Revue d'Histoire des Mathématiques

Louis Poinsot et la théorie de l'ordre : un chaînon manquant entre Gauss et Galois ?

Jenny Boucard

Tome 17 Fascicule 1 2011

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Publiée avec le concours du Centre national de la recherche scientifique

REVUE D'HISTOIRE DES MATHÉMATIQUES

Secrétariat :
Nathalie Christiaën
Société Mathématique de France
Institut Henri Poincaré
11, rue Pierre et Marie Curie, 75231 Paris Cedex 05
Tél. : (33) 01 44 27 67 99 / Fax : (33) 01 40 46 90 96
Mél : revues@smf.ens.fr / URL : http//smf.emath.fr/

Périodicité : La *Revue* publie deux fascicules par an, de 150 pages chacun environ.

Tarifs : Prix public Europe : 67 €; prix public hors Europe : 76 €;
prix au numéro : 38 €.
Des conditions spéciales sont accordées aux membres de la SMF.

Diffusion : SMF, Maison de la SMF, Case 916 - Luminy, 13288 Marseille Cedex 9
Hindustan Book Agency, O-131, The Shopping Mall, Arjun Marg, DLF Phase 1, Gurgaon 122002, Haryana, Inde
AMS, P.O. Box 6248, Providence, Rhode Island 02940 USA

Maquette couverture : Armelle Stosskopf

Revue d'histoire des mathématiques
17 (2011), p. 41–138

LOUIS POINSOT ET LA THÉORIE DE L'ORDRE : UN CHAÎNON MANQUANT ENTRE GAUSS ET GALOIS ?

JENNY BOUCARD

RÉSUMÉ. — Louis Poinsot est un mathématicien surtout connu pour ses travaux en mécanique et géométrie. Il est pourtant cité à plusieurs reprises dans des textes du XIX^{e} siècle comme mathématicien ayant joué un rôle dans l'histoire de la théorie des nombres et de l'algèbre. Dans cet article, nous étudions les travaux de Poinsot dans ces deux domaines à partir de ses publications et d'un manuscrit sur la théorie des permutations et nous essayons de montrer en quoi un examen du travail de Poinsot peut éclairer la période séparant les *Disquisitiones Arithmeticae* de Gauss de l'œuvre de Galois.

ABSTRACT (Louis Poinsot and theory of order : A missing link between Gauss and Galois ?)

The mathematician Louis Poinsot is principally known today for his contributions to mechanics and Geometry. In texts from the nineteenth century, however, he is frequently mentioned for his influence in the development of number theory and algebra. In this paper, we study Poinsot's work in these two domains through his publications and a manuscript of his on the theory of permutations. We then discuss how such a study may help to understand the transition from Gauss's *Disquisitiones Arithmeticae* to Galois's work.

Texte reçu le 22 octobre 2010, révisé le 7 mars 2011, accepté le 9 mars 2011.

J. BOUCARD, Institut mathématique de Jussieu.
Courrier électronique : jenny.boucard@gmail.com

Classification mathématique par sujets (2000) : 01A55.

Mots clefs : Poinsot, Gauss, Galois, *Disquisitiones Arithmeticae*, histoire de la théorie des nombres, histoire de l'algèbre, cyclotomie, racine primitive, congruence, permutations, polygone, théorie de l'ordre.

Key words and phrases. — Poinsot, Gauss, Galois, *Disquisitiones Arithmeticae*, history of number theory, history of algebra, cyclotomy, congruence, permutations, polygon, theory of order.

INTRODUCTION

En 1801 paraît un ouvrage de théorie des nombres écrit par un jeune mathématicien de 24 ans : ce sont les *Disquisitiones Arithmeticae* de Carl Friedrich Gauss (1777-1855) qui vont permettre à cette partie des mathématiques d'être considérée comme une discipline à part entière [1]. Au XIX^{e} siècle, des mathématiciens — comme Augustin Louis Cauchy (1789–1857), Carl Gustav Jakob Jacobi (1804–1851) ou encore Johann Peter Gustav Lejeune-Dirichlet (1805–1859) — fondent leurs travaux sur une des sept sections [2] des *Disquisitiones Arithmeticae* pour approfondir les théories des formes et des résidus quadratiques, des équations algébriques, voire des fonctions elliptiques, à partir d'outils de théorie des nombres, mais également d'algèbre et d'analyse.

L'objectif de cet article est d'analyser les travaux en théorie des nombres et en algèbre d'un de ces mathématiciens : Louis Poinsot (1777 - 1859). Ce savant [3] occupe plusieurs fonctions au sein de la communauté scientifique française au début du XIX^{e} siècle : professeur à l'École polytechnique et inspecteur général de l'Université dès 1809, puis Inspecteur des

---

1 On pourra se reporter à [Neumann 1979–1980], [Neumann 2005] et [Goldstein et al. 2007] pour comprendre les conséquences de cet ouvrage sur la théorie des nombres et ses liens avec les autres domaines des mathématiques ainsi que l'influence qu'il a eue dans différentes communautés mathématiques.

2 Les quatre premières sections des *Disquisitiones Arithmeticae* traitent des congruences du premier et du second degré, avec notamment une étude sur les résidus quadratiques. La section V est une théorie des formes quadratiques. Gauss présente des tests de primalité ainsi que des méthodes pour décomposer des fractions et pour résoudre les congruences de la forme $x^2 \equiv A$ modulo un nombre entier m dans la section VI. Dans la section VII, qui a grandement participé à la diffusion rapide du traité, Gauss obtient les conditions de constructibilité du polygone régulier à n côtés à la règle et au compas et donne une méthode générale pour la résolution par radicaux des équations binômes, qui est détaillée à partir de la page 55. Gauss prévoyait également d'ajouter une huitième section traitant des congruences d'ordre supérieur à 2, mais celle-ci n'a pas été publiée par manque de temps et de place. Néanmoins, Gauss s'y réfère régulièrement dans ses recherches.

3 Il existe très peu d'informations sur la vie de Poinsot, que ce soit dans les archives ou dans les correspondances. Joseph Bertrand (1822–1900) nous livre quelques anecdotes de la vie de Poinsot dans un éloge historique [Bertrand 1890] mais il est difficile d'en tirer des conclusions totalement fiables.

études [4] en 1815, élu à l'Institut en 1813 dans la classe des mathématiques à la mort de Joseph-Louis Lagrange (1736–1813), collaborateur au *Bulletin de Férussac* à partir de 1824. Dans ses publications, peu nombreuses [5], Poinsot aborde essentiellement la mécanique, la géométrie de situation et la théorie des nombres. C'est surtout pour les deux premières qu'il est très connu : ses *Éléments de statique* connaîtront douze éditions par exemple [6] ; son premier mémoire de géométrie, publié en 1809, sur la théorie des polygones et des polyèdres, reçoit également des éloges, et est notamment repris par Cauchy.

Pourquoi étudier les travaux de Poinsot en algèbre et théorie des nombres ? Il semble, à première vue, faire pâle figure devant les Gauss, Cauchy, ou encore Niels Henrik Abel (1802–1829) que l'on retrouve dans toutes les histoires des mathématiques. Au cours de nos recherches, nous avons rencontré plusieurs références à ce mathématicien qui laissent à penser que ses travaux en algèbre et théorie des nombres ne sont pourtant pas passés inaperçus au XIX^e siècle. Par exemple, en 1843, Joseph Liouville (1809–1882) fait référence à l'analyse faite par Poinsot en 1808 du *Traité des équations numériques de tous les degrés* de Lagrange dans le cadre d'un conflit avec Guillaume Libri (1803–1869) [7] :

---

4 Voir [Caplat 1986, p. 557]. Il sera mis à la retraite le 22 septembre 1824 en tant qu'inspecteur général à l'avènement de Charles X. En 1840, il intégrera le Conseil royal de l'Université, puis sera chargé de la préparation de la réforme des études scientifiques en 1845, par le ministre Salvandy.

5 Dans [Crosland 1992 (2002, p. 206], l'auteur commente ce fait en même temps que l'élection de Poinsot à l'Académie en remplacement de Lagrange en 1813 : « Poinsot lived on until 1859, proving to be one of the least productive membres of the Academy in the 1820s, 30s, 40s and 50s ». À côté de ses publications, la Bibliothèque de l'Institut de France possède 18 portefeuilles contenant des manuscrits de Poinsot. On y trouve des brouillons et textes de Poinsot relatifs à la mécanique, à l'enseignement, à l'algèbre et à la théorie des nombres. Dans la partie concernant la théorie des nombres, beaucoup de feuillets sont des réflexions sur la théorie des équations et des congruences ainsi que des recherches sur le dernier théorème de Fermat. Nous étudierons d'ailleurs dans cet article un mémoire sur la théorie des permutations trouvé dans ces manuscrits, mais qui n'a jamais été publié.

6 La thèse de Patrice Bailhache est d'ailleurs une analyse de certains travaux de Poinsot en mécanique et statique. Voir [Poinsot & Bailhache 1975].

7 Bruno Belhoste et Jesper Lützen détaillent les relations *détestables* entre Liouville et Libri — et en particulier le conflit dont il est question ici — dans [Belhoste & Lützen 1984]. Ce n'était pas le premier heurt entre les deux hommes puisque dès 1838,

> Pour m'épargner la rédaction que j'aurais d'ailleurs beaucoup moins bien faite, je viens de copier le passage de la préface de M. Poinsot, publiée dès 1808 dans le *Magasin encyclopédique*. M. Poinsot avait spécialement en vue les équations binômes, mais le raisonnement est général, et, pour qui comprend bien cette théorie, il devait l'être. Aussi, c'est le cas de dire que la démonstration du théorème se trouvait d'*avance* dans l'article de M. Poinsot. [8]

On retrouve également d'autres références à Poinsot jusqu'à la fin du XIX[e] siècle. Dans son *Report on the theory of numbers*, Smith inclut Poinsot dans une liste des quelques savants ayant développé le domaine de la théorie des nombres à partir de l'étude de l'ouvrage de Gauss :

> The arithmetical memoirs of Gauss himself, subsequent to the publication of the 'Disquisitiones Arithmeticae'; those of Cauchy, Jacobi, Lejeune Dirichlet, Eisenstein, Poinsot, and, among still living mathematicians, of MM. Kummer, Kronecker, and Hermite, have served to simplify as well as to extend the science. [Smith 1859–1865, p. 38]

Liouville a dénoncé à l'Académie des erreurs importantes contenues dans un travail de Libri. Dans le cas présent, le litige s'est produit quelques semaines après l'élection de Libri au Collège de France — élection dont il était finalement le seul candidat après les démissions de Cauchy et Liouville. Le 14 août 1843, Liouville soumet à l'Académie un rapport sur un mémoire de Charles Hermite (1822–1901) relatif à la division des fonctions abéliennes. Hermite y développe une méthode analogue à celle utilisée par Abel en 1827 pour déterminer la division des intégrales elliptiques. À la fin de l'exposé, Libri prend la parole pour affirmer que c'est lui qui a démontré pour la première fois la division en parties égales de la lemniscate, et donc également résolu les équations relatives aux fonctions elliptiques. Une semaine plus tard, Liouville répond aux réclamations de Libri. Ce dernier base sa requête sur un théorème qu'il a énoncé sans démonstration devant l'Académie en 1825 — mais qui n'a été publié qu'en 1833 — et qu'il a développé en 1830 seulement. On trouvera les détails de l'argumentation de Liouville dans les *Comptes rendus hebdomadaires des séances de l'Académie des Sciences* de l'année 1843 (tome 17, pages 327–334). Liouville formule correctement le résultat en question ainsi : « Quand les racines d'une équation algébrique peuvent être *toutes* rangées en cercle de telle manière que chacune d'elles se déduise de la précédente et engendre la suivante par une seule et même opération rationnelle, cette équation est nécessairement résoluble à l'aide de radicaux. », résultat dont il paraphrase ensuite la démonstration donnée par Poinsot en 1808. Toujours dans le cadre de ce conflit, Liouville annonce également son intention de publier les écrits d'Évariste Galois (1811–1832) lors de la séance du 4 septembre 1843. Pour une étude du contexte de cette publication, voir [Ehrhardt 2010].

8 *Comptes rendus hebdomadaires des séances de l'Académie des Sciences*, tome 17, année 1843, p. 332.

Poinsot est aussi cité dans *Les mathématiques en Portugal*[9], de Rodolphe Guimarães, à l'occasion d'un aperçu des sciences mathématiques de la première moitié du XIX^e siècle :

> Nous sommes, donc, à la moitié du XIX^e siècle : avec une théorie des nombres, dûe à Gauss, les groupant en classes moyennant les équations de congruence, qui s'élève jusqu'à la notion de nombre complexe ; avec les élégantes investigations de Poinsot, qui font dépendre l'Arithmétique et l'Algèbre de l'ordre et de la combinaison ; avec une Algèbre qui, en délaissant les fâcheuses et peu fécondes élucubrations que l'on devait appliquer dans la pratique, se renferme avec les théorèmes de Sturm et Cauchy, pour suivre une autre direction, soumise au concept de groupe des *substitutions* [...] [Guimarães 1900, p. 7]

Ces deux auteurs prêtent donc à Poinsot une place surprenante dans l'évolution de l'algèbre et la théorie des nombres au XIX^e siècle. La première citation est issue d'une source secondaire importante pour l'histoire de la théorie des nombres tandis que la seconde vient d'un ouvrage certes beaucoup moins connu, mais qui, à la fin du XIX^e siècle, place Poinsot parmi les quelques mathématiciens marquants de l'évolution de l'arithmétique et de l'algèbre. Nous voulons donc essayer de comprendre pourquoi Poinsot semble être pour certains savants un chaînon non négligeable dans le développement de ces deux domaines.

Il existe cinq publications de Poinsot relatives à l'algèbre et la théorie des nombres :

- un commentaire publié dans le *Moniteur universel* du 21 mars 1807 à l'occasion de la traduction française par Poullet - Delisle des *Disquisitiones Arithméticae* de Gauss ;
- un commentaire du *Traité des équations numériques de tous les degrés* de Lagrange paru en 1808 dans le *Magasin encyclopédique* ;
- un *Extrait de quelques recherches nouvelles sur l'algèbre et la théorie des nombres* lu en 1817 à l'Académie des Sciences puis publié en 1818 dans les *Mémoires de la classe des sciences mathématiques et physiques de l'Institut de France* ;

---

9 La première édition de cet ouvrage a été publiée en 1900, à l'occasion de l'Exposition Universelle de Paris.

– un *Mémoire sur l'application de l'algèbre à la théorie des nombres* publié en 1820 dans le *Journal de l'École polytechnique* ;

– des *Réflexions sur les principes fondamentaux de la théorie des nombres*, publiées dans le *Journal de Mathématiques Pures et Appliquées* en 1845.

Nous étudierons ici les textes de 1808, 1818, 1820, ainsi qu'un des manuscrits de Poinsot dans lequel il développe ses idées sur les permutations dans le cadre de la théorie algébrique des équations. Le commentaire sur les *Disquisitiones Arithmeticae* montre surtout que Poinsot est un des lecteurs parisiens de l'ouvrage dès le tout début du XIX^e siècle, comme Lagrange, Adrien-Marie Legendre (1752–1833) ou Sophie Germain (1776–1831), et un promoteur de sa lecture dans les cercles lettrés. D'autre part le mémoire publié en 1845, plus tardif, consiste en une synthèse approfondie sur plusieurs résultats de théorie des nombres et Poinsot n'y présente pas d'idées novatrices par rapport à ses travaux précédents [10]. Dans l'ensemble de ses textes, Poinsot lie la théorie des nombres, l'algèbre et la géométrie autour d'une notion centrale : la théorie de l'*ordre*. Notre objectif est donc d'essayer de comprendre ce que signifie cette idée, son origine et en quoi la façon de voir de Poinsot a pu avoir une influence sur l'histoire de la théorie des nombres et de l'algèbre. En mettant en avant cette idée, Poinsot dégage explicitement la théorie des équations de la recherche des valeurs numériques des solutions pour se concentrer sur relations entre racines. On peut donc en particulier se demander quel rôle son travail joue dans le développement qui conduit du point de vue de Gauss à celui de Galois.

1. 1808 : POINSOT ET LA THÉORIE GÉNÉRALE DES ÉQUATIONS

La deuxième édition [11] du *Traité de la résolution des équations numériques de tous les degrés* de Lagrange est publiée en 1808. Par rapport à la première édition, Lagrange a ajouté quatorze notes relatives à la *théorie des équations*

[10] Poinsot y développe notamment la théorie des équations binômes, et expose de nouvelles démonstrations de résultats de théorie des nombres comme les théorèmes de Fermat et de Wilson. Néanmoins, en 1845, le point de vue général de Poinsot sur l'algèbre et la théorie des nombres notamment est moins innovant qu'en 1820.

[11] La première édition de cet ouvrage a été publiée en 1798.

algébriques. Poinsot rédige un commentaire sur l'ouvrage, publié en 1808 dans le *Magasin encyclopédique, ou Journal des sciences, des lettres et des arts*[12]. Ce commentaire sera d'ailleurs intégré au début de la troisième édition posthume publiée en 1826 du *Traité* de Lagrange, vraisemblablement par Poinsot[13], avec une note indiquant qu'il « a reçu l'approbation de M. Lagrange ». Nous étudions ici des extraits de l'analyse de Poinsot relatifs à la définition de l'algèbre, la résolution algébrique des équations puis au cas particulier de la résolution algébrique des équations binômes.

1.1. *Une première définition de l'algèbre*

Au début de son analyse, Poinsot donne une définition de l'algèbre, domaine alors souvent assimilé à la théorie des équations[14] :

> D'abord si l'on jette un coup d'œil général sur l'Algèbre, on voit que cette science, abstraction faite des opérations ordinaires (au nombre desquelles on peut compter l'élimination), se partage naturellement en trois articles principaux. 1°. La théorie générale des équations, c'est-à-dire l'ensemble des propriétés qui leur sont communes à toutes. 2°. Leur résolution générale, qui consiste à trouver une expression composée des coefficiens de la proposée, et qui, mise au lieu de l'inconnue, satisfasse identiquement à cette équation, et que tout s'y détruise par la seule opposition des signes. 3°. La résolution des équations numériques, où il suffit de trouver des valeurs particulières qui satisfassent d'une manière aussi approchée qu'on le voudra, à une équation dont tous les coefficiens sont actuellement connus et donnés en nombre. [Poinsot 1808, p. 345–346]

Dans l'introduction de son *Traité*, Lagrange expose un point de vue légèrement différent : il divise également la théorie des équations en trois parties mais, pour lui, la résolution numérique des équations n'est pas à proprement dit une partie de l'algèbre :

---

12 Voir [Poinsot 1808].

13 Poinsot lui-même semble être à l'origine de cette édition. En effet, l'ouvrage se termine par une note de Poinsot commentant une correction faite par Lagrange. De plus, seuls les noms de Lagrange et Poinsot apparaissent dans la présentation de l'ouvrage.

14 Par exemple, dans [Sinaceur 1991, p. 51], l'auteur indique que cette définition restera la plus courante jusqu'à la fin du XIX^{e} siècle.

> Il faut bien distinguer la résolution des équations numériques de ce qu'on appelle en Algèbre la résolution générale des équations. La première est, à proprement parler, une opération arithmétique, fondée à la vérité sur les principes généraux de la théorie des équations, mais dont les résultats ne sont que des nombres, où l'on ne reconnaît plus les premiers nombres qui ont servi d'éléments, et qui ne conservent aucune trace des différentes opérations particulières qui les ont produits.
>
> [...] Aussi conviendrait-il de donner dans l'Arithmétique les règles de la résolution des équations numériques, sauf à renvoyer à l'Algèbre la démonstration de celles qui dépendent de la théorie générale des équations. [Lagrange 1808, p. 13-14]

La définition de l'algèbre qu'il donne ensuite est plus générale que celle de Poinsot :

> L'Algèbre plane pour ainsi dire également sur l'Arithmétique et sur la Géométrie ; son objet n'est pas de trouver les valeurs mêmes des quantités recherchées ; mais le système d'opérations à faire sur les quantités données pour en déduire les valeurs des quantités qu'on cherche, d'après les conditions du problème. Le tableau de ces opérations représentées par les caractères algébriques, est ce qu'on nomme en Algèbre une formule ; et lorsqu'une quantité dépend d'autres quantités, de manière qu'elle peut être exprimée par une formule qui contient ces quantités, on dit alors qu'elle est une fonction de ces mêmes quantités.
>
> L'Algèbre, prise dans le sens le plus étendu, est l'art de déterminer les inconnues par des fonctions des quantités connues, ou qu'on regarde comme connues ; et la résolution générale des équations consiste à trouver pour toutes les équations d'un même degré, les fonctions des coefficiens de ces équations qui peuvent en représenter toutes les racines. [Lagrange 1808, p. 14-15]

En 1808, pour Lagrange, Poinsot et certainement la plupart des mathématiciens, l'algèbre est donc considérée comme une science où l'on doit déterminer des inconnues en fonction de valeurs données. Au cours de notre étude, nous allons voir cette notion évoluer sensiblement chez Poinsot.

Dans son commentaire, Poinsot donne ensuite une présentation succincte des méthodes développées par Lagrange dans le cadre de la résolution numérique des équations dans les cinq premières pages de son

analyse. Les neuf pages restantes sont consacrées au résumé et commentaire des réflexions de Lagrange et de Gauss sur « le problème si fameux de la résolution générale des équations » [Poinsot 1808, p. 359]. Poinsot commence par citer des mathématiciens ayant produit des travaux dans le cadre de cette théorie, en insistant sur les écrits de Vandermonde et de Lagrange. Il donne notamment les idées générales développées par Lagrange pour la résolution générale des équations, ainsi que les principaux points du raisonnement de Gauss pour la résolution générale des équations binômes. Nous allons dans chacun de ces deux cas résumer les raisonnements développés par Lagrange et Gauss dans leurs œuvres avant de considérer l'analyse qu'en fait Poinsot.

1.2. *La théorie générale des équations*

1.2.1. *Les Réflexions sur la résolution algébrique des équations de Lagrange (1770)*

En 1770 paraît l'ouvrage *Réflexions sur la résolution algébrique des équations* de Lagrange [15]. Son objectif est annoncé dès l'introduction de son mémoire :

> Je me propose dans ce Mémoire d'examiner les différentes méthodes que l'on a trouvées jusqu'à présent pour la résolution algébrique des équations, de les réduire à des principes généraux et de faire voir *a priori* pourquoi ces méthodes réussissent pour le troisième et le quatrième degré, et sont en défaut pour les degrés ultérieurs.
>
> Cet examen aura un double avantage : d'un côté il servira à répandre une plus grande lumière sur les résolutions connues du troisième et du quatrième degré ; de l'autre il sera utile à ceux qui voudront s'occuper de la résolution des degrés supérieurs, en leur fournissant différentes vues pour cet objet et en leur épargnant surtout un grand nombre de pas et de tentatives inutiles. [Lagrange 1770a, p. 206-207]

---

[15] On pourra notamment se reporter à [Neumann 2007a], [Neumann 2007b], [Hamburg 1976/77] et [Houzel 2002, chap. IV et V] pour une analyse de certains passages de ce mémoire. Lagrange n'est pas le seul mathématicien à avoir publié un travail sur la résolution algébrique des équations à cette période. Edward Waring (1736–1798) fait publier en 1770 les *Meditationes Algebricae* et Alexandre-Théophile Vandermonde (1735–1796), dans son *Mémoire sur la résolution des équations* paru en 1774, résume les différentes questions à résoudre pour la résolution générale des équations et propose une méthode de résolution pour l'équation binôme de degré 11.

L'originalité de ce travail consiste en ce qu'il ne contient pas une suite de nouveaux résultats et méthodes ; il réside en un bilan critique des méthodes présentées jusque là pour les équations que l'on sait résoudre afin de dégager des principes communs pour guider les recherches ultérieures sur la théorie algébrique des équations. Les deux premières sections contiennent une analyse des méthodes connues pour la résolution des équations générales des troisième et quatrième degrés. Lagrange y observe que les méthodes déjà connues s'appuient sur la résolution d'une équation auxiliaire, appelée dans un premier temps *réduite*, et que l'on peut ramener à un degré inférieur à celui de l'équation proposée. La troisième section englobe des réflexions sur la résolution des équations de degré supérieur à 4. Dès le début, Lagrange revient entre autres sur la méthode exposée par Étienne Bezout (1730–1783). Dans ses travaux sur la théorie algébrique des équations [16], ce dernier obtient une *réduite* du cent-vingtième degré pour l'équation du cinquième degré, qui équivaut à une équation du vingt-quatrième degré. Selon lui, sa difficulté ne doit pas dépasser celle d'équations de degré inférieur à 5. Lagrange exprime son scepticisme à ce sujet :

> Mais cette conclusion, si j'ose le dire, me paraît un peu forcée, car j'avoue que je ne vois pas bien clairement ce qui pourrait empêcher que l'expression des racines de l'équation du vingt-quatrième degré dont il s'agit ne contint encore des radicaux cinquièmes ; du moins il n'est pas démontré que cela ne puisse absolument avoir lieu ; ainsi il pourrait bien arriver que cette équation du vingt-quatrième degré renfermât encore toutes les difficultés de l'équation proposée du cinquième degré ; auquel cas, après avoir trouvé cette équation par des calculs très-pénibles, on n'en serait que plus éloigné de la résolution de l'équation proposée.
>
> [...] Il serait donc fort à souhaiter que l'on pût juger *a priori* du succès que l'on peut se promettre dans l'application de ces méthodes aux degrés supérieurs au quatrième [...] [Lagrange 1770a, p. 307]

Lagrange doute donc de pouvoir arriver à la résolution algébrique des équations de degré supérieur à 4 à partir de sa méthode. Pour introduire la quatrième section, intitulée « Conclusion des réflexions précédentes, avec

16 Voir [Bezout 1764] et [Bezout 1765]. On renvoie en particulier à [Alfonsi 2005] pour une étude des travaux de Bezout.

quelques remarques générales sur la transformation des équations, et sur leur réduction ou abaissement à un moindre degré » [Lagrange 1770a, p. 355], Lagrange résume les principes généraux aboutissant à une méthode de résolution *a priori* :

> On a dû voir par l'analyse que nous venons de donner des principales méthodes connues pour la résolution des équations, que ces méthodes se réduisent toutes à un même principe général, savoir à trouver des fonctions des racines de l'équation proposée, lesquelles soient telles : 1° que l'équation ou les équations par lesquelles elles seront données, c'est-à-dire dont elles seront les racines (équations qu'on nomme communément les *réduites*), se trouvent d'un degré moindre que celui de la proposée, ou soient au moins décomposables en d'autres équations d'un degré moindre que celui-là ; 2° que l'on puisse en déduire aisément les valeurs des racines cherchées.
>
> L'art de résoudre les équations consiste donc à découvrir des fonctions des racines, qui aient les propriétés que nous venons d'énoncer ; mais est-il toujours possible de trouver de telles fonctions, pour les équations d'un degré quelconque, c'est-à-dire pour tel nombre de racines qu'on voudra ? C'est sur quoi il paraît très-difficile de se prononcer en général. [Lagrange 1770a, art. 86]

Voyons maintenant sur quels principes s'appuient la formation des équations auxiliaires [17]. Elles doivent être invariables sous toute permutation des racines de l'équation proposée [18]. Si l'équation initiale est de degré n, alors l'équation auxiliaire est de degré $n!$. Afin d'abaisser le degré de ces équations auxiliaires, Lagrange met en avant l'importance des racines de l'unité qui ont une particularité intéressante du point de vue des permutations : si l'on considère l'équation $x^n - 1 = 0$, il existe toujours une racine r de cette équation telle que ses différentes puissances r^i (pour i allant de 1 à n) donnent l'ensemble des solutions de l'équation $x^n - 1 = 0$, c'est-à-dire l'ensemble des racines n^e de l'unité.

---

17 On trouve dans les travaux de Lagrange les termes *réduite* et *résolvante*. La *réduite* désigne une équation auxiliaire formée à partir des coefficients de l'équation initiale et dont les racines sont des fonctions rationnelles des racines de l'équation proposée. La *résolvante* est une équation, ou un ensemble d'équations, donnant l'expression des racines de la *réduite* en fonction des racines de l'équation initiale. Selon [Vuillemin 1962, p. 79], Lagrange confond parfois l'utilisation de ces deux termes.

18 Cela vient du fait que les coefficients d'une équation sont des fonctions symétriques de ses racines.

Ainsi, remplacer dans une expression r par une de ses puissances induit une permutation circulaire des différentes racines. Utiliser les racines de l'unité pour former les équations auxiliaires permet ainsi d'abaisser leur degré.

Les travaux de Lagrange mettent en avant non seulement les problèmes à résoudre pour la résolution algébrique des équations mais également l'importance des permutations et des racines de l'unité en tant qu'outils de cette résolution.

1.2.2. *L'analyse de Poinsot*

Dans le commentaire de Poinsot relatif à la théorie générale des équations, on distingue deux parties : il commence par résumer quelques découvertes concernant la théorie générale des équations, avant de s'intéresser au cas particulier des équations pour lesquelles on connaît des relations entre les racines.

