INSTITUT
DE RECHERCHE
POUR L'ENSEIGNEMENT
DES MATHEMATIQUES

n°16

JUILLET 2000

M. : A. T. H.

MNEMOSYNE

UNIVERSITE DENIS DIDEROT
PARIS VII

Cette brochure est réalisée par l'IREM PARIS 7 DENIS DIDEROT avec le concours de la D.L.C., des MAFPEN de Paris, Créteil et Versailles.

Mnémosyne

personnification de la mémoire.

Elle s'unit à Zeus pendant 9 nuits de suite ;

de cette union naquirent les neufs Muses.

(Dictionnaire Robert des noms propres)

Illustration de la couverture : « **La mémoire** »

gravure allégorique d'après Gravelot (XVII^{e} siècle)

MNEMOSYNE

M: *Mathématiques*

A. *Approche par les*

T. *textes*

H. *historiques*

NOUVEAUX ELEMENS
DES
MATHEMATIQUES
OU
PRINCIPES GENERAUX
DE
TOUTES LES SCIENCES
Qui ont les grandeurs pour objet.

SECONDE EDITION, PLUS AMPLE ET MIEUX DIGERE'E.

PREMIER VOLUME

Qui comprend la ſcience des Nombres & l'Algébre, ou l'art de comparer toute ſorte de grandeurs par le moyen des chiffres & des lettres.

Et où tout eſt démontré dans un ordre naturel & facile, & les choſes expliquées plus à fond, & pouſſées plus loin que l'on n'a fait juſqu'ici.

Par JEAN PRESTET *Prêtre, ci-devant Profeſſeur des Mathématiques dans les Univerſitez d'Angers & de Nantes.*

A PARIS.
Chez ANDRE' PRALARD, ruë ſaint Jacques, à l'Occaſion.

M. DC. LXXXIX.
AVEC PRIVILEGE DU ROY.

SOMMAIRE

ELEMENS
DES
MATHEMATIQUES,
OU
PRINCIPES GENERAUX
DE
TOUTES LES SCIENCES,
QUI ONT LES GRANDEURS POUR OBJET.

CONTENANT VNE METHODE COVRTE ET FACILE pour comparer ces grandeurs & pour découvrir leurs rapports par le moyen des caracteres des nombres, & des lettres de l'alphabeth. Dans laquelle les choſes ſont démontrées ſelon l'ordre Geometrique, & l'Analyſe renduë beaucoup plus facile, & traittée plus à fond que l'on n'a fait juſqu'ici.

A PARIS,
Chez ANDRE' PRALARD, Marchand Libraire, ruë Saint Jacques, à l'Occaſion.

M DC. LXXV.
AVEC PRIVILEGE DV ROY.

Page de titre du 1er ouvrage de Prestet (1675)

EDITORIAL

Voici donc le seizième numéro de Mnémosyne.

L'Arithmétique –ou plutôt une présentation des fondements de cette discipline - ouvre le fascicule. Michèle Grégoire nous présente un mathématicien fort peu connu de nos jours, Jean Prestet (1648-1690), dont le nom n'est même pas repris dans les dictionnaires usuels. Il s'agit pourtant d'un personnage qui a joué un rôle non négligeable à la fin du XVII^{ième} siècle dans cette synthèse mathématique et philosophique cartésienne réalisée autour de Malebranche. En 1675 paraissent simultanément (ce n'est pas un hasard !) l'édition définitive en deux volumes de *la Recherche de la Vérité* de Malebranche et les *Éléments des Mathématiques*, ou principes généraux de toutes les sciences de J. Prestet. L'intérêt principal de cette première édition est, au début du livre second, un véritable traité des combinaisons sous le titre " De la résolution des questions par la composition ". Nous reviendrons sur ce sujet dans un numéro ultérieur de Mnémosyne. Cet ouvrage fut très attaqué, notamment par Wallis (*Treatise of Algebra*, 1684) qui y voyait la patte de Malebranche et a cherché à discréditer Prestet comme exécuteur des basses œuvres et reproche à l'auteur de ne citer que Viète et Descartes, en ignorant... les auteurs anglais. Signalons enfin que, vers cette époque, dans le cadre des oratoriens réunis autour de Malebranche, Prestet rencontre Leibniz, B. Lamy (qui se déclare son redeveur), C. R. Reynaud qui le remplace en 1676 à l'Université d'Angers. Mais c'est ici la seconde édition (1689) des *Éléments des Mathématiques*, œuvre de maturité, qui nous concerne. Le livre I de l'ouvrage (qui paraît maintenant en deux volumes) est augmenté d'un sixième chapitre qui est le premier exposé théorique de l'Arithmétique depuis Euclide. Nous renvoyons à l'analyse du texte donnée ci-dessous pour en dégager l'originalité et la modernité.

Avec l'étude centrale de ce numéro, vous avez accès à un texte clef, considéré comme tel par tous les historiens de l'Algèbre, le mémoire de Lagrange intitulé *Réflexions sur la résolution algébrique des équations* . Le problème de la résolubilité des équations algébriques était jusqu'alors posé en terme de transformation de leur expression algébrique. Ici Lagrange, à partir de l'analyse des résolutions connues des équations du troisième et du quatrième degrés, met en évidence le rôle de fonctions symétriques des racines invariantes par certaines permutations et introduit la notion d'équation résolvante.

Ce texte de 1771 est le point de départ d'une approche entièrement nouvelle, qui dégage –comme le dit Lagrange lui-même- la "métaphysique de la théorie des équations". Il me semble particulièrement intéressant pour nous dans notre lecture d'un texte ancien. Les indications données par Martine Bühler, qui nous permettent d'appréhender le texte, montrent la difficulté qu'il y aurait à une lecture directe, pour un non spécialiste de cette époque de l'histoire des mathématiques. Qu'ont pu comprendre les contemporains de Lagrange qui ignoraient la théorie des groupes et la théorie de Galois ? Et pourtant de là sont sortis les travaux de Ruffini, Gauss, Abel, Galois et les débuts de l'Algèbre moderne.

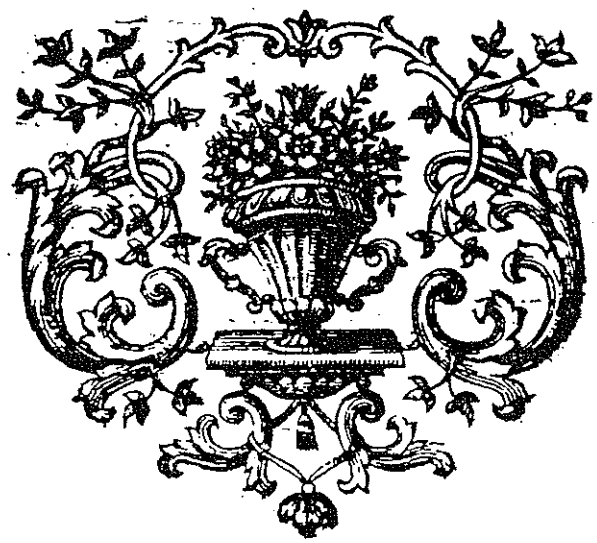
La rubrique "Dans nos classes" nous propose l'étude d'un texte de la *Collection mathématique* de Pappus sur la quadratice d'Hippias qui sensibilise les élèves à deux problématiques qui traversent l'histoire des mathématiques :

(a) Le célèbre problème de la quadrature du cercle, dont on ne sait rigoureusement que depuis 1882 qu'il est impossible.

(b) L'ingéniosité d'inventeurs (depuis l'Antiquité) qui, à défaut de pouvoir résoudre certains problèmes à la règle et au compas, ont inventé des " instruments mathématiques " capables de réaliser ces constructions.

Bonnes vacances!

Jean-Luc Verley



BONNES VIEILLES PAGES

Michèle Grégoire

Nouveaux Elémens des Mathématiques de Jean Prestet, LivreVI, Paris, 1689

Nous vous présentons un livre extrait d'un ouvrage peu connu, qui constitue un très intéressant traité d'arithmétique élémentaire ; son contenu est assez comparable à ce qu'on enseigne actuellement en terminale scientifique, et on peut s'étonner de remarquer qu'il est le premier recueil de résultats fondamentaux aussi complet depuis les livres arithmétiques d'Euclide.

On connaît assez peu de choses sur son auteur, Jean Prestet. Né à Chalons sur Marne en 1648, il est assez jeune employé au service de Malebranche, puis devient son élève. Sans doute poussé par Malebranche qui écrit et publie alors *La recherche de la vérité*, Prestet publie en 1675 des *Elémens de Mathématiques*, un traité de référence pour soutenir la réflexion philosophique de Malebranche. Prestet se destine à la prêtrise et, pendant qu'il enseigne dans différentes écoles de l'ordre de l'Oratoire, réécrit différentes versions de ses *Elémens de Mathématiques*. Il publie en 1689 ses *Nouveaux Elémens* dont sont extraites les pages ci-après, et meurt l'année suivante.

L'ouvrage propose une compilation de résultats mathématiques fondamentaux à la manière des *Elements* d'Euclide, contient bien entendu la géométrie élémentaire, mais il insiste surtout sur l'étude des nombres et des proportions et sur les méthodes algébriques héritées de Descartes. Ce sont les méthodes utilisées pour résoudre de nombreux problèmes tant géométriques que de théorie des nombres - quand il reprend par exemple un certain nombre de problèmes issus des *Arithmétiques* de Diophante -. Son intention, explicite dès le titre, est de donner les "principes généraux de toutes les sciences qui ont les grandeurs pour objet". Ainsi qu'il l'expose dans sa préface : "Par le mot grandeur on entend pas seulement l'étendue en longueur largeur et profondeur mais généralement tout ce que l'on conçoit comme capable du plus et du moins et qui se peut mesurer exactement soit parce qu'il est exactement connu soit parce qu'il est supposé tel (ainsi le temps, la pesanteur, la vitesse, les qualités même sensibles, les degrés de perfection...). (...)Tous les rapports exactement connus se pouvant donc exprimer par nombres, il est évident que les nombres renferment toutes les grandeurs de manière intelligible."

Prestet reconnaît sa dette à l'égard des mathématiciens de l'antiquité, mais à la manière de son temps il considère qu'il faut réécrire et réorganiser leurs traités afin de les rendre plus accessibles et surtout plus éclairants pour les commençants. Il veut mettre en évidence, dans la clarté et la facilité, le bon ordre des

propositions qui permette de comprendre ; et aussi, dans l'esprit de Descartes, son maître à penser, il souhaite "donner à l'esprit assez de force et de lumière pour inventer par lui-même", en proposant une méthode. "C'est un défaut qui n'est que trop ordinaire aux mathématiciens des siècles passés que de se contenter d'établir leurs propositions et leurs règles et de les prouver sans se mettre en peine de donner à l'esprit assez de force et de lumière pour les inventer par lui-même. (...) La méthode générale est ce que l'on doit principalement établir sans se mettre inutilement en peine de toutes les vérités qu'on peut découvrir."[1] L'ouvrage de Prestet, bien qu'il constitue une somme des connaissances de bases et des méthodes de la première partie du XVIII^{ème} siècle eut assez peu d'influence, car il arriva un peu tard, au moment où le calcul infinitésimal, tout à fait absent des Nouveaux Elémens, se diffuse plus largement et éclipse les autres domaines des mathématiques.

Le lecteur trouvera dans le livre VI un ensemble très complet de résultats sur la divisibilité des entiers, les nombres premiers entre eux, le PPCM et le PGCD de deux ou plusieurs nombres, la relation qui lie PPCM et PGCD (prop.48), l'infinité des nombres premiers (prop. 50), le crible d'Eratosthène (prop.52 à 56), des propositions sur le pair et l'impair, une démonstration simple, dans un cas générique tout à fait convaincant, du critère d'Euclide pour construire un nombre parfait , une liste correcte (à une coquille d'imprimerie près) de huit nombre parfaits (prop.33). Le premier résultat fondamental, intitulé théorème I (ou proposition 19), énonce que le produit de deux entiers premiers entre eux est leur plus petit multiple commun. Sa démonstration repose sur une utilisation assez complexe de l'algorithme d'Euclide et ce résultat servira d'outil de démonstration dans de nombreux raisonnements. Un de ses corollaires immédiats est, à la proposition 22, ce que l'on appelle le théorème de Gauss. Une autre conséquence tout à fait remarquable que Prestet tire de son théorème I est la détermination de tous les diviseurs d'un nombre, qu'il soit donné explicitement comme il le fait dans un certain nombre d'exemples, ou qu'il soit écrit sous forme d'une expression littérale (prop. 23 à 32). Il effectue donc en pratique, sur ses exemples, la décomposition en facteurs premiers d'un entier mais démontre aussi qu'un nombre quelconque ainsi décomposé en facteurs premiers n'a pas d'autres diviseurs que les divers produits que l'on peut fabriquer à l'aide de ces facteurs[2]. Prestet est, en avance sur son temps, le premier qui cherche à prouver qu'il a bien tous les diviseurs d'un entier et sa démarche est en fait celle de Gauss énonçant ce qu'on appelle maintenant le théorème fondamental de l'arithmétique, c'est à dire l'unicité de la décomposition en facteurs premiers de tout entier.

Nous remercions chaleureusement Catherine GOLDSTEIN de nous avoir permis de reproduire ici ces pages de l'exemplaire des *Nouveaux Elémens* qu'elle possède et renvoyons le lecteur plus curieux à son article *On a Seventeenth Century Version of the "Fundamental Theorem of Arithmetic"*, in Historia Mathematica 19 (1992), p.177-187.

[1] Préface

[2] Le livre VI fait suite à un livre de combinatoire dans lequel Prestet donne, entre autres, des techniques pour dénombrer et faire la liste de tous les produits que l'on peut former à l'aide d'un certain nombre de grandeurs données.

NOUVEAUX ELEMENS DES MATHEMATIQUES.

LIVRE SIXIEME.

DE LA DIVISION GENERALE *DES GRANDEURS.*

DEFINITIONS.

JE nomme *grandeur entiére* toute grandeur où l'on ne conçoit aucun partage, & même chacun des nombres entiers.

Et j'appelle *diviſeur entier*, ou ſimplement *diviſeur* ou *meſure* d'un nombre ou d'une grandeur entiére, chaque nombre entier qui peut diviſer au juſte le nombre, ou chaque grandeur entiére qui peut diviſer la grandeur éxactement & ſans réſte; & même l'unité. Ainſi 1 & 2 & 3 & 6 ſeront chacun un diviſeur ou une meſure du nombre 6; parce qu'il y a 6 fois 1 au juſte dans 6, & auſſi 2 fois 3, & encore 1 fois 6. Et pareillement 1, a, b, ab, ſont chacune un diviſeur ou une meſure de la grandeur ab; parceque diviſant ab par 1, l'expoſant eſt ab; & le diviſant par b, l'expoſant eſt a; & le diviſant par ab, l'expoſant eſt 1. Et pareillement 1, $a+b$, $a-b$, $aa+bb$, ſont chacune un diviſeur ou une meſure de la grandeur $aa-bb$; puiſque diviſant $aa-bb$ par 1, & par $a+b$, & par $a-b$, & par $aa-bb$; le premier expoſant eſt $aa-bb$, & le ſecond $a-b$, & le troiſiéme $a+b$, & le quatriéme 1.

Et je nommerai auſſi *diviſeur commun* ou *meſure commune* de divers nombres, ou de diverſes grandeurs entiéres, tout nombre entier qui pourra diviſer chacun des divers nombres, ou toute grandeur entiére qui pourra diviſer chacune des diverſes grandeurs éxactement & ſans aucun reſte. Ainſi 1, 2, 3, 6, ſont chacun un diviſeur commun, ou une meſure commune des deux nombres 18 & 24; parce qu'on trouve en 18 qu'il y a au juſte 18 fois 1, & 9 fois 2, & 6 fois 3, & 3 fois 6; & dans 24 qu'il y a pareillement au juſte 24 fois 1, & 12 fois 2, & 8 fois 3, & 4 fois 6. Et par la même raiſon 1 & 5 ſont chacun une meſure commune, ou un diviſeur commun des trois nombres 10, 15, 25. Et pareillement 1 & *a* ſont chacune un diviſeur commun, ou une meſure commune des grandeurs *ab* & *ac*. Et 1, *a*, *b*, *ab*, chacune un diviſeur commun, ou une meſure commune des grandeurs *ab* & *ac*. Et 1, *a*, *b*, *ab*, chacune un diviſeur commun, ou une meſure commune des trois diverſes grandeurs *abc*, *abd*, *abe*. Et 1 & $a+b$ des diviſeurs communs des grandeurs $aa+2ab+bb$ & $aa-bb$ & $aa+2ab+bb+ac+bc$.

Je nommerai *nombres ſimples* ou *premiers*, ceux qu'on ne peut diviſer au juſte ou ſans reſte par aucun autre entier que par eux-mêmes ou par l'unité; comme chacun des dix 1, 2, 3, 5, 7, 11, 13, 17, 19, 23.

Et tous les autres, ou ceux qui peuvent être diviſez ſans reſte par un autre entier que par eux-mêmes ou par l'unité, ſeront nommez *des nombres compoſez*; comme chacun des douze 2, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20.

Et on dit auſſi que ces nombres compoſez ſont *multiples* de leurs diviſeurs. Et qu'ils ſont *doubles*, s'ils les contiennent au juſte 2 fois. Et *quadruples*, ou *quintuples*, ou *ſextuples*, ou *ſeptuples*, ou *décuples*; ſi c'eſt 4 fois, ou 5 fois, ou 6 fois, ou 7 fois, ou 10 fois.

Et les diviſeurs ſont auſſi nommez *ſoûmultiples* de ceux qu'ils diviſent ſans reſte. *Soûdoubles* ou leurs *moitiez*, s'ils s'y trouvent au juſte 2 fois. Et *ſoûtriples* ou *tiers*, ſi c'eſt 3 fois au juſte. Et *ſoûquadruples* ou *quarts*, ſi c'eſt 4 fois. Et *ſouſquintuples*, *ſouſſextuples*, *ſouſſeptuples*, *ſoudécuples*; ſi c'eſt 5 fois, ou 6 fois, ou ſept fois, ou 10 fois, &c. Ou plus ſimplement *cinquiémes*, *ſixiémes*, *ſeptiémes*, *dixiémes*. Et pour les autres pareillement *huitiémes*, *neuviémes*, *onziémes*, *douziémes*, & ainſi du reſte juſques à l'infini.

On nomme *nombres pairs* tous ceux que 2 peut diviſer ſans reſte. Et *pairement pairs* ceux que 2 fois 2, ou 4, diviſe auſſi ſans reſte. Et tous ceux, que 2 ne peut diviſer ſans reſte, ſont nommez *nombres impairs*. Et on nomme encore *nombres pairement impairs*, tous ceux qui peuvent être au juſte diviſez par 2, & ne le peuvent être au juſte ou ſans reſte par 4.

Nombres pairs	2.	4.	6.	8.	10.	12.	14.	16.	18.	20.	22.	24.	26.
pairement pairs		4.		8.		12.		16.		20.		24.	
Nombres impairs	1.	3.	5.	7.	9.	11.	13.	15.	17.	19.	21.	23.	25.	27.
pairement impairs	2.		6.		10.		14.		18.		22.		26.

Je nommerai encore en général *grandeur ſimple* toute grandeur littérale & linéaire. Et grandeur *compoſée* toute autre, ou plane, ou ſolide, ou de divers degrez. Ainſi les grandeurs $a, b, a+b, a-b$, ſeront nommées ſimples, & les grandeurs $ab, ab+ad, ab+cd, a^3-b^3$ ſeront appellées compoſées.

Si divers nombres n'ont point de diviſeur commun autre que l'unité, on dit qu'ils ſont *premiers entr'eux*, quoi qu'ils ſoient ſouvent compoſez en eux-mêmes. Ainſi les nombres 2 & 9 ſont premiers entr'eux, quoique 9 ſoit compoſé. Et pareillement les deux 6 & 13 ſont premiers entr'eux. Et auſſi les trois 2, 6, 25, quoique 2 & 6 aient un diviſeur commun 2. Et les quatre 8, 15, 35, 49, ſont premiers entr'eux.

Mais ſi deux nombres ont un diviſeur commun ou une meſure commune autre que l'unité; on dit qu'ils ſont *compoſez entr'eux*, quoique ſouvent l'un d'entr'eux ſoit un nombre ſimple. Ainſi les nombres 3 & 6 ſont compoſez entr'eux, quoique 3 ſoit un nombre ſimple. Et pareillement les deux 5 & 10 ſont compoſez entr'eux. Et auſſi les trois 2, 12, 18. Et les quatre 6, 18, 9, 15.

Et je dirai pareillement que les grandeurs ſont *premières entr'elles*, ſi elles n'ont aucun diviſeur commun excepté l'unité. Et qu'elles ſont *compoſées entr'elles*, ſi elles en ont quelque autre. Ainſi les grandeurs ab & cd ſont premiéres entr'elles; & les deux a & ab ſont compoſées entr'elles.

Un nombre eſt appellé *parfait*, lorſqu'il eſt parfaitement égal à tous ſes diviſeurs enſemble, qui ſont moindres que luy. Comme 6 qui eſt parfaitement égal à tous ſes diviſeurs enſemble 1, 2, 3.

I COROLLAIRE.

1. TOute grandeur peut être diviſée ſans reſte par elle-même; puis qu'elle eſt toûjours au juſte une fois dans elle-même.

II COROLLAIRE.

2. LE plus grand diviſeur entier de chaque grandeur eſt la grandeur même; puis qu'elle n'en peut [b] jamais contenir au juſte une autre plus grande.

b. 6. 1.

III COROLLAIRE.

3. LE moindre diviſeur d'un nombre eſt toûjours l'unité; puis que tout autre diviſeur entier eſt toûjours un nombre, qui contient [b] au juſte pluſieurs unitez.

b. *définition.*

IV COROLLAIRE.

4. LE plus grand diviſeur commun de deux ou de pluſieurs nombres ne ſurpaſſe jamais le [b] moindre de ces nombres, ni l'unité le plus petit [c] de leurs diviſeurs communs.

b. 2.
c. 3.

V COROLLAIRE.

5. SI un nombre *a* meſure ou diviſe ſans reſte un autre nombre ζ, il eſt le plus grand diviſeur commun des deux *a* & *z*; parce qu'il eſt diviſeur[b] de luy-même, & qu'il n'en peut point[c] avoir un plus grand.

a. z. b. 1.
3. 12. c. 2.

VI COROLLAIRE.

6. SI deux nombres *a* & ζ ſont compoſez entr'eux, & *a* un nombre ſimple; il eſt luy-même un[c] diviſeur de ζ. Puiſque le nombre ſimple *a*, par la[b] ſuppoſition, ne peut avoir aucun diviſeur que luy-même ou l'unité; ni par conſéquent les deux *a* & ζ aucun diviſeur commun que le nombre *a* ou 1.

a. ζ. b. *définition.*
3. 12. c. 5.

VII COROLLAIRE.

7. SI deux nombres *a* & *z* ſont premiers entr'eux, & qu'un nombre *g* meſure l'un ſans reſte; ce même *g* eſt[b] premier à l'égard de l'autre. Puis qu'aucun nombre, autre que l'unité, n'en peut[b] meſurer deux qui ſont premiers entr'eux.

a. z. g. *a.* ζ. *g.* b. *définition.*
6. 25. 3. 6. 25. 5.

VIII COROLLAIRE.

8. SI un nombre ſimple *a* ne peut diviſer un nombre *y* ſans reſte; ces deux nombres *a* & *z* ſont premiers entr'eux. Puiſque le nombre *a* n'a point[b] de diviſeur que luy-même ou l'unité, ni les deux *a* & ζ par conſéquent que l'unité ſeule pour meſure commune.

a. ζ. b. *définition.*
3. 16.

IX COROLLAIRE.

