

A History of Galois fields

Frederic Brechenmacher

▶ **To cite this version:**

Frederic Brechenmacher. A History of Galois fields. 2012. hal-00786662

HAL Id: hal-00786662
https://hal.science/hal-00786662

Preprint submitted on 9 Feb 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A history of Galois fields

Frédéric Brechenmacher *

Université d'Artois
Laboratoire de mathématiques de Lens (EA 2462)
rue Jean Souvraz S.P. 18, 62307 Lens Cedex France.
&
École polytechnique
Département humanités et sciences sociales
91128 Palaiseau Cedex, France.

Abstract

This paper stresses a specific line of development of the notion of finite field, from Évariste Galois's 1830 "Note sur la théorie des nombres," and Camille Jordan's 1870 *Traité des substitutions et des équations algébriques*, to Leonard Dickson's 1901 *Linear groups with an exposition of the Galois theory*.

This line of development highlights the key role played by some specific algebraic procedures. These intrisically interlaced the indexations provided by Galois's number-theoretic imaginaries with decompositions of the analytic representations of linear substitutions. Moreover, these procedures shed light on a key aspect of Galois's works that had received little attention until now.

The methodology of the present paper is based on investigations of intertextual references for identifying some specific collective dimensions of mathematics. We shall take as a starting point a coherent network of texts that were published mostly in France and in the U.S.A. from 1893 to 1907 (the "Galois fields network," for short). The main shared references in this corpus were some texts published in France over the course of the 19th century, especially by Galois, Hermite, Mathieu, Serret, and Jordan. The issue of the collective dimensions underlying this network is thus especially intriguing. Indeed, the historiography of algebra has often put to the fore some specific approaches developped in Germany, with little attention to works published in France. Moreover, the "German abstract algebra" has been considered to have strongly influenced the development of the American mathematical community. Actually, this influence has precisely been illustrated by the example of Elliakim Hasting Moore's lecture on "abstract Galois fields" at the Chicago congress in 1893. To be sure, this intriguing situation raises some issues of circulations of knowledge from Paris to Chicago. It also calls for reflection on the articulations between the individual and the collective dimensions of mathematics. Such articulations have often been analyzed by appealing

*Electronic address: frederic.brechenmacher@euler.univ-artois.fr

Ce travail a bénéficié d'une aide de l'Agence Nationale de la Recherche : projet CaaFÉ (ANR-10-JCJC 0101)

to categories such as nations, disciplines, or institutions (e.g., the "German algebra," the "Chicago algebraic research school"). Yet, we shall see that these categories fail to characterize an important specific approach to Galois fields.

The coherence of the Galois fields network had underlying it some collective interest for "linear groups in Galois fields." Yet, the latter designation was less pointing to a theory, or a discipline, revolving around a specific object, i.e. $Gl_n(F_{p^n})$ (p a prime number), than to some specific procedures. In modern parlance, general linear groups in Galois fields were introduced in this context as the maximal group in which an elementary abelian group (i.e., the multiplicative group of a Galois field) is a normal subgroup.

The Galois fields network was actually rooted on a specific algebraic culture that had developed over the course of the 19th century. We shall see that this shared culture resulted from the circulation of some specific algebraic procedures of decompositions of polynomial representations of substitutions.

Contents

Introduction **4**

1 Problems, questions and methods **5**

1.1 Algebra and the collective dimensions of mathematics 5

1.2 Networks of texts as a method of investigation 9

1.3 The Galois fields network 10

1.4 The structure of the present paper 11

2 Linear groups in Galois fields from 1893 to 1907 **11**

2.1 The problematic collective dimensions of the Galois fields network 11

2.1.1 Disciplines : finite groups 11

2.1.2 Disciplines : abstract group 12

2.1.3 Nations 13

2.2 Moore's Galois fields 13

2.2.1 Research schools 13

2.2.2 Paying tribute to Klein... 14

2.2.3 ... but colliding to the implicit collective dimension lying beneath the use of Galois imaginaries 15

2.3 What's new in Moore's paper ? 16

2.3.1 The shadow of Klein-Fricke's textbook on Moore's incomplete references . 16

2.3.2 Every Galois field is a Galois field 17

2.3.3 Lost in a fog of old French works 18

3 Galois number-theoretical imaginaries in the long run **19**

3.1 On the variety of the forms of representations of substitutions in the 19th century 19

3.2 The analytic representation of substitutions 21

3.3 The special case of cycles : two indexations, two analytic representations 21

3.4 Cyclotomy . . . 22
3.5 Poinsot's groups . . . 23
3.6 Galois's criterion for irreducible equations of prime degree . . . 24
3.7 Galois's attempts to generalize his criterion to equations of degree p^n . . . 26
3.8 Galois's number theoretic imaginaries . . . 28
3.9 Generalities and applications . . . 30
3.10 The analytic representation of substitutions and the various forms of receptions of Galois's works . . . 32
3.10.1 The form $(k\ ak+b)$ . . . 34
3.10.2 The form $(k\ \frac{ak+b}{ck+d})$ . . . 35
3.10.3 The general linear form in n variables . . . 36

4 Jordan's general linear group **37**
4.1 The origin of the linear group . . . 37
4.2 Jordan's reduction of analytic representations . . . 40
4.3 The Jordan canonical form theorem . . . 42
4.4 The architecture of Jordan's *Traité* . . . 43
4.4.1 Livre I. On congruences . . . 43
4.4.2 Livre II. Des substitutions . . . 43
4.4.3 Livre III. On irrationnalities . . . 44
4.4.4 Livre IV. On solutions by radicals . . . 45

5 A shared algebraic culture **46**
5.1 Number-theoretic imaginaries and substitutions . . . 47
5.2 Number-theoretic imaginaries as an autonomous theory . . . 48
5.3 Jordan's *Traité* as a Chicagoan textbook . . . 49
5.4 Linear groups in Galois fields : a shared algebraic culture . . . 51
5.5 A space of circulation of specific practices of reductions of analytic representations 52

Conclusion **54**

Annex 2 : Indexations and the analytic representations of cycles **56**

Annex 3. The number of values of functions and the resolution of equations by radicals **60**

Bibliography **70**

Introduction

This paper investigates the history of Galois fields in the 19th century. Yet, many of the texts that one could relate to finite fields from a retrospective point of view will not be in the scope of the present investigation. I will rather analyze a specific line of development in which Galois fields were intrinsically interlaced with some procedures of decompositions of the analytic (i.e., polynomial) representations of linear groups. A key role in this context was played by Jordan's famed 1870 *Traité des substitutions et des équations algébriques* (the *Traité* for short). This treatise provided a specific approach to linear groups in Galois fields that would be taken up in the thesis Leonard Dickson completed in 1896 under the supervision of Eliakim Hastings Moore : *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group.* This approach would be developped a few years later in Dickson's 1901 monograph, *Linear groups with an exposition of the Galois field theory.*

I shall problematize the issues that will be tackled in the present paper in section I below. Yet, before getting into details about these issues, let me first introduce further the mathematics involved by summing up briefly the role played by Galois fields in Jordan's *Traité*.[1]

The "Théorie de Galois" alluded to in the very short Livre I is all about higher congruences $f \equiv 0 \pmod{P}$, for an irreducible polynomial of degree n with integer coefficients. It thus deals with what would nowadays be called finite fields, or Galois fields, in the tradition of the number-theoretical imaginaries which Galois had introduced in his 1830 "Note sur la théorie des nombres" (the *Note*, for short).[2] Yet, Galois's imaginaries bear only a very indirect relation to the general principles of his famous "Mémoire sur les conditions de résolubilité des équations par radicaux" (the *Mémoire*, for short), and therefore also to the correspondence between fields and groups which is today perceived as the very essence of Galois theory.[3] Indeed, for Galois, number-theoretic imaginaries were above all useful in enabling a practice for dealing with the substitutions involved in the investigation of primitive equations of prime power degree.[Galois, 1830b, p.405-407][Galois, 1832, p.410][4] More precisely, one of the first general principles of the *Mémoire* had been to consider as rational "every rational function of a certain number of determined quantities which are supposed to be known a priori - we shall [then] say that we adjoin them to the equation to be solved."[Galois, 1831b, p.418][5] The *Mémoire*'s first proposition stated that: "Let a given equation have the m roots a, b, c, ... There will always be a group of permutations of the

[1] For a description of Jordan's specific relation to Galois's works, and its reception, see [Brechenmacher, 2011]

[2] Independently of the legacy of Galois, finite fields had been developed in the legacy of Gauss by Schönemann, Dedekind, and Kronecker. See[Frei, 2007]. I will not deal in this paper with these lines of developments of finite fields. Even though Dedekind had lectured on Galois's works in Göttingen in the mid-1850s, his perspective remained disconnected from Jordan's approach before the turn of the 20th century.

[3] In 1846, Liouville had insisted on the distinction between Galois's imaginaries and the solvability of equations when he pointed out that the representation afforded by primitive roots did not imply any result on the solvability of higher congruences by radicals.[Galois, 1846, p.401]

[4] In this paper, the term "substitution group" designates a permutation group on a finite number of letters.

[5] See annex 2 for some examples. This recourse to "known rational functions" was not original with Galois in 1830. Lagrange had developed the notion of "similar" functions as early as 1770 (Cf.[Waerden, 1985, p.81]). Two functions f and g of the roots of a given equation are called similar, if all substitutions leaving f invariant also leave g invariant. It then follows that g is a rational function of f and of the coefficients of the initial equation.

letters a, b, c, ... [...] such that every function of the roots, invariant under the substitutions of the group, is rationally known."[Galois, 1831b, p.421] The known rational functions can be retrospectively understood as forming a field. But the substitutions were acting on indeterminate letters or on arrangements of letters, not directly on the field. In the case of an equation of prime power degree, the p^n roots could be indexed by number-theoretic imaginaries. These in turn could be substantiated via cyclotomy, thus providing an analytic representation for the substitutions involved.[6][Galois, 1830b, p.405] In sum, the finite fields underlying such indexations were considered both as additive and multiplicative abelian groups but without direct relation to the fields defined by rational functions of the roots.[7]

Only a few references to Galois can be found in Jordan's Livre II on substitutions, and none at all in its opening chapter "On substitutions in general," which may today be described as group theory. The main allusion to Galois occurs in the section on the "Analytic representation of substitutions" (chap. II, § I), precisely in connection with the *Traité*'s first use of number-theoretic imaginaries for the indexing mentioned above. This resumption is crucial as it leads to the "origin of the linear group" (chap. II, § II), i.e., to central objects of Jordan's treatise.[8] Indeed, underlying the indexing of p^n letters was one type of substitution (a cycle) appearing in two analytic forms: $(k\ k+1)$ and $(k\ gk)$. The "linear form" $(k\ ak+b)$ originated from the composition of these two forms.[9]

As we shall see, some specific procedures of decompositions of the analytic representation of n-ary substitutions would be one of the main specificities of Jordan's presentation of Galois's number-theoretic imaginaries in the long run.

1 Problems, questions and methods

In this section, I shall introduce the problems I am tackling in this paper as well as the methods I am appealing to.

1.1 Algebra and the collective dimensions of mathematics

Dealing with the history of a discipline, a theory, or a theorem immediately raises the issue of the selection of a relevant corpus of texts. Moreover, this issue poses the more general problem

[6]See annex 1 for some numerical examples.

[7]Because this paper will especially consider finite fields $GF(p^n)$, which are separable extensions (and even Galois extensions) on F_p, I will not deal with the retrospective linear algebraic standpoint of Artin's Galois theory: most of the texts under consideration were not resorting to the notions of vector space, normality, separability, field extension, or even to a clear separation between groups and finite fields. Moreover, Galois's theory of general equations was related to the formally different values of functions on n variables (or roots of general equations), it can therefore be applied to special equations with no multiple roots. For this reason, the equations considered in this paper will be supposed to have distinct roots.

[8]The groups considered are $GL_m(p^n)$ along with its subgroups $SL_m(p^n)$, $PSL_m(p^n)$, $SP_{2n}(p)$, $PSP_{2n}(p)$, $O_n(p^n)$, etc. Cf.[Dickson, 1901] as well as[Dieudonné, 1962].

[9]Following Galois and Jordan, in this paper the term "linear" substitutions/groups designate both linear and affine substitutions/groups. See[Galois, 1831b, p. 430-432],[Jordan, 1870, p.91].

of the categories that are used for articulating the individual and the collective dimensions of mathematics.

Let us exemplify this situation with one of the most well-known episode in the history of Galois fields. In a lecture he gave at the 1893 Chicago congress, E.H. Moore has often been considered to have introduced the "abstract notion of Galois field." Yet, most commentaries on Moore's lecture have not only celebrated the creation of a new abstract notion but also the starting point of the "Chicago research school in algebra." Moreover, Moore's lecture has often been considered as exemplifying the influence on the development of the American mathematical community of an abstract approach that was characteristic of "German mathematics"[Parshall, 2004, p.264]. But we shall see that in 1893 Moore stated that every finite field is the "abstract form" of a Galois field $GF(p^n)$ with no direct relation to the result that every finite field can be represented as a Galois extension of F_p, and therefore with little relation with the notion of "Körper" as it was developped in Germany. On the contrary, Moore's lecture resulted in the circulation in Chicago of a specific approach developped in France over the course of the 19th century.

The above example highlights how a label, such as the one of "abstract Galois field," implicitly points both to some collective organizations of mathematics and to some collectives of mathematicians. Moreover, this situation also suggests a tension in the evolution of mathematical knowledge, i.e., between individual creations, from which abstract notions are supposed to originate, and some collective dimensions, such as local social spaces (research schools) or more global institutional or national frames. Such tensions appear frequently in the historiography of algebra. The global evolutions of algebra from 1830 to 1930 have been analyzed as the transformation of a discipline focused on equations to one investigating abstractly defined mathematical entities. Small-scale historical investigations have often focused on the origins of abstract entities as the creations of some individuals (e.g., groups, fields, algebras, rings). Larger-scale diffusions of these abstract notions have been studied through some genealogies of individuals (e.g., Galois, Jordan, Dedekind, Frobenius, Steinitz, Noether, Artin), as well as through some specific national or more local frameworks (e.g., set theoretical methods in Germany, or Hilbert's axiomatic approach in Göttingen). As a result, categories that mix collective organizations of mathematics and collectives of mathematicians have often been used to analyze the historical evolutions of algebra, e.g., the "German abstract algebra," the "Chicago algebraic research school," the "French school of real analysis," etc. To be sure, these categories illuminate some important aspects of the evolutions of mathematical knowledge. Yet, they also raise some difficult issues.

First, both the categories of "nations" and "disciplines" were in the making in the time-period we would like to analyze. "Algebra," "fields," "equations," or "Germany," have had changing meanings in various times and spaces. Until the 1930s, "algebra" was not usually referring to an object-oriented discipline, i.e., as identifying both a corpus of specialized knowledge revolving around some specific objects and the institutionalized practices of transmissions of a group of professional specialists (i.e. the "algebraists").[Brechenmacher et Ehrhardt, 2010] In France, for instance, algebra was, on the one hand, traditionally considered in the teaching of mathematics as

an "elementary," or "intermediary," discipline encompassed by "the higher point of view" of analysis. On the other hand, algebra was also pointing to some procedures that made a "common link" between researches in the various branches of the mathematical sciences.[Brechenmacher, 2012a] What was explicitly identified as "algebraic" therefore often pointed to some implicit circulations between various theories. Therefore, appealing to the category "algebra" for thus a corpus of texts implicitely sheds a retrospective light on the evolutions we would like to analyze, which may bring both social and conceptual anachronisms, and therefore some inadequate collective dimensions.

Second, both disciplines and nations are actors categories. They were much involved in public discourses *on* mathematics. Yet, these discourses did not correspond directly to any actual collective dimensions *of* mathematics. Quite often, they involved some boundary work that reflected the roles taken on by some authorities in embodying some collective models of mathematical lives.[Brechenmacher, 2012b] These boundaries were not only setting delimitations between mathematicians and non mathematicians but were also supporting some hierarchies among the practitioners of mathematics (researchers vs teachers and engineers, analysts vs algebraists, etc.). Disciplines and nations played a key role in setting such boundaries (e.g., "German algebra" vs. "French analysis"). They were intrisically interlaced with some epistemic values ("abstract" vs "concrete", "pure" vs "applied", "modern" vs "classical" etc.).

For instance, in 1890, Émile Picard's academic obituary of Georges Halphen was structured on the opposition between two different orientations in the mathematical thought ("la pensée mathématique") :

> The ones aim above all at extending the domain of knowledge. Without always caring much about the difficulties they leave behind them, they do not fear to move forward, they always look for new fields of investigations. The others prefer to stay in a domain of already developed notions, which they seek to deepen further; they want to exhaust all consequences and they try to highlight the true grounds of the solution of each question. These two directions in the mathematical thought can be seen in all the branches of this Science [...] the first one can nevertheless be found more often in connection with integral calculus and functions theory, and the second one in connection to modern algebra and analytic geometry. Halphen's works were mostly related to the second orientation; this profound mathematician was above all an algebraist.[Picard, 1890, p.489]

To be sure, it was a mixed blessing to be qualified by Picard as an "algebraist." Again, in his 1922 obituary of Jordan, Picard highlighted the former's "tendency to develop a very general approach to mathematical questions as if he feared that some particularity may impeach him to see the true reasons of things." Thus, Picard concluded, "Jordan has really been a great algebraist; the fundamental notions he introduced in analysis will save his name from oblivion."[Picard, 1922]

At the turn of the 20th century, Picard was far from being isolated in attributing more value to analysis than to algebra *per se*. Recall that, in France, the mathematical sciences were mainly

divided between analysis, geometry and applications. Algebra and arithmetics were therefore included in analysis. At the turn of the century, several authorities such as Jules Tannery, Picard, and Henri Poincaré, contrasted the "richness" of the power of unification of analysis with the "poverty" of considering algebra and/or arithmetic as autonomous disciplines. Picard was one of the main advocate of such an opposition, which often aimed at blaming some approaches developed in Germany.

Yet, the collective dimensions that were put to the fore in such public discourses were rarely coherent with the mathematical works of the authors of the discourses. For instance, Picard celebrated publicly Jordan's presentation of the algebraic dimensions of Galois theory. Yet, in his own mathematical work, Picard was not appealing to Jordan's approach but to the one of the German Leopold Kronecker.

Moreover, these discourses were circulating in various medias and were far from drawing a homogeneous picture. For instance, in 1898 Louis Couturat published a paper in the *Revue de métaphysique et de morale* which opposed both the process of "arithmetization" of mathematics and the one of autonomization of algebra to the unified perspective provided by the "science of order" in the tradition of René Descartes, Louis Poinsot, and Galois.[Couturat, 1898] Yet, in Robert Adhémard's 1922 obituary of Jordan, the science of order was presented in a very similar way as German algebra in other discourses, but with a direct reference to the war with Germany :

> In 1860, Jordan was already devoting himself to the Algebra of order, i.e., an Algebra of ideas which is much higher than the Algebra of computations. He naturally followed Galois's works. [...] Whenever Jordan manipulates a mathematical being, it is with the austere hold of his powerful claw. Wherever [Jordan] passes, the trench is cleared.[Adhémard, 1922]

In the reviews they published in various journals, some actors who did not have prominent positions in key mathematical centers expressed publicly their appreciations of the collective developments of mathematics. These discourses were sometimes in direct opposition with the ones of the academic authorities of mathematics. Their views can be quite refreshing in regard with the themes and heroes the historiography of algebra has often put to the fore. Let us consider two examples. First, in a paper which aimed at expressing the importance of the notion of group, the American Georges A. Miller blamed David Hilbert's "Grundlagen der Geometrie" for avoiding the modern methods in group theory "even where it would simplify the treatment of the subject in hand."[Miller, 1903, p.89] Second, let consider the review the French Léon Autonne wrote on Jean-Armand de Séguier's works on group theory. One would recognize in this review a quite canonical statement about the origin of a conceptual approach to algebra, and its slow diffusion ... if only the name of Séguier was replaced by the one of Richard Dedekind :

> M. abbott de Séguier is one of the most eminent among contemporary algebraists. If his works are not as famous as they deserve to be, it is because they deal with such a deep and difficult order of idea - i.e., the most abstract and general group theory

> - that only a very few people, even among mathematicians, are able to follow the author.[Autonne, 1913]

In 1904, de Séguier had published a treatise entitled *Élements de la théorie des groupes abstraits* ("Elements of Abstract group theory"). That such a book was published in Paris at a time-period for which the historiography has often opposed the German abstract algebra to the French analyzis highlights the limits of both national and disciplinary categories. Moreover, de Séguier was not an exceptional isolated individual in France. His works were recognized by other mathematicians, not only in France, but also in the U.S.A. Séguier's books on group theory were indeed systematically listed in Miller's reports to the A.M.S. on the recent progresses in group theory, in company with some other Frenchmen's works, such as Edmond Maillet's and Raymond Levavasseur's.

1.2 Networks of texts as a method of investigation

Taking into consideration historical sources such as Séguier's works thus necessitates to go beyond the structurations of the collective dimensions of mathematics that are provided by nations, institutions and disciplines. As has been seen above, the evolutions of categories such as "algebra" during the time-period under consideration, especially raise difficulties in the very first step of the historical investigation, which is the selection of a corpus of text.

This situation makes it compulsory to study carefully the ways texts were referring one to another, thereby constituting some networks of texts. Yet, such networks cannot be simply identified as webs of quotations.[Goldstein, 1999] Not only do practices of quotations vary in times and spaces but intertextual relations may also be implicit. My approach to this problem consists in choosing a point of reference from which a first corpus is built by following systematically the explicit traces of intertextual relations. A close readings of the texts involved then gives access to some more implicit forms of intertextual references.[Brechenmacher, 2012c] Among these, I shall especially discuss in this paper the references to the "analytic representation of substitutions." The signification of such a reference may seem quite straightforward at first sight. Which may be the reason why the analytic representation of substitutions has actually remained unnoticed in the historiography. Yet, as shall be seen in this paper this reference designated a specific collective dimension of mathematics that played a key role in the development of Galois fields. Because they provide a *heuristic for the construction of a corpus*, and thus a *discipline for reading texts*, intertextual investigations permit to identify the collective dimensions of mathematics which are shaped by circulations of knowledge and practices.