Après avoir donné une petite chronologie du sujet de Cardan à Bezout, Poinsot conclut :

> Toutes ces méthodes dépendent de l'exécution actuelle d'un calcul, et l'on n'y voit point qu'on doive arriver, à moins qu'on n'arrive effectivement : or, par la nature du problème, la longueur des calculs croît avec une telle rapidité, que la question ne peut plus être aujourd'hui de chercher la formule, mais simplement de prédire la suite des opérations qui y conduirait à coup sûr. Aucune de ces méthodes ne peut donc satisfaire l'esprit, et c'est à des idées plus hautes sur la nature des équations qu'il faut s'élever à présent pour découvrir s'il y a ou non une route certaine qui ferait parvenir à leur résolution générale. [Poinsot 1808, p. 360]

Poinsot donne ici les objectifs que doivent se fixer, selon lui, les mathématiciens travaillant sur la théorie générale des équations : il ne faut plus chercher une formule explicite donnant les solutions de l'équation générale de degré n en fonction de ses coefficients — comme cela a été fait pour les équations de degrés 2, 3 et 4 — mais plutôt trouver une méthode pour démontrer qu'une équation est résoluble sans pouvoir nécessairement développer des calculs explicites. Ces idées sont déjà mises en

avant par Lagrange dès 1770, qui prône une méthode permettant de déterminer *a priori* afin d'éviter les calculs « pénibles » [19]. On retrouve d'ailleurs un commentaire [20] très semblable dans la préface écrite par Galois des années plus tard pour ses mémoires : « Le moment arrivera où les spéculations des analystes ne trouveront plus ni le temps ni la place de se produire ; à tel point qu'il faudra se contenter de les avoir prévues » [Galois 1908, p. 25-26].

Pour Poinsot et Galois, il faut donc *prévoir* ou *prédire* les calculs, sans les effectuer. Ainsi, en analysant les travaux de Lagrange sur la théorie des équations, Poinsot met en avant une idée générale sur la théorie des équations qui sera suivie quelques années plus tard par le jeune Galois : il faut adopter des raisonnements dont les fondements ne sont pas dans les calculs mais dans « des idées plus hautes sur la nature des équations ».

Poinsot présente ensuite les idées générales contenues dans les travaux de Vandermonde et Lagrange sur la théorie générale des équations. Il insiste notamment sur le lien mis en avant par Lagrange entre la résolution générale des équations et la théorie des permutations, ainsi que sur l'intérêt de considérer les racines de l'unité :

> Car, il est clair actuellement que le problème peut revenir à celui-ci : trouver des fonctions des racines qui soient telles d'abord qu'on en puisse aisément

---

19 Voir l'extrait cité plus haut, page 50.

20 Ce passage du texte de Galois est notamment commenté dans la thèse de Caroline Ehrhardt : [Ehrhardt 2007, p. 92-93]. On peut d'ailleurs également citer un passage du *Discours Préliminaire* où Galois suit la même idée :

> Il existe, en effet, pour ces sortes d'équations, un certain ordre de considérations Métaphysiques qui planent sur tous les calculs, et qui souvent les rendent inutiles. Je citerai, par exemple, les équations qui donnent la division des fonctions Elliptiques et que le célèbre Abel a résolues. Ce n'est certainement pas d'après leur forme numérique que ce géomètre y est parvenu. Tout ce qui fait la beauté et à la fois la difficulté de cette théorie, c'est qu'on a sans cesse à indiquer la marche des calculs et à prévoir les résultats sans jamais pouvoir les effectuer. [Galois 1908, p.22]

dégager ces racines, et en second lieu, qui ne dépendent que d'équations inférieures à la proposée dont les coefficients soient connus ou dépendent eux-mêmes d'équations aussi inférieures à cette proposée [21]. M. Lagrange choisit une fonction linéaire des racines : l'équation qui la donnerait et qu'on peut actuellement construire, s'élèverait au degré marqué par le nombre des permutations qu'on pourrait faire entre toutes ces racines, et passé le 2e degré, serait toujours plus haute que la proposée. Mais si l'on a soin de prendre pour les coefficients de cette fonction linéaire, les racines de l'unité du même degré que l'équation, ce que toutes les méthodes indiquent, la réduite s'abaissera, comme on peut le voir *a priori*, par la forme même de la fonction. [Poinsot 1808, p. 365]

Les réflexions générales de Poinsot exposées ici permettent de faire ressortir, de manière claire et précise, les principaux acquis sur la théorie générale des équations en ce début de XIXe siècle. À partir de l'exemple de l'équation générale du 5e degré, il explique pourquoi le fait de former la *réduite* à partir des racines de l'unité permet de faire diminuer son degré initial :

Pour en donner une idée, qu'il s'agisse par exemple, de résoudre l'équation du 5e degré. L'équation résolvante qui donnera la fonction linéaire de ses cinq racines, s'élèvera au degré 1.2.3.4.5 ou 120, nombre de manières dont on peut permuter cinq choses entre elles. Mais si les coefficiens de cette fonction sont les racines cinquièmes de l'unité, on observera que cette fonction multipliée successivement par ces 5 racines, fournira 5 fonctions pareilles où les racines de la proposée auront changé de place. Cette multiplication équivaudrait donc à 5 permutations qu'on ferait entre les racines. Donc, si la fonction simple a 120 valeurs, sa cinquième puissance n'en aura que la 5e partie ou 24. On cherchera donc la cinquième puissance de la fonction linéaire. Mais ces 24 valeurs se partageront encore en six groupes. Car, par la nature des racines imaginaires de l'unité, une seule, avec ses puissances successives, donne toutes les autres ; une autre avec ses puissances successives, les donne encore, mais rangées dans un ordre nouveau. Or, comme il y a ici quatre de ces racines, la même fonction où l'on emploierait successivement et de la même manière ces quatre racines, répondrait successivement à quatre de ses valeurs comme si l'on y eût permuté quatre fois les racines de la proposée. Toute expression semblable de ces quatre fonctions, telles que leur somme, la somme de leurs produits deux à deux, ou trois à trois, etc., n'aura donc que le quart de toutes les valeurs, ou simplement

21 Pour Poinsot, une équation est inférieure à une autre équation lorsque son degré est inférieur.

six valeurs différentes. La fonction pourra donc être regardée comme la racine d'une équation du 4e degré dont les coefficiens seront donnés par une équation du 6e qui sera entièrement connue. [Poinsot 1808, p. 365-366]

Ainsi, il arrive à la même conclusion que Lagrange : à l'aide de cette méthode, on ne peut pas réduire la résolution de l'équation générale du 5e degré à la résolution d'une équation de degré inférieur. Mais, on peut néanmoins, dans certains cas particuliers, résoudre des équations de degré supérieur à quatre : c'est le cas des équations où « les racines sont liées par quelque relation connue » [Poinsot 1808, p. 367]. En effet, le fait de connaître des relations entre des ensembles de racines permet de réduire encore plus le degré des équations auxiliaires. Les racines des équations binômes $x^n = 1$ ont cette propriété et c'est dans les *Disquisitiones Arithmeticae* que Gauss expose pour la première fois une méthode pour les résoudre algébriquement, en utilisant les outils mis en avant par Lagrange et un recodage particulier des racines.

1.3. *Un cas particulier : la résolution algébrique des équations binômes*

1.3.1. *La section VII des Disquisitiones Arithmeticae de Gauss*

Dans la section VII des *Disquisitiones Arithmeticae*, Gauss donne la solution d'un problème ancien de géométrie : déterminer si un polygone régulier à n côtés est constructible à la règle et au compas (ce qui revient à diviser un cercle en n parties égales à la règle et au compas). Cette question est réduite à déterminer les n pour lesquels les solutions de l'équation $x^n = 1$ peuvent être exprimées à l'aide des opérations élémentaires et par extractions successives de racines carrées. L'analyse plus générale que donne Gauss sur la résolubilité des ces équations pour tout n a constitué un modèle pour la théorie des équations du début du XIXe siècle. Ainsi, Gauss donne non seulement la solution d'un problème géométrique, mais il démontre également un résultat très important d'algèbre, et ceci dans un traité de théorie des nombres. Afin de comprendre pourquoi les « *principes* [de la théorie de la division du cercle] ne peuvent être puisés que dans

l'Arithmétique transcendante » [Gauss 1801, Préface] [22], nous allons résumer les principales étapes de son raisonnement en prenant appui sur la résolution d'un cas particulier [23] : l'équation $x^{13} - 1 = 0$.

L'équation $x^{13} - 1 = 0$ admet l'unité pour racine, comme toutes les équations considérées ici. Après division par $x - 1$, on obtient l'équation $x^{12} + x^{11} + x^{10} + \cdots + x + 1 = 0$, notée $X = 0$, appelée équation cyclotomique, et dont toutes les racines sont des nombres complexes. Ces racines de l'unité ont la propriété d'être liées entre elles : si on désigne par r une de ces racines, alors elles peuvent s'exprimer sous la forme r^k, pour un nombre entier k compris entre 1 et 12. Comme la notation r^k sera utilisée très régulièrement dans cette section, Gauss introduit la notation : $[k] = r^k$. Voici comment Gauss présente le fonctionnement général de sa méthode :

> Le but de nos recherches, qu'il n'est pas inutile d'annoncer ici en peu de mots, est de décomposer X *graduellement* en un nombre de facteurs de plus en plus grand, et cela de manière à ce que les coefficiens de ces facteurs puissent être déterminés par des équations du degré le plus bas possible, jusqu'à ce que, de cette manière, on parvienne à des facteurs simples, ou aux racines Ω. Nous ferons voir que si l'on décompose le nombre $p - 1$ en facteurs entiers quelconques α, β, γ, etc. (pour lesquels on peut prendre les facteurs premiers), X est décomposable en α facteurs du degré $\frac{n-1}{\alpha}$, dont les coefficiens seront déterminés par une équation du degré α ; que chacun de ces facteurs est décomposable en β facteurs du degré $\frac{n-1}{\alpha\beta}$, à l'aide d'une équation de degré β, etc. De sorte que ν étant le nombre de facteurs α, β, γ, etc. la recherche des racines Ω est ramenée à la résolution de ν équations des degrés α, β, γ, etc. [Gauss 1801, art. 342]

En d'autres termes, l'objectif de Gauss est de décomposer l'équation cyclotomique en une suite d'équations résolubles, dont le degré est de plus en plus bas. Le principe général utilisé par Gauss est d'ordonner d'une certaine façon les racines de l'équation afin d'obtenir des équations auxiliaires correspondant à ce qui est annoncé ci-dessus. Pour cela, il va utiliser

---

22 Toutes nos citations des *Disquisitiones Arithmeticae* sont empruntées à la traduction française publiée en 1807.

23 C'est un des cas particuliers sur lesquels Poinsot appuie son analyse du *Traité* de Lagrange.

un outil de théorie des nombres, qu'il a introduit dans la section III de son traité : les *racines primitives*[24]. Une racine primitive d'un nombre premier p est un nombre g tel que la suite de ses puissances g^k (pour k allant de 1 $p-1$ ou de 0 à $p-2$) est congrue modulo p à la suite des nombres entiers de 1 à $p-1$ (sans tenir compte de l'ordre).

Dans le cas où $p = 13$, $g = 2$ est une racine primitive. On détermine la suite des résidus obtenus après division par 13 :

Puissances	g^0	g^1	g^2	g^3	g^4	g^5	g^6	g^7	g^8	g^9	g^{10}	g^{11}
Résidus	1	2	4	8	3	6	12	11	9	5	10	7

On peut donc exprimer les racines de l'équation $X = 0$ à l'aide d'une puissance d'une racine primitive modulo p. Au lieu de considérer la suite $[1], [2], \ldots, [12]$, on travaille sur la suite : $[g^0], [g^1], [g^2], \ldots, [g^{11}]$.

La méthode de Gauss consiste maintenant à partager les racines en des ensembles ayant même cardinal pour former des sommes de racines appelées *périodes* (on utilise les diviseurs du nombre 12) et à obtenir des équations auxiliaires dont les racines sont ces *périodes*. Par exemple, on peut former quatre périodes de trois racines en prenant les racines de quatre en quatre dans la liste ci-dessus. On obtiendra ainsi la période $[g^0] + [g^4] + [g^8]$. Dans cette période, grâce à la réindexation des racines à partir d'une racine primitive, si on substitue la racine $[g^4]$ à $[g^0]$, on obtient la période $[g^4] + [g^8] + [g^0]$ puisque $g^{12} \equiv 1 \pmod{13}$. De même, connaître une racine d'une période permet de connaître la période complète :

> Donc deux périodes, de même nombre de termes (que nous nommerons périodes *semblables*), seront identiques, si elles ont une seule racine commune, et parconséquent il est impossible que de deux racines contenus dans une certaine période, il ne s'en trouve qu'une seule dans une période semblable [...] [Gauss 1801, page 440]

À la fin de la décomposition, on obtient des *périodes* contenant un seul terme : la résolution de l'équation auxiliaire correspondante permet alors

---

24 Les *racines primitives* ont été introduites pour la première fois par Leonhard Euler (1707–183) dans [Euler 1774]. Il a indiqué quelques-unes de leurs propriétés. Par contre, il n'a pas réussi à démontrer leur existence pour tout nombre premier, ce qui est fait dans la troisième section des *Disquisitiones Arithmeticae*. En termes actuels, les racines primitives d'un nombre premier p sont les générateurs du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$.

de trouver une des racines de l'équation. La notation de Gauss pour les périodes est : (nombre de termes, un terme de la période).

Pour notre exemple, le premier ensemble considéré est composé des douze racines : la période correspondante (qui peut être notée (12, [2]) par exemple) est égale à -1 (puisqu'elle correspond à la somme de toutes les racines de l'équation).

On obtient ensuite deux périodes de six éléments, en considérant les racines de deux en deux :

$$(12,1)\begin{cases}(6,1)\ldots[1]+[4]+[3]+[12]+[9]+[10]\\(6,2)\ldots[2]+[8]+[6]+[11]+[5]+[7]\end{cases}$$

On détermine ensuite l'équation dont ces deux périodes sont solutions, en utilisant les relations entre coefficients et racines d'une équation : :

$$(6,1)+(6,2)=(12,1)=-1,$$
$$(6,1)\times(6,2)=3(12,1)=-3,$$

donc les deux périodes sont solutions de l'équation quadratique[25] : $x^2+x-3=0$. On obtient ainsi facilement les valeurs des deux périodes $(6,1)$ et $(6,2)$.

On continue en considérant quatre périodes de trois racines. On décompose donc les deux périodes (6,1) et (6,2) en deux périodes de trois racines. Par exemple :

$$(6,1)\begin{cases}(3,1)\ldots[1]+[3]+[9]\\(3,4)\ldots[4]+[12]+[10]\end{cases}$$

En calculant la somme $(3,1)+(3,4)$ et le produit $(3,1)\times(3,4)$, on obtient une nouvelle équation du second degré à résoudre, $x^2-(6,1)x+3+(6,2)$, dont les solutions sont les deux périodes $(3,1)$ et $(3,4)$.

La dernière étape consiste à déterminer les douze périodes d'une racine, et donc à obtenir les solutions de l'équation proposée. Par exemple, en décomposant la période (3,1) en les trois périodes (1,1), (1,3) et (1,9), et en calculant la somme, la somme des produits deux à deux, et le produit de celles-ci, on obtient une équation du troisième degré, $x^3-(3,1)x^2+$

---

[25] Pour obtenir le coefficient 3, il suffit d'effectuer le produit et de regrouper les puissances pour former des expressions dont on connaît les valeurs.

$(3,4)x - 1 = 0$ dont les solutions sont trois racines de l'équation initiale $x^{13} - 1 = 0$.

Bien sûr, dans ce cas précis, on obtient des équations auxiliaires du deuxième et du troisième degrés que l'on sait résoudre par radicaux. Dans d'autres cas, pour l'équation $x^{11} - 1 = 0$ par exemple, on obtient notamment des équations auxiliaires du cinquième degré qui, *a priori*, ne sont pas nécessairement résolubles par radicaux. Néanmoins, Gauss démontre que toutes les équations auxiliaires obtenues à partir de sa méthode sont résolubles par radicaux.

Dans son *Traité de la résolution des équations numériques de tous les degrés*, Lagrange consacre la note XIV à la résolution des équations binômes, en s'appuyant sur la méthode exposée par Gauss. Lagrange lui-même qualifie son travail de « simplification de [la méthode] que M. Gauss a indiquée d'une manière générale, dans l'article 360 des *Disquisitiones arithmeticae* » [Lagrange 1808, p. 310]. En effet, Lagrange, tout en s'appuyant sur la méthode de Gauss va éviter les équations auxiliaires : sa méthode permet de résoudre l'équation binôme de degré n en s'appuyant seulement sur des résolutions d'équations binômes de degré inférieur, ce qui simplifie les calculs à faire. Notre but étant surtout de comprendre les commentaires de Poinsot, nous n'entrons pas ici dans les détails de cette méthode.

1.3.2. *L'analyse de Poinsot*

Après avoir exposé ses réflexions sur la théorie générale des équations, Poinsot remarque que l'on peut aller plus loin dans certains cas :

> Mais lorsque les racines sont liées par quelque relation connue, la difficulté descend toujours à celles des degrés inférieurs. Si une partie des racines est traitée d'une certaine manière, on pourra sur le champ dégager le polynome qui les renferme ; et s'il y a plusieurs groupes où les racines contenues soient semblablement traitées, on obtiendra un quelconque de ces groupes par une équation d'un degré marqué par leur nombre. [Poinsot 1808, p. 367-368]

Poinsot développe alors le cas des équations binômes en se référant à Gauss. Il illustre la méthode de ce dernier en prenant l'exemple de l'équation binôme du treizième degré :

> Ainsi, l'on verra sans peine que les douze racines imaginaires de l'équation binôme du 13^{e} degré se partage en quatre groupes de trois racines, telles, dans

chacun d'eux, qu'en mettant l'une à la place de l'autre, ces trois racines ne se séparent pas ; et par conséquent, si l'on échange les racines d'un groupe à l'autre, les groupes ne feront que changer de place en conservant toujours leurs mêmes racines. Ensuite on verra que, parmi ces quatre groupes, il y en a deux qui sont tels que, tout échange qui fait passer l'un à la place de l'autre, ramène celui-ci à la place du premier ; ainsi, les deux autres groupes sont dans le même cas. Si donc vous demandez à l'équation du 12^{e} degré, le diviseur du 3^{e} qui rassemblerait les trois racines d'un groupe, vous aurez les coefficiens de ce diviseur par une équation du 4^{e} degré [...] [Poinsot 1808, p. 370]

Poinsot ne donne donc aucun détail technique de la méthode de Gauss, il n'utilise pas la même terminologie que lui non plus. En effet, les *groupes de racines* de Poinsot désignent les *périodes* de Gauss. On retrouve d'ailleurs les quatre *périodes* de trois racines de l'exemple développé plus haut. Il retranscrit les propriétés des *périodes* énoncées par Gauss à l'aide du vocabulaire courant : « les racines ne se séparent pas ». Ici, son résumé met en avant le point fondamental de l'approche de Gauss : le fait que les racines de l'équation considérée soient liées entre elles permet de décomposer cet ensemble de racines en sous-ensembles dont dépendent des équations de degrés de plus en plus bas. Poinsot pointe du doigt l'outil qui permet de former ces *groupes de racines* ou *périodes* : l'utilisation des *racines primitives* pour ordonner les racines de l'équation proposée. Si l'on prend une racine n^{e} quelconque de l'unité, notée r, et qu'on calcule ses différentes puissances, r^2, r^3, r^4, ..., r^{n-1}, on obtient ainsi toutes les racines n^{e} de l'unité. Bien sûr, si l'on prend une autre racine quelconque n^{e} de l'unité, r', alors la série r', r'^2, r'^3, ..., r'^{n-1} contient également toutes les racines n^{e} de l'unité, mais dans un ordre complètement différent. Poinsot explique donc pourquoi le choix de Gauss, fait la différence :

Mais, au lieu de ranger ces exposants en progression arithmétique, M. Gauss, d'après le théorème de Fermat sur les résidus des puissances, eut l'idée heureuse de les ranger en progression géométrique, en prenant pour base un de ces nombres, qu'Euler nomme *racines primitives*, et qui sont tels que leurs puissances successives divisées par le nombre premier dont il s'agit, qui est ici onze, laissent des résidus successifs tous différents ; de cette manière, on a encore les dix même racines que si l'on eût pris les exposants 1, 2, 3, 4, etc. ; mais dans un ordre nouveau, ce qui est indifférent. Or, à présent l'on peut voir que cette disposition des racines est telle que, si l'on veut mettre une d'entre elles à la

> place d'une autre, et que par ce changement, une des racines s'avance d'une, de deux, de trois ou de quatre places, etc., toutes les autres s'avanceront en même temps d'une, de deux, de trois ou de quatre places, etc., de sorte que toutes les permutations possibles que vous voudriez faire entre ces dix racines, par le transport de l'une à la place de l'autre se réduiront uniquement aux dix permutations que vous obtenez en lisant de suite vos racines, d'abord à partir de la première, puis de la deuxième, puis de la troisième, etc., enfin de la dixième, exactement comme si elles étaient écrites en cercle. [Poinsot 1808, p. 372-373]

Son objectif est une fois de plus de mettre en lumière les raisons de la validité de la méthode : l'utilisation des racines primitives — outil de théorie des nombres — permet de ranger les racines de l'équation proposée dans un ordre où ces racines seront toujours placées de la même façon les unes par rapport aux autres, comme si elles étaient disposées régulièrement sur un cercle. Cette image avait déjà été utilisée par Gauss une première fois pour décrire le même type de structure dans une note de la section II des *Disquisitiones Arithmeticae*, dans le cadre de la démonstration d'un résultat sur les permutations. Gauss définit les *permutations semblables* :

> Lorsque dans deux permutations l'ordre des choses ne différera qu'en ce que celle qui tient la première place dans l'une, en occupe une différente dans l'autre, mais que du reste toutes les autres, à partir de celles-là, suivent le même ordre dans chacune des permutations, de manière que la dernière de l'une se trouve placée immédiatement avant la première dans l'autre ; nous les appellerons *permutations semblables* (*). Ainsi, *ABCDE* et *DEABC*, *ABAAB* et *ABABA* seront semblables. [Gauss 1801, art. 41]

Gauss illustre ce type de permutations dans une note correspondant au symbole * de la citation précédente :

> Si l'on écrivait en cercle les permutations semblables, de manière que la dernière chose touchât à la première, il n'y aurait aucune différence entre elles, parce qu'aucune place ne peut s'appeler la première ni la dernière. [Gauss 1801, art. 41]

Nous verrons que cette image du cercle est récurrente dans les travaux de Poinsot et fondamentale dans ce qu'il appelle la *théorie de l'ordre*, développée dans chacun de ses travaux. De manière plus générale, on retrouve

dans ce commentaire les prémisses des idées centrales que Poinsot va développer dans ses travaux ultérieurs. De plus, les ensembles analysés ici seront repris par Poinsot de manière plus approfondie, leurs caractéristiques communes avec d'autres ensembles seront mises en avant et ce sont celles-ci qui fonderont la notion d'*ordre* telle qu'elle est vue par Poinsot.

2. 1813 : POINSOT ET LA THÉORIE DES PERMUTATIONS

Nous allons étudier dans cette partie un manuscrit de Poinsot qui n'a jamais été publié auparavant [26]. Nous avons trouvé ce texte lors de notre dépouillement des manuscrits de Poinsot présents à la Bibliothèque de l'Institut de France. Dès notre première lecture, nous avons supposé qu'il correspondait au travail présenté en 1813 à l'Académie sous le nom de *Mémoire sur les Permutations* pour plusieurs raisons que nous développons en annexe [27]. Ce mémoire est important car il diffère des autres mémoires contemporains sur le même thème.

L'outil des permutations [28] prend de l'importance avec la publication des travaux de Waring, Lagrange et Vandermonde sur la théorie algébrique des équations dans les années 1770. Au début du XIX^{e} siècle, deux mathématiciens publient des mémoires sur la théorie des permutations : Paolo Ruffini (1765–1822) et Cauchy. Ruffini commence par publier un ouvrage d'algèbre en 1799, intitulé *Teoria generale delle equazione, in cui si domstra impossibile la soluzione algebrica delle equazioni generali di gradi superiore al quarto,* où il détaille les propriétés de l'ensemble des permutations d'un nombre de racines donné dans le but de démontrer l'impossibilité de la résolution de l'équation générale du cinquième degré. Celui-ci sera suivi, entre 1802 et 1813, de six autres versions et ajouts, principalement pour répondre aux remarques et propositions de son ami Pietro Abbati (1768–1842) et aux critiques De Gian-Francesco Malfatti (1731–1807), qui, selon

---

26 L'annexe B de cet article est une transcription de ce manuscrit, à laquelle nous nous référons lors de nos citations.

27 Voir Annexe A, page 122.

28 Au début du XIX^{e} siècle, une permutation est un ensemble ordonné d'objets. Pour une discussion plus approfondie sur les notions de permutation et de substitution, voir par exemple [Dahan 1980].

[Wussing 1984], ne voulait pas admettre la non-existence d'une solution générale de l'équation du cinquième degré. De son côté, Cauchy[29] publie dans un premier temps deux mémoires concernant la théorie des permutations en 1815, puis attendra 1840 pour faire évoluer sa théorie des permutations. Dès 1815, Cauchy donne de nouvelles notations et définitions. Il y introduit par exemple la notion de *substitution*, qui désigne le procédé permettant de passer d'une permutation à une autre, ainsi que la notation utilisée encore aujourd'hui. Il définit ensuite le produit de plusieurs substitutions, etc[30].

2.1. *Étude et analyse du manuscrit*

Dans ce texte, Poinsot essaie de comprendre comment on peut partager les permutations en différents ensembles, toujours dans le cadre de la résolution générale des équations. Nous nous intéressons ici prioritairement aux raisonnements concernant l'ordre et les relations entre les différents objets considérés. Dès les premières lignes (voir page 124), il introduit une fonction φ des racines $a, b, c, d, \ldots$. Il pose $\varphi = (a, b, c, d, \ldots)$, qu'il simplifie à l'aide de la notation $abcd\ldots$, appelée *permutation*. On peut supposer que Poinsot se base ici les travaux de Lagrange sur les équations algébriques exposés dans [Lagrange 1770a] ou [Lagrange 1808].

2.1.1. *Une première méthode pour classer les permutations*

Poinsot choisit de travailler avec l'exemple de l'équation générale du 5^e degré, il note les racines a, b, c, d, e. On obtient ainsi $5 \times 4 \times 3 \times 2 \times 1 = 120$ valeurs pour la fonction φ. Il affirme alors un résultat qu'il va ensuite justifier en rangeant les différentes permutations dans des tableaux :

> Or, ces 1.2.3.4.5. permutations peuvent être partagées en 5 groupes principaux de 1.2.3.4 permutations chacun et tels que les permutations d'un même groupe ne se séparent jamais malgré tous les échanges qu'on pourrait faire entre les lettres a, b, c, d, e. (page 124)

---

29 Voir [Cauchy 1815a] et [Cauchy 1815b]. Ces deux textes sont précédemment lus devant l'Académie le 30 novembre 1812.

30 On pourra lire une analyse des travaux de ces deux mathématiciens à ce sujet dans [Wussing 1984], [Dahan 1980] pour Cauchy, dans [Cassinet 1988] et [Houzel 2002, chap. IV et VI] pour Ruffini.

Comme précédemment, Poinsot ne définit pas les termes *permutation* et *groupe*. On peut supposer que, pour lui, une *permutation* est un ensemble ordonné de lettres[31]. D'autre part, le mot *groupe* paraît être associé à un ensemble d'objets *inséparables*. L'adjectif *inséparable* semble signifier que l'on peut passer d'un objet à un autre par un procédé semblable — ici, un échange de lettres — et que l'on ne peut pas de cette façon obtenir un objet d'un autre groupe. De même, plus loin, l'utilisation de la notion de *groupe* s'accompagne d'une mention similaire : « dont les permutations respectives ne pourront jamais se mêler » (voir page 125).

Poinsot illustre ses raisonnements en regroupant toutes les permutations possibles des cinq racines dans un tableau (voir page 125). Poinsot remarque que le premier groupe est stable lorsque l'on échange les lettres b, c, d, e d'une manière quelconque, c'est-à-dire, en utilisant le vocabulaire de Cauchy, lorsqu'on applique à toutes les permutations une substitution laissant fixe la lettre a. Si on échange la lettre a avec une autre lettre, on obtient un des quatre groupes suivants. Il qualifie ces cinq groupes de *groupes principaux*. Puis il continue à partager ces permutations en sous-ensembles — les *groupes secondaires* — en s'appuyant sur le même principe :

> Actuellement, chaque groupe qui est de 1.2.3.4 permutations pourra se partager en 4 groupes secondaires composés de 1.2.3 permutations. (page 125)

Dans le premier groupe de 24 permutations, il forme un premier groupe contenant les permutations telles que b soit à la deuxième place, puis un groupe tel que les permutations soient de la forme $ac\ldots$, et ainsi de suite : il forme ainsi quatre *groupes secondaires* de 6 éléments. Il continue en formant des *groupes ternaires* composés de deux permutations chacun, tels que ces permutations aient les mêmes trois premières lettres.

Enfin :

---

31 On verra que, dans son manuscrit, il n'introduit pas le concept de substitution, c'est-à-dire l'opération qui permet de passer d'une permutation à une autre. On retrouve ce concept dans les mémoires de Cauchy de 1815, puis dans les travaux de Galois, puis enfin, de façon beaucoup plus aboutie, dans les travaux de Cauchy de 1844.

> [...] chaque groupe ternaire, tel que le premier, se décomposera en deux permutations simples *abcde*, *abced* qui seront toujours conjuguées dans tous les échanges possibles des lettres entre elles. (page 125)

Ici, le terme *conjugué* n'a pas le sens de la conjugaison actuelle : deux permutations *conjuguées* semblent être pour Poinsot des permutations qui appartiennent au même *groupe*, quels que soient les échanges de lettres entre elles que l'on peut y faire.

