

Chapitre 1

Équations, corps et polynômes

Sommaire

1 Les équations algébriques : petit historique	2
1.1 Des origines à la Renaissance	2
1.2 Lagrange et Gauss	5
1.3 Galois et la transformation de l'algèbre	8
2 Polynômes à coefficients dans un corps	10
2.1 L'arithmétique de $\mathbb{K}[X]$: rappel	10
2.2 Irréductibles de $\mathbb{K}[X]$	11
2.3 Séparabilité (I)	14
2.4 Irréductibilité dans $\mathbb{Q}[X]$	15
2.5 (*) Un élément de $\mathbb{Z}[X]$ est en général irréductible sur \mathbb{Q}	20
3 Racines de l'unité	23
3.1 Groupes de racines de l'unité	23
3.2 Polynômes cyclotomiques (I)	25
4 Polynômes symétriques	27
4.1 Le théorème des polynômes symétriques	28
4.2 (*) Retour à Lagrange	33
4.3 Discriminant	34
4.4 (*) Résultant	37
4.5 (*) Les sommes de Newton	40
5 (*) Appendice : le théorème de d'Alembert-Gauss	42
5.1 Démonstrations topologiques et/ou analytiques	43
5.2 Démonstration par les fonctions symétriques	49

En guise d'introduction

Jusqu'au milieu du dix-neuvième siècle, les objets centraux de l'algèbre sont les équations algébriques. En 1930, le livre de Van der Waerden donne une présentation de l'algèbre fondée sur les structures. En une centaine d'année, les centres d'intérêt des algébristes ont donc considérablement évolué. Dans cette évolution, le travail de Galois, qui date de 1830, mais n'a été véritablement apprécié qu'aux alentours de 1870, a joué un rôle décisif. Cette place charnière et son intérêt intrinsèque en font un terrain privilégié pour une initiation à l'algèbre. Tel est l'objet de ce cours, qui a pour prérequis les premières notions sur les groupes, les polynômes et l'algèbre linéaire.

Ce qu'on appelle aujourd'hui « théorie de Galois » peut être exposé en peu de pages. Le caractère profus du présent texte s'explique par les raisons suivantes.

- Les exemples et exercices sont très nombreux. Pour ces derniers, les numéros entre ① et ⑤ donnent une indication de difficulté.

- J'ai essayé de mettre en évidence l'évolution de l'algèbre évoquée plus haut. En particulier, et quoique le point de vue adopté ici soit celui de Dedekind-Noether-Artin, fondé sur les extensions et les morphismes¹, j'ai, pour certains résultats, mentionné des démonstrations alternatives très « dix-neuvième siècle », reposant sur le théorème des polynômes symétriques.

- Le texte comporte un certain nombre de digressions, qui développent des notions intéressantes, liées aux objets étudiés, mais qui n'ont pas forcément un lien direct avec les équations algébriques et la théorie de Galois.

Chaque chapitre est précédé d'une description de son contenu. On propose le plan d'un exposé allégé, trame du cours oral. Les sections, paragraphes ou alinéas facultatifs sont repérés par le symbole (*).

Présentation du chapitre

Ce premier chapitre est un peu fourre-tout : on y trouve une mise en perspective historique, un certain nombre de résultats utilisés dans la suite (polynômes irréductibles, racines de l'unité, polynômes symétriques, discriminant), quelques compléments (résultant, sommes de Newton, démonstrations variées du théorème de d'Alembert-Gauss). Le contenu essentiel pour la suite est constitué des paragraphes 2.1 à 2.4, de la section 3 et des paragraphes 4.1 et 4.3. Il est souhaitable de lire la section 1, à titre de mise en contexte, sans cependant entrer dans les détails.

1 Les équations algébriques : petit historique

1.1 Des origines à la Renaissance

Pendant très longtemps, l'Algèbre s'est identifiée à l'étude des *équations algébriques*, c'est-à-dire polynomiales. La résolution de l'équation de degré 1 est immédiate. La mise sous forme canonique ramène une équation de degré 2 à l'extraction d'une racine carrée ; elle était en substance connue des Babyloniens, vers -2000 av J.C. Voici un exemple, lié à la construction du pentagone régulier.

Exercice 1. ② Soit $z = \exp\left(\frac{2ik\pi}{5}\right)$. En remarquant que : $\sum_{k=0}^4 z^k = 0$ et que $2 \cos\left(\frac{2\pi}{5}\right) = z + \frac{1}{z}$, trouver une équation de degré 2 satisfaite par $2 \cos\left(\frac{2\pi}{5}\right)$ et montrer que

$$\cos\left(\frac{2\pi}{5}\right) = \frac{-1 + \sqrt{5}}{4}.$$

Calculer également $\sin\left(\frac{2\pi}{5}\right)$, ainsi que la longueur des côtés d'un pentagone régulier inscrit dans un cercle de rayon 1.²

1. Cette présentation, bien adaptée à ce niveau, notamment par l'utilisation systématique de l'algèbre linéaire, gagne d'ailleurs à être complétée par la reformulation grothendickienne de la théorie de Galois (circa 1960).

2. On notera l'apparition du nombre d'or. La construction du pentagone régulier est le point culminant du quatrième livre d'Euclide (circa -300) ; le pentagone réapparaît dans le livre XIII, à propos de l'icosaèdre et du dodécaèdre. Pour nous, la construction se déduit des résultats de cet exercice (cf. chapitre 2, section 5), mais Euclide, qui ne dispose ni du cosinus ni des nombres complexes, procède de manière plus géométrique.

La résolution de l'équation du second degré pose la question suivante : peut-on résoudre par radicaux une équation algébrique de degré n , c'est-à-dire exprimer les solutions à partir des coefficients par des formules mettant en jeu les opérations de corps (i.e. les quatre opérations de l'arithmétique élémentaire) et l'extraction de radicaux ? Entre 1500 et 1550, des algébristes italiens (del Ferro, Cardan, Tartaglia, Bombelli, Ferrari) ont répondu positivement à cette question pour les équations de degré 3 et 4.

Expliquons, avec les notations actuelles³, la méthode de Cardan pour les équations de degré 3. Une remarque préliminaire est qu'une équation polynomiale de degré n :

$$(1) \quad x^n + \sum_{i=0}^{n-1} a_i x^i = 0$$

peut être ramenée, par translation de la variable, à une équation sans terme de degré $n-1$. Posons en effet $x = y + h$. L'équation en y déduite de (1) s'écrit

$$(2) \quad y^n + \sum_{i=0}^{n-1} b_i y^i = 0$$

où $b_{n-1} = a_{n-1} + nh$. Pour $h = -\frac{a_{n-1}}{n}$, (2) n'a pas de terme de degré $n-1$.

Les nombres complexes ont été inventés par les algébristes de la Renaissance, justement pour résoudre les équations de degré 3 à coefficients réels. Nous faisons ici une entorse à l'histoire et considérons l'équation

$$(3) \quad z^3 + pz + q = 0$$

à coefficients complexes p et q et d'inconnue complexe z . La méthode de Cardan consiste à écrire z comme somme de deux nombres complexes u et v , en imposant à u et v de vérifier une relation supplémentaire permettant une « résolution par radicaux ». L'équation (3) se réécrit

$$(4) \quad u^3 + v^3 + (3uv + p)(u + v) + q = 0,$$

ce qui suggère d'imposer $3uv = -p$. C'est possible : étant donnés deux nombres complexes a et b , le système

$$x_1 + x_2 = a, \quad x_1 x_2 = b$$

admet bien des solutions, à savoir les couples (x_1, x_2) de solutions de l'équation du second degré

$$t^2 - at + b = 0.$$

Le point-clé est alors que l'on connaît somme et produit de u^3 et v^3 :

$$(5) \quad u^3 + v^3 = -q, \quad u^3 v^3 = -\frac{p^3}{27}.$$

Autrement dit, u^3 et v^3 vérifient l'équation du second degré

$$(6) \quad t^2 + qt - \frac{p^3}{27} = 0.$$

3. Les algébristes italiens traitent des exemples numériques ; ils les classent selon des critères pour nous artificiels, qui s'expliquent par l'inadéquation de la notation algébrique. C'est ainsi que Cardan note l'équation $x^2 + 12x = 48$ sous la forme

1. quad. p : 12 pos. aeq. 48.

Posons alors⁴ :

$$\Delta = -(4p^3 + 27q^2).$$

Les solutions de (6) sont les deux nombres $\frac{-q}{2} \pm \frac{\sqrt{-\Delta}}{6\sqrt{3}}$, où $\sqrt{-\Delta}$ désigne l'une des racines carrées de $-\Delta$ dans \mathbb{C} . Les solutions de (3) sont donc les $u - \frac{p}{3u}$ où u est l'une des racines cubiques de $\frac{-q}{2} + \frac{\sqrt{-\Delta}}{6\sqrt{3}}$. On obtient ainsi les *formules de Cardan* pour les racines :

$$\sqrt[3]{\frac{-q}{2} + \frac{\sqrt{-\Delta}}{6\sqrt{3}}} - \frac{p}{3} \left(\sqrt[3]{\frac{-q}{2} + \frac{\sqrt{-\Delta}}{6\sqrt{3}}} \right)^{-1}.$$

Ces formules, inutilisables en vue de calculs approchés, ont peu d'intérêt « pratique ». Mais elles montrent que l'équation est résoluble par radicaux.

Exercice 2. ① Résoudre dans \mathbb{C} l'équation $z^3 - 6z - 40 = 0$. En déduire que

$$\sqrt[3]{20 + 14\sqrt{2}} + \sqrt[3]{20 - 14\sqrt{2}} = 4.$$

Exercice 3. ③ Trouver, par une méthode analogue à celle de l'exercice 1, une équation de degré 3 satisfaite par $\cos\left(\frac{2\pi}{7}\right)$; résoudre cette équation par la méthode de Cardan.

Exercice 4. ④ Soit $P = X^3 + pX + q \in \mathbb{C}[X]$. Montrer, sans utiliser les formules de Cardan, que P est à racines simples si et seulement si $\Delta \neq 0$.

Exercice 5. ③ Soit $P = X^3 + pX + q \in \mathbb{R}[X]$. Discuter le nombre de racines réelles de P en fonction du signe de Δ (cf. aussi exercice 73, 4.3).

L'équation de l'exercice ci-après a conduit Bombelli aux nombres complexes.⁵

Exercice 6. ② Soit $P = X^3 - 15X - 4$. Vérifier que 4 est racine de P , déterminer les autres racines. Calculer par ailleurs ces racines par la méthode de Cardan et constater que ce calcul conduit à des nombres complexes, bien que P soit scindé sur \mathbb{R} .

L'exercice ci-après propose la résolution de l'équation de degré 4 par la méthode de Ferrari.

Exercice 7. ③ On se propose de montrer comment une équation de degré 4 peut être ramenée à une équation de degré 3. On peut se borner au cas d'une équation de la forme $P(z) = 0$ où :

$$P = X^4 + pX^2 + qX + r, \quad \text{avec } (p, q, r) \in \mathbb{C}^3.$$

a) Soit $\lambda \in \mathbb{C}$. Expliciter un polynôme complexe T_λ de degré au plus 2 tel que :

$$P(X) = \left(X^2 + \frac{\lambda}{2} \right)^2 - T_\lambda(X).$$

4. Le signe $-$ tient au fait que Δ ainsi défini est le *discriminant* du polynôme $X^3 + pX + q$; cf. 4.3.

5. La situation apparemment paradoxale que cet exercice met en évidence vaut pour tous les polynômes de degré 3 réels de discriminant négatif : les racines sont réelles, mais les formules de Cardan conduisent à des imaginaires. C'est le *casus irreducibilis* des algébristes italiens. À la fin du dix-neuvième siècle, Hölder a expliqué ce phénomène à l'aide de la théorie de Galois (chapitre 5).

b) Montrer que T_λ est le carré d'un polynôme de degré 1 si et seulement si λ vérifie une équation de degré 3 que l'on précisera. En déduire une méthode de résolution d'une équation du quatrième degré ne faisant intervenir que les opérations de corps et l'extraction de racines carrées et cubiques.

On peut abaisser le degré de certaines équations algébriques. Un cas immédiat est celui d'une équation « en z^m » :

$$Q(z^m) = 0 \quad \text{avec} \quad Q \in \mathbb{K}[X], \quad m \geq 2.$$

L'exercice suivant étudie le cas des équations réciproques.

Exercice 8. ④ Soient $n \in \mathbb{N}^*$, $P \in \mathbb{C}[X]$ un polynôme réciproque de degré $2n$:

$$P = \sum_{k=0}^{2n} a_k X^k, \quad \text{où} \quad \forall k \in \{0, \dots, 2n\}, \quad a_k = a_{2n-k}.$$

Montrer qu'il existe $Q \in \mathbb{C}[X]$ de degré n tel que $P(X) = X^n Q\left(X + \frac{1}{X}\right)$. Qu'en déduit-on sur la résolution de l'équation $P(x) = 0$?

1.2 Lagrange et Gauss

Les calculs du paragraphe précédent, ingénieux mais mystérieux, n'expliquent pas « pourquoi » les équations de degré 3 ou 4 se résolvent par radicaux. D'autre part, ils ne se laissent pas généraliser aux degrés supérieurs.

Il faut plus de deux siècles pour que la compréhension des méthodes de résolution progresse significativement. Ce laps de temps permet d'améliorer la notation algébrique⁶, d'asseoir la place des nombres complexes, de dégager le lien entre multiplicité d'une racine et dérivation et de dépasser les formules de Viète en dégagant le théorème des polynômes symétriques, que nous démontrerons en 4.1 (mais dont la preuve est accessible dès maintenant).

Durant cette période, apparaissent également des résultats de nature différente, liés à la localisation des racines d'une équation, comme la règle de Descartes de l'exercice ci-après ; nous n'en parlerons pas davantage.⁷

Exercice 9. ④ Appelons nombre de changements de signe de la suite réelle presque nulle $(a_i)_{i \in \mathbb{N}}$ le nombre d'indices $i \in \mathbb{N}$ tels qu'existe $k \in \mathbb{N}^*$ tel que $a_i a_{i+k} < 0$ et

$$\forall j \in \{1, \dots, k-1\}, \quad a_{i+j} = 0.$$

Établir la règle de Descartes : si $P \in \mathbb{R}[X] \setminus \{0\}$, le nombre de racines de P dans \mathbb{R}^{+*} est majoré par le nombre de changements de signes de la suite de ses coefficients.

Exercice 10. ⑤ a) Soient $P \in \mathbb{R}[X]$ non constant, $(a, b) \in \mathbb{R}^2$ tel que $a < b$ et $P(a)P(b) \neq 0$. Pour x dans \mathbb{R} , soit $\delta(x)$ le nombre de changements de signe de la suite $(P^{(i)}(x))_{i \in \mathbb{N}}$. Établir le théorème de Fourier : le nombre de racines de P dans $[a, b]$ comptées avec multiplicité est de la forme $\delta(a) - \delta(b) - 2m$ avec $m \in \mathbb{N}$.

b) Retrouver la règle de Descartes à partir du théorème de Fourier.

6. C'est seulement avec Viète qu'apparaissent, à la fin du seizième siècle, les équations à coefficients littéraux, avec des usages d'écriture encore éloignés des nôtres. Les notations employées par Descartes dans *La Géométrie* (1637) commencent à ressembler à celles que nous employons.

7. Ces études se poursuivront jusqu'au vingtième siècle : théorème de Fourier (exercice 10) et théorème de Sturm sur les racines réelles, théorème de Gauss-Lucas, forme d'apolarité et théorème de Grace ...

L'exercice ci-après demande une certaine pratique des formules de Viète. Il introduit un type de calcul destiné à simplifier une équation, souvent nommé *transformation de Tschirnhaus*.

Exercice 11. ③ Soient \mathbb{K} un corps de caractéristique nulle, Ω un surcorps algébriquement clos de \mathbb{K} .

a) Soit $U \in \mathbb{K}[X]$ de degré $n \geq 2$. Montrer que les coefficients de X^{n-1} et X^{n-2} dans U sont nuls si et seulement si la somme des racines et la somme des carrés des racines de U sont nulles.

b) On veut ramener la résolution d'une équation de degré n à celle d'une équation de degré 2 et d'une équation de degré n sans terme en X^{n-1} et sans terme en X^{n-2} . On fixe donc $P \in \mathbb{K}[X]$ unitaire de degré n , que l'on écrit

$$P = \prod_{i=1}^n (X - x_i), \quad (x_1, \dots, x_n) \in \Omega^n.$$

Quitte à changer P en $P(X+h)$ avec h dans \mathbb{K} bien choisi, on suppose que P n'a pas de terme en X^{n-1} . Pour a et b dans Ω , soit

$$Q_{a,b} = \prod_{i=1}^n (X - (x_i^2 + ax_i + b)).$$

Déduire de a) l'existence de $a \in \Omega$ vérifiant une équation de degré 2 sur \mathbb{K} et de $b \in \mathbb{K}$ de sorte que $Q_{a,b}$ n'ait ni terme en X^{n-1} , ni terme en X^{n-2} .

c) Retrouver la résolubilité par radicaux de l'équation de degré 3.

Lagrange et l'équation générale

Dans ses *Réflexions sur la résolution algébrique des équations* (1770), Lagrange étudie l'« équation générale »⁸ de degré n . Il commence par une analyse des méthodes de résolution des équations de degré 3 et 4 mettant en lumière le rôle du groupe des permutations des racines.

Partons d'un polynôme de degré 3 de $\mathbb{C}[X]$:

$$P = X^3 + pX + q = (X - z_1)(X - z_2)(X - z_3),$$

où les z_i sont des nombres complexes. Les formules de Viète s'écrivent

$$z_1 + z_2 + z_3 = 0, \quad z_1z_2 + z_2z_3 + z_3z_1 = p, \quad z_1z_2z_3 = -q.$$

Lagrange observe que les méthodes de résolution de l'équation $P(z) = 0$ passent par la mise en évidence d'une équation de degré 2 satisfaites par des fonctions polynomiales de z_1, z_2, z_3 . Chez Cardan, ces quantités intermédiaires sont, en reprenant les notations de **1.1**, u^3 et v^3 .

Pour y voir plus clair, Lagrange exprime u^3 et v^3 en fonction des x_i : u et v sont racines du polynôme

$$Q = X^6 + qX^3 - \frac{p^3}{27}.$$

Les racines de Q sont de la forme y_1, jy_1, j^2y_1 et y_4, jy_4, j^2y_4 où j est une racine cubique de 1 autre que 1 et où $3y_1y_4 = -p$. Quitte à réindexer, z_1, z_2, z_3 sont donc donnés par

$$z_1 = y_1 + y_4 \quad z_2 = jy_1 + j^2y_4 \quad z_3 = j^2y_1 + jy_4.$$

8. Ce terme sera défini précisément dans le chapitre 2. Il s'agit d'une équation dont les coefficients ne vérifient aucune relation algébrique à coefficients dans \mathbb{K} .

Par suite

$$y_1 = \frac{z_1 + j^2 z_2 + j z_3}{3} \quad y_4 = \frac{z_1 + j z_2 + j^2 z_3}{3}.$$

Récapitulons : si z_1, z_2, z_3 sont les solutions de l'équation initiale, y_1 et y_4 ont leur cube qui est solution d'une même équation de degré 2.

Lagrange renverse alors cette approche et donne une nouvelle présentation, plus éclairante, de la méthode de Cardan. Si on introduit a priori

$$\alpha = z_1 + j z_2 + j^2 z_3 \quad \text{et} \quad \beta = z_1 + j^2 z_2 + j z_3,$$

les quantités déduites de α et β par permutation des z_i sont les $\omega\alpha$ et les $\omega\beta$ pour ω racine cubique de 1.⁹ Il s'ensuit que les seules quantités déduites de α^3 par permutation des x_i sont α^3 et β^3 . Calculons alors $\alpha^3\beta^3$ et $\alpha^3 + \beta^3$:

$$\begin{aligned} \alpha\beta &= z_1^2 + z_2^2 + z_3^2 - (z_1 z_2 + z_2 z_3 + z_3 z_1) = (z_1 + z_2 + z_3)^2 - 3(z_1 z_2 + z_2 z_3 + z_3 z_1), \\ \text{soit} \quad \alpha\beta &= -3p, \quad \text{puis} \quad \alpha^3\beta^3 = -27p^3. \end{aligned}$$

Par ailleurs

$$\begin{aligned} \alpha^3 + \beta^3 &= (\alpha + \beta)^3 - 3\alpha\beta(\alpha + \beta) = (2z_1 - z_2 - z_3)^3 + 9p(2z_1 - z_2 - z_3) \\ &= (3z_1)^3 + 27pz_1 = 27(z_1^3 + pz_1) = -27q. \end{aligned}$$

Ainsi, α^3 et β^3 sont racines du trinôme du second degré $X^2 + 27qX - 27p^3$. On peut donc calculer α et β par extraction de racines cubiques, puis déterminer les z_i à partir de α et β , en utilisant la « troisième relation » $z_1 + z_2 + z_3 = 0$.

L'idée essentielle que Lagrange tire de ces calculs est la suivante : *c'est parce que les seules quantités déduites de α^3 par permutation des x_i sont α^3 et β^3 que α^3 et β^3 sont racines d'une équation de degré 2 à coefficients dans \mathbb{K} .* Revenant à l'équation générale de degré n , Lagrange démontre une forme générale de ce principe : *si une expression polynomiale en les x_i prend m valeurs lorsque l'on permute les x_i , elle vérifie une équation de degré m sur le corps de base.*¹⁰ En **4.2**, nous démontrerons cet énoncé et expliquerons comment Lagrange l'applique à la résolution des équations de degré 4.

Lagrange montre que les méthodes utilisées pour les équations de degré 3 et 4 ne s'étendent pas aux degrés supérieurs, ce qui le conduit à douter de la résolubilité par radicaux des équations de degré 5. Ruffini publie, vers 1800, une première preuve, réputée incomplète, de l'impossibilité de la résolution par radicaux de l'équation générale de degré 5, basée sur une étude du groupe \mathcal{S}_5 . En 1824, Abel donne la première démonstration considérée comme probante de l'impossibilité. Ces travaux utilisent de manière cruciale l'action du groupe des permutations sur les racines.

