THÉORIE DE GALOIS

THÉORIE DE GALOIS

Cours et exercices corrigés

Jean-Pierre Escofier
Maître de conférences
à l'université Rennes 1

2e édition

DUNOD

11 rue Paul Bert, 92240 Malakoff

www.dunod.com

ISBN 978-2-10-082029-0

Table des matières

AVANT-PROPOS XV

CHAPITRE 1 • **DIFFÉRENTS ASPECTS HISTORIQUES DE LA RÉSOLUTION DES ÉQUATIONS ALGÉBRIQUES** 1

1.1 Calcul approché des racines d'une équation 1

1.2 Construction de solutions par intersections de courbes 2

1.3 Liens avec la trigonométrie 2

1.4 Problèmes de notation et de terminologie 2

1.5 Problème de la localisation des racines 4

1.6 Problème de l'existence des racines 4

1.7 Problème de la résolution algébrique des équations 5

CHAPITRE 2 • **HISTOIRE DE LA RÉSOLUTION DES ÉQUATIONS DE DEGRÉ 2, 3 OU 4 AVANT 1640** 7

2.1 Équations du second degré 7

2.1.1 Les Babyloniens 7

2.1.2 Les Grecs 9

2.1.3 Les Arabes 9

2.1.4 Usage des nombres négatifs 10

2.2 Équations du troisième degré 10

2.2.1 Les Grecs 10

2.2.2 Omar Khayyam et Sharaf al Din al Tusi 11

2.2.3 Scipio del Ferro, Tartaglia, Cardan 11

2.2.4 Résolution algébrique de l'équation du troisième degré 12
2.2.5 Premiers calculs avec les complexes 13
2.2.6 Raffaele Bombelli 14
2.2.7 François Viète 15
2.3 Équations du quatrième degré 15
EXERCICES 17
SOLUTIONS 20

CHAPITRE 3 • **POLYNÔMES SYMÉTRIQUES** 22
3.1 Polynômes symétriques 22
3.1.1 Rappel 22
3.1.2 Définitions 23
3.2 Polynômes symétriques élémentaires 24
3.2.1 Définition 24
3.2.2 Produit des $X - X_i$ et relations entre coefficients et racines 24
3.3 Polynômes symétriques et polynômes symétriques élémentaires 25
3.3.1 Théorème 25
3.3.2 Proposition 28
3.3.3 Proposition 28
3.4 Formules de Newton 28
3.5 Résultant de deux polynômes 31
3.5.1 Définition 31
3.5.2 Proposition 31
3.6 Discriminant d'un polynôme 33
3.6.1 Définition 33
3.6.2 Proposition 33
3.6.3 Formules 33
3.6.4 Polynômes à coefficients réels : racines réelles et signe du discriminant 34
EXERCICES 35
SOLUTIONS 39

CHAPITRE 4 • **EXTENSIONS DE CORPS** 44
4.1 Extensions de corps 44
4.1.1 Définition 44
4.1.2 Proposition 45
4.1.3 Degré d'une extension 45
4.1.4 Tour de corps 45

4.2 Formule de multiplicativité des degrés 45
4.2.1 Proposition 45
4.3 Extension engendrée 47
4.3.1 Proposition 47
4.3.2 Définition 47
4.3.3 Proposition 47
4.4 Éléments algébriques 48
4.4.1 Définition 48
4.4.2 Nombres transcendants 48
4.4.3 Proposition 48
4.4.4 Polynôme minimal d'un élément algébrique 49
4.4.5 Propriétés du polynôme minimal 49
4.4.6 Lien entre l'irréductibilité dans $\mathbb{Z}[X]$ et l'irréductibilité dans $\mathbb{Q}[X]$ 50
4.4.7 Méthodes pour prouver l'irréductibilité d'un polynôme de $\mathbb{Z}[X]$ 50
4.5 Extensions algébriques 52
4.5.1 Extension engendrée par un élément algébrique 52
4.5.2 Propriétés de $K[a]$ 52
4.5.3 Définition 53
4.5.4 Extensions de degré fini 53
4.5.5 Corollaire : tour d'extensions algébriques 53
4.6 Extensions algébriques par n éléments 53
4.6.1 Notation 53
4.6.2 Proposition 54
4.6.3 Corollaire 54
4.7 Construction d'une extension par adjonction de racine 54
4.7.1 Définition 55
4.7.2 Proposition 55
4.7.3 Corollaire 55
4.7.4 Propriété universelle de $\frac{K[X]}{(P)}$ 56
EXERCICES 57
SOLUTIONS 61

