Revue d'histoire des mathématiques
17 (2011), p. 211–270

CHARLES HERMITE'S STROLL THROUGH THE GALOIS FIELDS

Catherine Goldstein

Abstract. — Although everything seems to oppose the two mathematicians, Charles Hermite's role was crucial in the study and diffusion of Évariste Galois's results in France during the second half of the nineteenth century. The present article examines that part of Hermite's work explicitly linked to Galois, the reduction of modular equations in particular. It shows how Hermite's mathematical convictions—concerning effectiveness or the unity of algebra, analysis and arithmetic—shaped his interpretation of Galois and of the paths of development Galois opened. Reciprocally, Hermite inserted Galois's results in a vast synthesis based on invariant theory and elliptic functions, the memory of which is in great part missing in current Galois theory. At the end of the article, we discuss some methodological issues this raises in the interpretation of Galois's works and their posterity.

Texte reçu le 14 juin 2011, accepté le 29 juin 2011.

C. Goldstein, Histoire des sciences mathématiques, Institut de mathématiques de Jussieu, Case 247, UPMC-4, place Jussieu, F-75252 Paris Cedex (France).

Courrier électronique : cgolds@math.jussieu.fr

Url : http://people.math.jussieu.fr/~cgolds/

2000 Mathematics Subject Classification : 01A55, 01A85; 11-03, 11A55, 11F03, 12-03, 13-03, 20-03.

Key words and phrases : Charles Hermite, Évariste Galois, continued fractions, quintic, modular equation, history of the theory of equations, arithmetic algebraic analysis, monodromy group, effectivity.

Mots clefs. — Charles Hermite, Évariste Galois, fractions continues, quintique, équation modulaire, histoire de la théorie des équations, analyse algébrique arithmétique, groupe de monodromie, effectivité.

I warmly thank Jim Ritter for his linguistic help, in particular with the translation of the French quotes, and the two referees for very helpful suggestions.

Résumé (Les promenades galoisiennes de Charles Hermite)

Bien que tout semble les opposer, Charles Hermite a joué un rôle important dans l'étude et la diffusion des travaux d'Évariste Galois en France au milieu du XIX^e siècle. Cet article étudie les travaux d'Hermite en lien direct avec ceux de Galois, en particulier sur la réduction des équations modulaires. Il montre comment les convictions mathématiques d'Hermite, sur la nécessité de calculs effectifs et sur l'unité de l'algèbre avec l'analyse et l'arithmétique, ont modelé son interprétation de Galois et des pistes ouvertes par celui-ci. Réciproquement, Hermite a inséré les résultats de Galois dans une vaste synthèse appuyée sur la théorie des invariants et les fonctions elliptiques dont la théorie de Galois usuelle a mutilé la mémoire. La fin de l'article revient sur les problèmes méthodologiques ainsi soulevés dans l'interprétation des travaux de Galois et de leur postérité.

Bringing together Galois and Hermite may seem strange at first sight. Our images of them are so contradictory: the young, cheeky rebel and the crusty professor, the precursor of structural viewpoint and the opponent of Cantorian set theory, the revolutionary, rejecting authorities and rejected by them, and the conservative supporter of the Church and the monarchy, at the centre of French academic mathematics.

FIGURE 1. Two usual representations of Évariste Galois and Charles Hermite: rotogravures of Galois's portrait at 15 (left), published in [Dupuy 1896] and of Hermite's photo at 65 (right), at the beginning of [Hermite *Œuvres*, vol. 3].

Indeed, we can well imagine the outrage that one who wrote: "It was not then without pain and indignation that places in the Restoration government were seen to become the prey of the highest bidder in terms of monarchial and religious ideas,"[1] would have felt had he been privy to the other's explanation on one of his votes:

> In the person of M. Wurtz, M. B[ertrand] has a rival in the Academy for [election to] the High Council [for Public Education] but I have yet another reason, aside from that of kinship, to vote in favor of the latter. M. Wurtz, who may be an excellent man, will represent in the Council if he ends up there, M. Ferry's Article 7, that is, the expulsion from education of the Jesuits and religious communities.[2]

This opposition extends even to their views on how to do mathematics. "I thought I noticed a tendency of my mind to avoid calculations in subjects I was dealing with and, moreover, I recognized an insurmountable difficulty for whoever might wish to carry them out generally in the questions I dealt with," wrote Galois from the Sainte-Pélagie jail.[3] And his famous: "Take a flying leap over these calculations" and "here we do the analysis of analysis" have become legend. Hermite, on the contrary, presented himself as "doing this good old analysis which above all wants to be simple and clear, following such masters as Euler, Lagrange, Gauss and Jacobi,"[4] and put computations at the core of his conceptual practice: "Nothing seems to me more opposed to the truth and reality of things," he wrote, "than when M. Poinsot says: 'Computation is an instrument which produces nothing

---

1 E.G., Lettre sur l'enseignement des sciences, *Gazette des écoles*, January 2, 1831, repr. in [Galois 1962, p. 21]: *Ce n'était donc pas sans douleur et indignation que dans le gouvernement de la Restauration, on voyait les places devenir la proie des plus offrants en fait d'idées monarchiques et religieuses.*

2 Letter XVII of April 5, 1880 in [Hermite & Mittag-Leffler *Corresp.*, 5 (1984), p. 70]: *M. B[ertrand] a un rival à l'Académie pour le Conseil supérieur [de l'Instruction publique] dans M. Wurtz, mais j'ai pour voter en sa faveur un autre devoir encore que celui de la parenté. M. Wurtz qui est cependant un bien excellent homme, représentera dans le Conseil, s'il y parvient, l'article 7 de M. Ferry, c'est-à-dire l'expulsion des jésuites et des communautés religieuses de l'enseignement.*

3 Préface à deux mémoires d'analyse, manuscript written at Sainte-Pélagie, December 1831, in [Galois 1962, p. 11]: *J'ai cru observer cette tendance de mon esprit à éviter les calculs dans les sujets que je traitais et qui plus est j'ai reconnu une difficulté insurmontable à qui voudrait les effectuer généralement dans les matières que j'ai traitées.* The two other quotes, *Sauter à pieds joints sur ces calculs* and *ici on fait l'analyse de l'analyse* also come from this preface, p. 9 and 11.

4 Letter of February 22, 1878 in [Hermite & Genocchi *Corresp.*, p. 9–10]: *[N]ous faisons de cette analyse de la bonne vieille roche, qui avant tout veut être simple et claire, en suivant les maîtres qui se nomment Euler, Lagrange, Gauss et Jacobi.*

by itself and which in some way only gives back the ideas entrusted to it'."[5] The reference to Poinsot is especially relevant, because Poinsot's explicit views, not only on computations but also on the need to study permutations and relations *per se*, are remarkably close to those of Galois.[6]

But this is not the whole story and Galois and Hermite have more in common than one might suspect. Both were students in Louis Richard's mathematics class at the Lycée Louis-Le-Grand and both benefitted from his encouragement to read significant authors outside curricular limits. Richard's support of Galois is well documented, see [Dupuy 1896]. As for Hermite, he explained for instance to Gösta Mittag-Leffler:

> I studied first in Nancy and then in Paris, at the Collège Henri IV and the Collège Louis-le-Grand, where I had an excellent and highly qualified man for a mathematics teacher. I have kept a most grateful memory of M. Richard: he would send me to the Sainte-Geneviève Library to read articles in Gergonne's *Annales*. I spent long hours browsing through the publications of the Academies of Science of Paris, Berlin, and Saint-Petersburg, before I even knew differential calculus, simply concentrating on those that I could understand.[7]

Both then began to publish original work while still students and both first failed their entrance to Polytechnique. Hermite linked his mediocre achievement in intellectual competitions to his early involvement with real mathematics; he confessed to Thomas Stieltjes:

> I also abhorred examinations, and I passed one year, when I was a student in *Mathématiques spéciales*, reading the works of Euler, the publications of the Academies in the Sainte-Geneviève Library, etc. instead of revising problems in

---

5 Hermite to Leo Königsberger, March 2, 1876, Staatsbibliothek zu Berlin, Handschriftenabteilung: *Rien ne me semble plus contraire à la vérité et à la réalité des choses que ce que dit M. Poinsot, dans les termes suivants: 'Le calcul est un instrument qui ne produit rien par lui-même et qui ne rend en quelque sorte que les idées qu'on lui confie'.*

6 See for instance [Grattan-Guinness 1990, p. 1231–1232], [Goldstein, Schappacher & Schwermer 2007, p. 35], [Ehrhardt 2007, p. 94–100]. Poinsot's work on equations and permutations, and his view of algebra as the "science of order" are analyzed in depth in [Boucard 2011].

7 Letter LXXX, c. September 15, 1882, in [Hermite & Mittag-Leffler *Corresp.*, 5 (1984), p. 168–169]: *J'ai été d'abord au collège de Nancy, puis à Paris au collège Henri IV et au collège Louis-Le-Grand, où j'ai eu un homme excellent et d'un mérite supérieur pour professeur de mathématiques. M. Richard me laisse le plus reconnaissant souvenir; il m'envoyait à la bibliothèque Sainte Geneviève lire des articles des Annales de Gergonne. J'y passais de longues heures à feuilleter les mémoires des Académies des sciences de Paris, de Berlin, de Saint-Pétersbourg, que j'ai parcourus avant de connaître le calcul différentiel, en m'attachant à ceux que je pouvais comprendre.* On Louis Richard, see his obituary by Olry Terquem, [Terquem 1849], as well as [Brasseur 2010], for which I am indebted to Norbert Verdier.

> geometry, statics, etc. M. X… had taken an aversion to me and I paid for my whims of an *écolier savant* by a humiliating failure.[8]

And if Hermite, in contrast to Galois, finally succeeded—a more docile nature? fewer family and money problems? examiners in a better mood?—he remained at Polytechnique only one year before leaving and devoting himself completely to mathematics, a path Galois probably would have liked to follow. It was to Hermite that Richard chose to pass on Galois's surviving schoolwork, see [Ehrhardt 2008]. And it was Galois's ghost that a visitor to the Bertrand family home felt he saw when meeting there Hermite for the first time—an anecdote which fittingly closes Joseph Bertrand's review of Paul Dupuy's biography of Galois:

> One of my father's brothers, Dr. Stanislas Bertrand, who had never studied mathematics, lived in close relation with Galois. He had met him in 1830, both in the offices of the *La Tribune* newspaper, and in the secret meetings of the Society *Aide-toi, le ciel t'aidera* ('Help Yourself and Heaven Will Help You'); practices which found them sitting together on police station benches. Fifteen years later, my Uncle, coming to visit me, found me speaking with a young man whom he seemed to observe with particular attention and to listen to with astonishment. He told me the next day: 'I have undergone a great shock; for a quarter of an hour I thought I was seeing and hearing Évariste Galois!' He had seen and heard Charles Hermite.[9]

These intimations of a resonance between Galois and Hermite took on some deeper substance in 1847, when the 24-old Hermite, out of Polytechnique and still jobless, wrote to Carl Gustav Jacob Jacobi about number theory:

---

8 Letter 59 of July 2, 1884, in [Hermite & Stieltjes *Corresp.*, vol. I, p. 129]: *J'ai eu aussi les examens en horreur, et j'ai passé une année, étant élève de mathématiques spéciales, à lire à la bibliothèque Sainte-Geneviève les mémoires des collections académiques, les ouvrages d'Euler, etc. au lieu de me mettre en mesure de répondre sur les questions de géometrie, de statique, etc. M. X. m'avait pris en aversion et j'ai expié par un humiliant échec mes fantaisies d'écolier savant.* M. X. is Camille Gerono, the co-founder of the *Nouvelles Annales.*

9 [Bertrand 1899, p. 400]: *Un des frères de mon père, le Dr Stanislas Bertrand, qui jamais n'étudia les Mathématiques, a vécu dans l'intimité de Galois. Il le rencontrait en 1830, tantôt dans les bureaux du journal* La Tribune*, tantôt dans les réunions secrètes de la Société* Aide-toi, le ciel t'aidera*; ce qui les conduisit à s'asseoir ensemble sur les bancs de la police correctionnelle. Quinze ans après, mon oncle, venant me voir, me trouva causant avec un jeune homme, qu'il semblait regarder avec attention et écouter avec étonnement. Il me dit le lendemain: j'ai éprouvé une grande émotion, j'ai cru pendant un quart d'heure voir et entendre Évariste Galois. Il avait vu et entendu Charles Hermite.* The mathematician Joseph Bertrand was Hermite's brother-in-law. The Society 'Aide-toi, le ciel t'aidera' was a liberal society created in 1827 in order to lobby against Charles X for legislative elections. *La Tribune des départements* was a radical newspaper, opposed to monarchy, and published between 1829 and 1835.


FIGURE 2. "It suffices to compare [Hermite's very early portrait] and the sketch that we possess of the likeness of poor Galois to appreciate all the savour of [Bertrand's anecdote]," comments Gaston Darboux in his obituary of Hermite, [Darboux 1905]: this portrait (on the right) opens the first volume of Hermite's works, [Hermite *Œuvres*, vol. 1].

> I would liked particularly to be in a position to submit to you a work on modular equations, in which I have established a result proposed in Galois's *Œuvres posthumes*, printed in the *Journal de mathématiques*, and which shows that modular equations of the sixth, eighth and twelfth degree can be lowered to the fifth, seventh, and eleventh degree, respectively.[10]

References to Galois then appear from time to time in Hermite's writings, almost exclusively in relation to mathematics. While politics is a recurrent theme in Hermite's correspondence (particularly after the advent of the Third Republic to which he was deeply opposed), and also a topos in most discussions of Galois from this time on, I have not been able to find

10 [Hermite 1850], quoted from [Hermite *Œuvres*, vol. 1, p. 135]: *Je désirerais surtout pouvoir vous soumettre un Travail sur les équations modulaires, dans lequel j'ai établi une proposition énoncée dans les* Œuvres posthumes *de Galois, imprimées dans le* Journal de mathématiques, *et qui consiste en ce que les équations modulaires du sixième, huitième et douzième degré peuvent être abaissées respectivement au cinquième, septième et onzième degré.* There are substantial differences between Hermite's original papers and the versions published in his collected works, where numerous mistakes were corrected or elided by the editors. In what follows, I shall always quote from [Hermite *Œuvres*].

any allusion to Galois's political commitments in Hermite's letters or articles. Hermite simply refers to the "illustre Galois," in the same way as when speaking of Niels Henrik Abel or Gustav Adolph Göpel, two other brilliant mathematicians of interest to Hermite and who died early.

I shall follow suit here and concentrate on what Hermite did with Galois's mathematics. The decisive role of the former in shaping mathematics in the second half of the nineteenth century makes his involvement with the latter an intriguing, and mostly unknown,[11] part of Galois's heritage. I have tracked down every explicit mention of Galois in Hermite's complete works and constructed a relevant corpus for each of them. This systematic search of Galois's name in Hermite's papers reveals it in three mathematical circumstances: algebraic functions, modular and quintic equations, continued fractions. I shall therefore explore these three themes successively, in the order of Galois's papers published in 1846 by Liouville in the *Journal de mathématiques pures et appliquées*, [Galois 1846], which happens to be the reverse order of their apparent development in Hermite's articles.

1. CONTINUED FRACTIONS

Galois's first published paper, in 1828, [Galois 1828–1829], and Hermite's last, in 1901, [Hermite 1901], are both devoted to continued fractions. The theory of continued fractions, described in 1774 by Joseph-Louis Lagrange, at the beginning of his Additions to Leonard Euler's *Elements of Algebra*, as "one of the most useful for arithmetic, as it serves to resolve problems with facility, that, without its aid, would be almost unmanageable," but still "little known to mathematicians," [Euler 1810, vol. 2, p. 247], became during the nineteenth century a key tool in the study of algebraic equations and functions as well as in number theory.[12] They were one of the three main ways in which functions could be developed (the two others being series and infinite products) and, for instance, played a central role in Joseph Liouville's first proof of transcendence, as well as in Carl-Friedrich Gauss's work on hypergeometric functions.

At the beginning of the nineteenth century, in France, continued fractions appear, as far as algebra and number theory are concerned, as a topic at the interface between research and textbooks, where their rudiments were accessible at least to good students: Pierre Bourdon's

11 Exceptions are [Kiernan 1971, p. 101] and [Ehrhardt 2007, ch. 6.3].

12 For historical information about continued fractions, see [Brezinski 1991] and [Fowler 1990, ch. 9].

best-selling *Éléments d'arithmétique*, "adopted by the university" (more than 20 editions between 1820 and 1850), included a section about them, while a footnote warned the reader that a slightly more advanced knowledge of algebra than in the rest of the book was here required. Like Pierre-Antoine Tisserand's 1819 *Traité d'arithmétique algébrique* which also devoted about twenty pages to continued fractions, however, it stopped short of the application to quadratic equations or square roots. These were to be found in more advanced texts, Lagrange's *Traité de la résolution des équations numériques de tous les degrés*—which both Galois and Hermite carefully studied—or Adrien-Marie Legendre's *Essai sur la théorie des nombres* and its subsequent editions.[13] Several authors of the *Annales de Gergonne* (and later of the *Nouvelles Annales*) then proposed their own presentation of the topic. In the 1860s, the place of continued fractions seemed well established: Joseph-Alfred Serret devoted to them two full chapters (c. 80 pages) of his influential *Cours d'algèbre supérieure*, starting with the 1866 third edition, and in the *Jahrbuch über die Fortschritte der Mathematik*, which systematically reviewed mathematical papers from 1868 on, "continued fractions" was one of the three headings in the number theory section until the First World War. Much appreciated in numerical computations, they also provided models and resources in various scientific contexts.

Reading Jacobi's proof that no complex function of one variable can have three independent periods—a proof by contradiction based on the iterative construction of an infinite, strictly decreasing, sequence of periods, the first step of which is given by continued fractions—Hermite immediately interpreted it with great admiration as a new mode of approximation and recycled it in his own early work on the minima of forms, see [Goldstein 2007, p. 383-385]. Later, algebraic continued fractions played a central role in his proof of the transcendence of e, see [Serfati 1992] and [Waldschmidt 1983].

