maurice mignotte

mathématiques pour le calcul formel

puf
MATHÉMATIQUES

MATHÉMATIQUES

Mathématiques pour le calcul formel

MAURICE MIGNOTTE

Professeur à l'Université Louis-Pasteur
Strasbourg

PRESSES UNIVERSITAIRES DE FRANCE

COLLECTION DIRIGÉE PAR PAUL DEHEUVELS

ISBN 2 13 042259 4
ISSN 0246-3822

Dépôt légal — 1re édition : 1989, avril

© Presses Universitaires de France, 1989
108, boulevard Saint-Germain, 75006 Paris

SOMMAIRE

INTRODUCTION 11

CHAPITRE PREMIER / *Arithmétique élémentaire* 13

1. Représentation d'un entier en base b 13

1.1. Ordre lexicographique 13
1.2. Développement en base b, existence 14
1.3. Le passage développement $\rightarrow$ nombre 16
1.4. Le passage nombre $\rightarrow$ développement en base b 17
1.5. Cas des nombres de signe quelconque 21
1.6. Comparaison de deux nombres 21

2. Addition 23

2.1. Cas de deux nombres positifs 23
2.2. Cas de deux nombres de signe quelconque 25

3. Soustraction 26

4. Multiplication 27

5. Division euclidienne 30

5.1. Existence 30
5.2. Calcul 31

6. Le coût de la multiplication et de la division 34

6.1. Le coût de la multiplication 34
6.2. Le coût de la division 37

7. Le calcul de x^n 39

7.1. Premier algorithme 39
7.2. Second algorithme 40
7.3. Une application 44
7.4. Complexité du problème 45

8. Le p.g.c.d. 47
8.1. Existence. Relation de Bézout. Théorème d'Euclide-Gauss.. 47
8.2. Caldul du p.g.c.d..... 49
8.3. Le coût de l'algorithme d'Euclide 51
9. Le groupe G(n) 53
9.1. Définition..... 53
9.2. Le théorème d'Euler 54
9.3. Calcul de l'inverse d'un élément 55
9.4. Calcul des coefficients de la relation de Bézout 56
10. Le théorème chinois 58
10.1. Le théorème 58
10.2. Démonstration constructive 60
10.3. Calculs effectifs 61
11. Les nombres premiers 62

CHAPITRE II / *Arithmétique, compléments* 72
1. Retour à G(n) 72
1.1. Quelques lemmes sur les groupes finis 72
1.2. Application à G(p) 76
1.3. Structure de G(p^k), $k \geqslant 2$, p premier impair 78
1.4. Structure de G(2^k) 80
1.5. Structure de G(n) 81
2. Tests de primalité 83
2.1. Un théorème général 83
2.2. Un critère de primalité 88
2.3. Tests élémentaires 89
2.3.1. Le test de Solovay-Strassen 89
2.3.2. Le test de Miller-Rabin 89
2.3.3. Etude des coûts 90
2.4. Statistique sur G(n)..... 91
3. Factorisation des entiers 93
3.1. Méthode par divisions successives 93
3.2. Méthode de Fermat 95
3.3. Méthode de Sherman-Lehmann 95
3.4. Méthode ρ de Pollard 97

CHAPITRE III / *Polynômes, étude algébrique* 104
1. Définitions et propriétés élémentaires 104
1.1. Premières définitions 104
1.2. Opérations arithmétiques élémentaires 105
1.3. Notions de degré 106
1.4. Cas d'un anneau intègre 107

2. La division euclidienne 108

2.1. Polynômes unitaires 108
2.2. La division euclidienne 108
2.3. Cas d'un corps 109
2.4. Pseudo-division 112

3. Le théorème chinois 113

4. Factorisation 116

4.1. Cas d'un corps 116
4.2. Cas d'un anneau factoriel 117

5. Fonctions polynômes 121

5.1. Définition 121
5.2. Racines d'un polynôme 122
5.3. Multiplicité d'une racine 122
5.4. Dérivées et racines 124
5.5. Formule de Taylor 125

6. Le résultant 126

CHAPITRE IV / *Polynômes à coefficients complexes* 149

1. Le théorème de d'Alembert 149

1.1. Enoncé 149
1.2. Propriétés analytiques utilisées 149
1.3. Démonstration du théorème 151
1.4. Polynômes réels irréductibles 152

2. Estimations des racines 153

2.1. Principe de démonstration 153
2.2. Un lemme analytique 154
2.3. Majorations des racines 154

3. La mesure d'un polynôme 158

3.1. Définition 158
3.2. Un lemme algébrique 160
3.3. Une majoration de M(P) 160
3.4. Autres majorations 162
3.5. Résultats analytiques 163
3.6. Une méthode de calcul de M(P) 164
3.7. Un exemple d'évaluation de M(P) 166

4. Majoration de la taille des facteurs d'un polynôme 168

4.1. Définitions 168
4.2. Majoration des facteurs, le cas d'une seule variable 169
4.3. Définition de la mesure dans le cas de plusieurs variables ... 169
4.4. Majoration des facteurs d'un polynôme, cas de plusieurs variables 171
4.5. Un exemple dans le cas d'une variable 173

5. Sur la répartition des racines d'un polynôme 175
5.1. Majoration du nombre de racines réelles 175
5.2. Sur la répartition des arguments des racines d'un polynôme. 177
6. Séparation des racines d'un polynôme 178
6.1. Notations 178
6.2. Une première minoration de sep (P) 178
6.3. Autres minorations de la distance entre deux racines 180
6.4. Utilisation de propriétés galoisiennes 181
6.5. Un exemple 183

CHAPITRE V / *Polynômes à coefficients réels* 196
1. Polynômes irréductibles sur **R** 196
2. Le théorème de Rolle 197
2.1. Le théorème des valeurs intermédiaires 197
2.2. Le théorème de Rolle 198
3. Estimations des racines réelles 200
3.1. La règle de Newton 200
3.2. Règles de Lagrange et Mac Laurin 200
3.3. Un cas particulier de la règle de Descartes 201
3.4. La règle de Cauchy 201
3.5. Un exemple d'estimation des racines 202
4. Sur le nombre de zéros d'un polynôme dans un intervalle . 203
4.1. La règle de Sturm 203
4.2. Le théorème de Budan-Fourier 206
4.3. La règle de Descartes 208
4.4. Cas des polynômes dont toutes les variables sont réelles ... 209
4.5. Un exemple détaillé 211
4.6. Le théorème de Vincent 214
5. Equations dont toutes les racines ont une partie réelle négative 223

CHAPITRE VI / *Polynômes sur un corps fini* 242
1. Corps finis 242
1.1. Résultats généraux 242
1.2. Les opérations dans un corps fini 244
1.3. Détermination d'un élément primitif de $\mathbf{F}_{q^*}$ 246
1.4. Détermination de z tel que $\mathbf{F}_q = \mathbf{F}_p[z]$ 247
1.5. Un exemple : $\mathbf{F}_8$ 248
2. Statistiques sur $\mathbf{F}_q[X]$ 249
2.1. La fonction de Möbius 249
2.2. Calcul de I_n 250
2.3. Nombre de polynômes quadratfrei 251
2.4. Etude du nombre de facteurs irréductibles d'un polynôme ... 252

3. Factorisation d'un polynôme en produit de polynômes quadratfrei 255
3.1. Définitions et généralités 255
3.2. Cas de la caractéristique zéro 256
3.3. Cas de la caractéristique non nulle 257
3.4. Algorithmes de décomposition quadratfrei d'un polynôme.. 258

4. Factorisation des polynômes sur un corps fini 262
4.1. Détermination du nombre de facteurs irréductibles 262
4.2. Factorisation complète 265
4.3. Coût de l'algorithme 267
4.4. Cas où q est grand 268
4.5. Décomposition en produit de facteurs irréductibles de degré donné 271
4.6. La méthode de Mac Eliece 272

5. Recherche des racines d'un polynôme dans un corps fini.... 274
5.1. Une première réduction 274
5.2. Cas des polynômes qui se décomposent dans $\mathbf{F}_q$ 274
5.3. Résolution de l'équation binomiale $X^d = a$ 276

CHAPITRE VII / *Polynômes à coefficients entiers* 305

1. Principe des algorithmes de factorisation des polynômes à coefficients entiers 305
1.1. Existence d'un algorithme de factorisation 305
1.2. L'algorithme de Kronecker 306
1.3. Le principe des algorithmes modernes 308

2. Le choix du module p 309

3. Raffinement de la factorisation 310
3.1. La borne B 310
3.2. Le lemme de Hensel 312

4. Factorisation dans $\mathbf{Z}[X]$, la méthode de Berlekamp 316

5. L'algorithme L^3 318
5.1. Réseaux 318
5.2. Orthogonalisation de Gram-Schmidt 318
5.3. Bases réduites 319
5.4. Algorithme de réduction 322
5.5. Coût de l'algorithme 323

6. Facteurs des polynômes et réseaux 325

7. L'algorithme de factorisation 332

INDEX 340

Introduction

Ce livre correspond à un cours que j'ai donné en 1986-1987 à Strasbourg dans le cadre du DEA de mathématiques. Comme son titre l'indique, il s'agit d'un ouvrage de mathématiques. Je m'adresse à des lecteurs qui possèdent un niveau équivalant à celui de la licence de mathématiques, celui du DEUG devrait même suffire. A dire vrai, les notions utilisées implicitement sont assez limitées ; ce sont les conventions de la théorie des ensembles, la donnée des entiers naturels, des rudiments de combinatoire (peut-être seulement la formule du binôme de Newton), de l'analyse au niveau de la terminale des lycées ainsi qu'un peu d'algèbre : notions de groupe, d'anneau et de corps, quelques résultats élémentaires en algèbre linéaire. La quasi-totalité de ces résultats d'algèbre et de combinatoire figure dans mon livre Algèbre appliquée à l'informatique, *paru aux PUF en 1987, et qui est destiné aux étudiants du DEUG.*

La part consacrée aux algorithmes est relativement faible, mais les algorithmes les plus importants du calcul formel sont présentés dans l'excellent ouvrage de J. Davenport, Y. Siret et E. Tournier, Introduction au calcul formel, *paru chez Masson en 1987.*

Par contre, les exercices qui figurent à la fin de chaque chapitre prennent une place importante. Ce ne sont que rarement des applications directes du cours. Très souvent, ils constituent des compléments à ce cours que je n'ai pas voulu traiter en détail dans le texte, afin de ne pas trop l'alourdir et de conserver à cet ouvrage une taille raisonnable. En général, les indications suggérées ou les références fournies permettront facilement au lecteur de reconstituer les démonstrations.

La première partie du cours — les deux premiers chapitres — porte sur des résultats élémentaires en arithmétique ; par exemple l'algorithme d'Euclide, le théorème chinois, le théorème de Fermat... Presque tous ces résultats étaient naguère enseignés dans la classe de terminale C. C'est, d'une part, l'occasion d'étudier les opérations arithmétiques sur les grands entiers et, d'autre part, une introduction concrète aux notions d'algèbre utilisées dans les chapitres suivants (par exemple anneaux euclidiens,

principaux...). Un détail qui précise le niveau de cette introduction à l'arithmétique : la loi de réciprocité quadratique n'est pas démontrée, elle n'est indiquée qu'en exercice.

La seconde et dernière partie, qui s'étend sur cinq chapitres, est construite pour mener à un algorithme de factorisation des polynômes à coefficients entiers. Ce long chemin commence par la présentation des résultats algébriques généraux sur des polynômes généraux sur un anneau.

Ensuite, on étudie les polynômes à coefficients complexes ; en particulier, on démontre un certain nombre d'inégalités sur les racines ou les facteurs d'un polynôme à coefficients complexes, inégalités qui sont très utiles par la suite.

Le chapitre suivant est consacré aux polynômes à coefficients réels. Le thème principal de cette étude est la séparation des racines réelles d'un polynôme. On y présente des résultats anciens, qui sont difficiles à trouver dans les ouvrages récents : méthode de Sturm, règles de Descartes et de Budan-Fourier, théorème de Vincent. Ces travaux sont fondamentaux dans le domaine de la géométrie réelle, domaine actuellement en pleine activité.

Le sixième chapitre porte sur les polynômes à coefficients dans un corps fini. Pour le but que nous poursuivons, il s'agit d'un chapitre essentiel du fait qu'il contient l'algorithme de Berlekamp de factorisation des polynômes à coefficients dans un corps fini. Cet algorithme constitue la première étape des algorithmes modernes de factorisation des polynômes à coefficients entiers. Les exercices de ce chapitre doivent beaucoup au livre très complet de R. Lidl et H. Niederreiter, Finite Fields, *Addison Wesley, paru en 1983.*

Au dernier chapitre, on donne donc des méthodes de factorisation des polynômes à coefficients entiers. L'effort essentiel porte sur l'algorithme de Lenstra-Lenstra-Lovácz. Cet algorithme utilise plusieurs des résultats obtenus dans les chapitres antérieurs.

Dans tout ce cours, je me suis inspiré avant tout de l'ouvrage remarquable et extrêmement documenté de Knuth, The Art of Programming, *vol. 2 (seconde édition), Addison Wesley.*

La frappe a été réalisée entièrement par l'auteur sur ordinateur Macintosh Plus, grâce aux logiciels World et MacΣqn. La sortie a été effectuée sur imprimante laser Apple.

Ce texte a été relu par Eric Domenjoud, Philippe Glesser, Catherine Mignotte et Guy Viry ; je les remercie vivement pour leur patience et pour m'avoir signalé de nombreuses erreurs de frappe. J'adresse aussi des remerciements tout particuliers à mes collègues James Davenport et François Gramain qui ont apporté de nombreuses corrections et améliorations au manuscrit.

CHAPITRE PREMIER

Arithmétique élémentaire

Ce chapitre traite du codage des nombres entiers et, à partir de là, présente les algorithmes de base en arithmétique (addition, multiplication, division ...) . L'étude de ces exemples permet d'introduire la notion fondamentale de coût d'un algorithme.

1. Représentation d'un entier en base b .

1. Ordre lexicographique .

Afin de présenter le résultat fondamental sur l'écriture des entiers dans une base donnée, rappelons la définition de l'**ordre lexicographique** .

Soient $E_1, \ldots, E_r$ des ensembles ordonnés, on considère sur l'ensemble produit

$$E = E_1 \times \ldots \times E_r$$

la relation R suivante entre éléments $(x_1, \ldots, x_r)$ et $(y_1, \ldots, y_r)$ appartenant à E :

" pour le plus petit indice i tel que $x_i \neq y_i$ on a $x_i < y_i$ " .

On vérifie aussitôt que R est une relation d'ordre, on l'appelle l'ordre lexicographique sur E (c'est - comme son nom l'indique - l'ordre de classement des mots d'un dictionnaire).

L'ensemble E , muni de cette relation d'ordre, est appelé le **produit lexicographique** des ensembles E_i. Lorsque chacun des ensembles E_i est totalement ordonné, leur produit lexicographique E est aussi totalement ordonné.

2. Développement en base b, existence .

Le résultat fondamental de ce paragraphe est le théorème suivant, qui est évidemment bien connu mais qui est aussi très utile pour le calcul sur les grands entiers.

THEOREME 1 . – Soit b un entier > 1. Pour k entier strictement positif, soit E_k le produit lexicographique de k ensembles égaux à l'ensemble $\mathbf{B} = \{ 0, 1, \ldots , b - 1 \}$.

L'application

$$f_k : (r_0 , r_1 , \ldots , r_{k-1}) \rightarrow \sum_{i=0}^{k-1} r_i \, b^{k-i-1}$$

est un isomorphisme de l'ensemble ordonné E_k sur l'intervalle $\{ 0, 1, \ldots, b^k - 1 \}$.

> On raisonne par récurrence sur l'entier k . Il est d'abord facile de vérifier que l'image de l'application f_k est contenue dans l'intervalle $\{ 0, 1, \ldots b^k - 1 \}$. Ensuite, on vérifie que f_k est strictement croissante. D'où la conclusion ... Les détails sont laissés au lecteur.<

Pour tout entier naturel strictement positif a , il existe un plus petit entier $k > 0$ tel que $a < b^k$ et, d'après le théorème, il existe une suite finie et une seule $(r_0, \ldots , r_{k-1})$ telle que les r_i appartiennent tous à l'intervalle $\mathbf{B} = \{ 0, 1, \ldots , b - 1 \}$ et que l'on ait l'expression suivante de a

$$a = \sum_{i=0}^{k-1} r_i \, b^{k-i-1} ;$$

en outre, on a nécessairement $r_0 > 0$ (sans quoi on aurait $a < b^{k-1}$) .

On dit que l'expression précédente est le **développement en base b** de l'entier a et on écrit parfois

$$a = (r_0 , r_1 , \ldots , r_{k-1}) ,$$

ou encore

$$a = (r_0 \, r_1 \ldots r_{k-1})_b \; ;$$

les entiers r_i sont appelés les **chiffres** de a en base b (en anglais *digits*) .

Remarque : Les chiffres du développement de a en base b peuvent aussi parfois être considérés seulement comme des symboles d'un alphabet - l'alphabet **B** - et la seconde écriture comme un mot sur cet alphabet, ou encore une liste de nombres. Cette dernière interprétation est celle utilisée dans les systèmes de calcul formel qui sont écrits en langage LISP .

Exemples :

- Dans la vie courante, on utilise le système décimal pour lequel b est égal à dix.
- Comme chacun le sait, les ordinateurs travaillent avec des nombres représentés en binaire, c'est à dire en base deux. La raison principale de ce choix est que le développement en base deux ne nécessite que deux chiffres (qui correspondent à deux états possibles d'une unité de mémoire). Par ailleurs les opérations arithmétiques élémentaires sont particulièrement simples en base deux.
- Pour le calcul sur des entiers de taille arbitraire, il est commode de travailler avec une base b dont la valeur est proche du maximum permis par la taille du mot de la machine (par exemple si le mot d'une machine comporte seize bits, on peut prendre une base b avec $b \leq 2^{15}$) .

L'estimation suivante d'un entier en fonction de son écriture en base b est très utile.

PROPOSITION 1. – Si l'entier positif n admet le développement en base b,

$$n = \sum_{i=0}^{k} a_i\, b^i \qquad \text{avec} \quad a_k \neq 0$$

alors on a

$$b^k \leq a_k\, b^k \leq n \leq b^{k+1} - 1 .$$

> La seule inégalité non triviale est la dernière. Elle se démontre ainsi

$\forall i,\ a_i \leq b-1 \Rightarrow$ $n \leq (b-1) \times (1 + b + \ldots + b^k) = b^{k+1} - 1$. <

3. Le passage développement $\rightarrow$ nombre.

Pas de problème, la transformation est

$$f_k : (r_0, r_1, \ldots, r_{k-1}) \rightarrow \sum_{i=0}^{k-1} r_i\, b^{k-i-1}$$

donnée dans le théorème.

Ainsi, par exemple,

$$\begin{aligned}(1101110)_2 &= 2^6 + 2^5 + 2^3 + 2^2 + 2^1 \\ &= (64)_{\text{dix}} + (32)_{\text{dix}} + 8 + 4 + 2 \\ &= (110)_{\text{dix}} = 110 = \text{cent dix}.\end{aligned}$$

On peut aussi représenter cette transformation par un **algorithme,** c'est à dire un processus de calcul (écrit ici dans un langage sommaire) .

algorithme développement - nombre ;

données : b, k, r_0 , ... , r_{k-1} entiers ≥ 0 ;

n := r_0 ;

pour i := 1 **à** k-1 **faire** n := n b + r_i .#

4. Le passage nombre $\rightarrow$ développement en base b .

La formule

$$a = \sum_{i=0}^{k-1} r_i \, b^{k-i-1}$$

conduit à la relation

$$a = b\,q + r_{k-1} \quad ,$$

où

$$0 \leq r_{k-1} < b \, ,$$

qui montre que r_{k-1} est le reste de la division euclidienne de a par b , ce qu'on écrira

r_{k-1} = a mod b (on lit " a modulo b ") .

De plus l'entier q , le quotient (que l'on note aussi q = a div b) , est donné par la formule

$$q = \sum_{i=0}^{k-2} r_i \, b^{k-i-2} ,$$

d'où l'on déduit la valeur de r_{k-2} ,

$$r_{k-2} = q \bmod b ,$$

et ainsi de suite ....

D'où un procédé de fabrication du développement d'un entier a dans une base b qui peut être décrit symboliquement sous la forme

dev (a ; b) = (dev (a div b ; b) , a mod b) ,

ce qui conduit à une définition récursive d'un algorithme pour ce développement.

L'algorithme itératif correspondant est le suivant.

algorithme nombre-développement 1 ;

données : a entier > 0 , b entier ≥ 2 ;
i := 0 ; n := a ;
tant que n > 0 **faire**
début
x[i] := n **mod** b ;
i := i + 1 ;
n := n **div** b { **div** désigne la division entière}
fin . #

Faisons "tourner" cet algorithme sur un exemple : $a = 67$, $b = 3$. Le déroulement peut être représenté par le tableau suivant.

i	n	x
0	67	1
1	22	1
2	7	1
3	2	2
4	0	

Ce qui montre que

$$67 = (2111)_3$$

(en effet , $2 \times 27 + 9 + 3 + 1 = 67$) .

On peut aussi déterminer le développement en base b en calculant d'abord les chiffres de poids le plus élevé, à savoir r_0 , puis r_1 , puis r_2 ...

Ce second algorithme peut être décrit de la manière suivante.

```
algorithme nombre - développement 2 ;
    données : a entier > 0 , b entier ≥ 2 ;
    # k := 0 ; x := b ; n := a ;
    tant que a ≥ x faire
                    début
                    k := k + 1 ; x := x b
                    fin ;
    x := x div b ;
    pour i := 0 à k faire
        début
        r[i] := n div x ; n := n mod x ; x := x div b
        fin . #
```

Sur l'exemple de la recherche du développement ternaire du nombre 67 , on trouve d'abord k = 3 , puis le déroulement suivant

i	n	x	r
0	67	27	2
1	13	9	1
2	4	3	1
3	1	1	1

qui redonne bien $67 = (2111)_3$.

5. Cas des nombres de signe quelconque .

Pour coder un nombre entier n quelconque non nul, il suffit de noter son signe et sa valeur absolue :

si $|n| = (a_m \ldots a_0)_B$, on pose

$$\text{code}_B(n) = (\varepsilon, a_m, \ldots, a_0) ,$$

où

ε = si $n > 0$ alors '+' sinon '-' .

On définit la fonction signe d'un nombre entier n par les conditions

$$\text{signe}(n) = \begin{cases} +1 & \text{si } n > 0 , \\ 0 & \text{si } n = 0, \\ -1 & \text{si } n < 0 . \end{cases}$$

6. Comparaison de deux nombres .

On ne considérera que la comparaison entre deux nombres positifs, le cas général s'en déduit sans difficulté.

Soient donc deux nombres positifs a et b , où

$$a = (a_m \ldots a_0)_B \quad \text{et} \quad b = (b_n \ldots b_0)_B ,$$

avec comme d'habitude a_m et b_n non nuls.

Ce test de comparaison est une conséquence directe du théorème 1 .

On suppose que l'ordinateur sait comparer deux entiers dont la valeur absolue ne dépasse pas 2^k, et qu'il possède une fonction signe ainsi que l'opération de soustraction définie pour ces entiers. En outre, on suppose que les entiers B , m et n sont tous majorés par 2^k, ces restrictions n'ayant aucun inconvénient dans la pratique.

L'algorithme de comparaison entre a et b peut alors s'écrire comme suit.

algorithme comparaison entre deux entiers positifs ;

données : $a = (a_m \ldots a_0)_B$, $a_m \neq 0$, $b = (b_n \ldots b_0)_B$, $b_n \neq 0$;
{ la réponse est r = signe (a - b) }
si $m \neq n$ **alors** r := **signe** (m - n)
sinon **début**
i := m ;
tant que $a_i = b_i$ **faire** i := i - 1 ;
si i = -1 **alors** r := 0 **sinon** r := **signe** $(a_i - b_i)$
fin .#

2. Addition .

1. Cas de deux nombres positifs .

Soient deux nombres entiers positifs a et b écrits en base B, de longueurs respectives m et n . On veut calculer leur somme c . Supposons que

$$a = \sum_{i=0}^{m-1} a_i B^i \quad \text{et} \quad b = \sum_{i=0}^{n-1} b_i B^i \ .$$

On a par exemple $m \geq n$ et on peut écrire

$$b = \sum_{i=0}^{m-1} b_i B^i \ ,$$

avec $b_n = \ldots = b_{m-1} = 0$.

Ainsi,

$$c = \sum_{i=0}^{m-1} (a_i + b_i) B^i \ ,$$

mais, en général, ceci ne fournit pas l'écriture

$$c = \sum_{i=0}^{m} c_i B^i$$

de c en base B , il faut faire attention aux retenues !

Appelons r la retenue à un instant donné, on a l'algorithme suivant.

Algorithme somme en base B ;

données : $a = (a_{m-1} \ldots a_0)_B$, $a > 0$, $b = (b_{n-1} \ldots b_0)_B$, $b > 0$;

\# $r := 0$; $k := m-1$;

pour $i := 0$ **à** $m-1$ **faire**

début

$s := a_i + b_i + r$;

si $s < B$ **alors** **début** $c_i := s$; $r := 0$ **fin**

sinon **début** $c_i := s - B$; $r := 1$ **fin**

fin ;

si $r > 0$ **alors** **début** $k := m$; $c_m = 1$ **fin** . \#

Exercice : Démontrer que cet algorithme est correct.

Remarque : Comme l'algorithme le laisse supposer, la retenue ne peut valoir que 0 ou bien 1 ; en effet on a toujours

$$a_i + b_i \leq 2B - 2 .$$

Il est naturel de choisir pour coût de l'algorithme précédent le nombre d'opérations élémentaires (c'est à dire portant sur des entiers plus petits que B), ce coût est très facile à estimer : il est en $O (\max \{ m, n \})$.

Remarque : On ne peut remplacer cette borne par $O(\min\{m,n\})$ en raison de la propagation éventuelle de la retenue, comme dans la somme

$$\sum_{i=0}^{m-1} (B-1)B^i + 1 = B^m .$$

Exercice : Etant donnés deux nombres positifs a et b, codés en base B comme plus haut, évaluer la probabilité pour que la retenue se propage jusqu'au rang k, où k vérifie $n-1 \leq k \leq m-1$. En déduire une étude statistique du coût de l'algorithme de somme de deux entiers.

2. Cas de deux nombres de signe quelconque.

Soient a et b deux entiers codés en base B dont on veut calculer la somme c. Excluons le cas trivial où l'un au moins de ces deux nombres est nul.

Si a et b ont le même signe alors

$$c = \text{signe}(a).(|a|+|b|)$$

et il n'y a pas de problème.

Si a et b sont de signe contraire, on a les deux cas suivants

- si $|a| \geq |b|$ alors

  $c = \text{signe}(a).(|a|-|b|)$,

- si $|a| < |b|$ alors

  $c = \text{signe}(b).(|b|-|a|)$.

Pour être capable de calculer c il suffit donc de savoir

1°) comparer $|a|$ et $|b|$,

2°) calculer la différence de deux entiers positifs a' et b' , où $a' > b'$.

Ayant déjà vu comment on peut effectuer la première de ces opérations, il suffit d'étudier comment réaliser la seconde. Cette fois encore la seule question est de tenir compte des retenues. L'algorithme ci-dessous effectue cette opération.

algorithme différence de deux entiers positifs ;

données : $a = (a_m \ldots a_0)_B$, $b = (b_m \ldots b_0)_B$, $a > b > 0$;

{ on suppose $a_m > 0$ mais seulement $b_m \geq 0$, comme plus haut }

k := 0 ;

pour j := 0 **à** m **faire**

début

s := a_j - b_j + k

si s ≥ 0 **alors** **début** c_j := s ; k := 0 **fin**

sinon **début** c_j := s + B ; k := - 1 **fin**

fin . #

Exercice : Démontrer que cet algorithme est correct.

3. Soustraction .

On vient de voir comment ajouter deux entiers de signe quelconque, la soustraction est donc tout simplement réalisée grâce à la formule

a - b = a + (- b) .

4. Multiplication .

Il suffit de considérer le cas du produit de deux entiers positifs.

On veut cette fois calculer $c = a\,b$ où les entiers a et b sont donnés par les formules du paragraphe 2 , avec $m \geq n$.

Plus précisément, il s'agit à nouveau d'obtenir le développement de c en base B .

On a

$$c = \Big(\sum_{i=0}^{m-1} a_i B^i\Big) \cdot \Big(\sum_{j=0}^{n-1} b_j B^j\Big)$$

$$= \sum_{h=0}^{m+n-2} \Big(\sum_{i+j=h} a_i b_j\Big) B^h .$$

D'où l'algorithme (en désignant toujours la retenue par r) .

algorithme multiplication de deux entiers version 1 ;

données : $a = (a_{m-1} \ldots a_0)_B$, $a_{m-1} \neq 0$, $b = (b_{n-1} \ldots b_0)_B$, $b_{n-1} \neq 0$;

\# $r := 0$; $k := m + n - 2$;

pour $h := 0$ **à** $m + n - 2$ **faire**

début

$t := r$;

pour $i := \max(0, h - n + 1)$ **à** $\min(h, m - 1)$ **faire** $t := t + a_i\, b_{h-i}$;

$c_h := t$ **mod** B ; $r := t$ **div** B

fin

si $r \neq 0$ **alors début** $k := k + 1$; $c_k := r$ **fin** . \#

Pour vérifier que cet algorithme est correct, le seul point non évident est le fait que c_k est bien le chiffre de gauche du développement de c en base B . Pour le démontrer, il suffit de noter que

$$a < B^m \quad \text{et} \quad b < B^n \quad \Rightarrow \quad c < B^{m+n} \ ,$$

autrement dit, on a $k \leq m + n - 1$.

Il est facile de vérifier que le nombre d'opérations de cet algorithme est en $O(mn)$.

Mais , cet algorithme, écrit brutalement, présente un défaut sérieux : il fait intervenir des entiers intermédiaires dont la valeur peut dépasser le produit $(B - 1)^2 n$, avec n arbitrairement grand. Il ne s'agit pas d'opérations "élémentaires", car on ne peut considérer comme telles que des opérations qui portent sur deux entiers plus petits que le nombre B .

Il faut donc réécrire l'algorithme en tenant compte de cette remarque.

algorithme multiplication de deux entiers version 2 ;

données : $a = (a_{m-1} \ldots a_0)_B$, $a_{m-1} \neq 0$, $b = (b_{n-1} \ldots b_0)_B$, $b_{n-1} \neq 0$;

 # pour i := 0 **à** m - **faire** $c_i := 0$;

pour j := 0 **à** n - 1 **faire**

début

r := 0 ;

pour h := 0 **à** m - 1 **faire**

début

$t := a_h b_j + c_{h+j} + r$;

$c_{h+j} := t$ **mod** B ; r := t **div** B

fin ;

$c_{j+m} := r$

fin . #

Les nombres intermédiaires t_k vérifient cette fois

$$t_k = a_h\, b_j + c_{h+j} + r_k \leq (B-1)^2 + (B-1) + r_k \ ,$$

avec $r_k = t_{k-1}$ div B (en posant $t_{-1} = 0$) ; ce qui implique successivement

$$t_0 \leq B(B-1) \quad , \quad r_1 < B \ ,$$

$$t_1 \leq B(B-1) + (B-1) < B^2 \quad , \quad r_2 < B \ ,$$

.....

On voit donc que les nombres t sont tous strictement plus petits que B^2 et que l'on a toujours $r < B$.

Remarque : Cet algorithme diffère de l'algorithme ordinaire. Dans le cas de l'algorithme "papier-crayon", on stocke les produits intermédiaires, puis on effectue une seule addition globale. Ici, on effectue les additions partielles. Inconvénients de l'algorithme ordinaire : mémoire utilisée de taille $m \times n$, calculs intermédiaires sur des entiers de l'ordre de $m\,B$.

Voici un exemple qui illustre la différence entre les deux méthodes.

```
        4 5 6 7
    ×   6 7 8 9
      4 1 1 0 3
    3 6 5 3 6
  3 1 9 6 9
2 7 4 0 2
3 1 0 0 5 3 6 3
```

```
        4 5 6 7
    ×   6 7 8 9
      4 1 1 0 3
    3 6 5 3 6
      4 0 6 4 6 ...
  3 1 9 6 9
        3 6 0 3 3 ...
2 7 4 0 2
3 1 0 0 5 ...
```

5. Division euclidienne .

1. Existence .

THEOREME 2 . – Etant donnés deux entiers positifs a et b , il existe un couple d'entiers (q, r) et un seul vérifiant

$$a = bq + r \quad \text{où} \quad 0 \leq r < b ;$$

on pose

$$q = a \text{ div } b \quad \text{et} \quad r = a \bmod b ,$$

l'entier q est appelé le **quotient** et r le **reste** .

Lorsque le reste de la division de a par b est nul on dit que b **divise** a , ce qu'on note souvent $b \mid a$; on dit aussi que b est un **diviseur** de a ou encore que a est un **multiple** de b .

> L'existence se démontre par récurrence sur a :

- si $a < b$ on pose $q = 0$ et $r = a$,
- si $a \geq b$ on pose $q = 1 + (a - b \text{ div } b)$ et $r = (a - b) \bmod b$.

La démonstration de l'unicité est laissée au lecteur. <

COROLLAIRE . – Soit H un sous-groupe de $\mathbf{Z}$, alors il existe un entier $d \geq 0$, et un seul, tel que $H = d\mathbf{Z}$ ($= \{ dn ; n \in \mathbf{Z} \}$) .

> Si $H = \{ 0 \}$, le résultat est vrai avec $d = 0$. On suppose donc H non réduit à zéro. Alors, l'ensemble des éléments strictement positifs de H est non vide et possède donc un plus petit élément, que l'on notera d .

Soit maintenant un élément a quelconque de H . Par division euclidienne, on a

$$a = qd + r, \quad \text{où} \quad 0 \leq r < d .$$

L'entier r appartient à H, puisque $r = a - q\,d$. D'après la définition de d, on a nécessairement $r = 0$. Donc $a = q\,d$. <

2. Calcul.

On se donne deux entiers positifs a et b, de longueurs respectives m et n. Il s'agit de trouver deux entiers q et r tels que

$$a = b\,q + r \quad \text{avec} \quad 0 \leq r < b.$$

La démonstration de l'existence de la division euclidienne conduit à réaliser cette opération grâce à une suite de soustractions. Cette méthode peut être utile avec de grands nombres, mais nous allons plutôt étudier la méthode scolaire usuelle.

Dans un premier temps, comme dans la division à la main, on se ramène au cas où on a $m = n + 1$.

Choisissons alors les notations suivantes

$$a = (a_0\, a_1 \ldots a_n)_B \quad \text{et} \quad b = (b_1 \ldots b_n)_B$$

avec

$$a / b < B.$$

Il s'agit de déterminer le quotient

$$q = [\, a / b \,].$$

Le principe de la méthode qui suit consiste à prendre une valeur approchée de ce quotient. La valeur exacte étant ensuite obtenue en un tout petit nombre d'essais.

On prend comme valeur approximative du quotient l'entier

$$q^* = \min \left\{ \left[\frac{a_0 B + a_1}{b_1} \right], B - 1 \right\} .$$

(La notation [x] désigne la partie entière du nombre réel x .]

La suite montre que cette première valeur est très satisfaisante.

On a en effet

(i) $q^* \geq q$;

. c'est vrai si $q^* = B - 1$,

. sinon, on a

$$q^* = \left[\frac{a_0 B + a_1}{b_1} \right] ,$$

et donc

$$q^* b_1 \geq a_0 B + a_1 - b_1 + 1 ,$$

ce qui implique

$$\begin{aligned} a - q^* b &\leq a - q^* b_1 B^{n-1} \\ &\leq a_0 B^n + \ldots + a_n - a_0 B^n - a_1 B^{n-1} + b_1 B^{n-1} - B^{n-1} \\ &= a_2 B^{n-2} + \ldots + a_n - B^{n-1} + b_1 B^{n-1} < b_1 B^{n-1} \leq b . \end{aligned}$$

D'où le résultat, puisque q est le plus petit entier tel que $a - q b < b$.

(ii) $b_1 \geq [\, B/2 \,] \Rightarrow q^* \leq q + 2$.

Notons d'abord que

$$q^* \leq \frac{a}{b_1 B^{n-1}} < \frac{a}{b - B^{n-1}} \quad \text{et} \quad q > \frac{a}{b} - 1 .$$

Pour démontrer l'implication, on raisonne par l'absurde :

on suppose donc $q^* \geq q + 3$.

Alors

$$3 < \frac{a}{b - B^{n-1}} - \frac{a}{b} + 1 = \frac{a}{b} \left(\frac{B^{n-1}}{b - B^{n-1}} \right) + 1 ,$$

donc

$$\frac{a}{b} > 2 \left(\frac{b - B^{n-1}}{B^{n-1}} \right) \geq 2 (b_1 - 1) ,$$

puis

$$B - 4 \geq q^* - 3 \geq q = [\, a/b \,] \geq 2 (b_1 - 1) ,$$

et on a bien

$$b_1 < [\, B/2 \,] .$$

Remarque : On peut se ramener à la condition $b_1 \geq [\, B/2 \,]$ en remplaçant a et b par ka et kb où le facteur k vaut

$$k = \left[\frac{B}{b_1 + 1} \right] .$$

Exercice : Démontrer que la remarque précédente est correcte.

6. Le coût de la multiplication et de la division .

1. Le coût de la multiplication .

On désigne par $M(n)$ le coût du produit de deux entiers de n bits.

L'algorithme de multiplication de deux entiers de longueur n donné plus haut a un coût de l'ordre de n^2, donc

$$M(n) = O(n^2),$$

mais on peut construire des algorithmes dont le coût asymptotique est nettement plus petit.

La méthode très simple suivante, due à Karatsuba, utilise l'idée très souvent efficace en algorithmique de partager un problème donné en deux sous-problèmes de tailles égales.

Supposons n pair, $n = 2m$, et u et v deux entiers de n bits . On décompose ces entiers en

$$u = a\,2^m + b \quad , \quad v = c\,2^m + d,$$

et on calcule le produit $w = u\,v$ de la manière suivante.

Si

$$x = (a+b)(c+d) \quad , \quad y = ac \quad , \quad z = bd$$

alors

$$w = y\,2^{2m} + (x - y - z)\,2^{2m} + z \ .$$

Compte tenu du fait que les formules précédentes ne comportent que trois multiplications d'entiers de longueur m et des opérations (additions et décalages) dont le coût est linéaire en n , il existe une constante k telle que $M(n)$ vérifie la majoration suivante

$$M(n) \leq \begin{cases} k & \text{si } m = 1 \\ 3\,M(m) + k\,n & \text{si } m > 1 . \end{cases}$$

Soient n un entier positif quelconque et t le plus petit entier tel que 2^t soit au moins égal à n . Alors

$$M(n) \leq M(2^t) .$$

En appliquant la majoration précédente pour les entiers $2^t, 2^{t-1}$, ... et 2 , on obtient

$$M(2^t) = O(3^t) ;$$

ce qui implique

$$M(n) = O(n^{\alpha}) \quad \text{où} \quad \alpha = (\text{Log}\,3)/(\text{Log}\,2) \cong 1.585 < 2 .$$

L'idée précédente peut être généralisée : au lieu de découper les entiers en deux parts de même longueur, on les découpe en r morceaux. Il s'agira donc de trouver une méthode pour calculer le produit en effectuant aussi peu de multiplications que possible. La technique utilisée sera d'obtenir ce produit à partir d'un polynôme, ce polynôme étant déterminé par interpolation. Considérons cette fois deux entiers u et v de longueur égale à $n\,r$, dont on veut calculer le produit w .

Posons

$$u = U_r\, 2^{rn} + \ldots + U_1\, 2^n + U_0$$

et

$$v = V_r\, 2^{rn} + \ldots + V_1\, 2^n + V_0 .$$

On définit les polynômes U, V et W par les formules

$$U(X) = U_r\, X^{rn} + \ldots + U_1\, X^n + U_0 ,$$

$$V(X) = V_r\, X^{rn} + \ldots + V_1\, X^n + V_0 ,$$

$$W(X) = U(X)\, V(X) .$$

Alors

$$w = W(2^n) .$$

Pour calculer le polynôme W, dont le degré ne dépasse pas $2r$, on détermine d'abord ses valeurs en $2r+1$ points, par exemple $i = 0, 1, \ldots, 2r$ (ou encore aux points $-r, -r+1, \ldots, r$), grâce à la formule

$$W(i) = U(i)\, V(i),$$

puis on obtient les coefficients de W par interpolation (le coût de cette opération est linéaire en n). Ceci conduit à une majoration du type

$$M(rn) \leq (2r+1)\, M(n) + cn,$$

pour une certaine constante positive c.

Une démonstration analogue à la précédente permet d'en déduire l'estimation

$$M(n) = O(n^{\alpha'}) \quad \text{où} \quad \alpha' = (\mathrm{Log}(2r+1))/\mathrm{Log}(2r) ,$$

ainsi, en choisissant l'entier r suffisamment grand, on voit que

$$M(n) = O(n^{1+\varepsilon}) \quad \text{pour tout} \quad \varepsilon > 0 \text{ fixé}.$$

Actuellement la meilleure estimation connue est

$$M(n) = O(n \,.\, \mathrm{Log}\, n \,.\, \mathrm{LogLog}\, n) ,$$

elle est due à Schönhage et Strassen et utilise la technique de la transformée de Fourier rapide.

2. Le coût de la division .

On commence par traiter le cas particulier du calcul du quotient entier de 2^{2n-1} par un entier v, où v comporte n bits, donc $v \geq 2^{n-1}$, et on exclut le cas trivial où $v = 2^n$.

Ce calcul peut être effectué par la méthode suivante.

Supposons donné un entier v, $2^{n-1} \leq v < 2^n$ et que l'on veuille calculer le quotient

$$q = [\, 2^{2n-1} / v \,],$$

et appelons $C(n)$ le coût d'un tel calcul.

Pour estimer $C(n)$, supposons n pair, $n = 2m$. On écrit $v = 2^m v' + v''$, on a donc $v' \geq 2^{m-1}$.

On a

$$2^{2n-1} / v = (2^{3m-1} / v')(1 - x + x^2 - \ldots)$$

où

$$x = v'' / (2^m v') , \quad \text{donc} \quad 0 \leq x < 2^{-m+1} .$$

On en déduit

$$0 \leq (2^{2n-1} / v) - (2^{3m-1} / v')(1 - x) < 4 .$$

Il reste essentiellement à estimer le terme $(2^{3m-1} / v')(1 - x)$.

Posons

$$2^{2m-1} / v' = a + \varepsilon , \quad \text{où} \quad 0 \leq \varepsilon < 1 ,$$

alors

$$(2^{3m-1} / v')(1 - x) = 2^m a + 2^m \varepsilon - (2^{2m-1} v'') / v'^2$$

où

$$2^m \varepsilon = (2^{2m-1} - a v') \times (2^{2m-1} / v') \times 2^{-m+1}$$
$$= (2^{2m-1} - a v') \times a \times 2^{-m+1} + \varepsilon' \quad \text{avec} \quad 0 \leq \varepsilon' < 2 .$$

Ces calculs montrent que l'on peut obtenir le quotient q à partir du quotient a, des produits $a\,v'$, $(2^{2m-1} - a\,v') \times a$ et v'^2, du quotient $[(2^{2m-1} v'') / v'^2]$ et d'un certain nombre d'opérations dont le coût est linéaire en n.

D'où la majoration

$$C(n) \leq 2\,C(n/2) + 3\,M(n/2) + c\,n \quad (c = \text{constante}) ;$$

qui - sous l'hypothèse $M(2k) \geq 2\,M(k)$ pour tout k - conduit à l'estimation

$$C(n) = O(M(n)) + O(n \operatorname{Log} n).$$

Sous l'hypothèse supplémentaire (non infirmée à ce jour)

$$M(n) \geq c'\,n \operatorname{Log} n ,$$

pour une certaine constante $c' > 0$, on obtient

$$C(n) \leq O(M(n)).$$

Pour calculer le quotient entier d'un nombre u de 2n bits par un nombre v de n bits, on écrit tout simplement

$$[u/v] = [(u/2^{2n-1}) \times (2^{2n-1}/v)]$$

ce qui permet d'obtenir le quotient cherché en effectuant le calcul précédent suivi de la multiplication de deux entiers de n bits environ.

Ceci montre que la quantité

$D(n)$ = coût de la division d'un entier de $2n$ bits par un entier de n bits

vérifie l'estimation

$$D(n) = O(M(n)).$$

Ainsi, en termes un peu rapides, on peut dire que le coût de la division est, à une constante multiplicative près, majoré par celui de la multiplication.

7. Le calcul de x^n.

Soit x un objet tel que l'expression x^n ait un sens (par exemple x peut être un entier, une matrice, un élément d'un corps fini ...) . On se propose de calculer x^n.

1. Premier algorithme .

C'est le premier algorithme qui vient à l'esprit : on calcule successivement les éléments $x^2, x^3, ..., x^n$. Ce qui peut être présenté plus formellement de la façon suivante.

algorithme A1

données x , n ; { le résultat est noté z }

\# z := x ;

pour i = 1 à n-1 **faire** z := z x . #

On s'intéresse au nombre de multiplications nécessaires, c'est la quantité choisie ici comme représentant le **coût** de l'algorithme de l'algorithme A 1 considéré.

Dans ce cas, le coût est tout simplement

Coût (A 1) = n - 1 .

Remarque : Le choix du nombre de multiplications comme mesure du coût de l'algorithme précédent n'est pas toujours réaliste . Par exemple, si x est un entier le temps de calcul de x^n dépend de la longueur des entiers qui interviennent dans les multiplications et n'est pas linéaire en n . Par contre, si x est un élément d'un corps fini, les valeurs successives de y sont de longueurs uniformément bornées et le temps de calcul est proportionnel au nombre de multiplications effectuées.

2. Second algorithme.

Cet algorithme est connu depuis environ vingt siècles par les mathématiciens chinois et a été retrouvé de nombreuses fois. Le principe consiste à calculer successivement certaines puissances de x, à savoir $x^2, x^4, x^8, \ldots$ et à les combiner ensuite pour obtenir x^n.

Plus précisément, si l'exposant n admet l'écriture binaire

$$n = \sum_{i=0}^{k} e_i . 2^i \quad , \quad \text{où} \quad e_i \in \{ 0 , 1 \} \ ,$$

alors on a les formules

$$x^n = x^{\sum_{i=0}^{k} e_i . 2^i} = \prod_{i=0}^{k} x^{e_i . 2^i} = \prod_{i,\, e_i \neq 0} x^{2^i} .$$

Ce qui conduit à l'algorithme suivant.

algorithme A2

données x, $n > 0$; { le résultat est encore noté z }

\# $y := x$; $z := 1$; { y contient successivement x, x^2, x^4, ... }

tant que $n > 1$ **faire**

début $m := n$ **div** 2 ;

si $n > 2 * m$ **alors** $z := z * y$;

$y := y * y$; $n := m$ **fin** ;

$z := z * y$. \#

Faisons tourner cet algorithme sur un exemple : calculons x^{13} par cette méthode. Le déroulement de l'algorithme est résumé par le tableau suivant.

n	13	13	6	3	1
m		6	3	1	
y	x	x^2	x^4	x^8	
z	1	x	x	x^5	x^{13}

Maintenant nous allons étudier le nombre N de multiplications effectuées par cet algorithme. D'après la formule ci-dessus, on a

$$N = k + e_0 + e_1 + \ldots + e_k - 1 .$$

D'où l'on tire aussitôt la majoration

$$N \leq 2k .$$

Il reste, bien entendu, à majorer l'entier **k** . Dans la décomposition binaire de n on a

$$n = 2^k + e_{k-1} . 2^{k-1} + \ldots + e_0 ,$$

donc

$$2^k \leq n ,$$

ou encore, en passant aux logarithmes,

$$k \leq \log n .$$

Remarque : on notera toujours log le logarithme binaire, c'est à dire que

$$\log x = \frac{\mathrm{Log}\, x}{\mathrm{Log}\, 2} .$$

Ainsi N vérifie

$$N \leq 2 \log \mathbf{k} .$$

Par exemple, si n vaut un million, l'algorithme A 1 nécessite exactement 999 999 multiplications tandis que l'algorithme A 2 n'en effectue pas plus de 38 (en effet on sait que $2^{10} = 1024$, donc $2^{20} > 10^6$). Exercice : Calculer N lorsque $n = 10^6$.

Une première conséquence évidente de l'estimation précédente de N est que pour des valeurs de n assez grandes (ici par exemple pour $n \geq 20$) l'algorithme A 2 comporte nettement moins de multiplications que l'algorithme A 1 .

Mais il est important pour comparer les performances réelles de ces deux algorithmes de bien préciser quel est le domaine de calcul :

- si x est un entier de longueur h alors le second algorithme fait intervenir des nombres très grands et si on suppose que le coût du produit de deux entiers de longueurs respectives m et m' est de la forme c m m' (où c est une constante positive) alors le coût de A 2 vérifie

$$C_2(n) \cong c\,h^2 \sum_{i=0}^{k-1} 2^{2^{i+1}} + c\,h^2 \sum_{i=1}^{k} e_i \Big(\sum_{j=0}^{i-1} e_j\, 2^j \Big)\, 2^i ,$$

où les e_i sont les chiffres binaires de n (en particulier $e_k = 1$) , tandis que le premier algorithme a un coût de l'ordre de

$$C_1 = c\,h\,(h + 2h + 3h + \ldots + (n-2)h) \cong (c/2)\,n^2 h^2 .$$

Pour $n = 2^k$, on a

$$C_2(n) \cong (4/3)\,c\,n^2 h^2 \cong (8/3)\,C_1(n) ;$$

par contre, pour $n = 2^k + 2^{k-1}$, on a

$$C_2(n) \cong (4/3)\,c\,2^{2k} h^2 + c\,2^{2k-1} h^2 \cong (11/6)\,c\,2^{2k} h^2$$

alors que

$$C_1(n) \cong (9/4)\,c\,2^{2k} h^2 \cong (27/12)\,C_2(n) .$$

- si x appartient à un anneau fini dans lequel le coût du produit de deux éléments quelconques peut être considéré comme constant alors le second algorithme est nettement préférable au premier (par exemple pour $n \geq 20$).

Il est utile de savoir que l'algorithme A 2 est effectivement utilisé : par exemple en cryptographie, certaines méthodes de codage et de décodage nécessitent de calculer des expressions y de la forme

$$y = x^n \mod a ,$$

où n est un entier $> 10^{50}$; dans un tel cas, non seulement le second algorithme permet un calcul relativement rapide, mais le premier algorithme est absolument inutilisable (exercice : estimer le temps nécessaire pour que l' algorithme A 1 calcule y lorsque l'ordinateur utilisé effectue 10^{10} multiplications à la seconde ... ce qui est une situation optimiste !).

Revenons à une étude plus précise de N. On a vu que

$$N = k + s(n) - 1 ,$$

où $s(n)$ désigne la somme des chiffres de l'écriture binaire de l'entier n. Par ailleurs, l'entier k vérifie les inégalités $2^k \leq n < 2^{k+1}$, et donc $k = [\log n]$.

L'inégalité évidente $s(n) \geq 1$ implique la minoration

$$N \geq [\log n] ,$$

l'égalité étant atteinte pour toutes les valeurs de n qui sont des puissances de deux.

En résumé, la quantité N vérifie

$$[\log n] \leq N \leq 2[\log n] .$$

Il serait intéressant de faire une étude statistique plus fine de N en fonction de n, mais cette question est difficile et nous entraînerait trop loin.

3. Une application .

Nous allons appliquer l'algorithme précédent au calcul d'un terme d'une suite récurrente linéaire. Rappelons qu'une telle suite (u_n) est définie par ses premières valeurs $u_0 , u_1 , \dots , u_{h-1}$ et une condition de la forme

(*) $\quad u_n = a_1 u_{n-1} + a_2 u_{n-2} + \dots + a_h u_{n-h}$ pour $n \geq h$.

L'exemple le plus célèbre est celui de la suite de Fibonacci (qui date de 1202) , définie par

$$F_0 = 0 \ , \ F_1 = 1 \ , \ F_n = F_{n-1} + F_{n-2} \quad \text{pour} \quad n \geq 2 \ ;$$

si bien que

$$F_2 = 1 \ , \ F_3 = 2 \ , F_4 = 3 \ , F_5 = 5 \ , F_6 = 8 \ \dots\dots$$

Si on désigne par $\mathbf{u}_n$ le vecteur colonne dont les composantes sont $u_n , u_{n-1} , \dots , u_{n-h+1}$ alors la relation (*) peut s'écrire sous la forme matricielle

$$\mathbf{u}_n = A \, \mathbf{u}_{n-1}$$

où la matrice A vaut

$$A = \begin{pmatrix} a_1 & a_2 & \dots\dots & a_h \\ 1 & 0 & \dots\dots & 0 \\ 0 & 1 & 0 \dots\dots & 0 \\ \dots\dots & & & \\ 0 & & & 0 \ 1 \end{pmatrix} .$$

Si bien que l'on a

$$\mathbf{u}_n = A^{n-h+1} \, \mathbf{u}_{h-1}$$

et que l'on peut calculer $\mathbf{u}_n$, et donc en particulier u_n , en un nombre d'opérations qui est majoré par $O (\text{Log } n)$.

Cette méthode est particulièrement utile si on travaille modulo un entier, elle permet par exemple de trouver rapidement la période de la suite (u_n) .

4. Complexité du problème .

Après avoir donné un algorithme banal qui calcule x^n en un nombre d'opérations linéaire en n , nous avons trouvé un autre algorithme qui réalise le même travail en un nombre d'opérations logarithmique en n . Se pose alors la question : peut-on encore faire mieux ? Avant de pouvoir répondre à une telle question, il faut lui donner un sens très précis.

La première chose est de définir clairement la classe d'algorithmes que l'on considère. Dans le cas présent, nous n'envisagerons que des algorithmes qui n'effectuent que des multiplications. Plus précisément encore, nous nous limiterons aux algorithmes de la forme suivante qui calculent x^n , pour n fixé :

$1 : y_1 := u_1 \, v_1$ où $u_1 , v_1 \in \{ 1, x \}$,

.....

$i : y_i := u_i \, v_i$ où $u_i , v_i \in \{ 1, x, y_1, \ldots , y_{i-1} \}$,

.....

$t : y_t := u_t \, v_t$ où $u_t , v_t \in \{ 1, x, y_1, \ldots , y_{t-1} \}$ et $y_t = x^n$.

Le coût d'un tel algorithme étant évidemment égal à t (le nombre de multiplications) .

Remarquons d'abord que l' algorithme A 2 appartient bien à la classe précédente. On peut aussi noter que l'algorithme A 2 n'est pas toujours optimal dans cette classe.

En effet, si on considère le cas où $n = 15$ l'algorithme A 2 nécessite 6 multiplications tandis qu'il est possible de calculer x^{15} en 5 opérations de la manière suivante : on calcule x^3 (en deux multiplications) puis x^6 , x^{12} et enfin on obtient $x^{15} = x^3 . x^{12}$.

Passons maintenant à l'étude véritable de la **complexité** du calcul de x^n. Autrement dit, il s'agit de minorer le nombre t.

Pour un algorithme quelconque du type précédent, chaque valeur y_i peut s'écrire :

$$y_i := x^{e(i)},$$

où l'exposant $e(i)$ vérifie

$$e(1) \in \{0, 1, 2\},$$

$$e(i) = e(j) + e(h) \quad \text{avec } j, h < i, \text{ pour } i \geq 2,$$

$$e(t) = n.$$

On en déduit aussitôt les inégalités

$$e(i) \leq 2^i \quad \text{pour} \quad i = 1, \ldots, t;$$

donc en particulier

$$e(t) = n \leq 2^t.$$

Autrement dit,

$$t \geq \log n.$$

Nous avons ainsi montré que la complexité de notre problème est au moins $\log n$ et par conséquent que l' algorithme A 2 est, à peu de chose près, le meilleur possible.

Remarque : L'argument qui nous a permis de trouver la complexité de ce problème est très simple. Il ne faudrait pas croire que c'est toujours le cas. Bien au contraire, la plupart des questions de complexité sont très difficiles. Beaucoup de problèmes dans ce domaine restent ouverts, par exemple on ignore quelle est la complexité du produit de deux matrices carrées $n \times n$ pour $n \geq 3$.

8. Le p.g.c.d.

1. Existence . Relation de Bézout . Théorème d'Euclide-Gauss .

Le résultat suivant démontre l'existence du p.g.c.d. .

THEOREME 3 . – Soient a et b deux entiers, il existe un entier positif d qui divise à la fois a et b et tel que tout diviseur commun à a et b divise d ; cet entier est appelé le p.g.c.d. de a et b et noté p.g.c.d. (a , b) , ou encore simplement (a , b) quand il n'y a pas de confusion possible.

De plus, il existe deux entiers u et v tels que

$$d = u\,a + v\,b \ .$$

> Considérons l'ensemble des entiers de la forme $m\,a + n\,b$, où m et n parcourent tous deux $\mathbf{Z}$.

On vérifie aussitôt que cet ensemble est un sous-groupe de $\mathbf{Z}$. Comme nous l'avons déjà vu, cet ensemble est donc de la forme $d\,\mathbf{Z}$, pour un certain entier d positif. De plus, par construction, il existe deux entiers u et v tels $d = u\,a + v\,b$.

Pour conclure, il suffit maintenant de montrer que d divise a et b et que tout diviseur commun à a et b divise aussi d .

Comme

$$a = 1\,.\,a + 0\,.\,b \ ,$$

l'entier a appartient à $d\,\mathbf{Z}$, en d'autres termes d divise bien a ; de même l'entier d divise aussi b .

Soit enfin un entier c qui divise à la fois a et b . Il existe alors deux entiers a' et b' tels que $a = c\,a'$ et $b = c\,b'$. D'où la relation

$$d = u\,a + v\,b = (u\,a' + v\,b')\,.\,c$$

qui montre que l'entier c divise bien l'entier d . <

Lorsque le p.g.c.d. de a et b est égal à 1 , on dit que a et b sont **premiers entre eux** . Le théorème 1 possède le corollaire suivant.

THEOREME 4 . – Soient a et b deux entiers. Alors a et b sont premiers entre eux si, et seulement si, il existe deux entiers u et v tels que l'on ait la relation (dite de Bézout)

$$u\,a + b\,v = 1\,.$$

> La condition est nécessaire d'après le théorème 1 . Elle est aussi suffisante : si

$$u\,a + b\,v = 1\ ,$$

alors tout entier qui divise simultanément a et b divise 1 , donc a et b sont premiers entre eux. <

Ce théorème a le corollaire suivant, quelquefois appelé théorème d'Euclide-Gauss.

THEOREME 5 . – Soient a et b deux entiers premiers entre eux. Alors, si un entier c est divisible à la fois par a et b , il est aussi divisible par leur produit a b .

> Soient u et v deux entiers tels que $u\,a + v\,b = 1$. Alors

$$u\,a\,c + v\,b\,c = c\ ,$$

et comme le produit a b divise a c et b c , il divise aussi l'entier c . <

2. Calcul du p.g.c.d.

La démonstration du théorème 1 ne fait que prouver l'existence de l'entier d mais ne fournit pas de moyen direct de le calculer. En pratique, il est fort utile de savoir calculer le p.g.c.d. de deux entiers ; ce qu'on sait faire depuis environ vingt deux siècles grâce au (justement) célèbre **algorithme d'Euclide .**

L'algorithme d'Euclide ordinaire ne fournit que la valeur du p.g.c.d. mais, comme la connaissance des valeurs des entiers u et v du théorème 3 est souvent très utile et qu'on les obtient sans beaucoup compliquer l'algorithme d'Euclide, nous donnons directement la variante qui fournit aussi u et v .

Supposons $a > b > 0$, l'algorithme d'Euclide consiste à calculer la suite de triplets $W_i = (t_i , u_i , v_i)$ définis par les conditions

$$W_0 = (a , 1 , 0) \ ,$$
$$W_1 = (b , 0 , 1) \ ,$$
$$W_{i+1} = W_{i-1} - q_{i+1} W_i \quad \text{où} \quad q_{i+1} = [t_{i-1} / t_i] \quad \text{pour} \quad i \geq 2 \ ;$$

en s'arrêtant au premier entier j pour lequel t_j s'annule.

On a alors

$$d = t_{j-1}$$

et

$$d = u_{j-1} a + v_{j-1} b \ .$$

Pour démontrer ces dernières formules, remarquons d'abord que par construction on a

$$t_i = u_i\, a + v_i\, b \qquad \text{pour } i = 0, 1, 2, \ldots$$

et donc en particulier

$$t_{j-1} = u_{j-1}\, a + v_{j-1}\, b \quad , \text{ ainsi } t_{j-1} \in a\,\mathbf{Z} + b\,\mathbf{Z} \ .$$

Il reste à montrer que t_{j-1} est bien égal à d , le p.g.c.d. de a et b . D'après la démonstration du théorème, $a\,\mathbf{Z} + b\,\mathbf{Z} = d\,\mathbf{Z}$, donc d divise t_{j-1} .

Il suffit maintenant de montrer que t_{j-1} divise à la fois a et b . Or, par définition, t_{j-1} divise à la fois t_{j-1} et t_{j-2} et la formule

$$t_{i-2} = t_i + q_i\, t_{i-1} \ ,$$

appliquée successivement pour $i = j - 1,\ j - 2,\ \ldots,\ 3,\ 2$ montre que le terme t_{j-1} divise $t_{j-3}, t_{j-4}, \ldots, t_1, t_0$. Comme $t_1 = b$ et $t_0 = a$, on obtient le résultat. <

Exemple : Le tableau suivant présente le calcul du p.g.c.d. de 1812 et 1572 .

i	0	1	2	3	4	5	6	7
t	1812	1572	240	132	108	24	12	0
u	1	0	1	- 6	7	- 13	59	
v	0	1	- 1	7	- 8	15	- 68	
q			1	6	1	1	4	

D'où l'on déduit p.g.c.d. (1812 , 1572) = 12 , et aussi la relation

$$59 \times 1812 - 68 \times 1572 = 12 \ .$$

3. Le coût de l'algorithme d'Euclide .

Il est très intéressant d'analyser le coût de cet algorithme. Le résultat le plus spectaculaire est le suivant.

THEOREME 6 (G. Lamé, 1845) . – Soit n un entier ≥ 1 . Soient alors deux entiers u et v , $u > v > 0$, avec la propriété que u est le plus petit entier positif pour lequel l'algorithme d'Euclide sur (u , v') , où $u > v' > 0$, nécessite n étapes. Alors on a

$$u = F_{n+2} \quad \text{et} \quad v = F_{n+1} ,$$

où F_k désigne le k-ième nombre de Fibonacci.

> En effet, on a effectué les divisions successives

$$u_0 = u = q_1 v + r_1 ,$$

$$u_1 = q_2 r_1 + r_2 ,$$

$$\ldots .$$

$$u_{n-1} = q_n r_{n-1} + r_n = q_n r_{n-1} ,$$

et la conclusion résulte de la suite d'inégalités

$$u_{n-1} \geq 1 \quad , \quad u_{n-2} \geq u_{n-1} + 1 \geq 2 \quad , \quad u_{n-3} \geq u_{n-2} + u_{n-1} \quad , \ldots . <$$

COROLLAIRE 1 . – Si $0 \leq v \leq u$ alors le nombre n de pas de l'algorithme d'Euclide vérifie

$$n \leq \frac{\mathrm{Log}(\sqrt{5}\, u)}{\mathrm{Log}\left(\frac{1+\sqrt{5}}{2} \right)} - 2 .$$

> Exercice . <

Pour une analyse statistique détaillée du nombre de pas nécessaires dans l'algorithme d'Euclide, voir Knuth .

COROLLAIRE 2 . – Si $0 \leq v < u$, où u est un nombre de n bits. Alors le coût de l'algorithme d'Euclide est en $O(n^2)$.

> C'est une conséquence quasi immédiate du corollaire 1 . <

4. Le p.p.c.m.

Si a et b sont deux entiers non nuls, par définition leur **p.p.c.m.** est l'entier

$$\text{p.p.c.m.}(a, b) = a\,b / (a, b),$$

on le note aussi $[a, b]$ quand il n'y a pas de confusion possible.

On vérifie facilement que c'est un multiple commun à a et à b et que tout entier qui est à la fois un multiple de a et de b est un multiple de $[a, b]$.

Exercice : Démontrer les propriétés ci-dessus.

Exemple : Nous avons vu que le p. g. c. d. de 1812 et 1572 est égal à 12 , il en résulte que

$$\text{p.p.c.m.}(1812, 1572) = 1812 \times 572 / 12 = 237372 .$$

9. Le groupe G (n) .

1. Définition .

Soit n un entier au moins égal à deux. On note G (n) l'ensemble des éléments de l'anneau **Z** / n **Z** qui sont inversibles. D'après le théorème 3 , l'ensemble G (n) est constitué par les classes des entiers premiers avec n . On note φ (n) le cardinal de l'ensemble G (n) , c'est le nombre d'entiers de l'intervalle {1, 2, ..., n - 1} qui sont premiers avec n (par convention φ (1) = 1) ; cette fonction est appelée la **fonction phi d'Euler** .

Comme le produit de deux éléments inversibles est aussi inversible, on voit que l'ensemble G (n) est un groupe (multiplicatif).

Un nombre entier au moins égal à deux est dit **premier** s'il n'admet pas d'autre diviseur positif que lui-même et l'unité. Les nombres premiers sont 2, 3, 5, 7, 11, 13 ... On sait depuis Euclide qu'il existe une infinité de nombres premiers (voir l'exercice 19 ci-dessous) . Dans toute la suite, la lettre p désignera toujours un nombre premier.

Un nombre entier au moins égal à deux qui n'est pas premier sera dit **composé** .

Si p est un nombre premier alors tout les entiers de l'intervalle {1, 2, ..., p - 1} sont premiers avec lui, donc

$$\varphi(p) = p - 1 .$$

Pour n entier , $n \geq 2$, on a même l'équivalence

$$n \text{ premier} \Leftrightarrow \varphi(n) > n - 2 .$$

2. Le théorème d'Euler .

Le lemme suivant est un cas particulier très simple du **théorème de Lagrange** sur les groupes finis.

LEMME 1 . – Soit G un groupe abélien fini de cardinal k , dont la loi est notée multiplicativement. Alors tout élément x de G vérifie

$$x^k = 1 \ .$$

[Le théorème de Lagrange est le même résultat, mais pour un groupe fini quelconque.]

> Soit x un élément quelconque de G . La fonction $y \to x\,y$ de G dans lui-même est bijective. Par suite,

$$\prod_{y \in G} y = \prod_{y \in G} x\,y = x^k \prod_{y \in G} y \ ,$$

la dernière égalité provenant de la commutativité. D'où le résultat en simplifiant. <

L'application de ce lemme au cas du groupe G (n) donne le résultat suivant.

THEOREME 7 (Euler) . – Soit a un entier premier avec un entier $n \geq 2$, on a alors

$$a^{\varphi(n)} \equiv 1 \pmod{n} \ .$$

Exemple : Considérons le cas où $n = 56$ et $x = 19$.

On vérifie que $\varphi(56) = 24$ et le calcul peut être réalisé comme suit.

$$x^2 = 289 \equiv 9 \ , \quad x^4 \equiv 9^2 = 81 \equiv 25 \ ,$$

$$x^6 \equiv 25 \times 9 = 225 \equiv 1$$

donc $x^{24} \equiv 1$, comme l'indique le théorème.

3. Calcul de l'inverse d'un élément .

Soit x un élément du groupe $G(n)$, on veut calculer son inverse $u = x^{-1}$. Autrement dit, il s'agit de trouver un entier u qui vérifie

$$u\,x \equiv 1 \mod n ,$$

ou encore de trouver deux entiers u et v tels que

$$u\,x + v\,n = 1 .$$

Deux méthodes sont donc possibles :

- l'algorithme d'Euclide du p.g.c.d. de x et n qui fournit en particulier u ,
- le théorème d'Euler qui donne la solution

$$u = x^{\varphi(n)-1} \mod n .$$

Dans les deux cas, le nombre d'opérations est en $O(\text{Log } n)$, mais la seconde méthode est peut-être plus rapide (Mais seulement lorsque la fonction d'Euler $\varphi(n)$ est connue. Par contre on ne connaît pas de moyen rapide de calculer cette quantité ; ceci est tellement vrai que la sécurité de certaines méthodes de cryptographie repose sur la difficulté du calcul de $\varphi(n)$ lorsque n est un très grand entier .) .

Remarque : Dans le cas présent, le coût du calcul de l'inverse d'un élément est nettement supérieur au coût du calcul du produit de deux éléments. De façon générale, les coûts des opérations dans $G(n)$ et dans $\mathbf{N}$ sont très différents (nous l'avons déjà vu pour le calcul de x^n) .

4. Calcul des coefficients de la relation de Bézout .

Le théorème d'Euler permet de calculer les coefficients de la relation de Bézout sans utiliser l'algorithme d'Euclide.