CHAPITRE 5 • **CONSTRUCTIONS À LA RÈGLE ET AU COMPAS** 69
5.1 Points constructibles 69
5.2 Exemples de constructions classiques 70
5.2.1 Projection d'un point sur une droite 70
5.2.2 Construction d'un repère orthonormé à partir de deux points 70
5.2.3 Construction de la parallèle à une droite passant par un point 71

5.3 Lemme 71
5.4 Coordonnées des points constructibles en une étape 72
5.5 Condition nécessaire de constructibilité 72
5.6 Deux problèmes vieux de plus de deux mille ans 73
5.6.1 Duplication du cube 73
5.6.2 Trisection de l'angle 73
5.7 Condition suffisante de constructibilité 74
EXERCICES 76
SOLUTIONS 79

CHAPITRE 6 • **K-HOMOMORPHISMES** 81
6.1 Nombres conjugués 81
6.2 K-homomorphismes 82
6.2.1 Définitions 82
6.2.2 Propriétés 82
6.3 Éléments algébriques et K-homomorphismes 83
6.3.1 Proposition 83
6.3.2 Exemple 84
6.4 Extensions de plongements dans $\mathbb{C}$ 84
6.4.1 Définition 84
6.4.2 Proposition 84
6.4.3 Proposition 86
6.5 Théorème de l'élément primitif 87
6.5.1 Théorème et définition 87
6.5.2 Exemple 88
6.6 Indépendance linéaire des K-homomorphismes 88
6.6.1 Caractère 88
6.6.2 Théorème (Emil Artin) 88
6.6.3 Corollaire : théorème de Dedekind 89
EXERCICES 90
SOLUTIONS 91

CHAPITRE 7 • **EXTENSIONS NORMALES** 93
7.1 Corps de décomposition 93
7.1.1 Définition 93
7.1.2 Corps de décomposition d'un polynôme du troisième degré 94

7.2 Extensions normales 94
7.3 Extensions normales et K-homomorphismes 95
7.4 Corps de décomposition et extensions normales 95
7.4.1 Proposition 95
7.4.2 Réciproque 96
7.5 Extensions normales et extensions intermédiaires 96
7.6 Clôture normale 97
7.6.1 Définition 97
7.6.2 Proposition 97
7.6.3 Proposition 97
7.7 Corps de décomposition, cas général 97
EXERCICES 99
SOLUTIONS 101

CHAPITRE 8 • **GROUPES DE GALOIS** 103
8.1 Groupes de Galois 103
8.1.1 Groupe de Galois d'une extension 103
8.1.2 Ordre du groupe de Galois d'une extension normale de degré fini 103
8.1.3 Groupe de Galois d'un polynôme 104
8.1.4 Groupe de Galois comme sous-groupe d'un groupe de permutations 104
8.1.5 Petite histoire de la notion de groupe 105
8.2 Corps des invariants 106
8.2.1 Définition et proposition 106
8.2.2 Théorème (Emil Artin) 106
8.3 Exemple de $\mathbb{Q}\left[\sqrt[3]{2}, j\right]$, première partie 107
8.4 Groupes de Galois et extensions intermédiaires 109
8.5 La correspondance de Galois 110
8.6 Exemple de $\mathbb{Q}\left[\sqrt[3]{2}, j\right]$, seconde partie 111
8.7 Exemple de $X^4 + 2$ 111
8.7.1 Groupes diédraux 111
8.7.2 Cas particulier de D_4 112
8.7.3 Groupe de Galois de $X^4 + 2$ 113
8.7.4 Correspondance de Galois 114
8.7.5 Recherche de polynômes minimaux 115
EXERCICES 116
SOLUTIONS 121