Moreover, Lagrange's theorem, that a *periodic* development in continued fractions characterizes (real, irrational) roots of quadratic equations, accompanied Hermite all his algebraic life.[14] Léon Charve, a future professor and dean at the University of Marseilles, devoted his 1880 thesis, under

---

13 As is well-known, on the other hand, continued fractions were (almost) absent from Gauss's *Disquisitiones arithmeticae* and the textbooks directly inspired by it, see [Goldstein & Schappacher 2007a, p. 10–11].

14 The statement is proved in the "Additions au mémoire sur la résolution des équations numériques" published in the Proceedings of the Berlin Academy in 1770, [Lagrange *Œuvres*, vol. 2, p. 593] and reproduced in chapter VI of the *Traité de la résolution des équations numériques de tous les degrés*, published in 1798 and again in 1808 and 1826, [Lagrange *Œuvres* vol. 8, p. 94]. Both sources were at the Sainte-Geneviève Library.

Hermite's guidance, to adapt the model provided by continued fractions to the cubic case. He explained their programme at the beginning of his thesis:

> One knows that, if one develops a quadratic irrational number as a continued fraction, the computation is periodic. This periodicity constitutes a very remarkable property of the roots of quadratic equations, and can even be used as a definition of these irrational quantities. Now the theory of continued fractions is tightly linked to the theory of binary quadratic forms, such that the development in continued fractions of a root α of a quadratic equation is identical to the search for successive minima of the expression $(x-\alpha y)^2+\Delta(x-\beta y)^2$, where β designates the second root of the given equation and Δ a positive quantity that grows from 0 to ∞. On the other hand, the search for these minima comes back to the reduction of the binary form $f=(x-\alpha y)^2+\Delta(x-\beta y)^2$ for each value of Δ. While operating this reduction, one finds that the sequence of reduced forms equivalent to f for each value of Δ is obtained by a periodic computation. One is then led to wonder if a certain way of approximating quantities would not provide an analogous periodicity for irrational quantities of degree greater than 2. The consideration of quadratic forms leads to this extension of the theory of continued fractions and provides new methods of approximation.[15]

We shall come back to this programme. Let us remark here 1° that it focusses on the characterization of the roots of algebraic equations, 2° that it relies on some explicit representation of these roots, and 3° that it links the fundamental questions concerning algebraic equations to those concerning quadratic forms, in particular reduction theory. Moreover, there is no clear line of demarcation in this programme between themes usually associated with algebra and arithmetic, such as roots of polynomial equations, and themes associated with analysis, such as approximation. This harmonic

---

15 [Charve 1880, p. 36–37]: *On sait que, si l'on développe en fraction continue une irrationnelle du second degré, le calcul est périodique. Cette périodicité constitue une propriété très remarquable des racines des équations du second degré, et elle peut même servir de définition à ces irrationnelles. Or la théorie des fractions continues est liée étroitement à la théorie des formes quadratiques binaires, de sorte que le développement en fraction continue d'une racine α d'une équation du second degré est identique à la recherche des minima successifs de l'expression $(x-\alpha y)^2+\Delta(x-\beta y)^2$, où β désigne la deuxième racine de l'équation considérée et Δ une quantité qu'on fait croître positivement de 0 à ∞. D'un autre côté, la recherche de ces minima revient à la réduction de la forme binaire $f=(x-\alpha y)^2+\Delta(x-\beta y)^2$ pour toute valeur de Δ. En opérant cette réduction, on trouve alors que la suite des formes réduites équivalentes à f pour toute valeur de Δ s'obtient par un calcul périodique. On est alors conduit à se demander si quelque mode d'approximation des quantités ne donnerait pas une périodicité analogue pour les irrationnelles d'un degré supérieur au second. C'est la considération des formes quadratiques qui conduit à cette extension de la théorie des fractions continues, et donne ces nouvelles méthodes d'approximation.*

mixing is quite representative of Hermite's approach and will be seen at work in all his reflections on Galois's questions.

1.1. *Galois's theorem on periodic continued fractions*

Galois's first publication is precisely a follow-up of Lagrange's theorem. As has now been mentioned twice, this theorem states that the development as a continued fraction of a real irrational root of a quadratic equation with integral coefficients is periodic; reciprocally if the development as a continued fraction of a real number (of "a quantity" as was said at the time) is periodic, the number verifies a quadratic equation with integral coefficients. For instance, [Serret 1885, p. 54], the development as a continued fraction of the root $\frac{97-\sqrt{1093}}{54}$ of the quadratic equation $27x^2-97x+77$ is

$$2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{3+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{3+\cdots}}}}}}}$$

where the periodicity appears after the first two terms.

As for Galois's result, it displays a relation between continued fractions associated with the two roots of the same quadratic equation. More specifically, if the development as a continued fraction of one real root α is in Galois's words "immediately periodic," that is, if the periodicity appears at the first term (Serret calls this a "simply periodic" continued fraction, we would say "purely periodic"), the development of $\frac{-1}{\beta}$, where β is the second root, is also immediately periodic; moreover, its period is that of α, but in the reverse order.

To illustrate this statement, let us adapt the example above and choose

$$\alpha = 2+\cfrac{1}{4+\cfrac{1}{3+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{3+\cdots}}}}},$$

which is easily seen to verify the equation $13x^2 - 25x - 9 = 0$. Then the theorem says that the other root β is such that

$$\frac{-1}{\beta} = 3 + \cfrac{1}{4 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2 + \cdots}}}}},$$

Galois describes his proof for a root α greater than 1 and a period of 4 terms, for, he writes, "the uniform course of the calculation proves that it would be the same were we to choose more terms," [Galois 1828–1829, p. 295]. After noticing that, in this case, the root α verifies an equation

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

he manipulates the continued fraction, expressing $a - x$ from the first line, then extracting $\frac{1}{a-x}$, etc., until he obtains another expression, this time of $\frac{-1}{x}$, with the coefficients in the reverse order, and which is then associated with the other root. Galois also shows that immediate periodicity exactly occurs when one of the roots of the quadratic equation is greater than 1, and the other root between -1 and 0 (in our example, $\alpha = 2.23\ldots$ and $\beta = -0.31\ldots$).[16] He concludes his paper with a few simple consequences for the transformation and solution of quadratic equations.

Despite the elementary nature of the paper, its wording renders it sometimes slightly confusing, as some hypotheses are missing or mixed up with the conclusions. But this early paper also displays a way of doing mathematics that fits well with Caroline Ehrhardt's description of Galois's later work on equations: an immersion in the functioning of a significant example in order to seize a general scheme. However, here, both in the theme and the presentation—in particular the concrete applications of the main theorem

16 Quadratic irrational real numbers greater than 1, the conjugates of which lie between -1 and 0, are now called "reduced." Their interest lies in particular in their connection with the theory of reduction of quadratic forms with positive determinants, [Perron 1929, p. 80], though this link does not seem to have been commented on at the time, except in [Lebesgue 1831].

at the end—Galois complies with the standards of what was called "analysis" at the time, by "adapting the result to make it operational for families of cases," in Ehrhardt's terms ([Ehrhardt 2007, p. 159–163]).

1.2. *Hermite's proof*

Hermite's explicit interest for this elementary result appears to be one of pedagogical resistance. In the autumn of 1884, he wrote to Rudolph Lipschitz in Bonn: "Allow me a small remark in order to protest against the ban in our *mathématiques spéciales* curriculum against proving that the development into a continued fraction of the square root of an integer is periodic."[17] He then provided a (new) proof of Lagrange's statement, "simple enough to be given in a lesson," followed a month later by a shortening of Galois's proof, "a single little remark," as Hermite described it, as he had just suffered a benign attack of cholera. Both proofs were then reproduced from these letters almost verbatim in the *Bulletin des sciences mathématiques*, [Hermite 1885].

The approach is vintage Hermite, periodicity being linked to finiteness, as in Charve's thesis.[18] Let $Ax^2 + 2Bx + C = 0$ be a quadratic equation with integral coefficients and two real roots a and b (Hermite assumed for simplicity that one of them, say a, is positive). One then has the relation (in a notation adapted from Hermite's):

$$a = \frac{P'\lambda + P}{Q'\lambda + Q}$$

where $\frac{P}{Q}$ and $\frac{P'}{Q'}$ are two consecutive convergents of the continued fraction attached to a and λ the complete quotient corresponding to $\frac{P'}{Q'}$.[19] Then λ (a real number greater than 1, as all the terms in the continued fraction after the first are strictly positive integers) is a solution of another quadratic equation, with the same discriminant. Hermite easily shows that, from a

---

17 Letters 59 and 60 in Nachlass Lipschitz, Universitäts- und Landesbibliothek Bonn, Handschriften: *Permettez-moi une bien petite remarque pour protester contre la défense que l'on fait dans notre enseignement des mathématiques spéciales, de démontrer que le développement en fraction continue de la racine carrée d'un nombre entier est périodique.* Hermite often complained about the changes introduced by the Republic.

18 Indeed, Charve published essentially the same proof of Lagrange's theorem in [Charve 1877].

19 If $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$ is a continued fraction, a "convergent" (or "reduced fraction") is the (usual) fraction obtained by truncating the development at one of the

certain convergent on, the other root of this equation is negative and bigger than -1, and thus that the coefficients of the quadratic term and of the constant term of the equation have different signs. Then the middle coefficient is bounded (its square is smaller than the discriminant of the given equation), and thus also the two other coefficients. There are thus a finite number of possible equations in λ, thus a finite number of possible λ or of its integral part; but these integral parts are also the incomplete quotients, that is the successive integers composing the continued fraction of a. Thus this continued fraction must be periodic.

As for Galois's theorem (which Hermite qualifies as "of great interest"), he deduces it in the following way: assuming now that the development of a is "immediately periodic," he designates by $\frac{P}{Q}$ a convergent representing a full period in this development, and by $\frac{P_0}{Q_0}$ the preceding convergent. Then

$$a = \frac{Pa + P_0}{Qa + Q_0}$$

and Hermite shows that $\xi =: -\frac{1}{b}$ verifies

$$\xi = \frac{P\xi + Q}{P_0\xi + Q_0}.$$

The basic theory of continued fractions then says that $\frac{P}{P_0}$ is a full period in the continued fraction of ξ, that $\frac{Q}{Q_0}$ is the convergent before $\frac{P}{P_0}$, and that $\frac{P}{P_0}$ has the same incomplete quotients as $\frac{P}{Q}$, but in reverse order.[20] This gives directly the expected statement. While Galois seemed literally to *see* the result from manipulating the graphical display of the continued fraction, Hermite operated on the *known polynomial formulas* giving the numerators and the denominators of the convergents.

---

a_i. The corresponding "complete quotient" is what is left of the continued fraction, that is $a_{i+1} + \cfrac{1}{a_{i+2} + \cfrac{1}{a_{i+3} + \cdots}}$. The a_i are called "incomplete quotients."

[20] For instance, with a 3-term period, $\frac{P}{Q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}$ and $\frac{P_0}{Q_0} = a_0 + \frac{1}{a_1}$, giving $P = a_0a_1a_2 + a_0 + a_2$, $P_0 = a_0a_1 + 1$, $Q = a_1a_2 + 1$ and $Q_0 = a_1$. Thus $\frac{P}{P_0} = a_2 + \cfrac{1}{a_1 + \cfrac{1}{a_0}}$.

1.3. *A name and a theorem*

The *Encyklopädie der mathematischen Wissenschaften* attributed to Galois the first recognition of a relation between the continued fractions attached to the two roots of a quadratic equation, [Pringhseim 1898, p. 132], and from the end of the nineteenth century until now, Galois's theorem, as it is usually called, has benefitted from a faint but steady interest. It was integrated under Galois's name into various syntheses concerning continued fractions or roots of equations, for instance, in Eugène Cahen's *Théorie des nombres*, [Cahen 1914–1924, vol. 2, p. 205] or, more decisively because of its fame, in Oskar Perron's influential *Die Lehre von den Kettenbrüchen*, [Perron 1929, p. 80 and p. 82–85].

This attribution, however, seems to be a late phenomenon, and not without reason. Adrien-Marie Legendre for instance had devoted a whole section of his *Essai sur la théorie des nombres*, to the "comparison between the continued fractions resulting from the development of the two roots of the same quadratic equation," and had proved the reciprocal relation of their periods.[21] Still, Galois's result did not go unnoticed after its publication in the *Annales de Gergonne*. His "curious result," as it is here qualified, was reported in detail in Férussac's *Bulletin des sciences mathématiques* (vol. 11, p. 254–255). This report in the *Bulletin* was read by Augustus Möbius who integrated "the way in which two periodic continued fractions correspond as roots of a quadratic equation" into his own research on dioptrics, attributing it to Galois [Möbius 1830, p. 234]. A few issues of Crelle's *Journal* later, Moritz Stern again referred to Galois's result in the prelude to a long series of articles on continued fractions, but this time he also noticed the analogy with Legendre's result, [Stern 1832, p. 193]. In 1831, in any case, Victor-Amédée Lebesgue published in Férussac's *Bulletin* his own (slightly generalized) version of the theorem; while acknowledging Galois's article in a footnote, he added:

> I shall remark that, as early as 1828, I had sent from Russia a note identical to the present one, that it was transmitted to M. Dupré, a student at the École normale; but that he apparently did not succeed in inserting it into the *Annales de mathématiques* as he wished.[22]

---

21 See [Legendre 1798, §X]. Legendre's interest lying in the values of quadratic forms and in Pell equation, he did not pay particular attention neither to the property of pure periodicity, nor to the associated condition on the size of the roots as such, but this implicitly appears in §XIV.

22 [Lebesgue 1831]: *Je ferai observer que j'avais dès 1828 envoyé de Russie une note conforme à celle-ci, qu'elle fut remise à M. Dupré, élève à l'École normale; mais qu'il ne put à ce qu'il paraît la faire insérer dans les Annales mathématiques comme il le désirait.*

When the result was then discussed by Christian Ramus, at the Royal Society of Sciences in Copenhagen (with an extract published in Crelle), Ramus recognized, after proposing his own proof, that "this remarkable analogy between the continued fractions resulting from the development of the two roots of the same quadratic equation has not escaped the attention of the mathematicians,"[23] mentioning only Legendre and Lebesgue. Variants, by Lebesgue again or by Eugène Catalan, would appear in the 1840s in Liouville's *Journal* and in the *Nouvelles Annales*, and of course later still in the above-mentioned *Algèbre supérieure* of Serret, with no special reference to Galois.

Minor though it may seem, the fate of this early contribution of Galois is thus rather instructive. It already shows several phenomena that we shall find again concerning his work on equations and groups. It indicates that Galois had, at the beginning of his life, a reasonable access as an author to well-circulated publications, like the *Annales* of Gergonne—an access that was not so easy for many. In addition, while Galois seems to find the relations between the two continued fractions by hand, following closely simple transformations, the result was immediately taken up in an organized body of knowledge and furnished with new, more complete, proofs.

But at the end of the nineteenth century, the success of algebraic continued fractions gave an impulse to the creation of a new autonomous domain, which rendered rather trivial the results of the 1830s and 1840s and marginalized their authors; about that time, Galois's posthumous fame was growing. The collective memory of mathematicians concerning continued fractions then suffered a break; while in the 1840s, Galois was only one of several authors mentioned for their contributions to the comparison between the development in continued fractions of the two real roots of a quadratic equation, Galois's name alone was definitively attached to it by the end of the century, a development in which Hermite had pointed the way.

2. MODULAR (AND QUINTIC) EQUATIONS

Still following the order of Galois's texts in Liouville's journal, we see that the second topic to which Hermite contributed appeared in the "Analyse d'un mémoire sur la résolution algébrique des équations" and again in

---

23 [Ramus 1839, p. 14]: *Cette analogie remarquable des fractions continues résultantes du développement des deux racines d'une même équation du second degré n'a pas échappé aux géomètres.*

the 1832 letter to Auguste Chevalier, [Galois 1846, p. 396 and p. 410–413]. It concerns the application of Galois's ideas about equations to those arising from elliptic functions, in particular modular equations.

The objectives of the theory of polynomial equations were defined in many ways during the nineteenth century. Expressing the roots in terms of the coefficients of the equation, by means of the usual *five* algebraic operations (addition, subtraction, multiplication, division and extraction of radicals) had been at the center of attention until Niels Abel, in particular, proved that such a resolution was not to be expected in general after degree 4; but it had not been the single purpose of the theory, nor did Abel's result close the matter until Galois theory took the lead. Other possibilities existed and others opened up during the course of the century: situating the zeroes of the polynomial, computing them with sufficient approximation for various practical purposes, discovering interesting types of equations solvable by radicals, finding other simple auxiliary irrational quantities[24] from which the roots might be derived, etc. Accordingly, various families of equations occupied the front of the stage, either as privileged applications, or as inspirational models: after Gauss's *Disquisitiones arithmeticae*, for instance, cyclotomic equations (arising from irreducible factors of $x^n - 1$, whose zeroes are roots of unity) played such a role.[25]

These objectives, some compatible, some not, cannot be ignored as they were part and parcel of the mathematical work, motivating it of course, but also motivated by it. Though the later development of Galois theory and group theory favoured a retrospective interpretation of Galois's writings in terms of structures, see[Ehrhardt 2007], his concrete programme remains elusive. Hermite had more time than Galois to express his in detail and I shall adopt his perspective in this section—and thus his particular centers of interest, quintic (that is, fifth degree) equations and forms, and modular equations (arising from the transformation theory of elliptic functions, as will be explained later). Still, one should be aware of two problems that might blur this perspective: the first is the screen thrown upon Hermite's approach by Felix Klein's geometrical frame, [Klein 1884], which for all

24 One has of course to keep in mind that explicit "quantities" proved not "to be reducible to algebraic irrationals," that is, transcendental numbers, only appeared in Liouville's 1844 work, see [Waldschmidt 1983], while the very concepts of quantity and number were actively discussed in the second half of the century, see in particular [Boniface 2007] and [Petri & Schappacher 2007].

25 On this example, and in particular its use by Galois, see [Goldstein & Schappacher 2007a, p. 19–24 and p. 34–36] and [Neumann 2007, p. 119–122]. This role of special types of equations is clearly displayed in the table of contents of [Serret 1885] and [Jordan 1870].

its convincing coherence dislocated the disciplinary structure congenial to Hermite; we shall return to this later. The second problem is that, although the chronology of Hermite's work bears on the appreciation of his programme, it is difficult to establish it precisely. I shall explain this point now.