9. SI une grandeur *a* meſure ou diviſe ſans reſte une autre grandeur ζ, & que la grandeur *z* en meſure auſſi ſans reſte une troiſiéme *y*; la premiére *a* meſure enſuitte la troiſiéme *y*.

Car nommant *b* l'expoſant entier de la diviſion de *z* par *a*; le produit *ab* du diviſeur *a* par l'expoſant *b* eſt[b] égal à la grandeur ζ, & peut auſſi diviſer au juſte la grandeur *y*. Si donc *c* eſt l'expoſant de la diviſion de la grandeur *y* par *ab*, ou par *z*; le produit *abc* du diviſeur *ab* par l'expoſant *c* eſt[b] égal à la grandeur *y*. Comme donc *a* meſure *abc* ſans reſte, ou que l'expoſant *bc*, qui eſt un produit des grandeurs entiéres *b* & *c*, eſt une grandeur entiére, la 1ere grandeur *a* meſure auſſi la 3e *y* au juſte ou ſans reſte.

3. 6. 30. 2. 5. 10. b. 18. 2.
a. z. y. b. c. bc. ab. abc.

X COROLLAIRE.

10. SI un nombre *a* diviſe au juſte un nombre *z*, & qu'un nombre *b* diviſe encore au juſte l'expoſant *y*, & un nouveau *c* l'expoſant *x*, & un quatriéme *d* l'expoſant *v*, & que le dernier expoſant *e* ſoit auſſi diviſé par luy-même; le nombre ζ eſt égal au produit *abcde* des diviſeurs ſucceſ-

ſifs, *a*, *b*, *c*, *d*, *e*, & peut avoir pour diverſeur chacun de ces mêmes nombres, & chacun de leurs divers produits alternatifs.

b. 18. 2. Car le produit *de* du diviſeur *d* par le dernier expoſant *e*, eſt égal [b] au pénulme *v*. Et pareillement le produit *cv*, ou *cde*, du diviſeur *c* par *v*, ou par *de*, égal [b] au pénultiéme expoſant *x*. Et le produit *bx*, ou *bcde*, eſt [b] égal à l'expoſant *y*. Et le produit *ay*, ou *abcde*, du diviſeur *a* par *y*, ou par *bcde*, eſt égal [b] au nombre même *z*. Et les cinq diviſeurs ſucceſſifs *a*, *b*, *c*, *d*, *e*, & leurs 10 plans alternatifs *ab*, *ac*, *ad*, *ae*, *bc*, *bd*, *be*, *cd*, *ce*, *de*; & leurs 10 ſolides alternatifs *abc*, *abd*, *abe*, *acd*, *ace*, *ade*, *bcd*, *bce*, *bde*, *cde*; & leurs cinq ſurſolides alternatifs *abcd*, *abce*, *abde*, *acde*, *bcde*; & le

c. 9. produit même entier *abcde*; ſont chacun un diviſeur [c] éxact du nombre *abcde*, ou de *z* qui eſt le même.

abcde.	*bcde.*	*cde.*	*de.*	*e.*	1.	*ab.*	*ac.*	*ad.*	*ae.*	*bc.*	*bd.*
z.	*y.*	*x.*	*v.*	*e.*		15.	6.	21.	33.	10.	35.
2310.	770.	154.	77.	11.	1.	*abc.*	*abd.*	*abe.*	*acd.*	*ace.*	*ade.*
3.	5.	2.	7.	11.		30.	105.	165.	42.	66.	231.
a.	*b.*	*c.*	*d.*	*e.*		*abcd.*	*abce.*	*abde.*	*acde.*	*bcde.*	
						210.	330.	1155.	462.	770.	

be.	*cd.*	*ce.*	*de.*		
55.	14.	22.	77.		
bcd.	*bce.*	*bde.*	*cde.*		
70.	110.	385.	154.		
				abcde.	
				2310.	

XI COROLLAIRE.

11. TOut nombre entier *z* eſt diviſible par un nombre ſimple.

b. 1. Car s'il eſt ſimple, il ſe peut diviſer luy-même [b] au juſte & ſans reſte. Et s'il eſt compoſé; un de ſes diviſeurs, comme *y*, eſt ſimple ou compoſé; ſi ce diviſeur eſt ſimple, c'eſt ce que l'on prétend. Et s'il eſt compoſé, un de ſes diviſeurs, comme *y*, qui eſt moindre que luy, eſt ſimple ou compoſé. Et s'il eſt encore compoſé; un des ſiens, comme *x*, moindre encore que luy eſt pareillement ou ſimple ou compoſé. Et comme on ne peut pas reïtérer de ſemblables raiſonnemens plus de fois qu'il y a d'unitez dans *y* ou dans *x*, il en faudra venir enfin à un dernier diviſeur comme *t* moindre que chacun de ceux qui l'auront précédé, & qui n'aura point d'autre diviſeur que luy-même ou l'unité, ou qui ſera ſimple. Mais ce nombre *t* étant un diviſeur du diviſeur *v*,

c. 9. eſt auſſi un [c] diviſeur du précédent *x* que le pénultiéme *v* meſure. Et comme *x* meſure encore le diviſeur *y*, & *y* le premier nombre *z*, le nombre ſimple *t* meſure [c] au juſte *y*, & [c] l'autre *z* enſuitte que l'on a propoſé.

z.	*y.*	*x.*	*v.*	*t.*	1.
2310.	770.	154.	77.	11.	1.

XII COROLLAIRE.

12. SI deux nombres *a* & *z* ſont compoſez entr'eux; quelque nombre ſimple en peut être un diviſeur commun. Parce que tout diviſeur commun *g* des nombres *a* & *z* aura pour meſure

a 11. quelque [a] nombre ſimple *e* ou *t*, qui meſure auſſi

b. 9. chacun [b] de ces mêmes *a* & *z*.

a.	*z.*	*g.*	*e.*	*t.*
12.	30.	6.	2.	3.

XIII COROLLAIRE.

13. SI deux nombres n'ont aucun diviſeur commun qui ſoit ſimple, ils ſont premiers entr'eux. Puiſque tous ceux qui ne ſont point premiers

miers entr'eux, ou qui ſont compoſez entr'eux, peuvent avoir [b] quelque nombre ſimple pour diviſeur commun. b. 12.

XIV COROLLAIRE.

14. SI un nombre a meſure chacune des parties z & y d'un nombre; il meſure auſſi ce même nombre entier $z+y$. Car ſi b eſt l'expoſant entier de la partie z diviſée ſans reſte par a, & c l'expoſant entier de l'autre partie y auſſi diviſée par a; le produit ab eſt [b] égal à la partie z, & le produit ac à la [b] partie y, & tout le nombre $ab+ac$ égal [c] au nombre entier z & y. Mais le diviſeur a meſure au juſte $ab+ac$, puiſque l'expoſant $b+c$ eſt un nombre entier. Et par conſéquent le même diviſeur a meſure auſſi $z+y$ ſans reſte. b. 18. 2. c. 9. 1.

$ab+ac$.
$a.\ b.\ z+y.\ c.\ b+c.$
$3.\ 5.\ 15+6.\ 2.\ 5+2$ ou 7

XV COROLLAIRE.

15. SI un nombre a meſure une partie z d'un certain nombre x, & qu'il n'en puiſſe meſurer l'autre partie $x-z$ qui reſte; il ne [a] peut meſurer au juſte ce même nombre x. Puiſque s'il le pouvoit, il meſureroit [b] auſſi la partie $x-z$ qui reſte. Ce qui repugne à la ſuppoſition. a. 16. 1. b. 14.

$a.\ z.\ x.\ x-z$
$3.\ 21.\ 31.\ 31-21$ ou $10.$

XVI COROLLAIRE.

16. SI un nombre a meſure un nombre x & ſa partie y; il meſure auſſi la partie $x-y$ qui reſte. Car ſi d eſt l'expoſant du nombre x diviſé par a, & b l'expoſant de la partie y auſſi diviſée par a; le produit ad eſt égal [b] au nombre x, & le produit ab égal à la [b] partie y. Et $ad-ab$ égale à la [c] partie $x-y$ qui reſte. Et par conſéquent a, qui meſure au juſte $ad-ab$, puiſque l'expoſant $d-b$ eſt un nombre entier, doit auſſi meſurer ſans reſte la partie $x-y$. b. 18. 2. c. 10. 1.

$a.\ x.\ y.\ x-y.\ d-b.$
$3.\ 21.\ 15.\ 21-15.\ 7-5.$
$ad-ab.$

XVII COROLLAIRE.

17. SI deux nombres b & c ſont premiers entr'eux; chacun eſt premier à l'égard de la ſomme $b+c$ des deux. Car nul diviſeur de b ne pouvant [b] eſtre un diviſeur de c, ſi ce n'eſt l'unité, nul auſſi que l'unité ſeule ne peut meſurer au juſte [c] la ſomme $b+c$, ou être un diviſeur commun des deux nombres b & $b+c$. Et nul nombre par la même raiſon ne peut être un diviſeur commun des [c] deux c & $b+c$, ſi ce n'eſt l'unité. b. *ſuppoſition.* c. 14.

$b.\ c.\ b+c.$
$31.\ 7.\ 31+7$ *ou* $39.$

plutôt 16

XVIII COROLLAIRE.

18. SI deux nombres b & c ſont premiers entr'eux, & qu'on ôte une ou pluſieurs fois le moindre c de b, autant de fois, par éxemple, qu'il

y a d'unitez dans *a*; le nombre *c* & le reſte *d* ſont premiers entr'eux. Car s'ils étoient compoſez entr'eux, ou qu'un nombre *e* pût être leur diviſeur commun; ce même diviſeur *e* meſureroit auſſi [b] tous les nombres *c* exprimez par *ac*, qu'on auroit pris dans *b*: & par une ſuitte néceſſaire [c] il meſureroit tout le nombre *b*, ou chacun des deux *b* & *c* qui ſont premiers entr'eux. Ce qui répugne à la ſuppoſition. Et par conſéquent *c* & *d* ſont [d] premiers entr'eux.

b. 9. c. 14. d. 16. 1.

b. c. a. b — ac. e
31. 7. 3. 31 — 21 ou 10. 1.
d.

I THEOREME.

19. SI deux nombres *b* & *c* ſont premiers entr'eux; leur produit *bc* eſt le plus petit nombre que l'un & l'autre puiſſe diviſer au juſte ou ſans reſte.

DEMONSTRATION.

Soit ζ le plus petit des nombres que *b* & *c* meſurent l'un & l'autre ſans reſte, & *c* le moindre des deux *b* & *c*. Afin que *c* meſure les nombres *b* tous enſemble que *z* comprend au juſte, il faut que *c* étant pris dans chacun de ces nombres *b* autant de fois qu'il s'y peut trouver, les reſtes *d* puiſſent encore être tous enſemble [b] meſurez par *c*, ou que *c* & *d* meſurent l'un & l'autre la ſomme *y* de tous ces reſtes *d*. Et chaque *b* qui eſt dans ζ fourniſſant une fois *d* pour *y*, il eſt clair que *b* eſt au juſte autant de fois dans *z* que *d* dans *y*. Mais *c* & *d*, qui peuvent chacun meſurer *y*, ſont [c] premiers entr'eux. Et *d* qui meſure au juſte les nombres *c* tous enſemble que comprend *y*, étant pris dans chacun de ces nombres *e* autant de fois qu'il s'y peut trouver, meſure [b] encore la ſomme *x* de tous les reſtes *e*. Et chaque *c* qui eſt dans *y* fourniſſant auſſi une fois *e* pour *x*, il eſt clair que *c* eſt au juſte autant de fois dans *y* que le nombre *e* dans *x*. Et continuant de la même ſorte juſqu'au dernier reſte qui eſt toûjours 1, comme ici juſqu'au dernier reſte *f*; le nombre *e* qui meſure au juſte les nombres *d* tous enſemble que comprend *x* au juſte, meſure [c] encore la ſomme *v* de tous les reſtes *f*. Et *d* eſt dans *x* autant de fois au juſte que le nombre *f* dans *v*.

b. 9 & 15. c. 18.

Mais il eſt évident que l'unité *f* n'eſt pas moins de fois dans *v* que dans *e* qui meſure *v* au juſte. Et ainſi *d* qui eſt dans *x* autant de fois au juſte que le nombre *f* dans *v*, n'eſt pas moins de fois dans *x* que l'unité dans *e*, ou que *d* même dans le produit *de*, puiſque *d* eſt dans *de* autant de fois [d] au juſte qu'il y a d'unitez *f* dans *e*. Donc *x* n'eſt pas moindre que *de*, ni *e* par conſéquent moins de fois dans *x* que dans le produit *de*, ou qu'il y a [d] d'unitez dans *d*; le nombre *e* étant au juſte autant de fois dans *de*, qu'il y a d'unitez dans *d*. Et on prouvera en remontant de la même ſorte que *c* n'eſt pas moins de fois dans *y* que dans le produit *cd*, ou qu'il y [d] a d'unitez dans *d*. Et pareillement que *b* n'eſt pas moins de fois dans *z* que dans *bc*, ou qu'il y a [d] d'unitez dans *c*; ou ce qui revient au même, il ſera clair, que le moindre nombre *z*, que *b* & *c* puiſſent chacun meſurer au juſte, n'eſt pas moindre que leur produit *bc*, ou que ζ & *bc* ne ſont qu'un même nombre, & le plus petit que *b* & *c* puiſſent meſurer au juſte.

d. 8. 2.

b. c. bc. d. cd. e. de. f. ef.
12. 7. 84. 5. 35. 2. 10. 1. 2.
z. y. x. v.

I COROLLAIRE.

20. SI deux divers nombres *b* & *c* ſont ſimples ; leur produit *bc* eſt le plus petit nombre [b] que l'un & l'autre puiſſe meſurer au juſte. Puiſque ces deux nombres [c] ſont premiers entr'eux.

b. c. bc. 11. 7. 77. b. 19. c. *définition*

II COROLLAIRE.

21. SI deux nombres *b* & *c* meſurent au juſte l'un & l'autre un même nombre *a* ; le moindre comme *z* que chacun des deux *b* & *c* puiſſe meſurer au juſte, peut auſſi meſurer cet autre *a* ſans reſte. Car ζ ne peut ſurpaſſer *a* par la ſuppoſition. Et ſi ζ & *a* ſont égaux ; le nombre *z* ou *a* ſe meſure [b] luy-même. Et ſi ζ eſt moindre que le nombre *a* ; les deux *b* & *c*, qui meſurent *a* l'un & l'autre au juſte, meſurent auſſi tous les nombres *z* enſemble [c] qu'on pourra prendre en *a*, & encore le [d] reſte *e* s'il s'en peut trouver un. Et ainſi le nombre *z*, plus grand que le reſte *e*, n'eſt pas le moindre que chacun des deux *b* & *c* puiſſe meſurer au juſte. Ce qui repugne à la ſuppoſition. Le reſte *e* eſt donc [e] nul, & ζ meſure [e] au juſte le nombre *a*.

b. ζ *a. c. e.* 12. 84. 168. 7. 0. b. 1. c. 9. d. 15. e. 16. 1.

III COROLLAIRE.

22. SI un nombre *d* meſure au juſte un produit *bc* de deux nombres *b* & *c*, & que *c* & *d* ſoient premiers entr'eux ; le nombre *d* eſt un diviſeur de l'autre nombre *b*. Car *c* & *d* étant premiers entr'eux, & chacun meſurant au juſte le produit *bc* ; leur produit *cd*, qui eſt le moindre nombre [b] que l'un & l'autre puiſſe meſurer au juſte, eſt [c] un diviſeur de *bc*. Si donc *e* eſt l'expoſant entier de la diviſion de *bc* par *cd* ; le nombre *bc* eſt égal [d] au produit *cde* du diviſeur *cd* par l'expoſant *e*. Et ſi on diviſe l'un & l'autre par *c* ; les expoſans *b* & *de* ſont [e] égaux, ou ne ſont qu'un même nombre. Mais ſi on diviſe *de* par *d*, on aura l'expoſant entier *e*. Et ainſi *d* eſt un diviſeur du nombre *de* ou *b*.

d. bc. b. c. cd. e. 4. 84. 12. 7. 28. 3. *cde. de.* b. 19. c. 21. d. 18. 2. e. 27. 3.

IV COROLLAIRE.

23. SI deux divers nombres *a* & *b* ſont ſimples ; tout diviſeur de leur plan, ou produit *ab*, eſt 1, ou *a*, ou *b*, ou *ab*. Car nommant ζ tel diviſeur qu'on voudra du nombre plan *ab*. Si les nombres *a* & *z* ſont premiers entr'eux, le nombre ζ ſera un diviſeur [b] du nombre ſimple *b*, c'eſt à dire 1 ou *b*, qui ſont eux ſeuls [c] les diviſeurs du nombre ſimple *b*.

1. 2. 3. 6. 1. *a. b. ab.* ζ. 1. 2. 3. 6. 1. *a. b. ab.* *z.* b. 22. c. *définition.*

Et ſi les nombres *a* & ζ ſont compoſez entr'eux ; le ſimple *a* ſera un [d] diviſeur de *z*. Et nommant *y* l'expoſant entier de la diviſion de *z* par *a*, le produit *ay* eſt égal [e] au nombre *z*, & peut auſſi meſurer *ab*, dont *z* eſt diviſeur. Et nommant encore *x* l'expoſant entier de la diviſion du nombre

d. 6. e. 18. 2.

c. 18. 2. *ab* par *ay* ou *z*, le produit *ayx* est égal [c] au nombre *ab*. Et divisant *ayx* &
f. 27. 3. *ab* par *a*, les exposans *yx* & *b* sont [f] égaux, ou ne sont qu'un même nombre. Et par conséquent 1 & *b*, qui sont les diviseurs de *b*, sont aussi les seuls diviseurs du nombre *yx*. Et ainsi le diviseur *y*, qui est entier, est nécéssairement 1 ou *b*; & *ay*, ou *z* son égal, est le nombre simple 1*a*, ou le nombre plan *ab*. Si donc deux nombres *a* & *b* sont simples, tout diviseur *z* de leur plan *ab* est un seul des quatre 1, *a*, *b*, *ab*.

1.	2.	3.	6.
1.	*a.*	*b.*	*ab.*
y.	*z.*	*x.*	*ayx.*
		yx.	

1.	2.	3.	6.
1.	*a.*	*b.*	*ab.*
	x.	*y.*	*z.*
		yx.	
			ayx.

V COROLLAIRE.

24. SI trois divers nombres *a*, *b*, *c*, sont simples; tout diviseur de leur solide *abc* est un des quatre du nombre *ab*, ou un des produits de ces quatre par *c*, c'est à dire un des huit 1, *a*, *b*, *ab*, *c*, *ac*, *bc*, *abc*.

Car nommant *z* tel diviseur qu'on voudra du solide *abc*. Si les nombres *c* & *z* sont premiers entr'eux, le nombre *z* sera un diviseur du nombre
b. 22. plan [b] *ab*, ou l'un des [c] quatre 1, *a*, *b*, *ab*,
c. 23.

1.	2.	3.	6.	5.	30.
1.	*a.*	*b.*	*ab.*	*c.*	*abc.*
z.					

1.	2.	3.	6.	5.	30.
1.	*a.*	*b.*	*ab.*	*c.*	*abc.*
			z.		

1.	2.	3.	6.	5.	30.
1.	*a.*	*b.*	*ab.*	*c.*	*abc.*
			z.		

1.	2.	3.	6.	5.	30.
1.	*a.*	*b.*	*ab.*	*c.*	*abc.*
			z.		

d. 6. Et si les nombres *c* & *z* sont composez entr'eux; le nombre *c* sera [d] un diviseur de *z*. Et nommant *y* l'exposant de la division du nombre *z* par *c*, le
e. 18. 2. produit *cy* [e] est égal à *z*, & peut aussi diviser au juste *abc*, dont *z* est diviseur. Et nommant encore *x* l'exposant de la division du nombre *abc* par *cy*, le produit *cyx* est égal [e] au nombre *abc*. Et divisant *cyx* & *abc* par *c*, les ex-
f. 27. 3. posans *yx* & *ab* sont [f] égaux, ou ne sont qu'un même nombre. Et par conséquent 1, *a*, *b*, *ab*, qui sont les seuls diviseurs du nombre plan *ab*, sont
g. 23. aussi les seuls du plan *yx*, & le diviseur *y* du nombre *yx* est [g] nécessairement ou 1, ou *a*, ou *b*, ou *ab*; & le nombre *cy*, ou *z* qui luy est égal, un produit de *c* par 1, ou par *a*, ou par *b*, ou par le plan *ab*; c'est à dire un des nombres 1*c*, *ac*, *bc*, *abc*. Si donc trois divers nombres *a*, *b*, *c*, sont simples, tout diviseur de leur solide *abc* est un des huit 1, *a*, *b*, *ab*, *c*, *ac*, *bc*, *abc*, qui sont aussi les mêmes que les quatre simples 1, *a*, *b*, *c*, & leurs 3 plans alternatifs *ab*, *ac*, *bc*, & leur solide unique *abc*.

1.	2.	3.	6.	5.	30.
1.	*a.*	*b.*	*ab.*	*c.*	*abc.*
y.			*x.*	*z.*	
			yx.	*cy.*	*cyx.*

1.	2.	3.	6.	5.	10.	30.
1.	*a.*	*b.*	*ab.*	*c.*	*ac.*	*abc.*
	y.	*x.*			*z.*	
			yx.		*cy.*	*cyx.*

1.	2.	3.	6.	5.	15.	30.
1.	*a.*	*b.*	*ab.*	*c.*	*bc.*	*abc.*
	x.	*y.*			*z.*	
			yx.		*cy.*	*cyx.*

1.	2.	3.	6.	5.	30.
1.	*a.*	*b.*	*ab.*	*c.*	*abc.*
x.			*y.*		*z.*
					cy.
					cyx.

VI COROLLAIRE.

25. ON pourra démontrer en ſuivant le même ordre, que ſi quatre nombres a, b, c, d, ſont ſimples ; leur ſurſolide $abcd$ ne peut avoir aucun diviſeur que l'un des huit du ſolide abc, ou l'un des produits de ces huit par d, ou qu'un des ſeize $1, a, b, ab, c, ac, bc, abc, d, ad, bd, abd, cd, acd, bcd, abcd$, qui ſont les ſimples même 1, a, b, c, d, & leurs 6 plans alternatifs, & leurs 4 ſolides alternatifs, & leur ſurſolide unique $abcd$.

Et pareillement le produit $abcde$ des cinq nombres ſimples a, b, c, d, e, ne peut avoir que les 16 précédens, & les produits de ces 16 par e ; c'eſt à dire que 2 fois 16, ou 32 diviſeurs, qui ſeront les 6 ſimples $1, a, b, c, d, e$, & leurs 10 plans alternatifs, & leurs 10 ſolides alternatifs, & leurs 5 ſurſolides alternatifs, & leur produit unique des 5 degrez $abcde$.

Et le produit $abcdef$ n'auroit pareillement que 2 fois 32, ou 64 diviſeurs, qui ſeroient les ſimples $1, a, b, c, d, e, f$, & leurs 15 plans alternatifs, & leurs 20 ſolides alternatifs, & leurs 15 ſurſolides alternatifs, & leurs 6 produits alternatifs de 5 degrez, & leur produit unique de 5 degrez $abcdef$. Et on peut continuer de la même ſorte juſques à l'infini.

VII COROLLAIRE.

26. LE plan de deux nombres ſimples, ou le ſolide de trois, ou le ſurſolide de quatre, ou le produit de pluſieurs, ne peut avoir aucun diviſeur ſimple que [b] l'unité, ou l'un des deux, ou des trois, ou des quatre ſimples, &c, dont on ſuppoſe qu'il eſt un produit ; comme le produit $abcdefgh$ des ſimples a, b, c, d, e, f, g, h, aucun diviſeur ſimple que l'un de ces huit mêmes, ou l'unité. b. 23. 24. 25.

VIII COROLLAIRE.