CHAPITRE 9 • **RACINES DE L'UNITÉ** 128

9.1 Groupe $U(n)$ des unités de l'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$ 128

9.1.1 Définition et rappel 128

9.1.2 Structure de $U(n)$ 129

9.2 Fonction de Möbius 129

9.2.1 Fonction multiplicative 129

9.2.2 Fonction de Möbius 130

9.2.3 Proposition 130

9.2.4 Formule d'inversion de Möbius 130

9.3 Racines de l'unité 131

9.3.1 Racines n-ièmes de l'unité 131

9.3.2 Proposition 131

9.3.3 Racines primitives 131

9.3.4 Propriétés des racines primitives 131

9.4 Polynômes cyclotomiques 132

9.4.1 Définition 132

9.4.2 Propriétés du polynôme cyclotomique 132

9.5 Groupe de Galois sur $\mathbb{Q}$ d'une extension de $\mathbb{Q}$ par une racine de l'unité 134

EXERCICES 136

SOLUTIONS 141

CHAPITRE 10 • **EXTENSIONS CYCLIQUES** 153

10.1 Extensions cycliques et abéliennes 153

10.2 Extensions par une racine et extensions cycliques 153

10.3 Irréductibilité de $X^p - a$ 154

10.4 Théorème 90 de Hilbert 155

10.4.1 Norme 155

10.4.2 Théorème 90 de Hilbert 155

10.5 Extensions par une racine et extensions cycliques : réciproque 156

10.6 Résolvantes de Lagrange 156

10.6.1 Définition 156

10.6.2 Propriétés 157

10.7 Résolution de l'équation du troisième degré 158

10.8 Résolution de l'équation du quatrième degré 159

10.9 Commentaire historique 161
EXERCICES 162
SOLUTIONS 164

CHAPITRE 11 • **GROUPES RÉSOLUBLES** 166
11.1 Première définition 166
11.2 Groupe dérivé ou groupe des commutateurs 167
11.3 Seconde définition 167
11.4 Exemples de groupes résolubles 168
11.5 Troisième définition 168
11.6 Simplicité de A_n pour $n \geqslant 5$ 169
11.6.1 Théorème 169
11.6.2 A_n non résoluble pour $n \geqslant 5$, preuve directe 170
11.7 Des résultats récents 170
EXERCICES 171
SOLUTIONS 174

CHAPITRE 12 • **RÉSOLUBILITÉ DES ÉQUATIONS PAR RADICAUX** 177
12.1 Extensions radicales et polynômes résolubles par radicaux 177
12.1.1 Extensions radicales 177
12.1.2 Polynôme résoluble par radicaux 178
12.1.3 Première construction 178
12.1.4 Seconde construction 178
12.2 Si un polynôme est résoluble par radicaux, son groupe de Galois est résoluble 179
12.3 Exemple de polynôme non résoluble par radicaux 179
12.4 Réciproque du critère fondamental 180
12.5 Équation générale de degré n 180
12.5.1 Éléments algébriquement indépendants 180
12.5.2 Existence d'éléments algébriquement indépendants 180
12.5.3 Équation générale de degré n 181
12.5.4 Groupe de Galois d'une équation générale de degré n 181
EXERCICES 183
SOLUTIONS 185