Hermite's involvement with equations goes back to his earliest mathematical days; the very first issue of the *Nouvelles Annales de mathématiques*, a journal intended for students preparing the examinations for the École polytechnique and other schools, included a paper by Hermite, then a student in Richard's class at Louis-Le-Grand, on the general equation of the fifth degree, [Hermite 1842]. In this paper, Hermite offers a proof that Lagrange's resolvent equation (*équation résolvante*) for the quintic cannot generally be factorized into quadratic or cubic factors and thus be solved by radicals.

For a given algebraic equation, a resolvent was a certain function of the roots which has interesting properties (for instance it takes a rather small number of values) when the roots are permuted in all possible ways. The equation whose roots are these various values of the resolvent is then called the resolvent equation and it serves as an auxiliary equation to solve the given one. In the case of the quintic, Lagrange's resolvent is a function of the five roots which takes only 6 different values when the roots are permuted (instead of the 5! values one could expect from the 5! permutations of the 5 roots). Thus there is in this case a resolvent equation of degree six, the solution (by radicals) of which would provide the solution of the initial quintic, see [Lagrange *Œuvres*, vol. 8, n. XIII, in particular p. 324]. Mentioning only Lagrange, Hermite's article relies upon a study of functions of 5 variables taking only 6 values and upon a detailed analysis of the permutations on 5 letters and their possible decompositions—two types of questions linked to the construction of the resolvent, and which will remain key questions in the theory of equations during the whole nineteenth century.

After 1842, however, Hermite turned to elliptic and Abelian functions and would not return to the fifth degree equations until 1854, [Hermite 1854, Hermite 1856], as part of more general work on invariants of forms, and then from 1858 on, in a series of notes in the *Comptes rendus des séances hebdomadaires de l'Académie des sciences*, of which he had become a member in July 1856, [Hermite 1858a, Hermite 1865]. This time, he linked explicitly his work on the quintic to the modular equation of order 6. It is only here and in a later series of notes in the *Comptes rendus* entirely devoted to modular equations, [Hermite 1859], that he discussed and proved Galois's statement on the reduction of modular equations of order 5, 7, and 11—a

work announced, as previously mentioned, in the second of his letters to Jacobi on the theory of numbers written a decade earlier, in 1847, that is *just after* the republication of Galois's articles by Liouville.

Hermite's contacts with Liouville dated from his time at the Polytechnique and, indeed, one of the first mentions of Liouville's project concerning the publication of Galois was in 1843, after he presented some of Hermite's results on Abelian functions to the Academy, see [Belhoste & Lützen 1984]. Although Hermite's work during these years is above all considered as an important contribution to the theory of Abelian functions, algebraic aspects also were still essential for him. In the memoir presented then to the Academy, Hermite stated:

> The main object of Abel's first memoir on the theory of elliptic functions is the resolution of equations relative to their division into equal parts. The beautiful result at which he arrived, that is, that this resolution is always possible by radicals, if one supposes that the division of the complete function is known, [...] can be extended to these higher-order transcendants that Legendre called *ultra-elliptic functions* [...] This is what we shall try to see.[26]

Bruno Belhoste and Jesper Lützen have in fact suggested that around 1844-45, Hermite, as well as Serret and Bertrand (who both published at this time papers on functions of n variables having a definite number of values, see [Serret 1885, vol. 2, sec. IV, ch. V]) attended Liouville's private lessons on Galois's papers, [Belhoste & Lützen 1984]. Indeed, in the middle of a communication to the Academy of Sciences, Augustin Louis Cauchy alluded to a conversation with Hermite on November 19, 1845, during which the latter announced a construction of a transitive function of 6 variables with 6 distinct values:

> In the Memoir I published, about thirty years ago, *On the number of values that a function may acquire when the quantities it contains are permuted in all possible ways*, I had represented these quantities by letters with indices, and the indices by numbers. [...] It is also by substituting numbers for the various variables on which a function depends, that M. Hermite told me he succeeded, not only in showing the existence of a transitive function of six variables having six distinct values,

---

26 [Hermite 1848, p. 38]: *L'objet principal du premier Mémoire d'Abel sur la théorie des fonctions elliptiques est la résolution des équations relatives à leur division en parties égales. Le beau résultat auquel il est parvenu, savoir que cette résolution est toujours possible à l'aide de radicaux, en supposant connue la division de la fonction complète, peut être étendu aux transcendantes d'ordre plus élevé nommées par Legendre* fonctions ultra-elliptiques *[...] C'est ce qu'on va essayer de voir.* See also his first letter to Jacobi in 1843, [Hermite *Œuvres*, vol. 1, p. 10–17]. Galois of course also discussed these questions, but Hermite did not mention him here, only refering to Legendre, Abel, Jacobi.

> but also in obtaining other results, in particular some relative to the prime numbers 5, 7, 11 and applicable to the theory of the three modular equations whose degrees are these prime numbers increased by one.[27]

The letters on number theory written from 1847 on to Jacobi, in the middle of which Galois's name appeared for the first time in Hermite's printed papers, in connection with the reduction of modular equations, are thus less of a thematic break than might appear. Elliptic functions, algebraic equations and forms, this time sprinkled with some Gaussian arithmetic, are again united in a tightly coherent frame.[28] While some elements (for instance, the use of Lagrange's resolvents, this time to construct quadratic forms) are reminiscent of Hermite's previous interest, others already point to the 1854 series of articles. The announcement of his proof of Galois's statement is just one more illustration of these links. While the consideration of the titles or the results, as well as the loose style of writing, might give a superficial impression of fits and starts, with new elements incorporated as his readings of other mathematicians proceeded, a closer look then displays long threads running through the fabric of Hermite's articles until the 1860s at least, with recurrent constructions and favorite objects. Among them figure prominently modular equations.

2.1. *Modular Equations: an introduction*

The label "modular equations" includes various equations connected with the theory of the transformation of elliptic functions. For the sake of simplicity, I shall here only briefly explain what is relevant to our discussion of Galois and Hermite.[29]

---

27 [Cauchy *Œuvres*, 1re sér., vol. 9, p. 458–459]: *Dans le Mémoire que j'ai publié, il y a trente ans environ,* Sur le nombre des valeurs qu'une fonction peut acquérir, quand on y permute de toutes les manières possibles les quantités qu'elle renferme, *j'avais représenté ces quantités par des lettres affectées d'indices, et les indices par des nombres. [. . .] C'est aussi en remplaçant par des nombres les diverses variables desquelles une fonction dépend, que M. Hermite m'a dit être parvenu, non seulement à constater l'existence de la fonction transitive de six variables qui offre six valeurs distinctes, mais encore à d'autres résultats spécialement relatifs aux nombres premiers 5, 7, 11, et applicables à la théorie des trois équations modulaires dont les degrés sont ces nombres premiers augmentés de l'unité.* A function of n variables is transitive when (the group of) the substitutions of the variables which fix the function can transform any of the variables into any other, that is in more modern terms when this group is transitive (the terminology is due to Cauchy). A week later, on January 5, 1846, Cauchy wrote down Hermite's proof on the existence of this transitive function, [Cauchy *Œuvres*, 1re sér., vol. 9, p. 34–35].

28 On these letters in particular and their developments, see [Goldstein 2007].

29 Accordingly, Jacobi's point of view, [Jacobi 1829], is here privileged. See [Cayley 1876] for a detailed nineteenth-century presentation in the same spirit, [McKean &

Elliptic functions had been introduced at the turn of the century in connection with such integrals as

$$t(k,\Theta)=\int_0^{\Theta}\frac{d\theta}{\sqrt{1-k^2\sin^2\theta}},\qquad \text{for, say, } k \text{ real and } 0<k<1,$$

or, with $x=\sin\theta$,

$$\int_0^X\frac{1}{\sqrt{(1-x^2)(1-k^2x^2)}}dx.$$

Following Jacobi, the parameter k is called the modulus; k', such that $k^2+k'^2=1$, the complementary modulus; Θ (or am) the amplitude.

For $k=0$, such integrals would give rise to inverse circular functions: $\arcsin X=\int_0^X\frac{dx}{\sqrt{1-x^2}}$, or, up to multiples of 2π, $t=\int_0^{\sin t}\frac{dx}{\sqrt{1-x^2}}$.

This motivated the introduction and study of new functions, such as $\sin\mathrm{am}(.,k)$—or $\mathrm{sn}(.,k)$ in Christoph Gudermann's simplified notation:

$$t=\int_0^{\mathrm{sn}(t,k)}\frac{1}{\sqrt{(1-x^2)(1-k^2x^2)}}dx,$$

as well as analogous functions cn $(.\,,k)$ and dn $(.\,,k)$, with $\mathrm{cn}^2=1-\mathrm{sn}^2$ and $\mathrm{dn}^2=1-k^2\mathrm{sn}^2$. Addition formulas analogous to those for circular functions exist for these elliptic functions. The elliptic integrals K and K':

$$K=\int_0^1\frac{1}{\sqrt{(1-x^2)(1-k^2x^2)}}dx,$$

$$K'=\int_0^1\frac{1}{\sqrt{(1-x^2)(1-k'^2x^2)}}dx,$$

called the complete elliptic integrals, play a role analogous to π. Indeed, elliptic functions were shown to be doubly periodic; their periods are given by suitable combinations of $2K$ and $2iK'$ (for instance sn has the periods $4rK+2ir'K'$, with r and r' arbitrary integers).

As for circular and exponential functions, these properties give rise to algebraic equations. For instance, for a prime p, the cyclotomic equation $x^{p-1}+x^{p-2}+\cdots+1=0$ has for roots the non-trivial pth-roots of unity, that is the complex numbers $e^{\frac{\Omega}{p}}$, where Ω is a period of the exponential, $\Omega=2li\pi$, for $1\le l\le p-1$. For a prime p and a fixed modulus k, the values of the elliptic functions on $\frac{\Omega}{p}$, for Ω a period, also verify an algebraic

---

Moll 1999] for nicely established links with a contemporary perspective, and [Houzel 1978] for an overall history of the subject, explaining in particular the respective contributions of Legendre, Gauss, Abel, and Jacobi to the birth of the topic.

equation, this time of degree $p^2 - 1$, the so-called "equation of the division of the complete function"; Abel proved it to be solvable by radicals. Another equation, of degree p^2, came from the expression of $\mathrm{sn}(t,k)$ as a function of $\mathrm{sn}(\frac{t}{p},k)$ ("equation relative to the division into equal parts"). Both equations were the topic of intense studies (including by Galois) and are alluded to in Hermite's memoir quoted p. 228.

However, elliptic functions also displayed new features as compared to circular functions, in particular transformation theory. The point of this theory was to establish algebraic relations between elliptic functions of argument t and modulus k and elliptic functions of argument $\frac{t}{M}$ and another modulus λ. More precisely, k being given, one looked for a rational function $y = y(x) = \frac{U(x)}{V(x)}$, a modulus λ, and a constant M such that:

$$\frac{dy}{\sqrt{(1-y^2)(1-\lambda^2 y^2)}} = \frac{1}{M}\frac{dy}{\sqrt{(1-x^2)(1-k^2x^2)}}.$$

Choosing U and V relatively prime, U and V are given by polynomials of respective degree n and $n-1$ in x, with n being called the order of the transformation. If k is fixed, both the new modulus λ and the constant M (the *multiplier*) are given by irreducible algebraic equations of degree $n+1$, respectively known as the *modular equation* and the *multiplier equation*.

The complete elliptic integrals K and K' are obviously functions of the moduli k and k'. But reciprocally, k and k' can be expressed as functions of $\omega = i\frac{K'}{K}$. There exist two analytic functions of one complex variable, ϕ and ψ, such that $\phi(\omega) = \sqrt[4]{k}, \quad \psi(\omega) = \sqrt[4]{k'}$. In the *Fundamenta nova theoriae functionum ellipticarum*, [Jacobi 1829], Jacobi gave various developments in q-series of these functions ($q = e^{\pi i\omega}$) and used them to express the modular equations and solve the transformation problem.

For $n = 3$, for instance, if one puts $u = \phi(\omega) = \sqrt[4]{k}$, the modular equation in $v = \sqrt[4]{\lambda}$ is the fourth-degree equation

$$u^4 - v^4 + 2uv(1 - u^2v^2) = 0, \tag{1}$$

and the multiplier is given by the equation

$$3M^4 + 8(1 - 2u^8)M^3 + 6M^2 - 1 = 0.$$

Choosing a solution of the modular equation v and $M = \dfrac{v}{v+2u^3}$ yields $y = \dfrac{(v+2u^3)vx + u^6x^3}{v^2(1+v^3u^2(v+2u^3)x^2)}$.[30]

For $n = 5$, the case which will principally occupy us, the modular equation is

$$u^6 - v^6 + 5u^2v^2(u^2 - v^2) \pm 4uv(1 - u^4v^4) = 0. \tag{2}$$

Jacobi also gave analytic expressions for the solutions of these equations in terms of special values of the elliptic functions sn, cn, dn.

Hermite favoured an explicit form of the roots of the modular equation; one clearly displaying the fact that the transformation of order p (say, for p an odd prime number) links the modulus $k(\omega)$ and the modulus $k(p\omega)$. For a, d odd integers, b, c even integers such that $ad - bc = 1$, one has:

$$\sqrt[4]{k\left(\frac{a\omega+b}{c\omega+d}\right)} = (-1)^{\frac{a^2+ab-1}{8}} \sqrt[4]{k(\omega)} \tag{3}$$

and it then follows that the polynomial of degree $p+1$

$$\left[v - \left(\frac{2}{p}\right)\sqrt[4]{k(p\omega)}\right] \prod_{0\le l<p} \left[v - \sqrt[4]{k\left(\frac{\omega+16l}{p}\right)}\right] \tag{4}$$

has coefficients which are rational in $u = \phi(\omega)$.[31] This provides again the modular equation.[32]

---

[30] See [Jacobi 1829, p. 74] and [Cayley 1876, p. 188]. Another form of the modular equation of order 3, given by Legendre, is $\sqrt{k\lambda} + \sqrt{k'\lambda'} = 1$. Depending on the normalization of v, small variants also appear in the literature, cf. [Weber 1891, p. 22–23 and 283–284].

[31] As usual, $\left(\frac{\cdot}{p}\right)$ means the Legendre symbol modulo p, that is, for p an odd prime, $\left(\frac{2}{p}\right) = 1$ if 2 is congruent to a square, modulo p, and -1 if not; in particular it is -1 for $p = 3, 5, 11$ and 1 for $p = 7$.

[32] From the end of the nineteenth century on, moduli k withdrew in favour of absolute invariants j and the modular equation is now taken as linking $j(p\omega)$ and $j(\omega)$. In more modern terms, transformations correspond to isogenies between two elliptic curves, $\mathbf{C}/L'$ and $\mathbf{C}/L$, the lattice L', associated to the first, being a sublattice of index p of the lattice L associated to the second. The periods of the L' are deduced from the periods of L by a linear transformation with integral coefficients and determinant p. The decomposition in the formula (4) thus reflects the partition of the set of these transformations into $p+1$ equivalence classes under $SL_2(\mathbf{Z})$; representatives of the classes are $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & l \\ 0 & p \end{smallmatrix}\right)$, for $0 \le l < p$. This explains the formula (4). The extra factor 16 which appears in the formula comes from the fact that k^2, unlike j, is not invariant under $SL_2(\mathbf{Z})$, but under a smaller group. See [McKean & Moll 1999, ch. 4] for details.

Thus, for $p = 3$, for instance, the equation (1), again with $u = \phi(\omega) = \sqrt[4]{k(\omega)}$, has the 4 roots: $-\phi(3\omega)$, $\phi(\frac{\omega}{3})$, $\phi(\frac{\omega+16}{3})$ and $\phi(\frac{\omega+2.16}{3})$.

2.2. *Modular equations: Galois*

Two allusions to modular equations can be found in Galois's papers published by Liouville in 1846.[33] In a short 1830 memoir in the *Bulletin* de Férussac, Galois announced that "it is remarkable that the modular equation of the sixth degree, corresponding to the number 5, can be reduced to one of the fifth degree, of which it is a resolvent equation."[34] At this stage, he still believed that this was a unique exception, an error he would soon correct, adding 7 and 11 to the list of such exceptional cases. On May 29, 1832, his letter to Auguste Chevalier presented the study of modular equations as an application of the general theory of equations:

> The last application of the theory of equations is relative to modular equations of elliptic functions. [...] The modular equation corresponding [to the transformation of order p] will have as its group
>
> $$x_l \qquad x_{\frac{al+b}{cl+d}}$$
>
> in which l can take the $p+1$ values $\infty, 0, 1, 2, \ldots, p-1$. [...] If we assign all possible values to a, b, c, d, we obtain $(p+1)p(p-1)$ permutations. But this group properly decomposes into two groups whose substitutions are $x_l \quad x_{\frac{al+b}{cl+d}}$, $ad-bc$ being a quadratic residue of p. It cannot be properly decomposed any further, except if $p = 2$ or $p = 3$. Thus, whatever the way in which the equation is transformed, its group will always have the same number of permutations. But it is intriguing to know if the degree can decrease. [...] For the cases $p = 5, 7, 11$, the modular equation can be reduced to the degree p. This reduction is not rigourously possible in higher cases.[35]

---

33 There are many others in the manuscripts of course, see for instance [Galois 1962, p. 244–245, p. 265, p. 297].

34 [Galois 1846, p. 396] and [Galois 1962, p. 165]: *Il est remarquable que l'équation modulaire du 6^e^ degré, correspondant au nombre 5, peut s'abaisser à une du cinquième degré dont elle est la réduite.*

35 [Galois 1846, p. 410–412] and [Galois 1962, p. 177-181]: *La dernière application de la théorie des équations est relative aux équations modulaires des fonctions elliptiques. [...] L'équation modulaire correspondant [à la transformation d'ordre p] aura pour groupe* $x_l \quad x_{\frac{al+b}{cl+d}}$ *dans laquelle l peut avoir les* $p+1$ *valeurs* $\infty, 0, 1, 2, \ldots, p-1$. *[...] En donnant à* a, b, c, d, *toutes les valeurs, on obtient* $(p+1)p(p-1)$ *permutations. Or ce groupe se décompose proprement en deux groupes dont les substitutions sont* $x_l \quad x_{\frac{al+b}{cl+d}}$, $ad-bc$ *étant un résidu quadratique de* p. *[...] Il n'est plus décomposable proprement, à moins que* $p = 2$, *ou* $p = 3$. *Ainsi de quelque manière que l'on transforme l'équation, son groupe aura toujours le même nombre de permutations. Mais il est curieux de savoir si le degré peut s'abaisser [...] Pour les cas de* $p = 5, 7, 11$, *l'équation modulaire s'abaisse au degré* p. *En toute rigueur, cette réduction n'est*

A priori there could be $(p+1)!$ possible permutations of the $p+1$ roots of the modular equation of order p. The "group of the equation," in Galois's terms, is only a subset.[36] It keeps trace of all the rational relations among the roots of the equation. More precisely, it is such that any rational function of the roots which takes the same value when applied to all the permutations of the roots belonging to the group—a function which is invariant under the corresponding substitutions, Galois also says—is in fact rational in the coefficients of the equation; and reciprocally, a function of the roots which is rationally defined in the coefficients of the equation takes a single value when applied to the permutations of the group.[37]

As seen in the formula (4), the roots of the modular equation can be indexed by l, l taking $p+1$ values, $\infty, 0 \quad 1 \quad 2 \quad \dots p-1$:

$$x_\infty = -\sqrt[4]{k(p\omega)}, \quad x_l = \sqrt[4]{k(\frac{\omega + 16l}{p})}.$$

The possible permutations among the roots can thus be described as transformations on the indices l, thanks to formulas analogous to (3) above. Galois thus stated that there are only $p(p^2-1)$ relevant permutations in the group of the modular equation, and thus $p(p^2-1)$ transformations on the indices. These transformations are represented in modern terms by the group $PGL_2(\mathbf{F}_p)$ of homographies of the plane over the finite field $\mathbf{F}_p$. This gives the first part of the statement. For Galois, it seems to result from the analogous statement for the equation giving the division of the periods, supposed to be already known.