Considérons en effet deux entiers positifs a et b premiers entre eux. Il s'agit de déterminer deux entiers u et v tels que l'on ait

$$u\,a + v\,b = 1 .$$

Remarquons que cette relation implique les congruences

$$u\,a \equiv 1 \mod b \quad \text{et} \quad v\,b \equiv 1 \mod a .$$

Supposons les quantités $\varphi(a)$ et $\varphi(b)$ connues. On obtient une solution (u, v) en prenant

$$u = a^{\varphi(b) - 1} \mod b$$

et

$$v = (b^{\varphi(a) - 1} \mod a) - a .$$

En effet, d'après le théorème d'Euler, le nombre

$$u\,a + v\,b - 1$$

est divisible par a et par b , donc par le produit a b (puisque a et b sont premiers entre eux) ; d'autre part, on vérifie facilement que

$$| u\,a + v\,b - 1 | < a\,b .$$

La relation $u\,a + b\,v = 1$ a donc bien lieu.

Exemple : Reprenons les valeurs choisies précédemment pour l'exemple de l'algorithme d'Euclide. On note d'abord que

$$1812 = 12 \times 151 \quad \text{et} \quad 1572 = 12 \times 131$$

puis que

$$\varphi(151) = 150 \quad \text{et} \quad \varphi(131) = 130 \ .$$

Et enfin, on vérifie que

$$151^{129} \bmod 131 = 59$$

et

$$(131^{149} \bmod 151) - 151 = -68 \ ,$$

on retrouve donc les coefficients précédents.

Remarque : Pour deux entiers a et b, on a l'équivalence suivante

$$(a, b) = 1 \iff a^{\varphi(b)} \equiv 1 \bmod b \ .$$

L'implication $\Rightarrow$ a déjà été démontrée.

Réciproquement, si un entier d divise simultanément a et b, il divise aussi le nombre $a^k \bmod b$ pour tout entier $k > 0$; donc

$$a^k \bmod b = 1 \quad \Rightarrow \quad d = 1 \ .$$

Lorsque le nombre $\varphi(b)$ est connu, ceci fournit un moyen rapide de tester si a et b sont premiers entre eux.

Exercice : Soit n un entier qui est le produit de deux grands nombres premiers distincts p et q. Démontrer que la connaissance de $\varphi(n)$ permet facilement de déterminer les facteurs p et q, et réciproquement.

$\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$

$(p,q) = 1 \iff p^{\varphi(q)} = p^{q-1} \equiv 1 \ [q] \quad p^q \equiv p \ [q]$

$q^{p-1} \equiv 1 \ [p] \quad q^p \equiv q \ [p]$

10. Le théorème chinois .

1. Le théorème .

Il s'agit du résultat suivant, dont un cas particulier était connu par les astronomes chinois de l'antiquité.

THEOREME 8 . – Soient m et n deux entiers premiers entre eux, alors pour tout couple d'entiers a et b le système de congruences

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

admet des solutions entières ; de plus, deux quelconques de ces solutions diffèrent d'un multiple de mn .

> Considérons l'application naturelle

$$\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$$

qui à l'entier x associe le couple (x mod m , x mod n) .

Il est clair qu'il s'agit d'un homomorphisme d'anneaux. Son noyau est l'ensemble des entiers divisibles à la fois par m et par n donc, d'après le théorème 3 , c'est l'ensemble des multiples du produit mn . D'où un homomorphisme injectif

$$\mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \ .$$

Comme les ensembles de départ et d'arrivée de cette application injective ont le même nombre d'éléments, cette application est en fait bijective. Le théorème n'est que la traduction de cette bijection. <

COROLLAIRE 1 . – Soient $m_1, \ldots, m_k$ des entiers deux à deux premiers entre eux. Alors, pour tout k-uple d'entiers $(a_1, \ldots, a_k)$, le système de congruences

$$x \equiv a_i \pmod{m_i} \quad , \quad 1 \leq i \leq k \ ,$$

admet des solutions entières ; de plus, deux quelconques de ces solutions diffèrent d'un multiple du produit $m_1 \ldots m_k$.

> On raisonne par récurrence sur k en appliquant le théorème précédent. <

COROLLAIRE 2 . – Soient a et b deux entiers positifs premiers entre eux, on a

$$\varphi(a\,b) = \varphi(a) \cdot \varphi(b) \ .$$

En particulier si $p_1, \ldots p_r$ sont des nombres premiers distincts et $k_1, \ldots, k_r$ des entiers strictement positifs, on a la relation

$$\varphi(p_1^{k_1} \ldots p_r^{k_r}) = (p_1 - 1)\, p_1^{k_1 - 1} \ldots (p_r - 1)\, p_r^{k_r - 1} \ .$$

> La seconde assertion est une conséquence immédiate de la première, démontrons donc celle-ci.

D'après la démonstration du théorème, lorsque a et b sont deux entiers positifs, on a un isomorphisme d'anneaux

$$\mathbf{Z}/a\,b\,\mathbf{Z} \approx \mathbf{Z}/a\,\mathbf{Z} \times Z/b\,\mathbf{Z} \ .$$

Dans cet isomorphisme, les éléments inversibles s'envoient sur les éléments inversibles, d'où un isomorphisme de groupes (multiplicatifs)

$$G(a\,b) \approx G(a) \times G(b) \ ;$$

en prenant le cardinal de chaque membre on trouve la relation cherchée. <

2. Démonstration constructive .

La démonstration précédente du théorème chinois a le défaut majeur de ne pas fournir d'algorithme pour le calcul de x (autre que la recherche systématique de cette solution parmi les entiers $0, 1, \ldots, mn - 1 \ldots !$) .

Voici une autre démonstration qui, cette fois, fournit un algorithme pour calculer efficacement une solution entière x du système de congruences

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

du théorème chinois.

Soient donc m et n deux entiers premiers entre eux. Par l'algorithme d'Euclide, on sait calculer deux entiers u et v tels que

$$um + vn = 1 .$$

Alors l'entier

$$x = bum + avn$$

vérifie

$$x \equiv avn \equiv a \pmod{m}$$

et

$$x \equiv bvm \equiv b \pmod{n} ,$$

c'est donc une solution du système considéré .

Exemple : Résoudre le système

$$x \equiv 13 \pmod{151} \quad \text{et} \quad x \equiv 31 \pmod{131}.$$

On a vu que $59 \cdot 151 - 68 \cdot 131 = 1$, on peut donc prendre

$$x = (31 \times 59 \times 151 - 13 \times 68 \times 131) \bmod (151 \times 131) = 2127.$$

3. Calculs effectifs.

Soient $m_1, \ldots, m_k$ des entiers positifs deux à deux premiers entre eux, et M le produit de ces entiers. On cherche un algorithme de calcul de l'isomorphisme

$$\psi : \mathbf{Z}/M\mathbf{Z} \to \prod_{i=1}^{k} (\mathbf{Z}/m_i\mathbf{Z})$$

et de l'isomorphisme réciproque ψ^{-1}.

Le calcul de ψ est immédiat :

$$\psi(x) = (x \bmod m_1, \ldots, x \bmod m_k).$$

Pour calculer l'application réciproque, on peut procéder ainsi. Posons

$$M_i = M / m_i \qquad (\text{donc } (M_i, m_i) = 1).$$

On calcule ensuite des entiers $e_1, \ldots, e_k$ tels que

$$e_i M_i \equiv 1 \bmod m_i.$$

On vérifie alors instantanément que

$$\psi^{-1}(a_1, \ldots, a_k) = (a_1 e_1 M_1 + \ldots + a_k e_k M_k) \bmod M.$$

Comme on vient de le voir, les nombres e_i peuvent être calculés par l'algorithme d'Euclide ou par le théorème d'Euler.

11. Les nombres premiers .

Rappelons qu'un nombre entier au moins égal à deux est dit premier si ses seuls diviseurs positifs sont 1 et lui-même.

Dans la suite de ce chapitre, la lettre p désignera toujours un nombre premier.

De la définition d'un nombre premier, il résulte aisément que

$$\varphi(p) = p - 1$$

et, d'après le paragraphe précédent, $\mathbf{Z}/p\mathbf{Z}$ est un corps.

Le théorème 4 a la conséquence fondamentale suivante.

THEOREME 9 (Fermat) . – Soient p un nombre premier et a un entier non divisible par p , alors

$$a^{p-1} \equiv 1 \pmod{p}.$$

COROLLAIRE . – Soient p un nombre premier et a un entier quelconque, on a

$$a^p \equiv a \pmod{p}.$$

> En effet : lorsque p ne divise pas a c'est une conséquence évidente du théorème, sinon les deux membres de la relation du corollaire sont égaux à zéro. <

Remarque : Le théorème de Fermat fournit une condition nécessaire de primalité ; cependant cette condition n'est pas suffisante. Il existe des nombres - appelés **nombres de Carmichael** - qui vérifient la conclusion du théorème de Fermat, mais qui ne sont pas premiers, le plus petit d'entre eux est 561 . On ignore s'il y a ou non une infinité de nombres de Carmichael.

Le résultat suivant est bien connu.

THEOREME 10 . – Tout nombre entier au moins égal à deux est égal à un produit de facteurs premiers, de plus - à l'ordre des coefficients près - cette décomposition est unique.

On en déduit la proposition suivante.

COROLLAIRE . – Si m et n sont deux entiers positifs respectivement de la forme

$$m = p_1^{a_1} \dots p_r^{b_r} \quad \text{et} \quad n = p_1^{b_1} \dots p_r^{b_r}$$

où les p_i sont des nombres premiers et les a_i et b_i des nombres positifs ou nuls. Alors le p.g.c.d. de m et n est donné par la formule

$$\text{p.g.c.d.}\,(m, n) = p_1^{c_1} \dots p_r^{c_r} ,$$

où $c_i = \min \{ a_i , b_i \}$, $1 \leq i \leq r$;

tandis que le p.p.c.m. de m et n vaut

$$\text{p.p.c.m.}\,(m, n) = p_1^{d_1} \dots p_r^{d_r} ,$$

où $d_i = \max \{ a_i , b_i \}$, $1 \leq i \leq r$.

EXERCICES

1. Soient b_1 , b_2 ... des entiers ≥ 2 . Pour $n \geq 1$, on pose $B_n = b_1\, b_2 \ldots b_n$.

Démontrer que tout entier naturel a s'écrit d'une manière et d'une seule sous la forme

$$a = a_0 + a_1 B_1 + a_2 B_2 + \ldots \quad ,$$

avec pour tout i les inégalités

$$0 \leq a_i < b_{i+1} \ .$$

Déterminer un algorithme de calcul des entiers a_i .

2. Soient a_1 , a_2 , ... , a_k , ... des entiers strictement positifs. Démontrer que si les entiers a_i vérifient la condition

$$a_i > a_1 + a_2 + \ldots + a_{i-1} \quad \text{pour tout } i$$

alors un entier positif quelconque n s'écrit d'une manière au plus sous la forme

$$n = a_1 x_1 + a_2 x_2 + \ldots \quad , \ x_i \in \{ 0, 1 \} \ .$$

Lorsque la suite (a_i) vérifie cette condition, donner un algorithme qui, étant donné l'entier n ,

. soit calcule les x_i si n est de la forme ci-dessus,

. soit indique que n n'est pas de cette forme .

3. Soit (F_n) la suite des nombres de Fibonacci définie par $F_1 = 1$, $F_2 = 2$ et la condition $F_n = F_{n-1} + F_{n-2}$ pour $n \geq 3$.

Démontrer que tout entier positif a peut s'écrire

$$a = x_1 F_1 + x_2 F_2 + x_3 F_3 \ldots \quad , \; x_i \in \{0, 1\} .$$

Cette écriture est-elle unique ?

4. Dans l'étude de l'algorithme de Karatsuba, on a négligé le fait que certains entiers intermédiaires pouvaient avoir une longueur supérieure à $m = n / 2$. En effet les nombres $a + b$ et $c + d$ sont de longueur m et pour calculer leur produit par une procédure de multiplication d'entiers de taille m il faut décomposer les opérations. On pose

$$a + b = \alpha 2^m + \beta \; , \; c + d = \gamma 2^m + \delta \; , \text{ où } \alpha \in \{0, 1\} .$$

De sorte que

$$(a + b)(c + d) = \alpha\gamma 2^n + (\alpha\delta + \beta\gamma) 2^m + \beta\delta .$$

On constate que ce produit est décomposé en les opérations suivantes

- produit des deux bits α et γ,
- somme $\alpha\delta + \beta\gamma$ (rappelons que $\alpha \in \{0, 1\}$),
- produits par certaines puissances de deux (= décalages),
- produit des deux entiers β et δ, de taille m.

Démontrer que l'estimation donnée du coût de l'algorithme est correcte.

5. Soient a et b deux constantes ≥ 0 et k un entier > 1. On suppose que T est une fonction croissante, $T : \mathbf{N} \to \mathbf{R}$, qui vérifie

$$T(n) \leq \begin{cases} b & \text{si } n = 1, \\ a\,T(n/k) + b\,n & \text{si } n = k\,n' \ (n' \text{ entier}). \end{cases}$$

Démontrer les majorations

$$T(n) = \begin{cases} O(n) & \text{si } a < k, \\ O(n \operatorname{Log} n) & \text{si } a = k, \\ O(n^{\operatorname{Log} a / \operatorname{Log} b}) & \text{si } a > k. \end{cases}$$

6. Soit $T : \mathbf{N} \to \mathbf{R}$, une fonction croissante qui vérifie $T(1) = 1$.

Etudier le comportement asymptotique de T dans les cas suivants :

(i) $T(n) = a\,T(n-1) + b\,n^c$,

(ii) $T(n) = T(n/2) + b\,n^c$,

(iii) $T(n) = T(n/2) + b\,n(\operatorname{Log} n)^c$,

où a, b et c sont des constantes strictement positives.

7. Soit $(F_n)_{n \geq 0}$ la suite de Fibonacci définie par les conditions

$$F_0 = F_1 = 1$$

et

$$F_n = F_{n-1} + F_{n-2} \quad \text{pour } n \geq 2.$$

Démontrer la minoration

$$F_n \geq \alpha^{n-1} \quad \text{pour } n \geq 0 \quad , \text{où } \alpha = (1 + \sqrt{5})/2.$$

8. On pose

$l(n)$ = le nombre minimal r tel qu'il existe une suite $a_0, a_1, ..., a_r$ avec les conditions $a_0 = 1$, $a_n = r$ et, pour tout $i = 1, ..., r$, il existe j, k tels que l'on ait $a_i = a_j + a_k$, où $k \leq j < i$.

1°) Quel est le lien entre $l(n)$ et le calcul de x^n ?

2°) Démontrer que

(i) $l(n) \leq \log n + s(n) - 1$,

(ii) $l(mn) \leq l(m) + l(n)$.

3°) Soient a et b deux entiers, $a > b \geq 0$. Démontrer que

$$l(2^a) = a \quad \text{et} \quad l(2^a + 2^b) = a + 1 .$$

9. Soient B et B' deux entiers fixés ≥ 2 . Démontrer que le coût $C(n)$ de la conversion

$$(a_1, ..., a_n)_B \rightarrow (a'_1, ..., a'_m)_{B'}$$

vérifie

$$C(n) = O(M(n) \operatorname{Log} n) .$$

10. On considère l'algorithme suivant.

algorithme ? ;

données : a , b entiers , a > b > 0 ;

 # tant que b > 0 **faire**

début

r := min(a **mod** b , b - (a **mod** b)) ;

a := b ; b := r ;

fin ;

d := a . #

1°) Démontrer que l'algorithme se termine avec $d = \text{p.g.c.d.}(a, b)$.

2°) Majorer le nombre de passages dans la boucle.

3°) Comment modifier l'algorithme pour qu'il fournisse deux entiers u et v tels que

$$u\,a + v\,b = 1$$

11. Supposons que l'entier a soit premier avec les entiers $n_1, n_2, \ldots, n_k$. Démontrer que l'entier a est premier avec le produit $n_1 \ldots n_k$.

12. Soient a, b, c trois entiers positifs. Démontrer la formule

$$((a, b), c) = (a, (b, c)).$$

13. Soient a, b, c trois entiers positifs. Démontrer l'implication

$$c \mid a\,b \;\Rightarrow\; c \mid (a, c).(b, c).$$

14. Soient x, y, z trois nombres réels ≥ 0. Démontrer la relation

$$\max\{x,y,z\} = x + y + z - \min\{x,y\} - \min\{y,z\} - \min\{z,x\} + \min\{x,y,z\}.$$

En déduire la formule

$$[a, b, c] = \frac{a\,b\,c}{(bc, ac, ab)}.$$

15. Etudier l'équation

$$a\,x \equiv b \pmod{m}$$

dans le cas d'un entier m quelconque ≥ 2.

16. Etudier l'équation en nombres entiers

$$a\,x + b\,y = c\,.$$

17. Soient a, b, c, d, e, f et m des entiers donnés, $m > 0$. Etudier le système

$$a\,x + b\,y \equiv e \pmod{m}\,,$$

$$c\,x + d\,y \equiv f \pmod{m}\,.$$

Appliquer votre méthode pour résoudre le système

$$2\,x + 3\,y \equiv 1 \pmod{21}\,,$$

$$4\,x + 2\,y \equiv 5 \pmod{21}\,.$$

18. On reprend les notations du paragraphe sur le théorème chinois.

1°) Démontrer que les entiers e_i vérifient

$$e_i^2 \equiv 1 \pmod{M} \quad \text{pour} \quad 1 \leq i \leq k\,,$$

et

$$e_i\,e_j \equiv 0 \pmod{M} \quad \text{pour} \quad 1 \leq i < j \leq k\,.$$

Les e_i constituent donc des idempotents "orthogonaux" de l'anneau $\mathbf{Z}/M\mathbf{Z}$.

2°) Soit A un entier qui vérifie

$$A \equiv a_i \pmod{m_i} \quad \text{pour} \quad 1 \leq i \leq k\,.$$

Démontrer qu'il existe un entier E tel que

$$\frac{A}{M} = E + \sum_{i=1}^{k} \frac{a_i}{m_i}\,.$$

C'est la "décomposition en éléments simples" de la fraction A/M.

Démontrer en outre que cette écriture est unique si on suppose que les entiers a_i vérifient la condition $0 \leq a_i < m_i$ pour $1 \leq i \leq k$.

19. a) Démontrer qu'il existe une infinité de nombres premiers . (La preuve d'Euclide consiste à considérer le produit $2 . 3 . \ldots . p + 1$ et à démontrer que ce produit n'est divisible par aucun nombre premier $\leq p$.)

b) Démontrer qu'il existe une infinité de nombres premiers de la forme $4 n + 3$.

20. On considère l'algorithme suivant qui calcule l'inverse d'une fraction binaire.

algorithme calcul d'un inverse par la méthode de Newton ;

données : n , $v = (0 . v_1 v_2 \ldots v_n)$, $v_1 = 1$, $v_i \in \{ 0 , 1 \}$;

\# $z := [32 / (4 v_1 + 2 v_2 + v_3)] / 4$; $k := 0$; $h := 1$;

tant que $h < n$ **faire**

début

$h := 2 h$ { ici $h = 2^{k+1}$ } ; $V_k := (0 . v_1 \; v_2 \ldots v_{h+3})_2$;

$z := 2 z - V_k z^2$ { calcul exact ! } ;

$z := [2^{h+1} z + 0.5] 2^{-h-1}$; $k := k + 1$;

fin . \#

Démontrer que

(i) $0 < z \leq 2$,

(ii) $| z - 1 / v | \leq 2^{-h}$ avec $h = 2^k$, au bout de k étapes.

En déduire que le coût $C (n)$ de cet algorithme est

$$2 M (4 n) + 2 M (2 n) + \ldots . + O (n)$$

et donc que l'hypothèse habituelle,

$$M (2 m) \geq 2 M (m) \quad \text{pour tout } m ,$$

implique

$$C (n) \leq 4 \; M (4 n) + O (n) .$$

21. Soient a et n deux entiers ≥ 2. Démontrer que n divise $\varphi(a^n - 1)$.

[Appliquer le théorème de Lagrange.]

22. Soit p un nombre premier.

Démontrer les congruences

$$\binom{p-1}{j} \equiv (-1)^j \pmod{p}, \quad 0 \leq j \leq p-1.$$

En déduire que si a et b sont deux éléments d'un anneau tels que

$$p\,a = p\,b = 0 \quad \text{et} \quad a\,b = b\,a$$

alors on a la formule

$$(a - b)^{p-1} = \sum_{j=0}^{p-1} a^j\, b^{p-1-j}.$$

23. Soient p un nombre premier, k et m deux entiers vérifiant $1 \leq k < p^m$. Soit p^r la plus grande puissance de p qui divise k. Démontrer que p^{m-r} est la plus grande puissance de p qui divise le coefficient du binôme

$$\binom{p^m}{k}.$$

24. Faire une comparaison détaillée des coûts $C_1(n)$ et $C_2(n)$ définis au § 7. 2.

CHAPITRE II

Arithmétique, compléments

1. Retour à G (n) .

1. Quelques lemmes sur les groupes finis.

Si x est un élément d'un groupe G , on rappelle que l'ordre de x , noté $\text{ordre}_G(x)$, ou encore ordre (x) quand il n'y a pas d'ambiguïté, est le plus petit des entiers $k > 0$ tels que $x^k = 1$ (l'élément neutre de G), s'il existe, sinon on pose $\text{ordre}_G(x) = \infty$.

L'ordre vérifie les propriétés suivantes.

PROPOSITION 1 . – Soient x et y deux éléments d'un groupe G qui commutent et d'ordres finis respectivement égaux à a et b . Alors

(i) $\text{ordre}_G(xy)$ divise l'entier p.p.c.m. (a , b),

(ii) $(a, b) = 1 \Rightarrow \text{ordre}_G(xy) = ab$.

> **(i)** Soit m le p.p.c.m. de a et b, alors

$$(xy)^m = x^m y^m = 1 .$$

(ii) Supposons les entiers a et b premiers entre eux et soient u et v deux entiers tels que

$$u\,a + v\,b = 1 .$$

Alors, la relation

$$(x\,y)^{ua} = x^{ua}\, y^{1-vb} = y$$

montre que b divise $\text{ordre}_G(x\,y)$. De même a divise $\text{ordre}_G(x\,y)$. Comme les entiers a et b sont premiers entre eux, le produit a b divise $\text{ordre}_G(x\,y)$. Par (i), $\text{ordre}_G(x\,y)$ divise a b . D'où la conclusion. <

PROPOSITION 2 . – Soit G un groupe fini commutatif. Alors G contient un élément dont l'ordre est un multiple de ordre (y) , pour tout y de G.

> Soit x un élément de G dont l'ordre est maximal et y un élément quelconque de ce groupe.

On raisonne par l'absurde. Supposons donc que l'ordre de y ne divise pas l'ordre de x . Cela implique l'existence d'un nombre premier p et d'un entier $h > 0$ tel que le nombre p^h divise ordre (y) sans diviser ordre (x) .

Posons

$$\text{ordre}(x) = p^{h'}.a \qquad \text{avec} \quad 0 \leq h' < h\,,\ (a\,,p) = 1\,,$$

$$\text{ordre}(y) = p^{h}.b \quad ,$$

$$x' = x^{p^{h'}} \quad \text{et} \quad y' = y^{b}.$$

Alors

$$\text{ordre}(x') = a \quad , \quad \text{ordre}(y') = p^h \ , \text{où} \quad (a\,,p^h) = 1,$$

et, d'après la proposition 1, on arrive à la contradiction

$$\text{ordre}(x'y') = p^h a > \text{ordre}(x) \ . <$$

PROPOSITION 3 . – Soit G un groupe fini possédant n éléments. Alors il y a équivalence entre les propriétés suivantes :

(i) G est cyclique,

(ii) pour tout diviseur d de l'entier n , G possède au plus d éléments dont l'ordre divise d,

(iii) pour tout diviseur d de n , G possède au plus $\varphi(d)$ éléments d'ordre d.

> (i) $\Rightarrow$ (ii) : Supposons G cyclique, engendré par l'élément x . Soit d un diviseur de n . Alors les éléments de G dont l'ordre divise d sont

$$1, x^m, x^{2m}, \ldots, x^{(d-1)m} \quad \text{où} \quad m = n/d .$$

D'où l'implication.

(ii) $\Rightarrow$ (iii) : Soit d un diviseur de n . Si G ne possède pas d'élément d'ordre d alors l'assertion (iii) est vraie ; sinon, soit x un élément de G d'ordre d . Alors les éléments $1, x, x^2, \ldots, x^{d-1}$ sont deux à deux distincts et l'ordre de chacun d'eux est un diviseur de d . Si la propriété (ii) a lieu alors ce sont les seuls éléments de G dont l'ordre divise d . Ainsi, les seuls éléments de G dont l'ordre est d sont les x^k avec $1 \leq k < d$ et $(k, d) = 1$; il y en a exactement $\varphi(d)$.

(iii) $\Rightarrow$ (i) : 1ère démonstration.

On suppose G commutatif. Alors, la proposition 2 montre que G contient un élément x dont l'ordre est le p.p.c.m. des ordres des éléments de G. Supposons G non cyclique, autrement dit supposons ordre (x) < n . Soit H le sous-groupe de G engendré par x et soit y un élément de G qui n'appartient pas à H. Si d est l'ordre de y alors d divise ordre (x) = Card (H) et H contient $\varphi(d)$ éléments d'ordre d. Ainsi G contient au moins $\varphi(d) + 1$ éléments d'ordre d . Contradiction.

Cette première démonstration suppose le groupe commutatif, en voici une seconde qui n'a pas ce défaut.

2 -ième démonstration (Gauss).

Soit d un diviseur de n, on désigne par $\psi(d)$ le nombre d'éléments de G dont l'ordre vaut d.

On sait depuis Lagrange que l'ordre de tout élément de G divise n, donc

$$(1) \qquad \text{Card}(G) = n = \sum_{d \mid n} \psi(d) .$$

Dans le cas particulier où $G = \mathbf{Z}/n\mathbf{Z}$, on a $\psi(d) = \varphi(d)$ pour tout diviseur de n et la relation (1) s'écrit alors

$$(2) \qquad n = \sum_{d \mid n} \varphi(d) .$$

Par conséquent, si la propriété (iii) a lieu, c'est à dire si $\psi(d) \leq \varphi(d)$ pour tout diviseur d de l'entier n, alors les relations (1) et (2) impliquent

$$\psi(d) = \varphi(d) \quad \text{pour tout diviseur } d \text{ de } n .$$

En particulier on a $\psi(n) = \varphi(n)$: G possède $\varphi(n)$ éléments d'ordre n, il est donc cyclique ! <

2. Application à G (p) .

L'étude précédente conduit aussitôt au résultat suivant.

THEOREME 1 . – Si p est un nombre premier alors le groupe G (p) est cyclique.

> Soit p un nombre premier, alors G (p) possède p - 1 éléments. Soit d un diviseur quelconque de p - 1 , alors l'équation $X^d = 1$ possède au plus d solutions dans le corps commutatif $\mathbf{Z} / p\mathbf{Z}$. Donc la condition (ii) de la proposition 3 est vérifiée, G (p) est bien cyclique. <

Un entier g de l'intervalle { 1, ... , p - 1 } est appelé un **élément primitif** modulo p si sa classe engendre G (p) .

Voici la liste des plus petits éléments primitifs modulo p pour $p \leq 19$.

p	2	3	5	7	11	13	17	19
g	1	2	2	3	2	2	3	2

Faisons la vérification pour $p = 17$: l'ordre de tout élément est 16 ou un diviseur strict de 16 et on a

$$3^4 = 81 \equiv 13 \quad , \quad 3^8 \equiv 13^2 = 169 \equiv -1$$

donc l'ordre de 3 est bien 16 .

En conséquence, si p est un nombre premier et si d divise p - 1 alors G (p) possède exactement (p - 1) / d éléments qui sont de la forme x^d, $x \in G(p)$.

En particulier, si p est impair alors la moitié des éléments de G(p) sont des carrés ; un entier a , non divisible par p , dont la classe modulo p est un carré est appelé un **résidu quadratique modulo p** , sinon on dit que c'est un **non-résidu quadratique modulo l'entier p** ; on définit le **symbole de Legendre** ,

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{si a est résidu quadratique modulo p,} \\ -1 & \text{sinon.} \end{cases}$$

Le symbole de Legendre vérifie les propriétés suivantes.

THEOREME 2 . – Soit p un nombre premier impair et a et b deux entiers non divisibles par p , alors

(i) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,

(ii) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$, (Euler).

> Soit g un élément primitif modulo p . Posons $a \equiv g^h$ et $b \equiv g^k$.

Alors

$$\left(\frac{a}{p}\right) = (-1)^h \ , \ \left(\frac{b}{p}\right) = (-1)^k \quad \text{et} \quad \left(\frac{ab}{p}\right) = (-1)^{h+k},$$

d'où la première assertion.

Pour démontrer (ii) on procède ainsi : Chacun des membres de la relation (ii) définit un endomorphisme de G (p) : c'est clair pour le membre de droite, et pour celui de gauche cela résulte de (i) (on considère que $-1 \in G(p)$) .

Comme G (p) est cyclique il suffit de vérifier la relation lorsque $a = g$. On a d'une part

$$\left(\frac{g}{p}\right) = -1 ,$$

d'autre part, posons $y = g^{(p-1)/2} \bmod p$, alors

$$y^2 \equiv g^{p-1} \equiv 1 \quad \text{et} \quad y \neq 1 , \quad \text{donc} \quad y = -1.$$

D'où la conclusion. <

Si n est un entier impair et si a est un entier premier avc n , on définit le **symbole de Jacobi** par la formule

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{\alpha_i} \quad \text{si} \quad n = p_1^{\alpha_1} \ldots p_r^{\alpha_r} \quad (p_i \text{ distincts}) .$$

3. Structure de $G(p^k)$, $k \geq 2$, p premier impair.

On sait que le groupe $G(p^k)$ possède $\varphi(p^k) = (p-1)\,p^{k-1}$ éléments et que le groupe G (p) est cyclique. Soit a un entier dont la classe modulo p engendre G (p) , alors l'ordre de a modulo p^k est un multiple de $p - 1$.

Par ailleurs, considérons l'élément $b = 1 + p$. On a

$$(*) \qquad b^{p^h} \equiv 1 + p^{h+1} \pmod{p^{h+2}} .$$

En effet, cette congruence est vraie pour $h = 0$ et si elle est vérifiée au rang h alors

$$b^{p^h} = 1 + p^{h+1} + u\,p^{h+2} , \quad u \text{ entier},$$

et

$$b^{p^{h+1}} = (1 + p^{h+1}(1 + u\,p))^p = 1 + p^{h+2} + v\,p^{h+3} , \quad v \text{ entier},$$

ce qui montre que la formule (*) est encore vraie au rang $h + 1$.

Cette formule, appliquée pour $h = k - 2$ et $h = k - 1$ montre que l'élément b est d'ordre p^{k-1} modulo p^k.

Nous sommes maintenant en mesure de démontrer que $G(p^k)$ est cyclique. En fait, deux cas sont possibles : ou bien a engendre $G(p^k)$, ou bien l'élément a n'engendre pas $G(p^k)$.

Si le premier cas a lieu il n'y a rien à démontrer. Supposons donc que a n'engendre pas $G(p^k)$. Considérons alors l'élément $x = a(1 + p) \mod p^k$, et soit t son ordre. On a $x \equiv a \mod p$, donc t est un multiple de $p - 1$. De plus, du fait que a n'engendre pas $G(p^k)$, on a

$$a^{p^{k-2}(p-1)} \equiv 1 \quad (p^k)$$

et donc

$$x^{p^{k-2}(p-1)} \not\equiv 1 \mod p^k.$$

Il en résulte que t est égal à $\varphi(p^k)$, autrement dit, que x engendre $G(p^k)$.

En résumé, nous avons démontré le théorème suivant.

THEOREME 3. – Soient p un nombre premier impair et k un entier ≥ 2. Alors le groupe $G(p^k)$ est cyclique. De plus, si a est un entier dont la classe modulo p engendre $G(p)$ alors

. ou bien a engendre $G(p^k)$,

. ou bien $a(1 + p)$ engendre $G(p^k)$.

Exemples.

. $p = 3$, $k = 4$: Prenons $a = 2$, alors $a^6 = 64 \equiv -17 \quad (81)$, $a^{12} \equiv -35$ et enfin $a^{18} \equiv 28$, ce qui montre que 2 engendre $G(81)$.

. $p = 5$, $k = 3$: Prenons $a = 3$, on vérifie que $a^{20} \equiv 26 \quad (125)$, ce qui permet de montrer que 3 engendre $G(125)$.

4. Structure de $G(2^k)$.

Nous venons de démontrer que pour p premier impair et k positif quelconque, le groupe $G(p^k)$ est cyclique. Le cas de l'entier $p = 2$ est exceptionnel et la structure du groupe $G(2^k)$ dépend de k. C'est ce que nous allons voir maintenant.

Si $k = 1$, $G(2) = \{1\}$ est trivial.

Si $k = 2$, $G(4) = \{1, -1\}$ est cyclique, engendré par -1.

Pour $k \geq 3$, remarquons que l'on a pour tout entier x impair

$$x^{2^{k-2}} \equiv 1 \quad (2^k) .$$

En effet, cette congruence est vraie pour $k = 3$ (pour x impair on a $x = 4u \pm 1$ et donc $x^2 \equiv 1$ modulo 8) et si elle a lieu au rang k pour x entier impair quelconque on a

$$x^{2^{k-2}} = 1 + v\,2^k \quad \text{et} \quad x^{2^{k-1}} = (1 + v\,2^k)^2 \equiv 1 \quad (2^{k+1}) .$$

Ceci montre que pour $k \geq 3$, le groupe $G(2^k)$ n'est pas cyclique.

Le lemme ci-dessous est l'analogue de la congruence (*) du paragraphe précédent.

LEMME 1. – Pour tout entier $h \geq 0$ on a

$$5^{2^h} \equiv 1 + 2^{h+2} \pmod{2^{h+3}} .$$

› C'est vrai pour $h = 0$. Supposons ceci démontré au rang h alors

$$5^{2^{h+1}} = (1 + 2^{h+2}(1 + 2w))^2 \equiv 1 + 2^{h+3} \pmod{2^{h+4}} .$$

D'où la conclusion. ‹

En appliquant le lemme pour $h = k - 3$ on voit que la classe de 5 est d'ordre 2^{k-2} dans $G(2^k)$, autrement dit qu'elle engendre un sous-groupe H d'indice 2 dans le groupe $G(2^k)$.

Montrons enfin que -1 n'appartient pas à H. Si tel était le cas, on aurait

$$5^h \equiv -1 \quad (2^k) \quad \text{avec} \quad 0 \leq h < 2^{k-2}$$

et donc

$$5^{2h} \equiv 1 \quad (2^k),$$

ce qui implique $h = 2^{k-3}$ et le lemme fournit une contradiction.

Nous avons donc démontré le résultat suivant.

THEOREME 4. – Pour $k < 3$ le groupe $G(2^k)$ est cyclique. Par contre pour tout entier $k \geq 3$ le groupe $G(2^k)$ n'est pas cyclique, il est constitué par les classes des éléments de la forme $\pm 5^h$, $0 \leq h < 2^{k-2}$, et il est donc isomorphe au produit direct

$$(\mathbf{Z}/2^{k-2}\mathbf{Z}) \times \mathbf{Z}/2\mathbf{Z}.$$

5. Structure de $G(n)$.

Supposons que $n = p_1^{a_1} \ldots p_t^{a_t}$ soit la décomposition de n en facteurs premiers, alors

$$(*) \qquad G(n) \approx \prod_{i=1}^{t} G(p_i^{a_i}).$$

Si on désigne par $\lambda(n)$ le p.p.c.m. des ordres des éléments de $G(n)$, l'isomorphisme précédent implique

$$\lambda(n) = \text{p.p.c.m.} \left(\lambda(p_1^{a_1}), \ldots, \lambda(p_t^{a_t})\right).$$

Par ailleurs, les théorèmes ci-dessus montrent que

$$\lambda(2^k) = 2^{k-2} \text{ si } k \geq 3,\ \lambda(2) = 1,\ \lambda(4) = 2,$$

et

$$\lambda(p^k) = (p-1)\,p^{k-1} \text{ si } p \text{ est un nombre premier impair.}$$

D'où la détermination de $\lambda(n)$.

En particulier, on obtient

$$n \text{ impair} \Rightarrow \lambda(n) = p_1^{a_1 - 1} \ldots p_t^{a_t - 1} \text{ . p.p.c.m. } (p_1 - 1, \ldots, p_t - 1),$$

donc $\lambda(n)$ divise $2^{1-t}\varphi(n)$ pour n impair.

Notons que $G(n)$ est cyclique si, et seulement si, on a $\lambda(n) = \varphi(n)$. Pour n' impair et $n = n'$ ou $n = 2n'$, cette condition équivaut à $\omega(n') = 1$. Pour $n = 4n'$, avec n' quelconque, on a $\lambda(n) < \varphi(n)$.

D'où le résultat suivant.

PROPOSITION 5. – Soient n un entier sans facteurs carrés, a un entier quelconque et e un entier qui vérifie

$$e \equiv 1 \text{ modulo } \lambda(n),$$

alors on a

$$a^e \equiv a \pmod{n}.$$

> Grâce au théorème chinois, on se ramène au cas où n est premier. La proposition résulte alors de la congruence $a^p \equiv a \pmod{p}$: théorème de Fermat. <

2. Tests de primalité .

1. Un théorème général .

Le lemme technique suivant nous sera très utile.

LEMME 1 . – Soit n un entier impair,

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r} ,$$

on pose $v = v_2 (n - 1)$, où $v_2 (m)$ est le plus grand entier k tel que 2^k divise m.

Si $v' = \inf \{ v_2 (p_i - 1) \}$, on a toujours $v \geq v'$, et l'égalité a lieu si, et seulement si, le nombre de facteurs premiers p_i d'exposant impair, vérifiant $v_2 (p_i - 1) = v'$, est impair.

> Supposons les p_i ordonnés par $v_2 (p_i - 1)$ croissants. On a

$$n - 1 = \sum_{i=1}^{r} (p_i^{\alpha_i} - 1) (p_{i+1}^{\alpha_{i+1}} \dots p_r^{\alpha_r}) .$$

D'où aussitôt l'inégalité $v \geq v'$.

Supposons de plus que les indices i pour lesquels $v_2 (p_i - 1) = v'$ et α_i est impair sont $1, 2, \dots , k$ alors $2^{v'+1}$ divise les termes de la somme ci-dessus d'indice $i > k$, et seulement ceux-là, on a donc

$$n - 1 \equiv k 2^{v'} \pmod{2^{v'+1}} ,$$

d'où la seconde assertion. <

Considérons les propriétés suivantes d'un entier n tel que $n - 1 = 2^{v}n'$, n' impair.

$P(n)$: n est premier,

$Q(n)$: n est **quadratfrei**, (c'est à dire non divisible par le carré d'un nombre premier)

$F(n)$: $\forall a, (a, n) = 1 \Rightarrow a^{n-1} \equiv 1 \pmod{n}$,

$E(n)$: $\forall a, (a, n) = 1 \Rightarrow a^{(n-1)/2} \equiv \pm 1 \pmod{n}$,

$S(n,a)$: $(a,n) = 1$ et $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$,

$M(n,a)$: $(a,n) = 1$ et $a^{n'} \bmod n \neq 1 \Rightarrow \exists h, 0 \leq h < v, a^{2^h} \equiv -1 \pmod{n}$.

THEOREME 5. – Soit n un entier impair, $n - 1 = 2^{v}n'$, n' impair.

Alors on a les implications suivantes, (p désigne toujours un nombre premier)

$P(n) \Rightarrow E(n) \Rightarrow F(n)$,

$\forall a$, $(a, n) = 1 \Rightarrow (P(n) \Rightarrow M(n, a))$,

$M(n, a) \Rightarrow S(n, a)$,

$F(n) \Leftrightarrow Q(n)$ et $(p \mid n \Rightarrow (p - 1) \mid (n - 1))$,

$F(n) \Rightarrow \omega(n) \neq 2$, (où $\omega(n)$ désigne le nombre de p premiers, $p \mid n$)

$E(n) \Leftrightarrow P(n)$ ou $\{ Q(n)$ et $(p \mid n \Rightarrow (p - 1) \mid ((n - 1)/2)) \}$.

Enfin, soit $S(n)$ la propriété

$S(n)$: $\forall a, (a, n) = 1 \Rightarrow S(n, a)$

alors

$S(n) \Rightarrow P(n)$.

> Démonstration.

$P(n) \Rightarrow E(n) \Rightarrow F(n)$: c'est clair.

$\forall$ **a** , **(a, n) = 1** $\Rightarrow$ **(P (n)** $\Rightarrow$ **M (n, a)) :**

En effet, soit a un entier premier avec n , n premier, et tel que, modulo n , on ait la relation $a^{n'} \neq 1$, alors il existe un entier h , $0 \leq h < v$ tel que

$$y := a^{2^h n'} \neq 1 \quad \text{et} \quad a^{2^{h+1} n'} = 1 ,$$

alors y vérifie

$$y^2 = 1 \quad \text{et} \quad y \neq 1 ,$$

et comme n est premier ceci implique $y = -1$.

M (n, a) $\Rightarrow$ **S (n, a) :**

Soit a un entier premier avec n . Posons

$$\chi(a) = a^{(n-1)/2} \left(\frac{a}{n}\right) \mod n .$$

Il s'agit de montrer que M (n, a) implique $\chi(a) = 1$.

1°) Supposons $a^{n'} \equiv 1$ alors

$$a^{(n-1)/2} \equiv 1$$

et pour tout diviseur premier p de n , on a

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)^{n'} = 1 .$$

et donc $\chi(a) = 1$.

2°) Supposons maintenant que $a^{n'} \neq 1$ modulo n et que M (n, a) soit vrai. Alors, on a

$$a^{2^h n'} \equiv -1 \quad \text{et} \quad a^{2^{h+1} n'} \equiv 1 \quad \text{avec} \quad 0 \leq h < v .$$

Comme plus haut, soit

$$n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$$

la décomposition de n en facteurs premiers.

D'après la formule d'Euler, on a

$$h = v_2(p_i - 1) - 1 \Rightarrow \left(\frac{a}{p_i}\right) = -1,$$

$$h < v_2(p_i - 1) - 1 \Rightarrow \left(\frac{a}{p_i}\right) = 1.$$

Supposons d'abord $h = v - 1$. On est alors dans le cas $v = v'$ du lemme précédent, ce qui montre que l'on a (avec les notations de la démonstration de ce lemme) ,

$$\left(\frac{a}{p_i}\right) = 1 \quad \Leftrightarrow \quad i = k + 1, \ldots, r.$$

De plus $\alpha_1 + \ldots + \alpha_k$ est impair, donc

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \ldots \left(\frac{a}{p_k}\right)^{\alpha_k} \left(\frac{a}{p_{k+1}}\right)^{\alpha_{k+1}} \ldots \left(\frac{a}{p_r}\right)^{\alpha_r} = -1.$$

Par définition de h , on a $a^{(n-1)/2} = -1$, donc $\chi(a) = 1$.

Reste le cas où $h < v - 1$. On a alors

$$a^{(n-1)/2} = 1 \quad \text{et} \quad \left(\frac{a}{p_i}\right) = 1 \quad \text{pour} \quad i = 1, 2, \ldots, r.$$

Donc encore $\chi(a) = 1$.

$F(n) \Leftrightarrow Q(n)$ et $(p \mid n \Rightarrow (p - 1) \mid (n - 1))$:

Si n n'est pas quadratfrei, soit p un nombre premier tel que $n = p^{\alpha} m$, avec $\alpha \geq 2$ et $(m, p) = 1$, alors $G(n) \cong G(p^{\alpha}) \times G(m)$ et G (n) contient un élément a d'ordre p , comme p ne divise pas $n - 1$ on ne peut avoir $a^{n-1} \equiv 1 \pmod{n}$.

D'où l'implication $F(n) \Rightarrow Q(n)$.

Si p divise n , alors G (n) contient un élément d'ordre $p - 1$ et par conséquent , si la propriété F (n) a lieu alors $p - 1$ divise $n - 1$.

La réciproque est évidente.

F (n) $\Rightarrow$ ω (n) $\neq$ 2 :

Supposons maintenant n de la forme $n = p\,q$ avec p et q premiers impairs, et par exemple $p > q$. Alors $p - 1 \mid n - 1$.

On a aussi

$$p - 1 \mid (p - 1)(q - 1),$$

donc, par différence,

$$p + q - 2 = s(p - 1),$$

avec $s \geq 2$. D'où $q \geq p$, contradiction.

E (n) $\Leftrightarrow$ P (n) ou { Q (n) et (p | n $\Rightarrow$ (p - 1) | ((n - 1) / 2)) } :

Supposons E (n) vrai et n non premier, on sait déjà que n doit être quadratfrei.

Soit p un diviseur premier de n , du fait que G (p) est cyclique et que p et n / p sont premiers entre eux, il existe un élément a de G (n) tel que

$$\text{ordre}(a \bmod p) = p - 1 \quad \text{et} \quad a \equiv 1 \pmod{n/p}.$$

Alors

$$\left(a^{(n-1)/2} \equiv \pm 1 \bmod n \quad \text{et} \quad a \equiv 1 \pmod{n/p}\right) \Rightarrow a^{(n-1)/2} \equiv 1,$$

d'où le fait que $p - 1$ divise $(n - 1)/2$.

La réciproque est encore évidente.

S (n) $\Rightarrow$ P (n) :

Supposons n non premier ($n = p_1 \ldots p_r, r \geq 2$) et $\chi(a) = 1$ pour tout a de G (n). On sait déjà que les p_i sont deux à deux distincts. Soit a un élément de G (n) tel que

$$\left(\frac{a}{p_1}\right) = -1 \quad \text{et} \quad a \equiv 1 \pmod{p_2 \ldots p_r}.$$

Alors l'hypothèse $\chi(a) = 1$ implique

$$a^{(n-1)/2} \equiv -1 \pmod{n},$$

ce qui contredit la condition $a \equiv 1 \pmod{p_2}$. Ceci achève la démonstration. <

2. Un critère de primalité .

Le théorème précédent permet de donner un critère de primalité très simple :

THEOREME 6 . – Soit n un entier, $n > 1$. Alors le nombre n est premier si, et seulement si, la condition C (n) suivante a lieu

$$\left(\forall a, (a, n) = 1 \Rightarrow a^{(n-1)/2} \equiv \pm 1 \bmod n \right) \text{ et } \left(\exists a, a^{(n-1)/2} \equiv -1 \bmod n \right).$$

> Il est clair que la condition est nécessaire. Montrons qu'elle est suffisante. Pour cela on raisonne par l'absurde en supposant qu'un certain entier $n \geq 2$ vérifie C (n) sans être premier. Le théorème 5 montre que n est quadratfrei, puisque

$$C(n) \Rightarrow E(n) \Rightarrow F(n) \Rightarrow Q(n).$$

Supposons que x soit un entier tel que $x^{(n-1)/2} \equiv -1 \bmod n$ et que p soit un diviseur premier de n , $n = p\,n'$ avec $n' > 1$ (et $(p,n') = 1$) . D'après le théorème chinois, il existe un entier a qui vérifie $a \equiv x \pmod p$ et $a \equiv 1 \pmod{n'}$.

On a alors

$$a^{(n-1)/2} \equiv x^{(n-1)/2} \equiv -1 \ (p) \quad \text{et} \quad a^{(n-1)/2} \equiv 1 \ (n')$$

ce qui contredit la condition $a^{(n-1)/2} \equiv \pm 1 \pmod n$. <

Le critère ci-dessus n'est pas très utile dans la pratique : si on trouve une valeur de a telle que l'on ait $a^{(n-1)/2} \neq \pm 1$ modulo n on saura que n n'est pas premier, mais tant que l'on trouve $a^{(n-1)/2} \equiv 1$ on ne peut rien conclure.

On peut aussi noter qu'il existe des nombres n non premiers impairs tels que tout entier a premier avec n vérifie $a^{(n-1)/2} \equiv 1 \pmod n$, les deux plus petits de ces nombres sont $1729 = 7 \times 13 \times 19$ et $2465 = 5 \times 17 \times 29$; on ignore actuellement s'il existe une infinité de tels nombres.

3. Tests élémentaires .

Soit n un entier impair ≥ 3 dont on veut savoir s'il est premier ou non. On va déduire plusieurs tests de primalité du théorème 5 .

1. Le test de Solovay-Strassen .

On vérifie que $\chi(a) = 1$ pour un certain nombre de valeurs de a , par exemple pour les choix $a = 2, 3, 5, 7, 11$ ... Si on trouve une valeur telle que $\chi(a) \neq 1$ on a prouvé que n n'est pas premier. Dans le cas contraire, se pose la question d'un test d'arrêt, elle sera abordée plus loin. On peut noter que si n n'est pas premier alors le caractère χ n'est pas trivial et son noyau est donc d'indice au moins deux dans $G(n)$, ce qui montre que la moitié au plus des éléments a de $G(n)$ vérifient $\chi(a) = 1$.

2. Le test de Miller - Rabin .

Soit $n - 1 = 2^{v} n'$, avec n' impair. Pour un certain nombre d'entiers a , on évalue l'expression $b = a^{n'} \bmod n$, et si $b \neq 1$ on calcule $b^{2}, b^{4}, b^{8} \ldots, b^{h}$ où h vérifie $h \leq 2^{v-1}$, jusqu'à ce qu'on ait trouvé la valeur -1 .

La situation est la même que précédemment : si on n'a pas rencontré la valeur -1 on sait que n n'est pas premier, sinon on essaie éventuellement une autre valeur de a .

On a vu au théorème 5 que la propriété $M(n, a)$ implique $S(n, a)$, donc ce test est au moins aussi puissant que le test de Solovay - Strassen.

3 . Etude du coût .

Soit N le nombre d'essais effectués par l'un ou l'autre des deux tests précédents, alors le nombre d'opérations élémentaires effectuées est en $O (N \operatorname{Log} n)$ et le coût (en utilisant des algorithmes de multiplication ordinaires) est en $O (N (\operatorname{Log} n)^3)$.

Supposons n non premier et que l'on effectue l'un de ces tests pour les nombres premiers successifs $a = 2, 3, 5, 7, 11, \ldots$ et soit A le plus petit entier positif qui vérifie à la fois $(A, n) = 1$ et $\chi (A) \neq 1$, alors on a

$$N \leq A \quad (\text{et même } N = O (A / \operatorname{Log} A) .$$

Reste à majorer A , mais c'est une question difficile. Les résultats dans ce domaine sont les suivants :

- on sait, grâce aux travaux de A. Weil, Vinogradov et Burgess que A vérifie

$$A = O (n^{1/4\sqrt{e}}) ;$$

- Ankeny et Montgomery ont montré que, si l'hypothèse de Riemann généralisée est vraie alors

$$A \leq c (\operatorname{Log} n)^2 ,$$

et d'après Oesterlé et Weinberger on peut prendre respectivement $c = 70$ et $c = 4$.

A la suite de travaux de Adleman , Pomerance et Rumely , ainsi que H. Lenstra et H. Cohen , on sait tester la primalité d'un entier n en un temps

$$O ((\operatorname{Log} n)^{c \operatorname{Log} \operatorname{Log} \operatorname{Log} n}) \quad , \; c = \text{constante} .$$

Mais la méthode est trop complexe pour être détaillée ici.

4. Statistiques sur $G(n)$.

Le résultat suivant précise le théorème 5.

PROPOSITION 6. – Soit n un nombre premier impair qui n'est pas un carré ni une puissance d'un nombre premier, disons

$$n = p_1^{e_1} \dots p_r^{e_r}.$$

On pose

$$F = \{ x \in G(n) ; x^{n-1} \equiv 1 \ (n) \},$$

$$E = \{ x \in G(n) ; x^{(n-1)/2} \equiv \pm 1 \ (n) \},$$

$$H = \{ x \in G(n) ; \chi(x) = 1 \}, \text{ (notations précédente)}.$$

Alors F, E et H sont des sous-groupes de $G(n)$ qui vérifient

$$F \supset E \supset H,$$

$$E = F \Rightarrow [E : H] = 2,$$

$$\text{Card}(F) = d_1 \dots d_r \text{ où } d_i = \text{p.g.c.d.}(n-1, p_i - 1).$$

> Posons $G = G(n)$ pour simplifier un peu les notations.

La congruence $x^{n-1} \equiv 1 \ (n)$ équivaut à l'ensemble des conditions

$$x^{n-1} \equiv 1 \ (p_i^{e_i}) \ , \ i = 1, \dots, r.$$

Comme chacun des groupes $G(p_i^k)$ est cyclique, il contient

$$d_i = \text{p.g.c.d.}(n-1, p_i^{e_i - 1}(p_i - 1)) = \text{p.g.c.d.}(n-1, p_i - 1)$$

solutions de la congruence

$$x^{n-1} \equiv 1 \ (p_i^{e_i}),$$

d'où la formule donnant le cardinal de F.

Soit t le nombre d'indices i tels qu'il existe $x \in G$ vérifiant $x^{(n-1)/2} \equiv -1$ modulo p_i. On a les possibilités suivantes

(i) $t = 0$ et alors $E = F = \{ x \in G ; x^{(n-1)/2} \equiv 1 \ (n) \}$,

(ii) $0 < t < r$, alors $E = \{ x \in G ; x^{(n-1)/2} \equiv \pm 1 \ (n) \}$

et $[F : E] = 2^t$,

(iii) $t = r$ et alors la relation évidente

$E = \{ x \in G ; x^{(n-1)/2} \equiv 1 \ (n) \} \cup \{ x \in G ; x^{(n-1)/2} \equiv -1 \ (n) \}$

montre que $[F : E] = 2^{r-1}$.

En ce qui concerne le groupe H les possibilités sont les suivantes :

- si $E = \{ x \in G ; x^{(n-1)/2} \equiv 1 \ (n) \}$ (cas (i) et (ii)) alors

$$\chi(n) = \left(\frac{x}{n}\right)$$

et, comme n n'est pas un carré, le symbole de Jacobi n'est pas trivial et on a

$[E : H] = 2$, donc $[F : H] \geq 2$,

- sinon (cas (iii)) on a $[F : H] \geq 2^{r-1} \geq 2$.

Conséquences : soit n un entier qui n'est pas premier.

- si n n'est pas quadratfrei, on a $[G : F] \geq 3$ donc $[G : H] \geq 6$, (exercice)

- si n est quadratfrei $[G : H] \geq 4$ sauf si $G = E$, c'est à dire si n vérifie la condition $(a, n) = 1 \Rightarrow a^{(n-1)/2} \equiv 1$ modulo n.

Dans ce dernier cas, on a $n \equiv 1 \mod 4$. Posons alors

$$H' = \{ x \in G ; x^{(n-1)/2^{\mu}} \equiv \pm 1 \ (\mathrm{mod}\, n) \}, \text{ où } \mu = v - v' - 1,$$

alors tout entier x qui satisfait au test de Miller-Rabin appartient à H'. Le même argument que plus haut montre que

$$[G : H'] = 2^{r-1} \geq 4.$$

En conséquence, on a toujours

$$\mathrm{Card} \{ x \in G ; x \text{ vérifie } M(x, n) \} \leq \mathrm{Card}(G(n))/4.$$

3. Factorisation des entiers .

Dans tout ce paragraphe, on cherche à factoriser un entier n positif (c'est à dire à décomposer n en produit de facteurs premiers, cf. chap. I, th. 10) . Sans que cela restreigne la généralité, on supposera n impair ≥ 3 .

1. Méthode par divisions successives .

La méthode scolaire est un cas particulier de la méthode suivante : On effectue successivement la division euclidienne de n par les entiers d_1 , ... , d_k d'une suite croissante qui contient la suite des nombres premiers.

On peut par exemple faire les choix suivants de la suite (d_k) :

- la suite des nombres impairs 3, 5, 7, 9, 11, 13, 15 ... ce qui conduit à un algorithme très simple, mais qui comporte évidemment un certain nombre de divisions inutiles;

- la suite des nombres premiers impairs 3, 5, 7, 11, 13, 17 ... ce qui est optimal en ce qui concerne le nombre de divisions effectuées, mais qui nécessite de connaître et d'avoir stocké les nombres premiers au plus égaux à $\sqrt{n}$;

- par exemple la suite 3, 5, 7, 11, 13, 17, 19, 23 , 29, 31, 37, 41, 43, 49 , ... des nombres 3 et 5 suivis des nombres impairs ni divisibles par 3 , ni divisibles par 5 .

Cette troisième possibilité présente les avantages suivants :

- On évite une forte proportion des opérations inutiles effectués lors de la première méthode ; par exemple en éliminant les multiples (stricts) de 3 dans la liste on économise 33 % des divisions réalisées au cours de la première version de l'algorithme, en éliminant les nombres impairs non premiers avec 15 (autres que 3 et 5) on économise plus de 46 % des opérations.

Plus généralement, en éliminant les nombres non premiers avec un entier k donné, on économise une proportion d'opérations égale à

$$(n - \varphi(n)) / n .$$

Pour $k = 105$ cette proportion dépasse 54 % .

- Il n'est pas nécessaire de stocker la suite (d_n), elle est égale à une union de progressions arithmétiques, et on peut la construire facilement par "criblage" .

A titre d'illustration, donnons l'algorithme de recherche du plus petit facteur premier de n .

```
Algorithme factorisation par divisions ;
données : n entier ≥ 2 ;
# m := n ; i := 0 ;
tant que m mod 2 = 0 faire
        début i := i + 1 ; T [i] := 2 ; m := m div 2 fin ;
a := 3 ;
tant que a ² <= m faire
  début tant que m mod a = 0 faire début i := i + 1 ; T [i] := a ; m := m div a
fin ;
        a := a + 2
  fin ;
si m > 1 alors début i := i + 1 ; T [i] := m fin ;
fin . #
```

Si P (n) désigne le plus grand facteur premier de n alors le nombre d'opérations de cet algorithme est en O (P (n)) , dans le pire des cas (i. e. quand n est le produit de deux nombres premiers distincts voisins de $\sqrt{n}$) ce nombre est de l'ordre de $\sqrt{n}$.

2 . Méthode de Fermat .

L'idée consiste à remplacer une factorisation $n = a\,b$, avec $a \geq b$, par la décomposition

$$n = x^2 - y^2 = (x + y)(x - y) \quad (\text{soit } x = (a+b)/2 \text{ et } y = (a-b)/2).$$

Pour $x = [\sqrt{n}]$, $[\sqrt{n+1}]$, ... on calcule $x^2 - n$ jusqu'à ce qu'on trouve un carré. Supposons n de la forme $n = p\,q$ avec $p \leq q$ et $p \leq n^{\alpha}$ (donc $\alpha \leq 1/2$) , alors on doit pousser le calcul jusqu'à $x > n^{1-\alpha}/2$, donc pour α fixé $< 1/2$ le coût de cette méthode n'est pas en $O(\sqrt{n})$. La méthode de Fermat n'est donc utile que si n possède un facteur proche de $\sqrt{n}$.

3. Méthode de Sherman - Lehman .

L'idée de cette méthode remonte à Legendre : si on trouve deux entiers a et b tels que $a^2 \equiv b^2 \pmod{n}$ et $a \neq \pm b$ modulo n alors le p.g.c.d. de $a+b$ et n est un facteur non trivial de n .

La procédure est la suivante :

(i) on cherche les diviseurs premiers de n jusqu'à $n^{1/3}$. Si aucun facteur n'a été trouvé l'entier n est de la forme $n = p\,q$ avec $n^{1/3} < p \leq q < n^{2/3}$ (on suppose toujours n non premier) .

(ii) pour $h = 1, 2, \ldots, [n^{1/3}]$ et $d = 0, 1, \ldots, 1 + [n^{1/6}/(4\sqrt{k})]$ on teste si le nombre $([(4kn)^{1/2}] + d)^2 - 4kn$ est un carré. Si tel est le cas, on a trouvé des entiers a et b comme plus haut ; comme $a+b$ et $|a-b|$ sont tous deux dans l'intervalle $]1, n[$ (pour $n > 6$) , ceci fournit une factorisation de n .

Il reste à montrer que si $n = p\,q$ avec $n^{1/3} < p \le q < n^{2/3}$ alors le pas (ii) fournit toujours les facteurs p et q.

On a la propriété suivante, qui sera démontrée plus loin

$$(*) \quad \exists\, r, s \ge 1\,,\ r\,s < n^{1/3} \ \text{ et } \ |\,p\,s - q\,r\,| < n^{1/3}\,.$$

Posant alors $k = r\,s$, on a

$$4\,k\,n = (p\,s + q\,r)^2 - (p\,s - q\,r)^2$$

de sorte que $(p\,s+q\,r)^2 - 4\,k\,n$ est un carré $< n^{2/3}$. Soit $d = p\,s + q\,r - [\,2\sqrt{k\,n}\,]$, alors

$$n^{2/3} > (p\,s+q\,r)^2 - 4\,k\,n > 4\,(d-1)\sqrt{k\,n}\,,$$

donc $d < n^{2/3}\,(4\sqrt{k\,n})^{-1} + 1$ et on trouve la factorisation au pas (ii).

Démontrons maintenant la propriété (*). Soit (r_i / s_i), $i \ge 1$, la suite des réduites du développement en fraction continue de q/p ; de sorte que $r_1 = [\,q/p\,]$, $s_1 = 1$, donc $0 < r_1\,s_1 < n^{1/3}$. Soit m le plus grand entier tel que $r_m\,s_m < n^{1/3}$. Posons alors $r = r_m$ et $s = s_m$. On a bien $r \ge 1$, $s \ge 1$ et $r\,s < n^{1/3}$ ainsi que

$$|\,r\,p - q\,s\,| = p\,s\,\left|\frac{r}{s} - \frac{q}{p}\right| \le p\,s\,\frac{1}{s\,s_{m+1}} = \frac{p}{s_{m+1}}\,.$$

Si $p / s_{m+1} \le q / r_{m+1}$ ceci implique

$$|\,r\,p - q\,s\,| \le (p\,q / r_{m+1}\,s_{m+1})^{1/2} < n^{1/3}\,.$$

Si $p / s_{m+1} > q / r_{m+1}$ alors s/r et s_{m+1} / r_{m+1} sont des réduites de p/q et le résultat se démontre de façon analogue.

Il est clair que le nombre d'opérations utilisées par cette méthode est en $O(n^{1/3})$.

4. Méthode rho de Pollard .

Cette méthode consiste à calculer une suite (x_n) définie par les formules

$$x_1 = c \quad \text{et} \quad x_h = (x_{h-1}^2 + 1) \bmod n \quad \text{pour} \quad h \geq 2 .$$

Soit p le plus petit diviseur premier de n, alors la suite des nombres $x_h \bmod p$ est ultimement périodique et il existe donc un entier k tel que l'on ait

$$x_{2k} \equiv x_k \quad \text{modulo} \quad p ,$$

et alors p divise le p.g.c.d. de $x_{2k} - x_k$ et de n. Si ce p.g.c.d. est différent de n, on a trouvé un diviseur non trivial de n. Si, de plus, la suite $x_h \bmod p$ se comporte comme une suite au hasard on aura $x_{2k} \equiv x_k$ modulo p pour $k = O(\sqrt{p})$.

Exercice : Démontrer ce résultat [On pourra calculer la probabilité pour que les éléments $x_1 , x_2 , \ldots , x_i$ soient tous distincts] .

Expérimentalement, cette méthode fournit presque toujours une factorisation non triviale de n en un nombre d'opérations en $O(p^{1/2})$, où p est le plus petit diviseur premier de n. Donc en général, cette méthode fournit, pour n non premier, un facteur non trivial de n en un temps $O(n^{1/4})$.

Remarque : Le point essentiel pour cette méthode est le choix d'une suite (x_n) qui soit aléatoire modulo p (c'est à dire qui se comporte, en un certain sens, comme une suite au hasard) . Si on prend une suite vérifiant une récurrence linéaire, cette méthode échoue (et on peut le démontrer) . Par contre, pour le choix d'une suite qui vérifie la condition $x_h \equiv (x_{h-1}^2 + 1) \bmod p$ (ou, plus généralement, $x_h \equiv (x_{h-1}^2 + a) \bmod p$) la pratique montre que la méthode réussit, mais on ne sait pas le démontrer rigoureusement.

Exercices

1. Soit a un entier ≥ 2. Démontrer qu'il existe une infinité d'entiers n positifs tels que l'on ait $a^{n-1} \equiv 1 \pmod{n}$. [Soit p un nombre premier qui ne divise pas le produit $a(a^2-1)$, prendre $n = (a^{2p}-1)/(a^2-1)$. Démontrer que le produit $2p$ divise $n-1$ et que a vérifie $a^{2p} \equiv 1 \mod n$ ...]

2. Soient p un nombre premier impair et h un entier qui vérifie $2 \leq h < p$. On suppose que n est égal soit à $hp+1$ soit à hp^2+1 et que l'on a

$$2^h \not\equiv 1 \text{ modulo } n \quad \text{et} \quad 2^{n-1} \equiv 1 \pmod{n}.$$

Démontrer que n est premier. [Démontrer d'abord que si n n'est pas premier alors il admet un facteur premier q avec $q \equiv 1 \mod p$.]

3. Soit n un entier tel que $n-1 = p^a r$ avec $a \geq 1$ et r non divisible par p, p premier.

1°) On suppose qu'il existe un entier x tel que

$$(x^{(n-1)/p}-1, n) = 1 \quad \text{et} \quad x^{n-1} \equiv 1 \ (n).$$

Démontrer que si q est un diviseur premier de n alors p^a divise $q-1$.

2°) On suppose que n s'écrit

$$n = 1 + p_1^{a_1} \ldots p_r^{a_r} Q \quad \text{avec} \quad p_1^{a_1} \ldots p_r^{a_r} > Q$$

et que pour chacun des indices $i = 1, \ldots, r$ il existe un entier x_i qui vérifie

$$(x_i^{(n-1)/p_i} - 1, n) = 1 \quad \text{et} \quad x_i^{n-1} \equiv 1 \ (n).$$

Montrer que n est premier.

4. Soit n un entier positif impair. Démontrer que les propriétés suivantes sont équivalentes :

(i) n est premier,

(ii) $G(n)$ contient un élément d'ordre $> (n-1)/2$,

(iii) $x^2 \equiv 1 \mod n \Rightarrow x \equiv \pm 1 \mod n$,

(iv) si $n - 1 = 2^r n'$, n' impair, alors

$$(a \in G(n) \text{ et } a^{n'} \neq 1) \Rightarrow \exists\, s, 0 \leq s < r, a^{t n'} = -1 \text{ où } t = 2^s.$$

5. Pour n entier ≥ 0 on définit le **nombre de Fermat** F_n par la formule

$$F_n = 2^{2^n} + 1.$$

1°) Démontrer que si un nombre $a^n + 1$ est premier, $a \geq 2$, alors a est impair et n est égal à une puissance de 2.

2°) Démontrer les propriétés suivantes :

(i) pour tout $r > 0$, F_n divise $F_{n+r} - 2$,

(ii) pour $0 \leq m < n$, les entiers F_m et F_n sont premiers entre eux,

(iii) F_n est premier pour $n \leq 4$,

(iv) 641 divise F_5.

De plus, démontrer que si, pour $a \geq 2$, le nombre a^n est premier alors a est pair et l'exposant n est une puissance de 2.

6. On a vu que pour $k \geq 3$ tout élément a de $G(2^k)$ vérifie une et une seule congruence de la forme

$$a \equiv (-1)^e 5^f \pmod{2^k}, \quad e \in \{0, 1\} \text{ et } f \in \{0, 1, \ldots, 2^{k-2} - 1\}.$$

En déduire qu'un entier impair a est un carré modulo 2^k, pour $k \geq 3$, si et seulement si cet entier vérifie $a \equiv 1$ modulo 8.

7. Critère de Gauss .

Soit p un nombre premier impair et a un entier non divisible par p . On pose

$v = \text{Card}\{ k ; 1 \leq k \leq (p-1)/2 \text{ et } \exists\, s , 1 \leq s \leq (p-1)/2 , k a \equiv -s \bmod p \}$.

Démontrer la relation

$$\left(\frac{a}{p}\right) = (-1)^{v} .$$

En déduire que

$$\left(\frac{2}{p}\right) = +1 \iff p \equiv \pm 1 \pmod 8 .$$

8. Symbole de Jacobi .

Soient b et b' deux entiers impairs.

1°) Démontrer que le symbole de Jacobi possède les propriétés suivantes.

(i) $\left(\frac{a\,a'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$,

(ii) $\left(\frac{a}{b\,b'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$,

(iii) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$, $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$,

[Pour la deuxième formule, utiliser l'exercice précédent.]

(iv) $\left(\frac{a}{b}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} \left(\frac{b}{a}\right)$,

pour a impair, $b \geq 3$.

[On admettra la loi de réciprocité quadratique

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right),$$

lorsque p et q sont deux nombres premiers impairs distincts. Voir chap. VI, ex. 21 .]

2°) En déduire un algorithme de calcul du symbole de Jacobi à partir de l'algorithme d'Euclide.

Calculer le coût de cet algorithme et l'appliquer pour calculer le symbole

$$\left(\frac{753}{811}\right).$$

9. Soit F_n le n-ième nombre de Fermat (voir l'exercice 5 ci-dessus).

Démontrer que F_n divise l'entier

$$2^{F_n} - 2.$$

Vérifier que le nombre 341 n'est pas premier mais cependant divise $2^{341} - 2$.