CHAPITRE 13 • **VIE D'ÉVARISTE GALOIS** 187

CHAPITRE 14 • **CORPS FINIS** 193

14.1 Corps algébriquement clos 193

14.1.1 Définition 193

14.1.2 Clôture algébrique 194

14.1.3 Théorème (Steinitz, 1910) 194

14.2 Exemples de corps finis 195

14.3 Caractéristique d'un corps 195

14.3.1 Définition 195

14.3.2 Propriétés 195

14.4 Propriétés d'un corps fini 196

14.4.1 Proposition 196

14.4.2 Homomorphisme de Frobenius 197

14.5 Existence et unicité d'un corps fini à p^r éléments 197

14.5.1 Proposition 197

14.5.2 Corollaire 198

14.6 Extensions de corps finis 198

14.7 Normalité d'une extension finie de corps fini 199

14.8 Groupe de Galois d'une extension finie de corps fini 199

14.8.1 Proposition 199

14.8.2 Correspondance de Galois 200

14.8.3 Exemple 200

EXERCICES 201

SOLUTIONS 208

CHAPITRE 15 • **EXTENSIONS SÉPARABLES** 216

15.1 Séparabilité 216

15.2 Exemple d'élément inséparable 217

15.3 Critère de séparabilité 217

15.4 Corps parfaits 218

15.5 Corps parfaits et extensions séparables 218

15.6 Extensions galoisiennes 218

15.6.1 Définition 218

15.6.2 Proposition 218

15.6.3 Correspondance de Galois 219

CHAPITRE 16 • **DEUX DÉVELOPPEMENTS RÉCENTS** 220

16.1 Le problème inverse de la théorie de Galois 220

16.1.1 Le problème 220

16.1.2 Le cas abélien 220

16.1.3 Exemple 221

16.2 Calculs de groupes de Galois sur $\mathbb{Q}$ pour des polynômes de petit degré 221

16.2.1 Simplifications du problème 221

16.2.2 Problème de l'irréductibilité 222

16.2.3 Plongement de G dans S_n 222

16.2.4 Recherche de G parmi les sous-groupes transitifs de S_n 222

16.2.5 Sous-groupes transitifs de S_4 223

16.2.6 Étude de $\Phi(G) \subset A_n$ 224

16.2.7 Étude de $\Phi(G) \subset D_4$ 224

16.2.8 Étude de $\Phi(G) \subset \dfrac{\mathbb{Z}}{4\mathbb{Z}}$ 225

16.2.9 Algorithme d'étude pour $n = 4$ 226

BIBLIOGRAPHIE 229

INDEX 235

Avant-propos

Ce livre commence par une esquisse de l'histoire ancienne (avant 1600) de l'étude des équations algébriques (chapitres 1 et 2). Après quelques résultats sur les polynômes symétriques (chapitre 3), la théorie de Galois est développée (chapitres 4, 6, 7 et 8) pour les extensions algébriques de degré fini contenues dans le corps $\mathbb{C}$ des complexes, pour rester dans un cadre connu. Le chapitre 8 présente ce qui est sans doute l'idée la plus profonde de Galois : la correspondance entre extensions et groupes. On lira aussi :

- une digression sur les constructions à la règle et au compas (chapitre 5),
- de belles applications (chapitres 9, 10),
- un critère de résolubilité par radicaux (chapitres 11, 12)

qui donnent à cette partie un aspect d'achèvement. De nombreux résultats peuvent être généralisés sans difficulté à des corps quelconques (au moins en caractéristique 0), ou adaptés aux extensions de degré infini.

La vie exceptionnelle d'Évariste Galois ne pouvait pas ne pas être évoquée (chapitre 13). Pour celle de Niels Abel, si émouvante à la fin, on se reportera à la bibliographie.

Suivent quelques indications sur les corps finis (chapitre 14) et sur les extensions séparables (chapitre 15). Le chapitre 16 présente des sujets de recherches actuelles. D'abord l'étude, dans un cas très simple, du problème inverse de la théorie de Galois : savoir si tous les groupes finis sont groupes de Galois d'extensions finies de $\mathbb{Q}$. Ensuite une méthode de calcul de groupes de Galois développable sur ordinateur.

Des exercices et des problèmes complètent la plupart des chapitres de ce cours. Certains énoncés rassemblent des exercices d'entraînement ou reprennent des textes d'examen ; d'autres proposent des résultats intéressants mais qui ne peuvent s'intégrer dans le corps du texte ; les solutions sont parfois détaillées, parfois rapides. Les solutions d'exercices abordant des domaines qu'il est impossible de traiter plus à fond ici sont assez souvent omises.

Le tout a été rédigé en pensant aux étudiants qui le liront et à ce dont ils se souviendront quelques années plus tard.

J'ai enfin donné quelques aperçus de l'histoire de la théorie. Je remercie la bibliothèque municipale de Rennes de m'avoir permis de reproduire quelques fragments de ses nombreux trésors.