27. SI le nombre a eſt ſimple ; tout diviſeur de ſon quarré aa eſt un ſeul des trois $1, a, aa$. Et tout diviſeur de ſon cube a^3, un ſeul des quatre $1, a, aa, a^3$. Et de ſon quarré de quarré $a4$, un ſeul des cinq $1, a, aa, a^3, a^4$. Et de la 5[e] puiſſance $a5$, un ſeul des ſix $1, a, aa, a^3, a4, a^5$. Et ainſi des autres juſques à l'infini. Parce que tous les diviſeurs ſimples de ces diverſes puiſſances ne ſont que l'unité, & le ſeul nombre ſimple a ; & tous leurs plans alternatifs qu'un même quarré aa ; & tous leurs ſurſolides qu'un même cube a^3. Et ainſi du reſte.

Puiſſances 1. a. aa. a^3. $a4$. a^5. a^6. $a7$. a^8. $a9$. a^{10}. a^{11}. a^{12}. &c.
Nombres des diviſeurs 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. &c.

IX COROLLAIRE.

28. SI les nombres a & b ſont ſimples ; tout diviſeur aab des trois a, a, b, eſt un des trois $1, a, aa$, ou l'un des divers produits de ces trois par b ; c'eſt à dire, un des ſix $1, a, aa, 1b, ab, aab$. Parceque tous les plans alternatifs des ſimples a, a, b, ſont aa & ab.

Et tout diviſeur du ſurſolide *aabb* des quatre *a*, *a*, *b*, *b*, eſt un des 6 précédens, ou l'un des produits des 3 derniers par *b*; c'eſt à dire un des 9 diviſeurs 1, *a*, *aa*, 1*b*, *ab*, *aab*, 1*bb*, *abb*, *aabb*. Parceque tous les plans alternatifs des quatre nombres ſimples *a*, *a*, *b*, *b*, ſont *aa*, *ab*, *bb*; & tous leurs ſolides alternatifs, les deux *aab*, *abb*; Ou parceque les 6 produits alternatifs *aa*, *ab*, *aab*, *bb*, *abb*, *aabb*, ſont tous ceux des 4 nombres ſimples *a*, *a*, *b*, *b*.

Et pareillement tout diviſeur du produit *aabbb* des cinq nombres ſimples *a*, *a*, *b*, *b*, *b*, eſt un des 9 précédens, ou un des trois produits des trois derniers de ces 9 par *b*. Mais tout diviſeur du produit aab^3c auroit un des 12 précédens, ou un de leurs produits par *c*. Et tout produit du nouveau aab^3cc des ſept nombres ſimples *a*, *a*, *b*, *b*, *b*, *c*, *c*, auroit l'un de ces 24 diviſeurs, ou l'un des produits des 12 derniers par *c*. Et aab^3ccd auroit ces 36, & les produits de ces 36 par *d*, ou 72 diviſeurs. Et ainſi des autres.

1. *a*. *aa*. 3.
1*b*. *ab*. *aab*. 3. } 12
1*bb*. *abb*. *aabb*. 3.
1b^3. ab^3. aab^3. 3.

1*c*. *ac*. *aac*. 1*bc*. *abc*. *aabc*. 1*bbc*. *abbc*. *aabbc*. 1b^3c. ab^3c. aab^3c. 12
1*cc*. *acc*. *aacc*. 1*bcc*. *abcc*. *aabcc*. 1*bbcc*. *abbcc*. *aabbcc*. 1b^3cc. ab^3cc. aab^3cc. 12
1*d*. *ad*. *aad*. 1*bd*. *abd*. *aabd*. 1*bbd*. *abbd*. *aabbd*. 1b^3d. ab^3d. aab^3d.
1*cd*. *acd*. *aacd*. 1*bcd*. 1*abcd*. *aabcd*. 1*bbcd*. *abbcd*. *aabbcd*. 1b^3cd. ab^3cd. aab^3cd. } 36
ccd. *accd*. *aaccd*. 1*bccd*. *abccd*. *aabccd*. 1*bbccd*. *abbccd*. *aabbccd*. 1b^3ccd. ab^3ccd. aab^3ccd.

I PROBLEME.

29. *Pour trouver tous les diviſeurs ſimples égaux ou inégaux d'un certain nombre Z.*

On le diviſera par 2, s'il eſt pair; & l'expoſant pareillement par 2, s'il eſt encore pair; & auſſi l'expoſant nouveau par 2, s'il eſt pair. Et ainſi de ſuitte juſqu'au premier expoſant impair. Et on diviſera pareillement par 3, s'il eſt poſſible, l'expoſant impair; & par 3 encore, s'il eſt poſſible, l'expoſant qu'on aura trouvé. Et ainſi de ſuitte juſques au premier expoſant, que 3 ne pourra plus diviſer au juſte. Et on tentera par ordre de ſemblables diviſions par 5; & enſuitte par 7; & aprés cela par 11; & par chacun des ſimples qui les ſuivent, juſques à un dernier expoſant qui ſoit ſimple. Et le problême alors ſera [b] réſolu.

[b] 26 & 28.

PREMIER EXEMPLE.

Pour trouver tous les diviſeurs ſimples de 462. Je diviſe ce nombre premierement par 2; & enſuitte par 3 l'expoſant impair 231; & par 7 l'expoſant 77, que 3 & 5 ne peuvent diviſer au juſte. Et comme l'expoſant 11 eſt un nombre ſimple; l'opération eſt faite, & donne à connoître que tous les diviſeurs 2, 3, 7, 11, 1, ſont tous les ſimples de 462.

Diviſer 462(231(77(11(1
par 2 3 7 11

SECOND EXEMPLE.

Pour trouver tous les diviſeurs ſimples de 180. Je le diviſe par 2; & l'ex-

posant 90, qui est un nombre pair, encore par 2; & de nouveau l'exposant impair 45 par 3; & l'exposant 15 aussi par 3. Et comme le dernier exposant 5 est simple; je trouve enfin que tous les diviseurs simples égaux ou inégaux de 180 sont 1, 2, 2, 3, 3, 5.

Diviser 180(90(45(15(5(1
par 2 2 3 3 5

Et on trouvera de la même sorte que tous les diviseurs simples égaux ou inégaux de 540 sont 1, 2, 2, 3, 3, 3, 5. Et que tous ceux de 144 sont 1, 2, 2, 2, 2, 3, 3.

Diviser 540(270(135(45(15(5(1. *Diviser* 144(72(36(18(9(3(1.
par 2 2 3 3 3 5 *par* 2 2 2 2 3 3

DEMONSTRATION.

SI quelques puissances de divers nombres simples *a* & *b*, comme le quarré *aa*, & le cube b^3, peuvent l'un & l'autre diviser *z* sans reste; & que l'exposant de la division de *z* par *aa* soit *y*: le produit *aay* est égal [b] au nombre *z*, & on peut diviser l'un & l'autre par *a*; & l'exposant *ay* encore par *a*. Et comme *a* & *b* sont premiers [c] entr'eux, puisque l'un & l'autre est simple; le cube b^3 qui mesure au juste le nombre *z*, ou *aay*, divise aussi sans reste l'exposant *ay*, & ensuitte l'exposant *y* par la même raison. Et nommant *x* l'exposant entier de la division du nombre *y* par le cube b^3, le produit b^3x est égal [b] au nombre *y*, & l'autre aab^3x au [d] nombre *z* ou *aay*. Et on peut diviser b^3x ou *y* par *b*; & l'exposant *bbx* par *b*; & encore l'exposant *bx* par *b*. Et on démontreroit de la même sorte que tout diviseur simple du nombre aab^3x ou *z*, & qui est différent des deux *a* & *b*, peut encore diviser *x* au juste. Et ainsi du reste.

b. 18. 2.
c. *définition.*
d. 20. 3.

2. 3. 540. 4. 135. 27. 5.
z. *y.* *x.*
a. b. *aay. aa.* $b^3x.$ $b^3.$
$aab^3x.$

Diviser z 540(270(135(45(15(5(1. *Et z* 540(270(45(15(5(1.
aay(*ay*(*y*(b^3x(*bbx*(*bx*(*x*(1. aab^3x(ab^3x(b^3x(*bbx*(*bx*(*x*(1.
par a a b b b x *par a a b b b x*
2 2 3 3 3 5

II PROBLEME.

30. *POur trouver tous les diviseurs d'un certain nombre entier.*

On en prendra [b] tous les diviseurs simples égaux ou inégaux, & tous les divers produits [c] alternatifs de ces diviseurs simples. Et le problême sera [d] résolu.

b. 29.
c. 3. 5. 6. *du Livre 5.*
d. 23. 24. 25.

PREMIER EXEMPLE.

Pour trouver tous les diviseurs de 462. J'en cherche tous les simples 2, 3, 7, 11, négligeant l'unité qui ne change point les produits. Et je multiplie le premier 2 par le second 3; & l'un & l'autre, & leur plan 6, par le troisiéme 7. Et chacun des trois 2, 3, 7, & des quatre produits 6, 14, 21, 42, par le quatriéme 7. Et prenant encore 1, je connois que tous les diviseurs de 462 sont les 16 qu'on expose ici.

1er	2	*Diviſer* 462(231(77(11(1
2e	3	6 *par* 2 3 7 11
3e	7	14. 21. 42.
4e	11	22. 33. 77. 66. 154. 231. 462.
	1	

SECOND EXEMPLE.

Pour trouver tous les diviſeurs de 144. J'en cherche tous les ſimples 2, 2, 2, 2, 3, 3. Et je multiplie le premier 2 par le ſecond qui eſt encore 2. Et le quarré 4 par le troiſiéme 2. Et le cube 8 par le quatriéme 2. Et le premier 2, & chacun des produits 4, 8, 16, par le cinquiéme 3. Et chacun des cinq nombres 3, 6, 12, 24, 48, par le ſixiéme 3. Et prenant encore 1, je connois que tous les diviſeurs de 144 ſont les 15 qu'on expoſe ici.

1er	2	*Diviſer* 144(72(36(18(9(3(1
2e	2	4 *par* 2 2 2 2 3 3
3e	2	8
4e	2	16
5e	3	6. 12. 24. 48.
6e	3	9. 18. 36. 72. 144.
7e	1	

Et on trouvera de la même ſorte les 24 diviſeurs du nombre compoſé 540. Et pareillement les 24 du compoſé 360.

Diviſer 360(180(90(45(15(5(1

1er	2	
2d	2	4.
3e	2	8.
4e	3	6. 12. 24.
5e	3	9. 18. 36. 72.
6e	5	10. 15. 20. 40. 30. 60.
7e	1	120. 45. 90. 180. 360.

Diviſer 540(270(135(45(15(5(1

1er	2	
2d	2	4
3e	3	6. 12.
4e	3	9. 18. 36.
5e	3	27. 54. 108.
6e	5	10. 15. 20. 30. 60. 45. 90.
7e	1	180. 135. 270. 540.

III PROBLEME.

31. *POur connoître combien un nombre compoſé peut avoir de divers diviſeurs.*

b. 29. 4 & 1 *du Livre 5.* On en cherchera [b] tous les ſimples, & on prendra [c] le nombre de tous les divers produits alternatifs.

EXEMPLE.

Comme pour ſçavoir combien 15876000 peut avoir de divers diviſeurs. On cherchera tous les ſimples égaux ou inégaux 1, 2, 2, 2, 2, 2, 3, 3, 3, 3, 3, 5, 5, 5, 7, 7. Et on prendra 6, pour 1 & pour les 5 égaux 2, 2, 2, 2, 2; & 4 fois 6, pour les 4 égaux 3, 3, 3, 3. Et raſſemblant 6 & 24, la ſomme 30 ſera priſe 3 fois, pour les 3 égaux 5, 5, 5. Et raſſemblant

blant encore 6, 24, 90, la ſomme 120 ſera priſe encore 2 fois, pour les 2 égaux 7 & 7. Et enfin les nombres enſemble 6, 24, 90, 240, formeront la ſomme ou le nombre 360 de tous les diviſeurs du nombre propoſé, qui ſont 1, & les 4 ſimples 2, 3, 5, 7; & tous les 355 produits alternatifs des 14 ſimples égaux ou inégaux 2, 2, 2, 2, 2, 3, 3, 3, 3, 5, 5, 5, 7, 7. Et ſi on prend a pour 2, & b pour 3, & c pour 5, & d pour 7. le nombre propoſé 1587600 répond au produit $a^5b^4c^2dd$, & on le peut encore exprimer ainſi $2^5.4.5^2.7^2$.

Diviſer 1587600 (793800 (396900 (198450 (99225 (49612,5
par 2 2 2 2 2

Et 49612,5 (16537,5 (5512,5 (1837,5 (612,5 (122,5 (24,5 (4,9 (1
par 3 3 3 3 5 5 5 7 7

IV PROBLEME.

52. *Pour trouver tous les diviſeurs d'une grandeur littérale.*

On la diviſera par une linéaire ou ſimple, ou par une qui n'ait point d'autre diviſeur qu'elle-même ou l'unité. Et on diviſera l'expoſant de la même ſorte. Et ainſi du reſte. Et on cherchera enſuitte tous [b] les divers produits alternatifs de tous les diviſeurs égaux ou inégaux qu'on aura découverts. Et le problême ſera réſolu. Les éxemples éclairciront ces régles.

[b] 3 & 6 du Livre 5.

PREMIER EXEMPLE.

Pour trouver tous les diviſeurs de la grandeur $a^3b+aabb$. Je la diviſe premiérement par a; & l'expoſant $aab+abb$ encore par a; & l'expoſant nouveau $ab+bb$ par b. Et comme le dernier expoſant $a+b$ eſt ſimple ou linéaire: je multiplie le premier diviſeur a par le ſecond a, & les deux grandeurs a & aa par le troiſiéme b; & les deux a & b, & les produits aa, ab, aab, par le quatriéme $a+b$. Et je trouve enfin que tous les diviſeurs de la grandeur propoſée ſont les 18 qu'on expoſe ici, ſans conter l'unité.

		Diviſer $a^3b+aabb$ ($aab+abb$ ($ab+bb$ ($a+b$ (1
1er	a	
2e	a	aa *par* a a b $a+b$
3e	b	$ab.$ $aab.$
4e	$a+b$	$aa+ab.$ $ab+bb.$ $a^3+aab.$ $aab+abb.$ $a^3b+aabb.$
5e	1	

SECOND EXEMPLE.

Pour trouver tous les diviſeurs de la grandeur $a^6+2a^4cc+aac4$. Je la diviſe premiérement par a; & l'expoſant $a^5+2a^3cc+ac4$ pareillement par a; & l'expoſant nouveau $a4+2aacc+c4$ ne pouvant être diviſé ni par a, ni par c, ni par $a+c$, ni par $a-c$; je le diviſe par $aa+cc$. Et comme l'expoſant eſt encore cette même grandeur $aa+cc$, qui n'a point d'autre diviſeur qu'elle-même ou l'unité: je multiplie le premier diviſeur a par le ſecond a; & le premier a, & le produit aa, par le troiſiéme $aa+cc$; & ce troiſiéme

V

$aa+cc$, & chacun des deux derniers produits a^3+acc, & a^4+aacc, par le quatriéme $aa+cc$. Et je trouve enfin que tous les diviſeurs de la grandeur $a^6+2a^4cc+aac^4$ ſont les dix qu'on expoſe ici.

1ere	a	*Diviſer* $a^6+2a^4cc+aac^4$	($a^5+2a^3cc+ac^4$ ($a^4+2a^2cc+c^4$ ($aa+cc$ (1
2e	a	*aa. par* a	a $aa+cc$ $aa+cc$
3e	$aa+cc$	a^3+acc. a^4+aacc.	
4e	$aa+cc$	$a^4+2aacc+c^4$. $a^5+2a^3cc+ac^4$. $a^6+2a^4cc+aac^4$.	
5e	1		

I COROLLAIRE.

33. SI on prend par ordre 1, & 2, & les puiſſances ſucceſſives de 2, juſques à ce qu'on ait une ſomme qui ſoit un nombre ſimple; le produit de ce nombre ſimple par la derniére des puiſſances ſucceſſives de 2, que l'on aura priſes, eſt un nombre parfait.

DEMONSTRATION.

Si le nombre 2 eſt dénommé par a, & que la ſomme, par exemple, $1+a+aa+a^3+a4$ ſoit un nombre ſimple; ſon produit par la puiſſance $a4$, qui eſt la derniére des ſucceſſives $1, a, aa, a^3, a4$, que la ſomme comprend, eſt $1a^4+a^5+a^6+a^7+a^8$, dont tous les diviſeurs, qui ſont moindres que luy, ſont [b] les neuf 1, a, aa, a^3, a^4, $1+a+aa+a^3+a4$, $1a+aa+a^3+a^4+a^5$, $1aa+a^3+a4+a^5+a^6$, $1a^3+a4+a^5+a^6+a^7$. Mais le ſixiéme de tous ces diviſeurs eſt égal aux 5 premiers enſemble $1, a, aa, a^3, a^4$, puiſqu'il en eſt la ſomme. Et le ſeptiéme eſt double du ſixiéme $1+a+aa+a^3+a^4$, puiſqu'il eſt un produit de ce ſixiéme même par a ou par 2. Et ainſi le ſeptiéme eſt égal luy ſeul au ſixiéme & aux 5 premiers enſemble; puiſque le ſixiéme & les 5 premiers ſont auſſi tous enſemble le double du ſixiéme. Et par la même raiſon; le huitiéme, qui eſt encore le double du ſeptiéme $1a+aa+a^3+a4+a^5$, eſt égal aux 7 premiers enſemble. Et le neuviéme pareillement égal aux 8 qui le précédent. Et enfin le produit $1a4+a^5+a^6+a^7+a^8$, qui eſt le double du neuviéme diviſeur $1a^3+a4+a^5+a^6+a^7$, eſt égal à tous les neuf diviſeurs enſemble $1, a, aa, a^3, a4, 1+a+aa+a^3+a4, 1a+aa+a^3+a^4+a^5, 1aa+a^3+a^4+a^5+a^6, 1a^3+a4+a^5+a^6+a^7$. Et comme il ne peut avoir aucun diviſeur que l'un de [b] ces 9 ou luy-même; il eſt clair que ce nombre eſt [c] parfait. Et c'eſt la même choſe de tous les autres ſemblables juſques à l'infini.

b. 32.

c. *définition.*

Le nombre 6 eſt le premier des nombres parfaits. Et 28, qui eſt égal à tous ſes diviſeurs 1, 2, 4, 7, 14, eſt le ſecond de ces mêmes nombres.

1. 2. 4. 8. 16		
	1. a. aa. a^3. $a4$.	31
6e	$1+a+aa+a^3+a4$	31
7e	$1a+aa+a^3+a^4+a^5$	62.
8e	$1aa+a^3+a4+a^5+a^6$	124
9e	$1a^3+a4+a^5+a^6+a^7$	248
Produit	$1a^4+a^5+a^6+a^7+a^8$	496

Diviſer $a^4+a^5+a^6+a^7+a^8$ ($a^3+a^4+a^5+a^6+a^7$ ($aa+a^3+a4+a^5+a^6$

par $1a$ $1a$

Et $aa+a^3+a^4+a^5+a^6$ ($a+aa+a^3+a4+a^5$ ($1+a+aa+a^3+a^4$ (1

par $1a$ $1a$ $1+1a+1aa+1a^3+a4$

Et le troiſiéme eſt 496 égal à tous ſes diviſeurs 1, 2, 4, 8, 16, 31, 62, 124, 248. Et le quatriéme eſt 8128. Et le cinquiéme 2355036. Et le ſixiéme 85898690 56. Et le ſeptiéme 137438691328. Et le huitiéme 2385843008139521 28. Et la lettre *a* dénommant toûjours 2, le neuviéme des nombres parfaits eſt $a^{513}-a^{256}$, c'eſt à dire la puiſſance 513[c] du nombre 2 moins ſa puiſſance 256[c]. La longueur du calcul n'a pas permis d'en trouver encore d'autres. 33550336 (faux)

II COROLLAIRE.

34. TOut diviſeur ſimple du produit *bc* de deux nombres *b* & *c* eſt un diviſeur ſimple de l'un ou de l'autre. Car tout diviſeur ſimple *d* du produit *bc*, qui ne peut diviſer ſans reſte l'un des deux *b* & *c*, eſt premier à [b] l'égard de ce même nombre qu'il ne peut diviſer, & par conſéquent il eſt un [c] diviſeur de l'autre.

b. 12.
c. 7.
Produit bc. 84. (21
Diviſeur d. 4

b. 8.
c. 22.

III COROLLAIRE.

35. TOut diviſeur ſimple *d* d'un nombre quarré *bb*, ou d'un cubique b^3, ou d'une autre puiſſance de *b*, eſt auſſi un diviſeur [b] ſimple du même nombre *b*; Puiſque le quarré *bb* eſt un produit ou un plan des deux *b* & *b*. Et le cube b^3 un ſolide de *b* par le quarré *bb*. Et la puiſſance b^4 un ſurſolide du cube b^3 par le même côté *b*. Et ainſi du reſte.

côté b. 12.
Quarré bb. 144. (36
Diviſeur d. 4

b. 34.

IV COROLLAIRE.

36. SI deux nombres *a* & *z* ſont premiers entr'eux, & les deux *b* & *z* auſſi premiers entr'eux; le produit *ab* des deux *a* & *b* & le nombre *z* ſont premiers entr'eux. Car tout diviſeur ſimple du produit *ab* eſt auſſi l'un des ſimples [b] du nombre *a* ou *b*. Mais parmi tous les diviſeurs de chacun des nombres *a* & *b* & du nombre *z*, il ne s'en trouve aucun que l'unité qui puiſſe être commun [c] aux deux *a* & *z*, ou aux [c] deux *b* & *z*. Donc auſſi parmi tous les ſimples du produit *ab* & du nombre *z*, il ne s'en trouve aucun qui leur ſoit commun. Et par conſéquent le produit *ab* & le nombre *z* ſont [d] premiers entr'eux.

a. 5.
b. 12. *z.* 7.
ab. 60.

b. 34.
c. *ſuppoſition.*
d. 26. & *définition.*

V COROLLAIRE.

37. SI deux nombres *a* & *b* ſont premiers l'un & l'autre à l'égard de chacun des deux *z* & *y*; les produits ou les nombres *ab* & *zy* ſont premiers entr'eux. Car le produit *ab* & le nombre *z* ſont premiers [b] entr'eux. Et le produit *ab* & le nombre *y* auſſi premiers [b] entr'eux. Et par conſéquent le produit *ab* & l'autre *zy* ſont [b] premiers entr'eux.

5. *a.* *z.* 7.
12. *b.* *y.* 11.
60. *ab.* *zy.* 77.

b. 36.

VI COROLLAIRE.

38. SI deux nombres *a* & ζ ſont premiers entr'eux; chaque puiſſance de l'un de ces deux nombres eſt premiére à l'égard de chacune des puiſſances de l'autre. Car tout diviſeur ſimple de telle puiſſance du nombre *a* qu'on voudra eſt un diviſeur [b] ſimple de ce même nombre *a*. Et tout ſimple de telle qu'on voudra de ζ, un ſimple [b] auſſi de ζ. Comme donc parmi tous les diviſeurs des nombres *a* & ζ, il ne s'en trouve aucun qui leur ſoit [c] commun, ſi ce n'eſt l'unité; deux telles puiſſances qu'on voudra, l'une du nombre *a*, & l'autre du nombre ζ, n'ont [d] aucun diviſeur qui leur ſoit commun, ou ſont [e] premiéres entr'elles.

b. 35. *c. ſuppoſition.* d. 37. *e. définition.*

3.	9.	27.	81.	243.	729.	2187.
a.	*aa.*	a^3.	a^4.	a^5.	a^6.	a^7.
ζ.	ζζ.	$ζ^3$.	$ζ^4$.	$ζ^5$.	$ζ^6$.	$ζ^7$.
2.	4.	8.	16.	32.	64.	128.