10. Soit p un nombre premier impair. Grâce au critère de Gauss (voir exercice 7), démontrer les propriétés suivantes

(i) $\left(\frac{3}{p}\right) = +1$ si, et seulement si, $p \equiv \pm 1$ modulo 6 (pour $p \neq 3$),

(ii) $\left(\frac{5}{p}\right) = +1$ si, et seulement si, $p \equiv \pm 1$ modulo 5 (pour $p \neq 5$).

11. Soient x et y deux entiers. Démontrer les implications suivantes :

$$x^2 - y^2 \equiv 1 \pmod 3 \Rightarrow 3 \mid y,$$

$$x^2 - y^2 \equiv 1 \pmod 5 \Rightarrow 5 \mid xy.$$

12. Si p est un nombre premier impair, le nombre $M = M_p = 2^p - 1$ est appelé un **nombre de Mersenne** . L'objet de cet exercice est de démontrer un critère de primalité de ces nombres, le **critère de Lucas** .

1°) Démontrer que si le nombre $a^n - 1$ est premier alors $a = 2$ et n est premier.

2°) Déterminer les entiers $p \leq 17$ tels que M_p soit premier. [Réponse : $p \neq 11$.]

3°) Soit ω le **nombre d'or,** $\omega = (1 + \sqrt{5}) / 2$, et soit p un nombre premier impair. Grâce à l'exercice 10 (ii) , démontrer que

(i) $\quad p \equiv \pm 1 \pmod 5 \Rightarrow \omega^{p-1} \equiv 1 \pmod p$,

et

(ii) $\quad p \equiv \pm 2 \pmod 5 \Rightarrow \omega^{2(p+1)} \equiv 1 \pmod p$.

[Dans chacun des deux cas, on pourra considérer le nombre $\omega^p \bmod p$.]

4°) Soit $\omega' = (1 - \sqrt{5}) / 2$ le conjugué du nombre d'or. Pour n entier ≥ 0 , on pose

$$r_n = \omega^{2^n} + \omega'^{2^n} .$$

a) Démontrer que r_n est un entier.

b) Démontrer que, pour m et n distincts, les entiers r_m et r_n sont premiers entre eux.

5°) Démontrer l'implication suivante :

$$M_p \text{ premier} \Rightarrow r_{p-1} \equiv 0 \pmod{M_p} .$$

6°) On veut maintenant démontrer la réciproque de l'implication précédente, soit la propriété

$$r_{p-1} \equiv 0 \pmod{M_p} \Rightarrow M_p \text{ premier.}$$

a) Si p' est un diviseur premier de M_p , avec $p' \equiv \pm 1$ modulo 5 , démontrer que

$$2^{p+1} \mid p' - 1 .$$

[On pourra utiliser la question 3°) (i) .]

En déduire que M_p n'admet pas de diviseur de ce type.

b) Si q' est un diviseur premier de M_p, avec $q' \equiv \pm 2$ modulo 5, démontrer que

$$2p \mid q' + 1 .$$

En déduire que M_p admet au plus un diviseur de ce type.

c) Conclure.

7°) On a donc démontré le critère de Lucas :

$$M_p \text{ premier} \Leftrightarrow r_{p-1} \equiv 0 \pmod{M_p} .$$

Quel est le coût de ce test ?

13. Soient a et b deux entiers premiers entre eux. On considère la suite (u_n) définie par

$$u_0 = 1 , u_1 = 1 , u_{n+2} = a\, u_{n+1} - b\, u_n \text{ pour } n \geq 0 .$$

Soit m un entier premier impair qui est premier avec $a^2 - 4b$.

Démontrer que si m divise u_{m+1} mais ne divise aucun des nombres $u_{(m+1)/p}$, pour p diviseur premier quelconque de $m + 1$, alors le nombre m est premier.

14. L'objet de cet exercice est de démontrer la propriété suivante :

pour tout entier $k \in \mathbf{Z}$, $k \neq 1$, il existe une infinité d'entiers n tels que le nombre $S_n = 2^{2^n} + k$ soit composé.

Nous suivrons une démonstration donnée par A. Schinzel.

Considérons un nombre S_n fixé, où n est arbitrairement grand et on suppose que ce nombre S_n est premier (sinon, on a gagné), disons $S_n = p$.

On pose $p - 1 = 2^s h$, avec h impair, et $\varphi(h) = k$.

1°) Démontrer les congruences

$$2^k \equiv 1 \pmod{h} \text{ et } 2^{t+k} \equiv 2^t \pmod{p-1}, \text{ pour tout } t \geq s .$$

2°) Grâce au théorème de Fermat, démontrer que S_{n+k} est divisible par p.

En conclure que le nombre S_{n+k} est composé.

CHAPITRE III

Polynômes, étude algébrique

1. Définitions et propriétés élémentaires .

1. Premières définitions.

Soit $\{X_1 , \dots , X_n\}$ un ensemble fini et soit A un anneau commutatif unitaire, on appelle **polynômes** en les **indéterminées** (on dit aussi fréquemment en les **variables**) $X_1 , \dots , X_n$ et à coefficients dans A les sommes formelles

$$\sum_{i_1 , \dots , i_n \geq 0} a_{i_1 , \dots , i_n} X_1^{i_1} \dots X_n^{i_n} ,$$

où $a_{i_1,\dots,i_n} \in A$, qui ne possèdent qu'un nombre fini de **coefficients** $a_{i_1,\dots,i_n}$ non nuls.

Un polynôme de la forme $a_{i_1, \dots ,i_n} X_1^{i_1} \dots X_n^{i_n}$, qui comporte au plus un coefficient non nul, est appelé un **monôme** .

L'ensemble de ces polynômes est noté $A[X_1 , \dots X_n]$.

L'application $a \rightarrow a\, X_1^0 \dots X_n^0$ permet d'identifier A à un sous-ensemble de $A[X_1 , \dots X_n]$, ce monôme sera donc noté a .

2. Opérations arithmétiques élémentaires.

Soient P et Q deux polynômes de $A[X_1, \dots X_n]$ qui s'écrivent respectivement

$$P = \sum a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n} \quad \text{et} \quad Q = \sum b_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n} ,$$

et soit λ un élément de A.

On définit les opérations suivantes

$$P + Q = \sum (a_{i_1, \dots, i_n} + b_{i_1, \dots, i_n}) X_1^{i_1} \dots X_n^{i_n} ,$$

$$\lambda P = \sum (\lambda a_{i_1, \dots, i_n}) X_1^{i_1} \dots X_n^{i_n}$$

et

$$P \cdot Q = \sum_{k} \left(\sum_{i, j, i+j=k} a_i b_j \right) X^k ,$$

où, pour simplifier les notations, on a posé

$$\mathbf{i} = (i_1, \dots, i_n) , \quad \mathbf{j} = (j_1, \dots, j_n) , \quad \mathbf{i} + \mathbf{j} = (i_1 + j_1, \dots, i_n + j_n) ,$$

...

et

$$X^{\mathbf{i}} = X_1^{i_1} \dots X_n^{i_n} , \dots$$

abréviations que nous utiliserons aussi par la suite.

Muni de ces opérations, $A[X_1, \dots, X_n]$ est une A-algèbre commutative admettant le polynôme $P = 1$ comme unité.

Si m est un entier, avec $1 \leq m < n$, on a un isomorphisme naturel

$$A[X_1, \dots, X_m][X_{m+1}, \dots, X_n] \cong A[X_1, \dots, X_n] .$$

3. Notions de degré .

Si P est un polynôme non nul en $X_1 , \ldots X_n$ (i. e. un polynôme dont au moins un des coefficients est non nul) ,

$$P = \sum a_i X^i ,$$

on définit le **degré total** de P par la formule

$$\deg (P) = \max \{ i_1 + \ldots + i_n \ ; \ a_i \neq 0 \} ,$$

tandis que le **degré partiel** de P **par rapport à** X_j est défini par

$$\deg_{X_j} (P) = \max \{ i_j \ ; \ a_{i_1 , \ldots , i_n} \neq 0 \} ,$$

on le note parfois aussi $\deg_j (P)$.

Si P et Q sont deux polynômes non nuls, on a les propriétés suivantes

- si $\deg (P) \neq \deg (Q)$ alors

  $P + Q \neq 0$ et $\deg (P + Q) = \max \{ \deg (P) , \deg (Q) \}$,

- si $\deg (P) = \deg (Q)$ et $P + Q \neq 0$ alors

  $\deg (P + Q) \leq \max \{ \deg (P) , \deg (Q) \}$,

- si $P Q \neq 0$ alors

  $\deg (P Q) \leq \deg (P) + \deg (Q)$.

Remarque : Il est parfois commode de définir le degré du polynôme nul par

$$\deg (0) = - \infty ,$$

avec les conventions suivantes

$$n + (- \infty) = (- \infty) + (- \infty) = - \infty \quad \text{pour tout entier } n$$

et

$$\deg (0) \leq n \quad \text{pour tout entier } n .$$

4. Cas d'un anneau intègre .

Lorsque l'anneau A est **intègre** (i. e. tel que, si a et b sont deux éléments non nuls de A , le produit $a\,b$ est aussi non nul) , on a les résultats suivants.

PROPOSITION 1 . – Si A est un anneau intègre, il en est de même de l'anneau de polynômes $A[X_1, \dots X_n]$.

De plus, si P et Q sont deux polynômes non nuls de $A[X_1, \dots X_n]$, alors on a

$$\deg(PQ) = \deg(P) + \deg(Q),$$

ainsi que

$$\deg_j(PQ) = \deg_j(P) + \deg_j(Q), \quad \text{pour} \quad 1 \leq j \leq n .$$

> Remarquons d'abord que la relation ρ définie sur $\mathbf{N}^n$ par

$$i \,\rho\, j \;\Leftrightarrow\; \begin{cases} i_1 + \dots + i_n < j_1 + \dots + j_n \\ \text{ou} \\ i_1 + \dots + i_n = j_1 + \dots + j_n \quad \text{et} \quad i \leq j \ , \end{cases}$$

où $\leq$ désigne l'ordre lexicographique sur $\mathbf{N}^n$, est une relation d'ordre total sur $\mathbf{N}^n$.

Soient d et d' les degrés respectifs des polynômes P et Q . On peut écrire

$$P = a_i X^i + P_1 \ , \quad Q = b_j X^j + Q_1 \ , \quad a_i \neq 0 \quad \text{et} \quad b_j \neq 0 \ ,$$

où P_1 (respectivement Q_1) ne comporte que des coefficients dont les indices sont inférieurs à i pour l'ordre ρ (respectivement dont les indices sont inférieurs à j). Alors $PQ = a_i\, b_j\, X^{i+j} + R$, avec $a_i\, b_j \neq 0$, où le polynôme R ne comporte que des coefficients dont les indices sont inférieurs à $i+j$ pour l'ordre ρ . Il en résulte que le produit PQ est non nul et vérifie bien

$$\deg(PQ) = \deg(X^{i+j}) = d + d' .$$

La dernière relation se démontre de manière analogue, mais plus simple. <

2. La division euclidienne .

1. Polynômes unitaires .

Si $P = a_0 + ... + a_m X^m$ est un polynôme en une indéterminée avec $a_m \neq 0$, alors a_m est appelé le **coefficient dominant** de P ; lorsque $a_m = 1$, le polynôme P est dit **unitaire** (en anglais, *monic*) .

Remarque : Si P est unitaire et Q non nul, on a toujours

$$\deg (P Q) = \deg (P) + \deg (Q) .$$

2. La division euclidienne .

THEOREME 1 . – Soient F et G deux polynômes de A [X] , G unitaire. Il existe alors des polynômes Q et R uniques tels que

$$F = Q G + R \quad \text{avec} \quad R = 0 \quad \text{ou} \quad \deg (R) < \deg (G) .$$

> Posons $d = \deg (F)$ et $d' = \deg (G)$. Si $d < d'$ une relation du type cherché a lieu avec $Q = 0$ et $R = F$.

Considérons le cas où $d \geq d'$. Soit a le coefficient dominant du polynôme F . Le polynôme

$$F_1 = F - a X^{d - d'} G$$

a un degré inférieur à d . Par récurrence sur d , on peut écrire

$$F_1 = Q_1 G + R_1 \quad \text{avec} \quad R_1 = 0 \quad \text{ou} \quad \deg (R_1) < d' .$$

La relation cherchée a alors lieu en posant

$$Q = a X^{d - d'} + Q_1 \quad \text{et} \quad R = R_1 .$$

Montrons maintenant l'unicité. Une relation

$$Q_1 G + R_1 = Q_2 G + R_2 ,$$

avec $R_1 = 0$ ou $\deg(R_1) < d'$ et avec $R_2 = 0$ ou $\deg(R_2) < d'$, implique

$$(Q_1 - Q_2) G = R_2 - R_1 .$$

Puisque G est unitaire, en calculant les degrés de chaque membre, la remarque 2.1 montre que l'on a nécessairement $Q_1 = Q_2$. La relation $R_1 = R_2$ en résulte. <

Le polynôme R est appelé le **reste** de la division de F par G, tandis que Q est appelé le **quotient** de cette division.

Le théorème 1 admet la généralisation suivante, dont la preuve est immédiate.

COROLLAIRE . – Soient F et G deux polynômes de $A[X]$, le coefficient dominant de G étant inversible. Il existe alors des polynômes Q et R uniques tels que

$$F = Q G + R \quad \text{avec} \quad R = 0 \text{ ou } \deg(R) < \deg(G) .$$

3. Cas d'un corps .

Dans toute la suite, la lettre K désignera un corps commutatif.

Lorsque l'anneau A est un corps K, l'énoncé du théorème 1 et sa preuve se simplifient.

Dans ce cas il suffit en effet, d'après le corollaire, de supposer le polynôme G non nul.

D'autre part, la relation $F = Q\,G + R$ équivaut à un système linéaire de $d + 1$ équations à $d + 1$ inconnues, qui sont les coefficients des polynômes Q et R. Le système homogène associé s'écrit $Q\,G + R = 0$, et par l'argument ci-dessus, relatif à l'unicité, la seule solution est $Q = R = 0$. Le système considéré est donc de Cramer, il admet une solution et une seule.

Cependant la démonstration du théorème 1 présente l'avantage de conduire directement à un algorithme simple pour la division.

L'existence de la division euclidienne conduit aussitôt au résultat suivant (comme dans le cas de l'anneau $\mathbf{Z}$).

THEOREME 2 . – Soit I un idéal de $K[X]$, alors il existe un polynôme P tel que l'on ait $I = P.K[X]$.

> Si I est réduit à $\{0\}$ il suffit de poser $P = 0$. Supposons I non nul. Soit P un élément de I de degré minimal et soit F un élément quelconque de I. Soit R le reste de la division euclidienne de F par P, il appartient à I. Par définition de P, nécessairement $R = 0$. Donc F est un multiple de P. <

Un idéal I d'un anneau A qui est de la forme $x\,A$ pour un certain élément x est appelé **idéal principal,** un tel élément x est alors appelé un **générateur** de l'idéal I ; tout autre générateur de I est de la forme $u\,x$, où u est un élément inversible de A. Ici, si $I = P.K[X]$, tout générateur de I est de la forme λP, $\lambda \in K$, $\lambda \neq 0$. On écrira souvent $I = (P)$ au lieu de $I = P.K[X]$; plus généralement l'idéal engendré par une famille finie de polynômes $F_1, \ldots, F_r$ sera noté $(F_1, \ldots, F_r)$.

Le fait que tout idéal de $K[X]$ soit principal conduit à l'existence d'un p.g.c.d., avec la relation de Bézout, et l'existence d'une division euclidienne conduit à un algorithme d'Euclide pour le calcul du p.g.c.d. . Nous énoncerons seulement les résultats (les démonstrations sont les mêmes que celles du chapitre I).

THEOREME 3 . – Soient $F_1, \ldots, F_r$ des polynômes appartenant à $K[X]$. Tout générateur D de l'idéal $(F_1, \ldots, F_r)$ est appelé un **p.g.c.d.** des F_i . Il existe des polynômes $U_1, \ldots, U_r$ tels que l'on ait

$$U_1 F_1 + \ldots + U_r F_r = D .$$

Le polynôme D divise chacun des F_i et tout polynôme P qui divise chacun des F_i divise aussi D . En outre, tout autre p.g.c.d. des F_i est de la forme λD où λ est un élément non nul du corps K .

Enfin, grâce à l'algorithme d'Euclide, on peut calculer un p.g.c.d. des F_i ainsi que les polynômes U_i correspondants.

On dit que des polynômes $F_1, \ldots, F_r$ à coefficients dans un corps K sont **premiers entre eux** lorsqu'ils admettent 1 comme p.g.c.d. . D'après le théorème, on a le résultat suivant.

COROLLAIRE . – Si des polynômes $F_1, \ldots, F_r$ à coefficients dans un corps K sont premiers entre eux alors il existe des polynômes $U_1, \ldots, U_r$ de $K[X]$ tels que l'on ait la relation de Bézout

$$U_1 F_1 + \ldots + U_r F_r = 1 .$$

4. Pseudo-division .

On étend la division euclidienne de la manière suivante.

THEOREME 1 bis . – Soient F et G deux polynômes à coefficients dans un anneau intègre A , de degrés respectifs d et d', et soit b le coefficient dominant du polynôme G . Posons $\delta = \max \{ d - d' + 1, 0 \}$. Il existe alors des polynômes Q et R uniques tels que l'on ait

$$b^{\delta} F = Q G + R \text{ , avec } R = 0 \text{ ou } \deg(R) < \deg(G) .$$

> La démonstration est une généralisation immédiate du théorème 1 . Le remplacement du polynôme F par $b^{\delta} F$ permet exactement d'effectuer la division. <

On dit parfois que les polynômes Q et R du théorème sont respectivement le pseudo-quotient et le pseudo-reste de la (pseudo-) division de F par G .

La remarque suivante sera utile.

COROLLAIRE . – Soient F et G deux polynômes à coefficients dans un anneau A intègre. Si P est un polynôme de A [X] qui divise à la fois F et G , alors P divise aussi le pseudo-reste de la division de F par G .

> Ceci résulte aussitôt de la relation $b^{\delta} F = Q G + R$. <

3. Le théorème chinois .

Nous donnons une version générale de ce théorème. Avant d'énoncer ce théorème, le lemme suivant sera utile.

LEMME . – Soit A un anneau (commutatif ou non) et soient $I, I_1, \ldots, I_n$ des idéaux bilatères de A qui vérifient $I + I_k = A$ pour $1 \leq k \leq n$. Alors, on a

$$I + I_1 \cap \ldots \cap I_n = A \ .$$

> Il suffit de montrer que l'élément 1 appartient à $I + I_1 \cap \ldots \cap I_n$. Par hypothèse, il existe des éléments $a_k \in I$, $b_k \in I_k$ tels que $a_k + b_k = 1$, $1 \leq k \leq n$, et

$$1 = \prod_{k=1}^{n} (a_k + b_k) = \sum_{k=1}^{n} a_k \cdot \prod_{h \neq k} (a_h + b_h) + b_1 \ldots b_n \in I + I_1 \cap \ldots \cap I_n \ . <$$

THEOREME 4 . – Soient A un anneau et $I, I_1, \ldots, I_n$ des idéaux bilatères de A qui vérifient $I_h + I_k = A$ si $1 \leq h < k \leq n$. Alors

$$A \ / \ (I_1 \cap \ldots \cap I_n) \quad \cong \quad \prod_{k=1}^{n} (A / I_k) \ .$$

> On considère l'homomorphisme canonique

$$\varphi \ : \ A \ \rightarrow \ \prod_{k=1}^{n} (A / I_k) \ .$$

Son noyau est égal à $I_1 \cap \ldots \cap I_n$.

Il ne reste donc plus qu'à montrer que l'application φ est surjective.

On se donne des éléments $a_1, \ldots, a_n$ de A et il s'agit de montrer qu'il existe un élément x de A vérifiant $x \equiv a_k \pmod{I_k}$ pour $1 \leq k \leq n$.

Nous allons donner deux démonstrations de ce fait.

1°) Méthode de Lagrange .

Soit k un indice, $1 \leq k \leq n$. D'après le lemme, on a

$$I_k + \bigcap_{h \neq k} I_h = A ,$$

il existe donc un élément

$$\varepsilon_k \in \prod_{h \neq k} I_h$$

tel que $1-\varepsilon_k \in I_k$. Si δ_{hk} (= 1 si h = k et 0 sinon) est le **symbole de Kronecker,**

$$\varepsilon_k \equiv \delta_{hk} \pmod{I_h} .$$

L'élément

$$x = \sum_{k=1}^{n} a_k \varepsilon_k$$

est une solution du problème.

2°) Méthode de Newton.

On raisonne par récurrence sur n. Le cas n = 1 est trivial. Supposons $n \geq 2$ et que l'on ait trouvé un élément x' de A qui vérifie $x' \equiv a_k \pmod{I_k}$ pour $1 \leq k < n$.

Soit ε_n défini comme ci-dessus, on vérifie instantanément que

$$x = x' + \varepsilon_n (a_n - x')$$

est solution du problème considéré. <

COROLLAIRE . – Soient A un anneau commutatif et $I_1 , \dots , I_n$ des idéaux de cet anneau. Alors, les assertions suivantes sont équivalentes :

(i) $A \cong \prod_{k=1}^{n} (A / I_k)$,

(ii) il existe $e_1 , \dots , e_n \in A$ tels que $e_h^2 = e_h$ et $e_h e_k = 0 , 1 \le h < k \le n$,

$$e_1 + \dots + e_n = 1 \quad \text{et} \quad I_k = (1 - e_k) A \quad \text{pour} \quad 1 \le k \le n ,$$

où la notation λA désigne l'ensemble des éléments de la forme $\lambda x , x \in A$.

(iii) les idéaux considérés vérifient

$$I_h + I_k = A \quad \text{si} \quad 1 \le h < k \le n \quad \text{et} \quad I_1 \cap \dots \cap I_n = \{0\} .$$

> **(i) ⇒ (ii) :**

Si φ est l'isomorphisme de (i) , il suffit de poser $e_k = \varphi^{-1} (\delta_{1k} , \dots , \delta_{nk})$.

(ii) ⇒ (iii) : Notons au passage qu'un élément e de A tel que $e^2 = e$ est appelé un **idempotent** de A .

Puisque $1 - e_h \in I_h$ et $e_h = e_h (1 - e_k) \in I_k$, on a $I_h + I_k = A$ si $h \neq k$. De plus,

$$\prod_{k=1}^{n} (1 - e_k) = 1 - (e_1 + \dots + e_n) = 0 \Rightarrow I_1 \cap \dots \cap I_n = \{0\} .$$

(iii) ⇒ (i) : Appliquer le théorème . <

Dans le cas des polynômes, le théorème chinois a la conséquence suivante.

COROLLAIRE . – Soit K un corps et A = K [X] . Si des polynômes $F_1 , \dots , F_r$ de A sont premiers entre eux alors on a un isomorphisme naturel

$$A / (F_1 \dots F_r) \cong \prod_{i=1}^{r} \left(A / (F_i) \right) .$$

4. Factorisation .

Dans tout ce paragraphe A est un anneau intègre.

Un élément x non nul d'un anneau intègre B est dit **irréductible** si, et seulement si, l'anneau quotient B / xB est intègre. En particulier, un polynôme P de A [X] est irréductible si, et seulement si, l'anneau A [X] / (P) est intègre.

Deux éléments x et y de B sont dits **associés** si, et seulement si, il existe un élément inversible u de B tel que $x = u\,y$. En particulier, deux polynômes F et G appartenant à A [X] sont associés si, et seulement si, il existe un élément inversible u de l'anneau A tel que $F = u\,G$.

1. Cas d'un corps .

Un polynôme P de K [X] est irréductible si, et seulement si, le degré de P est > 0 et si P n'admet aucun diviseur Q vérifiant $0 < \deg(Q) < \deg(P)$. Il en résulte que tout polynôme F de K [X] de degré > 0 admet un diviseur irréductible, il suffit de prendre un diviseur quelconque de F de degré > 0 et minimal.

Comme dans le cas des entiers, grâce à la relation de Bézout, on a aussi le résultat suivant.

PROPOSITION 2 . – Un polynôme P de K [X] , de degré > 0 , est irréductible si, et seulement si, l'anneau quotient K [X] / (P) est un corps.

Toujours comme dans le cas des entiers, et toujours grâce à la relation de Bézout, on a aussi une décomposition en produit d'éléments irréductibles dans K [X] . L'énoncé précis est le suivant.

THEOREME 5 . – Tout polynôme F non nul de $K[X]$ admet une décomposition de la forme

$$F = c \prod_{i=1}^{k} P_i^{\alpha_i} \quad , \quad c \in K \, ,$$

où les polynômes P_i sont irréductibles, deux à deux non associés, et les α_i sont > 0.

De plus, si

$$F = c' \prod_{j=1}^{h} Q_j^{\beta_j} \quad , \quad c' \in K \, ,$$

où les polynômes Q_j sont irréductibles, deux à deux non associés, et les β_j sont > 0, alors on a $h = k$ et il existe une permutation σ de $\{1, \ldots , k\}$ telle que l'on ait

$$\beta_{\sigma(i)} = \alpha_i \quad \text{et} \quad Q_{\sigma(i)} \text{ associé à } P_i$$

pour $i = 1, \ldots , k$.

2. Cas d'un anneau factoriel .

Un anneau est dit **factoriel** s'il est intègre et si chacun de ses éléments non nuls admet une décomposition unique en produit d'éléments irréductibles, à l'ordre près et à des facteurs inversibles près (comme dans l'énoncé du théorème 5) .

Soit A un anneau factoriel, de corps des fractions K , et soit p un élément irréductible de A . Tout élément a non nul de K s'écrit, d'une manière et d'une seule, sous la forme

$$a = p^r b \quad , \quad r \in \mathbf{Z} \, ,$$

où b est le quotient de deux éléments de A dont aucun n'est divisible par p . L'entier r est appelé l' **ordre de a en p** , et noté $\mathrm{ord}_p(a)$. Par convention, $\mathrm{ord}_p(0) = +\infty$.

Si a et a' sont deux éléments quelconques de K , on a

$$\mathrm{ord}_p(a\,a') = \mathrm{ord}_p(a) + \mathrm{ord}_p(a') .$$

Si $F = a_0 + \ldots + a_n X^n$ est un polynôme non nul à coefficients dans K , on pose

$$\mathrm{ord}_p(F) = \min \{ \mathrm{ord}_p(a_i) \; ; \; a_i \neq 0 \} .$$

Si $\wp$ désigne un **système de représentants des éléments irréductibles** de A (ce qui signifie que, d'une part, pour tout élément irréductible q de A il existe un élément p de $\wp$ associé à q , et que, d'autre part, les éléments de $\wp$ sont deux à deux non associés), on définit le **contenu** de F (relativement à $\wp$) par la formule

$$\mathrm{cont}_{\wp}(F) = \prod_{p \in \wp} p^{\mathrm{ord}_p(F)} ,$$

quand il n'y a pas de confusion possible on pose $\mathrm{cont}(F) = \mathrm{cont}_{\wp}(F)$.

Après tous ces préliminaires, nous pouvons démontrer le résultat suivant.

PROPOSITION 2 (lemme de Gauss) . – Soit A un anneau factoriel et soit K son corps de fractions. Si F et G sont deux polynômes non nuls à coefficients dans le corps K , on a

$$\mathrm{cont}(F\,G) = \mathrm{cont}(F) . \mathrm{cont}(G) .$$

> D'après la définition du contenu d'un polynôme, il suffit de prouver que pour tout élément irréductible p de A on a la relation

$$\mathrm{ord}_p(F\,G) = \mathrm{ord}_p(F) + \mathrm{ord}_p(G) .$$

Posons $r = \mathrm{ord}_p(F)$ et $s = \mathrm{ord}_p(G)$. Alors il existe deux polynômes F_1 et G_1 à coefficients dans A tels que l'on ait

$$F = u\, p^r F_1 \quad , \quad G = v\, p^s G_1 \quad \text{et} \quad \mathrm{ord}_p(F_1) = \mathrm{ord}_p(G_1) = 0 \, ,$$

où u et v sont deux éléments non nuls de K vérifiant

$$\mathrm{ord}_p(u) = \mathrm{ord}_p(v) = 0 \, .$$

Par l'application canonique $A[X] \to (A / pA)[X]$, les polynômes F_1 et G_1 ont des images respectives f_1 et g_1 non nulles. Comme l'anneau A / pA est intègre le produit $f_1 g_1$ est non nul, on a donc $\mathrm{ord}_p(F_1 G_1) = 0$.

D'où l'égalité

$$\mathrm{ord}_p(FG) = r + s \, . <$$

Grâce au lemme de Gauss, on peut démontrer le résultat suivant.

THEOREME 6. – Soit A un anneau factoriel et soit K son corps de fractions. Alors l'anneau de polynômes $A[X]$ est aussi factoriel.

De plus, si $\wp$ est un système de représentants des éléments irréductibles de A et $\wp'$ un système de représentants des polynômes irréductibles de $K[X]$, chaque élément de $\wp'$ ayant un contenu relatif à $\wp$ égal à 1, alors $\wp \cup \wp'$ est un système de représentants des éléments irréductibles de l'anneau de polynômes $A[X]$.

Exemple : L'anneau $\mathbf{Z}[X]$ est factoriel. Si $\wp$ désigne l'ensemble des entiers et $\wp'$ l'ensemble des pôlynomes irréductibles de $\mathbf{Q}[X]$ à coefficients entiers premiers entre eux et de coefficient dominant positif alors $\wp \cup \wp'$ est un système de représentants des éléments irréductibles de $\mathbf{Z}[X]$.

> Soit F un polynôme non nul à coefficients dans A . Dans l'anneau K [X] , ce polynôme se décompose de manière unique sous la forme

$$F = a \prod_{P \in \wp'} P^{n_P} \quad , \quad a \in K \ , \ a \neq 0 \ , \ n_P \geq 0 \ .$$

D'après le lemme de Gauss, a est égal au contenu de F (relativement à $\wp$) , donc l'élément a appartient à l'anneau A et il s'écrit, de manière unique, sous la forme

$$a = u \prod_{p \in \wp} p^{m_p} \quad , \quad m_p \geq 0 \ ,$$

où u est un élément inversible de A .

D'où le théorème . <

En raisonnant par récurrence sur le nombre de variables, on en déduit le résultat suivant.

COROLLAIRE . – Soit A un anneau factoriel, alors l'anneau de polynômes en n variables $A [X_1 , \ldots , X_n]$ est encore un anneau factoriel. En particulier, si K est un corps quelconque, l'anneau $K [X_1 , \ldots , X_n]$ est un anneau factoriel.

Exemple : Pour tout $n \geq 1$ l'anneau $Z [X_1 , \ldots , X_n]$ est un anneau factoriel ; c'est certainement l'exemple le plus important en calcul formel.

5. Fonctions polynômes .

1. Définition .

Soit F un polynôme en $X_1, \dots, X_n$ à coefficients dans A ,

$$F = \sum a_{i_1,\dots,i_n} X_1^{i_1} \dots X_n^{i_n} ,$$

et soit B un anneau dont A est un sous-anneau. On définit la **fonction-polynôme**

$$F^* : B^n \to B$$

par

$$F^*(b_1, \dots, b_n) = \sum a_{i_1,\dots,i_n} b_1^{i_1} \dots b_n^{i_n} .$$

On dit que l'on a **substitué** b_i à X_i et, pour simplifier les notations, on écrira souvent $F(b_1, \dots, b_n)$ au lieu de $F^*(b_1, \dots, b_n)$.

Les propriétés suivantes sont évidentes

$$(F+G)^* = F^* + G^* ,$$

$$(FG)^* = F^* G^* ,$$

$$(aF)^* = a F^* \quad \text{si} \quad a \in A .$$

Attention : L'application $\varphi : F \to F^*$ n'est pas toujours injective : par exemple, si on prend pour anneau $A = \mathbf{Z}/2\mathbf{Z}$ et pour polynôme $F = X^2 - X$ alors F^* s'annule pour tout élément de A . Par contre l'application φ est injective lorsque l'anneau A est intègre et infini, voir le corollaire du théorème 7 ci-dessous. Ainsi, lorsque A est intègre et infini on pourra sans inconvénient confondre un polynôme et la fonction polynôme associée.

2. Racines d'un polynôme .

Si $F \in A[X]$, un élément a de A est appelé une **racine** de F si $F(a) = 0$; on dit aussi que a est un **zéro** du polynôme F .

PROPOSITION 3 . – Soit F un polynôme à coefficients dans A et soit a un élément de A . Alors le reste de la division euclidienne de F par le polynôme $X - a$ est égal à $F(a)$.

En particulier, a est une racine de F si, et seulement si, $X - a$ divise F .

> Si le résultat de la division euclidienne de F par $X - a$ est $F = (X - a)Q + b$, où $b \in A$, alors en substituant a à X on constate que $b = F(a)$.

Enfin, par définition, a est une racine de F si, et seulement si, $F(a)$ est nul. D'où la seconde assertion. <

3. Multiplicité d'une racine .

Si $F \in A[X]$, un élément a de A est appelé une **racine d'ordre k** de F si le polynôme F est divisible par $(X - a)^k$ mais pas par $(X - a)^{k+1}$; si $k \geq 1$, on dit que k est la **multiplicité** de la racine a . (D'après la proposition 3 , cette terminologie est cohérente avec celle du paragraphe précédent.)

On peut caractériser l'ordre d'une racine grâce au résultat suivant.

PROPOSITION 4 . – Soit F un polynôme à coefficients dans A et soit a un élément de A . Alors a est racine d'ordre k de F si, et seulement si, il existe un polynôme G à coefficients dans A qui vérifie

$$F = (X - a)^k G \quad \text{et} \quad G(a) \neq 0 .$$

> Si a est racine d'ordre k de F, alors $(X - a)^k$ divise F ; soit G le quotient. Si l'élément a était racine de G alors $(X - a)^{k+1}$ diviserait F, donc G (a) est non nul.

La réciproque est facile. <

COROLLAIRE . – Soit A un anneau intègre et soit $F \in A[X]$ un polynôme non nul. Alors toute racine de F dans A a un ordre au plus égal au degré de F .

Plus généralement, la proposition a la conséquence suivante.

THEOREME 7 . – Soit A un anneau intègre et soit $F \in A[X]$ un polynôme non nul. Alors la somme des multiplicités des racines de F appartenant à A ne dépasse pas le degré de F .

> Considérons un polynôme F non nul à coefficients dans A . Soient $a_1, \ldots, a_k$ des racines de F de multiplicités respectives au moins égales à $r_1, \ldots, r_k$. En appliquant k fois la proposition 4 , on voit que le polynôme F peut s'écrire sous la forme

$$F = (X - a_1)^{r_1} \ldots (X - a_k)^{r_k} G(X) ,$$

où G est un polynôme à coefficients dans A . D'où la majoration

$$r_1 + \ldots + r_k \leq \deg (F) . <$$

COROLLAIRE . – Si A est un anneau intègre et infini et si $F \in A[X]$ s'annule pour tout a appartenant à A , alors le polynôme F est nul.

4. Dérivées et racines .

Si $F = a_0 + a_1 X + ... + a_m X^m$, on définit la **dérivée** (formelle) du polynôme F par la formule

$$F' = a_1 + 2 a_2 X + ... + m a_m X^{m-1} .$$

La dérivation vérifie les propriétés usuelles

$$(F+G)' = F' + G' ,$$

$$(FG)' = F'G + FG' ,$$

$$(aF)' = a F' \quad \text{si} \quad a \in A .$$

Plus généralement, on pose $F^{(0)} = F$ et

$$F^{(k)} = (F^{(k-1)})' \quad \text{pour} \quad k \geq 1 .$$

Le résultat suivant relie l'ordre de F et de sa dérivée en un même point.

PROPOSITION 6 . – Si un élément a de l'anneau A est racine d'ordre $k \geq 1$ d'un polynôme F de $A[X]$, alors $F^{(i)}(a) = 0$ pour $i = 0, 1, ..., k-1$.

> Il suffit de démontrer que $(X - a)^{k-1}$ divise F' et de raisonner ensuite par récurrence sur l'entier i .

Par hypothèse, le polynôme F est de la forme $F = (X - a)^k Q$, donc sa dérivée est

$$F' = (X - a)^{k-1} (kQ + (X - a) Q') . <$$

5. Formule de Taylor .

Rappelons qu'un anneau A est dit de **caractéristique 0** lorsque l'application naturelle $\mathbf{Z} \to A$, qui envoie l'entier 1 sur l'unité de A , est injective.

Dans le cas d'une seule variable, la formule de Taylor peut s'énoncer ainsi.

PROPOSITION 7 . – Soit K un corps de caractéristique 0 et soit $F \in K[X]$ un polynôme qui s'écrit $F = a_0 + A_1 X + \ldots + a_n X^n$. Si Y est une nouvelle lettre, alors $F(X+Y)$ vérifie la relation, dite **formule de Taylor** ,

$$F(X+Y) = F(X) + Y F^{(1)}(X) + \frac{Y^2}{2!} F^{(2)}(X) + \ldots + \frac{Y^n}{n!} F^{(n)}(X) .$$

> En raison de la linéarité des applications $F \to F^{(k)}$, il suffit de prouver le résultat lorsque $F = X^m$, $m \leq n$.

On a alors

$$F(X+Y) = (X+Y)^m = \sum_{k=0}^{m} \binom{m}{k} Y^k X^{m-k},$$

tandis que

$$\frac{Y^k}{k!} F^{(k)}(X) = Y^k \frac{m(m-1) \ldots (m-k+1)}{k!} X^{m-k} = \binom{m}{k} Y^k X^{m-k} ,$$

d'où la conclusion. <

Dans le cas d'un corps de caractéristique zéro, la formule de Taylor montre que l'on peut caractériser l'ordre d'une racine grâce à la dérivation.

Il s'agit du résultat suivant.

COROLLAIRE .– Soit F un polynôme appartenant à $K[X]$, K étant un corps de caractéristique zéro, et soit a une racine d'ordre k de F, $k \geq 1$, alors $F^{(k)}(a)$ est non nul.

> La proposition 6, jointe à la formule de Taylor, montre que

$$F(X) = \sum_{m \geq k} \frac{(X - a)^m}{m!} F^{(m)}(a) .$$

Si $F^{(k)}(a) = 0$ alors $(X - a)^{k+1}$ divise F, contradiction. D'où le résultat. <

6 . Le résultant .

Soient f et g deux polynômes en une variable et à coefficients dans un corps K. Lorsque f et g possèdent un facteur commun non trivial d, disons que l'on a $f = f_1 h$ et $g = g_1 h$, et l'équation

$$u f + v g = 0 \text{ , avec } \deg(u) < \deg(g) \text{ et } \deg(v) < \deg(f)$$

possède les solutions $u = g_1$ et $v = -f_1$. Réciproquement, il est clair que l'existence de solutions non nulles à cette équation implique le fait que les polynômes f et g admettent un diviseur commun non trivial.

Posons

$$f(X) = \sum_{i=0}^{m} a_i X^i \quad \text{et} \quad g(X) = \sum_{j=0}^{n} b_j X^j \ .$$

Alors l'équation précédente équivaut à un système linéaire homogène de $n + m$ relations à $n + m$ inconnues (les coefficients des polynômes u et v) et on sait que ce système admet une solution non triviale si, et seulement si, son déterminant est nul. Le déterminant en question est

$$\begin{vmatrix} a_m & a_{m-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & a_m & a_{m-1} & \dots & a_1 & a_0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ b_n & b_{n-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & b_n & b_{n-1} & \dots & b_1 & b_0 \end{vmatrix} \ .$$

De manière plus précise, les coefficients de la matrice associée à ce déterminant sont donnés par les formules

$$c_{i,j} = a_{m-j+i} \quad \text{pour} \quad 1 \leq i \leq n \ ,$$

$$c_{n+i,j} = b_{n-j+i} \quad \text{pour} \quad 1 \leq i \leq m \ ,$$

où on a posé

$$a_i = 0 \quad \text{pour} \ i \notin \{ 0, 1, \dots, m \} \quad \text{et} \quad b_j = 0 \quad \text{pour} \ j \notin \{ 0, 1, \dots, n \} \ .$$

Ce déterminant est appelé le **résultant** des polynômes f et g, il est le plus souvent noté $\mathrm{Res}(f, g)$, ou encore $\mathrm{Res}_X(f, g)$ lorsqu'il est utile de préciser la variable. Plus généralement, le résultant de f et g est défini par le déterminant précédent si les coefficients de ces polynômes appartiennent à un anneau A ; ainsi $\mathrm{Res}(f, g)$ est un élément de A . La matrice correspondant au déterminant ci-dessus est appelée la **matrice de Sylvester** des polynômes f et g .

Nous allons démontrer que dans le cas général aussi le résultant de f et g est nul si, et seulement si, les polynômes f et g ont un facteur commun non trivial (voir la propriété (iv) ci-dessous) .

En fait, le résultant possède les propriétés suivantes :

(i) $\mathrm{Res}(f, 0) = 0$;

> C'est clair d'après la définition . <

(ii) $\mathrm{Res}(g, f) = (-1)^{mn}\ \mathrm{Res}(f, g)$;

> Ceci résulte du fait qu'un déterminant change de signe chaque fois qu'on échange deux rangées adjacentes. <

(iii) Si $\deg(f) = m \leq n = \deg(g)$ et si h est le reste de la division euclidienne du polynôme g par le polynôme f , alors on a

$$\mathrm{Res}(f, g) = a_m^{\,n-m}\ \mathrm{Res}(f, h) ;$$

> Ecrivons $g = f q + h$, et dans la matrice associée au résultant retranchons à chacune des m dernières lignes le vecteur correspondant au polynôme produit fq (ce vecteur étant décalé d'une position vers la droite quand on passe d'une ligne à la ligne suivante) . Ceci revient à retrancher à chacune des m dernières lignes de cette matrice une combinaison linéaire convenable de ses n premières lignes de telle sorte que le résultat soit une matrice de la forme suivante

$$Q = \begin{pmatrix} M & M' \\ 0 & N \end{pmatrix} ,$$

où M est une matrice triangulaire de taille $(n-m) \times (n-m)$, N la matrice de Sylvester associée aux polynômes f et h . Le résultat découle aussitôt de la formule

$$\det(Q) = \det(M) . \det(N) \ . <$$

(iv) $\mathrm{Res}(f, g) = 0$ si, et seulement si, f et g ont un facteur commun non trivial ;

> C'est une conséquence immédiate des propriétés (ii) et (iii) . <

(v) Supposons l'anneau A intègre et soient α_i , $i = 1, ..., m$, les racines du polynôme f et β_j , $j = 1, ..., n$, les racines de g (dans une extension convenable de l'anneau A) , alors on a les relations suivantes

$$\mathrm{Res}(f, g) = a_m^n \prod_{i=1}^{m} g(\alpha_i) = (-1)^{mn} b_n^m \prod_{j=1}^{n} f(\beta_j) = a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) .$$

> Il est clair que la deuxième expression et la troisième sont toutes deux égales à la quatrième, désignons par S cette quantité. I ne reste plus qu'à montrer que S coïncide avec le résultant des polynômes f et g . Pour ce faire remarquons tout d'abord que les propriétés (i) à (iii) définissent les résultant de manière unique : en effet, il est clair que ces trois propriétés permettent de calculer le résultant par récurrence sur le minimum des degrés des polynômes f et g . Il suffit donc de montrer que S vérifie les propriétés (i) à (iii) . Pour la propriété (i) c'est trivial, pour la seconde ceci résulte de l'égalité entre les trois expressions de S , enfin la dernière est une conséquence immédiate de la relation $h(\alpha_i) = g(\alpha_i)$, valable lorsque h est le reste de la division euclidienne du polynôme g par f (utiliser la formule $g = q f + h$ au point α_i) . <

On définit aussi le **discriminant d'un polynôme** f par la formule

$$\mathrm{Discr}(f) = a_m^{2m-2} \prod_{i=1}^{m} \prod_{\substack{j=1 \\ j \neq i}}^{m} (\alpha_i - \alpha_j) .$$

D'après la propriété (v) ci-dessus, on a la formule $\mathrm{Res}(f, f') = a_n \mathrm{Discr}(f)$, et on peut démontrer que le discriminant de f appartient à l'anneau A .

Exercices

1. Un polynôme de $A[X_1, \ldots, X_n]$ est dit **homogène** s'il est de la forme

$$\sum a_{i_1, \ldots, i_n} X_1^{i_1} \ldots X_n^{i_n} \qquad \text{avec} \quad i_1 + \ldots + i_n = \text{constante} .$$

On suppose que l'anneau de base A est intègre et que u, v, w sont des polynômes de $A[X_1, \ldots, X_n]$ vérifiant $u = v\,w$. Démontrer que si u est homogène alors v et w sont aussi homogènes.

2. Les dérivées partielles d'un polynôme étant définies de manière usuelle, démontrer l'équivalence suivante (due à Euler)

$$\sum_{i=1}^{n} \frac{\partial u}{\partial X_i}(\mathbf{X}) \,.\, X_i \;=\; r \,.\, u(\mathbf{X}) \;\Leftrightarrow\; u \text{ homogène de degré } r ,$$

lorsque $u \in A[X_1, \ldots, X_n]$, A étant un anneau de caractéristique 0.

3. Soit $F \in A[X_1, \ldots, X_n]$ un polynôme non nul, A étant un anneau intègre. On suppose que, pour $i = 1, \ldots, n$, H_i est une partie de A qui vérifie

$$\text{Card}(H_i) > \deg_i(F) .$$

Démontrer qu'il existe $\mathbf{a} \in H_1 \times \ldots \times H_n$ tel que $F(\mathbf{a})$ soit non nul.

4. Démontrer que le polynôme $X^2 + 1$ possède une infinité de zéros dans le corps des quaternions sur $\mathbf{C}$.

5. Soit K un corps, et soient $x_1, \ldots, x_n$ des éléments distincts de K. On pose $w(X) = (X - x_1) \ldots (X - x_n)$. Démontrer que le polynôme

$$F(X) = w(X) \cdot \sum_{i=1}^{n} \frac{y_i}{w'(x_i)(X - x_i)}$$

est l'unique polynôme de $K[X]$ de degré $< n$ qui vérifie $F(x_i) = y_i$ pour $i = 1, \ldots, n$; ce polynôme est appelé le **polynôme de Lagrange** (associé aux x_i et y_i).

En déduire que si $G \in K[X]$ est un polynôme de degré $< n - 1$ alors

$$\sum_{i=1}^{n} \frac{G(x_i)}{w'(x_i)} = 0 .$$

[On pourra considérer le polynôme $X\,G(X)$.]

6. Soient $x_1, \ldots, x_r$ des éléments distincts d'un corps K, et $n_1, \ldots, n_r$ des entiers > 0 dont la somme est égale à n. Soient enfin $y_{i,j}$ des éléments quelconques de K, $1 \leq j \leq n_i$, $1 \leq i \leq r$. Montrer qu'il existe un polynôme et un seul $F \in K[X]$ qui vérifie

$$\deg(F) < n \quad \text{et} \quad F^{(j-1)}(x_i) = y_{i,j} \quad \text{pour } 1 \leq j \leq n_i,\ 1 \leq i \leq r ;$$

ce résultat est dû à Hermite et ce polynôme est appelé le **polynôme d'Hermite.**

7. Soit A un anneau intègre et soit n un entier ≥ 1. Démontrer qu'un polynôme non nul $P(X_1, \ldots, X_n)$ à coefficients dans A est inversible dans $A[X_1, \ldots, X_n]$ si, et seulement si, son degré est nul et s'il est inversible dans l'anneau A.

8. Soit A un anneau intègre qui n'est pas un corps. Montrer que l'anneau $A[X]$ n'est pas principal.

[Rappelons qu'un anneau est dit **principal** lorsque c'est un anneau commutatif dont tout idéal I est principal, c'est à dire tel qu'il existe un élément a de A pour lequel l'idéal I est égal à (a).]

9. Soit A un anneau principal et soit $I_1 \subset \ldots \subset I_n \subset \ldots$ une chaîne croissante d'idéaux de A.

Démontrer que cette chaîne est stationnaire (i. e. qu'il existe un certain indice k tel que $I_m = I_k$ pour $m \geq k$).

10. Quel est le nombre de racines du polynôme $X^3 - X$ dans l'anneau $\mathbf{Z}/6\mathbf{Z}$?

11. Soit A un anneau factoriel dont le corps des fractions est K et soit $F \in A[X]$ un polynôme de degré > 0, irréductible dans $A[X]$.

Démontrer que F est aussi irréductible dans $K[X]$.

En déduire que si F est un polynôme unitaire de $A[X]$ et si a est une racine de F appartenant à K alors a appartient en fait à l'anneau A.

12. Soit A un anneau. Pour $a \in A$ et $F \in A[X]$, on désigne par $\mathrm{ord}(F, a)$ l'ordre de a en tant que racine de F (évidemment $\mathrm{ord}(F, a) \geq 0$).

Si $G \in A[X]$, démontrer les relations suivantes

$\mathrm{ord}(F + G, a) \geq \inf \{ \mathrm{ord}(F, a), \mathrm{ord}(G, a) \}$,

$\mathrm{ord}(F, a) \neq \mathrm{ord}(G, a) \Rightarrow \mathrm{ord}(F + G, a) = \inf \{ \mathrm{ord}(F, a), \mathrm{ord}(G, a) \}$,

$\mathrm{ord}(F\,G, a) \geq \mathrm{ord}(F, a) + \mathrm{ord}(G, a)$,

avec l'égalité dans la dernière relation lorsque A est intègre.

13. Soit n un entier ≥ 1. Soient $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ des lettres distinctes. On pose $\mathbf{X} = (X_1, \ldots, X_n)$, $\mathbf{Y} = (Y_1, \ldots, Y_n)$, $\mathbf{X} + \mathbf{Y} = (X_1 + Y_1, \ldots, X_n + Y_n)$.

Soit $u \in A[\mathbf{X}]$. On définit les polynômes $\Delta_\nu u$ de $A[\mathbf{X}]$ par la formule

$$u(\mathbf{X} + \mathbf{Y}) = \sum_\nu (\Delta_\nu u)(\mathbf{X}) \cdot \mathbf{Y}^\nu .$$

1°) Démontrer les formules

$$u(\mathbf{X}) = \sum_\nu (\Delta_\nu u)(\mathbf{0})\, \mathbf{X}^\nu ,$$

$$\Delta_\sigma(u\,v) = \sum_{\nu+\rho=\sigma} (\Delta_\nu u) \cdot (\Delta_\rho v) \quad , \quad \text{si} \quad v \in A[X] .$$

[Les lettres ν, ρ, σ désignent des multi-indices appartenant à $\mathbf{N}^n$.]

2°) Démontrer la relation

$$(\mathbf{X} + \mathbf{Y})^\nu = \sum_{\rho+\sigma=\nu} \frac{(\rho+\sigma)!}{\rho!\,\sigma!}\, \mathbf{X}^\rho\, \mathbf{Y}^\sigma .$$

[Où on a posé $\rho! = \rho_1! \ldots \rho_n!$ lorsque $\rho = (\rho_1, \ldots, \rho_n)$ et les analogues ...]

Soient $Z_1, \ldots, Z_n$ de nouvelles lettres, en considérant les développements possibles de l'expression $u(\mathbf{X} + \mathbf{Y} + \mathbf{Z})$ en déduire la relation

$$\Delta_\rho\, \Delta_\sigma u = \frac{(\rho+\sigma)!}{\rho!\,\sigma!}\, \Delta_{\rho+\sigma} u .$$

3°) Si $\nu = (\nu_1, \ldots, \nu_n)$, et si on pose

$$D^\nu = \frac{\partial^{\nu_1}}{\partial X_1^{\nu_1}} \cdots \frac{\partial^{\nu_n}}{\partial X_n^{\nu_n}}$$

démontrer la formule

$$D^\nu u = \nu!\, \Delta_\nu u .$$

4°) Si tout entier n est inversible dans A, démontrer les formules de Taylor en plusieurs variables

$$u(X+Y) = \sum_{\nu} \frac{1}{\nu!} (D^{\nu}u)(X)\, Y^{\nu} ,$$

et

$$u(X) = \sum_{\nu} \frac{1}{\nu!} D^{\nu}u(a) \,.\, (X-a)^{\nu}$$

lorsque $a \in A^n$.

14. Démontrer la formule de Leibnitz

$$(fg)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} f^{(i)}\, g^{(k-i)} \qquad \text{pour } f, g \in A[X] .$$

15. Soit A un anneau intègre infini. Soient $F, G_1, \ldots, G_n \in A[X_1, \ldots, X_n]$ des polynômes, les G_i étant non nuls. On suppose que

$$\forall\, a \in A^n ,\ (G_1(a) \neq 0 \text{ et } \ldots \text{ et } G_n(a) \neq 0) \Rightarrow F(a) = 0 .$$

Démontrer que le polynôme F est nul.

16. On désigne par $s_0, s_1, \ldots, s_n$ les fonctions symétriques élémentaires en les lettres $X_1, \ldots, X_n$. C'est à dire que

$$s_0 = 1 \ ,\ s_1 = \sum_i X_i \ ,\ s_2 = \sum_{i<j} X_i X_j \ ,\ \ldots \ ,\ s_n = \prod_i X_i \ .$$

Démontrer les formules

$$\prod_{i=1}^{n} (1 + T X_i) = \sum_{k=0}^{n} s_k T^k \quad , \quad \prod_{i=1}^{n} (X - X_i) = \sum_{k=0}^{n} (-1)^{n-k} s_{n-k} X^k .$$

17. Soit $f \in K(X_1, \ldots, X_n)$ une fraction rationnelle symétrique. Démontrer qu'il existe deux polynômes symétriques u et v de $K[X_1, \ldots, X_n]$ tels que $f = u / v$.

18. On pose

$$p_k = \sum_{i=1}^{n} X_i^k \quad \text{pour} \quad k \geq 1 .$$

Démontrer les formules de Newton

$$p_k = \sum_{i=1}^{k-1} (-1)^{i-1} s_i \, p_{k-i} + (-1)^{k-1} k \, p_k ,$$

où les s_i sont définis comme dans l'exercice 16.

19. Soit A un anneau intègre. On suppose que $a_1, \ldots, a_n, b_1, \ldots, b_n$ sont des éléments de A qui vérifient

$$t_k(a_1, \ldots, a_n) = t_k(b_1, \ldots, b_n) \quad \text{pour} \quad 1 \leq k \leq n ,$$

où t_k désigne le polynôme symétrique s_k (respectivement p_k), comme dans l'exercice précédent.

Démontrer qu'il existe une permutation σ de $\{1, \ldots, n\}$ telle $b_{\sigma(i)} = a_i$ pour les indices $i = 1, \ldots, n$.

20. Soit K un corps infini et soit E un espace vectoriel de dimension finie sur K. Soit $V_1, \ldots, V_n$ une famille finie de sous-espaces propres de E (i. e. $V_i \neq E$ pour i variant de 1 à n). Démontrer que l'union des V_i n'est pas égale à E.

[Soit d la dimension de E sur K. On fixe une base quelconque de E et soient alors $P_i[X_1, \ldots, X_n]$, $1 \leq i \leq n$, des polynômes non nuls tels que chaque P_i s'annule sur le sous-espace E_i. Considérer le produit $P_1 \ldots P_n$.]

21. Soit A l'anneau $\mathbf{Z}[\sqrt{-5}]$. On considère le polynôme $f(X) = 3X^2 + 4X + 3$.

1°) Démontrer que le polynôme f est irréductible dans $A[X]$.

2°) Démontrer que, par contre, f n'est pas irréductible dans le corps des fractions de l'anneau A.

[Noter la relation $f(X) = (3X + 2 + \sqrt{-5})(3X + 2 - \sqrt{-5})/3$.]

22. Soit A un anneau commutatif et soit f un polynôme non nul de $A[X]$ qui est un diviseur de zéro dans $A[X]$.

Démontrer le théorème de McCoy :

il existe un élément c de A tel que l'on ait $c \cdot f = 0$.

[Considérer un polynôme g non nul et de degré minimal tel que l'on ait $g \cdot f = 0$.]

23. Démontrer que si f est un polynôme à coefficients dans un anneau intègre alors on a l'équivalence

$$f \text{ quadratfrei} \Leftrightarrow \text{Discr}(f) \neq 0 .$$

24. Soient

$$f(X) = X^2 + a_1 X + a_0 \quad \text{et} \quad g(X) = X^2 + b_1 X + b_0$$

deux polynômes du second degré .

1°) Démontrer la formule

$$\mathrm{Res}(f, g) = (b_0 - a_0)^2 - (b_1 - a_1)(a_1 b_0 - a_0 b_1) .$$

2°) Lorsque f et g sont à coefficients réels et que de plus les racines α_1 et α_2 du polynôme f sont réelles (avec $\alpha_1 < \alpha_2$) alors on a $\mathrm{Res}(f, g) < 0$ si, et seulement si, le polynôme g a ses racines β_1 et β_2 réelles et vérifiant $\alpha_1 < \beta_1 < \alpha_1 < \beta_2$.

25. Soit $P(X)$ un polynôme non constant à coefficients dans un corps dont les racines sont $\alpha_1 , \ldots , \alpha_n$.

1°) Démontrer que le polynôme

$$R(Y) = \mathrm{Res}_X(P(X+Y), P(X))$$

admet pour racines les éléments $\alpha_i + \alpha_j$, $1 \le i , j \le n$.

2°) On suppose en outre qu'aucune des racines de P n'est nulle. Démontrer que le polynôme

$$S(Y) = \mathrm{Res}_X(P(XY), P(X))$$

admet pour racines les éléments α_i / α_j , $1 \le i , j \le n$.

3°) Par analogie, déterminer une formule qui fournit un polynôme dont les racines sont les éléments $\alpha_i . \alpha_j$, $1 \le i , j \le n$.

26. Soit $F(X) = P(X) / Q(X)$ une fraction rationnelle à coefficients dans un corps K, qui est écrite sous forme irréductible. Soit $R(X)$ un polynôme à coefficients dans K et dont les racines sont $\alpha_1, \ldots, \alpha_n$. On suppose que l'on a

$$Q(\alpha_i) \neq 0 \quad \text{pour} \quad i = 1, 2, \ldots, n .$$

Démontrer qu'il existe un polynôme $V(X)$ de degré plus petit que celui de R tel que l'on ait

$$F(\alpha_i) = P(\alpha_i)\ V(\alpha_i) \quad \text{pour} \quad i = 1, 2, \ldots, n .$$

27. Soit K un corps et soient $f(X)$ et $h(X)$ deux polynômes à coefficients dans K. On désigne par $\alpha_1, \ldots, \alpha_n$ les racines de f.

1°) Démontrer que le polynôme

$$g(Y) = \mathrm{Res}_X(f(X), Y - h(X))$$

admet pour racines les éléments $h(\alpha_i)$ pour $i = 1, 2, \ldots, n$.

2°) Lorsque $h(X) = X^k$, $k \geq 2$, démontrer la formule

$$g(Y) = (-1)^{kn} \prod_{i=0}^{n-1} f(\zeta^i Z),$$

où ζ est une racine k - ième primitive de l'unité (i.e. $\zeta^k = 1$ mais $\zeta^j \neq 1$ pour les entiers $j = 1, \ldots, k-1$) et où Z vérifie $Z^k = Y$.

En déduire la méthode de Graeffe (cas $k = 2$).

28. Soient R un anneau, A un sous-anneau de R et x un élément de R.
Démontrer que les propriétés suivantes sont équivalentes :

(i) il existe des éléments $a_1, \ldots, a_n$ de A tels que

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0,$$

(on dit alors que x est **entier** sur A)

(ii) l'anneau A [x] est un A-module de type fini,

(iii) il existe un sous anneau B de R qui contient A et qui est un A-module de type fini.

[Pour montrer que (iii) implique (i) on peut prendre un système de générateurs $y_1 \ldots y_k$ du A-module B et écrire

$$x\, y_i = \sum_{j=1}^{k} a_{ij}\, y_j \quad \text{pour} \quad 1 \leq i \leq k.$$

En déduire que les y_i sont solutions d'un système homogène de k équations. Soit Δ le déterminant de ce système démontrer que Δ est nul et qu'il existe une suite d'éléments $b_1, \ldots, b_n$ de A tels que

$$\Delta = x^n + b_1 x^{n-1} + \ldots + b_n \ . \ ]$$

2°) En déduire que l'ensemble A' des éléments de R qui sont entiers sur A est un sous-anneau de R.

Donner une autre démonstration de ce résultat grâce à l'exercice 25 ci-dessus.

3°) Si R est un anneau intègre, démontrer que A' est un corps si, et seulement si, A est aussi un corps.

29. Soit

$$f(X) = a_n X^n + \ldots + a_0$$

un polynôme à coefficients dans un corps et soient $\alpha_1, \ldots, \alpha_n$ ses racines.

1°) Démontrer que le discriminant Δ de ce polynôme vérifie

$$\Delta = (-1)^{n(n-1)/2} \left(\prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 \right) a_n^{2n-1} .$$

2°) Pour k entier ≥ 0 on définit la k - ième somme de Newton

$$S_k = \sum_{i=1}^{n} \alpha_i^k .$$

Soit D le déterminant de la matrice $A = (a_{ij})_{1 \le i, j \le n}$ où $a_{ij} = \alpha_i^{j-1}$.

Démontrer la **formule de Vandermonde**

$$D = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j) .$$

En déduire une relation entre Δ et D^2.

Démontrer enfin les relations

$$D^2 = \det(A) \det({}^tA) = \det(S)$$

où

$$S = (s_{ij})_{1 \le i, j \le n} \quad \text{avec} \quad s_{ij} = S_{i+j-2} .$$

30. Soient A et B deux polynômes à coefficients dans un anneau R et soit a un élément de cet anneau.

Par des manipulations élémentaires sur la matrice de Sylvester, démontrer la formule

$$\mathrm{Res}\left((X - a) A(X), B(X)\right) = B(a) . \mathrm{Res}\left(A(X), B(X)\right) .$$

En déduire les formules (v) du paragraphe 5, ainsi que la relation

$$\mathrm{Res}\left(A(X), B(X) C(X)\right) = \mathrm{Res}\left(A(X), B(X)\right) . \mathrm{Res}\left(A(X), C(X)\right)$$

lorsque C est un polynôme à coefficients dans R.

31. Lorsque f et g sont des polynômes à coefficient dans un corps, on a vu que ces polynômes ont un facteur commun non trivial si, et seulement si, il existe deux polynômes u et v tels que

$$u f + v g = 0 \text{ , avec } \deg(u) < \deg(g) \text{ et } \deg(v) < \deg(f) .$$

Généraliser ce résultat au cas de polynômes à coefficients dans un anneau factoriel.

32. Soit A un anneau et soient f et g deux polynômes homogènes appartenant à $A[X_1, \dots, X_s, Y]$ de degrés respectifs m et n et dont les degrés en Y sont aussi respectivement m et n.

Démontrer que le résultant en Y de ces polynômes est ou bien nul, ou bien un polynôme homogène de degré mn dans $A[X_1, \dots, X_s]$.

[Multiplier par t chacune des indéterminées $X_1, \dots, X_s$ et considérer la matrice de Sylvester des polynômes f et g ainsi transformés. En multipliant la $i^{ème}$ ligne de cette matrice par t^{n-i+1} pour $1 \leq i \leq n$, et la $(n+j)^{ième}$ ligne par t^{m-j+1} pour les indices $j = 1, \dots, m$, démontrer que le résultant $R = \mathrm{Res}_Y(f, g)$ vérifie la formule

$$t^p R(tX_1, \dots, tX_s) = t^p R(X_1, \dots, X_s) ,$$

où

$$p = n(n+1)/2 + m(m+1)/2 \quad \text{et} \quad q = (m+n)(m+n+1)/2 .$$

Conclure.]

En déduire une démonstration de la propriété (v) du résultant (voir § 5).

33. Le but de cet exercice est de démontrer que la formule donnant le résultant est indécomposable. De manière précise, si $u_0, \ldots, u_m, v_0, \ldots, v_n$ sont des indéterminées et si $f(X) = u_0 X^m + \ldots + u_{m-1} X + u_m$ et $g(X) = v_0 X^n + \ldots + v_{n-1} X + v_n$ sont deux polynômes à coefficients dans un corps K dont le résultant est

$$R(u, v) = \mathrm{Res}_X(f, g)$$

alors le polynôme $R(u, v)$ est irréductible dans l'anneau $K[u, v]$.

On procédera par récurrence sur l'entier $s = m + n$.

1°) Traiter la cas $s = 2$.

2°) Supposons le résultat vrai à l'ordre $s - 1$. Considérons le polynôme

$$Q = R(0, u_1, \ldots, u_m, v_0, \ldots, v_n).$$

a) Démontrer que

$$Q = (-1)^n v_0 R_0(u_1, \ldots, u_m, v_0, \ldots, v_n),$$

où R_0 est le résultant (par rapport à X) de deux polynômes en $s+1$ indéterminées.

b) En déduire que si R est réductible alors il ne peut admettre de décomposition que sous la forme $R = S T$ où

$$S = a u_0 + b v_0, \quad a, b \in K.$$

En outre, démontrer que a et b sont non nuls.

[Noter que R contient le monôme $u_0^n v_n^m$ ...]

c) Démontrer qu'une décomposition de ce type est impossible et conclure.

[Une telle décomposition entraînerait que deux polynômes quelconques f et g comme plus haut dont les coefficients u_0 et v_0 vérifient $a u_0 + b v_0 = 0$ ont toujours une racine commune ... Autre méthode possible : utiliser le fait que les polynômes S et T doivent être homogènes par rapport à chacune des familles de variables $u_0, \ldots, u_m$ et $v_0, \ldots, v_n$ ce qui implique $a\,b = 0$ ...]

34. Soient f et g deux polynômes à coefficients dans un anneau A .

Démontrer qu'il existe deux polynômes u et v à coefficients dans A tels que

$$\mathrm{Res}(f,g) = u(X)f(X) + v(X)g(X) .$$

[Soient $C_1, \ldots, C_{m+n}$ les vecteurs colonnes de la matrice de Sylvester des polynômes f et g . Remplacer la dernière colonne C_{m+n} par la combinaison linéaire $C_{m+n} + X\,C_{m+n-1} + X^2\,C_{m+n-1} + \ldots + X^{m+n-1}\,C_1 \ \ldots$]

En déduire la propriété (iv) du résultant (voir § 5).

35. Soient F et G deux polynômes à coefficients dans un corps K , de degrés respectifs m et n .

On suppose qu'il existe un polynôme D de degré d tel que

$$F(X) = D(X)\,F^*(X) \ , \ G(X) = D(X)\,G^*(X) \ , F^*, G^* \in K[X] .$$

Soit A la matrice des coefficients des polynômes $X^{n-1}F(X)$, $X^{n-2}F(X)$, ... , $X\,F(X)$, $F(X)$, $X^{m-1}G(X)$, $X^{m-2}F(X)$, ... , $X\,G(X)$, $G(X)$, sur la base usuelle $(X^{m+n-1}, \ldots, X, 1)$.

Pour $0 \le k \le \min\{ m, n \}$ on désigne par A_k la matrice obtenue à partir de A en supprimant les rangées (lignes et colonnes) d'indice $< k$ et celles d'indice $> m+n-k$. (Donc A_0 est égale à A , A_1 est la matrice A privée de tous ses éléments qui sont au "bord" , ...)

1°) Démontrer que les polynômes F* et G* ont un facteur commun non trivial si, et seulement si, il existe des polynômes U et V à coefficients dans K tels que

$$U\,F + V\,G = 0 \quad \text{avec} \quad \deg(U) \le n-d-1 \ \text{et} \ \deg(V) \le m-d-1 .$$

2°) On considère D fixé mais F* et G* variables.

Démontrer que

$$R^* = \mathrm{Res}_X (F^*, G^*)$$

est un polynôme homogène de degré $m + n - 2d$ par rapport à l'ensemble des indéterminées $a_0 , ..., a_{m-d} , b_0 , ..., b_{n-d}$.

Démontrer que le déterminant S de la matrice A_d est aussi un polynôme homogène de degré $m + n - 2d$ par rapport à $a_0 , ..., a_{m-d} , b_0 , ..., b_{n-d}$.

En déduire que R* et S sont égaux à un facteur multiplicatif constant (non nul) près.

[Utiliser l'irréductibilité du résultant : exercice 33. Référence : J. Lelong - Ferrand et J. M. Arnaudiès , *Cours de Mathématiques,* tome 1 , *Algèbre* , Dunod , Paris, 1971 .]

36. Soit P un polynôme à coefficients entiers de la forme

$$P (X) = a (X - \alpha_1) (X - \alpha_2) ... (X - \alpha_n) .$$

Soit r un entier, $1 \leq r \leq n$, montrer que le nombre $a \alpha_1 \alpha_2 ... \alpha_r$ est un entier algébrique (voir l'exercice 28) .

[En considérant le calcul de la division euclidienne, démontrer que si Q (X) est un polynôme à coefficients qui sont des entiers algébriques dont α est une racine alors le polynôme $Q (X) / (X - \alpha)$ est encore à coefficients entiers algébriques. Le résultat en découle puisque le terme constant du polynôme $P (X) / ((X - \alpha_{r+1}) ... (X - \alpha_n))$ n'est autre que le nombre $a \alpha_1 \alpha_2 ... \alpha_r$.]

37. Soient K un corps, $P \in K[X]$ un polynôme de degré $n > 0$ et m un entier vérifiant $0 \leq m \leq n$. Soient enfin $a_1, \ldots, a_m$ m éléments distincts de K.