Poinsot utilise ensuite ces réflexions pour raisonner sur le degré des fonctions des racines de l'équation proposée (voir page 125). L'exposé de Poinsot est un résumé partiel des travaux de Lagrange dans [Lagrange 1770a], basé sur la façon dont on peut ranger les permutations. On sait que la fonction φ admet 5! valeurs sous les permutations des racines a, b, c, d et e. Poinsot ne donne aucune condition pour le choix de cette fonction. Ensuite, il considère les fonctions φ' qui n'auront que 3.4.5 valeurs, et qui sont invariables (c'est-à-dire symétriques). On peut par exemple utiliser les fonctions $\varphi'_{1.1} = \varphi(a,b,c,d,e) + \varphi(a,b,c,e,d)$ et $\varphi'_{1.2} = \varphi(a,b,c,d,e) \times \varphi(a,b,c,e,d)$. On aurait deux autres couples équivalents de fonctions φ', avec les permutations (a,b,d,c,e) et (a,b,e,c,d). Dans ce cas, φ est bien racine d'une équation de degré 2 dont φ' est coefficient : $x^2 - \varphi'_{1.1}X + \varphi'_{1.2}$. On raisonnera de même avec les fonctions symétriques ayant trois variables pour obtenir les expressions des fonctions φ'', et ainsi de suite. Ainsi, la résolution d'une équation de degré n dépendrait de la résolution de plusieurs équations de degrés de 1 à n. On remarque qu'ici, Poinsot donne une idée générale de cette résolution, mais qu'il n'applique pas sa méthode à une équation particulière, et qu'il ne détaille pas comment choisir les fonctions φ, φ', etc. Son objectif ne semble pas être de trouver une méthode de résolution — ou une démonstration de l'impossibilité de la résolution générale du cinquième degré — mais bien de comprendre le fond des réflexions de Lagrange en analysant le comportement des permutations.

Pour conclure cette partie, Poinsot considère les différentes manières de partager les permutations et indique que la méthode de partage choisie ici ne « peut rien apprendre sur la résolution ». En effet, ici, Poinsot classe les différentes permutations pour former des *groupes* mais n'« opère » pas sur les permutations. Il raisonne à partir d'échanges de lettres seulement.

Dans la partie suivante, Poinsot présente une nouvelle classification fondée sur l'utilisation d'une *loi*.

2.1.2. *Une seconde méthode basée sur l'utilisation d'une loi*

La deuxième partie du manuscrit consiste à partager les permutations d'une nouvelle façon, qui se rapproche des calculs sur les permutations que l'on peut connaître aujourd'hui. Cette nouvelle manière consiste à considérer une permutation quelconque, et à utiliser une *loi* pour modifier l'ordre de ses lettres afin d'obtenir une nouvelle permutation. La *loi* correspond en fait à la façon de modifier les lettres les unes par rapport aux autres. Par exemple, une *loi* pourrait consister à échanger la première lettre avec la seconde lettre. Cela correspond en fait à ce que Cauchy appelle *substitution*, c'est-à-dire le procédé permettant de passer d'une permutation initiale à une seconde permutation. Les *lois* utilisées par Poinsot sont toujours d'un type particulier : elles vont lui permettre d'obtenir exclusivement des ensembles qui correspondent à ce que l'on appelle aujourd'hui des groupes cycliques d'ordre n. Il applique cette même *loi* à la permutation obtenue afin d'en obtenir une troisième et continue ainsi jusqu'à revenir à la *permutation primitive* :

> La manière générale de trouver les permutations qui s'assemblent est de prendre une quelconque de ces permutations, et d'y appeler toutes les lettres dans un nouvel ordre, ce qui fournira une nouvelle permutation, ensuite de tirer de celle-ci, par la même loi, une troisième permutation qui sera dérivée de la 2^{e} comme la 2^{e} est dérivée de la 1re ; on continuera de cette manière jusqu'à ce que l'on retombe sur la permutation primitive d'où l'on était parti, et l'on repassera ensuite dans les mêmes à l'infini.
>
> Ces différentes permutations dérivées successivement l'une de l'autre par la même loi seront conjuguées ; c'est-à-dire ne se sépareront jamais malgré tous les échanges possibles entre les lettres [...] (page 128)

Il obtient ainsi le groupe de permutations :

$$\begin{array}{ccccc} a & b & c & d & e \\ b & c & d & e & a \\ c & d & e & a & b \\ d & e & a & b & c \\ e & a & b & c & d \end{array}$$

On ne peut s'empêcher de penser ici aux raisonnements développés par Poinsot — à partir des travaux de Gauss et Lagrange — autour des racines des équations binômes et des racines primitives, qui engendrent également des ensembles correspondant à des groupes cycliques. Les racines primitives permettent d'obtenir la *loi* pour opérer sur les racines des équations binômes qui ont le même rôle que les permutations.

Poinsot observe ensuite que l'on peut obtenir le même groupe de permutations conjuguées en utilisant des lois semblables, c'est-à-dire en prenant les lettres de deux en deux, de trois en trois, ... En termes modernes, si on considère la substitution $\sigma = (a\ b\ c\ d\ e)$, une loi semblable est d'appliquer à la permutation initiale, et à celles obtenues ensuite, la substitution σ^2, ou σ^3, ... Si le nombre m est premier, les groupes inséparables que l'on obtient en appliquant une substitution circulaire (la *loi* utilisée par Poinsot) sont composés de m éléments, et à partir de l'un de ces éléments quelconques et avec une des $m-1$ lois équivalentes, on obtiendra toujours le groupe de m éléments. Par contre, si m est composé, et si on considère un groupe de m éléments, obtenu à partir d'une permutation quelconque, et en y appliquant la substitution $(a\ b\ c\ d\ e\ldots)$, alors ce groupe peut être décomposé en plusieurs sous-groupes dont le cardinal sera un diviseur de m (voir page 130). Poinsot partagera de la même façon les groupes de racines de l'unité. Il donne d'ailleurs des exemples plus concrets :

> Ainsi pour $m = 12$ par exemple, les douze permutations se pourraient partager en deux groupes de six, et chacun de ces groupes en deux autres de trois permutations.
>
> Voilà donc une manière très simple de partager le système des $1.2.3.4\ldots m$ permutations de m lettres, en $1.2.3.4\ldots m-1$ groupes de m permutations conjuguées par la même loi, et qui sont inséparables malgré tous les échanges qu'on pourrait faire entre les m lettres proposées. (page 131)

Lorsque Poinsot prend l'exemple $m = 12$, il obtient quatre groupes de trois permutations. On peut faire le lien avec son commentaire de 1808, où il considère l'équation binôme du treizième degré, qui se ramène à la résolution d'une équation du douzième degré (après division par $x-1$), et où « les douze racines imaginaires [...] se partagent en quatre groupes de trois racines » [Poinsot 1808, p. 370]. On reconnaît donc ici des raisonnements

très similaires à la méthode de Gauss pour la résolution des équations binômes. Poinsot ne l'indique pas explicitement ici, mais il essaie, comme en 1808, de faire ressortir les mécanismes qui font fonctionner les méthodes de Gauss et Lagrange sur la résolution des équations.

2.1.3. *Conjugaison mutuelle des groupes*

Après avoir exploré les différentes manières possibles de *conjuguer* les permutations, Poinsot reprend des raisonnements similaires pour *conjuguer* les groupes entre eux. Pour former un groupe de permutations, Poinsot applique la même loi à une permutation, puis aux permutations successivement obtenues, jusqu'à ce que l'on obtienne à nouveau la permutation initiale. En d'autres termes, il a pris les différentes puissances d'une substitution circulaire σ, qui correspond à prendre « toutes les lettres de n en n ». Pour obtenir des *groupes conjugués*, il va utiliser un *principe analogue* : il va appliquer la même loi à chacune des permutations d'un même groupe pour obtenir un *groupe conjugué*, puis il va faire de même avec ce nouveau groupe, et ainsi de suite jusqu'à obtenir de nouveau le groupe initial. Il donne également une méthode pour passer directement du premier groupe au troisième groupe par exemple : il suffit d'appliquer la substitution σ^2, ce qui revient à prendre les lettres de n^2 en n^2 (voir page 132). Il conclut en faisant un lien avec les racines primitives :

> Ce théorème est très remarquable, il donne une espèce de définition géométrique de ces nombres qu'Euler nomme racines primitives, et qui sont tels que toutes leurs puissances successives laissent par rapport au nombre premier μ que l'on considère des restes tous différents 1, 2, 3, 4, ... $\mu - 1$ et qui reparaissent ensuite périodiquement à l'infini.
>
> Si μ lettres sont rangées en cercle comme les angles d'un polygone, il y a toujours des nombres n tels qu'en joignant les points de n en n, ce qui donne un nouveau polygone, puis ceux-ci de n en n, ce qui forme un troisième polygone, et ainsi de suite, vous formez toutes les espèces de polygones de l'ordre μ ; et il y a juste autant de ces nombres ou racines primitives qu'il y a de nombres premiers à $\mu - 1$ et inférieurs à $\mu - 1$. (page 132)

Ainsi, Poinsot reprend cette image du cercle, et lie l'algèbre, la théorie des nombres, et la géométrie avec les permutations, les racines primitives et les polygones. Par exemple, une *loi* qui permet de générer toutes les permutations du groupe considéré correspond à une racine primitive, qui, en

considérant ses puissances successives, permet d'obtenir toutes les racines complexes d'une équation binôme. Les différents groupes que l'on obtient à partir du groupe initial et en le composant avec une substitution circulaire correspondent aux différentes *périodes* de Gauss que l'on peut obtenir à partir d'une même racine primitive. En effet, une *période* est constituée de certaines puissances d'une racine de l'équation donnée, et on obtient les périodes semblables en multipliant les exposants de chacune de ces racines par un même nombre.

Poinsot va encore plus loin en expliquant comment on peut former une suite de *systèmes* et de *systèmes partiels* : il applique aux permutations ce que Gauss a fait dans les *Disquisitiones Arithmeticae*, et que lui-même appliquera aux équations binômes plus tard, c'est-à-dire qu' il subdivise ces groupes en *systèmes partiels* encore conjugués, en utilisant les facteurs du nombre $m-1$ qui est un nombre composé puisque m est un nombre premier. En effet, prendre successivement les lettres de n en n dans chaque nouveau groupe obtenu revient à prendre, dans le groupe initial, les lettres de n^k en n^k pour k allant de 1 à $m-2$. On retrouve alors dans le raisonnement de Poinsot des points très semblables à la théorie de la cyclotomie de Gauss [32] :

> Mais la première manière de déduire successivement ces groupes l'un de l'autre par la même loi est plus avantageuse en ce qu'elle nous découvre encore une décomposition de ces $m-1$ groupes entre eux, et par l'ordre où elle les fait naître successivement [...] or supposez que α soit un facteur de $m-1$, et dans l'ordre où sont actuellement vos groupes, essayez de les déduire les uns des autres par la loi d'où le $\alpha+1^{e}$ dérive du 1^{er}, ce qui revient à prendre toutes les lettres de n^{α} en n^{α}, vous irez ainsi de l'un à l'autre, en sautant de α en α, et comme α est diviseur de $m-1$, vous ne passerez jamais que sur une même

[32] Voici le passage correspondant dans les *Disquisitiones Arithmeticae* :

> Le but de nos recherches [...] est de décomposer X *graduellement* en un nombre de facteurs de plus en plus grand, et cela de manière à ce que les coefficients de ces facteurs puissent être déterminés par des équations du degré le plus bas possible [...] Nous ferons voir que si l'on décompose $p-1$ en facteurs entiers quelconques α, β, γ, etc. X est décomposable en α facteurs du degré $\frac{n-1}{\alpha}$ [...] ; que chacun de ces facteurs est décomposable en β facteurs du degré $\frac{n-1}{\alpha\beta}$ [...] [Gauss 1801, art. 342].

> partie $\frac{m-1}{\alpha}$ de vos $m-1$ groupes, de sorte que le système sera partagé en α systèmes partiels de $\frac{m-1}{\alpha}$ groupes aussi conjugués entre eux. Et de même si $\frac{m-1}{\alpha}$ a pour diviseur β, vous pourrez subdiviser encore chacun des $\frac{m-1}{\alpha}$ systèmes partiels en β systèmes de $\frac{m-1}{\alpha\beta}$ groupes aussi conjugués entre eux, et ainsi de suite, jusqu'à ce que le système entier n'offre plus dans toutes ses subdivisions que les nombres premiers α, β, ... qui entrent dans la composition du nombre $m-1$; alors il y aura une dépendance mutuelle toute semblable 1°. entre les m permutations d'un même groupe ; 2°. entre les groupes d'un même système partiel ; 3°. entre les systèmes partiels d'un même système supérieur ; et ainsi de suite. (page 134)

Ici, Poinsot parle de « dépendance mutuelle toute semblable ». Aujourd'hui, on pourrait dire que l'on retrouve des structures semblables.

Pour finir, et comme nous l'avons indiqué précédemment, Poinsot « passe à une exposition plus claire et plus rapide » (page 136) en mettant en avant une fois de plus « une liaison intime » entre la théorie des polygones, la résolution générale des équations et la théorie des nombres. Ainsi, il reprend très rapidement ses raisonnements sur les ensembles de permutations que l'on peut faire entre 3, 4 et 5 racines, en illustrant ses propos à l'aide des polygones réguliers à 3, 4 et 5 côtés.

2.2. *Les apports de ce texte*

Dans ce texte, Poinsot n'a pas les mêmes objectifs que Ruffini et Cauchy : il n'essaie pas de construire une théorie des permutations. Il n'étudie pas techniquement le groupe symétrique comme peuvent le faire les deux autres mathématiciens. Il ne définit pas les termes particuliers qu'il utilise régulièrement — on peut penser à *groupe* et *conjugaison* par exemple — comme Cauchy peut le faire dès le début de ses travaux. Il ne perfectionne pas les techniques de calcul sur les permutations. Quand Cauchy définit précisément ce qu'est une substitution, Poinsot parle de *loi* pour passer d'une permutation à une autre, sans en donner une définition ou les caractéristiques. De plus, les *lois* abordées par Poinsot ne correspondent qu'aux *substitutions circulaires* de Cauchy : son étude de l'ensemble des permutations est donc très partielle.

Sur le fond, ce mémoire reste au niveau de ce que l'on peut retrouver quelques années auparavant chez Gauss ou Lagrange. Néanmoins, si l'on

place ce texte dans l'ensemble des écrits de Poinsot à ce sujet, on retrouve des caractéristiques intéressantes et plus originales. En particulier, il met en avant la *liaison intime* (page 136) qui existe selon lui entre la géométrie (avec la théorie des polygones), l'algèbre (avec la résolution des équations) et la théorie des nombres (avec les racines primitives et les congruences). D'autre part, Poinsot présente une partie de la structure du groupe symétrique, en faisant ressortir le type de relations qui existent entre certaines permutations, et entre certains sous-groupes du groupe symétrique. Bien sûr, Poinsot n'a pas en tête les notions de structure ou de groupe telles qu'elles seront définies à partir de la fin du XIX^{e} siècle, mais sa façon de présenter l'ensemble des permutations est originale dans le sens où elle se focalise sur la manière dont on peut relier et classer ces objets entre eux à l'aide d'une *loi*.

Ce texte n'ayant jamais été publié, il est vraisemblable qu'une grande majorité des mathématiciens de l'époque ne l'ait pas connu en détail. Certains ont certainement assisté à sa lecture en 1813, d'autres ont peut-être eu accès à une copie écrite [33]. Néanmoins, Poinsot présente ses réflexions sur la théorie des permutations en quelques paragraphes en 1817 à l'Académie, dont le mémoire correspondant est publié en 1818 dans les *Mémoires* de l'Académie. On peut donc supposer que les idées générales développées dans ce manuscrit sont connues, et que l'étude de ce texte permet de comprendre plus en détails ce que Poinsot résume quelques années plus tard.

L'intérêt de ce texte se situe donc dans la façon nouvelle dont Poinsot expose des idées déjà développées par Gauss et Lagrange. La théorie des permutations vue par Poinsot a-t-elle été reprise au cours du XIX^{e} siècle ? Un mathématicien au moins se réfère à la théorie des permutations de Poinsot : Théodore Despeyrous (1815–1886) [34]. Dans un mémoire intitulé

---

33 Nous avons par exemple retrouvé une version de ce texte dans les manuscrits de Joseph Bertrand à l'Institut de France.

34 Nous remercions Norbert Verdier pour nous avoir fait connaître les textes de ce mathématicien. Le *Cours de Mécanique de Théodore Despeyrous*, publié en 1884, est précédé d'une *Notice sur la vie et les travaux de M. Despeyrous*, écrite par l'éditeur A. Hermann, et dont nous extrayons les informations qui suivent. Ce mathématicien originaire de la région de Toulouse arrive à Paris en 1842 afin de poursuivre ses études à la Faculté des Sciences. C'est à cette même époque qu'il se laisse séduire par les idées de

Sur la détermination des nombres de valeurs que prennent les fonctions par les permutations des lettres qu'elles renferment, paru en 1865 dans le *Journal de Mathématiques pures et appliquées*, il explique qu'il ne travaille pas avec les principes de Cauchy mais à partir de la *théorie de l'ordre* de Poinsot [Despeyrous 1865a, p. 56]. Dans ce même volume, on trouve un autre texte de Despeyrous : *Classifications des permutations d'un nombre quelconque de lettres en groupes de permutations inséparables.* Il y travaille avec les polygones étoilés, comme l'avait fait Poinsot, et considère les permutations de m objets « qui sont relatives aux polygones de Poinsot, c'est-à-dire toutes celles qu'on déduit de cette permutation en prenant successivement les lettres, à partir de la première, de p_1 en p_1, de p_2 en p_2, ... » [Despeyrous 1865b, p. 179], où les p_i considérés sont les nombres inférieurs et premiers à m. De même, dans un mémoire antérieur, intitulé *Mémoire sur la théorie générale des permutations*, publié en 1861 dans le même journal, Despeyrous se réfère déjà aux polygones de Poinsot, et rappelle que Poinsot avait promis, en 1817, un travail sur la théorie des permutations :

> Telles sont les deux lois générales de classification que notre travail démontre. Le profond géomètre dont nous avons parlé, Poinsot, avait, dès l'année 1817, entrevu une partie de ces résultats, et avait promis sur cette matière plusieurs Mémoires. Les géomètres regretteront sans doute qu'il n'ait pas réalisé sa promesse : loin de nous la prétention d'y suppléer. [...] [Despeyrous 1861, p. 417–418]

3. 1818 : UN TOUR D'HORIZON DES SUJETS ABORDÉS PAR POINSOT EN LIEN AVEC LA THÉORIE DE L'ORDRE

Le texte que nous allons présenter ici est intitulé *Extrait de quelques recherches nouvelles sur l'algèbre et la théorie des nombres*, et a été lu le 5 mai 1817 à l'Académie des Sciences, puis publié en 1818 dans les *Mémoires* de l'Académie. Poinsot l'introduit en rappelant deux sujets de recherche qu'il a

---

Charles Fourier et Saint-Simon et collabore au journal *La Phalange*, fondé par Fourier. À partir de 1844, il commence à fréquenter des mathématiciens tels Charles-François Sturm (1803–1855), Libri et Poinsot. Il remplace Libri à la Faculté des Sciences de 1845 à 1847, est nommé à la Faculté des sciences de Dijon jusqu'en 1865, puis revient à Toulouse pour enseigner l'astronomie à l'Observatoire. Il meurt d'un accident de voiture en 1883.

abordés quelques années plus tôt, et qui ont pour lui un point commun avec ses recherches en théorie des nombres : *la science de l'ordre*[35].

> Il y a déjà quelques années[36] que nous avons lu à l'Académie un Mémoire assez étendu sur la théorie générale des permutations. Nous tâchions d'approfondir cette théorie, d'y ajouter de nouveaux principes, et d'en faire quelques applications importantes à l'algèbre et à l'analyse indéterminée. Les mêmes principes se retrouvaient encore en géométrie, dans les propriétés de ces nouvelles figures que nous avons fait connaître[37], et que nous avons rapportées, avec plusieurs spéculations du même genre, à cette partie singulière de la science de l'étendue que Leibnitz à nommée la Géométrie de situation.
>
> Nous avons repris et continué toutes ces recherches qui sont liées entre elles de la manière la plus intime, et qui ont en général pour objet, *la théorie de l'ordre et de la situation des choses sans aucune considération de la grandeur* : théorie neuve et profonde, dont les éléments nous sont à peine connus, mais qu'on doit regarder comme le premier fondement de l'algèbre, et la source naturelle des principales propriétés des nombres. [Poinsot 1818, p. 382-383]

Il utilise notamment cette notion d'*ordre* pour faire des parallèles entre les relations existant entre différents objets mathématiques : les racines primitives et les permutations, les racines primitives de l'unité et les racines primitives modulo un nombre premier p. Il place ici l'*ordre* comme fondement de l'algèbre. Sa définition de l'algèbre commence donc à évoluer vers un domaine plus large que la seule théorie des équations. De plus, ici, l'*ordre* est également présenté comme un point commun entre l'algèbre et la théorie des nombres. Enfin, remarquons que Poinsot est l'un des rares

---

35 L'association des mathématiques à l'ordre n'est bien sûr pas nouvelle. Rappelons Descartes : « [...] j'ai découvert que toutes les sciences qui ont pour but la recherche de l'ordre et de la mesure, se rapportent aux mathématiques [...] » [Descartes 1701, page 223].

36 Il précise une date en note : Mai 1813. Comme annoncé précédemment, il est vraisemblable que cela corresponde au manuscrit étudié dans la partie précédente.

37 Il se réfère ici à son *Mémoire sur les polygones et les polyèdres* publié en 1809. Il y décrit notamment deux polyèdres réguliers étoilés. En 1812, Cauchy publie également un mémoire à ce sujet, dans lequel il démontre que tous les polyèdres réguliers étoilés ont été découverts. L'auteur y rappelle également les résultats de Poinsot, mais ne reprend pas du tout les passages qui s'appuient sur la notion d'ordre et sur la théorie des nombres.

à insister sur le fait que la section VII des *Disquisitiones Arithmeticae* lie la géométrie, l'algèbre et la théorie des nombres [38].

Poinsot donne l'objectif de son intervention :

> Comme nous nous proposons de donner successivement plusieurs [39] Mémoires sur cette matière, nous avons cru qu'il pouvait être utile, en attendant, de présenter à l'Académie une analyse rapide des principaux résultats que nous avons obtenus. [Poinsot 1818, p. 383]

Nous allons donc suivre sa présentation afin d'avoir un aperçu des sujets que Poinsot lie à l'*ordre*.

3.1. *L'ordre et la géométrie de situation*

Dans le texte lu à l'Académie en 1817, Poinsot ne revient pas précisément sur son mémoire de géométrie. Nous allons néanmoins ici reprendre quelques passages de ce *Mémoire sur les Polygones et les Polyèdres* [40] pour montrer comment il utilise l'*ordre* dans ses raisonnements d'une part et comment il lie géométrie et théorie des nombres d'autre part. Ainsi :

---

38 La géométrie est effectivement souvent mise de côté. Poinsot insiste sur ce lien dès 1807 dans son commentaire sur les *Disquisitiones Arithmeticae*, publié dans le *Moniteur universel ou Gazette nationale*, vol. 80, p. 312 : « On pourrait s'étonner d'abord de trouver dans ce livre des problèmes de géométrie, et de les voir résolus par les nombres. Mais dans les sciences mathématiques toutes les vérités se tiennent par une chaîne nécessaire. Aucune idée n'y peut éclore sans éclairer la plupart des théories qui, à leur tour, perfectionnent les arts qui leur répondent [...] ».

39 Seuls deux mémoires de Poinsot seront publiés à ce sujet : le mémoire publié en 1820 que nous étudions dans la quatrième partie de cet article, et le mémoire intitulé *Réflexions sur les principes fondamentaux de la théorie des nombres* publié en 1845. Dans ce dernier, Poinsot indique : « J'avais jeté sur le papier ces réflexions et ces démonstrations relatives à la théorie des nombres, dans la seule intention d'éclaircir, pour quelques personnes, les premiers principes de cette importante théorie. On m'a persuadé qu'il pouvait être utile de les publier [...] » [Poinsot 1845, p. 1]. Il semble donc que Poinsot ait changé d'idée, ou qu'il n'ait pas pu écrire les mémoires prévus.

40 Ce texte a été lu à l'Académie en 1809, et publié en 1810 dans le *Journal de l'École polytechnique*. Un rapport positif sur ce mémoire est lu par Legendre lors de la séance du lundi 16 octobre 1809 à l'Académie. On peut néanmoins remarquer que Legendre n'y fait aucune référence au fait que Poinsot y lie la géométrie de situation à la théorie des nombres.

> On rapporte les questions suivantes à la géométrie de situation, parce qu'on y considère moins la grandeur et la proportion des figures, que l'ordre et la situation des divers éléments qui la composent.
>
> Cette espèce de géométrie, qui ne regarde que les lieux dans l'étendue, est à-peu-près, à la géométrie ordinaire, ce que la science des propriétés des nombres est à l'algèbre, qui est la science des grandeurs. [Poinsot 1810, p. 26]

Poinsot donne une définition de la théorie des nombres très semblable dans ses écrits ultérieurs. C'est pour cela, selon lui, que c'est la théorie des nombres qui peut s'appliquer à la géométrie de situation, « comme l'analyse ordinaire s'applique naturellement aux problèmes déterminés de la géométrie, et le calcul différentiel à la théorie des courbes [...] » [Poinsot 1810, p. 17]. Ici, il ne donne pas de définition précise de ce qu'il entend par la notion d'*ordre*. Il cite notamment Euler, Vandermonde et Marie-Jean Condorcet (1743–1794) en tant que mathématiciens ayant travaillé sur la géométrie de situation, dans le sens qu'il lui donne [41]. On peut d'ailleurs citer la définition donnée par Euler de la *géométrie de situation* dans un mémoire sur le problème des ponts de Köenigsberg, et qui correspond totalement aux vues de Poinsot :

> Outre cette partie de la Géométrie qui s'occupe de la grandeur et de la mesure, et qui a été cultivée dès les temps les plus reculés, avec une grande application, Leibniz fait mention, pour la première fois, d'une autre partie encore très inconnue actuellement, qu'il a appelée *Geometria situs*. D'après lui, cette branche de la science s'occupe uniquement de l'ordre et de la situation, indépendamment des rapports de grandeurs [42].

Dans son mémoire de 1810, Poinsot commence par donner des définitions aux objets étudiés puis il étudie les différentes sortes de polygones ayant un nombre donné de côtés, en obtenant des résultats proches de la théorie des racines primitives :

---

41 Poinsot remarque également que la définition donnée par d'Alembert dans l'*Encyclopédie* de la géométrie de situation selon Leibniz lui semble fausse, ou du moins incomplète (Voir [Poinsot 1810, p. 16-17]) et que la *Géométrie de position* de Condorcet n'a pas les mêmes objectifs.

42 Cette traduction est issue de [Lucas 1891, p. 21-22] et sa version originale se trouve dans le mémoire d'Euler intitulé *Solutio problematis ad geometriam situs pertinentis*, publié en 1741 [Euler 1741, p. 128].

[...] dans l'ordre des polygones de m côtés, il y a autant d'espèces différentes qu'il y a de nombres premiers à m, depuis l'unité jusqu'au nombre $\frac{m-1}{2}$.

Soit en effet un nombre h inférieur et premier à m, et considérez vos m points ou sommets rangés en cercle à égales distances dans l'ordre a, b, c, d, e, etc.. Si, à partir du premier a, vous les joignez successivement par des droites, en les prenant de h en h ; comme le nombre h n'a point avec m d'autre commune mesure que l'unité, vous serez obligé de passer par tous les points avant de revenir au premier ; alors vous aurez formé un polygone régulier de m côtés, avec m angles distincts a, b, c, d, e, etc [Poinsot 1810, p. 21]

Poinsot reprend cette image des racines rangées autour d'un cercle, utilisée dès 1808 dans son commentaire du *Traité* de Lagrange. Il lie également son raisonnement sur les polygones à la théorie des équations binômes, en rapprochant des cas particuliers, ce qui peut laisser supposer que les idées développées par Poinsot dans ses travaux ultérieurs lui sont familières dès 1809. En effet :

Dans l'analyse algébrique des polygones réguliers, ce cas répondrait à l'un de ceux où l'équation binôme se décompose, et où toutes les racines imaginaires ne sont pas propres à reproduire, par leurs puissances successives, toute la série des racines. Mais on reviendra là-dessus, comme on l'a dit : on a eu dessein de séparer ces considérations analytiques, pour ne faire ici qu'un mémoire de pure géométrie [...] [Poinsot 1810, p. 27]

De plus, on trouve également dans ce mémoire une définition géométrique de nombre premier :

Nous avons dit que, si h est un nombre premier à m, et qu'on joigne de h en h, m points rangés en cercle dans l'ordre a, b, c, d, e, etc., on passera nécessairement par tous ces points avant de revenir au premier ; on peut voir également la réciproque de ce théorème, c'est-à-dire que, si, joignant de h en h, m points a, b, c, d, e, etc., on passe par tous ces points avant de revenir au point de départ, le nombre h sera nécessairement premier à m. Si donc, en unissant ainsi plusieurs points par des intervalles quelconques égaux, on ne peut jamais revenir au premier sans avoir passé par tous les autres, on pourra assurer que tous ces points sont en nombre premier absolument : ce qui donne une espèce de définition géométrique d'un nombre *premier*. [Poinsot 1810, p. 27-28]

On voit donc ici une construction de relations réciproques entre deux domaines des mathématiques que Poinsot étend également à l'algèbre

avec la théorie des permutations et la théorie algébrique des équations. Il reprendra d'ailleurs cette image géométrique du nombre. Par exemple, dans le chapitre III de [Poinsot 1845], intitulé *Démonstrations nouvelles tirées de la considération de l'ordre*, il démontrera certaines propriétés fondamentales des nombres à partir de cette définition géométrique. Par exemple, il prouvera que si deux nombres a et b sont premiers à un troisième nombre c, alors le produit ab est également premier au nombre c.