To be sure, such networks of texts should nevertheless not be considered as constellations in an empty sky. First, each author usually belonged to several networks, which pointed to various topics, times and spaces. Second, in laying the emphasis on *textual* interrelations, my investigations therefore do not aim at discussing the main collective dimensions in which the *actors* were involved. Yet, that a group of text presents and objective intertextual coherence raises issues. What did the texts of such a group share ? What was circulating in such a network ?

1.3 The Galois fields network

In the framework of a collective research project,[10] a database of intertextual references has been worked out for all the texts published on algebra in France from 1870 to 1914.[11] Investigations of intertextual connections have then aimed at decomposing the global corpus into subgroups of texts. One of these subgroups gives rise to a coherent network, which was mostly active during a single ten-year period, from 1893 to 1907, and which involved mainly French and American authors.

This group initially involved actors in Chicago (e.g., Moore, Dickson, Ida May Schottenfels, Joseph H. Wedderburn, William Bussey, Robert Börger) and in Paris (Jordan, Émile Borel and Jules Drach, Le Vavasseur, de Séguier, Potron, Autonne) but quickly extended to actors in Stanford (Miller, William A. Manning, Hans Blichfeldt), and to other individuals such as William. L. Putnam, Edward V. Huntington, or Lewis Neikirk.

One of the main mathematical issue that was shared in this collection of texts was the one of "Galois fields," "champs de Galois," or "imaginaires de Galois." For this reason, I shall designate this collection as the *Galois fields network*. Yet, this designation should not be understood as pointing to a specific mathematical theory or discipline. There was no homogeneous way of considering such a theory for all the authors of the network. In this paper, I shall thus pose the identity of the Galois fields network as a problem.

This network is coherent in the sense that its texts refer not only frequently to each other but also to a core of shared references. Let us thus characterize further the Galois fields network by looking at its main shared references.

These were, on the one hand, some retrospective references to some papers published in France in the 1860s, mostly by Charles Hermite, Joseph-Alfred Serret, Émile Mathieu, and Jordan, as well as to Galois's works in the early 1830s. These references were not exclusive of others, such as those to more recent works of Georg Frobenius, Alfred Loewy, or Felix Klein, whose influence in the U.S.A has been well documented.[Parshall et Rowe, 1994, p.147-455] But none of these played as important a role for the collective identity of the network as the works of the 1860s. Moreover, this core of shared references played a key role in establishing links between texts. For instance, the issues tackled in a paper published by Moore in 1895, and entitled "Concerning Jordan's linear groups," were quickly discussed in France. Another paper, published by the French Le Vavasseur in 1896, "Sur les symboles imaginaires de Galois," immediately raised a controversy with the American Miller in the Academy of Paris.

On the other hand, the main shared references contemporary to the authors of the network were Moore's 1893 paper on Galois fields, Dickson's 1901 monograph on linear groups, and Séguier's 1904 monograph on abstract groups.

The Galois fields network thus revolved around a two-fold periodization : its authors were

[10] CaaFÉ : Circulations of algebraic and arithmetic practices and knowledge (1870-1945) : France, Europe, U.S.A ; http://caafe.math.cnrs.fr

[11] The corpus has been selected by using the classification of the *Jahrbuch*. On Thamous database of intertextual references, see http://thamous.univ-rennes1.fr/presentation.php

active from 1893 to 1907 and shared a core of references from the 1860s. We shall see that the two times and spaces involved here point to a *shared algebraic culture* that can neither be identified to a discipline nor to any simple national or institutional dimension. These two times ans spaces were mainly articulated by two treaties : Serret's 1866 *Cours d'algèbre supérieure* and Jordan's 1870 *Traité*.

1.4 The structure of the present paper

The methodology of the present investigation consists in starting with a micro-historical analysis of a local episode, which was one of the main shared reference in the Galois field corpus, i.e., the works of Moore and Dickson in Chicago from 1893 to 1896. We shall provide a detailed analysis of this episode with a careful attention to the algebraic procedures involved. This small-scale analysis highlights the key role played by some specific procedures that were interlaced to a specific notation : the analytic representation of substitutions.

In the third and fourth sections of this paper, we shall change the scale of analysis in investigating the long run circulation of these procedures in the 19th century, especially in the works of Galois and Jordan.

Finally, in the fifth section of this paper, we get back to Chicago in 1893 for the purpose of identifying the shared algebraic culture lying beneath the Galois fields network, which can be characterized as a specific approach to both linear groups and Galois fields, but with no interest in Galois Theory.

2 Linear groups in Galois fields from 1893 to 1907

Given the time-period during which the Galois fields network developped, it is quite natural to attempt to characterize the collective dimensions of this network as regard to the context of the institutionalization of finite group theory at the turn of the 20th century. Moreover, given the important proportion of American mathematicians involved, one may aim at inscribing the Galois fields network in the context of the development of the American mathematical research community. Yet, we shall see in this section that even though appealing to a discipline such as group theory, or to a nation such as the U.S.A., sheds light on some aspects of the Galois field network, neither the categories of discipline nor of nation succeed in characterizing the specificity of this network.

2.1 The problematic collective dimensions of the Galois fields network

2.1.1 Disciplines : finite groups

The institutionalization of finite group theory is an important collective trend in which the Galois fields network participated. Reports were produced ([Miller, 1898], [Miller, 1902], [Miller, 1907], [Dickson, 1899]), monographs were published ([Burnside, 1897b], [Dickson, 1901], [Séguier, 1904b],

[Le Vavasseur, 1904]), and discussions were developed on issues related to the teaching and the history of finite groups.

The network originated between Otto Hölder's abstract formulation of the notion of quotient group[Hölder, 1889] and the emergence of group representation theory. The determination of all groups of a given order was often proclaimed as a general goal. This question had already been presented as the "general problem" of substitutions in the third edition of Serret's *Cours*[Serret, 1866, p.283]. The texts of the network either pointed to Serret or to the "abstract" formulation Arthur Cayley had given to the "general problem of groups" in the first volume of the *American Journal of Mathematics*.[Cayley, 1878, p.50] The use of the composition series of the Jordan-Hölder theorem potentially reduced the general problem to the one of the determination of all simple groups. The identification of classes of simple groups therefore raised difficult issues related to the various concrete forms of representations of abstract groups such as substitutions groups or collineation groups.[Silvestri, 1979]

The latter problem was much related to the development of abstract group theory (i.e. groups defined by symbolic, and later axiomatic, operations). First, the use of the Jordan-Hölder theorem required the consideration of quotient groups that were not introduced by substitutions but by symbolic laws of operations.[Nicholson, 1993, p.81-85] Second, Hölder's use of Sylow's theorems for determining simple groups of order less than 200,[Hölder, 1892] or groups of orders p^3, pq^2, pqr, p^4,[Hölder, 1893] was based on the identification of abstract groups up to isomorphism.[12]

2.1.2 Disciplines : abstract group

Hölder's approach to abstract groups was a shared reference in the Galois fields network. In his paper of 1889, Hölder initially appealed to the abstract approach developed by Walther von Dyck[Dyck, 1882] in the legacy of Cayley. A symbolic approach was nevertheless developed earlier in 1877-1878 by Frobenius, partly in the legacy of Cayley as well.[Hawkins, 2008] After Hölder eventually appealed to Frobenius's approach in 1892, the two mathematicians would publish a series of papers on topics closely related one to the other (Sylow theorem, composition series, solvable groups etc.). But unlike Hölder's, Frobenius's works did not become a shared reference in the Galois fields network until 1901.

The variety of attitudes to Frobenius shows that the category of "abstract finite group theory" is not appropriate for identifying the collective dimensions of the Galois fields network.[13]

[12] In the mid-1860s, the use of Jordan's "method of reduction" of groups into composition series had raised representation issues.[Jordan, 1867a, p.108] The notion of isomorphism had been appropriated by Jordan from the framework of cristallography and had been presented as a general notion of the theory of substitutions.[Jordan, 1870, p.56] It would play a key role in the connections Klein would develop between various types of groups in the late 1870s and would become "abundant" in the 1890s.[Frobenius, 1895, p.168] First, Hölder's introduction of abstract quotient groups would point to the isomorphism theorems.[Frobenius, 1895] Second, the actual composition of groups from factor-groups could not be undertaken unless all the automorphisms of the groups involved would be known.[Hölder, 1893, p.313][Hölder, 1895, p.340]

[13] For instance, Moore did not refer to Frobenius in the 1890s even though[Burnside, 1896] pointed out that[Frobenius, 1893] had already made use of the notion of the group of automorphisms of a group

Moreover, that issues related to abstract groups circulated in the Galois fields network did not imply a shared approach toward abstraction. Unlike Moore, other key authors followed Frobenius's works closely. But, on the one hand, Burnside's 1897 *Theory of groups of finite order* indicated the longstanding concerns for symbolic laws of combination which had circulated from Cambridge to other academic contexts in Great Britain and the United States. On the other hand, it was on Georg Cantor's set theory that Séguier had grounded his 1904 monograph on abstract groups.

2.1.3 Nations

National categories were no more relevant than theories for identifying the Galois fields network. For instance, the works of the Americans Frank N. Cole and John W. Young were frequently referred to by Frobenius. Reciprocally, Miller appealed to Frobenius's works early on in the mid-1890s. In his first *Report on recent progress in the theory of the groups of finite order*, he put to the fore Frobenius's representation theory when he acknowledged the growing importance of linear groups.[Miller, 1898, p.248] But Dickson nevertheless mentioned Frobenius neither in his 1899 *Report on the recent progress in the theory of linear groups*, nor in his monograph. The situation did not change until 1901, when a review of Alfred Loewy criticized Dickson's restatement of some of Frobenius's results.

2.2 Moore's Galois fields

We have seen that large-scale categories, such as nations and disciplines, fail to characterize the collective dimensions of the Galois fields networks. Let us now change our scale of investigation. In this section, we shall focus on a micro-historical analysis of one the main shared references of the network, i.e., Moore's works on Galois fields from 1893 to 1896.

2.2.1 Research schools

In their work of reference on the development of the American mathematical community, Karen Parshall and David Rowe have analyzed in detail the institutional background of Moore's paper in the context of the emergence of the "Chicago research school." [Parshall et Rowe, 1994, p.261-455] They have especially highlighted the strong influence of Félix Klein's Göttingen. But even though the roles played by German universities in the training of many American mathematicians have been well documented, the influence of this institutional framework on mathematics has been assumed quite implicitly. The Chicago research school has indeed been characterized by its "abstract and structural" approach to algebra, which was called a "characteristic of trendsetting German mathematics."[Parshall, 2004, p.264] Here two difficulties arise.

that[Moore, 1894] had claimed to introduce. Several authors actually claimed independently to have abstractly identified the group of automorphisms of abelian groups of type $(1, 1, ..., 1)$ (i.e., Frobenius, Hölder, Moore, Burnside, Le Vavasseur, and Miller), a problem that pointed to the traditional introduction of the general linear group in the legacies of Galois and Jordan as will be seen in greater details later.

First, the role attributed to "abstract algebra" reflects the tacit assumption that the communication of some local knowledge should require direct contact. Because the historiography of algebra has usually emphasized the abstract and structural approaches developed in Germany, and especially in the center of Göttingen, other, more local, abstract approaches, such as in Cambridge or Chicago, have raised issues about the imperfect communication of some tacit knowledge, as exemplified by the late interbreeding in the 1930s of the German *Moderne Algebra* and the Anglo-American approach to associative algebras.[Fenster et Schwermer, 2005] In this framework, algebraic developments in France, such as Séguier's, have been either ignored or considered as some isolated attempts modeled on German or Anglo-American approaches.[Dubreil, 1982]

Second, as has already been highlighted in the previous section of this paper, both disciplines and nations are actors categories which were much involved in public discourses. Recall that Moore's 1893 paper was read at the congress that followed the World Columbian exposition in Chicago.[Parshall et Rowe, 1994, p. 296-330] The world fair was dedicated to the discovery of America and was the occasion of much display of national grandeur.[Brian et al., 1893] In parallel to the elevation of the first great wheel, presented by the Americans as a challenge to the Eiffel tower, or to the viking ship that sailed from Norway as a counterpoint to the replica of Columbus's three caravels, the architectural influence of the French École des Beaux arts was challenged by the German folk village. The latter especially included an exhibit of the German universities with a section on mathematics at Göttingen.

In regard with mathematics, Klein had been comissioned by the Prussian government to the fair. He had contributed "a brief sketch of the growth of mathematics in the German universities in the course of the present century" to the book *Die deutschen Universitäten*, which had been edited for the exhibit of the German universities.[Lexis, 1893] Moreover, during the fair, Klein delivered a series of lectures which aimed at "pass[ing] in review some of the principal phases of the most recent development of mathematical thought in Germany."[Klein, 1894] Klein was also the glorious guest of the congress while Moore was both the host of the congress and one of its main organizers.

2.2.2 Paying tribute to Klein...

As we shall in this section, Moore's lecture - the concluding lecture of the Chicago congress - was clearly aimed at both paying tribute to Klein's *Icosahedron* and to some recent works developped in the U.S.A.

On the one hand, Moore generalized to a "new doubly infinite system of simple groups," i.e., $PSl_2(p^n)$, what was then designated as the three "Galois groups" (i.e., $PSl_2(p), p = 5, 7, 11$) involved in the modular equations that had been especially investigated by Klein, following Galois, Hermite, and Kronecker among others.[Goldstein, 2011] The generalization consisted in having the analytic form of unimodular binary linear fractional substitutions (i.e. $PSl_2(p)$), with $ad - bc \equiv 1\ mod.p$

$$k' = \frac{ak + b}{ck + d}$$

operate on p^n letters indexed by Galois number theoretic imaginaries, instead of the usual case of a prime number p of letters $F_p = Z/pZ$.

On the other hand, the issues Moore tackled were those associated with the continuation of the lists of simple groups that had been established by the American Cole up to the order 500,[Cole, 1892][14] following Hölder's list up to order 200.[Hölder, 1892] For the purpose of continuing the list up to 600, Cole had put to the fore a simple group of order 504 (i.e. $PSl_2(2^3)$). Moore showed that Cole's group - as well as a simple group of order 360 he had introduced in 1892 - belonged to his "new doubly infinite" system of simple groups.

The extension of the system of indices from p elements to p^n elements was based on the introduction of the notion of a "field" as a "system of symbols" defined by "abstract operational identities" of addition and multiplication :

> Suppose that the s marks may be combined by the four fundamental operations of algebra [...]. Such a system of s marks we call a field of order s. The most familiar instance of such a field [...] is the system of p incongruous classes (modulo p) of rational integral numbers.
> Galois discovered an important generalization of the preceding field [...] the system of p^n incongruous classes (modulo p, $F_n(x)$).[15].[Moore, 1893]

2.2.3 ... but colliding to the implicit collective dimension lying beneath the use of Galois imaginaries

At first sight, the mathematical issues tackled by Moore in 1893 may seem very coherent with the institutional influence of Germany on the development of the American mathematical community.

Yet, the nature of the relevant collective dimensions changes if one shifts the scale of analysis from institutions to texts. Even though he aimed at celebrating the emergence of some abstract researches in the U.S.A. in the framework of the Göttingen tradition, Moore actually collided to the implicit collective dimension that was underlying the use of analytic representations of substitutions, such as $\frac{ak+b}{ck+d}$, on Galois number theoretic imaginaries.

This situation is illustrated by the fact that,in the context of the development of the Chicago research school, Moore's Galois fields would be collectively described as having given an "abstract," or "general," form to some previous works by Serret, Jordan, and Mathieu :

> The linear groups investigated by Galois, Jordan and Serret were defined for the field of integers taken modulo p ; the general Galois field entered only incidentally in their investigation. The linear fractional group on a general Galois Field was partially investigated by Mathieu, and exhaustively by Moore [...].[Dickson, 1901, p.1]

Moreover, a similar abstract formulation was not only often attributed to Borel and Drach's 1895 textbook but Moore's results on $PSl_2(p^n)$ were also traced back to Jordan's 1870 treatise :

[14]Except fot the orders 360 and 432 which Frobenius dealt with in 1893.

[15]In modern parlance, this sentence is identifying a Galois field as the finite field of incongruous classes of polynomials F modulo p and modulo a given irreducible integral polynomial F_n of degree n

> The expression Galois Field is perhaps not yet in general use. The notion is due To Galois and is fully developed by Serret [1866]. The theory in its abstract form is developed by Moore [1893 and 1896], and by Borel et Drach [1895]. Jordan [1870] and Moore [1898], have shown that the quaternary linear homogeneous substitution group of order 8!/2 in the Galois Field, and the alternating group of degree eight, both of which are simple, are holoedrically isomorphic.[Schottenfels, 1899]

2.3 What's new in Moore's paper ?

Let us now address the issue of the nature of Moore's individual contribution. What was actually new in the 1893 congress paper ?

It is obviously not possible to attribute to Moore the origin of the notion of Galois field as this notion had already been introduced by Galois (as well as by Carl Gauss and Poinsot before Galois, as will be seen later), and developped by several other authors such as Serret, Mathieu, Jordan, etc. One may thus be tempted to attribute to Moore a more "abstract" definition of the notion of Galois field, one that would fit the axiomatic approach developped in Göttingen and thereby herald the postulationist program that would develop at the beginning of the 20th century in Chicago. As a matter of fact, we have seen above that Moore was celebrated by his followers in Chicago for his truly abstract and general presentation of Galois fields. Yet, such an interpretation is contradicted by a closer look at the chronology of Moore's publications.

2.3.1 The shadow of Klein-Fricke's textbook on Moore's incomplete references

A first version of Moore's lecture was published in 1893. There, Moore had noted that : "it should be remarked further that every field of order s is in fact abstractly considered as a Galois field of order s."[Moore, 1893, p.75] But he neither provided any proof nor any further details about this remark until the second version he completed in autumn 1895 for the publication of the proceedings of the congress.[Moore, 1896, p.242] Yet, in the meantime, several other mathematicians provided an abstract definition of Galois field : Burnside dealt in 1894 with exactly the same issue of the simplicity of $PSL_2(p^n)$ and Drach gave in 1895 an abstract definition to "Galois imaginaries."[Borel et Drach, 1895, p.343-349] Moreover, Heinrich Weber and Hilbert claimed in 1893-1895 to lay new ground on Galois's theory of equations by appealing to Dedekind's concept of "Körper."[Weber, 1893][Weber, 1896][Hilbert, 1894][16]

The focus of the first version of Moore's paper was on the proof of the simplicity of $PSl_2(p^n)$ on the model of the case of $PSl_2(p)$ treated in[Klein et Fricke, 1890, p. 419-450]. Alongside with[Hölder, 1889], the textbook of Klein and Fricke was actually the main bibliographic reference of Moore's paper. Not only had Cole authored the references to the simple groups investigated by Jordan,[Moore, 1893, p.74][17] but most other references had been taken from the

[16] See[Kiernan, 1971, p.137-141] and[Corry, 1996, p.34-45]

[17] In a modern notation, Moore's paper referred to Jordan's investigations of $Alt(n)$, $PSl(n,p)$, and $P\Omega^{\epsilon}(n,p)$

Klein-Fricke textbook.[18] It is likely that Moore had not read[Gierster, 1881] closely, and had not read[Serret, 1859], and [Serret, 1865] at all. Moore even suggested that both mathematicians dealt only with the case $n = 1$, while in fact they used Galois imaginaries in some parts of their works.[Moore, 1893, p.76]

Moreover, even though the relevant works of[Mathieu, 1860, p.38], and [Mathieu, 1861b, p.261] on linear fractional substitutions and number-theoretic imaginaries were identified precisely by[Gierster, 1881, p.330], Moore did not mention Mathieu until 1895 when he would add a last-minute note to the revised version of his paper.[Moore, 1896, p.242] Mathieu had nevertheless investigated various aspects of $PSL_2(p^n)$, and had already introduced Cole's group of order 504 (with no concern about the issue of simplicity).[19]

2.3.2 Every Galois field is a Galois field

Had Moore built his 1893 lecture on the four pages Klein and Fricke had devoted to Galois imaginaries ? Actually, his use of the expression Galois theory indicates that Moore had certainly read Jordan's *Livre I*. Moreover, the formulation he gave of Galois fields pointed to the extensive development of Serret's 1866 *Cours*. Indeed, both[Klein et Fricke, 1890] and[Jordan, 1870] were faithful to Galois's original presentation in focusing on the fact that $GF(p^n)$ is isomorphic to $F_p(j)$, with j a root of $x^{p^{n-1}} \equiv 0$. In contrast, Serret had developed an arithmetic approach to $GF(p^n)$ as $F_p(X)/(f(x))$. Galois's (or Jordan's or Klein's and Fricke's) presentation was the one that was actually helpful for the group-theoretical purpose of Moore's paper. But Moore turned Galois upside down.

On the one hand, what he designated as a Galois field was actually Augustin Cauchy's approach to higher congruences,[Boucard, 2011b] as developed later by Serret's concrete function field representation, and which Moore nevertheless attributed to Galois.

On the other hand, Moore's notion of abstract field was close to Galois's initial presentation. The statement that a finite field can be abstractly considered as a Galois field actually echoed the connection between two perspectives on number theoretic imaginaries, as it had already been displayed in textbooks such as Serret's in 1866.[Serret, 1866, p.179-181] It was quite close to stating that every Galois field (in the sense of Galois) is the abstract form of a Galois field (in the sense of Cauchy or Serret) :

> The Galois field $GF[q^n]$ is uniquely defined for every q=prime, n=positive integer ; that is : $F_n(X)$ -which are irreducible (mod. q)- do exist ;
> The $GF[q^n]$ is independent of the particular irreducible $F_n(X)$ used in its construction. For the details of this Galois theory, see Galois : *Sur la théorie des nombres (Bulletin des Sciences mathématiques de M. Férussac*, vol. 13, p. 428, 1830

[18] Moore had indeed reproduced the references made to[Serret, 1866] and[Jordan, 1870] by[Klein et Fricke, 1890, p. 419] as well as the references to[Serret, 1859],[Serret, 1865] and[Gierster, 1881] in[Klein et Fricke, 1890, p. 411].

[19] In 1861, Mathieu had used the threefold transitive group $PSl_2(p^n)$ for introducing a five fold transitive group on 12 letters. He had also anounced the existence of a five fold transitive group on 24 letters which he would eventually introduce in 1873 (i.e. the Mathieu groups M_{12} and M_{24}).