Démontrer que les polynômes

$$P(X), P(X + a_1), \ldots, P(X + a_m), 1, X, \ldots, X^{n-m-1}$$

sont linéairement indépendants sur K.

[En supposant que l'on a une relation linéaire à coefficients dans K de la forme

$u_0 P(X) + u_1 P(X + a_1) + \ldots + u_m P(X + a_m) + v_0 + v_1 X + \ldots + u_{m'} X^{m'} = 0$,

où $m' = n - m + 1$, démontrer que la somme des u_i est nulle. On peut donc réécrire la relation précédente de la manière suivante

$u_1 (P(X + a_1) - P(X)) + \ldots + u_m (P(X + a_m) - P(X)) + v_0 + v_1 X + \ldots + u_{m'} X^{m'} = 0$.

En déduire que l'on peut raisonner par récurrence sur le degré du polynôme P ...]

38. Soient K un corps et $P \in K[X]$ un polynôme irréductible de degré n.

1°) Démontrer qu'il existe un corps L admetant K comme sous-corps et dans lequel le polynôme P possède une racine [Considérer $K[X] / (P)$.]. De plus, démontrer que le **degré** de L sur K (c'est à dire la dimension de L en tant que qu'espace vectoriel sur K) est égal à n et que L est unique à isomorphisme près.

2°) En déduire qu'il existe un corps L' admetant K comme sous-corps et dans lequel le polynôme P se factorise en facteurs du premier degré. De plus, démontrer que le degré de L' sur K est un diviseur de $n!$ et que L' est unique à isomorphisme près. Le corps L' est appelé **corps de décomposition**, ou encore **corps des racines,** du polynôme P.

39. Démontrer le résultat suivant dû à D. Masser : soient K un corps infini, Q un polynôme de $K[X, Y]$ et α, β, λ trois éléments de K, avec $\alpha\beta \neq 0$, tels que l'on ait

$$(*) \qquad Q(X+\beta, \alpha Y) = \lambda Q(X, Y),$$

alors Q appartient à $K[Y]$.

[Considérer d'abord le cas où Q appartient à $K[X]$ et vérifie $Q(X+\beta) = \lambda Q(X)$ avec $\beta \neq 0$, et démontrer qu'alors le polynôme Q est constant (sinon il aurait une infinité de zéros). Puis, dans le cas général, écrire

$$Q(X, Y) = \sum_{i=0}^{d} a_i(X) X^i,$$

et montrer que la condition (*) implique les relations $a_i(X+\beta)\alpha^i = \lambda a_i(X)$, pour $0 \leq i \leq d$. Conclure.]

Déterminer les polynômes $Q \in C[Y]$ qui vérifient la relation $Q(\alpha Y) = \lambda Q(Y)$.

[Considérer d'abord le cas où Q est irréductible et vérifie cette relation avec $\alpha \neq 1$, démontrer que Q est alors de la forme $Q(Y) = aY$ pour un certain élément a de K. (d'après le théorème de d'Alembert - démontré au chapitre suivant - le polynôme Q est alors de la forme $Q(Y) = aY + b$, avec $a \neq 0$), de $a\alpha Y + b = \lambda(aY + b)$, on déduit $\lambda = \alpha$ (car $a \neq 0$), puis $b = 0$ (puisque $\lambda = \alpha \neq 1$). Conclure.]

40. Soit K un corps et soient $F_1, \ldots, F_r$ des polynômes de $K[X, Y]$, de degré au plus L par rapport à X et au plus M par rapport à Y. Soient (ξ_i, η_i), pour des indices $1 \leq i \leq N$, des zéros communs dans K^2 à tous les polynômes $F_1, \ldots, F_r$, tels que les points $\xi_1, \ldots, \xi_N$ sont deux à deux distincts.

Démontrer que l'on a $N \leq 2LM$.

Indication : On utilise la technique du U-résultant de Kronecker. On introduit les $2r$ nouvelles variables $U_1, ..., U_r, V_1, ..., V_r$ et on pose

$$G = \sum_{j=1}^{r} U_j F_j(X,Y) \quad , \qquad H = \sum_{j=1}^{r} V_j F_j(X,Y) \quad .$$

Soit $R \in K[U_1, ..., U_r, V_1, ..., V_r, X]$ le résultant par rapport à Y des polynômes F et G. Démontrer les faits suivants : (i) $R \neq 0$; (ii) $\deg_X R \leq 2LM$; et

(iii) $\qquad R(U_1, ..., U_r, V_1, ..., V_r, \xi_i) = 0 \quad$ pour $\quad i = 1, ..., N$.

Puis conclure.

41. Des deux exercices précédents déduire le résultat suivant, dû à D. Masser :

Soient K un corps infini, Q un polynôme de $K[X, Y]$ et α, β, γ trois éléments non nuls de K. Soient U_1, U_2, V_1, V_2 des entiers positifs, on pose $U = U_1 + U_2$, et $V = V_1 + V_2$, et on suppose que

(a) pour $i = 1$ and $i = 2$, les points

$$u + v\beta \quad , \quad (-U_1 \leq u \leq U_1 \, , -V_1 \leq v \leq V_1)$$

sont deux à deux distincts et on a

$$(2U_1 + 1)(2V_1 + 1) > L ;$$

(b) $\text{Card}\{ \alpha^u \gamma^v \; ; -U_1 \leq u \leq U_1 \, , -V_1 \leq v \leq V_1 \} > M ;$

(c) $\text{Card}\{ u + v\beta \; ; -U_2 \leq u \leq U_2 \, , -V_2 \leq v \leq V_2 \} > 2LM .$

Alors au moins un des nombres $P(u + v\beta, \alpha^u \gamma^v)$, $(-U \leq u \leq U \, , -V \leq v \leq V)$ est non nul.

Démontrer en outre que ce résultat n'est plus vrai si l'une quelconque des conditions suivantes n'a pas lieu :

(i) $\text{Card}\{ (u + v\beta, \alpha^u \gamma^v) ; -U \leq u \leq U \, , -V \leq v \leq V \} \geq (L+1)(M+1)$,

(ii) $\text{Card}\{ u + v\beta \; ; -U \leq u \leq U \, , -V \leq v \leq V \} \geq L + 1$,

(iii) $\text{Card}\{ \alpha^u \gamma^v ; -U \leq u \leq U \, , -V \leq v \leq V \} \geq M + 1$.

42. Soit $f \in \mathbf{R}[X_1, \ldots, X_k]$ un polynôme à coefficients réels. Pour x entier positif, on pose

$$N_f(x) = N(x) = \text{Card}\{\mathbf{a} = (a_1, \ldots, a_k) \in \mathbf{Z}^k ; f(\mathbf{a}) = 0 \text{ et } \max\{|a_i| \leq x\}\}.$$

1°) Démontrer qu'il existe une constante C (qui dépend de f) telle que l'on ait

$$N(x) \leq C\, x^{k-1}.$$

[On écrit

$$f = g_m X_1^m + g_{m-1} X_1^{m-1} + \ldots + g_0 \ , \ g_i \in \mathbf{R}[X_2, \ldots, X_k] \text{ pour } 0 \leq i \leq m.$$

Alors $g = g_0^2 + \ldots + g_m^2$ est non nul et on a

$$N_f(x) \leq m(2x+1)^{k-1} + (2x+1) N_g(x).]$$

2°) Montrer que cette estimation est essentiellement la meilleure possible.

[Exemples : $f = X_1 \ldots X_k$, $f = X_1 + \ldots + X_k$.]

3°) Comment ce résultat se généralise-t-il si on suppose cette fois f à coefficients complexes et $\mathbf{a} \in (\mathbf{Z}[\sqrt{-1}])^n$?

43. Soit K un corps et soient $d_1, \ldots, d_n$ des entiers ≥ 1. Soit E l'ensemble des polynômes $P \in K[X_1, \ldots X_n]$ dont le degré partiel par rapport à X_i est $< d_i$ pour chacun des indices $i = 1, 2, \ldots, n$.

Montrer que l'application $f : E \to K[X]$ définie par

$$f\left(P(X_1, \ldots, X_n)\right) = P(X, X^{d_1}, X^{d_1 d_2}, \ldots, X^{d_1 d_2 \ldots d_{n-1}})$$

est un homomorphisme injectif.

(Ce résultat, dû à Kronecker, permet de ramener plusieurs questions sur les polynômes en plusieurs indéterminées au cas d'une variable. Malheureusement, en pratique, il a l'inconvénient de conduire à une explosion des degrés.)

CHAPITRE IV

Polynômes à coefficients complexes

Jusqu'au § 4.2 , tous les polynômes considérés sont en une seule indéterminée.

1. Le théorème de d'Alembert .

1. Enoncé .

Rappelons qu'un polynôme est dit **non constant** lorsque son degré est strictement positif. Grâce à cette définition, le théorème de d'Alembert-Gauss s'énonce ainsi.

THEOREME 1 . – Tout polynôme non constant à coefficients complexes admet au moins une racine dans **C** .

Il en résulte évidemment, par récurrence sur le degré, que tout polynôme sur **C** de degré n strictement positif admet exactement n racines complexes (chacune étant comptée autant de fois que son ordre de multiplicité) . On dit que **C** est un corps **algébriquement clos** .

2. Propriétés analytiques utilisées .

Les seules propriétés "analytiques" que nous admettrons sont les suivantes :

(i) Tout polynôme de degré impair sur **R** admet au moins une racine réelle.

(ii) Pour tout nombre réel y positif il existe $x \in \mathbf{R}$ tel que $x^2 = y$.

Notons d'abord le lemme suivant.

LEMME 1 . – Soient a, b, c trois éléments d'un corps K , $a \neq 0$. On suppose qu'il existe $t \in K$ tel que l'on ait $b^2 - 4ac = t^2$. Alors l'équation $ax^2 + bx + c = 0$ admet au moins une racine dans K ; plus précisément cette équation équivaut à

$$x = \frac{-b \pm t}{2a} .$$

> La démonstration est bien connue. L'équation

$$a x^2 + b x + c = 0 \quad , \quad a, b, c \in K \ , \ a \neq 0 ,$$

se réécrit sous la forme équivalente

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

D'où les solutions (distinctes ou confondues)

$$x = \frac{-b \pm t}{2a} . \ <$$

Montrons maintenant que la propriété (ii) implique la propriété

(ii') Pour tout nombre complexe z il existe $w \in \mathbf{C}$ tel que $w^2 = z$.

Soit en effet un nombre complexe $z = a + ib$, a et b réels. Cherchons w sous la forme $w = u + iv$, u et v réels. L'équation $w^2 = z$ équivaut aux deux conditions

$$u^2 - v^2 = a \quad \text{et} \quad 2uv = b \quad (\text{donc} \quad -u^2 v^2 = -b^2/4) .$$

Ainsi les nombres u^2 et v^2 sont solutions de l'équation

$$x^2 - ax - b^2/4 = 0$$

dont le discriminant est $a^2 + b^2$ donc positif.

Le lemme 1, joint à la propriété (ii), montre que cette dernière équation admet les solutions

$$u^2 = \frac{a+\sqrt{a^2+b^2}}{2} \quad \text{et} \quad -v^2 = \frac{a-\sqrt{a^2+b^2}}{2} .$$

Enfin, deux nouvelles applications de (ii) fournissent des nombres réels u et v qui vérifient $(u+iv)^2 = z$. D'où (ii').

En appliquant encore une fois le lemme, ainsi que (ii'), on obtient le résultat suivant.

PROPOSITION 1. – Toute équation du second degré dans le corps **C** possède deux racines complexes (distinctes ou confondues).

3. Démonstration du théorème.

La méthode que nous utilisons est essentiellement due à Lagrange. Nous suivons l'exposé donné par Samuel (*Théorie Algébrique des Nombres* , appendice du chapitre II).

Soit P un polynôme non constant à coefficients complexes. Quitte à le multiplier par son conjugué, on peut supposer que P est à coefficients réels.
(Si $(P\overline{P})(a) = 0$ alors l'un au moins des deux nombres a ou $\bar{a}$ est une racine de P.)

Considérons donc un polynôme P non constant, à coefficients réels. Soit $d = 2^n q$, avec q impair, son degré. On raisonne par récurrence sur l'entier n.

Si n est nul, la propriété (i) implique que P possède une racine réelle.

Supposons $n \geq 1$. Soient alors $x_1, \ldots, x_d$ les racines de P dans une extension convenable de **C**. Pour tout réel c, on pose

$$y_{hk}(c) = y_{hk} = x_h + x_k + c\, x_h\, x_k \text{ , pour } 1 \leq h \leq k \leq d.$$

Le polynôme $Q(X) = \prod_{h \leq k} (X - y_{hk})$ a pour coefficients des polynômes symétriques en les x_i dont les coefficients sont réels, les coefficients de Q sont donc aussi réels. On a

$$\deg(Q) = d(d\mp1)/2 = 2^{n-1} q(d\mp1) \text{ , avec } q(d\mp1) \text{ impair.}$$

On peut donc appliquer l'hypothèse de récurrence au polynôme Q : il existe une racine de Q dans le corps **C**, donc un couple (h, k) tel que $y_{hk}(c)$ soit dans **C**.

En prenant $d(d\mp1)/2 + 1$ valeurs différentes du paramètre c, on constate qu'il existe un certain couple d'indices (r, s) et deux réels distincts c et c' tels que les nombres $y_{rs}(c)$ et $y_{rs}(c')$ soient dans **C**. Il en résulte aussitôt que la somme $x_r + x_s$ et le produit $x_r\, x_s$ appartiennent aussi à **C**. Par conséquent, x_r et x_s sont solutions d'une équation du second degré à coefficients complexes, et d'après la proposition 1 ils appartiennent à **C**. D'où la conclusion.

Remarque : Nous avons en fait démontré que si **R** est un corps ordonné qui vérifie (i) et (ii) alors le corps $\mathbf{R}[\sqrt{-1}]$ est algébriquement clos.

4. Polynômes réels irréductibles.

Le théorème 1 a la conséquence suivante, dont la preuve est laissée en exercice.

PROPOSITION 2. – Les seuls polynômes irréductibles de $\mathbf{R}[X]$ sont les polynômes du premier degré et ceux du second degré dont le discriminant est négatif.

2. Estimations des racines .

Les résultats de ce paragraphe sont en grande partie dus à Cauchy. La présentation donnée ici s'inspire du livre *Calcul Infinitésimal* de Dieudonné (problème 1 du chapitre II) .

1. Principe de démonstration .

PROPOSITION 3 . – Soit $P(X) = X^d + a_{d-1} X^{d-1} + \ldots + a_0$ un polynôme à coefficients complexes qui a pour racines $z_1, \ldots, z_d$. Posons

$$r_0 = \max_{1 \leq k \leq d} \{ |z_k| \} .$$

Alors, si un réel $r > 0$ vérifie la condition

$$r^d \geq |a_{d-1}| r^{d-1} + \ldots + |a_0| ,$$

on a $r_0 \leq r$.

> Supposons $r_0 > 0$, sinon il n'y a rien à démontrer.

D'après le lemme 2 ci-dessous, le polynôme

$$X^d - |a_{d-1}| X^{d-1} - \ldots - |a_0|$$

admet une seule racine réelle positive, nous la noterons r_1 . Il est clair que r_0 est majoré par r_1 .

Par ailleurs, pour $j = 1, \ldots, d$, on a

$$|z_j^d| = |a_{d-1} z_j^{d-1} + \ldots + a_0| \leq |a_{d-1}| |z_j^{d-1}| + \ldots + |a_0| ,$$

et donc en particulier

$$r_0^d \leq |a_{d-1}| r_0^{d-1} + \ldots + |a_0| .$$

On en déduit les inégalités $r_0 \leq r_1 \leq r$. <

2. Un lemme analytique .

Le résultat utilisé plus haut est le suivant.

LEMME 2 . – Tout polynôme à coefficients réels de la forme

$$c_d X^d + c_{d-1} X^{d-1} + \ldots + c_j X^j - c_{j-1} X^{j-1} - \ldots - c_0 \quad , \; d \geq 1 \; ,$$

avec $c_i \geq 0$ pour $i = 0, \ldots, d$ et $c_d + \ldots + c_j > 0$, $c_{j-1} + \ldots + c_0 > 0$, admet une racine réelle > 0 et une seule .

> La fonction $f(x) = c_d x^{d-j} + \ldots + c_j - c_{j-1} x^{-1} - \ldots - c_0 x^{-j}$ est continue sur l'intervalle réel $]\, 0 , \infty \,[$, strictement croissante (comme somme de fonctions strictement croissantes) et tend vers $-\infty$ (respectivement $+\infty$) si x tend vers zéro (respectivement $+\infty$) ; elle admet donc un zéro positif et un seul. <

Remarque : Ce lemme est un cas particulier de la règle de Descartes (voir chapitre 5).

3. Majoration des racines .

La proposition 2 a le corollaire suivant.

THEOREME 2 . – Soit $P(X) = X^d + a_{d-1} X^{d-1} + \ldots + a_0$ un polynôme à coefficients complexes qui a pour racines $z_1, \ldots, z_d$. Posons

$$r_0 = \max_{1 \leq k \leq d} \{ |z_k| \} \; .$$

Alors r_0 vérifie les majorations suivantes :

(i) $r_0 \leq \max \{ 1 , \sum_{k=1}^{d} |a_k| \}$,

(ii) $r_0 < 1 + \max_{1 \leq k \leq d} \{ |a_k| \}$,

(iii) si $\lambda_1, \ldots, \lambda_d$ sont des réels > 0 vérifiant $\lambda_1^{-1} + \ldots + \lambda_d^{-1} = 1$ alors on a

$$r_0 \leq \max_{1 \leq k \leq d} \{ \lambda_k |a_{d-k}| \}^{1/k} ,$$

(iv) $$r_0 \leq \max_{1 \leq k \leq d} \{ d\, a_k \}^{1/k} ,$$

(v) si tous les coefficients a_k sont non nuls, on a

$$r_0 \leq \left\{ 2|a_{d-1}| , 2\left|\frac{a_{d-2}}{a_{d-1}}\right| , \ldots , 2\left|\frac{a_1}{a_2}\right| , \left|\frac{a_0}{a_1}\right| \right\} ,$$

(vi) $r_0 \leq |1 - a_{d-1}| + |a_{d-2} - a_{d-1}| + \ldots + |a_0 - a_1| + |a_0|$,

(vii) si tous les a_k sont réels et > 0, alors

$$r_0 \leq \max \left\{ a_{d-1} , \frac{a_{d-2}}{a_{d-1}} , \ldots , \frac{a_1}{a_2} , \frac{a_0}{a_1} \right\} ,$$

(viii) enfin

$$r_0 \leq \max_{1 \leq k \leq d} \left\{ \left(\frac{a_{d-k}}{\binom{d}{k}} \right)^{1/k} \left(2^{1/d} - 1 \right)^{-1} \right\} .$$

> Démonstrations .

(i) : Si $|a_{d-1}| + \ldots + |a_0| \leq 1$, on peut choisir $r = 1$ dans la proposition 1 , sinon on peut prendre $r = |a_{d-1}| + \ldots + |a_0|$.

(ii) : Soit A le maximum des $|a_k|$. On peut prendre $r = A + 1$, en effet on a alors

$$r^d = A\,(r^{d-1} + \ldots + 1) + 1 > |a_{d-1}|\,r^{d-1} + \ldots + |a_0| .$$

(iii) : Désignons par ρ le membre de droite de l'inégalité (iii) . On a alors

$$|a_{d-k}| \leq \lambda_k^{-1}\,\rho^k \quad \text{pour} \quad 1 \leq k \leq d .$$

D'où l'inégalité

$$\sum_{k=1}^{d} |a_{d-k}|\,\rho^{d-k} \leq \sum_{k=1}^{d} \rho^d \lambda_k^{-1} = \rho^d .$$

On peut donc prendre $r = \rho$.

(iv) : Prendre tous les λ égaux à d dans l'inégalité (iii) .

(Remarque : on peut même prendre λ = nombre de a_i non nuls.)

(v) : Appelons à nouveau ρ le membre de droite. On démontre successivement les majorations

$$|a_{d-1}| \leq \rho/2 \ , \ |a_{d-2}| \leq (\rho/2)^2 \ , \ \ldots$$

$$|a_1| \leq (\rho/2)^{d-1} \ , \ |a_0| \leq 2(\rho/2)^d .$$

D'où l'inégalité

$$\sum_{k=1}^{d} |a_{d-k}| \rho^{d-k} \leq \rho^{d} ,$$

et donc $\rho \geq r$.

(vi) : Appliquer (i) au polynôme $(X - 1) P(X)$.

(vii) : Soit ρ le membre de droite de l'inégalité (vii) . Par le changement de variable $X \to X / \rho$, le polynôme P est transformé en le polynôme

$$\rho^{d} X^{d} + a_{d-1} \rho^{d-1} X^{d-1} + \ldots + a_0 .$$

En appliquant la relation (vi) à ce polynôme, on obtient l'inégalité

$$\frac{r_0}{\rho} \leq \left| \frac{a_{d-1}}{\rho} - 1 \right| + \left| \frac{a_{d-2}}{\rho^2} - \frac{a_{d-1}}{\rho} \right| + \ldots + \left| \frac{a_0}{\rho^{d}} \right| .$$

Pour conclure, il suffit de noter que le membre de droite de cette dernière inégalité est tout égal à $-1 + 2 a_0 \rho^{-d}$, et donc majoré par 1 (on a $a_0 \leq \rho^{d}$) .

(viii) : Appliquer (iii) en choisissant

$$\lambda_k^{-1} = \binom{d}{k} \left(2^{1/d} - 1 \right)^{k} . \quad <$$

Remarque : En considérant le polynôme $X^{d} . P(X^{-1})$, appelé **polynôme réciproque** de P , et en supposant le terme constant a_0 non nul, on obtient des minorations des $|z_j|$. Par exemple,

$$\min_{1 \leq j \leq d} |z_j| \geq \frac{a_0}{1 + \max_{1 \leq k \leq d} |a_{d-k}|} .$$

3. La mesure d'un polynôme .

1. Définition .

Soit P un polynôme à coefficients complexes qui s'écrit

$$P = a_d X^d + a_{d-1} X^{d-1} + \ldots + a_0 = a_d (X - z_1) \ldots (X - z_d), \text{ avec } a_d \neq 0.$$

La **mesure** de P est définie par la formule

$$M(P) = |a_d| \prod_{j=1}^{d} \max \{ 1, |z_j| \} .$$

Cette notion a été introduite par K. Mahler .

Si P et Q sont des polynômes non nuls, on peut remarquer que

$$M(P.Q) = M(P).M(Q) ,$$

$$M(X^k . P(X)) = M(P(X)),$$

et aussi que pour tout entier positif k on a

$$M(P(X^k)) = M(P(X)).$$

On pose

$$\| P \| = \| P \|_2 = (|a_0|^2 + \ldots + |a_d|^2)^{1/2} .$$

Le théorème 2 fournit immédiatement des majorations de la mesure, mais on peut obtenir une estimation souvent bien meilleure en utilisant le théorème 3 ci-dessous.

Il est temps d'introduire quelques définitions. Soit A un sous-anneau d'un anneau B intègre . Un élément x de B est dit **algébrique** sur A lorsqu'il est racine d'un polynôme non nul à coefficients dans A ; il existe alors un polynôme non nul de A [X] , de degré minimal et dont les coefficients sont premiers entre eux qui s'annule en x , un tel polynôme est appelé **polynôme minimal** (sur A) de l'élément x . Un nombre complexe algébrique sur **Q** est appelé un **nombre algébrique.**

Quand α est un nombre algébrique non nul, nous définissons sa mesure $M(\alpha)$ par la formule $M(\alpha) = M(P)$, où P est le polynôme minimal de α sur $\mathbf{Z}$. La mesure des nombres algébriques vérifie quelques propriétés importantes, nous les rappelons brièvement.

Soient α et α' deux nombres algébriques non nuls, de degrés respectifs d et d'. La valeur absolue de α vérifie

(M1) $\qquad 1 / M(\alpha) \leq |\alpha| \leq M(\alpha)$.

La mesure du produit $\alpha.\alpha'$ vérifie

(M2) $\qquad M(\alpha . \alpha') \leq M(\alpha)^{d'} . M(\alpha')^{d}$,

et la mesure de la somme $\alpha + \alpha'$ vérifie

(M3) $\qquad M(\alpha + \alpha') \leq 2^{d d'} M(\alpha)^{d'} . M(\alpha')^{d}$.

Soit k un entier positif, alors

(M4) $\qquad M(\alpha^{1/k}) \leq M(\alpha)$.

Preuves:

(M1) : La preuve est presque évidente.

(M2) : Soient a et a' les coefficients dominants respectifs des polynômes minimaux de α et de α'. Soient $\{ \alpha_i ; 1 \leq i \leq d \}$ et $\{ \alpha'_j ; 1 \leq j \leq d' \}$ les ensembles respectifs des conjugués de α et de α', alors $\alpha.\alpha'$ est a racine du polynôme

$$a^{d'} . a^{d} . \prod (z - \alpha_i . \alpha'_j) ,$$

de plus ce polynôme a des coefficients entiers. Ce qui implique l'estimation

$$\begin{aligned} M(\alpha.\alpha') &\leq a^{d'} . a^{d} . \prod \max\{ 1 , |\alpha_i . \alpha'_j| \} \\ &\leq a^{d'} . a^{d} . \prod \max\{ 1, |\alpha_i| \}^{d'} . \prod \max\{ 1, |\alpha'_j| \}^{d} \\ &= M(\alpha)^{d'} . M(\alpha')^{d} . \end{aligned}$$

(M3) : La preuve est semblable à la précédente.

(M4) : Soit P le polynôme minimal de α sur $\mathbf{Z}$. Alors $\alpha^{1/k}$ est racine du polynôme $Q(X) := P(X^{k})$, de sorte que $M(\alpha^{1/k}) \leq M(Q) = M(P) = M(\alpha)$.

2. Un lemme algébrique .

Le résultat élémentaire suivant va nous permettre de majorer facilement M (P) .

LEMME 2 . – Pour un polynôme Q à coefficients complexes quelconque et pour tout nombre complexe z , on a la relation

$$\| (X + z)\, Q(X) \| = \| (\bar{z}\, X + 1)\, Q(X) \| .$$

> Supposons que le polynôme Q s'écrive $Q = \sum_{k=0}^{m} c_k X^k$. Le carré du membre de gauche admet alors pour développement

$$\sum_{k=0}^{m+1} (c_{k-1} + z\, c_k)(\bar{c}_{k-1} + \bar{z}\, \bar{c}_k) = (1 + |z|^2)\, \|Q\|^2 + \sum_{k=1}^{m} (z\, c_k\, \bar{c}_{k-1} + \bar{z}\, \bar{c}_k\, c_{k-1}) ,$$

où on a posé $c_{-1} = 0$ et $c_{m+1} = 0$.

On vérifie aussitôt que le carré du second membre admet exactement le même développement. <

3. Une majoration de M (P) .

THEOREME 3 (Vicente Gonçalves). – Soit $P = a_d X^d + a_{d-1} X^{d-1} + \ldots + a_0$ un polynôme non constant à coefficients complexes . La mesure de P vérifie l'inégalité

$$M(P)^2 + |a_0\, a_d|^2\, M(P)^{-2} \leq \|P\|^2 .$$

> Soient $z_1, \ldots, z_k$ les racines de P qui sont extérieures au disque unité. Alors la mesure de P vaut $M(P) = |a_0| |z_1 \ldots z_k|$.

Considérons le polynôme

$$R(X) = a_d \prod_{j=1}^{k} (\bar{z}_j X - 1) . \prod_{j=k+1}^{d} (X - z_j) = b_d X^d + \ldots + b_0 .$$

En appliquant k fois la relation du lemme précédent, on constate que $\| P \| = \| R \|$. Mais, d'autre part, on a

$$\| R \|^2 \geq |b_d|^2 + |b_0|^2 = M(P)^2 + |a_d a_0|^2 M(P)^{-2} .$$

D'où la conclusion. <

COROLLAIRE (inégalité de Landau). – Si le polynôme P n'est pas réduit à un monôme, on a

$$M(P) < \| P \| .$$

Remarque : Dans l'inégalité du théorème 3 , il y a en fait égalité lorsque le polynôme est de la forme $X^n - 1$.

Note : L'inégalité du corollaire figure déjà dans un article de Landau (*Sur quelques théorèmes de M. Petrovic relatifs aux zéros des fonctions analytiques* ; Bull. Soc. Math. France , t. 33, 1905, p. 251-261). Celle du théorème a été démontrée par Vicente Gonçalves [15], puis indépendamment par l'auteur (*an inequality about factors of polynomials* ; Math. of Computation, t. 28, 1974, pp. 1153-1157).

La démonstration donnée ici est une simplification de celle de ce dernier article .

4. Autres majorations .

Soit z un nombre complexe quelconque, d'après le calcul du lemme ci-dessus, on a

$$\| (X + z) P (X) \|^2 = (1 + | z |^2) \| P \|^2 + 2 \, \mathrm{Re} (za) ,$$

où $\mathrm{Re}(x)$ désigne la partie réelle du nombre complexe x, et a vaut

$$a = \sum_{k=1}^{d} a_k \bar{a}_{k-1} .$$

En choisissant $z = - \bar{a} \, \| P \|^{-2}$, on obtient la relation

$$\| (X - \bar{a} \, \| P \|^{-2}) P (X) \|^2 = \| P \|^2 - | a |^2 \| P \|^{-2} .$$

Par ailleurs, pour tout z, on a $M ((X + z) . P) \geq M (P)$.
En appliquant le corollaire précédent, on obtient l'estimation suivante.

PROPOSITION 4 . – Soit $P = a_d X^d + a_{d-1} X^{d-1} + \ldots + a_0$ un polynôme non constant à coefficients complexes . La mesure de P vérifie l'inégalité

$$M (P)^2 \leq \| P \|^2 - | a_d \bar{a}_{d-1} + a_{d-1} \bar{a}_{d-2} + \ldots + a_1 \bar{a}_0 |^2 \| P \|^{-2} .$$

Note : Cette majoration a été démontrée dans l'article *Entiers algébriques dont les conjugués sont proches du cercle unité* (Séminaire Delange-Pisot-Poitou , 1977-78 , exposé 39, 6 pages) , mais par une méthode beaucoup plus compliquée.

La même démonstration, appliquée à un polynôme de la forme $(X^j + z) P(X)$, fournit la majoration

$$M (P)^2 < \| P \|^2 - \max_{1 \leq j \leq d} \left\{ | \bar{a}_0 a_j + \bar{a}_1 a_{j+1} + \ldots + \bar{a}_{d-j} a_d |^2 \right\} . \| P \|^{-2} ,$$

valable lorsque le polynôme P n'est pas réduit à un monôme.

5. Résultats analytiques .

On démontre, grâce à la formule de Jensen, que la mesure d'un polynôme est aussi donnée par l'expression

$$M(P) = \exp \left\{ \frac{1}{2\pi} \int_0^{2\pi} \mathrm{Log}\,(P(e^{i\theta})\, d\theta \right\} .$$

Un théorème général de Szegö (voir – par exemple – l'ouvrage de H. Dym et H. P. McKean .– *Fourier Series and Integrals* , Acad. Press , London, 1972) , fournit le résultat suivant.

PROPOSITION 5 . – Soit P un polynôme non constant à coefficients complexes. Alors, on a

$$M(P) = \inf \{ \| PQ \| \ ; \ Q \in \mathbf{C}[X] , \text{unitaire} \} .$$

De plus, pour chaque entier n , il est possible de calculer la quantité

$$I_n(P) := \inf \{ \| PQ \| \ ; \ Q \in \mathbf{C}[X] , \text{unitaire, deg } (Q) = n \} .$$

En d'autres termes, on a

$$M(P) \leq I_n(P) \quad \text{pour tout } n \geq 0 ,$$

ce qui résulte directement du théorème 3, et

$$I_n(P) \to M(P) \quad \text{quand } n \to \infty ,$$

qui est la partie difficile du théorème de Szegö .

L'inégalité $M(P) \leq I_0(P)$ n'est autre que le corollaire du théorème 3 , tandis que l'inégalité $M(P) \leq I_1(P)$ correspond à la proposition 4 .

Citons aussi le théorème de Rouché qui est souvent utile pour situer les racines d'un polynôme (voir par exemple M. Marden .– *The geometry of the zeros of a polynomial in a complex variable* , Amer. Math. Soc. , New York, 1949) .

PROPOSITION 6 . – Lorsqu'un polynôme $c_d z^d + c_{d-1} z^{d-1} + \ldots + c_0$ non constant et à coefficients complexes vérifie la condition

$$|c_j| > |c_0| + \ldots + |c_{j-1}| + |c_{j+1}| + \ldots + |c_d| \cdot$$

pour un certain indice j , $0 \leq j \leq d$, alors ce polynôme possède exactement j racines de module < 1 et aucune de module 1 .

6. Une méthode de calcul de $M(P)$.

Cette méthode est adaptée de la méthode classique de Graeffe pour le calcul du plus grand des modules des racines d'un polynôme à coefficients complexes.

A un polynôme P de la forme

$$P(X) = a_d \prod_{j=1}^{d} (X - z_j) ,$$

on associe la suite de polynômes P_m définis par

$$P_m(X) = a_d^{2^m} \cdot \prod_{j=1}^{d} (X - z_j^{2^m}) \qquad , \ m \geq 0 ,$$

et qui peuvent être calculés très facilement de la manière suivante.

On pose $P_0 = P$, et si le polynôme P_m s'écrit sous la forme

$$P_m(X) = F_m(X^2) + X\,G_m(X^2)$$

alors

$$P_{m+1}(X) = F_m^2(X) - X\,G_m^2(X) .$$

Il est clair que ces polynômes vérifient

$$M(P_m) = M(P)^{2^m} .$$

On a d'une part

$$M(P_m) \leq \| P_m \|$$

et d'autre part

$$\| P_m \| \leq 2^d\, M(P_m) .$$

D'où le résultat suivant.

PROPOSITION 7 . – Soit P un polynôme de degré $d \geq 1$, à coefficients complexes et soit P_m, $m \geq 0$, la suite des polynômes qui lui sont associés dans la méthode de Graeffe.

La mesure de P vérifie l'encadrement

$$2^{-d \cdot 2^{-m}} \cdot \| P_m \|^{2^{-m}} \leq M(P) \leq \| P_m \|^{2^{-m}} .$$

(Donc $\| P_m \|^{2^{-m}} \to M(P)$ quand $m \to \infty$.)

Note : Cette méthode a été découverte indépendamment et presque simultanément par plusieurs personnes (D. Boyd, M. Langevin, C. Stewart, M. Mignotte ...) .

La présentation donnée ici, ainsi que l'exemple qui suit sont largement inspirés par l'article de L. Cerlienco, M. Mignotte , F. Piras .– *Computing the measure of a polynomial* , J. of Symb. Comp., vol. 4, n° 1, 1987 , pp. 21-34 .

7. Un exemple d'évaluation de $M(P)$.

Considérons, par exemple, le polynôme

$$P(X) = X^6 + X^5 + 6X^4 - 5X^3 + 3X^2 + 2 .$$

Nous allons lui appliquer quelques unes des estimations données plus haut.

Par le corollaire du théorème 3,

$$M(P) \leq \| P \| = (76)^{1/2} < 8.718 ,$$

et par la proposition 3

$$M(P) \leq (76 - (- 15 - 30 + 6 + 1)^2 / 76)^{1/2} < 7.55 .$$

En appliquant la méthode de Graeffe nous obtenons successivement

$$P_1(X) = X^6 + 11X^5 + 52X^4 + 15X^3 + 33X^2 + 12X + 4 ,$$

$$P_2(X) = X^6 - 17X^5 + 2440X^4 + 2951X^3 + 1145X^2 + 120X + 16,$$

$$P_3(X) = X^6 + 4591X^5 + 6056224X^4 - 3116689X^3 + 680865X^2 + 22240X + 256 .$$

Si nous appliquons la proposition 7 pour $m = 3$, nous obtenons

$$2^{-6/8} \| P_3 \|^{1/8} \leq M(P) \leq \| P_3 \|^{1/8} ,$$

de sorte que

$$4.252 < M(P) < 7.152 .$$

L'application de la proposition 3 au polynôme P_3 donne

$$M(P) < 7.053 .$$

Nous sommes beaucoup plus intéressés par une borne supérieure de $M(P)$ que par une borne inférieure, aussi arrêtons nous le calcul au troisième pas . Néanmoins, nous pouvons facilement raffiner la borne inférieure de $M(P)$; en regardant le troisième coefficient du polynôme P_3 , nous obtenons

$$6056224 \leq \binom{6}{2} M(P_3),$$

de sorte que

$$M(P) \geq (6056224/15)^{1/8} > 5.02 .$$

Il est facile de prouver que le polynôme P n'a aucune racine de valeur absolue ≥ 1 . De plus, le théorème de Rouché montre que P_3 – donc aussi le polynôme P – a exactement deux racines de module > 1 . Ainsi,le polynôme P a deux racines complexes conjuguées de module > 1 (comme P est unitaire cela montre qu'il est irréductible sur $\mathbf{Z}$) .

Ces informations conduisent à une estimation plus précise de $M(P)$. Pour cela nous considérons à nouveau le troisième coefficient $b := 6056224$ du polynôme P_3 . Ce coefficient est la somme de tous les produits de paires distinctes de racines de P_3 , il vérifie donc l'inégalité

$$M^8 - 8M^4 - 6 \leq b \leq M^8 + 8M^4 + 6,$$

où M désigne la mesure du polynôme P .

Ce qui implique

$$(b+22)^{1/2} - 4 < M^4 < (b+10)^{1/2} + 4,$$

et finalement

$$7.0404 < M(P) < 7.0462 .$$

4. Majoration de la taille des facteurs d'un polynôme .

1. Définitions .

Si $R = c_d X^d + \dots + c_0$ est un polynôme à coefficients complexes, on définit sa **longueur** par la formule

$$L(R) = \sum_{k=0}^{d} |c_k| .$$

On définit aussi la **hauteur** de R par

$$H(R) = \max_{0 \le k \le d} |c_k| .$$

Si $z_1, \dots, z_d$ désignent les racines du polynôme R , comptées avec leurs multiplicités, la formule $R = c_d (X - z_1) \dots (X - z_d)$ montre que l'on a les relations

$$c_{d-j} / c_d = (-1)^{d-j} \sum_{i_1 < \dots < i_j} z_{i_1} \dots z_{i_j} \quad \text{pour} \quad j = 1, 2, \dots, d .$$

D'où les majorations

$$|c_j| \le \binom{d}{j} M(R) ,$$

$$H(R) \le \binom{d}{[d/2]} M(R) ,$$

et

$$L(R) \le 2^d M(R) .$$

2. Majoration des facteurs, le cas d'une seule variable .

Le résultat fondamental est le suivant.

THEOREME 4 . – Soit $P \in \mathbf{Z}[X]$ un polynôme non constant qui admet une factorisation de la forme

$$P = Q_1 \dots Q_m Q \quad , \quad Q_1, \dots, Q_m, Q \in \mathbf{Z}[X] \ .$$

Alors, on a la majoration

$$\prod_{j=1}^{m} L(Q_j) \leq 2^D M(P) \ , \text{ où } D = \sum_{j=1}^{m} \deg(Q_j) \ ,$$

et donc

$$\prod_{j=1}^{m} L(Q_j) \leq 2^D \| P \| .$$

> D'après le paragraphe précédent, on a

$$\prod_{j=1}^{m} L(Q_j) \leq 2^D M(Q_1) \dots M(Q_m) \ .$$

La conclusion résulte alors des inégalités

$$M(Q_1) \dots M(Q_m) \leq M(P) \leq \| P \| \ . <$$

3. Définition de la mesure dans le cas de plusieurs variables .

Soit maintenant $P(X_1, \dots, X_n)$ un polynôme en n variables, $n \geq 2$. On définit récursivement la mesure de P par la formule

$$\text{Log } M(P) = \int_0^1 \text{Log} \left\{ M\left(P\left(e^{2i\pi t}, X_2, \dots, X_n \right) \right) \right\} dt \ .$$

D'après la formule du paragraphe 3.5 , cette expression est aussi valable pour $n = 1$. On en déduit, par récurrence sur n , que la mesure possède la propriété de multiplicativité

$$M(P\,Q) = M(P)\,M(Q)\,,$$

déjà remarquée dans le cas d'une variable.

Si le polynôme $P(X_1, \ldots, X_n)$ est de la forme

$$P = \sum a_{j_1 \ldots j_n} X_1^{j_1} \ldots X_n^{j_n} \,,$$

on pose encore

$$\| P \| = \left(\sum | a_{j_1 \ldots j_n} |^2 \right)^{1/2} .$$

Supposons que l'on ait démontré l'inégalité $M(R) \leq \| R \|$ dans le cas des polynômes en $n - 1$ variables, on a alors

$$\operatorname{Log} M(P) \leq \frac{1}{2} \int_0^1 \operatorname{Log} \left(\| P (e^{2i\pi t}, X_2, \ldots, X_n) \|^2 \right) dt \,.$$

L'inégalité de Jensen (voir par exemple G. H. Hardy, J. E. Littlewood, G. Pólya . *Inequalities*, Cambridge, 1934)

$$\int_0^1 \operatorname{Log} | f(t) | \, dt \leq \operatorname{Log} \left(\int_0^1 | f(t) | \, dt \right) .$$

fournit ensuite la majoration

$$M(P)^2 \leq \int_0^1 \| P (e^{2i\pi t}, X_2, \ldots, X_n) \|^2 \, dt \,.$$

Grâce à la formule de Parseval,

$$\int_0^1 \| P (e^{2i\pi t}, X_2, \ldots, X_n) \|^2 dt = \sum_{j_2, \ldots, j_n} \int_0^1 \left| \sum_{j_1} a_{j_1 \ldots j_n} e^{2i\pi j_1 t} \right|^2 dt = \| P \|^2 ,$$

on en déduit encore l'inégalité $M(P) \leq \| P \|$.

4. Majoration des facteurs d'un polynôme, cas de plusieurs variables .

Commençons par majorer les coefficients d'un polynôme en fonction de sa mesure.

PROPOSITION 7 . – Soit $P(X_1, \dots, X_n)$ un polynôme à coefficients complexes qui est de la forme

$$P = \sum a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n} ,$$

alors on a les inégalités

$$| a_{i_1 \dots i_n} | \leq \binom{d_1}{i_1} \dots \binom{d_n}{i_n} M(P) ,$$

où d_j désigne le degré partiel de P par rapport à X_j, pour $j = 1, 2, \dots, n$.

> D'après le § 1, cette inégalité est vraie pour $n = 1$.

Supposons $n \geq 2$. Alors pour $z_2, \dots, z_n$ quelconques on a

$$\Big| \sum_{i_2 \dots i_n} a_{i_1 \dots i_n} z_2^{i_2} \dots z_n^{i_n} \Big| \leq \binom{d_1}{i_1} M(P(X, z_2, \dots, z_n)) .$$

Désignons par P_{i_1} le polynôme en $X_2, \dots, X_n$ correspondant au membre de gauche.

En intégrant le logarithme de chaque membre de l'inégalité ci-dessus sur le domaine complexe $\{ |z_2| = \dots = |z_n| = 1 \}$, on obtient la majoration

$$M(P_{i_1}) \leq \binom{d_1}{i_1} M(P) .$$

En raisonnant par récurrence sur n, on peut écrire

$$| a_{i_1 \dots i_n} | \leq \binom{d_2}{i_2} \dots \binom{d_n}{i_n} M(P_{i_1}) .$$

D'où le résultat. <

En regroupant les résultats des deux paragraphes précédents, on obtient le théorème suivant.

THEOREME 4 bis . – Soit $P(X_1, \dots, X_n)$ un polynôme à coefficients complexes dont le degré par rapport à chacune des variables X_j est égal à d_j.

Alors la longueur de P vérifie

$$L(P) \leq 2^{d_1 + \dots + d_n} M(P) \leq 2^{d_1 + \dots + d_n} \| P \| .$$

De plus, si $P = Q_1 \dots Q_m$, on a

$$L(Q_1) \dots L(Q_m) \leq 2^{d_1 + \dots + d_n} \| P \| .$$

Remarque : Les premières inégalités de ce type semblent être dues à A. O. Gel'fond, *Transcendental and Algebraic Numbers*, Dover, New York, 1960, chap. III, § 4.

5. Un exemple dans le cas d'une variable .

La construction qui suit est destinée à montrer que l'inégalité

$$L(Q) \leq 2^{\deg(Q)} \| P \| ,$$

lorsque P et Q sont des polynômes à coefficients entiers, Q diviseur de P, est à peu de chose près la meilleure possible.

Il s'agit donc de montrer qu'il existe des polynômes P et Q non nuls, à coefficients entiers et tels que P ait de "petits" coefficients et Q une "grande" longueur. Pour ce faire, nous choisissons le polynôme Q ; nous prenons $Q = (X - 1)^n$, de sorte que la longueur de Q vaut $L(Q) = 2^n$.

Maintenant il nous faut trouver un polynôme P (non nul !) à coefficients entiers, qui est un multiple de Q et a de petits coefficients. Nous cherchons P de degré majoré par d (à déterminer) et de hauteur égale à 1 , c'est à dire à coefficients $0 , \pm 1$. La construction d'un tel polynôme, de degré "pas trop grand" – ou plutôt la démonstration du fait qu'un tel polynôme existe – utilisera le principe des tiroirs.

Soient donc n un entier positif fixé et d un entier qui sera précisé plus tard. Le fait que le polynôme P est un multiple de Q équivaut à l'ensemble des conditions

$$P(1) = P'(1) = \ldots = P^{(n-1)}(1) = 0 .$$

Si $P = a_0 + \ldots + a_d X^d$, où les coefficients a_i sont inconnus, ceci équivaut encore au système linéaire

$$\sum_{i=0}^{d} \binom{i}{t} a_i = 0 \quad , \quad t = 0, 1, \ldots , n-1 .$$

Soit E l'ensemble des polynômes de degré au plus d et à coefficients 0 ou 1. L'application f de E dans $\mathbb{N}^n$ définie par

$$(c_0 + \ldots + c_d X^d) \rightarrow \left(\sum_{i=0}^{d} \binom{i}{t} c_i \right)_{0 \le t \le n}$$

envoie l'ensemble E, qui possède 2^{d+1} éléments, sur l'ensemble F = f (E) dont le nombre d'éléments est au plus

$$(d+1)^{1+2+\ldots+n} = (d+1)^{n(n+1)/2} ;$$

en effet, pour t = 0, 1, ..., n - 1, on a

$$c_i \in \{0,1\} \Rightarrow \sum_{i=0}^{d} \binom{i}{t} c_i \le \sum_{i=0}^{d} \binom{i}{t} = \binom{d+1}{t+1} \le (d+1)^{t+1}.$$

Par conséquent, il existe une constante positive c_1 telle que la condition

$$d = [\, c_1 n^2 \operatorname{Log} n \,]$$

implique $2^{d+1} > (d+1)^{n(n+1)/2}$, et donc aussi Card (E) > Card (F).

Donc (principe des tiroirs !), il existe alors deux polynômes distincts de E qui ont la même image par f. Leur différence P est le polynôme cherché.

Nous avons démontré le résultat suivant.

PROPOSITION 9 . – Soit n un entier positif quelconque. Il existe alors des polynômes P et Q à coefficients entiers, non nuls, tels que deg (Q) = n, Q divise P et la longueur de Q vérifie

$$L(Q) \ge c_2 \, 2^n \, (n^2 \operatorname{Log} n)^{-1/2} \, \| P \| ,$$

où c_2 ($= 1 / c_1$) est une constante positive absolue.

Remarque : D'après le théorème 5 ci-dessous, le degré d d'un polynôme P à coefficients entiers, de hauteur 1, et multiple de $(X - 1)^n$ vérifie $d \ge n^2 / (8 n \operatorname{Log} n)$.

5. Sur la répartition des racines d'un polynôme .

Ce paragraphe est consacré à l'étude de la répartition des arguments des racines d'un polynôme à coefficients complexes, ceci en fonction du degré de ce polynôme et de sa longueur. Les résultats reproduits ici expriment de manière précise le fait – intuitivement évident – qu'un polynôme qui a beaucoup de racines dans une direction donnée doit avoir de grands coefficients (exemple typique : $(X-1)^n$) .

Le premier résultat ne concerne que les racines réelles, le second considère toutes les racines.

1. Majoration du nombre de racines réelles .

Le théorème qui suit , à la valeur de la constante près, est dû à E. Schmidt (Preuss. Akad. Wiss. Sitzungsber. , 1932 , p. 321) , il améliore un résultat de A. Bloch et G. Pólya (*On the roots of certain algebraic equations*, Proc. London Math. Soc., t. 33, 1931, p. 102-114). Avec la constante égale à 4, qui est la meilleure possible, ce théorème est dû à I. Schur (Preuss. Akad. Wiss. Sitzungsber. , 1933 , 403-428) .

THEOREME 5 . – Soit

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 \ , \quad \text{où} \quad a_0 a_n \neq 0 \ ,$$

un polynôme à coefficients complexes. On désigne par $L(P)$ la longueur de P , alors le nombre r de racines réelles de P vérifie la majoration

$$r^2 \leq 4n \operatorname{Log} \frac{L(P)}{\sqrt{|a_0 a_n|}} \ .$$

> Nous démontrerons seulement ce résultat avec une constante non explicite. Remarquons d'abord qu'il suffit de prouver que le nombre r' de racines réelles du polynôme P et de valeur absolue ≥ 1 vérifie

$$r' \leq c \sqrt{n \operatorname{Log}\left(L(P) / |a_n| \right)} \; ;$$

en effet l'estimation cherchée est une conséquence immédiate de ce résultat appliqué au polynôme P et à son polynôme réciproque.

Pour tout entier $k \geq 0$, le nombre r' est au plus égal à k augmenté du nombre de racines réelles et de valeur absolue ≥ 1 du polynôme

$$F(X) = n^{-k} \left(X \frac{d}{dX} \right)^k P(X),$$

(raisonner par récurrence sur k, en utilisant le théorème de Rolle) et ce dernier nombre est aussi le nombre de racines réelles de valeur absolue ≤ 1 du polynôme réciproque

$$F^*(X) = X^n F(X^{-1}).$$

On vérifie facilement que

$$F^*(X) = \sum_{j=0}^{n-k} a_{n-j} \left(1 - \frac{j}{n} \right)^k X^j .$$

Soit R un nombre réel > 1, l'inégalité de Jensen implique le nombre total de racines (complexes) du polynôme F^* dans le disque $|z| \leq 1$ est majoré par la quantité

$$\frac{\operatorname{Log} \left\{ \operatorname*{Max}_{|z|=R} |F^*(z)| / |F^*(0)| \right\}}{\operatorname{Log} R} .$$

En choisissant $R = \exp(k/n)$, on obtient

$$\operatorname*{Max}_{|z|=R} |F^*(z)| \leq \sum_{j=0}^{n} |a_{n-j}| \left(1 - \frac{j}{n} \right)^k e^{kj/n} \leq L(P) ,$$

le nombre de zéros de F^* dans le disque $|z| \leq 1$ est donc au plus

$$\frac{n}{k} . \operatorname{Log} \frac{L(P)}{|a_n|} .$$

Ainsi on a

$$r' \leq k + \frac{n}{k} \operatorname{Log} \frac{L(P)}{|a_n|} .$$

D'où le résultat souhaité en prenant

$$k = \left[\left(n \operatorname{Log} \frac{L(P)}{|a_n|} \right)^{1/2} \right] + 1 .$$

Cette démonstration montre que l'on peut prendre $c = 3$ et donc $c = 6$ dans l'énoncé du théorème. <

2. Sur la répartition des arguments des racines d'un polynôme .

Le résultat suivant, dû à Erdös et Turan (*On the distribution of the roots of polynomials* , Ann. Math. , t. 51, 1950, p. 105-119), généralise considérablement le théorème précédent.

THEOREME 6 . – Soit

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 , \quad \text{où} \quad a_0 a_n \neq 0 ,$$

un polynôme à coefficients complexes. On désigne par $L(P)$ la longueur de P. Soient $z_1 = r_1 \exp(i\varphi_1) , \ldots , z_n = r_n \exp(i\varphi_n)$ les racines du polynôme P, avec $r_k \in \mathbf{R}$, avec $r_k > 0$ et $0 \leq \varphi_k < 2\pi$ pour $k = 1, \ldots , n$.

Alors le nombre $N(\alpha, \beta)$ des arguments φ_k compris dans l'intervalle $[\alpha, \beta]$ vérifie l'inégalité

$$\left| N(\alpha,\beta) - \frac{\beta - \alpha}{2\pi} n \right| < 10 \sqrt{n \operatorname{Log} \frac{L(P)}{\sqrt{|a_0 a_n|}}} .$$

6. Séparation des racines d'un polynôme .

1. Notations .

Dans tout ce paragraphe, nous considérons un polynôme P , de degré $d \geq 2$, à coefficients complexes et de racines $\alpha_1, \ldots, \alpha_d$,

$$P(X) = a_d X^d + \ldots + a_0 = a_d (X - \alpha_1) \ldots (X - \alpha_d) , \quad a_d a_0 \neq 0 ,$$

dont les racines sont numérotées de sorte que l'on ait

$$|\alpha_1| \geq \ldots \geq |\alpha_d| .$$

La distance minimale entre deux racines distinctes de P est la quantité

$$\operatorname{sep}(P) := \min_{\alpha_i \neq \alpha_j} |\alpha_i - \alpha_j| ,$$

avec par convention $\operatorname{sep}(P) = \infty$ si P ne possède pas deux racines distinctes.

Le discriminant Δ du polynôme P est donné par la formule

$$\Delta = a_d^{2d-2} \prod_{i<j} (\alpha_i - \alpha_j)^2 ,$$

si les coefficients a_i sont tous des entiers alors Δ est aussi un entier.

2. Une première minoration de sep (P) .

La quantité utile à considérer pour minorer $\operatorname{sep}(P)$ est le discriminant du polynôme. On sait que le discriminant est aussi donné par l'expression

$$\Delta = \pm a_d^{2d-2} \left(\det (\alpha_k^h)_{0<k\leq d,\ 0\leq h<d} \right)^2 .$$

Par une manipulation élémentaire du déterminant D qui figure au membre de droite et l'inégalité de Hadamard, on obtient facilement la majoration

$$|D| \leq \Big(\sum_{h=1}^{d-1} |\alpha_i^h - \alpha_j^h|^2 \Big)^{1/2} \prod_{k \neq i} \big(1 + |\alpha_k|^2 + \ldots + |\alpha_k|^{2d-2} \big)^{1/2}$$

$$< |\alpha_i - \alpha_j| \, d^{(d+2)/2} \max\{1, |\alpha_i|\}^{-1} \, (M(P)/|a_d|)^{d-1} ,$$

pour tout choix d'indices i et j distincts.

En prenant deux indices i et j tels que $|\alpha_i - \alpha_j| = \text{sep}(P)$, on obtient le résultat suivant.

PROPOSITION 10 . – Soit P un polynôme à coefficients complexes dont le discriminant est Δ. Alors la distance minimale entre deux de ses racines distinctes, notée sep (P), vérifie la minoration

$$\text{sep}(P) > d^{-(d+2)/2} \, |\Delta|^{1/2} \, M(P)^{1-d} \geq d^{-(d+2)/2} \, |\Delta|^{1/2} \, \|P\|^{1-d} .$$

Le cas le plus fréquent en pratique est celui des polynômes à coefficients entiers, alors la proposition se simplifie considérablement.

THEOREME 6 . – Soit P un polynôme à coefficients entiers, alors sep (P) vérifie la minoration

$$\text{sep}(P) > d^{-(d+2)/2} \, M(P)^{1-d} \geq d^{-(d+2)/2} \, \|P\|^{1-d} .$$

> Lorsque le polynôme P est sans racine multiple, il suffit de noter que le discriminant de P est alors un entier non nul, et donc que l'on a $|\Delta| \geq 1$.

Par contre, si P admet des racines multiples, il existe un polynôme Q, à coefficients entiers, qui divise P et pour lequel sep (Q) = sep (P). On conclut en appliquant l'estimation du corollaire au polynôme Q et en utilisant les inégalités triviales

$$M(Q) \leq M(P) \quad \text{et} \quad \deg(Q) \leq \deg(P) \; . <$$

3. Autres minorations de la distance entre deux racines .

Reprenons l'étude du discriminant Δ . Soit Ω un ensemble d'indices (i,j) tel que

$$\Omega \subset \{ (i,j) ;\ 1 \le i < j \le d \}$$

et soit

$$\Omega' = \{ j ;\ (i,j) \in \Omega \} .$$

En utilisant l'inégalité triviale

$$|z - z'| \le 2 . \max\{1, |z|\} . \max\{1, |z'|\} ,$$

on obtient l'estimation

$$|\Delta| = \prod_{(i,j) \in \Omega} |\alpha_i - \alpha_j|^2 . \prod_{(i,j) \notin \Omega} |\alpha_i - \alpha_j|^2 . |a_d|^{2d-2}$$

$$\le \prod_{(i,j) \in \Omega} |\alpha_i - \alpha_j|^2 . |a_d|^2 . 2^{d(d-1)/2 - k} . |\alpha_1|^{2(d-1)} . |\alpha_2|^{2(d-2)} .. |\alpha_{d-1}|^{-2} \pi^{-2},$$

où on a posé

$$k = \mathrm{Card}\, \Omega \quad \text{et} \quad \pi = \prod_{j \in \Omega'} |\alpha_j| .$$

D'où le résultat suivant.

PROPOSITION 11 . – Soit Ω un ensemble de k couples d'indices (i, j) qui vérifient les inégalités $1 \le i < j \le d$. On désigne par Ω' l'ensemble des indices j tels que (i, j) appartienne à Ω . On suppose que P est un polynôme à coefficients réels. Avec les notations précédentes relatives au polynôme P et à ses racines, on a la minoration

$$\prod_{(i,j) \in \Omega} |\alpha_i - \alpha_j| \ge |\Delta|^{1/2} . 2^{k - d(d-1)/2} . |a_d|^{1-d} |\alpha_1|^{1-d} |\alpha_2|^{2-d} \ldots |\alpha_{d-1}|^{-1} . \prod_{j \in \Omega'} |\alpha_j| .$$

Cette proposition a les applications suivantes.

COROLLAIRE . – Les notations étant celles de la proposition, soient α_i et α_j deux racines distinctes du polynôme P . On a alors les estimations suivantes :

(i) si α_i est réel tandis que α_j ne l'est pas alors,

$$| \alpha_i - \alpha_j | \geq | \Delta |^{1/6} | \alpha_j | \, (2^{2 - d(d-1)/2} | a_d |^{1-d} | \alpha_1 |^{1-d} \ldots | \alpha_{d-1} |^{-1})^{1/3} ,$$

ce qui implique

$$| \alpha_i - \alpha_j | \geq (| \Delta |^{1/2} \, 2^{2 - d(d-1)/2} \, M(P)^{1-d})^{1/3} ,$$

(ii) si α_i et α_j sont tous deux imaginaires et non conjuguées alors,

$$| \alpha_i - \alpha_j | \geq | \Delta |^{1/4} \, 2^{1 - d(d-1)/4} \, | \alpha_j | \, (| a_d |^{1-d} | \alpha_1 |^{1-d} \ldots | \alpha_{d-1} |^{-1})^{1/2} ,$$

ce qui implique

$$| \alpha_i - \alpha_j | \geq | \Delta |^{1/4} \, 2^{1 - d(d-1)/4} \, M(P)^{-(d-1)/2} .$$

> Dans le cas (i) prendre $\Omega = \{ (i, j) , (i , j') , (j , j') \}$, où j' est l'indice du conjugué de α_j . Puis utiliser la proposition et l'inégalité $| \alpha_j - \alpha_{j'} | \leq 2 | \alpha_i - \alpha_j |$.

Dans le cas (ii) , on choisit $\Omega = \{ (i, j) , (i', j') \}$ où i' et j' sont les indices respectifs des conjugués de α_i et α_j . <

4. Utilisation de propriétés galoisiennes .

Supposons le polynôme P à coefficients entiers et irréductible sur le corps $\mathbf{Q}$ des rationnels. Soit d le degré de P et soit δ le degré du corps $\mathbf{Q} (\alpha_i, \alpha_j)$ au dessus du corps $\mathbf{Q} (\alpha_i)$.

Considérons le nombre

$$q = a_d^{2\delta} \prod_{\sigma} \sigma(\alpha_i - \alpha_j) ,$$

où σ parcourt l'ensemble E des plongements du corps $\mathbf{Q}(\alpha_i, \alpha_j)$ dans $\mathbf{C}$. Ce nombre q est un entier rationnel non nul, donc

$$1 \leq |q| \leq |\alpha_i - \alpha_j| \, |a_d|^{2\delta} \prod_{\sigma \neq Id} |\sigma(\alpha_i) + \sigma(\alpha_j)| ,$$

et donc

$$1 \leq |\alpha_i - \alpha_j| \, |a_d|^{2\delta} \prod_{\sigma \neq Id} \left(2 \max \{ |\sigma(\alpha_i)|, |\sigma(\alpha_j)| \} \right).$$

Rappelons que nous avons supposé $|\alpha_1| \geq |\alpha_2| \geq \ldots \geq |\alpha_n|$. En utilisant en outre le fait que pour chaque α_k la famille $(\sigma(\alpha_k))_{\sigma \in E}$ comporte chaque élément α_h répété exactement δ fois, on obtient

$$1 \leq |\alpha_i - \alpha_j| \, |a_d|^{2\delta} 2^{\delta d - 1} |\alpha_1^{2\delta} \alpha_2^{2\delta} \ldots \alpha_{\delta'}^{2\delta} \alpha_{\delta'+\varepsilon}^{\varepsilon\delta}| ,$$

où on a posé

$$\delta' = [\delta/2] \quad \text{et} \quad \varepsilon = \delta - 2\delta' .$$

D'où la minoration de $|\alpha_i - \alpha_j|$:

$$|\alpha_i - \alpha_j| \geq |a_d|^{-2\delta} 2^{-\delta d + 1} |\alpha_1 \alpha_2 \ldots \alpha_{\delta'}|^{-2\delta} |\alpha_{\delta'+\varepsilon}|^{-\varepsilon\delta} ,$$

qui implique le résultat suivant, moins précis mais plus simple,

$$|\alpha_i - \alpha_j| \geq 2^{-\delta d + 1} M(P)^{-2\delta} .$$

En général, le degré δ est égal à $d - 1$ et l'argument donné ici n'apporte rien de nouveau ; par contre, si δ est assez petit (en fait pour $\delta < (d-1)/2$) l'estimation que nous venons d'obtenir peut être meilleure que les précédentes.

5. Un exemple .

Le but de ce paragraphe est de construire un polynôme unitaire, à coefficients entiers, irréductible sur les rationnels, et qui possède deux racines très rapprochées.

Soit $d \geq 3$ un entier fixé et soit a un certain entier ≥ 10 . On considère le polynôme unitaire suivant $P = X^d - 2(aX - 1)^2$.

Le critère d'irréductibilité d'Eisenstein (voir exercice du chapitre précédent) , appliqué pour le nombre premier 2 , montre que P est irréductible sur les entiers.

Nous allons monter que P possède deux racines proches de $1/a$.

D'abord, $P(a^{-1}) = a^{-d} > 0$, et , si $h = a^{-(d+2)/2}$, on a

$$P(a^{-1} \pm h) < 2a^{-d} - 2a^2h^2 = 0 .$$

Ainsi, le polynôme P possède deux racines dans l'intervalle $]a^{-1} - h , a^{-1} + h[$, ce qui donne $sep(P) < 2h = 2a^{-(d+2)/2}$.

Cette construction implique le résultat suivant.

PROPOSITION 12 . – Pour tout entier $d \geq 3$, il existe une infinité de polynômes P unitaires, à coefficients entiers, irréductibles sur les rationnels et qui vérifient

$$sep(P) < 2^d H(P)^{-(d+2)/4} .$$

Note : Cette construction a été publiée dans l'article *Some Inequalities about univariate Polynomials* , Proceed. 1981 A.C.M. Symp. on Symbolic and Algebraic Computation, Snowbird.

De manière analogue, si a est un entier impair ≥ 11 alors $Q = aX^d - 2(aX - 1)^2$ est un polynôme irréductible sur le corps des rationnels et a deux racines proches de $1/a$.

On a d'une part $Q(a^{-1}) = a^{-d+1} > 0$, et, d'autre part,

$Q(a^{-1} \pm h) < 2a^{-d+1} - 2a^2h^2 = 0$, en posant cette fois $h = a^{-(d+2)/2}$.

Exercices

1. Le but de cet exercice est de démontrer le théorème de Gauss-Lucas : Lorsque f est un polynôme à coefficients complexes, l'ensemble des zéros complexes de sa dérivée f' est contenu dans l'enveloppe convexe de l'ensemble des zéros complexes de f.

1°) Soit P un polynôme à coefficients complexes dont toutes les racines sont dans le demi-plan $\mathrm{Im}(z) \geq 0$, démontrer que les racines de sa dérivée appartiennent à ce même demi-plan.

[Indication : Soient $z_1, \ldots, z_d$ ces racines, avec $\mathrm{Im}(z_j) \geq 0$ pour $1 \leq j \leq d$ alors

$$\frac{P'(z)}{P(z)} = \sum_{j=1}^{d} \frac{1}{z - z_j} = \sum_{j=1}^{d} \frac{\bar{z} - \bar{z}_j}{|z - z_j|^2} \quad \text{et} \quad \mathrm{Im}(z) < 0 \Rightarrow \mathrm{Im}\left(\frac{1}{z - z_j}\right) > 0 ,$$

donc $P'(z) \neq 0$ si z vérifie $\mathrm{Im}(z) < 0$.]

2°) En déduire le théorème de Gauss-Lucas.

2. Soit $P(X) = X^n + a_m X^m + \ldots + a_n$, $m < n$, un polynôme à coefficients complexes et soit A le maximum des modules des a_j, $m \leq j \leq n$.

Démontrer que toute racine complexe z de ce polynôme vérifie

$$|z| < 1 + A^{1/m} .$$

3. Soient P et Q deux polynômes à coefficients complexes, de degrés respectivement égaux à p et q. Démontrer que leur résultant vérifie les majorations

(i) $\quad |\mathrm{Res}(P,Q)| \leq \|P\|^q \, \|Q\|^p$

et

(ii) $\quad |\mathrm{Res}(P,Q)| \leq M(P)^q \, L(Q)^p$.

[Pour (i) : utiliser le déterminant de Sylvester et l'inégalité de Hadamard. Pour (ii) : si $x_1, \ldots, x_p$ sont les racines de P et c son coefficient dominant, on pourra utiliser la relation

$$\mathrm{Res}(P,Q) = \pm c^q \, Q(x_1) \ldots Q(x_p) \, . \,]$$

4. Soit f un polynôme unitaire à coefficients complexes, de mesure M et dont les racines sont $z_1, \ldots, z_n$. Démontrer les inégalités

$$L(f) \leq \prod_{k=1}^{n} (1 + |z_k|) \leq 2^n \, M.$$

5. Soient α et β deux nombres algébriques de degrés respectifs m et n.

Démontrer que les nombres $\alpha\beta$ et $\alpha+\beta$ sont des nombres algébriques de degré au plus mn [utiliser l'exercice 25 du chapitre III] et que leurs mesures vérifient les majorations respectives

$$M(\alpha\beta) \leq M(\alpha)^n \, M(\beta)^m$$

et

$$M(\alpha+\beta) \leq 2^{mn} M(\alpha)^n \, M(\beta)^m.$$

[Pour démontrer la seconde inégalité, on pourra utiliser la propriété suivante :

pour $x, y \in \mathbf{R}_+$, $\max\{1, x+y\} \leq 2 \max\{1, x\} \max\{1, y\}$.]

6. Soit P un polynôme quadratfrei à coefficients entiers, de degré $n \geq 2$. Soit α une racine complexe quelconque de la dérivée de P. Démontrer la minoration

$$| P'(\alpha) | \geq n^{-n} L(P)^{-2n+1} .$$

[On considèrera le discriminant Δ de P. Soient $\alpha_1 = \alpha, \ldots, \alpha_{n-1}$ les racines de P' et soit a le coefficient dominant de P. Montrer que $| \Delta | \geq 1$ et que

$$\prod_{i=2}^{n} | P(\alpha_i) | \leq L(P)^{n-1} M(P')^{n} \leq n^{n} L(P)^{2n-1} .]$$

7. Soit P un polynôme de degré $n \geq 2$ et soit a un nombre complexe. On pose

$$T(x) = P(a) + P'(a)(x - a) .$$

Démontrer que, pour $| x - a | \leq 1/2$, x complexe, on a

$$| P(x) - T(x) | \leq \sum_{i=2}^{n} \binom{n}{i} L(P) \max\{ 1, | a | \}^{n-2} | x - a |^{2} 2^{-i+2} .$$

[Utiliser la formule de Taylor.]

En déduire la majoration

$$| P(x) - T(x) | \leq 4 (3/2)^{n} L(P) \max\{ 1, | a | \}^{n-2} | x - a |^{2} .$$

8. Soit P un polynôme à coefficients complexes et soit α une de ses racines.

On pose $Q(X) = P(X) / (X - \alpha)$. Démontrer que l'on a

$$H(Q) \leq \deg(P) . H(P) .$$

[Utiliser les formules de la division euclidienne.]

9. Soit A l'ensemble des nombres complexes qui sont algébriques.

1°) Montrer que A est dénombrable.