For $n > 3$, $PGL_2(\mathbf{F}_p)$ has only one normal subgroup, $PSL_2(\mathbf{F}_p)$, of index 2, corresponding to elements of determinant 1 (or in Galois's equivalent formulation, with determinant a quadratic residue of p). This corresponds to the proper decomposition of the permutations into two blocks (again

pas possible dans les cas plus élevés. Galois used the letter k instead of l, but we need the former for the modulus.

36 In Galois's time, one usually distinguished between "permutations" and "substitutions": a permutation of n objects is an ordered disposition of these objects, while a substitution is the operation transforming one permutation to another. The word "group" is often used to designate a relevant grouping of permutations, while the modern sense of course would refer to a set of substitutions. Following Cauchy, several authors, including Serret who used the concept systematically, spoke of "systems of conjugate substitutions" to refer to what we call now "group." Galois's use of the words varied, as is well explained in Amy Dahan's analysis, [Dahan-Dalmedico 1982]. I shall use "group" in both senses, the context making clear which sense is meant.

37 See [Galois 1962, p. 421]. From the current point of view, the group of the equation would be the group of K-automorphisms of the field generated by the roots, K being the field of the coefficients of the equation.

called "groups" in Galois's letter); each of them is globally fixed by the homographies of $PSL_2(\mathbf{F}_p)$. From the point of view of the equation, this also means that the adjunction of an appropriate quadratic irrational reduces the group of the equation to $PSL_2(\mathbf{F}_p)$. As Galois pointed out, the procedure cannot be repeated since the new Galois group $PSL_2(\mathbf{F}_p)$ does not have a normal non-trivial subgroup if $p > 3$. In particular, the modular equation is not solvable by radicals.

Thus neither from the perspective of algebraic solvability, nor from the later perspective of Galois extensions with its emphasis on the structure of normal subgroups, is there reason to go any further. From the perspective of group theory, a natural question would be to list *all* the subgroups of $PSL_2(\mathbf{F}_p)$ (this will be done by Joseph Gierster, a student of Felix Klein, in 1881, [Gierster 1881]). It is thus an interesting testimony of Galois's full participation in the issues of his time that he would have reflected precisely on the possible "reduction" of the modular equations to lower degrees. As he explained, it is necessary for this that the group of the equation be decomposable into p blocks of $\frac{p^2-1}{2}$ elements. In other terms, one has to find a (not normal) subgroup of index p in $PSL_2(\mathbf{F}_p)$, which in turn defines an algebraic extension of degree p.[38]

In Galois's time, however, the reference was the resolvent equation, and the first results, by Paolo Ruffini and Cauchy, about the number of values taken by a function of p variables under permutations of the variables (a question directly linked to the construction of the resolvent, as we have seen, see [Cauchy *Œuvres*, 2e sér. 1, p. 64–90]). If one gets a partition of the permutations of the $p + 1$ roots of the modular equation, such that there exists a function of the roots taking exactly one value on each block of permutations, thus p values in all, say $z_0, \ldots, z_{p-1}$, then $(X - z_0)(X - z_1) \cdots (X - z_{p-1})$ is the required resolvent equation. It of course comes down to finding a partition of $PSL_2(\mathbf{F}_p)$. The choice of p as the degree of the resolvent equation (and the number of values taken by the function) is imposed by the situation, as Cauchy proved in 1815. Galois himself expressed his results in this language of "functions of the roots," see for instance [Galois 1962, p. 51, p. 75, p. 103]. As previously mentioned, Liouville's project for Galois's papers seemed to have revived an interest in such questions: Bertrand, Serret, Cauchy himself and others published articles in the mid 1840s on the number of values taken by a function of n variables under permutations of its variables. And Hermite's construction

38 A nice presentation in Klein's spirit is given in [Gray 2000, ch. 4, in particular 4.3 and 4.6].

of "a transitive function of 6 letters taking 6 values," which he communicated to Cauchy in November 1845, also seems a transparent reference to $PGL_2(\mathbf{F}_5)$.[39]

2.3. *Decomposing permutations*

The first published proof of the reduction of the modular equations we know is that of Enrico Betti, a part of the sequence of articles in which the Italian mathematician explored Galois's main results, see [Kiernan 1971, Mammone 1989, Ehrhardt 2007]. As Betti described it to Hermite a few years later

> In a memoir [...] published in 1853 in the *Annali di Tortolini*, I studied the substitutions
>
> $$(*) \quad \frac{al+b}{cl+d}$$
>
> to prove the possibility of reducing modular equations, and I obtained the results you communicated to me in your letter. These are, for the prime number $n = 4p+3$, the expressions I had then found for the decomposition in m groups of the group all the substitutions of which are given by the form $(*)$ when $ad-bc$ is a quadratic residue of n. [...] In the case $n = 5$, I obtained results similar to the preceding ones and built a group of twelve permutations while considering the three substitutions $\theta(l) = 4l, \frac{1}{l}, 3\frac{l+1}{l-1}$ and those deducible from them by composition.[40]

In modern terms, in the case $n = 5$, the group of the modular equation (on a quadratic extension) is $PSL_2(\mathbf{F}_5)$ which has 60 elements and no non-trivial normal subgroup. The equation is not solvable by radicals. As explained by Betti, in terms of the roots, the reduction to a fifth-degree equation comes down to finding an adequate partition of their 60 permutations into 5 sets of 12. Betti's partition is reproduced p. 238.

---

39 The substitutions fixing such a function define a subgroup of index 6 (the number of values) of the symmetric group on 6 letters, that is, a group with 120 elements. Because of transitivity, it is not however the stabilizer of one of the letters—in the vocabulary of the time, "it is not built up from the 120 substitutions of 5 letters."

40 Letter from Betti à Hermite, March 24, 1859 in [Hermite *Œuvres*, vol. 2, p. 73–75]: *Dans un mémoire [...] publié en 1853 dans les* Annali di Tortolini, *j'ai fait l'étude des substitutions* $(*)$ $\frac{al+b}{cl+d}$ *pour démontrer la possibilité de l'abaissement des équations modulaires, et j'ai obtenu les résultats que vous me communiquez dans votre Lettre. Voici pour le module premier* $n = 4p+3$ *les expressions que j'ai trouvées alors pour la décomposition en* n *groupes du groupe dont toutes les substitutions sont données par la forme* $(*)$ *où* $ad-bc$ *est un résidu quadratique de* n. *[...] Dans le cas où* $n = 5$ *j'avais obtenu des résultats semblables aux précédents et formé un groupe de douze permutations en considérant les trois substitutions* $\theta(l) = 4l, \frac{1}{l}, 3\frac{l+1}{l-1}$, *et celles qu'on en déduit en les composant entre elles.*

Each set of 12 permutations is deduced from the preceding set by the substitution $l \to l+1$ (up to multiples of 5). For instance, by this substitution, the first permutation of the first set (L), that is $(\infty, 0, 2, 3, 4, 1)$ goes to $(\infty, 1, 3, 4, 0, 2)$, which is the first permutation of the second set (L_1); the third permutation of the first set (L), that is $(\infty, 0, 3, 2, 1, 4)$, goes to $(\infty, 1, 4, 3, 2, 0)$, the third permutation of the second set (L_1), etc. Inside each set, the permutations are generated from the first one by the substitutions $\theta(l) = 4l, \frac{1}{l}, 3\frac{l+1}{l-1}$ or compositions thereof. For instance, $(\infty, 0, 2, 3, 4, 1)$ is sent to $(\infty, 0, 3, 2, 1, 4)$ by $l \to 4l$, to $(3, 2, 4, 1, 0, \infty)$ by $l \leftarrow 3\frac{l+1}{l-1}$, etc.

Betti also gave the relevant forms for the two other cases, $n = 7$ and $n = 11$. I shall not comment on the proof except to say that it relies in particular on the use of primitive roots modulo n to reindex the indices, following the model of Gauss's treatment of the cyclotomic equation. The way the various substitutions are represented plays in fact an important role, as testified to by the numerous remarks made by the mathematicians of the time on this particular issue. It is one of the contexts for Galois's elaboration of his imaginary solutions to congruence equations, and it allows what would come to be known as "the analytic representation of a substitution." As Serret explained in his *Cours d'algèbre supérieure*, [Serret 1885, vol. 2, p. 383–384], "in most cases when we have to consider substitutions of

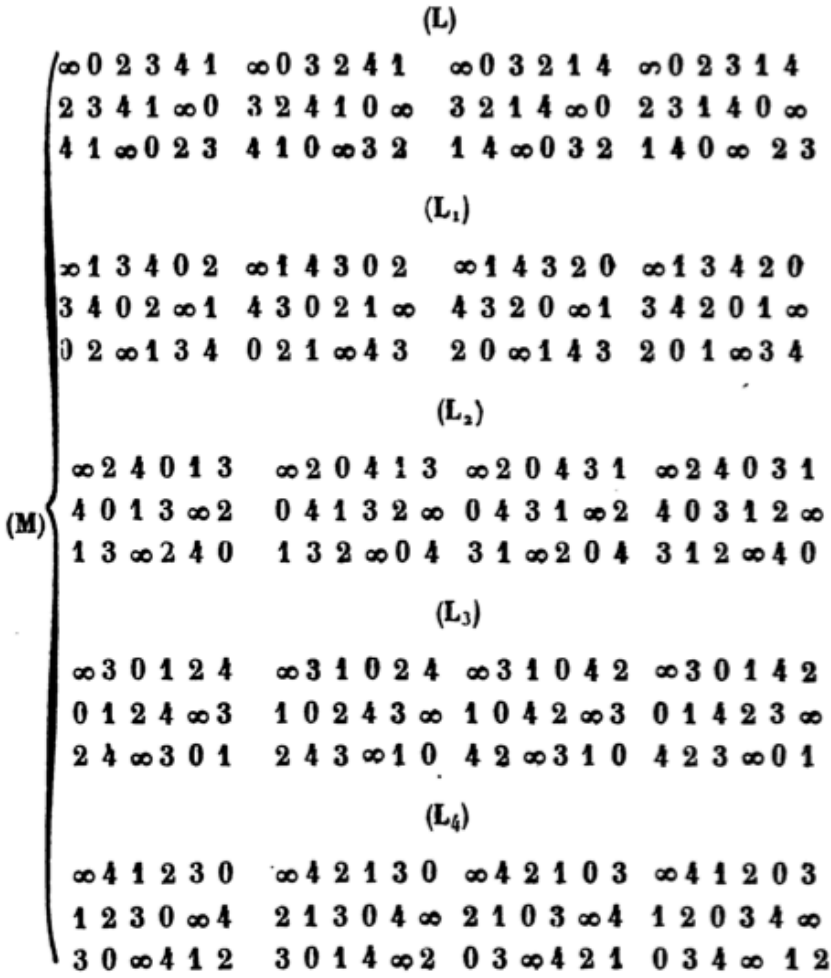

FIGURE 3. The partition of the permutations of the six roots of the modular equation of order 5, represented by their indices, into 5 sets of 12 permutations, *Annali di scienze matematiche e fisiche* 4 (1853), p. 98. There is a mistake in the second and fourth columns of the first lines: read $(0, \infty, 3, 2, 4, 1)$ instead of $(\infty, 0, 3, 2, 4, 1)$, $(0, \infty, 2, 3, 1, 4)$ instead of $(\infty, 0, 2, 3, 1, 4)$, etc.

several given quantities, it is convenient to represent these quantities, [...] by the same letter affected with a variable index [...] Then the substitutions we have to carry out bear on the indices. [...] Every substitution can then be represented analytically by means of a function." In 1863, before applying it to the substitutions used in the modular cases for $p = 5$ and $p = 7$, Hermite generally characterized the functions necessary to represent a substitution of p indices in the way we have dealt with here, [Hermite 1863]. Again, while we are perhaps more receptive now to the link this provides with linear groups and representations, it appears in Betti's work, as in Hermite's, as an efficient path to concrete expressions and thus to actual computations, in the analytic vein.

2.4. *Hermite's point of view*

One might wonder at this point why Hermite did not publish his proof on the reduction of modular equations earlier. This appears to have been a recurrent attitude of his—another well-known example is Dirichlet's theorem on the structure of algebraic units of which scattered elements appear as early as 1847 in Hermite's articles. Hermite went back and forth among his favorite topics, always involved in mathematical dialogues with others, leaving many of the announcements made in letters undeveloped for years, in striking contrast with the advice given to Leopold Kronecker by Ernst Eduard Kummer in August 1846: "From the very beginning, pursue your mathematical studies in such a way as to produce treatises, that is to say, you must work on certain subjects until they are sufficiently polished in such a way that even if, from certain points of view, they contain material to be further developed, they may constitute in themselves a finished whole."[41]

In any case, Hermite was not idle during this decade: although he still held no permanent position, he gave lectures at the Collège de France from 1848 to 1850, and published extensively on forms and elliptic functions, some of the latter being highly relevant, as we shall see, to his involvement with Galois and with algebraic equations. Indeed, one of his memoirs submitted to the Academy in 1849 on elliptic functions again promised a proof of Galois's reduction of modular equations: the fate

41 *Festschrift zur Feier des 100. Geburtstages Eduard Kummers*, ed. Vorstand der Berliner mathematischen Gesellschaft, Leipzig: Teubner, p. 70. See [Goldstein 1989] for an interpretation of this quote and [Goldstein 2007] for examples of Hermite's interactions with Gauss's and Jacobi's papers.

of this manuscript, which was never published and only recovered in the 1990s by Bruno Belhoste, might have discouraged Hermite.[42]

But a more interesting reason for Hermite's delay appears in a letter to Jacobi; it touches upon his mathematical priorities and what he considered a final result worthy of publication.

> I would have particularly liked to be in a position to submit to you a work on modular equations, in which I establish a result proposed in Galois's *Œuvres posthumes*, printed in the *Journal de mathématiques*, and which shows that modular equations of the sixth, eighth and twelfth degree can be lowered to the fifth, seventh, and eleventh degree respectively. I intended at the same time to get back to these singular relations that you first discovered among the roots M, M', … of the equation $F(k, M) = 0$, but I was unable to succeed despite all my efforts. These first examples of properties of algebraic irrational numbers that cannot be expressed by radicals, seem to me of the utmost interest; as the properties of the roots of the equations relative to the division of the circle, they can be used as a point of departure of advances in the general theory of equations.[43]

The equation $F(k, M) = 0$ is that of the multiplier, discussed above, while the "singular relations" refer to an analytic representation of the roots, somewhat analogous to that displayed in (4). They concern special values of *analytic* functions, which are at the same time solutions of *algebraic* equations. Hermite returned several times to this question and his reference to the equations "relative to the division of circle," or "cyclotomic equations," in this context is quite illuminating. We have already seen that these equations became the center of algebraic attention at the beginning of the century as the first example of a complete treatment of an infinite family of equations. But detailed examinations of Gauss's methods were multifarious: some would stress the cascade construction of auxiliary equations, others the way an appropriate indexation of the roots displayed their relations and the possible substitutions among them. And Hermite pointed out still another aspect of the cyclotomic equations;

---

42 On the story of this text, see [Belhoste 1996]. Again, the analogy with Galois is striking.

43 [Hermite 1850, p. 135]: *Je désirerais surtout pouvoir vous soumettre un Travail sur les équations modulaires, dans lequel j'ai établi une proposition énoncée dans les Œuvres posthumes de Galois, imprimées dans le Journal de Mathématiques, et qui consiste en ce que les équations modulaires du sixième, huitième et douzième degré peuvent être abaissées respectivement au cinquième, septième et onzième degré. Je me suis proposé en même temps de retrouver ces relations si singulières que vous avez le premier découvertes entre les racines M, M', … de l'équation $F(k, M) = 0$, mais je n'ai pu y réussir malgré tous mes efforts. Ces premières propriétés d'irrationnelles algébriques, non exprimables par radicaux, me paraissent du plus grand intérêt; comme les propriétés des racines des équations relatives a la division du cercle, elles serviront de point de départ pour pénétrer plus avant dans la théorie générale des équations.*