; reprinted, *Journal de Mathématiques pures et appliquées*, vol. 11, pp. 398-407, 1846) ; Serret, *Algèbre supérieure*, fifth edition, vol. 2, pp. 122-189 ; and Jordan : *Substitutions*, pp. 14-18.[Moore, 1893]

In Moore's approach, the relation of abstract fields to number-theoretic imaginaries was analogous to the relation between classes of abstract simple groups and the representation of a given simple group. On the one hand, because irreducible polynomials mod p "do exist," as Moore claimed, Serret's approach provided a construction of a field of p^n elements,[Moore, 1893, p.75] i.e., "an existence proof" of the abstract field.[Moore, 1896, p.212] On the other hand, the notion of abstract field was a normal interpretation of Galois's 1830 *Note* in the context of the considerations on the symbolic laws of complex numbers and associative algebras that had been developed since the 1870s.[20]. Klein-Fricke had indeed considered Galois imaginaries as complex numbers $aj^{n-1} + bj^{n-2} + ... + 1$. Commutative systems of hypercomplex numbers were typically investigated by the consideration of the minimal polynomial of the system. In the case of finite fields, the minimal polynomial was of the form $x^{p^{n-1}} - 1 \equiv 0$ as Moore would prove in 1896.

In short, Moore had stated that finite abstract fields can be represented as function fields. In contrast, this statement had no relation with Galois fields in the sense of field extensions and Galois groups.[21] In the framework of Weber's presentation of Dedekind's Galois theory, Moore's "Galois fields" were both "endlicher Körper" and "Congruenz Körper" but they were not "Galois'sche Körper."

2.3.3 Lost in a fog of old French works

Recall that the introduction of abstract Galois fields was not the initial aim of the 1893 lecture. But as a result, Moore nevertheless established a direct relation between[Serret, 1866] and[Klein et Fricke, 1890]. In doing so, he had jumped over more than twenty years of development of mathematics. Yet, unlike Burnside who mastered the relevant references to the works of Serret, Jordan, and Mathieu, Moore seems to have been lost in a fog of old French works.

But even more dramatically, Moore's system of simple groups had actually already been introduced by Mathieu in 1861. What Mathieu had done exactly on Galois fields was especially problematic to Moore. The 1893 version of the congress lecture was supposed to be followed by a more complete publication in *Mathematische Annalen*. But this did not happen and Moore published instead a paper on triple systems. When Moore referred to Mathieu for the first time, he promised he would devote a subsequent paper to point[ing] out the exact point of contact [of his works] with Mathieu's results."[Moore, 1895, p.38] But no such paper was ever published and

[20] In the tradition of investigations on associative algebras,[Borel et Drach, 1895, p.343-350] and[Moore, 1895] both provided tables of compositions of number-theoretic imaginaries. On the history of associative algebras, see[Hawkins, 1972, p.244-256] and[Parshall, 1985, p.226-261]

[21] As any finite field of p^n elements can be represented as the splitting field of $P(X) = X^{p^n} - X$ on F_p, every finite field can be represented as a Galois field. But such a splitting field was not considered as a Galois extension on F_p: Moore had no concern for the interplay between groups and fields which is characteristic of Galois theory

Moore eventually settled for the addition of a short allusive note to the revised edition of the congress paper.

As a result, before the publication of the proceedings of the congress in 1896, Moore and his student Dickson struggled to access the tacit collective dimension of some texts published in France in the 1860s, especially by appealing to Jordan's 1870 *Traité*. As will be seen in greater details later, the main problem of Dickson's thesis was actually to specify the relations between the works of Jordan and Mathieu on linear groups in Galois fields. [22]

Moore's 1893 paper thus eventually resulted in the circulation of some works that were foreign to Klein's legacy as is illustrated by the publication from 1893 to 1896 of a train of papers on "Jordan's linear groups in Galois fields." Not only was Dickson's doctoral thesis devoted to the investigation of the collective dimensions Moore's Galois fields had accidentally bumped into in 1893. But, more generally, many of the early works of the Chicago research school were systematic generalizations of some statements of Jordan's *Traité*.

In sum, Moore's works on Galois field from 1893 to 1896 can be analyzed as a process of appropriation of a specific collective framework associated to the use of analytic representations of substitutions on Galois imaginaries. This situation highlights the difficult problem of identifying the scales at which various forms of collective dimensions play a relevant role in the evolutions of mathematics, especially in respect to the articulation of the collective dimensions of texts with the ones of actors, such as disciplines or nations.

3 Galois number-theoretical imaginaries in the long run

Let us now investigate the collective dimension Moore accidently collided to in 1893. We shall thus change once again our scale of analysis by looking more closely into some texts that have been published in the long-term. This section is thus based on a retrospective approach of the 19th century from the standpoint of the Galois fields network at the turn of the 20th century.

3.1 On the variety of the forms of representations of substitutions in the 19th century

We have seen that Galois fields were intrinsically interlaced in Moore's works with the use of a specific form of representation of substitutions : the analytic representation. We shall thus start our present investigations with an overview of the variety of forms of representations of substitutions that have been used during the 19th century :

[22] One of the main results of Dickson's thesis was to generalize Moore's doubly-infinite system of simple groups to the triply-infinite system $Sl_m(p^n)/Z$ with Z the center of $Sl_m(p^n)$ and (m, n, p) different from $(2, 1, 2)$ or $(2, 1, 3)$.

- Two-lines representations (a turns into d ; b turns into c etc.) :

$$(a, b, c, d, e, ...)$$
$$(d, c, a, e, b, ...)$$

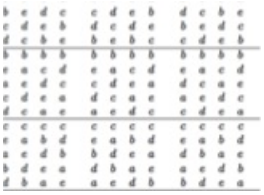
- Products of transpositions :

$$(ad)(de)(eb)(bc)(ca)$$

- Symbolic notations of the operations between substitutions :

$$ghg^{-1} = k$$

- Tabular representations of groups and subgroups of substitutions:



- Analytic representations, which consist in indexing the letters by a sequence of integers in order to represent the substitutions on these letters by polynomials.

The latter form of representation has remained unnoticed in most historiographical accounts on group theory. Yet, we shall see that the analytic representation has played a key role in both the development of the notions of Galois fields and linear groups.

This situation can be analyzed as a part of a large scale phenomenon, i.e., the crucial role played by polynomial representations of functions in the long run of the 18th and 19th centuries (with extensons to infinite sums or products). It is well known that such a conception of functions has been challenged in the 19th century, especially in connection to the issues raised by representations by Fourier series from which Cantor's set theory would emerge in the 1870s. Yet, analytical representations continued to play an important role even after the introduction of a more general notion of functions as applications, as is exemplified by Henri Poincaré's efforts in the 1880s to provide an analytical representation of fuchsian fuchsions by infinite sums or products.

Karl Weierstrass's factorization theorem is another example of the lasting influence of analytic representations. The theorem illustrates that such representations are not limited to a form of notation : the cannot be dissociated from some specific algebraic procedures modeled on the factorization of polynomial expressions. As a matter of fact, Weierstrass's theorem states that any analytical function - i.e. the sum of a power series - can be expressed as an infinite product which factors contains the zeros of the function considered. The factorization theorem also

highlitghts the limitations of analytic representations. It was indeed in attempting to generalize Weierstrass's theorem to infinite products of rational expressions that Gösta Mittag-Leffler was drawned to Cantor's set theory. In the case of functions with singular points, one can provide some global analytical representations only in some specific cases while, in general, one has to consider a function as an application between two sets of points. As Cantor wrote to Mittag-Leffler in 1882 : "In your approach, as well as in the path that Weierstrass is following in his lecture, you cannot access to any general concept because you are dependent of analytical representations." (cited in[Turner, 2012])

3.2 The analytic representation of substitutions

Given a substitution S operating on p letters a_k (p prime), the problem of the analytic representation is to find an analytic function f such that $S(a_k) = a_{f(k)}$. As shall be seen in greater details later, an influential approach to this problem (especially for Dickson's 1896 thesis) was the one of Hermite. In 1863, Hermite provided a complete characterization of the analytic representations of substitutions for the cases $p = 5$ and $p = 7$. For instance, any substitution on 5 letters can be represented by combinations of the following polynomial forms :

$$k\ ; k^2\ ; k^3 + ak$$

Hermite also stated a general criterion for substitutions to have an analytic form. His approach was based on the use of Joseph-Louis Lagrange's interpolation formula. Given two functions ϕ and ψ of degree p associated to two substitutions S and T on p letters, the substitution ST is then associated with the function $\phi\psi$. Now, in order to keep the degree of $\phi\psi$ equal to p, it is necessary to consider both the indices of the p letters and the coefficients of ϕ and ψ modulo p. The problem of the analytic representation is thus tightly linked to the one of the indexation of the letters on which the substitutions are acting. In case of substitutions acting on p^n letters, one has to consider Galois's number-theoretic imaginaries.

3.3 The special case of cycles : two indexations, two analytic representations

In the special case when the number of letters is is a prime number p, an indexation can be given by representing the p letters as the p^{th} roots of unity, i.e., as the roots of the binomial equation :

$$X^p - 1 = 0$$

As a matter of fact, all the roots of this equation can be expressed by the sequence (0, 1, ..., $p - 1$) of the powers of a single root, ω (i.e. a "primtive root" of the binomial equation) :

$$\omega^0, \omega^1, \omega^2, ..., \omega^{p-1}$$

In the above indexation, the root ω^k turns into ω^{k+1}, by adding 1 to the exponent k. This operation is associated to the substitution $(k\ k+1)$, which provides the analytic representation of a cycle by the affine function $f(k) = k+1$ (or, more generally, $f(k) = k+a$).

But let now consider the list of all the roots of unity less the unity itself, that is the roots of the irreducible cyclotomic equation (on $\mathbb{Q}$) deduced from the binomial equation :

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + ... + x + 1$$

This sequence of $p-1$ roots can be reindexed in the following way :

$$\omega^g, \omega^{g^2}, ..., \omega^{g^{p-1}}$$

by appealing to a primitive root g of the binomial *congruence* :

$$X^{p-1} - 1 \equiv 0\ mod(p)$$

Such a reindexation provides an alternative analytic representation of a cycle by the form $(k\ gk)$, i.e., the linear function $f(k) = gk$.

To sum it up, cycles can be represented analytically in the two following ways :

- an operation of addition $(k\ k+a)$
- an operation of multiplication $(k\ gk)$

This double representation is crucial. It allows to simultaneously decompose the set of roots of unity into subsets and to factorize binomial equations. As shall be seen in the next section, this procedure of decomposition plays a key role in Gauss's famous proof that cyclotomic equations can be solved by radicals.

3.4 Cyclotomy

Unlike Alexandre Théophile Vandermonde (1774) and Lagrange's (1771) approaches to the special cases $x^5 - 1 = 0$ and $x^{11} - 1 = 0$, Gauss's 1801 *Disquitiones arithmeticae* had introduced a general method of successive factorizations for proving the solvability by radicals of (irreducible) cyclotomic equations of degree $p-1$. The factorizations resorted to organizations of the roots in a specific order by appealing to the two indexings provided by a p^{th} primitive root of unity ω and by a primitive root g mod. p.[23] For any factorization $p - 1 = ef$, let $h = g^e$, and consider the equation of degree e whose roots correspond to the following e "periods" of sums of f terms :

$$\eta_i = \omega^i + \omega^{ih} + ... + \omega^{ih^{f-1}} (1 \leq i \leq e)$$

[23] On Gauss's proof of the existence of primitive roots of cyclotomic equations, see[Neumann, 2007].

Such decompositions of the roots into periods allows factorizing the initial (imprimitive) cyclotomic equation into e factors of degree f. A numerical example for $p = 19$ is provided in Annex 1.

A few years later, in 1808, Lagrange gave a new proof of the solvability of cyclotomic equations. The successive auxiliary equations attached to Gauss's periods were replaced by the direct consideration of an auxiliary function of the coefficients and of roots of unity, i.e., the Lagrangian resolvent

$$\omega + \alpha\omega^g + \alpha^2\omega^{g^2} + ... + \alpha^{p-1}\omega^{g^{p-2}}$$

(with α a primitive $p-1^{th}$ root of unity.[24]

3.5 Poinsot's groups

In his 1808 review of Lagrange's treatise, Louis Poinsot commented on the two approaches of Gauss and Lagrange. At this occasion, he had designated Gauss's periods as "groups" in a sense Galois would also use later on. Groups in this sense involved both partitions of "permutations of letters" (i.e. arrangements of the roots or indexing lists) and decompositions of "systems of substitutions" (the operations from one permutation to another).[25]

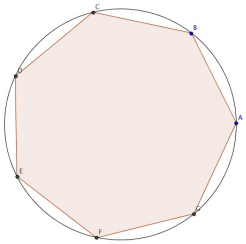
As seen before, Gauss's decomposition resorted to a single kind of substitution (i.e. cycles). But two forms of actions had to be distinguished depending on whether the cycles were acting within the groups or between the groups. Poinsot had discussed these two forms of actions from a geometric perspective. The roots generated by a primitive root of unity could be represented "as if they were in a circle"[Boucard, 2011a, p.62] (a numerical example is provided for the case $p = 7$ in annex 1).

- On the one hand, the operation (k gk) decomposes the set of roots into various subset, or blocks, that can be moved one on the other by rotations of the circle. For instance, in the circle below, one can distinguish the blocks B, C, E) et (D, F, G) : one passes from one block to the other by the multiplication of a primitive root g mod. p that turns B, C, E into D, F, G.

- On the other hand, the roots can be made to move forward by translations, i.e., by the operation (k $xk1$) on their indices, which for instance turns B into C, C into E, E into B etc.

[24] The Lagrangian resolvent line of development of Galois theory has been well documented. See[Kiernan, 1971, p.103-110].

[25] The ambivalence of the terminology "group" as regard to the distinction between the "permutations of the roots" and the "substitutions" has often been considered as a limitation of Galois's approach (e.g.[Dahan Dalmedico, 1980, p.282],[Radloff, 2002]). But it should be pointed out that this ambivalence was the very nature of "groups" as they originated from the decomposition of imprimitive groups by the consideration of blocks of imprimitivity of letters.



Gauss's procedure of indexation thus established a connection between arithmetics (congruences), algebra (factorization of equations), geometry (circular representation), and mechanics (translations and rotations on/of a circle).

In 1815, Cauchy introduced cycles by appealing to a similar circular representation [Cauchy, 1815, p.75-81] even though he did not focus on the analytic representations induced by the two forms of actions of cycles $(k\ k+1)$ and $(k\ gk)$. Cauchy indeed rather had favored other modes of representations of substitutions such as products of cycles,[Dahan Dalmedico, 1980, p.286-295] the two lines notation, the symbolic notation, and some tabular representations.[26] On the contrary, the analytic representation of substitutions played a key role role in Galois's approach as shall be seen in the next section.



[Cauchy, 1815]

3.6 Galois's criterion for irreducible equations of prime degree

We have seen that the analytic representation of substitutions is far from being limited to a specific notation. This representation cannot be dissociated from some specific procedures of decompositions. In this section, we shall highlight the role played by these procedures in the concluding theorem of Galois's famed *Mémoire*.

Recall that Galois's *Mémoire* is organized into two parts : the first provides a general presentation while the second is devoted to the application to a special class of equations.

- The first part is famous for its proposition V, which presents the problem of the solvability by radicals as resorting to the interplay between successive adjunctions of roots and the successive decompositions of a group caused by the successive adjunctions of roots to the equation.[27]

- The second part of the memoir follows proposition V. It is concluded by a criterion of solvability to irreductible equations of a prime degree :

[26] Cauchy also introduced a terminology that has been used throughout the 19th century, that of "arithmetic substitutions" for $(k\ k+a)$ and of "geometric substitutions"$(k\ gk)$.

[27] For some systematic comments on the general principles of Galois's *Mémoire*, see[Radloff, 2002] and [[Ehrhardt, 2012].

Theorem 1 ***Galois's criterion***

In order that an equation of prime degree be solvable by radicals, it is necessary and sufficient that, if two of its roots are known, the others can be expressed rationally.[Galois, 1831b, p.432]

This theorem provides an extension to the class of solvable equations that were already known before Galois, i.e., Gauss's binomial equations (all the roots are the successive powers of one of them) and Niels Henrik Abel's equations (all the roots are rational functions of one of them).

The analytic representation of substitutions plays a key role in both the statement and the proof of Galois's criterion. An alternative statement of the theorem is indeed the following :[28]

> An irreducible equation of prime degree is solvable by radicals *if* and *only if* any function invariable by the substitutions
>
> $$x_k, x_{ak+b}$$
>
> is rationnaly known[Galois, 1832, p.431]

The key argument of the proof is that the smallest non-trivial group in the successive reductions had to be generated by a cycle. Here, Galois explicitly referred to Cauchy even though he did not appeal to the latter's representation of substitutions as products of cycles but to analytic representations. Galois looked for the penultimate group in the successive reductions of the given equation. He showed that if its substitutions are represented by $(x_k,\ x_{f(k)})$, then f$(k+c) = f(k) + C$, i.e., these substitutions turn cycles $k+c$ into cycles $f(k)+C$.[29] Thus :

$$f(k+2c) = f(k) + 2C, ..., f(k+mc) = f(k) + mC$$

Let now consider that $c = 1$ and $k = 0$; let $b = f(0)$:

$$f(m) = Am + b$$

Let now $a = A$, Galois eventually deduced that:

$$f(k) = ak + b$$

Galois has designated such substitutions as "linear substitutions."[30]

As will be seen in greater detail later, the core argument of Galois's proof would circulate throughout the 19th century. The introduction of the general linear group in Jordan's *Traité* would especially "originate" from the exact same argument. In modern parlance Galois's theorem and its proofs boil down to showing that the linear group is the maximal group in which an

[28] In modern parlance, Galois's theorem states than an irreducible equation of degree p is solvable by radicals if and only if its Galois group is a subgroup of the affine group.

[29] This group is the maximal group in which the cyclic group $(k\ k+a)$ is a normal subgroup.

[30] In modern parlance, these are affine substitutions.

elementary abelian group (the cyclic group F_p^* in the case $n = 1$ or a direct product of cyclic groups in general) is a normal subgroup.

As we shall see in the next section, it was in attempting to generalize this theorem to the analytic forms of roots of equations of degree p^n that Galois introduced the number theoretic imaginaries.

> Considérons l'un quelconque des groupes semblables au groupe (G). D'après le théorème II, il devra s'obtenir en opérant partout dans ce groupe une même substitution; par exemple, en mettant partout dans le groupe (G), à la place de x_k, $x_{f(k)}$, f étant une certaine fonction.
>
> Les substitutions de ces nouveaux groupes devant être les mêmes que celles du groupe (G), on devra avoir
>
> $$f(k + c) = f(k) + C,$$
>
> C étant indépendant de k.
>
> Donc
>
> $$f(k + 2c) = f(k) + 2C,$$
> $$\cdots\cdots\cdots\cdots$$
> $$f(k + mc) = f(k) + mC.$$
>
> Si $c = 1$, $k = 0$, on trouvera
>
> $$f(m) = am + b,$$
>
> ou bien
>
> $$f(k) = ak + b,$$
>
> a et b étant des constantes.
>
> [Galois, 1846]

3.7 Galois's attempts to generalize his criterion to equations of degree p^n

It is well known that the *Mémoire* has remained unpublished until Joseph Liouville edited a selection of Galois's works in his journal in 1846. Yet, the criterion had already been stated in Galois's very first note on the issue of the solvability by radicals, "Analyse d'un mémoire sur la résolution algébrique des équations," which was published in the *Bulletin de Férussac* in 1830 (the *Analyse* for short).

In this paper, Galois was already looking for a more general statement for equations of compound degree. The note indeed started with the introduction of the distinction between primitive and imprimitive equations : a "non-primitive equation of degree mn is an equation that can be decomposed into m factors of degree n, by appealing to a single equation of degree m."[Galois, 1830a, p.395] These equations were also designated as Gauss's equations. In his "Fragment of second memoir",[31] Galois indeed appealed to "M. Gauss's method of decomposition" for reducing the problem of finding solvable irreducible equations of composite degree to the one of finding solvable primitive equations of degree p^n.[Galois, 1831a, p. 434]

[31]Recall that even though the second memoir remained unpublished until 1846, its redation is nevertheless anterior than the final version of the first memoir which two first versions have been lost after having been submitted to the Académie.

The aim of the second memoir was to generalize Galois's criterion to solvable primitive equations by the general characteristic that their degree had to be a power of a prime. Such a generalization raised the issue of the indexation of systems of p^n letters.

Galois first solved this problem in decomposing the letters into n blocs of p letters. He considered a primitive equation of degree N that turned into Q imprimitive equations by the adjunction of a radical of prime degree. The group of the equation was then partitioned into conjugated imprimitive groups. Let H be one of these imprimitive groups; its letters were decomposed on the model of Gauss's method of indexation into a table of p columns whose rows correspond to systems of imprimitivity :

$$\begin{array}{ccccc} a_0 & a_1 & a_2 & ... & a_{p-1} \\ b_0 & b_1 & b_2 & ... & b_{p-1} \\ c_0 & c_1 & c_2 & ... & c_{p-1} \\ .. & .. & .. & .. & .. \end{array}$$

Galois then argued that $N = p^n$. More importantly, the above allowed the introduction of n series of p indices for the indexing of the letters, and thereby to give an analytic representation to substitutions on p^n letters into n series of p indices :

> The general form of the letters will be
>
> $$\begin{array}{ccccc} {}^{a}k, & k, & k, & ... & k, \\ 1 & 2 & 3 & ... & \mu \end{array}$$
>
> with $\begin{array}{ccccc} k, & k, & k, & .... & k, \\ 1 & 2 & 3 & ... & \mu \end{array}$ some indices that can take the p values $0, 1, 2, 3, ..., p-1$.[Galois, 1831a, p.426]

Substitutions on p^n letters could then be represented by fonctions $\phi, \psi, \chi, ...\sigma$ of the indices :[32]

> [...] in the group H, all the substitutions have the form
>
> $$\left[\begin{array}{ccccccccccc} {}^{a}k, & k, & k, & ... & k, & {}^{a}\phi(k), & \psi(k), & \chi(k), & ... & \sigma(k), \\ 1 & 2 & 3 & ... & \mu & 1 & 2 & 3 & ... & \mu \end{array}\right]$$

Galois then investigated further the case of primitive equations of degree p^2. A cycle, or a

[32] In modern parlance, the indices form a finite field of p^n elements, which is introduced as a vector space of dimention n over the field $\mathbb{Z}/p\mathbb{Z}$.