2°) Démontrer que A est un sous corps de $\mathbf{C}$ et qu'il est algébriquement clos.

10. Soient α un nombre algébrique de degré n et Q un polynôme à coefficients entiers qui ne s'annule pas en α.

1°) Démontrer l'inégalité

$$| Q(\alpha) | \geq L(Q)^{-n+1} M(\alpha)^{-q}.$$

2°) En déduire le résultat suivant : si P est un polynôme quadratfrei à coefficients entiers, de degré n, et si α est une racine de P alors on a

$$| P'(\alpha) | \geq (n L(P) M(P))^{-n+1}.$$

3°) On revient à la première question dans le cas particulier où le polynôme Q est de degré un, disons $Q(X) = p X - q$. Démontrer qu'il existe une constante $C = C(\alpha) > 0$ telle que

$$\left| \alpha - \frac{p}{q} \right| \geq C q^{-n} \quad \text{si } p/q \neq \alpha.$$

Cette inégalité est appelée **inégalité de Liouville**.

Un nombre irrationnel α tel que

$$\liminf_{p,\, q \in \mathbf{Z}} \frac{\operatorname{Log} | \alpha - p/q |}{\operatorname{Log} q} = -\infty$$

est appelé un **nombre de Liouville** ; d'après ce qui précède, un tel nombre est donc **transcendant** (c'est à dire non algébrique). Démontrer que le nombre

$$\sum_{n=0}^{\infty} 2^{-n!}$$

est un nombre de Liouville.

Plus généralement, soit (ε_n) une suite d'entiers égaux à 0 ou 1 et qui comporte une infinité de 1, démontrer que le nombre

$$\sum_{n=0}^{\infty} \varepsilon_n \, 2^{-n!}$$

est aussi un nombre de Liouville. En déduire que l'ensemble des nombres de Liouville possède la puissance du continu (comparer avec l'exercice précédent).

11. Soit P un polynôme à coefficients complexes de racines $\alpha_1, \ldots, \alpha_n$. Soit ξ un nombre complexe et soit α une racine de P à distance minimale du point ξ.

Démontrer l'inégalité

$$|\xi - \alpha| \leq \frac{|P(\xi)|\, 2^{n-1}}{|P'(\alpha)|} .$$

Plus généralement, démontrer que l'on a

$$|\xi - \alpha|^r \leq |\alpha - \alpha_1| \ldots |\alpha - \alpha_{r-1}| \; \frac{|P(\xi)|\, 2^{n-r}}{|P'(\alpha)|} ,$$

pour r entier, $1 \leq r \leq n$, et $\alpha \notin \{\alpha_1, \ldots, \alpha_{r-1}\}$.

12. Soit P un polynôme quadratfrei à coefficients entiers, de racines $\alpha_1, \ldots, \alpha_n$ et de coefficient dominant égal à a. On désigne par ρ la valeur maximale des $|\alpha_i|$ pour les indices $i = 1, \ldots, n$, et on pose $s = \mathrm{sep}(P)$ $(= \min \{|\alpha_i - \alpha_j|,\ \alpha_i \neq \alpha_j\})$.

Si α est une racine quelconque de P, démontrer l'encadrement

$$(L(P')\, M(\alpha))^{-n+1} \leq |P'(\alpha)| \leq a\, s\, (2\rho)^{n-2} .$$

13. Soient P et Q deux polynômes du premier degré à coefficients complexes.

Démontrer l'inégalité

$$\frac{\sqrt{5} - 1}{2}\, H(P)\, H(Q) \leq H(PQ) ,$$

et déterminer les cas où l'égalité a lieu.

14. Grâce aux résultats de ce chapitre, démontrer qu'il existe un algorithme qui résoud le problème suivant :

" Etant donnés un polynôme P à coefficients entiers et de racines complexes distinctes $\alpha_1, \ldots, \alpha_m$ et $\varepsilon > 0$ un nombre réel fixé ; déterminer m ainsi que des nombres complexes $z_1, \ldots, z_m$ appartenant à $\mathbf{Q}(i)$ tels que

$$| \alpha_j - z_j | < \varepsilon \quad \text{pour} \quad j = 1, 2, \ldots, m . "$$

[Il suffit essentiellement d'utiliser des bornes sur les racines et une minoration de la distance $sep(P)$.]

De plus, démontrer qu'il existe un algorithme qui détermine le nombre de racines réelles de P et une approximation rationnelle de chacune d'elles à ε près.

[Minorer $| \mathrm{Im}(\alpha_j) |$ lorsque α_j est imaginaire, grâce à la formule $\mathrm{Im}(\alpha_j) = (\alpha_j - \overline{\alpha_j}) / 2$.]

Généraliser les deux résultats précédents au cas des polynômes de $\mathbf{C}[X]$ qui sont à coefficients algébriques.

15. Démontrer qu'il existe un algorithme qui résoud le problème suivant :

" Etant donné un polynôme P à coefficients entiers, déterminer des polynômes à coefficients entiers, irréductibles sur $\mathbf{Z}$, $P_1, \ldots, P_m$ tels que $P = P_1 \ldots P_m$.

[Il suffit d'utiliser des bornes sur les racines. Voir le chapitre VII .]

Généraliser ce résultat, de manière convenable, au cas des polynômes qui sont à coefficients algébriques.

16. Démontrer qu'il existe au plus $n(2H+1)^n$ nombres algébriques de degré au plus n et de hauteur majorée par H (la hauteur d'un nombre algébrique est, par définition, la hauteur de son polynôme minimal sur $\mathbf{Z}$).

En déduire le théorème de Kronecker : un nombre complexe α qui est un entier algébrique sur $\mathbf{Z}$ dont tous les conjugués (y compris lui-même) sont de module au plus un est nécessairement une racine de l'unité. [Démontrer que l'ensemble des puissances de α est fini.]

Montrer que ce théorème de Kronecker implique l'assertion suivante : pour tout entier $d > 1$, il existe une constante $C = C(d) > 1$ telle tout entier algébrique dont tous les conjugués (y compris lui-même) sont de module au plus C est nécessairement une racine de l'unité.

17. 1°) Soit P un polynôme à coefficients complexes et de racines $\alpha_1, \ldots, \alpha_n$ non nulles. On pose $\alpha_j = |\alpha_j| \zeta_j$ pour $j = 1, \ldots, n$. Démontrer l'implication suivante :

$$x \in \mathbf{C} \text{ et } |x| = 1 \Rightarrow \max\{|P(z)| ; |z| = 1\} \cdot \prod_{j=1}^{n} |x - \zeta_j| \leq 2^n |P(x)| .$$

[Démontrer que l'on a $(1 + |\alpha_j|)(x - |\zeta_j|) \leq 2|x - \alpha_j|$ si $|x| = 1$.]

2°) Soit $P \in \mathbf{C}[X_1, \ldots, X_n]$ un polynôme tel que $P = P_1 \ldots P_m$. En utilisant la question précédente, démontrer la majoration

$$\prod_{j=1}^{m} \| P_j \|_2 \leq 2^{D - s/2} \| P \|_2 .$$

[Utiliser aussi plusieurs fois la formule de Parseval, en intégrant par rapport à chacune des variables. La démonstration, qui est attribuée à Gel'fond, figure dans l'ouvrage de K. B. Stolarsky , *Algebraic Numbers and Diophantine Approximation* , M. Dekker, New York, 1974, chap. 4 , § 2 .]

3°) De manière analogue, pour tout entier positif k, démontrer l'inégalité suivante :

$$\| P \|_2^k \leq \| P^k \|_2 \prod_{h=1}^{n} (1 + 2 k d_h) ,$$

où d_h désigne le degré partiel du polynôme P par rapport à la variable X_h.

[Voir à nouveau Stolarsky, chap. 4 , § 2 .]

18. Soit m un entier ≥ 2 et soit $n = m^3$. Considérons le polynôme $P(X) = X^n - 1$, et pour $1 \leq k \leq m$ posons

$$P_k = \prod_{j=1}^{h-1} \Big(X - \exp \Big\{ \frac{2 i \pi (k - 1) h + j}{n} \Big\} \Big) , \text{ avec } h = m^2 .$$

Démontrer que $P = P_1 \ldots P_m$ et qu'il existe des constantes strictement positives c et c' telles l'on ait

$$\prod_{j=1}^{m} \| P_j \| \geq c \, 2^{n - c' n^{1/3} \operatorname{Log} n} .$$

[Ce résultat est aussi dû à Gel'fond, voir Stolarsky, p. 55 ; on peut le comparer à celui donné ici au paragraphe 4.5 .]

19. Soit n un entier fixé, $n \geq 1$. Démontrer qu'il existe des constantes strictement positives $c = c(n)$ et $C = C(n)$ telles que l'on ait l'encadrement

$$c H \leq \operatorname{Max} \{ | P (k) | ; \ k = 0, 1, \ldots , n \} \leq C H .$$

[L'inégalité de droite est triviale. Quant à celle de gauche, on peut la démontrer en utilisant les formules qui fournissent le polynôme de Lagrange, voir l'exercice n° 5 du chapitre III .]

Démontrer un résultat analogue pour le maximum des valeurs des $|P(\zeta)|$ lorsque ζ parcourt l'ensemble E des racines n - ièmes de l'unité.

[Pour démontrer l'inégalité de gauche, on peut cette fois utiliser la formule

$$P(0) = \sum_{\zeta \in E} P(\zeta),$$

et ses analogues qui donnent les différents coefficients du polynôme P .]

20. 1°) Soient $|z_1|, \ldots, |z_n|$ des nombres complexes de module 1 . Démontrer la majoration

$$\prod_{1 \le i < j \le n} |z_i - z_j| \le n^{n/2}.$$

[Utiliser la formule de Vandermonde ainsi que l'inégalité de Hadamard.]

2°) En déduire que si $z_1, \ldots, z_n$ sont des nombres complexes de module ρ (≥ 1) alors on a l'inégalité

$$\prod_{1 \le i < j \le n} |z_i \bar{z}_j - 1| \le \rho^{n(n-1)} n^{n/2}.$$

[Considérer le produit

$$\prod_{1 \le i < j \le n} |z_i \bar{z}_j - \omega_i \bar{\omega}_j| \quad \text{pour} \quad |z_1|, \ldots, |z_n|, |\omega_1|, \ldots, |\omega_n| \le \rho .$$

Grâce au principe du maximum (voir l'exercice qui suit) , démontrer que le maximum de ce produit est atteint pour des valeurs des $z_1, \ldots, z_n$ et $\omega_1, \ldots, \omega_n$ qui sont toutes de module égal à ρ . En déduire que ce produit est majoré par l'expression

$$\prod_{1 \le i < j \le n} |\omega_i \omega_j| \cdot \max \left\{ \prod_{1 \le i < j \le n} |u_i \bar{u}_j - 1| \; ; \; |u_1| = \ldots = |u_n| = 1 \right\}.$$

Puis conclure en utilisant la question précédente.]

21. Principe du maximum (pour les polynômes) .

Soit P un polynôme non constant à coefficients complexes et soit ρ un réel >0 . On désigne par M la borne supérieure de $|P(z)|$ lorsque z parcourt $D = \{ z ; |z| \leq \rho \}$.

1°) Démontrer qu'il existe un point x de ce disque pour lequel $|P(x)| = M$, et que, de plus, un tel point x est nécessairement sur le cercle $|z| = \rho$.

[Pour la seconde assertion, raisonner par l'absurde : si x vérifie $|x| < \rho$, en développant $P(x+y)$ pour y petit, démontrer qu'il existe un point $x+y$ de D tel que l'on ait $|P(x+y)| > |P(x)|$.]

2°) On suppose en outre que P ne s'annule pas sur le disque D . On désigne par m la borne inférieure de $|P(z)|$ lorsque z parcourt D .

Démontrer qu'il existe un point x de ce disque pour lequel $|P(x)| = m$, et que, de plus, un tel point x est nécessairement sur le cercle $|z| = \rho$.

[Même technique que pour 1°) .]

En déduire une autre démonstration du théorème de d'Alembert.

22. On reprend l'exercice 34 du chapitre III , dans lequel on a montré que si P et Q sont deux polynômes à coefficients dans un anneau A alors il existe deux polynômes U et $V \in A[X]$ tels que le résultant R des polynômes P et Q soit de la forme

$$(*) \qquad R = U(X)P(X) + V(X)Q(X) ,$$

avec $\deg(U) < \deg(Q)$ et $\deg(V) < \deg(P)$.

1°) On suppose que P et Q sont à coefficients dans un sous-anneau de $\mathbf{C}$, démontrer que l'on peut trouver des polynômes U et V comme ci-dessus et qui vérifient en outre

$$H(U) \leq \|P\|^{q-1} \|Q\|^{p} \quad \text{et} \quad H(V) \leq \|P\|^{q} \|Q\|^{p-1}.$$

où $p = \deg(P)$ et $q = \deg(Q)$.

2°) En déduire que si P et Q sont à coefficients entiers et n'ont pas de facteur commun alors, pour $z \in \mathbf{C}$, on a

$$|P(z)| + |Q(z)| \geq \left(\max\{p, q\}\right)^{-1} \|P\|^{-q} \|Q\|^{-p}.$$

[Utiliser la relation (*) pour $X = z$ et le fait que l'on a $|R| \geq 1$.]

23. Soit $P \in \mathbf{Z}[X]$ un polynôme de degré n, avec $n > 1$, de mesure M, et soit z un nombre complexe pour lequel on a $|P(z)| \leq 1$.

On veut démontrer qu'il existe un polynôme Q à coefficients entiers, **facteur primaire** (dans un anneau factoriel, un élément est dit **primaire** si c'est une puissance d'un élément irréductible) de P tel que

$$|Q(z)| \leq \left(2(n-1)\right)^{-2} \left\{ \binom{n}{n'} M \right\}^{-2(n-1)},$$

où on a posé $n' = [n/2]$.

Pour cela, on procède ainsi. Soient $P_1, \ldots, P_k$ les facteurs primaires de P, et posons $y_j = |P_j(z)|$ pour $j = 1, 2, \ldots, k$.

Noter qu'il existe un indice h, $1 \leq h \leq k$, tel que

$$y_1 \cdots y_{h-1} \leq y_h \cdots y_k \,, \quad y_1 \cdots y_h \leq y_{h+1} \cdots y_k .$$

En utilisant l'exercice ci-dessus, démontrer l' inégalité

$$\min\{ y_1 \cdots y_{h-1}, y_{h+1} \cdots y_k \} \geq \frac{1}{2(n-1)} \binom{n}{n'}^{-n+1} M^{-n+1}.$$

24. Soient $\alpha_1, .., \alpha_n$ des nombres algébriques de mesures respectives égales à $M_1, ..., M_n$ et de degrés respectifs $d_1, ..., d_n$. Soient $b_1, ..., b_n$ des nombres entiers tels que le nombre

$$\Lambda = b_1 \log \alpha_1 + ... + b_n \log \alpha_n$$

(où $\log \alpha_i$ est une détermination quelconque du logarithme de α_i, $1 \leq i \leq n$) soit non nul, alors démontrer que ce nombre vérifie la minoration

$$| \Lambda | > 2^{-D} \exp (- D (|b_1| h_1 + ... + |b_n| h_n))$$

où D est le degré du corps $\mathbf{Q}(\alpha_1, ..., \alpha_n)$ sur le corps $\mathbf{Q}$ des nombres rationnels et où on a posé $h_i = M_i / d_i$ pour $i = 1, 2, ..., n$.

[On peut supposer $| \Lambda | \leq 1/2$. Alors $\Lambda \notin 2\pi i \mathbf{Z}$ et le nombre $\zeta = \alpha_1^{b_1} ... \alpha_n^{b_n} - 1$ est non nul. Sans perte de généralité, on peut supposer $b_j \geq 0$ pour les indices $1 \leq j \leq r$ et $b_j \leq 0$ pour $r < j \leq n$. Soient $a_1, ..., a_n$ les coefficients dominants du polynôme minimal de $\alpha_1, ..., \alpha_n$ respectivement. Alors, montrer que l'on a

$$a_1^{|b_1| D / d_1} ... a_n^{|b_n| D / d_n} \prod_{\sigma} \sigma (\zeta \alpha_{r+1}^{-b_{r+1}} ... \alpha_n^{-b_n}) \Big| \geq 1$$

où σ parcourt l'ensemble des plongements du corps $\mathbf{Q}(\alpha_1, ..., \alpha_n)$ dans $\mathbf{C}$; ce qui donne $| \zeta | \geq 2^{-D+1} \exp(- D (h_1 | b_1 | + ... + h_n | b_n |))$. Le résultat s'ensuit grâce à l'inégalité $| e^z - 1 | < 2 | z |$ qui est vraie pour $0 < | z | \leq 1/2$.]

CHAPITRE V

Polynômes à coefficients réels

Dans ce chapitre on désigne par $\mathbf{R}$ un corps ordonné tel que le corps $\mathbf{C} = \mathbf{R}[\sqrt{-1}]$ soit algébriquement clos. Par abus de langage, on confondra le corps $\mathbf{R}$ avec le corps des nombres réels, et $\mathbf{C}$ avec le corps des nombres complexes.

1. Polynômes irréductibles sur $\mathbf{R}$.

Nous démontrons ici la proposition 1 du chapitre 4 .

PROPOSITION 1 . – Les polynômes à coefficients dans $\mathbf{R}$ et irréductibles sur $\mathbf{R}$ sont les polynômes du premier degré ou les polynômes du second degré de discriminant strictement négatif.

> Soit P un polynôme unitaire, à coefficients réels et irréductible sur $\mathbf{R}$ (donc non constant) . Si P admet une racine réelle α , alors $X - \alpha$ est un polynôme à coefficients réels qui divise P , donc $P = X - \alpha$. Si P n'a pas de racines réelles alors il admet au moins deux racines imaginaires conjuguées $a + i\,b$ et $a - i\,b$, a et b réels avec $b \neq 0$. Alors le polynôme $(X - a - i\,b)(X - a + i\,b) = X^2 - 2aX + a^2 + b^2$ est à coefficients réels et divise P , il est donc égal à P . Et on a $\mathrm{discr}(P) = -b^2 < 0$.

Inversement, il est clair que tout polynôme à coefficients réels de degré un ou de degré deux et de discriminant négatif est bien irréductible sur $\mathbf{R}$. (En effet, puisque $\mathbf{R}$ est un corps ordonné ses éléments négatifs ne sont pas des carrés : exercice.) <

Complément : Si P est un polynôme quadratique à coefficients réels irréductible sur le corps $\mathbf{R}$, alors $P(x)$ a un signe constant pour x parcourant l'ensemble des nombres réels.

2. Le théorème de Rolle .

1. Le théorème des valeurs intermédiaires .

Ce théorème est une conséquence du résultat suivant.

THEOREME 1 . – Soit f un polynôme à coefficients réels, et soient a et b deux nombres réels, $a < b$, tels que les valeurs $f(a)$ et $f(b)$ soient non nulles. Alors le nombre de racines de f dans l'intervalle $]a, b[$, comptées avec leurs multiplicités, est pair ou impair selon que le produit $f(a)\,f(b)$ est positif ou négatif.

> Ecrivons

$$f(X) = c \prod_{i=1}^{m} (X - \alpha_i) \prod_{j=1}^{n} (X^2 + \beta_j X + \gamma_j) ,$$

où chacun des polynômes de droite est irréductible sur $\mathbf{R}$.

Comme nous venons de le voir, chacun des polynômes quadratiques qui figure dans cette décomposition prend des valeurs positives en tout point réel.

Supposons que $\alpha_1, \ldots, \alpha_k$ soient exactement les racines du polynôme f comprises entre a et b .

On a alors

$$\frac{f(a)}{f(b)} = \frac{a - \alpha_1}{b - \alpha_1} \cdots \frac{a - \alpha_k}{b - \alpha_k} \prod_{i=k+1}^{m} \frac{a - \alpha_i}{b - \alpha_i} \prod_{j=1}^{n} \frac{a^2 + \beta_j a + \gamma_j}{b^2 + \beta_j b + \gamma_j} ,$$

ce qui conduit aussitôt à la relation

$$\text{signe}\,(f(a)\,f(b)) = (-1)^k . <$$

Le théorème des valeurs intermédiaires est le corollaire suivant.

COROLLAIRE . – Soit f un polynôme à coefficients réels, et soient a et b deux nombres réels, $a < b$, tels que l'on ait $f(a)\, f(b) < 0$. Alors le polynôme f possède au moins une racine dans l'intervalle $]\, a, b\, [$.

2. Le théorème de Rolle .

Il s'agit du résultat suivant.

THEOREME 2 (Rolle). – Soit f un polynôme à coefficients réels et soient a et b deux racines réelles successives de f , avec $a < b$. Alors le polynôme dérivé f ' possède un nombre impair de racines dans l'intervalle $]\, a, b\, [$.

> Soit m l'ordre de a , alors le polynôme f s'écrit

$$f(X) = (X - a)^m\, g(X) \text{ , avec } g(a) \neq 0 ,$$

et donc

$$f'(X) = m\,(X - a)^{m-1}\, g(X) + (X - a)^m\, g'(X) .$$

Pour h réel non nul assez petit, on a donc

$$f(a + h) / f'(a + h) \equiv h / m .$$

Ceci implique la relation

$$\text{signe}\,(f(x)\, f'(x)) > 0 \quad \text{pour} \quad x - a > 0 \text{ , assez petit .}$$

De la même manière

$$\text{signe}\,(f(x)\, f'(x)) < 0 \quad \text{pour} \quad x - b < 0 \text{ , assez petit .}$$

Comme f ne s'annule pas sur l'intervalle] a, b [(puisque a et b sont deux racines successives de f) , d'après le corollaire du théorème 1 le polynôme f ne change pas de signe sur l'intervalle] a, b [. Il en résulte que pour tout réel $h > 0$ assez petit on a

$$f'(a+h)\, f'(b-h) < 0 .$$

On conclut grâce au théorème 1 . <

COROLLAIRE 1 . – Soit f un polynôme à coefficients réels qui possède m racines (comptées avec leurs ordres de multiplicité) dans un intervalle fermé de **R** . Alors sa dérivée possède au moins m - 1 racines dans cet intervalle.

> Exercice. <

COROLLAIRE 2 . – (théorème des accroissements finis) Soit f un polynôme à coefficients réels, et soient a et b deux nombres réels, $a < b$. Alors il existe un nombre réel c , $a < c < b$, pour lequel on a

$$f(b) - f(a) = (b-a)\, f'(c) .$$

> Appliquer le théorème à $u(X) = (b-a)(f(X) - f(a)) - (X-a)(f(b) - f(a))$.<

COROLLAIRE 3 . – Soit f un polynôme à coefficients réels, et soient a et b deux nombres réels, avec $a < b$. On suppose que sa dérivée vérifie $f'(x) > 0$ (et respectivement $f'(x) < 0$) pour tout point x appartenant à l'intervalle] a, b [. Alors la fonction f (x) est strictement croissante (respectivement strictement décroissante) sur l'intervalle] a, b [.

> C'est une conséquence immédiate du corollaire 2 . <

3. Estimations des racines réelles .

Les résultats de ce paragraphe sont pour la plupart des variantes des estimations pour les racines complexes qui ont été démontrées au paragraphe 2 du chapitre précédent ; lorsque tel est le cas les nouvelles démonstrations seront assez brèves.

1. La règle de Newton .

PROPOSITION 1 . – Soit f un polynôme à coefficients réels de degré n . Soit L un réel tel que l'on ait $f^{(i)}(L) \geq 0$ pour $i = 0, 1, ..., n$. Alors toute racine réelle x du polynôme f vérifie $x \leq L$.

> Soit $x = L + y$, $y > 0$, un nombre réel. D'après la formule de Taylor, on a

$$f(x) = \sum_{i=0}^{n} \frac{y^i}{i!} f^{(i)}(L) \quad ,$$

donc $f(x)$ est strictement positif pour $x > L$. <

2. La règle de Lagrange et MacLaurin .

PROPOSITION 2 . – Soit f un polynôme à coefficients réels de la forme

$$f(X) = X^n + a_1 X^{n-1} + ... + a_n \quad \text{avec} \quad a_i \geq 0 \quad \text{pour} \quad i = 1, ..., m - 1 ,$$

et soit $A = \max \{ - a_m, ..., - a_n , 0 \}$.

Alors toute racine réelle x du polynôme f vérifie

$$x < 1 + A^{1/m} .$$

> Pour $x \geq 1 + A^{1/m}$, on a $f(x) \geq x^n - A(1 + x + ... + x^{n-m}) > 0$. <

3. Un cas particulier de la règle de Descartes .

PROPOSITION 3 . – Soit f un polynôme à coefficients réels de la forme

$$f(X) = X^n + a_1 X^{n-1} + \ldots + a_m X^{n-m} - a_{m+1} X^{n-m-1} - \ldots - a_n ,$$

avec $a_i \geq 0$ pour $i = 1, \ldots, n$.

Si c est un nombre réel positif ou nul pour lequel on a $f(c) \geq 0$, alors pour tout nombre réel $x > c$ on a l'inégalité $f(x) > 0$, par conséquent toute racine réelle x du polynôme f vérifie $x \leq c$.

> C'est une reformulation du lemme 1 du chapitre précédent. <

4. La règle de Cauchy .

PROPOSITION 4 . – Soient $a_m , a_{m'} , \ldots$ avec $m > m' > \ldots$ les coefficients strictement négatifs d'un polynôme f à coefficients réels,

$$f(X) = X^n + a_1 X^{n-1} + \ldots + a_n ,$$

et soit k le nombre de ses coefficients négatifs.

Alors toute racine réelle x du polynôme f vérifie

$$x \leq \max \{ (k \mid a_m \mid)^{1/m} , (k \mid a_{m'} \mid)^{1/m'} , \ldots \} .$$

> Soit M le maximum figurant dans l'inégalité de l'énoncé. Pour $x > M$, on a

$$f(x) \geq x^n - (a_m x^{n-m} + a_{m'} x^{n-m'} + \ldots) > 0 .$$

(Revoir la démonstration des inégalités (iii) et (iv) du théorème 2 du chapitre 4 .) <

5. Un exemple d'estimation des racines réelles .

Soit le polynôme

$$f(x) = x^6 - 12x^4 - 2x^3 + 37x^2 + 10x - 10 .$$

Ses dérivées successives valent

$$f'(x) = 2(3x^5 - 24x^3 - 3x^2 + 37x + 5),$$

$$f''(x) = 2(15x^4 - 72x^2 - 6x + 37),$$

$$f^{(3)}(x) = 12(10x^3 - 24x - 1),$$

$$f^{(4)}(x) = 72(5x^2 - 4),$$

$$f^{(5)}(x) = 720x \text{ , et } f^{(6)}(x) = 720 .$$

Appliquons les différentes règles que nous avons vues.

Règle de Newton :

Il faut trouver un réel c tel que $f^{(i)}(c)$ soit positif pour $i = 1, 2, ..., 6$. On vérifie facilement que l'on a $f^{(i)}(c) \geq 0$ pour $i = 2, ..., 6$ et $c \geq \sqrt{7}$; l'inégalité $f(\sqrt{8}) > 0$ montre que l'on peut prendre comme borne supérieure des racines la valeur $L = \sqrt{8}$.

Règle de Lagrange et MacLaurin :

On trouve instantanément la borne $1 + \sqrt{12}$.

Règle de Cauchy :

Avec les notations de la proposition 4 , on a ici $k = 3$ et on trouve la borne

$$\max \{ (3 \times 12)^{1/2}, (3 \times 2)^{1/3}, (3 \times 10)^{1/6} \} = 6 .$$

Règle de Laguerre (voir exercice 12) :

Elle fournit la borne $\sqrt{13}$.

4. Sur le nombre de zéros d'un polynôme dans un intervalle .

1. La règle de Sturm .

Avant d'énoncer le théorème de Sturm, nous avons besoin d'introduire deux définitions.

Soit f un polynôme et soient a et b deux réels, $a < b$. On dit qu'une suite de polynômes $f_0 = f , f_1 , \dots , f_s$ est une **suite de Sturm** pour f sur $[a, b]$ lorsque les conditions suivantes sont vérifiées :

(i) $f(a) f(b) \neq 0$,

(ii) la fonction polynôme f_s ne s'annule pas sur $[a, b]$,

(iii) si c est un réel tel que $a < c < b$ et $f_j(c) = 0$ pour un indice j vérifiant $0 < j < s$, alors on a $f_{j-1}(c) f_{j+1}(c) < 0$,

(iv) si c est un réel tel que $a < c < b$ et $f(c) = 0$, alors le polynôme produit $f(x) f_1(x)$ est du signe de $x - c$ au voisinage du point c .

A une telle suite et à un point x de l'intervalle $] a , b [$, on associe le " nombre de variations de signe de la suite au point x " , nombre noté $V (f_0, \dots, f_s ; x)$, ou plus simplement $V(x)$, et défini par la formule

$V(x) = \text{Card} \{ (i,j) ; 0 \leq i < j \leq s ; f_i(x) f_j(x) < 0 \text{ et } f_k(x) = 0 \text{ si } i < k < j \}$.

Nous pouvons maintenant énoncer le théorème de Sturm.

THEOREME 3. – (Sturm) Soit f un polynôme à coefficients réels et soient a et b deux nombres réels, $a < b$. Si $f_0, f_1, \ldots, f_s$ est une suite de Sturm pour f sur l'intervalle [a, b] . Alors le nombre de zéros distincts de f sur l'intervalle [a, b] est égal à la quantité V (a) - V (b) .

> Désignons par I l'intervalle [a, b] . On remarque d'abord que V(x) est constant sur tout intervalle contenu dans I et sur lequel aucune des fonctions f_i ne s'annule. Comme les fonctions f_i n'ont qu'un nombre fini de zéros, il suffit de montrer que la quantité V (x) possède les propriétés suivantes :

(α) V (x) diminue de 1 lorsque x traverse une racine c de f , $c \in I$,

(β) V (x) ne change pas lorsque x traverse un point c de I tel que f (c) soit non nul et $f_i(c) = 0$ pour au moins un indice $i \geq 1$.

Supposons d'abord que c soit une racine de f . D'après (iii), on a $f_1(c) \neq 0$. Tandis que, d'après (iv), pour $h \neq 0$ assez petit, on a

$$\text{signe}\,(f(c+h)\,f_1(c+h)) = \text{signe}\,(h)\,.$$

Ce qui montre qu'il y a un changement de signe en moins au début de la suite des $f_i(x)$ (en fait entre les indices 0 et 1) lorsque x passe de la valeur $c - \varepsilon$ à $c + \varepsilon$, pour tout nombre $\varepsilon > 0$ assez petit .

Supposons maintenant que c soit une racine de f_i avec $i \geq 1$, $c \in I$. D'après (ii) , on a $i < s$. D'après (iii) , on a $f_{i-1}(c)\, f_{i+1}(c) < 0$. Donc, il n'y a pas de variation du nombre de changements de signe des $f_j(x)$, où $i - 1 \leq j \leq i + 1$, lorsque le point x traverse c (en fait on a $f_{i-1}(x)\, f_{i+1}(x) < 0$ dans un voisinage de c) .

Les informations ci-dessus impliquent les propriétés (α) et (β) , d'où le théorème. <

Le résultat qui suit fournit un moyen de construire une suite de Sturm associée à un polynôme et donc d'appliquer le théorème précédent.

PROPOSITION 6 . – (Sturm) Soit f un polynôme à coefficients réels et soient a et b deux réels quelconques, a < b . Considérons la suite $f_0, f_1, \dots, f_{s+1}$ de polynômes définie par

$$f_0 = f \ , \ f_1 = f' \ , \ f_2 = - f \bmod f' \ , \ \dots, \ f_{i+1} = - f_{i-1} \bmod f_i \ , \ \dots, \ f_{s+1} = 0 \ ,$$

c'est -à -dire, aux signes près, la suite obtenue en calculant le p.g.c.d. de f et f ' par l'algorithme d'Euclide. Alors la suite de polynômes $g_i = f_i / f_s$, $0 \le i \le s$, est une suite de Sturm pour g_0 sur l'intervalle [a, b] , pourvu que l'on ait $g_0(a)\, g_0(b) \neq 0$.

> Il s'agit de vérifier les propriétés (i) à (iv) ci-dessus.

(i) : Vraie lorsque $g_0(a)\, g_0(b) \neq 0$.

(ii) : Résulte du fait que $g_s = 1$.

(iii) : Par construction, on a des relations de la forme

$$g_{j-1}(X) = q_j(X)\, g_j(X) - g_{j+1}(X) \quad \text{pour} \quad 0 < j < s \ .$$

Donc $g_{j-1}(c)\, g_{j+1}(c) < 0$ quand $g_j(c) = 0$ (c ne peut être ni racine de g_{j-1} ni racine de g_{j+1} , sinon c serait racine de $g_s = 1$) .

(iv) : On a $g_1(c) \neq 0$, et on conclut grâce au corollaire 2 du théorème de Rolle. <

COROLLAIRE . – Soit f un polynôme à coefficients réels et soient a et b deux réels quelconques, a < b . Considérons la suite $f_0, f_1, \dots, f_{s+1}$ de polynômes définie par

$$f_0 = f \ , \ f_1 = f' \ , \ f_2 = - f \bmod f' \ , \ \dots, \ f_{i+1} = - f_{i-1} \bmod f_i \ , \ \dots, \ f_{s+1} = 0 \ .$$

Alors, si f (a) et f (b) sont non nuls, le nombre de zéros distincts de f sur l'intervalle [a, b] est égal à la différence

$$V (f_0, f_1, \dots, f_s ; a) - V (f_0, f_1, \dots, f_s ; b) .$$

> Exercice facile. <

2. Le théorème de Budan - Fourier .

Ce résultat est moins précis, mais plus facile à utiliser que le théorème de Sturm. Nous verrons sur un exemple qu'il suffit quelquefois pour séparer les racines réelles d'un polynôme.

THEOREME 3 . – (Budan - Fourier) Soit f un polynôme à coefficients réels et soient a et b , $a < b$, deux nombres réels tels que $f(a) f(b) \neq 0$. On désigne par $v(x)$ le nombre de changements de signe dans la suite $f(x), f'(x), f''(x), ..., f^{(n)}(x)$.

Alors le nombre de zéros de f dans l'intervalle $[a, b]$, comptés avec leur ordres de multiplicité, est de la forme

$$v(a) - v(b) - 2m \ , \quad \text{avec} \quad m \in N .$$

> Désignons par I l'intervalle $[a, b]$. On remarque d'abord que la fonction $v(x)$ est constante sur tout intervalle contenu dans I et sur lequel aucune des fonctions $f^{(i)}$ ne s'annule. Comme les fonctions $f^{(i)}$ n'ont qu'un nombre fini de zéros, il suffit de montrer que la quantité $v(x)$ possède les propriétés suivantes :

(i) $v(x)$ diminue de $k + 2m'$, $m' \in N$, lorsque x traverse une racine c d'ordre k de f , $c \in I$,

(ii) $v(x)$ diminue de $2m''$, $m'' \in N$, lorsque x traverse un point c de I tel que $f(c)$ soit non nul et $f^{(i)}(c) = 0$ pour au moins un indice $i \geq 1$.

Supposons d'abord que c soit une racine d'ordre k de f . Alors $f^{(k)}(c)$ est non nul et, d'après la formule de Taylor, on a

$$f^{(i)}(x) \cong \frac{k\,(k-1)\,\ldots\,(k-i+1)}{k!}\,(x-c)^{k-i}\,f^{(k)}(c) \quad , \quad \text{pour} \quad 0 \le i \le k ,$$

pour x assez proche de c , $x \neq c$. Ce qui montre qu'il y a k changements de signe en moins au début de la suite des $f^{(i)}(x)$ (en fait entre les indices entre 0 et k) lorsque le point x passe de la valeur $c-\varepsilon$ à $c+\varepsilon$, pour $\varepsilon > 0$ assez petit .

Supposons maintenant que c soit une racine d'ordre k de $f^{(i)}$ avec $i \geq 1$, $c \in I$, et $f^{(i-1)}(c) \neq 0$. On applique à nouveau la formule de Taylor au point c , mais cette fois à la fonction $f^{(i)}$. Distinguons selon que k est pair ou impair.

Lorsque k est pair, $f^{(i)}(x)$ ne change pas de signe au voisinage de c ($x \neq c$) . On constate que la suite $f^{(i)}(x)$, ..., $f^{(i+k)}(x)$ comporte k changements de signe en moins lorsque le point x passe de la valeur $c-\varepsilon$ à $c+\varepsilon$, pour $\varepsilon > 0$ assez petit .

Lorsque k est impair, $f^{(i)}(x)$ change de signe au voisinage de c ($x \neq c$) . On voit que la suite $f^{(i-1)}(x)$, $f^{(i)}(x)$, ..., $f^{(i+k)}(x)$ comporte $k-1$, ou $k+1$, changements de signe en moins lorsque le point x passe de la valeur $c-\varepsilon$ à $c+\varepsilon$, pour $\varepsilon > 0$ assez petit , selon le signe de $f^{(i-1)}(c)$ (qui ne change pas dans un petit voisinage du point c) .

Les informations que nous venons d'obtenir impliquent les propriétés (i) et (ii) , d'où le théorème . <

3. La règle de Descartes .

THEOREME 4 . – (Descartes) Soit $f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$ un polynôme à coefficients réels, avec $a_n a_0 \neq 0$. Soit v le nombre de changements de signes dans la suite $(a_0 , \ldots, a_n)$ de ses coefficients et soit r le nombre de ses racines réelles positives, comptées avec leurs ordres de multiplicité, alors il existe un certain entier $m \in N$ tel que

$$r = v - 2 m .$$

> Soit M une borne des zéros positifs de f et soit L un nombre réel $\geq M$.

En zéro, on a $f^{(i)}(0) = i! a_i$. Tandis que, pour L assez grand , tous les $f^{(i)}(L)$ sont du signe de a_n . La conclusion résulte donc du théorème de Budan - Fourier appliqué dans l'intervalle $] 0 , L [$. <

Complément . – Avec les notations du théorème, lorsque v est égal à 0 ou à 1 , le nombre de racines > 0 du polynôme est égal à v .

> Ceci résulte des deux propriétés suivantes : $r = v - 2 m$ et $r \geq 0$. Remarquons que le cas $v = 1$ a déjà été démontré deux fois : proposition 3 ci-dessus et lemme 1 du chapitre précédent. <

Exemple : Considérons le polynôme $f (x) = x^6 - x^4 + 2 x^2 - 3 x - 1$. Pour ce polynôme, on a $v = 3$. Le nombre de racines > 0 de f est donc égal à 1 ou 3 . Il est visible que l'on a $f (x) < 0$ si $0 \leq x \leq 1$. Posons $x = 1 + y$, alors, en appliquant par exemple la formule de Taylor, on obtient la formule

$$f (1 + y) = - 2 + 3 y + 11 y^2 + 16 y^3 + 14 y^4 + 6 y^5 + y^6 ,$$

ce qui montre que f possède un seule racine réelle positive .

COROLLAIRE . – Un polynôme à coefficients réels qui comporte m coefficients non nuls possède au plus m - 1 racines réelles > 0 et aussi au plus m - 1 racines strictement négatives (même en comptant les ordres de multiplicité) .

> En effet, une suite qui comporte exactement m termes non nuls ne possède pas plus de m - 1 changements de signes. <

4. Cas des polynômes dont toutes les racines sont réelles .

On conserve les notations du théorème 4 . Soit v ' le nombre de variations de signes de la liste des coefficients du polynôme $f(-x)$, c'est à dire le nombre de variations de signes de la liste $a_0 , - a_1 , ..., (-1)^n a_n$.

Notons d'abord que si aucun des a_i n'est nul alors on a $v + v' = n$. En effet, pour chacune des deux listes il y a n comparaisons à effectuer et, lorsqu'il y a un changement de signe à une certaine position dans la première liste, il n'y en a pas à cette position dans la seconde liste, et vice versa.

Nous allons montrer que l'on a toujours $v + v' \leq n$. Pour éviter des notations un peu lourdes, nous allons raisonner par récurrence sur le nombre k de coefficients nuls de la suite $a_0 , a_1 , ..., a_n$.

Le cas où ce nombre est nul vient d'être traité. Supposons $1 \leq k \leq n$ et le résultat vrai pour k - 1 . Soit i le plus petit indice tel que a_i soit nul. Considérons alors la liste $a_0 , a_1 , ..., a_{i-1} , a_{i-1} , a_{i+1} , ..., a_n$: il est clair, d'une part, qu'elle comporte aussi v changements de signes et, d'autre part, que le nombre v " de changements de signes de la suite $a_0 , - a_1 , ..., (-1)^{i-1} a_{i-1} , (-1)^i a_{i-1} , (-1)^{i+1} a_{i+1} , ..., (-1)^n a_n$ est au moins égal à v ' . Par hypothèse de récurrence, on a $v + v'' \leq n$. D'où l'inégalité cherchée.

De ce qui précède, joint à la règle de Descartes, on déduit le résultat suivant.

PROPOSITION 7 . – Soit $f(x)$ un polynôme à coefficients réels, on désigne par v le nombre de changements de signes de la liste de ses coefficients et par v' celui de la liste des coefficients du polynôme $f(-x)$. Alors, si f a toutes ses racines réelles et non nulles, le nombre r de racines positives de f et le nombre r' de ses racines négatives vérifient

$$r = v \quad \text{et} \quad r' = v' .$$

> En appliquant la règle de Descartes aux polynômes $f(x)$ et $f(-x)$, on obtient les inégalités

$$r \leq v \quad \text{et} \quad r' \leq v' .$$

Par ailleurs, au cours de la démonstration ci-dessus, on a vu que

$$v + v' \leq \deg(f) .$$

Comme f a toutes ses racines réelles non nulles, on a aussi

$$r + r' = \deg(f) .$$

Il en résulte que les inégalités précédentes sont en fait des égalités.

D'où le résultat. <

5. Un exemple détaillé .

Considérons le polynôme

$$f(x) = x^5 - 5x^4 + 15x^3 - x^2 + 3x - 7 .$$

On cherche à déterminer le nombre de racines réelles de f et à les séparer. Dans ce but, calculons d'abord une suite de Sturm de ce polynôme. On a successivement

$$f_0 = f(x) = x^5 - 5x^4 + 15x^3 - x^2 + 3x - 7 ,$$

$$f_1(x) = f'(x) = 5x^4 - 20x^3 + 45x^2 - 2x + 3 ,$$

$$5 f_0 = (x - 1) f_1 + (10x^3 + 42x^2 + 10x - 32) ,$$

on peut donc prendre

$$f_2 = -5x^3 - 21x^2 - 5x + 16 ,$$

puis

$$5 f_1 = (-5x + 41) f_2 + (1061x^2 + 275x - 641) ,$$

d'où

$$f_3 = -1061x^2 - 275x + 641 .$$

On remarque déjà que le polynôme f_3 a toutes ses racines comprises entre -1 et +1 .

Considérons d'abord l'intervalle $[1, +\infty[$. Pour $x \geq 1$, on a

$$f(x) = x^5 - 5x^4 + 15x^3 - x^2 + 3x - 7 > x^5 - 5x^4 ,$$

donc f n'a pas de racine réelle ≥ 5 . De plus, on a

$$V(f_0, f_1, f_2, f_3 ; 1) = V(6, 29, -15, -695) = 1 ,$$

tandis que, pour b assez grand, la suite des signes des $f_i(b)$ est $(+, +, -, -)$ et donc

$$V(f_0, f_1, f_2, f_3 ; b) = 1 .$$

Ce qui montre que le polynôme f n'a pas de racine dans l'intervalle $[1, +\infty[$.

Remarquons d'ailleurs que l'on a

$$f(x) = x^5 - 5x^4 + 15x^3 - x^2 + 3x - 7,$$

$$f'(x) = 5x^4 - 20x^3 + 45x^2 - 2x + 3,$$

$$f''(x) = 2(10x^3 - 30x^2 + 45x - 1),$$

$$f^{(3)}(x) = 30(2x^2 - 4x + 3),$$

$$f^{(4)}(x) = 120(x - 1), \quad f^{(5)}(x) = 120,$$

et donc

$$f^{(i)}(1) \geq 0 \quad \text{pour} \quad i = 0, 1, ..., 5,$$

ce qui implique – grâce à la règle de Newton – que le polynôme n'a pas de racine dans l'intervalle $[1, +\infty[$.

Considérons maintenant l'intervalle $[0, +1]$. Pour x dans cet intervalle, on a

$$f'(x) = (45x^2 - 20x^3 + 5x^4) + (3 - 2x) > 0,$$

donc f est strictement croissante sur cet intervalle, et comme $f(0) = -7$ et $f(1) = 6$, le polynôme f possède exactement une racine dans l'intervalle $]0, +1[$. On peut remarquer que la règle de Budan - Fourier montre que f possède une ou trois racines dans l'intervalle $]0, +1[$.

Considérons enfin l'intervalle $]-\infty, 0]$. Tous les coefficients du polynôme $f(-x)$ sont négatifs, donc f n'a pas de zéro dans cet intervalle (cas trivial de la règle de Descartes).

On peut facilement préciser la position de la racine réelle ξ de f. On note par exemple que

$$f\left(\frac{1}{\sqrt{2}}\right) = \frac{1}{4\sqrt{2}} - \frac{5}{4} + \frac{15}{2\sqrt{2}} - \frac{1}{2} + \frac{3}{\sqrt{2}} - 7 = \frac{43}{4\sqrt{2}} - \frac{35}{4} < 0 ,$$

ce qui montre que ξ est compris entre $1/\sqrt{2}$ et 1.

Comme $f'(1) = 31$, la **méthode de Newton**, appliquée avec $x_0 = 1$ comme point de départ, fournit l'approximation

$$x_1 = x_0 - f(x_0)/f'(x_0) = 1 - 6/31 = 0{,}806 ...$$

En réappliquant deux fois la méthode de Newton avec $0{,}8$ comme nouveau point de départ, on trouve

$$\xi \equiv 0{,}766 .$$

La mesure de f vérifie

$$M(f) < (1 + 5^2 + 15^2 + 1 + 3^2 + 7^2)^{1/2} = 310^{1/2} < 17{,}61 ,$$

donc les racines complexes de f ont un module maximal $< 4{,}2$; en effet, si z est une racine imaginaire de f, alors son conjugué complexe est aussi une racine de f et on a

$$M(f) \geq |z|^2 ,$$

donc ici

$$|z| < \sqrt{17{,}61} < 4{,}2 .$$

6. Le théorème de Vincent .

THEOREME 5 . – (Vincent) Soit f un polynôme à coefficients réels sans racines multiples et soit une suite arbitraire $a_1, ..., a_k, ...$ d'entiers naturels > 0 . En transformant le polynôme $f(x)$ par les changements de variables successifs

$$x_i = a_i + \frac{1}{x_{i+1}} \quad , \quad i = 0, 1, ... , \quad (\text{avec } x_0 = x) ,$$

on aboutit, au bout d'un nombre fini d'étapes, à un polynôme dont la liste des coefficients ne présente qu'un changement de signe au plus.

> On considère la fraction continue définie par la suite $a_1, ..., a_k, ...$ Soit α la limite de cette fraction continue ; deux cas se présentent :

(i) α n'est pas une racine de f ,

(ii) on a $f(\alpha) = 0$.

Désignons par p_k / q_k la k-ième réduite du développement en fraction continue défini par la suite $a_1, ..., a_k, ...$ Au bout de m changements de variables comme dans l'énoncé, si la nouvelle variable est notée y , on a

$$x = \frac{p_m y + p_{m-1}}{q_m y + q_{m-1}} \quad , \text{ ou encore } \quad y = - \frac{p_{m-1} - q_{m-1} x}{p_m - q_m x} .$$

On sait que, pour tout k positif, on a

$$\left| \alpha - \frac{p_k}{q_k} \right| \leq \frac{1}{q_{k+1} q_k} < \frac{1}{q_k^2} ,$$

d'où l'estimation

$$y = - \frac{q_{m-1} (\alpha - x) + O(1/q_m)}{q_m (\alpha - x) + O(1/q_m)} .$$

[Comme référence sur les fractions continues, voir Hardy and Wright, chap.6 .]

Effectuons encore le changement de variable

$$y = \frac{q_{m-1}}{q_m} u ,$$

et soient $F(y)$ le polynôme transformé de f par le changement de variable $x \to y$ et respectivement $G(u)$ le transformé de F par le changement de variable $y \to u$. Alors, les polynômes F et G ont le même nombre de changements de signes dans la liste de leurs coefficients.

Il résulte aussitôt de l'estimation précédente de y que les racines de G transformées des racines de f autres que α sont arbitrairement proches de -1 lorsque m est assez grand.

Par conséquent, dans le cas (i), le polynôme G a des coefficients tous de même signe et le théorème de Vincent est démontré.

Considérons maintenant le second cas. Soit ω la racine de G associée à α, on a

$$\omega = - \frac{\frac{p_{m-1}}{q_{m-1}} - \alpha}{\frac{p_m}{q_m} - \alpha} , \quad \text{donc} \quad \omega > 1 .$$

A une constante multiplicative près, le polynôme G est de la forme

$$G(u) = (u - \omega)(u + 1 + \varepsilon_1) \dots (u + 1 + \varepsilon_{n-1}) ,$$

où les ε_i sont arbitrairement petits pour m assez grand, n désignant le degré de f.

D'après le lemme 1 ci-dessous, la suite quotients des coefficients consécutifs du polynôme $(u + 1)^{n-1}$ est décroissante ; un calcul direct montre en fait qu'elle est strictement décroissante. Il en est donc de même, dès que m est assez grand, pour le polynôme

$$(u + 1 + \varepsilon_1) \dots (u + 1 + \varepsilon_{n-1}) .$$

Enfin, une nouvelle application du lemme 1 montre que la liste des coefficients du polynôme G possède exactement un changement de signe et le théorème est démontré.<

LEMME 1 . – Soit

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$$

un polynôme à coefficients réels strictement positifs.

Les deux propriétés suivantes ont lieu

1°) Si toutes les racines de f sont réelles, alors la suite des quotients a_{i+1} / a_i est décroissante.

2°) Si la suite des quotients a_{i+1} / a_i est décroissante, alors pour tout réel $\xi > 0$ la liste des coefficients du polynôme $(x - \xi) f(x)$ possède exactement un changement de signe.

> Supposons d'abord que f ait toutes ses racines réelles ; puisque f est à coefficients positifs, ces racines sont négatives. Soit ξ un nombre réel positif quelconque. Comme le polynôme $(x - \xi) f(x)$ a toutes ses racines réelles dont une seule positive, la proposition 7 montre que la liste de ses coefficients possède exactement un changement de signe. Autrement dit, pour tout $\xi > 0$, il existe un indice j tel que

$$i < j \Rightarrow a_{i+1} - \xi a_i \geq 0 \quad \text{et} \quad i > j \Rightarrow a_{i+1} - \xi a_i \leq 0 \quad (\text{où } a_{-1} = 0),$$

ce qui montre bien que la suite des quotients a_{i+1} / a_i est décroissante. D'où la première assertion.

Supposons maintenant que la suite des quotients a_{i+1} / a_i soit décroissante. Alors, pour tout nombre réel $\xi > 0$, il existe un indice j tel que

$$i < j \Rightarrow a_{i+1} - \xi a_i \geq 0 \quad \text{et} \quad i > j \Rightarrow a_{i+1} - \xi a_i \leq 0 \quad (\text{où } a_{-1} = 0),$$

ce qui montre bien que la suite des coefficients du polynôme $(x - \xi) f(x)$ possède exactement un changement de signe. Ce qui démontre la seconde propriété. <

Vincent propose la méthode suivante pour la séparation des racines réelles d'un polynôme f à coefficients réels et sans racines multiples.

1°) On détermine deux entiers positifs L et L' tels que toutes les racines réelles de f soient comprises entre $-L'$ et L.

Pour simplifier les notations, on se limitera à la séparation des racines positives. En considérant le polynôme $f(-x)$, on peut d'ailleurs toujours se limiter à la recherche des racines réelles positives.

2°) Soient alors deux entiers a et a' avec $0 \leq a < a' \leq L$. On sait, d'après le théorème de Budan - Fourier, que le polynôme f ne peut avoir une racine dans l'intervalle $[a, a']$ que si l'on a $v(a) > v(a')$ où – rappelons-le – la notation $v(x)$ désigne le nombre de changements de signes dans la suite $f(x), f'(x), f''(x), \ldots, f^{(n)}(x)$, et où n est le degré du polynôme f.

Pour simplifier, on dira que $v(x)$ est la variation de f au point x et, lorsqu'il sera utile de préciser quel est le polynôme considéré, cette variation sera notée $v(f ; x)$.

Si on suppose que $a' = a + 1$, et que l'on a $v(a) > v(a')$, on pose

$$x = a + \frac{1}{x_1} ,$$

d'où un polynôme f_1 en x_1 tel que les racines de f appartenant à l'intervalle $[a, a+1]$ correspondent aux racines > 1 de f_1. Si r est le nombre de ces racines, on a donc

$$r \leq v(f_1 ; 1) .$$

On cherche ensuite à séparer les racines > 1 du polynôme f_1, ceci en appliquant le même procédé ... et ainsi de suite.

De cette manière, on trouve le début du développement en fraction continue de chacune des racines réelles de f. Et, grâce au théorème de Vincent, on peut supposer que tous ces calculs ont été poussés jusqu'à ce que, pour chacune des racines réelles du polynôme f, on soit parvenu à un polynôme transformé qui possède exactement une seule variation de signe.

3°) Pour une certaine racine réelle de f, désignons par g le dernier polynôme transformé de f calculé et par y la variable de g.

On suppose que la variation de g est égale à 1 et que l'on a trouvé une valeur approchée γ telle que l'unique racine > 0 de g soit égale à $\gamma + h$, avec $0 < h \leq \varepsilon < 1$. D'après le théorème de Budan-Fourier, on a $v(g ; \gamma) = 1$.

On supposera aussi, ce qui est toujours possible, que le coefficient dominant de g est positif.

On impose enfin la condition supplémentaire

$$g'(\gamma) > 0 ,$$

qui est vérifiée pour h assez petit puisque l'on a

$$\xi \cong \gamma - g(\gamma) / g'(\gamma) \quad \text{avec} \quad \gamma < \xi \quad \text{et donc} \quad g(\gamma) < 0 .$$

Les conditions $v(g ; \gamma) = 1$ et $g'(\gamma) > 0$ impliquent

$$g^{(i)}(\gamma) \geq 0 \quad \text{pour} \quad i = 1, 2, \ldots, n ,$$

et le développement de Taylor de $g(\gamma+h)$ montre que l'on a

$$\xi < \gamma - g(\gamma) / g'(\gamma) .$$

Enfin, un calcul d'erreur classique conduit ici à la minoration

$$\xi > \gamma - \frac{g(\gamma)}{g'(\gamma)} - \frac{1}{2} \frac{g''(\gamma+\varepsilon)}{g'(\gamma)} \varepsilon^2 .$$

Ce qui permet de trouver rapidement une bonne valeur approchée pour ξ et par conséquent, grâce au calcul de x en fonction de y effectué au cours de la preuve du théorème de Vincent, une bonne valeur approchée pour la racine α de f considérée.

Prenons un exemple tiré de l'article original de Vincent, et étudié auparavant par Lagrange, à savoir

$$f(x) = x^3 - 7x + 7 .$$

1-er pas : On détermine une borne L pour les racines positives. On peut noter que

$$x \geq 2 \Rightarrow f'(x) = 3x^2 - 7 > 0 ,$$

ce qui prouve que

$$x \geq 2 \Rightarrow f(x) \geq f(2) = 1 ,$$

et donc que $L = 2$ convient.

2-ième pas : On calcule les $f^{(i)}(x)$. On a le tableau suivant

x	f(x)	f '(x)	f''(x)/2	$f^{(3)}(x)/6$
0	7	- 7	0	1
1	1	- 4	3	1
2	1	5	6	1

Ce qui montre que les racines réelles positives sont dans l'intervalle $]1, 2[$ (et fournit une autre démonstration du fait que la valeur $L = 2$ est correcte) , et que cet intervalle contient zéro ou deux racines.

On transforme donc l'équation par $x = 1 + x_1^{-1}$, d'où le polynôme

$$f_1 = x_1^3 - 4x_1^2 + 3x_1 + 1 ,$$

lu directement sur le tableau précédent.

On calcule un tableau analogue au précédent :

x_1	$f_1(x_1)$	$f_1'(x_1)$	$f_1''(x_1)/2$	$f_1^{(3)}(x_1)/6$
1	1	- 2	- 1	1
2	- 1	- 1	2	1
3	1	6	5	1

Ce tableau montre que f_1 a une racine entre 1 et 2 et une autre entre 2 et 3 .

Ce qui conduit à faire le premier changement de variable $x_1 = 1 + x_2^{-1}$, d'où le polynôme

$$f_2 = x_2^3 - 2\,x_2^2 - x_2 + 1 ,$$

et le nouveau tableau

x_2	$f_2(x_2)$	$f_2'(x_2)$	$f_2''(x_2)/2$	$f_2^{(3)}(x_2)/6$
1	- 1	- 2	1	1
2	- 1	3	4	1
3	7	14	7	1

qui montre que le polynôme f_2 a exactement une racine comprise entre 2 et 3 . Le changement de variable $x_2 = 2 + y^{-1}$ donne le polynôme

$$g(y) = y^3 - 3\,y^2 - 4\,y - 1 ,$$

dont les coefficients ne comportent qu'une seule variation de signe, située entre le premier et le second terme, comme souhaité. Donc le polynôme g possède une, et une seule racine positive β , qui est comprise entre 4 et 5 (puisque l'on a $g(4) = -1 < 0$ mais $g(5) > 0$) .

Il faut aussi effectuer le changement de variable $x_1 = 2 + z^{-1}$ qui conduit au polynôme

$$h(z) = x^3 + x^2 - 2z - 1,$$

lu sur le second tableau, polynôme dont les coefficients ne comportent qu'une seule variation de signe. Donc le polynôme h possède une, et une seule racine positive β', qui est comprise entre 1 et 2 (puisque l'on a $h(1) = -1$ et $h(2) = 7$).

Maintenant nous allons estimer β et β' avec un peu plus de précision. Une première application de la formule de Newton fournit les valeurs

$$\beta \cong 4 + 1/20 = 4{,}05$$

et

$$\beta' \cong 1 + 1/3 \cong 1{,}33,$$

la précision pour la première valeur étant vraisemblablement meilleure que celle de la seconde.

Soient α et α' les racines de f associées respectivement à β et à β'. Pour avoir une meilleure précision relative à α', il est préférable de transformer une nouvelle fois le polynôme f. Sachant la racine positive de h est comprise entre 1 et 2, on prend pour nouvelle variable t définie par $z = 1 + t^{-1}$ d'où le polynôme

$$k(t) = t^3 - 3t^2 - 4t - 1,$$

qui n'est autre que le polynôme $g(t)$ déjà rencontré plus haut.

Revenons au polynôme f . On a les formules

$$\alpha = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \beta^{-1}}} ,$$

et

$$\alpha' = 1 + \cfrac{1}{2 + \beta'^{-1}} = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \beta^{-1}}} .$$

D'où les encadrements

$$\frac{27}{16} < \alpha < \frac{22}{13} \quad \text{et} \quad \frac{23}{17} < \alpha' < \frac{19}{14} ,$$

et les valeurs approchées

$$\alpha \cong 1{,}6920 \quad \text{et} \quad \alpha' \cong 1{,}3569 .$$

D'autres stratégies sont possibles à la place de celle de Vincent :

- Uspensky (*Theory of equations* , McGraw-Hill, New York, 1948) propose d'utiliser les seules transformations $x = 1 + y$ et $x = (1 + z)^{-1}$, ce qui permet de séparer les zéros positifs de f compris entre 0 et 1 de ceux > 1 , le même procédé est ensuite appliqué aux polynômes transformés ; ce qui semble *a priori* moins efficace que la procédure de Vincent ,

- Collins et Akritas (cf. Collins et Loos , in *Computer Algebra* , Ed. Buchberger, Collins et Loos, Springer-Verlag, Wien, 1982) proposent eux une technique de dichotomie pour séparer les racines, essentiellement entre celles de l'intervalle [0 , L / 2] et celles de l'intervalle [L / 2 , L] et ainsi de suite ... ; ce qui permet d'économiser des opérations. Voir l'article cité pour une analyse précise.

5. Equations dont les racines ont une partie réelle négative .

Cette question est liée à la stabilité des systèmes mécaniques, elle a été posée par Maxwell, traitée d'abord par Routh et résolue par Hurwitz, son résultat est le suivant.

THEOREME 6 . – Considérons un polynôme à coefficients réels

$$f(x) = p_0 + p_1 x + \ldots + p_n x^n \text{ , avec } p_0 > 0 \text{ , } p_n \neq 0 .$$

Alors toutes les racines de f ont une partie réelle négative si, et seulement si, on a les inégalités suivantes

$$D_i = \begin{vmatrix} p_1 & p_0 & 0 & \ldots & 0 \\ p_3 & p_2 & p_1 & \ldots & 0 \\ \cdots & \cdots & \cdots & & \\ p_{2i-1} & p_{2i-2} & \cdots & & p_i \end{vmatrix} > 0 \quad \text{pour } i = 1, 2, \ldots, n ,$$

où l'on a posé $p_j = 0$ si $j < 0$ ou $j > n$.

> Nous suivrons la démonstration donnée par I. Schur. On raisonne par récurrence sur le degré n du polynôme f.

Si n est égal à 1 alors $f(x) = p_0 + p_1 x$ et $D_1 = p_1$ donc le théorème est vrai.

Pour traiter le cas général, le lemme suivant sera utile.

LEMME 2 . – Si f est un polynôme à coefficients réels qui n'a que des racines dont la partie réelle est < 0 , alors pour tout nombre complexe z on a

$$\text{signe} (| f(z) | - | f(-z) |) = \text{signe} (\text{Re} (z)) .$$

> On peut se limiter au cas où la partie réelle de z est positive , on écrit donc z sous la forme $z = a + i b$, avec a et b réels et $a \geq 0$.

Soit α un nombre complexe quelconque, $\alpha = \beta + i \gamma$, β et γ réels et $\beta < 0$.

On a alors la relation

$$|(z-\alpha)(z-\bar{\alpha})|^2 = (a-\beta)^4 + 2(a-\beta)^2(b^2+\gamma^2) + (b^2-\gamma^2)^2.$$

Par le changement de z en $-z$ la quantité qui figure au membre de droite reste invariante si a est nul et diminue pour $a > 0$.

Le lemme en résulte en appliquant cette remarque pour chacune des racines du polynôme f. <

Revenons à la démonstration du théorème. Nous allons construire un polynôme ψ de degré $< n$ dont les racines ont toutes une partie réelle négative si, et seulement si, il en est de même pour f. On pourra ensuite raisonner par récurrence sur le degré. On définit le polynôme ψ par la formule

$$\psi = p_0 p_1 + \omega(p_1 p_2 - p_0 p_3)x + p_0 p_3 x^2 + \omega(p_1 p_4 - p_0 p_5)x^3 + \ldots$$

d'où la relation

$$2x\psi = A(x) f(x) - B(x) f(-x)$$

avec

$$A(x) = (p_0(1 - \omega/x) + p_1\omega) \quad \text{et} \quad B(x) = (p_0(1-\omega/x) - p_1\omega).$$

On vérifie que ψ est un polynôme de degré $n-1$. Et on a l'implication

$$(p_0 > 0, p_1 > 0, \omega > 0, z \in \mathbf{C}^*, \mathrm{Re}(\omega/z) < 1) \Rightarrow |A(z)| > |B(z)|.$$

Si $\omega \in]0, 1[$ est assez petit, pour toute racine ξ de ψ, on a $\mathrm{Re}(\omega/\xi) < 1$; en raison du lemme 2 et de l'implication ci-dessus. D'où les conséquences suivantes

$$\psi(\xi) = 0 \Rightarrow A(\xi) f(\xi) = B(\xi) f(-\xi) \quad \text{avec} \quad |A(\xi)| > |B(\xi)|,$$

et donc $\mathrm{Re}(\xi) < 0$, du fait que toutes les racines de f ont une partie réelle négative.

Inversement, on vérifie que

$$2\, p_0\, p_1\, \omega\, f(x) = x\, A(-x)\, \psi(x) - x\, B(x)\, \psi(-x) .$$

Soit α une racine de f de partie réelle ≥ 0, alors on a

$$A(-\alpha)\, \psi(\alpha) = B(\alpha)\, \psi(-\alpha) ,$$

et, si $\alpha^{-1} = \beta + i\gamma$, avec $\beta \geq 0$,

$$A(-\alpha) = p_0 (1 + \beta\omega + i\gamma\omega) + p_1 \omega ,$$

$$B(\alpha) = p_0 (1 - \beta\omega - i\gamma\omega) - p_1 \omega ,$$

de sorte que

$$|A(-\alpha)|^2 - |B(\alpha)|^2 = 4\omega p_0^2 \beta + 4 p_0 p_1 \omega > 0 ,$$

et donc

$$|A(-\alpha)| > |B(\alpha)|$$

et finalement l'inégalité

$$|\psi(\alpha)| > |\psi(-\alpha)| ;$$

ce qui, d'après le lemme, est impossible lorsque toutes les racines ξ de ψ ont toutes une partie réelle < 0.

On peut donc appliquer l'hypothèse de récurrence au polynôme ψ.

Pour conclure, on vérifie que les déterminants associés à ψ sont

$$\Delta_1 = \omega (p_1 p_2 - p_0 p_3) = \omega D_2 ,$$

$$\Delta_2 = \omega p_0 ((p_1 p_2 - p_0 p_3) p_3 - (p_1 p_4 - p_0 p_5) p_1) = \omega p_0 D_3 ,$$

et, plus généralement, que le déterminant Δ_k est de la forme

$$\Delta_k = \lambda_k D_{k+1} ,$$

où le facteur λ_k est > 0. <

Exercices

1. Démontrer la règle de Descartes en raisonnant par récurrence sur le degré n du polynôme f et en considérant la dérivée de f.

[Si $n \leq 1$, le résultat est évident. Si $n > 1$ et si $f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$, avec $a_0 a_n \neq 0$, on peut écrire $f' = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \ldots + q a_q X^{q-1}$, avec $a_q \neq 0$. Par hypothèse de récurrence, le nombre r' de zéros positifs de f' est de la forme $v' - 2m'$, $m' \in \mathbf{N}$.

Si f' n'a pas de zéro positif alors, d'une part v' est pair et d'autre part $r = 0$ ou 1 selon que le produit $a_n a_0$ est positif ou négatif ...

Si f' a au moins un zéro positif, utiliser en particulier le théorème de Rolle sur l'intervalle $[0, c]$, où c est le plus petit zéro > 0 de f' ...]

2. Le but de cet exercice consiste d'abord à démontrer le lemme suivant, dû à Segner :

si on désigne par $V(P)$ le nombre de changements de signe de la suite des coefficients d'un polynôme unitaire réel P, alors, pour tout réel $c > 0$, le nombre de changements de signe de la suite des coefficients du polynôme $Q(X) = (X - c) P(X)$ est de la forme $V(P) + 1 + 2m$, $m \in \mathbf{N}$.

[On pose $P = X^n + a_1 X^{n-1} + \ldots + a_n$. Soit $V = V(P)$ et soient $i_1, \ldots, i_V$ les indices où les coefficients de P changent de signe, si bien que

signe $(a_h) = (-1)^j$ pour $h = i_j$ et signe $(a_h) = (-1)^j$ ou 0 pour $h = i_j + 1, \ldots, i_{j+1}$.

On écrit $Q(X) = X^{n+1} + b_1 X^n + .. + b_k X^{n+1-k} + \ldots + b_n X - c a_0$. Alors, on a les relations $b_k = a_k - c a_{k-1}$, et donc signe $(b_h) = (-1)^j$ pour $h = i_j$ ...]

En déduire une autre démonstration de la règle de Descartes.

3. Soit $f = X^n + a_{n-1} X^{n-1} + \ldots + a_0$ un polynôme unitaire à coefficients réels positifs ou nuls et majorés par M. Démontrer l'implication suivante

$$z \in \mathbf{C} \text{ et } f(z) = 0 \Rightarrow \mathrm{Re}(z) \leq 0 \text{ ou } |z| \leq (1 + \sqrt{(1+4M)})/2 .$$

[Pour $\mathrm{Re}(z) > 0$, démontrer la propriété suivante

$$|1 + \frac{a_{n-1}}{z}| \geq 1 \text{ et } |z| > \frac{1}{2}\left(1 + \sqrt{1+4M}\right) \Rightarrow \sum_{k=0}^{n-2} |a_k z^{k-n}| < 1 .$$

Conclure en considérant la quantité $|z^{-n} f(z)|$.]

4. Soit f un polynôme à coefficients réels, on considère le polynôme

$$F(x) = x f'(x) + a f(x) ,$$

où a est un réel quelconque. Soit r^+ le nombre de racines > 0 de f – comptées avec leurs multiplicités – on veut montrer que le nombre de racines réelles > 0 de F est au moins égal à $r^+ - 1$ (théorème dû à de Gua).

1°) Soient $b_1, \ldots, b_s$ les racines > 0 de f, avec $b_1 < \ldots < b_s$. La multiplicité de chaque b_i étant égale à r_i, le nombre de racines > 0 de f est $r^+ = r_1 + \ldots + r_s$. Démontrer que, pour $r_i > 1$, b_i est une racine de multiplicité $r_i - 1$ de F.

