{\frac{\mathrm{X}}{\left(\frac{x^n}{\mathrm{Y}}\right)}}$$

Massimo Galuzzi has observed that the second formula is misprinted. It should be the same as the first except for interchange of X and Y.

les deux fonctions φx et ψx sont toujours, comme on voit, l'une plus grande, l'autre plus petite que x. Ainsi à l'aide de ces deux fonctions, on pourra avoir les deux racines de l'équation les plus approchées d'un nombre donné a, l'une en plus et l'autre en moins.

Mais cette méthode a l'inconvénient d'exiger à chaque opération l'extraction d'une racine n$^{\text{ième}}$. Voici deux formes plus commodes. Cherchons un nombre k tel, que la fonction

Misprint n for n.

$$x + \frac{\mathrm{F}x}{k\,x^n}$$

croisse avec x, quand $x > 1$. (Il suffit, en effet, de savoir trouver les racines d'une équation qui sont plus grandes que l'unité.)

Nous aurons pour la condition proposée

p. 414

$$1 + \frac{d\,\frac{\mathrm{X}-\mathrm{Y}}{kx^n}}{dx} > 0 \qquad \text{ou bien} \quad 1 - \frac{n\mathrm{X} - x\mathrm{X}'}{k\,x^{n+1}} + \frac{n\mathrm{Y} - x\mathrm{Y}'}{k\,x^{n+1}} > 0$$

216. Note on the solution of numerical equations; by Mr E. Galois.

Mr Legendre was the first to notice that when an algebraic equation was put in the form

$$\varphi x = x$$

where φx is a function of x that grows constantly at the same time as x does, it was easy to find the root of this equation immediately smaller than a given number a if $\varphi a < a$, and the root immediately greater than a if $\varphi a > a$.

To show this one constructs the curve $y = \varphi x$ and the straight line $y = x$. Let an abscissa $= a$ be taken, and suppose, to fix ideas, that $\varphi a > a$. I say that it will be easy to obtain the root immediately above a. Indeed, the roots of the equation $\varphi x = x$ are nothing other than the abscissae of the points of intersection of the straight line and the curve, and it is clear that one will approach the point which is nearest neighbour to the intersection by substituting for the abscissa a the abscissa φa. One will have a value even closer by taking $\varphi\varphi a$; then $\varphi\varphi\varphi a$; and so on.

Let $Fx = 0$ be a given equation of degree n, and $Fx = X - Y$, where X and Y have only positive terms. Mr Legendre puts the equation successively into these two forms:

$$x = \varphi x = \sqrt[n]{\frac{X}{\left(\frac{Y}{x^n}\right)}}, \qquad x = \psi x = \sqrt[n]{\frac{Y}{\left(\frac{X}{x^n}\right)}}.$$

Misprint corrected: see opposite.

As can be seen, the two functions φx and ψx are always, the one greater, the other smaller, than x. Thus with the aid of these two functions, one may get the two roots of the equation closest to a given number a, the one greater, the other less.

But this method has the disadvantage of requiring the extraction of an n^{th} root at each step. Here are two more convenient forms. Seek a number k such that the function

$$x + \frac{F x}{k\, x^n}$$

is increasing when $x > 1$. (Indeed, it is enough to know how to find the roots of an equation which are greater than unity.)

For the proposed condition we will have

$$1 + \frac{d\,\frac{X - Y}{k x^n}}{dx} > 0 \qquad \text{that is,} \quad 1 - \frac{nX - xX'}{k\, x^{n+1}} + \frac{nY - xY'}{k\, x^{n+1}} > 0\,.$$

Sentences merged without punctuation in the original.

or on a identiquement

$$nX - xX' > 0 \qquad\qquad nY - xY' > 0$$

il suffit donc de poser

$$\frac{nX - X'x}{k\,x^{n+1}} < 1 \qquad \text{pour } x > 1$$

et il suffit pour cela de prendre pour k la valeur de la fonction $nX - X'x$ relative à $x = 1$.

On trouvera de même un nombre h tel que la fonction

$$x - \frac{Fx}{h\,x^n}$$

croîtra avec x quand x sera > 1, en changeant Y en X.

Ainsi l'équation donnée pourra se mettre sous l'une des formes

$$x = x + \frac{Fx}{k\,x^n} \qquad\qquad x = x - \frac{Fx}{h\,x^n}$$

qui sont toutes deux rationnelles, et donnent pour la résolution une méthode facile.

Now one has identically

$$nX - xX' > 0\,, \qquad nY - xY' > 0\,.$$

It therefore suffices to set

$$\frac{nX - X'x}{k\,x^{n+1}} < 1 \quad \text{for } x > 1\,,$$

and for that it suffices to take k to be the value of the function $nX - X'x$ relative to $x = 1$.

Similarly, by exchanging Y for X, one will find a number h such that the function

$$x - \frac{F\,x}{h\,x^n}$$

grows with x when $x > 1$.

In this way the given equation can be put into one of the forms

$$x = x + \frac{F\,x}{k\,x^n}\,, \qquad x = x - \frac{F\,x}{h\,x^n}\,,$$

both of which are rational and give an easy method of solution.

II.4 On the theory of numbers

We present here the original version of this paper extracted from *Bulletin des Sciences Mathématiques, Physiques et Chimiques* (Férussac's *Bulletin*), Vol. 13, pp. 428–435 (June 1830). It was reprinted in [Liouville (1846), pp. 398–407], [Picard (1897), pp. 15–23], and in [B & A (1962), pp. 112–127]. As with the other published articles, it has not been easy to copy the original faithfully, even allowing for the differences between the typography of 1830 and our time. Some of the obscurities in the original are simple misprints, including confusion in formulae between *o* and 0, etc. Misprints p_ν or $p\nu$ for p^ν, are hard to distinguish because the printer uses a small letter ν set, like many Greek letters, slightly below the line of type. Moreover, random sizes of letters are used: the formula x^{p^ν}, for example, is rendered variously as $x^{p^{\nu}}$, $x^{p\nu}$, x^{p}_{ν}, and it is a moot point whether the second of these was designed by the printer to be $x^{p\nu}$, which would have been a simple misprint.

In addition to typographical obscurities and misprints there are mathematical difficulties where Galois made a slip in his treatment of the example of a primitive root in the field of size 7^3 and then continued his miscalculation. The errors were corrected without comment by Liouville in his 1846 edition. Although my transcription copies the original as closely as possible (subject to modern typographical constraints and my personal sensibilities), the English translation is based on the corrected French version.