"circular substitution" as he said following Cauchy, would have the following form:

$$\begin{bmatrix} {}^{a}k, & k', & {}^{a}k+\alpha, & k'+\alpha' \\ 1 & 2 & 11 & 22 \end{bmatrix}$$

But then, Galois argued, because the substitutions of the group have to transform cycles into cycles, they must have a "linear form" :[Galois, 1831a, p.439]

$$\begin{bmatrix} {}^{a}k, & k', & {}^{a}mk+n, & mk'+n \\ 1 & 2 & 11 & 22 \end{bmatrix}$$

Galois then successively computed the number of linear substitutions on p^2 letters and looked for solvable "divisors" (i.e. subgroups) of the group by investigating substitutions of the following form:

$$\frac{ak+b}{ck+d}\ (ad-bc\neq 0)$$

In the *Analyse*, Galois had already made it clear that the groups of orders p or $p+1$ formed by the above substitutions were related to the modular equations of elliptic functions. We shall get back to this issue later.

3.8 Galois's number theoretic imaginaries

The problem of the analytic representation of substitutions on p^n letters is also related to the introduction of number theoretic imaginaries in a note Galois published in 1830 in the *Bulletin de Férussac*.[33] The aim of the Note was actually to show that any system of p^n indices could be reindexed "in analogy with" the indexing of p letters $0, 1, 2, ..., p-1$ by the roots $1, g, g^2, ..., g^{p-1}$ of Gauss's congruence $x^p \equiv x(mod.p)$, i.e., by the iterated powers of a primitive root j of $x^{p^n} \equiv x(mod.p)$.[34] We have seen before that in the case of a prime number p, such reindexations allow to pass from one form of representation of cycles, $(k\ k+1)$, to the other $(k\ gk)$, and thus play a key role in Galois's criterion. As a matter of fact, Galois presented his note on number theoretic imaginaries as a "lemma"' for the investigation of primitive substitutions on p^n letters.[Galois, 1832, p.410]

Let

$$f(x) \equiv 0\ mod(p)$$

be an irreducible higher congruence of degree n. As was common at the time, Galois legitimized the introduction of imaginary roots j by appealing to the analogy carried on by the process (of factorization) used for the case of ordinary equations.[35] He expressed the rational functions of

[33]Before Galois, higher congruences had been considered in the "missing section eight" of Gauss's *Disquitiones Arithmeticae*,[Frei, 2007] as well as by Poinsot[Boucard, 2011a].

[34]In modern parlance, a Galois field $GF(p^n)$ is both an additive group, which can be represented as an n-dimensional vector space on F_p, and a multiplicative cyclic group of p^{n-1} elements.

[35]On these issues, see[Durand-Richard, 1996],[Durand-Richard, 2008]

the roots as "general expressions"

$$a^{j^{n-1}} + b^{j^{n-2}} + ... + 1$$

(with a, b, ... mod. p) and first proved that these p^n "algebraic quantities" could be considered as the roots of

$$x^{p^n} \equiv x \ mod(p)$$

Reciprocally, he argued that the roots of the latter equation "all depend on one congruence of degree n."[Galois, 1830b, p.399-402]

The conclusion of the Note was devoted to the characterization of solvable primitive equations of degree p^n[Galois, 1830b, p.405]. The roots x_k of such an equation could now be indexed by the solutions of the congruence

$$k^{p^n} \equiv k(mod.p)$$

Galois then claimed that if any function of the roots invariable by the substitutions of the form

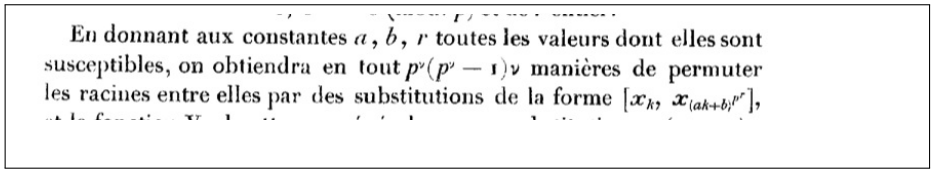
$$(k \ (ak+b)^{p^r})$$

has a rational value, then the equation is solvable, and reciprocally. The proof was presented as a direct consequence of the decomposition of linear substitutions into a product of the two forms of cycles, i.e., in the form $a'(k+b')^{p^r}$: "those who are accustomed to the theory of equations will have no trouble seeing this."[Galois, 1830b, p.406]

As has been seen above, the proof Galois alluded to in the *Note* was given in the *Mémoire* for the case $n = 1$ by appealing to the decomposition of the analytic representation of substitutions. This statement was generalized in 1832 to the substitutions of primitive solvable equations of degree p^n, which Galois claimed, have the linear form :[Galois, 1832, p.410]

$$x_{k,l,m,...}, \ x_{ak+bl+cm+...+h,a'k+b'k+c'm+...+h',a''k+...},$$

Yet, Jordan would contradict this claim in the 1860s in proving that Galois's statement is a necessary condition but not a sufficient one : in the case of p^n letters, it is compulsary to decompose further the analytic representation of linear substitutions.


En donnant aux constantes a, b, r toutes les valeurs dont elles sont susceptibles, on obtiendra en tout $p^{\nu}(p^{\nu}-1)\nu$ manières de permuter les racines entre elles par des substitutions de la forme $[x_k, x_{(ak+b)^{p^r}}]$,

> On remarque que, dans ces circonstances, l'équation $fx = 0$ sera soluble par radicaux, et, pour parvenir à cette conséquence, il suffit d'observer que la valeur substituée à k, dans chaque indice, peut se mettre sous les trois formes
>
> $$(ak + b)^{p^r} = [a(k + b^1)]^{p^r} = a^1 k^{p^r} + b'' = a'(k + b')^{p^r}.$$
>
> Les personnes habituées à la théorie des équations le verront sans peine.
>
> [Galois, 1830b, p.406]

3.9 Generalities and applications

As said before, the introduction of Galois's *Mémoire* had laid the emphasis on a distinction between the "general principles" of a theory and its three "applications" to special classes of equations.[Galois, 1831b, p.417] These application were discussed in more details in the famous letter Galois wrote to Auguste Chevalier in 1832. During the 20th century, most commentators have focused on Galois's general principles. In this section, I would like to highlight the crucial role played by the three analytic representations involved in Galois's applications :

- The linear form in one variable
$$(k\ ak + b)$$
associated to the criterion for solvable equations of prime degree
- The general linear form in n variables
$$(k,\ l,\ m...\ ;\ ak + bl + cm + ..,\ a'k + b'l + c'm + ...,\ a''k + b''l + c''m + ...)$$
associated to the investigation of solvable equations of composite degree
- binary fractional linear substitutions
$$\frac{ak + b}{ck + d}\ (ad - bc \neq 0)$$
associated to the modular equations of the transformations of elliptic functions

The three applications were intrinsically interlaced with one another in the evolution of Galois's investigations. They were not limited to applications but played also the role of special model cases for the general principles of the *Mémoire*. Each application modeled a special form of decomposition of a group.

First, as Galois would make it clear in his letter to Chevalier, the "simplest decompositions are the ones of M. Gauss" by which the investigation of solvable transitive equations of composite degree was reduced to the one of solvable primitive equations of prime power degree. But, wondered Galois, "what are the decompositions that can be practiced on an equation that Gauss's

method would not simplify ?"[Galois, 1832, p.409] As has been seen above, the decomposition of primitive equations of p^n or p degrees was modeled on the decomposition of linear substitutions into the two forms of representation of cycles. Recall that there was no clear concept of factor group yet. In the reduction of $(ak + b)$ into two cyclic substitutions, the two analytic forms $(k\ k+1)$ and $(k\ gk)$ provided a model for the operations involved in composition series. It was on this model that Galois stated that the substitutions of primitive solvable equations of degree p^n had to have the linear form $x_{k,l,m,\ldots}$, $x_{ak+bl+cm+\ldots+h,a'k+b'k+c'm+\ldots+h',a''k+\ldots,}$.

The "proper decomposition" had been modeled on the traditional use of auxiliary equations $x^p = a$ in issues of solvability by radicals (and therefore of the binomial equation $x^n - 1 = 0$). This situation may be illustrated by propositions II and III of the *Mémoire*. The first described the proper decomposition of a group relative to the adjunction of a root to an equation. The second stated that if "one adjoins to an equation all the roots of an auxiliary equation, the groups of theorem II would have the additional property of possessing the same substitutions."[Galois, 1846, p.423-425] But this proposition had been previously stated differently. Its original formulation was that if one considers all the $p - th$ roots of unity to have been adjoined to an equation, then the same decomposition of the original group would originate from the adjunction of any of the root of $x^p = a$. In that case, the adjunction of a root would imply the adjunction of all roots, i.e., the situation to which the proposition III had been generalized afterward.

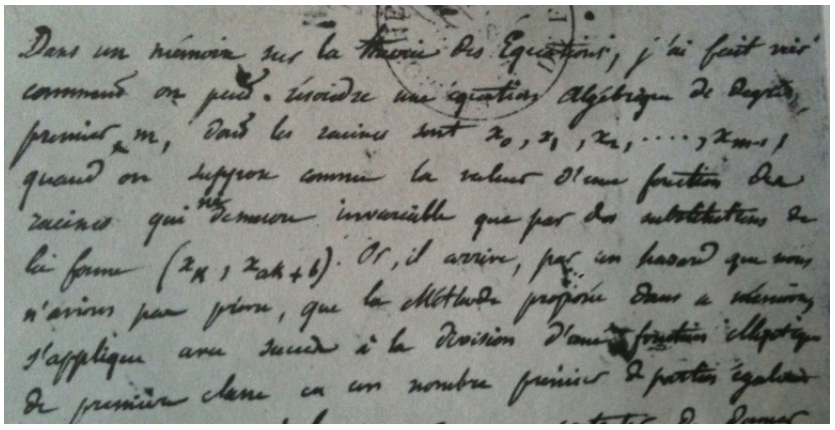
Moreover, the issue of the reduction of the degree of the modular equations gave an example of improper decomposition, i.e., of non-normal subgroups of a group.[Galois, 1832, p.408] According to Galois, the difference between improper and proper decompositions was the difference between adjoining one root or all the roots of an auxiliary equation to an equation. Galois's auxiliary equations could involve non-solvable equations on the model of the reduced modular equations. In 1832 Galois indeed claimed he had not focused all his attention on solvability by radicals but had also investigated "all possible transformation on an equation, whether it is solvable by radicals or not."[Galois, 1832, p.408]

The general quartic, and quintic had also played the role of model cases for Galois's investigations. [Galois, 1846, p.428, 433] But it must be pointed out that all the "applications" were pointing to the legacy of Gauss, while general equations were related to the legacy of Lagrange. The two legacies of Gauss and Lagrange did not play the same role in the *Mémoire*. In short, and on the one hand, three forms of decompositions had been modeled on Gauss's equations. On the other hand, Lagrange's legacy was related to the consideration of the number of values of rational functions of the roots under the action of substitutions, a problem that would become one of the main lines of development of the theory of substitutions. We shall get back in more details to this issue in discussing Jordan's 1860 thesis.

In a word, we have seen that Galois's general principles of decompositions of groups had been modeled on the decomposition of the three analytic forms of representations associated to Galois's three applications. Moreover, this model-role played by the polynomial decomposition was not limited to the investigations on equations. A same analytic representation can indeed

be used for expressing various objects in different branches of mathematics, such as analysis, algebra, or arithmetics. Such representations, and their associated operatory procedures can thus support some analogies between various issues. In the first page of his "Mémoire sur les fonctions elliptiques," Galois appealed to the permanence of a same analytic form for transfering his works on equations to investigations on complex functions :

> In a memoir on the theory of equations I have shown how one can solve an algebraic equation of prime degree m whose roots are x_0, x_1, x_2, ..., x_{m-1}, when one suppose known that the value of a function of the roots that remains invariable by substitutions of the form $(x_k,\ x_{ak+b})$. But it happens, by a chance I did not expect, that the Method I proposed in my memoir can be successfully applied to the division of an elliptic function of the first class into a prime number of equal parts.[Galois, 1962]



3.10 The analytic representation of substitutions and the various forms of receptions of Galois's works

This section aims at providing a brief overview of the different lines of developments of Galois's works in the 19th century.

The analytic representation of substitutions had circulated with both Galois's applications and general principles. Even at the turn of the 20th century, in a textbook such as Weber's *Lehrbuch der Algebra* - which as often been celebrated for the novelty of its presentation -, the two analytic forms of cycles still played a key role in the conclusion of the presentation of Galois theory.[Weber, 1896, p.637]

Yet, apart from Enrico Betti's and Jordan's systematic comments on Galois's works, the three applications were not usually presented together in the framework of a comprehensive theory. The three analytic representations associated to these applications thus provide some indications on the different lines of development in which Galois's applications were involved.

Actually, in contrast with works such as Cauchy's 1844-46 papers on substitutions,[Cauchy, 1844] [Cauchy, 1845] the focus on the decomposition of analytic representations was specific to the

works which referred to Galois. Let us illustrate this situation by alluding briefly to the works of Betti and Hermite.[36]

In 1852, Betti had begun his commentary on Galois with representing substitutions $(x_k\ x_{\phi(k)})$ by a bijective function ϕ (with the indices k either integer mod. p. or Galois imaginaries). As has been seen before, finding all the possible expressions of such functions was later identified as the problem of the analytic representation of substitutions. Betti had nevertheless not given any specific expression to ϕ until he had discussed Galois's notion of decomposition of a group. Following Galois in 1830 and preceding Jordan in 1860, Betti had then raised the issue of determining the "maximal multiplier of a group," i.e., the last step of a decomposition.[Betti, 1852, p.45] For the case of a prime number of letters, this group was generated by cycles of form $(x_k\ x_{k+1})$ or $(x_k\ x_{gk})$, while the composition of both forms generated the linear form $(x_k\ x_{ak+b})$. As in Galois's criterion, Betti's analytic representations were thus interlaced with some specific procedures of decomposition of linear substitutions

Hermite's first public reference to Galois in 1851 occured in a paper that succeeded Puiseux's 1850 "Recherches sur les fonctions algébriques." In both the framework of Cauchy's complex analysis and of Hermite's 1844 investigations of the division equation of abelian functions, Puiseux had considered algebraic functions $f(z,w)=0$ on the complex plane.[37] He had shown that in the neighborhood of any point z_0 which is not a branch point, the roots $w_1, w_2, ..., w_n$ can be expended as convergent power series in $z-z_0$. If one makes z move on a closed circuit avoiding the branch points, the roots are permuted by a system of substitutions (i.e. the monodromy group of the equation), which Puiseux had investigated by appealing to Cauchy's representation of cycles.[Puiseux, 1850, p.384] In 1851, Hermite responded to Puiseux by representing analytically the substitutions involved for stating a criterion of the solvability for equations with parameters, analogous to Galois's criterion. Hermite indeed stated that for equations of a prime degree, "the necessary and sufficient condition for the solvability by radicals is that all the functions of the roots invariant for the substitutions of the following special form

$$\begin{pmatrix} u_k \\ u_{ak+b} \end{pmatrix}$$

are rationally known."[Hermite, 1851, p.461] On the model of the proof of Galois's criterion, Hermite's proof was based on the decomposition of the above form into products of

$$\begin{pmatrix} u_k \\ u_{k+1} \end{pmatrix}$$

[36]Unlike Galois's decompositions, Cauchy composed the "conjugated system" of substitutions by the two forms of cycles (i.e. the linear group) but for the sole purpose of computing its order and with no interest in the analytic form of the resulting substitutions.

[37]The polynomial $f(z,w)$ in w is irreducible in the field of rational functions of z.

and

$$\binom{u_k}{u_{gk}}$$

Let us now caracterize the various lines of developments of Galois's three applications

3.10.1 The form $(k\ ak+b)$

> THÉORÈME I. — *Si une équation irréductible* $f(x)=0$, *d'un degré premier* n, *est résoluble par radicaux, ses* n *racines pourront être représentées par* x_z [l'indice z, pris suivant le module n, devant être réduit à l'un des nombres $0, 1, 2, \ldots, (n-1)$], *de telle manière que le système conjugué actuellement propre à l'équation ne renferme que des substitutions linéaires et entières, c'est-à-dire des substitutions de la forme* $\binom{az+b}{z}$, a *et* b *étant des constantes.*

Serret's *Cours d'algèbre supérieure*, 1866

> **Lehrsatz XII. Die allgemeinen auflösbaren Gleichungen vom Primzahlgrade p sind die Galois'schen Gleichungen. Ihre Gruppe hat die Ordnung $p(p-1)$; sie wird aus den Substitutionen der Form**
>
> $$s=\left|z \quad az+\alpha\right|; \quad (\alpha=1,2,\ldots p-1;\ \alpha=0,1,\ldots p-1) \pmod p$$

Netto's 1882 textbook on substitutions

References to Galois's criterion have been one of the principal form of references to Galois's works until the end of the 19th century. This situation is directly the consequence of Liouville's presentation of Galois's achievements in 1846. As a matter of fact, references to the criterion eventually diseappeared when Liouville's Avertissement was replaced by Picard's introduction to the 1897 reprinting of Galois's works.

In the Avertissement to the 1846 edition of Galois's works, Liouville had claimed that Galois had laid the grounds for a "general" theory of the solvability of equations by radicals. It is well known that he did not comment further on the content of such a general theory. But Liouville had nevertheless celebrated "Galois's method" through its "particular" use for the proof of the criterion. Following Liouville, the presentation of the criterion as a particular application of a general theory of equations dominated public discourse on Galois's works until the mid-1890s. Liouville's presentation of Galois was in fact reproduced word for word in publications targeting larger audiences than specialized mathematical journals, e.g., the 1848 biography of Galois in the *Magasin encyclopédique* or the many notices that would be published in several encyclopedic dictionaries.

But the citation of Liouville citing Galois could also be found in Serret's *Cours d'algèbre supérieure*. Despite the fact that the first edition of 1849 had made almost no use of Galois's

works, its introduction presented Galois's criterion as the endpoint of a longue durée history of the "theory of equations" involving Cardano, Lagrange, Ruffini, and Abel among others.[Serret, 1849, p.1-4] . In 1854, Serret's second edition included two additional notes relative to the criterion. The first consisted of a translation of[Kronecker, 1853] involving a discussion on Galois's theorem with regard to Abel's approach. The second was a new proof of the criterion by Hermite.

Serret would include a presentation of Galois's general theory of equations in the third edition of his *Cours* in 1866. The criterion would then be presented as the conclusion of the theory. Apart from Jordan's *Traité* and Klein'ss *Icosahedron*, the solvable prime degree "Galois equations" - or "metacyclic equations" - would conclude most presentations of Galois theory until the turn of the century, e.g.[Netto, 1882, p.278],[Bolza, 1891],[Borel et Drach, 1895, p.334],[Vogt, 1895, p.188],[Weber, 1896, p. 597,648],[Picard, 1896, p.481],[Pierpont, 1900].

3.10.2 The form $(k\ \frac{ak+b}{ck+d})$

> lorsqu'on fait la substitution $\begin{pmatrix} v_k \\ v_{k+1} \end{pmatrix}$; et si l'on vérifie encore qu'il en est de même à l'égard de celle-ci $\begin{pmatrix} v_k \\ v_{-\frac{1}{k}} \end{pmatrix}$, on arrivera à cette conclusion qu'ils demeurent invariables pour toutes les substitutions où l'on met, au lieu de k, $\frac{ak+b}{ck+d}$, $ad-bc$ étant résidu de n. En effet, cette expression, dans toute sa généralité, s'obtient en composant entre elles celles que nous venons de considérer. Le théorème du § XIV suffit donc pour nous
>
> [Hermite, 1859]

Unlike textbooks, papers published in specialized journals rarely referred to the criterion. When Hermite first referred to Galois publicly in 1851, he already expressed his interest in the cases in which the degrees of the modular equations could be reduced, a problem Betti would investigate in 1853. In 1858-1859, Hermite would appeal to Galois's works again at the occasion of the series of papers in which he would use the modular equation to provide an analytic expression of the roots of the general quintic through elliptic functions.[38] The reduction of the degree of modular equations, as Hermite said, "depends on a deeper investigation of the substitutions:"[Hermite, 1859, p.58]

$$\frac{ak+b}{ck+d}$$

Following Hermite, Serret and Mathieu considered linear fractional substitutions with number-theoretic imaginaries as variables in 1859.

From this point on, Galois's third application was usually referred to in connection to the works of "Galois-Betti-Hermite." This became one of the main types of reference to Galois in the second half of the century, both in periodical specialized publications and in treatises such as[Jordan, 1870],[Briot et Bouquet, 1875], [Klein, 1884], and[Klein et Fricke, 1890]. At the turn of the 1870s-1880s, the expression "Galois groups" was used by Klein and his followers for

[38] See[Goldstein, 2011]

designating the groups associated to the three modular equations. Later on, at the Chicago congress of 1893, Joseph Perott still designated the group of order 660 of the modular equation of order 11 as the Galois group, while, as has been seen above, Moore aimed at generalizing the Galois groups by introducing abstract Galois fields.

This situation highlights that the reception of Galois's works has never been limited to the strictly algebraic framework of the theories of equations or substitutions. On the contrary, most early interpretations of Galois's works were connected to issues in complex analysis (monodromy) and number theory (arithmetical properties of elliptic functions). In this context, Galois's works have been especially connected to the investigation of the types of "irrational" quantities defined by classes of algebraic equations, which are non solvable by radicals. Recall that Abel's proof of the impossibility to solve the general quintic by radicals had not been considered by most authors as the conclusion of a long history, one that should give rise to the new algebraic perspectives of Galois theory. On the contrary, several mathematicians generalized the traditional problem of the expression of the roots of the general equations of degree 2, 3, or 4 to the one of finding the simplest functions that express the roots of higher degree equations. The works of Betti, Hermite, Kronecker, and Francesco Brioschi on the general quintic are representative on this situation, as well as Klein's later approach on the icosahedron. Moreover, even Jordan's *Traité*, which as often been celebrated as the starting point of an autonomous theory of groups, actually presented Galois's general principles in a section entitled "On the irrationals," which developped applications to arithmetics, analysis, and geometry.[39]

3.10.3 The general linear form in n variables

On trouvera ci-jointe [*] la démonstration des théorèmes suivants :

1°. Pour qu'une équation primitive soit soluble par radicaux, elle doit être du degré p^ν, p étant premier.