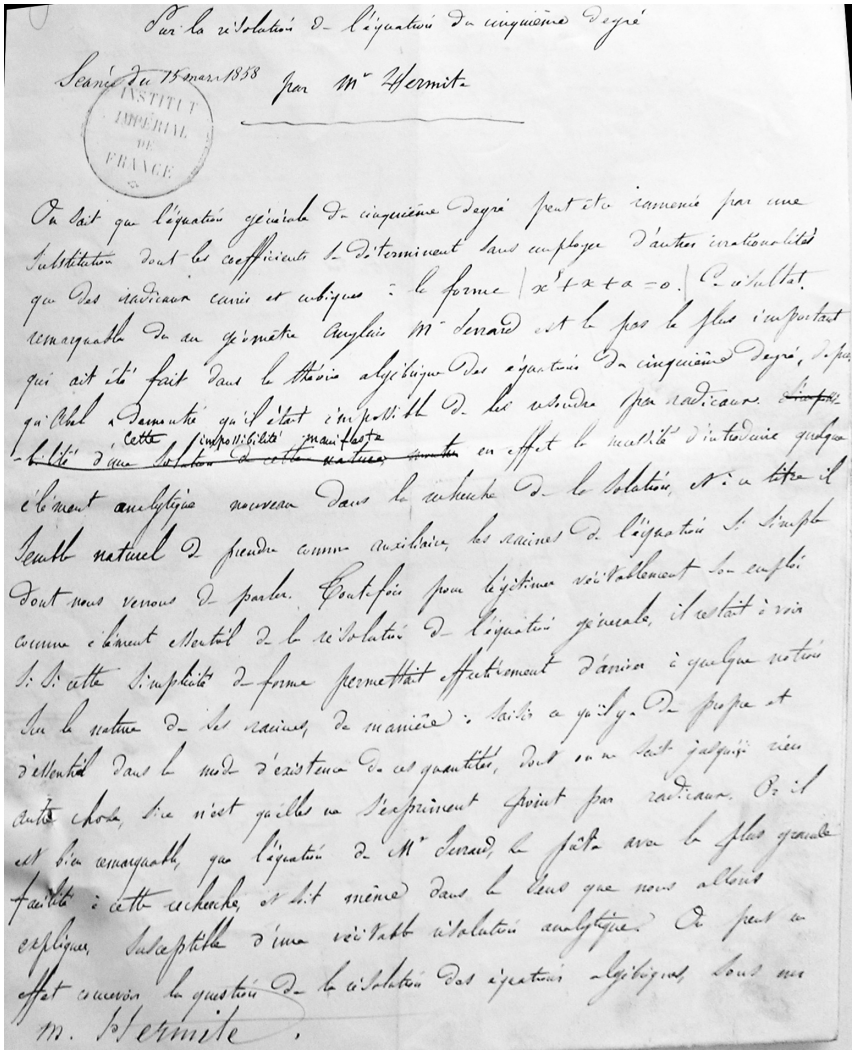

FIGURE 4. Hermite's manuscript on his article on the quintic, [Hermite 1858a]. By courtesy of the Archives of the Académie des sciences de l'Institut de France.

their roots are also special division values of analytic functions, in this case of exponential or circular type, and the relations among the roots can be read off directly and explicitly from their analytic expressions.

This emphasis on effectiveness is an important clue in understanding his approach to the modular equation:

> I shall take up only the very important fact announced by Galois; that [modular equations] are susceptible of a reduction to a degree lowered by 1 in the cases of $n = 5$, $n = 7$, and $n = 11$. Although we possess only a few fragments of his work on this matter, it is not difficult to follow the path he opened and to find the proof of this beautiful proposition; but one succeeds then only in guaranteeing the possibility of the reduction and an important lacuna remained to be filled to push the question to its final completion. [...] It is from a completely different point of view [to that of M. Betti] that I shall now treat the same questions. Thus, leaving aside all considerations relative to the decompositions of groups, I define a priori, for $n = 5$, $n = 7$, and $n = 11$ the roots of the reduced equations. [44]

Let us illustrate this with the simplest case, $n = 5$, following Hermite's papers, [Hermite 1858a] and [Hermite 1859]. We need a function of the roots of the modular equation which takes five different values when the roots are permuted under the substitutions of $PSL_2(\mathbf{F}_5)$, that is under the substitutions $i \to \frac{ai+b}{ci+d}$, where $ad - bc$ is a quadratic residue modulo 5 (or simply 1). Hermite defined, for all integers $i = 0, \ldots, 4$:

$$z_i = (x_\infty - x_i)(x_{1+i} - x_{4+i})(x_{2+i} - x_{3+i}),$$

where the x_i are the roots of the modular equation. In other words, using the formula (4) and putting

$$\Phi(\omega) =: \left[\phi(5\omega) + \phi(\frac{\omega}{5})\right]\left[\phi(\frac{\omega+16}{5}) - \phi(\frac{\omega+4\cdot 16}{5})\right] \times \left[\phi(\frac{\omega+2\cdot 16}{5}) - \phi(\frac{\omega+3\cdot 16}{5})\right], \tag{5}$$

one obtains $z_0 = \Phi(\omega)$, $z_1 = \Phi(\omega + 16)$, $z_2 = \Phi(\omega + 2 \cdot 16)$, $z_3 = \Phi(\omega + 3 \cdot 16)$, $z_4 = \Phi(\omega + 4 \cdot 16)$.

---

44 [Hermite 1858a, p. 10 and Hermite 1859, p. 75]: *Je m'attacherai seulement au fait si important annoncé par Galois et qui consiste en ce que [les équations modulaires] sont susceptibles d'un abaissement au degré inférieur d'une unité dans les cas de $n = 5$, $n = 7$ et $n = 11$. Bien que nous ne possédions que quelques fragments de ses travaux sur cette question, il n'est pas difficile en suivant la voie qu'il a ouverte de retrouver la démonstration de cette belle proposition; mais on n'arrive ainsi qu'à s'assurer de la possibilité de la réduction, et une lacune importante restait à remplir pour pousser la question jusqu'à son dernier terme. [...] C'est sous un point de vue bien différent [de celui de M. Betti] que je vais maintenant traiter les mêmes questions. Ainsi, laissant de côté toute considération relative aux décompositions de groupes, je définis, a priori, pour $n = 5$, $n = 7$ et $n = 11$ les racines z des équations réduites.*

The set of the z_i is invariant under $PSL_2(\mathbf{F}_5)$, and provides the five values of the function z_0, say, under these substitutions. For example, the substitution defined on the indices by $i \to i + b$, for any $b = 0, 1, 2, 3, 4$, fixes x_∞ and transforms x_i in x_{i+b} for all i, thus changing z_0 to z_b. As for the substitution $i \to -1/i$, say, it transforms x_∞ into x_0, x_0 into x_∞, x_1 into x_4, x_4 into x_1, while fixing x_2 and x_3: it thus fixes z_0, but exchanges z_1 and z_2, z_3 and z_4. Parenthetically, it shows that $PSL_2(\mathbf{F}_5)$ is isomorphic to the alternate group $\mathscr{A}_5$ of even permutations on 5 letters.

Hermite deduces that the $z_i = \Phi(\omega + 16i)$ are thus the five roots of an equation of degree 5, with coefficients which are rational in $\phi(\omega)$ and $\sqrt{5}$:[45]

$$(6) \qquad \Phi^5 - 2^4 5^3 \Phi \phi^4(\omega)\psi^{16}(\omega) - 2^6\sqrt{5^5}\phi^3(\omega)\psi^{16}(\omega)[1 + \phi^8(\omega)] = 0$$

This equation is obtained from considerations on the q-development of the roots (that is, their development in in series of $q = e^{\pi i\omega}$). Hermite also explains how to find the 12 substitutions constituting one of the "groups" (L) in Betti's work, p. 238: they are just the substitutions which fix one of the roots, say z_0. For instance, the substitution $i \to -1/i$ which, as just seen, fixes z_0, sends the permutation $(2\ 3\ 4\ 0\ \infty)$ (first column, second line in Betti's table) to $(2\ 3\ 1\ 4\ \infty\ 0)$ (last column, second line).

This gives *explicitly* the reduced equation. Effectivity and thus computational issues were always handled with care (if not always with success) by Hermite.[46] This way of dealing with the reduction of modular equations might seem a complete deviation from Galois, but this is not how Hermite saw it. Turning to this question in his 1859 articles, he wrote that "Galois was the first to discover the quite remarkable fact of this reduction, from the *double point of view of the theory of elliptic functions and of algebra*" ([Hermite 1859, p. 71], my emphasis). Still following "Galois's ideas," he then

---

45 The presence of $\sqrt{5}$ is connected with the restriction to those substitutions where $ad-bc$ is a quadratic residue modulo 5. In modern terms, the Galois group of the modular equation is $PSL_2(\mathbf{F}_5)$ over the quadratic extension generated by $\sqrt{5}$ over $\mathbf{Q}(u)$. In Hermite's terms and perspective, which are Galois's ones, it corresponds to the "adjunction" of a certain quantity to what will be considered as "rationally known," see [Galois 1846, p. 418].

46 In the same series of papers, [Hermite 1859], Hermite studies the discriminant of modular equations. He links its zeroes, corresponding to the multiple roots of the equation, with the values of $\phi(\omega)$, for ω solutions to certain quadratic equations. He is thus led to the calculation of $q = e^{\pi i\omega}$, for such quadratic ω and discovers that "the numerical transcendent $e^{\pi\sqrt{\Delta}}$ then approaches an integer extremely closely." He points out in particular the twelve 9s beginning the decimal part of the so-called Ramanujan constant, $e^{\pi\sqrt{163}}$, see [Hermite 1859, p. 61].

formulated that "proposition of Galois," which he claimed serves as the fundamental principle of his work:

> Every nonsymmetric rational function of the roots v_k (of the modular equation) which does not change when the various indices l are replaced by $\frac{al+b}{cl+d}$, a, b, c, d being integers taken modulo n and the determinant $ad-bc$ being not $\equiv 0$, can be expressed as a rational function of u.[47]

Here "groups" as such seem to be receding backstage. But the clue is indeed borrowed from Galois. In the manuscript submitted to the Academy on the solvability by radicals, which was reproduced by Liouville, its first proposition, which established the existence of the group of an equation, characterized it as explained before by the fact that: "every function of the roots invariant under the substitutions of this group is rationally known," explaining in a footnote what "invariant" and "rationally known" meant. The wording is thus exactly the one adopted by Hermite, see [Galois 1846, p. 421]. Hermite placed his work on modular equations directly in Galois's wake. What this meant for the theory of equations in general will now be discussed.

2.5. *Back to algebraic equations*

An important spin-off of Hermite's requirement to get the equation of the reduced equation, and not only its existence, is well-known.[48] He was thus able to invert this procedure, in the sense that he used the modular equation of the sixth degree, to which the reduced fifth-degree equation corresponds, as a resolvent equation,[49] that is to solve the quintic equation in general.

Hermite highly praised the result he attributed to George Birch Jerrard,[50] that by means of transformations involving only the extraction of quadratic and cube roots, any fifth-degree algebraic equation in one

---

47 [Hermite 1859, p. 72]: *Toute fonction rationnelle non symétrique des racines v_k (de l'équation modulaire) qui ne change pas en remplaçant les divers indices l par $\frac{al+b}{cl+d}$, a, b, c, d étant des nombres entiers pris suivant le module n et le déterminant $ad-bc$ n'étant pas $\equiv 0$ sera exprimable en fonction rationnelle de u.*

48 This aspect of Hermite's work is discussed in several historical studies, in the perspective opened by Felix Klein, [Klein 1884], see in particular [Pierpont 1895, Gray 2000, Houzel 2003].

49 Again the terminology might be confusing: several things are called "reduced," in particular the resolvent equation is sometimes said to be the "reduced equation".

50 For the complicated story and the references of this result, see the footnotes of [Klein 1884, p. 143].

variable can be put into the simpler form:

$$x^5 - x - a = 0 \tag{7}$$

which makes it depend on a single parameter, a. Comparing this form and the quintic equation (6) obtained by reduction from the modular equation of order 5, led Hermite to the identification:

$$a = \frac{2}{\sqrt[4]{5^5}} \frac{1 + \phi^8(\omega)}{\phi^2(\omega)\psi^4(\omega)}.$$

He then easily showed how to find $k = \phi^4(\omega)$ from a given a by solving a quartic equation with coefficients rational over $\mathbf{Q}[\sqrt{5}]$. As the roots of (6) are known, the roots of any quintic $x^5 - x - a = 0$ can thus be expressed as functions of ω: "this is thus the solution of the equation, inasmuch as the roots are represented separately by uniform functions," Hermite wrote [Hermite 1858a, p. 11].

To interpret this result, we have to come back again to what is meant by "solving an equation." Hermite underlined that such expressions of the roots were very favorable for numerical computations, since "the extraordinary convergence of the series which figure in the numerator and denominator of de $\phi(\omega)$ makes it quite short"—a feature he appreciated in this case, as he did with the use of continued fractions to solve lower-degree equations. However, good estimations of the roots are not the sole objective here. Hermite's hope in 1847 had been "to go further in the general theory of equations," via a closer examination of the "properties of algebraic irrationals, that cannot be expressed by radicals," [Hermite 1850, p. 135]. Inheriting a state of the art where general equations of degree higher than 4 had been proved (by Abel and others) not to be solvable by radicals, and equations solvable by radicals had been characterized, at least for prime degrees (by Galois's work), Hermite proposed:

> This impossibility [of solving by radicals equations of degree higher or equal to 5] reveals indeed the need to introduce some new analytic element into the search for the solution [...] Instead of trying to represent by a radical formula with multiple determinations the system of roots so tightly linked together when we consider them as functions of the coefficients, one can try, by introducing auxiliary variables, as in the example given for the third degree, to obtain the roots separately, expressed by so many distinct and uniform functions with respect to these new variables.[51]

---

51 [Hermite 1858a, p. 5–6: *Cette impossibilité [de résoudre par radicaux les équations de degré supérieur ou égal au 5^e] manifeste en effet la nécessité d'introduire quelque élément analytique nouveau dans la recherche de la solution... Au lieu de chercher à représenter par une formule radicale à déterminations multiples le système des racines si étroitement liées entre elles*

The suggestion may be better understood with the example of the cubic equation:

$$x^3 - 3x + 2a = 0,$$

where a is a real positive number less than 1. The so-called Cardano formulas

$$x = \sqrt[3]{\sqrt{a^2 - 1} - a} - \sqrt[3]{\sqrt{a^2 - 1} + a},$$

correspond to the first approach: one represents the system of roots by a single formula, expressing them as a function of the coefficients (here a) by means of radicals, with multiple determinations.[52] This approach is familiar, but paradoxically it became all the more so when its very possibility was challenged by a better understanding of the nature of complex functions. For Poinsot, the uniqueness of the formula encompassing potentially multiple determinations—at a moment when neither complex numbers, nor functions of a complex variable were completely stabilized concepts—was an important characteristic of *algebra*, as opposed to arithmetic, understood here simply as the domain of actual, numerical computations:

> One may try to distinguish and isolate by certain signs the different roots of a radical formula but this separation is totally illusory, because these roots always coexist in any of them, insofar as one lets in those radicals that give rise to the multiplicity of values. But by the very nature of Algebra it is necessary that these equivocal signs remain, because this science has for its sole object to indicate the operations to perform, but without executing them, so that the picture of these operations, the unique thing that the mind has in sight, is perfectly conserved. [...] When one goes to numerical applications, then operations are executed.[53]

---

lorsqu'on les considère comme fonctions des coefficients, on peut, ainsi que l'exemple en a été donné dans le troisième degré, chercher, en introduisant des variables auxiliaires, à obtenir les racines séparément exprimées par autant de fonctions distinctes et uniformes relatives à ces nouvelles variables.

52 As well-known, to get exactly the three roots, one has to require that the a-priori independent determinations of the two cubic roots are such that their product is here 1.

53 Louis Poinsot, Note, in J.-L. Lagrange, *Traité des équations numériques de tous les degrés*, 3e éd., Paris: Bachelier, p. 313–314: *On essaye de distinguer et d'isoler, par certains signes, les différentes racines d'une formule radicale, et cette séparation est tout à fait illusoire, car ces racines coexistent toujours dans une seule quelconque d'entre elles; tant qu'on y laisse ces radicaux qui donnent lieu à cette multiplicité de valeurs. Or par la nature même de l'Algèbre il faut que ces signes équivoques demeurent, puisque cette science n'a d'autre objet que d'indiquer les opérations à faire, mais sans les exécuter, afin que le tableau de ces opérations, la seule chose que l'esprit ait en vue, soit parfaitement conservé. [...] Lorsqu'on passe aux applications numériques les opérations s'effectuent.* On Poinsot's viewpoint on arithmetic and algebra, see [Boucard 2011].

For Poinsot, and his followers, algebra is the science of order, keeping trace of the ordered relations among things; radicals appear as a symbolism capturing these relations, in particular the intrinsic irreducibility of the set of roots.

As for the other approach, that which Hermite recommends, it is connected in this case to solving the cubic equation by means of the three roots

$$2\sin(\frac{\alpha}{3}), \quad 2\sin(\frac{\alpha+2\pi}{3}), \quad 2\sin(\frac{\alpha+4\pi}{3})$$

where the quantity α (with $a = \sin\alpha$) serves as an auxiliary variable. The three roots are represented by distinct uniform functions, as in the equation (5).

The difference between the two approaches stops neither at what is acceptable as a solution, nor in the importance accorded to calculation. Our current frontier between algebra and analysis is blurred: Hermite reinterprets the solution by radicals (Cardano's formulas in this case) also as one based on complex functions. Poinsot's demarcation line was drawn between a systemic representation of the roots and their numerical determination, Hermite's one between uniform functions and multiple-valued ones.[54]

This point of view is coherent with Hermite's programme, which we met above in connection with continued fractions; a complete classification of "algebraic irrationalities," that is, roots of algebraic equations. For him, it relies on the discovery of so-called "analytic elements," which would provide characteristic properties of the roots and allow one to exhibit them in a unique way—in the way, for instance, that the periodicity of their development as continued fractions characterized quadratic irrationals. As Hermite explained:

> Perhaps one will succeed in deducing [...] a complete system of characters for each species of these kinds of quantities, analogous for instance to those given by the theory of continued fractions for the roots of quadratic equations. We cannot in any event have too many elements concurring in throwing some light on this infinite variety of algebraic irrationals, among which the symbols

54 An intriguing question is to determine on which side one should situate Galois's theory of ambiguity, hinted at in the letter to Chevalier, [Galois 1846, p. 415] and [Galois 1962, p. 185]: "to see in a relation between transcendental quantities or functions which exchanges one can carry out, which quantities one can substitute for the given ones without the relation ceasing to exist." Although its usual interpretation as a theory of extended Galois groups, and of course the name itself, suggest a kinship with the first point of view, it could equally apply to the second if one thinks of representations in the style of (4), inspired as they were by the reading of Jacobi (of course, today the two directions would not be seen as so opposed).