3.2. *L'ordre et la théorie des permutations*

Après l'introduction générale, Poinsot consacre les trois premiers points de son texte à résumer son travail sur la théorie des permutations [43]. Le premier paragraphe ci-dessous correspond à un résumé de la première partie du manuscrit :

> Et d'abord, nous avons fait voir comment le système de toutes les permutations possibles de plusieurs choses, peut-être partagé en plusieurs groupes de permutations associées entre elles de manière que, malgré tous les échanges qu'on voudrait faire de ces choses, les permutations d'un même groupe ne pussent jamais se séparer. Et de même on a montré comment chacun de ces groupes principaux pouvaient se partager en groupes secondaires de permutations également inséparables ; et ainsi de suite pour les groupes successifs qui se subdivisent d'après les diviseurs du nombre total des permutations. On forme ainsi des tableaux qui offrent sur-le-champ plusieurs conséquences remarquables. Et, par exemple, on sait en algèbre que si l'on cherche à déterminer une fonction quelconque des racines d'une équation proposée, la résultante qui la donne s'élève au degré marqué par le nombre de toutes les permutations que ces racines pourraient offrir sous la fonction que l'on considère : or il résulte de la théorie précédente que cette équation élevée n'a point de difficulté supérieure à celle de la proposée elle-même, et qu'elle peut actuellement se résoudre à l'aide d'équations de degrés marqués par les diviseurs de son exposant. [Poinsot 1818, p. 382-383]

---

[43] En parcourant les publications de Poinsot relatives à l'algèbre ou la théorie des nombres, on trouve des références générales relatives à la théorie des permutations dans le commentaire du *Traité* de Lagrange analysé précédemment. Or, comme on va le voir, les idées présentées par Poinsot ici sont bien plus détaillées que dans son texte de 1808 mais sont souvent de simples paraphrases de ce qui se trouve dans le manuscrit étudié précédemment : nous n'analyserons donc que certains extraits.

En comparaison avec la publication de 1808, Poinsot réutilise le même vocabulaire : les *groupes de racines* sont remplacés par les *groupes de permutations* pour travailler sur le même sujet, la théorie générale des équations. La caractéristique du *groupe* pour les permutations reste la même que précédemment : « malgré tous les échanges qu'on voudrait faire de ces choses, les permutations d'un même groupe ne [peuvent] jamais se séparer ». Par contre, Poinsot ne précise pas quelle est la nature de ces *échanges*. L'étude des permutations pour la résolution des équations est une idée commune, mais la particularité de Poinsot est de mettre en avant les mécanismes validant les méthodes. On retrouve les idées fondamentales développées dans le manuscrit avec le partage des permutations d'une part, et la formation des groupes secondaires d'autre part.

Après avoir remarqué, comme dans le manuscrit, que cette première manière de partager les permutations ne permet pas d'en tirer des conséquences sur la résolution générale des équations, Poinsot signale sa deuxième façon de ranger les permutations : « en les faisant naître l'une de l'autre par une même loi ». Cela permet de comprendre très facilement les résultats obtenus par Lagrange concernant les équations du cinquième degré dans [Lagrange 1770a] et d'obtenir des informations supplémentaires sur l'équation générale du 4^e degré. Néanmoins, dans sa présentation de 1817, il ne donne aucune précision sur la nature des *lois* utilisées pour classer les permutations. Pour finir, il tisse un lien entre ce sujet et la géométrie des polygones :

> Or, le point le plus essentiel dans les spéculations de ce genre, étant la simplicité de la représentation de tant de formules, nous avons cherché, dans les nouveaux polygones que nous avons fait connaître, un moyen de les réduire et de les peindre avec une extrême facilité : de sorte que, par ces figures, on peut très-brièvement exposer, et, pour ainsi dire, montrer aux yeux, tout ce qu'on a trouvé jusqu'ici de plus général et de plus profond sur la résolution des équations algébriques. [Poinsot 1818, p. 385]

L'utilisation de la géométrie de situation sert donc ici à comprendre les résultats obtenus sur la théorie des permutations, et donc plus généralement la théorie générale des équations.

La transition entre la théorie des équations et la théorie des nombres est faite par Poinsot à l'aide d'un objet déjà cité précédemment : les racines primitives.

> 4. Cette théorie des permutations nous fait voir encore pourquoi toutes les équations binômes, et celles qui en dépendent, peuvent se résoudre algébriquement. Elle apprend à classer leurs racines imaginaires, de manière qu'elles se conjuguent entre elles d'après les diviseurs du nombre de ces racines ; etc., etc.
>
> 5. Elle conduit naturellement à la considération de cette espèce de nombres qu'Euler a nommés *racines primitives*, et dont la nature et la détermination lui paraissaient l'un des points les plus difficiles de la théorie des nombres. [Poinsot 1818, p. 385]

Là encore, Poinsot ne détaille pas vraiment ses affirmations : ces résultats sont supposés maîtrisés par le lecteur. Le fait que ses réflexions sur la théorie des permutations permettent de justifier la résolubilité des équations binômes vient des *lois* indiquées plus tôt, et est à relier aux relations particulières existant entre les racines des équations binômes : elles sont toutes engendrées par les puissances successives d'une quelconque d'entre elles. Le lien avec les racines primitives s'explique par l'utilisation de ces dernières pour ranger les racines des équations binômes dans un ordre particulier : cet ordre permettra d'utiliser une même *loi* pour passer d'une racine à l'autre.

3.3. *L'ordre et la théorie des nombres*

Poinsot justifie les travaux qu'il va résumer dans la suite de son exposé par l'étude des racines primitives : « nous nous sommes particulièrement appliqués à l'étude de ces nombres, et nous sommes parvenus à en découvrir l'expression analytique [44], en suivant une analogie singulière dont nous allons parler » [Poinsot 1818, p. 385-386]. Poinsot explique comment il a eu l'idée de cette analogie : il a remarqué des faits analogues entre les racines primitives d'un nombre premier p, qui sont en fait certaines racines de la congruence $x^{p-1} - 1 \equiv 0 \pmod{p}$, et les racines complexes de

---

44 L'adjectif *analytique* utilisé par Poinsot semble indiquer certainement que, grâce à sa méthode, les racines primitives d'un nombre premier vont être déterminées à l'aide d'une formule algébrique.

l'équation binôme $x^{p-1} - 1 = 0$. Par exemple, les puissances successives d'une racine primitive r du nombre premier p donnent tous les résidus de 1 à $p-1$ après division par p. De manière analogue, la série des puissances successives de certaines racines imaginaires de l'équation $x^{p-1} - 1 = 0$ donne toutes les racines de cette équation. Poinsot en déduit ainsi une analogie entre l'ensemble des racines de l'équation binôme $x^n - 1 = 0$ et l'ensemble des racines des congruences binômes $x^n - 1 \equiv 0 \pmod{p}$, où p est un nombre premier :

> Cette analogie remarquable, qu'il est facile d'étendre plus loin, et qui est complète, nous a fait penser que ces racines imaginaires devaient être la représentation analytique des racines primitives du nombre premier dont il s'agit : que, vues simplement comme résidus relatifs à ce nombre premier, elles leur devaient être tout-à-fait équivalentes : que, par conséquent, si l'on ajoutait aux nombres qui sont sous les radicaux, des multiples convenables de ce nombre premier (ce qui ne peut jamais altérer les valeurs résidues), ces expressions imaginaires deviendraient réelles, rationnelles et entières, donneraient exactement les racines primitives, et ne produiraient que ces seuls nombres. C'est en effet ce que nous avons établi de plusieurs manières, et confirmé par une foule d'exemples curieux. [Poinsot 1818, p. 386–387]

Cette analogie et la manière dont on peut passer des racines primitives de l'unité aux racines primitives modulo un nombre premier p est détaillée dans [Poinsot 1820]. Poinsot y explique comment, à partir d'une racine complexe primitive de l'unité, on peut trouver les racines primitives du nombre p. A posteriori, on remarque que Poinsot construit une analogie entre deux domaines — théorie des équations et théorie des nombres — en remarquant des similarités entre les relations liant les objets qui composent des ensembles relatifs à ces deux domaines. Il met donc en avant des structures semblables, sans travailler avec la forme des objets. Il n'est pas le premier mathématicien à avoir eu l'idée de développer cette analogie, même s'il semble être le premier à l'avoir exposée dans une publication. En effet, comme nous l'avons indiqué dans l'introduction, les *Disquisitiones Arithmeticae* de Gauss aurait dû être composées d'une huitième section traitant des polynômes modulo un nombre premier p. Une version manuscrite de cette section VIII, qui aurait été rédigée au cours de l'année

1797 et qui est intitulée *Disquisitiones Generales de Congruentiis*, a été retrouvée en 1855 dans les papiers de Gauss, puis publiée en 1863 par Richard Dedekind (1831–1916) dans le second tome des *Werke* de Gauss [45]. Selon Günther Frei, les recherches relatives à la section VII, où Gauss expose sa théorie de la cyclotomie, ont été initiées par l'étude des congruences binômes $x^n - 1 \equiv 0$ (mod. p), où p est un nombre premier. On peut ainsi citer plusieurs passages où l'auteur montre que Gauss utilise l'analogie entre les équations algébriques et les congruences pour construire sa théorie des polynômes modulo p :

> Gauss's theory of polynomials mod p in the *Caput Octavum* was planned to run parallel to the theory of rational integers as treated in the seven sections of the D.A. In particular, it was also to contain a theory of cyclotomy (division of the circle) modulo p. For these reasons, many proofs in the *Disquisitiones Arithmeticae* are formulated in such a way that they are not only valid for the domain of rational integers but also for the domain of polynomials over the integers or rationals or over a "finite field" with p elements, and even, as we would say today, for integral domains. This is one reason why the *Disquisitiones Arithmeticae* appeared so advanced and abstract for many readers. [Frei 2007, p. 164]
>
> [...]
>
> He announces that in the present section he will try to base the theory of congruences, at least as far as this is possible at present, on higher principles, following the salient analogy with the theory of [algebraic] equations, an analogy he has observed many times [...] [Frei 2007, p. 178]
>
> [...]
>
> Gauss studies in detail how to find the roots of the cyclotomic polynomial $X^m - 1$ modulo a prime number p in terms of Gaussian periods, all expressed by means of a primitive root mod p. [Frei 2007, p. 188]

Ces affirmations sont très intéressantes puisque l'on retrouve des ressemblances frappantes avec les idées présentées par Poinsot, même si ce dernier les développe de façon moins détaillée et moins technique que Gauss. Comme on le verra d'ailleurs lors de notre étude du *Mémoire sur l'application de l'algèbre à la théorie des nombres* de Poinsot, la justification du

---

45 Les informations relatives à la section VIII des *Disquisitiones Arithmeticae* sont extraites de [Frei 2007].

passage des équations binômes algébriques aux congruences binômes reprend la méthode utilisée par Gauss dans la section VII des *Disquisitiones Arithmeticae.*

Après quelques détails supplémentaires sur l'analogie construite, Poinsot commente le fait d'utiliser des nombres complexes en théorie des nombres :

> C'est au premier coup-d'œil, un étrange paradoxe que d'employer des imaginaires à la représentation actuelle de certains nombres entiers. Mais, quand on songe qu'il ne s'agit uniquement que de valeurs résidues, le paradoxe s'évanouit. Car si l'on remplace les nombres soumis aux radicaux par les puissances mêmes dont ils ne sont que les moindres résidus, toute l'expression devient claire et parfaitement égale aux nombres entiers dont il s'agit [...] [Poinsot 1818, p. 387-388]

Là encore, plusieurs mathématiciens ont été confrontés à l'utilisation de nombres complexes dans le cadre de la théorie des congruences à cette époque. Gauss les utilise peu dans les *Disquisitiones Arithmeticae* et dans les *Disquisitiones Generales de Congruentiis*[46], mais s'appuie sur certaines classes de nombres complexes dans ses travaux sur les résidus biquadratiques, publiés entre 1825 et 1832. Il y introduit les nombres de la forme $a + bi$, où a et b sont des nombres entiers relatifs, que l'on appelle aujourd'hui *entiers de Gauss* et qui forment l'anneau $\mathbb{Z}[i]$. Il justifie ainsi l'introduction des nombres complexes en théorie des nombres :

> So leicht sich aber alle dergleichen specielle Theoreme durch die Induction entdecken lassen, so schwer scheint es, auf diesem Wege ein allgemeines Gesetz für diese Formen aufzufinden, wenn auch manches Gemeinschaftliche bald in die Augen fällt, und noch viel schwerer ist es, für diese Lehrsätze die Beweise zu finden.
>
> [...] Man erkennt demnach bald, dass man in dieses reiche Gebiet der höhern Arithmetik nur auf ganz neuen Wegen eindringen kann, [...] dass für die wahre Begründung der Theorie der biquadratischen Reste das Feld der höhern Arithmetik, welches man sonst nur auf die reellen ganzen Zahlen ausdehnte,

---

46 Pour les références relatives à la théorie des résidus biquadratiques de Gauss, nous nous appuyons sur les analyses de [Goldstein & Schappacher 2007] et [Frei 2007].

auch über die imaginären erstreckt werden, und diesen das völlig gleiche Bürgerrecht mit jenen eingeräumt werden muss. Sobald man diess einmal eingesehen hat, erscheint jene Theorie in einem ganz neuen Lichte, und ihre Resultate gewinnen eine höchst überraschende Einfachheit. [Gauss 1863, p. 170–171] [47]

Ainsi, l'utilisation des nombres complexes en théorie des nombres apporte de la simplicité, de la clarté pour les deux mathématiciens. Néanmoins, les nombres imaginaires considérés par Gauss et Poinsot en théorie des nombres sont très différents. L'étude des entiers de Gauss mène des années plus tard à la théorie des nombres algébriques, développée notamment par Eduard Kummer (1810–1893) et Dedekind. Les nombres imaginaires introduits par Poinsot ne sont pas des entiers de Gauss. Comme nous le verrons dans notre étude de son *Mémoire sur l'application de l'algèbre à la théorie des nombres*, les nombres considérés par Poinsot font partie pour nous d'extensions algébriques des corps $\mathbb{Z}/p\mathbb{Z}$. D'autres mathématiciens vont introduire ce type de nombres dans leurs travaux de théorie des nombres dans les années 1820, c'est-à-dire peu de temps après la publication des mémoires en question de Poinsot. On peut évoquer Jacobi dont un article de quatre pages est publié dans le deuxième tome du *Journal de Crelle* en 1827. Ce texte s'intitule *De residuis cubicis commentatio numerosa* et contient des résultats sans démonstration donnant des indications sur les relations des caractères cubiques de deux

47 Ce passage est extrait de l'annonce (*Anzeige*) du texte *Theoria residuorum biquadraticorum. Commentatio secunda*, publié pour la première fois en 1832. Voici une traduction possible de ces paragraphes :

Il est aussi facile de découvrir tous ces théorèmes particuliers par induction qu'il est difficile de trouver une loi générale pour ces formes de cette même manière, même si plusieurs caractéristiques communes sont évidentes.

[...] On reconnaît bientôt que des approches totalement nouvelles sont nécessaires pour pénétrer ce riche domaine qu'est l'arithmétique supérieure, [...] que, pour le fondement réel de la théorie des résidus biquadratiques, le champ de l'arithmétique supérieure, qui s'était auparavant prolongé aux entiers réels uniquement, doit être étendu pour inclure également les entiers imaginaires et que l'on doit donner exactement le même droit de citoyenneté à ces derniers qu'aux premiers. Dès que l'on a intégré cela, cette théorie apparaît sous une lumière totalement nouvelle, et ses résultats acquièrent une étonnante simplicité.

nombres premiers, en considérant des nombres imaginaires de la forme $a+b\sqrt{-3}$, où a et b sont des nombres entiers, modulo un nombre premier. Augustin Cournot (1801–1877) en résume le contenu dans le *Bulletin de Férussac*, après avoir remarqué que des travaux de Gauss à ce sujet sont attendus depuis quelques années déjà :

> À son imitation, M. Jacobi, qui a beaucoup médité sur le même sujet, nous fait part, sans les démontrer, de trois théorèmes principaux découverts par lui, mais en y joignant quelques éclaircissements et notamment l'annonce d'une théorie neuve et piquante, celle des racines imaginaires des congruences et de leurs racines primitives. Depuis long-temps nous avions pensé (et les derniers mémoires de M. Poinsot l'indiquaient assez clairement) que la considération de cette sorte de racines était nécessaire pour compléter la théorie des nombres et étendre ses rapports avec l'analyse algébrique [Cournot 1827].

Un autre mathématicien étudie ces nombres imaginaires : Galois, en 1829, publie un article *Sur la théorie des nombres* en 1830 dans le treizième tome du *Bulletin de Férussac*. Ce texte porte sur l'étude de toutes les racines des congruences de degré supérieur à 2. Galois réduit ses recherches au cas particulier où la congruence est irréductible modulo p et il indique alors une analogie possible entre les nombres complexes et les racines de la congruence ainsi considérée :

> Dans ce cas, la congruence n'admettra donc aucune racine entière, ni même aucune racine incommensurable de degré inférieur. Il faut donc regarder les racines de cette congruence comme des espèces de symboles imaginaires, puisqu'elles ne satisfont pas aux questions de nombres entiers, symboles dont l'emploi dans le calcul sera souvent aussi utile que celui de l'imaginaire $\sqrt{-1}$ dans l'analyse ordinaire. [...]
>
> C'est la classification de ces imaginaires et leur réduction au plus petit nombre possible, qui va nous occuper [Galois 1830, p. 428].

Le travail de Galois relatif à ces nombres, qualifiés aujourd'hui d'« imaginaires de Galois », est notamment repris par Joseph Serret (1819–1885) dans la troisième édition du *Cours d'algèbre supérieure*[48], dans un paragraphe intitulé *De point de vue sous lequel Galois a envisagé les congruences suivant un module premier et une fonction modulaire.* Serret indique d'ailleurs : « Ainsi

48 Voir [Serret 1866, p. 178-188].

peuvent s'introduire dans l'analyse de nouvelles imaginaires dont l'emploi offre certains avantages, bien qu'il ne soit pas indispensable. Cette conception est entièrement due à Galois, qui l'a exposée succinctement dans le *Bulletin des Sciences mathématiques de Férussac* » [Serret 1866, p. 178]. Néanmoins, même si l'étude de ces nombres par Galois est bien plus approfondie que celle de Poinsot, c'est bien ce dernier qui les utilise plusieurs années auparavant dans son *Mémoire sur l'application de l'algèbre à la théorie des nombres* lu en 1818 à l'Académie des Sciences.

3.4. *Conclusion*

Dans ce texte, Poinsot nous livre bien un tour d'horizon des sujets qu'il aborde dans le cadre de sa *théorie de l'ordre.* Il indique les principales idées qu'il développe plus précisément dans ses textes : cela lui permet d'annoncer à l'Académie ses recherches en géométrie, algèbre et théorie des nombres articulées autour de la notion fondamentale d'*ordre* (qu'il ne définit toutefois pas de manière explicite). Les sujets abordés sont étudiés par d'autres mathématiciens dans ce premier tiers du XIX^e^ siècle. Nous allons maintenant examiner un mémoire plus original.

4. 1820 : ANALOGIE ENTRE ALGÈBRE ET THÉORIE DES NOMBRES

Le mémoire que l'on va étudier ici a été présenté en 1818 à l'Académie sous le nom de *Représentation analytique des résidus des puissances par la formule des racines imaginaires de l'unité,* publié en 1820 dans le *Journal de l'École polytechnique* et en 1824 dans les *Mémoires* de l'Académie sous la forme d'un texte intitulé *Mémoire sur l'application de l'algèbre à la théorie des nombres,* puis présenté par Cournot dans le *Bulletin de Férussac* en 1825. Le contenu de ce mémoire était déjà annoncé dans le texte présenté en 1817 à l'Académie, commenté précédemment.

4.1. *Sur le sens du résultat*

L'objectif de ce mémoire est d'utiliser une analogie entre les équations binômes $x^n - 1 = 0$ et les congruences $x^n - 1 \equiv 0 \pmod{p}$, où p est un

nombre premier et n est, dans un premier temps, un diviseur de $p-1$, afin de résoudre ces dernières :

> J'ai observé les propriétés analogues de ces nombres entiers et de ces racines imaginaires ; et, suivant jusqu'au bout cette analogie, j'ai avancé que la formule générale qui résout l'équation binôme $x^n - 1 = 0$, est, dans le sens que je vais dire, la représentation analytique de chacun des nombres entiers qui résolvent l'équation semblable, $x^n - 1 = Mp$, mais où le second membre, au lieu d'être nul, désigne un multiple du nombre premier p ou du module que l'on considère.
>
> Ce théorème remarquable est la base de toute la théorie des *résidus des puissances* [...] [Poinsot 1820, p. 343]

Pour justifier cela, nous allons voir que Poinsot s'appuie une fois de plus sur les travaux de Gauss dans les *Disquisitiones Arithmeticae*, et plus particulièrement sur la section VII. Avant de donner l'énoncé exact de son théorème et d'en donner une démonstration, Poinsot illustre à l'aide d'exemples la façon dont on peut passer d'égalités absolues à des égalités modulo un nombre premier p, après avoir explicité le lien entre ces deux types d'égalités : « Cette égalité consiste proprement dans celle des restes que laisseraient les deux membres relativement à ce module ; de manière qu'en l'ajoutant une ou plusieurs fois aux divers nombres qui se trouvent engagés dans la proposée, on rendrait les membres parfaitement égaux entre eux, et que cette égalité relative dont nous parlions deviendrait une égalité absolue » [Poinsot 1820, p. 343]. Voici le premier exemple présenté par Poinsot : $\sqrt{-1} = \pm 2$ «relativement au module 5» (car $\sqrt{-1+5} = \sqrt{4} = \pm 2$). Il prend un autre exemple : $\sqrt{-1}$ modulo 13, qui revient à $\sqrt{-1+2\times 13} = \sqrt{25} = \pm 5$ modulo 13. Il prend un troisième exemple en utilisant cette-fois ci la formule d'une des racines cubiques de l'unité : $\frac{-1+\sqrt{-3}}{2}$, avec $p = 7$. Comme, dans $\mathbb{Z}/7\mathbb{Z}$, $-3 = -3+7 = 4$, l'expression précédente revient à $\frac{\sqrt{-1+7+\sqrt{-3+7}}}{2}$, ce qui est égal à 2 ou 4 selon le signe choisi pour $\sqrt{4}$. Pour les deux premiers exemples, le module est un nombre premier de la forme $4n+1$, ce qui correspond au cas où le nombre -1 est un résidu quadratique modulo p. Il est donc certain que l'on puisse trouver un multiple np de p tel que $-1+np$ soit un carré. De même, on peut démonter facilement que le nombre -3 est un résidu quadratique modulo 7. Mais Poinsot ne précise à aucun moment

pourquoi il a choisi ces exemples. La raison de ce silence peut être que, depuis la publication des ouvrages de théorie des nombres de Legendre et Gauss, les résultats liés aux résidus quadratiques et en particulier à la loi de réciprocité quadratique font partie du « bagage nécessaire » pour qui veut lire des travaux de théorie des nombres [49].

Enfin, Poinsot fait quelques remarques générales autour de cette analogie. D'une part, il insiste sur la puissance de cette propriété qui met en avant des relations entre une infinité d'ensembles de nombres, les solutions de l'équation $x^n = 1$ et les solutions des équations $x^n \equiv 1 \pmod{p}$ pour n'importe quel nombre premier p :

> Sous ce point de vue donc, je dis que l'expression algébrique imaginaire qui rend nul le binôme $x^n - 1$, représente les divers nombres entiers qui rendent ce même binôme multiple d'un nombre premier p.
>
> [...] C'est en cela sur-tout que consistent la nouveauté et l'étendue de notre théorème : car on n'aperçoit aucune relation, ni entre les divers nombres qui résolvent la proposée pour un module particulier, ni entre les différentes classes des nombres qui la peuvent résoudre pour des modules différens ; et pourtant nous voyons que tous ces nombres sont réductibles à une même expression imaginaire, composée de nombres actuellement déterminés et connus, qui ne dépendent point des modules, mais uniquement du degré de la proposée. Cette réduction si frappante, cette même représentation analytique de tant de nombres différens, et qui ne paraissent soumis à aucune loi, nous indique de nouvelles routes dans l'analyse indéterminée, et nous offre, comme on l'a dit, le premier et singulier exemple de l'application de l'algèbre à la théorie des nombres. [Poinsot 1820, p. 344]

Il ajoute que ce résultat peut d'ailleurs se généraliser, mais que la démonstration en est bien plus difficile. L'intérêt d'exposer cette théorie pour les équations binômes est qu'elles forment une classe d'équations qui est la base de la résolution des équations générales. Il rappelle enfin

---

49 De même, Poinsot ne revient pas sur la définition de la notation $\sqrt{4}$ modulo p. En effet, dans une égalité absolue, c'est-à-dire en considérant les nombres réels, l'équation $x^2 = 4$ a deux solutions mais la notation $\sqrt{4}$ désigne le nombre 2, c'est-à-dire la racine positive de l'équation. Par contre, la notation $\sqrt{4}$ modulo p, désigne ici une des racines de l'équation $x^2 \equiv 4$ modulo p. Gauss, dans les *Disquisitiones Arithmeticae*, explicite cette différence : « et comme $\sqrt[n]{A}$ ne signifie autre chose que la racine de l'équation $x^n = A$; en ajoutant le module, $\sqrt[n]{A}$ (mod. p) représentera une racine quelconque de la congruence $x^n \equiv A$ (mod. p) » [Gauss 1801, art. 60].

que, comme il l'a déjà indiqué en 1817, son théorème permet de déterminer les racines primitives d'un nombre premier p : on les obtient en effet à partir de l'expression des racines complexes primitives de l'équation $x^{p-1} - 1 = 0$. Mais la méthode de Gauss pour résoudre les équations binômes se base sur l'utilisation des racines primitives modulo un nombre premier p. Poinsot remarque donc que son théorème peut sembler amener à « une espèce de cercle vicieux » [Poinsot 1820, page 345], ce qui n'est pas le cas : en effet, pour déterminer les racines primitives du nombre premier p, il faut résoudre la congruence $x^{p-1} - 1 \equiv 0 \bmod p$, qui correspond à l'équation binôme $x^{p-1} - 1 = 0$. Or, résoudre cette équation à l'aide de la méthode de Gauss revient à résoudre des équations binômes de la forme $x^k - 1 = 0$, où k est un diviseur premier du nombre $p - 1$: cela nécessite donc de connaître une racine primitive du nombre premier $k < p$. Il observe également que sa méthode, qui permet de déterminer les racines primitives d'un nombre premier, est très indirecte mais que l'intérêt est ici de mettre en avant «la théorie et les méthodes générales» [Poinsot 1820, p. 346] [50].

Poinsot explique enfin les fondements de sa démonstration en abordant la résolution de l'équation réciproque $x^{n-1}+x^{n-2}+x^{n-3}+\cdots+x+1 = 0$. Il se réfère alors à Lagrange, Vandermonde et Gauss, qui a rangé les racines telles que leurs exposants forment « la suite naturelle des puissances d'une racine primitive du nombre premier n ». La considération des racines primitives permet en effet la résolution systématique des équations binômes : en utilisant l'ordre de Gauss obtenu à l'aide des racines primitives, toute substitution de racines induit une permutation simultanée de ces racines qui est de plus circulaire.

4.2. *Théorème et démonstration*

Après ces généralités, Poinsot énonce le théorème qui permet de déterminer les racines des congruences $x^n \equiv 1 \pmod p$ à partir des racines de l'équation $x^n = 1$:

---

50 Il donne d'ailleurs des méthodes de recherche de racines primitives plus efficaces dans ses textes de 1817 et 1845.

Considérons donc l'équation binôme indéterminée, $x^n - 1 = Mp$, où Mp désigne un multiple quelconque du nombre premier p, et n un exposant quelconque premier, que je supposerai d'abord diviseur de $p-1$, afin que l'équation $x^n - 1 = Mp$ ait n racines ou solutions en nombres entiers inférieurs à p. Je dis que si l'on prend, à la place de cette équation indéterminée, l'équation binôme déterminée $x^n - 1 = 0$, et qu'on la résolve, l'expression algébrique de ses n racines, qui, excepté l'unité, sont toutes imaginaires, sera la représentation analytique des n nombres entiers qui résolvent l'équation $x^n - 1 = Mp$; c'est-à-dire qu'en ajoutant aux nombres qui sont sous les divers radicaux de cette formule imaginaire, des multiples convenables de p, on fera disparaître les imaginaires et les irrationnelles, on rendra toutes les opérations indiquées parfaitement exécutables, et l'on parviendra précisément aux n nombres entiers qui satisfont à la proposée $x^n - 1 = Mp$. [Poinsot 1820, p. 349]

Dans ce texte, il n'aborde que le cas des congruences binômes où le module p est un nombre premier. Il considère dans un premier temps le cas où le nombre n est premier et divise $p - 1$, puis il justifie le cas plus général où n est un nombre composé. Enfin, il donne des exemples pour le cas où $n - 1$ ne divise pas le nombre p. Il étudiera des cas plus généraux dans [Poinsot 1845] [51].

Pour démontrer le cas où n est un nombre premier [52] diviseur de $p - 1$, Poinsot transpose les étapes fondamentales de la méthode de Lagrange, exposée dans la Note XIV de son *Traité de la résolution des équations numériques de tous les degrés*, pour la résolution des équations binômes en terme de congruences. Comme dans son *Analyse du traité*, il commence par insister sur la forme des racines des équations binômes et sur la « considération

---

51 Dans les *Disquisitiones Arithmeticae*, Gauss indique le nombre de racines de l'équation $x^n \equiv 1 \pmod{p}$. Il trouve cette quantité à l'aide de la notion d'*indice*, mais annonce qu'il compte démontrer ces résultats à l'aide de *considérations plus profondes* [Gauss 1801, art. 61] dans la section VIII. Gauss étudie également cette équation pour un module de la forme p^k à l'aide des outils qu'il a introduits précédemment, tout en ajoutant qu'il en proposera une preuve plus simple dans la section VIII. De son côté, Poinsot détermine, dans son texte de 1845, le nombre de racines de l'équation $x^n \equiv 1 \pmod{p}$ en démontrant que l'équation $x^n \equiv 1 \pmod{p}$ admet les mêmes racines que l'équation $x^\theta \equiv 1 \pmod{p}$, où θ est le plus grand diviseur commun de n et de $p - 1$. C'est la méthode qui est reprise par Serret dans son *Cours d'Algèbre Supérieure*.