2°. Toutes les permutations d'une pareille équation sont de la forme

$$x_{k,l,m\ldots}\,|\,x_{ak+bl+cm+\ldots+h,\ a'k+b'l+c'm+\ldots+h',\ a''k+\ldots,\ \ldots},$$

k, l, m,... étant ν indices, qui, prenant chacun p valeurs, indiquent toutes les racines. Les indices sont pris suivant le module p; c'est-à-dire

Galois's letter to Auguste Chevalier

Galois's treatment of primitive equation of degree p^n had had few echoes until the mid-1860s. In 1852, Betti had followed Galois in extending his investigations to groups of prime power order and therefore to n-ary linear substitutions. In 1856, Alexandre Allégret had published two notes with the aim of generalizing Galois's criterion to equations of composite degree. Referring to the works of Kronecker, Betti, and Pierre-Laurent Wantzel, he had considered the "group of linear substitutions defined by Galois" in connection to congruences and cyclotomic equations. The interest Allégret had for groups was nevertheless not shared by most of the authors who dealt with substitutions at the time.

[39] On this aspect of Jordan's treatise, see [Brechenmacher, 2011]

In the first note related to Galois that Jordan addressed to the *Comptes rendus* in 1864, the latter reactivated the issue of the determination of solvable equations of prime power degree. His aim was to lay the emphasis on his "method" whose "essence" was to "reduce" a group into a "chain" of subgroups. Jordan indeed argued that the problem had to be reduced further than Galois's two-step decomposition of solvable transitive equations, to primitive equations with linear substitutions. One thus had to devote specific attention to linear substitutions. In the following years, Jordan repeatedly pointed out the incorrectness of Galois's generalization of his criterion to p^n variables.[Galois, 1830b, p.406], i.e., that the condition of linearity was sufficient for characterizing solvable primitive groups :

> Galois claimed that that there is a single type of primitive equations that are solvable by radicals [...]. The statements [I made] above show that one has to make an assertion almost opposite to [Galois's] claim.[Jordan, 1868, p.113]

Most of the second section of Jordan's 1870 *Traité* dealt with the problem of characterization and classification of subgroups of $GL_n(p)$, while most of the huge final fourth section investigated the roles played by general linear groups in the chain reduction of solvable transitive groups.

Yet, the n-variable generality of Jordan's approach on linear groups was not taken on by most later presentations of the theory of substitutions.[Netto, 1882], [Klein, 1884], [Klein et Fricke, 1890], [Bolza, 1891], [Borel et Drach, 1895], [Weber, 1896], [Picard, 1896], [Pierpont, 1900] focused rather on the binary linear and fractional linear substitutions associated with solvable equations of prime degree and with modular equations.

For the purpose of understanding how this approach eventually reappeared in connection to Moore's congress paper in 1893, we shall now look in greater details into Jordan's works in the 1860s.

4 Jordan's general linear group

The focus on general analytic representations in n variables is a strong specificity of Jordan's works. As has been seen above, most of his contemporaries focused on linear forms in one variable ($k\ ak+b$) or linear fractional substitutions ($k\ \frac{ak+b}{ck+d}$). Yet, Jordan had introduced the general linear group before he had started studying Galois's works.[40] As we shall see in this section, Jordan had indeed inscribed his 1860 thesis in the legacy of Poinsot's "theory of order."

4.1 The origin of the linear group

One of the two theses Jordan had defended in 1860 was devoted to the problem of the number of values of functions. This problem is one of the roots of the theory of substitutions. It developped

[40] As a matter of fact, Jordan acknowledged in a footnote of his thesis in 1860 that he had "discovered recently in the works of Galois the statement of the theorem" that he had concluded his thesis with, i.e., the order of $Gl_n(p)$.

from some works in the 18th century that connected the solvability by radicals of an algebraic equation of degree n to the number of values that can be obtained by a resolvent function of n variables (see annex 2 for a few examples). Recall that in the 19th century, substitutions were usually not studied autonomously but rather through the investigation of functions of n variables, such as Lagrange's "fonctions semblables" that are invariant for a substitutions group. These functions not only played a key role in Galois's general principles but also in a variety of other works such as Hermite's theory of quadratic forms or Poincaré's theory of fuchsian functions.

Given a function $\phi(x_1, x_2, ..., x_n)$ of n "letters," a "value" of ϕ was a function obtained by permuting the variables, i.e., for any $\sigma \in Sym(n)$, $\phi(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$ was a value of ϕ.[41] In general, ϕ can take up to $n!$ distinct values. Yet, it may happen that some of these values are identical. Jordan's thesis aimed at identifying the number of values associated to some classes of substitutions groups.

In 1860, the problem of the number of values of functions had been chosen as the topic of the Grand prix des sciences de mathématiques de l'Académie des sciences de Paris. Two young mathematicians devoted their first research work to this problem : Jordan and Mathieu. Both appealed to Cauchy's approach to substitution theory, which had especially highlighted the notion of "conjugate systems," i.e., the equivalent of a substitution group.

The main result of Jordan's thesis was the introduction of a type of "conjugate systems" of n-ary linear substitutions (i.e. $Gl_n(p)$) by a "method of reduction" of a "permutation group." Jordan's notion of "permutation group" amounted to the simultaneous consideration of blocks of imprimitivity and substitutions groups. Unlike Galois, though, Jordan appealed to a precise distinction between permutation groups and conjugate systems of substitutions. In the introduction of his thesis, Jordan had explicitly attributed the notion of group to Poinsot. When the number of values of a function was less than $n!$, he had considered that a "symmetry occurred within the function" as an application of "what Poinsot has distinguished from the rest of mathematics as the theory of order."[Jordan, 1860, p.3] According to Jordan, other examples of applications of this theory were Cauchy's determinants, Abel's works on the general quintic, as well as Galois's works on "the conditions of algebraic solvability, the whole theory of equations considered in its full generality, and the classification of algebraic irrationals." When he first referred to Galois, Jordan thus aimed at stressing the generality of the theory of order as opposed to "most geometers who have considered this question [of the many valued functions] in the aim of applying it to the theory of equations."[42]

[41] This problem is tantamount to finding the possible orders for subgroups of the symmetric group. If ϕ takes only one value, then it is symmetric and can therefore be expressed as a rational function of the elementary symmetric functions. If $x_1, ..., x_n$ are the roots of an equation with coefficients on a given "rational domain", this means that ϕ can be expressed as a rational function on the rational domain. To intermediary cases between 1 and $n!$, normal subgroups of the symmetric group can potentially be associated to ϕ by considering the set of substitutions leaving ϕ invariant. If ϕ takes, for instance, ρ distinct values $\phi_1, \phi_2, ..., \phi_\rho$, these values can be considered as the roots of an equation of degree ρ whose coefficients are the symmetric functions of the initial variables. See also annex 2.

[42] Similar claims about the generality of a broad framework related to both symmetry and groups could be

Some previous works, such as Cauchy's (1815, 1844-1846), Joseph Bertrand's (1845) or Serret's (1849), had aimed at stating some boundaries for the number of values of certain general types of functions[43] while others, such as Hermite's and Kronecker's had focused on some special functions, such as a function of six variables that take exactly six values. Jordan emphasized the specificy of his own work in regard with the ones of his predecessors in claiming to have developped a "general approach" to the problem through its "successive reductions" to "sub-problems." One may recognize in this claim the traditional definition of the "analysis" in mathematics. Yet, Jordan's reductions were not limited to a general heuristic for solving problems. His reductions consisted in decomposing simulaneously the sets of letters into blocks and the substitutions groups into subgroups. Jordan's reductions were thus intrisically interlaced with some specific algebraic procedures of decomposition of analytic representations.

Jordan's thesis was organized on a two-step reduction of the general problem of the number of values of functions. First, a general transitive system of substitutions was reduced to a substitutions group T of p^n letters (i.e. a primitive quotient group). The issue at stake was to index the letters by n sequences of p integers (1, 2, ..., p) in order to represent the substitutions analytically. The letters were thus reorganized into the "imprimitive system," represented below as a succession of lines (that we shall denote as $\Gamma_1, \Gamma_2, ..., \Gamma_m$), and on which the substitutions operated by permuting either the letters in a same line or the lines themselves :

$$\begin{array}{cccc} a_1 & a_2 & ... & a_p \\ b_1 & b_2 & ... & b_p \\ c_1 & c_2 & ... & c_p \\ . & . & . & . \end{array}$$

Second, the substitutions of T were decomposed into "primitive" systems, i.e., into the case in which it is not possible any more to decompose the system of letters into several lines $\Gamma_1, \Gamma_2, ..., \Gamma_m$ as above. Jordan's key argument here was to show that the substitutions operating on imprimitive systems of letters can be decomposed into two "species" of substitutions, which correspond to the two analytic representations of cycles.

- On the one hand, inside each block of imprimitivity Γ_i, the letters were cyclically substituted by first species of substitutions $(x\ x+a)$ on the indices. In the general case of letters indexed by n indices $a_{x,x',x'',...}$ these substitutions take the form :

$$a_{x+\alpha\ mod.p,\ x'+\alpha'\ mod.p,\ x''+\alpha''\ mod.p,\ ...}$$

- On the other hand, the second specie (x, gx) of substitutions substituted cyclically the blocks $\Gamma_1, \Gamma_2, ..., \Gamma_n$ themselves by operating on the indices by the multiplication of a prim-

found in the contemporary writings of Théodore Despeyrous,[Despeyrous, 1861, p.417] another follower of Poinsot. Unlike Jordan, Despeyrous nevertheless never attributed any role to Galois as regards permutation groups.

[43]For instance, at the beginning of the century, Ruffini and Cauchy had stated that the number of values that a non-symmetric rational function of 5 variables attains cannot be lesser than 5 unless it is 2.

itive root g mod. p. In the general case of n indices, these substitutions thus take the form

$$a_{ax+bx'+cx''...mod.p,a'x+b'x'+c'x''...mod.p,a''x+b''x'+c''x''...mod.p}$$

Thus, in exactly the same sense that powers of a primitive root composed each block Γ, the sequence $\Gamma_1, \Gamma_2, ..., \Gamma_m$ of the blocks could itself be considered as the cycle (or the orbit) of powers of Γ_1. Each specie of substitution corresponded to one of the two forms of representation of cycles. Their products generated linear forms $(x\ ax + b)$ with $x \in F_{p^n}$, i.e., if $x = (x, x', x'', ..., x^{(n)})$:

Theorem 2 ***Jordan's first theorem***

- *The number of letters in primitive systems is the power of a prime number p^n.*
- *The analytic representation of the substitutions on these systems is linear :*

  $$(x, x', x''...; ax + bx' + cx'' + ... + d, a'x + b'x' + c'x'' + ... + d', a''x + b''x' + c''x'' + .. + d'', ...)$$

  which can also be noted by :

$$\left|\begin{array}{cc} x & ax + bx' + cx'' + ... + d \\ x' & a'x + b'x' + c'x'' + ... + d' \\ x'' & a''x + b''x' + c''x'' + ... + d'' \\ .. & ..... \end{array}\right| mod(p)$$

Jordan named "linear group" the group "originating" from this procedure of reduction. In modern parlance, Jordan's first theorem and its proofs boil down to showing that the linear group is the maximal group in which an elementary abelian group (the cyclic group F_p^* in the case $n = 1$ or a direct product of cyclic groups in general) is a normal subgroup.[44] In this sense, it generalizes to p^n the proof involved in Galois's criterion for the case $n = 1$.[45]

4.2 Jordan's reduction of analytic representations

We have seen that the main result of Jordan's thesis is a theorem from which the general linear group originates. As a matter of fact, this group was not defined by a list of axioms, as would

[44] In modern parlance, the "groups of permutations" correspond to a decomposition of the field into blocks of imprimitivity under the action of an imprimitive substitution group which is itself decomposed into a primitive quotient group. Let G be a transitive group operating on a set V. A subset V_1 of V is called a block of imprimitivity if $V_1 \neq \emptyset$ and for every $g \in G$, either $V_1 g = V_1$ or $V_1 g \cap V_i = \emptyset$. If V_1 is such a block and V_1, V_2, ..., V_m are the distinct sets $V_1 g$ for $g \in G$, then $(V_1, V_2, ..., V_m)$ is a partition of V. G is said to be imprimitive if there is no trivial proper block. G is primitive if it is not imprimitive. See[Neumann, 2006] for a discussion on primitivity in Galois's works. On the roles played by primitivity in Jordan's classification of solvable transitive groups, see[Brechenmacher, 2006, p.195-202].

[45] Later on, Jordan would devote a key chapter of his 1870 *Traité* to the "origin" of the linear group. Yet, this origin would be presented differently than in Jordan's 1860 thesis through a generalization of the proof of Galois's criterion, i.e. as a reponse to the problem of finding the analytic form of the maximal group T in which the group of substitutions $(k, k', ..., k^{(n)}; k + a, k' + a', ..., k^{(n)} + a^{(n)})$ (i.e., $F_{p^n}^*$) is a normal subgroup.

be natural to mathematicians nowadays. On the contrary, the general linear group originated from a chain of successive reductions of a general problem into sub-problems. Moreover, we have seen that linear substitutions were above all identified by their analytic representations. The reindexation of the letters based on the two different analytic representation of cycles played a key role in the procedure of reduction of linear groups, which was explicitly presented as modeled on Poinsot's reformulation of Gauss's decomposition (see the numerical examples in annex 1). From the retrospective point of view of Jordan's 1860 thesis, the Gauss-Poinsot method consisted in dividing the letters into groups, each of the same cardinal p^n, while systems of substitutions T were simultaneously partitioned into a "combination of displacements between the groups" [i.e. blocks] "and of permutations of the letters within each of the groups" [i.e., blocks].[Jordan, 1860, p.5]

Jordan commented the reindexation underlying his reduction in analogy with the reduction of a helicoidal motion into motions of translation and rotation. This implicitly referred to Poinsot. Moreover, he eventually appealed to the legacies of Gauss and Abel to claim that what could be designated as the unscrewing of the method of reduction of groups was the "very essence" of his approach :

> One could see an image of this result in the theorem of mechanics that reduces the general motion of a solid body to a motion of translation combined with a rotation around the center of gravity [...]. This principle of classification of letters in various groups is the same as the one Gauss and Abel showed the fertility in the theory of equations : to my opinion, this principle is the very essence of the question, it lays the ground for all my analysis.[Jordan, 1860, p.5]

The question of how Jordan accessed Poinsot's works is open. But the echoes between Galois's decomposition and Jordan's early works might have been the consequence of a perspective on Gauss and Lagrange that Poinsot, Galois, and Jordan had shared. It was indeed in the framework of the reduction of imprimitive groups to primitive groups on the model of Gauss's decomposition that the general linear group had originated from the two forms of representations of cycles in the works of both Galois and Jordan.

Jordan first commented on Galois in the seven-page supplement he added to his thesis in the memoir he sent to the Académie for the Grand Prix of 1860. He immediately focused on Galois's distinction between imprimitive and primitive equations. More importantly, he began to consider later steps of reduction that would thus resort to other forms of decomposition (i.e. into normal subgroups). Jordan's deep investigations on the decompositions of the general linear groups into subgroup would culminate in his *Traité* of 1870. The procedures of reductions of the analytic representations of linear substitutions played a key role in these investigations. They actually gave rise to a very general practice of reduction of a problem into a chain of sub-problems that Jordan applied to various issues, such as cristallography, complex analysis, geometry, or differential equations.

4.3 The Jordan canonical form theorem

The statement of the Jordan canonical form theorem between 1868 and 1870 exemplifies the crucial role played by reductions of the analytic representations of substitutions in Jordan's works. This theorem also highlights once again the model-role played by the decomposition of the linear form into the two analytic representations of cycles. In his investigations of the general linear groups, Jordan aimed at reducing any linear substitution on F_{p^n} into an analytic "form as simple as possible." We have seen that in the case of one variable, the substitution $(x\ ax+b)$ can be easily decomposed into two cycles $(x\ gx)$ et $(x\ x+1)$. Yet, such a decomposition cannot be directly generalized to the case of n variables. In modern parlance, a matrix of n lines and n columns can only be decomposed to a sequence of operations of the type $(x\ gx)$ if this matrix can be diagonalized.

Let first consider the special case of linear substitutions on p^2 letters (i.e. in 2 variables) that Jordan investigated in details in 1868 (thereby following Galois's second memoir). The determination of the simplest analytical forms was based on the polynomial decomposition of an equation of degree 2 (the characteristic equation of a matrix, in modern parlance). If this equation has two distinct roots, the letters can be reindexed in two blocks in such a way that the substitution is simply acting as a multiplication on each block,[46] i.e., by multiplying the indices by α and β if the two roots are real, or by $\alpha+\beta i$, $\alpha+\beta i^p$ (with $i^2 \equiv 1 mod(p)$) if the roots are two conjugated imaginary numbers :

$$\begin{vmatrix} z & \alpha z \\ u & \beta u \end{vmatrix}, \begin{vmatrix} z & (\alpha+\beta i)z \\ u & (\alpha+\beta i^p)u \end{vmatrix}$$

Yet, if the characteristic equation has a double root, the substitution cannot be reduced to operations of multiplication as above, unless it is a trivial homothety. In the general case, the canonical form involves a combination of multiplcations and additions :

$$\begin{vmatrix} z & \alpha z \\ u & \beta z+\gamma u \end{vmatrix}$$

In Jordan's *Traité*, the canonical form was generalized to n variables in Livre II and was used in Livre IV for reducing n-ary linear groups on the model of the groups of order $n=p^2$. Later on, Jordan would appeal frequently to reductions of substitutions (in $GF(p^n)$ or $\mathbb{C}$) in his works on groups, differential equations, algebraic forms, etc.

Theorem 3 ***Jordan's canonical form theorem***

[46] In modern parlance, one decomposes a vector space of dimension 2 into two subspaces each of dimension 1

This simple form

$$\begin{vmatrix} y_0, z_0, u_0, ..., y'_0, ... & K_0 y_0, K_0(z_0 + y_0), ..., K_0 y'_0 \\ y_1, z_1, u_1, ..., y'_1, ... & K_1 y_1, K_1(z_1 + y_1), ..., K_1 y'_1 \\ .... & ... \\ v_0, ... & K'_0 v_0, ... \\ ... & ... \end{vmatrix}$$

to which one can reduce the substitution à A by an adequate choice of indices, will be designated as its canonical form.[Jordan, 1870, p.127]

4.4 The architecture of Jordan's *Traité*

Let us now sketch a brief overview of the architecture of Jordan's *Traité*. We shall see that, even though Jordan's first theorem is scattered into pieces in the four sections of the treatise, the practice of reduction that lied beneath this theorem plays a transversal structuring role in the whole *Traité*. This practice actually supports a chain of successive generalizations that runs through the first three sections of the *Traité* until the "fundamental theorem" on the solvability of algebraic equation that opens Livre IV. This theorem then allows to reverse this chain of generalizations into a method of successive reductions of general linear groups.

4.4.1 Livre I. On congruences

The *Traité* begins with a presentation of the notions related to congruences that permit the indexation of letters and thus the analytic representation of substitutions. After a general presentation of binomial congruences $X^p - 1 \equiv 0$ *mod.p* in connection to the indexations of systems of p letters, Jordan turned to what he designated as the "Galois theory." This designation do not correspond to the modern Galois theory but to the theory of Galois's number theoretic imaginaries which allows to index systems of p^n letters. Jordan's presentation of this theory was modeled closely on the cyclotomy of the indexing of the primitive roots of Gauss's binomal congruence, which he generalized to congruences $X^{p^n} - 1 \equiv 0$ *mod.p*. Livre I thus introduces a special case of analytic representation of substitutions, that of the cycles $(x\ x + a)$ et $(x\ gx)$.

4.4.2 Livre II. Des substitutions

When they return in Livre II, Galois imaginaries play the role of a model case for later generalisations of the problem of the analytic representation of substitutions. The generation of the linear group is indeed presented as a generalisation of the special type of substitution underlying the indexing methods of Livre I, i.e., $(x\ x + 1)$ or $(x\ gx)$.

Following a first chapter devoted to a general synthesis of previous works on substitutions (such as Cauchy's, Serret's, Bertrand's or Mathieu's), the second chapter on linear groups represents the main part of Livre II. It opens with the problem of the analytic representation of

substitutions, which "generates the linear group." There, one may recognize an upside down presentation of Jordan's first theorem : while, in 1860, the linear group originated from successive reductions of a general problem, in 1870 the same group was generated by a direct generalization of Galois's criterion, i.e., from the problem of finding the analytic form of all the substitutions that leave invariant the following analytic form

$$|x, x', ..., x + \alpha, x' + \alpha', ...|$$

In modern parlance, the above substitutions correspond to direct products of cycles (i.e., elementary abelian groups). The problem is thus tantamount to finding the analytic form of the substitutions g that turn such products of cycles c into another product of cycles c':

$$gcg^{-1} = c' :$$

g thus have to take the following "linear form" :

$$\begin{vmatrix} x & ax + bx' + cx'' + ... \\ x' & a'x + b'x' + c'x'' + ... \\ x'' & a''x + b''x' + c''x'' + ... \\ .. & ..... \end{vmatrix}$$

The proof is a direct generalization of the one given by Galois to his criterion. On this occasion, Jordan insisted that, in modern parlance, $GF(p^n)$ could either be represented as $F_p(j)$ with j a root of $x^{p^{n-1}} \equiv 0$, or as a direct product of copies of F_p (i.e. as a vector space over F_p). In the first case, $GF(p^n)$ is immediately associated to a multiplicative cyclic group generated by the substitution $(x\ jx)$.