I have not found it easy to identify all the external references in this paper. The mention of Gauss in the first paragraph is clear enough. This should be to the first four parts of *Disquisitiones* [Gauss (1801)], although I find no explicit use of the notation $F\,x \equiv 0$ there. The paragraph *Ensuite on prouvera, ..., toute la suite des autres racines* (p. 64), in which Galois explains the existence of a primitive root (a generator of the multiplicative group) in the Galois field of size p^ν, clearly refers to the fact that there is always a primitive root modulo a prime number. According to [Gauss (1801), § 56] and [Dickson (1919), p. 181] this existence had been recognised by Lambert in 1769 and by Euler in 1773. Proofs appeared in Legendre's *Essai sur la théorie des nombres* [Legendre (1798/1808), § 341–2] and in Gauss's *Disquisitiones* [Gauss (1801), §§ 52–56] and Galois would surely have been familiar with these treatments—and would have assumed that his reader was familiar with them too. The phrase *la méthode de M. Gauss* must have a very different meaning at p. 68 from its meaning in the *Lettre testamentaire* **f.8b** (p. 86), and it is not clear to me what Galois had in mind at this point. On p. 70 *la formule de Newton* is simply the Binomial Theorem (for positive integer exponents). Although I have not studied the issue carefully enough to be certain, it seems possible that the mention of Libri on p. 72 refers either to [Libri (1830)] or to [Libri (1833), pp. 18–26]. The latter bears a publication date three years later than that of Galois, but it is annotated as having been read at the Académie des Sciences on 15 June 1825, so it is entirely possible that Galois knew something of its contents.

p. 428

218. Sur la théorie des nombres; par M. Galois.

(Ce mémoire fait partie des recherches de M. Galois sur la théorie des permutations et des équations algébriques).

Quand on convient de regarder comme nulles toutes les quantités qui, dans les calculs algébriques, se trouvent multipliées par un nombre premier donné p, et qu'on cherche dans cette convention les solutions d'une équation algébrique $\mathrm{F}x = o$, ce que M. Gauss désigne par la notation $\mathrm{F}x \equiv o$, on n'a coutume de considérer que les solutions entières de ces sortes de questions. Ayant été conduit par des recherches particulières à considérer les solutions incommensurables, je suis parvenu à quelques résultatsque je crois nouveaux.

Interword space missing in original.

Soit une pareille équation ou congruence, $\mathrm{F}x = o$ et p le module. Supposons d'abord, pour plus de simplicité, que la congruence en question n'admette aucun facteur commensurable, c'est-à-dire qu'on ne puisse pas trouver 3 fonctions φx, ψx, χx telles que

$$\varphi x \,.\, \psi x = \mathrm{F}x + p\,\chi x\,.$$

Dans ce cas, la congruence n'admettra donc aucune racine entière, ni même aucune racine incommensurable du degré inférieur. Il faut donc regarder les racines de cette congruence comme des espèces de symboles imaginaires, puisqu'elles ne satisfont pas aux questions de nombres entiers, symboles dont l'emploi dans le calcul sera souvent aussi utile que celui de l'imaginaire $\sqrt{-1}$ dans l'analyse ordinaire.

C'est la classification de ces imaginaires et leur réduction au plus petit nombre possible, qui va nous occuper.

Appelons i l'une des racines de la congruence $\mathrm{F}x = o$, que nous supposerons du degré ν.

Considérons l'expression générale

$$a + a_1 i + a_2 i^2 + \ldots\ldots\ldots + a_{\nu-1} i^{\nu-1} \quad \text{(A)}$$

où $a \;\; a_1 \;\; a_2 \;\ldots\ldots\; a_{\nu-1}$ représentent des nombres entiers. En donnant à ces nombres toutes les valeurs, l'expression (A) en acquiert p^ν, qui jouissent, ainsi que je vais le faire voir, des mêmes propriétés que les nombres naturels dans la *théorie des résidus des puissances*.

Otiose comma in original.

Ne prenons des expressions (A) que les $p^\nu - 1$, valeurs où $a \;\; a_1 \;\; a_2 \;\ldots\; a_{\nu-1}$ ne sont pas toutes nulles: soit α l'une de ces expressions.

p. 429

Si l'on élève successivement α aux puissances 2^{e} 3^{e} …, on aura une suite de quantités de même forme (parce que toute fonction de i peut se réduire au $\nu - 1^{\mathrm{e}}$ degré). Donc on devra avoir $\alpha^n = 1$, n étant un certain nombre, soit n le plus petit

On the theory of numbers; by Mr Galois.

(This memoir forms part of the research by Mr Galois on the theory of permutations and algebraic equations.)

When one agrees to treat as zero all quantities in algebraic calculations which are multiplied by a given prime number p, and under this convention one looks for the solutions of an algebraic equation $Fx = 0$, which Mr Gauss writes using the notation $Fx \equiv 0$, it is customary to consider only integer solutions to this sort of question. Having been led by a particular line of research to consider incommensurable solutions I have come across some results that I believe to be new.

Let $Fx = 0$ be such an equation or congruence, and let p be the modulus. First let us suppose for simplicity that the congruence in question does not admit any commensurable factors, that is to say, that one cannot find 3 functions φx, ψx, χx such that

$$\varphi x.\psi x = Fx + p\,\chi x\,.$$

In this case, then, the congruence will have no integer root, nor even any incommensurable roots of lower degree. One must therefore think of the roots of this congruence as a species of imaginary symbols because they do not answer questions about whole numbers, symbols whose deployment in calculations will often be just as useful as that of the imaginary $\sqrt{-1}$ in ordinary analysis.

It is the classification of these imaginaries, and their reduction to the smallest possible number, that will occupy us.

Let us call i one of the roots of the congruence $Fx = 0$, which we suppose of degree ν.

Consider the general expression

$$a + a_1 i + a_2 i^2 + \cdots + a_{\nu-1} i^{\nu-1} \quad \text{(A)}$$

where $a, a_1, a_2, \ldots, a_{\nu-1}$ represent whole numbers. Giving to these numbers all their values, the expression (A) takes p^ν of them, which, as I shall show, enjoy the same properties as natural numbers in the theory of residues of powers.

Take only the $p^\nu - 1$ values of the expression (A) where $a, a_1, a_2, \ldots, a_{\nu-1}$ are not all zero: let α be one of these expressions.

If one raises α successively to the 2^{nd}, 3^{rd}, ... powers one will have a sequence of quantities of the same form (because every function of i can be reduced to the $(\nu-1)^{\text{th}}$ degree). Therefore one must have $\alpha^n = 1$, n being some number. Let n be the smallest

nombre qui soit tel que l'on ait $\alpha^n = 1$. On aura un ensemble de n expressions toutes différentes entr'elles.

$$1 \quad \alpha \quad \alpha^2 \quad \alpha^3 \quad . \quad . \quad . \quad \alpha^{n-1}$$

The original uses an old-style β that I have been unable to reproduce faithfully.