2°) Démontrer que F a une racine dans chaque intervalle $]b_i, b_{i+1}[$.

[On pourra démontrer d'abord les faits suivants :

$x f(x) / f'(x) \to +\infty$ si $x \to b_i +$,

$x f(x) / f'(x) \to -\infty$ si $x \to b_{i+1} -$,

f ne change pas de signe sur l'intervalle $]b_i, b_{i+1}[$.]

3°) En déduire que le nombre de racines réelles > 0 du polynôme F est au moins égal à $r^+ - 1$.

4°) Démontrer que l'on peut déduire la règle de Descartes du théorème de de Gua.

[On pourra procéder ainsi . Soit f un polynôme à coefficients réels et soit V le nombre de variations de signes de ses coefficients et soit r^+ le nombre de ses racines strictement positives. On veut démontrer que l'on a $V = r^+ + 2m$, où $m \in \mathbf{N}$.

On raisonne par récurrence sur V. Si $V = 0$, la règle de Descartes est évidente : r^+ est nul. Si $V > 0$, et si le premier changement de signe a lieu entre les coefficients des termes x^{n-i} et x^{n-j}, considérer le polynôme

$$F(x) = x f(x) - a f(x) \quad \text{où} \quad a = n - (i+j)/2 .$$

Démontrer que le nombre de changements de signe de F est $V - 1$.

En déduire la majoration $r^+ \leq V$.

Démontrer enfin que r^+ et V ont même parité.]

5°) Soit r^- le nombre de racines < 0 de f. Démontrer que le nombre de racines négatives de F est au moins égal à $r^- - 1$.

6°) Soit r_0 l'ordre de f en zéro. Démontrer que F est d'ordre au moins r_0 en zéro.

7°) Soit r le nombre de racines réelles de f. Démontrer que le nombre de racines réelles de F est au moins égal à $r - 2$.

Démontrer que ce nombre est exactement $r - 2$ dans le cas du polynôme $f = x^3 - x$ pour $a = -2$.

8°) Dans cette question, on suppose que toutes les racines de f sont réelles et on désigne par n le degré de f, $n \geq 1$.

(i) Démontrer que les racines de F sont toutes réelles pour $a > 0$.

[Supposons que f possède au moins une racine > 0 et soit b_1 la plus petite. Pour $\varepsilon > 0$ assez petit, démontrer que les nombres $f(\varepsilon)$ et $F(\varepsilon)$ sont de même signe tandis que les nombres $f(b_1 - \varepsilon)$ et $F(b_1 - \varepsilon)$ sont de signe contraire. En déduire que F possède une racine dans l'intervalle $]0, b_1[$. Conclure ...]

(ii) Démontrer que les racines de F sont toutes réelles pour $a < -n$.

5. Démontrer qu'un polynôme à coefficients réels possède au moins deux racines imaginaires dans l'un ou l'autre des trois cas suivants :

(i) il existe deux indices i et j tels que $i < j - 1$, pour lesquels les coefficients a_i et a_j soient non nuls et de même signe tandis que les a_k sont nuls pour $i < k < j$;

(ii) il existe deux indices i et j tels que $i < j - 2$, pour lesquels les coefficients a_i et a_j soient non nuls et de signes contraires tandis que les a_k sont nuls pour $i < k < j$;

(iii) le polynôme possède trois coefficients successifs qui sont en progression géométrique.

6. (Euler) Si les racines du polynôme $f(x) = a_n x^n + \ldots + a_0$ sont toutes réelles, alors on a

$$a_i^2 \geq a_{i-1} a_{i+1} \quad \text{pour} \quad i = 1, 2, \ldots, n .$$

7. Le but de cet exercice est de démontrer le théorème suivant dû à M. Riesz : Soit f un polynôme à coefficients réels, dont toutes les racines sont réelles et simples et soit d le minimum des distances entre deux racines de f . Alors f ' a toutes ses racines réelles et simples, de plus deux quelconques d'entre elles sont à une distance > d.

La démonstration suggérée ici est celle de A. Stoyanoff, *Sur un théorème de M. Marcel Riesz*, Nouvelles Annales de Mathématique, (6) , t. 1, 1926, p. 97-99 .

Considérons donc un polynôme f comme dans l'énoncé.

1°) Démontrer que les racines du polynôme dérivé f ' sont toutes réelles et simples et que si $x_1, \ldots, x_n$ sont les racines de f et $y_1, \ldots, y_{n-1}$ celles de f ' , rangées dans l'ordre croissant, alors on a $x_1 < y_1 < x_2 < y_2 < \ldots < x_{n-1} < y_{n-1} < x_n$.

[Penser au théorème de Rolle !] .

2°) Soit k un indice tel que la différence $y_{k+1} - y_k$ soit minimale. On veut montrer que l'on a l'inégalité

(i) $y_{k+1} - y_k > d$.

Montrer que l'on peut supposer que l'on a $y_k + d > x_{k+1}$, autrement dit que les points $y_k + d$ et y_{k+1} appartiennent tous deux à l'intervalle $] x_{k+1} , x_{k+2} [$.

Montrer que la fonction $F(x) = f'(x) / f(x)$ est strictement décroissante dans cet intervalle et vérifie $F(y_{k+1}) = 0$.

[Noter la relation

$$F(x) = \sum_{j=1}^{n} \frac{1}{x - x_j} \quad . \ ]$$

En déduire que l'inégalité (i) est vraie si on a $F(y_k + d) > 0$.

Démontrer cette dernière inégalité. [On pourra noter que

$$F(y_k + d) = F(y_k + d) - F(y_k) = \sum_{j=1}^{n} \left(\frac{1}{y_k + d - x_j} - \frac{1}{y_k - x_j} \right)$$

$$= \frac{1}{y_k + d - x_1} + \frac{1}{x_n - y_k} + \sum_{j=1}^{n-1} \frac{x_{j+1} - x_j - d}{(y_k - x_j)(y_k + d - x_{j+1})},$$

et vérifier que cette dernière somme est formée de termes ≥ 0, non tous nuls.]

8. Soient $a_1, ..., a_n$ des nombres réels donnés. On considère le polynôme

$$f(X) = (X + a_1) ... (X + a_n),$$

et on pose

$$f(X) = \sum_{i=0}^{n} p_i \binom{n}{i} X^i,$$

de sorte que

$$p_0 = 1 \text{ , et } p_i = \frac{\sum a_1 a_2 ... a_i}{\binom{n}{i}} \quad \text{pour } 1 \leq i \leq n,$$

où la somme est étendue à tous les produits de i termes extraits de $a_1, ..., a_n$.

1°) Soit s un entier ≥ 1. Démontrer la formule

$$f^{(s)}(X) = n(n-1)...(n-s+1) \left(X^{n-s} + ... + \binom{n-s}{k} p_k X^{n-s-k} + ... + p_{n-s} \right).$$

2°) Supposons désormais que les points a_i sont deux à deux distincts. Démontrer que le polynôme $f^{(s)}$ a toutes ses racines réelles et deux à deux distinctes.

Soit k un entier compris entre 0 et n, en déduire qu'il en est de même pour le polynôme

$$p_{k+1} Y^{k+1} + \binom{k+1}{1} p_k Y^k + \binom{k+1}{2} p_{k-1} Y^{k-1} + ... + 1.$$

3°) Montrer que le polynôme

$$p_{k+1} Y^2 + 2 p_k Y + p_{k-1}$$

possède deux racines réelles distinctes . [Dériver k - 1 fois le polynôme précédent ...]

4°) En déduire l'inégalité

$$p_k^2 > p_{k-1} p_{k+1} .$$

5°) On suppose en outre que les a_i sont tous positifs. Démontrer la suite d'inégalités

$$p_n^{1/n} < \ldots < p_3^{1/3} < p_2^{1/2} < p_1 ;$$

d'où, en particulier, l'inégalité entre moyenne arithmétique et moyenne géométrique :

$$(a_1 \ldots a_n)^{1/n} < (a_1 + \ldots + a_n) / n .$$

9. On s'intéresse au nombre r de racines réelles distinctes d'un trinôme à coefficients réels

$$f(x) = x^n + p x^m + q .$$

1°) On suppose n impair. Démontrer que, par un changement de variable simple, on peut supposer m impair. Lorsque tel est le cas, démontrer que r est égal à un ou trois et que f possède trois racines distinctes si, et seulement si, on a

$$\left(\frac{m p}{n}\right)^n + \left(\frac{m q}{n - m}\right)^{n - m} < 0 .$$

Qu'obtient-on quand n vaut trois ?

2°) On suppose maintenant n pair.

Démontrer que, par un changement de variable simple, on peut se ramener à l'un ou l'autre des deux cas suivants :

(i) m est impair et on a $p > 0$, (ii) m est pair .

On désigne par s le signe de l'expression

$$\left(\frac{m\,q}{n-m}\right)^{n-m} - \left(\frac{m\,p}{n}\right)^{n}.$$

de sorte que $s \in \{ 0, \pm 1 \}$. Démontrer que, le nombre r est donné par les formules suivantes

$$r = 1 - s \quad \text{dans le cas (i)},$$

et

$$r = 2(1 - s) \quad \text{dans le cas (ii)}.$$

10. Démontrer qu'un polynôme de degré n à coefficients réels a toutes ses racines réelles si, et seulement si, la suite de Sturm associée à ce polynôme est constituée de n polynômes dont les coefficients dominants ont tous le même signe.

Qu'en résulte-t-il pour le polynôme $x^3 + p\,x + q$?

11. On considère une suite $f_0, f_1, \ldots, f_s$ de polynômes à coefficients réels qui vérifient les conditions suivantes

(i) on ne peut avoir simultanément $f_i(c) = f_{i+1}(c) = 0$ avec $0 \le i < s$ et c réel,

(ii) si c est un réel tel que $f_i(c) = 0$, avec $0 < i < s$, alors on a

$$f_{i-1}(c)\, f_{i+1}(c) < 0,$$

(ii) f_s ne s'annule pas.

On suppose que $f = f_0$ est un polynôme de degré n. Démontrer que si la relation

$$V(f_0, f_1, \ldots, f_s; -\infty) - V(f_0, f_1, \ldots, f_s; +\infty) = n$$

a lieu alors f a toutes ses racines réelles et distinctes.

12. Le but de cet exercice est de démontrer la règle de Laguerre, qui permet de majorer les racines réelles d'un polynôme à coefficients réels.Soit

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$$

un polynôme à coefficients réels de degré égal à n . On pose

$$f_0 = a_0 \ , \ f_1 = x f_0 + a_1 \ , \ldots , f_i = x f_{i-1} + a_i \ , \ldots , f_n = x f_{n-1} + a_n = f \ .$$

1°) Démontrer que, pour tout nombre réel c , on a la relation

$$f_i(x) = (x - c) \ (f_0(c) x^{i-1} + \ldots + f_{i-1}(c)) \ + \ f_i(c) \ .$$

2°) En supposant que l'on a $f_i(c) \geq 0$ pour $i = 0, 1, \ldots, n$, démontrer que le polynôme f vérifie $f(x) > 0$ pour $x > c$.

3°) Démontrer l'implication

$$(f_i(c) \geq 0 \text{ pour } 0 \leq i \leq k) \Rightarrow (f_i(c') \geq 0 \text{ pour } 0 \leq i \leq k \text{ si } c' \geq c) \ .$$

4°) En déduire que la procédure suivante permet de trouver un nombre réel c tel que l'on ait $f_i(c) \geq 0$ pour $i = 0, 1, \ldots, n$.

(i) prendre c tel que $f_1(c) \geq 0$,

(ii) soit k le plus petit entier qui vérifie $k = n+1$ ou bien les deux conditions $k \leq n$ et $f_k(c) \leq 0$,

(iii) si $k \leq n$ alors remplacer c par un nombre $c' > c$ tel que $f_k(c') \geq 0$ et retourner en (ii) ,

(iv) ici, c convient .

13. Le but de cet exercice est de démontrer le théorème suivant, dû à Jensen :

- soit f un polynôme à coefficients réels et soit U l'union des disques fermés ayant pour diamètres les segments joignant deux racines imaginaires conjuguées de f, alors toute racine imaginaire du polynôme f' appartient à l'ensemble U.

[Développer en éléments simples la fraction rationnelle $f'(z)/f(z)$ et utiliser les faits suivants : lorsque u est une racine de f et z un point complexe extérieur à U,

$$\text{signe} \left\{ \text{Im} \left(\frac{1}{z-u} + \frac{1}{z-\bar{u}} \right) \right\} .]$$

14. Démontrer le corollaire de la proposition 7 en utilisant seulement le théorème de Rolle.

15. Soit f un polynôme de degré n à coefficients réels. Pour x réel, on note $v(x)$ le nombre de changements de signes de le suite des valeurs $f^{(i)}(x)$ pour i variant de 0 à n. On suppose que f a toutes ses racines réelles.

Démontrer que pour a et b réels, avec $a < b$, non racines de f, le nombre de racines réelles de f comprises entre a et b est exactement $v(a) - v(b)$.

16. Démontrer le théorème suivant dû à Laguerre :

- Soit $f(x) = a_0 x^n + ... + a_n$, un polynôme à coefficients réels. Pour x réel on pose

$f_0(x) = a_0$, $f_1(x) = x f_0(x) + a_1$, ..., $f_i(x) = x f_{i-1}(x) + a_i$, ..., $f_n(x) = x f_{n-1}(x) + a_n$, et on désigne par $v(x)$ le nombre de changements de signes de le suite des valeurs des nombres $f_i(x)$ pour i variant de 0 à n.

Soient a et b deux réels, $0 < a < b$, qui ne sont pas des racines de f. Alors le nombre r de racines de f comprises entre a et b est de la forme

$$r = v(a) - v(b) - 2m \quad , \quad \text{où} \quad m \in \mathbf{N} \ .$$

Généraliser ce résultat aux fonctions de la forme

$$F(x) = a_1 x^{\alpha_1} + \ ... \ + a_n x^{\alpha_n} \ ,$$

où les exposants sont des nombres réels quelconques.

17. Détermner, suivant les valeurs du paramètre réel a , le nombre de racines réelles du polynôme $X^4 - 3X^2 + 2X + a$.

18. Démontrer la " règle de Sturm " : soit a un réel > 0 tel que la suite des coefficients du polynôme $(x - a) f(x)$ admette $2k + 1$ changements de signe de plus que celle des coefficients du polynôme réel $f(x)$, alors f possède au moins $2k$ racines imaginaires.

[Soient p le nombre de racines positives de f , et q celui des racines négatives et enfin soit v le nombre de changements de signes de la suite des coefficients du polynôme f ; démontrer les inégalités $p \leq v$ et $q + v + 2k + 1 \leq n + 1$.]

19. Soit $f(X) = \alpha_0 X^n + ... + \alpha_n$, un polynôme à coefficients complexes. On pose

$$\alpha_j = a_j + i\, b_j \text{ , où } a_j \text{ et } b_j \text{ sont réels , } j = 0, 1, ..., n ,$$

et

$$P(X) = a_0 X^n + ... + a_n \ , \quad Q(X) = b_0 X^n + ... + b_n \ .$$

On suppose que tous les zéros de f ont une partie imaginaire > 0. Démontrer alors que les zéros des polynômes P et Q sont réels. [Soient $z_1, ..., z_n$ les racines de f et soit z un zéro de P ou de Q, démontrer la relation

$$|z - \bar{z}_1| \ ... \ |z - \bar{z}_n| = |z - z_1| \ ... \ |z - z_n| .$$

20. Soient m un entier strictement positif, n un entier ≥ 2, n nombres réels non nuls $a_1, ..., a_n$ et une suite strictement croissante de n nombres réels $x_1, ..., x_n$. Démontrer que le nombre r de racines réelles du polynôme

$$f(x) = a_1 (x - x_1)^m + ... + a_n (x - x_n)^m$$

est de forme $v - 2k$, où $k \in \mathbf{N}$ et v désigne le nombre de changements de signe de la suite $a_1, a_2, ..., a_n, (-1)^m a_1$. [Considérer la dérivée de $f(x)(x - x_n)^{-m}$.]

21. Soient P et Q deux polynômes à coefficients réels, sans racines communes et vérifiant $\deg(P) - 1 \leq \deg(Q) \leq \deg(P)$.

1°) Démontrer l'équivalence entre les deux propriétés suivantes :

(i) les polynômes P et Q ont toutes leurs racines réelles et ces racines sont intercalées (c'est à dire que si $x_1, ..., x_p$ sont les racines de P et si $y_1, ..., y_q$ sont celles de Q alors on a $x_1 < y_1 < x_2 < ...$)

(ii) Pour tout couple de nombres réels a et b non tous deux nuls, le polynôme $F(x) = a P(x) + b Q(x)$ n'a que des racines réelles.

[(i) $\Rightarrow$ (ii) : Noter que l'on a $F(x_k) = b Q(x_k)$ et que les $Q(x_k)$ changent de signe quand k augmente d'une unité. En déduire que F possède au moins $p - 1$ racines réelles. Conclure.

(ii) $\Rightarrow$ (i) : Démontrer d'abord que, pour z imaginaire, le quotient $h(z) = P(z)/Q(z)$ est aussi imaginaire (sinon F aurait une racine imaginaire). En déduire, d'une part que la partie imaginaire de $h(z)$ conserve un signe constant dans tout domaine où celle de z conserve aussi un signe constant et, d'autre part que P et Q ont toutes leurs racines réelles. Démontrer que tous les résidus de $h(z)$ doivent être de même signe. Démontrer enfin que si y et y' sont deux racines consécutives de Q alors $h(y+)$ et $h(y'-)$ sont de signes contraires, donc que $P(x)$ change de signe entre y et y'.]

2°) En déduire que si f et g sont deux polynômes ayant toutes leurs racines réelles et intercalées alors il en est de même pour leurs dérivées .

[Considérer $F(x) = a f(x) + b f(x)$ et sa dérivée ...]

Donner une autre démonstration du théorème de Riesz (voir exercice 7) en procédant comme suit : si d désigne la distance minimale entre deux racines distinctes de f et si $h < d$ alors $f(x)$ et $f(x+h)$ ont leurs racines réelles et intercalées, puis considérer $f'(x)$ et $f'(x+h)$ et utiliser ce qui vient d'être démontré.

22. Soit a un nombre réel et soit P un polynôme non constant à coefficients réels. Démontrer que le polynôme $a P(x) + P'(x)$ n'a pas plus de racines imaginaires que le polynôme P lui-même .

23. Soient $\xi_1, \ldots, \xi_n$ des nombres réels appartenant à un intervalle fermé $[\alpha, \beta]$. Soit r le nombre de zéros réels $> \beta$ du polynôme

$$f(x) = a_0 + a_1 (x - \xi_1) + a_2 (x - \xi_1)(x - \xi_2) + \ldots + a_n (x - \xi_1) \ldots (x - \xi_n),$$

où les a_i sont des nombres réels.

Démontrer qu'il existe un entier naturel m tel que l'on ait

$$r = v^+ - 2m,$$

où v^+ désigne le nombre de changements de signes de la suite $a_0, a_1, \ldots, a_n$.

Démontrer aussi qu'il existe un entier naturel m' tel que l'on ait

$$r^- = v^- - 2m',$$

où v^- désigne le nombre de changements de signes de la suite $a_0, -a_1, \ldots, (-1)^n a_n$ et r^- le nombre de racines de f qui sont $< \alpha$.

24. Démontrer la généralisation suivante, due à Hurwitz, du théorème de Budan-Fourier.

Soient a et b deux nombres réels, $a < b$. Soit f un polynôme qui ne s'annule ni en a ni en b, et soit r un entier tel que $f^{(r)}$, la dérivée r-ième de f, ne s'annule pas non plus ni en a ni en b. Soit N, respectivement N_r, le nombre de zéros (comptés avec leurs multiplicités) de f, respectivement de $f^{(r)}$, sur l'intervalle $[a, b]$. Alors il existe un entier $m \geq 0$ tel que

$$N - N_r = v(a) - v(b) - 2m,$$

où $v(x)$ désigne le nombre de changements de signes de la suite

$$(f(x), f'(x), \ldots, f^{(r)}(x)).$$

25. Soit f un polynôme à coefficients réels, de degré n, et soient a et b deux nombres réels, $a < b$. On reprend les notations du théorème de Budan - Fourier et on suppose que l'on a

$$N = v(a) - v(b) - 2m.$$

Démontrer que le polynôme f possède au moins $2m$ racines imaginaires.

[Soit N_1 le nombre de racines $< a$ et N_2 le nombre de racines $> b$. Avec des notations évidentes, on a $N + N_1 + N_2 + 2(m + m_1 + m_2) = n$ ...]

26. Démontrer la proposition suivante : Pour qu'un polynôme à coefficients réels de degré n possède n racines réelles distinctes, il faut et il suffit que la suite de Sturm qui lui est associée se compose de $n + 1$ polynômes ayant chacun un coefficient dominant du même signe que le coefficient dominant de ce polynôme.

Appliquer ce résultat au polynôme $x^3 + p\,x + q$.

27. Soit f un polynôme à coefficients réels dont la dérivée ne s'annule pas sur un certain intervalle $I =]\,a, b\,[$.

1°) Démontrer que la fonction

$$\varphi = x - f(x) / f'(x)$$

est croissante (respectivement décroissante) dans tout sous-intervalle de I où les quantités f et f'' ont le même signe (respectivement sont de signes contraires).

2°) On considère la situation suivante, rencontrée lors du théorème de Vincent, où on a les inégalités

$$f(a) < 0\ ,\ f^{(i)}(a) \geq 0 \quad \text{pour} \quad i \geq 1 \quad \text{et} \quad f(b) > 0\ .$$

Démontrer les inégalités

$$b - \frac{f(b)}{f'(b)} < \xi < a - \frac{f(a)}{f'(a)}\ .$$

3°) On conserve les hypothèses de la question précédente et on pose

$$M = \max \left\{ \frac{f''(x)}{2\,f'(x)}\ ;\ a \leq x \leq b \right\}\ .$$

On considère la fonction

$$\psi(x) = \varphi(x) - M\,(x - \xi)^2\ .$$

Démontrer que la fonction ψ est décroissante sur I. En déduire les inégalités

$$\xi > b - \frac{f(b)}{f'(b)} - M\,(x - \xi)^2$$

et

$$\xi > b - \frac{f(b)}{f'(b)} - \frac{f''(b)}{2\,f'(a)}\,(b - a)^2\ .$$

28. A un polynôme f à coefficients réels on associe le polynôme unitaire F dont les racines sont les carrés des différences des racines de f.

1°) Démontrer que F a toutes ses racines réelles et > 0 si, et seulement si, le polynôme f a toutes ses racines réelles et distinctes.

2°) En déduire que f a toutes ses racines réelles et distinctes si, et seulement si, F a tous ses coefficients non nuls et de signes contraires pour deux indices consécutifs quelconques.

Appliquer ceci au polynôme $x^2 + a x + b$.

29. Démontrer que les seuls polynômes $A, B, C \in \mathbf{R}[X]$ tels que

$$A^2(X) = X(B^2(X) + C^2(X))$$

sont les polynômes nuls.

Qu'en est-il sur $\mathbf{C}[X]$?

CHAPITRE VI

Polynômes sur un corps fini

1. Corps finis .

1. Résultats généraux .

Dans tout ce chapitre la lettre K désignera un corps fini (commutatif, d'ailleurs tout corps fini est commutatif : théorème de Wedderburn) .

L'unique morphisme de $\mathbf{Z}$ dans le corps K qui envoie l'entier 1 sur l'élément unité du corps K (aussi noté 1) n'est pas injectif, son noyau est de la forme $m\mathbf{Z}$, $m \geq 1$ (c'est un sous-groupe de $\mathbf{Z}$, et on applique le corollaire du théorème 2 du chapitre 1) . D'où une injection $\varphi : \mathbf{Z} / m\mathbf{Z} \to K$, ce qui montre que l'anneau $\mathbf{Z} / m\mathbf{Z}$ est intègre, donc que l'entier m est un nombre premier p . Le nombre p est appelé la **caractéristique** du corps K .

Ainsi un corps fini de caractéristique p contient un sous-corps qui est isomorphe au corps $\mathbf{Z} / p\mathbf{Z}$ (l'image $\varphi (\mathbf{Z} / p\mathbf{Z})$) . Le corps $\mathbf{Z} / p\mathbf{Z}$ sera noté $\mathbf{F}_p$. Il est facile de vérifier que K a une structure d'espace vectoriel sur $\mathbf{F}_p$, par conséquent – si n est la dimension de cet espace vectoriel – le corps K possède p^n éléments.

Si K est un corps commutatif de caractéristique p et si x et y sont deux éléments quelconques de K , la formule du binôme de Newton, jointe au fait que les coefficients du binôme $C (p , k)$ sont divisibles par p pour $k = 1, 2, ..., p - 1$, montre que l'on a

$$(x + y)^p = x^p + y^p .$$

Si q est une puissance de p , $q = p^n$, il en résulte aussitôt, par récurrence sur n , que l'on a aussi

$$(x + y)^q = x^q + y^q .$$

Si le corps K possède q éléments, l'ensemble K* des éléments non nuls de K est un groupe de cardinal q - 1 . D'après le théorème de Lagrange (chapitre 1) , tout élément de K* vérifie donc $x^{q-1} = 1$, et comme $0^q = 0$, on a $x^q = x$ pour tout élément x de K . Par conséquent, K est isomorphe au corps de décomposition du polynôme $X^q - X$ au dessus du corps $\mathbf{F}_p$. Si K et K' sont deux corps finis de même cardinal q , alors ils sont isomorphes ; d'où le fait qu'un corps à q éléments peut être noté $\mathbf{F}_q$.

Inversement, si q désigne une puissance d'un nombre premier p , et si Ω_p désigne une clôture algébrique fixée du corps $\mathbf{F}_p$, l'ensemble E des éléments de Ω_p qui vérifient $x^q = x$ constitue un sous-corps de Ω_p : en effet,

$$x, y \in E \Rightarrow (xy)^q = xy \quad \text{donc} \quad xy \in E,$$

$$x \in E \text{ et } x \neq 0 \Rightarrow x^{-1} \in E,$$

$$x, y \in E \Rightarrow (x+y)^q = x^q + y^q = x + y \quad \text{donc} \quad x+y \in E,$$

$$x \in E \Rightarrow -x \in E.$$

Enfin, l'ensemble E comporte q éléments puisque les racines du polynôme $X^q - X$ sont simples (la dérivée de ce polynôme est égale à -1) . Par conséquent E est un corps possédant q éléments. Autrement dit, $\mathbf{F}_q$ existe !

Enfin, en appliquant la proposition 3 du chapitre 2 , on obtient le résultat suivant.

PROPOSITION 1 . – Tout sous-groupe multiplicatif fini d'un corps commutatif est cyclique. En particulier, le groupe multiplicatif $\mathbf{F}_q^*$ est cyclique.

Résumons ce qui vient d'être démontré.

THEOREME 1 . – Tout corps K fini a un cardinal de la forme p^n, $n \geq 1$, où p est un nombre premier égal à la caractéristique de K .

Inversement, si p est un nombre premier et n un entier ≥ 1, il existe un corps fini, et un seul à isomorphisme près, de cardinal $q = p^n$; on le note $\mathbf{F}_q$.

Tout élément x de $\mathbf{F}_q$ vérifie $x^q = x$; de plus, si K est un corps dont $\mathbf{F}_q$ est un sous-corps, cette relation caractérise les éléments de $\mathbf{F}_q$ parmi ceux de K . On a donc

$$X^q - X = \prod_{x \in \mathbf{F}_q} (X - x) .$$

2. Les opérations dans un corps fini .

Nous allons étudier les opérations arithmétiques dans le corps fini $\mathbf{F}_q$. Si, du point de vue mathématique, il n'existe essentiellement qu'un corps fini à q éléments, du point de vue du calcul la situation est toute autre : il faut choisir une représentation des éléments du corps $\mathbf{F}_q$ et la réalisation de ces opérations dépend beaucoup de la nature de cette représentation. Une étude très détaillée de cette importante question figure dans l'ouvrage de E. R. Berlekamp, *Algebraic Coding Theory* , McGraw-Hill, New York, 1968.

Si $q = p$, la représentation de $\mathbf{F}_q$ ne pose pas de problème. Supposons $q = p^n$, avec $n \geq 2$. Pour simplifier, nous ne considérerons que les deux représentations suivantes :

(i) $\mathbf{F}_q$ est un $\mathbf{F}_p$-espace vectoriel de dimension n , on choisit une certaine base $\{b_1, ..., b_n\}$ de cet espace et on repère chaque élément de $\mathbf{F}_q$ par ses composantes sur cette base.

(ii) On prend un élément x de $\mathbf{F}_q^*$ qui engendre ce groupe et tout élément non nul de $\mathbf{F}_q$ s'écrit d'une manière, et d'une seule, sous la forme x^m , avec $0 \leq m < q - 1$.

Dans la représentation (i) , l'addition s'effectue très simplement composante par composante, elle équivaut à n additions modulo p . Par contre, la représentation (ii) est très mal adaptée à l'addition. Il n'y a pas de loi simple permettant, pour h et k donnés avec $x^h + x^k \neq 0$, de déterminer un entier m tel que $x^m = x^h + x^k$. Il semble *a priori* qu'on doive construire une table de q(q-1)/2 éléments ; toutefois, si par exemple on a l'inégalité $k \geq h$, on peut écrire $x^h + x^k = x^h (1 + x^{k-h})$ et se limiter à calculer une fois pour toutes la table des q éléments $1 + x^j$ pour $j = 0, 1, ..., q - 2$.

Le calcul de l'opposé se fait très simplement dans les deux représentations. C'est clair pour la première. Pour la seconde, on note que le problème ne se pose pas en caractéristique deux, puisque dans ce cas $-y = y$, tandis que pour q impair on a

$x^{(q-1)/2} = -1$, (en effet $(x^{(q-1)/2})^2 = 1$ et $x^{(q-1)/2} \neq 1$)

et donc,

si $y = x^k$ alors $-y = x^j$ où $j = k + (q-1)/2 \mod q - 1$.

Pour calculer le produit, la représentation (ii) est très commode puisque

$x^h . x^k = x^j$ où $j = h + k \mod q-1$.

Par contre, le calcul du produit dans la représentation (i) exige la connaissance des valeurs des produits $b_i . b_j$. Ceci incite à choisir une base de la forme $\{1, z, ..., z^{n-1}\}$ – autrement dit à considérer l'isomorphisme $\mathbf{F}_q \cong \mathbf{F}_p[X] / (P(X))$ où P est le polynôme minimal de z sur le corps $\mathbf{F}_p$ (P est de degré n si $\{1, z, ..., z^{n-1}\}$ est une base) – dans ce cas il suffit de calculer une fois pour toutes les représentations sur cette base des puissances $z^n, ..., z^{2n-2}$ (on prouvera plus loin qu'un tel z existe). On est alors amené à effectuer au plus n^2 produits dans $\mathbf{F}_p$ suivis d'au plus n^2 additions.

Le calcul de l'inverse est trivial dans la représentation (ii) : si $y = x^k$ alors son inverse y^{-1} est égal à x^{q-1-k} .

Pour effectuer le calcul de y^{-1} dans le cas de la représentation (i) on peut utiliser la relation $y^{-1} = y^{q-2}$, ce qui ne nécessite que $O(\text{Log } q)$ produits. Comme nous l'avons déjà vu, cette méthode est aussi utilisable pour le corps $\mathbf{F}_p$.

Dans le cas de la représentation $\mathbf{F}_q \cong \mathbf{F}_p[X] / (P(X))$, on peut calculer l'inverse grâce à l'algorithme d'Euclide : en effet, si un élément x non nul de $\mathbf{F}_q$ est représenté par le polynôme $A(z)$ et si on a calculé une relation de Bézout

$$A\,U + P\,V = 1 ,$$

alors l'inverse de x est $U(z)$.

3. Détermination d'un élément primitif de $\mathbf{F}_q^*$.

Un élément primitif x de $\mathbf{F}_q^*$ est caractérisé par le fait qu'il ne vérifie aucune des relations $x^r = 1$, où r est un diviseur strict de $q - 1$, ce qui équivaut à la condition

$$s \mid (q-1) \quad \text{et} \quad s \text{ premier} \Rightarrow x^{(q-1)/s} \neq 1 .$$

Les éléments primitifs de $\mathbf{F}_q^*$ sont exactement les racines du polynôme

$$\Phi_{q-1}(X) = (X^{q-1} - 1) / S(X) ,$$

où

$$S(X) = \text{p.g.c.d.} \left(X^{q-1} - 1 , \prod_{r \mid q-1 \,;\, 1 \le r < q-1} (X^r - 1) \right) .$$

Le polynôme $\Phi_{q-1}(X)$ est appelé le **polynôme cyclotomique** d'ordre $q - 1$.

Comme le groupe $\mathbf{F}_q^*$ est cyclique et de cardinal $q-1$, il possède exactement $\varphi(q-1)$ générateurs, ainsi la proportion d'éléments primitifs dans $\mathbf{F}_q^*$ est $\varphi(q-1) / (q-1)$. On démontre la minoration $\varphi(n) / n \geq c\,(\text{LogLog } n)^{-1}$, (voir exercice 1) , d'où le fait qu'en prenant successivement k éléments au hasard dans l'ensemble $\mathbf{F}_q^*$ jusqu'à ce qu'on trouve un élément primitif on a presque toujours $k = O(\text{LogLog } n)$.

4. Détermination de z tel que $\mathbf{F}_q = \mathbf{F}_p[z]$.

Nous savons déjà qu'un élément z tel que $\mathbf{F}_q = \mathbf{F}_p[z]$ vérifie $z^{q-1} = 1$, mais il ne doit pas vérifier $z^{q'-1} = 1$ où $q' = p^d$, d étant un diviseur strict de n : sinon il appartient au sous-corps $\mathbf{F}_{q'}$ de $\mathbf{F}_q$.

Il en résulte que les éléments z cherchés sont exactement les racines du polynôme

$$P(X) = (X^{q-1} - 1) / R(X) ,$$

où

$$R(X) = \text{p.g.c.d.} \left(X^{q-1} - 1 , \prod_{d \mid n \, ; \, 1 \le d < n} (X^{p^d - 1} - 1) \right) .$$

De plus, chaque z est racine d'un polynôme de $\mathbf{F}_p[X]$ irréductible et de degré n. Ainsi, $P(X)$ est égal au produit des polynômes de $\mathbf{F}_p[X]$ irréductibles et de degré n. Si Q désigne l'un quelconque de ces polynômes, le corps $\mathbf{F}_q$ est isomorphe à l'anneau quotient

$$\mathbf{F}_p[X] / (Q(X)) .$$

Pour déterminer un de ces polynômes, il suffit évidemment de factoriser le polynôme P sur le corps $\mathbf{F}_p$; mais il est plus facile – lorsque q est assez petit – de procéder comme suit : on effectue tous les produits possibles d'un polynôme de degré n' sur $\mathbf{F}_p$ par un polynôme de degré $n - n'$ sur $\mathbf{F}_p$, d'où la liste des polynômes réductibles de degré n et le fait qu'un polynôme Q est un polynôme quelconque de degré n qui n'apparaît pas dans cette liste.

Il est aussi possible de choisir un polynôme arbitraire de degré n et de tester s'il divise P, si tel est le cas alors il est irréductible, sinon on essaie un autre polynôme de degré n. Comme nous le verrons bientôt, le nombre I_n de polynômes de $\mathbf{F}_p[X]$ irréductibles et de degré n est équivalent à p^n / n, chacun des essais précédents a donc une "chance" d'aboutir voisine de $1/n$; pour k essais consécutifs, la "chance" d'échouer est voisine de $(1 - 1/n)^k$, on a donc "en général" $k = 0(n)$.

5. Un exemple : $\mathbf{F}_8$.

Nous allons déterminer $\mathbf{F}_8$, "le" corps à huit éléments. Si z est un élément quelconque de $\mathbf{F}_8$ autre que 0 ou 1 (les éléments de $\mathbf{F}_2$) , alors $\mathbf{F}_8 = \mathbf{F}_2[z]$. Le premier pas consiste à déterminer les polynômes minimaux possibles pour z , c'est à dire les polynômes irréductibles de degré trois sur $\mathbf{F}_2$.

Le plus simple est de noter que les polynômes de degré 1 ou 2 qui ne s'annulent pas en zéro sont

$$X + 1 \ , \ X^2 + 1 \ , \ X^2 + X + 1$$

et donc que les polynômes réductibles de degré trois qui ne s'annulent pas en zéro sont

$$X^3 + X^2 + X + 1 \ , \ X^3 + 1 \ ;$$

ce qui montre que les polynômes irréductibles de degré trois sont

$$P(X) = X^3 + X + 1 \quad \text{et} \quad Q(X) = X^3 + X^2 + 1 \ .$$

On vérifie d'ailleurs que

$$X^8 - X = X(X - 1) P(X) Q(X) \ .$$

Prenons par exemple pour z une racine du polynôme $P(X)$. L'application $x \to x^2$ laisse le polynôme P invariant mais permute ces racines. Les deux autres racines de P sont donc z^2 et $z^4 = z^2 + z$ (puisque $z^3 + z + 1 = 0$) .

La " table de multiplication " est donnée par

$$z^4 = z^2 + z \ , \ z^5 = z^3 + z^2 = z^2 + z + 1 \ , \ z^6 = z^3 + z^2 + z = z^2 + 1 \ .$$

On a $z^7 = 1$ et z engendre $\mathbf{F}_8^*$ (comme tout élément de $\mathbf{F}_8^*$ autre que 1 , puisque ce groupe est de cardinal premier) . Le polynôme cyclotomique Φ_7 est égal à

$$\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \ ,$$

et on a

$$\Phi_7(X) = P(X) Q(X) \ .$$

2. Statistiques sur $\mathbf{F}_q[X]$.

1. La fonction de Möbius .

La fonction de Möbius est définie par la formule

$$\mu(n) = \begin{cases} (-1)^k \text{ si } n = p_1 \dots p_k \text{ , } k \geq 0 \text{ , } p_i \text{ entiers premiers distincts} \\ 0 \quad \text{sinon .} \end{cases}$$

Elle vérifie la propriété suivante

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 \text{ si } n = 1 \text{ ,} \\ 0 \text{ sinon .} \end{cases}$$

Désignons en effet par $S(n)$ le membre de gauche, si $n = n' n''$ où n' et n'' sont premiers entre eux on a alors

$$S(n'n'') = \sum_{d \mid n'n''} \mu(d) = \sum_{d' \mid n' \text{ ; } d'' \mid n''} \mu(d'd'') = \sum_{d' \mid n' \text{ ; } d'' \mid n''} \mu(d')\,\mu(d'') = S(n')\,S(n'') \text{ ,}$$

ce qui prouve qu'il suffit de vérifier la formule lorsque n est une puissance d'un nombre premier, auquel cas on a bien

$S(1) = 1$ et $S(p^k) = 1 - 1 = 0$ pour $k \geq 1$.

On en déduit la **formule d'inversion de Möbius** :

PROPOSITION 1 . – Si f et g sont deux fonctions définies sur $\mathbf{N}^*$, à valeurs dans un groupe G commutatif (dont la loi est notée additivement) , et liées par la relation

$$f(n) = \sum_{d \mid n} g(d) \text{ ,}$$

alors

$$g(n) = \sum_{d \mid n} \mu(d)\, f(n/d) \text{ .}$$

> On a en effet

$$\sum_{d \mid n} \mu(d)\, f(n/d) = \sum_{d \mid n} \mu(d) \sum_{d' \mid n/d} g(d') = \sum_{d,\, d' ;\, dd' \mid n} \mu(d)\, g(d') = \sum_{d'} g(d') \sum_{d \mid n/d'} \mu(d) = g(n) \,.\, <$$

COROLLAIRE . – Soit $\Phi_n(X) \in \mathbf{Z}[X]$ le polynôme cyclotomique d'ordre n, c'est à dire le polynôme minimal d'une racine primitive n - ième de l'unité, alors on a

$$\Phi_n(X) = \prod_{d \mid n} \left(X^{n/d} - 1 \right)^{\mu(d)} .$$

> On prend pour G le groupe multiplicatif $\mathbf{Z}(X)^*$, et on utilise la relation

$$X^n - 1 = \prod_{d \mid n} \left(X^{n/d} - 1 \right) . \; <$$

2. Calcul de I_n .

Rappelons que I_n désigne le nombre de polynômes irréductibles unitaires, de degré égal à n et à coefficients dans le corps $\mathbf{F}_q$.

En regroupant les éléments de $\mathbf{F}_{q'}$, $q' = q^n$, selon leur degré sur $\mathbf{F}_p$, on obtient :

$$q^n = \sum_{d \mid n} d\, I_d \,.$$

Une application de la formule d'inversion de Möbius fournit le résultat suivant.

PROPOSITION 2 . – Le nombre I_n de polynômes unitaires irréductibles de degré n à coefficients dans le corps fini $\mathbf{F}_q$ est donné par la formule

$$I_n = \frac{1}{n} \sum_{d \mid n} \mu(d)\, q^{n/d} \,,$$

d'où résulte l'encadrement $q^n - 2\, q^{n/2} < n\, I_n \leq q^n$ (inégalité stricte si $n \geq 2$).

3. Nombre de polynômes quadratfrei .

Le résultat est le suivant.

PROPOSITION 3 . – Le nombre de polynômes unitaires quadratfrei sur $\mathbf{F}_q$, de degré $d \geq 2$ est égal à $q^d - q^{d-1}$.

> Nous ne donnons que le principe de la démonstration.

La fonction caractéristique des polynômes unitaires sur $\mathbf{F}_q$ est égale à

$$\frac{1}{1 - qT} ,$$

celle de leurs carrés est donc

$$\frac{1}{1 - qT^2} .$$

Du fait qu'un polynôme unitaire quelconque s'écrit de manière unique comme produit d'un polynôme unitaire quadratfrei et du carré d'un polynôme unitaire, la fonction caractéristique des polynômes unitaires et quadratfrei est égale à

$$\frac{1}{1 - qT} \cdot \left(\frac{1}{1 - qT^2} \right)^{-1} = \frac{1 - qT^2}{1 - qT} .$$

D'où le résultat. <

4. Etude du nombre de facteurs irréductibles d'un polynôme .

Les résultats de ce paragraphe sont extraits de l'article de M. Mignotte et J. L. Nicolas , *Statistiques sur* $F_q[X]$, Ann. de l'Inst. Henri Poincaré, v. XIX, n° 2, 1983, pp. 113 -121. Mais ici les constantes sont calculées explicitement.

On désigne par E_n l'ensemble des polynômes unitaires de degré n appartenant à l'anneau $\mathbf{F}_q[X]$. On a donc Card (E_n) = q^n . Si un polynôme $F \in E_n$ admet la décomposition en produit de facteurs irréductibles

$$F = P_1^{a_1} \dots P_k^{a_k} ,$$

on pose $\omega(F) = k$, autrement dit

$$\omega(F) = \sum_{P \mid F \, ; \, P \text{ irréductible}} 1 \quad .$$

LEMME 1 . – Soit T un nombre entier, $1 \le T \le n$. Pour $F \in E_n$ on pose

$$\omega_T(F) = \sum_{P \mid F \, ; \, P \text{ irr.} \, ; \, \deg P \le T} 1 \quad ,$$

ainsi $\omega_T(F)$ désigne le nombre de facteurs irréductibles distincts de F dont le degré ne dépasse pas T (en particulier, si $F \in E_n$ alors $\omega_n(F) = \omega(F)$) . On a

$$\sum_{F \in E_n} \omega_T(F) = q^n (\operatorname{Log} T - c) \text{ , avec } -1 < c < 2{,}5 .$$

> On a

$$\sum_{F \in E_n} \omega_T(F) = \sum_{F \in E_n} \sum_{P \mid F \, ; \, \deg P \le T} 1 = \sum_{i=1}^{T} \sum_{P \, ; \, \deg P = i} \sum_{F \, ; \, P \mid F} 1 = \sum_{i=1}^{T} I_i \, q^{n-i} ,$$

où P désigne un polynôme unitaire irréductible et où F parcourt E_n .

D'après la proposition 2 , on a

$$I_i = \frac{q^i}{i} - R_i q^{i/2} \qquad \text{avec} \quad 0 \le R_i \le \frac{2}{i} .$$

Donc

$$\sum_{F \in E_n} \omega_T(F) = q^n \left(\sum_{i=1}^{T} \frac{1}{i} - \sum_{i=1}^{T} R_i q^{-i/2} \right) = q^n (\operatorname{Log} T - c),$$

où $\quad c = \operatorname{Log} T - \sum_{i=1}^{T} \frac{1}{i} + \sum_{i=1}^{T} R_i q^{-i/2}$.

Il est facile d'estimer c , on a d'une part

$$\operatorname{Log} T < \sum_{i=1}^{T} \frac{1}{i} < 1 + \operatorname{Log} T \qquad (\text{considérer l'intégrale } \int_1^T \operatorname{Log} t \, dt),$$

et d'autre part

$$0 < \sum_{i=1}^{T} R_i q^{-i/2} < 2 \sum_{i=1}^{T} \frac{(1/\sqrt{q})^i}{i} < 2 \sum_{i=1}^{\infty} \frac{(1/\sqrt{2})^i}{i} = -2 \operatorname{Log}(1 - (1/\sqrt{2})) < 2{,}456 .$$

D'où la conclusion. <

PROPOSITION 4 . – Avec les notations du lemme précédent, on a, pour tout nombre entier T , $2 \le T \le n$,

$$\sum_{F \in E_n} \left(\omega_T(F) - \operatorname{Log} T \right)^2 < 2 q^n (1 + \operatorname{Log} T) .$$

> Suivons la démonstration de Hardy and Wright (*An Introduction to the Theory of Numbers* , Oxford, at the Clarendon Press, 1960) pour la fonction ω relative aux nombres entiers.

La quantité $\omega_T(F)\,(\omega_T(F) - 1)$ est le nombre de paires (P, Q) de polynômes irréductibles distincts telles P et Q divisent F (en comptant $(P, Q) \neq (Q, P)$) . On a donc

$$\omega_T(F)\,(\omega_T(F) - 1) = \sum_{P \neq Q\,;\ \deg P,Q \leq T\,;\ PQ \mid F} 1 \quad .$$

Ce qui implique

$$\sum_{F \in E_n} \omega_T(F)\,(\omega_T(F) - 1) \leq \sum_{\deg P \leq T\,;\ \deg P.Q \leq n} \sum_{F\,;\ P\,Q \mid F} 1$$

$$\leq \sum_{i=1}^{T} I_i \sum_{j=1}^{T} I_j\, q^{n-i-j} \leq q^n \left(\sum_{i=1}^{T} \frac{1}{i} \right)^2 < q^n \left(1 + \operatorname{Log} T \right)^2 .$$

La démonstration du lemme s'achève en utilisant la formule

$(\omega_T(F) - \operatorname{Log} T)^2 = \omega_T(F)\,(\omega_T(F) - 1) + (1 - 2 \operatorname{Log} T)\,\omega_T(F) + (\operatorname{Log} T)^2$,

ainsi que le lemme 1. <

COROLLAIRE . – (Inégalité de Tchebytcheff pour la fonction ω) Pour tout nombre entier $n \geq 3$ et tout nombre réel λ strictement positif on a l'inégalité

$$\operatorname{Card} \left\{ F \in E_n\ ;\ |\omega(F) - \operatorname{Log} n| \geq \lambda \sqrt{\operatorname{Log} n} \right\} \leq 3\, q^n\, \lambda^{-2} .$$

> On applique la proposition avec $T = n$. <

4. Factorisation d'un polynôme en produit de polynômes quadratfrei .

Dans tout ce paragraphe, K est un corps quelconque, non nécessairement fini.

1. Définitions et généralités .

Soit K un corps commutatif quelconque et soit F un polynôme non nul à coefficients dans K . On dit que F est **quadratfrei** si F ne possède que des racines simples dans tout corps contenant K .

Soit F ' la dérivée du polynôme F et soit Q le p.g.c.d. unitaire de F et de F ' . Si ce p.g.c.d. est égal à 1 , la relation de Bézout entre F et F '

$$U F + V F' = 1$$

montre que F et F ' n'ont pas de racines communes et donc que F n'a que des racines simples, autrement dit que F est quadratfrei.

Inversement, si F n'est pas quadratfrei et admet, dans un certain corps contenant L , la décomposition

$$F = \lambda P_1^{e_1} \dots P_k^{e_k} ,$$

où les P_i sont des polynômes sur L , unitaires, de degré un et deux à deux distincts, avec $e_1 \geq 2$, alors la dérivée F ' est de la forme

$$F' = \lambda P_1^{e_1} \dots P_k^{e_k - 1} R ,$$

et

$$P_1^{e_1 - 1} \dots P_k^{e_k - 1} \text{ divise } Q ,$$

donc P_1 divise Q , ainsi F et F ' ne sont pas premiers entre eux.

Le polynôme R est en fait donné par la formule

$$R = \sum_{i=1}^{k} e_i P_1 \ldots P_{i-1} P_{i+1} \ldots P_k ,$$

et F / Q divise $P_1 \ldots P_k$, c'est donc un polynôme quadratfrei.

Nous avons donc démontré le résultat suivant.

PROPOSITION 5 . – Soit F un polynôme non constant, à coefficients dans un corps K . Alors F est quadratfrei si, et seulement si, il est premier avec sa dérivée.

De plus, le polynôme F / p.g.c.d. (F , F ') est toujours quadratfrei, et si, d'une part, la dérivée F ' est non nulle et d'autre part on a p.g.c.d. (F , F ') $\neq 1$ alors ce polynôme est un diviseur non trivial de F .

2. Cas de la caractéristique zéro .

Lorsque K est de caractéristique zéro, l'expression précédente de R montre qu'aucun des polynômes P_i ne divise le polynôme R .

Dans ce cas, on a les relations

$$Q = P_1^{e_1 - 1} \ldots P_k^{e_k - 1} ,$$

et

$$F / Q = P_1 \ldots P_k .$$

3. Cas de la caractéristique non nulle .

Supposons maintenant K de caractéristique p . L'expression du facteur R montre qu'un des polynômes P_i divise R si, et seulement si, l'entier p divise l'exposant e_i .

Si p ne divise pas tous les exposants e_i , il divise par exemple les premiers exposants $e_1, \ldots, e_h$ mais ne divise pas $e_{h+1}, \ldots, e_k$, avec $0 \leq h < k$, alors F ' n'est pas nul et le polynôme Q vaut

$$Q = P_1^{e_1} \ldots P_h^{e_h} P_{h+1}^{e_{h+1} - 1} \ldots P_k^{e_k - 1} ;$$

ce qui montre que l'on a

$$F / Q = P_{h+1} \ldots P_k .$$

Le cas où p divise tous les exposants e_i se produit si, et seulement si, la dérivée F ' du polynôme F est nulle. Si F s'écrit $F = \sum a_i X^i$ et a une dérivée nulle alors p divise chaque indice i pour lequel a_i est non nul ; soit p^e la plus grande puissance de le nombre p telle que p^e divise le p.g.c.d. des entiers i pour lesquels a_i est non nul, alors on a $e \geq 1$ et on peut écrire le polynôme F sous la forme

$$F = H (X^{p^e}) , \text{ avec } H \in K [X] .$$

Inversement, si le polynôme F est de cette forme alors sa dérivée est nulle.

Considérons le cas particulier où le corps K est égal à $\mathbf{F}_q$ et où F est sous la forme précédente. Soient u et v deux entiers tels que l'on ait la relation de Bézout

$$u p^e + v (q-1) = 1 , \text{ avec } 1 \leq u < q .$$

Alors, pour tout élément x de $\mathbf{F}_q$, on a

$$(x^u)^{p^e} = x^{1 - v (q-1)} = x ;$$

ce qui signifie que x^u est une racine p^e - ième de x .

Ceci permet de calculer facilement un polynôme H_1 tel que

$$H(X^{p^e}) = H_1(X)^{p^e} ;$$

en fait il suffit de $O(d\, p^e \operatorname{Log} q)$ multiplications dans $\mathbf{F}_q$, où d est le degré de H.

Grâce à la proposition 5 et à l'étude ci-dessus, on obtient le résultat suivant.

PROPOSITION 6. – Soit K un corps fini ou de caractéristique zéro, alors tout polynôme irréductible de $K[X]$ est quadratfrei (et a donc une dérivée non nulle).

Remarque : Si $K = \mathbf{F}_p[Y]$ et $F(X) = Y X^p - 1$, alors $F' = 0$ et cependant F est irréductible sur K (exercice : le démontrer).

4. Algorithmes de décomposition en produit de polynômes quadratfrei.

Dans ce paragraphe, K est un corps de caractéristique zéro ou un corps fini, dont la caractéristique est notée p. Soit F un polynôme non constant de $K[X]$ pour obtenir une décomposition de F en produit de polynômes quadratfrei on peut procéder ainsi :

(i) on calcule la dérivée F' de F ;

(ii) Si $F' \neq 0$, on calcule le p.g.c.d. Q de F et de F'. Alors, si $Q = 1$ le polynôme F est quadratfrei, sinon $F = Q R$, où R est quadratfrei, avec les inégalités $0 < \deg R < \deg F$, et on applique la procédure au polynôme Q ;

(iii) Si $F' = 0$ on peut calculer un polynôme $H \in \mathbf{F}_q[X]$ tel que l'on ait

$$F = H^{p^e}, \quad e \geq 1, \quad \text{et} \quad H' \neq 0 ;$$

et on applique ensuite la procédure au polynôme H.

Si d désigne le degré du polynôme F , on peut noter que l'étape (i) comporte au plus d multiplications, tandis que le calcul de Q s'effectue en $O(d^2)$ opérations sur le corps K . Enfin le troisième pas ne peut s'appliquer que si la caractéristique est non nulle et comporte au plus $O(d/p \cdot \text{Log } q)$ multiplications, où $q = \text{Card}(K)$.

L'article *On square-free Decomposition Algorithms* , in Proc. of the 1976 AMS Symp. on Symb. and Alg. Comp., Yorktown, ed. R. D. Jenks de D. Y. Y. Yun contient les trois méthodes suivantes de décomposition en produit de polynômes quadratfrei.

On se donne un polynôme $F \in K[X]$, et l'algorithme calcule des polynômes quadratfrei, deux à deux premiers entre eux $P_1, ..., P_k$ tels que $F = P_1 P_2^2 ... P_k^k$, avec $k \geq 1$ et $P_k \neq 1$.

méthode 1 (Tobey et Horowitz) :

$C_1 := \text{p.g.c.d.}(F, F')$; $D_1 := P / C_1$; $i := 1$;

tant que $C_i \neq 1$ **faire**

début $C_{i+1} := \text{p.g.c.d.}(C_i, C_i')$; $D_{i+1} := C_i / C_{i+1}$; $P_i := D_i / D_{i+1}$; $i := i + 1$

fin.

En caractéristique zéro, le déroulement est le suivant :

$$C_1 = P_2 P_3^2 ... P_k^{k-1} \; ; \; D_1 = P_1 P_2 ... P_k \; ; \; ..... \; ;$$

$$C_i = P_{i+1} P_{i+2}^2 ... P_k^{k-i} \; ; \; D_i = P_i P_{i+1} ... P_k \; ; \; ...$$

méthode 2 (D. Musser) :

$C_1 := p.g.c.d.(F, F')$; $D_1 := P / C_1$; $i := 1$;

tant que $D_i \neq 1$ **faire**

début $D_{i+1} := p.g.c.d.(C_i, D_i)$; $C_{i+1} := C_i / D_{i+1}$; $P_i := D_i / D_{i+1}$; $i := i + 1$

fin.

En caractéristique zéro, le déroulement est à nouveau le suivant :

$$C_1 = P_2 P_3^2 \ldots P_k^{k-1} \; ; \; D_1 = P_1 P_2 \ldots P_k \; ; \; \ldots\ldots ;$$

$$C_i = P_{i+1} P_{i+2}^2 \ldots P_k^{k-i} \; ; \; D_i = P_i P_{i+1} \ldots P_k \; ; \; \ldots$$

méthode 3 (D. Yun) :

$Q := p.g.c.d.(F, F')$; $C_1 := P / G$; $D_1 := F' - C_1'$; $i := 1$;

tant que $C_i \neq 1$ **faire**

début $P_i := p.g.c.d.(C_i, D_i)$; $C_{i+1} := C_i / P_i$; $D_{i+1} := D_i / P_i - C_{i+1}'$; $i := i+1$ **fin** .

En caractéristique zéro, le déroulement est cette fois le suivant :

$$Q = P_2 P_3^2 \ldots P_k^{k-1} \; ; \; C_1 = P_1 P_2 \ldots P_k \; ;$$

$$D_1 = \sum_{i=1}^{k} (i-1) P_i' \prod_{j \neq i} P_j = P_1 . \left(\sum_{i=2}^{k} (i-1) P_i' \prod_{1 < j \neq i} P_j \right) ;$$

$$C_2 = P_2 P_3 \ldots P_k \; ; \; \ldots\ldots ;$$

$$C_h = P_h P_{h+1} \ldots P_k \; ;$$

$$D_h = \sum_{i=1}^{k} (i-h) P_i' \prod_{h < j \neq i} P_j = P_h . \left(\sum_{i=h+1}^{k} (i-h) P_i' \prod_{h < j \neq i} P_j \right) ; \; \ldots$$

Mais , aucun de ses trois algorithmes n'est valable en caractéristique non nulle.

Prenons en effet l'exemple du polynôme $F(X) = X^3 + X^2$ sur le corps $\mathbf{F}_2$.

Le premier procédé calcule

$F' = X^2$; $C_1 = X^2$; $D_1 = X + 1$; et indéfiniment $C_i = X^2$ ....

Le second algorithme calcule

$C_1 = X^2$; $D_1 = X + 1$; $D_2 = 1$; $C_2 = X^2$ et donne $F = (X + 1)(X^2)$, ce qui n'est pas la décomposition cherchée.

Le troisième algorithme calcule

$Q = X^2$; $C_1 = X + 1$; $D_1 = 0$; $C_2 = 1$ et donne comme le précédent

$F = (X + 1)(X^2)$.

L'algorithme qui figure plus haut se déroule ainsi pour cet exemple :

$Q = X^2$; $R = X + 1$; $Q' = 0$; $Q = (X)^2$ et $F = (X + 1)(X)^2$, ce qui fournit enfin la décomposition cherchée.

L'étude des coûts faite par Yun (loc. cit.) pour les méthodes 1 à 3 , démontre que - pour un corps de caractéristique zéro - la seconde méthode est plus économique que la première mais moins que la troisième.

4. Factorisation des polynômes sur un corps fini .

Soit F un polynôme unitaire, de degré d , à coefficients dans le corps $K = \mathbf{F}_q$ que l'on cherche à factoriser. Grâce à la procédure du paragraphe précédent, on peut se limiter au cas où F est quadratfrei, disons $F = P_1 \ldots P_k$ où les P_i sont des polynômes unitaires irréductibles deux à deux distincts, avec deg (P) = $d_i \geq 1$. La méthode qui suit est essentiellement due à Berlekamp.

1. Détermination du nombre de facteurs irréductibles .

On considère l'algèbre quotient

$$A = K[X] / (F(X)) .$$

D'après le théorème chinois, cette algèbre est isomorphe au produit

$$\prod_{i=1}^{k} K[X] / (P_i(X)) ,$$

mais comme chaque P_i est un polynôme irréductible de degré d_i , on a

$$K[X] / (P_i(X)) \cong K_i ,$$

où K_i est un corps de degré d_i au dessus de K et donc

$$K_i = \mathbf{F}_{q_i} \text{ , où } q_i = q^{d_i} .$$

En résumé,

$$A \cong K_1 \times \ldots \times K_k .$$

Soit $L : A \to A$ l'application qui à un élément α de algèbre A associe l'élément $\alpha^q - \alpha$; puisque K, et donc aussi A, est de caractéristique p l'application L est linéaire (la démonstration figure au paragraphe 1.1).

Par l'isomorphisme

$$A \cong K_1 \times \ldots \times K_k ,$$

l'application L induit sur chaque corps K_i l'application $L_i : x \to x^q - x$.

D'après le théorème 1, le noyau de L_i est égal à $\mathbf{F}_q$. Ainsi, le noyau de L est isomorphe à

$$\text{Ker } L \cong K^k ,$$

et en particulier, on a

$$\dim_K (\text{Ker } L) = k .$$

Pour déterminer le nombre de facteurs irréductibles de F sur le corps $\mathbf{F}_q$ il suffit donc de calculer la dimension du noyau de l'application L.

En conséquence, on a l'équivalence

$$F \text{ irréductible} \Leftrightarrow \dim_K (\text{Ker } L) = 1 ,$$

ce qui fournit un moyen rapide de tester l'irréductibilité d'un polynôme de $\mathbf{F}_q[X]$.

Plus généralement, considérons, pour $h \geq 1$, l'application de A dans elle-même

$$L_h : \alpha \to \alpha^{q^h} - \alpha ,$$

c'est encore une application linéaire, et elle induit sur chaque corps K_i l'application

$$L_{h,i} : x \to x^{q^h} - x .$$

Le noyau de $L_{h,i}$ est isomorphe à l'intersection $K_i \cap K^{(h)}$, où $K^{(h)}$ désigne le corps à q^h éléments ; il est donc égal au corps à

$$q^{(d_i, h)} \text{ éléments .}$$

En conclusion, on a la formule

$$\dim_K (\mathrm{Ker}\, L_h) = \sum_{i=1}^{k} (d_i , h) \ .$$

Par exemple,

$\dim_K (\mathrm{Ker}\, L_2)$ = # (facteurs irréd. de F) + # (fact. irréd. de F de degré pair) ,

où le symbole # est une abréviation pour "nombre" .

Le calcul de la dimension du noyau de L_h permet donc d'obtenir des informations précieuses sur le type de factorisation de F .

Du point de vue pratique, on représente l'application L_h par la matrice $Q_h - I$, où Q_h est la matrice $d \times d$ sur **K** dont la i-ième ligne représente

$$X^{q^{h(i-1)}} \quad \text{modulo } F(X) ,$$

sur la base $(1, X , \ldots , X^{d-1})$ de **A** . Le calcul de la matrice Q_h s'effectue en un nombre d'opérations dans **K** qui est de la forme $O (h\, d^2 \mathrm{Log}\, q)$.

Etant donnée une matrice **M** de taille $n \times n$ sur un corps, l'algorithme usuel de triangularisation de **M** permet de déterminer le rang de cette matrice et une base du noyau qui lui est associé en $O (n^3)$ opérations (voir par exemple Knuth, loc. cit., p. 388).

On peut donc calculer la dimension du noyau de L_h et une base de cet espace en au plus $O (d^3)$ opérations. En particulier, on peut tester si F est irréductible sur K en un nombre total de $O (d^3 + d^2 \mathrm{Log}\, q)$ opérations dans le corps K .

2. Factorisation complète .

La clef de l'algorithme de Berlekamp est le résultat suivant, dont la démonstration repose sur la décomposition de l'algèbre A , $A \cong K_1 \times \ldots \times K_k$ déjà utilisée plus haut (voir aussi la remarque à la fin du § 4 ci-dessous) .

THEOREME 2 . – On considère un polynôme F quadratfrei à coefficients dans le corps K à q éléments dont la décomposition en produit de facteurs irréductibles est

$$F = P_1 \ldots P_k .$$

Soit L l'application définie plus haut. Les propriétés suivantes ont lieu :

(i) Si G est un polynôme dont l'image modulo F appartient au noyau de L , on a la relation

$$F(X) = \prod_{y \in K} \text{p.g.c.d.} \left(F(X), G(X) - y \right) .$$

(ii) Si $G_1 , \ldots , G_{k-1} , G_k$ est une base du noyau de L , avec $G_k = 1$, alors pour tout couple d'indices i, j vérifiant $1 \leq i < j \leq k$ il existe un indice h , avec $h < k$, et deux éléments distincts y_i et y_j du corps K tels que le polynôme P_i divise $G_h - y_i$ tandis que le polynôme P_j divise $G_h - y_j$.

(iii) Si G_h est un polynôme comme en (ii) , avec $h < k$, il existe un élément y du corps K tel que le p.g.c.d. de $F(X)$ et de $G(X) - y$ soit un facteur non trivial du polynôme F .

> Soit G un polynôme dont l'image appartient au noyau de L . Par hypothèse le polynôme F divise $G^q - G$. Mais, d'après le théorème 1 , on a la relation

$$G(X)^q - G(X) = \prod_{y \in K} (G(X) - y) .$$

Donc le polynôme F (X) divise le membre de droite de la formule du théorème.

Inversement, chaque facteur du membre de droite divise F (X) , et – comme ces facteurs sont deux à deux premiers entre eux – le membre de droite divise le membre de gauche. D'où la première assertion.

Soit maintenant $G_1 , \ldots , G_{k-1} , G_k$ une base du noyau de L , avec $G_k = 1$. Dans l'isomorphisme $A \cong K_1 \times \ldots K_k$ déjà utilisé, l'image des éléments $G_1 , \ldots , G_k$ engendre le produit $K \times \ldots \times K$; donc un certain élément G_h s'envoie nécessairement sur un élément de A dont les i-ème et j-ième composantes y_i et y_j sont distinctes. Et on a bien sûr $h < k$ puisque $G_k = 1$.

Ce qui démontre la seconde propriété.

Soit G_h un polynôme comme en (iii) et soit $(y_1, \ldots , y_k)$ son image par l'isomorphisme $\mathrm{Ker}\ L \cong K \times \ldots \times K$. Comme G_h et G_k sont linéairement indépendants, les y_i ne sont pas tous égaux. Si ces y_i prennent exactement m valeurs notées $z_1 , \ldots , z_m$ (où on a $m \geq 2$) , alors le polynôme F s'écrit

$$(*) \qquad F(X) = \prod_{j=1}^{m} \text{p.g.c.d.} \left(F(X) , G_h(X) - z_j \right) ,$$

où chacun des facteurs de droite est non trivial .

D'où la dernière assertion. <

3. Coût de l'algorithme .

Résumons les différentes étapes qui conduisent à la factorisation d'un polynôme F à coefficients dans le corps $K = \mathbf{F}_q$. Le degré de F est noté d .

(i) On factorise F en un produit de polynômes quadratfrei. Ce qui permet de supposer F quadratfrei au cours des étapes ultérieures.

(ii) On détermine une base du noyau de l'application L définie plus haut. On note $G_1, ..., G_k$ une telle base, où $G_k = 1$. Alors k est le nombre de facteurs irréductibles de F .

(iii) On applique la formule (ii) du théorème 2 en prenant tout d'abord le polynôme G_1 , d'après ce théorème ceci fournit une factorisation non triviale de F. Tant qu'on n'a pas obtenu k facteurs distincts de F, on recommence le même travail avec les polynômes successifs G_2, G_3 , ... et si nécessaire jusqu'à G_{k-1} ; l'assertion (iii) du théorème 2 nous assure qu'en procédant de la sorte on obtiendra tous les facteurs irréductibles du polynôme F .

On vérifie facilement que la partie (i) nécessite au plus $O (d^3 + d \operatorname{Log} q)$ opérations dans le corps K .

Le calcul de la matrice qui représente L peut s'effectuer en $O (d^2 \operatorname{Log} q)$ opérations. Puis le calcul d'une base du noyau de L est possible en $O (d^3)$ opérations. Le nombre d'opérations nécessaires pour le deuxième pas est donc majoré par $O (d^3 + d^2 \operatorname{Log} q)$.

Il est clair que le calcul du p.g.c.d. de deux polynômes P et Q à coefficients dans le corps K est possible en $O (\deg P . \deg Q)$ opérations dans K . Par conséquent le troisième pas de l'algorithme nécessite au plus $O (q k d^2)$ opérations dans K .

En définitive, l'algorithme complet comporte $O(q\,d^3)$ opérations et c'est la dernière étape qui, en général, est la plus coûteuse. En particulier, lorsque q est grand, disons pour $q \geq 25$, cette dernière étape peut devenir trop dispendieuse. C'est pourquoi il est utile de trouver un moyen rapide de calcul des points z du corps K tels qui fournissent des termes non triviaux dans la formule notée (*) obtenue au cours de la démonstration du théorème 2, à savoir la formule

$$(*) \qquad F(X) = \prod_{z \in S} \text{p.g.c.d.}\,\big(F(X), G_h(X) - z\big),$$

où on a posé $S = \{ z_1, \ldots, z_m \}$. Le paragraphe qui suit est consacré à l'étude de la détermination rapide de cet ensemble S lorsque q est grand.

4. Cas où q est grand.

On suppose évidemment F non irréductible, donc $k \geq 2$. Pour déterminer l'ensemble S défini ci-dessus, H. Zassenhaus (*On Hensel factorisation I*, J. Number Theory, tome 1, 1969, p. 291-311) propose la méthode suivante.

Posons

$$H(X) = \prod_{z \in S} (X - z).$$

La relation de la fin du paragraphe précédent montre que le polynôme F divise le polynôme composé $H(G(X))$.

Ceci permet de déterminer H en cherchant le polynôme minimal de l'image de G dans l'algèbre A. Ensuite, on obtient l'ensemble S en calculant les racines du polynôme H.

Nous étudierons le problème du calcul des racines d'un polynôme sur un corps fini dans le paragraphe suivant.

Une autre méthode, que l'on retrouvera aussi dans le paragraphe suivant, a été proposée indépendamment d'une part par Cantor et Zassenhaus et d'autre part par Camion et consiste à se ramener au cas où les z_j valent 0 ou 1, autrement dit à déterminer des éléments idempotents de l'algèbre A, qui nécessairement appartiennent au noyau de L.