Gauss et l'équation cyclotomique

Dans les *Disquisitiones Arithmeticae*, publiées en 1801, Gauss examine le problème de la construction des polygones réguliers à la règle et au compas ». La construction du pentagone régulier était connue des Grecs (exercice 1, **1.1**). La question est en fait algébrique : comme nous le verrons dans la section **5** du chapitre **2**, il s'agit de savoir si on peut « calculer » les racines de l'unité par opérations de corps et extractions de racines carrées. Le problème revient donc à l'étude algébrique d'une équation particulière, l'équation cyclotomique $x^n - 1 = 0$, dont Gauss donne une

9. Le choix des racines cubiques de 1 pour les coefficients est crucial ; c'est, à proportionnalité près, le seul qui entraîne que α^3 ne prend que deux valeurs par permutation des x_i .

10. A priori $m \leq n!$. Si $m < n$, on obtient une équation auxiliaire, vérifiée par p , de degré $< n$.

analyse profonde. Son résultat le plus spectaculaire est la construction à la règle et au compas du polygone régulier à 17 côtés, liée à l'assez stupéfiante formule :

$$\cos\left(\frac{2\pi}{17}\right) = \frac{1}{16} \left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}} \right).^{11}$$

En fait, $\cos\left(\frac{2\pi}{17}\right)$ est racine d'une équation de degré 8 à coefficients dans \mathbb{Q} dont la résolution se ramène à celle de trois équations de degré 2. Gauss montre plus généralement que, si $p \in \mathcal{P}$ s'écrit $2^m + 1, m \in \mathbb{N}^*$, on peut calculer $\cos\left(\frac{2\pi}{p}\right)$ en résolvant m équations de degré 2 « emboîtées ».

Exercice 12. ③ Déterminer $P \in \mathbb{Z}[X]$ unitaire de degré 8 annihilant $2 \cos\left(\frac{2\pi}{17}\right)$.

On doit à Gauss une autre contribution fondamentale à la théorie des équations. Dès 1629, Girard tient pour vrai que le corps \mathbb{C} est algébriquement clos. C'est Gauss qui donne la première preuve complète de ce résultat, maintenant nommé théorème de d'Alembert-Gauss. Nous en proposerons plusieurs démonstrations dans la section 5.

Lagrange et Gauss font progresser de manière décisive deux versants de la théorie des équations algébriques. Galois saura unifier ces deux contributions.

1.3 Galois et la transformation de l'algèbre

Galois

Galois s'inscrit dans la double filiation de Lagrange et de Gauss.¹² Son travail le plus connu est le *Mémoire sur les conditions de résolubilité des équations par radicaux*, déposé à l'Académie en janvier 1831. Il y caractérise les équations résolubles par radicaux.¹³ Son idée maîtresse est d'associer à une équation à coefficients dans un corps \mathbb{K} un groupe, appelé *groupe de Galois de l'équation*, qui reflète les *symétries algébriques de l'équation vis à vis de \mathbb{K}* . Ce groupe dépend du corps de base. La façon dont il varie lorsque l'on change \mathbb{K} (a priori uniquement assujéti à contenir les coefficients de l'équation) est le thème fondamental de la théorie.

Qu'entend-on par symétries algébriques? Soit $P \in \mathbb{K}[X]$ de degré n , admettant n racines distinctes x_1, \dots, x_n dans un surcorps adéquat de \mathbb{K} . Les x_i vérifient des identités polynomiales à coefficients dans \mathbb{K} , dont les formules de Viète sont les exemples les plus immédiats. Pour certains polynômes, il existe d'autres identités de cette forme. Ainsi, si P est de degré 4 et « bicarré », c'est-à-dire de la forme $X^4 + aX^2 + b$, l'opposé d'une racine est également une racine : les racines se regroupent donc en deux paires $\{x, -x\}$. Autrement dit, on a deux relations

$$x_1 + x_2 = 0 \quad x_3 + x_4 = 0.$$

Le groupe de Galois de P est le sous-groupe du groupe des permutations de $\{x_1, \dots, x_n\}$ qui préservent les relations algébriques à coefficients dans \mathbb{K} entre les x_i ; c'est donc un groupe fini dont l'ordre divise $n!$. Plus nombreuses sont ces relations, plus le groupe est petit, plus l'équation peut être considérée comme « simple ». Si les x_i sont dans \mathbb{K} , l'équation est « résolue vis-à-vis de

11. Noter l'apparition de $\sqrt{17}$, à relier à celle de $\sqrt{5}$ pour le pentagone. Explication en 4.3.

12. Même si, curieusement, il cite Gauss mais pas Lagrange.

13. Abel avait lui aussi entrepris de comprendre les équations résolubles par radicaux et mis en évidence les « équations abéliennes », i.e. à groupe de Galois commutatif.

\mathbb{K} » et le groupe est trivial. À l’opposé, si toutes les relations algébriques à coefficients dans \mathbb{K} entre les x_i proviennent des relations de Viète, toute permutation des x_i appartient au groupe : tel est le cas pour l’« équation générale ». Autre exemple : le groupe du polynôme bicarré $X^4 + aX^2 + b$ est toujours de cardinal au plus 8, strictement inférieur à $4! = 24$.

Le point-clé est que la résolubilité par radicaux d’une équation se traduit en termes de groupe de Galois. De même pour la résolubilité par racines carrées, ce qui permet de retrouver les résultats de Gauss. Ces traductions reposent sur un résultat profond, la *correspondance de Galois*. Implicite chez Galois, cette correspondance est en fait le résultat central de la théorie des équations. La caractérisation des équations résolubles par radicaux n’en est qu’une application.

La théorie de Galois de Galois à Artin

Le travail de Galois marque une rupture décisive. Simultanément, Galois :

- résout le problème central de la théorie des équations ;
- inscrit la question de la résolubilité par radicaux dans le cadre plus vaste d’une « classification des irrationnelles » fondée sur la notion de groupe ;
- crée un nouveau champ d’études, la théorie des groupes.

Le travail de Galois assimilé, l’intérêt des algébristes se tourne vers des objets et problèmes plus « structurels ». ¹⁴ Indiquons trois directions, ayant chacune conduit à des reformulations d’une partie du travail de Galois, ainsi qu’à des résultats importants hors théorie des équations.

- Le premier véritable continuateur de Galois est Jordan, qui précise et approfondit les notions relatives aux groupes. Son *Traité des Substitutions et des équations algébriques*, paru en 1870, qui se présente comme un « commentaire des idées de Galois », contient une foule de résultats concernant les groupes de permutations et ce que nous appelons maintenant les « groupes classiques » sur les corps \mathbb{F}_p , et stimule fortement l’étude des groupes et des matrices. Jordan rattache ses résultats aux équations, mais la théorie des groupes commence ici à s’autonomiser.

- À la fin du dix-neuvième siècle, Dedekind développe l’étude arithmétique des corps de nombres. Il donne, dans ce cadre, une présentation novatrice de la théorie de Galois, publiée dans le onzième supplément aux *Vorlesungen über Zahlentheorie* de Dirichlet (1894). Les extensions, les morphismes et la correspondance y prennent le pas sur les équations.

- En 1910, Steinitz rédige une grande synthèse sur la théorie des corps, d’esprit axiomatique. Il met notamment en évidence les notions de sous-corps premier, de caractéristique, d’algébricité et de transcendance, de séparabilité.

Un peu avant 1930, Emmy Noether étend l’exposé de la théorie de Galois donné par Dedekind au cadre axiomatique fixé par Steinitz. Van der Waerden publie en 1930 un des livres d’algèbre les plus influents de l’histoire ¹⁵ ; l’exposé de la théorie de Galois y suit celui de Noether. En 1945, Emil Artin donne à ces idées une forme radicale : les arguments utilisant le théorème des fonctions symétriques et celui de l’élément primitif disparaissent complètement.

Le groupe de Galois et la correspondance de Galois seront introduits dans le chapitre 4 de ce cours. L’application aux équations sera traitée dans le chapitre 5.

14. Ce mouvement est lent. Ainsi, Jordan a d’abord en vue l’application des méthode de la théorie des groupes de permutations aux équations. L’article de 1872 dans lequel Sylow établit les théorèmes qui portent son nom a pour titre *Théorème sur les groupes de substitutions*. Le *Lehrbuch der Algebra* de Weber, un des traités d’algèbre majeurs de la fin du dix-neuvième siècle, reste centré sur les équations algébriques. Tel est encore le cas des ouvrages « pré-Van der Waerden » des années 1920 (Dickson, Hasse ...).

15. *Moderne Algebra*, ayant connu sept éditions, la dernière (et première en anglais) en 1970.

2 Polynômes à coefficients dans un corps

Une équation algébrique n'est qu'une équation polynomiale. La notion de polynômes s'avère plus maniable que celle d'équation. Cette section a pour but de rappeler l'arithmétique des anneaux $\mathbb{K}[X]$ et de donner une certaine familiarité avec la notion de polynôme irréductible, centrale en théorie de Galois. On suit l'usage actuel :

- les anneaux sont unitaires ;
- on appelle corps tout anneau commutatif dans lequel tout élément non nul est inversible.

Le lecteur connaît les corps \mathbb{Q} , \mathbb{R} , \mathbb{C} , les corps de fractions rationnelles $\mathbb{K}(X)$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier. Nous en rencontrerons beaucoup d'autres. Si \mathbb{L} est un corps et \mathbb{K} un sous-corps de \mathbb{L} , on dit que \mathbb{L} est un *surcorps* de \mathbb{K} .

Les corps donnent un bon cadre pour l'étude des équations algébriques. En effet, si l'anneau commutatif \mathbb{A} n'est pas intègre et si a et b sont deux éléments non nuls de \mathbb{A} de produit 0, le polynôme $(X - a)(X - b)$ s'annule en a , b et 0 : un polynôme peut donc avoir plus de racines que son degré. C'est également le cas si \mathbb{A} est un anneau à division non commutatif. L'exemple le plus simple d'anneau à division est donné par l'*anneau des quaternions réels*, noté \mathbb{H} que l'on peut définir comme l'ensemble des matrices de $\mathcal{M}_2(\mathbb{C})$ de la forme

$$\begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}$$

avec $(a, b) \in \mathbb{C}^2$. Des calculs simples montrent que \mathbb{H} est une sous-algèbre à division de dimension 4 de la \mathbb{R} -algèbre $\mathcal{M}_2(\mathbb{C})$, dont le centre est $\mathbb{R}I_2$. On vérifie aussitôt que l'équation $X^2 = -1$ a une infinité de solutions dans \mathbb{H} .¹⁶

Exercice 13. ② Vérifier les propriétés ci-dessus de l'algèbre des quaternions.

Exercice 14. ② Soit \mathbb{A} un anneau commutatif non intègre. Construire un polynôme de degré 1 de $\mathbb{A}[X]$ n'ayant de racine dans aucun anneau dont \mathbb{A} soit sous-anneau.

Cette section est centrée sur la notion de polynôme irréductible. Les paragraphes **2.1** à **2.4** sont essentiels pour la suite, **2.5** est un divertissement.

2.1 L'arithmétique de $\mathbb{K}[X]$: rappel

Si \mathbb{K} est un corps, l'étude de l'arithmétique de $\mathbb{K}[X]$ s'effectue selon le plan suivant.

- On vérifie que les inversibles de $\mathbb{K}[X]$ sont les constantes non nulles. Conformément la terminologie générale en algèbre commutative, on dit que deux éléments P et Q de $\mathbb{K}[X]$ sont *associés* s'il existe c dans \mathbb{K}^* tel que $Q = cP$.

- On établit l'existence et l'unicité de la division euclidienne dans $\mathbb{K}[X]$. Rappelons incidemment que l'algorithme de la division euclidienne vaut dans un anneau commutatif, à condition de diviser par un polynôme unitaire.

- On montre, à l'aide de la division euclidienne, que tout idéal non nul de $\mathbb{K}[X]$ admet un unique générateur unitaire. Deux polynômes P et Q engendrent le même idéal de $\mathbb{K}[X]$ si et seulement s'ils sont associés.

- La suite de l'étude suit le plan général de l'arithmétique dans un anneau principal. Le caractère principal des idéaux de $\mathbb{K}[X]$ permet de définir le pgcd de deux éléments de $\mathbb{K}[X]$ (voire d'une famille

16. Les matrices de la forme $\begin{pmatrix} ix & -\bar{b} \\ b & -ix \end{pmatrix}$ avec $x \in \mathbb{R}$ et $b \in \mathbb{C}$ (Cayley-Hamilton).

quelconque d'éléments de $\mathbb{K}[X]$) et d'obtenir la relation de Bézout. On définit alors les polynômes premiers entre eux et on déduit le lemme de Gauss de la relation de Bézout.

- Après avoir défini la notion de polynôme irréductible, on déduit du lemme de Gauss celui d'Euclide : si P est un irréductible de $\mathbb{K}[X]$, A et B deux éléments de $\mathbb{K}[X]$, si P divise AB , alors P divise A ou B .

- En raisonnant par récurrence sur le degré, on montre que tout polynôme non constant de $\mathbb{K}[X]$ est produit d'irréductibles de $\mathbb{K}[X]$. Le lemme d'Euclide entraîne d'autre part que cette décomposition est « unique à l'ordre près ».

Exercice 15. ② Soient \mathbb{A} un anneau commutatif intègre qui n'est pas un corps, a un élément non nul et non inversible de \mathbb{A} . Montrer que l'idéal de $\mathbb{A}[X]$ engendré par X et a n'est pas principal.

2.2 Irréductibles de $\mathbb{K}[X]$

Fixons deux points de terminologie :

- on dit indifféremment « P est un irréductible de $\mathbb{K}[X]$ » ou « P est irréductible sur \mathbb{K} » ;
- si \mathbb{K} un sous-corps du corps \mathbb{L} , on dit que \mathbb{L} est un surcorps de \mathbb{K} .

La discussion de 2.1 ramène l'arithmétique de $\mathbb{K}[X]$ à la détermination des irréductibles. Cette détermination dépend du corps \mathbb{K} . Les polynômes de degré 1 sont toujours irréductibles.

Corps algébriquement clos

Le corps \mathbb{K} est dit *algébriquement clos* si les seuls irréductibles de $\mathbb{K}[X]$ sont les polynômes de degré 1. En utilisant la décomposition en produit d'irréductibles, on voit que tel est le cas si et seulement si tout polynôme non constant de $\mathbb{K}[X]$ a une racine dans \mathbb{K} .

Le corps \mathbb{C} des nombres complexes est algébriquement clos (*théorème de d'Alembert-Gauss*, section 5). On établit également les résultats suivants, dont on trouvera une démonstration dans la section 3 du chapitre 2, mais que nous utiliserons librement dès maintenant.

Théorème 1. Soit $P \in \mathbb{K}[X]$ non constant. Il existe un surcorps de \mathbb{K} sur lequel P est scindé.

Théorème 2. Tout corps admet un surcorps algébriquement clos.

Le théorème 2 est évidemment beaucoup plus fort que le théorème 1. Sa démonstration en toute généralité nécessite l'axiome du choix. Le théorème 1 suffit pour bien des applications.

Exercice 16. ② Montrer que le corps \mathbb{K} est algébriquement clos si et seulement si tout élément non constant de $\mathbb{K}[X]$ induit une surjection de \mathbb{K} sur \mathbb{K} .

Exercice 17. ③ Montrer qu'un corps fini ne peut être algébriquement clos.

Le corps des nombres réels

Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle. Ce résultat se démontre en combinant au théorème de d'Alembert l'observation suivante : si l'élément λ de $\mathbb{C} \setminus \mathbb{R}$ est racine du polynôme P de $\mathbb{R}[X]$, il en est de même de $\bar{\lambda}$. Or,

$$(X - \lambda)(X - \bar{\lambda}) = X^2 - 2\operatorname{Re}(\lambda)X + |\lambda|^2 \in \mathbb{R}[X].$$

Exercice 18. ③ Soit $P \in \mathbb{R}[X]$. Montrer qu'il existe A et B dans $\mathbb{R}[X]$ tels que $P = A^2 + B^2$ si et seulement si

$$\forall x \in \mathbb{R}, \quad P(x) \geq 0.$$

Exercice 19. ⑤ On note \mathcal{P} l'ensemble des polynômes non nuls à coefficients dans \mathbb{R}^+ . Soit P dans $\mathbb{R}[X]$. Démontrer qu'il existe A et B dans \mathcal{P} tels que $P = \frac{A}{B}$ si et seulement si

$$\forall x \in \mathbb{R}^{+*}, \quad P(x) > 0.$$

Irréductibilité sur \mathbb{K} et racines dans \mathbb{K}

Si $P \in \mathbb{K}[X]$ est de degré 2 ou 3, P est irréductible dans \mathbb{K} si et seulement s'il n'a pas de racine dans \mathbb{K} . C'est faux si le degré de P dépasse 4. Exemples : $\mathbb{K} = \mathbb{R}$ et $P = X^4 + 1$, ou $P = (X^2 + 1)^2$.

Le lemme ci-dessous propose un test simple pour détecter les éventuelles racines rationnelles d'un polynôme de $\mathbb{Q}[X]$.

Lemme 1. Soit $P = a_n X^n + \dots + a_0$ un polynôme de $\mathbb{Z}[X]$ de degré $n \geq 1$. Soient p dans \mathbb{Z} et q dans \mathbb{N}^* deux entiers premiers entre eux tels que $\frac{p}{q}$ soit racine de P . Alors $q|a_n$ et $p|a_0$.

En particulier, si P est unitaire, toute racine rationnelle de P est entière.

Preuve. Démontrons le premier point, l'autre se traitant de même. Le second membre de l'égalité

$$a_n p^n = - \sum_{i=0}^{n-1} a_i p^i q^{n-i}$$

est divisible par q , d'où, grâce au lemme de Gauss, $q|a_n$.

Application Racine m -ième d'un entier naturel

Soient $n \geq 2$ et $m \geq 2$ deux entiers Alors $\sqrt[m]{n}$ annule le polynôme $X^m - n$. Il s'ensuit que

$$\sqrt[m]{n} \in \mathbb{Q} \iff \exists \ell \in \mathbb{N}^*, n = \ell^m.$$

Ce résultat peut être démontré de manière un peu différente : si $\sqrt[m]{n} = \frac{u}{v}$ avec u et v dans \mathbb{N}^* , alors $u^m = n v^m$. Par conséquent, pour tout nombre premier p , $v_p(n)$ est divisible par m et n est puissance m -ième d'un entier.

Exercice 20. ② Montrer que $X^3 - X - 1$ est irréductible sur \mathbb{Q} .

Exercice 21. ② Décomposer $X^4 + 2X^2 + 9$ en produit d'irréductibles sur \mathbb{Q} .

Binômes de degré premier

Le résultat suivant donne une condition nécessaire et suffisante d'irréductibilité pour un binôme de degré premier. Il a été établi par Abel dans le cas où le corps de base contient les racines p -ièmes de 1 afin de compléter la preuve de Ruffini relative à la non résolubilité de l'équation de degré 5.

Proposition 1. Soient \mathbb{K} un corps, $p \in \mathcal{P}$, $a \in \mathbb{K}$. S'équivalent :

- i) le polynôme $X^p - a$ est irréductible sur \mathbb{K} ,
- ii) le polynôme $X^p - a$ n'a pas de racine dans \mathbb{K} .

Preuve. Seule l'implication $ii) \Rightarrow i)$ est à prouver. Supposons le polynôme $X^p - a$ réductible sur \mathbb{K} . Soient P un diviseur irréductible unitaire de $X^p - a$ dans $\mathbb{K}[X]$, d le degré de P : $d \in \{1, \dots, p-1\}$. Soient \mathbb{L} un surcorps de \mathbb{K} sur lequel P est scindé, u une racine de $X^p - a$ dans \mathbb{L} , c'est-à-dire une racine p -ième de a . Les racines de P dans \mathbb{L} sont de la forme εu où ε est une racine p -ième de 1. La factorisation de P en produit d'irréductibles de $\mathbb{L}[X]$ est de la forme

$$\prod_{j=1}^d (X - \varepsilon_j u)$$

où les ε_j sont tous racines p -ièmes de 1. Le terme constant de P est donc de la forme $\pm \varepsilon u^d$ où ε est une racine p -ième de 1 dans \mathbb{L} . Ainsi, $\varepsilon u^d \in \mathbb{K}$. La relation de Bézout fournit d'autre part $(\alpha, \beta) \in \mathbb{Z}^2$ tel que $\alpha d + \beta p = 1$. Mais alors, $(\varepsilon u^d)^\alpha a^\beta = \varepsilon^\alpha u \in \mathbb{K}$ est racine de $X^p - a$.

Le corps des nombres rationnels

La détermination des irréductibles de $\mathbb{Q}[X]$ est délicate. Montrons d'abord que, pour $n \in \mathbb{N}^*$, $X^n - 2$ est irréductible sur \mathbb{Q} , ce qui établit l'existence d'irréductibles de tout degré.

Soit, par l'absurde, P un diviseur unitaire de $X^n - 2$ dans $\mathbb{Q}[X]$ de degré $d \in \{1, \dots, n-1\}$. La factorisation complexe de $X^n - 2$ montre que le terme constant de P est de la forme $\pm \varepsilon 2^{d/n}$ où ε est une racine n -ième de 1 dans \mathbb{C} . Si $P \in \mathbb{Q}[X]$, alors $\pm \varepsilon 2^{d/n}$ est dans \mathbb{Q} , donc dans \mathbb{R} , $\varepsilon \in \{\pm 1\}$, et $2^{d/n} \in \mathbb{Q}$. Or, ceci est impossible (application suivant le lemme 1).

Exercice 22. ② À quels binômes $X^n - m$ de $\mathbb{Z}[X]$ peut-on généraliser la démonstration ci-dessus ?

Le corps \mathbb{F}_p

On montre que, si $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$, il existe un polynôme de degré n de $\mathbb{F}_p[X]$ irréductible sur \mathbb{F}_p . Mieux, Gauss a dénombré les polynômes vérifiant ces conditions et établi que, si p^n est « grand », parmi les p^n polynômes unitaires de degré n de $\mathbb{F}_p[X]$, il y en a à peu près $\frac{p^n}{n}$ d'irréductibles.¹⁷ Contentons nous du cas $n = 2$. Ceux qui sont réductibles sont les $(X - x)^2$ avec $x \in \mathbb{F}_p$ et les $(X - x)(X - y)$ avec $(x, y) \in \mathbb{F}_p^2$, $x \neq y$. Soit au total, si $p \geq 3$, $p + \frac{p(p-1)}{2} = \frac{p(p+1)}{2}$ polynômes réductibles, donc $\frac{p(p-1)}{2}$ polynômes de degré 2 unitaires irréductibles.