4.4.3 Livre III. On irrationnalities

The opening chapter of Livre III presents what would be nowadays considered as Galois Theory. However, the association between groups and equations is inscribed in the broader framework of a "General theory of irrationalities." While the "Algebraic applications" (chap. II) to Galois's theory of equations represents only a small part of Livre III, the emphasis is on "Geometric applications" (chap, III) and on "Applications to the theory of transcendental functions" (chap. IV).[Brechenmacher, 2011] In the present paper, I shall nevertheless focus on the chapter of "algebraic applications."

Jordan had first considered the "commutative groups" associated with Abel's equations, whose roots are rational functions of one of them. Primitive abelian equations actually corresponded to cyclic groups, and Jordan quickly focused on the binomial equations $x^n = 1$ and the associated cyclotomic equation of degree $n = p^\alpha$ (p an odd prime). All the roots can then be expressed by a primitive root ω, ω^2, ..., $\omega^{p^{\alpha-1}}$. The group of the equation is thus cyclic and generated by

$(x\ x+1)$. But the roots can also be reordered by the use of a primitive root g of the congruence $x^{p^\alpha} \equiv 1 mod.p$, i.e., by the following sequence corresponding to $(x\ gx) : \omega, \omega^g, \omega^{g^2}, ..., \omega^{g^{p^\alpha-1}}$.

Second, "Galois equations" are introduced as generalizing Abel's in three different ways. First, they are irreducible equations of prime degree p all of whose roots can be expressed rationally by two of them, an obvious generalization of the equations considered by Abel. Second, their groups are constituted of substitutions of the form $(x\ ax + b)$, i.e., those originating from the cycles of abelian equations. Third, a special case of Galois equation is given by $x^p - A = 0$, i.e., an obvious generalization of binomial equations.

Galois's equations could thus be understood as the result of a chain of generalizations based on the relations between number-theoretic imaginaries, cyclic groups, and linear groups. But from the standpoint of Livre III, the chain could now be considered the other way round. Indeed, the relation between abelian and Galois equations provided an application of the reduction of a group by the "adjunction of irrationals to the [associated] equation." Given a Galois equation, let ϕ_1 be a function of the roots invariant by $(x\ x+b)$. Recall that such substitutions form a normal subgroup of the group $(x\ ax+b)$ (origin of the linear group). Let then ϕ_1 be adjoined to the Galois equation: the group of the equation is then reduced to a cyclic group and the equation itself into an abelian equation; as for the group of the equation in ϕ_1 , it is composed of substitutions $(x\ ax)$ and is then a commutative group too. The initial Galois equation has eventually been reduced to two abelian equations and its linear groups to two commutative simple groups.

4.4.4 Livre IV. On solutions by radicals

But the general theory of Livre III was itself a special model case for the next step of generalisation. Livre IV opens with two theorems, the first stating that abelian equations of prime degree are solvable by radicals, the second, that "an equation is solvable by radicals if and only if its solution can be reduced to the one of a sequence of abelian equations of prime degrees."[Jordan, 1870, p.386] The reduction of Galois equations into abelian equations had thus incidentally proved Galois's criterion. But Jordan did not state the criterion explicitly. The special case of the reduction of linear groups to commutative groups did not aim at imitating Galois's criterion, but instead at the following theorem, which concerned any chain of normal subgroups with quotient groups that are abelian and that Jordan designated as "the criterion of solvability":

Theorem 4 ***Jordan's fundamental theorem***

A group L is solvable if and only if it is possible to form a sequence of groups 1, *F, G, H, ..., L, such that, 1° each of these groups is included in the previous one and permutable to its the substitutions of L ; 2° any two of its substitutions are exchangeable one with another, up to the substitutions of the previous group.[Jordan, 1870, p.395]*

Jordan claimed his theorem laid the ground for a method by which one would "rise progressively to the knowledge of [solvable] groups," i.e., the problem to which all the rest of the treatise

would be devoted. By the use of this method, "each new step toward the solution will make the field of research narrower."[Jordan, 1870, p.396][47]

Let us now come to some conclusions about the structure of the *Traité*. Recall that Jordan introduced the linear group as a generalisation of the special case of the cyclic substitutions associated with number-theoretic imaginaries. Later on, when the notion of a group of an equation had been introduced, the origin of the linear group could be considered as a model for the generalisation of cyclotomic equations to Galois equations. Special cases were both models for the general theory and applications of it. Each link in the resulting chain of generalisation was providing a "higher point of view" toward the previous links. In Livre IV, the relation between linear substitutions $(x\ ax+b)$ on the one hand, and the two forms of representations of cycles $(x\ x+1)$ and$(x\ gx)$ on the other hand, would eventually provide a model for the fundamental theorem. In a sense, this theorem crystallized the chain of generalisations that structured the *Traité*, and which could thus be reversed in turning special model cases into applications. For instance, Livre II's origin of the linear group now appeared as a crucial step for the determination of solvable transitive groups. After having reduced the problem from solvable transitive groups to solvable primitive groups, Jordan indeed showed that a minimal normal subgroup A of a solvable primitive group G is commutative and isomorphic to sums of cyclic groups (i.e. of type (1, 1, ..., 1) in modern parlance). But G is actually acting on A by linear substitutions: it therefore corresponds to the general linear group, originating from A. On thus recognize here a new presentation of the method of reduction underlying Jordan's first theorem.

The fundamental theorem indeed supported a chain of reductions from the most general groups to the most special ones : transitive, primitive, linear, symplectic groups etc., until the simple cyclic groups. Most of Livre IV was actually devoted to this chain of reduction.

> The essence of my method consists in determining successively the partial groups $F, G, H, ...$[Jordan, 1864, p.963]

The linear group played a crucial role in this chain of reduction. It was indeed the most general group the substitutions of which had an analytic representation. Moreover, Livre IV made constant use of procedures of decompositions of the analytic form of linear substitutions.

5 A shared algebraic culture

Let us now come back to the issues raised in the second section of this paper as regard to Moore's works on Galois fields from 1893 to 1896. We have seen that even though he obviously aimed at paying tribute to Klein, Moore had collided in 1893 with the tacit collective dimensions of a constellation of papers published in France in the 19th century. We have seen also that Moore and his student Dickson had struggled to access this collective dimensions, especially by appealing to

[47] Jordan distinguished between three types of problems: A. The reduction from maximal solvable transitive groups to maximal solvable primitive groups and thereby to B. Maximal solvable groups in $Gl_n(p)$, which included the particular cases of C. Maximal solvable groups in $Sp_{2n}(p)$ or $O^+_{2n}(2)$ and $0^-_{2n+1}(2)$. See[Dieudonné, 1962].

Jordan's 1870 *Traité*. Yet, we are now able to develop a finer analysis of the situation than the one that is suggested by national frames. Indeed, we have seen that Galois's number theoretic imaginaries had followed different lines of developments in France and abroad, in connection with different uses of the analytic representation of substitutions. Let us recapitulate the various forms of interactions between number-theoretic imaginaries and substitutions we have analyzed in this paper.

5.1 Number-theoretic imaginaries and substitutions

At the turn of the 1850s-1860s, Galois's imaginaries were used as a way to extend analytic forms of substitutions from p to p^n variables. Most texts actually dealt with binary linear fractional substitutions ([Hermite, 1859], [Serret, 1859], [Serret, 1865], [Serret, 1866]], [Mathieu, 1860], [Mathieu, 1861b], [Mathieu, 1861a]). Jordan nevertheless investigated general linear substitutions on n variables.

On the one hand, authors such as Hermite had focused on the special substitutions attached to special equations, such as the one-variable linear representation $(k\ ak+b)$ associated to Galois's criterion, and more importantly the linear fractional representation $(k\ \frac{ak+b}{ck+d})$ attached to modular equations. Hermite eventually generalized his investigations on modular equations in 1863 in stating a necessary and sufficient condition for an analytic function to represent a substitution on p^n letters. This approach laid the groundwork for most later presentations of the problem of the analytic representation until the turn of the century (e.g.[Serret, 1866, p.383], [Jordan, 1870, p.88], [Netto, 1882, p.140], [Borel et Drach, 1895, p.306], [Dickson, 1901, p.59]).[48] Yet, it is clear that Hermite's main interest remained focused on special equations. Recall that his 1863 paper had systematically stated all the reduced forms of analytic expressions of substitutions on 5, and 7 letters, a problem that Hermite had explored in 1858-1859 in connection to his investigations of the modular equations of order 5 and 7. Later on, most treatises presented the problem of the analytic representation of substitutions just before they introduced linear substitutions (i.e. the form generated by the two forms of cycles). Moreover, this presentation usually played the role of an intermediary between substitutions and equations. Following Hermite, all treatises, except Jordan's, therefore limited themselves to the considerations of the substitutions $(k\ ak+b)$ and $(k\ \frac{ak+b}{ck+d})$ related to solvable equations of prime degree and to modular equations.

On the other hand, we have seen that Jordan had developped a specific approach to general classes of solvable equations by dealing with general linear groups. The higher level of generality of Jordan's groups was nevertheless problematic. A "general" development was indeed supposed to be valid for all the objects under consideration, such as in Hermite's 1863 paper that both stated a truly general result on the analytic representation of substitutions in n variables and investigated special cases. On the contrary, Jordan's n-ary linear substitutions did not provide any general solution to the problem of the number of values of functions for which they had been introduced.

[48] In the introduction of his 1882 thesis, Edmond Maillet attributed to Hermite the introduction of the analytical notation $(x_k\ x_{\phi(k)})$ itself[Maillet, 1892, p.2].

In the 1870s, Jordan's general linear groups were explicitly criticized by Kronecker for their false generality and formal nature.[Brechenmacher, 2007] Indeed, Kronecker accused Jordan of having mixed up tools relative to the orientation he had given to his investigations (i. e. n-ary linear substitutions) with the inherent significations of "objects of investigation" (e.g. the number of values of functions, the analytic forms of all substitutions on 5 letters etc.). Following Kronecker, in his 1882 treatise on substitutions, Eugen Netto did not consider general linear groups as a special type of group (in contrast with cyclic, abelian, metacyclic, and modular groups) : they were limited to the object of investigation of the problem of the analytic representation of substitutions.[Netto, 1882, p.128-139]

For decades Galois's legacy opposed two approaches which both aimed at reaching the "essence" of mathematics. On the one hand, some authors, following Hermite and Kronecker, aimed at characterizing the special nature of general equations of a given degree. On the other hand, some others, following Jordan, focused on the relations between classes of solvable equations (or groups) of a general degree n. The two approaches were nevertheless both presented in Jordan's *Traité*. The first approach was indeed included in the synthesis of the *Traité*'s Livre III on the types of irrational quantities associated to types of equations.[Brechenmacher, 2011] The second went with Jordan's specific practice of reduction. It structured the *Traité* in a complex chain of generalizations of special model cases. This approach had almost no circulation until it was developed in the 1890s in the Galois fields network.

Recall that Moore's 1893 investigations on linear fractional substitutions ($k\ \frac{ak+b}{ck+d}$) were initially stemming from the first of the two above approaches, which Moore had learned from the Klein and Fricke textbook. Yet, in aiming at generalizing the groups attached to modular equations of order 5, 7, and 11 to n variables, his paper collided with the specificity of Jordan's general linear groups.

5.2 Number-theoretic imaginaries as an autonomous theory

We have seen that even though number-theoretic imaginaries were tightly linked to substitutions in Galois's works, the latter presented his 1830 *Note* as an autonomous topic in number theory.

In the 1854 edition of Serret's *Cours*, Galois's imaginaries were presented as the conclusion of a series of three lectures devoted to the theory of congruences. Unlike the notion of primitive root of binomial congruences, they were not connected to cyclotomic (and abelian) equations or to the additional notes of Hermite and Kronecker on Galois's criterion of solvability. Apart from a short note of[Allegret, 1856], Galois imaginaries were not used again in connection with equations until the works of Jordan in the mid-1860s. When Dedekind started to develop his approach on higher congruences in 1857, he alluded to both the presentations of Theodor Schönemann in the legacy of Gauss and Abel, and those of Serret in the legacy of Galois.

In the third edition of the *Cours* in 1866, Serret went further, inscribing number-theoretic imaginaries in a comprehensive theory of congruences. The presentation included a development on integer polynomials modulo a "modular function,"[Serret, 1865],[Serret, 1866] thereby follow-

ing Cauchy's approach to congruences rather than Galois's. Serret's approach was endorsed later by treatises such as[Jordan, 1870],[Borel et Drach, 1895], and[Vogt, 1895].

Yet, we have seen that Jordan's presentation included Galois's original approach in addition to Serret's. Moreover, in Jordan's *Traité*, Galois's imaginaries could not be dissociated from substitutions theory : as in Galois's works, both topics were interlaced through the issue of the indexing of letters and of the analytic representation of substitutions, which gave rise to the investigations on the general linear group as originating from direct products of cyclic groups. Further, contrary to Serret's approach, Jordan appealed to a traditional way of legitimizing the use of imaginaries by resorting to the analogies carried on by "instruments of computation" :

> The consideration of the imaginary roots of irreductible congruences introduces itself naturally in my analysis, which would have certainly not been successful should have I hesited to adopt them. I would be pleased to have contributed by these examples to show the power of this new instrument of analysis, that some eminent geometers are still apparently considering with mistrust.[Jordan, 1867b, p.269]

It is well known that Kronecker contested the legitimacy of such traditional presentations of algebraic imaginaries. In his influential 1882 *Grundzüge*, he developped an effective presentation of the problem in the tradition of congruences of polynomial forms, as developped by Cauchy and Serret in France.

Despite Kronecker's opposition, Jordan's traditional perspective on Galois imaginaries continued to circulate, especially from Jordan to[Gierster, 1881], [Klein et Fricke, 1890], [Moore, 1893], and [[Burnside, 1894]. Moore's 1893 congress paper especially illustrates that both Serret's *Cours* and Jordan's *Traité* were alternative reference to Kronecker's theory in the 1890s. In the framework of Kronecker's 1882 *Grundzüge*, Serret's "fonctions modulaires" should have been understood by Moore as "modular systems" on "domains of rationality." As a matter of fact, Hölder resorted in 1893 to Kronecker's framework to formulate Galois imaginaries.[Hölder, 1893] . In contrast with Kronecker's legacy, the influence of Jordan's approach can be seen in the parallel evolution of the works of Moore (and later Dickson) and Burnside. As shall be seen in the next section, both Moore and Burnside indeed investigated the same groups (i.e., $PSl_2(p)$, $PSl_3(p)$, $PSl_m(p)$, and eventually $Gl_n(p)$). Moreover, both stated independently the same theorems.

5.3 Jordan's *Traité* as a Chicagoan textbook

We shall now question how, in the context of the institutionalization of group theory in 1890s, Jordan's *Traité* could have supported the discontinuous circulation of some specific algebraic practices from Paris in the late 1860s to Chigago at the turn of the 20th century.

We have seen that Moore had resorted to Klein's mediation of a longstanding French tradition. But as for the circulation of either linear fractional substitutions or number-theoretic imaginaries, Serret's *Cours* played initially a much more important role than Jordan's *Traité*. We shall see that this situation changed in the years following the Chicago congress.

In 1894-1895, Moore published two papers closely related to his 1893 lecture. The first connected the groups of automorphisms of an abelian group of order 2^3 and of type $(1,1,1)$ to the simple linear group of 168 elements (i.e., $PSl_3(F_2)$).[Moore, 1894, p.65] As was already the case with Galois fields, Moore's approach can be understood as shedding new light on older works. We have indeed seen that linear groups had been presented as originating from abelian groups of type $(1,1,...,1)$ in Jordan's *Traité*.

This traditional dimension of the problem sheds light on the parallel works developped almost simultaneously by Moore and Burnside. About nine months before Moore, Burnside had indeed proven the more general result that the group of automorphisms of the abelian group of p^n elements of type $(1,1,..,1)$ is isomorphic to $GL_n(p)$.[Burnside, 1894, p.139][49] Exactly the same theorem constituted the core of Moore's 1895 "Concerning Jordan's Linear Groups." This paper was presented as a demonstration of the efficiency of Galois fields in group theory; it concluded with tables of primitive elements of Galois imaginaries that had been computed by Moore's students. Amongst them, Dickson might have been already in charge of investigating the works of Mathieu. He had indeed identified that a group of substitutions on p^n letters introduced in[Mathieu, 1861b] was isomorphic to $GL_n(p)$. Moore concluded that "this seems to be the source from which Mr Jordan's linear groups were drawn."[Moore, 1895]

Dickson's thesis would then especially investigate the relations between the works of Mathieu and Jordan. It ended with a proof that $GL_n(p)$ is isomorphic to the Betti-Mathieu group, i.e., the set of all "quantics" (polynomials) of an analytic form $\phi(k)$ as follows that represent a substitution on $GF(p^{mn})$ (considered as a vector space on$GF(p^n)$):

$$\phi(k) = \Sigma_{i=0}^{n-1} a_i k^{p^i}$$

for each $a_i \in GF(p^n)$

As a result, Dickson's investigations raised some new interest in Mathieu's works on multiply transitive groups on Galois fields. These groups indeed provided classes of simple groups and it was through their investigations that the notion of Galois field circulated to the works of Miller and, from there, to the works of Séguier (1901-1904, see esp.[Séguier, 1904a]) and Frobenius (1902, 1904, see esp.[Frobenius, 1902]).

Moreover, Dickson's very close reading of Jordan's *Traité* resulted in a flood of papers that systematically generalized results from linear substitutions on F_p to $GF(p^n)$.[Parshall, 2004, p.265][50]

[49]Neither Moore nor Burnside referred to one another at that time and it is unclear if their works were independent or were actually competing. The introduction of[Burnside, 1896] seems to have aimed at contradicting[Moore, 1895] and[Moore, 1896] in claiming that the notion of the group of automorphisms of a group was not a new concept. In 1896 Moore sent to the London mathematical society a paper on the abstract definition of the symmetric group. Burnside introduced the paper he published on the same topic by claiming he had asked the Council of the society permission to withdraw his communication given the "more complete" results stated by Moore[Burnside, 1897a]. Burnside would not refer to either Moore or Dickson in his 1897 treatise and the other way round with[Dickson, 1901]

[50]The very close reading of Jordan by Dickson is illustrated by the latter's adoption of terminologies which had already been much criticised such as the one of "abelian group" for what Hermann Weyl would designate as

In Dickson's 1901 monograph on linear groups, the theorem on the Betti-Mathieu group was the hinge between the first section on Galois fields, based on Hermite's 1863 approach on "substitution quantics," i.e., the investigation of the analytic representation of substitutions of less than 11 variables, and the second section on Jordan's n-ary linear groups. This new synthesis between the approaches of Hermite and Jordan acted as an impulse for the development of the Galois fields network both within the framework of the Chicago school and for other close readers of the *Traité*, especially in France.

5.4 Linear groups in Galois fields : a shared algebraic culture

Let us now get back to the issue of the collective dimensions of the Galois fields network. This network can now be understood as a shared algebraic culture. On the one hand, this culture was based on Serret's presentation of Galois's number theoretic imaginaries as an autonomous topic and on Hermite's approach to the problem of the analytic representation of substitutions. On the other hand, it was rooted on Jordan's intertwining of Galois's imaginaries with the reduction of the analytic representation of n-ary linear substitutions.

Jordan's approach especially played a key role in the specificy of this algebraic culture as regard to some other contemporary works. It's legacy can not only be traced in France in the works of authors such as Poincaré, Autonne, Maillet, Séguier, etc.,[Brechenmacher, 2012a] but it also circulated in the U.S.A. after Dickson's 1896 thesis.

It was because they shared this culture that some French and American authors were able to interact with each others, even though most of them did not have any direct contact and did not share any social framework, as is exemplified by such different figures as de Séguier, an aristocrat jesuit abbot, and Schottenfels, one of the first women to graduate in mathematics at Chicago, or as Dickson, who had met with Jordan in person during his one-year student trip in Europe, and other Americans who had not developed a close reading of the *Traité*, such as Miller.

Communication was nevertheless partial and was actually mostly limited to the shared algebraic practices mentionned above. Yet, this shared algebraic culture was sufficient for texts to circulate between France and the U.S.A., to respond to each other, and even for controversies to detonate. A telling example is the new formulation that was given repeatedly and indepently to Jordan's "origin" of the linear group as the theorem stating that the group of automorphisms of an elementary abelian group A is the general linear group $Gl(F_{p^n})$.

This theorem was, for instance, stated by Le Vavasseur in 1895. Given a root x of the congruence

$$f(x) \equiv 0$$

Levavasseur considered the Galois number theoretic imaginary

$$j = \alpha_1 + \alpha_2 x + \alpha_3 x^2 + ... + \alpha_n x^{n-1}$$

"symplectic groups".

and formed the group of the n distinct operations

$$\alpha_1, \alpha_2, ..., \alpha_n$$

as generated by a unique operation a :

$$a^j = a_1^{\alpha_1} a_2^{\alpha_2} a_3^{\alpha_3} ... a_n^{\alpha_n}$$

This analytic formulation of the problem was sufficient for Miller to react promptly to Le Vavasseur's note in claiming his priority by sending a note to the Académie de Paris. The discussion between the two went on with two other notes. Yet, this theorem had also been stated a few months earlier by Burnside and Moore. And it would be stated again a few months later by Dickson and Séguier. As has been seen in the previous section, the issue at stake had a long background in the context of the problem of the number of values of functions. Authors such as Le Vavasseur, Miller, Moore, Dickson or Séguier shared a same basis of sources even though they also had divergent individual agendas and belonged to various social spaces.

5.5 A space of circulation of specific practices of reductions of analytic representations

The network of texts that revolved around "Jordan's linear groups in Galois field" at the turn of the 20th century had thus underlying it a shareed algebraic culture. In this section, we shall discuss further the procedures of reductions of the analytic forms of substitutions that were at the root of this shared culture.

The growing importance of linear groups was a large-scale trend at the turn of the 20th century. Yet, in the early 1890s, "linear groups" usually designated the groups of binary or ternary unimodular fractional linear substitutions Klein and his followers had investigated (i.e. $PSL_2(p)$ and $PSL_3(p)$). Even though Klein's linear groups would still play an important role at the turn of the century,[Wiman, 1900] some collective interest in Jordan's general linear groups in Galois fields emerged by that time. A telling example is the adoption of the term "special linear groups" for designating what used to be "linear groups" in the early 1890s.