VII COROLLAIRE.

39. LE ſolide *bcd* de trois divers nombres ſimples *b*, *c*, *d*, eſt le moindre que chacun de ces ſimples puiſſe meſurer au juſte. Car le moindre, que chacun des divers nombres ſimples *b*, *c*, *d*, puiſſe meſurer au juſte, peut être luy-même meſuré par le moindre *bc*, que chacun [b] des deux *b* & *c* peut meſurer ſans reſte; & il peut être encore diviſé par *d*. Mais *bc* & *d* ſont [c] premiers entr'eux. Et par conſéquent *bcd* eſt le plus [b] petit nombre que les deux *bc* & *d* puiſſent chacun meſurer au juſte. Et ce même produit *bcd* des divers ſimples *b*, *c*, *d*, eſt le plus petit nombre qu'ils puiſſent chacun meſurer au juſte.

b. 19. c. 36.

b.	*c.*	*d.*	*bcd.*	*bc.*
2.	3.	5.	30.	6.

VIII COROLLAIRE.

40. ET on démontrera en ſuivant le même ordre que le ſurſolide de quatre, ou le produit de divers nombres ſimples, eſt toûjours le moindre que chacun d'eux puiſſe meſurer au juſte.

IX COROLLAIRE.

41. SI un nombre ζ eſt le plus petit que divers ſimples *a*, *b*, *c*, *d*, puiſſent chacun meſurer au juſte; nul autre ſimple n'eſt diviſeur de ζ. Parceque le nombre ζ eſt le produit [b] même *abcd* de tous ces divers ſimples, qui ne peut avoir aucun diviſeur [c] ſimple que l'un d'entr'eux, ou 1.

b 40. c. 26.

ζ.	*a.*	*b.*	*c.*	*d.*
210.	7.	2.	3.	5.
abcd.				

V PROBLEME.

42. *POur trouver la meſure commune la plus grande de deux grandeurs.*

On ôtera la moindre *c* de la plus grande *b* autant de fois qu'on le pourra; & le reſte *d* pareillement autant de fois qu'on le pourra de la moindre *c*; & le nouveau reſte *e* de la même ſorte du premier reſte *d*; & l'autre reſte *f* du ſecond reſte *e*. Et ainſi de ſuitte juſques à celuy des re-

ſtes, comme *g*, qui n'en laiſſe aucun. Et ce reſte *g* ſatisfait enfin au problême.

DEMONSTRATION.

La meſure commune la plus grande des grandeurs *b* & *c* diviſant *b* ſans reſte, & toutes les grandeurs *c* que l'on peut prendre en *b*, meſure encore au juſte [b] le premier reſte *d*. Et par conſéquent elle eſt encore une meſure commune des deux grandeurs *c* & *d*. Et pareillement la plus grande commune des deux *c* & *d* eſt encore commune [b] aux deux *d* & *e*. Et enſuitte aux reſtes *e* & *f*. Et auſſi [b] aux deux *f* & *g*. Et ainſi de ſuitte juſqu'au dernier *g*, qui diviſe ou meſure au juſte le pénultiéme *f*. Mais le dernier reſte *g* ne peut avoir une meſure juſte plus [c] grande qu'il n'eſt luy-même; ni par conſéquent les deux reſtes *f* & *g* une commune qui ſurpaſſe *g*; ni pareillement les deux *e* & *f*; ni enſuitte les deux *d* & *e*; ni encore les grandeurs *c* & *d*; ni enfin les deux *b* & *c*. b. 16. c. 2.

Mais *g* meſurant *f*, & ſe meſurant [c] luy-même, meſure auſſi au juſte [d] tous les reſtes *f* qui ſont dans *e*, & le [e] reſte *g*, ou [f] le reſte entier *e*. Et par la même raiſon, il meſure encore tous les reſtes *e* qui ſont en *d*, & le reſte *f*, ou le reſte entier *d*; Et pareillement tous les reſtes *d* qui ſont compris dans *c*, & le reſte *e*, ou la grandeur *c*; & enfin toutes les grandeurs *c* qui ſont compriſes en *b*, & le reſte *d*, ou la grandeur *b*. De ſorte que le reſte *g*, qui eſt le dernier, étant un diviſeur commun des grandeurs *b* & *c*; & ces deux grandeurs *b* & *c* ne pouvant en avoir un commun qui ſurpaſſe *g*; il eſt évident que ce dernier reſte *g* eſt la meſure commune la plus grande des grandeurs *b* & *c*. Et qu'ainſi le problême a preſcrit ce qu'il falloit faire. d. 9. e. 1. f. 14.

La grande b. 86 (2 1^er^ *expoſant*
la petite c. 36 (2 2^d^ *expoſant*
1^er^ *reſte d.* 14 (1 3^e^ *expoſant*
2^d^ *reſte e.* 8 (1 4^e^ *expoſant*
3^e^ *reſte f.* 6 (3 5^e^ *expoſant juſte*
4^e^ *reſte g.* 2 *plus grand diviſeur commun.*

PREMIER EXEMPLE.

Pour trouver la meſure commune la plus grande, ou le plus grand diviſeur commun, des deux nombres 32 & 64 je diviſe 64 par 32. Et parceque la diviſion eſt juſte ou ſans reſte; je connois que le diviſeur 32 eſt luy-même le plus grand diviſeur commun des deux nombres 32 & 64.

Diviſer 64 (2 *expoſant juſte*
par 32 *plus grand diviſeur commun.*

SECOND EXEMPLE.

Pour trouver le plus grand diviſeur commun des deux nombres 25 & 30. Je diviſe 30 par 25, & 25 par le reſte 5, qui fait la diviſion ſans reſte, & qui eſt le plus grand diviſeur commun de 25 & de 30.

Diviſer 30 (1 *expoſant*
par 25 (5 *expoſant juſte*
par 5 *plus grand diviſeur commun.*

TROISIEME EXEMPLE.

Et pour trouver le plus grand diviſeur commun des deux nombres 27 & 21. Je diviſe 27 par 21 ; & 21 par le reſte 6 ; & ce reſte 6 par l'autre reſte 3, qui fait la diviſion ſans reſte, & qui eſt auſſi le plus grand diviſeur commun des nombres 27 & 21.

Diviſer 27 (1 *expoſant*
par 21 (3 *expoſant*
par 6 (2 *expoſant juſte*
par 3 *plus grand diviſeur commun.*

QUATRIEME EXEMPLE.

Et on trouve de la même ſorte que 2 eſt le plus grand diviſeur commun des nombres 86 & 36. Et pareillement que le dernier reſte, ou l'unité ſeule, eſt le plus grand diviſeur commun des deux nombres 98 & 47, qui ſont premiers entr'eux.

Diviſer 98 (2 *expoſant*
par 47 (11 *expoſant*
par 4 (1 *expoſant*
par 3 (3 *expoſant*
par 1 *plus grand diviſeur commun.*

VI PROBLEME.

43. *POur trouver la meſure commune la plus grande, ou le plus grand diviſeur commun, des grandeurs littérales.*

On cherchera auſſi tous les diviſeurs ſimples égaux ou inégaux de l'une & de l'autre. Et prenant enſuitte le produit de tous ceux qu'on trouve également diſtribuez de part & d'autre ; on aura [b] le diviſeur qu'on cherche.

b. 32.

PREMIER EXEMPLE.

Pour trouver le plus grand diviſeur commun des grandeurs *abc*, *acd*. Je prens tous les ſimples *a*, *b*, *c*, de l'une, & tous les ſimples *a*, *c*, *d*, de l'autre. Et le produit *ac* des deux *a* & *c*, qui ſont une fois chacune de part & d'autre, eſt le plus grand diviſeur commun des deux grandeurs *abc* & *acd*.

abc. *acd.*
a. b. c. *a. c. d.*
ac.

Et pour trouver le plus grand diviſeur commun des grandeurs a^5bbcd & a^3b^3dde. Je prens le produit a^3bbd des 6 ſimples *a*, *a*, *a*, *b*, *b*, *d*, qui ſe trouvent également de part & d'autre. Et ce produit réſout la queſtion.

$a^5bbcd.$ $a^3b^3dde.$
$a.a.a.a.a.b.b.c.d.$ $a.a.a.b.b.b.d.d.e.$

SECOND EXEMPLE.

Pour trouver le plus grand diviſeur commun des grandeurs $4a^6ccm^3p + a^6ccoomm$ & $oopp\zeta^4 + 4mp^3\zeta^4$. Je prens tous les diviſeurs ſimples *a*, *a*, *a*, *a*, *a*, *a*, *c*, *c*, *m*, *m*, $oo+4mp$, de l'une, & tous les ſimples *p*, *p*, ζ, ζ, ζ, ζ, $oo+4mp$ de l'autre Et parceque le ſeul $oo+4mp$ eſt une fois de part & d'autre, & que nul autre ne s'y trouve ; il eſt le ſeul commun, &

par conſéquent le plus grand des grandeurs propoſées. Pour abbréger, on peut diviſer d'abord la premiére grandeur par a^6ccmm, & la ſeconde par $ppz4$. On donnera une régle plus méthodique ailleurs pour trouver facilement ces plus grands diviſeurs communs, ſans être obligé d'en chercher tous les ſimples.

Diviſer $a^6ccoomm+4a^6ccm^3p$ par $2a^6ccmm$ ($oo+4mp$ *expoſant* (1 ; $2oo+4mp$

Diviſer $oopp\zeta4+4mp^3\zeta4$ par $2pp\zeta^4$ ($oo+4mp$ *expoſant* (1 ; $2oo+4mp$

COROLLAIRE.

44. TOute meſure commune de deux grandeurs diviſe ou meſure auſſi leur plus grande au juſte.

Comme ſi z eſt une meſure commune des grandeurs b & c, & g la plus grande qui leur eſt commune; il eſt viſible que z meſure au juſte[b] toutes les grandeurs c qu'on pourra prendre en b, & le reſte d; & pareillement tous[b] les reſtes d qu'on pourra prendre en c, & encore le reſte e; & auſſi tous les[b] reſtes e qu'on pourra prendre en d, & le nouveau reſte f; & enfin tous[b] les reſtes f qu'on pourra prendre en e, & le reſte ou la meſure commune la plus grande g des grandeurs b & c.

$b.$	104	(1	
$c.$	76	(2	
$d.$	28	(1	b. 16.
$e.$	20	(2	
$f.$	8	(2	
$g.$	4	(2	
$z.$	2		

VII PROBLEME.

45. *POur trouver le plus grand diviſeur commun, ou la meſure commune la plus grande, de trois grandeurs.*

Comme pour trouver la plus grande des trois b, c, d, on cherchera premiérement[b] la plus grande g des grandeurs b & c. Et enſuitte[b] la plus grande h des grandeurs d & g. Et la meſure h ſera la plus grande commune des grandeurs b, c, d. b. 42 & 43.

Car la plus grande, qui leur eſt commune, étant commune[c] aux deux b & c, eſt auſſi[d] un diviſeur de g; & par conſéquent un diviſeur commun des deux d & g. Comme donc h eſt le plus grand de ces deux d & g; il eſt auſſi le plus grand des trois b, c, d. Et ainſi on a preſcrit ce qu'il falloit faire. c. *ſuppoſition.* d. 44.

72. $b.$
48. $c.$ $g.$ 24.
64. $d.$ $h.$ 8.

Et on trouvera en ſuivant le même ordre le plus grand diviſeur commun, ou la meſure commune la plus grande, de quatre grandeurs; & pareillement de trois, ou de quatre divers nombres; ou d'autant de grandeurs, ou de nombres qu'on voudra.

I COROLLAIRE.

46. SI deux nombres z & y ſont l'un & l'autre diviſez par leur plus grand diviſeur commun g; les expoſans f & e ſont premiers entr'eux.

Car ſi on diviſe premiérement z & y par un diviſeur ſimple a, qui leur

roit commun ; & les deux exposans *x* & *v* par un simple *b*, qui leur soit pareillement commun ; & encore les nouveaux exposans *t* & *s* par un simple *c* ; & ainsi de suitte jusques aux derniers exposans, comme les deux *p* & *n*, qui soient premiers entr'eux, ou qui n'ayent plus aucun diviseur simple qui leur soit commun. Il est visible que ces diviseurs simples & successifs égaux ou inégaux sont [b] tous ceux qui peuvent être également distribuez de part & d'autre ; & que les deux nombres *z* & *y* ne peuvent avoir [c] aucun diviseur commun, qu'un des divers produits alternatifs des simples même *a*, *b*, *c*, *d*, ou l'un des simples 1, *a*, *b*, *c*, *d*. Mais *abcd* est le plus grand de tous ces divers produits alternatifs. Et *abcd* mesure *g* au [d] juste. Et par conséquent *g*, qui est le plus [e] grand des diviseurs communs des nombres *z* & *y*, & qui ne peut surpasser le produit *abcd*, est un même nombre que ce produit.

b. 29. c. 26. d. 44. e. *supposition*.

Comme donc en divisant chacun des nombres *z* & *y* par *abcd*, on a pour exposans [f] deux nombres *p* & *n*, qui sont premiers entr'eux ; si on divise chacun des mêmes *z* & *y* par *g*, on trouve [f] aussi les mêmes exposans *p* & *n*, ou *f* & *e*, qui sont premiers entr'eux.

f. 10.

f.	*z.*	*y.*	*e.*
2.	120.	180.	3.
p.	60.		*n.*
	g.		
	abcd.		

z.	*a.*	*x.*	*b.*	*t.*	*c.*	*r.*	*d.*	*p.*
120.	2.	60.	2.	30.	3.	10.	5.	2.
180.	2.	90.	2.	45.	3.	15.	5.	3.
y.	*a.*	*v.*	*b.*	*s.*	*c.*	*q.*	*d.*	*n.*

AUTRE DEMONSTRATION.

Ou pour démontrer encore par une autre voie la même proposition. Si *g* est le plus grand diviseur commun des deux nombres *fg* & *eg* ; les exposans *f* & *e* sont premiers entr'eux. Car si un nombre *d* pouvoit être un diviseur commun ; & que l'exposant du nombre *f* divisé par *d* fust *c*, & *b* celuy du nombre *e* divisé par *d* : le produit *cd* seroit égal [b] au nombre *f* ; & le produit *bd* à [b] l'autre nombre *e*. Et multipliant *f* & *cd* par *g*, & encore *e* & *bd* par *g* ; les produits *fg* & *cdg* ne seroient [c] qu'un même nombre. Et les produits *eg* & *bdg* pareillement qu'un [c] même. Mais *dg* qui est un diviseur entier & commun des deux nombres *bdg* & *cdg*, ou des deux *eg* & *fg* qui ne sont que les mêmes ; ne peut surpasser leur plus grand diviseur commun qui est *g*. Et *d* par conséquent diviseur commun des nombres *e* & *f*, ou *bd* & *cd*, ne peut surpasser 1. Et ainsi les deux exposans *e* & *f* sont premiers [d] entr'eux.

b. 18. 2. c. 20. 3. d. *définition*.

cdg.	*fg.*	130.	180.	*eg.*	*bdg.*
dg.	*g.*	60.	60.	*g.*	*dg.*
cd.	*f.*	2.	3.	*e.*	*bd.*
	d.	1.	1.	*d.*	
	c.	2.	3.	*b.*	

II COROLLAIRE.

47. ET on démontrera dans un ordre semblable, que si plusieurs nombres sont chacun divisez par leur plus grand diviseur commun ; les exposans sont premiers entr'eux.

VIII

VIII PROBLEME.

48. POur trouver le plus petit nombre, que deux z & y puiſſent l'un & l'autre diviſer ſans reſte.

Si z & y ſont premiers entr'eux; leur produit zy ſatisfait [b] au probleme. b. 19.

Mais ſi les nombres z & y ſont compoſez entr'eux; on cherchera [c] leur plus grand diviſeur commun g; & diviſant par g l'un des deux z & y, on multipliera le premier expoſant a par le nombre y, ou le ſecond expoſant b par l'autre nombre z. Et le produit ay ou bz réſoudra le problême. c. 42.

DEMONSTRATION.

Le nombre a étant l'expoſant de z diviſé par g, & b de l'autre y auſſi diviſé par g; le produit ag & le nombre z ſont [b] égaux, ou ne ſont qu'un même nombre. Et le produit bg & le nombre y pareillement [b] qu'un même. Et ſi on nomme p le moindre nombre, que chacun des deux z & y peut diviſer au juſte; ce nombre p eſt auſſi le moindre que chacun des deux ag & bg puiſſe diviſer au juſte. Et ſi p eſt diviſé par g; l'expoſant x peut [b] encore être diviſé ſans reſte par chacun des nombres a & b. Et ainſi le nombre x n'eſt pas moindre que le nombre ou le produit ab, qui eſt [c] le plus petit que chacun des deux a & b peut meſurer au juſte, puiſque ces deux a & b ſont premiers [d] entr'eux. Le nombre gx ou [e] p n'eſt donc pas moindre que le produit ay ou bz, ou [d] abg, du nombre y ou bg par a, ou de l'autre z ou ag par b. Mais ag ou z, & bg ou y, meſurent chacun au juſte le nombre abg. Et ainſi le le nombre abg ou ay ou bz, qui ne [f] peut ſurpaſſer le nombre gx ou p, convient parfaitement avec luy. Et il eſt au juſte le plus petit des nombres que les deux z & y puiſſent chacun diviſer ſans reſte. b. 18. 2. b. 9. c. 19. d. 46. e. 18. 2. f *démonſtration.*

		$ag.$	$z.$	72.	60.	$y.$	$bg.$	
			$g.$	12.	12.	$g.$		
			$a.$	6.	5.	$b.$		
$abg.$	$gx.$	$p.$	$ay.$	360.	360.	$bz.$	$p.$ $gx.$	$abg.$
		$g.$		12.	12.		$g.$	
	$ab.$	$x.$		30.	30.		$x.$ $ab.$	

I COROLLAIRE ET PROBLEME IX.

49. POur trouver le plus petit nombre que les trois z, y, x, puiſſent chacun diviſer ſans reſte.

On cherchera [b] le moindre v que les deux z & y puiſſent déja diviſer ſans reſte. Et enſuitte [b] le moindre t que les deux x & v puiſſent auſſi chacun diviſer ſans reſte. Et on ſuivroit un ordre ſemblable, ſi l'on en propoſoit pluſieurs. b. 48

PREMIER EXEMPLE.

Pour trouver le plus petit nombre, que les deux 7 & 11 puiſſent diviſer ſans reſte. Je prends leur produit 77, parce qu'ils ſont premiers entr'eux. 7 & 11. *Produit* 77

Et pour trouver le moindre que 72 & 60 puiſſent diviſer ſans reſte. Je prens leur plus grand diviſeur commun qui eſt 12, & je diviſe 72 par 12; & enſuitte je multiplie par l'expoſant 6 l'autre nombre 60. Ou, ce qui revient au même, je diviſe 60 par 12; & par l'expoſant 5 je multiplie le nombre 72. Et de part & d'autre le produit 360 réſout la queſtion.

Multiplier 72. 60. 12.
par 5. 6.
Produit 360. 360 *Produit*

SECOND EXEMPLE.

Pour trouver le plus petit nombre que 72 & 60 & 25 puiſſent diviſer au juſte. Je cherche le moindre 360, que les deux 72 & 60 puiſſent diviſer ſans reſte. Et enſuitte le plus petit 1800, que 360 & 25 puiſſent diviſer au juſte, & qui ſatisfait au problême.

Multiplier 360. 25. 5.
par 5. 72.
Produit 1800. 1800 *Produit*

II COROLLAIRE.

50. *Les nombres ſimples vont juſqu'à l'infini.*

Car ſoit donnée telle multitude qu'on voudra de ces nombres ſimples, comme les cinq *a*, *b*, *c*, *d*, *e*. Si on cherche[b] le moindre nombre ζ que chacun d'eux peut diviſer ſans reſte, & qu'on luy ajoûte 1; nul[c] de tous les divers nombres ſimples qu'on aura propoſé ne pourra diviſer au juſte le nouveau nombre $\zeta+1$: puiſque chacun d'eux diviſe la partie ζ au juſte, & ne peut diviſer[d] au juſte l'autre partie 1 qui reſte. D'où il eſt[e] évident que chacun des divers ſimples, qui diviſeront ſans reſte le nombre $\zeta+1$, ſera différent de chacun des ſimples qu'on aura propoſé. Et on en pourra toûjours trouver de la même ſorte tant d'autres qu'on voudra juſqu'à l'infini.

b. 49. c. 15. d. 6. 1. e. 11.

a. b. c. d. e. ζ. $\zeta+1$.
2. 3. 5. 7. 11. 2310. 2311.

II THEOREME.

51. TOus les nombres entiers peuvent être chacun meſurez au juſte par 1. Puiſque l'unité ſe meſure toûjours elle-même, & qu'elle meſure auſſi la différence 1, qui eſt entre 1 & 2; & par conſéquent[c] le nombre même 2; & enſuitte 3 par[c] la même raiſon; & pareillement[c] 4; & chacun des naturels ou conſécutifs 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, & autres juſques à l'infini.

c. 14.

$1+1$ *ou* $2+1$ *ou* $3+1$ *ou* 4 &c. *Révolution.*

52. Et parmi ces mêmes nombres naturels, il y en a toûjours de deux un ſeul qui eſt un nombre impair. Car 2 ne[b] peut diviſer la différence 1 qui eſt entre 2 & 3, ni 3 par[c] conſéquent. Mais il peut diviſer les différences enſemble 1 & 1, qui ſont entre 2 & 3, & entre 3 & 4; ou la ſeule différence 2, qui eſt entre 2 & 4. Et par conſéquent 2 qui ſuit l'unité, meſure[d] ou diviſe 4. Et comme la révolution des différences 1 & 1 revient toûjours de 2 en 2; il y aura toûjours de deux en deux nombres, un impair & un autre pair.

b. 6. 1. c. 15. d. 14.

Révolution 1−+1 *ou* 2, −+1−+1 *ou* 4, −+1−+1 *ou* 6, &c.
Nombres naturels 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16.
Nombres impairs 1. 3. 5. 7. 9. 11. 13. 15.
Nombres pairs 2. 4. 6. 8. 10. 12. 14. 16.

53. Et parmi tous les nombres impairs, il y en a toûjours un ſeul de trois en trois, que 3 meſure au juſte, en commençant par 3.

Car 3 ne peut diviſer au juſte [b] la différence 2, qui eſt entre le premier impair 1 & le ſecond 3; ni la différence 2, qui eſt entre le ſecond impair 3 & le troiſiéme 5; ni les deux enſemble 2 & 2, qui ſont entre 3 & 5, & entre 5 & 7. Et par conſéquent 3, qui ſe diviſe ou meſure au juſte, ne peut diviſer ou meſurer au juſte ni 5 ni 7. Mais comme il peut meſurer au juſte les différences enſemble 2 & 2 & 2, qui ſont entre 3 & 5, & entre 5 & 7, & entre 7 & 9; ou la ſeule différence 6 qui eſt entre 3 & 9: il meſure [c] auſſi 9. Et parceque la même révolution des différences 2, 2, 2, revient toûjours de trois en trois; il y aura toûjours de trois en trois parmi les nombres impairs, en commençant par 3, deux impairs que le ſimple 3 ne pourra diviſer, & un ſeul dont il ſera diviſeur. b. 6. 1. c. 14.

Nombres impairs 3. 5. 7. 9. 11. 13. 15. 17. 19. 21. 23. 25. 27.
diviſibles par 3. 3. 9. 15. 21. 27.
Révolution 2−+2−+2. 2−+2−+2. 2−+2−+2. 2−+2−+2.

III. THEOREME.

54. SI on ôte de tous les nombres impairs tous ceux qui ſont diviſibles par 3; il y aura préciſément de dix en dix parmi tous ceux qui reſtent, deux ſeuls diviſibles par 5.