Multiplions ces n quantités par une autre expression β de la même forme. Nous obtiendrons encore un nouveau groupe de quantités toutes différentes des premières et différentes entr'elles. Si les quantités (A) ne sont pas épuisées, on multipliera encore les puissances de α par une nouvelle expression γ, et ainsi de suite. On voit donc que le nombre n divisera nécessairement le nombre total des quantités (A). Ce nombre étant $p_\nu - 1$, on voit que n divise $p\nu - 1$. De là, suit encore que l'on aura

Misprints $p_\nu - 1$ (or possibly $p\nu - 1$) and $p\nu - 1$ corrected to $p^\nu - 1$ in L1846.

$$\alpha^{p^\nu - 1} = 1 \qquad \text{ou bien} \quad \alpha^{p^\nu} = \alpha\,.$$

Ensuite on prouvera, comme dans la théorie des nombres, qu'il y a des racines primitives α pour lesquelles on ait précisément $p^\nu - 1 = n$, et qui reproduisent par conséquent, par l'élévation aux puissances, toute la suite des autres racines.

Et l'une quelconque de ces racines primitives ne dépendra que d'une congruence du degré ν, congruence *irréductible*, sans quoi l'équation en i ne le serait pas non plus, parce que les racines de la congruence en i sont toutes des puissances de la racine primitive.

On voit ici cette conséquence remarquable, que toutes les quantités algébriques qui peuvent se présenter dans la théorie, sont racines d'équations de la forme

$$x^{p^\nu} = x$$

Changed in L1846 to 'Étant donnés'.

Cette proposition énoncée algébriquement, est celle-ci. Étant donné une fonction $\mathrm{F}\,x$ et un nombre premier p, on peut poser

$$f\,x\,.\,\mathrm{F}\,x = x^{p^\nu} - x + p\,\varphi\,x$$

$f\,x$ et $\varphi\,x$ étant des fonctions entières, toutes les fois que la congruence $\mathrm{F}\,x \equiv o \pmod{p}$ sera irréductible.

Si l'on veut avoir toutes les racines d'une pareille congruence

p. 430

au moyen d'une seule, il suffit d'observer que l'on a généralement

$$\left(\mathrm{F}\,x\right)^{p^n} = \mathrm{F}\left(x^{p^n}\right)$$

et que par conséquent l'une des racines étant x, les autres seront

number with the property that one has $\alpha^n = 1$. One will have a collection of n expressions all different from one another

$$1, \quad \alpha, \quad \alpha^2, \quad \alpha^3, \quad \ldots, \quad \alpha^{n-1}.$$

Multiply these n quantities by another expression β of the same form. We will obtain again a new group of quantities all different from the first and different from each other. If the quantities (A) are not all exhausted, one will again multiply the powers of α by a new expression γ, and so on. One sees thus that the number n will necessarily divide the total number of quantities (A). This number being $p^\nu - 1$, one sees that n divides $p^\nu - 1$. It then follows that one will have

$$\alpha^{p^\nu - 1} = 1 \quad \text{or equally} \quad \alpha^{p^\nu} = \alpha .$$

Then one proves, as in the theory of numbers, that there are primitive roots α for which one has $p^\nu - 1 = n$ precisely, and which consequently reproduce the whole sequence of the other roots on being raised to powers.

And any one of these primitive roots depends only on a congruence of degree ν, which is an *irreducible* congruence otherwise the equation for i would not be either, because all the roots of the congruence for i are powers of the primitive root.

One sees now the remarkable consequence that all the algebraic quantities which can appear in the theory are roots of equations of the form

$$x^{p^\nu} = x .$$

Expressed algebraically this proposition is the following. Given a function $\mathrm{F}\,x$ and a prime number p, whenever the congruence $\mathrm{F}\,x \equiv 0 \pmod{p}$ is irreducible one can set

$$f\,x \,.\, \mathrm{F}\,x = x^{p^\nu} - x + p\,\varphi\,x$$

$f\,x$ and $\varphi\,x$ being entire functions [polynomials].

If one wants to have all the roots of such a congruence

by means of a single one, it suffices to observe that generally one has

$$(F\,x)^{p^n} = F(x^{p^n})$$

and consequently x being one of the roots, the others will be

$$x^p \qquad x^{p^2} \qquad \ldots . x^{p^{\nu-1}} \qquad (1)$$

Il s'agit maintenant de faire voir que, réciproquement à ce que nous venons de dire, les racines de l'équation ou de la congruence $x^{p^\nu} = x$ dépendront toutes d'une seule congruence du degré ν.

Soit en effet i une racine d'une congruence irréductible, et telle que toutes les racines de la congruence $x^{p^\nu} = x$ soient fonctions rationnelles de i. (Il est clair qu'ici, comme dans les équations ordinaires, cette propriété a lieu) (2).

Il est d'abord évident que le degré μ de la congruence en i

(1) De ce que les racines de la congruence irréductible de degré ν,

$$\mathrm{F}\, x = 0$$

sont exprimées par la suite

$$x \quad x^p \quad x^{p^2} \quad .. x^{p^{r-1}}$$

Misprint corrected to $x^{p^\nu - 1}$ in all editions.

on aurait tort de conclure que ces racines soient toujours des quantités exprimable par radicaux. Voici un exemple du contraire:

La congruence irréductible

$$x^2 + x + 1 = 0 \qquad (\text{mod. } 2)$$

donne

$$x = \frac{-1 + \sqrt{-3}}{2}$$

qui se réduit

$$\frac{0}{0} \qquad (\text{mod. } p)$$

Misprint corrected to (mod. 2) in L1846.

formule qui n'apprend rien.

(2) La proposition générale dont il s'agit ici peut s'énoncer ainsi: étant donnée une équation algébrique, on pourra trouver une fonction rationnelle θ de toutes ses racines, de telle sorte, que réciproquement chacune des racines s'exprime rationnellement en θ. Ce théorême était connu d'Abel, ainsi qu'on peut le voir par la première partie du mémoire que ce célèbre géomètre a laissé sur les fonctions elliptiques.

Misprint for 'théorème' corrected in all editions.

p. 431

ne saurait être plus petit que ν, sans quoi la conguence

$$x^{p^\nu - 1} - 1 = 0\,. \qquad (\nu)$$

aurait toutes ses racines communes avec la congruence

$$x^{p^\mu - 1} - 1 = 0$$

ce qui est absurde, puisque la congruence (ν) n'a pas de racines égales, comme on le voit en prenant la dérivée du premier membre. Je dis maintenant que μ ne peut non plus être $> \nu$.