Exercice 23. ③ Dénombrer les polynômes irréductibles unitaires de degré 3 de $\mathbb{F}_p[X]$.

L'exercice suivant introduit les *polynômes d'Artin-Schreier*, qui jouent un rôle important dans l'étude des corps de caractéristique p .

Exercice 24. ④ Soient $p \in \mathcal{P}$, \mathbb{K} un corps de caractéristique p , $a \in \mathbb{K}$ et $P = X^p - X - a$. Montrer que, si x est une racine de P dans un surcorps de \mathbb{K} , il en est de même de $x + \lambda$ pour tout λ de \mathbb{F}_p . En déduire l'équivalence des deux assertions suivantes :

- i) P est scindé sur \mathbb{K} ,
- ii) P est réductible sur \mathbb{K} .

17. Voici le résultat de Gauss. Soit μ la fonction de Moebius. Pour tout n dans \mathbb{N}^* , le nombre de polynômes unitaires de degré n de $\mathbb{F}_p[X]$ est $\frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$.

2.3 Séparabilité (I)

Le résultat ci-après est simple, mais fondamental. Cependant, le lecteur qui souhaite se borner à la théorie de Galois en caractéristique 0 peut laisser de côté la suite de ce paragraphe.

Proposition 2. *Supposons \mathbb{K} de caractéristique 0. Si P est un irréductible de $\mathbb{K}[X]$, les racines de P dans un surcorps de \mathbb{K} sont simples.*

Preuve. Le polynôme P' est non nul, de degré strictement plus petit que celui de P . Le polynôme P' est donc premier à P dans $\mathbb{K}[X]$. Grâce à l'inertie du pgcd (remarque 1 ci-après), P et P' sont aussi premiers entre eux dans $\mathbb{L}[X]$ pour tout surcorps \mathbb{L} de \mathbb{K} .

Remarques

1. Inertie du pgcd

Si A et B sont dans $\mathbb{K}[X]$ et si \mathbb{L} est un surcorps de \mathbb{K} , l'algorithme d'Euclide montre que le pgcd de A et B est le même vu dans $\mathbb{K}[X]$ ou $\mathbb{L}[X]$.

2. Dérivation et racines simples

Si \mathbb{K} est un corps de caractéristique nulle, $P \in \mathbb{K}[X] \setminus \{0\}$, $x \in \mathbb{K}$, la formule de Taylor permet de calculer la multiplicité de x comme racine de P . Ce lien tombe en défaut en caractéristique p , la raison étant que certains polynômes non constants ont une dérivée nulle. Précisément, si \mathbb{K} est de caractéristique p ,

$$\forall P \in \mathbb{K}[X], \quad P' = 0 \iff P \in \mathbb{K}[X^p].$$

On conserve cependant l'équivalence entre « x est racine de P de multiplicité au moins 2 » et $P(x) = P'(x) = 0$. La vérification est élémentaire : si x est racine de P , P s'écrit $(X - x)Q$ avec Q dans $\mathbb{K}[X]$. La relation

$$P' = (X - x)Q' + Q$$

montre que $Q(x) = 0$ si et seulement si $P'(x) = 0$.

3. Un contre-exemple

Si \mathbb{K} est de caractéristique $p \in \mathcal{P}$, T une indéterminée, t une racine de $X^p - T$ dans un surcorps de $\mathbb{K}(T)$, on a : $X^p - T = (X - t)^p$. Pourtant, $X^p - T$ est irréductible sur $\mathbb{K}[T]$ (proposition 1).

L'exemple 3 montre que la proposition 2 est fautive en caractéristique p . Nous allons introduire un peu de vocabulaire afin de préciser ce point. Disons qu'un polynôme P de $\mathbb{K}[X]$ est *séparable* s'il est premier à sa dérivée ou, de manière équivalente, si les racines de P dans un surcorps de \mathbb{K} scindant P sont simples. La proposition 2 dit que, si \mathbb{K} est de caractéristique zéro, tout irréductible de $\mathbb{K}[X]$ est séparable. En caractéristique p , on a le résultat suivant.

Proposition 3. *Soient $p \in \mathcal{P}$, \mathbb{K} un corps de caractéristique p , P un irréductible de $\mathbb{K}[X]$. Alors P est séparable si et seulement si P n'appartient pas à $\mathbb{K}[X^p]$.*

Preuve. L'argument de la proposition 2 montre que P est séparable si et seulement si P' n'est pas nul, d'où le résultat.

Corps parfaits

Le corps \mathbb{K} est dit *parfait* si tout irréductible de $\mathbb{K}[X]$ est séparable. Les corps de caractéristique nulle sont parfaits. Si \mathbb{K} est de caractéristique $p > 0$, soit $\text{Frob}_{\mathbb{K}}$ l'endomorphisme de Frobenius de \mathbb{K} , défini par

$$\forall x \in \mathbb{K}, \quad \text{Frob}_{\mathbb{K}}(x) = x^p.$$

Théorème 3. Soient $p \in \mathcal{P}$, \mathbb{K} un corps de caractéristique p . Alors \mathbb{K} est parfait si et seulement si $\text{Frob}_{\mathbb{K}}$ est surjectif.

Preuve. Soient a_0, \dots, a_n des éléments de \mathbb{K} . Alors

$$\left(\sum_{i=0}^n a_i X^i \right)^p = \sum_{i=0}^n a_i^p X^{ip}.$$

Il s'ensuit que, si $\text{Frob}_{\mathbb{K}}$ est surjectif, les éléments de $\mathbb{K}[X^p]$ sont des puissances p -ièmes d'éléments de $\mathbb{K}[X]$, donc non irréductibles. Par suite, les irréductibles de $\mathbb{K}[X]$ n'appartiennent pas à $\mathbb{K}[X^p]$ et sont donc séparables grâce à la proposition 3 : le corps \mathbb{K} est parfait.

Supposons maintenant que $\text{Frob}_{\mathbb{K}}$ n'est pas surjectif, soit a un élément de \mathbb{K} qui n'est pas puissance p -ième d'un élément de \mathbb{K} . Alors $X^p - a$ est irréductible sur \mathbb{K} (proposition 1) et appartient à $\mathbb{K}[X^p]$: \mathbb{K} n'est pas parfait.

Exercice 25. ③ Soient \mathbb{K} un corps de caractéristique p , $a \in \mathbb{K}$ qui n'est pas puissance p -ième d'un élément de \mathbb{K} , α une racine de $X^p - a$ dans un surcorps de \mathbb{K} . Utiliser la relation $X^p - a = (X - \alpha)^p$ pour retrouver dans ce cas l'irréductibilité de $X^p - a$ dans $\mathbb{K}[X]$.

Les corps de caractéristique nulle sont parfaits. L'énoncé ci-après montre qu'il en est de même des corps finis. L'exemple de $X^p - T$ sur $\mathbb{F}_p(T)$ est donc aussi simple que possible.

Corollaire 1. *Tout corps fini est parfait.*

Preuve. Le résultat est une conséquence immédiate du lemme suivant, que nous utiliserons fréquemment par la suite.

Lemme 2. Soient \mathbb{K} un corps, φ un morphisme d'anneaux de \mathbb{K} dans un anneau \mathbb{A} . Alors φ est injectif.

Preuve. Pour $x \in \mathbb{K}^*$, $x \times \frac{1}{x} = 1$, donc $\varphi(x) \times \varphi\left(\frac{1}{x}\right) = 1$, donc $\varphi(x) \neq 0$.

2.4 Irréductibilité dans $\mathbb{Q}[X]$

Comment se ramener de \mathbb{Q} à \mathbb{Z}

Un polynôme de $\mathbb{Q}[X]$ a des associés dans $\mathbb{Z}[X]$. On peut donc se borner à étudier l'irréductibilité sur \mathbb{Q} des éléments de $\mathbb{Z}[X]$. En suivant Gauss, nous allons montrer que l'on peut en fait se ramener à étudier l'irréductibilité dans $\mathbb{Z}[X]$ des éléments de $\mathbb{Z}[X]$. Les arguments sont en fait plus généraux : on peut, sans changement, remplacer \mathbb{Z} par un anneau factoriel \mathbb{A} , \mathbb{Q} par le corps des fractions \mathbb{K} de \mathbb{A} .

Soit $P \in \mathbb{Z}[X] \setminus \{0\}$. On appelle *contenu de P* et on note $C(P)$ le pgcd des coefficients de P . Un polynôme de contenu égal à 1 est dit *primitif*. Le résultat fondamental est le lemme suivant.

Lemme 3. *Le produit de deux polynômes primitifs est primitif.*

Preuve. Soient P_1 et P_2 dans $\mathbb{Z}[X]$, $P = P_1 P_2$. Supposons P non primitif. Il existe alors un nombre premier p divisant $C(P)$. En notant \bar{U} la réduction modulo p de l'élément U de $\mathbb{Z}[X]$, on a

$$0_{\mathbb{F}_p[X]} = \bar{P} = \bar{P}_1 \bar{P}_2.$$

Comme $\mathbb{F}_p[X]$ est intègre, l'un des deux polynômes $\overline{P_1}, \overline{P_2}$ est nul. Or, si $\overline{P_i}$ est nul, p divise $C(P_i)$, ce qui contredit le caractère primitif de P_i .

Remarque *Sans la réduction modulo p*

On peut démontrer le lemme 3 de la manière suivante. Posons

$$P_1 = \sum_{i=0}^m a_i X^i ; \quad P_2 = \sum_{j=0}^n b_j X^j .$$

Soit p un nombre premier. Montrons que p ne divise pas $C(P_1 P_2)$. Puisque P_1 et P_2 sont primitifs, on dispose des entiers

$$k = \min\{i \in \{0, \dots, m\} ; a_i \notin p\mathbb{Z}\} ; \quad \ell = \min\{j \in \{0, \dots, n\} ; b_j \notin p\mathbb{Z}\} .$$

Le coefficient de $X^{k+\ell}$ dans la décomposition canonique de $P_1 P_2$ est congru à $a_k b_\ell$ modulo p , donc n'est pas divisible par p .

Si $P \in \mathbb{Z}[X]$, P s'écrit $C(P)\tilde{P}$ où \tilde{P} est un élément primitif de $\mathbb{Z}[X]$. On généralise donc le lemme 3 en l'énoncé suivant, nommé - comme plusieurs autres- *lemme de Gauss*.

Proposition 4. *Si P et Q sont dans $\mathbb{Z}[X] \setminus \{0\}$, $C(PQ) = C(P) C(Q)$.*

Le lemme de Gauss permet de réaliser le programme annoncé au début de ce paragraphe : si $P \in \mathbb{Z}[X] \setminus \{0\}$, une factorisation de P dans $\mathbb{Q}[X]$ se relève en une factorisation de P dans $\mathbb{Z}[X]$.

Théorème 4. *Soit P dans $\mathbb{Z}[X] \setminus \{0\}$. Si P s'écrit $P_1 P_2$ avec P_1, P_2 dans $\mathbb{Q}[X]$, il existe Q_1 et Q_2 dans $\mathbb{Z}[X]$ primitifs, associés respectivement à P_1 et P_2 dans $\mathbb{Q}[X]$, tels que $P = C(P) Q_1 Q_2$.*

Preuve. Si $i \in \{1, 2\}$, on écrit $P_i = \frac{u_i}{v_i} Q_i$ où u_i, v_i sont des éléments non nuls de \mathbb{Z} et Q_i un polynôme primitif de $\mathbb{Z}[X]$. Alors, $u_1 u_2 Q_1 Q_2 = v_1 v_2 P$ et, grâce au lemme de Gauss, $u_1 u_2 = \pm C(P) v_1 v_2$.

Corollaire 2. *Soient P_1 et P_2 deux polynômes unitaires de $\mathbb{Q}[X]$ tels que $P_1 P_2$ appartienne à $\mathbb{Z}[X]$. Alors P_1 et P_2 appartiennent à $\mathbb{Z}[X]$.*

Remarques

1. Point de vue algorithmique

Le théorème 4 entraîne l'existence d'un algorithme de factorisation dans $\mathbb{Q}[X]$. Il suffit en effet d'établir que, si $P \in \mathbb{Z}[X]$, on peut expliciter une partie finie de $\mathbb{Z}[X]$ contenant les éventuels diviseurs de P dans $\mathbb{Z}[X]$. On utilise la localisation des racines ci-après.

Lemme 4. *Soient $n \in \mathbb{N}^*$, $P = \sum_{k=0}^n a_k X^k \in \mathbb{C}[X]$ de degré n . Toute racine de P dans \mathbb{C} est de module au plus*

$$M = \max \left\{ 1, \sum_{k=0}^{n-1} \frac{|a_k|}{|a_n|} \right\} .$$

Preuve. Soit z une éventuelle racine de P telle que $|z| > 1$. Alors

$$z^n = - \sum_{k=0}^{n-1} \frac{a_k}{a_n} z^k ,$$

d'où, via l'inégalité triangulaire et puisque $|z| > 1$,

$$|z|^n \leq \sum_{k=0}^{n-1} \frac{|a_k|}{|a_n|} |z|^k \leq M |z|^{n-1}.$$

Adoptons les notations du lemme 4, en supposant $P \in \mathbb{Z}[X]$. Si Q est un diviseur de P dans $\mathbb{Z}[X]$, le coefficient dominant de Q divise a_n . Les formules de Viète bornent par ailleurs les coefficients de Q par des fonctions explicites de M . On en déduit la finitude annoncée.¹⁸

2. Factorialité d'un anneau de polynômes

On déduit facilement du théorème 4 que $\mathbb{Z}[X]$ (qui n'est pas principal, cf exercice 15, **2.1**) est factoriel, ses irréductibles étant les $\pm p$ avec $p \in \mathcal{P}$ et les polynômes de $\mathbb{Z}[X]$ irréductibles sur \mathbb{Q} et de contenu 1. Plus généralement, si l'anneau commutatif intègre \mathbb{A} est factoriel, il en est de même de $\mathbb{A}[X]$. Nous n'utiliserons pas ces résultats.

Exercice 26. ③ *Prouver les résultats de la remarque 2.*

Exercice 27. ③ *Soient $P = \sum_{k=0}^n a_k X^k \in \mathbb{Z}[X]$ de degré n , $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $p \wedge q = 1$.*

a) *Si $\frac{p}{q}$ est racine de P , montrer que $qX - p$ divise P dans $\mathbb{Z}[X]$.*

b) *Si $\frac{p}{q}$ est racine de multiplicité d de P , montrer que q^d divise a_n .*

Exercice 28. ③ *Avec les notations du lemme 4, montrer que les racines de P sont de module au plus $1 + \max \left\{ \frac{|a_i|}{|a_n|} ; i \in \{0, \dots, n-1\} \right\}$.*

Exercice 29. ④ *Les notations sont celles du lemme 4, avec $P \in \mathbb{R}[X]$. On suppose de plus que $a_n \geq 1$, que $a_{n-1} \geq 0$ et que, si $0 \leq k \leq n-2$, $|a_k| \leq C$, où $C \in \mathbb{R}^{+*}$. Montrer que, si $z \in \mathbb{C}$ est racine de P , z est soit de partie réelle négative, soit de module strictement inférieur à $\frac{1}{2} (1 + \sqrt{1 + 4C})$.*

L'exercice ci-après propose une majoration non triviale des coefficients des diviseurs dans $\mathbb{Z}[X]$ d'un élément donné de $\mathbb{Z}[X]$. Cette borne remonte en substance à Landau.

Exercice 30. ⑤ *Soit $P \in \mathbb{C}[X]$ de degré $d \geq 1$. On pose*

$$P = c \prod_{j=1}^d (X - z_j) = \sum_{k=0}^d p_k X^k, \quad m(P) = |c| \prod_{j=1}^d \max(1, |z_j|).$$

18. Cet argument donne des bornes prohibitives. Voici un algorithme légèrement moins naïf, dû à Kronecker. Soit Q un diviseur de P dans $\mathbb{Z}[X]$ de degré majoré par $\frac{n}{2}$. Alors, pour tout a de \mathbb{Z} , $Q(a)$ divise $P(a)$. Par conséquent, il

n'y a qu'un nombre fini de valeurs possibles pour $Q(a)$. Comme Q est déterminé par ses valeurs en $\left\lfloor \frac{n}{2} \right\rfloor + 1$ points, il n'y a qu'un nombre fini de possibilités pour Q .

L'algorithme de Kronecker n'est pas réellement utilisable. Mais il existe d'excellents algorithmes de factorisation dans $\mathbb{Z}[X]$. Ces algorithmes combinent des aspects archimédiens (par exemple, l'utilisation de bornes dans \mathbb{C}) et des aspects p -adiques (dont le plus élémentaire est l'emploi de la réduction modulo un nombre premier p). En 1982, A.Lenstra, H.Lenstra et L.Lovász en 1982 ont découvert l'« algorithme LLL », fondé sur la géométrie des réseaux, qui a sur ses prédécesseurs l'avantage d'être polynomial.

a) Pour $z \in \mathbb{C}$, montrer que $\int_0^1 \ln(|e^{2i\pi t} - z|) dt = \max(0, \ln(|z|))$.

b) En utilisant a), l'inégalité de Jensen et l'égalité $\int_0^1 |P(e^{2i\pi t})|^2 dt = \sum_{k=0}^d |p_k|^2$, établir la majoration

$$m(P) \leq \sqrt{\sum_{k=0}^d |p_k|^2}.$$

c) Montrer que, pour $k \in \{0, \dots, d\}$, $|p_k| \leq \binom{d}{k} m(P)$.

d) On suppose que $P \in \mathbb{Z}[X]$, que Q est un diviseur de P dans $\mathbb{Z}[X]$. On écrit $Q = \sum_{k=0}^e q_k X^k$.

Montrer que

$$\sum_{k=0}^e |q_k| \leq 2^e m(Q) \leq 2^d \sqrt{\sum_{k=0}^d |p_k|^2}.$$

Exemples d'irréductibles de $\mathbb{Q}[X]$ (exercices)

On dispose de très nombreux exemples d'irréductibles de $\mathbb{Q}[X]$. Les démonstrations combinent des éléments d'arithmétique des entiers et des éléments archimédiens (inégalités relatives aux valeurs de polynômes, ou à la localisation des racines). En voici quelques-uns.

Exercice 31. ② a) Soient $P \in \mathbb{Z}[X]$ non constant, $p \in \mathcal{P}$ ne divisant pas le coefficient dominant de P . Montrer que, si la réduction de P dans $\mathbb{F}_p[X]$ est irréductible sur \mathbb{F}_p , alors P est irréductible sur \mathbb{Q} .

b) En déduire, à l'aide de l'exercice 24, que, si $p \in \mathcal{P}$, $X^p - X - 1$ est irréductible sur \mathbb{Q} .

L'exercice ci-après nécessite de connaître un peu de théorie des corps finis.

Exercice 32. ④ Montrer que $P = X^4 + 1$ est irréductible sur \mathbb{Q} , mais que, pour tout nombre premier p , la réduction de P dans $\mathbb{F}_p[X]$ est réductible sur \mathbb{F}_p .

Exercice 33. ③ Soient $n \in \mathbb{N}^*$, a_1, \dots, a_n des entiers relatifs deux à deux distincts. Établir l'irréductibilité sur \mathbb{Q} de $P = \prod_{i=1}^n (X - a_i) - 1$.

Exercice 34. ④ a) Soit $P \in \mathbb{Z}[X]$ prenant quatre fois la valeur 1 sur \mathbb{Z} . Montrer que P ne peut pas prendre la valeur -1 sur \mathbb{Z} .

b) Soit $n \geq 12$ un entier. Montrer que tout $P \in \mathbb{Z}[X]$ de degré n prenant les valeurs ± 1 pour au moins $\left\lfloor \frac{n}{2} \right\rfloor + 1$ entiers est irréductible sur \mathbb{Q} (Dorwart et Ore, 1933).

Exercice 35. ⑤ Soit $n \in \mathbb{N}^*$.

a) Soient $P \in \mathbb{R}[X]$ dont le terme de plus haut degré est cX^n , E une partie de \mathbb{Z} de cardinal $n + 1$. Montrer que

$$\max\{|P(x)|; x \in E\} \geq \frac{|c| n!}{2^n}.$$

b) Soient $P \in \mathbb{Z}[X]$ de degré n , $m = \left\lfloor \frac{n+1}{2} \right\rfloor$. On suppose qu'il existe une partie E de \mathbb{Z} de cardinal m telle que

$$\forall x \in E, \quad 0 < |P(x)| < \frac{m!}{2^m}.$$

Montrer que P est irréductible sur \mathbb{Q} (Polya, 1919).

Exercice 36. ④ a) Soit $P \in \mathbb{Z}[X]$ unitaire, non constant, tel que $|P(0)|$ soit premier et que les racines de P soient de modules strictement supérieurs à 1. Montrer que P est irréductible sur \mathbb{Q} .

b) Soient $n \in \mathbb{N}^*$, $P = \sum_{i=0}^n a_i X^i$ dans $\mathbb{Z}[X]$ de degré n . On suppose que $|a_0| \in \mathcal{P}$ et que $|a_0| > \sum_{i=1}^n |a_i|$. Montrer que P est irréductible sur \mathbb{Q} .

Exercice 37. ④ Si $n \in \mathbb{N}^*$, $p \in \mathcal{P}$, montrer que $P = \sum_{i=1}^n X^i + p$ est irréductible sur \mathbb{Q} .

Exercice 38. ④ Soient $P \in \mathbb{Z}[X]$ unitaire de degré $n \geq 1$, $M \in \mathbb{R}^{+*}$. On suppose que les racines z_1, \dots, z_n de P dans \mathbb{C} sont de modules au plus M et que, s'il existe $k \in \mathbb{Z}$ tel que $|k| > M + 1$ et que $|P(k)|$ soit premier, alors P est irréductible sur \mathbb{Q} (Brillhart, 1980).

Exercice 39. ④ a) Soit $P \in \mathbb{Z}[X]$ unitaire de degré $n \geq 2$ tel que $P(0) \neq 0$ et admettant exactement une racine de module supérieur ou égal à 1. Montrer que P est irréductible sur \mathbb{Q} .

b) Soient a_0, \dots, a_{n-1} des entiers tels que $|a_{n-1}| > |a_n| + \sum_{k=0}^{n-2} |a_k|$. Montrer que $P = \sum_{k=0}^n a_k X^k$ est irréductible sur \mathbb{Q} (Perron, 1907). On pourra, en s'aidant du théorème de Rouché montrer que P vérifie l'hypothèse de la question a).