Car 5 ne peut diviſer la différence 2, qui eſt entre 5 & 7; ni les deux enſemble 2 & 4, qui ſont entre 5 & 7, & entre 7 & 11; ni les trois enſemble 2, 4, 2, qui ſont entre 5 & 7, & entre 7 & 11, & entre 11 & 13; ni les quatre enſemble 2, 4, 2, 4; ni les cinq enſemble 2, 4, 2, 4, 2; ni les ſix enſemble 2, 4, 2, 4, 2, 4; ni [b] par conſéquent aucun des 6 nombres 7, 11, 13, 17, 19, 23. Mais comme il peut meſurer les ſept enſemble 2, 4, 2, 4, 2, 4, 2, ou la ſeule 20, qui eſt entre 5 & 25; il peut [c] auſſi meſurer 25. Et parce que 5 ne peut encore meſurer la différence 4, qui eſt entre 25 & 29; ni les deux enſemble 4 & 2, qui ſont entre 25 & 29, & entre 29 & 31; il ne peut auſſi meſurer ni 29 ni 31. Mais comme il peut meſurer les trois enſemble 4, 2, 4, qui ſont entre 25 & 29, & entre 29 & 31, & entre 31 & 35; il peut encore [c] meſurer 35. Et comme la même révolution de ſept différences 2, 4, 2, 4, 2, 4, 2, & des trois 4, 2, 4, ou la révolution des dix 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, revient toûjours de dix en dix; il y aura toûjours de dix en dix de ces nombres qu'on ſuppoſe, huit que 5 ne pourra diviſer ſans reſte, & deux dont il ſera diviſeur; c'eſt à dire alternativement un de ſept, & enſuitte un de trois; & un autre de ſept, & apres un de trois. Et ainſi du reſte juſques à l'infini. b. 15. c. 14.

Révolution 2−+4−+2−+4−+2−+4−+2. *Et* 4−+2−+4.

IV THEOREME.

55. ET ſi on ôte encore tous ces nombres diviſibles par 5 ; il y en aura huit au juſte parmi tous ceux du reſte, de cinquante-ſix en cinquante-ſix, diviſibles par 7, en commençant par 7.

Car 7 pourra ſeulement diviſer les 12 différences enſemble 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 2 ; & enſuitte les 7 enſemble 4, 6, 2, 6, 4, 2, 4 ; & encore enſuitte les quatre enſemble 2, 4, 6, 2. Et les 7 autres enſemble 6, 4, 2, 4, 2, 4, 6. Et de nouveau les 4 enſemble 2, 6, 4, 2. Et aprés cela les ſept autres enſemble 4, 2, 4, 6, 2, 6, 4. Et encore tous les 12 enſemble 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 2, 4. Et enfin les trois enſemble 6, 2, 6. De ſorte que parmi les 56 nombres, entre leſquels on trouve ſucceſſivement toutes ces différences, il y aura ſeulement 8 nombres, que 7 pourra diviſer ſans reſte. Et comme la même révolution des 56 différences revient toûjours de 56 en 56 nombres ; il y en aura auſſi toûjours 48 au juſte de 56 en 56, que 7 ne pourra pas diviſer ſans reſte, & 8 dont il ſera diviſeur ; c'eſt à dire, un de douze, & un de ſept, & un de quatre, & enſuitte encore un de ſept, & un de quatre, & de nouveau un de ſept, & un de douze, & un de trois.

Révolution.

4+2+4+2+4+6+2+6+4+2+4+2. (4+6+2+6+4+2+4.
(2+4+6+2.(6+4+2+4+2+4+6.(2+6+4+2.(4+2+4+6+2+6+4.
(2+4+2+4+6+2+6+4+2+4+2+4.(6+2+6.

V THEOREME.

56. ET ſi on ôte auſſi tous ces nombres diviſibles par 7 ; il y aura 38 des nombres au juſte parmi tous ceux du reſte, de 432 en 432, diviſibles par 11, en commençant par 11.

Car on trovera toûjours une même révolution des 48 différences qu'on expoſe ici. Et une autre révolution auſſi toûjours la même de toutes ces 48 différences diſpoſées ſelon le même ordre, & réïtérées juſques à 9 fois. Et chacune de ces grandes & nouvelles révolutions, qui comprendra toûjours 432 différences, fournira au juſte 38 de leurs divers aſſemblages, dont chacun ſera diviſible par 11. De ſorte que de 432 en 432 des nombres ſuppoſez, il y en aura toûjours 394 au juſte, que le nombre ſimple 11 ne pourra pas diviſer ſans reſte, & 38 dont il ſera diviſeur ; c'eſt à dire un premiérement de 26, & enſuitte un de 5, & encore un de 10, & un de 5, & un de 11, & pareillement un, & de 15, & de 4, & de 16, & de 10, & de 5, & de 9, & de 15, & de 16, & de 5, & de 15, & de 10, & de 5, & de 15, & de 11, & de 14, & de 20, & de 11, & de 5, & de 9, & de 5, & de 11, & de 20, & de 14, & de 11, & de 15, & de 5, & de 10, & de 23, & de 7, & de 10, & de 5, & de 17, & de 12. Et comme cette révolution reviendra toûjours la même ; il y aura toûjours au juſte de 432 en 432 des nombres que l'on a ſuppoſé, 38 diviſibles par 11, en commençant par 11. Et on pourra éxaminer de la même ſorte les révo-

lutions pour les autres nombres diviſibles par 13 ; & enſuitte par 17 ; & par 19 ; & par 23 ; & par 29 ; & par les autres qui les ſuivent, & qui ſont premiers entr'eux. Et s'il y avoit quelque ſuitte uniforme, que l'on puſt obſerver dans ces révolutions ; on en pourroit tirer ſans doute un grand jour, pour découvrir d'abord ſi un nombre propoſé eſt compoſé ou ſimple.

Révolution des 48 différences priſes 9 fois.

2. 4. 2. 4. 6. 2. 6. 4. 2. 4. 6. 6. 2. 6. 4. 2. 6. 4. 6. 8. 4. 2. 4. 2.
4. 8. 6. 4. 6. 2. 4. 6. 2. 6. 6. 4. 2. 4. 6. 2. 6. 4. 2. 4. 2. 10. 2. 10.

Révolution des nombres des différences qui fourniſſent chacun 1.

26. 5. 10. 5. 11. 15. 4. 16. 10. 5. 9. 15. 16. 5. 15. 10. 5. 15. 11. 14.
20. 11. 5. 9. 5. 11. 20. 14. 11. 15. 5. 10. 23. 7. 10. 5. 17. 12.

I COROLLAIRE.

57. L'Aſſemblage z de pluſieurs nombres pairs a, b, c, d, eſt un nombre pair. Car ſi 2 diviſe chaque nombre, il diviſe [b] au juſte la ſomme de deux, & enſuitte [b] la ſomme de trois, & celle de quatre [b] par la même raiſon, & ainſi du reſte. [b. 14.]

$$\begin{cases} a+b+c+d. & z. \\ 1+4+8+6. & 20. \end{cases}$$

II COROLLAIRE.

58. TOute multitude paire de pluſieurs nombres impairs a, b, c, d, donne un nombre pair z. Car ayant ôté l'unité de chacun, tous les reſtes y, x, v, t, ſont [b] pairs. De ſorte que raſſemblant tous ces reſtes & la ſomme paire f de toutes les unitez retranchées, l'aſſemblage entier z ou $r+f$ eſt un [c] nombre pair. [b. 52.] [c. 14.]

$$\begin{cases} 3. & a. \\ 7. & b. \\ 5. & c. \\ 11. & d. \\ \hline 26. & z. \end{cases} \qquad \begin{cases} a-1. & y & 2 \\ b-1. & x & 6 \\ c-1. & v & 4 \\ d-1. & t & 10 \\ \hline z-4. & r & 22 \end{cases} \quad f$$

III COROLLAIRE.

59. ET toute multitude impaire de pluſieurs nombres impairs a, b, c, eſt un nombre impair z. Car ôtant l'un des nombres, comme c, l'aſſemblage $a+b$ de tous ceux qui reſtent eſt un nombre [b] pair ; auquel ayant ajoûté l'impair c, qu'on avoit mis à part, tout l'aſſemblage z eſt un nombre [c] impair. [b. 58.] [c. 15.]

$$\begin{cases} 3. & a. \\ 7. & b. \\ 5. & c. \\ \hline 15. & z. \end{cases} \qquad \begin{cases} a+b. & 10. \\ c. & 5. \\ \hline z. & 15. \end{cases}$$

IV COROLLAIRE.

60. SI d'un nombre pair on ôte un nombre pair ; le reſte eſt un nombre pair. Parce que ſi 2 diviſe un nombre a ſans reſte, & l'une de ſes parties b ; il diviſe auſſi l'autre [b] partie $a-b$ au juſte. [b. 16.]

$$a-b \qquad 10-4.$$

V COROLLAIRE.

61. ET ſi on ôte un nombre impair b d'un nombre pair a ; le reſte $a-b$ eſt un nombre pair. Car ôtant 1 du nombre impair b, le reſte

b. 52. $b-1$ est [b] pair. Et ce reste étant retranché du nombre pair a, donne un nouveau reste $a-b+1$ qui [c] est
c. 60. pair. Et si on luy ôte 1, le reste $a-b$ est [b] impair.

$a-b$. 10—3.
$a-b+1$. 10—2.

VI COROLLAIRE.

62. ET si on ôte un pair b d'un impair a; le reste $a-b$ est impair. Car
b. 52. ôtant 1 du nombre impair a, le reste $a-1$ sera [b] pair. Et si on luy
c. 60. ôte b; le nouveau reste $a-1-b$ sera [c] encore pair. Et ajoûtant 1 à ce nouveau reste, on trouvera le [b] nombre impair $a-b$.

$a-b$. 7 — 2.
$a-1-b$. 7—1—2.

VII COROLLAIRE.

63. ET si on ôte un impair b d'un autre impair a; le reste $a-b$ est [b] pair.
b. 52. Car ôtant 1 de la partie impaire b, son reste $b-1$ est [b] pair. Et si on
c. 62. ôte ce reste $b-1$ du nombre impair a; le reste $a-b+1$ est [c] impair. Et si on luy ôte 1; le reste $a-b$ sera [b] pair.

$a-b$. 1—2.
$a-b+1$. 7—2.

VIII COROLLAIRE.

64. TOut produit ab d'un impair b par un pair a est [b] pair. Puis qu'en
b. 58. prenant le produit de ces nombres, on ne fait autre chose que prendre une multitude paire, exprimée par a, du nombre impair b.

a. 6
b. 3
ab. 18.

IX COROLLAIRE.

65. ET tout produit ab d'un impair b par un impair a est [b] impair. Puis
b. 59. qu'en prenant le produit de ces nombres, on ne fait autre chose que prendre une multitude impaire, exprimée par a, du nombre impair b.

a. 7.
b. 3.
ab. 21.

X COROLLAIRE.

66. SI un nombre impair b divise au juste un nombre pair $2a$; il di-
b. 22. vise [b] aussi sa moitié a sans reste.

18. $2a$. a. 9.
3. b. b. 3.

XI COROLLAIRE.

67. ET si un nombre impair b est premier à l'égard d'un nombre a; il
b. 36. l'est encore à l'égard [b] du double $2a$ de ce même nombre a.

a. b. $2a$.
7. 5. 14.

XII COROLLAIRE.

68. LEs puissances successives du nombre simple 2 n'ont aucun diviseur
b. 27. que l'une de ses [b] puissances.

2. 4. 8. 16. 32. 64.

DEFINITION.

Quoique les nombres divisibles par 4 soient pairement pairs; s'ils sont encore divisibles par un nombre impair, on dit qu'ils sont *pairement impairs*.


J. Ldh. de Dalpach
Lagrange?
Lagrange

DE LA RESOLUTION DES EQUATIONS ALGEBRIQUES A L'EMERGENCE DU CONCEPT DE GROUPE

Martine Bühler

En 1770 et 1771, Lagrange publie dans les *Mémoires de L'Académie Royale des Sciences et des Belles-Lettres* de Berlin un important mémoire intitulé *Réflexions sur la résolution algébrique des équations*. Il s'y interroge sur l'échec des mathématiciens dans la résolution des équations de degré supérieur ou égal à 5. La voie semblait pourtant tracée à partir des remarquables succès de Cardan (*Ars Magna* 1545) et Ferrari pour les degrés 3 et 4, qui avaient jusque-là résisté aux efforts. Lagrange ne cherche pas de nouvelles méthodes de résolution : il s'interroge sur les raisons pour lesquelles les méthodes efficaces pour les degrés trois et quatre sont inopérantes pour des degrés plus élevés. Cet article a pour objectif d'étudier en détail de larges extraits du mémoire de Lagrange. Il doit beaucoup au travail remarquable effectué par J.P. Friedelmeyer et je conseille vivement aux lectrices et aux lecteurs que le sujet intéresse de lire la brochure de l'A.P.M.E.P. Fragments d'histoire des mathématiques III "*Emergence du concept de groupe*", à laquelle j'ai d'ailleurs emprunté le titre de l'atelier. Elles ou ils y trouveront un exposé éclairant et complet de l'histoire de la résolution des équations. Mon objectif ici, plus modeste, est de faire comprendre les idées de Lagrange, en espérant que la lectrice ou le lecteur y trouvera le même plaisir que moi.

Comme Lagrange, nous considérerons que nous savons résoudre une équation polynomiale si des changements de variables ramènent cette résolution à celles d'équations "binômes" du type $Y^n = \alpha$ ou à des équations de degré inférieur déjà "résolues", sans nous poser de questions sur l'extraction algébrique d'une racine $n^{ième}$ d'un nombre α qui peut être complexe. C'est bien un tel changement de variable qui permet de résoudre la toute simple équation de degré 2 :

$$x^2 + bx + c = 0$$

$$\left(x + \frac{b}{2}\right)^2 = \frac{b^2}{4} - c$$

En posant $X = x + \frac{b}{2}$, on se ramène à une équation binôme.

L'introduction du texte présente les progrès de l'algèbre au dix-huitième siècle, mais aussi ses limites.

La théorie des équations est de toutes les parties de l'Analyse celle qu'on eût cru devoir acquérir les plus grands degrés de perfection et par son importance et par la rapidité des progrès que les premiers inventeurs y ont fait ; mais quoique les Géomètres qui sont venus depuis n'aient cessé de s'y appliquer, il s'en faut de beaucoup que leurs efforts aient eu le succès qu'on pouvait désirer. On a à la vérité épuisé presque tout ce qui concerne la nature des équations, leur transformation, les conditions nécessaires pour que deux ou plusieurs racines deviennent égales, ou aient entre elles une relation donnée, et la manière de trouver ces racines, la forme des racines imaginaires, et la méthode de trouver la valeur de celles qui, quoique réelles, se présentent sous une forme imaginaire, etc.

...

A l'égard de la résolution des équations littérales, on n'est guère plus avancé qu'on ne l'était du temps de Cardan, qui le premier a publié celle des équations du troisième et du quatrième degré. Les premiers succès des Analystes italiens dans cette matière paraissent avoir été le terme des découvertes qu'on y pouvait faire ; du moins est-il certain que toutes les tentatives qu'on a faites jusqu'à présent pour reculer les limites de cette partie de l'Algèbre n'ont encore servi qu'à trouver de nouvelles méthodes pour les équations du troisième et du quatrième degré, dont aucune ne paraît applicable, en général, aux équations d'un degré plus élevé.

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 à 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.

L'idée fondamentale de Lagrange est que, pour progresser désormais, il ne faut pas chercher des méthodes nouvelles mais commencer par s'interroger sur les méthodes efficaces pour les équations du troisième et du quatrième degré. POURQUOI les changements de variables utilisés dans la résolution de ces équations permettent-ils de résoudre, d'abaisser le degré des équations proposées ? Lagrange effectue ce travail pour toutes les méthodes connues à l'époque ; nous nous contenterons d'examiner en détail la méthode "de Cardan" pour le troisième degré et celle "de Ferrari" pour le quatrième degré, afin de comprendre quelle est la raison profonde de l'efficacité de ces méthodes.

1. Comme la résolution des équations du second degré est très facile et n'est d'ailleurs remarquable que par son extrême simplicité, j'entrerai d'abord en matière par les équations du troisième degré, lesquelles demandent pour être résolues des artifices particuliers qui ne se présentent pas naturellement.

Soit donc l'équation générale du troisième degré

$$x^3 + mx^2 + nx + p = 0\,,$$

et comme on sait qu'on peut toujours faire disparaître le second terme de toute équation en augmentant ses racines du coefficient du second terme divisé par l'exposant du premier, on pourra supposer d'abord, pour plus de simplicité, $\mathrm{m}=0$, *ce qui réduira la proposée à la forme*

$$x^3+nx+p=0.$$

C'est dans cet état que les équations du troisième degré ont été d'abord traitées par Scipio Ferreo et par Tartalea, à qui l'on doit leur résolution ; mais on ignore le chemin qui les y a conduits. La méthode la plus naturelle pour y parvenir me paraît être celle que Hudde a imaginée, et qui consiste à représenter la racine par la somme de deux indéterminées qui permettent de partager l'équation en deux parties propres à faire en sorte que les indéterminées ne dépendent que d'une équation résoluble à la manière de celles du second degré.

Suivant cette méthode on fera donc $\mathrm{x}=\mathrm{y}+\mathrm{z}$, *ce qui étant substitué dans la proposée la réduira à celle-ci*

$$y^3+3y^2z+z^3+n(y+z)+p=0\ ,$$

qu'on peut mettre sous cette forme plus simple

$$y^3+z^3+(y+z)(3yz+n)+p=0.$$

Qu'on fasse maintenant ces deux équations séparées

$$y^3+z^3+p=0$$
$$3yz+n=0$$

on aura

$$z=-\frac{n}{3y}$$

et, substituant dans la première,

$$y^3-\frac{n^3}{27y^3}+p=0,$$

c'est-à-dire

$$y^6+py^3-\frac{n^3}{27}=0.$$

Cette équation est à la vérité du sixième degré, mais comme elle ne renferme que deux différentes puissances de l'inconnue, dont l'une a un exposant double de celui de l'autre, il est clair qu'elle peut se résoudre comme celles du second degré. En effet, on aura d'abord

$$y^3=-\frac{p}{2}\pm\sqrt{\frac{p^2}{4}+\frac{n^3}{27}}$$

et de là

$$y=\sqrt[3]{-\frac{p}{2}\pm\sqrt{\frac{p^2}{4}+\frac{n^3}{27}}}\ .$$

Ainsi l'on connaîtra y et z, et de là, on aura

$$x=y+z=y-\frac{n}{3y}$$

2. Il se présente différentes remarques à faire sur cette solution. D'abord il est clair que la quantité y doit avoir six valeurs, puisqu'elle dépend d'une équation du sixième degré ; de sorte que la quantité x aura aussi six valeurs ; mais comme la quantité x est la racine d'une équation du troisième degré, on sait qu'elle ne peut avoir que trois valeurs différentes ; donc il faudra que les six valeurs dont il s'agit se réduisent à trois, dont chacune soit double. C'est aussi de quoi on peut se convaincre par le calcul, en éliminant y des deux équations

$$y^6 + py^3 - \frac{n^3}{27} = 0,\ x = y - \frac{n}{3y}$$

Le calcul aboutit alors à. $\left(x^3 + nx + p\right)^2 = 0$

C'est pourquoi x prend "*six valeurs qui se réduisent à trois*".

On peut également voir comment les six valeurs de x se groupent deux par deux en examinant de plus près la façon dont on les obtient. y étant une racine de $y^6 + py^3 - \frac{n^3}{27} = 0$ (1), on obtient une solution x de l'équation initiale (E) par : $x = y - \frac{n}{3y}$. Or, si y est solution de (1), $z = -\frac{n}{3y}$ en est une autre car $\left(-\frac{n}{3y}\right)^6 + p\left(-\frac{n}{3y}\right)^3 - \frac{n^3}{27} = \left(-\frac{n}{3y}\right)^3 \times \frac{1}{y^3}\left[\left(-\frac{n}{3}\right)^3 + py^3 + y^6\right] = 0$. On obtient alors comme solution de (E) $z - \frac{n}{3z} = -\frac{n}{3y} - \frac{n}{3\left(-\frac{n}{3y}\right)} = y - \frac{n}{3y}$, c'est-à-dire la même solution que précédemment. Mais Lagrange ne s'arrête pas là.

5. L'équation du sixième degré

$$y^6 + py^3 - \frac{n^3}{27} = 0$$

s'appelle la réduite du troisième degré, parce que c'est à sa résolution que se réduit celle de la proposée $x^3 + nx + p = 0$.

Or nous avons déjà vu plus haut comment les racines de cette dernière équation dépendent des racines de celle-là ; voyons réciproquement comment les racines de la réduite dépendent de celles de la proposée.

Soit $y = \sqrt[3]{-\frac{p}{2} + \sqrt{\frac{p^2}{4} + \frac{n^3}{27}}}$

Les autres racines de la réduite sont, avec les notations de Lagrange, $y' = \alpha y, y'' = \beta y, z = -\frac{n}{3y}, z' = -\frac{n}{3y'}, z'' = -\frac{n}{3y''}$ où α et β sont les racines cubiques de l'unité différentes de 1.

Les trois racines de la proposée sont alors : $a = y - \frac{n}{3y}, b = y' - \frac{n}{3y'} = \alpha y - \frac{n}{3\alpha y}, c = y'' - \frac{n}{3y''} = \beta y - \frac{n}{3\beta y}$.

Le calcul de $a-b$ et $a-c$ et l'élimination de $\frac{n}{3y}$ entre les expressions obtenues donne : $y = \frac{a + \beta b + \alpha c}{3}$.

Lagrange échange alors les rôles de α et β (il n'a jamais précisé lequel était $e^{2i\frac{\pi}{3}}$) et obtient :

$$y = \frac{a + \alpha b + \beta c}{3}.$$

6. On voit d'abord par cette expression de y pourquoi la réduite est nécessairement du sixième degré ; car comme cette réduite ne dépend pas immédiatement des racines a, b, c de la proposée, mais seulement des coefficients m, n, p, où les trois racines entrent également, il est clair que dans l'expression de y on doit pouvoir échanger à volonté les quantités a, b, c entre elles ; par conséquent la quantité y devra avoir autant de valeurs différentes que l'on pourra en former par toutes les permutations possibles dont les trois racines a, b, c sont susceptibles ; or on sait par la théorie des combinaisons que le nombre des permutations, c'est-à-dire des arrangements différents de trois choses, est 3.2.1 ; donc la réduite en y doit être aussi du degré 3.2.1., c'est-à-dire du sixième.