Supposons la caractéristique de K impaire. Partant d'un polynôme $G \neq 1$ dont l'image modulo F appartient au noyau de L, on obtient la racine carrée d'un idempotent de A en prenant l'image modulo F de $G^{(q-1)/2}$; en effet, si l'image de G dans le produit $K \times \ldots \times K$ est l'élément $(x_1, \ldots, x_k)$ celle de sa puissance $G^{(q-1)/2}$ est l'élément $(x_1^{(q-1)/2}, \ldots, x_k^{(q-1)/2})$ et on a bien sûr $x_i^{(q-1)/2} = 0$ ou ± 1. Si on note I l'ensemble des indices i tels que $x_i^{(q-1)/2} = 1$ et J l'ensemble des indices i tels que $x_i^{(q-1)/2} = -1$ alors on a les relations

$$\text{p.g.c.d.} (F , G^{(q-1)/2} - 1) = \prod_{i \in I} P_i ,$$

et

$$\text{p.g.c.d.} (F , G^{(q-1)/2} + 1) = \prod_{i \in J} P_i .$$

Et donc

$$\text{p.g.c.d.} (F , G) = \prod_{i \notin I \cup J} P_i .$$

L'une au moins des trois décompositions précédentes est non triviale lorsque le polynôme G vérifie la condition supplémentaire

$$G^{(q-1)/2} \neq \pm 1 \quad \text{modulo } F ,$$

et le coût du calcul de ces trois p.g.c.d. (y compris le calcul de $G^{(q-1)/2}$, pour lequel le polynôme G est supposé connu) est de $O (d^2 \operatorname{Log} q)$ opérations sur le corps K. La condition ci-dessus a lieu avec une probabilité $> 1/2$ puisque, sur les q^k éléments G du noyau de L il y en a seulement $2 ((q-1)/2)^k$ pour lesquels $G^{(q-1)/2} \equiv \pm 1$.

Remarque :

Tout le principe de l'algorithme de Berlekamp et de ses améliorations consiste à déterminer la structure de l'algèbre quotient

$$A = K[X] / (F(X)) .$$

En supposant comme plus haut que F est un polynôme quadratfrei dont la décomposition en facteurs irréductibles est $F = P_1 \dots P_k$, l'isomorphisme du théorème chinois est l'application

$$\varphi : A \rightarrow \prod_{i=1}^{k} K[X] / (P_i(X)) ,$$

définie par $\varphi(G) = (G \bmod P_1, \dots, G \bmod P_k)$.

On ne calcule jamais φ (son calcul équivaut à la connaissance des P_i) mais son existence seule a été largement utilisée.

Au départ, l'algèbre A est donnée par sa base "naturelle" $1, X, \dots, X^{d-1}$ et les calculs effectués consistent essentiellement à trouver des éléments G de A, dont l'image par φ possède certaines propriétés remarquables.

Dans la première partie de l'algorithme de Berlekamp, les G doivent s'envoyer sur une base du sous-espace $K \times \dots \times K$ du produit $K_1 \times \dots \times K_k$ (où K_i désigne le corps $K[X] / (P_i(X))$).

Dans l'étape finale, on cherche à déterminer les éléments y_i de K tels qu'un polynôme G donné du noyau de L s'envoie par φ sur le k-uple $(y_1, \dots, y_k)$ de l'ensemble produit $K \times \dots \times K$.

La méthode de Camion - Cantor - Zassenhaus revient à déterminer des polynômes tels que les y_i précédents soient égaux à 0 ou ± 1. Enfin la recherche des idempotents primitifs de l'algèbre A équivaut à la détermination de polynômes dont l'image par φ est la base canonique de l'espace vectoriel $K \times \dots \times K$ (un **idempotent primitif** d'un anneau est un idempotent $e \neq 0$ tel que pour tout autre idempotent e' on ait la relation $e.e' = 0$).

5. Décomposition en produit de facteurs irréductibles de degré donné .

Soit h un entier ≥ 1 , le polynôme

$$R_h(X) = \text{p.g.c.d.} \left(F(X) , X^{q^h} - X \right)$$

fournit le produit des facteurs irréductibles de F dont le degré divise h .

Pour effectuer le calcul de ce polynôme, on calcule d'abord

$$X^{q^h} \quad \text{modulo} \quad F(X) ,$$

ce qui est possible en $O (h \, d \, \text{Log} \, q)$ opérations, puis le p.g.c.d. en $O (d^2)$ opérations.

De plus, si le premier calcul a été effectué pour l'entier h , le même calcul pour l'entier suivant $h + 1$ est possible en $O (d \, \text{Log} \, q)$ opérations. Pour h variant de 1 à H on obtient donc un total de $O (d H \, \text{Log} \, q + d^2 H)$ opérations.

On peut aussi noter que le calcul des polynômes R_h pour $1 \leq h \leq H$ permet d'obtenir facilement le produit S_h des facteurs irréductibles de F dont le degré est égal à h , ceci pour $1 \leq h \leq H$; la formule est

$$S_h = \frac{R_h}{\displaystyle\prod_{j \mid h \, ; \, j < h} S_j} ,$$

ou encore

$$S_h = \frac{R_h}{\text{p.g.c.d.} \left(R_h , \displaystyle\prod_{j \mid h \, ; \, j < h} R_j \right)} .$$

6. La méthode de MacEleice .

La référence de l'algorithme de R. J. MacEleice que nous présentons ici est *Factorization of polynomials over finite fields* , Math. of Computation, t. 23, n° 108, 1969, pp. 861-868. Démontrons d'abord un lemme, puis une proposition sur laquelle repose cet algorithme.

LEMME 2 . – Soient F et G deux polynômes quadratfrei à coefficients dans $\mathbf{F}_q$ tels que F divise G . On pose $A_F = \mathbf{F}_q[X]/(F)$ et $A_G = \mathbf{F}_q[X]/(G)$ et on note respectivement L_F et L_G les applications L correspondantes (définies au § 4.1). Et soit $\pi : A_G \to A_F$ la surjection canonique. Alors on a

$$\text{Ker } L_F = \pi(\text{Ker } L_G) .$$

> Soient $P_1, ..., P_r$ les diviseurs irréductibles de G , numérotés de telle sorte que l'on ait $F = P_1 ... P_k$. Alors les idempotents primitifs $e_1, ..., e_r$ de A_G sont les images modulo G de polynômes E_i qui vérifient

$$E_i \equiv \delta_{ij} \pmod{P_j} \quad \text{pour} \quad j = 1, ..., r .$$

Il est clair que les éléments $\pi(E_1), ..., \pi(E_k)$ sont les idempotents primitifs de A_F. D'où la conclusion. <

PROPOSITION 6 . – Soit F un polynôme sur le corps $\mathbf{F}_q$ qui vérifie $F(0) \neq 0$. Soit t la **période** de F (c'est à dire le plus petit entier j tel que F divise $X^j - 1$). Alors les polynômes $T_i = T_{i,F}$ définis, pour $i = 1, ..., t - 1$, par les formules

$$T_i(X) = X^i + X^{iq} + X^{iq^2} + ... + X^{iq_i} \quad \text{modulo } F(X),$$

où l'entier q_i est la plus petite puissance de q telle que le polynôme F divise $X^i - X^{iq_i}$, engendrent le noyau de l'application L calculée au cours de l'algorithme de Berlekamp.

> Par définition même il est clair que chacun des T_i appartient au noyau de L.

Supposons d'abord F égal à $X^t - 1$, et posons $H = X^t - 1$.

Posons $q_i = q^{m_i - 1}$, alors m_i est le plus petit entier tel que t divise le produit $i\,q^{m_i - 1}$.

Les exposants de $T_{i,H}$ sont donc les différents résidus modulo t des m_i nombres i, $i\,q$, $i\,q^2$, ...Considérons maintenant un polynôme G appartenant au noyau de L_H. On a alors $G^q \equiv G \pmod{X^t - 1}$, et si $G(X) = a_0 + a_1 X + \ldots + a_{t-1} X^{t-1}$ on en déduit la relation $a_n = a_{n'}$ s'il existe $u \in \mathbf{Z}$ tel que l'on ait

$$n \equiv n' q^u \quad \text{modulo } t ;$$

ce qui montre bien que G est une combinaison linéaire des polynômes $T_{i,H}$.

Soit maintenant F un diviseur strict de H. D'après le lemme 2 et la démonstration ci-dessus, la famille des polynômes $T_{i,H}$ modulo F, $i = 1, \ldots, t - 1$ engendre le noyau de L_F. Mais il est facile de voir que chaque $T_{i,H}$ est de la forme $T_{i,H} = a\,T_{i,F}$, où a est un entier dépendant de i. D'où la conclusion. <

Ce résultat est surtout utile lorsque t est petit. Ceci est le cas quand F a tous ses facteurs irréductibles de même degré, et on peut réaliser cette condition grâce à l'algorithme du paragraphe précédent.

Remarque : Supposons que le polynôme F soit le produit de k facteurs irréductibles distincts, de même degré d', et soit t la période de F. Alors t divise $q^{d'} - 1$. Soit t' un diviseur de t tel que le quotient $r = t / t'$ soit premier. Il existe alors au moins un facteur irréductible de F dont la période ne divise pas t'. Donc – à moins que tous les facteurs irréductibles de F aient une période égale à t – le polynôme

$$\text{p.g.c.d.}\,(F(X),\ X^{t'} - 1)$$

constitue un facteur non trivial de F pour au moins une des valeurs possibles de t'.

5. Recherche des racines d'un polynôme dans un corps fini .

1. Une première réduction .

Comme nous l'avons déjà vu, le calcul du p.g.c.d. des polynômes $F(X)$ et $X^q - X$ permet de se ramener au cas de la recherche des racines d'un polynôme qui se factorise complètement dans le corps $\mathbf{F}_q$. Nous supposerons en outre que le polynôme F ne s'annule pas en zéro.

On peut aussi noter que les procédures décrites dans l'article de Berlekamp, *Factoring polynomials over large finite fields* , Math. of Computation, T. 24, n° 111, 1970, pp. 713-735, § 5 et 6 , permettent de se ramener au cas de la recherche des racines d'un polynôme F à coefficients dans le corps premier $\mathbf{F}_p$ et qui se factorise complètement dans ce corps.

2. Cas des polynômes qui se décomposent dans $\mathbf{F}_q$.

Considérons donc un polynôme F de la forme

$$F(X) = \prod_{i=1}^{d} (X - s_i) ,$$

où les s_i sont des éléments non nuls (inconnus) du corps $\mathbf{F}_q$. La méthode de factorisation en produit de polynômes quadratfrei permet de se ramener au cas où les s_i sont distincts, ce que nous supposerons aussi.

D'après une remarque déjà rencontrée, on peut écrire

$$F(X) = \text{p.g.c.d.}\left(F(X), X^{(q-1)/2} - 1\right) . \text{ p.g.c.d.}\left(F(X), X^{(q-1)/2} + 1\right),$$

formule qui sépare les racines s_i suivant qu'elles sont ou non des carrés dans $\mathbf{F}_q$. Si cette décomposition est triviale, on remplace le polynôme $F(X)$ par un polynôme de la forme $F(X - a)$. On peut considérer que la probabilité pour qu'une valeur de a conduise à une décomposition triviale est voisine de 2^{-d+1}. En général, on aboutit à une décomposition non triviale de F au bout d'un très petit nombre de choix de la valeur a de la translation.

Exemple : Considérons le polynôme

$$F(X) = X^4 - 3X^3 - 3X^2 - 3X + 1$$

sur le corps $\mathbf{F}_7$.

On a

$$(F(X), X^3 + 1) = (-3X^3 - 3X^2 + 3X + 1, X^3 + 1)$$
$$= (-3X^2 + 3X - 3, X^3 + 1) = X^2 - X + 1,$$

et

$$F(X) = (X^2 - X + 1)(X^2 - 2X + 1).$$

D'une part on a

$$(X^2 - 2X + 1) = (X - 1)^2,$$

et d'autre part, le polynôme du second degré $X^2 - X + 1$ est congru modulo 7 au polynôme $X^2 + 6X + 1$ dont le discriminant est égal à 4 modulo 7, donc

$$X^2 + 6X + 1 = (X - 3)(X - 5).$$

D'où la décomposition

$$F(X) = (X - 1)^2 (X - 3)(X + 2).$$

3. Résolution de l'équation binomiale $X^d = a$.

Soit K un corps fini possédant q éléments. On considère une équation, que l'on notera E , de la forme $x^d = a$ où a est un élément non nul du corps K , et on cherche à déterminer toutes les solutions de E qui appartiennent à ce corps.

Soit h l'ordre de l'élément a dans le groupe K^* des éléments non nuls de K . Posons $k = (q - 1) / h$. Le groupe K^* est cyclique et admet un générateur tel que l'on ait $a = z^k$. Cherchons x sous la forme $x = z^u$, où u est inconnu. L'équation E est équivalente à la congruence

$$u\,d \equiv k \quad \text{modulo } q - 1 .$$

Soit e le p.g.c.d. des entiers d et $q - 1$. Posons $d = e\,d'$ et $q - 1 = e\,q'$. Pour que l'équation E possède une solution dans K il est nécessaire que e divise k . Inversement si $k = e\,k'$, k' entier, alors la congruence précédente équivaut à $u\,d' \equiv k'$ modulo q' et l'équation E possède donc e solutions dans K . Notons enfin que la condition e divise k équivaut à la relation $a^{d'} = 1$, condition que l'on peut tester en au plus $O(\text{Log } q)$ multiplications dans le corps K . Dans la suite, on supposera toujours cette condition réalisée.

Pour résoudre l'équation E , on peut d'abord résoudre l'équation $y^e = a$ puis l'équation $x^{d'} = y$. Ceci ramène le problème étudié au deux cas suivants :

(i) $(d , q - 1) = 1$,

(ii) d divise $q - 1$.

Le premier cas est très facile à traiter : soient u et v deux entiers tels que l'on ait

$$u d + v(q-1) = 1 \text{ , avec } 1 \leq u < q \text{ ;}$$

alors

$$x = a^u$$

est une solution de E (en effet $(a^u)^d = a^{1-v(q-1)} = a$), de plus E ne possède pas d'autre solution dans le corps K . Le calcul de l'entier u puis celui de a^u peuvent tous deux s'effectuer en O (Log q) opérations.

Exemple : Si q est congru à -1 modulo 6 , l'équation $X^3 = a$ est résoluble dans le corps $\mathbf{F}_q$ en O (Log q) opérations. Plus généralement on peut trouver une solution dans $\mathbf{F}_q$ de toute équation cubique en O (Log q) opérations, au moins quand on connait un élément de K* qui n'est pas un carré (utiliser les formules de Cardan et la résolution de l'équation $X^2 = b$ donnée ci-dessous) .

Etudions maintenant le cas (ii) . Il est utile de considérer d'abord le cas le plus simple de l'équation $x^2 = a$, avec q impair et $a^{(q-1)/2} = 1$.

La présentation donnée ici s'inspire de l'article de Lehmer , *Computer Technology Applied to the Theory of Numbers* , Studies in Number Theory, pp. 117-151, ed. W. J. Leveque, Englewood Cliff, Prentice Hall, 1969 , qu'elle étend au cas où q n'est pas premier et auquel elle apporte quelques simplifications.

Si q est de la forme $4k + 3$, les solutions sont $x = \pm a^{k+1}$, en effet on a alors la relation $x^2 = a^{2k+2} = a^{1+(q-1)/2} = a$. D'où un calcul des solutions en O (Log q) opérations.

Dans le cas général où q est de la forme $4k + 1$, la proposition suivante fournit un moyen de calcul des solutions.

PROPOSITION 7 . – Soit q une puissance d'un nombre premier , avec q de la forme $4k+1$. Soient a et b deux entiers tels que l'élément a soit un carré dans $\mathbf{F}_q^*$ mais que $b^2 - 4a$ n'en soit pas un. Soit enfin v_n la suite récurrente définie par

$$v_0 = 2 \ , \ v_1 = b \ , \ v_n = b\, v_{n-1} - a\, v_{n-2} \quad \text{pour } n \geq 2 \ .$$

Alors les solutions de l'équation $x^2 = a$ dans $\mathbf{F}_q$ sont $x = \pm (1/2)\, v_{(q+1)/2}$.

> Soit K' le corps de cardinal q^2 et soient α et β les racines dans K' de l'équation

$$X^2 - bX + a = 0 \ .$$

On vérifie aisément que l'on a $v_n = \alpha^n + \beta^n$, pour tout $n \geq 0$. D'où la relation

$$v_{(q+1)/2}^2 = (\alpha^{(q+1)/2} + \beta^{(q+1)/2})^2 = \alpha^{q+1} + \beta^{q+1} + 2(\alpha\beta)^{(q+1)/2} \ .$$

La transformation $y \rightarrow y^q$ laisse invariante l'équation ci-dessus, α^q est donc une de ses racines ; or $\alpha^q \notin \mathbf{F}_q$ (puisque $b^2 - 4a$ n'est pas un carré dans le corps $\mathbf{F}_q$), donc $\alpha^q = \beta$. De même $\beta^q = \alpha$. D'autre part, a étant un carré non nul de $\mathbf{F}_q$, on a la relation $a^{(q-1)/2} = 1$. En définitive,

$$v_{(q+1)/2}^2 = 2\alpha\beta + 2a^{(q+1)/2} = 4a \ . \ <$$

On peut calculer $v_{(q+1)/2}$ en $O(\text{Log } q)$ opérations grâce à l'une quelconque des formules (faciles à vérifier)

$$v_{2m} = v_m^2 - 2a^m \qquad \text{ou} \qquad \begin{pmatrix} v_{m+1} \\ v_m \end{pmatrix} = \begin{pmatrix} b & -a \\ 1 & 0 \end{pmatrix}^m \begin{pmatrix} v_1 \\ v_0 \end{pmatrix} \ .$$

On a donc montré que si une équation du second degré sur le corps $\mathbf{F}_q$ est résoluble dans ce corps, alors on peut trouver ses solutions en $O(\text{Log } q)$ opérations – à condition de connaître un élément non résidu quadratique de ce corps.

Passons maintenant au cas général de la condition (ii) . Nous allons donner une procédure qui s'inspire de celle de Gauss, *Disquisitiones arithmeticae* , Fleischer, Leipzig, 1801, § 67-68 . On suppose donc que l'exposant d divise $q - 1$ et que a vérifie $a^{(q-1)/d} = 1$. On supposera aussi que d est premier, ce qui n'ôte rien à la généralité puisque toute extraction de racine se ramène à une suite d'extractions de racines d'ordre premier. Posons maintenant $q - 1 = d^r q'$ et $k = d^s k'$, où d ne divise ni q' ni k' . Supposons que l'on connaisse un élément y de K* d'ordre d^r. Soient w et t deux entiers tels que l'on ait $w d = 1 + t q'$. Si x est une solution de E alors on a la relation $(x a^{-w})^d = a^{-tq'}$ dans laquelle le membre de droite a un ordre qui divise l'entier d^r. Les solutions x de l'équation E sont donc de la forme

$$x = y^j a^w \text{ , où w vérifie } w d \equiv 1 \text{ modulo } q' .$$

Posons $w d = 1 + t q'$. On a $y = z^{q' m}$, où d ne divise pas l'entier m , z désignant le générateur de K* choisi plus haut. Il s'agit donc de trouver un entier j tel que l'on ait $m j + t d^{s-1} k' \equiv 0$ modulo d^{r-1}. Il y a donc au plus d^{r-1} essais de l'entier j à effectuer. Enfin, si x est une solution dans K toutes les autres solutions de l'équation E qui appartiennent à ce corps sont de la forme

$$x' = y^{i d^{r-1}} x \quad \text{pour } i = 0, 1, \ldots , d - 1 .$$

On trouve donc toutes les solutions de l'équation E en $O (d^r \text{ Log } q)$ opérations dans le corps K , à condition de connaître un élément de K* qui est d'ordre d^r.

Résumons cette étude.

PROPOSITION 8 . – Soit d un nombre premier qui divise $q - 1$. On suppose que l'on connait un élément du corps $\mathbf{F}_q$ d'ordre d^r, la plus grande puissance de d qui divise $q - 1$. Soit a un élément non nul de $\mathbf{F}_q$ qui vérifie $a^{(q-1)/d} = 1$. Alors, on peut calculer toutes les solutions de l'équation $x^d = a$, $x \in \mathbf{F}_q$, en $O (d^r \text{ Log } q)$ opérations dans le corps fini $\mathbf{F}_q$.

Exercices

1. Estimation de $\varphi(n)$.

1°) Démontrer que la série

$$\sum_{n \geq 2} \left(\operatorname{Log} \frac{1}{1 - 1/n} - \frac{1}{n} \right)$$

est convergente.

2°) Soit $(c_n)_{n \geq 1}$ une suite de nombres réels. On pose

$$C(t) = \sum_{n \leq t} c_n \ .$$

Soit $f : [1, \infty[\to \mathbf{R}$ une fonction. Démontrer la relation

$$\sum_{n \leq x} c_n f(n) = \sum_{n \leq x-1} C(n) \left(f(n) - f(n+1) \right) + C(x) f([x]) \ .$$

En déduire que, dans le cas où f est continûment dérivable, on a

$$\sum_{n \leq x} c_n f(n) = C(x) f(x) - \int_1^x C(t) f'(t) \, dt \ .$$

3°) Démontrer que si p est un nombre premier, et si p^h divise $n!$ alors on a l'inégalité $h \geq (n/p) - 1$. En déduire la majoration

$$\sum_{p \leq x} \frac{\operatorname{Log} p}{p} \leq \operatorname{Log} x + O(1) \ .$$

4°) Démontrer la majoration

$$\sum_{p \mid n} \frac{1}{p} \leq 1 + \int_1^x \frac{(\operatorname{Log}(t) + c)}{t (\operatorname{Log} t)^2} \, dt \ , \text{ où } c \text{ est une constante .}$$

5°) En déduire la minoration

$$\frac{\varphi(n)}{n} \geq \frac{c'}{\operatorname{Log} \operatorname{Log} n} \ , \text{ où } c' \text{ est une constante .}$$

2. Résolution de l'équation $x^p = a$ dans un groupe fini .

Soit G un groupe fini de cardinal n et soit p un nombre premier qui divise n , de sorte que $n = p^r n'$, où p ne divise pas n' .

1°) On pose $G(p) = \{ x \in G ; \exists k$, ordre $(x) \mid p^k \}$. Démontrer que

$$G(p) = \{ x \in G ; x^{p^r} = 1 \} ,$$

où 1 désigne l'élément neutre de G .

2°) Soient a et x deux éléments de G tels que $x^p = a$.

(i) Démontrer que $a^{n/p} = 1$.

(ii) Soit u un entier tel que $u\,p \equiv 1 \pmod{n'}$. Démontrer que $x\,a^{-u}$ appartient à $G(p)$.

(iii) En déduire que la connaissance de $G(p)$ permet d'obtenir une procédure de résolution de l'équation $x^p = a$ dans G , a étant donné, en un nombre d'opérations dans G majoré par $O(p^r \operatorname{Log} n)$.

(iv) Dans le cas particulier où a vérifie la relation $a^{n'} = 1$, démonter que l'élément $x = a^u$ est une solution de l'équation $x^p = a$.

3. Dénombrements dans $\mathbf{F}_q[X]$.

A un sous-ensemble E de $\mathbf{F}_q[X]$, on associe une série formelle, appelée **fonction génératrice** de E,

$$S(t) = S_E(t) = \sum_{m=0}^{\infty} a_m t^m \quad , \text{ où } \quad a_m = \text{Card}\{ F \in E ; \deg F = m \} .$$

1°) Démontrer les propriétés suivantes :

(i) si $E = \{ F \in \mathbf{F}_q[X] ; F \text{ unitaires} \}$ alors

$$S(t) = S_E(t) = \frac{1}{1 - qt} ,$$

(ii) si E est l'union disjointe de deux ensembles E' et E" alors

$$S_E(t) = S_{E'}(t) + S_{E''}(t) .$$

2°) Soient $E_1, E_2, \ldots, E_n$ des ensembles de polynômes unitaires tels que

$$(F \in E_i , G \in E_j , i \neq j) \Rightarrow \text{p.g.c.d.}(F, G) = 1 .$$

On désigne par E l'ensemble des polynômes de la forme $F_1 \ldots F_n$ où $F_i \in E_i$ pour tout i. Démontrer que

$$S_E(t) = \prod_{i=1}^{n} S_i(t) ,$$

où S_i est la fonction génératrice de E_i pour $i = 1, 2, \ldots, n$.

Généraliser ce résultat au cas d'une suite infinie $(E_i)_{i \geq 0}$ de parties de $\mathbf{F}_q[X]$ possédant certaines propriétés convenables.

3°) Soient, pour $m = 1, 2, \ldots$, des ensembles R_m constitués par i_m polynômes irréductibles de degré m, unitaires. Soit E l'ensemble des polynômes unitaires dont tous les facteurs irréductibles sont dans l'union R des R_m.

Démontrer la relation

$$S_E(t) = \prod_{m=1}^{\infty} (1 - t^m)^{-i_m} .$$

En déduire la formule

$$\frac{1}{1 - q\,t} = \prod_{m=1}^{\infty} \left(\frac{1}{1 - t^m} \right)^{I_m} ,$$

où I_m est le nombre de polynômes de $\mathbf{F}_q[X]$, irréductibles, unitaires et de degré m.

Soit E' l'ensemble des polynômes unitaires qui sont produits de facteurs irréductibles, tous distincts, et appartenant à R.

Démontrer que

$$S_{E'}(t) = \prod_{m=1}^{\infty} (1 - t^m)^{i_m} .$$

4°) Démontrer que la fonction génératrice de l'ensemble des carrés des polynômes unitaires est

$$\frac{1}{1 - q\,t^2} .$$

5°) (référence : E. R. Berlekamp , *Algebraic Coding Theory* , § 3.3)

Soit Q l'ensemble des polynômes unitaires et quadratfrei de $\mathbf{F}_q[X]$, et soient

$$Q' = \{ F \in Q ;\ \omega(Q) \text{ pair} \} \quad \text{et} \quad Q'' = \{ F \in Q ;\ \omega(Q) \text{ impair} \} .$$

Démontrer les relations suivantes

$$S_Q(t) = \prod_{m=1}^{\infty} (1+t^m)^{I_m} = \frac{1-qt^2}{1-qt} ,$$

$$S_{Q'}(t) - S_{Q''}(t) = \prod_{m=1}^{\infty} (1-t^m)^{I_m} = 1 - qt .$$

En déduire que, pour $m \geq 2$, le nombre de polynômes quadratfrei de degré m ayant un nombre pair de facteurs irréductibles et le nombre de ceux ayant un nombre impair de facteurs irréductibles sont égaux.

Démontrer les formules

$$S_{Q'}(t) = \frac{1 - qt + (1-qt^2)/(1-qt)}{2} ,$$

$$S_{Q''}(t) = \frac{-1+qt + (1-qt^2)/(1-qt)}{2} .$$

6°) Démontrer que la fonction génératrice de l'ensemble des polynômes unitaires qui n'ont pas de racine dans le corps $\mathbf{F}_q$ est

$$\frac{(1-t)^q}{1-qt} = \prod_{m=2}^{\infty} (1-t^m)^{-I_m} .$$

Généraliser ce résultat à l'ensemble des polynômes unitaires qui n'ont pas de facteur irréductible de degré $\leq k$, où k est un entier positif fixé.

4. Polynômes cyclotomiques.

On désigne par Φ_n le polynôme cyclotomique d'ordre n, et – pour des raisons de commodité – on pose $F(n;X) = \Phi_n(X)$.

1°) Démontrer les formules suivantes

si p est premier et ne divise pas m, $F(mp^k;X) = F(mp;X^{p^{k-1}})$, pour $k \geq 1$,

$$F(mp;X) = \frac{F(m;X^p)}{F(m;X)} ,$$

n impair, $n \geq 3 \Rightarrow F(2n;X) = F(n;-X)$.

2°) En déduire les relations

$$\Phi_n(1) = \begin{cases} 0 & \text{si } n = 1, \\ p & \text{si } n = p^k,\ k \geq 1, \\ 1 & \text{si } \omega(n) \geq 2, \end{cases}$$

et

$$\Phi_n(-1) = \begin{cases} 0 & \text{si } n = 2, \\ -2 & \text{si } n = 1, \\ 2 & \text{si } n = 2^k,\ k \geq 2, \\ p & \text{si } n = 2n',\ \text{où } n' \text{ est une puissance de } p,\ n' > 1, \\ 1 & \text{sinon.} \end{cases}$$

3°) Soit n un entier ≥ 2 et soit d un diviseur de n, $1 \leq d < n$. Démontrer que le polynôme $\Phi_n(X)$ divise $(X^n - 1)/(X^d - 1)$.

4°) On suppose les entiers n et q premiers entre eux. Démontrer que le polynôme cyclotomique Φ_n se décompose alors dans le corps $\mathbf{F}_q$ en $\varphi(n)/d$ facteurs irréductibles, de degré d, où d est le plus petit entier > 0 tel que $q^d \equiv 1 \pmod{n}$.

5. Congruences de Lucas .

Soit p un nombre premier. Les congruences qui suivent sont toutes modulo p , elles ont été démontrées pour la première fois par Lucas.

1°) Soit a un entier, $0 \leq a < p$. Démontrer les congruences

$$(1+X)^{np+a} \equiv (1+X^p)^n (1+X)^a .$$

2°) Soit b un entier , $0 \leq b < p$. En égalant les coefficients de X^{kp+b} dans la formule précédente, démontrer la relation

$$\binom{np+a}{kp+b} \equiv \binom{n}{k}\binom{a}{b} \quad (\text{donc} \equiv 0 \text{ si } a<b).$$

3°) Conclure que si l'écriture de n en base p est $n = (n_j \ldots n_1)$ et celle de k est de la forme $k = (k_j \ldots k_1)$ (où les k_i sont ≥ 0) alors on a

$$\binom{n}{k} \equiv \binom{n_1}{k_1} \cdots \binom{n_j}{k_j} .$$

6. Soit L le corps fini à q^n éléments. Démontrer que le nombre de n - uples d'éléments de L qui sont des bases de L sur le corps $\mathbf{F}_q$ est égal à

$$(q^n - 1)(q^n - q) \ldots (q^n - q^{n-1}) .$$

7. Extensions de $\mathbf{F}_q$.

Le corps $\mathbf{F}_q$ sera noté K . On considère un entier n fixé ≥ 2 , et on désigne par L le corps fini à q^n éléments. On fixe aussi un polynôme $f \in K[X]$, irréductible sur K et de degré n .

1°) Démontrer que le polynôme f est quadratfrei.

2°) Démontrer qu'il existe $\alpha \in L$ tel que $f(\alpha) = 0$.

Démontrer aussi que, pour un tel α , on a $L = K[\alpha]$.

3°) Démontrer que f se décompose en facteurs linéaires dans le corps L et que ses racines sont les n éléments distincts de L :

$$\alpha , \alpha^q , \alpha^{q^2} , \ldots , \alpha^{q^{n-1}} .$$

4°) Si α et β sont deux racines de f dans L , démontrer l'égalité

$$\text{ordre}(\alpha ; L^*) = \text{ordre}(\beta ; L^*) .$$

5°) Démontrer que l'ensemble G des automorphismes $\sigma : L \to L$ qui vérifient la condition $\sigma(x) = x$ pour tout élément x du corps K est un groupe.

Soit j un entier, $0 \leq j < n$. Démontrer qu'il existe une seule application K - linéaire φ de L dans lui-même qui vérifie

$$\varphi(\alpha) = \alpha^{q^j} \quad \text{et} \quad \varphi(\alpha^i) = \varphi(\alpha)^i \quad \text{pour tout } i \geq 0 ;$$

on la notera σ_j .

Démontrer que σ_j appartient à G puis que $G = \{ \sigma_0 , \sigma_1 , \ldots , \sigma_{n-1} \}$.

En déduire que G est un groupe cyclique isomorphe au groupe additif $\mathbf{Z} / n\mathbf{Z}$.

6°) Soit $Tr : L \to L$ l'application K - linéaire définie par les relations

$$Tr(\alpha^i) = \alpha^i + \alpha^{iq} + \ldots + \alpha^{iq^{n-1}} , \quad \text{pour } i = 0, 1, \ldots, n-1 .$$

Démontrer que $Tr(L) = K$ et que, pour tout élément β de L on a

$$Tr(\beta^p) = Tr(\beta)^p \quad \text{et} \quad Tr(\beta^q) = Tr(\beta) .$$

Si $\beta \in L$ démontrer que l'application T_β de L dans lui-même définie par

$$T_\beta(x) = Tr(\beta x) \quad \text{pour tout } x \text{ de } L$$

est une application K - linéaire dont l'image est contenue dans le corps K .

Si β et γ sont deux éléments distincts de L , démontrer que les applications T_β et T_γ sont différentes.

En déduire que si $T : L \to K$ est une application K - linéaire alors il existe β dans le corps L tel que $T = T_\beta$.

Soit $\alpha_1, \ldots, \alpha_n$ une base de L en tant que K - espace vectoriel. Démontrer qu'il existe une base $\beta_1, \ldots, \beta_n$ de L telle que l'on ait

$$Tr(\alpha_i \beta_j) = \delta_{ij}$$ (comme d'habitude, δ_{ij} est le symbole de Kronecker) .

7°) Pour $\beta \in L$ on définit le vecteur $V(\beta) = (\beta_1, \ldots, \beta_n)$ où

$$\beta_i = \beta^{q^{i-1}} \qquad \text{pour } i = 1, 2, \ldots, n .$$

Démontrer que $\alpha_1, \ldots, \alpha_n$ est une base de L (en tant que K - espace vectoriel) si, et seulement si, les vecteurs $V(\alpha_1), \ldots, V(\alpha_n)$ sont K - linéairement indépendants.

En déduire l'équivalence suivante

$$\alpha_1, \ldots, \alpha_n \text{ base de } L \iff \det(A) \neq 0 \text{ où } A = (\alpha_{ij}) \text{ avec } \alpha_{ij} = \alpha_i^{q^{j-1}} .$$

8°) Si $\alpha_1, \ldots, \alpha_n$ sont des éléments de L, on pose

$$b_{ij} = \mathrm{Tr}(\alpha_i \alpha_j) \quad \text{et} \quad B = (b_{ij}) \quad , \ 1 \leq i, j \leq n ;$$

démontrer la relation

$$B = {}^tA\,A \qquad (\text{où } {}^tA \text{ est la matrice transposée de } A).$$

En déduire le critère suivant

$$\alpha_1, \ldots, \alpha_n \text{ base de } L \iff \det(B) \neq 0 \ .$$

8. Matrice compagnon.

Soit K un corps et soit f un polynôme unitaire à coefficients dans ce corps, donné par la formule

$$f(X) = X^n - a_{n-1} X^{n-1} - a_{n-2} X^{n-2} - \ldots - a_0 .$$

On considère la matrice $A = A_f$ définie par

$$A = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & \ldots & 0 & a_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & 1 & a_{n-1} \end{pmatrix} .$$

1°) On désigne par e_i, $1 \leq i \leq n$, le vecteur-colonne de composantes $(\delta_{ij})_{1 \leq j \leq n}$.

Démontrer les formules

$$A(e_i) = e_{i+1} \quad \text{pour } 1 \leq i < n \quad \text{et} \quad A(e_n) = a_0 e_1 + a_1 e_2 + \ldots + a_{n-1} e_n .$$

Démontrer que les matrices I, A, ... et A^{n-1} sont linéairement indépendantes sur le corps K et que l'on a $F(e_1) = 0$ où

$$F = f(A) = A^n - a_{n-1} A^{n-1} - a_{n-2} A^{n-2} - \ldots - a_0 I .$$

En déduire que F est nulle et que f est le polynôme minimal de la matrice A.

2°) Soit $K[A]$ l'ensemble des matrices qui sont des combinaisons linéaires à coefficients dans K des puissances de la matrice A et de la matrice identité I.

Démontrer que l'application

$$\varphi : K[X]/(f(X)) \rightarrow K[A]$$

qui, pour $i = 1, 2, ..., n-1$, associe A^i à X^i et qui envoie 1 sur la matrice I est un isomorphisme d'anneaux et de K-espaces vectoriels.

En déduire en particulier que si K est un corps fini et L est une extension finie de K alors on peut représenter L comme un certain anneau de matrices sur K. Donner un tel exemple pour $K = \mathbf{F}_3$ et $L = \mathbf{F}_9$.

3°) Démontrer que pour tout entier $k \geq 1$ on a l'équivalence

$$f(X) \text{ divise } X^k - 1 \Leftrightarrow A^k = I .$$

9. Corps de décomposition.

Soit K le corps $\mathbf{F}_q$ et soit f un polynôme à coefficients dans K de degré $n \geq 2$. On désigne par L la plus petite extension du corps K dans laquelle le polynôme f se décompose en produits de polynômes du premier degré (une telle extension existe, voir l'exercice n° 38 du troisième chapitre). On désigne par $r = r(f)$ le degré de L en tant qu'espace vectoriel sur le corps K.

1°) Soient $f_1, ..., f_k$ les polynômes unitaires, irréductibles sur K, qui divisent f. Démontrer la relation

$$r(f) = \text{p.p.c.m.}(d_1, ..., d_k) \quad \text{où} \quad d_i = \deg(f_i), \ i = 1, ..., k .$$

2°) Démontrer que l'on a

$$\max \{ r(f) ; f \in K[X], \deg(f) = n \} = g(n)$$

où

$$g(n) = \max \{ \text{p.p.c.m.} (m_1 , \ldots , m_s) ; s , m_1, \ldots, m_s , m_1 + \ldots + m_s \leq n \} .$$

Démontrer l'estimation

$$\text{Log } g(n) \sim \sqrt{n \text{ Log } n} .$$

[Voir l'article de J. L. Nicolas .– *Ordre maximal d'un élément du groupe S_n des permutations et " highly composite numbers "* , Bull. Soc. Math. France, t. 97, n° 108, 1969, p. 861-868]

3°) Soit, comme dans la première question, k le nombre de facteurs irréductibles du polynôme f .

Démontrer la majoration

$$r(f) \leq \left(\frac{n}{k} \right)^k .$$

En déduire que, pour tout $\varepsilon < 0$ fixé et pour tout entier n assez grand, on a " en général "

$$r(f) \leq \exp \{ (1 + \varepsilon) (\text{Log } n)^2 \} .$$

[Remarque : On peut montrer que la minoration $r(f) \geq \exp \{ (1 - \varepsilon) (\text{Log } n)^2 \}$ est aussi vraie " en général " ; mais la preuve est beaucoup plus difficile. Voir l'article de M. Mignotte et J. L. Nicolas .– *Statistiques sur $F_q[X]$* , Ann. Inst. Henri Poincaré, v. XIX, n° 2 , 1983, pp. 113 - 121).]

10. Période d'un polynôme .

On note K le corps fini $\mathbf{F}_q$. Et on considère un polynôme f non constant de degré égal à n, à coefficients dans K et qui vérifie $f(0) \neq 0$.

1°) Démontrer qu'il existe un entier $k > 0$ tel que $f(X)$ divise $X^k - 1$.

Le plus petit de ces entiers est appelé la **période** de f, et noté $per(f)$.

Démontrer la majoration

$$per(f) \leq q^n - 1 .$$

2°) Si $f = g\,h$ où les polynôme f et g sont premiers entre eux, démontrer la relation

$$per(f) = \text{p.p.c.m.}(per(g), per(h)) .$$

3°) Démontrer que si f est irréductible alors on a

$$per(f) \text{ divise } q^n - 1 .$$

4°) On suppose en outre que f est unitaire et se décompose sous la forme

$f = f_1^{n_1} \ldots f_k^{n_k}$, où les f_i sont distincts, irréductibles et unitaires.

Démontrer que l'on a

$$per(f) = e\,p^s \quad \text{où} \quad e = \text{p.p.c.m.}(per(f_1), \ldots, per(f_k))$$

et l'entier s est défini par la condition

$$p^s \geq \max\{n_1, \ldots, n_k\} > p^{s-1} .$$

5°) Comparer $per(f(X))$ et $per(f(-X))$. [Voir R. Lidl et H. Niederreiter .– *Finite Fields* , Add. Wesley, 1983, Reading Mass.]

6°) Si f est unitaire, soit r le plus petit entier tel que X^r soit congru à un élément du corps K modulo le polynôme f et soit a tel que $X^r \equiv a$. Démontrer que l'on a

$$per(f) = r\,h ,$$

où h est l'ordre de a dans le groupe K^*.

11. Démontrer que le produit des polynômes unitaires irréductibles de degré n sur le corps $\mathbf{F}_q$ est donné par la formule

$$\prod_{d \mid n} \left(X^{q^d} - X \right)^{\mu(n/d)} .$$

12. Soient K et L les corps finis possédant respectivement q et $q' = q^m$ éléments. Soit

$$f = \sum_{i=0}^{q'-1} a_i X^i ,$$

un polynôme à coefficients dans L.

Démontrer que les propriétés suivantes sont équivalentes :

(i) $f(L) \subset K$,

(ii) $X^{q'} - X$ divise $f(X)^q - f(X)$,

(iii) on a $a_{q'-1} = a_{q'-1}^q$ et $j \equiv q\, i \Rightarrow a_j = a_i^q$ pour $0 \leq i, j < q - 1$.

13. Soit $f : \mathbf{F}_q \to \mathbf{F}_q$ une fonction quelconque.

Démontrer qu'il existe un polynôme et un seul $F \in \mathbf{F}_q$ tel que l'on ait $f(x) = F(x)$ pour tout élément x de $\mathbf{F}_q$.

Démontrer la formule

$$F(X) = \sum_{\alpha \in \mathbf{F}_q} f(\alpha) \left(1 - (X - \alpha)^{q-1} \right) .$$

14. Soit α un élément non nul du corps $\mathbf{F}_q$ et soit k un entier, $1 \leq k < q$. On considère le binôme $f(X) = X^k - \alpha$.

Démontrer que les propriétés suivantes sont équivalentes

(i) f divise $X^q - X$,

(ii) $k \mid q-1$ et $\alpha^{(q-1)/k} = 1$.

15. Le théorème de König - Rados.

Soit $f \in \mathbf{F}_q[X]$ un polynôme. On s'intéresse au nombre

$$N = \#\{ x \in \mathbf{F}_q^* \; ; \; f(x) = 0 \}.$$

1°) Démontrer qu'on peut se limiter au cas où le degré de f est au plus égal à $q-2$. Par conséquent on supposera que f est de la forme

$$f = a_0 + a_1 X + \ldots + a_{q-2} X^{q-2}.$$

2°) Soit A la matrice définie par

$$A = (a_{ij}) \quad \text{où} \quad a_{ij} = a_k \text{ avec } k = (j-i) \bmod (q-2).$$

Soient $\{ b_1, \ldots, b_{q-1} \}$ les éléments de $\mathbf{F}_q$ numérotés de telle sorte que l'on ait

$$f(b_j) = 0 \quad \text{pour} \quad j = q-N, \ldots, q-1.$$

On considère la matrice $B = (b_j^{i-1})$. Démontrer la relation

$$A\,B = (b_j^{1-i} f(b_j)).$$

Démontrer que la matrice B est inversible tandis que le rang de la matrice $A\,B$ est égal à $q-1-N$.

3°) En déduire le théorème de König-Rados :

$$N = q - 1 - \text{rang}(A).$$

4°) Application numérique : déterminer le nombre de racines dans le corps $\mathbf{F}_7$ du polynôme $2X^3 - 3X^2 + X + 3$.

16. Le théorème de Chevalley - Warning .

1°) Soit k un entier ≥ 0 . Démontrer que l'on a

$$\sum_{c \in \mathbf{F}_q} c^k = \begin{cases} 0 & \text{si } k = 0 \text{ ou } k \text{ non divisible par } q-1 , \\ -1 & \text{sinon .} \end{cases}$$

[Par convention : $0^0 = 1$.]

2°) Soit $f \in \mathbf{F}_q [X_1 , \dots , X_n]$ un polynôme de degré total $\deg (f) < n (q - 1)$.

Démontrer la relation

$$\sum_{c_1 , \dots , c_n \in \mathbf{F}_q} f (c_1 , \dots , c_n) = 0 .$$

[Démontrer d'abord le résultat pour un monôme.]

3°) Soit F le polynôme $1 - f^{q-1}$.

Démontrer que l'on a

$$F (c_1, \dots , c_n) = \begin{cases} 1 & \text{si } f (c_1, \dots , c_n) = 0 , \\ 0 & \text{sinon .} \end{cases}$$

4°) Soit $f \in \mathbf{F}_q [X_1 , \dots , X_n]$ un polynôme de degré total $\deg (f) < q - 1$.

On pose

$$N = \# \{ (x_1 , \dots , x_n) \in (\mathbf{F}_q)^n \ ; \ f (x_1 , \dots , x_n) = 0 \} .$$

Démontrer le théorème de Warning :

$N \equiv 0$ (modulo p), où p est la caractéristique du corps $\mathbf{F}_q$.

En déduire le théorème de Chevalley :

Si $f \in \mathbf{F}_q [X_1 , \ldots , X_n]$ est un polynôme de degré total $\deg (f) < q - 1$ tel que $f (0, \ldots, 0) = 0$ alors l'équation $f (x_1 , \ldots , x_n) = 0$ admet une solution non triviale $(x_1 , \ldots , x_n) \in (\mathbf{F}_q)^n$.

5°) Démontrer que si $f_1 , \ldots, f_m \in \mathbf{F}_q [X_1 , \ldots , X_n]$ vérifient

$$\deg (f_1) + \ldots + \deg (f_m) < n$$

alors le nombre

$$N = \# \{ (x_1 , \ldots , x_n) \in \mathbf{F}_q^n \ ; \ f_i (x_1 , \ldots , x_n) = 0 \text{ pour } i = 0, 1, \ldots, m \}$$

est divisible par p.

[Considérer $F = (1 - f_1^{q-1}) \ldots (1 - f_m^{q-1})$.]

En déduire une généralisation du théorème de Chevalley.

6°) Soit L le corps à q^n éléments et soit $e_1 , \ldots , e_n$ une base de L en tant qu'espace vectoriel sur le corps $\mathbf{F}_q$. On pose

$$N (X_1, \ldots , X_n) = \prod_{k=0}^{n-1} \left(e_1^{q^k} X_1 + \ldots + e_n^{q^k} X_n \right) .$$

(i) Démontrer que le polynôme N est à coefficients dans $\mathbf{F}_q$.

[On pourra vérifier la relation $N^q (X_1 , \ldots , X_n) = N (X_1^q , \ldots , X_n^q)$.]

(ii) Démontrer l'implication

$$x_1 , \ldots , x_n \in \mathbf{F}_q \text{ et } N (x_1 , \ldots , x_n) = 0 \ \Rightarrow \ x_1 = \ldots = x_n = 0 .$$

(iii) Calculer explicitement des exemples de tels polynômes N pour $n = 2$ et 3 et le corps $\mathbf{F}_2$.

17. Soit $f \in \mathbf{F}_q[X_1, \ldots, X_n]$ un polynôme non nul de degré d et soit

$$N = \#\{(x_1, \ldots, x_n) \in \mathbf{F}_q^n \ ; \ f(x_1, \ldots, x_n) = 0\}.$$

1°) Démontrer la majoration

$$N \leq d\, q^{n-1}.$$

[On pourra raisonner par récurrence sur n et sur d, en distinguant le cas où il existe un élément c de $\mathbf{F}_q$ tel que $X_1 - c$ divise le polynôme f.]

2°) Dans le cas particulier où f est homogène, soit N' le nombre de zéros non triviaux de f, c'est à dire que

$$N' = \#\{(x_1, \ldots, x_n) \in (\mathbf{F}_q)^n \ ; \ f(x_1, \ldots, x_n) = 0 \text{ et } x_1 \ldots x_n \neq 0\}.$$

Démontrer l'inégalité

$$N' \leq d(q^{n-1} - 1).$$

18. Soit E_d l'ensemble des $f \in \mathbf{F}_q[X_1, \ldots, X_n]$ de degré $\leq d$ et soit C le cardinal de cet ensemble.

1°) Démontrer que l'on a

$$C = q^{\binom{n+d}{d}}.$$

2°) Soit $(c_1, \ldots, c_n) \in (\mathbf{F}_q)^n$ un point fixé. Démontrer la formule

$$\#\{f \in E_d \ ; \ f(c_1, \ldots, c_n) = 0\} = C / q^{n-1}.$$

[Considérer le terme constant de f.]

3°) Pour $f \in \mathbf{F}_q [X_1 , \dots , X_n]$, on pose

$$N (f) = \# \{ (x_1 , \dots , x_n) \in (\mathbf{F}_q)^n \ ; \ f (x_1 , \dots , x_n) = 0 \} .$$

Démontrer la relation

$$\sum_{f \in E_d} N (f) = C q^{n-1} .$$

Ainsi, " en moyenne ", un polynôme de $\mathbf{F}_q [X_1 , \dots , X_n]$ possède q^{n-1} zéros dans $(\mathbf{F}_q)^n$.

4°) Démontrer la relation

$$\sum_{f \in E_d} \left(N (f) - q^{n-1} \right)^2 = C \left(q^{n-1} - q^{n-2} \right) .$$

[On pourra d'abord démontrer les formules

$$\sum_{f \in E_d} N (f)^2 = \sum_{b, c \in \mathbf{F}_q^n} \ \sum_{f \in E_d \, ; \, f(b) = f(c) = 0} 1 \quad ,$$

et

$$\sum_{f \in E_d} N (f)^2 = \sum_{c \in \mathbf{F}_q^n} C / q \ + \sum_{b, c \in \mathbf{F}_q^n ; \, b \neq c} C / q^2 \ .]$$

Ainsi, " en général ", $| N (f) - q^{n-1} |$ est de l'ordre de $q^{(n-1)/2}$.

19. Soit K un corps fini et soit a un élément de K . Démontrer qu'il existe x et y dans K tels que $a = x^2 + y^2$.

[Si K est de caractéristique paire, on peut trouver x tel que $a = x^2$. Si $K = \mathbf{F}_q$, avec q impair, noter que l'on a $\# \{ x^2 ; x \in K \} = (q + 1) / 2 \dots]$

20. Rappelons que le résultant de deux polynômes

$$f = a \prod_{i=1}^{m} (X - \alpha_i) \quad \text{et} \quad g = b \prod_{j=1}^{n} (X - \beta_j)$$

peut être défini par la formule

$$\mathrm{Res}(f, g) = a^n b^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) \ .$$

(Donc $\mathrm{Res}(g, f) = (-1)^{mn} \mathrm{Res}(f, g)$.)

1°) Démontrer la formule de Swan

$$\mathrm{Res}(X^j - \alpha^j, X^k - \beta^k) = (-1)^j (\beta^m - \alpha^m)^d$$

où $d = \text{p.g.c.d.}(j, k)$ et $m = \text{p.p.c.m.}(j, k)$.

[Soit R la valeur du résultant cherché et soit ζ une racine primitive j-ième de l'unité. Démontrer d'abord les formules

$$R = (-1)^j \alpha^{md} \prod_{i=1}^{j} \left((\beta / \alpha)^k - \zeta^{ki} \right) ,$$

et

$$\prod_{i=1}^{j/d} \left(X - \zeta^{ki} \right) = X^{j/d} - 1 \ . \ ]$$

2°) Si f est un polynôme unitaire de degré $n \geq 1$, on définit son discriminant par la formule

$$\mathrm{Discr}(f) = (-1)^{n(n-1)/2} \mathrm{Res}(f, f') \ .$$

Démontrer le théorème de Swan :

$$\mathrm{Discr}(X^n + a X^k + b) = (-1)^{n(n-1)/2} b^{k-1} (n^N b^{N-K} - (-1)^N (n - k)^{N-K} k^K a^N)^d ,$$

où on a $n > k > 0$, $d = \text{p.g.c.d.}(n, k)$, $N = n / d$, $K = k / d$.

[cf. Berlekamp .– *Algebraic Coding Theory* , th. 6.67]

3°) Soient g et h deux polynômes unitaires démontrer la formule

$$\text{Discr}(g, h) = \text{Discr}(g)\ \text{Discr}(h)\ (\text{Res}(g, h))^2 .$$

En déduire la formule générale

$$\text{Discr}\left(\prod_{i=1}^{k} f_i\right) = \prod_{i=1}^{k} \text{Discr}(f_i) \cdot \left(\prod_{1 \le i < j < k} \text{Res}(f_i, f_j)\right)^2 ,$$

lorsque $f_1, \ldots, f_k$ sont des polynômes unitaires.

4°) Dans cette question, on suppose q impair. Soit $f \in \mathbf{F}_q[X]$ un polynôme unitaire irréductible de degré m admettant une racine α dans le corps à q^m éléments.

Démontrer la formule

$$\text{Discr}(f) = \Delta^2 \quad \text{où} \quad \Delta = \prod_{0 \le i < j \le m-1} (\alpha^{q^i} - \alpha^{q^j}) .$$

Démontrer que le discriminant de f est un carré dans le corps $\mathbf{F}_q$ si, et seulement si, le degré du polynôme f est pair. [Calculer Δ^q .]

Grâce à la question précédente, en déduire le théorème de Stickelberger :

pour q impair, soit un polynôme unitaire $f \in \mathbf{F}_q[X]$, quadratfrei, de degré égal à m, possédant k facteurs irréductibles sur le corps $\mathbf{F}_q$, alors on a

$$k \equiv m \pmod 2 \Leftrightarrow \text{Discr}(f) \text{ est un carré dans } \mathbf{F}_q .$$

21. La loi de réciprocité quadratique .

Soient maintenant p et q deux nombres premiers impairs distincts.

1°) Soit $D = \text{Discr}(X^q - 1)$, démontrer la formule

$$D = (-1)^{q(q-1)/2}\, q^q .$$

2°) Démontrer que le polynôme $X^q - 1$ possède dans le corps $\mathbf{F}_p$ un nombre de facteurs irréductibles r donné par la formule

$$r = 1 + (q-1)/m ,$$

où m est l'ordre de l'entier p modulo l'entier q.

En déduire la relation

$$\left(\frac{p}{q}\right) = (-1)^{r+1} .$$

3°) En appliquant le théorème de Stickelberger (exercice précédent) , démontrer la formule

$$\left(\frac{D}{p}\right) = (-1)^{q-r} .$$

Démontrer la relation

$$\left(\frac{D}{p}\right) = \left(\frac{p}{q}\right) .$$

4°) Démontrer finalement la " loi de réciprocité quadratique " :

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) . (-1)^{(p-1)(q-1)/4} .$$

[Cette preuve est due à Swan.]

22. Soit $f \in \mathbf{F}_q[X]$ un polynôme quadratfrei et soit g un polynôme de $\mathbf{F}_q[X]$ tel que f divise $g^q - g$.

On désigne par S le sous-ensemble des points de $\mathbf{F}_q$ pour lesquels le p.g.c.d. entre les polynômes $f(X)$ et $g(X) - s$ est non trivial. Et on pose

$$H(X) = \prod_{s \in S} (X - s) .$$

Démontrer que H est le polynôme non nul de degré minimal tel que $f(X)$ divise le polynôme composé $H(g(X))$. [Résultat dû à H. Zassenhaus.]

23. Soit A un anneau factoriel intègre de caractéristique p ($p \geq 0$). Si un polynôme irréductible $g \in A[X]$ divise un polynôme $f \in A[X]$, et si on a

$$g^k \parallel f \quad , \; p \text{ ne divise pas } k \quad , \quad g' \neq 0 \, ,$$

alors $g^{k-1} \parallel f'$; où la notation $u^h \parallel v$ est équivalente à $u^h \mid v$ et u^{h+1} ne divise pas v.

24. Soit $\mathbf{F}_q$ un corps fini de caractéristique impaire. Démontrer que l'équation

$$w^2 + x^2 + y^2 + z^2$$

a exactement $(q+1)(q^2-1)+1$ solutions dans $\mathbf{F}_q{}^4$.

25. Soit $f \in \mathbf{F}_q[X]$ un polynôme irréductible de degré n et soit $g \in \mathbf{F}_q[X]$ un polynôme tel que f ne divise aucun des polynômes $g^{q^d} - g$, pour $d \mid n$, $1 \leq d < n$.

Démontrer que la congruence

$$h(g(X)) \equiv X \quad \text{modulo} \quad F$$

possède alors une solution $h \in \mathbf{F}_q[X]$.

[Considérer une racine ξ de f dans le corps L à q^n éléments et démontrer d'abord que $g(\xi)$ n'appartient à aucun sous corps propre de L . En déduire qu'il existe un polynôme $h \in \mathbf{F}_q[X]$ tel que l'on ait $\xi = h(g(\xi))$. Conclure.]

26. Soit $f \in \mathbf{F}_q[X]$ un polynôme irréductible de degré n de la forme

$$f(X) = X^n + a_{n-1} X^{n-1} + \ldots$$

Démontrer la propriété suivante :

$$f \text{ divise le polynôme } a_1 + X + X^q + \ldots + X^{q^{n-1}} \, .$$

[Soit ξ comme dans l'exercice précédent, démontrer la relation

$$\xi + \xi^q + \ldots + \xi^{q^{n-1}}$$

et conclure.]

27. Soient f et $f_1 \in \mathbf{F}_q[X]$ deux polynômes irréductibles de degré n. Démontrer qu'il existe un polynôme $g \in \mathbf{F}_q[X]$ tel que

(i) f divise le polynôme $f_1(g(X))$,

(ii) f ne divise pas $f_1'(g(X))$,

(iii) f ne divise aucun des polynômes g^{q^k} pour $k = 1, 2, \ldots, n-1$.

[Comme pour l'exercice 25, considérer dans le corps L deux éléments ξ et ξ_1 qui sont respectivement racines des polynômes f et f_1 et noter qu'il existe un polynôme g de $\mathbf{F}_q[X]$ tel que $\xi_1 = g(\xi)$ ...]

28. Soit p un nombre premier. Démontrer que tout élément a non nul de $\mathbf{F}_p$ le polynôme $X^p - X + a$ est irréductible sur le corps $\mathbf{F}_p$.

[On pourra d'abord démontrer les congruences $X^{p^n} \equiv n\,a \pmod{f}$ pour $n \geq 0$.

30. Soit n un entier ≥ 2 et soit p un nombre premier qui ne divise pas n.

Démontrer que le polynôme cyclotomique Φ_n est irréductible sur le corps fini $\mathbf{F}_p$ si, et seulement si, l'ordre de l'entier p dans le groupe $G(n)$ est égal à $\varphi(n)$.

31. Le théorème de la base normale .

Soient K et L deux corps finis, L contenant K , avec Card (L) = q . On note f l'automorphisme de Frobenius de L , donc $f : L \to L$ est l'application qui à tout x associe x^q .

Soit P (X) le polynôme minimal de f (en tant qu'application K - linéaire) .

1°) Démontrer que P divise $X^n - 1$.

2°) Démontrer que les applications Id , f , f^2 , ... , f^{n-1} sont linéairement indépendantes sur K (cas particulier d'un théorème de Dirichlet) .

3°) En déduire que $P = X^n - 1$.

4°) A tout élément x de L on associe le diviseur Q_x de P de degré minimal tel que l'on ait $Q_x (f) (x) = 0$.

Démontrer que si x et y sont deux éléments de L tels que les polynômes Q_x et Q_y soient premiers entre eux alors on a

$$Q_{x+y} = Q_x \cdot Q_y .$$

Démontrer qu'il existe un élément z de L tel que $Q_z = P$.

5°) Démontrer que pour l'élément z de la question précédente, la famille

$$z , z^q , z^{q^2} , \ldots , z^{q^{n-1}}$$

est une base de L sur K . On dit que c'est une **base normale** .

6°) Si L est représenté comme K - espace vectoriel rapporté à une certaine base normale, démontrer que l'élévation à la p - ième puissance d'un élément de L équivaut à une permutation circulaire sur les composantes de cet élément.

CHAPITRE VII

Polynômes à coefficients entiers

Dans tout ce chapitre on ne considérera que des polynômes en une seule variable.

1. Principes des algorithmes de factorisation des polynômes à coefficients entiers.

1. Existence d'un algorithme de factorisation.

Soit F un polynôme à coefficients entiers de degré d et de hauteur $H = H(F)$, on supposera toujours que f est **primitif**, c'est à dire que ses coefficients sont premiers entre eux dans leur ensemble.

Si le polynôme F est réductible (sur $\mathbf{Z}$), il admet alors un diviseur $G \in \mathbf{Z}[X]$ non constant de degré $d' \leq d/2$. On sait majorer les coefficients d'un tel diviseur G, plus précisément on a les inégalités

$$H(G) \leq 2^{d'} H \leq 2^{d/2} H .$$

D'ailleurs, toute majoration des racines de f conduit aussitôt à une majoration des coefficients du polynôme g. C'est ainsi, par exemple, que l'inégalité de Cauchy fournit la majoration (nettement moins bonne)

$$H(G) \leq 2^{d/2} (H+1)^{d/2} .$$

En conclusion, pour trouver un éventuel facteur g comme ci-dessus, il suffit de tester les polynômes dont le degré est au plus d/2 et la hauteur majorée par $e^{d/2} H$. Comme le nombre de ces polynômes est de l'ordre de

$$(2H)^{d/2} e^{d^2/4} .$$

cet algorithme est inutilisable en pratique.

2. L'algorithme de Kronecker .

Cet algorithme est décrit en détail dans l'exercice 3 , nous nous contenterons ici de le présenter grâce à un exemple. Son principe consiste à utiliser le fait, qu'en tout point entier a , la valeur G (a) d'un facteur quelconque de F doit diviser F (a) . Il suffit de choisir un nombre de points a au plus égal à (d + 2) / 2 puisque la connaissance de ses valeurs en ce nombre de points détermine complètement un polynôme G de degré majoré par d / 2 .

Considérons le polynôme

$$F(X) = X^5 - 5X^4 + 10X^3 - 10X^2 + 1 .$$

Il ne possède pas de racines dans $\mathbf{Z}$ puisque l'on a

$$F(1) = -3 \quad \text{et} \quad F(-1) = -25 .$$

Si F est réductible, il admet donc un diviseur G de degré deux. On peut se limiter à un polynôme de coefficient dominant positif et donc chercher G sous la forme

$$G(X) = X^2 + aX + b .$$

Comme $F(0) = 1$, on doit avoir $b = \pm 1$. De plus,

$$F(1) = -3 \Rightarrow G(1) \in \{ \pm 1 , \pm 3 \} ,$$

soit

$$a = -1 - b + G(1) \quad \text{avec} \quad G(1) \in \{ \pm 1 , \pm 3 \} ,$$

ce qui fournit huit candidats G possibles et montre que a est impair.

De la même manière,

$$F(-1) = -25 \Rightarrow G(-1) \in \{ \pm 1 , \pm 5 , \pm 25 \} ,$$

soit

$$a = 1 + b - G(-1) \quad \text{avec} \quad G(-1) \in \{ \pm 1 , \pm 5 , \pm 25 \} .$$

Par soustraction, on trouve

$$2b = G(-1) + G(1) - 2 \quad (\text{avec } b = \pm 1),$$

ce qui exclut les possibilités $G(1) = \pm 25$, et ne laisse que les cas

(i) $b = -1$ et $G(1) = -G(-1) = \pm 1$, (soit $a = \pm 1$),

(ii) $b = 1$ et $G(-1) = 1$, $G(1) = 3$, (soit $a = 1$),

(iii) $b = 1$ et $G(-1) = 5$, $G(1) = -1$, (soit $a = -3$).

Comme $F(2) = -7$, on a aussi

$$G(2) \in \{\pm 1, \pm 7\},$$

donc

$$4 + 2a + b = \pm 1 \text{ ou } \pm 7,$$

ce qui montre que dans le cas (i) la seule possibilité est $a = -1$.

Par division euclidienne, on constate que les cas (i) et (ii) n'ont pas lieu ; par contre la troisième possibilité fournit la factorisation

$$F(X) = (X^2 - 3X + 1)(X^3 - 2X^2 + 3X + 1).$$

Remarque : Nous n'avons pas exactement suivi la méthode de Kronecker puisque, plutôt que de calculer directement par interpolation tous les diviseurs possibles, nous avons préféré en exclure certains en considérant plusieurs valeurs du polynôme F.

Dans cet exemple, le nombre de cas à tester était particulièrement petit du fait du petit degré de G et surtout du fait que les valeurs de F utilisées avaient la particularité d'avoir très peu de diviseurs. Il est clair que cette méthode devient vite extrêmement coûteuse quand le degré de F croît. Elle nécessite *a priori* un nombre de tests qui est au moins égal à $2^{d/2}$ (seulement à cause du choix des signes des valeurs de G aux points utilisés) et même très supérieur à ce nombre dans la plupart des cas.

3. Le principe des algorithmes modernes .

Depuis la découverte de l'algorithme de Berlekamp pour la factorisation des polynômes sur un corps fini tous les algorithmes de factorisation des polynômes à coefficients entiers comportent les étapes suivantes :

(o) on peut supposer le polynôme quadratfrei ;

(i) soit $F \in \mathbf{Z}[X]$ le polynôme étudié, on choisit un nombre premier p convenable et on factorise le polynôme f dans $\mathbf{F}_p[X]$, où f est l'image de F modulo l'entier p ;

(ii) on raffine la factorisation précédente modulo p^n pour un exposant n assez grand (disons $p^n \geq B$), ceci grâce au lemme de Hensel ;

(iii) on cherche dans cette factorisation raffinée un diviseur éventuel de F dans l'anneau $\mathbf{Z}[X]$.

Notre tâche est maintenant claire, il faut étudier les problèmes suivants :

- choix de l'entier p utilisé comme module ,
- choix de la borne B et construction de Hensel,
- recherche des facteurs dans $\mathbf{Z}[X]$.

Les deux premières étapes ne présentent pas de difficulté et leur étude a été longuement préparée au cours des précédents chapitres. Il n'en est pas de même pour la dernière partie où nous allons présenter l'algorithme récent dit " L^3 " , par abréviation du nom de ses auteurs A. Lenstra , H. Lenstra et L. Lovász .

2. Le choix du module p.

Comme nous l'avons déjà dit, nous allons d'abord factoriser f dans $\mathbf{F}_p[X]$, où f est égal à F modulo p. Pour appliquer l'algorithme de Berlekamp, nous devons nous ramener au cas où f est quadratfrei.

Dans un premier temps, on teste si F est quadratfrei en calculant son p.g.c.d. avec sa dérivée F '. Grâce à l'algorithme vu au chapitre précédent, on peut facilement se ramener au cas où F est quadratfrei (dans $\mathbf{Z}[X]$). Dans la suite, nous supposerons donc que F n'a pas de facteur carré.

On a les équivalences suivantes (dans $\mathbf{F}_p[X]$)

$$f \text{ quadratfrei} \iff \text{p.g.c.d.}(f, f') = 1 \iff \text{résultant}(f, f') \neq 0 .$$

Relativement à F, la traduction est

$$f \text{ quadratfrei} \iff p \text{ ne divise pas } \operatorname{discr}(F) .$$

Comme F est supposé quadratfrei, son discriminant Δ n'est pas nul. Il est facile de majorer $|\Delta|$; en appliquant l'inégalité de Hadamard, on obtient par exemple

$$|\Delta| \leq \|F\|^{d-1} . \|F'\|^{d} \leq d^{d} \|F\|^{2d-1} \leq (d+1)^{2d} H^{2d-1},$$

où on a posé

$$d = \deg(F) \quad \text{et} \quad H = \text{hauteur}(F),$$

notations qui seront conservées par la suite.

D'autre part un entier $n > 2$ possède au plus $1 + \operatorname{Log} n$ facteurs premiers distincts (en effet un diviseur premier autre que deux est au moins égal à trois, on a donc la majoration $\omega(n) \leq 1 + (\operatorname{Log} n)/(\operatorname{Log} 3)$).

Le nombre de diviseurs premiers du discriminant Δ vérifie donc

$$\omega(\Delta) = O(d \operatorname{Log} d + d \operatorname{Log} H).$$

D'où le fait qu'on peut trouver un nombre premier p ne divisant pas Δ et vérifiant

$$p = O((d \operatorname{Log} d + d \operatorname{Log} H) \operatorname{Log}(d \operatorname{Log} d + d \operatorname{Log} H)).$$

Un argument un peu moins grossier, fournit

$$\omega(n) = O((\operatorname{Log} n)/(\operatorname{Log} \operatorname{Log} n)) \quad \text{pour} \quad n \geq 3,$$

et donc en fait

$$p = O(d \operatorname{Log} d + d \operatorname{Log} H).$$

Voir l'exercice 5 pour une étude plus précise.

3. Raffinement de la factorisation .

1. La borne B .

Soit G un diviseur quelconque du polynôme F dans $\mathbf{Z}[X]$. On a vu au chapitre quatre que si le polynôme G est de la forme

$$G(X) = b_m X^m + b_{m-1} X^{m-1} + \ldots + b_0,$$

alors ses coefficients vérifient les inégalités

$$|b_j| \leq \binom{m}{j} M(F) \quad \text{pour} \quad j = 0, 1, \ldots, m.$$

On en déduit la majoration

$$H(G) \leq 2^m M(F) \quad , \text{ où } \quad m = \deg(G).$$

A partir de là on peut

- soit calculer une valeur approchée de la mesure du polynôme F, par exemple en utilisant la méthode décrite au chapitre 4 ;

- soit se contenter de la majoration $M(F) \leq \| F \|$.