Exercice 40. ④ Soient $b \geq 3$ un entier, $p \in \mathcal{P}$, que l'on écrit en base b : $p = \sum_{k=0}^{n-1} b_k p^k$ où, pour $0 \leq k \leq n-1$, $0 \leq b_k \leq p-1$ et $b_n \neq 0$. En utilisant l'exercice 29, montrer que $P = \sum_{k=0}^n a_k X^k$ est un irréductible de $\mathbb{Z}[X]$.¹⁹

Exercice 41. ⑤ Notons E l'ensemble des polynômes non constants de $\mathbb{C}[X]$ ne s'annulant pas en 0. Si $P \in E$ de degré n et s'écrit : $P = \sum_{i=0}^n a_i X^i = \prod_{j=1}^n (X - z_j)$, on pose :

$$\lambda(P) = \sum_{j=1}^n \left(z_j - \frac{1}{z_j} \right).$$

a) Calculer $\lambda(P)$ en fonction des a_k . Montrer que, si a_0 et a_n sont dans $\{\pm 1\}$ et P dans $\mathbb{Z}[X]$, alors $\lambda(P)$ est dans \mathbb{Z} .²⁰

b) Soient $n \geq 3$ un entier, $S_n = X^n - X - 1$. Justifier que, pour établir que S_n est irréductible sur \mathbb{Q} , il suffit de démontrer que, pour tout diviseur non constant A de S_n dans $\mathbb{Z}[X]$, $\lambda(A) > 0$.

19. Brillhart, Filaseta, Odlyzko, 1980. La démonstration proposée est due à Murty. Le résultat vaut si $b = 2$, au prix d'une légère complication.

20. L'article original motive l'introduction de la quantité $\lambda(P)$, quelque peu parachutée ici.

c) Soit z une racine de S_n , $z = re^{i\theta}$ avec r dans \mathbb{R}^{+*} et θ dans \mathbb{R} . Vérifier

$$\cos(\theta) = \frac{r^{2n} - r^2 - 1}{2r}, \quad 2 \operatorname{Re} \left(z - \frac{1}{z} \right) > \frac{1}{r^2} - 1.$$

d) En utilisant l'inégalité précédente et l'inégalité arithmético-géométrique, démontrer que S_n est irréductible sur \mathbb{Q} (Selmer, 1956).

Le critère d'Eisenstein

La réduction modulo p , utilisée pour démontrer le lemme 3, est également la clé du critère d'Eisenstein ci-après.

Proposition 5. Soient $p \in \mathcal{P}$, a_0, \dots, a_n des entiers tels que p divise a_0, \dots, a_{n-1} mais pas a_n , et que p^2 ne divise pas a_0 . Alors, le polynôme $P = \sum_{i=0}^n a_i X^i$ est irréductible sur \mathbb{Q} .

Preuve. Dans le cas contraire, P s'écrirait comme produit de deux polynômes P_1 et P_2 non constants de $\mathbb{Z}[X]$. Notant bX^r et cX^s les termes de plus haut degré respectifs de P_1 et P_2 , on voit que p ne divise ni b ni c . En réduisant modulo p , on obtient $\overline{P_1 P_2} = \overline{a_n} X^n$. Ainsi, $\overline{P_1}$ et $\overline{P_2}$ sont des monômes, donc $\overline{P_1} = \overline{b} X^r$ et $\overline{P_2} = \overline{c} X^s$. Comme r et s sont dans \mathbb{N}^* , les termes constants de P_1 et P_2 sont divisibles par p . Leur produit a_0 est donc divisible par p^2 : absurde.

En appliquant le critère avec $p = 2$, on retrouve l'irréductibilité sur \mathbb{Q} de $X^n - 2$. Nous verrons une application plus frappante en **3.2** (théorème 7).

Exercice 42. ④ Démontrer le critère d'Eisenstein sans utiliser la réduction modulo p , par un raisonnement du type de celui utilisé dans la seconde démonstration du lemme 3.

Exercice 43. ④ Soit $P \in \mathbb{Z}[X]$. Montrer que, pour $p \in \mathcal{P}$ assez grand, le polynôme $P + \frac{1}{p}$ est irréductible sur \mathbb{Q} .

Exercice 44. ③ Soient $n \in \mathbb{N}^*$, $p \in \mathcal{P}$, $P = \sum_{k=0}^n a_k X^k \in \mathbb{Z}[X]$, $d \in \{1, \dots, n\}$. On suppose que p divise a_k si $0 \leq k \leq d-1$, que p ne divise pas a_n , que p^2 ne divise pas a_0 . Montrer que l'un au moins des facteurs irréductibles de P est de degré supérieur ou égal à d .

Exercice 45. ④ Soient $n \geq 2$ un entier, $p \in \mathcal{P}$. Montrer que le polynôme $X^n + pX + p^2$ est irréductible sur \mathbb{Q} .

2.5 (*) Un élément de $\mathbb{Z}[X]$ est en général irréductible sur \mathbb{Q}

Si $P = \sum_{k=0}^{+\infty} a_k X^k$ est dans $\mathbb{C}[X]$, on pose

$$H(P) = \max\{|a_k| ; k \in \mathbb{N}\}.$$

Pour n et t dans \mathbb{N}^* , soit \mathcal{P}_n^t l'ensemble des P de $\mathbb{Z}[X]$ de degré n tels que $H(P) \leq t$. Si n est fixé,

$$|\mathcal{P}_n^t| = 2t(2t+1)^n \underset{t \rightarrow +\infty}{\sim} (2t)^{n+1}.$$

Soit aussi \mathcal{R}_n^t l'ensemble des P de \mathcal{P}_n^t réductibles sur \mathbb{Q} , c'est-à-dire, d'après le théorème 4, produits de deux polynômes non constants de $\mathbb{Z}[X]$. Le quotient $\pi_{n,t} = \frac{|\mathcal{R}_n^t|}{|\mathcal{P}_n^t|}$ est la probabilité pour qu'un polynôme aléatoire suivant la loi uniforme sur \mathcal{P}_n^t soit réductible sur \mathbb{Q} . Le résultat suivant (Kuba, 2009) améliore des énoncés bien plus anciens et justifie le titre de ce paragraphe.

Théorème 5. *On a*

$$\forall n \geq 3, \quad \pi_{n,t} \underset{t \rightarrow +\infty}{=} O\left(\frac{1}{t}\right) \quad \text{et} \quad \pi_{2,t} \underset{t \rightarrow +\infty}{=} O\left(\frac{\ln(t)}{t}\right).$$

La démonstration est fondée sur le résultat suivant.²¹

Lemme 5. *Soient k et ℓ dans \mathbb{N} . Il existe une constante $c_{k,\ell} > 0$ telle que*

$$\forall (U, V) \in \mathbb{C}_k[X] \times \mathbb{C}_\ell[X], \quad H(UV) \geq c_{k,\ell} H(U) H(V).$$

Preuve. Munissons l'espace $\mathbb{C}_k[X] \times \mathbb{C}_\ell[X]$ de la topologie usuelle. L'ensemble

$$K = \{(U, V) \in \mathbb{C}_k[X] \times \mathbb{C}_\ell[X] ; H(U) = H(V) = 1\}$$

est alors une partie compacte de cet espace. La fonction

$$(U, V) \in \mathbb{C}_k[X] \times \mathbb{C}_\ell[X] \mapsto H(UV)$$

est continue et prend des valeurs > 0 sur K . Reste à noter $c_{k,\ell}$ le minimum de cette fonction sur le compact K pour conclure par homogénéité.

Le lemme immédiat ci-après est formulé pour plus de clarté.

Lemme 6. *Soit $j \in \mathbb{N}^*$. Si \mathcal{Q}_j^t est l'ensemble $\mathcal{P}_j^t \setminus \mathcal{P}_j^{t-1}$ des P de $\mathbb{Z}[X]$ de degré j tels que $H(P) = t$, alors*

$$|\mathcal{Q}_j^t| = 2(t(2t+1)^{j+1} - (t-1)(2t-1)^{j+1}), \quad |\mathcal{Q}_j^t| \underset{t \rightarrow +\infty}{\sim} (j+1) 2^{j+1} t^j.$$

Preuve du théorème 5. Pour $k \in \{1, \dots, n-1\}$, soit $\mathcal{R}_{n,k}^t$ l'ensemble des éléments de \mathcal{R}_n^t de la forme UV où U et V sont dans $\mathbb{Z}[X]$, de degrés respectifs k et $n-k$. On a

$$\mathcal{R}_n^t = \bigcup_{k=1}^{n-1} \mathcal{R}_{n,k}^t.$$

Pour conclure, il suffit donc d'établir que, pour $n \geq 3$ et $1 \leq k \leq n-1$,

$$|\mathcal{R}_{n,k}^t| \underset{t \rightarrow +\infty}{=} O(t^n)$$

et que

$$|\mathcal{R}_{2,1}^t| \underset{t \rightarrow +\infty}{=} O(t^2 \ln(t))$$

Le cardinal de $\mathcal{R}_{n,k}^t$ est majoré par le nombre de couples (U, V) de $\mathbb{Z}[X]^2$ tels que U soit de degré k , V de degré $n-k$ et $H(UV) \leq t$, donc, grâce au lemme 5, par le nombre de couples (U, V) de $\mathbb{Z}[X]^2$ tels que U soit de degré k , V de degré $n-k$ et $H(U)H(V) \leq \frac{t}{c_{k,n-k}}$.

21. Dans lequel il est possible de donner une constante $c_{k,\ell}$ explicite, au prix d'une preuve un peu plus compliquée.

D'autre part, grâce au lemme 6, on dispose, pour $j \in \mathbb{N}^*$, de $\kappa_j > 0$ tel que

$$\forall t \in \mathbb{N}^*, \quad |\mathcal{Q}_j^t| \leq \kappa_j t^j.$$

Finalement

$$|\mathcal{R}_{n,k}^t| \leq \sum_{\substack{(x,y) \in \mathbb{N}^{*2} \\ xy \leq \frac{t}{c_{k,n-k}}}} |\mathcal{Q}_k^x| |\mathcal{Q}_{n-k}^y| \leq \kappa_k \kappa_{n-k} \sum_{\substack{(x,y) \in \mathbb{N}^{*2} \\ xy \leq \frac{t}{c_{k,n-k}}}} x^k y^{n-k}.$$

Le théorème 5 résulte donc en fin de compte du lemme suivant.

Lemme 7. *Soient a et b dans \mathbb{R}^+ . Pour T dans \mathbb{R}^{+*} , posons*

$$S_{a,b}(T) = \sum_{\substack{(x,y) \in \mathbb{N}^{*2} \\ xy \leq T}} x^a y^b.$$

Alors $a \neq b \implies S_{a,b}(T) \underset{T \rightarrow +\infty}{=} O(T^{\max(a,b)+1})$ et $S_{a,a}(T) \underset{T \rightarrow +\infty}{=} O(T^{a+1} \ln(T))$.

Preuve du lemme 7. On peut supposer que $a \geq b$. On a d'abord

$$S_{a,b}(T) = \sum_{\substack{y \in \mathbb{N}^* \\ y \leq T}} y^b \left(\sum_{\substack{x \in \mathbb{N}^* \\ x \leq T/y}} x^a \right).$$

Alors

$$\sum_{x \leq T/y} x^a \underset{T \rightarrow +\infty}{=} O(T^{a+1}/y^{a+1}).$$

Si $a > b$, la série $\sum \frac{1}{y^{a+1-b}}$ converge et le résultat suit. Si $a = b$, on conclut via l'estimation classique des nombres harmoniques.

Exercice 46. ③ *Donner un équivalent de $S_{a,b}(T)$ lorsque T tend vers $+\infty$.*

Pour $n \geq 3$, on voit, en considérant l'ensemble des polynômes nuls en 0, que $\pi_{n,t} \geq \frac{1}{2t+1}$: l'estimation est optimale. Si $n = 2$, l'optimalité subsiste, mais la démonstration est plus délicate.²²

Exercice 47. ⑤ *Montrer que*

$$\frac{\ln(t)}{t} \underset{t \rightarrow +\infty}{=} O(\pi_{2,t}).$$

Exercice 48. ② *Si $n \geq 2$ est un entier, p un nombre premier, $t \in \mathbb{N}^*$, on note $\mathcal{E}_{n,p}^t$ l'ensemble des P de \mathcal{P}_n^t vérifiant le critère d'Eisenstein pour le nombre premier p . Pour n et p fixés, déterminer la limite de $\frac{|\mathcal{E}_{n,p}^t|}{|\mathcal{P}_n^t|}$.*²³

22. En 2014, Dubickas a donné un équivalent de $\pi_{n,t}$ lorsque t tend vers $+\infty$.

23. Soit \mathcal{P} l'ensemble des nombres premiers. En utilisant une méthode de crible, Dubickas a montré, en 2014, que $\frac{|\bigcup_{p \in \mathcal{P}} \mathcal{E}_{n,p}^t|}{|\mathcal{P}_n^t|}$ converge, lorsque $t \rightarrow +\infty$ vers une limite $\ell_n < 1$ explicite (un produit infini), qui tend vers 0 lorsque n tend vers $+\infty$. L'application directe du critère d'Eisenstein manque donc la plupart des irréductibles.

3 Racines de l'unité

Les racines de l'unité jouent un rôle important (resp. central) dans la résolubilité par radicaux (resp. dans le travail de Gauss sur les polygones réguliers). On entame ici leur étude.

3.1 Groupes de racines de l'unité

Cyclicité d'un sous-groupe fini de (\mathbb{K}^, \cdot)*

Le théorème ci-après est bien connu pour $\mathbb{K} = \mathbb{C}$.²⁴

Théorème 6. *Soit \mathbb{K} un corps. Tout sous-groupe fini de (\mathbb{K}^*, \times) est cyclique.*

Voici deux preuves de ce résultat, toutes deux fondées sur le fait que, dans un corps, une équation polynomiale de degré d admet au plus d racines. La première utilise en outre la notion d'exposant d'un groupe abélien fini, la seconde les propriétés élémentaires de la fonction d'Euler. Dans les deux démonstrations, G est un sous-groupe fini de (\mathbb{K}^*, \times) .

Preuve 1. Soit n l'exposant de G , c'est-à-dire le ppcm des ordres des éléments de G . Par définition, tout élément de G est racine de $X^n - 1$; puisque \mathbb{K} est un corps, on en déduit que $|G| \leq n$. D'autre part, il est classique que, comme tout groupe abélien fini, G contient un élément x d'ordre n . Il est alors clair que G est cyclique engendré par x .

Preuve 2. Soit D l'ensemble des diviseurs de $|G|$ dans \mathbb{N}^* . Pour $d \in D$, soit O_d l'ensemble des éléments de G d'ordre d . On souhaite démontrer que O_d est non vide. On va en fait établir que, pour tout $d \in D$, O_d est de cardinal $\varphi(d)$.

Soit $d \in D$. Si Γ_d est l'ensemble des éléments x de G tels que $x^d = 1$, alors Γ_d est de cardinal au plus d (ensemble des racines d'un polynôme de degré d dans un corps). D'autre part, la famille $(O_d)_{d \in D}$ est une partition de G , d'où :

$$\sum_{d \in D} |O_d| = g.$$

En utilisant la relation classique²⁵ :

$$\forall m \in \mathbb{N}^*, \quad \sum_{d|m} \varphi(d) = m,$$

on voit qu'il suffit de démontrer que, pour tout d de D , $|O_d|$ est majoré par $\varphi(d)$. Supposons O_d non vide. Tout x de O_d engendre un sous-groupe de cardinal d contenu dans Γ_d et donc égal à Γ_d ; il s'ensuit que Γ_d est cyclique, que O_d est l'ensemble de ses générateurs et donc de cardinal $\varphi(d)$, ce qui achève la démonstration.

Remarque Ineffectivité

Ces démonstrations ne produisent pas de générateur de G . De fait, dans le cas du groupe (\mathbb{F}_p^*, \times) , qui remonte à Gauss, on n'a que peu de renseignements sur le plus petit x de $\{1, \dots, p-1\}$ dont la classe modulo p engendre (\mathbb{F}_p^*, \times) .²⁶

24. Si G est un sous-groupe d'ordre n de \mathbb{C}^* , tout z de G vérifie $z^n = 1$, d'où $G \subset \mathbb{U}_n$, puis l'égalité au vu des cardinaux.

25. Qui est d'ailleurs conséquence du lemme 8 du paragraphe suivant.

26. On dispose cependant d'estimations. La première (Vinogradov) assure ainsi que la plus petite racine primitive modulo p est, pour tout $\varepsilon > 0$, $O\left(p^{\frac{1}{2} + \varepsilon}\right)$ lorsque p tend vers $+\infty$. L'exposant critique $1/2$ a été abaissé par Burgess. On a en fait beaucoup mieux en acceptant l'« hypothèse de Riemann généralisée ».

Groupe des racines n -ièmes

Si \mathbb{K} est un corps et $n \in \mathbb{N}^*$, on notera $\mathbb{U}_n(\mathbb{K})$ le groupe des racines n -ièmes de 1 dans \mathbb{K} :

$$\mathbb{U}_n(\mathbb{K}) = \{x \in \mathbb{K} ; x^n = 1\}.$$

Pour $\mathbb{K} = \mathbb{C}$, on note, selon l'usage :

$$\mathbb{U}_n(\mathbb{C}) = \mathbb{U}_n.$$

Il se peut que $\mathbb{U}_n(\mathbb{K})$ soit réduit à $\{1\}$; exemple : \mathbb{K} est un sous-corps de \mathbb{R} et n est impair. Le cas intéressant est celui où $X^n - 1$ est scindé sur \mathbb{K} . Calculons alors le cardinal de $\mathbb{U}_n(\mathbb{K})$.

En caractéristique nulle, il est clair que les racines de $X^n - 1$ sont simples (sa dérivée est nX^{n-1} dont la seule racine est 0), et $\mathbb{U}_n(\mathbb{K})$ est de cardinal n .

En caractéristique $p \in \mathcal{P}$, l'argument ne fonctionne plus, car la dérivée nX^{n-1} de $X^n - 1$ est nulle si p divise n . On pose donc $n = p^r m$ où $r \in \mathbb{N}$ et $m \wedge p = 1$. Si $x \in \mathbb{K}$, on a :

$$x^n = 1 \Leftrightarrow x^{p^r m} = 1 \Leftrightarrow (x^m)^{p^r} - 1 = 0 \Leftrightarrow (x^m - 1)^{p^r} = 0 \Leftrightarrow x^m = 1.$$

Ainsi $\mathbb{U}_n(\mathbb{K}) = \mathbb{U}_m(\mathbb{K})$. Et puisque p ne divise pas m , $X^m - 1$ est à racines simples ; en fin de compte, $\mathbb{U}_n(\mathbb{K}) = \mathbb{U}_m(\mathbb{K})$ est de cardinal m .

On peut retenir de cette petite discussion le résultat suivant.

Proposition 6. *Soient \mathbb{K} un corps, n dans \mathbb{N}^* . Alors $\mathbb{U}_n(\mathbb{K})$ est de cardinal n si et seulement si $X^n - 1$ est scindé sur \mathbb{K} et la caractéristique de \mathbb{K} ne divise pas n .*

Sous les hypothèses de la proposition, on appelle *racine n -ième primitive de l'unité* tout générateur de $\mathbb{U}_n(\mathbb{K})$, i.e. tout élément d'ordre n du groupe (\mathbb{K}^*, \times) .

Classiquement, un groupe cyclique G de cardinal n admet $\varphi(n)$ générateurs, où φ est la fonction d'Euler. Si x est un tel générateur, l'ensemble de tous les générateurs de G est

$$\{x^k ; 1 \leq k \leq n \text{ et } k \wedge n = 1\}.$$

Ainsi les générateurs de (\mathbb{U}_n, \times) (ou racines primitives n -ièmes de 1 dans \mathbb{C}) sont les $e^{\frac{2ik\pi}{n}}$ avec $0 \leq k \leq n - 1$ et $k \wedge n = 1$.

Exercice 49. ③ *Soit \mathbb{K} un corps algébriquement clos. Pour quels $n \in \mathbb{N}^*$ existe-t-il un sous-groupe d'ordre n de (\mathbb{K}^*, \times) ?*

Exercice 50. ④ *Soit \mathbb{K} un corps algébriquement clos de caractéristique nulle.*

a) *Montrer que le groupe multiplicatif $\text{Tor}(\mathbb{K}^*)$ des racines de 1 dans \mathbb{K} est isomorphe au groupe additif \mathbb{Q}/\mathbb{Z} .*

b) *Si p est un nombre premier, soit C_p le sous-groupe de \mathbb{Q}/\mathbb{Z} constitué des éléments dont l'ordre est une puissance de p . Montrer que \mathbb{Q}/\mathbb{Z} est somme directe des C_p pour p premier.*

Exercice 51. ④ *Si \mathbb{K} est un corps algébriquement clos de caractéristique p première, montrer que le groupe $\text{Tor}(\mathbb{K}^*)$ est isomorphe à la somme directe des C_q pour q premier différent de p .*

Exercice 52. ④ *Soit \mathbb{H} l'anneau à division des quaternions réels, introduit au début de la section 2. Montrer que, pour tout $m \in \mathbb{N}^*$, \mathbb{H}^* contient un groupe isomorphe au groupe diédral \mathcal{D}_m . Le théorème 4 n'est donc pas vrai sans hypothèse de commutativité.²⁷*

²⁷. On peut décrire tous les sous-groupes finis de \mathbb{H}^* . Le plus célèbre est le « groupe quaternionique » \mathbb{H}_8 , constitué, dans la description classique des quaternions, des 8 éléments $\pm 1, \pm i, \pm j, \pm k$, qui n'est ni commutatif ni isomorphe au groupe diédral \mathcal{D}_4 .

3.2 Polynômes cyclotomiques (I)

« Cyclotomie » signifie « division du cercle ». La version algébrique, i.e. l'étude des racines de l'unité, fait apparaître une importante famille de polynômes.