> for the roots represent merely the smallest part. [...] What an immense task it is for number theory and integral calculus, to penetrate into the nature of such a multitude of entities created by reason, classifying them into mutually irreducible groups, constituting them all individually through characteristic and elementary definitions.[55]

For Hermite, the theory of forms, supported by elliptic functions, was the best hope for such a project,[56] Gauss's classification of binary quadratic forms with integral coefficients in the section V of the *Disquisitiones arithmeticae* providing a first step and a motivation.

At the beginning of the 1850s, the theory of invariants supplied the missing fuel. An example of its use will explain how. In section VII of [Hermite 1854], Hermite came back to a now familiar topic, the construction of the resolvent equation (of 6th degree) of the quintic. One would need, as explained, a function of the 5 roots of the quintic taking only 6 values when the roots are permuted, the resolvent equation being that having these 6 values as roots. With this usual construction, the coefficients of the resolvent equation would appear as polynomial functions of degree 12, at least, of the coefficients of the given quintic, which at the time hampered the path to direct inspection. Hermite considered instead the binary form of the fifth degree, $(x-\alpha y)(x-\beta y)(x-\gamma y)(x-\delta y)(x-\epsilon y)$, where $\alpha, \beta, \ldots, \epsilon$ are the roots of the quintic, and showed how to construct a function of the roots with six values which is *an invariant* of this form. Because such invariants can be derived from a finite number of fundamental ones, the coefficients of the associated resolvent equation could then be expressed as (much simpler) functions of the fundamental invariants. Hermite was then able to characterize important properties of quintic equations by simple

---

55 [Hermite 1850, p. 131]: *Peut-être parviendra-t-on à déduire [...] un système complet de caractères pour chaque espèce de ce genre de quantités, analogue par exemple à ceux que donne la théorie des fractions continues pour les racines des équations du second degré. On ne peut du moins faire concourir trop d'éléments pour jeter quelque lumière sur cette variété infinie des irrationnelles algébriques, dont les symboles d'extraction des racines ne nous représentent que la plus faible partie.[...] Quelle tâche immense pour la théorie des nombres et le calcul intégral de pénétrer au milieu d'une telle multiplicité d'êtres de raisons en les classant par groupes irréductibles entre eux, de les constituer tous individuellement, par des définitions caractéristiques et élémentaires.*

56 After Dedekind and above all after Hilbert's *Zahlbericht* the main direction in the study of algebraic numbers would be for a time that of number fields, see [Goldstein & Schappacher 2007a, Goldstein & Schappacher 2007b] for these contrasting developments. But the use of analytic functions to study (or even to classify) algebraic objects did not disappear, far from it. Two well-known success stories of the twentieth century along these lines are the further developments of Kronecker's *Jugendtraum*, and the modularity of all elliptic curves defined over the rational numbers, used in the proof of Fermat Last Theorem.

conditions on the invariants and covariants.[57] In the 1860s, Hermite came back to the other resolution of the quintic by means of elliptic functions, as proposed by Francesco Brioschi and Leopold Kronecker: both used the multiplier equation, instead of the modular equation. Hermite provided then a large unified picture of both approaches by means of invariant theory, [Hermite 1865].

Galois's results are part and parcel of this programme, among those "elements concurring in throwing some light on this infinite variety of algebraic irrationals," side by side with the q-series, the study of substitutions of a given type of forms, congruences, or the reciprocity laws of invariant theory.

Hermite's treatment of the quartic equation, [Hermite 1858b], allows us to illustrate in a simple case how all these aspects combine together. First of all, he uses invariant theory to transform a general quartic equation $Ax^4 + 4Bx^3 + 6Cx^2 + 4Dx + E = 0$ into another, of which the quadratic invariant $(AE - 4BD + 3C^2)$ is zero. This new equation is of the type $x^4 - 6Sx^2 - 8Tx - 3S^2 = 0$ (thus depending only on two parameters), and it plays the same role as the Bring-Jerrard equation $x^5 - x - a$ in the study of the quintic. Hermite observes that these equations

> do not belong to the most complex type of irrationalities for general quartic equations. Indeed, in their case, if one considers Galois's equation in V, the degree of which distinguishes and characterizes so precisely what one can call the *various orders of irrationalities*, one finds it to be only of the twelfth degree, while in the general case it is necessarily of the twenty-fourth. There thus exist for such equations non-symmetric functions which can be expressed rationally by the coefficients.[58]

Indeed, by choosing $k^2 = u^8 = \frac{2\sqrt{S^3}}{T+\sqrt{S^3}}$, Hermite identifies this equation with the modular equation of order 3, the quartic (1), associated to the modulus k. Now, the roots can be expressed by the analytic expressions of the roots (4) of the modular equation; this then provides the solution of quartic equations via elliptic functions.

---

57 See [Hermite 1854] and [Hermite 1865]. For instance, he could give this way the number of their real or complex roots, at that time still provided by variants of Sturm theorem.

58 [Hermite 1858b, p. 27–28]: *Effectivement, si l'on considère à leur égard l'équation en V de Galois, dont le degré distingue et caractérise d'une manière si précise ce qu'on peut appeler les* divers ordres d'irrationalité*, on la trouve seulement du douzième degré, tandis que dans le cas général elle est nécessairement du vingt-quatrième. Il existe donc pour ces équations des fonctions non symétriques, exprimables rationnellement par les coefficients.* Their group is $PSL_2(\mathbf{F}_3)$, of order 12, while the full symmetric group on 4 elements is of order 24.

The tools provided by Galois's approach (adjunction of roots, analytic expression of the substitutions by means of congruences, "group of the equation," and especially the "equation in V"), among other instruments also used for classifying algebraic irrationalities, are thus fully integrated into Hermite's programme. We shall see Hermite's other uses of "the equation in V" in the next section.

3. ANALYSIS AND ALGEBRA

I now turn to the part of Galois's heritage with which, in the historiography, Hermite is mainly associated:[59] the definition of the monodromy group and, more generally, the transfer of Galois's ideas, mostly expressed in the setting of algebraic equations, to a function-theoretical setting. This work was triggered by a double publication of Victor Puiseux in the *Journal de mathématiques pures et appliquées* in 1850 and 1851.

In these two important articles, [Puiseux 1850, Puiseux 1851], Puiseux studied algebraic equations of the type $F(u,z) = 0$, where z was a complex variable and $u(z)$ an analytic function. Joseph Bertrand offered his vivid version of the main result in his eulogy for Puiseux at the Academy of Sciences, on May 5, 1884:

> Ch[arles] Sturm [...] came to me once with this question, that no one before Puiseux had asked: "If you follow along a closed circuit the root of an equation, a parameter of which represents a point on the circuit, what would you obtain when you come back to the point of departure?"—"I should find my root again," I said, without hesitation.—"Well, no! You will not find it again, and Puiseux proves it." [60]

Let us explain a bit more what is in question. Puiseux considers an algebraic equation $F(u,z) = 0$, with F a polynomial of degree m without multiple factors, and $u = u(z)$ a complex function of a complex variable z; we are thus considering algebraic functions, instead of algebraic numbers. As in the case of standard equations, when the discriminant is zero, one obtains multiple roots. Here the discriminant is a polynomial in z, and thus is zero for a finite number of values of z. Unless z is one of these

---

59 For instance, see [Kiernan 1971], [Neumann 1996], [Ehrhardt 2007, ch. 6.3].

60 [Bertrand 1884, p. 231]: *Ch. Sturm [...] m'aborda un jour par cette question que personne avant Puiseux ne s'était proposée: "Si vous suivez le long d'un contour fermé la racine d'une équation dont un paramètre représente un point du contour, qu'obtiendrez-vous en revenant au point de départ?"—"Je retrouverai ma racine, répondis-je sans hésiter."— "Eh bien, non! vous ne la retrouverez pas: ce Puiseux le démontre."*

branch points,[61] the equation $F(u,z) = 0$ with z fixed has m solutions $u_0, u_1, \ldots, u_{m-1}$; they are continuous functions of the variable z. Sturm's question to Bertrand, then, is: what happens to the function $u_i(z)$ when z varies, in particular when z runs continuously around a closed circuit in the complex plane? After z comes back to the point of departure, the function should still of course verify the same equation, thus be one of the roots $u_j(z)$ for this value of z. Puiseux showed that if the circuit does not enclose one of the branch points, or a point where the function becomes infinite, the function will come back unchanged to its initial value. But if the circuit does enclose such a point, it could be different from the function of departure. Indeed, at a branch point, the equation has multiple roots, which means that several of the u_i coincide; near the branch point, they become distinct (because the equation has then m distinct roots), but close (because of the continuity); after a circuit around the branch point, the functions may have been exchanged.

In other words, when z describes a closed path in the complex plane, the roots $u_0, \cdots, u_{m-1}$ are interchanged. How to describe their permutations? By means of an extremely careful study of the paths in the complex plane, Puiseux proved that, for the circuits around a single branch point, say z_0, the functions u_i are distributed into several "circular systems," the functions belonging to one system being exchanged in a circular permutation when the variable z describes a small circuit around z_0. He also described the behavior of each function around a branch point z_0 by developing it in series in fractional powers (now called a Puiseux series), the denominator of the fractions being the order of the circular system to which the given function belongs. In his second paper, he explored in detail the relation between the irreducibility of the algebraic equation $F(u,z) = 0$ and the way the functions u_i are permuted depending on the circuits described by the variable z.[62]

The importance of Puiseux's articles for his contemporaries was to rid the theory of functions of the paradoxes opened up by the multiple periodicity of otherwise apparently well-defined integrals of algebraic functions, such as elliptic integrals. The different values of the integrals of algebraic

---

61 The terminology again varies, from no name at all to "critical point", or "singular point."

62 For a more complete description of Puiseux's articles and of his techniques, see [Brill & Noether 1894, p. 197–202]. Olaf Neumann places Puiseux's work in the development of Galois theory as applied to topology and function theory in [Neumann 1996].

differentials naturally arise from Puiseux's study of the behavior of algebraic functions along different paths of integration. Puiseux provided in particular a thorough discussion of the periods of elliptic integrals in his papers.

Puiseux illustrated these results by several examples, of which I shall briefly present one (see [Puiseux 1850, p. 405–407 and p. 416] and [Puiseux 1851, p. 239–240]): the equation $u^3 - u + z = 0$. Its discriminant is $4(-1)^3 + 27z^2$, and thus there are two branch points, $z_0 = \frac{2}{3\sqrt{3}}$ and $z_1 = -\frac{2}{3\sqrt{3}}$, to which one associates the two points A and A' in the complex plane. Let $u_1(z)$, $u_2(z)$, $u_3(z)$ be the solutions of the equation which take respectively the values 0, 1 and -1 for $z = 0$. For $z = z_0$, the equation has one double root ($\frac{1}{\sqrt{3}}$) and one simple one ($\frac{-2}{\sqrt{3}}$), which correspond to the values taken by the three solutions at this point; here $u_1(z_0) = u_2(z_0) = \frac{1}{\sqrt{3}}$ and $u_3(z_0) = \frac{-2}{\sqrt{3}}$. Very near A, u_1 and u_2 are distinct, but close in value; Puiseux explained that when the variable describes a (very) small circle around A, u_1 and u_2 are exchanged. As for u_3, it returns to its original value. In Puiseux' terms, there is one circular system of order 2 and one circular system of order 1. He could thus develop the two functions u_1 and u_2 in series of the powers of $(z - \frac{2}{3\sqrt{3}})^{\frac{1}{2}}$, valid for z in any disk centered in A and small enough not to contain the other branch point; as for u_3, it can be developed in a series of powers of $(z - \frac{2}{3\sqrt{3}})$. For the other branch point z_1, u_1 and u_3 are exchanged, while u_2 comes back to the same value. Moreover, as u_1 takes three values, Puiseux obtained a new proof that the equation is irreducible. He could also explain how the different values of of $\int u_1 dz$ depend on the various possible paths used to define the integral.

It is now well-known that Puiseux's articles followed in the wake of Cauchy:[63] Puiseux used Cauchy's representation of the complex variable in the plane, Cauchy's results on substitutions, Cauchy's definition of an integral, Cauchy's development in series, etc. More generally, he insisted on the advantages of Cauchy's approach to properly understand the phenomena linked to complex functions, and above all the multiple values taken by their integrals, depending on the integration paths.

Puiseux's first paper appeared in the November issue of Liouville's *Journal* and Hermite proposed his own note to the Academy the following

63 See [Belhoste 1996], [Gray 2000]. Puiseux even devoted a few pages at the end of the first paper to carefully explain what could be found, if only in the form of a hint, in Cauchy's papers, and what properly belonged to himself, in particular, the detailed analysis of the paths.

March. This quick jump, however, is a bit less surprising if one recalls that Hermite had himself proposed a new foundation of the theory of elliptic functions following Cauchy's ideas as early as 1849, in the memoir submitted to the Academy I hinted at earlier and which remained unpublished.[64] He thus already had a working knowledge of them, as he obviously had also of Galois's ideas. Hermite began his note in a tone reminiscent of the programme he had explained to Jacobi a few years before:

> The propositions given by M. Puiseux on the roots of algebraic equations considered as functions of a variable z seem to open a large field of investigations, destined to throw a great light on the analytic nature of this kind of quantity [...]. I shall limit myself here to the question of the resolution by radicals; later, I shall study modular equations from the same point of view and I shall show how M. Puiseux's theorems lead to the realization of the reduction of these equations in the cases announced by Galois, whose principles, moreover, will underlay everything we shall say.[65]

Here, algebraic functions have replaced algebraic irrationals, but the questions are the same: to understand their "analytic nature," that is to classify and characterize them. One cannot help but be reminded of Galois's project, a dissertation "on the classification of the problems of Mathematics, and on the nature of transcendental quantities and functions," [Galois 1962, p. 29].

Again, as in 1847 and 1849, Hermite announced an application of his ideas to the reduction of modular equations, and again delayed its publication. What he did not delay was a discussion of their application to the solvability by radicals of equations satisfied by algebraic functions, and I shall present it now.

Hermite's first step here is also to be found in Puiseux's second paper, and the differences between them, in the case of a proposition that results immediately from Puiseux's work, are illuminating. Puiseux had written that "if an algebraic function of z has only one value, that is, comes back to

---

64 See [Belhoste 1996] for the detailed chronology of Cauchy's reports on both Puiseux's and Hermite's memoirs and their implications, as well as for a study of Hermite's manuscript. Approaches and aims of the two men were of course quite different.

65 [Hermite 1851, p. 276]: *Les propositions données par M. Puiseux sur les racines des équations algébriques considérées comme fonctions d'une variable z me semblent ouvrir un vaste champ de recherches destinées à jeter un grand jour sur la nature analytique de ce genre de quantités. [...] Je me borne ici à la question de la résolution par radicaux; plus tard, je ferai au même point de vue, l'étude des équations modulaires et je monterai comment les théorèmes de M. Puiseux conduisent à effectuer l'abaissement de ces équations dans les cas annoncés par Galois dont les principes serviront d'ailleurs de base à tout ce que nous allons dire.*

its initial value [when z does], the function is necessarily rational" (Puiseux 1851, p. 229). In Hermite's formulation this becomes

> Every function of the roots u, invariant under the substitutions S_0, $S_1, \ldots, S_{\mu-1}$, can be rationally expressed in terms of z, and also the converse. Every function of the roots u which is rationally determined in z, is invariant under the same substitutions S_0, $S_1, \ldots, S_{\mu-1}$.[66]

Here S_0, $S_1, \ldots, S_{\mu-1}$ are the substitutions which interchange the u_i of one circular system around each branch point $z_0, \ldots, z_{\mu-1}$.[67]

Hermite's *naming* the substitutions (with the same notations he was simultaneously using for studying substitutions of forms in other articles), while Puiseux did not and gave names only to the complex functions themselves, marks a significant shift, from the complex functions to the substitutions among them. A second difference is that the proposition is central for Hermite, as we shall see, but is only an auxiliary statement for Puiseux in his study of the periods of integrals. A final difference is, of course, the formulation in terms of invariance, instead of in terms of the values of the function. In a coherent manner, Puiseux stated the converse theorem, [Puiseux 1851, p. 237], as "an algebraic function of z which takes m values for each value of z satisfies an irreducible equation of degree m," letting the substitutions of the circular systems recede to the shadows. The two formulations of course are equivalent, as we have now seen several times; Galois and Hermite used constantly both. But the difference of emphasis will here create a direct bridge to Galois.

The point of Hermite's reformulation indeed becomes clear if we turn once more to the 1846 issue of Liouville's *Journal*, and Galois's definition of the group of an equation, his Proposition I:

> Let there be given an equation, of which a, b, c, ..., are the m roots. There will always be a group of permutations of the letters, a, b, c, ..., which will possess the following property: 1° that every function of the roots, invariant under the substitutions of this group, is rationally known; 2° conversely, every function of the roots which is rationally determined is invariant under these substitutions.[68]

---

66 [Hermite 1851, p. 277]: *Toute fonction des racines u, invariable par les substitutions S_0, $S_1, \ldots, S_{\mu-1}$ pourra être exprimée rationnellement par la variable z; et aussi la proposition réciproque. Toute fonction des racines u déterminable rationnellement en z, est invariable par les mêmes substitutions S_0, $S_1, \ldots, S_{\mu-1}$.*

67 In this paper, Hermite treated only the simplest case, with one circular system for each branch point, and thus one single S_i for each i, while Puiseux had spent considerable energy in discussing the general situation.

68 [Galois 1846, p. 421], [Galois 1962, p. 51]: *Soit une équation donnée, dont a, b, c, ..., sont les m racines. Il y aura toujours un groupe de permutations des lettres a, b, c, ... qui jouira de la propriété suivante: 1. que toute fonction des racines, invariable par les substitutions*

When the functions u_i replace the roots $a, b, c, \ldots$, we get almost word by word Hermite's statement.