En tout cas, on a toujours

$$H(G) \leq 2^m (d+1)^{1/2} H \quad , \quad \text{où} \quad m = \deg(G) .$$

Si on calcule une factorisation de F modulo p^n, les coefficients des facteurs étant choisis dans l'intervalle $\left[-(p^n - 1)/2 , +(p^n - 1)/2 \right]$, on choisira n assez grand pour que l'on ait

$$p^n \geq 2 H(G) \quad \text{pour tout diviseur } G \text{ de } F \text{ de degré } \leq d/2 ;$$

on pourra donc prendre n tel que

$$p^n \geq 2^{1+d/2} (d+1)^{1/2} H .$$

Pour simplifier nous ne retiendrons que cette dernière valeur, qui conduit à l'estimation

$$n = O((d + \operatorname{Log} H)/(\operatorname{Log} p)),$$

et on posera

$$B = 2^{1+d/2} (d+1)^{1/2} H$$

sauf précision contraire.

2. Le lemme de Hensel .

Le lemme de Hensel a de nombreuses variantes, nous démontrerons le résultat suivant.

THEOREME 1 . – (Hensel) Soit p un nombre premier. Soient f , g_0 et h_0 des polynômes de $\mathbf{Z}[X]$ qui vérifient les propriétés suivantes

(i) g_0 est unitaire et $\deg(g_0) + \deg(h_0) = \deg(f)$,

(ii) $f(X) - g_0(X)\, h_0(X) \equiv 0 \pmod{p^{1+2k}}$, où $p^k \| \operatorname{res}(g_0, h_0)$.

[La notation $p^k \| x$ signifie que p^k divise x mais que p^{k+1} ne divise pas x .]

Alors pour tout entier $n \geq 0$, il existe des polynômes g_n et h_n à coefficients entiers tels que l'on ait

(1) g_n est unitaire et $\deg(g_n) + \deg(h_n) = \deg(f)$,

(2) $g_n \equiv g_0 \pmod{p^{k+1}}$, $h_n \equiv h_0 \pmod{p^{k+1}}$,

(3) $f \equiv g_n h_n \pmod{p^{n+2k+1}}$.

Remarque : Le lemme de Hensel montre donc que, si on part d'une solution suffisamment approchée d'une certaine relation, on peut trouver une solution meilleure. Cette situation est fréquente en analyse numérique et la méthode de preuve du lemme de Hensel n'est autre que l'analogue modulo p de la méthode de Newton.

> Nous allons donner deux démonstrations différentes de ce résultat.

première démonstration : convergence linéaire.

Partant de g_0 et h_0 , il s'agit de construire la suite des g_n et h_n . On procède bien entendu par récurrence sur n .

Le cas $n = 0$ correspond exactement aux hypothèses du théorème.

Supposons $n \geq 1$ et les suites (g_i) et (h_i) construites jusqu'au rang $n-1$. Cherchons les polynômes g_n et h_n sous la forme

$$g_n = g_{n-1} + p^{n+k} g_n^* \quad \text{et} \quad h_n = h_{n-1} + p^{n+k} h_n^*$$

avec

$$\deg(g_n^*) \leq \deg(g_0) - 1 \quad \text{et} \quad \deg(h_n^*) \leq \deg(h_0) .$$

Les propriétés (1) et (2) sont alors automatiquement vérifiées. Reste à réaliser la condition (3). Compte tenu des formules choisies pour g_n et h_n, cette condition se traduit par la relation

$$f - g_{n-1} h_{n-1} - p^{n+k} (g_{n-1} h_n^* + h_{n-1} g_n^*) \equiv 0 \pmod{p^{n+2k+1}} .$$

En posant

$$f(X) - g_{n-1}(X) h_{n-1}(X) = p^{n+2k} r_{n-1}(X) ,$$

on aboutit à l'équation

$$(*) \quad g_{n-1}(X) h_n^*(X) + h_{n-1}(X) g_n^*(X) \equiv p^k r_{n-1}(X) \pmod{p^{k+1}} .$$

Il s'agit d'un système linéaire où les inconnues sont les coefficients des deux polynômes h_n^* et g_n^*. Soit d le degré du polynôme f. Le nombre d'inconnues de ce système est le nombre total de coefficients des polynômes h_n^* et g_n^*, c'est donc

$$\deg(h_n^*) + 1 + \deg(g_n^*) + 1 = \deg(h_0) + 1 + \deg(g_0) = d + 1 ;$$

tandis que son nombre d'équations est $\deg(f) + 1 = d + 1$. Il y a donc autant d'équations que d'inconnues.

Le déterminant associé à ce système est le résultant des polynômes g_{n-1} et h_{n-1}, il est donc divisible par p^k mais pas par p^{k+1} (d'après la propriété (ii)). Les formules de Cramer montrent que le système

$$g_{n-1}(X) h_n^*(X) + h_{n-1}(X) g_n^*(X) = p^k r_{n-1}(X)$$

admet une solution dans $\mathbf{Q}$, dont le dénominateur commun (disons a) n'est pas divisible par p. Si u est un entier tel que $ua \equiv 1 \pmod{p^{k+1}}$ alors la solution précédente multipliée par ua fournit deux polynômes à coefficients entiers dont la réduction modulo p^k vérifie l'équation (*). D'où le résultat.

deuxième démonstration : convergence quadratique.

Oublions les notations de la première démonstration. Nous allons construire une suite de polynômes g_i et h_i qui vérifient

$$f - g_i h_i \equiv 0 \quad \text{modulo } p^{2k+2^i} .$$

On raisonne par récurrence sur i. Pour $i = 0$, les polynômes g_0 et h_0 donnés dans l'énoncé conviennent. Supposons ces polynômes construits à l'ordre i et cherchons les polynômes g_{i+1} et h_{i+1} de la forme

$$g_{i+1} = g_i + p^{k+2^i} g_i^* \quad \text{et} \quad h_{i+1} = h_i + p^{k+2^i} h_i^* ,$$

à nouveau avec $\deg(g_i^*) \leq \deg(g_0) - 1$ et $\deg(h_i^*) \leq \deg(h_0)$. On a alors

$$f - g_{i+1} h_{i+1} \equiv f - g_i h_i - p^{k+2^i} (g_i h_i^* + h_i g_i^*) \quad \text{modulo } p^{2k+2^{i+1}} ,$$

où l'hypothèse de récurrence permet d'écrire

$$f - g_i h_i = p^{2k+2^i} r_i \quad \text{avec} \quad r_i \in \mathbf{Z}[X] .$$

Il s'agit cette fois de résoudre l'équation

$$g_i h_i^* + h_i g_i^* \equiv p^k r_i \quad \text{modulo } p^{k+2^i} .$$

Comme plus haut, p^k est la plus grande puissance de p qui divise le déterminant du système correspondant et une modification facile de l'argument qui achève la première démonstration montre que cette équation a bien des solutions g_i^*, h_i^*. [Les polynômes à coefficients rationnels considérés au début ont encore pour dénominateur commun un entier a non divisible par p ; et on prend ensuite un entier u tel que $u\,a \equiv 1 \mod p^{2^i}$ ...]

Ce qui achève cette démonstration.

La suite construite dans cette seconde démonstration fournit des solutions approchées de l'équation $f - g\,h = 0$, avec une " précision " qui double presque à chaque pas (et qui double exactement lorsque k est nul) .

COROLLAIRE 1 . – Soient f, g_0 et h_0 des polynômes de $\mathbf{Z}[X]$ tels que

(i) g_0 et h_0 sont unitaires,

(ii) $f \equiv g_0 h_0$ modulo p,

(iii) les polynômes $(g_0 \bmod p)$ et $(h_0 \bmod p)$ sont premiers entre eux .

Alors, pour tout entier $n \geq 0$, il existe des polynômes g et h de $\mathbf{Z}[X]$ qui vérifient

$$f \equiv g h \text{ modulo } p^n,$$

avec g unitaire et

$$g \equiv g_0 \pmod p , \quad h \equiv h_0 \pmod p .$$

COROLLAIRE 2 . – Soit $f \in \mathbf{Z}[X]$ un polynôme, et soit f' sa dérivée. Soient k et $m \in \mathbf{N}$ deux entiers tels que $2k < m$. On suppose qu'il existe $x \in \mathbf{Z}$ tel que

$$f(x) \equiv 0 \pmod{p^m} \quad \text{et} \quad p^k \| f'(x) .$$

Alors, pour tout entier $n \geq m$, il existe $y \in \mathbf{Z}$ tel que

$$f(y) \equiv 0 \pmod{p^n} , \quad p^k \| f'(y) \quad \text{et} \quad y \equiv x \pmod{p^{m-k}}.$$

> Par division euclidienne, on peut écrire

$$f(X) = f(x) + (X - x) f_1(X), f_1 \in \mathbf{Z}[X] .$$

Il n'y a plus qu'à vérifier que les hypothèses du théorème ont bien lieu. C'est clair pour l'hypothèse (i) . En ce qui concerne la seconde condition, on note d'abord que

$$\operatorname{res}(g_0 , h_0) = \pm f_1(x) \equiv \pm f'(x) \pmod{p^{k+1}} ,$$

(exercice) , donc $p^k \| \operatorname{res}(g_0 , h_0)$.

En tenant compte de l'hypothèse

$$f(x) \equiv 0 \pmod{p^m} \text{ avec } m > 2k ,$$

on obtient bien la congruence

$$f(X) - (X - x) f_1(X) \equiv 0 \pmod{p^{2k+1}} ,$$

qui n'est autre que la condition (ii) . D'où le résultat. <

4. Factorisation dans Z [X] , la méthode de Berlekamp .

On considère un polynôme quadratfrei $F \in \mathbf{Z}[X]$, de degré d et de hauteur H , que l'on cherche à factoriser. Pour simplifier on supposera F unitaire (voir exercice 4).

La méthode de Berlekamp comporte les étapes suivantes :

1°) On choisit un nombre premier p qui ne divise pas le discriminant de F.

2°) On factorise dans $\mathbf{F}_p[X]$ le polynôme f , image de F modulo p ; soient $P_1, \ldots, P_k$ les facteurs irréductibles de f dans $\mathbf{F}_p[X]$.

3°) Si k est égal à 1 alors F est irréductible, et on arrête évidemment la procédure.

4°) Par contre, si on a $k > 1$, on choisit une partition quelconque de l'ensemble $\{ 1, 2, \ldots , k \}$ en deux parties S et T non vides et on pose

$$g_0 = \prod_{i \in S} P_i \quad \text{et} \quad h_0 = \prod_{i \in T} P_i \ ,$$

de sorte que l'on a

$$F \equiv g_0 h_0 \pmod{p} \ , \quad \text{avec} \quad \operatorname{res}(g_0 , h_0) \neq 0 \mod p \ ,$$

(en considérant que g_0 et h_0 sont à coefficients entiers) .

5°) Le lemme de Hensel s'applique, ce qui permet de raffiner la congruence précédente en

$$F \equiv g\, h \pmod{p^n} \quad \text{avec} \quad p^n \geq B \ ,$$

la borne B étant choisie comme plus haut, et les polynômes g et h ayant leurs coefficients entiers et compris entre $-p^n/2$ et $p^n/2$.

6°) On teste ensuite si g divise F (dans $\mathbf{Z}[X]$),

- si g divise F alors on a trouvé un facteur non trivial de F et on peut appliquer cette procédure aux polynômes g et F/g,
- s'il n'existe plus aucune partition non traitée la procédure s'arrête en concluant que F est irréductible sinon on choisit une nouvelle partition de l'ensemble $\{ 1, 2, \ldots, k \}$ et on retourne à l'étape 4 .

Etudions rapidement le coût de cet algorithme. Le coût des étapes 1 à 3 a déjà été calculé, et on sait qu'il est en $O (d^3 p (\text{Log } p)^2)$. Par ailleurs, on a vu que l'on peut supposer $p = O (d \text{ Log } (d H))$, le temps de calcul des trois premières étapes est donc majoré par

$$O (d^4 (\text{Log } d H)^2) .$$

Pour un choix quelconque de la partie S, les étapes suivantes ont un coût

$$C = O (d^2 (d + \text{Log } H)^2) \quad \text{(exercice : le démontrer)} .$$

Mais, on peut avoir à tester tous les 2^{k-1} ensembles S possibles, et le coût des parties 4 à 6 de l'algorithme est alors $2^{k-1} C$. Comme nous l'avons vu au chapitre précédent, on a " en général "

$$k \leq 2 \text{ Log } d \quad (\text{ et donc } 2^k < d^{3/2})$$

et l'algorithme de Berlekamp a donc " en général " un coût total majoré par

$$O ((\text{Log } d)^2 d^4 (\text{Log } d H)^2) .$$

Cependant, il existe des polynômes irréductibles sur $\mathbf{Z}$ et pour lesquels, quel que soit le choix du nombre premier p, on a toujours $k \geq d/2$ (et donc $2^{k-1} \geq 2^{d/2-1}$) ; ce qui montre que l'algorithme de Berlekamp n'est pas polynomial en fonction du degré du polynôme F (voir l'exercice 5).

L'objet des prochains paragraphes sera de donner un algorithme de factorisation dont le coût est polynômial, l'algorithme " L^3 ".

5 . L'algorithme L^3 .

1. Réseaux .

Soit n un entier positif, un sous - ensemble L de l'espace $\mathbf{R}^n$ est appelé un **réseau** (en anglais *lattice*) s'il existe une base $b_1, \ldots, b_n$ de l'espace $\mathbf{R}^n$ telle

$$L = \sum_{i=1}^{n} b_i \mathbf{Z} = \left\{ \sum_{i=1}^{n} r_i b_i \; ; \; r_i \in \mathbf{Z}, 1 \le i \le n \right\} .$$

Par définition, le **déterminant** de L est

$$\det(L) = |\det(b_1, \ldots, b_n)| ,$$

il ne dépend pas du choix de la base $b_1, \ldots, b_n$. L'entier n est appelé le **rang** de L.

2. Orthogonalisation de Gram-Schmidt .

Soit $b_1, \ldots, b_n$ une base de $\mathbf{R}^n$. Les vecteurs b_i^* , $1 \le i \le n$, et les scalaires μ_{ij} , pour $1 \le j < i \le n$, sont définis récursivement par

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^* \quad , \quad \text{où} \quad \mu_{ij} = \frac{(b_i, b_j^*)}{(b_j^*, b_j^*)} ,$$

où $(\ ,\ )$ désigne le produit scalaire dans $\mathbf{R}^n$. Alors $b_1^*, \ldots, b_n^*$ est une base orthogonale de $\mathbf{R}^n$.

D'après la construction des b_i^* , on a

$$\det(L) = |\det(b_1^*, \ldots, b_n^*)| ,$$

et du fait que $b_1^*, \ldots, b_n^*$ est une base orthogonale on a aussi

$$|\det(b_1^*, \ldots, b_n^*)| = |b_1^*| \ldots |b_n^*| ,$$

et donc

$$\det(L) = |b_1^*| \ldots |b_n^*| .$$

Notons que

$$| b_i |^2 = | b_i^* + \sum_{j=1}^{i-1} \mu_{ij} b_j^* |^2 = | b_i^* |^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 | b_j^* |^2 \geq | b_i^* |^2 \quad , \ 1 \leq i \leq n .$$

D'où le résultat suivant.

THEOREME 2 . – (Inégalité de Hadamard) Soient $b_1, b_2, \ldots, b_n$ n vecteurs non nuls de l'espace $\mathbf{R}^n$, alors on a

$$| \det (b_1, \ldots, b_n) | \leq | b_1 | \ldots | b_n | ,$$

l'égalité n'ayant lieu que si ces vecteurs sont deux à deux orthogonaux.

3. Bases réduites .

A partir de là, nous suivons de très près l'article de A. K. Lenstra , H. W. Lenstra Jr. et L. Lovász .– *Factoring Polynomials With Rational Coefficients* , Math. Ann. , t. 261, 1982, pp. 515-534.

Dans la suite, cet article sera désigné par [L^3] .

Ces auteurs ont introduit la définition suivante :

une base $b_1, b_2, \ldots, b_n$ d'un réseau est dite **réduite** si elle vérifie les conditions suivantes

$$| \mu_{ij} | \leq 1/2 \quad \text{pour} \quad 1 \leq j \leq i \leq n$$

et

$$| b_i^* + \mu_{i\,i-1} b_{i-1}^* |^2 \geq (3/4) | b_{i-1}^* |^2 \quad \text{pour} \quad 1 < i \leq n .$$

PROPOSITION 1 . – Soit $b_1, b_2, \ldots, b_n$ une base réduite d'un réseau L de l'espace $\mathbf{R}^n$, et soient $b_1^*, b_2^*, \ldots, b_n^*$ définis par le procédé de Gram - Schmidt. Alors on a

$$|b_j|^2 \leq 2^{i-1} |b_i^*|^2 \quad \text{pour} \quad 1 \leq j \leq i \leq n .$$

> Par définition d'une base réduite, on a

$$|b_i^*|^2 \geq \left(\frac{3}{4} - \mu_{i\,i-1}^2\right) |b_{i-1}^*|^2 \geq \frac{1}{2} |b_{i-1}^*|^2 ,$$

pour $1 < i \leq n$, d'où l'on déduit

$$|b_j^*|^2 \leq 2^{i-j} |b_i^*|^2 \quad \text{pour} \quad 1 \leq j \leq i \leq n .$$

Ce qui implique

$$|b_i|^2 \leq |b_i^*|^2 + \frac{1}{4} \sum_{j=1}^{i-1} 2^{i-j} |b_i|^2 \leq 2^{i-1} |b_i^*|^2 .$$

Et, en définitive,

$$|b_j|^2 \leq 2^{j-1} |b_j^*|^2 \leq 2^{i-1} |b_i^*|^2 ,$$

pour $1 \leq j \leq i \leq n$. <

COROLLAIRE 1 . – Sous les hypothèses de la proposition, on a les estimations

$$\det(L) \leq |b_1| \ldots |b_n| \leq 2^{n(n-1)/4} \det(L) ,$$

et

$$|b_1| \leq 2^{(n-1)/4} \det(L)^{1/n} .$$

> La première inégalité est celle de Hadamard. La seconde résulte de la proposition et de la formule

$$\det(L) = |b_1^*| \ldots |b_n^*| .$$

La troisième découle de la proposition et de la seconde. <

COROLLAIRE 2 . – Soit L un réseau dont $b_1, b_2, \ldots, b_n$ est une base réduite. Soient $x_1, x_2, \ldots, x_t$ des vecteurs linéairement indépendants de L. Alors, on a

$$| b_j |^2 \leq 2^{n-1} \max \{ | x_1 |^2, | x_2 |^2, \ldots, | x_t |^2 \}$$

pour $j = 1, 2, \ldots, t$.

> Tout vecteur x non nul de L peut s'écrire sous la forme

$$x = \sum_{i=1}^{m} r_i b_i = \sum_{i=1}^{m} r_i' b_i^* \quad \text{avec } r_i \in \mathbf{Z} \text{ et } r_i' \in \mathbf{R}, r_m \neq 0,$$

pour un certain entier $m = m(x)$.

On a alors $r_m' = r_m$ et donc

$$| x |^2 \geq r_m'^2 | b_m^* |^2 \geq | b_m^* |^2 .$$

Posons $m(x_j) = m(j)$ pour $j = 1, 2, \ldots, t$, on a alors

$$| x_j |^2 \geq | b_{m(j)}^* |^2 \quad \text{pour } j = 1, 2, \ldots, t .$$

Quitte à modifier l'ordre des x_j, on peut supposer que l'on a

$$m(1) \leq m(2) \leq \ldots \leq m(t) .$$

Comme les x_j sont linéairement indépendants, il est clair que l'on a $j \leq m(j)$ pour tous les indices $j = 1, 2, \ldots, t$.

D'où les inégalités

$$| b_j |^2 \leq 2^{m(j)-1} | b_{m(j)}^* |^2 \leq 2^{n-1} | b_{m(j)}^* |^2 \leq 2^{n-1} | x_j |^2 ,$$

pour $j = 1, 2, \ldots, t$.

Ce qui démontre le résultat. <

4. Algorithme de réduction .

Cet algorithme est détaillé dans [L^3] , nous donnerons seulement son énoncé.

algorithme L^3 ;

données : une base $b_1, b_2, \ldots, b_n$ quelconque d'un réseau L ;

sortie : une base réduite de L ;

{ premier pas : orthogonalisation de Gram - Schmidt }

début

pour i : = 1 **jusqu'à** n **faire**

début $b_i^* := b_i$;

pour j : = 1 **jusqu'à** i - 1 **faire**

début $\mu_{ij} := (b_i , b_j^*) / B_j$; $b_i^* := b_i^* - \mu_{ij} b_j^*$ **fin** ;

$B_i := (b_i^* , b_i^*)$

fin ;

k : = 2 ;

(**i**) Trans (k - 1) ; { la procédure trans assure la condition $| \mu_{ij} | \leq 1/2$ }

{ on teste maintenant la seconde condition au rang k }

si $B_k < (3/4 - \mu_{k\,k-1}^2) B_{k-1}$ **alors**

début

modif ; { cette procédure permute les vecteurs b_k et b_{k-1} }

si k > 2 **alors** k : = k - 1 ; { retour en arrière }

fin ;

pour h : = k - 2 , k - 3 , ... , 1 **faire** Trans (h) ;

si k = n **alors arrêt** ; { si k atteint n , on a une base réduite, on s'arrête }

k : = k + 1 ; **aller en** (**i**) ; { sinon on repart en avant }

procédure trans (h) ;

si $|\mu_{kh}| > 1/2$ **alors**

début $r := [\mu_{kh} + 1/2]$; $b_k := b_k - r\, b_h$;

pour $j := 1$ **jusqu'à** $h - 1$ **faire** $\mu_{kj} := \mu_{kj} - r\,\mu_{hj}$;

$\mu_{kh} := \mu_{kh} - r$

fin ;

procédure modif ;

début

$\mu := \mu_{k\,k-1}$; $B := B_k + \mu^2 B_{k-1}$; $\mu_{k\,k-1} := \mu\, B_{k-1} / B$;

$B_k := B_{k-1}\, B_k / B$; $B_{k-1} := B$;

permuter (b_k , b_{k-1}) ;

pour $j := 1$ **jusqu'à** $k - 2$ permuter ($\mu_{k\,j}$, $\mu_{k-1\,j}$) ;

pour $i := k + 1$ **jusqu'à** n **faire**

début $\mu' := \mu_{i\,k-1} - \mu\,\mu_{i\,k}$; $\mu_{i\,k-1} := \mu_{i\,k} + \mu_{k\,k-1}\,\mu'$; $\mu_{i\,k} := \mu'$ **fin** ;

fin ;

fin .

5. Coût de l'algorithme.

Il faut déjà montrer que l'algorithme s'arrête. Dans ce but les auteurs de [L^3] introduisent les quantités

$$d_i = |\det((b_j, b_k))_{1\le j,k\le i}| = |b_1^*|^2 \ldots |b_i^*|^2 \quad , \quad 0 \le i \le n ,$$

et

$$D = d_1 \ldots d_{n-1} .$$

De sorte que $d_0 = 1$ et $d_n = \det(L)^2$.

Au cours du déroulement de l'algorithme, le nombre D ne change que si l'un des b_i^* est modifié, ce qui ne se produit que si la condition

$$(*) \quad | b_k^* + \mu_{k\,k-1} b_{k-1}^* |^2 \geq (3/4) | b_{k-1}^* |^2$$

a lieu pour un entier $k \geq 2$. Et, dans ce cas la quantité d_{k-1} est multipliée par un facteur strictement plus petit que $3/4$ tandis que les autres termes d_i restent inchangés; donc D est réduit par un facteur $< 3/4$. Pour démontrer que l'algorithme s'arrête, il suffit donc de minorer D par une quantité > 0 qui ne dépend que du réseau L et que chaque passage dans la zone (i) de l'algorithme conduit à la modification d'au moins un des vecteurs b_i. Posons

$$m(L) = \min \{ |x|^2 ;\ x \in L, x \neq 0 \}.$$

Pour $i > 0$, le nombre d_i est égal au carré du déterminant du réseau L_i engendré par les vecteurs $b_1, \ldots, b_i$ dans l'espace $\mathbf{R} b_1 + \ldots + \mathbf{R} b_i$. On sait qu'un réseau L_i quelconque de dimension i contient un vecteur x_i qui vérifie

$$|x_i|^2 \leq (4/3)^{(i-1)/2} (\det(L_i))^{2/i},$$

voir par exemple J. W. S. Cassels .– *An introduction to the geometry of numbers*, Springer, Heidelberg, 1971 (lemme 4 du chapitre 1 et théorème 1 du chapitre 2). On en déduit la minoration

$$d_i \geq (3/4)^{i(i-1)/2} m(L)^i.$$

Comme au départ on a

$$d_i \leq |b_1|^2 \ldots |b_i|^2 \leq B^i, \quad \text{où} \quad B = \max \{ |b_k|^2 ;\ 1 \leq k \leq n \},$$

la condition (*) ne peut se produire que $O(n^2 \operatorname{Log} B)$ fois pour chaque valeur de l'entier k. On en déduit ensuite facilement que l'algorithme L^3 ne nécessite pas plus de $O(n^4 \operatorname{Log} B)$ opérations arithmétiques, et on peut vérifier que ces opérations portent sur des entiers d'au plus $O(n \operatorname{Log} B)$ chiffres binaires.

Voir [L^3] pour les démonstrations .

Des raffinements ont été apportés en particulier par les auteurs suivants :

- E. Kaltofen .– *On the Complexity of Finding Short Vectors in Integer Lattices* , EUROCAL' 83 , London , ed. van Hulzen , Lecture Notes in Computer Science , n° 162 , Springer, Heidelberg, 1983 ;

- A. Schönhage .– *Factorization of univariate integer polynomials by diophantine approximation and an improved basis reduction algorithm* , Proc. of 11-th ICALP , Antwerpen , 1984, Lecture Notes in Computer Science , n° 172, Springer, Heidelberg, 1984 ;

- C. P. Schnorr .– *A more efficient Algorithm for Lattice Basis Reduction* , manuscrit, Journal of algorithms, t. 9 , 1988, pp. 47 - 62 .

Les progrès obtenus sont assez techniques. Aussi, pour plus de détails, nous renvoyons le lecteur à ces trois articles.

6. Facteurs des polynômes et réseaux .

Dans ce paragraphe p est un nombre premier donné et k un entier strictement positif fixé.

On représente les éléments de l'ensemble $\mathbf{Z}/p^k\mathbf{Z}$ par des entiers qui appartiennent à l'intervalle $]-p^k/2\,,\ p^k/2]$ et, avec cette convention, on note $a \bmod p^k$ l'image naturelle d'un entier a dans l'ensemble $\mathbf{Z}/p^k\mathbf{Z}$.

Pour un polynôme

$$g = \sum_i a_i X^i \in \mathbf{Z}[X] ,$$

on pose

$$(g \bmod p^k) = \sum_i (a_i \bmod p^k) X^i \in (\mathbf{Z}/p^k\mathbf{Z})[X] .$$

On considère un polynôme $f \in \mathbf{Z}[X]$ de degré $n > 0$ ainsi qu'un deuxième polynôme $h \in \mathbf{Z}[X]$, de degré d, $0 < d \leq n$, possédant les propriétés suivantes :

(1°) h est unitaire,

(2°) $(h \bmod p^k)$ divise $(f \bmod p^k)$ dans $(\mathbf{Z}/p^k\mathbf{Z})[X]$,

(3°) $(h \bmod p)$ est irréductible dans $\mathbf{F}_p[X]$,

(4°) $(h \bmod p)^2$ ne divise pas $(f \bmod p)$ dans $\mathbf{F}_p[X]$.

PROPOSITION 2. – Avec les notations ci-dessus, le polynôme f admet un facteur irréductible h_0 dans $\mathbf{Z}[X]$ pour lequel $(h_0 \bmod p)$ est un multiple de $(h \bmod p)$ dans $\mathbf{F}_p[X]$.

Au signe près, le polynôme h_0 est unique.

De plus, si g est un diviseur de f dans $\mathbf{Z}[X]$ alors les propriétés suivantes sont équivalentes

(i) $(h \bmod p)$ divise $(g \bmod p)$ dans $\mathbf{F}_p[X]$,

(ii) $(h \bmod p^k)$ divise $(g \bmod p^k)$ dans $(\mathbf{Z}/p^k\mathbf{Z})[X]$,

(iii) h_0 divise g dans $\mathbf{Z}[X]$.

En particulier, $(h \bmod p^k)$ divise $(h_0 \bmod p^k)$ dans $(\mathbf{Z}/p^k\mathbf{Z})[X]$.

> L'existence de h_0 , ainsi que son unicité – au signe près – ne posent pas de difficulté.

(iii) $\Rightarrow$ **(ii)** : c'est clair.

(ii) $\Rightarrow$ **(i)** : évident.

(i) $\Rightarrow$ **(ii)** : Supposons que $f = g\,q$ dans $\mathbf{Z}[X]$ et que le polynôme $(h \bmod p)$ divise $(g \bmod p)$ dans $\mathbf{F}_p[X]$. Du fait que le carré de $(h \bmod p)$ ne divise pas $(f \bmod p)$ dans $\mathbf{F}_p[X]$, les polynômes $(h \bmod p)$ et $(q \bmod p)$ sont premiers entre eux dans $\mathbf{F}_p[X]$; il existe donc des polynômes u, v et w de $\mathbf{Z}[X]$ tels que

$$u\,h + v\,q = 1 - p\,w \quad \text{dans} \quad \mathbf{Z}[X].$$

En multipliant cette égalité par le produit $g\,.\,(1 + p\,w + \ldots + (p\,w)^{k-1})$, on obtient une relation de la forme

$$u_1\,h + v_1\,f = (1 - p^k\,w^k)\,g \quad \text{dans} \quad \mathbf{Z}[X],\ u_1 \text{ et } v_1 \in \mathbf{Z}[X].$$

D'où la propriété (ii) .

La dernière assertion est un cas particulier de l'implication (i) $\Rightarrow$ (ii) .<

Dans la suite de ce paragraphe on fixe un entier $m \geq d$, et on désigne par $\mathbf{L}$ l'ensemble des polynômes de $\mathbf{Z}[X]$ de degré au plus m dont l'image modulo p^k est divisible par $(h \bmod p^k)$ dans $(\mathbf{Z}/p^k\mathbf{Z})[X]$.

En identifiant un polynôme avec la suite de ses coefficients, on voit que $\mathbf{L}$ est un réseau de l'espace $\mathbf{R}^{m+1}$ de base

$$\{\, p^k X^i ;\ 0 \leq i < d \,\} \cup \{\, h\,X^j ;\ 0 \leq j \leq m - d \,\}.$$

Le déterminant de $\mathbf{L}$ est donc $\det(\mathbf{L}) = p^{kd}$.

La clef de l'algorithme de factorisation est le résultat suivant.

PROPOSITION 3. – Soient f et h_0 des polynômes comme dans l'énoncé de la proposition 2. Alors si b est un élément non nul du réseau L défini ci-dessus qui vérifie

$$|b|^n \, |f|^m < p^{kd},$$

le polynôme h_0 divise b dans $\mathbf{Z}[X]$.

> Posons g = p.g.c.d.(f, b). D'après la proposition 2, il suffit de montrer que le polynôme (h mod p) divise (g mod p) dans $\mathbf{F}_p[X]$. On raisonne par l'absurde, en supposant que (h mod p) ne divise pas (g mod p). Comme (h mod p) est irréductible dans $\mathbf{F}_p[X]$, il existe des polynômes u_2, v_2 et $w_2 \in \mathbf{Z}[X]$ tels que

$$(*) \quad u_2 h + v_2 g = 1 - p w_2 .$$

Posons e = deg (g), m' = deg (b) ; ainsi $0 \le e \le m' \le m$.

On définit

$$L' = \{ u f + v b + w ; \; u, v, w \in \mathbf{Z}[X], \deg(u) < m' - e, \deg(v) < n - e, \deg(w) < e \}.$$

Montrons que L' est un réseau qui admet pour base

$$\{ 1, X, ..., X^{e-1} \} \cup \{ X^i f ; \; 0 \le i < m' - e \} \cup \{ X^j b ; \; 0 \le j < n - e \}.$$

Il suffit pour cela de prouver qu'une relation de la forme

$$u f + v b = w \quad \text{avec} \quad \deg(u) < m' - e, \deg(v) < n - e, \deg(w) < e$$

implique u = v = w = 0 ; ce qui résulte aussitôt de ce que

$$\mathbf{Z}[X] . f + \mathbf{Z}[X] . b = \mathbf{Z}[X] . g \quad , \text{ puisque } g = \text{p.g.c.d. } (f, b),$$

et du fait que g est de degré e.

L'inégalité de Hadamard implique

$$\det(L') \le |f|^{m'-e} . |b|^{n-e} \le |f|^m . |b|^n < p^{kd} .$$

Nous allons maintenant minorer le déterminant de L'.

Montrons l'implication suivante

(**) $\quad z \in L'$ et $\deg(z) < e+d \Rightarrow \deg(z \bmod p) < e$.

Soit z un polynôme appartenant à L' et de degré $< e+d$. Par division euclidienne,

$$z = q\,g + r \text{ , avec } \deg(r) < e .$$

En multipliant la relation (*) par le produit $q \cdot (1 + p\,w_2 + \ldots + (p\,w_2)^{k-1})$, on aboutit à une formule du type

$$u_3\,h + v_3\,q\,g \equiv q \mod p^k \mathbf{Z}[X] \text{ , } u_3, v_3 \in \mathbf{Z}[X] .$$

Comme b appartient à L', le polynôme $(h \bmod p^k)$ divise $(g \bmod p^k)$ donc aussi $(q \bmod p^k)$. Mais, d'une part h est unitaire de degré d, et, d'autre part, le degré de q est $< d$, donc q est nul. D'où l'implication (**) cherchée.

On peut choisir une base $b_0, b_1, \ldots, b_{n+m'-e-1}$ de L' où chaque polynôme b_i est de degré i (voir par exemple Cassels, théorème I.A, chapitre I). D'après (**), le coefficient dominant de b_i est divisible par p^k pour les indices $i = e, e+1, \ldots, e+d-1$, ce qui implique

$$\det(L') > p^{kd} .$$

Contradiction. <

COROLLAIRE 1. – On conserve les notations précédentes, et on suppose que la suite $b_1, b_2, \ldots, b_{m+1}$ est une base réduite de L. On désigne par M la mesure du polynôme f. Alors,

(i) $\quad |b_1| < (p^{kd}\,|f|^{-m})^{1/n} \Rightarrow \deg(h_0) \leq m$,

(ii) si on a l'inégalité

$$p^{kd} > 2^{mn/2} \binom{2m}{m}^{n/2} |f|^m\, M^n ,$$

et si le degré du polynôme h_0 est majoré par m alors b_1 vérifie

$$|b_1| < (p^{kd}\,|f|^{-m})^{1/n} .$$

> La propriété (i) est une conséquence immédiate de la proposition puisque le polynôme b_1 est de degré au plus m.

Supposons que h_0 soit de degré au plus m, alors h_0 appartient à L et on a

$$|h_0|^2 \leq \sum_{i=0}^{m} \binom{m}{i}^2 . \text{ mes}(h_0) \leq \binom{2m}{m} . M$$

Et le corollaire 2 de la proposition 1, avec $t = 1$ et $x_1 = h_0$ donne

$$|b_1| \leq 2^{m/2} |h_0| \leq 2^{m/2} \binom{2m}{m}^{1/2} M ,$$

d'où la propriété (ii). <

COROLLAIRE 2. – On reprend les notations du corollaire précédent et on suppose que p vérifie l'inégalité

(i) $$p^{kd} > 2^{mn/2} \binom{2m}{m}^{n/2} |f|^m M^n ,$$

et qu'il existe un indice j, $1 \leq j \leq m+1$, pour lequel on a

(ii) $$|b_j| < (p^{kd} |f|^{-m})^{1/n} .$$

Soit alors t le plus grand de ces indices j ; alors on a

$$\deg(h_0) = m + 1 - t ,$$

$$h_0 = \text{p.g.c.d.}(b_1, b_2, \ldots, b_t) ,$$

et l'inégalité (ii) a lieu pour tous les indices $j \in \{1, 2, \ldots, t\}$.

> Soit J l'ensemble des entiers j, $1 \leq j \leq m+1$, tels que l'inégalité (ii) ait lieu. Le corollaire 1 nous apprend que le polynôme h_0 divise b_j pour tout indice j appartenant à J. Donc h_0 divise le p.g.c.d. des polynômes b_j, j parcourant J. Notons h_1 ce p.g.c.d. . Les polynômes b_j, $j \in J$, sont linéairement indépendants, divisibles par h_1 et de degré au plus m, d'où l'inégalité

$$\text{Card}(J) \leq m + 1 - \deg(h_1) .$$

Du fait que les polynômes $X^i h_0$ appartiennent au réseau L pour les entiers $i = 1, 2, ..., m - \deg(h_0)$, le corollaire 2 de la proposition 1 et la majoration de $|h_0|$ déjà utilisée montrent que l'on a

$$|b_j| \leq 2^{m/2} \binom{2m}{m}^{1/2} M ,$$

pour $1 \leq j \leq m + 1 - \deg(h_0)$, et donc que tous ces indices appartiennent à J, ce qui implique

$$\text{Card}(J) \geq m + 1 - \deg(h_0) .$$

En comparant la minoration et la majoration de $\text{Card}(J)$ obtenues ci-dessus, on constate que l'on a nécessairement

$$\deg(h_0) = \deg(h_1) = m + 1 - t \quad \text{et} \quad J = \{ 1, 2, ..., t \} .$$

Il ne reste plus qu'à montrer que h_1 est égal à h_0 au signe près, et pour cela il suffit de montrer que le polynôme h_1 est primitif. Soit d_1 le contenu du polynôme b_1, alors le polynôme b_1 / d_1 est divisible par h_0, donc b_1 / d_1 appartient au réseau L ; mais le polynôme b_1 étant un élément d'une base de L, on a $d_1 = 1$.

En conclusion, b_1 est primitif, donc h_1 l'est aussi.

Ce qui achève la démonstration. <

Remarque : Les preuves des propositions 1 et 2 montrent que le corollaire ci-dessus reste vrai si l'inégalité (i) est remplacée par la condition plus faible

$$p^{kd} > \beta^n \gamma^n |f|^m ,$$

où $\beta = \max \{ |b_j| / |b_i^*| ; 1 \leq j \leq i \leq m + 1 \}$

et $\gamma = \max \{ |g| ; g \in \mathbf{Z}[X], g \text{ divisant } f \}$.

7. L'algorithme de factorisation .

On considère un polynôme F de $\mathbf{Z}[X]$, quadratfrei, primitif et de degré $n > 0$ (on suppose aussi F unitaire pour simplifier). On suppose que l'on a choisi un nombre premier p, un entier $k > 0$ et calculé un polynôme $h \in \mathbf{Z}[X]$ vérifiant les propriétés 1°) à 4°) considérées au paragraphe précédent – si h est de degré n alors ($F \bmod p$) est irréductible et donc F est aussi irréductible dans $\mathbf{Z}[X]$ et l'algorithme s'arrête.

On supposera donc que h est de degré strictement inférieur à n . (On aura, par exemple, calculé ($h \bmod p$) grâce à l'algorithme de Berlekamp et raffiné le calcul modulo p^k en appliquant la méthode de Hensel) . On suppose que les coefficients du polynôme h sont réduits modulo p^k (donc compris entre $-p^k/2$ et $p^k/2$), de sorte que

$$|h|^2 \leq 1 + d \cdot p^{k}/2 \quad , \quad \text{où} \quad d = \deg(h) .$$

On considère un entier m donné $\geq d$, et on suppose que p et k vérifient l'inégalité

$$\text{(i)} \qquad p^{kd} > 2^{mn/2} \binom{2m}{m}^{n/2} |F|^m M^n .$$

Soit L le réseau considéré au paragraphe précédent, de base

$$\{ p^k X^i \; ; \; 0 \leq i < d \} \cup \{ h X^j \; ; \; 0 \leq j < m - d \} .$$

On calcule une base réduite $b_1, b_2, \ldots, b_{m+1}$ de L grâce à l'algorithme L^3 .

D'après le corollaire 2 de la proposition 2 , on a alors

- soit : $|b_1| \geq (p^{kd} |F|^{-m})^{1/n}$ et alors $\deg(h_0) > m$,
- soit : $|b_1| < (p^{kd} |F|^{-m})^{1/n}$ et alors $\deg(h_0) \leq m$ et

$$h_0 = \text{p.g.c.d.} (b_1 , b_2 , \ldots , b_t) ,$$

l'entier t étant défini comme dans le corollaire 2 de la proposition 2 .

Ce qui achève la description de l'algorithme.

Cet algorithme fournit un facteur irréductible h du polynôme F dans $\mathbf{Z}[X]$. Pour une factorisation complète de F dans $\mathbf{Z}[X]$, on peut par exemple procéder ainsi

- factoriser complètement le polynôme $(F \bmod p)$, p étant un nombre premier qui ne divise pas le discriminant de F,
- choisir un polynôme h_1 de $\mathbf{Z}[X]$ tel que $(h \bmod p)$ soit un facteur irréductible de $(F \bmod p)$,
- déterminer comme il vient d'être dit un polynôme $h_{1,0}$ de $\mathbf{Z}[X]$ qui est un facteur irréductible de F dans $\mathbf{Z}[X]$,
- si le degré du polynôme $h_{1,0}$ est strictement plus petit que celui de F, choisir un polynôme de $\mathbf{Z}[X]$ dont l'image modulo p est un facteur irréductible du polynôme

$$(F / h_{1,0} \bmod p) \text{ dans l'anneau } \mathbf{F}_p[X],$$

puis reprendre le même algorithme avec $F / h_{1,0}$ comme nouveau polynôme ... et ainsi de suite, jusqu'à ce que le polynôme considéré soit irréductible dans $\mathbf{Z}[X]$.

En tenant compte du coût de l'algorithme L^3, et en examinant les calculs auxiliaires à effectuer on démontre le résultat suivant (cf. [L^3]).

THEOREME 2 . – L'algorithme décrit ci-dessus factorise tout polynôme primitif à coefficients entiers en produit de polynômes irréductibles dans $\mathbf{Z}[X]$.

Il nécessite un nombre d'opérations en $O(n^6 + n^5 \operatorname{Log} |F|)$, ces opérations portant sur des entiers de longueur binaire $O(n^3 + n^2 \operatorname{Log} |F|)$.

Exercices

1. Soit $F \in \mathbf{Z}[X]$ un polynôme tel que $F(0)$ et $F(1)$ soient impairs. Démontrer que ce polynôme n'a pas de racine dans $\mathbf{Z}$. Qu'en est-il relativement à $\mathbf{Q}$?

2. Soit p un nombre premier et soit f un polynôme à coefficients entiers.

Démontrer que les deux propriétés suivantes sont équivalentes :

(i) $\forall\, a \in \mathbf{Z}$, $f(a) \equiv 0$ modulo p ,

(ii) $\exists\, g, h \in \mathbf{Z}[X]$, $f(X) = (X^p - X)\, g(X) + p\, h(X)$.

3. On considère la procédure suivante, due à Kronecker, pour la factorisation des polynômes à coefficients entiers.

donnée : $f \in \mathbf{Z}[X]$, de degré $d \geq 1$.

pour $s = 1, 2, \ldots, [d/2]$ **faire**

(i) choisir $s+1$ entiers $x_0, x_1, \ldots, x_s$ distincts ;

(ii) **si** il existe x_i tel que $f(x_i) = 0$ **alors renvoyer** $g = X - x_i$ et **arrêt**

sinon déterminer l'ensemble E des $(s+1)$-uples d'entiers

$(d_0, d_1, \ldots, d_s) \in \mathbf{Z}^{s+1}$ tels chacun des d_i parcourt

l'ensemble des diviseurs de $f(x_i)$;

(iii) **pour tout** $\mathbf{d} = (d_0, d_1, \ldots, d_s) \in E$ calculer le polynôme $g_{\mathbf{d}} \in \mathbf{Z}[X]$ qui vérifie $g_{\mathbf{d}}(x_i) = d_i$ pour $i = 0, 1, \ldots, s$;

si $g_{\mathbf{d}}$ divise f (dans $\mathbf{Q}[X]$) **alors renvoyer** $g_{\mathbf{d}}$ et **arrêt .**

Démontrer que si cette procédure s'arrête sans avoir renvoyé un polynôme g alors f est irréductible sur $\mathbb{Q}[X]$.

Grâce à cette méthode, démontrer que le polynôme

$$f(X) = 2X^5 + 8X^4 - 7X^3 - 35X^2 + 12X - 1$$

admet la décomposition

$$f(X) = (2X^2 + 6X - 1)(X^3 + X^2 - 6X + 1).$$

4. Démontrer que, pour tout n, le polynôme cyclotomique Φ_n est irréductible dans l'anneau $\mathbb{Q}[X]$.

[On montrera d'abord qu'il suffit de prouver l'irréductibilité de Φ_n sur $\mathbb{Z}$. On considère ensuite le polynôme minimal f sur $\mathbb{Z}$ du nombre complexe $\zeta = e^{2i\pi/n}$. Alors f divise Φ_n. Soit p un nombre premier qui ne divise pas n et soit g le polynôme minimal sur $\mathbb{Z}$ de ζ^p alors f divise $g(X^p)$ et si g est différent de f alors le polynôme Φ_n admet une racine double modulo p. Montrer que tel n'est pas le cas et conclure.]

5. Choix du module p.

Comme au paragraphe 2, on cherche une majoration du plus petit nombre premier qui ne divise pas un entier N donné (on s'intéresse en fait au cas où N est la valeur absolue du discriminant d'un certain polynôme à coefficients entiers).

1°) Soit n un entier ≥ 2. On considère le coefficient du binôme

$$C_n = \binom{2n}{n}.$$

Démontrer les implications suivantes :

(i) $n < p \leq 2n \Rightarrow p \mid C_n$,

(ii) $3n/2 < p \leq n \Rightarrow p$ ne divise pas C_n,

(iii) $p^h \mid C_n \Rightarrow p^h \leq 2n$.

En déduire la formule

$$(*) \quad 0 \leq \operatorname{Log} C_n - \sum_{n < p \leq 2n} \operatorname{Log} p \leq \sum_{\sqrt{2n} < p \leq 3n/2} \operatorname{Log} p + \rho \; ; \; 0 \leq \rho \leq \sum_{p \leq \sqrt{2n}} \operatorname{Log} n .$$

2°) Démontrer l'estimation

$$\operatorname{Log} C_n = 2n \operatorname{Log} 2 + O(\operatorname{Log} n) .$$

3°) Pour $x > 0$ réel, on pose

$$\theta(x) = \sum_{p \leq x} \operatorname{Log} p .$$

Grâce à la première inégalité de (*), démontrer la majoration

$$\theta(x) \leq 2x \operatorname{Log} 2 + O(\operatorname{Log} x) .$$

6 . On suppose que F est un polynôme à coefficients entiers et de coefficient dominant égal à $a > 1$. Démontrer que pour factoriser le polynôme F on peut considérer le polynôme $G = aF$ et se limiter à chercher les diviseurs de G dont le coefficient dominant est égal à a .

7 . Etudier la factorisation du polynôme $X^4 + 1$ dans tous les corps $\mathbf{F}_p$ et démontrer que ses facteurs irréductibles sur un tel corps sont de degré au plus égal à deux. Vérifier que ce polynôme est irréductible dans $\mathbf{Z}[X]$.

8. Soit n un entier et $p_1, \ldots, p_n$ des nombres premiers distincts.

1°) Démontrer qu'il n'existe pas de [illegible] sous la forme

$$\sum_{\sigma} \varepsilon_\sigma \sqrt{\pi_\sigma} = \sqrt{p_n} \ ,$$

σ parcourant l'en[illegible] de $\{ 1, 2, \ldots, n- \}$ et où on a posé

$$\pi_\sigma = \prod_{k \in \sigma} p_k \ .$$

[On pourra raisonner par récurrence sur n .]

2°) Démontrer que le polynôme f (X) défini par

$$f(X) = \prod_{\varepsilon_i \in \{0,1\}} \left(\sum_{i=1}^{n} \varepsilon_i \sqrt{p_i} \right)$$

est à coefficients entiers.

Grâce à la question précédente, démontrer que f est irréductible sur $\mathbf{Z}$.

3°) Démontrer que pour tout p premier le polynôme f mod p se factorise dans l'anneau $\mathbf{F}_p[X]$ en produit de facteurs irréductibles de degré au plus deux.

[Cet exemple est dû à H. P. F. Swinnerton - Dyer. On pourra consulter l'article de E. Kaltofen, *Factorization of Polynomials* paru dans l'ouvrage *Computer Algebra* , ed. B. Buchberger, G. E. Collins, R. Loos, Springer, 1982, pp. 95 -113 .]

9. Critère d'irréductibilité d'Eisenstein .

Soit

$$f(X) = X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

un polynôme à coefficients entiers tel qu'il existe un nombre premier p divisant chacun des entiers a_i mais tel que p^2 ne divise pas a_0.

Démontrer que f est irréductible sur l'anneau $\mathbf{Q}[X]$.

Application : En déduire que le polynôme cyclotomique

$$\Phi_p(X) = X^{p-1} + \ldots + X + 1$$

est irréductible sur $\mathbf{Q}[X]$. [Considérer le polynôme $\Phi_p(X+1)$.]

10. 1°) Montrer qu'il existe un polynôme linéaire à coefficients entiers qui n'admet pas de zéro dans $\mathbf{Z}$, mais qui a une racine dans tout corps fini .

[On pourra prendre par exemple le polynôme $2X + 4$.]

2°) Soient a et b deux entiers. Démontrer que si la congruence

$$a x + b \equiv 0 \pmod m$$

est résoluble pour tout module m alors l'équation $a x + b = 0$ admet une solution entière. [Considérer le module $m = a$.]

3°) Démontrer que la congruence

$$6 x^2 + 5 x + 1 \equiv 0 \pmod m$$

est résoluble pour tout module m , mais qu'elle n'admet pas de solution dans $\mathbf{Z}$.

[Pour la première assertion, on pourra factoriser le polynôme $6 x^2 + 5 x + 1$ sur $\mathbf{Z}$ puis appliquer le théorème chinois.]

11. Au chapitre VI, on a vu qu'un polynôme au hasard de degré n sur un corps fini a une probabilité voisine de $1 - 1/n$ d'être réductible. En utilisant le théorème chinois, en déduire qu'un polynôme au hasard de $\mathbf{Z}[X]$ est " presque toujours " irréductible.

12. Soit E le $\mathbf{Z}$ - module des polynômes $P \in \mathbf{Q}[X]$ tels que $P(n)$ soit entier pour tout entier n.

Démontrer que la famille des polynômes $(P_n)_{n \geq 0}$ définis par

$$P_0(X), \; P_n(X) = X(X+1)\ldots(X+n-1)/n! \quad \text{pour } n \geq 1$$

constitue une base de E sur $\mathbf{Z}$.

INDEX

Algébriquement clos (corps —), IV.1.1, *149*.
Algorithme, I.1.3, *17*.
Algorithme d'Euclide, I.8.2, *49*.
Algorithme de Berlekamp, VI.4.2, *265*.
Algorithme de factorisation de Lenstra-Lenstra-Lovász, VII.6, *332*.
Algorithme de Karatsuba, I.6.1, *34*.
Algorithme de Kronecker, VII.1.2, *306*.
Algorithme de Musser, VI.3.4, *260*.
Algorithme de réduction de Lenstra-Lenstra-Lovász, VII.5.4, *322*.
Algorithme de Tobey et Horowitz, VI.3.4, *259*.
Algorithme de Yun, VI.3.4, *260*.
Anneau de caractéristique zéro, III.5.5, *125*.
Anneau factoriel, III.4.2, *117*.
Anneau principal, III ex. 8, *131*.
Associés (éléments — d'un anneau), III.4, *116*.

Base normale, VI ex. 30, *306*.
Base réduite (d'un réseau), VII.5.3, *319*.

Caractéristique d'un corps, VI.1.1, *242*.
Caractéristique zéro (anneau de —), III.5.5, *125*.
Chiffre, I.1.2, *15*.
Coefficient (d'un polynôme), III.1.1, *104*.
Coefficient dominant (d'un polynôme), III.2.1, *108*.
Complexité (d'un algorithme), I.7.4, *46*.
Composé, I.9.1, *53*.
Congru (entiers congrus modulo *m*), I.8.4, *53*.
Congruences de Lucas, VI ex. 5, *286*.
Contenu d'un élément d'un anneau, III.4.2, *118*.
Corps algébriquement clos, IV.1.1, *13*.
Corps de décomposition d'un polynôme, VI ex. 38, *283*.
Corps des racines d'un polynôme, VI ex. 38, *283*.
Coût (d'un algorithme), I.7.1, *39*.
Critère d'irréductibilité d'Eisenstein, VII ex. 9, *338*.
Critère de Gauss, II ex. 7, *100*.
Critère de Lucas, II ex. 12, *102*.

Décomposition en éléments simples d'une fraction, I ex. 18, *69*.
Degré partiel (d'un polynôme par rapport à une variable), III.1.3, *106*.
Degré total (d'un polynôme), III.1.3, *106*.
Degré d'un corps sur un de ses sous-corps, IV ex. 38, *190*.
Dérivée d'un polynôme, III.5.4, *124*.
Déterminant d'un réseau, VII.5.1, *318*.
Développement en base *b*, I.1.2, *15*.
Discriminant d'un polynôme, III.6, *129*.
Diviser, I.5, *30*.
Diviseur, I.5, *30*.
Division euclidienne (d'un polynôme par un autre), III.2.2, *108*.
Division euclidienne (sur les entiers), I.5, *30*.

Elément irréductible (d'un anneau), III.4, *116*.
Elément primaire (d'un anneau), IV ex. 23, *194*.
Elément primitif (modulo p), II.1.2, *76*.
Elément primitif d'un corps fini, VI.1.3, *246*.
Eléments associés (d'un anneau), III.4, *116*.
Entier algébrique, III ex. 28, *137*.
Euler (fonction phi d'—), I.9.1, *53*.

Facteur primaire d'un polynôme, IV ex. 23, *194*.
Factorisation d'un entier, I.3, *34*.
Factoriel (anneau —), III.4.2, *117*.
Fermat (méthode de factorisation de —), II.3.2, *95*.
Fonction génératrice, VI ex. 3, *282*.
Fonction phi d'Euler, I.9.1, *53*.
Fonction-polynôme, III.5.1, *121*.
Fonction de Möbius, VI.2.1, *247*.
Fonction symétrique élémentaire, III ex. 16, *134*.
Formule d'inversion de Möbius, VI.2.1, *247*.
Formule de Leibnitz, III ex. 14, *134*.
Formule de Newton, III ex. 18, *135*.
Formule de Parseval, IV.4.3, *170*.
Formule de Taylor (en plusieurs variables), III ex. 13, *134*.
Formule de Taylor (en une variable), III.5.5, *125*.
Formule de Vandermonde, III ex. 29, *140*.

Générateur (d'un idéal), III.2.3, *110*.

Hauteur (d'un nombre algébrique), IV ex. 16, *189*.
Hauteur (d'un polynôme), IV.4.1, *168*.
Homogène (polynôme), III ex. 1, *130*.

Idéal principal, III.2.3, *110*.
Idempotent (d'un anneau), III.3, *115*.
Idempotent primitif (d'un anneau), VI.4.4, *270*.
Idempotents orthogonaux, I ex. 18, *69*.
Indéterminée (d'un polynôme), III.1.1, *13*.
Inégalité d'Euler, V ex. 6, *229*.
Inégalité de Hadamard, VII.5.2, *319*.
Inégalité de Jensen, IV.4.3, *170*.
Inégalité de Landau, IV.3.2, *161*.
Inégalité de Liouville, IV ex. 10, *187*.
Inégalité de Tchebytcheff, VI.2.4, *256*.
Inégalité entre moyennes géométrique et arithmétique, V ex. 8, *232*.
Intègre (anneau), III.1.4, *107*.
Irréductible (élément — d'un anneau), III.4, *116*.

Lemme de Gauss, III.4.2, *118*.
Lemme de Hensel, VII.3.2, *312*.
Lemme de Segner, V ex. 2, *226*.
Lexicographique (ordre —), I.1.1, *13*.
Lexicographique (produit —), I.1.1, *13*.
Loi de réciprocité quadratique, VI ex. 21, *300*.
Longueur (d'un polynôme), IV.4.1, *168*.

Matrice compagnon d'un polynôme, VI ex. 8, *289*.
Matrice de Sylvester (de deux polynômes), III.6, *127*.
Mesure (d'un polynôme en plusieurs variables), IV.4.3, *169*.
Mesure (d'un polynôme en une variable), IV.3.1, *158*.
Mesure d'un nombre algébrique, IV.3.1, *159*.
Mesure de Mahler (d'un polynôme), IV.3.1, *158*.
Méthode d'Uspensky, V.4.6, *222*.
Méthode de Berlekamp, VII.4, *316*.
Méthode de Camion-Cantor-Zassenhaus, VI.4.4, *269*.
Méthode de Collins-Akritas, V.4.6, *222*.
Méthode de factorisation de Fermat, II.3.2, *95*.
Méthode de factorisation de Sherman-Lehmann, II.3.3, *95*.

Méthode de factorisation par divisions successives, II.3.1, *93*.
Méthode de Graeffe, IV.3.6, *164*.
Méthode de Karatsuba, I.6.1, *34*.
Méthode de Lagrange, III.3, *114*.
Méthode de MacEliece, VI.4.6, *272*.
Méthode de Newton (pour le théorème chinois), III.3, *114*.
Méthode de Newton (pour calculer u/v), I ex. 20, *70*.
Méthode de Newton (pour le calcul d'une racine), V.3.5, *213*.
Méthode de Zassenhaus, VI.4.4, *267*.
Méthode rho de Pollard, II.3.4, *97*.
Monôme, III.1.1, *104*.
Multiple, I.5, *30*.
Multiplicité d'une racine d'un polynôme, III.5.3, *122*.

Nombre de Carmichael, I.11, *63*.
Nombre de Fermat, II ex. 5, *99*.
Nombre de Liouville, IV ex. 10, *187*.
Nombre de Mersenne, II ex. 12, *102*.
Nombre d'or, II ex. 12, *92*.
Nombre premier, I.9, *53*.
Nombre transcendant, IV ex. 10, *187*.
Non-résidu quadratique (modulo p), II.1.2, *77*.
Non constant (polynôme —), IV.1.1, *149*.

Ordre (d'un élément dans un groupe), II.1.1, *72*.
Ordre d'un élément d'un anneau selon un élément irréductible, III.4.2, *117*.
Ordre d'une racine d'un polynôme, III.5.3, *122*.
Ordre lexicographique, I.1.1, *13*.
Orthogonalisation de Gram-Schmidt, VII.5.2, *318*.

p.g.c.d. (de deux entiers), I.8.1, *47*.
p.g.c.d. (de plusieurs polynômes), III.2.3, *111*.
p.p.c.m., I.8.4, *52*.
Période d'un polynôme, VI ex. 10, *292*.
Polynôme, III.1.1, *104*.
Polynôme cyclotomique, VI.1.3, *246*.
Polynôme de Lagrange, III ex. 5, *131*.
Polynôme d'Hermite, III ex. 6, *131*.
Polynôme homogène, III ex. 1, *130*.
Polynôme minimal d'un nombre algébrique, IV.3.1, *158*.
Polynôme non constant, IV.1.1, *149*.
Polynôme primitif, VII.1.1, *305*.
Polynôme quadratfrei, VI.3.1, *255*.
Polynôme réciproque, IV.2.3, *157*.
Premier (nombre —), I.9.1, *53*.
Premiers entre eux (entiers —), I.8.1, *48*.
Premiers entre eux (polynômes —), III.2.3, *110*.
Primaire (élément — d'un anneau), IV ex. 23, *194*.
Principal (anneau —), III ex. 8, *131*.
Principe du maximum, IV ex. 21, *193*.
Produit lexicographique, I.1.1, *13*.
Pseudo-division euclidienne (d'un polynôme par un autre), III.2.4, *112*.
Pseudo-quotient (de la division d'un polynôme par un autre), III.2.4, *112*.
Pseudo-reste (de la division d'un polynôme par un autre), III.2.4, *112*.

Quadratfrei (nombre entier —), II.2.1, *84*.
Quadratfrei (polynôme —), VI.3.1, *255*.
Quotient (de la division euclidienne), I.5, *30*.

Racine d'ordre k d'un polynôme, III.5.3, *122*.
Racine d'un polynôme, III.5.2, *122*.
Racine multiple d'un polynôme, III.5.3, *122*.
Rang d'un réseau, VII.5.1, *318*.
Règle de Cauchy, V.3.4, *201*.
Règle de Descartes, V.4.3, *208*.
Règle de Descartes (cas particulier), V.3.3, *201*.
Règle de Lagrange et MacLaurin, V.3.2, *200*.
Règle de Laguerre, V ex. 12, *234*.
Règle de Newton, V.3.1, *200*.
Règle de Sturm, V.4.1, *203*.

Règle de Sturm, V ex. 18, *236*.
Relation de Bézout, I.8.1, *48*.
Relation d'Euclide, III ex. 2, *130*.
Représentation (d'un entier en base *b*), I.1, *13*.
Réseau, VII.5.1, *318*.
Résidu quadratique (modulo *p*), II.1.2, *77*.
Reste (de la division euclidienne), I.5, *30*.
Résultant (de deux polynômes), III.6, *127*.

Séparation des racines d'un polynôme, IV.6.1, *178*.
Substituée (valeur — à une variable), III.5.1, *121*.
Substitution d'une valeur à une variable, III.5.1, *121*.
Suite de Fibonacci, I.7.3, *44*.
Suite de Sturm, VI.3.1, *249*.
Symbole de Jacobi, II.1.2, *78*.
Symbole de Kronecker, III.3, *114*.
Symbole de Legendre, II.1.2, *77*.
Système de représentants des éléments irréductibles, III.4.2, *118*.

Test de primalité de Miller-Rabin, II.2.3, *89*.
Test de primalité de Solovay-Strassen, II.2.3, *89*.
Théorème chinois (pour les entiers), I.10, *58*.
Théorème chinois (cas général), III.3, *113*.
Théorème d'Erdös-Turan, IV.5.2, *177*.
Théorème d'Euclide-Gauss, I.8.1, *48*.
Théorème d'Euler, I.9.2, *54*.
Théorème de Schmidt-Schur, IV.5.1, *175*.
Théorème de Budan-Fourier, V.4.2, *206*.
Théorème de Chevalley-Warning, VI ex. 16, *295*.
Théorème de d'Alembert, IV.1.1, *149*.
Théorème de de Gua, V ex. 4, *227*.
Théorème de Fermat, I.11, *62*.
Théorème de Gauss-Lucas, IV ex. 1, *184*.
Théorème de Hurwitz-Routh, V.5, *223*.
Théorème de Hurwitz-Budan-Fourier, V ex. 24, *239*.
Théorème de Jensen, V ex. 13, *235*.
Théorème de König-Rados, VI ex. 15, *294*.
Théorème de Kronecker, VI ex. 16, *282*.
Théorème de la base normale, VI ex. 30, *303*.
Théorème de Lagrange, V.9.2, *237*.
Théorème de Laguerre, V ex. 16, *236*.
Théorème de Lamé, I.8.3, *51*.
Théorème de Lehmer, VI.5.3, *278*.
Théorème de McCoy, III ex. 22, *136*.
Théorème de Riez, V ex. 7, *230*.
Théorème de Rolle, V.2.2, *198*.
Théorème de Rouché, IV.3.5, *164*.
Théorème de Sturm, V.4.1, *203*.
Théorème de Swan, VI ex. 20, *299*.
Théorème de Szegö, IV.3.5, *163*.
Théorème de Vicente Gonçalves, IV.3.2, *160*.
Théorème de Vincent, V.4.6, *214*.
Théorème de Wedderburn, VI.1.1, *242*.
Théorème des accroissements finis, V.2.2, *245*.
Théorème des valeurs intermédiaires, V.2.1, *243*.

Unitaire (polynôme), III.2.1, *108*.

Variable (d'un polynôme), III.1.1, *104*.

Zéro (d'un polynôme), III.5.2, *122*.

NOTATIONS

$(r_0\, r_1 \ldots r_{k-1})_b$	Ecriture d'un entier en base b, I.1.1, *15*.
$a \bmod b$	a modulo b, I.1.4, *17*.
$a \operatorname{div} b$	Quotient entier de a par b, I.1.4, *18*.
signe (n)	Signe d'un nombre, I.1.5, *21*.
$b \mid a$	b divise a, I.5.1, *30*.
$d\mathbf{Z}$	Ensemble des multiples de d, I.5.1, *30*.
$[x]$	Partie entière du nombre réel x, I.5.2, *32*.
$\log x$	Logarithme binaire, I.7.2, *41*.
(a, b)	p.g.c.d. des entiers a et b, I.8.1, *47*.
$[a, b]$	p.p.c.m. des entiers a et b, I.8.4, *52*.
$\mathbf{Z}/n\mathbf{Z}$	{ Classes d'entiers modulo n }, I.8.4, *53*.
$a \equiv b \pmod m$	a congru à b modulo c, I.8.4, *53*.
$G(n)$	{ Eléments inversibles de $\mathbf{Z}/n\mathbf{Z}$ }, I.9.1, *53*.
$\varphi(n)$	Fonction phi d'Euler, I.9.1, *53*.
ordre $G(x)$	Ordre d'un élément d'un groupe G, II.1.1, *72*.
$\left(\frac{a}{p}\right)$	Symbole de Legendre, II.1.2, *77*.
$\left(\frac{a}{b}\right)$	Symbole de Jacobi, II.1.2, *78*.
$\lambda(n)$	p.p.c.m. des ordres des $x \in G(n)$, II.1.5, *81*.
$\omega(n)$	Nombre de diviseurs premiers de n, II.2.1, *84*.
$P(n)$	Plus grand facteur premier de n, II.3.1, *94*.
A[X, Y...]	Anneau des polynômes en X, Y..., III.1.1, *104*.
deg (P)	Degré (total) d'un polynôme, III.1.3, *106*.
$\deg_X(P)$	Degré partiel en X d'un polynôme, III.1.3, *106*.
(F, G, ...)	Idéal engendré par F, G..., III.2.3, *110*.
$\operatorname{ord}_p(x)$	Ordre de x relativement à p, III.4.2, *118*.
$\operatorname{cont}_{\mathscr{P}}(x)$	Contenu de x relativement à $\mathscr{P}$, III.4.2, *118*.
F'	Dérivée d'un polynôme F, III.5.4, *124*.
$F^{(i)}$	Dérivée i-ème d'un polynôme F, III.5.4, *124*.
$\operatorname{Res}_X(f, g)$	Résultant de f et g par rapport à X, III.6, *127*.
Discr (f)	Discriminant du polynôme f, III.6, *129*.
ord (F, a)	III ex. 12, *132*.
M(P)	Mesure de Mahler du polynôme P, IV.3.1, *158*.
$\|\| P \|\|$ (ou $\|\| P \|\|_2$)	Norme quadratique du polynôme P, IV.3.1, *158*.
$M(\alpha)$	Mesure d'un nombre algébrique, IV.3.1, *160*.

L(P)	Longueur d'un polynôme P, IV.4.1, *168*.
H(P)	Hauteur d'un polynôme P, IV.4.1, *168*.
sep (P)	Distance minimale entre racines, IV.6.1, *178*.
V(x)	Nombre de chg. de signe (Sturm), V.3.1, *203*.
v(x)	*Idem* (au sens de Budan-Fourier), V.3.1, *206*.
$\mathbf{F}_q$	Corps à q éléments, VI.1.1, *243*.
Ω_p	Clôture algébrique de $\mathbf{F}_p$, VI.1.1, *243*.
$\mathbf{F}_q^*$	{ Eléments non nuls de $\mathbf{F}_q$ }, VI.1.1, *243*.
Φ_n	Polynôme cyclotomique d'ordre n, VI.1.5, *248*.
$\mu(n)$	Fonction de Möbius, VI.2.1, *249*.
$\omega(F)$	Nombre de fact. irré. distincts de F, VI.2.4, *252*.
$L : A \to A$	Appl. de Berlekamp, $\alpha \to \alpha^q - \alpha$, VI.4.1, *263*.
$\#(E)$	Cardinal de l'ensemble E, VI ex. 15, *294*.
$u^h \mid\mid v$	$u^h \mid v$ mais u^{h+1} ne divise pas v, VI ex. 23, *302*.
det (L)	Déterminant du réseau L, VII.5.1, *318*.

Imprimé en France
Imprimerie des Presses Universitaires de France
73, avenue Ronsard, 41100 Vendôme
Avril 1989 — N° 34 534

Les ordinateurs réalisent maintenant la plupart des calculs algébriques ou analytiques exigés par les exercices de mathématiques des lycées. Cet ouvrage présente les outils mathématiques utilisés dans les programmes qui effectuent ces calculs.

Le but principal poursuivi est la factorisation des polynômes. La première partie de cet ouvrage traite de l'arithmétique élémentaire et contient des résultats qui sont aussi utiles en cryptographie.

165 FF

22406468 / 4 / 89

9 782130 422594