Si $n \in \mathbb{N}^*$, on note μ_n l'ensemble des éléments d'ordre n de \mathbb{C}^* , ou de \mathbb{U}_n . On a

$$\mu_n = \left\{ e^{\frac{2ik\pi}{n}} ; 1 \leq k \leq n, k \wedge n = 1 \right\}.$$

Le cardinal de μ_n est $\varphi(n)$ (indicateur d'Euler). On définit le n -ième polynôme cyclotomique :

$$\Phi_n = \prod_{\omega \in \mu_n} (X - \omega) = \prod_{1 \leq k \leq n, k \wedge n = 1} \left(X - e^{\frac{2ik\pi}{n}} \right).$$

Le degré de Φ_n est $\varphi(n)$.

Exercice 53. ② Écrire Φ_n pour $1 \leq n \leq 10$.

Soit p un nombre premier. On a $\mu_p = \mathbb{U}_p \setminus \{1\}$, donc $\Phi_p = \frac{X^p - 1}{X - 1} = \sum_{i=0}^{p-1} X^i$. Plus généralement, si p est premier et si α appartient à \mathbb{N}^* , on a

$$\mu_{p^\alpha} = \mathbb{U}_{p^\alpha} \setminus \mathbb{U}_{p^{\alpha-1}}, \quad \Phi_{p^\alpha} = \frac{X^{p^\alpha} - 1}{X^{p^{\alpha-1}} - 1} = \Phi_p(X^{p^{\alpha-1}}).$$

Lemme 8. On a²⁸ :

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

Preuve. Il suffit de regrouper les éléments de \mathbb{U}_n selon leur ordre, i.e. d'écrire :

$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega) = \prod_{d|n} \left(\prod_{\omega \in \mu_d} (X - \omega) \right) = \prod_{d|n} \Phi_d.$$

On peut alors établir par récurrence sur n la :

Proposition 7. Le polynôme Φ_n appartient à $\mathbb{Z}[X]$.

Preuve. Pour $n = 1$, c'est clair. Pour faire fonctionner la récurrence, il suffit d'écrire

$$\Phi_n = \frac{X^n - 1}{\prod_{d|n, d < n} \Phi_d}$$

et de remarquer que le numérateur du second membre est unitaire.

Le théorème ci-après est fondamental. Nous l'établissons ici dans un cas particulier. Le cas général recevra deux démonstrations dans la suite (chapitre 2, 1.6, chapitre 4, 3.4).

Théorème 7. Pour tout n de \mathbb{N}^* , le polynôme Φ_n est irréductible sur \mathbb{Q} .²⁹

28. Ce résultat contient la classique relation d'Euler : $n = \sum_{d|n} \varphi(d)$.

29. Gauss a énoncé ce résultat de manière générale, mais ne l'a démontré que pour n premier. La première preuve publiée du cas général semble due à Kronecker.

Preuve pour $n = p \in \mathcal{P}$. On dispose dans ce cas d'une preuve simple et élégante. On a

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \sum_{i=0}^{p-2} \binom{p}{i+1} X^i.$$

La conclusion résulte du critère d'Eisenstein (proposition 5) et du fait que, puisque p est premier, p divise $\binom{p}{j}$ pour tout j de $\{1, \dots, p-1\}$.

Exercice 54. ③ Si $p \in \mathcal{P}$ et si $\alpha \in \mathbb{N}^*$, montrer que Φ_{p^α} est irréductible sur \mathbb{Q} .

Exercice 55. ③ Préciser le terme constant de Φ_n .

Exercice 56. ③ Soit n un élément de \mathbb{N}^* .

a) Montrer que, si n est impair et différent de 1, $\Phi_{2n}(X) = \Phi_n(-X)$.

b) Montrer que, si n est divisible par 4, Φ_n est pair. Réciproque ?

c) Si p est un nombre premier et n un entier divisible par p (resp. non divisible par p), montrer

$$\Phi_{pn}(X) = \Phi_n(X^p) \quad (\text{resp.} \quad \Phi_{pn}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}).$$

Exercice 57. ③ Si μ est la fonction de Moebius, établir, pour n dans \mathbb{N}^* :

$$\Phi_n = \prod_{d|n} (X^d - 1)^{\mu\left(\frac{n}{d}\right)}.$$

Exercice 58. ③ Soient p et q deux nombres premiers tels que $p < q$. Montrer que les coefficients de Φ_{pq} sont dans $\{-1, 0, 1\}$.

Exercice 59. ④ Calculer $\Phi_n(1)$ et en déduire l'ensemble des n de \mathbb{N}^* tels que tous les coefficients de Φ_n appartiennent à $\{0, 1\}$.

Exercice 60. ⑤ Montrer que, si $(a_i)_{1 \leq i \leq n}$ est une suite strictement croissante d'éléments de \mathbb{N}^* , alors on a la relation de divisibilité dans $\mathbb{Z}[X]$:

$$\prod_{1 \leq i < j \leq n} (X^j - X^i) \mid \prod_{1 \leq i < j \leq n} (X^{a_j} - X^{a_i}).$$

L'exercice suivant établit que, si m et n sont deux éléments distincts de \mathbb{N}^* , les valeurs de Φ_m et Φ_n sur les entiers sont « presque premières entre elles ».

Exercice 61. ④ Soient m et n deux éléments distincts de \mathbb{N}^* , q dans \mathbb{Z} . On pose

$$\ell = \Phi_m(q) \wedge \Phi_n(q).$$

a) Montrer que ℓ divise $(m \vee n)q^{(m \vee n) - 1}$. On pourra dériver la factorisation de $X^{m \vee n} - 1$ fournie par le lemme 8.

b) Montrer qu'il existe V_m et V_n dans $\mathbb{Z}[X]$ tels que

$$(X^n - 1)V_n(X) + (X^m - 1)V_m(X) = X^{m \wedge n} - 1.$$

En déduire que ℓ divise $q^{m \wedge n} - 1$, puis que ℓ divise $(m \vee n) \wedge (q^{m \wedge n} - 1)$.

La littérature relative aux coefficients de Φ_n est riche. Le calcul de Φ_n pour les petites valeurs de n suggère que les coefficients de Φ_n valent tous 0, 1 ou -1 . L'exercice suivant montre qu'il n'en est rien : tout entier relatif apparaît comme coefficient d'un polynôme cyclotomique.³⁰

Exercice 62. ⑤ Soient $m \in \mathbb{N}$ impair, $(p_i)_{1 \leq i \leq m}$ une suite strictement croissante de nombres premiers, $n = \prod_{i=1}^m p_i$.

a) Montrer que

$$(X - 1) \Phi_n \equiv \prod_{i=1}^m (X^{p_i} - 1) [X^{p_1 p_2}].$$

b) On suppose que $p_m < p_1 + p_2$. Montrer que le coefficient de X^{p_m} dans Φ_n est $1 - m$. Calculer le coefficient de $X^{p_m - 2}$ dans Φ_n .

c) Montrer que, pour tout m impair, on peut construire une suite $(p_k)_{1 \leq k \leq m}$ de nombres premiers possédant les propriétés précédentes.

d) Montrer que, si $\ell \in \mathbb{Z}$, il existe $N \in \mathbb{N}^*$ tel que ℓ soit un coefficient de Φ_N (Suzuki, 1987).

Exercice 63. ④ Pour $n \in \mathbb{N}^*$, on pose

$$F_n = \prod_{d|n} \left(\sum_{j=0}^{\frac{n}{d}-1} X^{jd} \right).$$

a) Notons $c_k(P)$ le coefficient d'indice k de l'élément P de $\mathbb{C}[X]$. Montrer :

$$\forall n \in \mathbb{N}^*, \quad \forall k \in \mathbb{N}, \quad |c_k(\Phi_n)| \leq c_k(F_n).$$

b) Pour n dans \mathbb{N}^* , soit A_n la somme des valeurs absolues des coefficients de Φ_n . Montrer l'inégalité suivante (Bateman, 1949) :

$$A_n \leq F_n(1).$$

c) Soient $n \in \mathbb{N}^*$, $d(n)$ le nombre de diviseurs de n . Montrer que :

$$F_n(1) = n^{d(n)/2}.$$

4 Polynômes symétriques

Un des principaux outils de la théorie classique des équations est le *théorème des polynômes symétriques*. Ce résultat, démontré en 4.1, a joué un rôle central dans les premières présentations de la théorie de Galois, avant d'en être écarté par Dedekind, Noether et Artin. Il conserve un intérêt véritable, notamment par son caractère effectif. Nous lui préférons des arguments plus abstraits fondés sur la notion d'extension, mais signalerons la possibilité de l'utiliser le cas échéant.

La lecture de 4.2 n'est pas nécessaire pour la suite. On y montre comment Lagrange a utilisé les polynômes symétriques dans le travail évoqué en 1.2.

Autre outil important d'algèbre polynomiale « effective » : le résultant. Nous introduisons en 4.3 le cas particulier du discriminant, seul véritablement utile pour nous, le cas général en 4.4.

³⁰. Ainsi, l'exercice montre que le coefficient de X^7 dans Φ_{105} est égal à -2 . Pour $n \leq 104$, tous les coefficients de Φ_n sont dans $\{-1, 0, 1\}$.

Le paragraphe final 4.5, relatif aux sommes de Newton, ne sera pas utilisé dans la suite. On y présente les classiques relations de récurrence de Newton et l'énoncé moins connu de Waring exprimant lesdites sommes comme polynômes en les fonctions symétriques élémentaires.

Dans cette section, \mathbb{A} est un anneau commutatif, n un élément de \mathbb{N}^* . On note $\mathbb{A}[X_1, \dots, X_n]$ l'anneau des polynômes en les indéterminées algébriquement indépendantes X_1, \dots, X_n à coefficients dans \mathbb{A} . La construction de cet anneau est analogue à celle des anneaux de polynômes à une variable. Ensemblistement, $\mathbb{A}[X_1, \dots, X_n]$ est l'ensemble des familles $(a_\alpha)_\alpha \in \mathbb{A}^{(\mathbb{N}^n)}$.³¹ L'addition et la multiplication sont définies de la façon naturelle. Si $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, on note

$$X^\alpha = \prod_{i=1}^n X_i^{\alpha_i}.$$

Par définition, les éléments de $\mathbb{A}[X_1, \dots, X_n]$ sont donc les combinaisons linéaires presque nulles, à coefficients dans \mathbb{A} :

$$(1) \quad \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha.$$

De plus, l'écriture (1) d'un élément de $\mathbb{A}[X_1, \dots, X_n]$ est unique (indépendance algébrique de X_1, \dots, X_n). Les aX^α , $a \in \mathbb{A} \setminus \{0\}$, $\alpha \in \mathbb{N}^n$, sont appelés *monômes*.

Si $(\alpha, a) \in \mathbb{N}^n \times \mathbb{A} \setminus \{0\}$, on définit le *degré* de aX^α est $|\alpha| = \sum_{i=1}^n \alpha_i$. Le degré d'un élément de $\mathbb{A}[X_1, \dots, X_n] \setminus \{0\}$ est le maximum des degrés de ses monômes.

Soit $k \in \mathbb{N}$. Un élément de $\mathbb{A}[X_1, \dots, X_n]$ est *homogène de degré k* s'il s'écrit $\sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha|=k}} a_\alpha X^\alpha$.

Il suit immédiatement de cette définition qu'un élément de $\mathbb{A}[X_1, \dots, X_n]$ s'écrit d'une unique façon $\sum_{k \in \mathbb{N}} P_k$, où, pour tout $k \in \mathbb{N}$, $P_k \in \mathbb{A}[X_1, \dots, X_n]$ est homogène de degré k .

Enfin, on vérifie que, si \mathbb{A} est intègre, il en est de même de $\mathbb{A}[X_1, \dots, X_n]$.³²

4.1 Le théorème des polynômes symétriques

Ordre lexicographique sur les monômes

On munit \mathbb{N}^n de l'ordre lexicographique, que l'on note \leq_{lex} . Rappelons qu'un ordre \leq sur un ensemble non vide E est un *bon ordre* si toute partie non vide de E admet un plus petit élément, ou, de façon équivalente, si \leq est total et s'il n'existe pas de suite infinie d'éléments de E strictement décroissante pour \leq .³³

Lemme 9. *L'ordre lexicographique sur \mathbb{N}^n est un bon ordre.*³⁴

Preuve. On raisonne par récurrence sur n . Le résultat est clair si $n = 1$. Supposons $n \geq 2$ et le résultat vrai à l'ordre $n - 1$. Notons π l'application de \mathbb{N}^n dans \mathbb{N}^{n-1} définie par

$$\forall (x_1, \dots, x_n) \in \mathbb{N}^n, \quad \pi(x_1, \dots, x_n) = (x_1, \dots, x_{n-1}).$$

Soit E une partie non vide de \mathbb{N}^n . Par hypothèse de récurrence, $\pi(E)$ admet un plus petit élément (e_1, \dots, e_{n-1}) . Si $e = (e_1, \dots, e_n) \in E$ est tel que e_n soit minimal, e est le plus petit élément de E .

31. Rappelons que $\mathbb{A}^{(I)}$ est l'ensemble des familles d'éléments de \mathbb{A} indexées par I et presque nulles.

32. En revanche, $\mathbb{A}[X_1, \dots, X_n]$ est principal si et seulement si $n = 1$ et \mathbb{A} est un corps : exercice 15, 2.1.

33. Les puristes noteront l'utilisation de l'axiome du choix dépendant.

34. On suggère au lecteur de se représenter graphiquement l'ordre lexicographique sur \mathbb{N}^2 .

Exercice 64. ② Quels sont les x de \mathbb{N}^n tels que l'ensemble des éléments de \mathbb{N}^n plus petits que x pour l'ordre lexicographique soit fini ?

Un bon ordre est évidemment total. L'intérêt des bons ordres est de permettre des démonstrations par récurrence, grâce au lemme immédiat ci-après (« principe de récurrence transfinie »)

Lemme 10. Soient (E, \leq) un ensemble bien ordonné, $\mathcal{P}(x)$ une propriété dépendant d'un élément x de E . Supposons que, pour tout x de E , on ait l'implication

$$\forall y \in E, y < x, \mathcal{P}(y) \text{ vraie} \implies \mathcal{P}(x) \text{ vraie.}$$

Alors $\mathcal{P}(x)$ est vraie pour tout x de E .

Preuve. Supposons non vide l'ensemble X des x de E tels que $\mathcal{P}(x)$ soit fausse. On obtient une contradiction en considérant le plus petit élément de X .³⁵

On transporte l'ordre lexicographique de \mathbb{N}^n à l'ensemble des monômes de $\mathbb{A}[X_1, \dots, X_n]$. Pour $P = \sum_{\alpha \in \mathbb{N}^n} c_\alpha X^\alpha$ dans $\mathbb{A}[X_1, \dots, X_n] \setminus \{0\}$, on note $M(P)$ le plus grand monôme de P pour l'ordre \leq_{lex} . Par exemple

$$M(X_1^2 X_2 X_3^5 - 6X_1^3 X_3 + 8X_1^2 X_2^7 X_3^8) = -6X_1^3 X_3.$$

Lemme 11. Si P et Q sont dans $\mathbb{A}[X_1, \dots, X_n] \setminus \{0\}$ et si le coefficient dominant de P n'est pas divisible de 0, on a :

$$M(PQ) = M(P) M(Q).$$

Preuve. Car, si $\alpha, \alpha', \beta, \beta'$ sont dans \mathbb{N}^n , alors

$$(\alpha \leq_{\text{lex}} \alpha' \quad \text{et} \quad \beta \leq_{\text{lex}} \beta') \implies \alpha + \beta \leq_{\text{lex}} \alpha' + \beta'.$$

Polynômes symétriques élémentaires

Les formules de Viète permettent d'exprimer les coefficients d'un polynôme en fonction de ses racines. Elles font apparaître les *polynômes symétriques élémentaires*, définis de la façon suivante. Pour k dans $\{1, \dots, n\}$, soit

$$\Sigma_k = \Sigma_k(X_1, \dots, X_n) = \sum_{\substack{I \in \mathcal{P}(\{1, \dots, n\}) \\ |I|=k}} \prod_{i \in I} X_i.$$

Pour tout k , Σ_k est homogène de degré k . Si T est une nouvelle indéterminée (algébriquement indépendante de X_1, \dots, X_n), on a donc

$$\prod_{k=1}^n (T - X_k) = T^n + \sum_{k=1}^n (-1)^k \Sigma_k T^{n-k}.$$

Par exemple

$$\Sigma_1 = \sum_{i=1}^n X_i, \quad \Sigma_2 = \sum_{1 \leq i < j \leq n} X_i X_j, \quad \Sigma_n = \prod_{i=1}^n X_i.$$

On a d'autre part

$$\forall k \in \{1, \dots, n\}, \quad M(\Sigma_k) = \prod_{i=1}^k X_i.$$

³⁵. Il n'y a pas d'initialisation (quantification sur le vide).

Polynômes symétriques

Faisons agir \mathcal{S}_n sur $\mathbb{A}[X_1, \dots, X_n]$ par permutation des indéterminées :

$$\forall (\sigma, P) \in \mathcal{S}_n \times \mathbb{A}[X_1, \dots, X_n], \quad \sigma.P(X_1, \dots, X_n) = P(X_{\sigma^{-1}(1)}, \dots, X_{\sigma^{-1}(n)}).$$

Un polynôme P de $\mathbb{A}[X_1, \dots, X_n]$ est dit *symétrique* s'il est fixe sous cette action, i.e. si

$$\forall \sigma \in \mathcal{S}_n, \quad P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n).$$

Exemples

1. À partir de $P \in \mathbb{A}[X_1, \dots, X_n]$, on forme les deux polynômes symétriques

$$\sum_{\sigma \in \mathcal{S}_n} \sigma.P \quad \text{et} \quad \prod_{\sigma \in \mathcal{S}_n} \sigma.P.$$

2. Les $\Sigma_k, 1 \leq k \leq n$, sont des polynômes symétriques. Il en est de même de $Q(\Sigma_1, \dots, \Sigma_n)$ pour tout polynôme Q à n indéterminées à coefficients dans \mathbb{A} .

Le théorème des polynômes symétriques est la réciproque de l'exemple 2.³⁶ La démonstration de la partie « existence » est un algorithme, qui repose sur le fait que \leq_{lex} est un bon ordre et sur le lemme suivant.

Lemme 12. *Soit P dans $\mathbb{A}[X_1, \dots, X_n] \setminus \{0\}$ un polynôme symétrique. Posons $M(P) = c_\alpha X^\alpha$ avec $c_\alpha \in \mathbb{A} \setminus \{0\}$. Alors*

$$\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n.$$

Preuve. Le polynôme P contient tous les monômes déduits de $c_\alpha X^\alpha$ par permutation.

Théorème 8. *Soient P dans $\mathbb{A}[X_1, \dots, X_n]$ un polynôme symétrique, Y_1, \dots, Y_n des indéterminées indépendantes. Il existe un unique Q dans $\mathbb{A}[Y_1, \dots, Y_n]$ tel que*

$$P(X_1, \dots, X_n) = Q(\Sigma_1, \dots, \Sigma_n).$$

Preuve du théorème 8 : existence. Soit P dans $\mathbb{A}[X_1, \dots, X_n] \setminus \{0\}$ un polynôme symétrique. Posons $M(P) = c_\alpha X^\alpha$ avec $c_\alpha \in \mathbb{A} \setminus \{0\}$. Comme \leq_{lex} est un bon ordre sur \mathbb{N}^n , le lemme 10 entraîne qu'il suffit, pour conclure, d'établir que l'on peut trouver $S \in \mathbb{A}[X_1, \dots, X_n]$ tel que, si $T = P - S(\Sigma_1, \dots, \Sigma_n)$, on ait

$$S = 0 \quad \text{ou} \quad T <_{\text{lex}} P.$$

Construisons S . Le lemme 12 assure que $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$. L'observation-clé est alors que, grâce au lemme 11,

$$M(c_\alpha \Sigma_1^{\alpha_1 - \alpha_2} \Sigma_2^{\alpha_2 - \alpha_3} \dots \Sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \Sigma_n^{\alpha_n}) = c_\alpha X^\alpha. \quad 37$$

Le polynôme $S = c_\alpha \Sigma_1^{\alpha_1 - \alpha_2} \Sigma_2^{\alpha_2 - \alpha_3} \dots \Sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \Sigma_n^{\alpha_n}$ vérifie la propriété voulue.

³⁶. Cet énoncé est démontré par Waring dans ses *Meditationes Algebraicae* de 1770, en utilisant l'algorithme proposé plus bas. Le résultat semble déjà bien établi à l'époque.

³⁷. Formule facile à découvrir : comme X_n n'intervient que dans Σ_n , il faut « partir de la fin » i.e. de $\Sigma_n^{\alpha_n}$ et ajuster successivement les exposants.

Preuve du théorème 8 : unicité. Il suffit d'établir que le seul Q de $\mathbb{A}[X_1, \dots, X_n]$ vérifiant

$$Q(\Sigma_1, \dots, \Sigma_n) = 0$$

est le polynôme nul. On note à cet effet que

$$\forall c \in \mathbb{A} \setminus \{0\}, \forall \alpha \in \mathbb{N}^n, \quad M \left(c \prod_{i=1}^n \Sigma_k^{\alpha_k} \right) = c \prod_{j=1}^n X_j^{\sum_{i=j}^n \alpha_i}.$$

Pour conclure, il suffit d'utiliser l'injectivité de l'application

$$\alpha \in \mathbb{N}^n \mapsto \left(\sum_{i=1}^n \alpha_i, \sum_{i=2}^n \alpha_i, \dots, \alpha_n \right) \in \mathbb{N}^n.$$

Remarques

1. Homogénéité

Si P est homogène de degré k , il en est de même de $P - Q(\Sigma_1, \dots, \Sigma_n)$: l'algorithme s'effectue composante homogène par composante homogène.