Galois proved his statement by constructing a function, the famous V function, already alluded to in the preceding section, such that all the roots $a, b, c, \ldots$ of the given equation are rational functions of V, that is, $a = a(V), b = b(V), c = c(V), \ldots$ The point, this time, is to choose a function of the roots which takes different values when the roots are permuted. Then V is a solution of an irreducible equation, "Galois's equation in V," in Hermite's terms. And the permutations of the roots $a = a(V)$, $b = b(V), c = c(V), \ldots$, obtained when V is replaced in these expressions by the other roots $V', V'', \ldots$ of this equation, provide the sought-for group of permutations.[69]

Hermite's rewording of Puiseux, then, places the statement squarely in the wake of Galois, while interpreting the group in the modern sense. It naturally explains Hermite's immediate comment: "the group of substitutions in question will thus play exactly the same role as the group of Galois's irreducible equation in V."[70]

This group, in the case of algebraic functions, has been known as the *monodromy group*, at least since Camille Jordan's *Traité des substitutions et des équations algébriques* in 1870. One also finds in this treatise the determination of the monodromy group as well as that of the algebraic group, for the equation of the division of the periods of an elliptic function, and for

---

de ce groupe, soit rationnellement connue; 2. réciproquement, que toute fonction des racines, déterminable rationnellement, soit invariable par ces substitutions.

69 Let me remind the reader a last time that the substitutions exchanging the permutations of this "group of permutations" form a group in the modern sense. "Substitutions of this group," might thus mean "substitutions relative to this group of permutations," that is, exchanging the permutations that belong to a certain group, or "substitutions which are elements of this group," as the current understanding of the term would require. It depends on the authors, and sometimes of the moment. Contrarily to Hermite, Galois had trouble with the terminology at this precise place, see [Galois 1962, p. 52]. It also explains why taking "the group of the equation" as a fundamental object of investigation was not immediately meaningful. Serret's efforts to deal with the issue in the section IV of his *Cours d'algèbre*, playing on "systems of conjugate substitutions" and "groups of permutations" are very telling, see [Serret 1885, p. 243–350]. Hermite's modern use of group here has been noticed in [Kiernan 1971, p. 101].

70 [Hermite 1851, p. 277]: *Le groupe des substitutions en question jouera donc précisément le même rôle que le groupe de l'équation irréductible en V de Galois.*

modular equations, [Jordan 1870, p. 337–340, p. 345–346], two applications that Hermite had already announced in his 1851 articles, without presenting them explicitly.[71]

What Hermite did present, however, was in his words a "very simple example," giving conditions on the substitutions of the circular systems, such that the equation $F(u, z) = 0$ be solvable by radicals, for the case where m is a prime number. Here again, Hermite literally mimicked Galois's famous Proposition VII characterizing the group of an algebraic equation which is solvable by radicals, in order to adapt it to the new situation of equations containing algebraic functions, [Galois 1846, p. 429–433], Galois 1962, p. 65–69]. The results of both men are based on an analytic representation of the substitutions among the roots (that is, the substitutions of the group of the equation should be of the type $u_i \to u_{\alpha i+\beta}$) and on the choice of appropriate resolvents.

It would be tempting, but misleading, to read into *this* transfer a testimony of the unifying power of groups. Hermite, who used groups of substitutions extensively to study many things, from forms to analytic functions, objected all his life to the idea of founding mathematics on just a single one.[72] The vast field of investigations that, in his own terms and with his usual enthusiasm, Hermite saw opening up thanks to Puiseux's articles was more a further extension of his favorite research field, unified by constant comings and goings among its intertwined arithmetical, algebraic and analytic aspects, than a step towards the reduction to one main theory.

Norbert Schappacher and myself have, somewhat anachronistically, baptized this research field "arithmetic algebraic analysis." In the mid-nineteenth century, it interrelated a number of mathematicians around congruences, algebraic equations (specially those arising from analysis), and elliptic functions, as we have seen above, incorporating new techniques along the way, of which invariant theory, Cauchy analysis and

---

71 We see nonetheless several preparatory results in this direction in his later papers. To give just one example, Hermite's 1859 series of notes on modular equations opened with a recital of his difficulties with the determination of the discriminant of modular equations, something we can now recognize as an important step in following Puiseux's approach: "this difficulty stopped me for a long time from constructing the reduced equation of the eleventh degree of the modular equation of the twelfth," writes Hermite before undertaking the study of this discriminant [Hermite 1859, p. 38].

72 On this issue, see [Goldstein 2011]. In any case, if he had had to choose just one, it would have been elliptic functions, not groups, or for that matter, integers. In 1881, he characteristically wrote to Leopold Kronecker: "I see [in your work] a confirmation of what I think I told you once, that arithmetic is mainly an anticipation of the theory of elliptic functions," see [Goldstein 2007, p. 405].

Galois's theorems are but a few examples. Observing computations and formulas played a crucial role in their shared practice, but less as an objective in itself than as a means to detect key objects or phenomena, often with the expressed hope of finding a structured classification of numbers, functions, equations.[73] In this environment, this first publication of Hermite bearing on Galois's work does not appear as a singular investigation left to others to pursue, but as one of the threads of a dense decade-long weaving.

4. *ON COMBAT [...] LE PASSÉ PAR UN AUTRE PASSÉ*

In his classic paper on the development of Galois theory, Melvin Kiernan mused [Kiernan 1971, p. 101]:

> The writings of Charles Hermite during this period raise some interesting questions. What is his connection with the works of Galois? None of Hermite's papers at this time are directly related to Galois's work on equations and groups. Yet [...] his use of the term "group of substitutions" in 1851 in a way correct by modern standards indicates an understanding well in advance of anyone writing on the topic at that time. His ideas seem to take effect only in the writings of Jordan, over ten years later.

I have tried to show, on the contrary, how thorough, pervasive and fruitful was Hermite's connection with Galois.[74] Both men shared a common background of important sources: Lagrange, Gauss, Jacobi. Hermite read Galois early in his career and understood him well. He incorporated Galois's results, along with those of others, into his life-long programme on algebraic numbers and functions. He used them in his construction of two important bridges: one between invariant theory and linear substitutions, in connection with the modular and quintic equations; the other between Cauchy function theory and Galois theory, in connection with Puiseux's

---

73 These points are explained and illustrated in [Goldstein & Schappacher 2007a].

74 I have only followed the explicit traces of Galois's name in Hermite's papers; still other aspects would be worth looking at, in particular references to Abelian functions and Galois imaginaries. They would require a different approach and I shall not try and comment on them here.

work on algebraic functions. Inversely, Hermite contributed towards securing a place for Galois in mathematics. Not so much in establishing a ready-made Galois for textbooks[75] but in relaying him to the whole web of arithmetic algebraic analysis: traces of this are visible in papers by Betti, Kronecker, Carl Wilhelm Borchardt, among others, as of course theirs are in his.

Why have Hermite's dealings with Galois been so undervalued? One part of the answer lies in the drastic change in disciplinary organization at the end of the nineteenth century. The history of Galois's mathematics has been mostly told from the point of view of group theory, a discipline which, as Hans Wussing showed in 1969, won its autonomy in the 1870s [Wussing 1969]. Hermite relied on the inner properties of substitutions to study forms and equations and, as Kiernan noticed, he helped to fix the word "group" in its modern sense. But he was not interested in the description and labeling of the anatomy of groups *per se*.

A discipline is not only a bibliographical rubric.[76] It is defined by shared core objects and ways of constructing them, theorems and proof systems, mathematical values advocated in evaluating its results, etc.[77] What disciplinary change might mean for shaping what counts as an acceptable question can be illustrated by looking at how mathematicians pursued Galois's proposition on the reduction of modular equations: while Hermite in the 1850s felt the need to search for an effective construction of this reduction, by the 1880s Gierster thought it important to list all the subgroups of the groups of modular equations.

Moreover, a discipline is usually accompanied by the writing of a collective memory, including a chronology of the main advances in the discipline, for instance. Caroline Ehrhardt has shown in her thesis how

---

75 Still, a section in Serret's treatise on higher algebra was devoted to the analytic representation of substitutions with Hermite's characterization of them; Serret also included Hermite's proof of Galois's statement that if one equation is solvable by radicals, all its roots can be expressed rationally from two of them, a proof close to that used by Hermite in 1851 for algebraic functions, see [Serret 1885, p. 383–389, and 677–683], and also [Hermite *Œuvres*, vol. 3, p. 479–484]. How Galois's and Hermite's contributions, were introduced in the various editions of Serret's treatise is explained in detail in [Ehrhardt 2007, p. 359–392].

76 I am using the word "discipline," as defined in [Guntau & Laitko 1987, p. 26], that is "an object-oriented system of scholarly activities" with a list of criteria attached to it. This definition of discipline is larger than that which restricts the word to official parts of academic curriculum.

77 These criteria are not exhaustive, but an important point is that they are collective ones. These issues are discussed in detail for the case of number theory in [Goldstein & Schappacher 2007a, Goldstein & Schappacher 2007b].

discontinuous the history of the reception of Galois's work appears when represented from the disciplinary perspective of group theory: scattered works of apparently no lasting impact (including those of Hermite) until the 1870s, then suddenly the appearance of landmarks like Jordan's *Traité des substitutions et des équations algébriques* or Klein's *Erlanger Programm*, followed by a blossoming of textbooks, etc. The reason for this is that the past is interrogated using criteria of the current discipline, in particular its concepts and ways of shaping them. Hermite's practice went against the idea of ontologizing tools, like groups or Riemann surfaces: in particular it did not fit into the new disciplinary structure and his work was thus either partially dismissed as irrelevant, or mined in a purely local way, for specific results or techniques.[78]

In this respect it is particularly telling to look at Klein's 1884 *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*; it offers a vast synthesis of previous work on the quintic, including that of Hermite, Brioschi and Kronecker. This synthesis is based on a geometrical point of view, supported by group and invariant theory as in the *Erlanger Programm*. The Galois group $PSL_2(\mathbf{F}_5)$ of the modular equation of order 5, for instance, is interpreted as the group of transformations of the icosahedron.[79] When we recall that Hermite in the course of his work linked invariant theory and substitution groups, on one hand, and Cauchy analysis and Galois groups on the other, Klein's presentation of the first part of his book cannot but awake a sense of déjà vu:

> If we look back, in the second chapter we have just finished, we have succeeded in linking the geometric group-theoretical results of the first chapter with a particular domain of the most recent mathematics, namely the algebra of linear substitutions and its corresponding invariant theory. In the same way, the two following chapters will be devoted to forging a link with two other modern disciplines. These are Riemann's function theory and Galois's theory of algebraic equations.[80]

---

78 The change in the conception of mathematical objects at the end of the nineteenth century is discussed in [Gray 1996], Hermite's point of view in [Goldstein 2011].

79 Klein's book is presented in detail, both mathematically and historically, in [Gray 2000].

80 [Klein 1884, p. 61]: *Blicken wir zurück, so haben wir in dem zweiten nunmehr beendeten Kapitel dieses erreicht, dass wir die geometrisch-gruppen-theoretischen Resultate des ersten Kapitels mit einem bestimmten Gebiete der neueren Mathematik in Verbindung gesetzt haben, nämlich mit der Algebra der linearen Substitutionen und der zugehörigen Invariantentheorie. In ganz ähnlicher Weise sollen die folgenden beiden Kapitel bestimmt sein, die Verbindung mit zwei anderen modernen Disciplinen herzustellen. Es sind die Riemann'sche Functionentheorie und die Galois'sche Theorie der algebraischen Gleichungen.*

Now, it is true that Hermite's technical contributions are used at various places in Klein's book—monodromy groups, the identification of $PSL_2(\mathbf{F}_5)$ with the group of even permutations on five letters, $\mathscr{A}_5$, the use of invariant theory to renormalize algebraic equations, etc.—and most of Hermite's papers we have mentioned here appear scattered in the references. But Hermite's own synthesis on the quintic, elaborated in [Hermite 1865], and the bridges he had already constructed, are not credited. Moreover, Klein dismisses the old way of mixing with analytic functions what he wants to isolate as the "purely algebraic" problems of the reduction to the quintic :

> We have shown [...] that such a use of transcendental functions possesses above all a practical value and should not be mixed up with the theoretical investigations of the theory of equations. [...] Hermite's work has no relation whatsoever to the algebraic theory of the quintic [...] because, in the view we will maintain here, the use of elliptic functions appears to be completely secondary.[81]

The disciplinary choices here are manifest: pushing Jacobian elliptic functions out by the revolving door while projective geometry comes in; replacing Cauchy by Riemann, the theory of invariants of Cayley, Hermite and Sylvester by that of his own coworker Paul Albert Gordan; defining what will be considered "algebraic"; and transforming Richard Dedekind's motto, "concepts instead of formulas," into "theory instead computations." On the contrary, Hermite (and other contributors to arithmetic algebraic analysis) defended the viewpoint that ideas came from computations and the observation of formulas; for them, theory was not reducible to conceptual creation; and unification itself, an issue shared by both Hermite and Klein, was not understood in the same way.[82]

If Hermite's contributions in the small were known and used, Hermite's work on quintic equations in the large was assigned to complex analysis and practical issues, and thus severed from Galois's heritage, associated now with the new group theory. As it is Klein's viewpoint that became the basis of a new orthodoxy we can understand why Kiernan might think that

---

81 [Klein 1884, p. 140–141, p. 149]: *Wir haben [...] gezeigt, dass eine solche Benutzung transcendenter Funktionen zuvörderst nur praktischen Werth besitzt und mit den theoretischen Untersuchungen der Gleichungstheorie nicht untermischt werden soll. [...] Hermite's Arbeit hat [...] in keiner Weise Beziehung zur algebraischen Theorie der Gleichungen fünften Grades [...] denn der Gebrauch der elliptischen Funktionen erscheint bei der Auffassung, die wir weiterhin festzuhalten haben, durchaus als sekundär.*

82 This comparison and its consequences will be discussed elsewhere, as well as its personal and tactical components.

Hermite's work concerned neither group theory nor the algebraic theory of equations.

Taking into account Hermite's contribution helps us to connect some of the apparently discontinuous elements of the usual version of the history of Galois's ideas, in particular, revealing important elements of transmission from Galois to Jordan and Klein.[83] Can it also contribute to a better understanding of Galois's work itself? There is no way of knowing if Galois would have been, had he lived, a participant in arithmetic algebraic analysis, as Dirichlet and Kummer were. Moreover, this research field, as it developed, was never a discipline in the sense adopted earlier; in particular it was not defined by a key method or a key object clearly detectable in mathematical writings. Hermite did not take from Galois one single general conceptual insight, but important mathematical ideas.

> There are living questions that catch the most enlightened minds, as if in spite of themselves. [...] If one looks for the cause, it is easy to find in the works that have preceded us. [... Scientists] also belong to their time,[84]

wrote Galois. The fact is that his sources, his mathematical interests, his results, all fit rather well the predilections of arithmetic algebraic analysis: congruences in the service of the theory of equations, equations linked to the division or the transformation of elliptic functions, periods of integrals of algebraic functions, substitutions applied to analysis. The younger generation of analysts, Serret, Hermite, Kronecker and Betti—all born between 1819 and 1823, all familiar with the same sources—had little difficulty in understanding him.

As hinted earlier, his practice, if one risks speculating with so few texts, did not provide an overlook on permutations as the group-theoretical approach would do.[85] From the point of view of group theory, it is Galois's Proposition VII (met in sec. 3) which entails the quintessential result, as it describes the conditions for an irreducible equation of prime degree to be solvable by radicals in terms of a group (via a slight confusion on the meaning of the word "group"). But Galois did not stop after this statement: he gave two other formulations, one in terms of the resolvent equation,[86] and

---

83 On the transfer to Jordan of Hermitian themes, see [Brechenmacher 2011].

84 [Galois 1962, p. 19]: *Il y a des questions vivantes qui fixent les esprits les plus éclairés, comme malgré eux [...], si l'on en cherche la cause, il est aisé de la trouver dans les ouvrages de ceux qui nous ont précédés. [... Les savants] eux aussi appartiennent à leur époque.*

85 [Goldstein & Schappacher 2007a, p. 34–35]. Galois's early practice is studied in depth in [Ehrhardt 2007, ch. 1-3 and 2.1].

86 Galois added: "This is the means that one should apply in practice," (*C'est là le moyen qu'il faudrait employer dans la pratique*), [Galois 1962, p. 69], which might or

one, the final Proposition VIII, which reads: "such an equation is solvable by radicals if and only if all its roots can be deduced rationally from two of them." This last formulation was indeed that used when Liouville or Serret, for instance, explained Galois's main results to a mathematical audience. This formulation, not that in terms of groups, provides the thread running from Gauss and Abel on equations whose roots can be deduced rationally from one of them, as the cyclotomic equations, to Kronecker on Abelian equations in the 1850s ([Kronecker 1853]). As for Galois's conception of science itself:

> [The life of science] is rough and resembles that of minerals that grow by accretion, … analysts do not deduce, they combine, they compose: immaterial as it is, analysis is no more in our power than any other [science]; one has to spy upon it, sound it out, solicit it.[87]

Echoes of this are to be found in Hermite and Kronecker, in stark contrast to Hilbert's belief that, "instead of the erratic progress characteristic of the youngest age of science, a sure and continuous development is now occuring, thanks to the systematic construction of the theory of number fields."[88]

To study how Galois's crystals were accreted with others in Hermitian arithmetic algebraic analysis may help us to avoid taking for granted what was often described as the incommensurability of Galois's proposal with the mathematical world before the 1870s. It may help us to see Galois, not only through his rather dismal biography or through the simplified conceptual prism that group theory projects back on his writings, but as a mathematician who, in the "safe haven of actual mathematics," intervened in "the many questions of a new kind [that in his days] engaged the analysts."[89]

On ajoutera: 'je ne sais pas le reste'.[90]

---

might not be a taunt at Poisson, whose report on Galois's memoir criticized its lack of applicability. In any case, it testifies to what was considered important in the 1830s, and still in the 1850s.