En effet, s'il en était ainsi, toutes les racines de la congruence

Read as $x^{p\mu} = x$ in L1846

$$x^{p\mu} = x$$

$$x^p, \quad x^{p^2}, \quad \ldots, \quad x^{p^{\nu-1}}. \quad (1)$$

Our concern now is to show the converse of what we have just said: the roots of the equation or of the congruence $x^{p^\nu} = x$ will all depend on a single congruence of degree ν.

Indeed, let i be a root of an irreducible congruence, and such that all the roots of the congruence $x^{p^\nu} = x$ are rational functions of i. (It is clear that here, as in ordinary equations, this property will hold) (2).

It is clear from the start that the degree μ of the congruence for i

(1) One would be wrong to conclude from the fact that the roots of the irreducible congruence

$$Fx = 0$$

of degree ν are expressed by the sequence

$$x^p \quad x^{p^2} \quad \ldots \quad x^{p^{\nu-1}}$$

that these roots are always quantities expressible by radicals. Here is a counterexample:

The irreducible congruence

$$x^2 + x + 1 = 0 \pmod 2$$

gives

$$x = \frac{-1 + \sqrt{-3}}{2}$$

which reduces to

$$\frac{0}{0} \pmod 2$$

a formula which says nothing.

(2) The general proposition that is relevant here can be formulated thus: given an algebraic equation, one can find a rational function θ of all its roots, of such a kind that conversely each of the roots may be expressed rationally in θ. This theorem was known to Abel as one can see in the first part of the memoir on elliptic functions which this famous geometer has left us.

could not be smaller than ν, otherwise the congruence

$$x^{p^\nu - 1} - 1 = 0 \qquad (\nu)$$

would have all its roots in common with the congruence

$$x^{p^\mu - 1} - 1 = 0,$$

which is absurd because the congruence (ν) has no equal roots, as is seen by taking the derivative of the first member. I say now that also μ cannot be $> \nu$.

Indeed, if it were so then all the roots of the congruence

$$x^{p^\mu} = x$$

devraient dépendre rationnellement de celles de la congruence

$$x^{p^\nu} = x$$

Read as $x^{p^\nu} = x$ in L1846

Mais il est aisé de voir que si l'on a

$$i^{p^\nu} = i$$

Read as $i^{p^\nu} = i$ in L1846. Paragraphing corrected in L1846. Indent removed, capitalisation retained in BA1962.

Toute fonction rationnelle $h = f\,i$ donnera encore

$$\left(f\,i\right)^{p^\nu} = f\left(i^{p^\nu}\right) = f\,i, \quad \text{d'où} \quad h^{p^\nu} = 4$$

The three exponents read as p^ν and last symbol corrected to h in L1846.

Donc toutes les racines de la congruence $x^{p^\mu} = x$ lui seraient communes avec l'équation $x^{p^\nu} = x$. Ce qui est absurde.

Nous savons donc enfin que toutes les racines de l'équation ou congruence $x^{p^\nu} = x$ dépendent nécessairement d'une *seule* congruence *irréductible* de degré ν.

Maintenant, pour avoir cette congruence irréductible d'où dépendent les racines de la conguence $x^{p^\nu} = x$, la méthode la plus générale sera de délivrer d'abord cette congruence de tous les facteurs communs qu'elle pourrait avoir avec des congruences de degré inférieur et de la forme

$$x^{p^\mu} = x$$

On obtiendra ainsi une congruence qui devra se partager en congruences irréductibles de degré ν. Et comme on sait exprimer toutes les racines de chacune de ces congruences irréductibles au moyen d'une seule, il sera aisé de les obtenir toutes par la méthode de M. Gauss.

p. 432

Le plus souvent, cependant, il sera aisé de trouver par le tâtonnement une congruence irréductible d'un degré donné ν, et on doit en déduire toutes les autres.

Soient, par exemple, $p = 7 \quad \nu = 3$. Cherchons les racines de la congruence

$$x^{7^3} = x \qquad \text{(mod. 7.)} \tag{1}$$

J'observe que la congruence

$$i^3 = 2 \qquad \text{(mod. 7.)} \tag{2}$$

étant irréductible et du degré 3, toutes les racines de la congruence (1) dépendent rationnellement de celles de la congruence (2), en sorte que toutes les racines de (1) sont de la forme

$$a + a_1 i + a_2 i^2 \qquad \text{ou bien} \qquad a + a_1 \sqrt[3]{2} + a_2 \sqrt[3]{4} \tag{3}$$

Il faut maintenant trouver une racine primitive, c'est-à-dire une forme de l'expression (3) qui, élevée à toutes les puissances, donne toutes les racines de la congruence

$$x^{7^3-1} = 1 \quad \text{savoir} \quad x^{2^1.3^2.19} = 1 \quad \text{(mod. 7.)}$$

would have to depend rationally on those of the congruence

$$x^{p^\nu} = x\,.$$

But it is easy to see that if one has

$$i^{p^\nu} = i\,,$$

every rational function $h = f\,i$ would yield also

$$(f\,i)^{p^\nu} = f(i^{p\nu}) = f\,i, \quad \text{from which} \quad h^{p^\nu} = h\,.$$

Therefore all the roots of the congruence $x^{p^\mu} = x$ would be in common with those of the equation $x^{p^\nu} = x$, which is absurd.

We know finally then that all the roots of the equation or congruence $x^{p^\nu} = x$ necessarily depend on a single irreducible congruence of degree ν.

Now the most general method to get this irreducible congruence on which the roots of the congruence $x^{p^\nu} = x$ depend will be first to rid this congruence of all the factors that it could have in common with congruences of lower degree and which are of the form

$$x^{p^\mu} = x\,.$$

In this way one will get a congruence which must be partitioned [factorised] into irreducible congruences of degree ν. And since one knows how to express all the roots of each of these irreducible congruences by means of a single one it will be easy to obtain all of them by the method of Mr Gauss.

Most often, however, it will be easy to find an irreducible congruence of degree ν by trial and error, and one should deduce all the others from it.