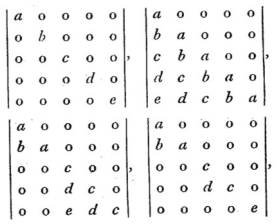
The label linear groups was thus far from pointing to a unified category at the turn of the 20th century. For instance, Weber's influential *Lehrbuch der Algebra* introduced homogeneous linear groups of n variables by appealing to the analytic form of n-ary linear substitutions. But it nevertheless only stated a few general properties before focusing on special groups such as $PSL_2(p)$. In contrast, Dickson's 1896 thesis followed Jordan in introducing $Gl_n(p)$ as the maximal group in which an abelian group of type $(1, 1, .., 1)$ would be a normal subgroup. The second part of the thesis was then devoted to generalizations of Jordan's results from F_p to $GF(p^n)$.

Moreover, various ways of dealing with linear substitutions had parallel circulations until

the constitution of linear algebra as a discipline in the 1930s.[Brechenmacher, 2010] Amongst these, the most influential approach was based on Frobenius's 1877-1879 presentation of the theory of bilinear forms. This approach appealed to symbolic methods and to computations of invariants by determinants such as Weierstrass's elementary divisors.[Hawkins, 1977] It incorporated the notion of matrix in the 1890s, and played a key role in Frobenius's representation theory.[Brechenmacher, 2006, p.279-461]

But the main protagonists of the Galois fields network shared an alternative approach based on Jordan's reduction of a linear substitution to its canonical form. This collective attitude has to be regarded as an important specific feature of the Galois fields network. Jordan's canonical form did indeed embody the method of reduction we have seen to be specific to Jordan's relation to Galois. It especially resorted to the unscrewing into the two forms of actions of cycles $(k\ gk)$ and $(k\ k+a)$ which it assimilated to issues involving n variables. Yet, Jordan's canonical form theorem had almost disappeared from the public scene since it had been strongly criticized by Kronecker a few years after it had been stated.[Brechenmacher, 2007] Kronecker not only rejected the formal generality of Jordan's linear groups, but also criticized the non-effectiveness of the canonical reduction, which required the determination of the roots of arbitrary algebraic equations. Moreover, Frobenius not only presented Jordan's canonical form as a corollary of Weierstrass's elementary divisor theorem, but also insisted that the validity of Jordan's form was limited to the case when one would allow the use of "irrationals" such as "Galois's imaginary numbers."[Frobenius, 1879, p.544] In contrast, the reformulation Kronecker had given to Weierstrass's theorem in 1874 was based on a rational method of computations of invariants in any "domain of rationality" (i.e. the invariant factors of matrices in a principal ideal domain).

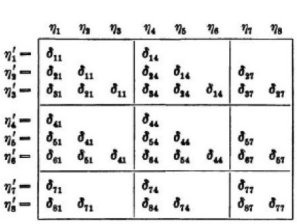
During the 1880s and 1890s, Jordan's canonical form had an underground circulation in the works of authors such as Poincaré or Élie Cartan, where it was neither considered as a theorem nor attributed to Jordan.[Brechenmacher, 2012a] On the contrary, it circulated in plain sight at the turn of the century. Much work would be devoted to making some procedures of matrix decomposition explicit that had never been considered as mathematical methods per se until then ([Burnside, 1899], [Dickson, 1900], [Dickson, 1902], [Séguier, 1902], [Autonne, 1905], [Séguier, 1908]). Moreover, Séguier and Dickson would both publicly challenge the traditional structure of the theory of bilinear forms ([Séguier, 1907], [Dickson, 1928]). Later on in the 1930s, decompositions to canonical forms would lay the ground for expositions of the theory of matrices, such as the ones of Cyrus Colton Mac Duffee a student of Dickson.[Mac Duffee, 1933]



Poincaré 1884

$$A=\begin{Vmatrix} a & 1 & 0 & 0 & . & .0 \\ 0 & a & 1 & 0 & . & .0 \\ 0 & 0 & a & 1 & . & .0 \\ . & . & . & . & . & .. \\ 0 & 0 & . & . & 0 & a1 \\ 0 & 0 & . & . & . & .a \end{Vmatrix},$$

Autonne 1905



Dickson 1901

In a word, the Galois fields network had underlying it a shared algebraic culture based on

the space of circulation of key algebraic practices of Jordan's *Traité*. The use of the terminology "practice" here aims at highlighting the fact that reducing a substitution to its canonical form was not limited to a computational process. Unlike the static nature of the invariants of the Frobenius theory, this approach was based on dynamic decompositions of the analytic representations of matrices (or "Tableaux" as the French used to say at the time). Moreover, Kronecker's criticisms of canonical forms in 1874 resorted to issues involving the nature of the essence of mathematics, which the latter had laid on the special objects of investigations of arithmetic (forms, especially) as opposed to the general relations shown by groups in algebra.

The extent of the space of circulation of algebraic practices such as Jordan's was neither directly the consequence of the efficiency of the underlying procedures or of a preexisting social framework. It is therefore difficult to determine the respective roles played by shared perspectives on the *Traité* on the one hand, and preexisting spaces of circulation on the other hand. Such issues shall thus be left open in the present paper. They would require further investigations on algebra and number theory at the turn of the 20th century, with a closer attention to actors, such as Le Vavasseur, Séguier, or Miller, who did not have key positions in the main centers of production of mathematical knowledge. The question of the time-period during which the Galois fields network functioned will also be left open in this paper. To begin with, the fact that the expression "champs de Galois" was used for a long time in France in parallel to the use of the term "corps fini" should be studied further.[51] Second, the linear algebraic identity of the network is associated with other developments over the course of 19th century. For instance, some of the procedures of decomposition underlying Jordan's canonical form circulated from Cauchy's "calcul des Tableaux" to Cambridge in the 1840s, were incorporated into Cayley and Sylvester's matrices in the 1850s, and circulated with matrices to the U.S.A. where they would meet again with the "Tableaux" in the Galois fields network.[Brechenmacher, 2010]

Conclusion

The introduction of Galois fields in Chicago in 1893 might have appeared somewhat chaotic at first sight. But, on the one hand, Moore's approach unveiled a long tradition dealing with substitutions and number-theoretic imaginaries. On the other hand, Moore's move was coherent with some other contemporary reorganizations of the legacies of Klein and Kronecker in finite group theory. Indeed, in that same year of 1893, Weber appealed to Dedekind's *Körper* to lay new grounds for "Galois's theory of general equations." As a conclusion of this paper, I shall discuss the impact of Jordan's legacy in regard with the one of Dedekind. Both approaches had indeed been blamed by Kronecker in the 1870s-1880s. Moreover, in the mid-1890s, Jordan's approach was being developped in the U.S.A. at the same time as Dedekind's legacy was being incorporated

[51] After 1905 the intertextual relationships seemed to change as well as the topics studied. On the one hand, the use of the reference to Galois field would be more widely used in the U.S.A. On the other hand, the works of Dickson as well as the ones of Séguier would focus on the invariants of quadratic forms and their geometric interpretations.

in algebraic number theory in Germany : in this framework, number-theoretic imaginaries were presented as a special case of Endlicher Körper: the Congruenz Körper.[Weber, 1893, p.534]

In the 1896 edition of his congress paper, Moore noted the equivalence of the terms "Field" and "Endlicher Körper." Yet, we saw that the algebraic number aspect of Galois theory - as developped by Kronecker who rejected Jordan's approach - had not played any role in Moore's approach. Moreover, the notion of Galois field did not have the same evolution as that of Körper. As a matter of fact, Moore repeatedly insisted that the "purely abstract form" of Galois fields "would seem to fit best for immediate use wherever it can with advantage be introduced,"[Moore, 1896, p.212] i.e., the investigation of "Jordan's linear groups" [Moore 1895, p. 38]. When he eventually referred to Kronecker in 1897,[Moore, 1897] Moore presented modular systems as a "concrete purely arithmetic phrasing" of abstract Galois fields.[Moore, 1898, p.281] In 1898, the bibliography of Dickson's *Report* on linear groups included the works of Sch´onemann (as well as the ones of Auguste Pellet in the 1880s), thereby illustrating the efforts that had been done for making the collective dimensions of both Galois fields and linear groups precise. But Dickson's *Report* nevertheless insisted on the autonomy of abstract Galois fields in linear group theory in connection with number theory. In the legacy of the essence Jordan attributed to the theory of order, Galois fields came to represent an abstract algebraic alternative to Weber-Hilbert's arithmetic-algebraic Körper.

Linear groups in Galois fields eventually reorganized lines of development in a no less radical way than Weber and Hilbert did when they celebrated Dedekind's approach. References to Galois played a key role in the reorganizations based on both the notions of field and Körper. Both had jumped over Kronecker on behalf of two alter egos, Jordan and Dedekind. In Moore's 1893 congress paper, Dickson's 1898 *Report*, or the latter's 1901 *Linear Groups*, the reference to Jordan-Galois played a role analogous to the reference to Dedekind-Galois in Weber's 1893 "Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie," the 1895 *Lehrbuch*, or Hilbert's 1897 *Zahlbericht*.

Let end the present paper with some considerations on the type of collective dimensions of mathematics we have investigated. We have seen that the history of algebra is not limited to issues related to the origins of diffusions of some abstract notions or structures. On the contrary, the circulations of some specific algebraic practices and forms of representations played a key role in shaping some collective dimensions of mathematics that did not correspond to any discipline, nation, or institution. The example of the quite unexpected circulation of Jordan's specific approach in Chicago, despite a very strong German influence, highlights how complex some algebraic cultures can be. The identification of such cultures not only recquires the micro-historical identification of some specific procedures. It also necessitates the analysis of the circulation of these procedures, in appealing to scale-games between the local and the global, the short-term and the long run. The history of algebra especially recquires a carefull attention to practices of writings. As we have seen, modalities of representations are often interlaced with some specific procedures, as well as with both cultural and epistemic values of generality or simplicity.

We have seen also that the systematic investigation of traces of intertextual relations sheds light on some implicit collective forms of references, such as the one that lied beneath expressions such as the "analytic representation of substitutions" or "linear groups in Galois fields." This situation highlights the crucial role played by some networks of texts for the identification of some collective dimensions of mathematics at a time when "algebra" was not yet referring to an object-oriented discipline.

One should nevertheless keep in mind that each individual actor was involved in several networks of texts at the same time, as well in several social spaces. Recall that the starting point of the network we have analyzed in this paper was the choice of a point of reference, i.e., Moore's 1893 congress paper. It is from this point of reference that intertextual references have been worked out systematically. The choice of another point of reference, such as Burnside's works, would have resulted in a different collection of texts, with a much stronger presence of some works on matrices published in the U.K. Moreover, at the beginning of our investigations, a specific problem has been posed, that is the one of the collective dimension of a group of texts published from 1893 to 1907. It is this collective dimension on the short term we have identified as a shared algebraic culture. In this purpose, we have investigated a collection of texts in the long run of the 19th century. Yet, the coherence of this corpus results from the retrospective point of view of the turn of the century, especially in the sense that some of these texts were considered altogether by the Chicagoans as "French" mathematics. But this whole collection did no correspond to any objective collective dimension *per se*. On the contrary, its texts belonged to various collective dimensions. The "theory of order" in which Jordan inscribed his early works was for instance very different from the context in which Hermite's works on the analytic representation of substitutions took place.

To be sure, networks of texts should nevertheless not be reified as an abstract notion. Yet, investigating intertextual references nevertheless provides a heuristic method for identifying various collective spaces in which mathematics have evolved.

Annex 1. Indexations and the analytic representations of cycles

It is well known that the cubic roots of unity can be either expressed by radicals :

$$1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}$$

or by the exponential notation :

$$1, e^{\frac{2i\pi}{3}}, e^{\frac{-2i\pi}{3}}$$

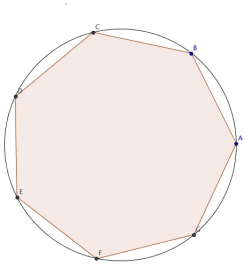
The above form of representation highlights that all the roots can be expressed by the sequence (0, 1, 2) of the powers of one of them, i.e., a primitive root such as $\omega = e^{\frac{2i\pi}{3}}$. Indeed, $\omega^2 = e^{\frac{-2i\pi}{3}}$,

$\omega^3 = 1 = \omega^0$ etc. The three cubic roots are thus indexed by the additive group $\mathbb{Z}/3\mathbb{Z}$: a root is turned into the successive one by the cycle that is represented analytically by $(x\ x+1)$.

But the sequence of the roots can also be reindexed by using another analytic represenation of a cycle : $(x\ gx)$. For instance, the cycle, $(x\ 2x)$ generates the multiplicative group $\mathbb{Z}/3\mathbb{Z}^*$: ω, ω^2, $\omega^4 = \omega$ etc.

This double indexation is crucial. It allows to decompose simultaneously the set of the roots of unity into subsets, or blocks, and cyclic groups into subgroups.

Let us consider in more details the example of the seventh roots of unity, associated to the additive group $\mathbb{Z}/7\mathbb{Z}$. These roots can be represented as points on a a circle :



Let $g = 3$. Starting with the primitive root $\omega = exp(\frac{2i\pi}{7})$, corresponding to the point B, the operation $(x\ 3x)$ provides all the roots of unity, less the unity itself (represented by the point A) :

- ω^3, corresponds to the point D
- ω^{3^2}, corresponds to the point C because $3^2 \equiv 2\ mod(7)$
- ω^{3^3}, corresponds to the point G because $3^3 \equiv 6\ mod(7)$
- ω^{3^4}, corresponds to the point E because $3^4 \equiv 4\ mod(7)$
- ω^{3^5}, corresponds to the point F because $3^5 \equiv 5\ mod(7)$
- ω^{3^6}, corresponds to the point B because $3^6 \equiv 1\ mod(7)$

The cycle $(x\ 3x)$ thus generates the cyclic group $\mathbb{Z}/7\mathbb{Z}^*$.

But let us now consider the operation $(x\ g^2x)$, i.e., $(x\ 2x)$ (because $3^2 \equiv 2\ mod(7)$). Starting with ω, one only gets the three roots corresponding to the points (B, C et E) :

- ω^2, corresponds to the point C
- ω^{2^2}, corresponds to the point E because $2^2 \equiv 4\ mod(7)$
- ω^{2^3}, corresponds to the point B because $2^3 \equiv 1\ mod(7)$

The set of the roots has thus been decomposed into the two blocks corresponding to (B, C et E) on the one hand, and (D, F et G) on the other hand.

This procedure of decomposition allows to prove that cyclotomic equations can be solved by radicals. For expressing by radicals the seventh roots of unity, it is compulsory to solve an equation of the sixth degree. Yet, the decomposition of the roots into two blocks allows to reduce the problem to the one of the resolution of two equations, one of the second degree and the other of the third degree. Indeed, if one sums the elements in each of the blocks, the two resulting expressions :

$$\omega + \omega^2 + \omega^4$$

and

$$\omega^3 + \omega^5 + \omega^6$$

are the roots of an equation of the second degree.

It is important to note that one can pass from one block of roots to the other by muliplying the indices by $g^3 \equiv 6\ mod.7$. Indeed :

$$2 \times 6 = 12 \equiv 5\ mod(7)$$

$$4 \times 6 = 24 \equiv 3\ mod(7)$$

$$1 \times 6 = 6$$

Geometrically, the operation (x $6x$) can be understood as a rotation of the circle on itself, of angle $\frac{4\pi}{7}$, and that turns B, C, E on D, F, G.

On the other hand, the permutation (x $x+2$) allows to circulate between the roots of the same block : it can be understood as a translation that urns each root into the following one.

In sum, the cycle (x gx) allows to decompose the roots into blocks, that can be turned one into the other by rotations of the circle, while the operation (x $x+a$) permits to translate the roots within the same block.

Let us now detail the case of the binomial equation of degree $p = 19$, i.e., of the cyclotomic equation of degre $p - 1 = 18$. The 18 cyclotomic roots :

$$\omega, \omega^2, ..., \omega^{18}$$

can be decomposed into 6 blocks (i.e., Gauss's periods) of 3 roots because $18 = 3.6$. The equation then factors into two equations of degree 3 and 6. For instance, the block of 3 roots η_1, η_2, η_3 of the equation

$$x^3 + x^2 - 6x - 7 = 0$$

corresponds to the following sums :

$$\eta_1 = \omega + \omega^7 + \omega^8 + \omega^{11} + \omega^{12} + \omega^{18}$$

$$\eta_2 = \omega^2 + \omega^3 + \omega^5 + \omega^{14} + \omega^{16} + \omega^{17}$$

$$\eta_3 = \omega^4 + \omega^6 + \omega^9 + \omega^{10} + \omega^{13} + \omega^{15}$$

Each sequence of exponents in each of the sum above is indexed by the successive powers of a primitive root *mod.*19, such as $g = 2$ (because $2^{18} = 262144 = 1 + 19.13797$). The indexation (1, 7, 8, 11, 12, 18) of the powers of the ω that composes each of the above η_i corresponds to the 3 cycles of 6 powers of 2^3 *mod.*19 :

$$(2^3)^0 \equiv 1 mod(19)$$
$$(2^3)^1 \equiv 8 mod(19)$$
$$(2^3)^2 \equiv 7 mod(19)$$
$$(2^3)^3 \equiv 18 mod(19)$$
$$(2^3)^4 \equiv 11 mod(19)$$
$$(2^3)^5 \equiv 12 mod(19)$$

The exponents of the second sequence (2, 3, 5, 14, 16, 17) are given by the multiplication of the above sequence by $g \equiv 2\ mod(19)$:

$$1 \times 2 \equiv 2 mod(19)$$
$$7 \times 2 \equiv 14 mod(19)$$
$$8 \times 2 \equiv 16 mod(19)$$
$$11 \times 2 \equiv 3 mod(19)$$
$$12 \times 2 \equiv 5 mod(19)$$
$$18 \times 2 \equiv 17 mod(19)$$

Similarly, the multiplication by $g^2 \equiv 4\ mod(19)$ provides the exponents (4, 6, 9, 10, 13, 15) of the third sequence :

$$1 \times 4 \equiv 4 mod(19)$$
$$7 \times 4 \equiv 9 mod(19)$$
$$8 \times 4 \equiv 13 mod(19)$$
$$11 \times 4 \equiv 6 mod(19)$$
$$12 \times 4 \equiv 10 mod(19)$$
$$18 \times 4 \equiv 15 mod(19)$$

Annex 2. The number of values of functions and the resolution of equations by radicals

The quadratic equation

Let us start with the case of the quadratic equation on the field of rational numbers:

$$x^2 - c_1 x + c_2 = 0$$

The coefficients c_1 et c_2 are symetric functions of the roots x_1 et x_2. They are thus functions that take only a single value by permutations of the roots :

$$c_1 = x_1 + x_2 \ ; \ c_2 = x_1 x_2$$

The other way round, any function that take a single value can be expressed rationally in the number field to which the coefficients c_1 and c_2 belong. On the contrary,

$$x_1 - x_2$$

takes two values by permutation of the roots and is therefore not rationally known on $\mathbb{Q}$. One can look for the group of substitutions that leaves this function invariant. This group thus leaves also the root x_1 invariant. Thus, x_1 and $x_1 - x_2$ can be expressed rationally one with the other :

$$x_1 = \frac{c_1 + x_1 - x_2}{2}$$

Thus, if one adjoins to theinitial number field the number $x_1 - x_2$, one also gets the number x_1 : in the 19th century, functions of many values - or resolvents- were used for dealing with what would be nowadays understood as fields and fields extensions.

Let us now come back to the quadratic equation. The discriminant Δ is a function of a single value and can thus be expressed rationally with c_1 and c_2 :

$$\Delta = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1 x_2 = c_1^2 - 4c_2$$

The function $\sqrt{\Delta}$ is a two-valued function, as well as the roots x_1 et x_2 themselves. These functions can thus be expressed rationally one with the other by the well known fomulas that give the resolution by radicals of the quadratic equation.

The general cubic

In the case of the cubic

$$x^3 - c_1 x^2 + c_2 x - c_3 = 0$$

The resolution necessitates the determination of three functions x_1, x_2, x_3 that take three values by permutations, i.e., the determination of one function that take $3! = 6$ values. Let a_1, a_2, a_3 be three paramaters, the function $\xi = a_1x_1 + a_2x_2 + a_3x_3$ is precisely a function of $3! = 6$ values. Following Enrico Betti, such a function was called a "Galois resolvent" in the 19th century. If one expresses the roots of the cubic by radicals, then ξ will also be expressed by radicals, and reciprocally.

In a way, the problem of the algebraic resolution of equations thus consists in passing from three functions of a single value, c_1, c_2, c_3, to a function of six values, ξ.

Like in the case of the quadratic equation, the root of the discriminant provides a two-values function by which any two-valued function can be expressed rationally. Thus, to solve the cubic, one has to find a function of the roots, of which a certain power takes two values. Such is the case of the cube of the Lagrange resolvent :

$$\phi = x_1 + \omega^2 x_2 + \omega x_3$$

where ω is a primitive root of unity ($\omega^3 = 1$).

One can thus express ϕ rationally thanks to $\sqrt{\Delta}$:

$$\phi^3 = \frac{1}{2}(2c_1^3 - 9c_1c_2 + 27c_2 + 3\sqrt{(}-3\Delta))$$

from which one can deduce Cardano's famous formulas.

In general

To solve an equation of degree n necessitates the consideration of a resolvent function that takes $n!$ distinct values. It was through the consideration of all the substitutions leaving such a function invariant that Galois defined the group of an equation (that is, in modern parlance, the group that let stable the fields of the roots). One then has to investigate the groups of substitutions that leave invariant the factors into which the initial equation break when one adds some roots to the initial fields of coefficients.

A Galois resolvent is a function of $n!$ values. It is therefore invariant only for the trivial group, i.e., the group reduced to the permutation identity. On the opposite, a symetric function is invariant for all the substitutions of the symetric group. Adjoining roots to an equation, as we did aobve with $\sqrt{\Delta}$, implies breaking the Galois resolvent into factors. To each of these factors, one associate the substitution group that leaves it invariant. For instance, for $n = 4$,the following function can be understood as expressing the relations between the roots of an irreductible equation of the fourth degree :

$$\phi = x_1x_2 + x_3x_4$$

This function takes three values for all the $4! = 24$ permutations of $\Sigma(4)$:

$$x_1x_2 + x_3x_4, x_1x_3 + x_2x_4, x_1x_4 + x_2x_3$$

The group G associated to the function ϕ is composed of the eight substitutions that leave ϕ invariant :

$$G = I, (x_1x_2), (x_3x_4), (x_1x_2)(x_3x_4), (x_1x_3)(x_2x_4), (x_1x_4)(x_2x_3), (x_1x_3x_2x_4), (x_1x_4, x_2x_3).$$

References

[Adhémard, 1922] Adhémard, R. d. (1922). Nécrologie. Camille Jordan. Revue générale des sciences pures et appliquées, 3:65–66.