87 [Galois 1962, p. 15]: *[La vie de la science] est brute et ressemble à celles des minéraux qui croissent par juxtaposition. …Les analystes ne déduisent pas, ils combinent, ils composent: toute immatérielle qu'elle est l'analyse n'est pas plus en notre pouvoir que d'autres; il faut l'épier, la sonder, la solliciter.*

88 On this point, see [Goldstein & Schappacher 2007b, p. 76–90]

89 The first quote is from Kronecker [Edwards 1995, p. 45–46], the second from Galois himself [Galois 1962, p. 19].

90 [Galois 1962, p. 11]. The title of this section, "On combat le passé…" comes from [Galois 1962, p. 27], the exact sentence being: *On combat les professeurs par l'institut, l'institut par le passé, le passé par un autre passé.*

REFERENCES

BELHOSTE (Bruno)

[1996] Autour d'un mémoire inédit: la contribution d'Hermite au développement de la théorie des fonctions elliptiques, *Revue d'histoire des mathématiques* 2 (1996), p. 1–66.

BELHOSTE (Bruno) & LÜTZEN (Jesper)

[1984] Joseph Liouville et le Collège de France, *Revue d'histoire des sciences* 37 (1984), p. 255–304.

BERTRAND (Joseph)

[1884] Éloge de M. Victor Puiseux, lu dans la séance publique annuelle de l'Académie des sciences du 5 mai 1884, *Bulletin des sciences mathématiques et astronomiques* 2e sér., 8 (1884), p. 227–234.

[1899] Compte-rendu de *La Vie d'Évariste Galois* par P. Dupuy, *Journal des savants* (juillet 1899), p. 389–400.

BONIFACE (Jacqueline)

[2007] The Concept of Number from Gauss to Kronecker, in [Goldstein, Schappacher & Schwermer 2007], p. 314–342.

BOUCARD (Jenny)

[2011] Louis Poinsot et la théorie de l'ordre: un chaînon manquant entre Gauss et Galois?, *Revue d'histoire des mathématiques* 17 (2011), p. 41–138.

BRASSEUR (Roland)

[2010] Quelques scientifiques ayant enseigné aux classes préparatoires aux grandes écoles, *Bulletin de l'UPS* 232 (octobre 2010), p. 1–15.

BRECHENMACHER (Frédéric)

[2007] La controverse de 1874 entre Camille Jordan et Leopold Kronecker, *Revue d'Histoire des Mathématiques* 13 (2007), p. 187–257.

[2011] Self-portraits with Evariste Galois (and the shadow of Camille Jordan), this issue.

BREZINSKI (Claude)

[1991] *History of Continued Fractions and Padé Approximants*, Berlin, New York: Springer, 1991.

BRILL (Alexander von) & NOETHER (Max)

[1894] Bericht über die Entwicklung der Theorie der algebraischen Functionen in älterer und neuerer Zeit, *Jahresbericht der deutschen Mathematiker-Vereinigung* 3 (1894), p. 107–565.

Briot (Charles) & Bouquet (Claude)
[1875] *Traité des fonctions elliptiques*, 2e ed., Paris: Gauthier-Villars, 1875.

Cahen (Eugène)
[1914–1924] Théorie des nombres, 2 vols., Paris: Hermann, vol. 1: "Le Premier Degré," 1914; vol. 2: "Le Second Degré binaire," 1924.

Cauchy (Augustin Louis)
[*Œuvres*] *Œuvres complètes*, 27 vol. en deux séries, Paris: Gauthier-Villars, 1882–1974.

Cayley (Arthur)
[1876] *An elementary treatise on elliptic functions*, Cambridge: Deighton, Bell; London: Bell, 1876.

Charve (Léon)
[1877] Démonstration de la périodicité des fractions continues, engendrées par les racines d'une équation du deuxième degré, *Bulletin des sciences mathématiques et astronomiques* 2e sér. 1 (1877), p. 41–43.

[1880] *De la réduction des formes quadratiques ternaires positives et de leur application aux irrationnelles du troisième degré*, thèse présentée à la faculté des sciences de Paris, Paris: Gauthier-Villars, 1880. Repr. *Annales de l'École normale supérieure* 2e sér. 9 (1880), p. 3–156 (supplément).

Dahan-Dalmedico (Amy)
[1982] Résolubilité des équations par radicaux et premier mémoire d'Évariste Galois, *Présence d'Evariste Galois*, no 48, Paris: Publication de l'A.P.M.E.P, 1982, p. 43–53.

Darboux (Gaston)
[1905] *Notice historique sur Charles Hermite*, Paris: Gauthier-Villars, 1905.

Dupuy (Paul)
[1896] La vie d'Évariste Galois, *Annales scientifiques de l'École Normale Supérieure* 3e sér. 13 (1896), p. 197–266.

Edwards (Harold M.)
[1995] Kronecker on the Foundations of Mathematics, in J. Hintikka (ed.), *From Dedekind to Gödel. Essays on the Development of the Foundations of Mathematics*, Dordrecht: Kluwer, 1995, p. 45–52.

EHRHARDT (Caroline)

[2007] *Évariste Galois et la théorie des groupes. Fortunes et réélaborations (1811–1910)*, Thèse de l'EHESS, 2007.

[2008] Évariste Galois, un candidat à l'école préparatoire en 1829, *Revue d'histoire des mathématiques* 14-2 (2008), p. 289–328.

[2011] *Évariste Galois, la fabrication d'une icône mathématique*, Paris: EHESS, 2011.

EULER (Leonard)

[1810] *Elements of Algebra, translated from the French, with the Additions of Lagrange*, 2nd ed., 2 vols., London: Johnson.

FOWLER (David)

[1990] *The Mathematics of Plato's Academy: a new reconstruction*, Oxford: Clarendon Press, 1990.

GALOIS (Évariste)

[1828–1829] Analyse algébrique. Démonstration d'un théorème sur les fractions continues périodiques, *Annales de mathématiques pures et appliquées = Annales de Gergonne* 19 (1828–1829), p. 294–301. Repr. (with corrections) in [Galois 1846], p. 385–392, and in [Galois 1962], p. 365–377.

[1846] Œuvres mathématiques, *Journal de mathématiques pures et appliquées* 1re sér. 11 (1846), p. 381–444.

[1962] *Écrits et mémoires mathématiques*, éd. R. Bourgne et J.-P. Azra, Paris: Gauthier-Villars, 1962.

GIERSTER (Joseph)

[1881] Die Untergruppen der Galois'schen Gruppe der Modulargleichungen fur den Fall eines primzahligen Transformationsgrades, *Mathematische Annalen* 18 (1881), p. 319–365.

GOLDSTEIN (Catherine)

[1989] Le métier des nombres aux XVIIe et XIXe siècles, in M. Serres (dir.), *Éléments d'histoire des sciences*, Paris: Bordas, 1989, p. 274–295; eng. transl. *A History of Scientific Thought*, Oxford: Blackwell, 1995, p. 344–371.

[2007] The Hermitian Form of Reading the *Disquisitiones*, in [Goldstein, Schappacher & Schwermer 2007], p. 377–410.

[2011] Un arithméticien contre l'arithmétisation: les principes de Charles Hermite, in D. Flament et P. Nabonnand (dir.), *Justifier les mathématiques*, Paris: MSH, 2011, p. 119–155.

GOLDSTEIN (Catherine) & SCHAPPACHER (Norbert)

[2007a] A Book in Search of a Discipline, in [Goldstein, Schappacher & Schwermer 2007], p. 3–65.

[2007b] Several Disciplines and a Book, in [Goldstein, Schappacher & Schwermer 2007], p. 66–103.

GOLDSTEIN (Catherine), SCHAPPACHER (Norbert) & SCHWERMER (Joachim) (eds.)

[2007] *The Shaping of Arithmetic after C. F. Gauss's* Disquisitiones Arithmeticae, Berlin: Springer, 2007.

GRATTAN-GUINNESS (Ivor)

[1990] *Convolutions in French Mathematics, 1800–1840*, 3 vols., Basel: Birkhäuser, 1990.

GRAY (Jeremy)

[1996] The Nineteenth-Century Revolution in Mathematical Ontology, in D. Gillies (ed.), *Revolutions in Mathematics*, Oxford: Oxford University Press, 1996, p. 226–248.

[2000] *Linear Differential Equations and Group Theory from Riemann to Poincaré*, 2nd ed., Boston: Birkhäuser, 2000.

GUNTAU (Martin) & LAITKO (Hubert)

[1987] Entstehung und Wesen wissenschaftlicher Disziplinen, in M. Guntau, H. Laitko (eds.), *Der Ursprung der modernen Wissenschaften*, Berlin: Akademie-Verlag, 1987, p. 17–89.

HERMITE (Charles)

[*Œuvres*] *Œuvres*, ed. E. Picard, 4 vol., Paris: Gauthier-Villars, 1905–1917.

[1842] Considération sur la résolution algébrique de l'équation du cinquième degré, *Nouvelles annales* 1re sér. 1 (1842), p. 329–336. Repr. in [Hermite *Œuvres*], vol. 1, p. 3–9.

[1848] Sur la division des fonctions abéliennes ou ultra-elliptiques, *Mémoires présentés par divers savants à l'Académie royale des sciences* 10 (1848), p. 563–574. Repr. in [Hermite *Œuvres*], vol. 1, p. 38–48.

[1850] Lettres à M. Jacobi sur différents objets de la théorie des nombres, *Journal für die reine und angewandte Mathematik* 40 (1850), p. 261–315. Repr. in [Hermite *Œuvres*], vol. 1, p. 100–163.

[1851] Sur les fonctions algébriques, *Comptes rendus hebdomadaires des séances de l'Académie des sciences* 32 (1851), p. 458–461. Repr. in [Hermite *Œuvres*], vol. 1, p. 276–280.

[1854] Sur la théorie des fonctions homogènes à deux indéterminées, *Cambridge and Dublin Mathematical Journal* 9 (1854), p. 172–217. Repr. in [Hermite *Œuvres*], vol. 1, p. 296–349.

[1856] Sur la théorie des fonctions homogènes à deux indéterminées, *Journal für die reine und angewandte Mathematik* 52 (1856), p. 1–38. Repr. in [Hermite *Œuvres*], vol. 2, p. 350–396.

[1858a] Sur la résolution de l'équation du cinquième degré, *Comptes rendus hebdomadaires des séances des l'Académie des sciences* 46 (1858), p. 508–515. Rep. in [Hermite *Œuvres*], vol. 2, p. 5–12.

[1858b] Sur la résolution de l'équation du quatrième degré, *Comptes rendus hebdomadaires des séances des l'Académie des sciences* 46 (1858), p. 715–722. Rep. in [Hermite *Œuvres*], vol. 2, p. 22–29.

[1859] Sur la théorie des équations modulaires, *Comptes rendus hebdomadaires des séances des l'Académie des sciences* 48 (1859), p. 940–47, 1079–1084, 1096–1102, and 49 (1859), p. 16–24, 110–118, 141–144. Rep. in [Hermite *Œuvres*], vol. 2, p. 38–82.

[1863] Sur les fonctions de sept lettres, *Comptes rendus hebdomadaires des séances des l'Académie des sciences* 57 (1863), p. 750–757. Rep. in [Hermite *Œuvres*], vol. 2, p. 280–288.

[1865] Sur l'équation du cinquième degré, *Comptes rendus hebdomadaires des séances des l'Académie des sciences* 61 (1865), p. 877–882, 965–972, 1073–1081 and 62 (1866), p. 65–72, 157–162, 245–252, 715–722, 919–924, 959–966, 1054–1059, 1161–1167, 1213–1215. Rep. in [Hermite *Œuvres*], vol. 2, p. 347–424.

[1885] Sur la théorie des fractions continues, *Bulletin des sciences mathématiques* 2e sér. 9 (1885), p. 11–13. Repr. in [Hermite *Œuvres*], vol. 4, p. 178–180.

[1901] Sulle frazioni continue, *Le matematiche pure ed applicate* I (1901), p. 1–2. Repr. in [Hermite *Œuvres*], vol. 4, p. 552–553.

HERMITE (Charles) & GENOCCHI (Angelo)

[*Corresp.*] *Le Lettere di Charles Hermite a Angelo Genocchi (1868–1887)*, ed. G. Michelacci, Quaderni matematici (2ª ser.) 546, Trieste: Dipartimento di scienze matematiche, 2003.

HERMITE (Charles) & MITTAG-LEFFLER (Gösta)

[*Corresp.*] Lettres de Charles Hermite à Gösta Mittag-Leffler, [ed. P. Dugac], *Cahiers du séminaire d'histoire des mathématiques* 5 (1984), p. 49–285 (letters 1874–1883); 6 (1985), p. 79–217 (letters 1884–1891); 10 (1989), p. 1–82 (letters 1892–1900).

HERMITE (Charles) & STIELTJES (Thomas)

[*Corresp.*] *Correspondance d'Hermite et de Stieltjes*, ed. B. Baillaud, H. Bourget, 2 vols., Paris: Gauthier-Villars, 1905.

Houzel (Christian)
[1978] Fonctions elliptiques et intégrales abéliennes, in J. Dieudonné (dir.), *Abrégé d'histoire des mathématiques 1700–1900*, 2 vols., Paris: Hermann, vol. 2, p. 1–113.
[2003] L'équation générale du cinquième degré, in *La Géométrie algébrique. Recherches historiques*, Paris: Blanchard, 2003.

Jacobi (Carl Gustav Jacob)
[1829] *Fundamenta nova theoriae functionum ellipticarum*, Berlin: Bornträger, 1829. Repr. in *Gesammelte Werke*, ed. C. W. Borchardt, Berlin: Reimer, 1881, vol. 1, p. 49–239.

Jordan (Camille)
[1870] *Traité des substitutions et des équations algébriques*, Paris: Gauthier-Villars, 1870.

Kiernan (B. Melvin)
[1971] The Development of Galois Theory from Lagrange to Artin, *Archive for History of Exact Sciences* 8 (1971), p. 40–154.

Klein (Felix)
[1884] *Vorlesungen über das Ikosaeder*, Leipzig: Teubner, 1884.

Kronecker (Leopold)
[1853] Über die algebraisch auflösbaren Gleichungen, *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* (1853), p. 365–374. Repr. in *Werke*, ed. K. Hensel, Leipzig, Berlin: Teubner, 1929, vol. IV, p. 1–13.

Lagrange (Joseph Louis)
[*Œuvres*] *Œuvres*, ed. J.-A. Serret, 14 vols., Paris: Gauthier-Villars, 1867–1892.

Lebesgue (Victor-Amédée)
[1831] Note sur les fractions continues périodiques, *Bulletin des sciences mathématiques, physiques et chimiques* 15 (1831), p. 155–158.
[1840] Résolution de l'équation du second degré à une inconnue par les fractions continues. *Journal de mathématiques pures et appliquées* 1re sér. 5 (1840), p. 281–310.

Legendre (Adrien-Marie)
[1798] *Essai sur la théorie des nombres*, Paris: Duprat, an VI.

Mammone (Pasquale)
[1989] Sur l'apport d'Enrico Betti en théorie de Galois, *Bollettino di storia delle scienze matematiche* 9 (2) (1989), p. 143–169.

McKean (Henry) & Moll (Victor)
[1999] *Elliptic Curves*, Cambridge: Cambridge University Press, 1999.

Möbius (Augustus)
[1830] Beiträge zu der Lehre von den Kettenbrüchen, nebst einem Anhange dioptrischen Inhalts, *Journal für die reine und angewandte Mathematik* 5 (1830), p. 215–243.

Neumann (Olaf)
[1996] Die Entwicklung der Galois-Theorie zwischen Arithmetik und Topologie (1850 bis 1960), *Archive for History of Exact Sciences* 50 (1996), p. 291–329.
[2007] The *Disquisitiones arithmeticae* and the Theory of Equations, in [Goldstein, Schappacher & Schwermer 2007], p. 107–127.

Perron (Oskar)
[1929] *Die Lehre von den Kettenbrüchen*, 2nd ed., Stuttgart: Teubner 1929.

Petri (Birgit) & Schappacher (Norbert)
[2007] On Arithmetization, in [Goldstein, Schappacher & Schwermer 2007], p. 343–374.

Pierpont (James)
[1895] Zur Geschichte der Gleichung des V. Grades (bis 1858), *Monatshefte für Mathematik und Physik* 6 (1895), p. 15–68.

Pringsheim (Alfred)
[1898] Irrationalzahlen und Konvergenz unendlicher Prozesse, in *Encyklopädie der mathematischen Wissenschaften mit Einschluss ihrer Anwendungen*, vol. 1, Leipzig: Teubner, 1898, p. 47–146.

Puiseux (Victor)
[1850] Recherches sur les fonctions algébriques, *Journal de mathématiques pures et appliquées* 1re sér. 15 (1850), p. 365–480.
[1851] Nouvelles recherches sur les fonctions algébriques, *Journal de mathématiques pures et appliquées* 1re sér. 16 (1851), p. 228–240.

Ramus (Christian)
[1839] Remarques sur les fractions continues périodiques, *Journal für die reine und angewandte Mathematik* 20 (1839), p. 13–27.

Serret (Joseph-Alfred)
[1885] *Cours d'algèbre supérieure*, Paris: Bachelier, 1849; 2nd ed., Paris: Mallet-Bachelier, 1854; Paris: Gauthier-Villars, 2 vol., 3rd ed., 1866, 4th ed., 1877; 5th ed., 1885, 6th ed., 1910; 7th ed., 1928. All quotes are from the 5th ed.

Serfati (Michel)
[1992] *Quadrature du cercle, fractions continues, et autres contes. Sur l'histoire des nombres irrationnels et transcendants aux XVIII^e et XIX^e siècles*, Paris: Éditions de l'Association des Professeurs de Mathématiques, 1992.

Stern (Moritz)
[1832] Observationes in fractiones continuas, *Journal für die reine und angewandte Mathematik* 8 (1832), p. 192–193.

Terquem (Olry)
[1849] Biographie. Richard, professeur, *Nouvelles Annales de Mathématiques* 1re sér. 8 (1849), p. 448–452.

Waldschmidt (Michel)
[1983] Les débuts de la théorie des nombres transcendants (à l'occasion du centenaire de la transcendance de π), *Cahiers du séminaire d'histoire des mathématiques* 4 (1983), p. 93–115.

Weber (Heinrich)
[1891] *Elliptische Funktionen und algebraische Zahlen*, Braunschweig: Vieweg, 1891.

Wussing (Hans)
[1969] *Die Genesis des abstrakten Gruppenbegriffes. Ein Beitrag zur Entstehungsgeschichte der abstrakten Gruppentheorie*, Berlin: Deutscher Verlag der Wissenschaften, 1969.