For example, let $p = 7,\ \nu = 3$. Let us seek the roots of the congruence

$$x^{7^3} = x \pmod 7. \tag{1}$$

I observe that the congruence

$$i^3 = 2 \pmod 7 \tag{2}$$

being irreducible and of degree 3, all the roots of the congruence (1) depend rationally on those of the congruence (2), so that all the roots of (1) are of the form

$$a + a_1 i + a_2 i^2 \qquad \text{or} \qquad a + a_1 \sqrt[3]{2} + a_2 \sqrt[3]{4}\,. \tag{3}$$

Now it is necessary to find a primitive root, that is, a form of the expression (3) which, when raised to all powers, gives all the roots of the congruence

$$x^{7^3-1} = 1, \quad \text{that is} \quad x^{2^1.3^2.19} = 1 \pmod 7\,,$$

et nous n'avons besoin pour cela que d'avoir une racine primitive de chaque congruence

$$x^2 = 1 \qquad x^{3^2} = 1 \qquad x^{19} = 1$$

La racine primitive de la première est -1; celles de $x^{3^2} - 1 = 0$ sont données par les équations

$$x^3 = 2 \qquad x^3 = 4$$

en sorte que i est une racine primitive de $x^{3^2} = 1$.

Il ne reste qu'à trouver une racine de $x^{19} - 1 = 0$ ou plutôt de

$$\frac{x^{19} - 1}{x - 1} = 0$$

et essayons pour cela si l'on ne peut pas satisfaire à la question en posant simplement $x = a + a_1 i$, au lieu de $a + a_1 i + a_2 i^2$, nous devrons avoir

$$(a + a_1 i)^{19} = 1$$

ce qui, en développant par la formule de Newton et réduisant les puissances de a, de a_1 et de i par les formules

$$a^{m(p-1)} = 1 \qquad a_1^{m(p-1)} = 1 \qquad i^3 = 2$$

se réduit à

$$3\left\{a - a^4 a_1^3 + 3(a^5 a_1^2 + a^2 a_1^5) i^2\right\} = 1$$

p. 433

d'où, en séparant

$$3a - 3a^4 a^3 = 1, \quad a^5 a_1^2 + a^2 + a_1^5 = 0$$

Second equation corrected in L1846. See English.

Ces deux dernières équations sont satisfaites en posant $a = -1, a_1 = -1$. Donc

$$-1 - i$$

Second equation corrected to $a_1 = 1$ in L1846; then $-1 - i$ corrected to $-1 + i$ hereafter.

est une racine primitive de $x^{19} = 1$. Nous avons trouvé plus haut pour racines primitives de $x^2 - 1$ et de $x^{3^2} = 1$ les valeurs -1 et i, il ne reste plus qu'à multiplier entr'elles les 3 quantités

Misprint corrected to x^{3^2} in L1846.

$$-1, \quad i, \quad -i - 1$$

et le produit $i + i^2$ sera une racine primitive de la congruence

Here and below $i + i^2$ corrected to $i - i^2$ in L1846.

$$x^{7^3 - 1} = 1$$

Donc ici l'expression $i + i^2$ jouit de la propriété, qu'en l'élevant à toutes les puissances, on obtiendra $7^3 - 1$ expressions différentes de la forme

$$a + a_1 i + a_2 i^2$$

and for that we only need to have a primitive root of each congruence

$$x^2 = 1\,, \qquad x^{3^2} = 1\,, \qquad x^{19} = 1\,.$$

The primitive root of the first is -1; those of $x^{3^2} - 1 = 0$ are given by the equations

$$x^3 = 2\,, \qquad x^3 = 4\,,$$

so that i is a primitive root of $x^{3^2} = 1$.

It remains only to find a root of $x^{19} - 1 = 0$ or rather of

$$\frac{x^{19} - 1}{x - 1} = 0\,,$$

and for that, trying if one might answer the question by setting simply $x = a + a_1 i$ instead of $a + a_1 i + a_2 i^2$, we will need to have

$$(a + a_1 i)^{19} = 1\,,$$

which, on expanding by Newton's formula and reducing the powers of a, a_1 and i by the formulae

$$a^{m(p-1)} = 1\,, \qquad a_1^{m(p-1)} = 1\,, \qquad i^3 = 2\,,$$

reduces to

$$3\{a - a^4 a_1^3 + 3(a^5 a_1^2 + a^2 a_1^5) i^2\} = 1$$

from which, on separating,

$$3a - 3a^4 a_1^3 = 1, \qquad a^5 a_1^2 + a^2 a_1^5 = 0\,.$$

These last two equations are satisfied by setting $a = -1, a_1 = 1$. Therefore

$$-1 + i$$

is a primitive root of $x^{19} = 1$. We have found above the values -1 and i as primitive roots of $x^2 - 1$ and of $x^{3^2} = 1$, and what remains is only to multiply together the 3 quantities

$$-1, \quad i, \quad i - 1$$

and the product $i - i^2$ will be a primitive root of the congruence

$$x^{7^3 - 1} = 1\,.$$

Thus here the expression $i - i^2$ enjoys the property that on raising it to all powers one obtains $7^3 - 1$ different expressions of the form

$$a + a_1 i + a_2 i^2.$$

Si nous voulons avoir la congruence de moindre degré d'où dépend notre racine primitive, il faut éliminer i entre les deux équations

$$i^3 = 2 \qquad \alpha = i + i^2$$

Corrected to $\alpha = i - i^2$ in L1846.

On obtient ainsi

$$\alpha^3 + 3\alpha + 1 = 0$$

Corrected to $\alpha^3 - \alpha + 2 = 0$ in L1846.

Il sera convenable de prendre pour base des imaginaires, et de représenter par i la racine de cette équation, ensorte que

$$i^3 + 3i + 1 = 0 \qquad (i)$$

Corrected to $i^3 - i + 2 = 0$ in L1846.

et l'on aura toutes les imaginaires de la forme

$$a + a_1 i + a_2 i^2$$

en élevant i à toutes les puissances, et réduisant par l'équation (i).

Le principal avantage de la nouvelle théorie que nous venons d'exposer, est de ramener les congruences à la propriété (si utile dans les équations ordinaires) d'admettre précisément autant de racines qu'il y a d'unités dans l'ordre de leur degré.

La méthode pour avoir toutes ces racines sera très simple. Premièrement on pourra toujours préparer la congruence donnée $\mathrm{F}x = o$, de manière à ce qu'elle n'ait plus de racines égales, ou en d'autres termes, à ce qu'elle n'ait plus de facteur

p. 434

commun avec $\mathrm{F}'x = o$, et le moyen de le faire est évidemment le même que pour les équations ordinaires.

Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à $\mathrm{F}x = o$ et à $x^{p-1} = 1$.

Si maintenant on veut avoir les solutions imaginaires du second degré, on cherchera le plus grand facteur commun à $\mathrm{F}x = o$ et à $x^{p^2-1} = 0$ et en général, les solutions de l'ordre ν seront données par le plus grand commun diviseur à $\mathrm{F}x = o$ et à $x^{p^\nu - 1} = 1$.

Misprint corrected to $x^{p^2-1} = 1$ in L1846; no comment in BA1962.