[Allegret, 1856] Allegret, A. (1856). Nouvelles recherches sur le caractère et les propriétés des équations algébriques solubles par radicaux. Comptes rendus hebdomadaires des séances de l'Académie des sciences, 43:275.

[Autonne, 1905] Autonne, L. (1905). Sur les formes mixtes. A. Rey, and Gauthier-Villars, Lyon, and Paris.

[Autonne, 1913] Autonne, L. (1913). Recension, de Séguier. Revue générale des sciences pures et appliquées.

[Betti, 1852] Betti, E. (1852). Sulla risoluzione delle equazioni algebriche. Annali di scienze matematiche e fisiche, 3:. 49–115.

[Bolza, 1891] Bolza, O. (1891). On the theory of substitution-groups and its applications to algebraic equations. American Journal of mathematics, 13:59–144.

[Borel et Drach, 1895] Borel, E. et Drach, J. (1895). Introduction à l'étude de la théorie des nombres et de l'algèbre supérieure. Nony, Paris.

[Boucard, 2011a] Boucard, J. (2011a). Louis Poinsot et la théorie de l'ordre : un chaînon manquant entre Gauss et Galois ? Revue d'histoire des mathématiques, 17(1):41–138.

[Boucard, 2011b] Boucard, J. (2011b). Un "rapprochement curieux de l'algèbre et de la théorie des nombres" : études sur l'utilisation des congruences en France de 1801 à 1850. Thèse de doctorat, Université Paris 6.

[Brechenmacher, 2006] Brechenmacher, F. (2006). Histoire du théorème de Jordan de la décomposition matricielle (1870-1930). Formes de représentations et méthodes de décompositions. Thèse de doctorat, Thèse de doctorat. Ecole des hautes études en sciences sociales.

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

[Brechenmacher, 2010] Brechenmacher, F. (2010). Une histoire de l'universalité des matrices mathématiques. Revue de Synthèse, 4:569–603.

[Brechenmacher, 2011] Brechenmacher, F. (2011). Self-portraits with Évariste Galois (and the shadow of Camille Jordan). http://hal.archives-ouvertes.fr/aut/Frederic+Brechenmacher/.

[Brechenmacher, 2012a] Brechenmacher, F. (2012a). Autour de pratiques algébriques de Poincaré : héritages de la réduction de jordan. http://hal.archives-ouvertes.fr/aut/Frederic+Brechenmacher/.

[Brechenmacher, 2012b] Brechenmacher, F. (2012b). Galois got his gun. à paraître.

[Brechenmacher, 2012c] Brechenmacher, F. (2012c). Linear groups in galois fields. a case study of tacit circulation of explicit knowledge. Oberwolfach Reports, 4-2012:48–54.

[Brechenmacher et Ehrhardt, 2010] Brechenmacher, F. et Ehrhardt, C. (2010). On the identities of algebra in the 19th century. Oberwolfach Reports, 7(1):24–31.

[Brian et al., 1893] Brian, T. et al., éditeurs (1893). The World's Columbian Exposition, Chicago, 1893. International Pub. Co, Philadelphia and Chicago.

[Briot et Bouquet, 1875] Briot, C. et Bouquet, C. (1875). Théorie des fonctions doublement périodiques et, en particulier, des fonctions elliptique. Paris, 2de ed. édition.

[Burnside, 1894] Burnside, W. (1894). Notes on the theory of groups of finite order. Proceedings of the London Mathematical Society,, 25:9–18.

[Burnside, 1896] Burnside, W. (1896). On the isomorphism of a group with itself,. Proceedings of the London Mathematical Society, 27:354–367.

[Burnside, 1897a] Burnside, W. (1897a). Note on the symmetric group. Proceedings of the London Mathematical Society, 28(119)129).

[Burnside, 1897b] Burnside, W. (1897b). Theory of Groups of Finite Order. Cambridge University Press, Cambridge.

[Burnside, 1899] Burnside, W. (1899). On the reduction of a linear substitution to the canonical form. Proceedings of the London Mathematical Society, 30:180–194.

[Cauchy, 1815] Cauchy, A.-L. (1815). Sur les fonctions qui ne peuvent obtenir que deux valeurs égales et de signes contraires par suite des transpositions opérées entre les variables qu'elles renferment. Journal de l'École polytechnique, 10:29–112.

[Cauchy, 1844] Cauchy, A.-L. (1844). Mémoire sur les arrangements que l'on peut former avec des lettres données, et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre.

[Cauchy, 1845] Cauchy, A.-L. (1845). Mémoire sur la résolution des équations linéaires symboliques, et sur les conséquences remarquables que cette résolution entraîne après elle dans la théorie des permutations Â».

[Cayley, 1878] Cayley, A. (1878). Desiderata and suggestions. n °1: The theory of groups. American journal of Mathematics, 1:50–52.

[Cole, 1892] Cole, F. N. (1892). Simple groups from order 201 to order 500. American journal of Mathematics, 14:378–388.

[Corry, 1996] Corry, L. (1996). Modern Algebra and the Rise of Mathematical Structures. Birkhäuser, Basel.

[Couturat, 1898] Couturat, L. (1898). Sur les rapports du nombre et de la grandeur. Revue de métaphysique et de morale, 6:422–447.

[Dahan Dalmedico, 1980] Dahan Dalmedico, A. (1980). Les travaux de cauchy sur les substitutions. étude de son approche du concept de groupe. Archive for History of Exact Sciences, 23:279–319.

[Despeyrous, 1861] Despeyrous, T. (1861). Mémoire sur la théorie générale des permutations. Journal de mathématiques pures et appliquées, (2) 6:417–439.

[Dickson, 1899] Dickson, L. E. (1899). Report on the recent progress in the theory of linear groups. Bulletin of the American Mathematical Society, (2) 6:13–27.

[Dickson, 1900] Dickson, L. E. (1900). Canonical form of a linear homogeneous substitution in a galois field. American Journal of Mathematics, 22:121–137.

[Dickson, 1901] Dickson, L. E. (1901). Linear groups with an exposition of the Galois field theory. Teubner, Leipzig.

[Dickson, 1902] Dickson, L. E. (1902). Canonical form of a linear homogeneous transformation in an arbitrary realm of rationality. American Journal of Mathematics, 24:101–108.

[Dickson, 1928] Dickson, L. E. (1924 /1928). A new theory of linear transformation and pairs of bilinear forms. Proceedings Congress Toronto, pages 361–363.

[Dieudonné, 1962] Dieudonné, J. (1962). Notes sur les travaux de Camille Jordan relatifs à l'algèbre linéaire et multilinéaire et la théorie des nombres. in [Jordan Œuvres, 3, p. V-XX].

[Dubreil, 1982] Dubreil, P. (1982). L'algèbre, en france, de 1900 à 1935. Cahier du Séminaire d'histoire des mathématiques de l'IHP, 3:69–81.

[Durand-Richard, 1996] Durand-Richard, M.-J. (1996). L'école algébrique anglaise : les conditions conceptuelles et institutionnelles d'un calcul symbolique comme fondement de la connaissance. In [GOLDSTEIN, GRAY, RITTER 1996], pages 445–477.

[Durand-Richard, 2008] Durand-Richard, M.-J., éditeur (2008). L'analogie dans la démarche scientifique. l'Harmattan.

[Dyck, 1882] Dyck, W. v. (1882). Gruppentheorische studien. Mathematische Annalen, 20:1–44.

[Ehrhardt, 2012] Ehrhardt, C. (2012). Itinéraire d'un texte mathématique Itinéraire d'un texte mathématique. Les réélaborations des écrits d'Evariste Galois au XIXe siècle. Hermann.

[Fenster et Schwermer, 2005] Fenster, D. D. et Schwermer, J. (2005). A delicate collaboration: Adrian albert and helmut hasse and the principal theorem in division algebras in the early 1930's. Archive for History of Exact Sciences, 59:349–379.

[Frei, 2007] Frei, G. (2007). The unpublished section eight: On the way to function fields over a finite field. In [Goldstein, Schappacher, Schwermer 2007], pages 159–198.

[Frobenius, 1879] Frobenius, G. (1879). Theorie der bilinearen formen mit ganzen coefficienten. Journal für die reine und angewandte Mathematik, 86:147–208.

[Frobenius, 1893] Frobenius, G. (1893). Ueber auflösbare gruppen. Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin, pages 337–345.

[Frobenius, 1895] Frobenius, G. (1895). Ueber endliche gruppen. Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin, pages 163–194.

[Frobenius, 1902] Frobenius, G. (1902). Ueber gruppen des graders p oder $p+1$. Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin, pages 351–369.

[Galois, 1830a] Galois, É. (1830a). Analyse d'un mémoire sur la résolution algébrique des équations. In [Galois 1846, p.395-396], volume 13, pages 171–172.

[Galois, 1830b] Galois, É. (1830b). Sur la théorie des nombres. In [Galois 1846, p.398-407], volume 13, pages 428–435.

[Galois, 1831a] Galois, É. (1831(?)a). Fragment d'un second Mémoire. Des équations primitives qui sont solubles par radicaux. In [Galois 1846], pages 434–444.

[Galois, 1831b] Galois, É. (1831b). Mémoire sur les conditions de résolubilité des équations par radicaux. In [Galois 1846], pages 417–433.

[Galois, 1832] Galois, É. (1832). Lettre du 29 mai 1832 à Auguste Chevalier. In [Galois 1846, p. 408-415]., volume septembre, pages 568–576.

[Galois, 1846] Galois, É. (1846). œuvres mathématiques. Journal de mathématiques pures et appliquées, 11:381–444.

[Galois, 1962] Galois, É. (1962). Ecrits et mémoires mathématiques. Gauthier-Villars, Paris.

[Gierster, 1881] Gierster, J. (1881). Die untergruppen der galois'schen gruppe der modulargleichungen für den fall eines primzahligen transformationsgrades. Mathematische Annalen, 18:319–365.

[Goldstein, 1999] Goldstein, C. (1999). Sur la question des méthodes quantitatives en histoire des mathématiques : le cas de la théorie des nombres en france (1870- 1914). Acta historiae rerum necnon technicarum, 3:187–214.

[Goldstein, 2011] Goldstein, C. (2011). Charles Hermite's Stroll through the Galois fields. Revue d'histoire des mathématiques, 17:135–152.

[Goldstein et al., 2007] Goldstein, C., Schappacher, N. et Schwermer, J., éditeurs (2007). The Shaping of Arithmetics after C. F. Gauss's Disquisitiones Arithmeticae. Springer, Berlin.

[Hawkins, 1972] Hawkins, T. (1972). Hypercomplex numbers, lie groups, and the creation of group representation theory. Archive for History of Exact Sciences,, 8:243–87.

[Hawkins, 1977] Hawkins, T. (1977). Weierstrass and the theory of matrices. Archive for History of Exact Sciences,, 17:119–163.

[Hawkins, 2008] Hawkins, T. (2008). Frobenius and the symbolical algebra of matrices. Archive for History of Exact Sciences, 62:23–57.

[Hermite, 1851] Hermite, C. (1851). Sur les fonctions algébriques. Comptes rendus hebdomadaires des séances de l'Académie des sciences, 32:458–461.

[Hermite, 1859] Hermite, C. (1859). Sur la théorie des équations modulaires et la résolution de l'équation du cinquième degré. Mallet-Bachelier, Paris.

[Hilbert, 1894] Hilbert, D. (1894). Grundzüge einer theorie des Galois'schen zahlkörpers. Göttingen Nachrichten, 224-236.

[Hölder, 1889] Hölder, O. (1889). Zurückführung einer beliebigen algebraischen gleichung auf eine kette von gleichungen. Mathematische Annalen, 34:26–56.

[Hölder, 1892] Hölder, O. (1892). Die einfachen gruppen im ersten und zweiten hundert der ordnungzahlen. Mathematische Annalen, 40:55–88.

[Hölder, 1893] Hölder, O. (1893). Die gruppen der ordnungen p^3, pq^2, pqr, p^4. Mathematische Annalen, 43:301–412.

[Hölder, 1895] Hölder, O. (1895). Bildung zusammengesetzter gruppen. Mathematische Annalen, 46:321–422.

[Jordan, 1860] Jordan, C. (1860). Sur le nombre des valeurs des fonctions. Thèses présentées à la Faculté des sciences de Paris par Camille Jordan, 1re thèse. Mallet-Bachelier, Paris.

[Jordan, 1864] Jordan, C. (1864). Mémoire sur les groupes des équations solubles par radicaux. Comptes rendus hebdomadaires des séances de l'Académie des sciences, 58:963–966.

[Jordan, 1867a] Jordan, C. (1867a). Lettre à M. Liouville sur la résolution algébrique des équations. Journal de mathématiques pures et appliquées, 12(2):105–108.

[Jordan, 1867b] Jordan, C. (1867b). Mémoire sur la résolution algébrique des équations. Comptes rendus hebdomadaires des séances de l'Académie des sciences, 64:269–272, 586–590, 1179–1183.

[Jordan, 1868] Jordan, C. (1868). Sur la résolution algébrique des équations primitives de degré p^2. Journal de mathématiques pures et appliquées, 32(2):111–135.

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

[Kiernan, 1971] Kiernan, M. (1971). The development of Galois theory from Lagrange to Artin. Archive for History of Exact Sciences, 8(1-2):40–152.

[Klein, 1884] Klein, F. (1884). Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade. Teubner, Leipzig.

[Klein, 1894] Klein, F. (1894). The Evanston Colloquium. Macmillan and Co, New York and London.

[Klein et Fricke, 1890] Klein, F. et Fricke, R. (1890). Vorlesungen über die Theorie der elliptischen Modulfunctionen, volume 1. B.G. Teubner, Leipzig.

[Kronecker, 1853] Kronecker, L. (1853). Ueber die algebraisch auflösbaren gleischungen. Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin, pages 365–374.

[Le Vavasseur, 1904] Le Vavasseur, R. (1904). Quelques considérations sur les groupes d'ordre fini et les groupes finis continus. Annales de l'université de Lyon and Gauthier-Villars, Lyon and Paris.

[Lexis, 1893] Lexis, éditeur (1893). Die deutschen Universitäten. Asher, Berlin.

[Mac Duffee, 1933] Mac Duffee, C. C. (1933). The Theory of Matrices. Chelsea, New-York.

[Maillet, 1892] Maillet, E. (1892). Thèses présentées à la Faculté des sciences de Paris. Recherches sur les substitutions et en particulier sur les groupes transitifs. Gauthier-Villars, Paris.

[Mathieu, 1860] Mathieu, É. (1860). Mémoire sur le nombre de valeurs que peut acquérir une fonction quand on y permute ses variables de toutes les manières possibles. Journal de mathématiques pures et appliquées, 5:9–42.

[Mathieu, 1861a] Mathieu, É. (1861a). Mémoire sur la résolution des équations dont le degré est une puissance d'un nombre premier. Annali di matematica pura ed applicata, 4:113–132.

[Mathieu, 1861b] Mathieu, É. (1861b). Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables. Journal de mathématiques pures et appliquées, (2) 6:241–323.

[Miller, 1898] Miller, G. A. (1898). Report on recent progress in the theory of the groups of a finite order. Bulletin of the American Mathematical Society, 2(5):227–249.

[Miller, 1902] Miller, G. A. (1902). Second report on recent progress in the theory of the groups of a finite order. Bulletin of the American Mathematical Society, (2) 9:106–123.

[Miller, 1903] Miller, G. A. (1903). Appreciative remarks on the theory of groups. The American Mathematical Monthly, 10:87–89.

[Miller, 1907] Miller, G. A. (1907). Third report on recent progress in the theory of the groups of a finite order. Bulletin of the American Mathematical Society, (2) 14:78–91, 124–133.

[Moore, 1893] Moore, E. H. (1893). A doubly-infinite system of simple groups. Bulletin of the New York Mathematical Society, III(3):73–78.

[Moore, 1894] Moore, E. H. (1894). The group of holoedric transformation into itself of a given group. Bulletin of the American Mathematical Society, I(3):61–66.

[Moore, 1895] Moore, E. H. (1895). Concerning Jordan's linear groups. Bulletin of the American Mathematical Society, II:33–43.

[Moore, 1896] Moore, E. H. (1896). A doubly-infinite system of simple groups. In Mathematical Papers Read at the International Mathematical Congress Held in Connection with the World's Columbian Exposition, pages 208–242. Chicago.

[Moore, 1897] Moore, E. H. (1897). The decomposition of modular systems of rank n in n variables. Bulletin of the American Mathematical Society, 10:372–380.

[Moore, 1898] Moore, E. H. (1898). An universal invariant for finite groups of linear substitutions: with application in the theory of the canonical form of a linear substitution of finite period. Mathematische Annalen, 50:213–219.

[Netto, 1882] Netto, E. (1882). Subtitutionentheorie und ihre Anwendung auf die Algebra„,. Teubner, Leipzig.

[Neumann, 2007] Neumann, O. (2007). The Disquisitiones Arithmeticae and the Theory of Equations. in [Goldstein, Schappacher, Schwermer, 2007].

[Neumann, 2006] Neumann, P. M. (2006). The concept of primitivity in group theory and the second memoir of galois. Archive for History of Exact Sciences, 60:379–429.

[Nicholson, 1993] Nicholson, J. (1993). The development and understanding of the concept of quotient group. Historia Mathematica, 20:68–88.

[Parshall, 1985] Parshall, K. H. (1985). J. H.M. Wedderburn and the structure theory of algebras. Archive for History of Exact Sciences, 32:223–349.

[Parshall, 2004] Parshall, K. H. (2004). Defining a mathematical research school: the case of algebra at the university of chicago, 1892-1945. Historia Mathematica, 31:263–278.

[Parshall et Rowe, 1994] Parshall, K. H. et Rowe, D. E. (1994). The Emergence of the American Mathematical Research Community (1876–1900): J.J. Sylvester, Felix Klein, and E.H. Moore. American Mathematical Society, Providence.

[Picard, 1890] Picard, É. (1890). Notice sur la vie et les travaux de Georges-Henri Halphen. Comptes rendus hebdomadaires des séances de l'Académie des sciences, 110:490.

[Picard, 1896] Picard, É. (1896). Traité d'analyse, volume III. Gauthier-Villars, Paris.

[Picard, 1922] Picard, É. (1922). Résumé des travaux mathématiques de Jordan. Comptes rendus hebdomadaires des séances de l'Académie des sciences, 174:210–211.

[Pierpont, 1900] Pierpont, J. (1899-1900). Galois' theory of algebraic equations. The Annals of Mathematics, (2) 1-2:113–143, 22–56.

[Puiseux, 1850] Puiseux, V. (1850). Recherches sur les fonctions algébriques. Journal de mathématiques pures et appliquées, 15:365–480.

[Radloff, 2002] Radloff, I. (2002). Évariste Galois: principles and appications. Historia Mathematica, 29:114–137.

[Schottenfels, 1899] Schottenfels, I. M. (1899). Two non isomorphic simple groups of the same order 20160. Annals of Mathematics, (2)1:147–152.

[Séguier, 1902] Séguier, J.-A. d. (1902). Sur la forme canonique des substitutions linéaires. Bulletin de la Société mathématique de France, 30:247–252.

[Séguier, 1904a] Séguier, J.-A. d. (1904a). Sur les groupes de mathieu. Comptes rendus hebdomadaires des séances de l'Académie des sciences, 137:37–38.

[Séguier, 1904b] Séguier, J.-A. d. (1904b). Théorie des groupes finis. Éléments de la théorie des groupes abstraits. Gauthier-Villars, Paris.

[Séguier, 1907] Séguier, J.-A. d. (1907). Sur la théorie des matrices. Comptes rendus hebdomadaires des séances de l'Académie des sciences, 145:1259–1260.

[Séguier, 1908] Séguier, J.-A. d. (1908). Sur la théorie des matrices. Bulletin de la société mathématique de France, 36:20–40.

[Serret, 1849] Serret, J.-A. (1849). Cours d'algèbre supérieure. Bachelier, Paris.

[Serret, 1859] Serret, J.-A. (1859). Sur les fonctions rationnelles linéaires prises suivant un module premier et sur les substitutions auxquelles conduit la considération de ces fonctions. Comptes rendus hebdomadaires des séances de l'Académie des sciences, 48:178–182.

[Serret, 1865] Serret, J.-A. (1865). Mémoire sur la théorie des congruences suivant un module premier et suivant une fonction modulaire irréductible. Comptes rendus hebdomadaires des séances de l'Académie des sciences, 61:973–975.

[Serret, 1866] Serret, J.-A. (1866). Cours d'algèbre supérieure. Gauthier-Villars, Paris, 3e éd. édition.

[Silvestri, 1979] Silvestri, R. (1979). Simple groups of finite order in the nineteenth century. Archive for History of Exact Sciences, 20:313–356.

[Turner, 2012] Turner, L. E. (2012). The Mittag-Leffler theorem: The origin, evolution and reception of a mathematical result, 1876–1884. Historia Mathematica.

[Vogt, 1895] Vogt, H. (1895). Leçons sur la résolution algébrique des équations. Nony, Paris.

[Waerden, 1985] Waerden, Bartel, v. d. (1985). A history of Algebra : from Al-Khwàrizmi to Emmy Noether. Springer Verlag, New York.

[Weber, 1893] Weber, H. (1893). Die allgemeinen grundlagen der galois'schen gleichungstheorie. Mathematische Annalen, 43:521–549.

[Weber, 1896] Weber, H. (1895-1896). Lehrbuch der Algebra, volume 2 vols. F. Vieweg und Sohn„ Braunschweig.

[Wiman, 1900] Wiman, A. (1900). Endlich gruppen linearer substitutionen. In Encyklopadie der mathematischenWissenschaften, volume I, chapitre art. IB3 f, pages 522–554. Teubner, Leipzig.