De grands remerciements également à mes collègues Annette Houdebine-Paugam, qui m'a aidé à de nombreuses reprises, et Bernard Le Stum, ainsi qu'aux éditions Masson et Dunod ; ils ont relu les derniers états du texte en suggérant maintes corrections et transformations.

À BCDEF,

Jean-Pierre Escofier

Un ❑ marque la fin d'une démonstration.

Chapitre **1**

Différents aspects historiques de la résolution des équations algébriques

Dans ce chapitre, nous nous proposons de rappeler brièvement que l'étude des équations algébriques comporte de nombreux aspects et de donner un minimum de points de repère historiques pour chacun. Il faut toujours se rappeler que des notions, des techniques qui nous paraissent aller de soi ont souvent été conçues par les mathématiciens des siècles passés après de longs efforts ; pour le sentir, il faut s'imaginer avec leurs seules connaissances et méthodes. On trouvera dans la bibliographie les références de quelques textes anciens importants ainsi que des textes récents sur l'histoire de ces sujets (ouvrages de J.-P. Tignol, de H. Edwards, articles de C. Houzel).

1.1 CALCUL APPROCHÉ DES RACINES D'UNE ÉQUATION

Les Babyloniens donnaient déjà, vers 1600 av. J.-C., des valeurs approchées très précises des racines carrées. Par exemple, ils avaient calculé une valeur approchée à 10^{-6} près de $\sqrt{2}$: 1.24.51.10 en notation sexagésimale, c'est-à-dire $1+\frac{24}{60}+\frac{51}{60^2}+\frac{10}{60^3} = 1,41421296\ldots$; on connaît bien la méthode esquissée par Héron d'Alexandrie (vers 200) pour les obtenir à l'aide de la suite définie par $u_{n+1} = \frac{1}{2}\left(u_n + \frac{a}{u_n}\right)$.

Il n'est pas possible ici de détailler l'histoire des calculs approchés qu'effectuent les mathématiciens chinois (on trouve des calculs de racines cubiques dès 50 av. J.-C.) ou du monde

arabe. Notons cependant que la méthode de linéarisation d'Isaac Newton utilisant la suite $u_{n+1} = u_n - \dfrac{f(u_n)}{f'(u_n)}$ est déjà connue de l'Arabe Sharaf al Din al Tusi, né en 1201.

En 1225, Léonard de Pise donne 1.22.7.42.33.40 (en base 60) pour valeur approchée de la racine positive de l'équation $x^3 + 2x^2 + 10x = 20$, ce qui est une approximation à 10^{-10}, excellente ; nous ne savons comment il l'obtint.

1.2 CONSTRUCTION DE SOLUTIONS PAR INTERSECTIONS DE COURBES

Les Grecs pouvaient construire géométriquement toute solution positive d'une équation du second degré à l'aide d'intersections de droites et de cercles mais ils ne formulaient pas ce problème en termes algébriques. Nous y reviendrons au chapitre 5. Pour résoudre les équations du troisième degré, ils utilisaient des coniques, comme Omar Khayyam vers 1100 (voir 2.2.2), ce qu'Archimède (287- 212 av. J.-C.) avait peut-être déjà compris.

René Descartes, dans sa *Géométrie*, un des trois traités adjoints à son *Discours de la méthode* (1637), relie la résolution d'équations algébriques aux intersections de courbes algébriques. Ce thème est l'une des sources de la géométrie algébrique.

1.3 LIENS AVEC LA TRIGONOMÉTRIE

La division du cercle en un certain nombre de parties égales, ou cyclotomie (mot venant du grec), a fait l'objet de nombreuses études. Les mathématiciens du monde arabe ont mis en évidence (par exemple, en étudiant la construction du polygone régulier à 9 côtés, qui conduit à une équation du troisième degré) le lien, que François Viète (1540-1603) décrira aussi, entre la trisection d'un angle et la résolution d'une équation du troisième degré (voir Ex. 2.5). Viète donne également des formules exprimant $\sin n\theta$ et $\cos n\theta$ en fonction de $\sin\theta$ et de $\cos\theta$. Laurent Wantzel a montré (1837) que le problème posé par les Grecs, trisecter un angle quelconque à l'aide d'une règle et d'un compas, était impossible (voir 5.6).