C'est surtout dans la théorie des permutations, où l'on a sans cesse besoin de varier la forme desindices, que la considération des racines imaginaires des congruences paraît indispensable. Elle donne un moyen simple et facile de reconnaître dans quel cas une équation primitive est soluble par radicaux, comme je vais essayer d'en donner en deux mots une idée.

Interword space missing in original.

Soit une équation algébrique $f\,x = o$ de degré p^ν; supposons que les p^ν racines soient désignées par x_k, en donnant à l'indice k les p^ν valeurs déterminées par la congruence $k^{p^\nu} = k \pmod{p}$.

If we wish to have the congruence of least degree on which our primitive root depends, it is necessary to eliminate i between the two equations

$$i^3 = 2\,, \qquad \alpha = i - i^2\,.$$

In this way one obtains

$$\alpha^3 - \alpha + 2 = 0\,.$$

It will be convenient to represent by i the root of this equation, so that

$$i^3 - i + 2 = 0\,, \qquad (i)$$

and to take it as basis of the imaginaries, so that one will have all the imaginaries in the form

$$a + a_1 i + a_2 i^2$$

by raising i to all powers, and reducing by the equation (i).

The principal benefit of the new theory that we have just expounded is to carry over to congruences the property (so useful in ordinary equations) of admitting precisely as many roots as there are units in the order of their degree.

The method to get all these roots will be very simple. First one can always prepare [adjust] the given congruence $Fx = 0$ in such a way that it does not have equal roots any more, or in other words, so that it will have no factor

in common with $F'x = 0$, and the way to do this is clearly the same as for ordinary equations.

After that, to get the integer solutions it will suffice, as Mr Libri seems to have been the first to notice, to seek the greatest common factor of $Fx = 0$ and $x^{p-1} = 1$.

If one now wishes to have the imaginary solutions of the second degree one will seek the greatest common factor of $Fx = 0$ and $x^{p^2-1} = 1$, and in general the solutions of order ν will be given by the greatest common factor of $Fx = 0$ and $x^{p^\nu - 1} = 1$.

It is above all in the theory of permutations, where one forever needs to vary the form of indices, that consideration of the imaginary roots of congruences appears to be indispensable. It gives a simple and easy means of recognising the cases in which a primitive equation is soluble by radicals, of which I shall try to give an idea in two words.

Let $fx = 0$ be an algebraic equation of degree p^ν. Suppose that the p^ν roots are denoted by x_k, where the index k is given the p^ν values determined by the congruence $k^{p^\nu} = k \pmod p$.

Prenons une fonction quelconque rationnelle V des p^ν racines x_k. Transformons cette fonction en substituant partout à l'indice k l'indice $(ak+b)^{p^r}$, a, b, r étant des constantes arbitraires satisfaisant aux conditions de $a^{p^\nu - 1} = 1 \quad b^{p^\nu} = b \pmod{p}$ et de r entier.

En donnant aux constantes a, b, r toutes les valeurs dont elles sont susceptibles, on obtiendra en tout $p^\nu(p^\nu - 1)\nu$, manières de permuter les racines entr'elles par des substitutions de la forme $\begin{pmatrix} x_k, & x_{(ak+b)^{p^r}} \end{pmatrix}$, et la fonction V admettra en général par ces substitutions $p^\nu(p^\nu - 1)\nu$, formes différentes.

Otiose comma removed in L1846.

Otiose comma removed in L1846.

Admettons maintenant que l'équation proposée $f\,x = o$ soit telle, que toute fonction des racines invariable par les $p^\nu(p^\nu - 1)\nu$ permutations que nous venons de construire, ait pour cela même une valeur numérique rationnelle.

Perhaps *permutations* should be *substitutions*.

p. 435

On remarque que dans ces circonstances, l'équation $f\,x = o$ sera soluble par radicaux, et pour parvenir à cette conséquence, il suffit d'observer que la valeur substituée à k dans chaque indice peut se mettre sous les trois formes

$$\Big(ak + b\Big)^{p^r} = \Big(a\,\{k + b^1\}\Big)^{p^r} = a^1 k^{p^r} + b'' = a'\Big(k + b'\Big)^{p^r}$$

Les personnes habituées à la théorie des équations le verront sans peine.

Cette remarque aurait peu d'importance, si je n'étais parvenu à démontrer que réciproquement une équation primitive ne saurait être soluble par radicaux, à moins de satisfaire aux conditions que je viens d'énoncer. (J'excepte les équations du 9$^{\text{e}}$ et du 25$^{\text{e}}$ degré).

Ainsi, pour chaque nombre de la forme p^ν, on pourra former un groupe de permutations tel que toute fonction des racines invariable par ces permutations devra admettre une valeur rationnelle quand l'équation de degré p^ν sera primitive et soluble par radicaux.

Perhaps 2nd occurrence of *permutations* should be *substitutions*.

D'ailleurs, il n'y a que les équations d'un pareil degré p^ν qui soient à la fois primitives et solubles par radicaux.

Le théorème général que je viens d'énoncer précise et développe les conditions que j'avais données dans le *Bulletin* du mois d'avril. Il indique le moyen de former une fonction des racines dont la valeur sera rationnelle, toutes les fois que l'équation primitive de degré p^ν sera soluble par radicaux, et méne par conséquent aux caractères de résolubilité de ces équations, par des calculs sinon praticables, du moins qui sont possibles en théorie.

Misprint 'méne' corrected to 'mène' in L1846, BA1962.

Il est à remarquer que dans le cas où $\nu = 1$, les diverses valeurs de k ne sont autre chose que la suite des nombres entiers. Les substitutions de la forme $\begin{pmatrix} x_k, & x_{ak+b} \end{pmatrix}$ seront au nombre de $p(p-1)$.

La fonction qui, dans le cas des équations solubles par radicaux, doit avoir une valeur rationnelle, dépendra en général d'une équation de degré $1.2.3 \ldots\ldots (p-2)$, à laquelle il faudra par conséquent appliquer la méthode des racines rationnelles.

Take an arbitrary rational function V of the p^ν roots x_k. Transform this function by substituting for the index k the index $(ak+b)^{p^r}$ throughout, a, b, r being arbitrary constants satisfying the conditions that $a^{p^\nu-1} = 1, b^{p^\nu} = b \pmod p$ and that r be a whole number.

Giving to the constant a, b, r all the values of which they are capable, one will obtain in all $p^\nu(p^\nu-1)\nu$ ways of permuting the roots amongst themselves by substitutions of the form $(x_k, x_{(ak+b)^{p^r}})$, and under these substitutions the function V will in general admit $p^\nu(p^\nu-1)\nu$ different forms.