2. Un exemple

En pratique, on peut utiliser des raccourcis. Prenons ainsi $n = 4$ et

$$P = (X_1 X_2 + X_3 X_4) (X_1 X_3 + X_2 X_4) (X_1 X_4 + X_2 X_3).$$

On a $M(P) = X_1^3 X_2 X_3 X_4$. L'algorithme conduit à former $P_1 = P - \Sigma_1^2 \Sigma_4$. Comme P est homogène de degré 6, il en est de même de P_1 , dont le plus grand monôme s'écrit donc $c X^\alpha$ avec $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 6$, $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) <_{\text{lex}} (3, 1, 1, 1)$ et (lemme 12) $\alpha_1 \geq \dots \geq \alpha_4$. Seuls $(2, 2, 2, 0)$ et $(2, 2, 1, 1)$ conviennent, ce qui assure que P est combinaison \mathbb{Z} -linéaire de $\Sigma_1^2 \Sigma_4$, Σ_3^2 et $\Sigma_2 \Sigma_4$. En substituant aux X_i des valeurs particulières, on arrive à

$$P = \Sigma_1^2 \Sigma_4 + \Sigma_3^2 - 4 \Sigma_2 \Sigma_4.$$

3. Autre démonstration

On peut également démontrer la partie « existence » du théorème par récurrence sur n et le degré de P de la manière suivante. Considérons $P \in \mathbb{A}[X_1, \dots, X_n] \setminus \{0\}$ symétrique et

$$Q(X_1, \dots, X_{n-1}) = P(X_1, \dots, X_{n-1}, 0).$$

Alors Q est un polynôme symétrique de $\mathbb{A}[X_1, \dots, X_{n-1}]$. Par récurrence sur n , on peut supposer que

$$Q(X_1, \dots, X_{n-1}) = R(\Sigma'_1, \dots, \Sigma'_{n-1}),$$

où les Σ'_k , $1 \leq k \leq n-1$, sont les polynômes symétriques élémentaires en X_1, \dots, X_{n-1} et où R est un polynôme à $n-1$ indéterminées à coefficients dans \mathbb{A} . Formons

$$S = P - R(\Sigma_1, \dots, \Sigma_{n-1}).$$

Le polynôme S de $\mathbb{A}[X_1, \dots, X_n]$ s'annule lorsqu'on substitue 0 à X_n et est donc divisible par X_n . Comme il est symétrique, il est divisible par Σ_n :

$$P = R(\Sigma_1, \dots, \Sigma_{n-1}) + \Sigma_n U,$$

où U est un élément de $\mathbb{A}[X_1, \dots, X_n]$ symétrique et de degré strictement inférieur à celui de P . Reste à raisonner par récurrence sur le degré.

Exercice 65. ① Écrire $X_1^2 X_2 + X_1^2 X_3 + X_2^2 X_1 + X_2^2 X_3 + X_3^2 X_1 + X_3^2 X_2$. comme un polynôme en les polynômes symétriques élémentaires.

Exercice 66. ③ Soit $\mathcal{P}(n)$ l'ensemble des $(\lambda_1, \dots, \lambda_n)$ de \mathbb{N}^n tels que $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$. Pour $\alpha \in \mathbb{N}^n$, soit $\lambda(\alpha)$ l'unique λ de $\mathcal{P}(n)$ de la forme $(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$ avec $\sigma \in \mathcal{S}_n$. Enfin, pour $\lambda \in \mathcal{P}(n)$, posons

$$m_\lambda = \sum_{\substack{\alpha \in \mathbb{N}^n \\ \lambda(\alpha) = \lambda}} X^\alpha.$$

Si $d \in \mathbb{N}$, montrer que la famille $(m_\lambda)_{\substack{\lambda \in \mathcal{P}(n) \\ |\lambda| = d}}$ est une \mathbb{A} -base du \mathbb{A} -module des polynômes symétriques homogènes de degré d de $\mathbb{A}[X_1, \dots, X_n]$.

Les exposés de la théorie de Galois « pré-Dedekind-Noether-Artin » utilisent le théorème 8 pour établir des résultats de rationalité.³⁸ Voici un exemple.

Corollaire 3. Soient \mathbb{K} un corps, \mathbb{A} un sous-anneau de \mathbb{K} , P dans $\mathbb{A}[X]$ unitaire, Ω un surcorps de \mathbb{K} sur lequel P est scindé :

$$P = \prod_{i=1}^n (X - x_i).$$

Alors, pour tout polynôme U de $\mathbb{A}[X_1, \dots, X_n]$ symétrique, on a

$$U(x_1, \dots, x_n) \in \mathbb{A}.$$

Preuve. Les $\Sigma_k(x_1, \dots, x_n)$ sont dans \mathbb{A} , d'où le résultat en appliquant le théorème 8 à U .

Fractions rationnelles symétriques

Si l'anneau de base est un corps, on a une version « fractions rationnelles » du théorème 8.

Corollaire 4. Soient \mathbb{K} un corps, Y_1, \dots, Y_n des indéterminées indépendantes, F dans $\mathbb{K}(X_1, \dots, X_n)$. Alors il existe G dans $\mathbb{K}(Y_1, \dots, Y_n)$ telle que

$$F(X_1, \dots, X_n) = G(\Sigma_1, \dots, \Sigma_n)$$

si et seulement si

$$\forall \sigma \in \mathcal{S}_n, \quad F(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = F(X_1, \dots, X_n).$$

Preuve. Seule l'implication réciproque mérite démonstration. Soit $F \in \mathbb{K}(X_1, \dots, X_n)$ invariante sous l'action de \mathcal{S}_n . Il nous suffit d'établir que F est quotient de deux polynômes symétriques pour conclure via le théorème 8. On écrit $F = \frac{P}{Q}$ où P et Q sont dans $\mathbb{K}[X_1, \dots, X_n]$ et $Q \neq 0$. Posons

$$\tilde{Q} = \prod_{\sigma \in \mathcal{S}_n} \sigma.Q.$$

Le polynôme \tilde{Q} est symétrique. Il en est de même de $U = \tilde{Q} F$, d'où le résultat.

³⁸. Rationalité = appartenance à l'anneau de base.

4.2 (*) Retour à Lagrange

Nous pouvons maintenant prouver le résultat de Lagrange mentionné dans la section 1.2.

Proposition 8. *Soit U un élément de $\mathbb{A}[X_1, \dots, X_n]$. Notons $\omega(U)$ l'orbite de U sous l'action de \mathcal{S}_n , T une nouvelle indéterminée indépendante de X_1, \dots, X_n . Alors*

$$\prod_{V \in \omega(U)} (T - V) \in \mathbb{A}[\Sigma_1, \dots, \Sigma_n][T]$$

est un polynôme unitaire de degré $|\omega(U)|$ qui annule U .

Preuve. Les coefficients de $\prod_{V \in \omega(U)} (T - U)$ vu comme polynôme en T sont symétriques.

Lagrange a établi des résultats plus généraux de même nature; nous y reviendrons dans le chapitre 4.³⁹

Corollaire 5. *Soient \mathbb{K} un corps, \mathbb{A} un sous-anneau de \mathbb{K} , P dans $\mathbb{A}[X]$ unitaire scindé sur \mathbb{K} :*

$$P = \prod_{i=1}^n (X - x_i).$$

Pour U dans $\mathbb{A}[X_1, \dots, X_n]$,

$$\prod_{V \in \omega(U)} (T - V(x_1, \dots, x_n)) \in \mathbb{A}[T].$$

La notion de groupe de Galois nous permettra d'améliorer le corollaire 5 : en tenant compte des symétries de P , c'est-à-dire des relations algébriques entre les x_i , on peut obtenir un annulateur de $V(x_1, \dots, x_n)$ divisant le précédent.

Les équations de degré 3 et 4 selon Lagrange

Revenons à l'approche de Lagrange de la méthode de Cardan. L'ensemble

$$\{(X_1 + jX_2 + j^2X_3)^3, (X_1 + j^2X_2 + jX_3)^3\}$$

est une orbite pour l'action de \mathcal{S}_3 . Avec les notations de 1.2, on retrouve que y^3 et z^3 sont racines du polynôme du second degré $X^2 + 27qX - 27p^3$.

Passons à l'équation de degré 4. L'orbite de $X_1X_2 + X_3X_4$ pour l'action de \mathcal{S}_4 est

$$\{X_1X_2 + X_3X_4, X_1X_3 + X_2X_4, X_1X_4 + X_2X_3\}.$$

On considère toujours p, q, r dans \mathbb{C} et le polynôme :

$$X^4 + pX^2 + qX + r = \prod_{i=1}^4 (X - x_i).$$

Posons

$$R = (T - (x_1x_2 + x_3x_4)) (T - (x_1x_3 + x_2x_4)) (T - (x_1x_4 + x_2x_3)).$$

³⁹. Incidemment, Lagrange a établi que, si G_U désigne le stabilisateur de U , $|\omega(U)| |G_U| = n!$, en employant la méthode qui nous sert maintenant à établir que l'ordre d'un sous-groupe d'un groupe fini divise l'ordre du groupe. Jordan a énoncé le résultat général en le créditant à Lagrange, d'où la terminologie actuelle.

Un calcul laissé au lecteur (qui pourra noter que le coefficient le plus compliqué est déterminé dans l'exemple de 4.1) montre que

$$R = X^3 - pX^2 - 4rX + 4pr - q^2.$$

Pour montrer que l'équation de degré 4 est résoluble par radicaux, il suffit donc de voir que les x_i peuvent s'exprimer par radicaux à partir de

$$\alpha = x_1x_2 + x_3x_4, \quad \beta = x_1x_3 + x_2x_4, \quad \gamma = x_1x_4 + x_2x_3.$$

Or

$$(x_1 + x_3)(x_2 + x_4) = \alpha + \beta, \quad (x_1 + x_3) + (x_2 + x_4) = 0.$$

Il s'ensuit que $x_1 + x_3$ et $x_2 + x_4$ sont racines carrées de $-\alpha - \beta$. En procédant de manière analogue pour les autres sommes $x_i + x_j$, on arrive aux formules de Ferrari : l'équation de degré 4 est résoluble par radicaux.

Exercice 67. ④ *Expliciter les calculs.*

Le lien entre l'« équation générale » et le groupe symétrique

Soient X_1, \dots, X_n des indéterminées indépendantes sur le corps \mathbb{K} . Ce qui précède suggère la stratégie suivante pour résoudre par radicaux l'équation générale de degré n : chercher des éléments P dans $\mathbb{K}[X_1, \dots, X_n]$

- dont l'orbite sous l'action de \mathcal{S}_n soit de cardinal $< n$, pour que l'on puisse calculer ces éléments en résolvant des équations de degré $< n$;
- en nombre suffisant pour qu'ils permettent d'accéder aux racines de l'équation initiale.

Cette stratégie conduit à déterminer des sous-groupes stricts de \mathcal{S}_n d'indice strictement inférieur à n . Or, si $n \geq 5$, \mathcal{S}_n admet un seul sous groupe de ce type, le groupe alterné \mathcal{A}_n , ce qui conduit à penser que l'équation générale de degré n n'est pas résoluble par radicaux.

4.3 Discriminant

Le polynôme symétrique

$$\Delta = \prod_{1 \leq i < j \leq n} (X_j - X_i)^2$$

est appelé *discriminant*. Le théorème 8 fournit un polynôme D à n indéterminées à coefficients dans \mathbb{Z} tel que

$$\Delta = D(\Sigma_1, \dots, \Sigma_n).$$

Soient \mathbb{K} un corps, $P \in \mathbb{K}[X]$ unitaire de degré $n \geq 1$, Ω un surcorps de \mathbb{K} scindant P . On écrit

$$P = \prod_{i=1}^n (X - x_i) \quad \text{où} \quad (x_1, \dots, x_n) \in \Omega^n.$$

On pose alors

$$(1) \quad \Delta(P) = \Delta(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_j - x_i)^2 = D(\sigma_1, \dots, \sigma_n)$$

L'énoncé suivant résume les propriétés du discriminant.

Proposition 9. Soient \mathbb{K} un corps, $P \in \mathbb{K}[X]$ unitaire de degré $n \geq 1$, Ω un corps surcorps de \mathbb{K} scindant P :

$$P = \prod_{i=1}^n (X - x_i) \quad \text{où } (x_1, \dots, x_n) \in \Omega^n.$$

- On a

$$\Delta(P) = (-1)^{\frac{n(n-1)}{2}} \prod_{j=1}^n P'(x_j).$$

- Le polynôme P est séparable si et seulement si son discriminant est non nul.

- Soit \mathbb{A} un sous-anneau de \mathbb{K} . Si $P \in \mathbb{A}[X]$, $\Delta(P) \in \mathbb{A}$.

Preuve. Le premier point provient de la relation

$$\forall j \in \{1, \dots, n\}, \quad P'(x_j) = \prod_{\substack{1 \leq i \leq n \\ i \neq j}} (x_j - x_i).$$

Le deuxième point est évident, le dernier se déduit de la dernière égalité de (1).

Exemples

1. *Second degré*

Si $P = X^2 + bX + c$ avec $(b, c) \in \mathbb{K}^2$,

$$\Delta(P) = -(2x_1 + b)(2x_2 + b) = -4x_1x_2 - 2b(x_1 + x_2) - b^2 = b^2 - 4c.$$

2. *Troisième degré*

Si $P = X^3 + pX + q$ avec $(p, q) \in \mathbb{K}^2$, alors $\Delta(P)$ vaut

$$\prod_{i=1}^3 (3x_i^2 + p) = 27(x_1x_2x_3)^2 + 9p(x_1^2x_2^2 + x_2^2x_3^2 + x_3^2x_1^2) + 3p^2(x_1^2 + x_2^2 + x_3^2) + p^3.$$

On a

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1) = -2p.$$

En appliquant au polynôme symétrique $X_1^2X_2^2 + X_2^2X_3^2 + X_3^2X_1^2$ l'algorithme du paragraphe précédent, on arrive à l'expression aperçue dans l'exercice 4 de **1.1** et en **1.2** :

$$\Delta(P) = -4p^3 - 27q^2.$$

3. *Binômes*

Soit a un élément du corps \mathbb{K} . Supposons que la caractéristique de \mathbb{K} ne divise pas n , de sorte que $X^n - a$ est séparable. Soient α une racine de $X^n - a$ dans Ω . On a alors

$$(2) \quad \Delta(X^n - a) = (-1)^{\frac{n(n-1)}{2}} \prod_{\omega \in \mathbb{U}_n(\Omega)} (n \omega^{n-1} \alpha) = (-1)^{\frac{n(n-1)}{2}} n^n a.$$

Prenons $\mathbb{K} = \Omega = \mathbb{C}$, $n = p$ premier impair et $a = 1$. On déduit de (2) que tout corps contenant \mathbb{U}_p contient une racine carrée de $(-1)^{\frac{p(p-1)}{2}} p$. L'apparition de $\sqrt{5}$ dans $\cos\left(\frac{2\pi}{5}\right)$

(**1.1**), celle de $\sqrt{17}$ dans $\cos\left(\frac{2\pi}{17}\right)$ (**1.2**), sont ainsi justifiées. L'explication complète de la formule de Gauss donnant $\cos\left(\frac{2\pi}{17}\right)$ attendra le chapitre **5**.

4. Polynômes non unitaires

Supposons que $P \in \mathbb{K}[X]$ soit de degré $n \geq 1$, scindé sur le surcorps Ω de \mathbb{K} :

$$P = p_n \prod_{i=1}^n (X - x_i) \quad \text{où } (x_1, \dots, x_n) \in \Omega^n, \quad p_n \in \mathbb{K}^*.$$

On définit alors

$$\Delta(P) = p_n^{2n-2} \prod_{1 \leq i < j \leq n} (x_j - x_i)^2.$$

Cette normalisation est raisonnable pour raison d'homogénéité. On en donnera une meilleure explication en 4.4. Constat rassurant :

$$\forall (a, b, c) \in \mathbb{K}^* \times K \times \mathbb{K}, \quad \Delta(aX^2 + bx + c) = b^2 - 4ac.$$

Exercice 68. ① Ramener le calcul du discriminant d'un polynôme de degré n « général » à celui d'un polynôme de degré n sans terme en X^{n-1} .

Exercice 69. ③ Soient \mathbb{A} un sous-anneau de \mathbb{K} , U et V des éléments unitaires non constants de $\mathbb{A}[X]$. Montrer que $\Delta(UV)$ est divisible par $\Delta(U) \Delta(V)$.

Exercice 70. ③ Pour $n \in \mathbb{N}^*$, soit E_n l'élément $\sum_{k=0}^n \frac{X^k}{k!}$ de $\mathbb{C}[X]$. Calculer $\Delta(E_n)$.

Exercice 71. ④ Pour $n \in \mathbb{N}^*$, $a \in \mathbb{C}$, calculer $\Delta(X^n - X - a)$.

Exercice 72. ⑤ Soit $n \geq 3$ un entier. Démontrer la formule

$$\Delta(\Phi_n) = (-1)^{\frac{\varphi(n)}{2}} \frac{n^{\varphi(n)}}{\prod_{\substack{p \in \mathcal{P} \\ p|n}} p^{\frac{\varphi(n)}{p-1}}}.$$

Exercice 73. ③ a) Soit $P \in \mathbb{R}[X]$ séparable. Déterminer le signe de $\Delta(P)$ en fonction du nombre de paires de racines irrégulières de P .

b) Selon les valeurs de (p, q) de \mathbb{R}^2 , déterminer le nombre de racines réelles de $X^3 + pX + q$ (cf exercice 5, 1.1).

Exercice 74. ④ Soit $P \in \mathbb{Z}[X]$ unitaire de degré $n \geq 1$. On écrit

$$P = \prod_{i=1}^n (X - x_i) \quad \text{avec } (x_1, \dots, x_n) \in \mathbb{C}^n.$$

a) Montrer que $\prod_{1 \leq i < j \leq n} (x_i + x_j) \in \mathbb{Z}$.

b) Conclure que $\Delta(P)$ est congru à 0 ou 1 modulo 4.

Exercice 75. ③ Soient $P \in \mathbb{Z}[X]$ non constant et séparable. Décrire en utilisant $\Delta(P)$ l'ensemble des nombres premiers P tels que la réduction de P modulo p soit séparable. En déduire que, si P est séparable, l'ensemble des ombres premiers P tels que la réduction de P modulo p soit séparable est fini.

Exercice 76. ③ Soit \mathbb{A} un anneau intègre. Si $P \in \mathbb{A}[X_1, \dots, X_n]$, P est dit antisymétrique si

$$\forall \sigma \in \mathcal{S}_n, \quad \sigma.P = \varepsilon(\sigma) P.$$

On pose $\delta = \prod_{1 \leq i < j \leq n} (X_j - X_i)$. Montrer que les éléments antisymétriques de $\mathbb{A}[X_1, \dots, X_n]$ sont les δU où U est un polynôme symétrique. En déduire le degré minimal d'un polynôme homogène antisymétrique non nul.

Exercice 77. ② Soit \mathbb{A} un anneau intègre de caractéristique différente de 2. On se propose de décrire les $P \in \mathbb{A}[X_1, \dots, X_n]$ tels que

$$\forall \sigma \in \mathcal{A}_n, \quad \sigma.P = P.$$

Soient P un tel polynôme, $\tau = (1\ 2)$.

a) Vérifier que $P + \tau.P$ est symétrique, que $P - \tau.P$ s'écrit δQ où Q est symétrique.

b) En déduire que les polynômes recherchés sont les $U + \delta V$ où U et V sont des polynômes symétriques.

Exercice 78. ⑤ On reprend les notations de l'exercice 67 de 4.1. On note $\mathcal{P}^+(n)$ l'ensemble des $(\lambda_1, \dots, \lambda_n)$ de \mathbb{N}^n tels que $\lambda_1 > \lambda_2 > \dots > \lambda_n$.

a) Pour $\lambda \in \mathcal{P}^+(n)$, soit a_λ l'antisymétrisé de $X^\lambda : a_\lambda = \det(X_i^{\lambda_j})_{1 \leq i, j \leq n}$. Montrer que, si $d \in \mathbb{N}$, $(a_\lambda)_{\substack{\lambda \in \mathcal{P}^+(n) \\ |\lambda|=d}}$ est une \mathbb{A} -base du \mathbb{A} -module des polynômes antisymétriques homogènes de degré d de $\mathbb{A}[X_1, \dots, X_n]$.

b) Soit $\rho = (n-1, \dots, 1, 0)$. Expliciter a_ρ .

c) Si $\lambda \in \mathbb{N}^n$, montrer que $\lambda \in \mathcal{P}(n) \iff \lambda + \rho \in \mathcal{P}^+(n)$.

c) Montrer que, si $\lambda \in \mathcal{P}^+(n)$, a_λ est divisible par a_ρ dans $\mathbb{A}[X_1, \dots, X_n]$.

d) Soit $d \in \mathbb{N}$. Montrer que $\left(\frac{a_{\lambda+\rho}}{a_\rho} \right)_{\substack{\lambda \in \mathcal{P}(n) \\ |\lambda|=d}}$ est une \mathbb{A} -base du \mathbb{A} -module des polynômes symétriques homogènes de degré d de $\mathbb{A}[X_1, \dots, X_n]$.⁴⁰

4.4 (*) Résultant

Il peut sembler paradoxal de présenter le discriminant avant le résultant, dont il n'est qu'un cas particulier. La justification est que nous n'utiliserons le résultant que lors de remarques marginales, alors que le discriminant apparaîtra naturellement dans l'étude de l'action du groupe de Galois d'un polynôme sur les racines (chapitre 4). En fait, le choix de consacrer un paragraphe au résultant est en grande partie motivé par le rôle de cet outil dans l'algèbre « classique ».

Soient \mathbb{K} un corps, m et n deux éléments de \mathbb{N}^* , $P = \sum_{i=0}^m p_i X^i$ et $Q = \sum_{i=0}^n q_i X^i$ deux éléments de $\mathbb{K}[X]$, avec $\deg(P) \leq m$, $\deg(Q) \leq n$. Considérons :

- la base $\mathcal{B} = (X^{m+n-1}, X^{m+n-2}, \dots, 1)$ de $\mathbb{K}[X]$;

- la famille $\mathcal{F} = (X^{n-1}P, X^{n-2}P, \dots, XP, P, X^{m-1}Q, X^{m-2}Q, \dots, XQ, Q)$, constituée de $m+n$ éléments de $\mathbb{K}_{m+n-1}[X]$.

40. Les $\left(\frac{a_{\lambda+\rho}}{a_\rho} \right)$ pour $\lambda \in \mathcal{P}(n)$ sont les polynômes de Schur. Schur les a introduits dans sa thèse (1901) afin de décrire les caractères polynomiaux des groupes linéaires.