Carl Friedrich Gauss, sans doute inspiré par des travaux d'Alexandre Vandermonde de 1770, a montré comment il était possible de résoudre algébriquement la division du cercle en p parties égales si p est un nombre premier de Fermat : $p = 17, 257, 65537$; il présente ses résultats dans la septième partie des *Disquisitiones arithmeticae* (*Recherches arithmétiques*) publiées en 1801, préparant la voie à Abel et à Galois.

1.4 PROBLÈMES DE NOTATION ET DE TERMINOLOGIE

Avant le XVI^{e} siècle, les mathématiciens n'utilisaient pas, sauf exception, de notations et on conçoit la difficulté de la mise en œuvre de méthodes algébriques dans ces conditions. Les usages actuels datent, en gros, de Descartes qui les impose dans sa *Géométrie*.

Donnons une idée des notations de Viète ; dans les *Zététiques* (1591, de $\zeta\eta\tau\varepsilon\iota\nu$, « chercher » en grec) l'expression :

$$\frac{F.H + F.D}{D + F} = E$$

est écrite :

$$\left\{\begin{array}{l} F \text{ in } H \\ +F \text{ in } B \\ \hline D + F \end{array}\right\} \quad \text{æquabitur } E$$

Pour les puissances de l'inconnue, Viète est encore très lourd ; il écrit *A* quadratum pour A^2, *A* cubus pour A^3, *A* quadrato-quadratum pour A^4, etc., et *A* potestas, *A* gradum pour A^m, A^n. Pour indiquer la dimension du paramètre *F*, il écrit *F* planum pour *F* de dimension 2, *F* solidum pour *F* de dimension 3, etc.

Par exemple, pour l'équation générale du second degré en *A*, Viète, qui suppose une homogénéité de dimension entre les variables et les paramètres *B*, *D*, *Z*, écrit :

B in *A* quadratum plus *D* plano in *A* æquari *Z* solido,

c'est-à-dire $BA^2 + DA = Z$.

Cette condition d'homogénéité ne sera définitivement abandonnée qu'au temps de Descartes (voir 5.7). Le grand apport de Viète est la création du calcul avec des lettres pour les quantités connues ou inconnues (*logistice speciosa* par opposition à la *logistice numerosa*) ; il transforme par là profondément les méthodes et la conception de l'algèbre : au lieu de travailler sur des exemples numériques, on écrit le cas général. L'économie de pensée, les nouvelles possibilités de comprendre une situation vont permettre les progrès ultérieurs. Certains avant lui avaient déjà utilisé des lettres mais sans calculer avec, notant une quantité par une lettre, son carré par une autre, etc.

Rappelons que Viète était connu à son époque comme conseiller de Henri III et qu'il a été conseiller du Parlement de Bretagne à Rennes (où j'écris) de 1573 à 1580.

Donnons quelques dates marquantes de l'histoire des notations algébriques.

Les décimaux sont introduits par Al Uqlidisi, l'*Euclidien* (vers 950), Al Kashi (1427), Viète (1579), Simon Stevin (1585). C'est John Neper qui répand l'usage du point pour séparer les parties entière et fractionnaire (en France, nous utilisons une virgule). Mais on écrira longtemps encore l'entier avec, à sa suite, la fraction donnant la partie fractionnaire : $11\,\frac{224\,176}{1\,000\,000}$.

Les signes + et − existent vers 1480 (+ serait une déformation de &) mais leur usage ne se généralise qu'au début du XVII^{e} siècle ; la multiplication est notée M par Michael Stifel (1545), *in* par Viète (1591) ; nos usages datent de William Oughtred (1637) pour ×, de Wilhelm Leibniz (1698) pour le point.