Now let us accept moreover that the proposed equation $fx = 0$ is such that every function of the roots invariant under the $p^\nu(p^\nu-1)\nu$ permutations that we have just constructed will take a numerical value that is rational.

Note that under these circumstances the equation $fx = 0$ will be soluble by radicals, and to reach this conclusion it suffices to observe that the value substituted for k in each index can be put into the three forms

$$(ak+b)^{p^r} = (a\{k+b'\})^{p^r} = a'k^{p^r} + b'' = a'(k+b')^{p^r}.$$

People who are used to the theory of equations will see this without trouble.

This remark would have little importance had I not been able to prove that conversely a primitive equation cannot be soluble by radicals unless it satisfies the conditions that I have just formulated. (I except equations of the 9th and of the 25th degree.)

Thus for each number of the form p^ν, one may form a group of permutations such that every function of the roots invariant under these permutations [its substitutions] will have to admit a rational value when the equation of degree p^ν is primitive and soluble by radicals.

Moreover, it is only equations of such a degree p^ν that can be both primitive and soluble by radicals.

The general theorem that I have just formulated makes more precise and develops the conditions that I gave in the *Bulletin* for the month of April. It shows the way to form a function of the roots whose value will be rational whenever the primitive equation of degree p^ν is soluble by radicals, and consequently leads to the characteristics [conditions] for solubility of these equations by calculations which, if not practicable, at least are possible in theory.

It is worth noting that in the case where $\nu = 1$ the various values of k are none other that the sequence of whole numbers. The substitutions of the form (x_k, x_{ak+b}) will be $p(p-1)$ in number.

In the case of equations that are soluble by radicals the function which must have a rational value will depend in general on an equation of degree $1.2.3...(p-2)$, to which it will therefore be necessary to apply the method of rational roots.

II.5 On some points of analysis

This paper was published in Gergonne's *Annales de Mathématiques pures et appliquées*, 21, 183–184 (December 1830), when Galois had just started at the École Normale. It appears in a section of the journal containing material classified as *Analyse transcendante*. It was reprinted in [Liouville (1846), pp. 392–394], in [Picard (1897), pp. 9–10], and in [B & A (1962), pp. 382–385]. There are several misprints in the Gergonne original—beginning with the author's name. Most of them were corrected in the reprints but they are faithfully reproduced here. Punctuation and typography are also adjusted in those editions—I have tried to copy the original as far as modern typography permits.

I have had some difficulties with the translation here: the phrase *fonction déterminée* could be any of 'determinate function', 'well-defined function', 'certain function', 'specific function'. Indeed, the context indicates that its meaning is subtly different at each of its three occurrences. The phrase *perpendiculaire abaissée* is usually translated as 'altitude' (in the context of geometry of triangles). Here the translation 'perpendicular dropped [from ... to ...]' fits the meaning much better. Note that in modern English 'radius' is ambiguous: it can (and usually does) mean the distance from the centre of a circle to any of its points; but it can also mean, and in the past very frequently did mean, a line segment from the centre to a point on the circumference.

Galois gives us no clue as to what stimulated him to write the two little essays in this paper. It might have been passages in textbooks, it might have been articles in one or another of the journals that he had read. One would have circumstantial evidence if one identified passages in other writings that treated similar questions with similar notation, or if one could identify to what 'known theorems' of differential geometry the last sentence refers. I have not succeeded—but nor have I embarked on any systematic search.

This article, with its two separate little essays, seems to me to be of a different calibre and style from most of Galois' mathematical writing. Had I been editor, and had I been given the choice, I might have been inclined to publish either or both of the essays in Dossier 21 (on the integration of linear differential equations) and in Dossier 22 (on surfaces of the second degree) rather than this. They were written at about the same time; they seem to me to be less inconsequential; they seem to me to be more polished and more convincing as mathematics. But these are matters of taste and judgment inappropriate to an editor. My substantive point is that those two unpublished essays may be compared in very broad terms with this published article.

p. 182

Notes sur quelques points d'analyse;

par M. GALAIS, élève à l'Ecole normale

'Galais' *sic*! All editions note the misprint.

§. I.

Démontration d'un théorème d'analyse.

'Démontration' *sic*! All editions correct or overlook the misprint.

THÉORÈME. Soient $\mathrm{F}x$ et $\mathrm{f}x$ deux fonctions quelconques données; on aura, quels que soient x et h,

$$\frac{\mathrm{F}(x+h)-\mathrm{F}x}{\mathrm{f}(x+h)-\mathrm{f}x}=\varphi(k)\,,$$

φ étant une fonction déterminée, et k une quantité intermédiaire entre x et $x+h$.

Démonstration. Posons, en effet,

$$\frac{\mathrm{F}(x+h)-\mathrm{F}x}{\mathrm{f}(x+h)-\mathrm{f}x}=P\ ;$$

on en déduira

$$\mathrm{F}(x+h)-P\mathrm{f}(x+h)=\mathrm{F}x-P\mathrm{f}x\ ,$$

d'où l'on voit que la fonction $\mathrm{F}x-P\mathrm{f}x$ ne change pas quand on y change x en $x+h$; d'où il suit qu'à moins qu'elle ne reste constante entre ces limites, ce qui ne pourrait avoir lieu que dans des cas particuliers, cette fonction aura, entre x et $x+h$, un ou plusieurs *maxima* et *minima*. Soit k la valeur de x répondant à l'un d'eux; on aura évidemment

$$k=\psi(P)\ ,$$

ψ étant une fonction déterminée; donc on doit avoir aussi

p. 183

$$P=\varphi(k)\ ,$$

φ étant une autre fonction également déterminée; ce qui démontre le théorème.

De là on peut conclure, comme corollaire, que la quantité

$$\mathrm{Lim.}\frac{\mathrm{F}(x+h)-\mathrm{F}x}{\mathrm{f}(x+h)-\mathrm{f}x}=\varphi(x)\ ,$$

pour $h=0$, est nécessairement une fonction de x, ce qui démontre, à *priori*, l'existence des fonctions dérivées.

Printed roman in L1846, BA1962; corrected to 'a priori' in BA1962.

§. II.

Rayon de courbure des courbes dans l'espace.

Word 'dans' changed to 'de' in P1897, although L1846 is faithful.

Le rayon de courbure d'une courbe en l'un quelconque de ses points M est la perpendiculaire abaissée de ce point sur l'intersection du plan normal au point M

Notes on some points of analysis

by Mr GALOIS, student at the Ecole normale

§. I.

Proof of a theorem of analysis.

THEOREM. *Let* $\mathrm{F}x$ *and* $\mathrm{f}x$ *be two arbitrarily given functions. Whatever* x *and* h *may be one will have*

$$\frac{\mathrm{F}(x+h)-\mathrm{F}x}{\mathrm{f}(x+h)-\mathrm{f}x}=\varphi(k)\,,$$

φ being a certain function and k a quantity intermediate between x and $x+h$.