La matrice de présentation de \mathcal{F} dans \mathcal{B} est :

$$M_{m,n}(P, Q) = \begin{pmatrix} p_m & 0 & \cdots & \cdots & 0 & q_n & 0 & \cdots & 0 \\ p_{m-1} & p_m & \ddots & & \vdots & q_{n-1} & q_n & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & 0 \\ p_1 & & \ddots & \ddots & 0 & \vdots & & \ddots & q_n \\ p_0 & \ddots & & \ddots & p_m & q_1 & & & q_{n-1} \\ 0 & \ddots & \ddots & & p_{m-1} & q_0 & q_1 & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & p_1 & \vdots & \ddots & \ddots & q_1 \\ 0 & \cdots & \cdots & 0 & p_0 & 0 & \cdots & 0 & q_0 \end{pmatrix}$$

Les n premières colonnes contiennent les coefficients de P (et des zéros) ; les m dernières colonnes contiennent les éléments de Q (et des zéros). On note $\text{Res}_{m,n}(P, Q)$ l'élément de \mathbb{K} :

$$\text{Res}_{m,n}(P, Q) = \det(M_{m,n}(P, Q)).$$

Si P et Q sont de degrés respectifs m et n , le résultant de P et Q est

$$\text{Res}(P, Q) = \text{Res}_{m,n}(P, Q).$$

On remarquera que, si \mathbb{A} est un sous-anneau de \mathbb{K} et si P et Q sont dans $\mathbb{A}[X]$, $\text{Res}(P, Q)$ est un élément de \mathbb{A} .

Exercice 79. ① Calculer $\text{Res}(P, Q)$ si $(P, Q) = (X-a, X-b)$, puis si $(P, Q) = (X-a, X^2+bX+c)$.

Exercice 80. ② Relier $\text{Res}(P, Q)$ et $\text{Res}(Q, P)$.⁴¹

Proposition 10. Soient P et Q deux polynômes non constants de $\mathbb{K}[X]$. Alors P et Q sont premiers entre eux dans $\mathbb{K}[X]$ si et seulement si $\text{Res}(P, Q) \neq 0$.

Preuve. Soient m et n les degrés respectifs de P et Q . Dire que $\text{Res}_{m,n}(P, Q)$ est nul, c'est dire que les colonnes de $M_{m,n}(P, Q)$ sont liées, ou qu'il existe $U \in \mathbb{K}_{n-1}[X]$ et $V \in \mathbb{K}_{m-1}[X]$, non tous deux nuls, tels que $UP + VQ = 0$.

Si P et Q sont premiers entre eux dans $\mathbb{K}[X]$, le lemme de Gauss assure que, si $UP + VQ = 0$, U est divisible par Q et V par P , donc que U (resp. V) est nul ou de degré supérieur ou égal à n (resp. m). Il s'ensuit que $\text{Res}(P, Q) \neq 0$.

Sinon, on dispose de $D \in \mathbb{K}[X]$ de degré $d \geq 1$ divisant P et Q . Posons $U = \frac{Q}{D}$ et $V = -\frac{P}{D}$. Alors $U \in \mathbb{K}_{n-1}[X] \setminus \{0\}$, $V \in \mathbb{K}_{m-1}[X] \setminus \{0\}$, $UP + VQ = 0$. Par suite, $\text{Res}(P, Q) = 0$.

Exercice 81. ③ On munit $\mathbb{C}_m[X] \times \mathbb{C}_n[X]$ de sa topologie naturelle. Montrer que l'ensemble des couples (P, Q) de $\mathbb{C}_m[X] \times \mathbb{C}_n[X]$ tels que $\deg(P) = m$, $\deg(Q) = n$ et $P \wedge Q = 1$ est ouvert.

Exercice 82. ③ Soient P et Q deux éléments de $\mathbb{Z}[X]$ sans racine commune dans \mathbb{C} . Montrer que, si $p \in \mathcal{P}$ est assez grand, les réductions de P et Q modulo p sont premières entre elles.

41. La formule obtenue peut conduire, avec un peu de travail, à une preuve de la loi de réciprocité quadratique.

Exercice 83. (4) a) Soit $\Phi_{m,n}(P, Q)$ l'élément de $\mathcal{L}(\mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X], \mathbb{K}_{m+n-1}[X])$ défini par

$$\forall (U, V) \in \mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X], \quad \Phi_{m,n}(P, Q)(U, V) = UP + VQ.$$

Interpréter $M_{m,n}(P, Q)$ à l'aide de $\Phi_{m,n}(P, Q)$

b) On considère un sous-anneau \mathbb{A} un sous-anneau de \mathbb{K} , on suppose que P et Q sont dans $\mathbb{A}[X]$. Montrer que l'image de $\Phi_{m,n}(P, Q)$ contient $\text{Res}_{m,n}(P, Q) \mathbb{A}_{m+n-1}[X]$. En déduire qu'il existe U et V dans $\mathbb{A}[X]$, de degrés strictement inférieurs respectivement à n et m tels que

$$UP + VQ = \text{Res}_{m,n}(P, Q).$$

Nous allons préciser la proposition 10, en calculant $\text{Res}(P, Q)$ en fonction des factorisations de P et Q dans un surcorps de \mathbb{K} scindant ces deux polynômes. Cet énoncé admet plusieurs démonstrations. Nous utiliserons la réduction des matrices, précisément la notion de matrice compagnon et la possibilité de trigonaliser une matrice carrée de polynôme caractéristique scindé.

Théorème 9. Soient m et n dans \mathbb{N}^* , P et Q dans $\mathbb{K}[X]$ de degrés respectifs m et n , Ω un surcorps de \mathbb{K} scindant P et Q

$$P = p_m \prod_{i=1}^n (X - x_i) \quad Q = q_n \prod_{j=1}^n (X - y_j), \quad \text{où } (x_1, \dots, x_m, y_1, \dots, y_n) \in \Omega^{m+n}, (p_m, q_n) \in \mathbb{K}^2.$$

Alors

$$\text{Res}(P, Q) = p_m^n q_n^m \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} (x_i - y_j).$$

Preuve. Notons R_P l'endomorphisme de $\mathbb{K}[X]$ obtenu en associant à $U \in \mathbb{K}[X]$ le reste de sa division par P . La multilinéarité du déterminant fait que $R_{m,n}(P, Q)$ est le déterminant dans la base \mathcal{B} du système de vecteurs

$$(X^{n-1}P, X^{n-2}P, \dots, XP, P, R_P(X^{m-1}Q), R_P(X^{m-2}Q), \dots, R_P(XQ), R_P(Q)).$$

Par conséquent,

$$M_{m,n}(P, Q) = \begin{pmatrix} M' & 0 \\ M'' & N \end{pmatrix},$$

où $M' \in \mathcal{M}_n(\mathbb{K})$ est triangulaire inférieure, dont tous les termes diagonaux valent p_m , et où N est la matrice dans la base $(X^{m-1}, \dots, 1)$ de $\mathbb{K}_{m-1}[X]$ de l'endomorphisme $S_{m,P,Q}$ de $\mathbb{K}_{m-1}[X]$ défini par

$$\forall U \in \mathbb{K}_{m-1}[X], \quad S_{m,P,Q} = R_P(QU).$$

Mais on vérifie immédiatement que

$$S_{m,P,Q} = Q(S_{m,P,X}).$$

D'autre part, la matrice de $S_{m,P,X}$ dans la base canonique $(1, \dots, X^{m-1})$ de $\mathbb{K}_{m-1}[X]$ est la matrice compagnon de $\frac{P}{p_m}$, de polynôme caractéristique $\frac{P}{p_m}$ et donc semblable, sur Ω , à une matrice triangulaire supérieure dont les termes diagonaux sont x_1, \dots, x_m . Il en résulte que $S_{m,P,Q}$ est semblable sur Ω à une matrice triangulaire supérieure de termes diagonaux $Q(x_1), \dots, Q(x_m)$, puis que

$$\text{Res}(P, Q) = \det(M') \det(M'') = p_m^n \prod_{i=1}^n Q(x_i) = p_m^n q_n^m \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} (x_i - y_j).$$

Exercice 84. ③ Soient m et n dans \mathbb{N}^* , E un \mathbb{K} -espace vectoriel de dimension m , $u \in \mathcal{L}(E)$, $Q \in \mathbb{K}_{n-1}[X]$. Montrer que

$$\det(Q(u)) = \text{Res}(\chi_u, Q).$$

Remarques

1. Retour sur le discriminant

Supposons que $Q = P'$, donc que $m \geq 2$ et que $n = m - 1$. On a

$$\text{Res}(P, P') = p_m^{m-1} \prod_{i=1}^{m-1} P'(x_i) = p_m^{2m-2} (-1)^{\frac{m(m-1)}{2}} \prod_{1 \leq i < j \leq m} (x_i - x_j)^2 = (-1)^{\frac{m(m-1)}{2}} \Delta(P),$$

en tenant compte de la définition donnée dans l'exemple 4 de **4.3**.

2. Utilisation de l'anneau quotient $\mathbb{K}[X]/(Q)$

On peut écrire plus agréablement la démonstration du théorème 9 en voyant $S_{m,X,Q}$ comme la multiplication par X dans $\mathbb{K}[X]/(Q)$, ce qui rend apparent le fait que $S_{m,P,Q}$ n'est autre que $P(S_{m,X,Q})$.

4.5 (*) Les sommes de Newton

Reprenons les notations du paragraphe **4.1** :

$$P(T) = \prod_{i=1}^n (T - X_i) = T^n + \sum_{k=0}^{n-1} (-1)^k \Sigma_k T^k.$$

Pour $j \in \mathbb{N}^*$, soit

$$N_j = \sum_{i=1}^n X_i^j.$$

Les N_j sont des polynômes symétriques. On complète la définition en posant $N_0 = n$. En 1666, Newton a donné des relations de récurrence qui permettent d'exprimer les N_j en fonction des Σ_i . Dans ses *Meditationes Algebraicae* (1770), Waring a explicité N_j .⁴² Ces résultats, marginaux pour la théorie de Galois, mais emblématiques d'une époque de l'algèbre, font l'objet de ce paragraphe.

Exercice 85. ③ Montrer que le déterminant de la matrice $(N_{i+j-2})_{1 \leq i, j \leq n}$ est le discriminant Δ . On notera que Δ est le carré d'un déterminant de Vandermonde.

Les formules de Newton

Notons d'abord que, si $k \geq n$, alors

$$\forall i \in \{1, \dots, n\}, \quad X_i^k = \Sigma_1 X_i^{k-1} - \Sigma_2 X_i^{k-2} + \dots + (-1)^{n-1} \Sigma_n X_i^{k-n}.$$

En sommant sur $i \in \{1, \dots, n\}$, on obtient la première partie de l'énoncé suivant.

Proposition 11. Pour $k \geq n$,

$$N_k = \sum_{j=1}^n (-1)^{j-1} \Sigma_j N_{k-j}.$$

42. Les cas $k = 1, 2, 3, 4$ avaient été écrits dès 1629 par Girard.

On a également $N_1 = \Sigma_1$ et, pour $2 \leq k \leq n-1$:

$$N_k = \sum_{j=1}^{k-1} (-1)^{j-1} \Sigma_j N_{k-j} + (-1)^{k-1} k \Sigma_k.$$

Si la caractéristique de \mathbb{A} ne divise pas $n!$, N_1, \dots, N_n déterminent les Σ_k , donc P .

Fin de la preuve de la proposition 11. La dernière assertion est immédiate en raisonnant par récurrence sur k . Prouvons les relations pour $k \leq n-1$. On se ramène au cas $k = n$ par l'argument ci-après. Le polynôme

$$N_k - \left(\sum_{j=1}^{k-1} (-1)^{j-1} \Sigma_j N_{k-j} + (-1)^{k-1} k \Sigma_k \right)$$

est homogène de degré k . Il s'écrit donc $\sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha|=k}} c_\alpha X^\alpha$ où les c_α sont dans \mathbb{A} . D'après le cas $k = n$, ce polynôme est nul si on substitue 0 à $n-k$ des X_i . Ainsi

$$0 = P(X_1, \dots, X_k, 0, \dots, 0) = \sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha|=k, (\alpha_{k+1}, \dots, \alpha_n) \neq (0, \dots, 0)}} c_\alpha X_1^{\alpha_1} \dots X_k^{\alpha_k}.$$

Ainsi, dès que $\alpha_{k+1}, \dots, \alpha_n$ sont non tous nuls c_α est nul. Par symétrie, tous les c_α sont nuls.

Exercice 86. ② Soient $n \in \mathbb{N}^*$, \mathbb{K} un corps de caractéristique ne divisant pas $n!$, A et B dans $\mathcal{M}_n(\mathbb{K})$. Montrer que $\chi_A = \chi_B$ si et seulement si

$$\forall k \in \{1, \dots, n\}, \quad \text{tr}(A^k) = \text{tr}(B^k).$$

Les formules de Waring

Nous supposons ici que \mathbb{A} est intègre et utiliserons librement les anneaux de séries formelles et de fractions rationnelles. Il est en effet naturel d'accéder aux N_k via la série génératrice

$$\sum_{k=0}^{+\infty} N_k T^k = \sum_{i=1}^n \frac{1}{1 - X_i T} = \frac{P'(1/T)}{T P(1/T)}.$$

Introduisons le polynôme réciproque de P :

$$Q(T) = \prod_{i=1}^n (1 - X_i T) = T^n P(1/T) = 1 - \Sigma_1 T + \Sigma_2 T^2 + \dots + (-1)^n \Sigma_n T^n.$$

Alors

$$-\frac{Q'(T)}{Q(T)} = \sum_{j=1}^{+\infty} N_j T^j.$$

En identifiant, on retrouve les formules de Newton.

Supposons désormais l'anneau \mathbb{A} de caractéristique nulle. Nous allons calculer les N_k en intégrant formellement la relation précédente. Écrivons

$$\prod_{i=1}^n (1 - X_i Y) = 1 - \Sigma_1 Y + \Sigma_2 Y^2 + \dots + (-1)^n \Sigma_n Y^n.$$

Considérons la série formelle du logarithme

$$L(1 - T) = - \sum_{k=1}^{+\infty} \frac{T^k}{k}.$$

On montre que, si T et U sont deux indéterminées, on a l'égalité de séries formelles

$$L((1 - (T + U) + TU) = L(1 - T) + L(1 - U).$$

On en déduit

$$\sum_{i=1}^k L(1 - X_i Y) = L(1 - \Sigma_1 Y + \Sigma_2 Y^2 + \dots + (-1)^n \Sigma_n Y^n).$$

Le membre de gauche s'écrit $-\sum_{k=1}^{+\infty} \frac{N_k}{k} Y^k$. Le membre de droite n'est autre que

$$-\sum_{i=1}^{+\infty} \frac{1}{i} (-\Sigma_1 Y + \Sigma_2 Y^2 + \dots + (-1)^n \Sigma_n Y^n)^i.$$

En utilisant la formule du multinôme, on arrive au résultat suivant.

Proposition 12. *Avec les notations précédentes, on a*

$$N_k = k \sum_{\substack{(i_1, \dots, i_n) \in \mathbb{N}^n \\ \sum_{j=1}^n j i_j = k}} (-1)^{k-n} \frac{(i_1 + \dots + i_n - 1)!}{\prod_{j=1}^n i_j!} \prod_{j=1}^n \Sigma_j^{i_j}.$$

Terminons par le jeu de formules inverse de celui de la proposition 12, également dû à Waring.

Exercice 87. ④ a) *Montrer l'égalité de séries formelles*

$$1 + \sum_{k=1}^n (-1)^k \Sigma_k T^k = \exp \left(- \sum_{j=1}^{+\infty} \frac{N_j}{j} T^j \right).$$

b) *Si $k \in \{1, \dots, n\}$, exprimer Σ_k en fonction des N_i pour $1 \leq i \leq k$.*

5 (*) Appendice : le théorème de d'Alembert-Gauss

La construction la plus satisfaisante du corps \mathbb{C} des nombres complexes à partir du corps \mathbb{R} des nombres réels est sans doute celle de Cauchy, dans laquelle \mathbb{C} apparaît comme corps de rupture de $X^2 + 1$ sur \mathbb{R} . Nous la rappellerons dans le chapitre 2. Il est remarquable que l'adjonction à \mathbb{R} d'une racine carrée de -1 suffise pour obtenir un corps algébriquement clos. Ce résultat, conjecturé par Girard dès 1629, a fait l'objet de nombreuses tentatives de démonstration à partir du milieu du dix-huitième siècle : d'Alembert (1746), Euler, Lagrange, Laplace... Il semble que la première preuve complète remonte à Gauss (1799).⁴³

43. L'idée est d'établir, si $P \in \mathbb{C}[X]$ est non constant, que les deux « courbes » $\{(x, y) \in \mathbb{R}^2 ; \operatorname{Re}(P(x + iy)) = 0\}$ et $\{(x, y) \in \mathbb{R}^2 ; \operatorname{Im}(P(x + iy)) = 0\}$ se coupent. Gauss a en fait donné quatre démonstrations du résultat.

Théorème 10. *Le corps \mathbb{C} est algébriquement clos.*⁴⁴

Les constructions de \mathbb{R} à partir de \mathbb{Q} mettent l'accent sur la topologie (complétion) ou sur la relation d'ordre (sections commençantes, coupures). Il est donc naturel que les preuves les plus classiques du théorème 10 soient essentiellement topologiques (compacité, connexité, simple connexité, indice) et/ou analytiques (inversion locale, fonctions holomorphes, fonctions harmoniques). Les démonstrations plus algébriques ont la vertu de mettre en évidence celles des propriétés du corps ordonné \mathbb{R} qui sont réellement indispensables : existence de la racine carrée d'un nombre réel positif, d'une racine réelle pour un polynôme à coefficients réels de degré impair.

Cette section, qui est un exercice de style, ne sera pas utilisée dans la suite. On y propose huit démonstrations de nature topologique et/ou analytique, rangées par ordre de sophistication plus ou moins croissant. Elle contient également une démonstration nettement plus « algébrique », qui utilise de manière cruciale le théorème des polynômes symétriques. Nous indiquerons dans le chapitre 5 une dernière approche, fondée sur la théorie de Galois et les théorèmes de Sylow.⁴⁵

5.1 Démonstrations topologiques et/ou analytiques

Dans les démonstrations 1 à 6,

$$P = \sum_{k=0}^n a_k X^k$$

est un polynôme de $\mathbb{C}[X]$ de degré $n \geq 1$. On établit que P a une racine dans \mathbb{C} . Notons déjà que

$$|P(z)| \underset{|z| \rightarrow +\infty}{\sim} |a_n| |z|^n, \quad \text{d'où} \quad |P(z)| \underset{|z| \rightarrow +\infty}{\longrightarrow} +\infty.$$

En d'autres termes, P est une application propre de \mathbb{C} dans \mathbb{C} , ce qui signifie que l'image réciproque d'un compact de \mathbb{C} est un compact de \mathbb{C} . On en déduit aussitôt que $P(\mathbb{C})$ est fermé dans \mathbb{C} .

Preuve 1 : principe du minimum

Cette preuve, sans doute la plus élémentaire, suppose connue l'exponentielle complexe. L'idée de base remonte à d'Alembert.

Étape 1. La fonction $|P|$ atteint son minimum sur \mathbb{C} .

Puisque $|P(z)| \rightarrow +\infty$ quand $|z| \rightarrow +\infty$, la locale compacité de \mathbb{C} et la continuité de $|P|$ donnent le résultat.

Étape 2. Si $|P|$ atteint un minimum local en $z_0 \in \mathbb{C}$ alors $P(z_0) = 0$.

Supposons par l'absurde que $P(z_0) \neq 0$. Nous allons montrer, par un développement limité complexe, que, pour tout z situé sur une demi-droite bien choisie d'origine z_0 , distinct de z_0 et assez près de z_0 , on a $|P(z)| < |P(z_0)|$.

Posons $P(z_0) = a e^{i\alpha}$ avec $a \in \mathbb{R}^{+*}$ et $\alpha \in \mathbb{R}$. Puisque P n'est pas constant, la formule de Taylor entraîne que l'ensemble

$$E = \left\{ j \in \mathbb{N}^*, P^{(j)}(z_0) \neq 0 \right\}$$

44. Ce résultat est nommé « théorème de d'Alembert-Gauss » ou « théorème fondamental de l'algèbre ».

45. Il existe également des preuves fondées sur la géométrie riemannienne et des preuves probabilistes utilisant le mouvement brownien ! Mentionnons enfin l'existence de démonstrations « constructives », i.e. produisant à partir de $P \in \mathbb{C}[X]$ non constant une suite complexe convergeant vers une racine de P .

n'est pas vide. Notons $k = \min E$, $P^{(k)}(z_0) = k! b e^{i\beta}$ avec $b \in \mathbb{R}^{+*}$ et $\beta \in \mathbb{R}$. On a alors le développement limité complexe :

$$P(z_0 + h) \underset{h \rightarrow 0}{=} a e^{i\alpha} + b e^{i\beta} h^k + o(h^k).$$

On choisit alors h de manière à rendre l'argument de $b e^{i\beta} h^k$ égal à $\alpha + \pi$:

$$P\left(z_0 + t e^{i(\alpha+\pi-\beta)/k}\right) \underset{t \rightarrow 0^+}{=} e^{i\alpha} (a - b t^k) P + o(t^k),$$

d'où

$$\left| P\left(z_0 + t e^{i(\alpha+\pi-\beta)/k}\right) \right| \underset{t \rightarrow 0^+}{=} a - b t^k + o(t^k).$$

En particulier, pour $t > 0$ assez petit :

$$\left| P\left(z_0 + t e^{i(\alpha+\pi-\beta)/k}\right) \right| < a.$$

La seconde partie de la preuve s'étend aux fonctions holomorphes : si Ω est un ouvert connexe non vide de \mathbb{C} , f une fonction holomorphe non constante sur Ω , si $|f|$ atteint un minimum local en z_0 alors $f(z_0) = 0$. Ce résultat (principe du minimum) peut bien sûr se déduire du principe du maximum appliqué à $\frac{1}{f}$.

Exercice 88. ⑤ *Formuler cette preuve de manière à éviter l'exponentielle complexe.*

Preuve 2 : théorème de Liouville

Plusieurs démonstrations du théorème de d'Alembert-Gauss reposent sur les rudiments de la théorie des fonctions holomorphes ; c'est déjà, implicitement, le cas de la précédente. En voici une très rapide. Supposons par l'absurde que P ne s'annule pas sur \mathbb{C} . Alors $\frac{1}{P}$ est entière⁴⁶ et tend vers 0 à l'infini, donc est constante (théorème de Liouville) ; contradiction.