Pour les puissances de l'inconnue, $1\,225 + 148\,x^2$ est écrit $1\,225\widetilde{p}\,148^2$ par Nicolas Chuquet (1484), $3x^2$ est écrit $3^{\underline{2}}$ par Rafaelle Bombelli (1572), tandis que Stevin écrit 3 ③+5 ②−4 ① pour $3x^3 + 5x^2 - 4x$. L'écriture exponentielle x^2, x^3, etc., s'impose avec Descartes dont les formules sont écrites dans une forme très proche de la nôtre. Au XVIII^{e} siècle, on écrit *bb* pour b^2 mais b^3, b^4, etc.

C'est seulement quand le calcul littéral et la notation exponentielle ont été bien mis au point qu'il a été possible de penser clairement le calcul sur les polynômes (c'est Descartes qui

montre qu'un polynôme s'annule en a si et seulement s'il est divisible par $X - a$). L'histoire de la façon de parler de l'inconnue, de la noter est très complexe et ne sera pas décrite ici. Le signe =, qui apparaît chez Michel Recorde (1557), prend le pas sur le signe de Descartes (un alpha renversé : ɷ) à la fin du XVII^{e} siècle, grâce à Leibniz. Albert Girard (1595-1632) introduit la notation $\sqrt[3]{\ }$ qu'il substitue à $\left(\frac{1}{3}\right)$, les abréviations pour sinus et tangente et emploie les signes $<$, $>$ comme Harriot. Les indices sont introduits par Gabriel Cramer (1750) pour écrire ses célèbres formules (les $'$, $''$, $'''$ suivis par ^{iv}, ^{v}, etc. deviennent usuels à la même époque), les indices d'indices sont introduits par Galois. Le signe $\sum$ est introduit par Leonhard Euler (1707-1783). L'usage de ces dernières notations ne s'est généralisé qu'au cours du XX^{e}siècle.

1.5 PROBLÈME DE LA LOCALISATION DES RACINES

Le problème est posé pour des polynômes à coefficients réels. Les résultats de Descartes basés sur le nombre de changements de signe dans la suite des coefficients (voir Ex. 3.7), sont perfectionnés au XIX^{e}siècle par Jean-Baptiste Fourier et François Budan puis par Charles Sturm qui donne, en 1830, un algorithme permettant de déterminer le nombre de racines réelles dans un intervalle donné.

1.6 PROBLÈME DE L'EXISTENCE DES RACINES

Al Khwarizmi (vers 830) semble être le premier à signaler les équations du second degré qui admettent deux racines strictement positives (voir cependant 2.1.1). Les racines négatives ne seront prises en considération qu'à la fin du XVI^{e} siècle (voir 2.1.4).

Girard est le premier à affirmer qu'une équation de degré (de *dénomination* dit-il) n a n racines (Fig. 1.1). Il ne donne aucune démonstration et ses idées sont floues sur la nature des solutions, qui peuvent être des nombres complexes *ou autres nombres semblables*. Ce flou ne l'empêche pas d'innover en calculant avec les racines comme si c'étaient des nombres (voir 3.4). Tout mathématicien appréciera cette merveilleuse formulation :

« pour la certitude de la reigle generale ».

Descartes sera moins précis sur le nombre de racines, le bornant par le degré de l'équation : « Autant que la quantité inconnue a de dimensions, autant *peut-il* y avoir de diverses racines. »

La nature des racines échappe encore à Leibniz qui ne voit pas que $\sqrt{\sqrt{-1}}$ est un nombre complexe (1702). Mais les méthodes d'intégration des fractions rationnelles, que Leibniz et Jean Bernoulli mettent au point à cette époque, conduisent Euler au problème de montrer qu'une équation algébrique $P(x) = 0$, où P est un polynôme de degré n à coefficients réels, possède n racines réelles ou complexes (1749 : *Recherches sur les racines imaginaires des équations*).

Ce théorème est appelé, en France seulement, théorème de d'Alembert, celui-ci en ayant proposé une démonstration intéressante, mais incomplète, en 1746. Pierre Simon de Laplace, dans ses cours à l'École normale de l'an III, en donne une démonstration élégante en admettant l'existence de racines *quelque part*. Gauss le prouve de façon satisfaisante à quatre