52 Le cas où n est composé et diviseur de $p - 1$ se déduit de celui où n est premier et Poinsot l'aborde sans le justifier à la fin de la démonstration ; il le détaillera dans son mémoire de 1845.

ingénieuse » [Poinsot 1820, p. 348] de Gauss, à savoir l'utilisation des racines primitives. Ainsi, la résolution de l'équation $x^n - 1 = Mp$ se ramène à la résolution de l'équation $x^{n-1} + x^{n-2} + x^{n-3} + \cdots + x + 1 = Mp$, où les racines sont des nombres entiers supérieurs à l'unité (car $n < p$). Si r est solution de cette équation, alors $r^2, r^3, r^4, \ldots, r^{n-1}$ le seront également. Il considère alors la suite, déjà considérée par Gauss dans la section VII des *Disquisitiones Arithmeticae*, $r, r^a, r^{a^2}, r^{a^3}, \ldots, r^{a^{n-1}}$, où a est une racine primitive du nombre n. Ainsi :

> [...] les racines de la proposée, non-seulement sont représentées par les différentes puissances d'une *même* racine, mais encore elles sont rangées dans un ordre où chacune d'elles est une *même* puissance de celle qui la précède.
> [...] cet ordre ingénieux, dont rien ne paraît d'abord nous indiquer le choix entre tous les autres, est au fond un ordre analytique déterminé par la nature même des choses. Car, comme il s'agit de racines qui jouissent toutes également de la même propriété, et qu'il n'y a aucune raison de préférer l'une à l'autre, il est clair que l'ordre le plus naturel est celui qui conviendrait également à toutes les racines, et qui par conséquent ne changerait point, quelle que fût la racine r d'où l'on voulut partir. Ainsi, par la nature même de la question, on est porté à chercher, s'il est possible, un ordre où les racines naîtraient successivement l'une de l'autre par la même fonction, et où il serait alors indifférent d'y changer une racine en une autre quelconque à volonté.
>
> [...] aucun échange de racines ne pourra troubler l'ordre ; les racines ne feront que s'avancer toutes à la fois d'un même nombre de places, et elles garderont toujours entre elles la même disposition, exactement comme si elles étaient rangées en cercle. [Poinsot 1820, p. 350-351]

Une fois de plus, Poinsot met ici la notion d'*ordre* en avant en détaillant pourquoi l'ordre obtenu à partir de l'utilisation des racines primitives permet d'obtenir la solution du problème et comment on peut y penser *a priori*. Il donne au lecteur une définition très précise de l'*ordre* auquel il semble se référer dans sa *théorie de l'ordre* : non seulement, chaque élément est représenté par une puissance d'un même objet primitif, mais ces objets sont rangés de telle sorte que pour passer de l'un à l'autre, on applique toujours la même *loi* ou la même *fonction*. Cela caractérise bien les ensembles étudiés par Poinsot — racines des équations binômes, permutations — et également par Gauss. De plus, en utilisant à nouveau l'image du cercle,

Poinsot met encore en avant le fait que ces ensembles sont cycliques pour la *loi* choisie.

Poinsot expose alors sa démonstration en s'appuyant sur les travaux de Gauss revus par Lagrange et en transposant les égalités absolues en des égalités modulo p dans les raisonnements des deux mathématiciens. Il justifie cette transposition par l'addition ou la soustraction d'un certain multiple du nombre premier p, puis conclut enfin sur le contenu de son théorème :

> Mais il est évident que cette supposition de $r^n = 1$, au lieu de $r^n = 1+Mp$, et de $r+r^2+r^3+\&c. = -1$ au lieu de $r+r^2+r^3+\&c. = -1+Mp$, revient à supprimer dans les expressions θ, θ', θ'', & c. qui sont sous les radicaux, certains multiples du nombre premier p que l'on considère. Donc, puisque par cette suppression de multiples p, on passe de l'expression du nombre entier r, à l'expression de la racine imaginaire n^e de l'unité, il s'ensuit que, par la restitution dans celle-ci de ces mêmes multiples de p, on reviendrait à l'expression exacte du nombre entier r. [Poinsot 1820, p. 354]

En énonçant son théorème, Poinsot construit une analogie entre les racines complexes de l'équation $x^n - 1 = 0$ et les racines des congruences $x^n - 1 \equiv 0$ modulo un nombre premier p, qu'il prolonge sans justification dans sa démonstration.

Poinsot considère ensuite une autre décomposition, en utilisant des *groupes* particuliers des racines :

> [...] au lieu de considérer à la fois toutes les racines r, r^2, r^3, r^4, r^5, & c. r^{n-1}, il faudra les partager en plusieurs groupes de racines liées entre elles de la même manière. On formera immédiatement chacun de ces groupes au moyen de la suite ordonnée,
>
> $$r, r^a, r^{a^2}, r^{a^3}, r^{a^4}, \&c., r^{a^{n-2}},$$
>
> en y prenant les racines de h en h, si h est un diviseur de $n-1$. On aura ainsi h groupes composés de $\frac{n-1}{h}$ racines ; et ces divers groupes seront aussi ordonnés entre eux, de manière que chacun d'eux produira le suivant, en y changeant la racine r en r^a.
>
> On décomposera de même chaque groupe, en y prenant les racines de k en k, si k est un diviseur de leur nombre $\frac{n-1}{h}$, et ainsi de suite. Et si l'on applique enfin à la représentation des racines de ces groupes partiels, et des sommes de racines contenues dans ces groupes eux-mêmes, une analyse toute semblable à celle qu'on a suivie plus haut pour l'ensemble de toutes les racines, on parviendra facilement à une formule qui ne présentera point de radicaux d'exposans

supérieurs aux facteurs 2, h, k, &c. du nombre composé $n-1$ [...] [Poinsot 1820, p. 356]

Comme précédemment, Poinsot s'appuie sur le travail que Gauss a exposé pour la résolution de l'équation $x^n - 1 = 0$, les *périodes* de Gauss devenant des *groupes de racines*. Cet extrait est également similaire à ce que l'on trouve dans le manuscrit de Poinsot sur les permutations, lorsqu'il décompose les groupes de permutations en *groupes secondaires*, *groupes ternaires*, ... On retrouvera des raisonnements similaires à la fin de ce *Mémoire*.

Poinsot aborde alors le cas où n n'est pas un diviseur de $p - 1$:

> Lorsque n ne divise pas $p - 1$, l'équation indéterminée $x^n - 1 = Mp$ n'a qu'une seule racine ou solution entière, qui est l'unité ; et toutes les autres sont impossibles ou irrationnelles. Mais la formule des racines n. mes de l'unité n'en est pas moins encore l'expression analytique de ces racines même impossibles. [Poinsot 1820, p. 357]

En effet, ces racines vérifient les mêmes conditions (leur somme doit être égale à $-1 + Mp$), et on peut donc reproduire le raisonnement précédent. Cette remarque est importante dans le sens où la considération de ces racines *impossibles* est une première introduction des nombres complexes dans la théorie des congruences. Poinsot avait d'ailleurs déjà insisté sur ce point dans son exposé de 1817.

Pour illustrer son théorème et donner un exemple de ces racines *impossibles*, Poinsot prend l'exemple de l'équation $x^3 - 1 = Mp$ pour $p = 43$, cas où le nombre 3 divise le nombre $p - 1$, puis pour $p = 29$, qui est un cas où 3 ne divise pas $p - 1$. Dans les deux cas, il utilise l'expression des deux racines complexes de l'équation $x^3 - 1 = 0$: $\frac{-1\pm\sqrt{-3}}{2}$. Dans le cas où $p = 43$, -3 est résidu quadratiques modulo 43, et on obtient donc trois racines entières qui « existent réellement » [Poinsot 1820, p. 358] : -7 et 6 à partir de la formule ci-dessus et l'unité [53]. Dans le cas où $p = 29$, -3 n'est pas un résidu quadratique, donc le radical $\sqrt{(-3)}$ ne deviendra jamais un

---

53 En effet : $-3 + 4 \times 43 = 169 = 13^2$ donc $\frac{-1\pm\sqrt{-3}}{2} = \frac{-1\pm13}{2} = 6$ ou -7. On vérifie d'ailleurs facilement que ces deux nombres sont bien solutions de la congruence binôme $x^3 - 1 \equiv 0 \bmod 43$. Dans son texte, Poinsot indique que les solutions de cette congruence sont -6 et 7 : on suppose qu'il s'agit d'une erreur de signe.

nombre entier modulo 29. Poinsot explique comment on peut néanmoins obtenir une expression des racines imaginaires de l'équation considérée :

> Mais si $p-1$ n'est pas divisible par 3, comme dans le cas de $p=29$, alors il n'y a que le seul nombre entier 1 à chercher, et les deux autres racines sont impossibles ; mais on peut toujours supposer ces racines également représentées par la formule $\frac{-1\pm\sqrt{-3}}{2}$, que l'on changera, si l'on veut, en $\frac{-1+ip\pm\sqrt{(-3+op)}}{2}$, en ajoutant aux nombres les multiples ip et op du module p. A la vérité, on ne pourra jamais, par cette addition, rendre le nombre -3 un carré parfait, et la quantité $\frac{-1+ip\pm\sqrt{(-3+op)}}{2}$ sera toujours une incommensurable, quelque soit le multiple de p que l'on veuille introduire : mais cette expression irrationnelle, pouvant toujours satisfaire à l'équation $x^3-1=Mp$ (comme on le voit en supposant i et o tous deux nuls, ou même seulement, $3i^2p-6i+o=0$), sera l'expression analytique de ces racines même impossibles. Cette expression sera donc aussi parfaite que celle des imaginaires dans l'analyse ; je veux dire qu'on pourra, sans crainte, l'employer dans le calcul, et que si, par une combinaison quelconque de semblables valeurs, les irrationnelles viennent à se détruire, le résultat final sera aussi exact, et la démonstration aussi bien établie, que si l'on eût point passé par ces valeurs irrationnelles. [Poinsot 1820, p. 359]

Poinsot donne de façon explicite l'expression des racines complexes d'une congruence, de manière analogue aux nombres complexes. Néanmoins, il ne justifie ni l'existence ni la validité des opérations pour ces nombres imaginaires dans $\mathbb{Z}/p\mathbb{Z}$, et ne fait aucun commentaire sur les difficultés que l'introduction de ces nombres peut impliquer. Il admet pourtant que l'on peut « sans crainte, [les] employer dans le calcul [...] », ce qu'il fait plus loin pour analyser des exemples particuliers où l'on retrouve des expressions des racines faisant apparaître des nombres imaginaires qui s'annulent entre eux[54]. D'autre part, comme on l'a observé précédemment, Poinsot ne cite à aucun moment les travaux d'Euler, Legendre ou Gauss relatifs à la théorie des résidus quadratiques, alors qu'il doit s'en servir pour construire les exemples convenables. Ces résultats peuvent effectivement être supposés connus des lecteurs de Poinsot. Cette absence de référence reste cependant surprenante puisque Poinsot fait

---

54 Poinsot étudie dans ce mémoire (pages 116-120) l'équation $x^7-1=Mp$ pour $p=43$ et $p=29$ que nous ne détaillerons pas dans ce texte. Dans le deuxième cas, on retrouve des racines cubiques incommensurables modulo p qui se simplifient entre elles.

régulièrement référence aux travaux de ses prédécesseurs pour la théorie algébrique des équations.

Après avoir détaillé quelques exemples, montré comment l'on peut déterminer les racines primitives d'un nombre premier à l'aide de sa méthode, et déduit des théorèmes généraux, Poinsot conclut :

> Je reviendrai ailleurs sur ce rapprochement curieux de l'algèbre et de la théorie des nombres ; et je ferai voir que les principes généraux de l'analyse mathématique ont leur source naturelle dans la simple considération de l'*ordre*, ou de la disposition mutuelle qu'on peut observer actuellement entre plusieurs objets : ce qui me paraît le plus haut point d'abstraction et de généralité où il soit permis de porter la science. [Poinsot 1820, p. 402]

Ce passage résume bien les idées fondamentales des travaux de Poinsot en algèbre et en théorie des nombres. Ici, Poinsot raisonne de manière plus générale : l'*ordre* devient le fondement de l'*analyse mathématique*. Poinsot ne précise pas ce qu'il entend par cette expression. Au XIX^e^ siècle, l'*analyse mathématique* peut désigner une méthode générale ou une discipline incluant la théorie des équations [55]. La notion d'*ordre* est également utilisée de manière plus générale que précédemment : ici, Poinsot ne relie pas l'*ordre* à des structures cycliques comme on a pu le voir jusqu'ici, mais à la *disposition mutuelle qu'on peut observer actuellement entre plusieurs objets*. Poinsot insiste ainsi sur l'importance de l'étude des relations qui peuvent exister entre les objets d'un même ensemble.

4.3. *Un retour sur la notion d'ordre*

Le mémoire se termine par une addition sur les différentes manières dont on peut partager les racines des équations binômes. Poinsot y montre dans un premier temps pourquoi l'ordre dans lequel sont rangées les racines de l'équation binôme à partir d'une racine primitive ne dépend ni de la racine r de l'équation binôme de degré n que l'on prend pour commencer, ni de la racine primitive a choisie [56].

---

55 On pourra notamment se reporter à [Sinaceur 1991, p. 51].

56 Gauss démontre également cette indépendance : on pourra se reporter à l'article 343 des *Disquisitiones Arithmeticae*.

En effet, si on considère l'ordre

$$r, r^a, r^{a^2}, r^{a^3}, \ldots, r^{a^{n-1}},$$

et que l'on parcourt les racines de h en h, où h est un nombre inférieur et premier à n. On passera alors par toutes les racines avant de revenir à celle de départ. On obtient ainsi un nouvel ordre :

$$r, r^{a^h}, r^{a^{2h}}, r^{a^{3h}}, \ldots, r^{a^{(n-2)h}}.$$

Si on pose $b = a^h$, b est également une racine primitive du nombre n, et l'ordre précédent peut s'écrire :

$$r, r^b, r^{b^2}, r^{b^3}, \ldots, r^{b^{n-1}}.$$

Poinsot nous explique alors pourquoi ces deux suites peuvent être considérées comme dans le même ordre :

> Ainsi, les différens ordres qu'on peut former en employant les différentes racines primitives de n sont comme un seul et même ordre, mais où l'on regarderait les $n-1$ racines r, r^a, r^{a^2}, r^{a^3}, & c. soit de suite ou de 1 en 1, soit de h en h, soit de h' en h', & c. ; &, h, h', & c., étant les différens nombres inférieurs et premiers à $n-1$. Et comme l'idée de cet intervalle plus ou moins grand, par lequel on va de l'une à l'autre, ne peut entrer dans l'idée de l'*ordre*, qui, par sa nature, ne dépend point de la *grandeur*, il s'ensuit que ces différens ordres coexistent tous dans un seul quelconque d'entre eux, comme les racines d'une même équation, sans qu'on puisse les distinguer ou les isoler par aucune analyse. [Poinsot 1820, p. 404]

Poinsot approfondit encore les concepts de *grandeur* et d'*ordre* dans son mémoire de 1845. On peut donc considérer les différents ordres obtenus à partir de racines primitives différentes comme équivalents si l'on ne prend en compte que la notion d'ordre. Par exemple, on peut obtenir la suite de racines $r, r^b, r^{b^2}, r^{b^3}, \ldots, r^{b^{n-1}}$ donnée par Poinsot ci-dessus en considérant les racines de la suite $r, r^a, r^{a^2}, r^{a^3}, \ldots, r^{a^{n-1}}$ de h en h. Avant de développer cette idée sur l'exemple $x^{13} - 1 = 0$, Poinsot fait à nouveau un parallèle entre la théorie des nombres et la géométrie, en reliant la disposition des racines les unes par rapport aux autres à celle des sommets d'un polygone régulier.

Après avoir donné les différents ordres équivalents que l'on peut obtenir à partir des racines de l'équation $x^{13} - 1 = 0$, Poinsot remarque que

l'intérêt de prendre cet ordre pour les racines est que cela montre que les racines sont liées deux à deux, mais plus généralement d à d, où d est un diviseur de $p-1$, soit 12 dans l'exemple actuel. Cela revient à représenter les périodes que Gauss a défini dans les *Disquisitiones Arithmeticae* pour la résolution de l'équation cyclotomique. En effet, il considère l'ordre des racines que l'on obtient à partir de la racine primitive 2 :

$$r, r^2, r^4, r^8, r^3, r^6, r^{12}, r^{11}, r^9, r^5, r^{10}, r^7.$$

On a $12 = 4 \times 3$, donc en prenant les racines de 4 en 4, on forme 4 groupes de 3 racines (ce qui correspond aux 4 périodes de Gauss formées de 3 éléments) :

$$(r, r^3, r^9) \quad (r^2, r^6, r^5) \quad (r^4, r^{12}, r^{10}) \quad (r^8, r^{11}, r^7).$$

Ces quatre groupes sont en fait constitués des racines (r^h, r^{h+4}, r^{h+8}), où h est un des nombres 1, 2, 4, 8 selon les groupes. Donc, si on remplace par exemple r^h par r^{h+4}, on obtient le groupe : $(r^{h+4}, r^{h+8}, r^{h+12})$. Or, $r^{h+12} = r^h r^{12} = r^h$, et on obtient bien le groupe de départ. Poinsot développe ici les relations existant entre les différents *groupes*, ce qui rappelle la partie *Conjugaison mutuelle des groupes* de son manuscrit sur la théorie des permutations.

Ainsi, si l'on construit une fonction φ symétrique des trois racines r, r^3, r^9, notée $\varphi(r)$, cette fonction ne prendra que quatre valeurs : $\varphi(r)$, $\varphi(r^2)$, $\varphi(r^4)$, et $\varphi(r^8)$. Donc cette fonction sera déterminée par une équation du quatrième degré. Ainsi, tout polynôme symétrique élémentaire de ces quatre fonctions sera symétrique en r, r^2, r^3, ... et pourra être déterminé.

On peut réitérer ce raisonnement en rassemblant les groupes[57] 2 à 2 : $(\varphi(r), \varphi(r^4))$ et $(\varphi(r^2), \varphi(r^4))$. Poinsot en conclut donc que la résolution de l'équation du quatrième degré se réduit à celle de deux équations quadratiques.

4.4. *Conclusion*

Même s'il l'avait auparavant présenté dans son *Extrait de quelques recherches nouvelles...*, Poinsot expose pour la première fois un nouveau

---

[57] Poinsot confond ici les écritures des groupes de racines avec celles des fonctions symétriques en ces racines. On peut observer que Gauss faisait de même dans les *Disquisitiones Arithmeticae*, lorsqu'il n'y avait pas d'ambiguïté possible.

résultat de théorie des nombres. De plus, la méthode exposée ici pour résoudre les congruences binômes est très différente de l'approche utilisée par Gauss dans les *Disquisitiones Arithmeticae*, où il raisonne à partir de la notion d'*indice*. La méthode de Poinsot s'appuie notamment sur une analogie entre la structure de l'ensemble des racines de l'équation binôme $x^n - 1 = 0$ d'une part et celle des racines des congruences $x^n - 1 \equiv 0$ modulo un nombre premier d'autre part. C'est cette analogie qui l'autorise (bien sûr sans aucune justification) à transposer des raisonnements des nombres complexes aux résidus modulo p. D'autre part, il considère également des racines imaginaires modulo un nombre premier p, ce qui est un autre point original de son travail puisque celui-ci est une des premières publications sur la théorie des congruences contenant des raisonnements sur les nombres complexes.

Poinsot présente donc au lecteur un texte développant des outils innovants de théorie des nombres. Néanmoins, ce *Mémoire sur l'application de l'algèbre à la théorie des nombres* est surtout basé, comme les travaux précédents de Poinsot, sur les résultats déjà obtenus par Gauss. Poinsot s'intéresse au sujet de la section VIII inédite des *Disquisitiones Arithmeticae* : les congruences supérieures développées en parallèle avec les équations. D'autre part, comme nous l'avons indiqué précédemment, Poinsot se réfère régulièrement à Gauss et Lagrange dans ses raisonnements autour de la théorie algébrique des équations et utilise explicitement leurs méthodes. Par contre, il est étonnant de ne trouver pratiquement aucune référence[58] sur les résultats relatifs à la théorie des résidus quadratiques lorsqu'il travaille sur les racines carrés modulo un nombre premier p. On peut également remarquer que Poinsot n'utilise pas la notation $\equiv$ des congruences, introduite par Gauss en 1801 dans les *Disquisitiones Arithmeticae*, mais celle de Legendre.

Comme dans ses textes précédents, Poinsot insiste sur la notion d'*ordre*, notamment dans son *Addition*. On y retrouve une étude de la structure de l'ensemble des racines des équations binômes et des congruences binômes, très semblable à ce qui est exposé dans son manuscrit sur la

58 Poinsot renvoie à Euler pour l'introduction des racines primitives. Cette référence est néanmoins faite dans le cadre de la résolution des équations binômes.

théorie des permutations. De plus, la notion d'*ordre* est caractérisé de manière plus précise dans son mémoire. On y retrouve des définitions claires à deux reprises. La première fois, il est défini dans le cadre de l'étude de structures cycliques : les objets considérés doivent *naître successivement les uns des autres par la même loi, ou même fonction.* La seconde caractérisation est plus générale : « la disposition mutuelle qu'on peut observer actuellement entre plusieurs objets » [Poinsot 1820, p. 402].

Le travail de Poinsot sur la résolution des congruences binômes n'est pas cité dans le cours d'*Algèbre supérieure* de Serret par exemple, bien que ce manuel contienne un chapitre sur les congruences dans chaque édition. Serret fait référence à Poinsot en ce qui concerne des méthodes exposées dans son mémoire de 1845 mais ne fait aucune allusion à son travail sur l'analogie que l'on peut retrouver entre la résolution des équations et celle des congruences. Il cite par contre Galois et l'utilisation des imaginaires dans les congruences.

D'un autre côté, ce même travail est cité en exemple par Smith dans son article *Solution of the Congruence* $x^n \equiv 1$, *mod* p que l'on retrouve dans le *Report on the Theory of Numbers* :

> The methods of Gauss, Lagrange, and Abel for the solution of the binomial equation $x^n - 1 = 0$ are in a certain sense applicable to binomial congruences of this special form. It is evident, from a comparison of several passages in the Disquisitiones Arithmeticae [Smith cite les articles 61, 73 et 335], that Gauss himself contemplated this arithmetical application of his theory of the division of the cercle, and that he intended to include it in the 8th section of his work, which, however, has never been given to the world. [...] When, for any prime modulus, an Abelian equation admits of being considered as an Abelian congruence, so precise is the correspondance of the equation and the congruence, that (as Poinsot has observed in a memoir in which he has occupied himself with the comparative analysis of the equation $x^n - 1 = 0$, and the congruence $x^n \equiv 1 \pmod{p}$) we may consider the analytical expression of the roots of the equation as also containing an expression of the roots of the congruence; and by giving a congruential interpretation to the radical signs which occur in that expression, we may elicit from it the actual values of the roots of the congruence. An exemple taken from Poinsot's memoir will rend this intelligible. [Smith 1859–1865, p. 141–142, art. 66]

Après avoir détaillé l'exemple développé par Poinsot, Smith conclut : « Theorically, however, the relation between the analytical expression of the equation-roots and the values of the congruence-roots is of considerable importance, and the subject would certainly repay a closer examination than it has yet received » [Smith 1859–1865, p. 144, art. 66].

5. LA NOTION D'ORDRE CHEZ POINSOT

5.1. *L'utilisation des analogies chez Poinsot*

L'analogie joue un rôle important dans la recherche mathématique. Selon Eberhard Knobloch, « les mathématiques sont le domaine légitime de l'analogie » [Knobloch 1991, p. 217] et poursuit :

> [...] les mathématiciens les plus créateurs et les plus féconds comme Johannes Kepler, John Wallis, Leibniz, Isaac Newton, Leonhard Euler, Pierre Simon de Laplace ont mis en évidence le rôle éminent de l'analogie pour la découverte de nouvelles vérités mathématiques.
>
> Ils distinguaient le contexte de la découverte du contexte de la justification : d'après cela, l'analogie guide la connaissance mais ne la justifie pas. [Knobloch 1991, p. 217-218]

En particulier, les analogies jouent un rôle significatif dans les travaux de Poinsot. Bien sûr, son *Mémoire sur l'application de l'algèbre à la théorie des nombres* est basé sur l'étude de l'analogie entre les équations et les congruences binômes. Mais on remarque également qu'il produit des raisonnements très analogues pour décrire d'une part les ensembles de permutations en 1808 et 1818 et d'autre part les ensembles de racines d'équations binômes de 1808 à 1820. Ces deux types d'analogies développées par Poinsot entrent bien dans le *contexte de découverte* annoncé par Knobloch comme nous allons le voir ci-dessous.

5.1.1. *Analogies dans les procédés opératoires*

Le *Mémoire sur l'application de l'algèbre à la théorie des nombres*, publié en 1820, Poinsot annonce qu'il a « observé [des] propriétés analogues » entre deux types de nombres — les racines des congruences binômes et les racines des équations binômes — et que cela l'a amené à considérer une analogie entre les expressions des solutions de ces congruences et équations. À

partir de cette analogie, il en déduit son théorème qu'il démontre en transposant les opérations [59] valables pour les nombres complexes aux nombres modulo un nombre premier p.

D'une part, Poinsot affirme que l'analogie à partir de laquelle il a obtenu son résultat sur les congruences binômes peut être étendue à toutes les équations résolubles. À ce sujet, Smith remarque que le principe de Poinsot est effectivement valide pour les équations et congruences jusqu'au quatrième degré mais que pour les équations de degré supérieur résolubles, la démonstration de Poinsot n'est plus suffisante :

> But this reasoning ceases to be applicable to equations of an order higher than the fourth, because no general formula exists representing the roots of an equation of the fifth or any higher order. If, therefore, $F(x) = 0$ be an equation of the nth order, the roots of which can be expressed by a radical formula, and which is also completely resoluble when considered as a congruence for the modulus p, so that $F(x) \equiv (x-a_1)(x-a_2)\ldots(x-a_n)$, mod. p, it will not necessarily follow that the formula which gives the roots of $F(x) = 0$ is also capable (when we add multiples of p to the numbers contained in it) of giving the roots of $(x-a_1)(x-a_2)\ldots(x-a_n) = 0$, *i. e* the roots of the congruence $F(x) \equiv 0$, mod p ; and thus the principle enunciated by M. Poinsot is, it would seem, not rigorously demonstrated. [Smith 1859–1865, p. 145]

Poinsot donne d'ailleurs une précision à ce sujet dans son mémoire de 1820, mais sans soulever le problème de savoir si on peut supposer *a priori* que les formules donnant les expressions des racines d'une équation de degré n, $n > 4$, peuvent être dans tous les cas transposées pour donner les expressions des racines de la congruence correspondante :

> Quant à notre démonstration considérée en elle-même, on verra qu'elle réside, au fond, bien plutôt dans la supposition d'une formule générale qui résoudrait la proposée, que dans la manière d'obtenir cette formule ; et même les géomètres sentiront d'abord comment le théorème que je propose s'étendrait à une équation complète, dont la résolution algébrique serait supposée connue. Il suffirait de considérer que les coefficiens de cette équation sont les mêmes, aux multiples près du module, que ceux de l'équation semblable déterminée

[59] Sur la question des analogies utilisées au XIX^e siècle pour transférer des processus opératoires, voir [Durand-Richard 2008]. Une originalité de Poinsot est la place accordée à la cyclicité dans ce transfert.

qui aurait les mêmes racines ; que par conséquent la formule générale qui résoudrait la première équation, conviendrait à la seconde, en restituant aux coefficiens les multiples du module et nous donnerait ainsi les racines entières de la proposée. [Poinsot 1820, p. 348]

D'autre part, dans sa démonstration, il traduit une démonstration valable dans $\mathbb{C}$ en une démonstration dans $\mathbb{Z}/p\mathbb{Z}$, une fois de plus sans justifier rigoureusement les propriétés de cet ensemble et poser explicitement des questions à ce sujet. Il reproduit simplement des suites d'égalités algébriques en argumentant que l'on peut ajouter ou supprimer des multiples de p. Quelques années plus tard, Libri produit le même type de raisonnement dans son mémoire, intitulé *Mémoire sur la théorie des nombres*, publié en 1825. Il affirme que le théorème de Poinsot sur l'analogie des équations $x^n - 1 = 0$ et $x^n - 1 \equiv 0 \pmod{a}$, où a est un nombre quelconque, est évident « dans tous les cas », c'est-à-dire pour toutes les équations algébriques. En effet : « si l'on ajoute des multiples de a sous les radicaux compris dans l'expression des racines de cette équation, on aura les racines de la congruence proposée. » [Libri 1838, p. 21]. Dans ces deux cas, Poinsot et Libri manipulent des expressions algébriques, les transforment sans se poser la question de l'existence des objets avec lesquels ils travaillent.

D'un point de vue moderne, Poinsot transpose donc des raisonnements sur des équations valables dans $\mathbb{C}$ à des raisonnements analogues sur des congruences dans $\mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier. $\mathbb{C}$ et $\mathbb{Z}/p\mathbb{Z}$ ont à la fois des propriétés communes (par exemple, ce sont des corps), et des différences profondes. Poinsot, pas plus que Libri plus tard, ne semble jamais s'interroger sur les propriétés qui permettent (ou non) le transfert d'un ensemble à l'autre.