Il y a plus : la même expression de y montre aussi pourquoi la réduite est résoluble à la manière des équations du second degré ; car il est clair que cela vient de ce que cette équation ne renferme que les puissances y^3 et y^6, c'est-à-dire des puissances dont les exposants sont multiples de 3 ; en sorte que, si r est une des valeurs de y, il faut que αr et βr en soient aussi à cause de $\alpha^3 = 1$ et $\beta^3 = 1$; or c'est ce qui a lieu dans l'expression de y trouvée ci-dessus. Pour le faire voir plus aisément nous remarquerons que $\beta = \alpha^2$, car, puisqu'on a $\alpha\beta = 1$ et $\alpha^3 - 1 = 0$, on aura aussi $\alpha\beta = \alpha^3$, et de là $\beta = \alpha^2$; de sorte que l'expression de y pourra se mettre sous cette forme

$$y = \frac{a + \alpha b + \alpha^2 c}{3}.$$

d'où, en faisant toutes les permutations possibles des quantités a, b, c, on tire les six valeurs suivantes

$$y = \frac{a + \alpha b + \alpha^2 c}{3}$$

$$y = \frac{a + \alpha c + \alpha^2 b}{3}$$

$$y = \frac{b + \alpha a + \alpha^2 c}{3}$$

$$y = \frac{b + \alpha c + \alpha^2 a}{3}$$

$$y = \frac{c + \alpha b + \alpha^2 a}{3}$$

$$y = \frac{c + \alpha a + \alpha^2 b}{3},$$

qui seront les six racines de la réduite. Maintenant si l'on multiplie la première par α, *et ensuite par* β *ou par* α^2, *on aura, à cause de* $\alpha^3 = 1$, *ces deux-ci* $y = \frac{c + \alpha a + \alpha^2 b}{3}$ *et* $y = \frac{b + \alpha c + \alpha^2 a}{3}$, *qui sont la sixième et la quatrième ; et si l'on multiplie de même la seconde par* α *et par* α^2, *on aura* $y = \frac{b + \alpha a + \alpha^2 c}{3}$ *et* $y = \frac{c + \alpha b + \alpha^2 a}{3}$, *qui sont la troisième et la cinquième. Il en sera de même si l'on multiplie la troisième et la quatrième, ou la cinquième et la sixième par* α *et par* α^2, *car on aura par là également toutes les autres.*

Ainsi donc on comprend pourquoi le changement de variable proposée mène à une réduite qu'on sait résoudre ; en fait, on a augmenté le degré de l'équation, passé de 3 à 6, mais seules les puissances 3 et 6 de y intervenant, on peut résoudre cette réduite à la manière d'une équation du second degré. En analysant les autres méthodes connues pour résoudre les équations du troisième degré, Lagrange s'aperçoit qu'elles reviennent toutes à prendre comme nouvelle inconnue, soit $y = a + \alpha b + \alpha^2 c$,

soit $y^3 = \left(a + \alpha b + \alpha^2 c\right)^3$ (ou des quantités proportionnelles à celles-ci). Il conclut (avec un changement de notations: les trois racines *a, b, c* de la proposée deviennent *x', x'', x'''*) :

20. Telles sont les principales méthodes qu'on a trouvées jusqu'à présent pour résoudre les équations du troisième degré. Par l'analyse que nous venons d'en faire il est visible que ces méthodes reviennent toutes au même pour le fond, puisqu'elles consistent à trouver des réduites dont les racines soient représentées en général par $x' + \alpha x'' + \alpha^2 x'''$, *ou par* $\left(x' + \alpha x'' + \alpha^2 x'''\right)^3$, *ou bien, ce qui est la même chose, par des quantités proportionnelles à celles-ci. Dans le cas où la racine de la réduite est* $x' + \alpha x'' + \alpha^2 x'''$, *cette réduite est du sixième degré, résoluble à la manière du second parce qu'elle ne renferme que la troisième et la sixième puissance de l'inconnue. Nous en avons donné la raison dans le numéro 6. Dans l'autre cas, où la racine de la réduite est* $\left(x' + \alpha x'' + \alpha^2 x'''\right)^3$, *cette réduite ne peut être que du second degré, ce qui suit nécessairement du cas précédent, et que nous avons aussi démontré d'une manière directe.*

Il faut bien comprendre l'intérêt de cette remarque de Lagrange. Faire un changement de variable, c'est poser $y = f(x', x'', x''')$ où f est une fonction rationnelle des trois racines, à coefficients s'exprimant rationnellement à l'aide des coefficients n et p de l'équation de départ. Lorsqu'on effectue les six permutations possibles des trois racines *x', x'', x'''*, *y* prend a priori six valeurs $y_1 = y ; y_2 ; y_3 ; y_4 ; y_5 ; y_6$. Ces six valeurs sont solutions d'une équation du sixième degré dont on sait calculer les coefficients à l'aide de n et p car ces coefficients sont au signe près les fonctions symétriques élémentaires de $y_1 ; y_2 ; y_3 ; y_4 ; y_5 ; y_6$, qui sont invariantes par toutes les permutations de *x', x'', x'''* (étant donnée la génération des y_i) ; ces coefficients, fonctions symétriques de *x', x'', x'''*, s'expriment donc rationnellement à l'aide des fonctions symétriques élémentaires de *x', x'', x'''* donc de *n* et *p*. Or que se passe-t-il si on choisit $y = \left(x' + \alpha x'' + \alpha^2 x'''\right)^3$? Cette fois, *y*

ne prend que deux valeurs y_1, y_2 lorsqu'on effectue les six permutations possibles des trois racines x', x'', x''', car les six valeurs de $x'+\alpha x''+\alpha^2 x'''$ sont du type $z, \alpha z, \alpha^2 z, z', \alpha z', \alpha^2 z'$ et $\left(\alpha^2\right)^3 = \alpha^3 = 1$. Donc $y_1 + y_2$ et $y_1 y_2$ sont des fonctions symétriques des racines et s'expriment à l'aide de n et p. Donc y est solution d'une équation du second degré puis on obtient la valeur de $x'+\alpha x''+\alpha^2 x'''$ en résolvant une équation binôme du type $Y^3 = y$. La méthode permet de trouver ensuite x', x'', x''' car ces trois nombres s'expriment à l'aide de Y. Nous reviendrons sur ce point plus loin avec Lagrange.

La section seconde du mémoire est consacrée à l'examen des méthodes de résolution des équations du quatrième degré.

26. On sait que Louis Ferrari, contemporain et même disciple de Cardan, est le premier qui ait trouvé une règle générale pour la résolution des équations du quatrième degré. Sa méthode consiste à partager l'équation en deux membres, et à ajouter à l'un et à l'autre une même quantité telle, qu'on puisse extraire séparément la racine carrée des deux membres de l'équation, en sorte qu'elle soit par là abaissée au second degré.

...

Je suppose d'abord avec Ferrari que l'équation du quatrième degré qu'il s'agit de résoudre soit privée de son second terme, ce qu'on sait d'ailleurs être toujours possible, en sorte que cette équation soit représentée ainsi

$$x^4 + nx^2 + px + q = 0.$$

Qu'on fasse passer dans le second membre tous les termes excepté le premier, et qu'ensuite on ajoute à l'un et l'autre membre la quantité $2yx^2 + y^2$, *y étant une indéterminée, on aura*

$$x^4 + 2yx^2 + y^2 = (2y - n)x^2 - px + y^2 - q,$$

équation où le premier membre est évidemment le carré de $x^2 + y$, *de sorte qu'il ne s'agira plus que de rendre aussi carré le second ; or pour cela il faut, comme on sait, que le carré de la moitié du coefficient du second terme -px soit égal au produit des coefficients des deux autres, ce qui donne cette condition*

$$\frac{p^2}{4} = (2y - n)\left(y^2 - q\right),$$

laquelle produit l'équation cubique

$$y^3 - \frac{n}{2}y^2 - qy + \frac{4nq - p^2}{8} = 0.$$

Supposant donc la résolution de cette équation en sorte qu'on connaisse une valeur de y, le second membre de la proposée deviendra

$$(2y - n)\left[x - \frac{p}{2(2y - n)}\right]^2 ;$$

donc, tirant la racine carrée des deux membres, on aura

$$x^2+y=\left[x-\frac{p}{2(2y-n)}\right]\sqrt{2y-n}\,,$$

équation où l'inconnue x ne monte qu'au second degré, et qui n'a par conséquent plus de difficulté.

De la même manière que pour l'équation du troisième degré, Lagrange veut éclaircir les raisons qui rendent le changement de variable efficace. Pourquoi y est-elle solution d'une équation du troisième degré ? Pour cela, nous allons exprimer y à l'aide des quatre racines a, b, c, d de l'équation de départ (E) $x^4+nx^2+px+q=0$. Pour le "bon choix" de y indiqué par Lagrange, on a : $\left(x^2+y\right)^2=\left[x-\frac{p}{2(2y-n)}\right]^2(2y-n)$, c'est-à-dire

$$\left[x^2+y+\left[x-\frac{p}{2(2y-n)}\right]\sqrt{2y-n}\right]\left[x^2+y-\left[x-\frac{p}{2(2y-n)}\right]\sqrt{2y-n}\right]=0 \text{ équivalente à}$$

$$(1)\ x^2+y+\left[x-\frac{p}{2(2y-n)}\right]\sqrt{2y-n}=0 \text{ ou } (2)\ x^2+y-\left[x-\frac{p}{2(2y-n)}\right]\sqrt{2y-n}=0\,.$$

Donc parmi les racines *a, b, c, d* de (E), deux (par exemple *a* et *b*) sont racines de (1) et les deux autres (*c* et *d*) de (2). Dans les deux cas, on peut obtenir la somme et le produit des racines :

$$a+b=-\sqrt{2y-n} \qquad c+d=+\sqrt{2y-n}$$
$$ab=y-\frac{p}{2\sqrt{2y-n}} \qquad cd=y+\frac{p}{2\sqrt{2y-n}}$$

d'où $y=\frac{ab+cd}{2}$.

Cette valeur de y nous fait voir d'abord pourquoi la réduite en y est du troisième degré. En effet il est visible que la quantité y doit avoir autant de valeurs différentes qu'on en pourra former par toutes les permutations possibles des racines a, b, c, d dans l'expression $\frac{ab+cd}{2}$ *; on ne peut avoir de cette manière que les trois quantités suivantes*

$$\frac{ab+cd}{2},\ \frac{ac+bd}{2},\ \frac{ad+bc}{2},$$

de sorte que l'équation dont y sera la racine, devra donner chacune de ces trois quantités et, par conséquent, devra être du troisième degré.

On comprend maintenant pourquoi on sait résoudre l'équation en y. Puisque $y=\frac{ab+cd}{2}$ prend seulement trois valeurs $y_0=y, y_1, y_2$ lorsqu'on effectue les 24 permutations des quatre racines *a, b, c, d*, alors $y_0y_1y_2$, $y_0+y_1+y_2$, $y_0y_1+y_2y_0+y_1y_2$ sont des fonctions symétriques de *a, b, c, d* et s'expriment donc rationnellement à l'aide des coefficients de l'équation de départ, donc y_0, y_1, y_2 sont racines d'une équation du

troisième degré. Si on sait exprimer *a, b, c, d* à l'aide de y_0, y_1, y_2 , alors on sait résoudre l'équation de départ. C'est le calcul de Lagrange dans le numéro 31 (avec une nouvelle notation : $u = 2y$).

31. Voyons maintenant comment, en connaissant une des valeurs de u, on pourra trouver les quatre racines a, b, c, d. Puisque :

$$u = ab + cd \quad et \quad abcd = q,$$

il est clair que les deux quantités ab et cd seront les racines de cette équation du second degré

$$t^2 - ut + q = 0,$$

de sorte qu'en nommant t' et t'' ces deux racines on connaîtra les deux produits

$$ab = t' \quad et \quad cd = t'';$$

de plus on a

$$-p = ab(c+d) + cd(a+b) = t'(c+d) + t''(a+b)$$

Comme $a+b+c+d = 0$, on obtient : $a+b = \frac{p}{t'-t''}$ et $c+d = \frac{p}{t''-t'}$, et puisque $ab = t'$ et $cd = t''$, a et b sont solutions de : $x^2 - \frac{p}{t'-t''}x + t' = 0$ et c et d de $x^2 - \frac{p}{t''-t'}x + t' = 0$. La connaissance d'une des racines de la réduite permet donc de calculer les quatre racines de la proposée.

Lagrange examine alors les autres méthodes connues de résolution des équations du quatrième degré et conclut :

50. Nous terminerons ici notre analyse des méthodes qui concernent la résolution des équations du quatrième degré. Non seulement nous avons rapproché ces méthodes les unes des autres, et montré leur liaison et leur dépendance mutuelle ; nous avons encore, ce qui était le point principal, donné la raison a priori pourquoi elles conduisent, les unes à des réduites du troisième degré, les autres à des réduites du sixième, mais qui peuvent s'abaisser au troisième ; et l'on a dû voir que cela vient en général de ce que les racines de ces réduites sont des fonctions des quantités x', x'', x''', x^{IV}, telles qu'en faisant toutes les permutations possibles entre ces quatre quantités, elles ne peuvent recevoir que trois valeurs différentes comme la fonction $x'x''+x'''x^{IV}$, ou six valeurs, mais deux à deux égales et de signes contraires, comme la fonction $x'+x''-x'''-x^{IV}$, ou bien six valeurs telles, qu'en les partageant en trois couples et prenant la somme ou le produit des valeurs de chaque couple, ces trois sommes ou ces trois produits soient toujours les mêmes, quelque permutation qu'on fasse entre les quantités x', x'', x''', x^{IV}. Comme la fonction trouvée au numéro 42. C'est uniquement de l'existence de telles fonctions que dépend la résolution générale des équations du quatrième degré.

On commence à voir là changer l'objet d'étude du mathématicien. On ne s'intéresse plus aux racines de l'équation proposée, mais à l'effet des permutations des racines sur une fonction de ces racines. A priori, lorsqu'on effectue les 24 permutations des quatre racines, une telle fonction prend 24 valeurs. On s'intéressera

aux fonctions qui ne prennent pas "trop" de valeurs par ces 24 permutations, sans pour autant être symétriques, car alors on ne saurait pas exprimer *a, b, c, d* avec elles.

La section troisième consiste en des réflexions sur les changements de variable possibles lorsqu'on cherche à résoudre une équation et leurs chances d'aboutir :

Il serait donc fort à souhaiter que l'on pût juger à priori du succès que l'on peut se promettre dans l'application de ces méthodes aux degrés supérieurs au quatrième ; nous allons tâcher d'en donner les moyens par une analyse semblable à celle dont nous nous sommes servis jusqu'ici à l'égard des méthodes connues pour la résolution des équations du troisième et du quatrième degré.

Enfin, la quatrième section donne la *CONCLUSION DES REFLEXIONS PRECEDENTES, AVEC QUELQUES REMARQUES GENERALES SUR LA TRANSFORMATION DES EQUATIONS, ET SUR LEUR REDUCTION OU ABAISSEMENT A UN MOINDRE DEGRE.*

86. On a dû voir par l'analyse que nous venons de donner des principales méthodes connues pour la résolution de 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 ce sur quoi il paraît très difficile de pouvoir se prononcer en général.

...

87. Comme jusqu'ici nous n'avons fait que chercher ces sortes de fonctions à posteriori et d'après les méthodes connues pour la résolution des équations, il est nécessaire de faire voir maintenant comment il faudrait s'y prendre pour les trouver à priori et sans supposer d'autres principes que ceux qui suivent immédiatement de la nature même des équations : c'est l'objet que je me propose principalement dans cette Section.

Je donnerai d'abord des règles directes et générales pour déterminer le degré et la nature de l'équation d'où une fonction quelconque proposée des racines d'une équation de degré donné devra dépendre ; quoique cette matière ait déjà été traitée par d'habiles Géomètres, je crois qu'elle peut l'être encore d'une manière plus directe et plus générale, surtout dans le point de vue où nous l'envisageons ici, relativement à la résolution générale des équations.

Je ferai voir ensuite quelles sont les conditions nécessaires pour que l'équation dont il s'agit puisse admettre la résolution en supposant celle des équations des degrés inférieurs à celui de l'équation proposée ;

et je donnerai à cette occasion les vrais principes et, pour ainsi dire, la métaphysique de la résolution des équations du troisième et du quatrième degré.

Je traiterai enfin en peu de mots de la réduction des équations qui peuvent se décomposer en d'autres plus simples à cause de quelque relation particulière qu'il y a entre leurs racines, et je montrerai par quelques exemples comment on peut découvrir ces relations, et abaisser par là les équations proposées à des degrés moindres.

On s'intéresse à l'équation de degré μ : $x^{\mu}+mx^{\mu-1}+nx^{\mu-2}+...=0$ qui a μ racines $x', x'', x''', x^{IV},...,x^{(\mu)}$. De manière générale, si f est une fonction rationnelle quelconque des racines $x', x'', x''', x^{IV},...,x^{(\mu)}$, on va chercher de quelle équation $f(x', x'', x''', x^{IV},...,x^{(\mu)})$ est solution. Lagrange note $\Theta=0$ cette équation et il commence par faire le travail pour μ=2, μ=3, μ=4 pour expliquer comment son point de vue lui permet de trouver **à priori** les bons changements de variable.

Lorsqu'on effectue les μ ! permutations des μ racines, $f(x', x'', x''', x^{IV},...,x^{(\mu)})$ prend à priori μ! valeurs $f_0, f_1,....,f_{\mu!}$ et est donc solution d'une équation de degré μ ! : $(t-f_0)(t-f_1)...(t-f_{\mu!})=0$ *i.e.* $\Theta=0$, dont les coefficients, étant les fonctions symétriques élémentaires de $f_0, f_1,....,f_{\mu!}$ sont symétriques en $x', x'', x''', x^{IV},...,x^{(\mu)}$ et s'expriment donc rationnellement à l'aide des coefficients *m*, *n*, ... de l'équation de départ. Peut-on abaisser le degré de Θ ?

97.Quoique l'équation Θ = 0 doive être, en général, du degré $1.2.3....\mu=\varpi$ $1.2.3...\mu=\varpi$, *qui est égal au nombre de permutations dont les μ racines x', x'', x''', ... sont susceptibles, cependant s'il arrive que la fonction soit telle, qu'elle ne reçoive aucun changement par quelqu'une ou quelques-unes de ces permutations, alors l'équation dont il s'agit s'abaissera nécessairement à un degré moindre.*

Car supposons, par exemple, que la fonction $f[(x'),(x''),(x'''),(x^{IV}),...]$ *soit telle , qu'elle conserve la même valeur en échangeant x' en x'', x'' en x''', et x''' en x', en sorte que l'on ait*

$$f[(x'),(x''),(x'''),(x^{IV}),...]=f[(x''),(x'''),(x'),(x^{IV}),...],$$

il est clair que l'équation Θ = 0 aura déjà deux racines égales ; mais je vais prouver que dans cette hypothèse toutes les autres racines seront aussi égales deux à deux.

Il faut bien comprendre que, lorsque Lagrange dit que la fonction f conserve la même valeur en effectuant une permutation des racines, il s'agit, non pas de conserver la même valeur numérique, mais de conserver la même **fonction** f . Autrement dit, après permutation, on obtient une fonction des racines qui, **en tant que fonction**, est égale à f. Avec des notations plus habituelles, soit $f(X_1,X_2,....X_{\mu})$ une fonction rationnelle de μ variables. Pour toute permutation σ de $\{1,2,....,\mu\}$, on obtient une nouvelle fonction de μ variables : $g(X_1,X_2,....X_{\mu})=f(X_{\sigma(1)},X_{\sigma(2)},....X_{\sigma(\mu)})$ $g(X_1,X_2,...,X_{\mu})=f(X_{\sigma(1)},X_{\sigma(2)},...,X_{\sigma(\mu)})$. On peut noter : $g=\sigma f$. Lorsque σ parcourt l'ensemble Σ_{μ} de toutes les permutations de $\{1,2,....,\mu\}$, on obtient ainsi -

à priori- $\mu!$ fonctions rationnelles. Supposons que f soit invariante - en tant que fonction - par une permutation σ, c'est-à-dire que $g = \sigma f = f$ (en tant que fonction). Alors, pour toute permutation τ de Σ_μ, $(\tau\sigma)f = \tau(\sigma f) = \tau f$. En particulier : $\sigma^k f = \sigma^{k-1}(\sigma f) = \sigma^{k-1} f = f$. Soit H le groupe engendré par σ : f est invariante par toute permutation de $H = \{id, \sigma, \sigma^2, ..., \sigma^{p-1}\}$. Mais alors, on va pouvoir grouper p à p les valeurs prises par f (en tant que fonction) lorsqu'on effectue les μ ! permutations de Σ_μ . En effet, les classes à gauche selon H forment une partition de Σ_μ : H, τH $\{\tau\sigma^i, i = 0 \text{ à } p\}$, τ'H, etc., le cardinal de chaque classe étant égal à p =card(H) (puisque $\tau\sigma^1 = \tau\sigma^j \Rightarrow \sigma^1 = \sigma^j$). Or, on a déjà vu que f est invariante par toute permutation de H. Il est clair que f prend la même valeur (en tant que fonction) par toutes les permutations de τH car $(\tau\sigma^i)f = \tau(\sigma^i f) = \tau f$. Donc, les valeurs prises par f se groupent en valeurs égales p à p et donc f prend $\frac{\mu!}{p}$ valeurs distinctes lorsqu'on effectue les $\mu!$ permutations de Σ_μ. $f(x', x'', x''', x^{IV}, ..., x^{(\mu)})$ est donc solution d'une équation de degré $\frac{\mu!}{p}$. Ce n'est bien sûr pas le langage employé par Lagrange, mais l'idée de base est bien celle-ci. Reprenons le texte :

En effet, considérons une racine quelconque de la même équation, laquelle soit représentée par la fonction

$$f[(x^{IV}), (x'''), (x'), (x''), ...],$$

comme celle-ci dérive de la fonction

$$f[(x'), (x''), (x'''), (x^{IV}), ...],$$

en échangeant x' en x^{IV}, x'' en x''', x''' en x', x^{IV} en x'', il s'ensuit qu'elle devra garder aussi la même valeur en y en changeant x^{IV} en x''', x''' en x' et x' en x^{IV} ; de sorte qu'on aura aussi

$$f[(x^{IV}), (x'''), (x'), (x''), ...] = f[(x'''), (x'), (x^{IV}), (x''), ...] .$$

Donc, dans ce cas, la quantité Θ sera égale à un carré θ^2, et par conséquent l'équation $\Theta = 0$ se réduira à celle-ci $\theta = 0$, dont la dimension sera $\frac{\varpi}{2}$.

On démontrera de la même manière que, si la fonction

$$f[(x'), (x''), (x'''), (x^{IV}), ...]$$

est de sa propre nature telle, qu'elle conserve la même valeur en faisant deux, ou trois, ou un plus grand nombre de permutations différentes entre les racines x', x'', x''', x^{IV},..., les racines de l'équations $\Theta = 0$ seront égales trois à trois, ou quatre à quatre, ou etc. ; en sorte que la quantité Θ sera égale à un cube θ^3, ou à un carré-carré θ^4, ou etc., et que par conséquent l'équation $\Theta = 0$ se réduira à celle-ci $\theta = 0$, dont le degré sera égal à $\frac{\varpi}{3}$, ou égal à $\frac{\varpi}{4}$, ou, etc.

On remarquera que l'interprétation moderne en termes de groupes conduit accessoirement au fait que l'ordre du sous-groupe H divise l'ordre de Σ_μ, cas particulier du "théorème de Lagrange" (l'ordre d'un sous-groupe divise l'ordre du groupe).

Le travail de Lagrange montre qu'il faut s'intéresser à l'effet des permutations de Σ_μ sur les fonctions de μ variables. C'est donc ce que Lagrange va faire dans les paragraphes suivants. Deux fonctions f et g de $X_1, X_2, \ldots X_\mu$ sont dites *semblables* si elles sont invariantes par les mêmes permutations. Nous venons de voir que, dans ce cas, elles prennent le même nombre de valeurs distinctes. Lagrange écrit :

99. De tout ce que nous venons de démontrer il s'ensuit donc, en général : 1°que toutes les fonctions semblables des racines x', x'', x''',... d'une même équation sont nécessairement données par des équations du même degré ; 2°que ce degré sera toujours égal au nombre 1.2.3...μ (μ étant le degré de l'équation donnée), ou à un sous-multiple de ce nombre ; 3°que pour trouver directement l'équation la plus simple $\theta = 0$, par laquelle devra être déterminée une fonction quelconque donnée de x', x'', x''', ..., il n'y aura qu'à chercher toutes les différentes valeurs que cette fonction peut recevoir par les permutations des quantités x', x'', x''', ... entre elles, et, prenant ces valeurs pour les racines de l'équation cherchée, on déterminera par leur moyen les coefficients de cette équation suivant les méthodes connues et employées déjà plusieurs fois dans ce Mémoire.