For translation of 'déterminée' see p. 77.

Proof. Indeed, set

$$\frac{\mathrm{F}(x+h)-\mathrm{F}x}{\mathrm{f}(x+h)-\mathrm{f}x}=P\ .$$

From this it may be deduced that

$$\mathrm{F}(x+h)-P\mathrm{f}(x+h)=\mathrm{F}x-P\mathrm{f}x\ ,$$

from which it may be seen that the function $\mathrm{F}x-P\mathrm{f}x$ does not change when x is changed to $x+h$; from which it follows that, unless it remains constant between these limits, which could not happen except in special cases, this function will have one or more maxima and minima between x and $x+h$. Let k be the value of x corresponding to one of them. Clearly one will have

$$k=\psi(P)\ ,$$

ψ being a certain function. Therefore one must also have

$$P=\varphi(k)\ ,$$

φ being another, equally well defined function; which proves the theorem.

One may conclude from that, as a corollary, that the quantity

$$\mathrm{Lim}\frac{\mathrm{F}(x+h)-\mathrm{F}x}{\mathrm{f}(x+h)-\mathrm{f}x}=\varphi(x)\ ,$$

for $h=0$, is necessarily a function of x, which proves *a priori* the existence of derived functions.

§. II.

Radius of curvature of curves in space.

The radius of curvature of a curve at an arbitrary one of its points M is the perpendicular dropped from this point to the intersection of the normal plane at the point M

avec le plan normal consécutif, comme il est aisé de s'en assurer par des considérations géométriques.

Cela posé, soit (x, y, z) un point de la courbe; on sait que le plan normal en ce point aura pour équation

$$(X-x)\frac{\mathrm{d}x}{\mathrm{d}s}+(Y-y)\frac{\mathrm{d}y}{\mathrm{d}s}+(Z-z)\frac{\mathrm{d}z}{\mathrm{d}s}=0\,. \qquad \text{(N)}$$

X, Y, Z étant les symboles des coordonnées courantes. L'intersection de ce plan normal avec le plan normal consécutif sera donnée par le système de cette équation et de la suivante

$$(X-x)\frac{\mathrm{d}.\left(\frac{\mathrm{d}x}{\mathrm{d}s}\right)}{\mathrm{d}s}+(Y-y)\frac{\mathrm{d}.\left(\frac{\mathrm{d}y}{\mathrm{d}s}\right)}{\mathrm{d}s}+(Z-z)\frac{\mathrm{d}.\left(\frac{\mathrm{d}z}{\mathrm{d}s}\right)}{\mathrm{d}s}=1\,, \qquad \text{(I)}$$

attendu que

$$\left(\frac{\mathrm{d}x}{\mathrm{d}s}\right)^2+\left(\frac{\mathrm{d}y}{\mathrm{d}s}\right)^2+\left(\frac{\mathrm{d}z}{\mathrm{d}s}\right)^2=1\,.$$

Or, il est aisé de voir que le plan (I) est perpendiculaire au plan (N); car l'on a

Misprints: stops missing after 2nd and 3rd occurrences of d supplied in all editions.

$$\frac{\mathrm{d}x}{\mathrm{d}s}\,\mathrm{d}.\left(\frac{\mathrm{d}x}{\mathrm{d}s}\right)+\frac{\mathrm{d}y}{\mathrm{d}s}\,\mathrm{d}\left(\frac{\mathrm{d}y}{\mathrm{d}s}\right)+\frac{\mathrm{d}z}{\mathrm{d}s}\,\mathrm{d}\left(\frac{\mathrm{d}z}{\mathrm{d}s}\right)=0\,;$$

donc la perpendiculaire abaissée du point (x, y, z) sur l'intersection des deux plans (N) et (I) n'est autre chose que la perpendiculaire abaissée du meme point sur le plan (I). Le rayon de courbure est donc la perpendiculaire abaissé du point (x, y, z) sur le plan (I). Cette considération donne, très-simplement, les théorèmes connus sur les rayons de courbure des courbes dans l'espace.

Misprints 'meme' and 'abaissé' corrected to 'même' and 'abaissée' in all editions.

with the consecutive [adjacent] normal plane, as one may easily persuade oneself by geometrical considerations.

That said, let (x, y, z) be a point of the curve. It is known that the normal plane at this point will have equation

$$(X - x)\frac{\mathrm{d}x}{\mathrm{d}s} + (Y - y)\frac{\mathrm{d}y}{\mathrm{d}s} + (Z - z)\frac{\mathrm{d}z}{\mathrm{d}s} = 0 \,, \qquad \text{(N)}$$

X, Y, Z being symbols for the usual coordinates. The intersection of this normal plane with the consecutive [adjacent] normal plane will be given by the system of this equation and the following

$$(X - x)\frac{\mathrm{d}.\left(\frac{\mathrm{d}x}{\mathrm{d}s}\right)}{\mathrm{d}s} + (Y - y)\frac{\mathrm{d}.\left(\frac{\mathrm{d}y}{\mathrm{d}s}\right)}{\mathrm{d}s} + (Z - z)\frac{\mathrm{d}.\left(\frac{\mathrm{d}z}{\mathrm{d}s}\right)}{\mathrm{d}s} = 1 \,, \qquad \text{(I)}$$

given that

$$\left(\frac{\mathrm{d}x}{\mathrm{d}s}\right)^2 + \left(\frac{\mathrm{d}y}{\mathrm{d}s}\right)^2 + \left(\frac{\mathrm{d}z}{\mathrm{d}s}\right)^2 = 1 \,.$$

Now it is easy to see that the plane (I) is perpendicular to the plane (N), for one has

$$\frac{\mathrm{d}x}{\mathrm{d}s}\,\mathrm{d}.\left(\frac{\mathrm{d}x}{\mathrm{d}s}\right) + \frac{\mathrm{d}y}{\mathrm{d}s}\,\mathrm{d}.\left(\frac{\mathrm{d}y}{\mathrm{d}s}\right) + \frac{\mathrm{d}z}{\mathrm{d}s}\,\mathrm{d}.\left(\frac{\mathrm{d}z}{\mathrm{d}s}\right) = 0 \,.$$

Therefore the perpendicular dropped from the point (x, y, z) to the intersection of the two planes (N) and (I) is nothing other than the perpendicular dropped from this self-same point to the plane (I). The radius of curvature is therefore the perpendicular dropped from the point (x, y, z) to the plane (I). This consideration gives very easily the known theorems on radius of curvature of curves in space.