Dans son *Report on the Progress and Present Sate of certain Branches of Analysis*[60], George Peacock (1791–1858) résume et analyse également le travail de Poinsot sur l'équation $x^n - 1 = Mp$:

Poinsot has given a very remarkable extension to the theory of the solution of the binomial equation $x^n - 1 = 0$, by showing that its imaginary roots may be considered in a certain sense as the analytical representation of the whole

60 Ce rapport est contenu dans le *Report of the Third Meeting of the British Association for the Advancement Of Science.* Cette rencontre à eu lieu à Cambridge en 1833.

numbers which satisfy the congruence or equation $x^n - 1 = M(p)$ whose *modulus* (a prime number) is p [...]

These views of Poinsot are chiefly interesting and valuable as connecting the theory of indeterminate with that of ordinary equations. It has, in fact, been too much the custom of analysts to consider the theory of numbers as altogether separated from that of ordinary algebra. The methods employed have generally been confined to the specific problem under consideration, and have been altogether incapable of application when the known quantities employed were expressed by general symbols and not by specific numbers. It is to this cause that we may chiefly attribute the want of continuity in the methods of investigation which have been pursued, and the great confusion which has been occasioned by the multiplication of insulated facts and propositions which were not referable to, nor deducible from, any general and comprehensive theory. [Peacock 1834, p. 320–322]

Peacock défend donc également une théorie générale, qui ne s'applique pas seulement aux nombres entiers, ou rationnels, mais également à des quantités symboliques qui n'ont pas le statut de nombre, comme les congruences par exemple. En effet, ces réflexions de Poinsot correspondent en partie aux idées de Peacock sur l'algèbre, comme nous le préciserons plus loin.

Dans son mémoire de 1820, Poinsot ne développe pas l'analogie entre les équations et les congruences binômes uniquement dans le but de transposer la méthode de Gauss aux congruences. Il met également en avant des analogies dans la structure des ensembles des deux types de racines, analogies que l'on retrouve dispersées dans tous les textes étudiés ici.

5.1.2. *Analogies dans les structures étudiées et la notion d'ordre*

D'un point de vue moderne, si l'on liste les structures étudiées par Poinsot dans ses textes — permutations, raisonnements sur les polygones, racines des équations et congruences binômes, elles correspondent toutes à des groupes et sous-groupes cycliques. Dans chacun de ces cas, Poinsot met en avant des analogies entre ces ensembles : les relations existant entre les objets des ensembles considérés (permutations ou racines d'une équation binôme par exemple) sont similaires — elles permettent de passer d'un objet à un autre en utilisant toujours le même procédé et d'obtenir ainsi tous les objets composant l'ensemble. Il utilise cette particularité

pour partager ces ensembles en *groupes*, qui correspondent aujourd'hui à des groupes et sous-groupes cycliques. Pour décrire ces structures cycliques, Poinsot utilise d'ailleurs la même image dans tous ses textes de géométrie, d'algèbre et de théorie des nombres de 1808 à 1820 (image qu'il reprend en 1845) : celle d'objets disposés régulièrement autour d'un cercle. Cela permet à plusieurs reprises à Poinsot d'illustrer les structures qu'il étudie et d'appuyer ses décompositions en groupes et sous-groupes sur cette image de cercle. Bien sûr, Poinsot n'a pas en tête les notions de structure ou de groupe telles qu'elles seront définies à partir de la fin du XIX^e^ siècle, mais sa façon de présenter l'ensemble des permutations ou des racines des équations binômes est originale dans le sens où elle se focalise sur la manière dont on peut relier et classer ces objets entre eux à l'aide d'un même procédé opératoire qu'il nomme dans certains cas une *loi*. Ces analogies sont notamment mises en avant par le fait qu'il utilise toujours le même vocabulaire (*groupes, inséparables*, ...) pour produire ses raisonnements sur ce thème entre 1808 et 1820.

Revenons ici sur l'utilisation du mot *groupe* par Poinsot dans le cadre de son étude des structures cycliques. Lors de l'examen de celles-ci, Poinsot classe les objets étudiés en ensembles et sous-ensembles qu'il nomme systématiquement *groupes*. À la lecture du commentaire de Poinsot sur le *Traité* de Lagrange, publié en 1808, le lecteur moderne peut être surpris de retrouver à plusieurs reprises l'expression *groupe de racines* pour désigner ce qui correspond aujourd'hui à des groupes ou sous-groupes cycliques. Il peut cependant estimer que Poinsot emploie le mot *groupe* pour désigner un ensemble quelconque d'objets, sans lui donner une caractéristique particulière et que cette utilisation n'a aucun lien avec celle qu'en fera notamment Galois et ses lecteurs des années plus tard. De plus, il ne donne aucune définition de ce qu'il appelle *groupe* ou de ce qu'il qualifie d'*inséparable* dans ce texte, ni dans ses écrits ultérieurs.

Cependant, il est difficile d'ignorer le fait que Poinsot utilise ensuite ce même terme dans tous ces textes d'algèbre et de théorie des nombres, pour désigner à chaque fois un ensemble d'objets qui ne se *séparent* jamais, que ce soit pour désigner des *groupes de racines* ou des *groupes de permutations*. D'un point de vue moderne, les *groupes* de Poinsot désignent invariablement des groupes ou sous-groupes cycliques. Certes, comme à

de nombreuses reprises, Poinsot ne donne aucune définition de ce terme, comme s'il l'utilisait dans son sens courant, sans aucune caractéristique supplémentaire, c'est-à-dire une réunion quelconque d'objets dans un ensemble. Cette hypothèse semble cependant peu plausible. Il nous paraît juste d'affirmer que pour Poinsot, un *groupe* désigne un ensemble d'objets tel que l'on peut obtenir tous ces objets à partir d'un seul, en lui appliquant à plusieurs reprises un même procédé et tel qu'il est impossible d'obtenir un objet n'appartenant pas à ce groupe en appliquant ce procédé à un objet appartenant au groupe. On est donc encore très loin de la définition mathématique actuelle du mot *groupe*, ou même du *groupe cyclique*. Néanmoins, Poinsot utilise ce terme du vocabulaire courant dans un sens technique qu'il n'explicite pas. On observe donc le début d'une transformation sémantique : un terme du vocabulaire courant commence à prendre une signification technique nouvelle ; ce même mot désignera quelques dizaines d'années plus tard une notion mathématique abstraite, définie rigoureusement. Par contre, il semble à l'heure actuelle impossible d'affirmer qu'il y a une quelconque relation entre l'utilisation du mot *groupe* par Poinsot dans ce cadre bien particulier et le fait que, quelques années plus tard, ce même mot sera également utilisé dans un sens mathématique, plus général, par le mathématicien Galois. Enfin, on trouve une note sur Poinsot et sur son utilisation du mot *groupe* dans l'*Encyclopédie des sciences mathématiques pures et appliquées*[61] :

> *L. Poinsot* [Recherches sur l'Algèbre et sur la Théorie des nombres, mémoire présenté à la classe des sciences de l'Institut de France en mai 1813, publié Mém. classe sc. math. phys. Institut France 14 (1813/5), éd. 1818, p. 382] fait déjà usage du mot « groupe » dans un sens technique. Il y parle de « groupes de permutations associées entre elles », de « groupes principaux et secondaires de permutations » et de « groupes semblables ». [Meyer & Molk 1904 - 1916, p. 141]

---

61 Ce paragraphe est écrit par E. Bortolotti. La référence donnée semble inexacte : lors de la séance du 17 mai 1813, Poinsot a lu un *Mémoire sur les Permutations*, ce qui ne correspond pas au titre donné ici. Par contre, lors de la séance du 5 Mai 1817, Poinsot a bien lu un Mémoire intitulé *Extrait de quelques recherches nouvelles sur l'algèbre et la théorie des nombres.*

Ce sont ces particularités qui rendent les travaux de Poinsot différents. Néanmoins, la considération de ces structures cycliques et de ces analogies, cette vision de l'algèbre se retrouvent déjà en partie dans ce qui est la source principale des écrits de Poinsot en algèbre et en théorie des nombres : les *Disquisitiones Arithmeticae* de Gauss. En effet, dans son traité de théorie des nombres, Gauss étudie de façon récurrente des structures cycliques : dans le cadre des théories des résidus, des formes quadratiques et de la cyclotomie [62]. Les analogies sont également mises en avant, par exemple à propos de démonstrations sur des résultats relatifs aux formes quadratiques et aux résidus :

> On remarquera sur-le-champ l'analogie de la démonstration du théorème précédent, avec les démonstrations des n^os^ 45, 49 ; et effectivement, la théorie de la multiplication des classes a une grande affinité avec le sujet traité dans la Section III. [Gauss 1801, art. 306]

L'analyse des relations a également une place importante chez Gauss. José Ferreirós précise d'ailleurs ce point dans [Ferreirós 2007] en donnant plusieurs citations de Gauss issue de ses œuvres ultérieures démontrant que pour Gauss, les mathématiques sont la « science des relations » [Ferreirós 2007, p. 254]. Ainsi, Gauss écrit en 1825 :

> Les mathématiques sont ainsi, dans le sens le plus général, la science des relations dans laquelle on isole les relations de tous les contenus. [63]

Ces points communs entre les idées générales des deux mathématiciens et le fait que de nombreux passages des travaux de Poinsot consistent en des reformulations des méthodes de Gauss peuvent pousser à se demander si les travaux de Poinsot apportent réellement quelque chose par rapport aux *Disquisitiones Arithmeticae* de Gauss, publiées en 1801. Il nous semble que la formulation des travaux de Gauss par Poinsot est justement un des

---

62 L'étude des structures cycliques par Gauss est commenté dans [Goldstein et al. 2007].

63 Nous avons traduit la phrase originale : « Die Mathematik ist so im allgemeinsten Sinne die Wissenschaft der Verhältnisse, indem man von allem Inhalt der Verhältnisse abstrahirt. », issue de la page 396 du volume X-1 des *Werke* de Gauss, *Nachträge zur reinen Mathematik*, publié en 1917.

points-clés des travaux de ce dernier. En effet, pour comprendre l'importance des structures, de l'étude des relations, des analogies dans le travail de Gauss, il est nécessaire d'étudier attentivement un ouvrage volumineux de théorie des nombres. Par contre, dans ses différentes publications, Poinsot insiste explicitement sur ces points fondamentaux puisqu'il centre ses réflexions autour de la *théorie de l'ordre*.

5.2. *La théorie de l'ordre au cœur de l'algèbre et de la théorie des nombres*

C'est dans le texte publié en 1818 que Poinsot utilise pour la première fois la notion d'*ordre*, et l'expression *théorie de l'ordre*, qu'il place au cœur de l'algèbre, de la théorie des nombres et de la géométrie de situation. Ce vocabulaire est toujours employé dans le cadre de l'étude des relations entre des objets, que ce soit pour les permutations ou les racines d'équations et de congruences. Bien qu'il définisse l'ordre comme la « disposition mutuelle qu'on peut observer actuellement entre plusieurs objets » [Poinsot 1820, p. 402], la structure des ensembles étudiés est toujours cyclique : en usant des termes de Poinsot, ces objets *naissent successivement l'un de l'autre* à partir d'une même *loi*.

Lors de notre étude, nous avons signalé à plusieurs reprises la façon dont Poinsot définit l'algèbre. Ainsi, en 1808, il assimile l'algèbre à la théorie des équations. En 1817, l'algèbre est fondée sur « *la théorie de l'ordre et de la situation des choses sans aucune considération de la grandeur* » [Poinsot 1818, p. 383]. En 1818, « les principes généraux de l'analyse mathématique [qui inclut vraisemblablement l'algèbre et la théorie des nombres] ont leur source naturelle dans la simple considération de l'*ordre*, ou de la disposition mutuelle qu'on peut observer actuellement entre plusieurs objets » [Poinsot 1820, p. 402]. L'algèbre et la théorie des nombres doivent donc être basées sur cette notion d'*ordre*, c'est-à-dire sur l'étude des relations existant entre les objets étudiés. Cette caractérisation de l'algèbre, plus générale et plus moderne *a posteriori* que celle donnée par Poinsot en 1808, est remarquable. Il donne d'ailleurs dans son mémoire de 1845 une définition semblable :

> Mais il y a une algèbre supérieure, qui repose toute entière sur la théorie de l'ordre et des combinaisons, qui s'occupe de la nature et de la composition des

> formules considérées en elles-mêmes, comme de purs symboles, et sans aucune idée de valeur ou de quantité. C'est à cette partie qu'on doit rapporter la théorie profonde des équations [...] et c'est même cette seule partie élevée de la science qui mérite, à proprement parler, le nom d'*algèbre.* [Poinsot 1845, page 4]

Comme nous l'avons remarqué plus haut, Peacock développe des idées que l'on peut rapprocher de celles de Poinsot sur la partie de l'algèbre qu'il nomme *Algèbre symbolique.* Il fait partie d'un groupe de mathématiciens que Novy appelle *École Algébrique Anglaise* dans [Nový 1968] et développe une *Algèbre symbolique*[64] dans les années 1830. Il aborde la notion d'*Algèbre symbolique* dans le *Report*[65] de 1833 :

> [...] we do necessarily arrive at a new science much more general than arithmetic, whose principles, however derived, may be considered as the immediate, though not the ultimate foundation of that system of combinations of symbols which constitutes the science of algebra.
> [...] the real distinction between them [arithmetical algebra and symbolic algebra] will arise from the *supposition or assumption that the symbols in symbolical algebra are perfectly general and unlimited both in value and representation, and that the operations to which they are subject are equally general likewise.* [Peacock 1834, p. 194-195]

Pour Peacock, l'Algèbre arithmétique et l'Algèbre symbolique sont indépendantes :

> En définissant l'Algèbre symbolique comme science de l'esprit, G. Peacock affirme l'indépendance de la rationalité de ses opérations vis-à-vis des objets sur lesquels elle s'exerce. L'Algèbre arithmétique et l'Algèbre symbolique sont donc deux sciences indépendantes, l'une est science des quantités, l'autre est science des opérations. [Durand-Richard 1990, p. 146]

Ainsi, on retrouve bien une similitude entre les deux hommes sur leurs définitions de l'algèbre : l'algèbre de Peacock a pour but l'étude des opérations quand Poinsot prône une algèbre qui se base sur les relations entre

---

64 Nous nous appuyons sur l'analyse de Marie-José Durand-Richard pour les références aux travaux de Peacock. On pourra notamment se reporter à [Durand-Richard 1990] et [Durand-Richard 1996].

65 Il la développe ensuite de manière plus approfondie dans la deuxième édition de son *Treatise of Algebra.*

les objets. Néanmoins, les opérations de Peacock et les *lois* utilisées de Poinsot ne sont pas de même nature. En effet, les procédés opératoires caractérisant l'Algèbre symbolique de Peacock sont limités à quatre opérations : addition, soustraction, multiplication et division. Les *lois* de Poinsot sont plus générales : par exemple, dans ses travaux sur les permutations, Poinsot considère une *loi* permettant de passer d'une permutation à une autre qui correspond en fait à une substitution et non pas à une des quatre opérations considérées par Peacock [66].

Comme nous allons le voir dans la conclusion, on retrouve des réflexions autour de la définition de l'algèbre de Poinsot en particulier et sur sa *théorie de l'ordre* en général dans plusieurs textes de la deuxième moitié du XIX^e siècle.

CONCLUSION : POINSOT, LA THÉORIE DE L'ORDRE ET LES AUTRES

Les travaux de Poinsot en algèbre et en théorie des nombres ne contiennent que très peu de résultats nouveaux et il utilise régulièrement des objets ou des raisonnements dont il ne démontre pas la validité. Il développe des idées déjà présentes dans les *Disquisitiones Arithmeticae* mais son originalité consiste en sa façon de présenter les différentes notions étudiées autour d'un concept fondamental : l'*ordre*, c'est-à-dire l'étude des relations entre des objets. Il développe encore cette notion dans son mémoire publié en 1845 mais ses idées principales sont déjà exprimées de façon claire et précise dans les mémoires analysés dans cet article. Il pose l'*ordre* comme fondement de trois disciplines : la théorie des nombres, l'algèbre et la géométrie de situation, ce qui constitue un lien fort entre elles. Dans la section VII des *Disquisitiones Arithmeticae*, Gauss introduit un outil de théorie des nombres — les racines primitives — pour résoudre un problème d'algèbre. Comme on peut le lire dans [Goldstein & Schappacher 2007], à partir des années 1820, beaucoup de travaux liés à la théorie des nombres s'appuient sur un autre domaine des mathématiques. On retrouve déjà une utilisation d'outils algébriques et

66 Marie-José Durand-Richard discute cette limitation par Peacock aux quatre opérations dans [Durand-Richard 1990] notamment.

analytiques dans les travaux en théorie des nombres de Lagrange, mais cela deviendra plus systématique avec la génération de mathématiciens ayant étudié très tôt les *Disquisitiones Arithmeticae* de Gauss. On peut par exemple citer Lejeune-Dirichlet qui utilise les séries infinies dans ses travaux de théorie des nombres, Abel et Jacobi avec leurs travaux relatifs aux fonctions elliptiques, ou encore Kummer, Hermite, Gotthold Eisenstein (1823–1852) et Kronecker. Ces travaux font partie de ce que les auteurs de [Goldstein et al. 2007] appellent l'*arithmétique algébrique analytique*. L'œuvre de Poinsot est donc originale par rapport à ce courant, car il lie l'algèbre et l'arithmétique à la géométrie et non à l'analyse réelle ou complexe. Cela s'explique par sa vision des mathématiques liée à la notion d'*ordre* : cela l'incite à rapprocher des sujets dont l'étude est simplifiée en se basant sur cette idée.

Évaluer la portée réelle de la singularité des travaux de Poinsot reste néanmoins très difficile et ce, pour plusieurs raisons. D'une part, les travaux de Poinsot à ce sujet sont en nombre restreint. D'autre part, le peu d'indications biographiques, de correspondances à ce sujet rend plus ardu l'établissement d'un réseau autour de Poinsot. La quasi-absence de résultats nouveaux par rapport à ses prédécesseurs immédiats, en particulier Gauss, complique encore la mesure de son influence éventuelle : comment décider de celle d'un point de vue, d'une manière de voir ?

Les travaux de Poinsot publiés en 1820 et avant sont cités par des mathématiciens lors de la première moitié du XIX^e^ siècle. Comme nous l'avons indiqué précédemment, Liouville cite l'analyse du *Traité* de Lagrange de 1808, Libri reprend le travail de Poinsot sur l'analogie entre les équations et les congruences binômes. Cauchy cite également Poinsot dans ses travaux lorsqu'il définit ce qu'est une racine primitive pour une équation ou une congruence par exemple [Cauchy 1829a, p. 89]. Par contre, ces savants ne font pas de remarques relatives à sa *théorie de l'ordre*. Néanmoins, Poinsot est associé à sa *théorie de l'ordre* et à sa définition de l'algèbre à plusieurs reprises, notamment après la publication de son mémoire de 1845.

Ainsi, Cournot, dès 1825, remarque le point de vue particulier de Poinsot sur l'algèbre [67] :

---

67 Ce compte rendu, publié dans le *Bulletin de Férussac* et signé « C. », peut vraisemblablement être attribué à Cournot. En effet, René Taton arrive à cette conclusion

> On sait que parmi les géomètres de l'école actuelle, aucun n'a porté dans la philosophie des sciences mathématiques des aperçus plus nouveaux et plus piquans que M. Poinsot. Dans de précédens mémoires, il a fait voir comment la multiplicité des valeurs dont un radical algébrique est susceptible, constituait l'un des caractères propres de l'algèbre, et en faisait une science indépendante, non pas seulement une *arithmétique universelle,* comme l'appelait Newton, ou une *langue des calculs,* ainsi que le voulait Condillac. [Cournot 1825, p. 144]

En 1847, le philosophe Cournot reprend la définition de l'algèbre par Poinsot dans le cadre de la théorie de l'ordre dans *De l'origine et des limites de la correspondance entre l'algèbre et la géométrie* :

> Enfin, pour ne pas abuser des citations, suivant M. Poinsot, l'algèbre est la science de l'ordre : idée fine et profonde, mais qui a besoin de commentaire, et que l'auteur lui-même, dans un de ces derniers écrits, a lucidement commenté. [Cournot 1847, p. 61]

Il cite ensuite la définition de l'algèbre donnée par Poinsot en 1845. Cournot se réfère à plusieurs reprises à Poinsot dans ses travaux. Dans [Martin 1996], la philosophie de Cournot est d'ailleurs présentée comme « philosophie de l'ordre ». L'auteur ajoute :

> C'est dire notamment qu'elle se propose de mettre à jour la diversité des relations qui unissent les différents objets qu'elle envisage, afin d'y déceler l'organisation interne qui leur confère leur unité sur la base de leurs différences [Martin 1996, p. 24].

Cela correspond bien, de façon plus générale, aux idées développées par Poinsot dans ses travaux d'algèbre et de théorie des nombres[68].

---

dans [Taton 1947]. D'autre part, selon [Bru & Martin 2005], même si le nom de Cournot n'apparaît dans la liste des collaborateurs qu'à partir de 1826 dans le tome 5, il est fort probable que Cournot ait collaboré au journal dès le troisième tome en 1825. Bernard Bru s'est de plus intéressé au *Bulletin de Férussac* dans le cadre de la publication de écrits de jeunesse de Cournot, pour y insérer les comptes-rendus vraisemblablement écrits par celui-ci. Pour eux, il est certain que les comptes-rendus signés des lettres A. C. sont de Cournot, et fort probable que Cournot soit également l'auteur de comptes-rendus signés A. ou C.

68 Nous tenons à remercier Bernard Bru et Thierry Martin pour avoir répondu à nos interrogations sur Cournot, notamment dans le cadre de sa collaboration au *Bulletin de Férussac,* et pour nous avoir fourni des documents sur les écrits de jeunesse du philosophe. D'autre part, signalons que Poinsot a également été très proche d'Auguste

La définition de l'algèbre par Poinsot citée par Cournot est également reprise dans le *Vocabulaire technique et critique de la philosophie* de Lalande : « Algèbre [...] D. Science de l'ordre (POINSOT). Cette définition a été louée par COURNOT pour sa profondeur, dans un chapitre où il recueille une série de définitions de l'Algèbre (*Correspondance*, ch. IV) mais lui-même adopte finalement le sens C » [Lalande 1932, p. 28].

Le philosophe Louis Couturat cite Poinsot dans le cadre de la *théorie de l'ordre* dans son article *Sur les rapports du nombre et de la grandeur*, publié en 1898 dans la *Revue de Métaphysique et de Morale*. Il y explique que la notion d'ordre est déjà utilisée dans les travaux de Descartes, qui définit les mathématiques comme la « recherche de l'ordre et de la mesure » [69] et qui explique : «Toute la méthode consiste dans l'ordre et la disposition des objets». On retrouve des traces de l'importance de cette notion chez Fermat, Pascal, Leibniz et Bernoulli mais :

> ce n'est que dans ce siècle qu'elle [la science de l'ordre] a véritablement été fondée par Galois. Depuis lors (1832), elle a pris un développement extraordinaire, non seulement en prenant place dans la mathématique à côté des sciences traditionnelles et classiques, mais encore en les envahissant et en les transformant presque toutes. Cette science, que Sylvestre et Cayley appelaient la *Tactique*, et Cournot la *Syntactique*, consiste principalement dans la théorie des substitutions. [Couturat 1898, p. 437]

Galois est ici mis en avant par rapport à ses travaux de 1832, puis Couturat ajoute plus loin :

> Voyons maintenant quels sont les rapports de la théorie des substitutions avec l'algèbre. C'est à Cournot, après Poinsot[Couturat donne pour références [Cournot 1847] et [Poinsot 1845].], que revient le mérite d'avoir mis en lumière l'importance de l'idée d'ordre comme fondement des sciences mathématiques. Ces auteurs distinguent dans l'algèbre deux parties : 1° une

---

Comte : il fait partie des savants ayant assisté aux premières leçons de philosophie positiviste de Comte et l'a soutenu dans sa carrière. Les idées de Poinsot semblent également avoir été reprises par des savants proches du réseau saint-simonien, comme Despeyrous par exemple. Il serait donc intéressant de faire une analyse approfondie des liens entre Poinsot et Comte d'une part, et entre Poinsot et les saint-simoniens d'autre part.

69 Les citations de Descartes données par Couturat sont tirées de [Descartes 1701].

arithmétique universelle, fondée sur la généralisation des opérations élémentaires et sur l'extension corrélative de l'idée de nombre ; 2° la science de l'ordre et des combinaisons, science formelle et abstraite, applicable à toutes sortes d'objets et d'opérations. Cette distinction est juste et profonde ; seulement, elle est trop radicale pour qu'on puisse confondre sous le même titre deux sciences tout à fait hétérogènes. Nous réserverons donc le nom d'algèbre à l'arithmétique universelle, science du nombre généralisé, comprenant la théorie des équations, qui a pour but de déterminer des nombres inconnus par leurs relations arithmétiques avec des nombres connus ; et nous verrons dans la théorie de l'ordre une science à part, indépendante des sciences du nombre et de la grandeur, quoique pouvant leur prêter un précieux concours.

Mais si l'algèbre est bien distincte de la science de l'ordre, si même elle en est en principe indépendante, il n'en est pas moins vrai qu'elle a du y avoir recours pour la résolution algébrique des équations ; et le mérite de Galois a précisément consisté à apercevoir le secours que l'algèbre pouvait tirer de la notion d'ordre, en apparence étrangère à ses spéculations. [Couturat 1898, p. 438-439]

C'est néanmoins Poinsot qui place explicitement la notion d'ordre au cœur de l'algèbre et de la théorie des nombres dès 1818. La théorie de l'ordre de Poinsot est également mise en avant dans des manuels d'algèbre. Par exemple, on peut citer la préface du *Cours d'algèbre élémentaire* de Léon Lecointe, publié en 1859, dans laquelle l'auteur tente de définir l'algèbre :

Je définis l'algèbre : la science qui s'occupe de la détermination du nombre représentant une grandeur et de la recherche des propriétés de ce nombre, abstraction faite de toute détermination d'unité. J'aurais pu ajouter : ET QUI TRAITE DES RELATIONS QUI EXISTE ENTRE CES GRANDEURS, INDÉPENDAMMENT DES VALEURS PARTICULIÈRES DONT ELLES SONT SUSCEPTIBLES ET DES UNITÉS ARBITRAIRES L'EXPRESSION NUMÉRIQUE.

Je justifie cette définition par une autorité :

M^r^ Poinsot [Il renvoie au mémoire de Poinsot publié en 1845], après avoir établi qu'il existe une première algèbre, qu'il appelle arithmétique universelle, ajoute : « *il y a une algèbre supérieure qui repose toute entière sur la théorie de l'ordre et des combinaisons, qui s'occupe de la nature et de la composition des formules considérées en elles-mêmes comme de purs symboles et sans aucune idée de valeur ou de quantité [...] c'est même cette seule partie élevée de la science qui mérite, à proprement parler, le nom d'*ALGÈBRE. » [Lecointe 1859, Préface]

On retrouve également l'association entre la notion d'*ordre* et Poinsot dans le *Cours de Mathématiques à l'usage des candidats à l'École polytechnique, ...* publié en 1890, où De Comberousse indique dans le cadre de son exposé sur la résolution algébrique des équations :

> Nous sommes forcés d'indiquer seulement ces résultats et de renvoyer le lecteur aux écrits mêmes des savants illustres qui ont commencé à élucider ces questions si vastes et si difficiles. LAGRANGE et GAUSS, ABEL et GALOIS, CAUCHY et J. -A. SERRET, MM. BERTRAND, HERMITE, E. MATHIEU, CAMILLE JORDAN, ainsi que d'autres célèbres géomètres étrangers, ont jeté les fondements de cette Algèbre transcendante, où l'*ordre* a pris la place prédominante que lui assignait POINSOT [l'auteur donne comme référence le mémoire de 1845]. [De Comberousse 1890, p. 619]

D'autre part, Camille Jordan (1838–1922) également associe Poinsot à la théorie de l'ordre dans son *Mémoire sur le nombre des valeurs d'une fonction* : « L'étude de ces diverses sortes de symétries offre un grand intérêt car c'est la base et le point de départ naturel de ce genre de recherches que M. Poinsot a distingué de tout le reste des mathématiques,sous le nom de *théorie de l'ordre* : elle présente en outre d'importantes applications » [Jordan 1861, p. 113].

Ainsi, Poinsot est régulièrement associé à l'*ordre* après la publication de son mémoire de 1845. Par exemple, Couturat attribue l'utilisation de la notion d'*ordre* dans la théorie des équations à Galois, bien que Poinsot ait déjà signalé cette relation importante dès 1817. Il exprime également très clairement la notion d'*ordre* dès son mémoire publié en 1820.

De plus, il semble clair que, parmi les mathématiciens qui travaillent dans la suite de Galois en France, certains se réclament de l'ordre et de Poinsot. En particulier, Jordan que nous avons cité précédemment insiste à nouveau sur le rôle de la théorie de l'ordre de Poinsot dans la *Notice sur les travaux de Camille Jordan* où il présente ses propres travaux en vue d'une élection à l'Académie des Sciences pour la section géométrie. En effet, dans l'avant-propos, il cite partiellement les définitions des mathématiques, de l'algèbre et de la géométrie de situation données par Poinsot dans le mémoire de 1845 puis indique :

> Ces réflexions de Poinsot, qui ont servi d'épigraphe à mes premiers essais, caractérisent assez nettement la tendance générale de mes recherches.

> Elles ont presque constamment pour but d'approfondir la *théorie de l'ordre* au double point de vue de la Géométrie pure et de l'Analyse. [Jordan 1881, p. 8]

Finalement, Poinsot témoigne d'une réflexion théorique sur ce qui permet la résolubilité des équations, insiste sur les relations entre les racines au détriment des calculs explicites et suggère une théorie des imaginaires pour les congruences. Toutes ces incitations jouent vraisemblablement un rôle dans le développement des mathématiques de Galois, même s'il est difficile de le préciser davantage. Les mentions récurrentes à la théorie de l'ordre de Poinsot tout au long du XIX^e^ siècle montre que sa façon de voir a eu un impact sur un ensemble de mathématiciens et de philosophes. Prendre en compte Poinsot et sa théorie de l'ordre incite finalement à mieux situer l'originalité de Galois dans la théorie des équations : en particulier, l'intérêt pour la forme des relations entre racines et non pour leur calcul, le transfert de la notion de racines complexes aux congruences sont des idées déjà en discussion dans les publications des premières décennies du XIX^e^ siècle.