Puis Lagrange démontre des résultats essentiels sur les fonctions de μ variables :

104. Donc :

1°Si l'on a deux fonctions quelconques t et y des racines x', x'', x''', ... de l'équation

$$x^\mu + mx^{\mu-1} + nx^{\mu-2} + \ldots = 0,$$

et que ces fonctions soient telles, que toutes les permutations entre les racines x', x'', x''', ... , qui feront varier la fonction y, fassent varier aussi en même temps la fonction t on pourra, généralement parlant, avoir la valeur de y en t et en m, n, p, ..., par une expression rationnelle, de manière que connaissant une valeur de t on connaîtra aussi immédiatement la valeur correspondante de y ; nous disons généralement parlant, car s'il arrive que la valeur connue de t soit une racine double , ou triple, etc., de l'équation en t, alors la valeur correspondante de y dépendra d'une équation carrée, ou cubique, etc., dont tous les coefficients seront des fonctions rationnelles de t et de m, n, p, ...

2°Si les fonctions t et y sont telles, que la fonction t conserve la même valeur par des permutations qui font varier la fonction y, alors on ne pourra trouver la valeur de y en t et en m, n, p, ... qu'au moyen d'une équation du second degré, si à une même valeur de t répondent deux valeurs de y , ou du troisième degré, si à une même valeur de t répondent trois valeurs différentes de y, et ainsi de suite. Les coefficients de ces équations en y seront, généralement parlant, des fonctions rationnelles de t et de m, n, p, ..., en sorte qu'étant donnée une valeur de t, on aura y par la simple résolution d'une équation du second ou du troisième degré, etc. ; mais s'il arrive que la valeur connue de t soit une racine double ou triple, etc., de l'équation en t, alors

les coefficients des équations dont il s'agit dépendront encore eux-mêmes d'une équation du second ou du troisième degré, etc.

De là on peut déduire les conditions nécessaires pour pouvoir déterminer les valeurs mêmes des racines x', x'', x''', ..., au moyen de celles d'une fonction quelconque des racines ; car il n'y aura pour cela qu'à prendre la simple valeur de x à la place de la fonction y, et à appliquer à ce cas les conclusions précédentes.

Examinons à la lumière de ces résultats la méthode de Ferrari pour résoudre les équations de degré quatre. Nous noterons $\begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \end{pmatrix}$ une permutation σ de Σ_4. Par exemple $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ est la permutation σ telle que : $\sigma(1)=2, \sigma(2)=3, \sigma(3)=1, \sigma(4)=4$.

Considérons les fonctions suivantes des racines *a, b, c, d* d'une équation du quatrième degré :

$f_0(a,b,c,d)=a+b+c+d \quad f_1(a,b,c,d)=ab+cd \quad f_2(a,b,c,d)=ab \quad f_3(a,b,c,d)=a$

f_0 est symétrique, invariante par toutes les permutations σ de Σ_4, donc est connue : c'est la somme des racines, nulle dans le cas étudié (résolution de l'équation $x^4+nx^2+px+q=0$).

Les permutations laissant f_1 invariante sont celles de

$$H_1=\left\{Id,\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\right\}$$

qui est d'ordre 8. Cela signifie que f_1 prend $\frac{4!}{8}=\frac{24}{8}=3$ valeurs lorsqu'on effectue les 24 permutations de Σ_4.

Donc f_1 est racine d'une équation de degré trois dont les coefficients s'expriment rationnellement à l'aide des coefficients de l'équation à résoudre (et de f_0, mais f_0=0).

Examinons maintenant l'effet des permutations de H_1 sur f_2. Parmi les permutations de H_1 , celles qui laissent f_2 invariante sont celles de $H_2=\left\{Id,\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\right\}$, qui est d'ordre 4.

Cela signifie que f_2 prend $\frac{card(H_1)}{card(H_2)}=2$ valeurs lorsqu'on lui applique les permutations de H_1. Le résultat du numéro 104 du texte de Lagrange affirme donc que est solution d'une équation de degré 2 dont les coefficients s'expriment rationnellement à l'aide de f_1 et des coefficients de l'équation de départ.

Enfin examinons l'effet de H_2 sur f_3. Les permutations de H_2 laissant f_3 invariante sont celles de $H_3=\left\{Id,\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}\right\}$, qui est d'ordre 2. Cela signifie que f_3 prend $\frac{4}{2}=2$ valeurs lorsqu'on lui applique les quatre permutations de H_2 . Donc f_3 = a est solution d'une équation de degré 2 dont les coefficients s'expriment rationnellement à l'aide de f_2 et des coefficients de l'équation de départ.

Résoudre une équation, c'est donc trouver une chaîne de fonctions des μ racines telles que la première est symétrique, la dernière est une des racines, chacune d'elles prenant "peu de valeurs" par les permutations qui laissent la précédente invariante. Lorsqu'on veut résoudre une équation de degré quatre, "peu de valeurs" signifie 2 ou 3 afin d'abaisser le degré de l'équation à résoudre. Le fait de terminer par f_3 = a répond au souci de Lagrange de *pouvoir déterminer une des racines à l'aide d'une fonction des racines* (numéro 104). Lagrange ne

parle qu'en termes de valeurs prises par une fonction des racines lorsqu'on effectue des permutations des racines, mais c'est ce type de réflexions qui mènera Galois à dégager le concept de groupe d'une équation. Il est clair que la résolution de l'équation de degré quatre est liée à l'existence d'une chaîne de sous-groupes de Σ_4 et c'est ce que précisera Galois dans son Mémoire *Sur les conditions de résolubilité des équations par radicaux* paru en 1846 dans le *Journal de Mathématiques Pures et Appliquées.*

Le travail de Lagrange ouvre de manière remarquable un champ nouveau aux investigations des mathématiciens ; les créateurs du concept de groupe tels Cauchy, Abel, Galois, Gauss ont lu les écrits de Lagrange. Et on peut voir dans ce mémoire l'amorce des changements fondamentaux des objets d'étude de l'algèbre qui, de résolution d'équations numériques, va devenir étude des structures.

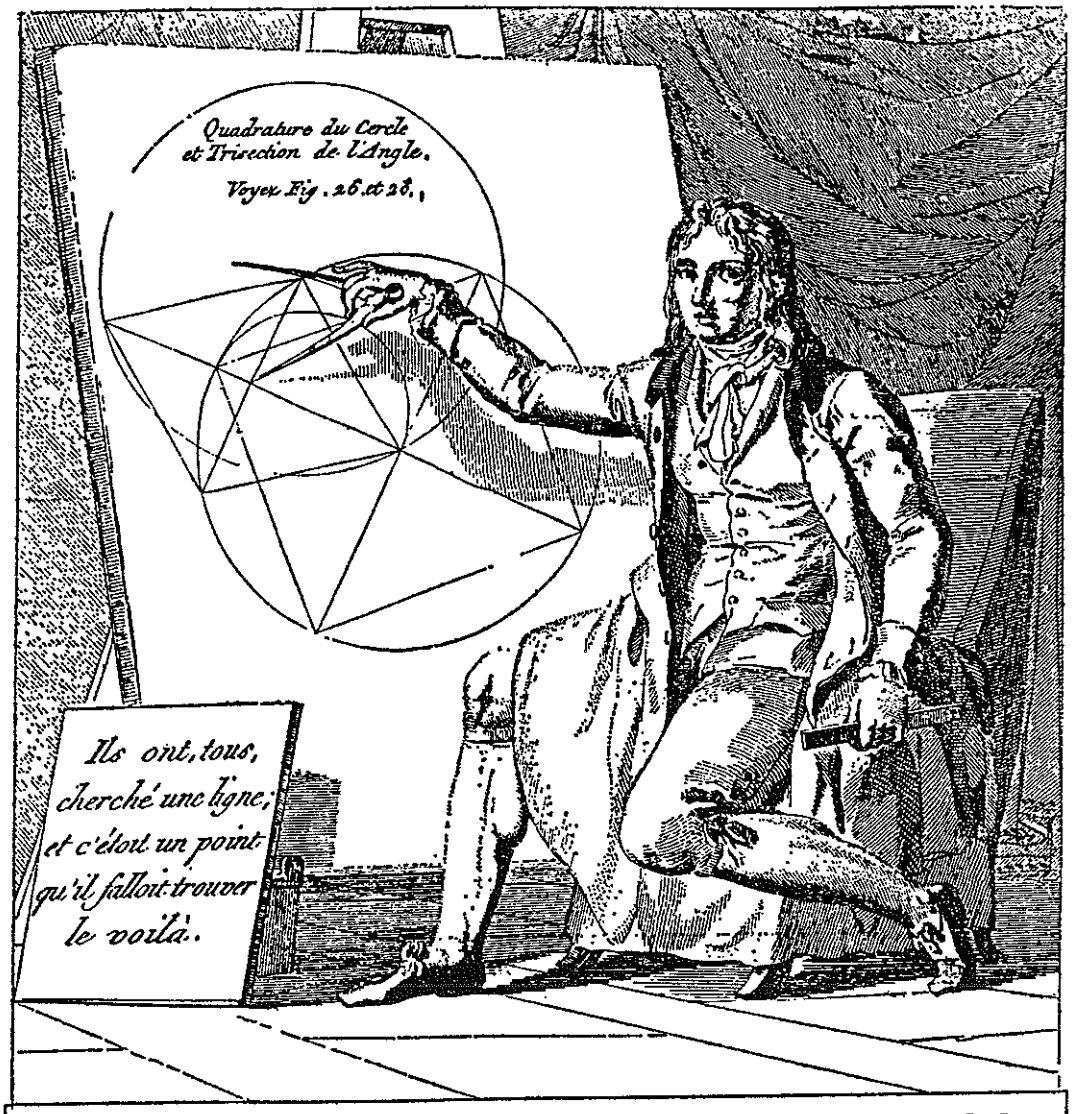
Bibliographie

FRIEDELMEYER J.P. *Emergence du concept de groupe à travers le problème de la résolution des équations algébriques*, Fragments d'histoire des mathématiques III . Brochure A.P.M.E.P. n°83. 1991

FRIEDELMEYER J.P. *Recherche inconnue désespérément* in *Histoires de problèmes, histoire des mathématiques*, Ellipses, Paris, 1993.

LAGRANGE *Réflexions sur la résolution algébrique des équations* (Mémoire de l'Académie Royale des Sciences et Belles-Lettres de Berlin, 1770 in *Œuvres de Lagrange* publiées par Serret, Gauthier-Villars, Paris, 1861 (tome 3, p. 205 - 421).

MUTAFIAN *Equations algébriques et théorie de Galois*, Vuibert, Paris, 1980.



Supériorité du Cercle, marquée dans toute la nature. incommensurabilité de la ligne circulaire avec la ligne droite. Demie-circonférence des cercles rectifiée dans la diagonale des quarrés. Rapport *de la circonférence du cercle à son diamètre.* Quadrature *du cercle.* Circulature *du quarré. Solution géométrique de ce grand problême. Seconde partie de cette solution qui donne la mesure arithmétique d'ou dépend tout le mecanisme du cercle et du quarré. Quatrième proportionnelle ajoutée à l'hypothénuse. Solution de la* Trisection *de l'angle, si fameux dans l'antiquité. (Voyez sa démonstration, page 129). Ce sont autant de vérités cachées jusqu'à ce jour aux hommes, et découvertes en l'an 12, par L. Polier Deslauriers du Mans..*

M.r de Méley, ami des sciences, pénétré de toute l'importance de la découverte de la Quadrature du Cercle, a légué par testament une somme de cinquante mille écus en faveur de celui qui la feroit, d'après le jugement de l'Académie des Sciences

DANS NOS CLASSES

La quadrature du cercle:

Pappus et la quadratrice d'Hippias

Martine Bühler

Jusqu'à l'année 1997-1998 incluse, le programme de terminale scientifique comprenait l'introduction de la notion de continuité et quelques résultats relatifs à cette notion. Tout ceci disparaît à la rentrée 1998, et on peut lire dans le B.O. hors série n°4 du 12 Juin 1997, page 17 : *« les fonctions étudiées dans le cadre du programme sont dérivables par intervalles. C'est donc au théorème des valeurs intermédiaires énoncé en classe de première que l'on se réfère, notamment pour résoudre une équation du type f(x) = λ et pour définir une fonction réciproque. Ces divers travaux seront l'occasion de donner une première approche non formalisée d'une fonction continue sur un intervalle ou d'une fonction discontinue en un point. Mais la notion de continuité demeure en dehors des objectifs du programme. »*

Il nous faut donc, à travers les travaux que nous faisons faire à nos élèves, leur donner une idée de la notion de continuité et de son intérêt, et ce d'autant plus qu'ils en auront besoin pour leur études après le Baccalauréat. C'est dans cet esprit que nous avons élaboré le problème suivant lié à la quadrature du cercle ; il permet d'utiliser les courbes paramétrées (revenues en 1998 dans le giron du programme « obligatoire » de TS) et de faire comprendre la nécessité de prolonger une fonction par continuité pour le résoudre.

Les mathématiciens grecs, plus de trois siècles avant notre ère, s'intéressaient - entre autres - au problème de la quadrature du cercle : il s'agit, un cercle étant donné, de construire à la règle et au compas un carré de même aire que ce cercle. Le problème est entièrement géométrique mais on peut le formuler ainsi : un segment unité étant donné (le rayon du cercle), peut-on construire à la règle et au compas un carré dont l'aire a pour mesure π ? les mathématiciens grecs, tout comme leurs successeurs, échouèrent dans cette construction dont l'impossibilité ne fut prouvée qu'en 1882 ; cette longue quête a laissé des traces jusque dans notre vocabulaire, puisque l'expression «c'est la quadrature du cercle » est communément utilisée pour désigner une tâche très difficile, voire impossible à accomplir. Cependant, les grecs imaginèrent d'autres moyens de « quarrer le cercle », utilisant en particulier des courbes dites « mécaniques », que l'on ne peut tracer à la règle et au compas. C'est ce qu'explique Pappus dans le texte - extrait de la *Collection mathématique* que nous allons étudier.

Pappus d'Alexandrie (fin III^{ème} siècle- début IV^{ème} siècle) a écrit principalement la *Collection mathématique* qui comportait huit livres. Il s'agit d'une compilation de travaux de mathématiciens antérieurs - en particulier Euclide, Archimède, Apollonius, Ptolémée - enrichie de nombreux commentaires et résultats nouveaux. Bien que ne nous soient parvenus qu'une partie du livre II et les six derniers livres, ils nous sont un témoin précieux des mathématiques grecques.

I. Préliminaires sur les fonctions trigonométriques

On définit sur $\mathbb{R}^+$ la fonction φ par $\varphi(t) = \sin t - t + \frac{t^3}{6}$.

1°) Déterminer φ', φ'', φ'''.

2°) a) Etudier le signe de $\varphi'''(t)$ pour $t \in \mathbb{R}^+$.

b) En déduire les variations de φ'' puis son signe sur $\mathbb{R}^+$.

3°) Etudier de même les variations puis le signe de φ' sur $\mathbb{R}^+$; enfin faites de même pour φ.

4°) En déduire les inégalités, pour $t \in \mathbb{R}^+$,

$$1 - \frac{t^2}{2} \le \cos t \le 1$$

$$t - \frac{t^3}{6} \le \sin t \le t$$

5°) a) Rappeler $\lim_{t \to 0} \frac{\sin t}{t}$.

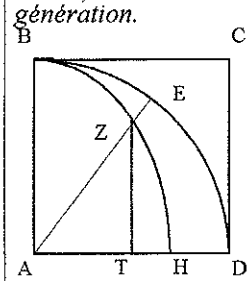
b) Montrer que pour $t \in]0,1]$, $\frac{1}{t} \le \frac{1}{\sin t} \le \frac{1}{t}\left(1 + \frac{t^2}{6} + \frac{t^4}{30}\right)$.

c) Montrer que pour $t \in]0,1]$, $-\frac{t}{2} \le \frac{\cos t}{\sin t} - \frac{1}{t} \le \frac{t}{6} + \frac{t^3}{30}$ et en déduire $\lim_{\substack{t \to 0 \\ t>0}} \left(\frac{\cos t}{\sin t} - \frac{1}{t}\right)$.

II. Définition de la quadratrice

1°) Lire le texte[3] suivant (les "droites" désignent, pour nous, des segments) :

Une ligne qui tire sa dénomination de sa propriété même a été adoptée par Dinostrate, Nicomède et certains autres auteurs récents pour effectuer la quadrature du cercle ; ils l'ont appelée la quadratrice, et voici sa génération.



Posons un carré ABCD et décrivons l'arc BED autour du centre A. Faisons mouvoir la droite AB de telle sorte que, le point A restant fixe, le point B se déplace suivant l'arc BED et que la droite BC, se maintenant toujours parallèle à la droite AD, accompagne le point B qui se déplace suivant la droite AB. De plus, que la droite AB, se mouvant d'une manière uniforme, parcoure l'angle compris sous les droites BA, AD, c'est-à-dire que le point B parcoure l'arc BED dans le même temps que la droite BC se déplace le long de la droite BA, c'est-à-dire que le point B se déplace suivant la droite BA.

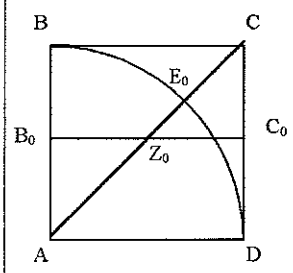
Il se fera évidemment que les droites AB et BC coïncideront simultanément l'une et l'autre avec la droite AD. En conséquence, un tel mouvement ayant lieu, les droites AB, BC se couperont mutuellement en un point qui est continuellement transporté avec elles, lequel décrira une ligne concave d'un même côté, telle que BZH, dans l'espace compris entre les droites BA, AD et l'arc BED ; ligne qui paraît commode pour trouver un carré équivalent à un cercle donné.

---

[3] PAPPUS d'Alexandrie, trad. P. VER EECKE, *La collection mathématique*, Blanchard, 1982, t. I, p. 191.
Dinostrate : géomètre grec, début du IV^{ème} siècle av. J. C.. Proclus en parle comme d'un frère de Menechme, lui-même élève d'Eudoxe et de Platon. On pense qu'il fut le premier à utiliser la quadratrice pour la résolution de la quadrature du cercle.
Nicomède : géomètre grec, on ne sait rien de sa vie, il vécut aux environs de 250 av. J. C..

Commentaire : le segment [BC] se déplace d'un mouvement de translation uniforme parallèlement à (BA) et le segment [AB] d'un mouvement de rotation uniforme autour de A. Lorsque [BC] prend la position [AD], [AB] la prend également. A chaque instant, les deux segments se coupent en un point Z qui décrit donc une certaine courbe BZH

2°) Traçons quelques points.

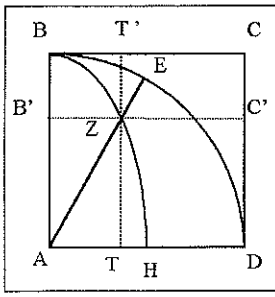


Les deux mouvements étant uniformes, les segments arrivent « à mi-parcours » en même temps ; donc [BC] prend la position [B_0C_0] (avec B_0 milieu de [AB]) en même temps que [AB] prend la position [AE_0] (où (AE_0) est la bissectrice de BAD). Le point Z_0 est donc un point de la quadratrice. Il en est de même pour le quart de parcours (avec B_1 milieu de [B_0B] et (AE_1) bissectrice de BAE_0), les trois-quarts de parcours, les huitièmes de parcours, etc. On peut donc placer une infinité de points de la quadratrice grâce à des bissections successives obtenues à la règle et au compas.

Tracer un carré ABCD ayant 16 cm de côté et placer 7 points de la quadratrice en appliquant la méthode expliquée ci-dessus.

Remarque : en utilisant la règle et le compas on peut placer autant de points que l'on veut par bissections successives ; mais on ne peut pas placer ainsi **tous** les points et donc la quadratrice **n'est pas** constructible à la règle et au compas.

3°) a) Lire la fin du paragraphe XXX.



Du reste, sa propriété principale est telle que, si une droite quelconque AZE est menée transversalement à l'arc, la droite BA sera à la droite ZT comme l'arc entier est à l'arc ED ; car cela résulte manifestement de la génération de la ligne.

b) Commentaire : Pappus énonce là que : $\frac{BA}{ZT} = \frac{\text{arc}(BD)}{\text{arc}(ED)}$, c'est-à-dire que le rapport de proportionnalité entre les longueurs BA et ZT est le même que celui entre les arcs BD et ED.

Justification : la construction précédente permet de comprendre que, si T désigne le temps de parcours de B jusqu'à D sur l'arc BD, et T' le temps de parcours jusqu'en E, alors : $\frac{\text{arc}(BD)}{\text{arc}(BE)} = \frac{T}{T'} = \frac{BA}{BB'}$.

En déduire : $\frac{BA}{ZT} = \frac{\text{arc}(BD)}{\text{arc}(ED)}$.

III. Etude de la quadratrice. Paramétrisation

Le plan est rapporté au repère orthonormal (A, $\overrightarrow{AD}$, $\overrightarrow{AB}$). On note t la mesure en radians de l'angle DAZ, t appartenant à $\left[0, \frac{\pi}{2}\right]$ et Z étant un point de la quadratrice.

Z a pour coordonnées (x(t), y(t)), dans le repère (A, $\overrightarrow{AD}$, $\overrightarrow{AB}$).

1°) Trouver une relation entre x(t), y(t) et tan t.

2°) Déduire de II 3°) l'expression de y(t) en fonction de t, puis celle de x(t) à l'aide de t, cost, sint.

3°) Voyez-vous un problème apparaître ?

4°) Lire l'extrait suivant :

> XXXI.
>
> *C'est à juste titre cependant que Sporos n'a pas agréé cette ligne [...]*
>
> *Ensuite, l'extrémité de la ligne dont certains se servent pour la quadrature du cercle, c'est-à-dire le point où la ligne coupe la droite AD, n'est nullement trouvée. Représentons-nous d'ailleurs les choses que nous avons dites sur la délinéation proposée : lorsque les droites CB, BA mises en mouvement seront stabilisées simultanément, elles s'appliqueront sur la droite AD et ne feront plus section entre elles ; car, la section cesse avant l'application sur la droite AD ; section qui deviendrait, au contraire, l'extrémité de la ligne où celle-ci rencontrerait la droite AD ; à moins qu'on ne dise d'imaginer la ligne comme étant prolongée jusqu'à la droite DA de la manière dont nous établissons les lignes droites.*

Commentaire : le problème posé par Pappus - et d'autres avant lui - est que, lorsque les segments [AB] et [BC] terminent leurs mouvements, ils sont tous les deux confondus avec [AD] et donc on ne peut plus déterminer Z.

Question : comment se traduit ce problème dans la paramétrisation de la quadratrice ?

Pappus explique qu'il faudrait « imaginer la ligne comme étant prolongée jusqu'à la droite DA ». Autrement dit, il faut prolonger la quadratrice par la « position-limite » qu'occuperait le point Z lorsque t tend vers 0. C'est ce que nous allons faire pour obtenir le point H.

5°) Déterminer $\ell = \lim_{t \to 0} x(t)$.

6°) On définit alors la fonction f sur $[0, \frac{\pi}{2}]$ par :

$$\begin{cases} f(t) = \frac{2}{\pi} t \frac{\cos t}{\sin t} \text{ pour } t \in \left]0, \frac{\pi}{2}\right] \\ f(0) = \ell \end{cases}$$

La fonction f et la fonction x sont-elles les mêmes ou sont-elles différentes ? Pourquoi ?

Remarque : f, définie sur $[0, \frac{\pi}{2}]$, coincide avec x sur $]0, \frac{\pi}{2}]$ et vérifie $f(0) = \lim_{t \to 0} x(t)$. On dit que f est le « prolongement par continuité » de x en 0.

7°) La quadratrice Γ est alors définie de la manière suivante :

pour $t \in [0, \frac{\pi}{2}]$, Z(t) a pour coordonnées : $\begin{cases} X(t) = f(t) \\ Y(t) = \frac{2}{\pi} t \end{cases}$

a) Quel est le point de paramètre $\frac{\pi}{2}$?

b) Etablir le tableau des variations simultanées de X et Y sur $[0, \frac{\pi}{2}]$.