L'exercice ci-après suggère une variante un peu plus élémentaire de cet argument : comme la preuve 1, elle contourne la théorie de Cauchy.

Exercice 89. ③ *Déduire le théorème de d'Alembert-Gauss du principe du maximum pour les fractions rationnelles et de l'analyticité d'une fraction rationnelle.*

A contrario, l'exercice suivant propose une démonstration fondée sur une utilisation un peu plus sophistiquée de la théorie des fonctions holomorphes.

Exercice 90. ② *On rappelle qu'une fonction holomorphe non constante sur un ouvert connexe de \mathbb{C} y est ouverte. En déduire le théorème de d'Alembert-Gauss.*

Preuve 3 : inversion locale

L'application P est de classe C^1 sur \mathbb{C} , sa différentielle $dP(z)$ au point z de \mathbb{C} étant la multiplication par $P'(z)$. En particulier, l'ensemble des z de \mathbb{C} tels que $dP(z)$ ne soit pas inversible est l'ensemble des zéros de P' , donc fini. Le théorème résulte de la proposition ci-après.

46. C'est-à-dire développable en série entière sur \mathbb{C} . Cette assertion utilise la théorie de Cauchy .

Proposition 13. Soient n un entier ≥ 2 , E un \mathbb{R} -espace vectoriel de dimension n muni de son unique topologie d'espace normé, f une application de classe C^1 de E dans E . On suppose que :

i) l'application f est propre ;

ii) l'ensemble $C = \{x \in E ; df(x) \notin GL(E)\}$ est au plus dénombrable.

Alors $f(E) = E$.

Étape 1. L'ensemble $F = f(E)$ est un fermé d'intérieur non vide de E , dont la frontière est contenue dans $f(C)$, donc au plus dénombrable.

Puisque f est propre, F est fermé dans E . Si $x \in E \setminus C$, le théorème d'inversion locale donne un voisinage ouvert U (resp. V) de x (resp. $f(x)$) dans E tel que f induise un C^1 -difféomorphisme de U sur V ; en particulier $f(x)$ est dans l'intérieur de $f(E)$, d'où les propriétés désirées.

Étape 2. Si X est un fermé d'intérieur non vide de E distinct de E , la frontière de X n'est pas dénombrable.

Soient $e \in E \setminus X$, x un point intérieur à X , H un hyperplan affine passant par x et pas par e . Puisque $n \geq 2$, l'intersection I de H et de l'intérieur de X est infinie non dénombrable. Tout segment $[y, e]$ avec $y \in I$ coupe la frontière de X (« passage des douanes »). Pour $(y, y') \in I^2$, on a $[y, e] \cap [y', e] = \{e\}$. Le résultat suit.

Exercice 91. ① Cette proposition subsiste-t-elle en dimension 1 ?

Preuve 4 : indice

Indice d'un point par rapport à un lacet du plan.

Soient a et b dans \mathbb{R} avec $a < b$, $S = [a, b]$, γ un lacet plan de classe C^1 et de source S , i.e. une application de classe C^1 de S dans \mathbb{C} telle que $\gamma(a) = \gamma(b)$. Si $z_0 \in \mathbb{C} \setminus \gamma(S)$, on peut définir le nombre de tours orientés que fait γ autour de z_0 , ou *indice de γ par rapport à z_0* .

Formalisons. Si $\rho = |\gamma - z_0|$, alors $u = \frac{\gamma - z_0}{\rho}$ est une application de classe C^1 de S dans le cercle unité. L'ensemble $R(u)$ des applications θ de classe C^1 de S dans \mathbb{R} telles que $u = e^{i\theta}$ n'est pas vide, et deux éléments de $R(u)$ diffèrent d'une constante appartenant à $2\pi\mathbb{Z}$ (« théorème de relèvement C^1 »). Nous sommes conduits à définir l'indice $\text{Ind}_\gamma(z_0)$ de γ par rapport à z_0 en posant :

$$\forall \theta \in R(u), \quad \text{Ind}_\gamma(z_0) = \frac{1}{2\pi} (\theta(b) - \theta(a)).$$

Puisque $u(a) = u(b)$, cet indice appartient à \mathbb{Z} .⁴⁷

On peut alors donner la définition intégrale de l'indice. De $\gamma - z_0 = \rho e^{i\theta}$ on tire, par dérivation logarithmique :

$$\frac{\gamma'}{\gamma - z_0} = \frac{\rho'}{\rho} + i\theta'.$$

D'où, vu que $[\ln(\rho)]_a^b = 0$:

$$\text{Ind}_\gamma(z_0) = \frac{1}{2i\pi} \int_a^b \frac{\gamma'}{\gamma - z_0}.$$

Ceci nous suffira. Signalons néanmoins que la fonction qui à $z_0 \in \mathbb{C} \setminus \gamma(S)$ associe $\text{Ind}_\gamma(z_0)$ est continue et à valeurs dans \mathbb{Z} , donc constante sur chaque composante connexe de $\mathbb{C} \setminus \gamma(S)$, et tend vers 0 quand $|z_0| \rightarrow +\infty$, donc est nulle sur la composante non bornée de $\mathbb{C} \setminus \gamma(S)$.⁴⁸

47. Le théorème de relèvement continu montre que ce qui précède vaut si l'application γ est seulement continue.

48. Ces propriétés subsistent si γ est continue, au prix de preuves légèrement plus élaborées.

Retour aux polynômes. Supposons que P ne s'annule pas sur \mathbb{C} . Pour r dans \mathbb{R}^+ , soit :

$$\varphi(r) = \text{Ind}_{\gamma_r}(0) \quad \text{où} \quad \begin{array}{ccc} \gamma_r : [-\pi, \pi] & \rightarrow & \mathbb{C} \\ \theta & \mapsto & P(re^{i\theta}) \end{array} .$$

On a :

$$\varphi(r) = \frac{1}{2\pi} \int_{-\pi}^{\pi} r \frac{e^{i\theta} P'(re^{i\theta})}{P(re^{i\theta})} d\theta.$$

La fonction φ est continue sur \mathbb{R}^+ , à valeurs dans \mathbb{Z} et nulle en 0. De :

$$\frac{z P'(z)}{P(z)} \xrightarrow{|z| \rightarrow +\infty} n,$$

on déduit que $\varphi(r) \rightarrow n$ quand $r \rightarrow +\infty$. Contradiction.⁴⁹

Exercice 92. ③ Si f est une fonction méromorphe sur \mathbb{C} et si f ne s'annule pas sur le cercle de centre 0 et de rayon r , que vaut l'intégrale de $\frac{f'}{f}$ sur ce cercle parcouru une fois dans le sens direct ? En déduire le théorème 7.

L'indice déguise un argument de topologie algébrique, plus apparent dans l'énoncé ci-après.

Exercice 93. ④ Soient $r \in \mathbb{R}^{+*}$, $a \in \mathbb{C}^*$, $n \in \mathbb{N}^*$, f une application continue de \mathbb{C} dans \mathbb{C} telle que

$$\forall z \in \mathbb{C}, \quad |z| = r \implies |f(z) - az^n| < |az^n|.$$

Montrer que f a une racine de module strictement inférieur à r . On pourra utiliser la notion de degré d'une application continue d'un cercle dans \mathbb{C}^* .

Preuve 5 : formule de la moyenne pour les fonctions harmoniques

Rappelons les deux faits suivants.

- Si g est une fonction harmonique sur l'ouvert Ω de \mathbb{C} et si Ω contient la boule fermée de centre z_0 et de rayon r , alors :

$$g(z_0) = \frac{1}{2\pi} \int_{-\pi}^{\pi} g(z_0 + re^{it}) dt.$$

Ce résultat est la *formule de la moyenne pour les fonctions harmoniques*.

- Si f est une fonction holomorphe ne s'annulant pas sur l'ouvert Ω de \mathbb{C} , la fonction $\ln(|f|)$ est harmonique sur Ω .

Supposons que P ne s'annule pas sur \mathbb{C} . Grâce aux deux points précédents,

$$\forall r \in \mathbb{R}^{+*}, \quad \ln(|P(0)|) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \ln(|P(re^{it})|) dt.$$

Mais, à partir de l'équivalent à l'infini de $|P(z)|$ mentionné au début de la section 1, on montre facilement à la relation suivante, qui donne la contradiction désirée :

$$\frac{1}{2\pi} \int_{-\pi}^{\pi} \ln(|P(re^{it})|) dt \xrightarrow{r \rightarrow +\infty} +\infty.$$

⁴⁹. Cet argument admet des variantes : on peut ainsi déduire le théorème de d'Alembert-Gauss du théorème de Rouché ou du principe de l'argument.

Preuve 6 : théorème de Cauchy

Soient u et v dans \mathbb{R}^{+*} . Supposons que P ne s'annule pas sur \mathbb{C} . Soit Q le polynôme défini par

$$\forall z \in \mathbb{C}, \quad Q(z) = P(z) \overline{P(\bar{z})} = \left(\sum_{k=0}^n a_k z^k \right) \left(\sum_{k=0}^n \overline{a_k} z^k \right).$$

Alors Q appartient à $\mathbb{R}[X]$, est de degré $2n$, ne s'annule pas sur \mathbb{C} et vérifie

$$\forall x \in \mathbb{R}, \quad Q(x) > 0.$$

Soient u et v deux éléments de \mathbb{R}^{+*} . Nous allons appliquer le théorème de Cauchy à la fonction holomorphe $\frac{1}{Q}$ sur le rectangle limité par les segments

$$[-u, u], [u, u + iv], [u + iv, -u + iv], [-u + iv, -u].$$

Soit γ un lacet continu et de classe C^1 par morceaux paramétrant le bord de ce rectangle parcouru une fois dans le sens positif. Alors $\int_{\gamma} \frac{dz}{Q(z)} = 0$, c'est-à-dire

$$\int_{-u}^u \frac{dt}{Q(t)} + i \int_0^v \frac{dt}{Q(u + it)} + \int_u^{-u} \frac{dt}{Q(t + iv)} + i \int_v^0 \frac{dt}{Q(-u + it)} = 0.$$

Le polynôme Q est de degré $2n \geq 2$ et ne s'annule pas sur \mathbb{C} . Les intégrales

$$\int_{-\infty}^{+\infty} \frac{dt}{Q(t)} \quad \text{et} \quad \int_{-\infty}^{+\infty} \frac{dt}{Q(t + iv)}$$

convergent. De plus, par convergence uniforme,

$$\int_0^v \frac{dt}{Q(\pm u + it)} \xrightarrow{u \rightarrow +\infty} 0.$$

On en déduit la relation

$$\int_{-\infty}^{+\infty} \frac{dt}{Q(t)} = \int_{-\infty}^{+\infty} \frac{dt}{Q(t + iv)}.$$

On fait alors tendre vers v vers $+\infty$ pour obtenir, en laissant la justification simple au lecteur,

$$\int_{-\infty}^{+\infty} \frac{dt}{Q(t)} = 0.$$

On contredit ainsi la stricte positivité de Q sur \mathbb{R} .

Preuve 7 : fonctions implicites et discriminant

Fixons $n \geq 2$ entier, et supposons, en raisonnant par récurrence, que tout polynôme complexe de degré $n - 1$ est scindé sur \mathbb{C} . Notons \mathcal{U}_n l'ensemble des polynômes unitaires de degré n de $\mathbb{C}[X]$. Munissons cet ensemble de sa topologie usuelle. Notons \mathcal{S}_n (resp. \mathcal{M}_n) l'ensemble des P de \mathcal{U}_n scindés sur \mathbb{C} (resp. l'ensemble des P de \mathcal{U}_n admettant au moins une racine complexe de multiplicité supérieure ou égale à 2). Comme l'ensemble $\mathcal{S}'_n = \mathcal{S}_n \setminus \mathcal{M}_n$ n'est évidemment pas vide, les deux étapes suivantes entraînent que $\mathcal{U}_n = \mathcal{S}_n$.

Étape 1. L'ensemble $\mathcal{U}_n \setminus \mathcal{M}_n$ est connexe par arcs, donc connexe.

Notons $\Delta(P)$ le discriminant d'un élément P de \mathcal{U}_n . Si $P \in \mathcal{U}_n$, P' est scindé sur \mathbb{C} . Il s'ensuit que \mathcal{M}_n est l'ensemble des P de \mathcal{U}_n tel que $\Delta(P) = 0$. Si on identifie \mathcal{U}_n à \mathbb{C}^n via l'application

$$X^n + \sum_{k=0}^{n-1} a_k X^k \longmapsto (a_0, \dots, a_{n-1}),$$

l'ensemble \mathcal{M}_n devient une hypersurface algébrique de \mathbb{C}^n , c'est-à-dire l'ensemble des zéros d'un élément de $\mathbb{C}[X_1, \dots, X_n]$. On conclut par le lemme suivant.

Lemme 13. *Soient R un élément non nul de $\mathbb{C}[X_1, \dots, X_n] \setminus \{0\}$,*

$$V_R = \{(x_1, \dots, x_n) \in \mathbb{C}^n ; R(x_1, \dots, x_n) = 0\}.$$

Alors $\mathbb{C}^n \setminus V_R$ est une partie connexe par arcs de \mathbb{C}^n .

Preuve. Soient x et y dans $\mathbb{C}^n \setminus V_D$. En posant

$$\forall t \in \mathbb{C}, \quad G(t) = R((1-t)x + ty),$$

on définit une fonction polynomiale qui ne s'annule pas en 0 et 1 ; l'ensemble des $t \in \mathbb{C}$ qui annulent G est donc fini, en particulier de complémentaire dans \mathbb{C} connexe par arcs, d'où le résultat.

Étape 2. L'ensemble \mathcal{S}'_n est un ouvert fermé de $\mathcal{U}_n \setminus \mathcal{M}_n$.

Notons que \mathcal{S}'_n est l'ensemble des P de \mathcal{U}_n simplement scindés sur \mathbb{C} .

Ouvert. Il suffit d'établir que \mathcal{S}'_n est ouvert dans \mathcal{U}_n . On utilise le lemme ci-après.

Lemme 14. *Soient $P \in \mathcal{U}_n$, $z \in \mathbb{C}$ une racine simple de P , V un voisinage de z dans \mathbb{C} . Alors tout Q de \mathcal{U}_n suffisamment proche de P a une racine dans V .*

Preuve. Soit Φ l'application de $\mathbb{C}_n[X] \times \mathbb{C}$ dans \mathbb{C} définie par

$$\forall (Q, z) \in \mathbb{C}_n[X] \times \mathbb{C}, \quad \Phi(Q, z) = Q(z).$$

L'application Φ est de classe C^1 (au sens complexe) et

$$\forall (Q, z) \in \mathbb{C}_n[X] \times \mathbb{C}, \quad \partial_2 \Phi(Q, z) = Q'(z).$$

En appliquant le théorème des fonctions implicites à Φ au point (P, z) , on obtient le résultat.

Soient $P \in \mathcal{S}'_n$, z_1, \dots, z_n ses racines (dans \mathbb{C}). Choisissons, pour $1 \leq i \leq n$, un voisinage V_i de z_i dans \mathbb{C} , de sorte que V_1, \dots, V_n soient deux à deux disjoints. Si $Q \in \mathcal{U}_n$ est suffisamment proche de P , il a une racine dans chaque V_i , donc n racines complexes distinctes : $Q \in \mathcal{S}'_n$.

Fermé. Il suffit d'établir que \mathcal{S}_n est fermé dans \mathcal{U}_n . Soit $(P_k)_{k \geq 1}$ une suite d'éléments de \mathcal{S}_n convergeant vers $P \in \mathcal{U}_n$. Pour $k \geq 1$, écrivons

$$P_k = \prod_{i=1}^n (X - z_{i,k}) \quad \text{avec} \quad (z_{1,k}, \dots, z_{n,k}) \in \mathbb{C}^n.$$

Grâce au lemme 4 (2.4), $(z_{1,k}, \dots, z_{n,k})_{k \geq 1}$ est une suite bornée de \mathbb{C}^n , et admet donc une valeur d'adhérence $(z_1, \dots, z_n) \in \mathbb{C}^n$. On en déduit que

$$P = \prod_{i=1}^n (X - z_i) \in \mathcal{S}_n.$$

Preuve 8 : inversion locale et revêtements

Cette preuve anticipe sur le chapitre 2 par l'usage de la notion d'extension. Puisque tout élément de \mathbb{R}^+ a une racine carrée dans \mathbb{R} , toute extension quadratique de \mathbb{R} est isomorphe à \mathbb{C} . Il suffit donc de démontrer la :

Proposition 14. *Soit \mathbb{A} une \mathbb{R} -algèbre commutative de dimension finie $n \geq 3$. Alors \mathbb{A} ne peut être un corps.*

Preuve. Munissons \mathbb{A} de sa topologie d'espace normé et considérons :

$$q : \mathbb{A} \setminus \{0\} \rightarrow \mathbb{A} \setminus \{0\} \\ x \mapsto x^2$$

L'application q est de classe C^1 . Sa différentielle en $x \in \mathbb{A} \setminus \{0\}$ est la multiplication par $2x$; l'application q induit donc un C^∞ -difféomorphisme d'un voisinage de x sur un voisinage de x^2 .

Supposons que \mathbb{A} est un corps. Alors

$$x^2 = y^2 \iff x = \pm y$$

par suite, $(\mathbb{A} \setminus \{0\}, q)$ est un revêtement à deux feuillets de $\mathbb{A} \setminus \{0\}$. Or, la condition $n \geq 3$ implique que $\mathbb{A} \setminus \{0\}$ est simplement connexe, donc que tout revêtement de $\mathbb{A} \setminus \{0\}$ est trivial; contradiction.

Cette démonstration s'applique verbatim à une algèbre de Banach de dimension infinie. On obtient ainsi un résultat fondamental de la théorie des algèbres de Banach, le *théorème de Gelfand-Mazur*.⁵⁰

Théorème 11. *Une \mathbb{R} -algèbre de Banach qui est un corps est isomorphe à \mathbb{R} ou à \mathbb{C} .*

Exercice 94. ④ *Soit A une C -algèbre de Banach complexe. Si $a \in A$, on note $\sigma(a)$ le spectre de a , i.e. des $\lambda \in \mathbb{C}$ tels que $a - \lambda 1_A$ soit non inversible.*

a) *En raisonnant par l'absurde et en utilisant la fonction qui à $\lambda \in \mathbb{C}$ associe $(a - \lambda 1_A)^{-1}$, montrer que, pour tout $a \in A$, $\sigma(a)$ est non vide.*

b) *Retrouver, à partir de la question a), le cas complexe du théorème de Gelfand-Mazur.*

5.2 Démonstration par les fonctions symétriques

Cette dernière démonstration remonte à Laplace (1795). Laplace utilise sans justification qu'un polynôme complexe a des racines « quelque part », i.e. le théorème 1 de 2.2, que nous établirons dans le chapitre 2; à ce point près, sa démonstration est complète.

a) Il suffit d'établir que tout polynôme non constant de $\mathbb{R}[X]$ a une racine dans \mathbb{C} . En effet, si $P = \sum_{k=0}^n a_k X^k$ est un polynôme de degré $n \geq 1$ de $\mathbb{C}[X]$, et si $\bar{P} = \sum_{k=0}^n \bar{a}_k X^k$, $Q = P\bar{P}$ est un polynôme de degré $2n$ de $\mathbb{R}[X]$. De plus, si $z \in \mathbb{C}$ est une racine de Q , z ou \bar{z} est racine de P .

b) Démontrons par récurrence l'assertion \mathcal{A}_m suivante : « si P est un polynôme de $\mathbb{R}[X]$ de degré $2^m q$ où q est impair, alors P a une racine dans \mathbb{C} . »

⁵⁰. Mazur (1938); mais c'est surtout Gelfand qui, dans son article de 1941, « Normierte Ringe », a montré le parti que l'on pouvait tirer de ce résultat.

Le cas $m = 0$ provient du théorème des valeurs intermédiaires, car alors

$$a_n P(x) \xrightarrow{x \rightarrow +\infty} +\infty, \quad a_n P(x) \xrightarrow{x \rightarrow +\infty} -\infty.$$

Supposons \mathcal{A}_m établie. Soient $P \in \mathbb{R}[X]$ unitaire de degré $n = 2^{m+1}q$ avec q impair, \mathbb{K} un surcorps de \mathbb{C} sur lequel P est scindé, et x_1, \dots, x_n dans \mathbb{K} tels que :

$$P = \prod_{i=1}^n (X - x_i).$$

Montrons qu'un des x_i est dans \mathbb{C} . À cet effet considérons, pour $c \in \mathbb{R}$, le polynôme :

$$P_c = \prod_{1 \leq i < j \leq n} (X - (x_i + x_j + c x_i x_j)).$$

Si $\sigma \in \mathcal{S}_n$, σ induit une permutation de l'ensemble des parties à deux éléments de $\{1, \dots, n\}$. Par conséquent :

$$P_c = \prod_{1 \leq i < j \leq n} (X - (x_{\sigma(i)} + x_{\sigma(j)} + c x_{\sigma(i)} x_{\sigma(j)})).$$

Chaque coefficient de P_c est ainsi de la forme $U(x_1, \dots, x_n)$ où U est un polynôme symétrique de $\mathbb{R}[X_1, \dots, X_n]$; le corollaire 3 de 4.1 entraîne que P_c est à coefficients dans \mathbb{R} . De plus, le degré $\frac{n(n-1)}{2}$ de P_c est de la forme $2^m q'$ avec q' impair. Grâce à \mathcal{A}_m , P_c a une racine dans \mathbb{C} : il existe deux éléments distincts i_c et j_c de $\{1, \dots, n\}$ tels que

$$x_{i_c} + x_{j_c} + c x_{i_c} x_{j_c} \in \mathbb{C}.$$

Comme \mathbb{R} est infini, on dispose de deux nombres réels distincts c et c' tels que

$$(i_c, j_c) = (i_{c'}, j_{c'}).$$

Soient $(i, j) = (i_c, j_c) = (i_{c'}, j_{c'})$, $s = x_i + x_j$ et $p = x_i x_j$. Alors, s et p sont dans \mathbb{C} , de sorte que x_i et x_j sont racines du trinôme du second degré complexe $X^2 - sX + p$. Il s'ensuit que x_i et x_j sont dans \mathbb{C} (résolution d'une équation du second degré à coefficients complexes) : le polynôme P a une racine complexe.