Remerciements

Je remercie particulièrement Catherine Goldstein et Pierre Lamandé pour leurs précieuses suggestions lors de mes recherches et de l'écriture de cet article, ainsi que les deux rapporteurs pour leurs commentaires.

BIBLIOGRAPHIE

ABEL (Niels Henrik)

[1824] Mémoire sur les équations algébriques, où l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré Christiania, 1824 ; Repr. in *Œuvres complètes*, ed. L. Sylow, S. Lie, t. 1, p.28–33, Grøndahl & Søn, Christiania.

ALFONSI (Liliane)

[2005] *Étienne Bézout (1730–1783) : mathématicien, académicien et professeur au siècle des Lumières*, Thèse, Université Paris 6, 2005.

BELHOSTE (Bruno) & LÜTZEN (Jesper)

[1984] Joseph Liouville et le Collège de France, *Revue d'Histoire des Sciences*, 37 (3–4) (1984), p. 255–304.

BERTRAND (Joseph)

[1890] Éloge historique de Louis Poinsot. Lu dans la séance publique annuelle de l'Académie des Sciences du 29 décembre 1890, Paris, Institut de France, 1890.

BEZOUT (Étienne)

[1765] Sur la résolution générale des équations de tous les degrés, *Histoire de l'Académie royale des sciences, avec les Mémoires de mathématiques et de physique*, 1765, p. 533–552.

[1764] Recherches sur le degré des équations résultantes de l'évanouissement des inconnues et sur les moyens qu'on doit employer pour trouver ces équations, *Histoire de l'Académie royale des sciences, avec les Mémoires de mathématiques et de physique*, 1764, p. 288–338.

BRU (Bernard) & MARTIN (Thierry)

[2005] Le baron de Férussac, la couleur de la statistique et la topologie des sciences, *Journal Electronique d'Histoire des Probabilités et de la Statistique*, 1(2) (2005), p. 1–43 URL `http://www.jehps.net/Novembre2005/BruMartin.pdf`.

CAPLAT (Guy (dir.))

[1986] *Les inspecteurs généraux de l'instruction publique*, INRP / CNRS, 1986.

CASSINET (Jean)

[1988] Paolo Ruffini (1765–1822) : la résolution algébrique des équations et les groupes de permutations, *Bollettino di Storia delle Scienze Matematiche*, VIII (1) (1988), p. 21–69.

CAUCHY (A. L.)

[1829] Mémoire sur la théorie des nombres, *Bulletin des sciences mathématiques, physiques et chimiques*, t. XII (1829), p. 205–221 ; Repr. in *Œuvres complètes*, ed. Académie des sciences, 2e sér. , t. 2 , p. 88–107, Gauthier-Villars, Paris, 1882–1974.

[1815a] Mémoire sur le nombre de valeurs qu'une fonction peut acquérir lorsqu'on y permute de toutes les manières possibles les quantités qu'elles renferment, *Journal de l'École polytechnique*, 17e cahier, t. X (1815), p. 1–28 ; Repr. in *Œuvres complètes*, ed. Académie des sciences, 2e sér. , t. 1 , p. 64–90, Gauthier-Villars, Paris, 1882–1974.

[1815b] Mémoire 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*, 17e cahier, t. X (1815), p. 29–97 ; Repr. in *Œuvres complètes*, ed. Académie des sciences, 2e sér. , t. 1 , p. 91–169, Gauthier-Villars, Paris, 1882–1974.

COURNOT (Antoine Augustin)

[1847] *De l'origine et des limites de la correspondance entre l'algèbre et la géométrie*, Paris : L. Hachette et Cie, 1847.

[1827] Des résidus cubiques ; par le Dr. Jacobi, *Bulletin des sciences mathématiques, astronomiques, physiques et chimiques*, 8 (1827), p. 302.

[1825] Mémoire sur l'application de l'algèbre à la théorie des nombres ; par M. Poinsot, *Bulletin des sciences mathématiques, astronomiques, physiques et chimiques*, 3 (1825), p. 144–145.

COUTURAT (Louis)

[1898] Sur les rapports du nombre et de la grandeur, *Revue de métaphysique et de morale*, VI (1898), p. 422–447.

CROSLAND (Maurice)

[1992 (2002)] *Science under control — The French Academy of Sciences, 1795–1914*, Cambridge : Cambridge Univ. Press, 1992 (2002).

DAHAN (Amy)

[décembre 1980] Les travaux de Cauchy sur les substitutions. Étude de son approche du concept de groupe, *Archive for History of Exact Sciences*, 23(4) (1980), p. 279–319.

DE COMBEROUSSE (Charles)

[1890] *Cours de Mathématiques à l'usage des candidats à l'École polytechnique, à l'École normale supérieure, à École centrale des arts et manufactures. Tome Quatrième. Algèbre Supérieure. Seconde Partie*, Paris : Gauthier Villars et Fils, 1890.

DESCARTES (René)

[1701] Regulae ad directionem ingenii, dans *Opuscula posthuma, physica et mathematica*, Amsterdam : P. & J. Blaeu, 1701 ; Repr. in *Œuvres de Descartes, publiées par Victor Cousin*, t. 11 , p. 216–329, F.-G. Levrault, Paris, 1826.

DESPEYROUS (Théodore)

[1884] *Cours de Mécanique par M. Despeyrous, avec des Notes par M. G. Darboux, Tome Premier*, Paris : A. Hermann, Librairie Scientifique, 1884.

[1865a] Sur la détermination des nombres de valeurs que prennent les fonctions par les permutations des lettres qu'elles renferment, *Journal de Mathématiques Pures et Appliquées*, 10 (2^{e} série) (1865), p. 54–64.

[1865b] Classifications des permutations d'un nombre quelconque de lettres en groupes de permutations inséparables, *Journal de Mathématiques Pures et Appliquées*, 10 (2^{e} série) (1865), p. 177–202.

[1861] Mémoire sur la théorie générale des permutations, *Journal de Mathématiques Pures et Appliquées*, 6 (2^{e} série) (1861), p. 417–439.

DURAND-RICHARD (Marie-José)

[1996] L'Ecole algébrique anglaise : les conditions conceptuelles et institutionnelles d'un calcul symbolique comme fondement de la connaissance, dans Goldstein (Catherine), Gray (Jeremy) & Ritter (Jim), éd., *L'Europe mathématique — Mythes, histoires, identités*, Paris : Editions de la Maison des sciences de l'homme, 1996, p. 445–478.

[1990] Genèse de l'Algèbre symbolique en Angleterre : une influence possible de John Locke, *Revue d'histoire des sciences*, 43, n° 2–3 (1990), p. 129–180.

DURAND-RICHARD (Marie-José), éd.

[2008] *L'analogie dans la démarche scientifique*, Paris : L'Harmattan, 2008.

EHRHARDT (Caroline)

[2010] La naissance posthume d'Évariste Galois (1811–1832), *Revue de synthèse*, 131 (6e série, n° 4) (2010), p. 543–568.

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

EULER (Leonhard)

[1774] Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia, dans *Novi Commentarii academiae scientiarum Petropolitanae*, vol. 18, 1774, p. 85–135.

[1741] Solutio problematis ad geometriam situs pertinentis, dans *Commentarii academiae scientiarum Petropolitanae*, vol. 8, 1741, p. 128–140.

FERREIRÓS (José)

[2007] The Rise of Pure Mathematics as Arithmetic with Gauss, dans Goldstein (Catherine), Schappacher (Norbert) & Schwermer (Joachim), éd., *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Berlin : Springer, 2007, p. 234–268.

FREI (Günther)

[2007] The Unpublished Section Eight : On the Way to Function Fields over a Finite Field, dans Goldstein (Catherine), Schappacher (Norbert) & Schwermer (Joachim), éd., *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Berlin : Springer, 2007, p. 159–198.

GALOIS (Évariste)

[1908] *Manuscrits de Évariste Galois, publiés par Jules Tannery*, Paris : Gauthier Villars, 1908.

[1830] Sur la théorie des nombres, *Bulletin des sciences mathématiques, physiques et chimiques*, 13 (1830).

GAUSS (Carl Friedrich)

[1863] *Werke, Band II, Höhere Arithmetik*, Göttingen : ed. Königliche Gesellschaft der Wissenschaften zu Göttingen., 1863 ; Repr. in 2nd éd. augm., 1876.

[1801] *Disquisitiones Arithmeticae*, Leipzig : Fleischer, 1801 ; traduction française par A. C. M. Poullet-Delisle, *Recherches arithmétiques*, Courcier, Paris, 1807.

GOLDSTEIN (Catherine) & SCHAPPACHER (Norbert)

[2007] A Book in Search of a Discipline (1801–1860), dans Goldstein (Catherine), Schappacher (Norbert) & Schwermer (Joachim), éd., *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Berlin : Springer, 2007, p. 3–65.

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

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

GUIMARÃES (Rodolphe)

[1900] *Les mathématiques en Portugal*, Coïmbre : Imprimerie de l'Université, 1900.

HAMBURG (Robin Rider)

[1976/77] The theory of equations in the 18th century : the work of Joseph Lagrange, *Archive for History of Exact Sciences*, 16(1) (1976/77), p. 17–36.

HOUZEL (Christian)

[2002] *La géométrie algébrique. Recherches historiques*, Paris : Librairie Scientifique et Technique Albert Blanchard, 2002.

JACOBI (Carl Gustav Jacob)

[1827] De residuis cubicis commentatio numerosa, *Journal für die reine und angewandte Mathematik*, 2 (1827), p. 66–69.

JORDAN (Camille)

[1881] *Notice sur les travaux de M. Camille Jordan, ingénieur des Mines, professeur à l'École polytechnique, à l'appui de sa candidature à l'Académie des Sciences (section de géométrie)*, Paris : Gauthier Villars, 1881.

[1861] Mémoire sur le nombre des valeurs d'une fonction, *Journal de l'École polytechnique*, 22 (1861), p. 113–194.

KNOBLOCH (Eberhard)

[1991] L'analogie et la pensée mathématique, dans Rashed (Roshdi), éd., *Mathématiques et philosophie de l'Antiquité à l'âge classique*, Paris : CNRS, 1991, p. 217–237.

LAGRANGE (Joseph-Louis)

[1770] Réflexions sur la résolution algébrique des équations, dans *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin, années 1770 et 1771*, vol. 3, Berlin, 1770 ; Repr. in *Œuvres*, vol. 3 , p. 205-421, Gauthier-Villars, Paris, 1869.

[1808] *Traité de la résolution des équations numériques de tous les degrés, avec des Notes sur plusieurs points de la Théorie des équations algébriques*, Paris : Courcier, 2e éd. édition, 1808 ; Repr. in. 3e éd., conforme à celle de 1808, et précédée d'une Analyse de l'Ouvrage par M. POINSOT, Bachelier, 1826.

LALANDE (André)

[1932] *Vocabulaire technique et critique de la philosophie*, Paris : Quadrige - PUF, 1932.

LEBESGUE (Henri)

[1922] L'œuvre mathématique de Georges Humbert, quelques mots sur Camille Jordan (Extrait de la leçon inaugurale de mathématiques donnée au Collège de France le 6 janvier 1922), *Bulletin des sciences mathématiques*, 57 (1922), p. 220–233.

LECOINTE (Léon)

[1859] *Cours d'algèbre élémentaire*, Bruxelles : Emile Flatau, 1859.

LIBRI (Guglielmo)

[1838] Mémoire sur la théorie des nombres, dans *Mémoires présentés par divers Savants à l'Académie Royale des Sciences de l'Institut de France ; sciences mathématiques et physiques*, vol. 5, 1838, p. 1–75 ; Lu à l'Académie Royale des Sciences le 15 juin 1825.

LUCAS (Edouard)

[1891] *Récréations Mathématiques*, Paris : Gauthier Villars et fils, 1891 ; Repr. in 2e éd., Sceaux, Jacques Gabay, 1991.

MARTIN (Thierry)

[1996] *Probabilités et critique philosophique selon Cournot*, Paris : Vrin, 1996.

MEYER (Franz) & MOLK (Jules), éd.

[1904 - 1916] *Encyclopédie des sciences mathématiques pures et appliquées, tome I : Arithmétique et Algèbre (4 vols)*, Paris, Leipzig : Gauthier-Villars, Teubner, 1904 - 1916 ; Repr. in 2e éd., Paris, Jacques Gabay, 1992.

NEUMANN (Olaf)

[2007a] Cyclotomy : From Euler through Vandermonde to Gauss, dans Bradley (Robert E.) & Ed (Sandifer), éd., *Leonhard Euler : Life, Work and Legacy*, Amsterdam : Elsevier, 2007, p. 323–362.

[2007b] The *Disquisitiones Arithmeticae* and the Theory of Equations, dans Goldstein (Catherine), Schappacher (Norbert) & Schwermer (Joachim), éd., *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Berlin : Springer, 2007, p. 107–127.

[2005] Carl Friedrich Gauss's Disquisitiones Arithmeticae (1801), dans Grattan-Guinness (I.), éd., *Landmark Writings in Western Mathematics 1640–1940*, Amsterdam : Elsevier Science, 2005, p. 303–315.

[1979–1980] Bemerkungen aus heutiger Sicht über Gauss' Beiträge zu Zahlentheorie, Algebra und Funktionentheorie., *NTM-Schriftenreihe*, 16 : 2, 22–39 ; 17 : 1, 32–48 ; 17 : 2, 38–58 (1979–1980).

NOVÝ (Luboš)

[1968] L'École Algébrique Anglaise, *Revue de Synthèse*, 49–52 (1968), p. 211–222.

ORE (Øystein)

[1957] *Niels Henrik Abel : Mathematician extraordinary*, Minneapolis : University of Minnesota Press, 1957.

PEACOCK (George)

[1834] Report on the recent Progress and present State of certain Branches of Analysis, dans *Report of the Third Meeting of the British Association for the Advancement Of Science*, London : John Murray, Albemarle Street, 1834, p. 185–352.

POINSOT (Louis)

[1845] Réflexion sur les principes fondamentaux de la théorie des nombres, *Journal de Mathématiques Pures et Appliquées*, 10 (1845), p. 1–101.

[1820] Mémoire sur l'application de l'algèbre à la théorie des nombres, *Journal de l'École polytechnique*, 11 (1820), p. 342–410.

[1818] Extrait de quelques recherches nouvelles sur l'algèbre et la théorie des nombres, dans *Mémoires de la classe des sciences mathématiques et physiques de l'Institut de France, Années 1813, 1814, 1815*, Paris : Firmin Didot, 1818, p. 381–392.

[1810] Mémoire sur les Polygones et les Polyèdres, *Journal de l'École polytechnique*, 10^{e} cahier, Tome IV (1810), p. 16–49.

[1808] Analyse du Traité de la Résolution des Équations numériques... par J.-L. Lagrange, *Magasin encyclopédique, ou Journal des Sciences, des lettres et des arts*, 4 (1808), p. 343–375.

POINSOT (Louis) & BAILHACHE (Patrice)
[1975] *La théorie générale de l'équilibre et du mouvement des systèmes. Édition critique et commentaires par Patrice Bailhache*, Paris : Vrin, 1975.

SERRET (Joseph-Alfred)
[1866] *Cours d'algèbre supérieure*, vol. II, Paris : Gauthier-Villars, 3e édition édition, 1866.

SINACEUR (Hourya)
[1991] *Corps et Modèles*, Paris : Vrin, 1991.

SMITH (Henry J. S.)
[1859–1865] Report on the Theory of Numbers, dans *Report of the British Association for the Advancement of Science*, Oxford Clarendon Press, 1859–1865, p. 1859, 228–267 ; 1860, 120–169 ; 1861, 292–340 ; 1862, 503–526 ; 1863, 768–786 ; 1865, 322–375 ; Repr. in *The collected mathematical papers*, ed. J.W.L. Glaisher, vol. 1, p. 38–364, Oxford, Clarendon Press, 1894.

TATON (René)
[1947] Les mathématiques dans le « Bulletin de Férussac », *Archives internationales d'histoire des sciences*, 26 (1947), p. 100–125.

VANDERMONDE (A.T.)
[1774] Mémoire sur la résolution des équations, dans *Histoire et Mémoires de l'Académie des Sciences, année 1771*, 1774, p. 365–416.

VUILLEMIN (Jules)
[1962] *La philosophie de l'algèbre*, Paris : Presses Universitaires de France, 2e éd., 1993 édition, 1962.

WARING (Edward)
[1770] *Meditationes Algebraicæ*, Cantabrigiae : Typis Academis Excudebat J. Archdeacon. Veneunt apud J. Woodyer, 1770.

WUSSING (Hans)
[1984] *The genesis of the abstract group concept*, Cambridge, MA : MIT Press, 1984.

ANNEXE A : QUAND POINSOT A-T-IL ÉCRIT SON TEXTE SUR LES PERMUTATIONS ?

Comme nous l'avons indiqué précédemment, nous pensons que ce manuscrit correspond au texte sur la théorie des permutations lu par Poinsot à l'Académie des Sciences le 17 mai 1813. Nous allons donc développer ici les raisons de cette hypothèse.

D'une part, nous avons connu l'existence de ce travail sur les permutations grâce au mémoire lu à l'Académie le 5 mai 1817 par Poinsot [70] : après avoir introduit la notion de *théorie de l'ordre*, point commun entre plusieurs de ses travaux, il résume un mémoire de mai 1813 concernant la théorie des permutations sur les quatre premiers paragraphes, et ceux-ci sont très similaires à certains passages du manuscrit sur les permutations. D'autre part, la qualité du manuscrit présent à l'Institut de France est bonne, et l'écriture très lisible, ce qui laisse à penser que ce texte avait été travaillé et était achevé, prêt à être lu ou publié. Il est donc plausible que cela corresponde à un travail à présenter devant l'Académie.

De plus, on retrouve les idées présentées par Poinsot dans ce manuscrit dans plusieurs de ses textes présentés en 1813 ou avant. On retrouve par exemple dans le commentaire du *Traité* de Lagrange (1808) des raisonnements sur des *groupes de racines*, où le mot *groupe* semble déjà avoir la signification que Poinsot utilise dans le manuscrit. Le paragraphe concernant l'équation binôme du 13^{e} degré cité précédemment page 60 de cet article contient des idées très similaires à celles que l'on retrouve dans le manuscrit.

Les Procès Verbaux de l'Académie des Sciences permettent également de confirmer le fait qu'en 1813, Poinsot est convaincu de l'importance de la théorie des permutations dans la théorie générale des équations. En effet, lors de la séance du 27 décembre 1813, Poinsot lit un rapport sur un mémoire de M. Corancez :

> [...] Telle est la méthode nouvelle contenue dans le Mémoire de M. Corancez. Si nous la considérons d'abord du côté de la théorie des équations, nous ne voyons pas qu'elle puisse répandre une lumière nouvelle sur leur résolution générale. Les principes qui regardent ce problème célèbre résident essentiellement dans la théorie des combinaisons et dans celle des nombres. C'est ce qu'on peut démontrer par la nature même des choses, et, sous ce point de vue général, Vandermonde et l'illustre Lagrange semblent avoir porté la recherche presque aussi loin qu'elle pouvait aller ; du moins, s'il est possible de l'avancer encore,

70 Voir [Poinsot 1818].

ce n'est que par des idées du même genre et par quelques éléments nouveaux qui manquent encore à la théorie des permutations. [71]

Ainsi, il paraît tout à fait cohérent que Poinsot ait fait des recherches sur les permutations à cette époque.

Réciproquement, on retrouve à la page 136 de notre transcription du manuscrit cette remarque de Poinsot :

> Je passe à une exposition plus claire et plus rapide, et qui est tirée de la considération des nouveaux polygones que nous avons fait connaître. Cette théorie des polygones a une liaison intime avec la résolution générale des équations et la théorie des nombres.

Or, les travaux de Poinsot sur les polygones ont été lus en 1809 devant l'Académie, et publiés en 1810 dans le *Journal de l'École polytechnique.* Cela correspond donc bien à l'appellation « nouveaux polygones ». On peut donc penser que ce manuscrit a été écrit — ou au moins lu — peu de temps après les recherches de Poinsot sur les polygones et les polyèdres.

Finalement, il est très probable que Poinsot ait produit ce manuscrit pour le lire à l'Académie en 1813. Il est même possible que ces idées aient été relativement claires pour Poinsot avant cette période là. Il reste par contre difficile de savoir si Poinsot a développé ces idées dès le début de sa carrière, soit bien avant les travaux de Cauchy. Les travaux de Cauchy, lus en 1812, ont pu lui permettre d'étudier plus facilement les différents groupes de permutations. Néanmoins, on retrouve également dans le texte de ce dernier le fait que les permutations puissent être rangées « en cercle ou plutôt en polygone régulier » [Cauchy 1815a, p. 75], raisonnement qui est mis en avant dans le texte de Poinsot sur les polygones et polyèdres dès 1809.

---

71 *Procès-Verbaux des séances de l'Académie,* tome V (An 1812–1815), Imprimerie de l'Observatoire d'Abbadia, 1914, page 294.

ANNEXE B : MANUSCRIT DE POINSOT SUR LA THÉORIE DES PERMUTATIONS [72]

Sur le degré des équations d'où dépend une fonction quelconque des racines d'une équation proposée

Soient a, b, c, d, & c. les racines et $(a, b, c, d, \dots) = \varphi$ la fonction donnée où l'on suppose que les racines a, b, c, d, ... ne sont pas traitées de la même manière ; qu'on représente même plus simplement la fonction φ par la permutation $abcd\dots$; toutes les valeurs de φ seront représentées par les diverses permutations $abcd\dots$, $abdc\dots$, $bacd\dots$, & c des m lettres a, b, c, d, & c, et la fonction φ aura, comme on sait, $1.2.3.4\dots m$ valeurs et dépendra immédiatement d'une équation de ce degré dont on pourra calculer tous les coefficients.

Or il s'agit de faire voir que cette équation ne renferme au fond que la difficulté des degrés respectifs 2, 3, 4, ... m.

Pour nous faire mieux comprendre, considérons seulement l'équation du 5^e degré et ses cinq racines a, b, c, d, e ; on aura $1.2.3.4.5 = 120$ permutations ou valeurs de la fonction φ.

Or, ces 1.2.3.4.5. permutations peuvent être partagées en 5 groupes principaux de 1.2.3.4 permutations chacun et tels que les permutations d'un même groupe ne se séparent jamais malgré tous les échanges qu'on pourrait faire entre les lettres a, b, c, d, e. En effet, mettez ensemble toutes les permutations qui commencent par a ; ensemble toutes celles qui commencent par b, par c, par d, par e ; il est manifeste à [73] l'aspect de ce tableau, que dans tous les échanges possibles des quatre lettres b, c, d, e, le premier groupe où toutes les permutations commencent par a, restera à sa place ; et que dans l'échange de a avec une des quatre autres lettres b, c, d, e, ce groupe passera tout entier à la place d'un autre, lequel reviendra à la place du premier.

---

72 Nous remercions Michèle Vergne et Gérard Laumon, membres de l'Académie des Sciences, ainsi que Mireille Pastoureau, directeur de la Bibliothèque de l'Institut, pour nous avoir donné accès à ce manuscrit. Nous remercions également la Commission des bibliothèques et archives de l'Institut de France ainsi que sa présidente, Madame Hélène Carrère d'Encausse, secrétaire perpétuel de l'Académie française, pour leur autorisation de publier ce manuscrit dans nos travaux. Le texte présenté ici est contenu dans les feuillets 92 à 107 du manuscrit MS954. Le manuscrit original ne contient aucune rature.

73 Le tableau suivant est placé à cet endroit dans le manuscrit.

a	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*	*a*
e	*b*	*c*	*d*	*e*	*b*	*c*	*d*	*e*	*b*	*c*	*d*	*e*	*b*	*c*	*d*	*e*	*b*	*c*	*d*	*e*	*b*	*c*	*d*
b	*e*	*d*	*c*	*c*	*d*	*e*	*b*	*d*	*c*	*b*	*e*	*b*	*e*	*d*	*c*	*c*	*d*	*e*	*b*	*d*	*c*	*b*	*e*
c	*d*	*e*	*b*	*d*	*c*	*d*	*e*	*b*	*e*	*d*	*c*	*d*	*c*	*b*	*e*	*b*	*e*	*d*	*c*	*c*	*d*	*e*	*b*
d	*c*	*b*	*e*	*b*	*e*	*b*	*c*	*c*	*d*	*e*	*b*	*c*	*d*	*e*	*b*	*d*	*c*	*b*	*e*	*b*	*e*	*d*	*c*
b	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*	*b*
e	*a*	*c*	*d*	*e*	*a*	*c*	*d*	*e*	*a*	*c*	*d*	*e*	*a*	*c*	*d*	*e*	*a*	*c*	*d*	*e*	*a*	*c*	*d*
a	*e*	*d*	*c*	*c*	*d*	*e*	*a*	*d*	*c*	*a*	*e*	*a*	*e*	*d*	*c*	*c*	*d*	*e*	*a*	*d*	*c*	*a*	*e*
c	*d*	*e*	*a*	*d*	*c*	*a*	*e*	*a*	*e*	*d*	*c*	*d*	*c*	*a*	*e*	*a*	*e*	*d*	*c*	*c*	*d*	*e*	*a*
d	*c*	*a*	*e*	*a*	*e*	*d*	*c*	*c*	*d*	*e*	*a*	*c*	*d*	*e*	*a*	*d*	*c*	*a*	*e*	*a*	*e*	*d*	*c*
c	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*
e	*a*	*b*	*d*	*e*	*a*	*b*	*d*	*e*	*a*	*b*	*d*	*e*	*a*	*b*	*d*	*e*	*a*	*b*	*d*	*e*	*a*	*b*	*d*
a	*e*	*d*	*b*	*b*	*d*	*e*	*a*	*d*	*b*	*a*	*e*	*a*	*e*	*d*	*b*	*b*	*d*	*e*	*a*	*d*	*b*	*a*	*e*
b	*d*	*e*	*a*	*d*	*b*	*a*	*e*	*a*	*e*	*d*	*b*	*d*	*b*	*a*	*e*	*a*	*e*	*d*	*b*	*b*	*d*	*e*	*a*
d	*b*	*a*	*e*	*a*	*e*	*d*	*b*	*b*	*d*	*e*	*a*	*b*	*d*	*e*	*a*	*d*	*b*	*a*	*e*	*a*	*e*	*d*	*b*
d	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*	*d*
e	*a*	*b*	*c*	*e*	*a*	*b*	*c*	*e*	*a*	*b*	*c*	*e*	*a*	*b*	*c*	*e*	*a*	*b*	*c*	*e*	*a*	*b*	*c*
a	*e*	*c*	*b*	*b*	*c*	*e*	*a*	*c*	*b*	*a*	*e*	*a*	*e*	*c*	*b*	*b*	*c*	*e*	*a*	*c*	*b*	*a*	*e*
b	*c*	*e*	*a*	*c*	*b*	*a*	*e*	*a*	*e*	*c*	*b*	*c*	*b*	*a*	*e*	*a*	*e*	*c*	*b*	*b*	*c*	*e*	*a*
c	*b*	*a*	*e*	*a*	*e*	*c*	*b*	*b*	*c*	*e*	*a*	*b*	*c*	*e*	*a*	*c*	*b*	*a*	*e*	*a*	*e*	*c*	*b*
e	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*	*e*
d	*a*	*b*	*c*	*d*	*a*	*b*	*c*	*d*	*a*	*b*	*c*	*d*	*a*	*b*	*c*	*d*	*a*	*b*	*c*	*d*	*a*	*b*	*c*
a	*d*	*c*	*b*	*b*	*c*	*d*	*a*	*c*	*b*	*a*	*d*	*a*	*d*	*c*	*b*	*b*	*c*	*d*	*a*	*c*	*b*	*a*	*d*
b	*c*	*d*	*a*	*c*	*b*	*a*	*d*	*a*	*d*	*c*	*b*	*c*	*b*	*a*	*d*	*a*	*d*	*c*	*b*	*b*	*c*	*d*	*a*
c	*b*	*a*	*d*	*a*	*d*	*c*	*b*	*b*	*c*	*d*	*a*	*b*	*c*	*d*	*a*	*c*	*b*	*a*	*d*	*a*	*d*	*c*	*b*

Ainsi l'on aura 5 groupes principaux dont les permutations respectives ne pourront jamais se mêler, celles de l'un avec celles de l'autre.

Actuellement, chaque groupe qui est de 1.2.3.4 permutations pourra se partager en 4 groupes secondaires composés de 1.2.3 permutations.

Par exemple, le premier groupe principal qui commence par *a* se décomposera en 4 groupes secondaires : le premier composé de toutes les permutations qui ont *b* à la 2^{e} place ; le second de toutes celles qui ont *c* à la 2^{e} place ; le troisième de toutes celles qui ont *d* à la 2^{e} place ; et le quatrième, *e* à cette même place.

Or il est clair comme tout-à-l'heure, que ces 4 groupes ne se mêleront jamais ensemble malgré l'échange des lettres *b*, *c*, *d*, *e* les unes dans les autres.

Maintenant chaque groupe secondaire, tel que le premier où toutes les permutations, qui sont au nombre de 1.2.3, commençant par *ab*, se décomposera en 3 groupes ternaires composés chacun de 1.2 permutations ; le premier aura *c* à la 3^{e} place, le second aura *d*, et le troisième, *e* à cette même place.

Enfin, chaque groupe ternaire, tel que le premier, se décomposera en deux permutations simples *abcde*, *abced* qui seront toujours conjuguées dans tous les échanges possibles des lettres entre elles.