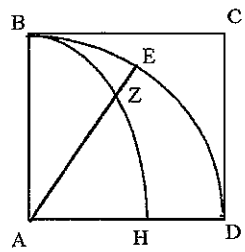
c) Déterminer la tangente à Γ au point de paramètre $\frac{\pi}{2}$.

d) f est-elle dérivable en 0 ? (**Attention** : il faut revenir à la définition de la dérivabilité d'une fonction en un point).

e) Quelles sont les coordonnées du point H de paramètre 0 ? Déterminer la tangente à Γ en ce point.

f) Terminer alors le tracé de la quadratrice commencé au II. 2°).

8°) a) Lire la proposition 26.



PROPOSITION 26.

Ayant un carré ABCD, l'arc BED décrit autour du centre A et la quadratrice BZH étant obtenue comme nous l'avons dit précédemment, il faut démontrer que la droite BA est à la droite AH comme l'arc DEB est à la droite BA.

b) Traduire la conclusion en termes d'égalité de rapports.

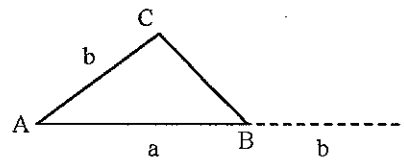
c) Dans le travail que vous avez fait précédemment, quel est le résultat équivalent à celui énoncé par Pappus ? (Vous expliquerez clairement la réponse).

Remarque : Pappus, lui, établit ce résultat en utilisant une méthode démonstrative assez technique, la méthode d'exhaustion ou encore méthode par double réduction à l'absurde. Cette méthode sera utilisée jusqu'au XVII^{ème} siècle ; Pascal l'appelait « la méthode des Anciens ».

IV. Mais quel est donc le lien avec la quadrature du cercle ?

Soient deux nombres réels non nuls a et b. On appelle « troisième proportionnelle des nombres a et b » le nombre c tel que : $\frac{a}{b} = \frac{b}{c}$.

1°) Deux segments [AB] et [AC] de longueurs a et b étant donnés, construire la troisième proportionnelle de a et b.



2°) Lire la conclusion de la proposition 26 de Pappus , la justifier et la traduire en termes de rapports :

Et il est clair que la droite prise comme troisième proportionnelle des droites AH, AB sera égale à l'arc BED, et que le quadruple de cette droite sera égal à la circonférence du cercle entier.

On peut donc construire la longueur de l'arc BED.

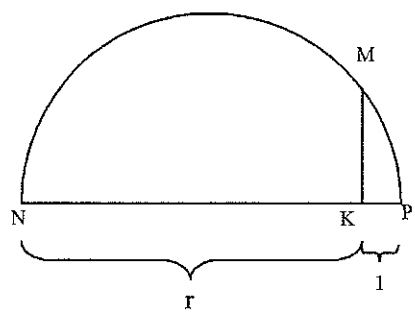
3°) Lire la proposition 27 :

Proposition 27

Or, la droite égale à la circonférence du cercle étant trouvée, on voit clairement que l'on construira facilement le carré équivalent au cercle.

Cette proposition affirme que si l'on sait « rectifier » le cercle (i.e. construire un segment ayant pour longueur le périmètre du cercle), alors on sait le « quarrer ».

Expliquer comment on peut construire à la règle et au compas un carré d'aire r, un segment de longueur unité et un segment de longueur r étant donnés.

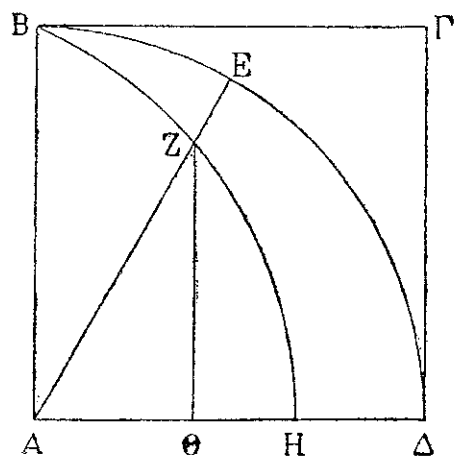


Calculez MK.

XXX.

Une ligne qui tire sa dénomination de sa propriété même a été adoptée par Dinostrate, Nicomède et certains autres auteurs récents pour effectuer la quadrature du cercle ; ils l'ont appelée la quadratrice (1), et voici sa génération.

Posons un carré ABΓΔ et décrivons l'arc BEΔ autour du centre A. Faisons mouvoir la droite AB de telle sorte que, le point A restant fixe, le point B se déplace suivant l'arc BEΔ, et que la droite BΓ, se maintenant toujours parallèle à la droite AΔ, accompagne le point B qui se déplace suivant la droite AB. De plus, que la droite AB, se mouvant d'une manière uniforme, parcoure l'angle compris sous les droites BA, AΔ, c'est-à-dire que le point B parcoure l'arc BEΔ dans le même temps que la droite BΓ se déplace le long de la droite BA, c'est-à-dire que le point B se déplace suivant la droite BA. Il se fera évidemment que les droites AB et BΓ coïncideront simultanément l'une et l'autre avec la droite AΔ. En conséquence, un tel mouvement ayant lieu, les droites AB, BΓ se couperont mutuellement en un point qui est continuellement transporté avec elles, lequel décrira une ligne concave d'un même côté, telle que BZH, dans l'espace compris entre les droites BA, AΔ et l'arc BEΔ ; ligne qui paraît commode pour trouver un carré équivalent à un cercle donné. Du reste, sa propriété principale est telle que, si une droite quelconque AZE est menée transversalement à l'arc, la droite BA sera à la droite ZΘ comme l'arc entier est à l'arc EΔ ; car cela résulte manifestement de la génération de la ligne (2).



---

1. τετραγωνίζουσα γραμμὴ, la ligne tétragonisante ou quadratrice.

2. Le texte exprime d'une manière un peu confuse que, si une droite BΓ se meut uniformément et parallèlement à elle-même le long du rayon AB et, qu'en même temps qu'elle part du point B, le rayon BA tourne uniformément autour du centre A, vers le point Δ, de manière qu'il se confonde avec AΔ au moment où la droite BΓ s'y confondra aussi, on aura, par l'intersection continuelle de ces deux lignes, une courbe BZH, appelée quadratrice de Dinostrate, mais dont l'invention remonte probablement au sophiste Hippias d'Elis qui vécut dans la seconde moitié du cinquième siècle avant J.-C. L'équation cartésienne de

PAPPUS D'Alexandrie, trad. P.VER EECKE, La collection mathématique, Blanchard, t.I, p.191–196.

XXXI.

C'est à juste titre cependant, que Sporos (1) n'a pas agréé cette ligne, parce qu'on y assume d'abord comme hypothèse ce à quoi elle semble pouvoir être utilisée (2).

En effet, si deux points commencent à se mouvoir à partir du point B, comment pourront-ils se stabiliser en même temps, l'un au point A suivant une droite, l'autre au point Δ suivant un arc, sans connaître au préalable le rapport de la droite AB à l'arc BEΔ ? (3) Car, il faut nécessairement que les vitesses des mouvements soient dans le même rapport. Dès qu'on use de vitesses non ordonnées, comment ces points se stabiliseront-ils ainsi simultanément, à moins que cela n'arrive par hasard ? Or, cela n'est-il pas déraisonnable ? Ensuite, l'extrémité de la ligne dont certains se servent pour la quadrature du cercle, c'est-à-dire le point où la ligne coupe la droite AΔ, n'est nullement trouvée. Représentons-nous d'ailleurs les choses que nous avons dites sur la délinéation proposée : Lorsque les droites ΓB, BA mises en mouvement seront stabilisées simultanément (4), elles s'appliqueront sur la droite AΔ et ne feront plus de section entre elles ; car,

---

cette courbe est : $x = \frac{y}{\text{tang.}\frac{\pi}{2}\frac{y}{r}}$; mais son équation polaire : $\rho \sin\varphi = R\,\frac{\varphi}{\frac{1}{2}\pi}$ est l'expression la plus simple qui corresponde à la définition qui en est donnée par Pappus.

1. Sporos de Nicée est mentionné comme commentateur (Σπόρος ὁ ὑπομνηματιστής) par quelques auteurs, notamment dans le petit traité : *Sur la Sphère d'Aratus*, dû au mécanicien Léontius, au sixième siècle après J.-C. Paul Tannery a cherché à établir l'existence d'une compilation intitulée : *Le Rucher Aristotélique* (Ἀριστοτελικὰ κηρία) qui aurait été composée par Sporos vers la fin du troisième siècle après J.-C., laquelle contenait des extraits mathématiques sur la quadrature du cercle et sur la duplication du cube, et a pu être utilisée par Pappus. Voir : PAUL TANNEY, *Sur Sporos de Nicée*, dans *Archives de la Faculté des Lettres de Bordeaux*, n° 3, 1882, t. IV, pp. 257-267, ou bien : *Mémoires scientifiques de Paul Tannery*, vol. I, pp. 178-184.

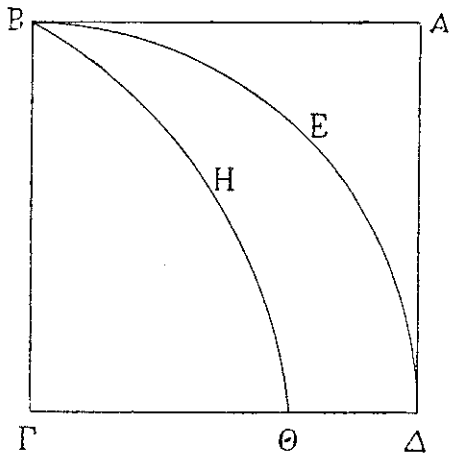
2. Si l'on pose : $y = 0$ dans l'équation cartésienne de la note avant-précédente, on a : $x = AH = \frac{2AB}{\pi}$ d'où : $\pi = \frac{2AB}{AH}$. La critique de Sporos vise la difficulté de calculer π au moyen d'un rapport en l'absence d'un procédé mécanique permettant de tracer la courbe d'un mouvement continu, et de déterminer par conséquent le point H.

3. C'est-à-dire sans connaître le rapport de la circonférence au rayon.

4. C'est-à-dire lorsque les droites ΓB, BA seront arrivées en fin de course.

la section cesse avant l'application sur la droite AΔ ; section qui deviendrait, au contraire (1), l'extrémité de la ligne où celle-ci rencontrerait la droite AΔ ; à moins qu'on ne dise d'imaginer la ligne comme étant prolongée jusqu'à la droite ΔA de la manière dont nous établissons les lignes droites (2). Or, cela ne répond pas à ce qui a été supposé au début, notamment que le point H soit pris en ayant pris au préalable le rapport de l'arc à la droite. D'ailleurs, à moins que ce rapport ne soit donné, il ne convient pas que, se confiant à la réputation des hommes qui l'ont inventée, l'on admette une ligne qui soit en quelque sorte trop mécanique [et utile aux mécaniciens pour beaucoup de problèmes] (3). Mais, exposons d'abord le problème qui se démontre au moyen de cette ligne (4).

PROPOSITION 26. — Ayant un carré ABΓΔ, l'arc BEΔ décrit autour du centre Γ et la quadratrice BHΘ étant obtenue comme nous l'avons dit précédemment, il faut démontrer que la droite BΓ est à la droite ΓΘ comme l'arc ΔEB est à la droite BΓ.

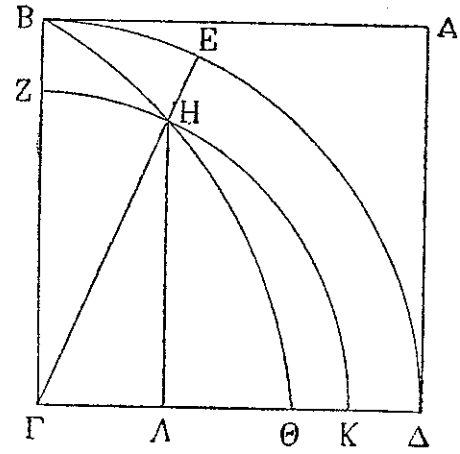


En effet, s'il n'en est pas ainsi, la droite BΓ sera à une droite plus grande ou plus petite que la droite ΓΘ (5).

Qu'elle soit d'abord, si possible, à une droite plus grande ΓK. Décrivons, autour du centre Γ, l'arc ZHK qui coupe la ligne (6) au point H ; menons la perpen-

1. C'est-à-dire d'après les protagonistes de la quadratrice.
2. C'est-à-dire à moins de considérer la ligne courbe comme étant prolongée à partir du dernier point de section de la même manière que l'on prolonge une ligne droite.
3. Hultsch considère ce membre de phrase comme ayant été interpolé (Cfr. *loc. cit.*, vol. I, p. 254, l. 24). S'il s'agit cependant d'une interpolation très ancienne, la phrase peut avoir été puisée dans l'ouvrage de Sporus, et indiquer que des équerres en forme de quadratrices étaient utilisées dans la pratique.
4. Voir le problème dont il est question au début du chap. XXX.
5. Sous-entendu : comme l'arc ΔEB est à la droite BΓ.
6. C'est-à-dire la quadratrice BHΘ.

diculaire HΛ et prolongeons la droite de jonction ΓH jusqu'au point E. Dès lors, puisque la droite BΓ, c'est-à-dire la droite ΓΔ, est à la droite ΓK comme l'arc ΔEB est à la droite BΓ (1), et que l'arc BEΔ est à l'arc ZHK comme la droite ΓΔ est à la droite ΓK (car une circonférence de cercle est à une circonférence comme le diamètre de ce cercle est au diamètre) (2), il est clair que l'arc ZHK est égal à la droite BΓ. Et puisque, en raison de la propriété de la ligne, la droite BΓ est à la droite HΛ comme l'arc BEΔ est à l'arc EΔ, il s'ensuit que la droite BΓ est aussi à la droite HΛ comme l'arc ZHK est à l'arc HK. Or, on a démontré que l'arc ZHK est égal à la droite BΓ ; donc, l'arc HK est aussi égal à la droite HΛ ; ce qui est absurde. En conséquence, la droite BΓ n'est pas à une droite plus grande que la droite ΓΘ comme l'arc BEΔ est à la droite BΓ (3).



XXXII.

Mais, je dis qu'elle n'est pas non plus à une droite plus petite (4).

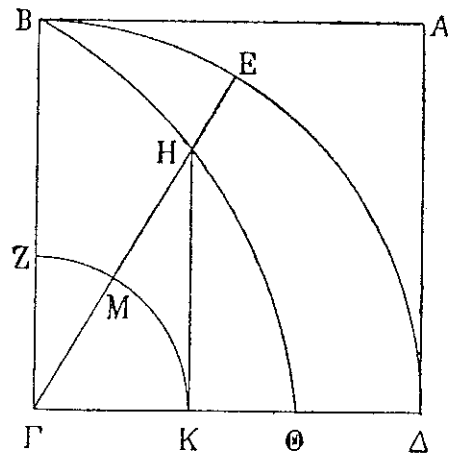
1. Par hypothèse.

2. Théorème démontré par Euclide, dont Pappus donnera deux démonstrations à sa manière, l'une à la proposition 11 du livre V, l'autre à la proposition 22 du livre VIII ; et il admet donc ici tacitement que les arcs qui mesurent des angles égaux sont entre eux comme les rayons des cercles auxquels ils appartiennent.

3. Cette démonstration apagogique se déroule comme suit. On a, par hypothèse : $\frac{B\Gamma}{\Gamma K > \Gamma\Theta} = \frac{\Gamma\Delta}{\Gamma K} = \frac{\text{arc } \Delta EB}{B\Gamma}$. Or, $\frac{\text{arc } \Delta EB}{\text{arc } ZHK} = \frac{\Gamma\Delta}{\Gamma K}$; donc : $\frac{\text{arc } \Delta EB}{\text{arc } ZHK} = \frac{\text{arc } \Delta EB}{B\Gamma}$, d'où : arc ZHK = droite BΓ. Or, la propriété de la quadratrice (voir chap. XXX, *in fine*) donne : $\frac{B\Gamma}{H\Lambda} = \frac{\text{arc } BE\Delta}{\text{arc } E\Delta}$, tandis que l'on a : $\frac{\text{arc } BE\Delta}{\text{arc } E\Delta} = \frac{\text{arc } ZHK}{\text{arc } HK}$; donc : $\frac{B\Gamma}{H\Lambda} = \frac{\text{arc } ZHK}{\text{arc } HK}$; d'où en présence de l'égalité : arc ZHK = BΓ, il vient : arc HK = droite HΛ ; ce qui est impossible.

4. C'est-à-dire que l'on n'a pas non plus : $\frac{B\Gamma}{K\Gamma < \Gamma\Theta} = \frac{\text{arc } BE\Delta}{\text{droite } B\Gamma}$.

En effet, qu'elle soit, si possible, à une droite ΚΓ. Décrivons l'arc ZMK autour du centre Γ ; menons, à angles droits sur la droite ΓΔ, la droite ΚΗ qui coupe la quadratrice au point Η, et prolongeons la droite de jonction ΓΗ jusqu'au point Ε. Dès lors, pareillement à ce que nous avons écrit précédemment, nous démontrerons que l'arc ZMK est égal à la droite ΒΓ, et que la droite ΒΓ est à la droite ΗΚ comme l'arc ΒΕΔ est à l'arc ΕΔ, c'est-à-dire comme l'arc ZMK est à l'arc ΜΚ. D'après cela, il est clair que l'arc ΜΚ sera égal à la droite ΚΗ ; ce qui est absurde. En conséquence, la droite ΒΓ ne sera pas à une droite plus petite que la droite ΓΘ comme l'arc ΒΕΔ est à la droite ΒΓ (1). Or, on a démontré qu'elle n'est pas à une droite plus grande ; donc, elle est à la droite ΓΘ même.



Et il est clair aussi que la droite prise comme troisième proportionnelle des droites ΘΓ, ΓΒ sera égale à l'arc ΒΕΔ, et que le quadruple de cette droite sera égal à la circonférence du cercle entier.

Proposition 27. — Or, la droite égale à la circonférence du cercle étant trouvée, on voit clairement que l'on construira facilement le carré équivalent au cercle.

En effet, le rectangle compris sous le périmètre du cercle et le rayon est le double du cercle, comme Archimède l'a démontré (2).

1. Cette démonstration apagogique se déroule comme dans la note avant-précédente.

2. Pappus énonce en d'autres termes la proposition I du traité *De la Mesure du Cercle* d'Archimède : « Tout cercle équivaut au triangle rectangle pour lequel on a le rayon égal à l'un des côtés adjacents à l'angle droit et le périmètre égal à la base ». Voir *Œuvres d'Archimède*, trad. de P. Ver Eecke, p. 127.

Brochures du groupe M.:A.T.H.

n° 61 : Mathématiques : Approche par des textes historiques - Tome 1 -.....	50 F	450 gr
n° 79 : Mathématiques : Approche par des textes historiques - Tome 2 -	60 F	530 gr
n° 90 : Mathématiques : Approche par des textes historiques - Tome 3	(parution juillet 2000)	

Reproduction de textes anciens

(Ancienne série) :

I	Disme	Simon Stevin.	14 F	80 gr
II	Géométrie élémentaire	Félix Klein	25F	180 gr
III	Dictionnaire Mathématiques	M. Ozanam (1er fascicule)	31F	250 gr
IV	Dictionnaire Mathématique	M. Ozanam (2ème fascicule)	32F	250 gr

(Nouvelle série) :

N° 1 : Histoire des recherches sur la quadrature du cercle	J.E Montucla	38F	340 gr
N° 2 : Elémens du calcul des probabilités	Marquis de Condorcet	28F	240 gr
N° 3 : Traité des Indivisibles	Gilles-Personne de Roberval	32F	270 gr
N° 4 : Les Porismes d'Euclide	Michel Chasles	35F	300 gr
N° 5 : Sur la théorie des Ensembles	Georg Cantor	52F	450 gr
N° 6 : Traité des sections coniques	M. de La Chapelle	42F	450 gr
N° 7 : Traité élémentaire de calcul des probabilités	S-F Lacroix	37F	300 gr
N° 8 : Elémens d'algèbre	Alexis-Claude Clairaut	41F	350 gr
N° 9 : Recueil d'exercices sur le calcul infinitésimal	Jean-Frédéric Frénet	44F	384 gr
N° 10 Problèmes pour les arpenteurs	Lorenzo Mascheroni	21F	156 gr
N° 11 Méthode des moindres carrés	Carl-Friedrich Gauss.....	36F	295 gr
N° 12 Traité du calcul différentiel et du calcul intégral	Sylvestre-François Lacroix	70 F	600 gr
N° 13 Géométrie ou de la mesure de l'étendue	P. Lamy	52 F	395 gr
N°14 Algèbre	J.Peletier du Mans	36 F	291 gr

Le groupe M.:A.T.H.

(Mathématiques: Approche par les Textes Historiques)

vous propose:

La revue Mnémosyne pour échanger expériences et réflexions à propos de l'histoire et de l'enseignement des mathématiques.

Numéro 1 :	La démonstration par exhaustion chez les grecs et les arabes.	26 F	200 gr
Numéro 2 :	La querelle entre Descartes et Fermat.	30 F	210 gr
Numéro 3 :	Fragments d'étude des systèmes linéaires.	30 F	220 gr
Numéro 4-5 :	L'élaboration du calcul des variations et ses applications à la dynamique.	40 F	300 gr
Numéro 6 :	Leibniz et l'Ecole continentale.	30 F	220 gr
Numéro 7 :	Autour du théorème de Fermat : C. Goldstein	33 F	230 gr
Numéro 8 :	Isaac Newton. Détermination de tangentes à des courbes à l'aide de la méthode des fluxions.	33 F	250 gr
Numéro 9 :	Desargues et Pappus. R. Tossut	33 F	240 gr
Numéro 10 :	Le jeu des paradoxes dans l'élaboration des séries. A. Michel-Pajus	33 F	260 gr
Numéro 11 :	Des cartes-portulants à la formule d'Edward Wright. M.T. Gambin	33 F	255 gr
Numéro 12 :	Histoire de quelques projections cartographiques. M. Benedittini	33 F	255 gr
Numéro 13 :	Leibniz. Histoire et origine du calcul différentiel. A.Michel-Pajus	33 F	210 gr
Numéro 14 :	La méthode des pesées chez Archimède. M. Bathier –Fauvet	33 F	214 gr
Numéro 15 :	Recherche de deux grandeurs connaissant leur somme et leur produit. Odile Kouteynikoff	33 F	217 gr
Numéro 16	De la résolution des équations algébriques à l'émergence du concept de groupe. M. Buhler	33F	210 gr
Numéro spécial :	N° 1 : Histoire de Pyramides. M. Grégoire	46 F	380 gr

Nous vous indiquons le prix des brochures sans le port, le poids et le tarif postal pour calculer le coût du port.

Poids jusqu'à	Ordinaires
20 gr	3,00 F
50 gr	4,50 F
100 gr	6,70 F
250 gr	11,50 F
500 gr	16,00 F
1000 gr	21,00 F
2000 gr	28,00 F
3000 gr	33,00 F

✂----------

BON DE COMMANDE

Je désire recevoir les numéros suivants de Mnémosyne:

	Prix	port
n° 1		
n° 2		
n° 3		
n° 4		
n° 5		
n° 6		
n° 7		
n° 8		
n° 9		
n° 10		
n° 11		
n° 12		
n° 13		
n° 14		
n° 15		
n° spécial		

Total:

Nom:
Prénom:
Adresse:

Date:

Ci-joint un chèque d'un montant de
A l'ordre de l'Agent comptable de l'Université Denis Diderot Paris 7
Désirez-vous recevoir une facture? Oui Non