Donc, en remontant, la fonction $\varphi = abcde$ aura 1.2.3.4.5 valeurs, mais toute fonction invariable φ' telle que la somme ou le produit des deux fonctions conjuguées *abcde*, *abced* n'en aura que 3.4.5 ; de même, toute fonction invariable φ'' des trois fonctions conjuguées φ', n'en aura que

4.5, et toute fonction invariable φ''' des quatre fonctions conjuguées φ'', n'en aura que 5.

Ainsi, en représentant les fonctions invariables des diverses valeurs conjuguées par des permutations qui les renferment, on aura ce tableau :

φ	φ'	φ''		
	$\overbrace{\quad}$	$\overbrace{\quad}$	$\overbrace{\quad}$	$\overbrace{\quad}$
a	aa	aa	aa	aa
b	bb	bb	bb	bb
c	cc	cc	dd	ee
d	de	de	ce	cd
e	ed	ed	ec	dc

φ'''

aa	aa	aa	aa	aa	aa	aa	aa	aa	aa	aa	aa
	bb	bb	bb	cc	cc	cc	dd	dd	dd	ee	ee	ee
	cc	dd	ee	bb	dd	ee	bb	ce	ec	bb	cc	dd
	de	ce	cd	de	be	bd	ce	bc	be	cd	bd	be
	ed	ec	dc	ed	eb	db	ec	eb	cb	dc	db	eb

où l'on voit que φ dépend d'une équation du 2^{d} degré dont φ' est coefficient ; que φ' dépend d'une équation du 3^{e} degré dont φ'' est coefficient ; que φ'' dépend d'une équation du 4^{e} degré dont φ''' est coefficient, et φ''' enfin d'une équation du 5^{e} degré dont tous les coefficients sont connus.

Et ce raisonnement est général quel que soit le nombre des racines, a, b, c, d, & c ou le degré de la proposée ; d'où l'on voit que l'équation supérieure d'où dépend une fonction de ses racines ne renfermera jamais de difficulté supérieure à celle de la proposée elle-même.

Lorsque, sous la fonction φ, deux ou plusieurs racines se trouvent traitées de la même manière, le nombre des permutations se réduit, et les équations successives d'où dépend cette fonction φ s'abaissent.

S'il n'y a dans la fonction φ qu'une partie des racines, on peut prouver comme précédemment que la difficulté n'est jamais supérieure au degré de la proposée.

Soit, comme dans le 1er exemple, une équation du 5^{e} degré, et a, b, c, d, e ses racines, et qu'on demande une fonction φ abc qui n'en renferme que trois.

On partagera d'abord toutes les permutations qui sont au nombre de 5.4.3 en 5 groupes principaux, le 1er où l'on voit a partout à la 1re place, le 2^{e} où l'on voit la lettre b, le 3^{e} c, le 4^{e} d, et le 5^{e} e à cette même place.

Le 1er où, comme on le voit ici, toutes les permutations commencent par a, se partagera en quatre groupes où l'on voit dans chacun les deux mêmes lettres occuper les deux premières places :

φ''

aaa	*aaa*	*aaa*	*aaa*
bbb	*ccc*	*ddd*	*eee*
cde	*bde*	*bce*	*bcd*
φ'	φ'	φ'	φ'

Chacun de ces groupes ne renfermant que trois valeurs, la fonction $\varphi.abc$ dépendra d'une équation du 3e degré dont φ' sera coefficient ; φ' dépendra d'une équation du 4e degré dont φ'' sera coefficient ; et φ'' enfin dépendra d'une équation du 5e degré dont tous les coefficients seront connus.

Et en général, pour trouver une fonction φ de n racines d'une équation proposée du degré m, il suffira de résoudre des équations des degrés respectifs m, $m-1$, $m-2$, jusqu'à n.

On vient de prouver que toutes les valeurs ou permutations φ peuvent être partagées en divers groupes inséparables malgré l'échange des lettres a, b, c, d, ... les unes dans les autres. Dans l'exemple proposé, on a formé les cinq groupes principaux en composant chacun de toutes les permutations où une même lettre occupe la seconde place, ou la 3e, ou la 4e, ou la 5e, ce qui nous fait voir d'abord que le partage des 2.3.4.5 permutations en 5 groupes principaux n'est point unique, mais peut se faire de 5 manières différentes ; ainsi, l'on peut former 5 tableaux où l'on verra toutes les permutations différemment groupées, mais de telle manière dans chacun d'eux, que les 5 groupes qui le composent ne pourront jamais mêler leurs permutations malgré tous les échanges possibles des lettres a, b, c, d, e entre elles.

De même, chaque groupe principal, en y faisant, pour plus de clarté, abstraction de la lettre commune qui occupe partout la même place, pourra être partagé en 4 groupes secondaires de 4 manières différentes ; chaque groupe secondaire se pourra décomposer de même de 3 manières différentes en groupes ternaires et ainsi de suite.

D'où il résulte en général qu'on a m manières de partager toutes les permutations de m lettres en m groupes principaux, ce qui donne lieu à m tableaux ou systèmes différents ;

Que dans chaque tableau ou système, on a $m-1$ manières de partager les permutations de chaque groupe, ce qui produit $m.m-1$ tableaux différents ;

Que dans chaque tableau, on a $m-2$ manières de grouper les permutations de chaque groupe secondaire ; ce qui fournira $m.m-1.m-2$ tableaux différents ; et ainsi de suite.

Et dans tous ces tableaux, deux permutations conjuguées ne se sépareront jamais ; trois groupes conjugués ne se sépareront jamais ; quatre de ces groupes conjugués ne se sépareront jamais, et ainsi de suite, malgré tous les échanges possibles qu'on voudra faire entre les lettres a, b, c, d, e, & c.

La manière dont nous venons de grouper les permutations en mettant dans les groupes une ou plusieurs lettres aux mêmes places, est la plus naturelle et la plus simple qui puisse s'offrir ; mais quoiqu'elle abaisse les degrés des équations d'où elles dépendent jusqu'au degré de la proposée elle-même, elle ne peut rien apprendre sur la résolution ; par cela même qu'elle considère chaque racine comme servant de chef aux divers groupes, elle renferme essentiellement la difficulté du degré marqué par le nombre de ces racines.

II.

Il nous reste à voir s'il n'y a pas d'autres conjugaisons ou d'autres manières de partager les permutations en divers groupes qui ne puissent jamais se mêler malgré l'échange des lettres a, b, c, d, & c. les unes dans les autres.

Nous avons d'abord assemblé nos permutations par deux, puis ces couples par trois ; ensuite ces groupes résultants par quatre, et ainsi de suite jusqu'à m ; commençons au contraire par assembler nos permutations de m lettres par m, et pour plus de clarté, reprenons l'exemple de cinq lettres a, b, c, d, e.

La manière générale de trouver les permutations qui s'assemblent est de prendre une quelconque de ces permutations, et d'y appeler toutes les lettres dans un nouvel ordre, ce qui fournira une nouvelle permutation, ensuite de tirer de celle-ci, par la même loi, une troisième permutation qui sera dérivée de la 2^{e} comme la 2^{e} est dérivée de la 1^{re} ; on continuera de cette manière jusqu'à ce que l'on retombe sur la permutation primitive d'où l'on était parti, et l'on repassera ensuite dans les mêmes à l'infini.

Ces différentes permutations dérivées successivement l'une de l'autre par la même loi seront conjuguées ; c'est-à-dire ne se sépareront jamais malgré tous les échanges possibles entre les lettres, ou ces permutations ne feront que s'échanger les unes dans les autres, ou tout le groupe changera et deviendra un groupe semblable de permutations nouvelles, mais dérivées les unes des autres par la même loi qu'auparavant.

La dérivation la plus simple [74] est celle d'appeler les lettres dans l'ordre naturel 2e, 3e, 4e, 5e, 1re ; ou 3e, 4e, 5e, 1re, 2e, ou 4e, 5e, 1re, 2e, 3e ; & c ; ce qui revient à les avancer toutes d'une place, ou toutes de deux places, & c. ; ainsi, d'après cette règle,

a b c d e

je tire

b c d e a;

de celle-ci je tire de même

c d e a b;

de celle-ci je déduis également

d e a b c;

de celle-ci

e a b c d,

et de celle-ci enfin, je tirerai la 1re

a b c d e

d'où j'étais parti. Ainsi l'on a ce groupe de permutations dérivées que j'écris maintenant suivant les lignes verticales de cette manière :

a	*b*	*c*	*d*	*e*
b	*c*	*d*	*e*	*a*
c	*d*	*e*	*a*	*b*
d	*e*	*a*	*b*	*c*
e	*a*	*b*	*c*	*d*

Si l'on eût dérivé suivant l'ordre 3e, 4e, 5e, 1re, 2e, on aurait retrouvé les mêmes permutations, mais rangées différemment ; et de même en dérivant suivant l'ordre 4e, 5e, 1re, 2e, 3e, ou 5e, 1re, 2e, 3e, 4e, on aurait encore le même groupe.

Considérons en effet la 1re loi, ou la première manière de dériver les permutations ; nous voyons que la première permutation

a b c d e

fait naître la deuxième

b c d e a;

---

74 Il y a en effet plusieurs manières de dériver les permutations les unes des autres ; pour cinq lettres, on peut dériver de 6 manières différentes ; pour sept lettres, on pourrait faire la même chose de 2.3.4.5 manières différentes, mais nous ne pouvons ici qu'indiquer ces théorèmes.

celle-ci la 3e

c d e a b;

celle-ci la 4e

d e a b c;

celle ci enfin la 5e

e a b c d.

La 2e loi de dérivation ferait naître de la première permutation la 3e ; de celle-ci la 5e ; de celle-ci la 2e ; de celle-ci la 4e, en sautant ainsi de 2 en 2 ; et si 2 ne divise pas le nombre m, comme dans cet exemple où $m = 5$, il faut nécessairement retrouver nos m permutations différentes avant de revenir à la première.

Par la même raison la troisième manière de dériver reproduira les m permutations si 3 n'est pas diviseur de m, et ainsi des autres ; de sorte que m étant un nombre premier, il y aura $m-1$ lois équivalentes de dérivation. Les m permutations conjuguées seront entre elles dans une dépendance toute semblable, et l'on pourra les considérer indifféremment comme dérivées successivement l'une de l'autre par la loi dont une quelconque d'entre elles dériverait de l'une quelconque des autres à volonté.

Si le nombre m est un nombre composé, en appelant les lettres d'une première permutation dans l'ordre naturel 2, 3, 4, 5, 6, & c., on assemble aussi m permutations différentes qui sont conjuguées entre elles ; mais ces permutations n'offrent point cette même similitude de dépendance mutuelle. Elles ne peuvent pas être envisagées comme formées toutes par la loi dont une quelconque d'entre elles dériverait de l'une quelconque des autres à volonté. Elles se partagent en plusieurs groupes suivant les facteurs premiers de m.

Soient, en effet, nos m permutations formées par la 1re loi et rangées dans l'ordre où elles naissent d'après cette loi ; si vous vouliez les retrouver par la loi d'où la n^e dérive de la 1re et que n fût diviseur de m, vous iriez ainsi de l'une à l'autre en sautant de n en n, et comme n divise exactement m, vous ne passeriez jamais que sur la même partie $\frac{m}{n}$ de vos m permutations ; donc si m est composé, il y aura seulement autant de manières de les former toutes les unes par les autres, qu'il y aura de nombres inférieurs premiers à m.

Soit α l'un des facteurs premiers de m qui sera ainsi de la forme $m = \alpha N$, en dérivant de la 1re permutation, d'après l'ordre

$$\alpha + 1,\ \alpha + 2,\ \alpha + 3,\ \&\ \text{c.},$$

vous assemblerez N de vos permutations, et par conséquent les m permutations proposées seront partagées en α groupes conjugués de N permutations.

Soit β l'un des facteurs premiers de N, de sorte qu'on ait $N = \beta N'$; en dérivant d'après l'ordre

$$\beta + 1, \beta + 2, \beta + 3, \text{ \& c.},$$

vous formerez un groupe de N' permutations conjuguées et par conséquent β groupes semblables des N permutations de chacun des groupes précédents, et ainsi de suite. Pour le cas de $m = \alpha\beta\gamma$, α, β, et γ étant des nombres premiers, le système de vos m permutations dérivées se partagerait donc en α groupes de $\beta\gamma$ permutations, et ces α groupes seraient conjugués entre eux d'une manière toute semblable ; chacun des groupes $(\beta\gamma)$ se partagerait de même en β groupes de γ, et les β groupes seraient conjugués entre eux d'une manière semblable ; enfin les γ permutations de chacun de ces groupes seraient aussi conjuguées entre elles d'une manière semblable, à cause que γ est aussi un nombre premier. Ainsi pour $m = 12$ par exemple, les douze permutations se pourraient partager en deux groupes de six, et chacun de ces groupes en deux autres de trois permutations.

Voilà donc une manière très simple de partager le système des $1.2.3.4 \ldots m$ permutations de m lettres, en $1.2.3.4 \ldots m - 1$ groupes de m permutations conjuguées par la même loi, et qui sont inséparables malgré tous les échanges qu'on pourrait faire entre les m lettres proposées.

Conjugaison mutuelle des groupes

Mais actuellement, il peut y avoir plusieurs de ces groupes qui se conjuguent aussi entre eux d'une manière inséparable, je veux dire qui soient tels que tout échange qui ferait passer une permutation à la place de celle d'un autre groupe, non seulement ferait passer le groupe entier à la place de cet autre, mais ramènerait encore celui-ci à la place du premier ; ou bien, si les groupes s'assemblaient en plus grand nombre, tout échange de lettres ne ferait que les convertir les uns dans les autres, ou changerait à la fois tout le système en l'un des systèmes semblables formés par le reste des autres permutations.

(Dans les permutations dérivées d'un même groupe, il n'y a aucune lettre qui soit à la même place dans deux permutations ; mais dans les groupes conjugués il y a nécessairement autant de permutations où la même lettre occupe la même place.)

Si l'on voulait découvrir à la seule inspection quels sont les groupes qui s'assemblent, on n'aurait qu'à regarder les permutations qui commencent par la même lettre dans ces divers groupes, et voir quel est l'aspect relatif des $m - 1$ lettres restantes : cet aspect doit être le même pour les $m - 1$ lettres restantes des autres permutations qui commencent aussi par une autre même lettre, et ainsi de suite. De cette manière, la conversion mutuelle des permutations commençant par la même lettre entraînera la conversion mutuelle des groupes auxquels ces permutations appartiennent, et l'on aura trouvé les groupes qui peuvent se conjuguer.

Mais on y peut également parvenir par le principe analogue à celui qui nous a fait d'abord assembler les permutations d'un même groupe. En effet, si plusieurs groupes sont conjugués d'une manière inséparable, il faut que le même changement d'ordre qui ferait déduire le 2^{e} du 1er, fit aussi déduire le 3^{e} du 2nd, le 4^{e} du 3^{e} et ainsi de suite, jusqu'à ce qu'on retombât sur le 1er groupe d'où l'on est parti.

Or, si dans le 1er groupe de m permutations, nous prenez toutes les lettres de n en n, et que n soit premier à m, vous formerez évidemment un nouveau groupe de permutations conjuguées entre elles par la même loi que les premières : car il est manifeste que dans ces permutations toutes les lettres se suivront aussi entre elles dans le même ordre. Si dans ce nouveau groupe vous prenez de même toutes les lettres de n en n, vous trouverez un troisième groupe de permutations nouvelles, mais conjuguées encore par la même loi, et ainsi de suite, jusqu'à ce que vous retombiez sur le premier groupe d'où vous étiez parti.

Mais il n'est pas difficile de voir et de démontrer que si, dans une permutation, on prend les lettres de n en n, ce qui fournit une nouvelle permutation, et que dans celle-ci on prenne encore les lettres de n en n, ce qui donne une troisième permutation, ce passage de la 1re à la 3^{e} peut également se faire en prenant tout d'un coup dans la 1re les lettres de n^2 en n^2, et de même si l'on continuait à prendre les lettres de n en n dans la 3^{e} permutation pour arriver à une 4^{e}, ce passage de la 1re à la 4^{e} pourrait s'effectuer tout d'un coup en prenant les lettres de n^3 en n^3, et ainsi de suite, en observant que si les nombres n^2, n^3, & c. deviennent supérieurs à m, il faut entendre par ces nombres leurs plus petits résidus par rapport à m.

Ce théorème est très remarquable, il donne une espèce de définition géométrique de ces nombres qu'Euler nomme racines primitives, et qui sont tels que toutes leurs puissances successives laissent par rapport au nombre premier μ que l'on considère des restes tous différents 1, 2, 3, 4, ... $\mu - 1$ et qui reparaissent ensuite périodiquement à l'infini.

Si μ lettres sont rangées en cercle comme les angles d'un polygone, il y a toujours des nombres n tels qu'en joignant les points de n en n, ce qui donne un nouveau polygone, puis ceux-ci de n en n, ce qui forme un troisième polygone, et ainsi de suite, vous formez toutes les espèces de polygones de l'ordre μ ; et il y a juste autant de ces nombres ou racines primitives qu'il y a de nombres premiers à $\mu - 1$ et inférieurs à $\mu - 1$. (La raison de ce dernier théorème est qu'il doit y en avoir autant qu'il y a de permutations dérivées entre les $\mu - 1$ lettres qui suivent celle d'où l'on part ; or pour un nombre composé $\mu - 1$, il y a autant de manières de former les permutations dérivées toutes par une même loi qu'il y a de nombres inférieurs et premiers à ce nombre).

Donc si m est un nombre premier et n un nombre dont toutes les puissances successives laissent des résidus différents 1, 2, 3, 4, ... $m-1$, on trouvera $m - 1$ groupes conjugués avant de revenir au premier d'où l'on était parti ; et l'on voit en même temps qu'on peut trouver ces $m - 1$ groupes sans connaître le nombre n : il suffira de considérer le 1er et d'y prendre d'abord toutes les lettres de 2 en 2, puis de 3 en 3, puis de 4 en 4, & c., et enfin de $m - 1$ en $m - 1$.

Ainsi dans l'exemple de 5 lettres a, b, c, d, e, prenez dans le 1er groupe

$$\begin{array}{c} a\,b\,c\,d\,e \\ b\,c\,d\,e\,a \\ c\,d\,e\,a\,b \\ d\,e\,a\,b\,c \\ e\,a\,b\,c\,d \end{array}$$

les lettres de 2 en 2, et vous avez :

$$\begin{array}{c} a\,b\,c\,d\,e \\ c\,d\,e\,a\,b \\ e\,a\,b\,c\,d \\ b\,c\,d\,e\,a \\ d\,e\,a\,b\,c\,; \end{array}$$

dans le 1er groupe prenez les lettres de 3 en 3, et ensuite de 4 en 4, et vous aurez ces deux autres :

$$\begin{array}{c} a\,b\,c\,d\,e \\ d\,e\,a\,b\,c \\ b\,c\,d\,e\,a \\ e\,a\,b\,c\,d \\ c\,d\,e\,a\,b \end{array} \qquad \begin{array}{c} a\,b\,c\,d\,e \\ e\,a\,b\,c\,d \\ d\,e\,a\,b\,c \\ c\,d\,e\,a\,b \\ b\,c\,d\,e\,a \end{array}$$

et ces quatre groupes de 5 permutations seront conjugués d'une manière inséparable.

Mais la première manière de déduire successivement ces groupes l'un de l'autre par la même loi est plus avantageuse en ce qu'elle nous découvre encore une décomposition de ces $m-1$ groupes entre eux, et par l'ordre où elle les fait naître successivement.

En effet, puisque du 1^{er} groupe vous tirez un 2^{d} groupe en prenant les lettres de n en n ; de ce 2^{d} un 3^{e} en prenant les lettres de n en n ; de ce 3^{e} un 4^{e} en y prenant encore les lettres de n en n, et ainsi de suite ; que d'un autre côté, cela reviendrait à déduire toujours du même 1^{er} groupe, d'abord de n en n, puis de n^2 en n^2, puis de n^3 en n^3, & c., et enfin de n^{m-2} en n^{m-2} ; il s'en suit que le système de ces $m-1$ groupes conjugués se partage lui-même en systèmes partiels aussi conjugués. Car le nombre m étant premier, le nombre $m-1$ est nécessairement composé ; or supposez que α soit un facteur de $m-1$, et dans l'ordre où sont actuellement vos groupes, essayez de les déduire les uns des autres par la loi d'où le $\alpha+1^{e}$ dérive du 1^{er}, ce qui revient à prendre toutes les lettres de n^{α} en n^{α}, vous irez ainsi de l'un à l'autre, en sautant de α en α, et comme α est diviseur de $m-1$, vous ne passerez jamais que sur une même partie $\frac{m-1}{\alpha}$ de vos $m-1$ groupes, de sorte que le système sera partagé en α systèmes partiels de $\frac{m-1}{\alpha}$ groupes aussi conjugués entre eux. Et de même si $\frac{m-1}{\alpha}$ a pour diviseur β, vous pourrez subdiviser encore chacun des $\frac{m-1}{\alpha}$ systèmes partiels en β systèmes de $\frac{m-1}{\alpha\beta}$ groupes aussi conjugués entre eux, et ainsi de suite, jusqu'à ce que le système entier n'offre plus dans toutes ses subdivisions que les nombres premiers α, β, ... qui entrent dans la composition du nombre $m-1$; alors il y aura une dépendance mutuelle toute semblable 1°. entre les m permutations d'un même groupe ; 2°. entre les groupes d'un même système partiel ; 3°. entre les systèmes partiels d'un même système supérieur ; et ainsi de suite.

Pour aller plus loin dans la réduction des groupes il faudrait chercher si les $1.2.3.4\ldots m-2$ systèmes pourraient se grouper encore, et ceux-ci à leur tour, & c. par les nombres $m-2$, $m-3$, & c ou par leurs diviseurs ; de sorte que la décomposition entière de toutes les permutations se fît toujours par des nombres inférieurs à m.

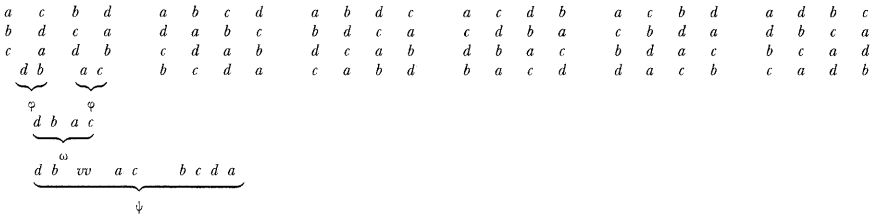
Dans le cas où m est un nombre composé, on n'assemble plus immédiatement $m-1$ des groupes comme ci-dessus, mais seulement autant de ces groupes qu'il y a de nombres premiers à m au dessous de lui : pour 4, par exemple, on n'assemble que deux groupes de permutations conjuguées ; cela est facile à conclure de ce qui a été dit précédemment.

Il est bien facile de faire l'application de ces principes aux cas de 3, 4, 5 lettres et de voir la raison métaphysique de la résolution des équations du 3e et du 4e degré, et celle de la réduction de la difficulté dans le cas du 5e degré, à la difficulté d'une équation particulière du 6e.

On a pour le 3e le tableau suivant :

$$\begin{array}{ll} a\,b\,c & a\,b\,c \\ b\,c\,a & c\,a\,b \\ c\,a\,b & b\,c\,a\,; \end{array}$$

pour le 4e on a celui-ci :



On peut remarquer dans ce dernier tableau que les quatre permutations, de chaque groupe, du 1er par exemple, se partagent en deux groupes partiels de deux permutations conjuguées, comme cela doit être. Ainsi la fonction quelconque de a, b, c, d, $f(a,b,c,d)$ peut être regardée comme racine d'une équation du 2e degré dont φ serait coefficient ; φ peut être regardée comme racine d'une équation du 2d degré dont ω serait coefficient ; ω à son tour, comme racine d'une équation du 2d degré dont ψ serait coefficient, et ψ enfin comme la racine d'une équation du 3e degré dont tous les coefficients seraient connus. D'où l'on peut conclure ce théorème qui nous paraît nouveau et remarquable :

L'équation du 24e degré qui donne les 24 valeurs d'une fonction des quatre racines a, b, c, d d'une équation du 4e degré peut se résoudre actuellement à l'aide d'équations du 2d et 3e degré, sans faire sur cette fonction aucun hypothèse particulière qui réduise les 24 valeurs à 3 en les rendant égales 8 à 8.

Cette résolution tient donc essentiellement à la nature du nombre 4 qui permet ainsi de grouper les 24 valeurs par 2 et par 3, et non point au choix qu'on fait de certaines fonctions particulières des racines qui offrent moins de valeurs différentes qu'il n'y a de permutations entre les quatre racines. Il n'en est pas de même dans le 3e degré : à cause du nombre premier 3 on a toujours à résoudre une équation du 3e degré pour obtenir les trois permutations d'un même groupe ; mais par la dépendance semblable de

ces trois permutations qui fait qu'elles se produisent également les unes par les autres comme les racines 3^es de l'unité, cette équation n'a que la difficulté des équations binômes du 3^e degré.

Soient en effet vos trois fonctions

$$\begin{array}{ccc} \varphi & \varphi & \varphi \\ a & b & c \\ b & c & a \\ c & a & b \\ A & A' & A'' ; \end{array}$$

les fonctions A, A', A'' des trois lettres a, b, c sont telles que si A est changée en A', A' l'est en A'' et A'' en A ; si A est changé en A'', A' l'est en A, A'' en A' ; ainsi ces trois fonctions A, A', A'' ne peuvent présenter que ces trois permutations :

$$\begin{array}{ccc} A & A' & A'' \\ A' & A'' & A \\ A'' & A & A' ; \end{array}$$

ces fonctions sont donc liées entre elles comme les trois racines de l'unité 1, α, α^2 ; la fonction $(A+\alpha A'+\alpha^2 A'')$ élevée au cube n'a donc qu'une seule valeur pour le 1^er groupe.

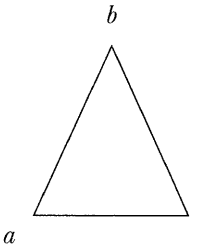
Par ce que j'ai dit plus haut sur le cas de 5 lettres a, b, c, d, e, on peut voir aussi que la résolvante du 120^e degré où l'on est conduit pour la résolution du 5^e degré, n'a que la difficulté d'une équation particulière du 6^e, mais qui a résisté jusqu'ici à tous les efforts des géomètres. Nous avons bien trouvé une manière très simple de la réduire elle-même au 5^e degré, mais cette réduction paraît inutile, et le problème se replie en quelque sorte lui-même, sans qu'on puisse voir s'il y aurait quelqu'avantage à cette transformation. J'ai à peine le temps d'indiquer la plupart des résultats auxquels je suis parvenu et[75]

Je passe à une exposition plus claire et plus rapide, et qui est tirée de la considération des nouveaux polygones que nous avons fait connaître. Cette théorie des polygones a une liaison intime avec la résolution générale des équations et la théorie des nombres.

---

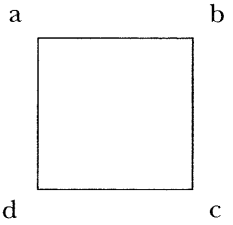
75 Cette page n'est pas achevée.

3e degré



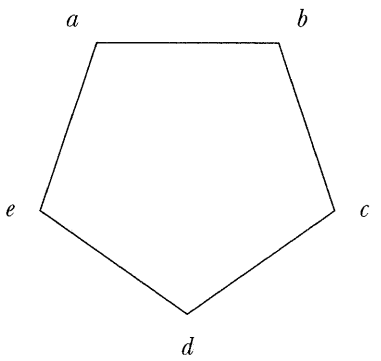
Ce triangle offre les six permutations des trois lettres a, b, c qui sont aux angles, savoir trois permutations conjuguées qu'on obtient en lisant dans le même ordre en partant successivement de a, de b, de c ; et 3 autre conjuguées en lisant de 2 en 2, ce qui reviendrait ici à renverser.

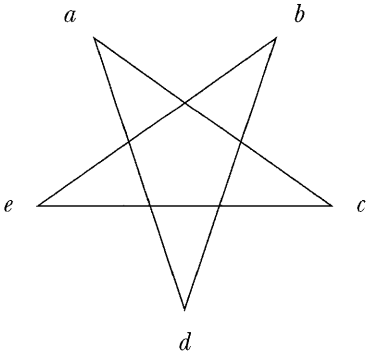
4e degré



Le carré renferme 8 permutations, savoir 4 en lisant de suite dans le même ordre, et 4 conjuguées en lisant de 3 en 3 ou dans l'ordre renversé.

5e degré





Il y a deux espèces de pentagones réguliers ; chacun d'eux renferme actuellement 10 permutations savoir, 5 en lisant de suite dans le même ordre, et 5 conjuguées en lisant dans l'ordre renversé, ou de 4 en 4 comme vous

pouvez le voir ; il en résulte donc 20 permutations conjuguées. Les cinq permutations d'un groupe sont liées entre elles comme les cinq racines cinquièmes de l'unité ; elles ne dépendent au fond que d'une équation binôme du 5^{e} degré ; leurs fonctions semblables ne dépendent que d'une équation du 2^{e} degré, à cause des deux 1ers groupes conjugués ; les fonctions semblables des coefficients de cette équation ne dépendent encore que d'une équation du 2^{d} degré par ce que le 1er couple des groupes est conjugué avec le 2^{d} couple ; enfin les coefficients de cette équation du 2^{d} degré ne dépendent plus que d'une équation du 6^{e} degré dont tous les coefficients sont connus.

Ces résultats s'accordent parfaitement avec ceux que M. Lagrange obtient par son analyse (*Mém. de Berlin*, 1771), mais on voit de plus qu'il n'y a pas réellement d'équation du 4^{e} degré à résoudre, mais bien 2 équations du 2^{d} degré, de sorte que les radicaux cubiques ne proviendront que de la réduite du 6^{e} degré.